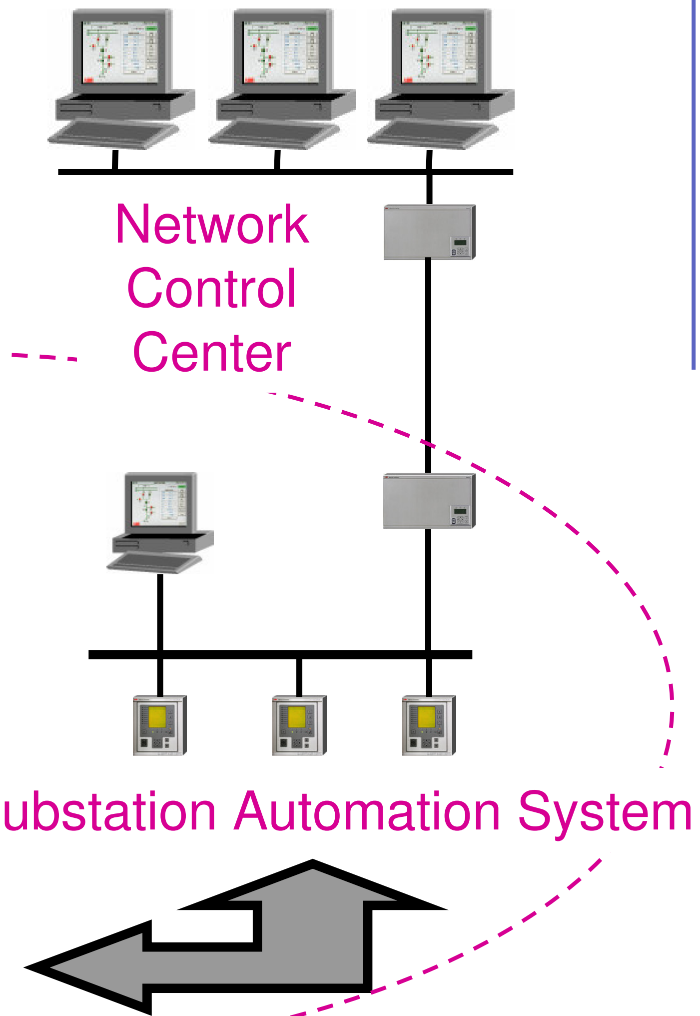
Substation Automation

SA as process interface for network control

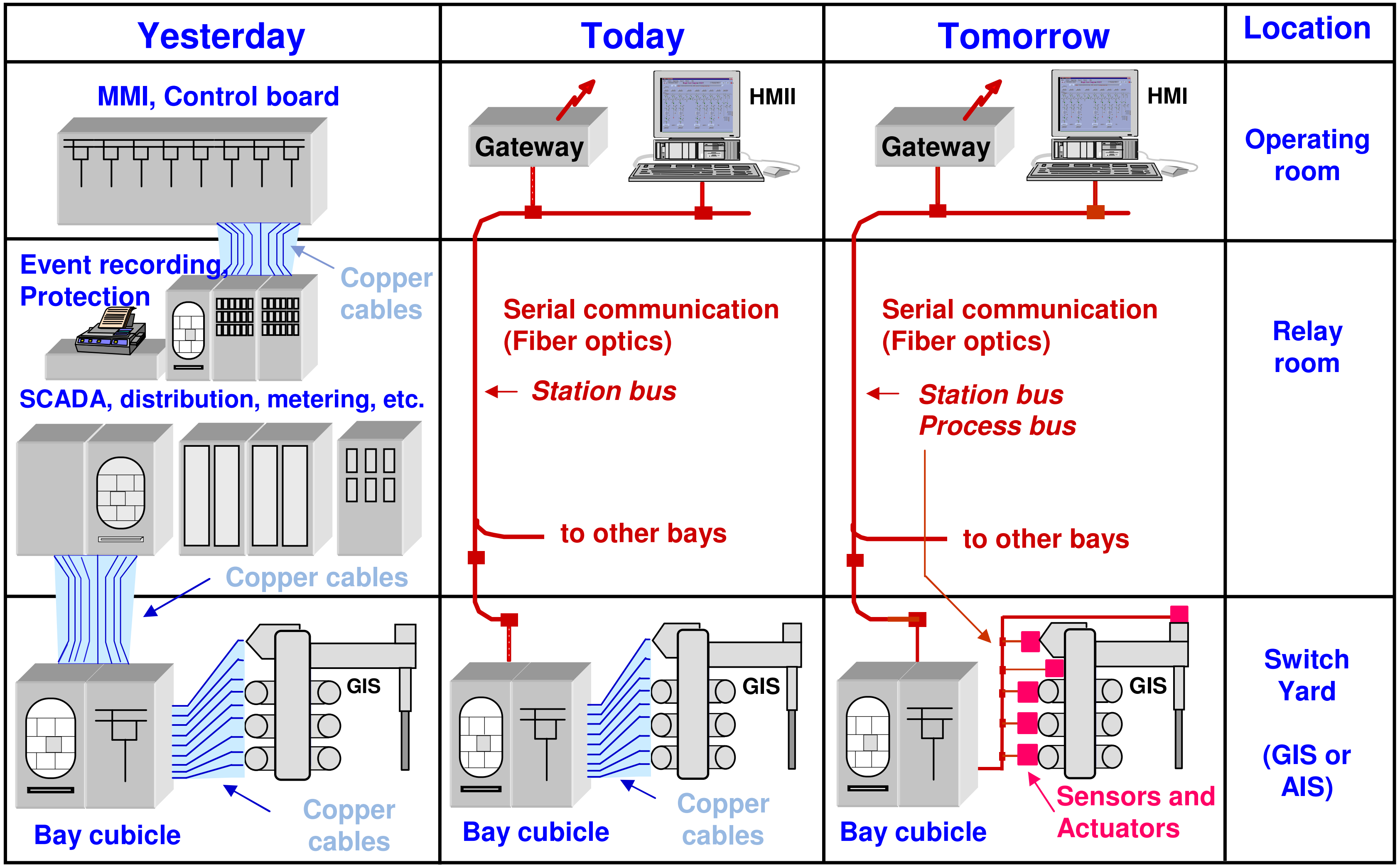
All information from process (Power System) are acquired by the Substation Automation system*

All actions on the process (Power System) are performed by the Substation Automation System*

*) protection integral part of SA

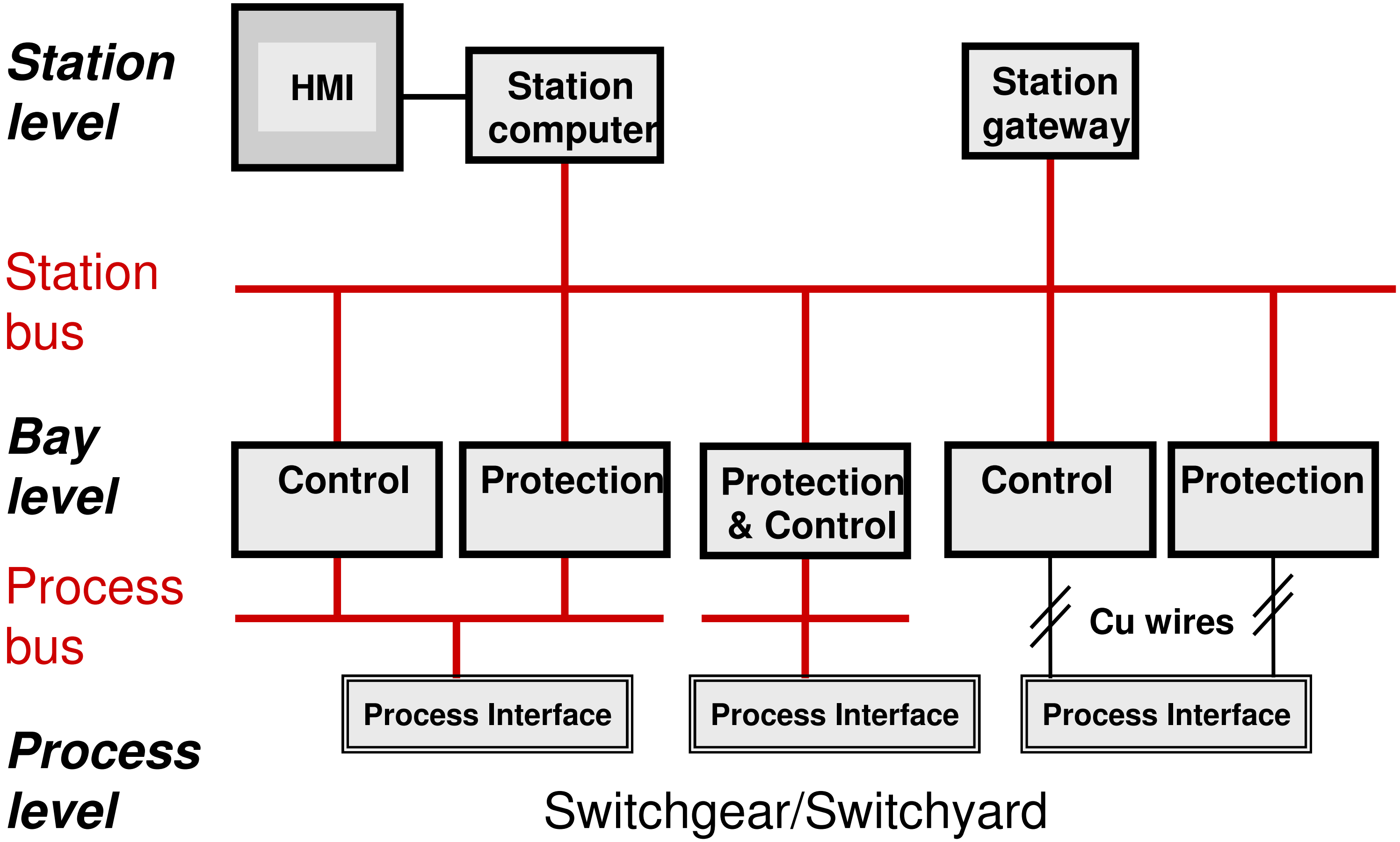


Trends in Substation Automation (SA)

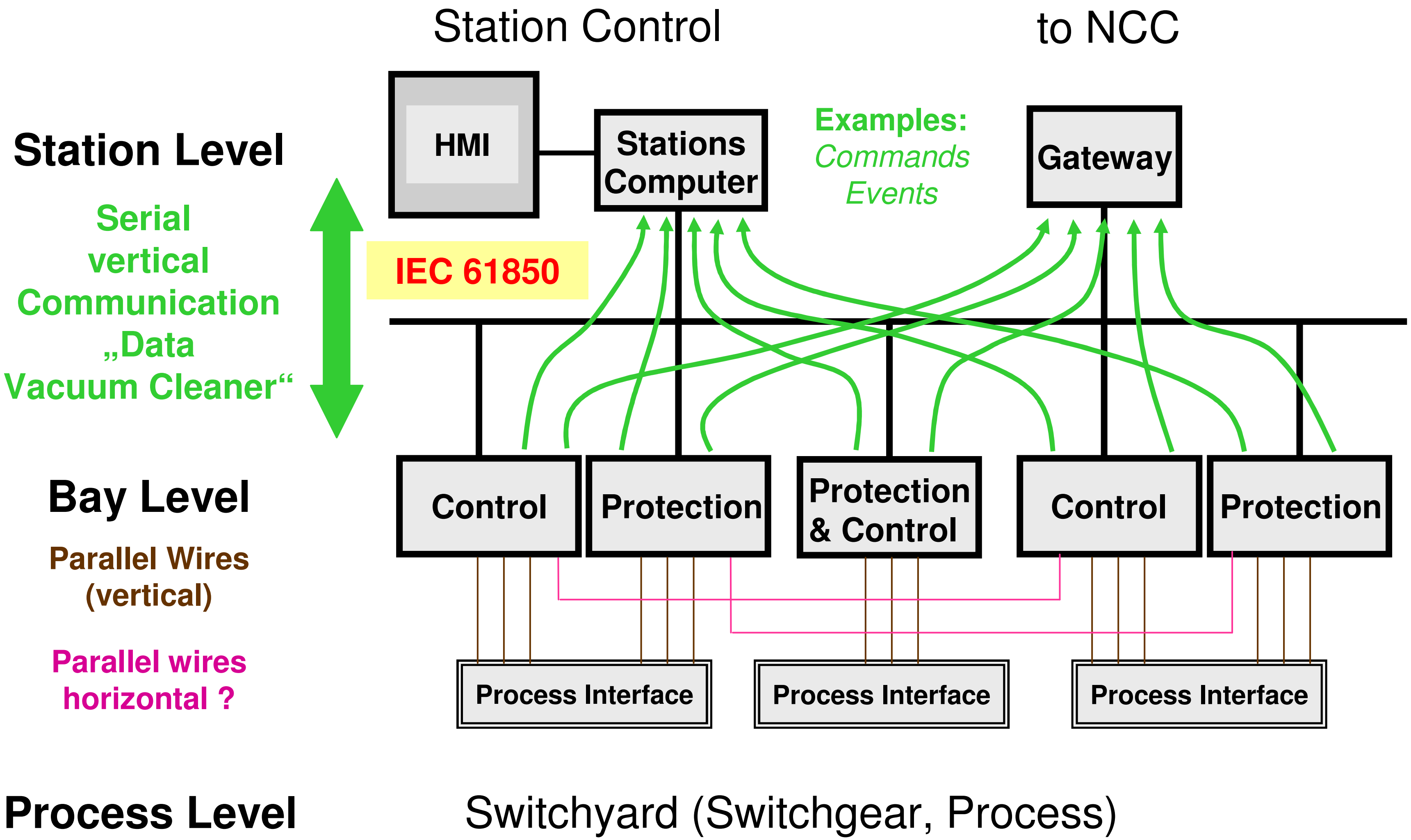


Functionality: ***SA to control,operate, monitor, and protect the substation***

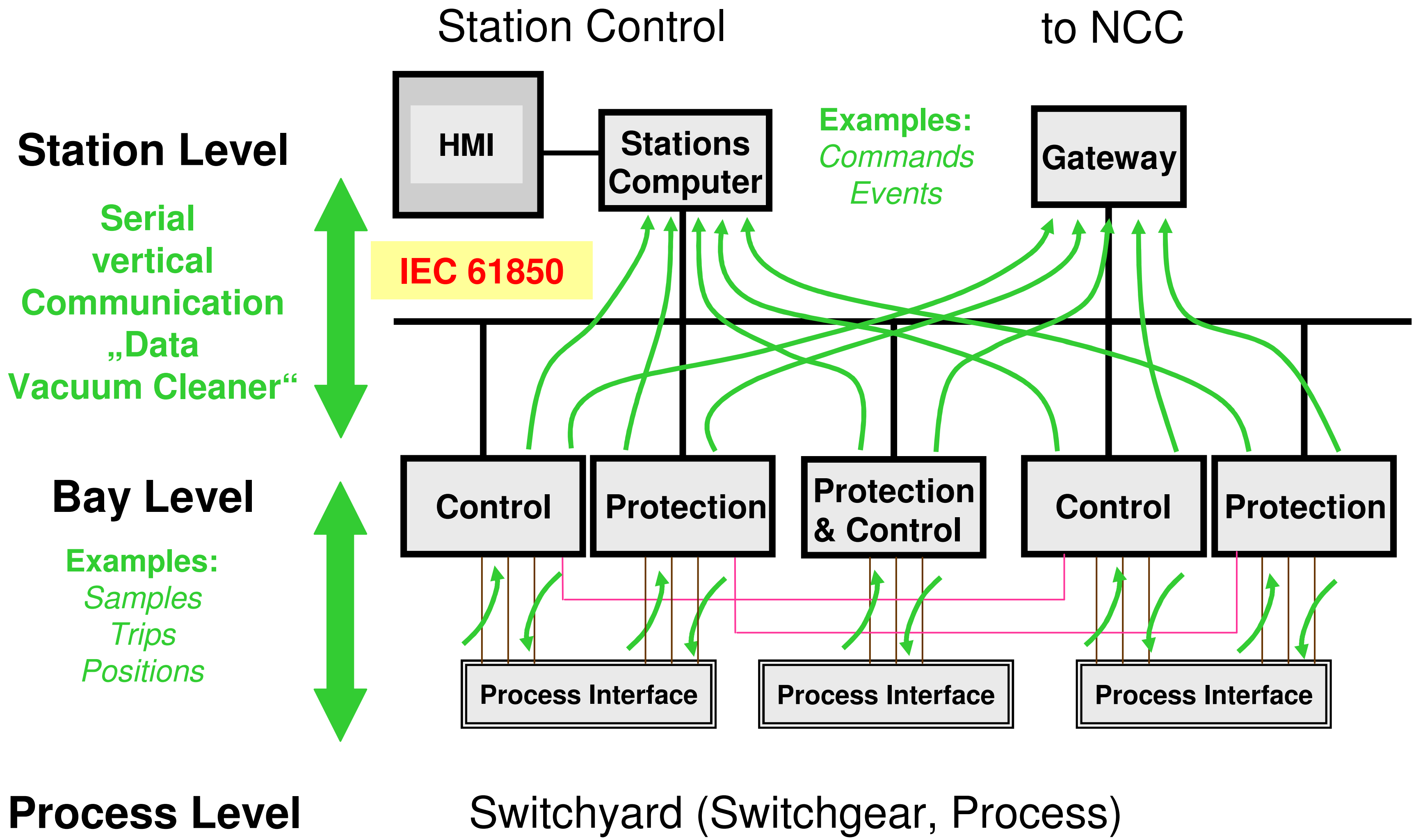
Serial communication in SA



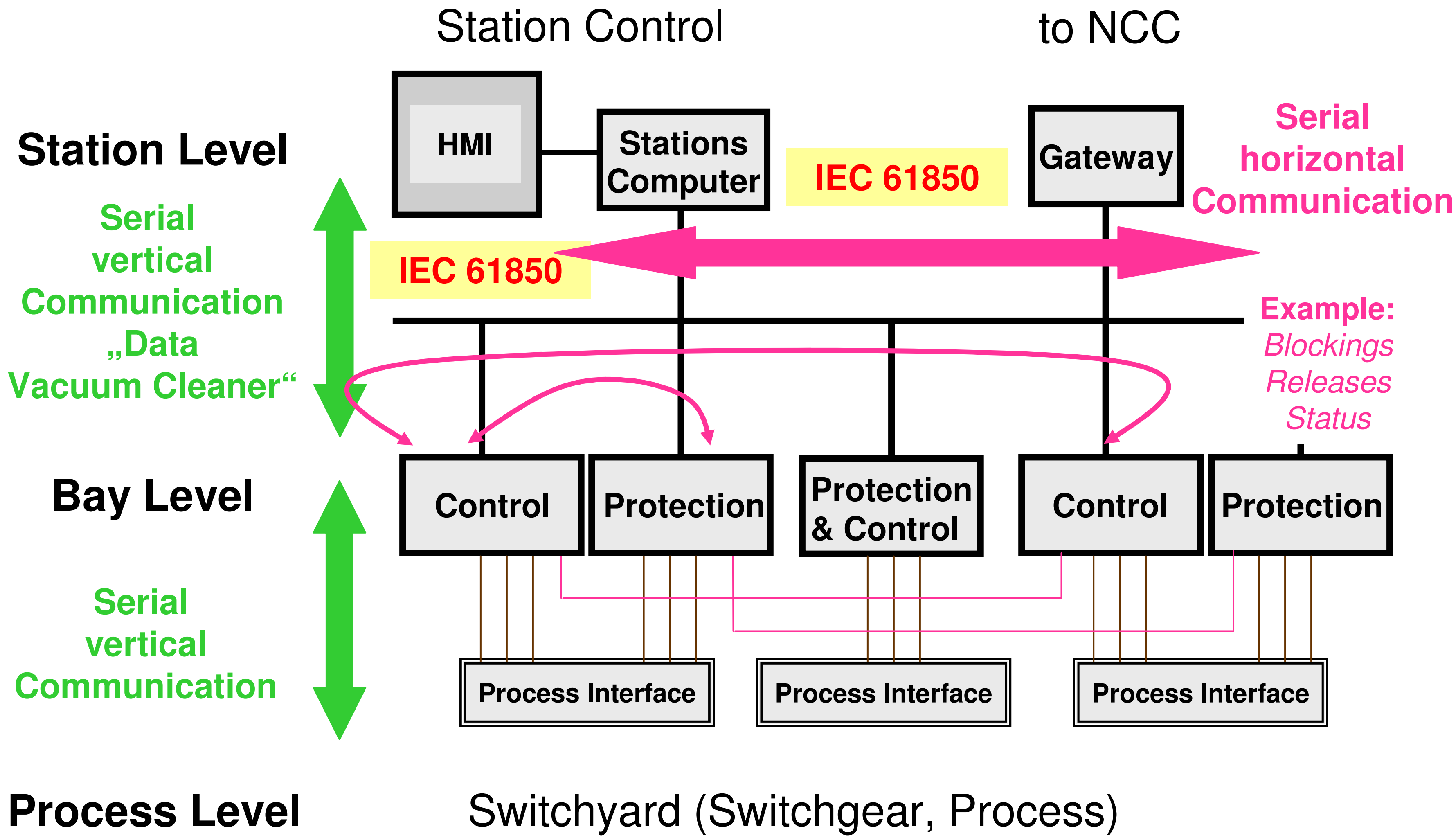
Vertical Communication



Vertical Communication



Vertical Communication



Function in SA (1) – *Headlines from IEC*

- **HMI and related station level functions**
  - Access control & access security management
  - Operators access to the system
  - Display of data and information
  - Storage of data in the station computer
  - Log management
- **Operational or control functions**
  - Operational control (switching devices, …)
  - Indication handling
  - Event (SER) and alarm handling
  - Parameter setting and parameter set switching
  - Data retrieval
- **Monitoring and metering functions**
  - Metering
  - Power equipment and system monitoring
  - Disturbance recording

Function in SA (2) – *Headlines from IEC*

- **Local process automation functions**
  - Protection
  - Automatics
  - Bay interlocking
- **Distributed automatic support functions**
  - Station interlocking
  - Distributed synchrocheck
  - Synchronized switching
  - Automatic switching sequences
  - Load shedding and restoration
- **System support functions**
  - System supervision
  - Configuration management
  - Time synchronization (tagging of events 1 ms, phasors 1µs)
  - Communication

Basics of Market Requirements

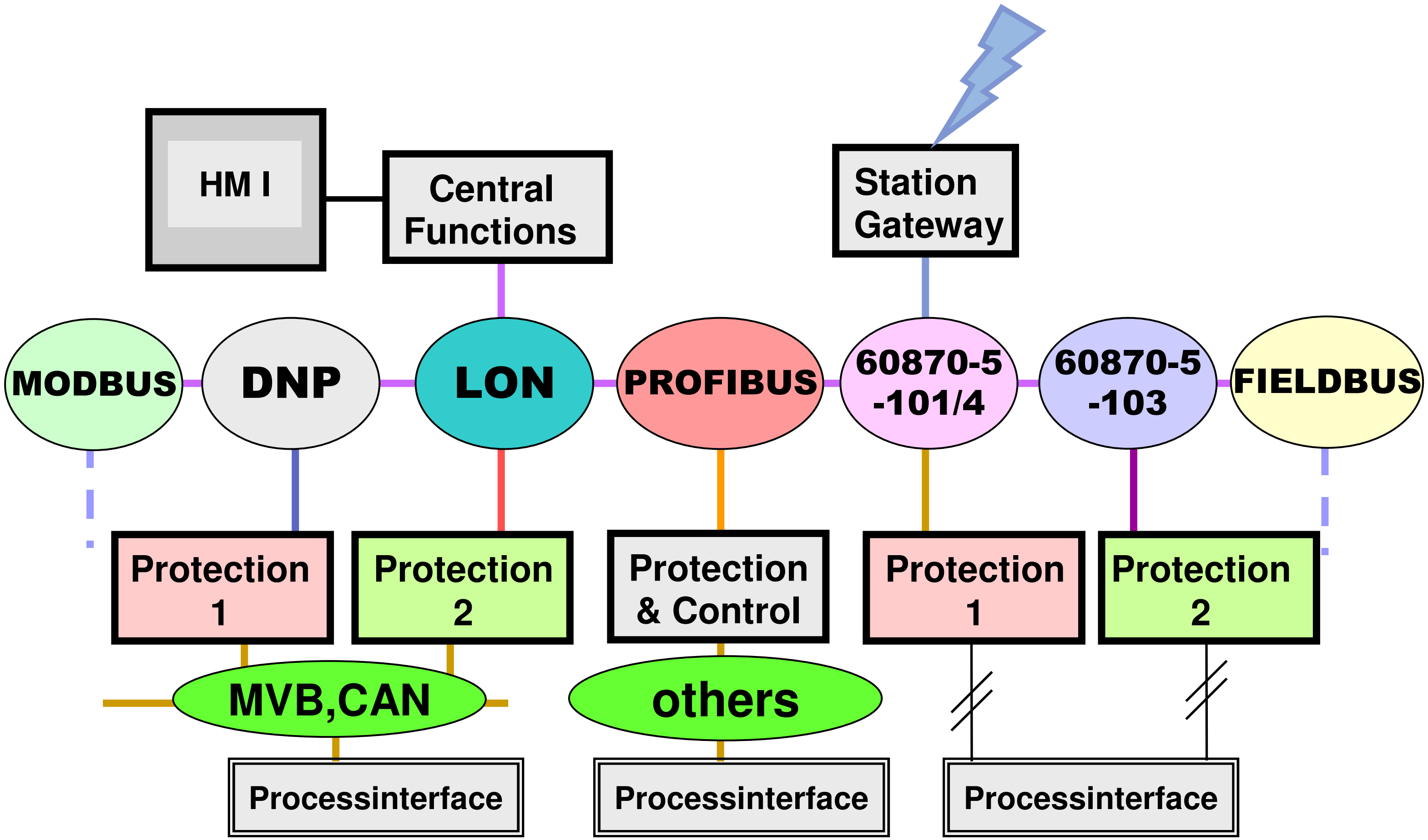
- Substation Automation (SA) Systems with IEDs (intelligent electronic devices) with serial communication have been now very well accepted on the market (some 4000 systems worldwide)

- Numerical devices with serial communication from different suppliers cannot be combined in a system as in the old hardwired systems because of a missing standard (only with an uneconomic effort)

- The global, highly competitive market requests a standard for
  - competitive performance
  - cost reduction

- Both providers and utilities are global companies and request such an integration or have to perform such integrations

One global standard instead of proprietary ones

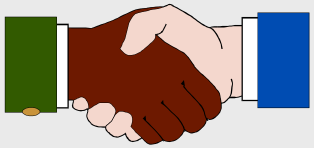


Details of Market Requirements

- **The global market**
  - needs a global standard
  - means a standard supporting all design & operation philosophies
- **Mixing of devices**
  - at least like with copper cables
- **Cost reduction**
  - by competition
  - by more intelligent functions
- **Cost reduction**
  - for investments
  - operation and maintenance
- **Open, future-proof standard**
  - for safe-guarding of investments
  - regarding suppliers and improving technology
  - for future extensions by bays or functions

Requirements for Standard in SA

Interoperability

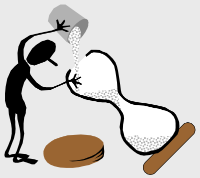


The ability for IED's from one or several manufacturer to exchange information and use the information for the their own functions.

Free configuration

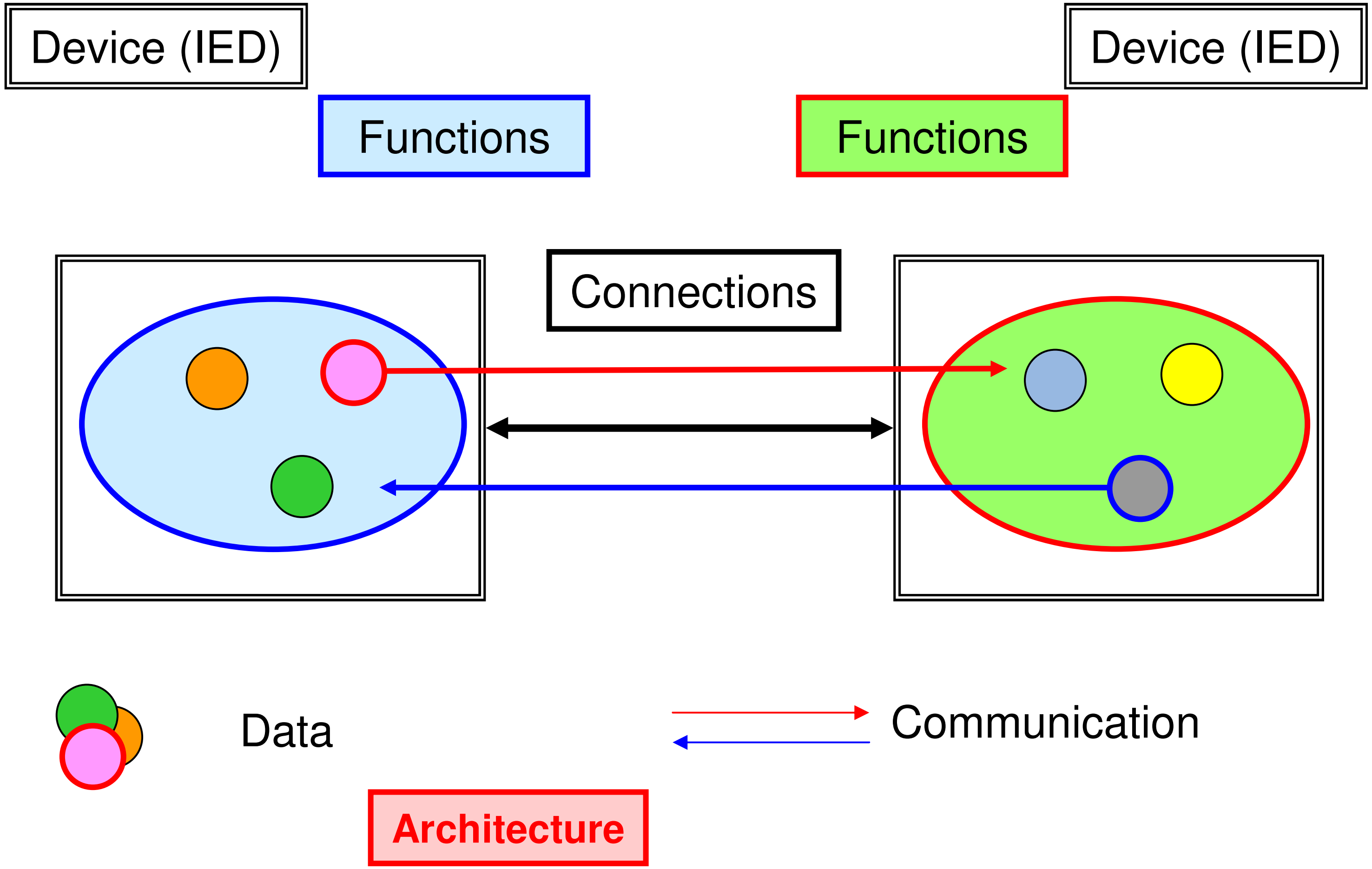
The standard shall support different philosophies and allow a free allocation of functions e.g. it must work equally well for centralized (RTU like) or decentralized (SCS like) systems.

Long term stability



The standard shall be future proof, i.e. it must be able to follow the progress in communication technology as well as evolving system requirements.

Elements of Substation Automation

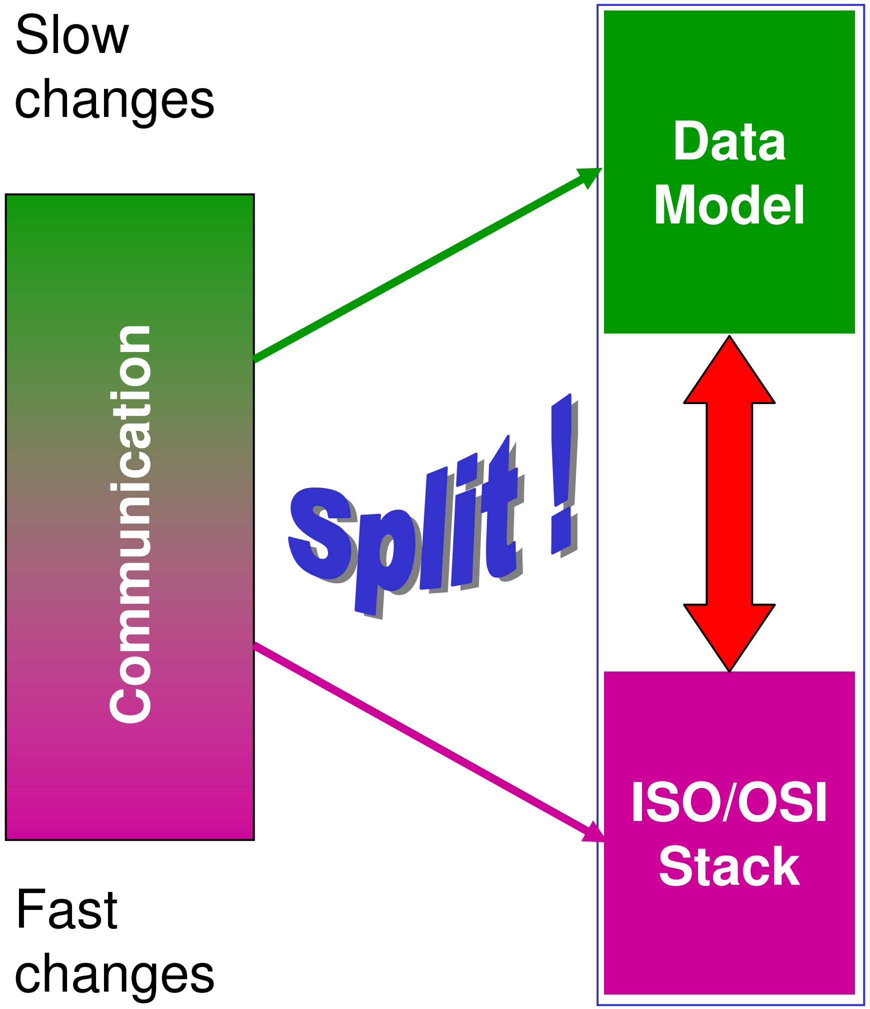


What shall be standardized?

Split in Data Model and Stack

Domain Substation :
What data have to be communicated ?

Communication Technology:
How are the data communicated ?



DEFINITION
Data and Services according to the Domain Substation

MAPPING
Data Model to the Communication Stack

SELECTION
ISO/OSI Stack from the Main Stream

IEC 61850

Communication Networks and Systems in Substations

14 parts: IEC 61850-x-y

Structure of IEC 61850 (14 parts)

System Aspects

Part 1:	Introduction and Overview
Part 2:	Glossary
Part 3:	General Requirements
Part 4:	System and Project Management
Part 5:	Comm. Requirements for Functions and Device Models

Configuration

Part 6:	Configuration description Language for Communication in electrical Substations related IEDs

Testing

Part 10:	Conformance Testing

Data Models

Part 7-4:	Compatible Logical Node Classes and Data Classes
Part 7-3:	Common Data Classes

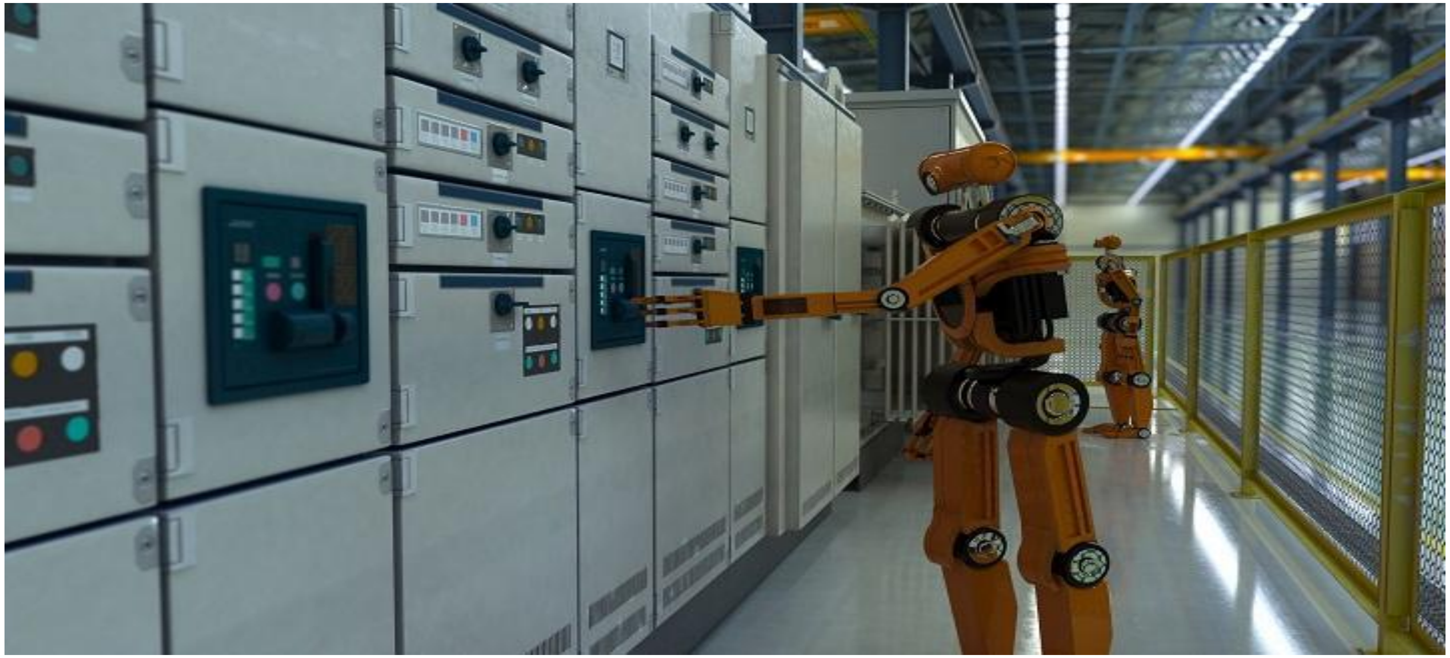
Abstract Communication Services

Part 7-2:	Abstract Communication Services (ACSI)
Part 7-1:	Principles and Models

Mapping to real Comm. Networks (SCSM)

Part 8-1:	Mapping to MMS and to ISO/IEC 8802-3
Part 9-1:	Sampled Values over Serial Unidirectional Multidrop Point-to-Point link
Part 9-2:	Sampled values over ISO 8802-3

Estándar IEC 61850

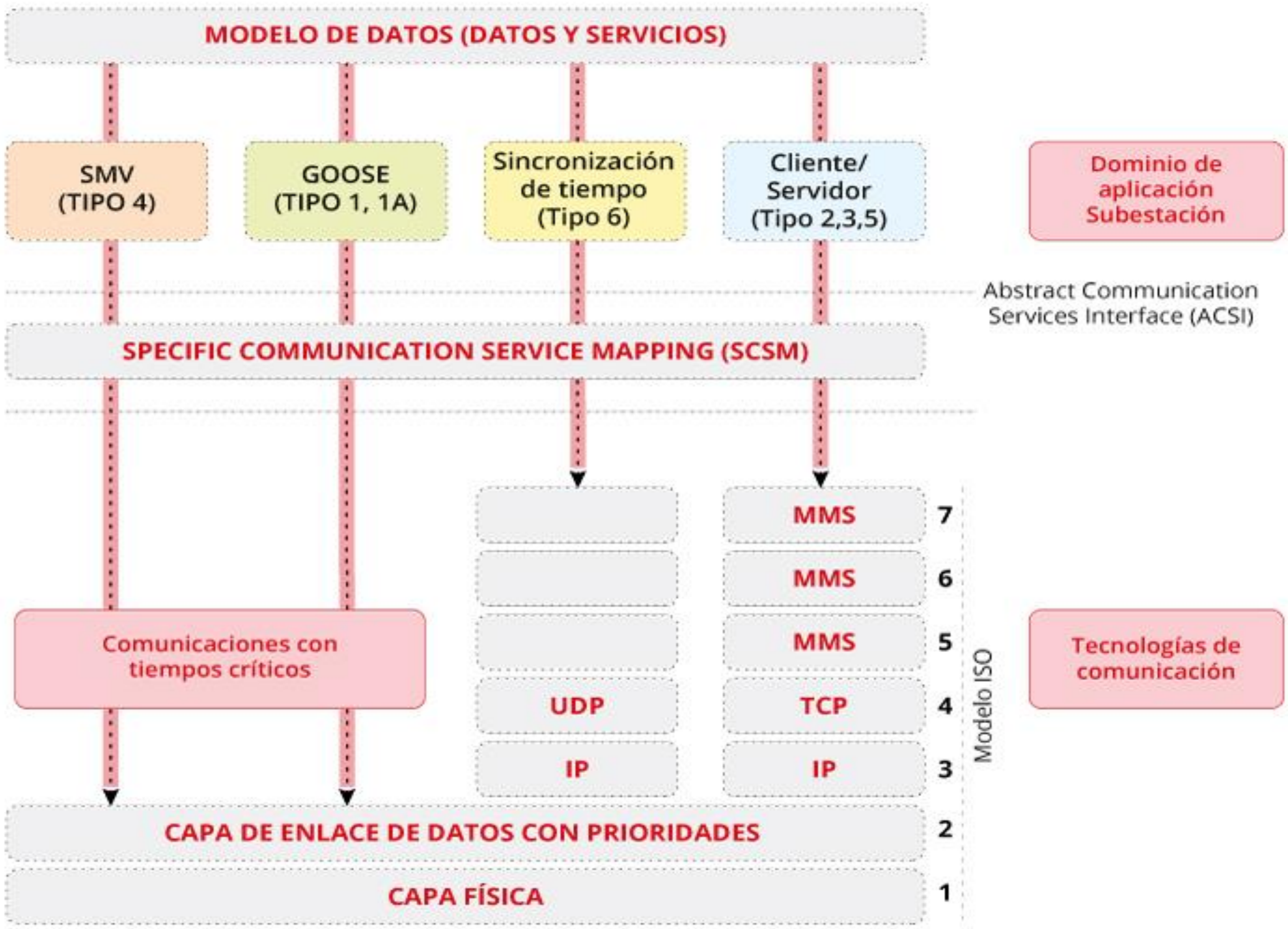


- Desarrollado por la Comisión Electrotécnica Internacional (IEC, ***International Electrotechnical Commission***),

- Define una **serie de protocolos de comunicación** entre los distintos dispositivos de subestaciones eléctricas.

Estos protocolos son:

- *Sampled Measured Values* (**SMV**),
- *Simple Network Time Protocol* (**SNTP**),
- *Manufacturing Message Specification* (**MMS**) y
- *Generic Substation Events* (**GSE**), que a su vez se dividen en
  - *Generic Object Oriented Substation Events* (**GOOSE**) y
  - *Generic Substation State Events* (**GSSE**, actualmente en desuso).



- Modelo de capas -

Los protocolos que conforman el estándar IEC 61850

- **Sampled Measured Values** es utilizado para ***proporcionar una comunicación rápida de valores de medición***, protección y control. Funciona a ***través de Ethernet*** (Capa 2 OSI) y los mensajes son encapsulados como *multicast*, siguiendo una estructura de emisor – suscriptor, donde el emisor envía los datos a todos los equipos de la red y cada equipo se suscribe a los datos para acceder a los mismos.

- **GOOSE** es utilizado para ***la transmisión en tiempo real de eventos críticos y funciona, al igual que Sampled Measured Values, a través de mensajes multicast de Ethernet*** (Capa 2 OSI). El modelo de funcionamiento de GOOSE también sigue la estructura emisor – suscriptor.

- ***Protocolo SNTP para la sincronización de tiempo de los dispositivos***. Como su propio nombre indica, es una versión simplificada del protocolo NTP, utilizado en equipos que no necesitan la funcionalidad completa del protocolo. Para la transmisión de los mensajes SNTP se utiliza el protocolo UDP (Capa 4 OSI).

- Por último, el ***protocolo MMS es la base de las comunicaciones de datos de aplicación en el estándar IEC 61850***. El protocolo envía sus mensajes a través de conexiones TCP (Capa 4 OSI) y es utilizado para las comunicaciones cliente/servidor. Así, es utilizado para el intercambio de datos de la aplicación, así como parámetros de configuración de los dispositivos o datos de monitorización.

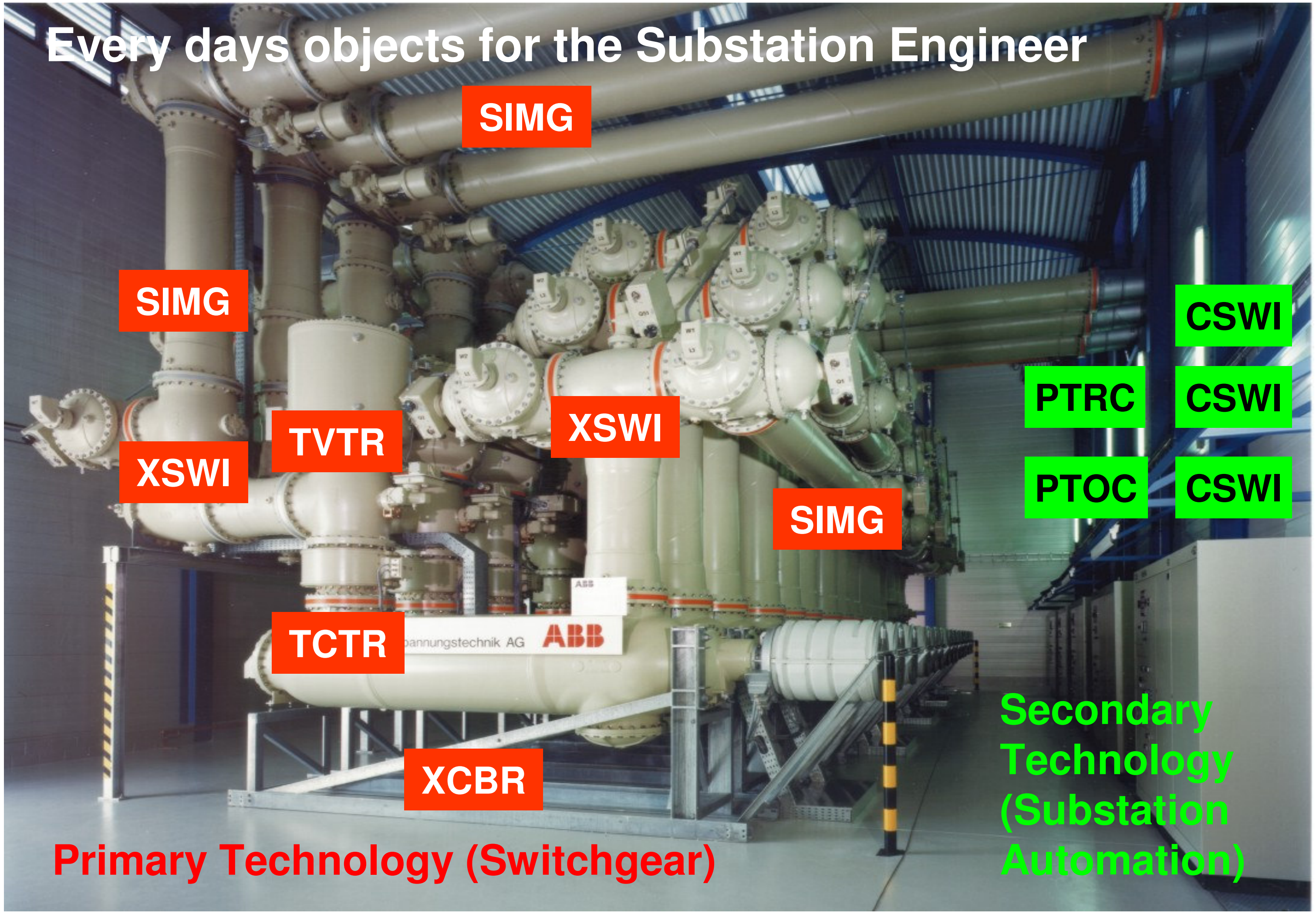
- En definitiva, GOOSE y Sampled Measured Values son utilizados para el envío de datos críticos en tiempo real, al contrario que MMS.

Content

IEC 61850
The Data Model
Refers to IEC 61850-7-y

- Objects and Logical Nodes
- Hierarchical Data Model
- Communication Services

User-near, object oriented Data model



Example :
Object
Current
Breaker
XCBR
What
data
belong to
this object ?

These
Objects
are called
Logical Nodes.

Communication & Logical nodes: Functional view

Communication relations between functions in a Substation Automation System

- Information is exchanged between all ***devices*** which comprise the system
- More precisely, data are exchanged between the ***functions*** and ***sub-functions*** residing in the devices
- The smallest part of the ***function*** that exchanges data is called ***Logical Node (LN)*** in IEC 61850. The LN performs some operations for the overall function

Functions are not standardized ?

Communication & Logical nodes: Data view

Exchanged Data in Substation Automation System

- More precisely, data are exchanged between the ***functions*** and ***sub-functions*** residing in the devices
- The ***exchanged data*** are grouped to into objects belonging to functions
- The objects called ***Logical Node (LN)*** may be seen as ***Containers*** containing the data provided by a dedicated function for exchange (communication)
- The ***Name of the Logical Node*** may be seen as a ***Label*** attached to this container

Functions are not standardized !

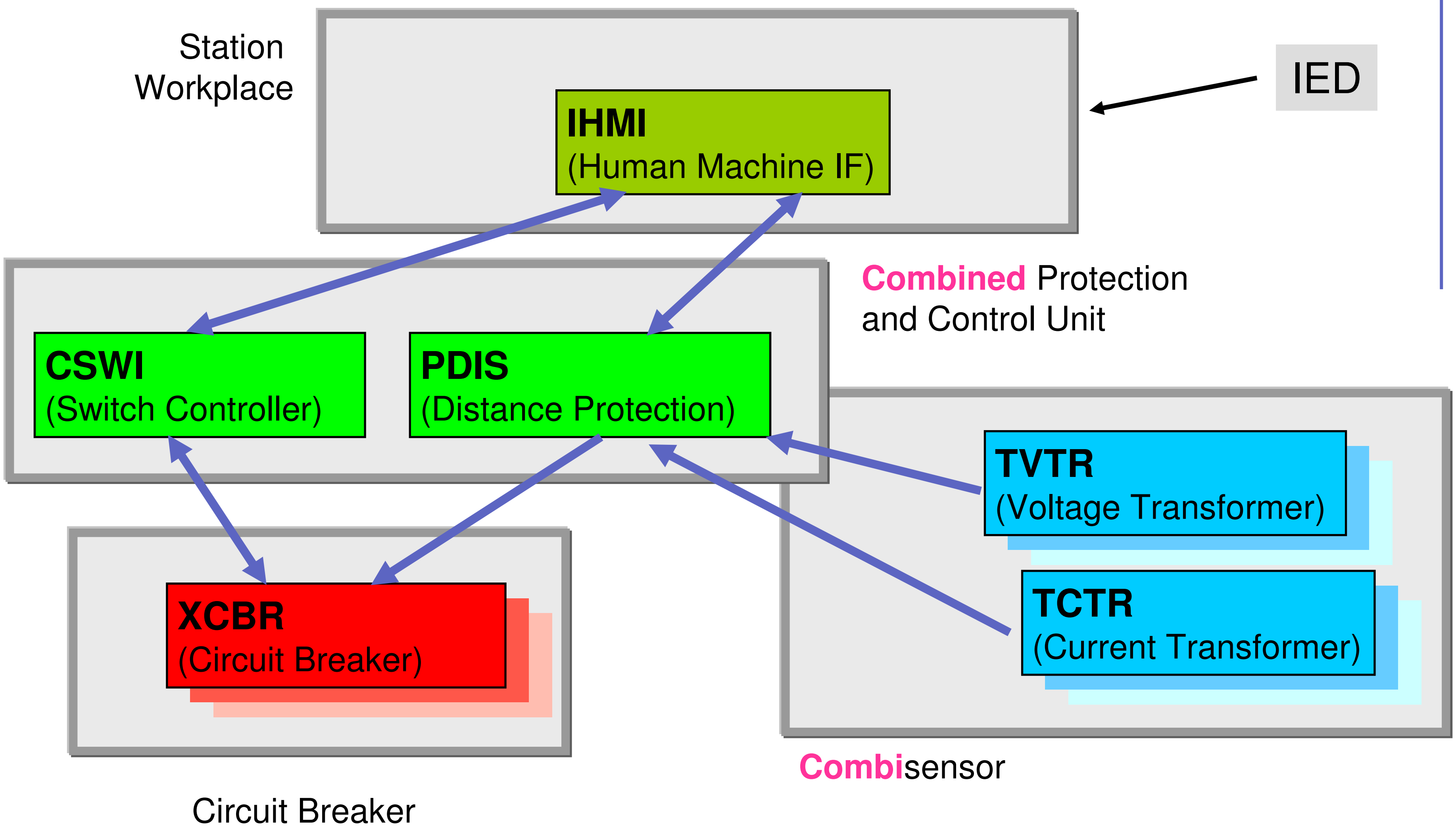
Naming and Groups of LNs

- **L** System LN (2)
- **P** Protection (28)
- **R** Protection related (10)
- **C** Control (5)
- **G** Generic (3)
- **I** Interfacing and archiving (4)
- **A** Automatic control (4)
- **M** Metering and measurement (8)
- **S** Sensor and monitoring (4)
- **X** Switchgear (2)
- **T** Instrument transformers (2)
- **Y** Power transformers (4)
- **Z** Further power system equipment (15)

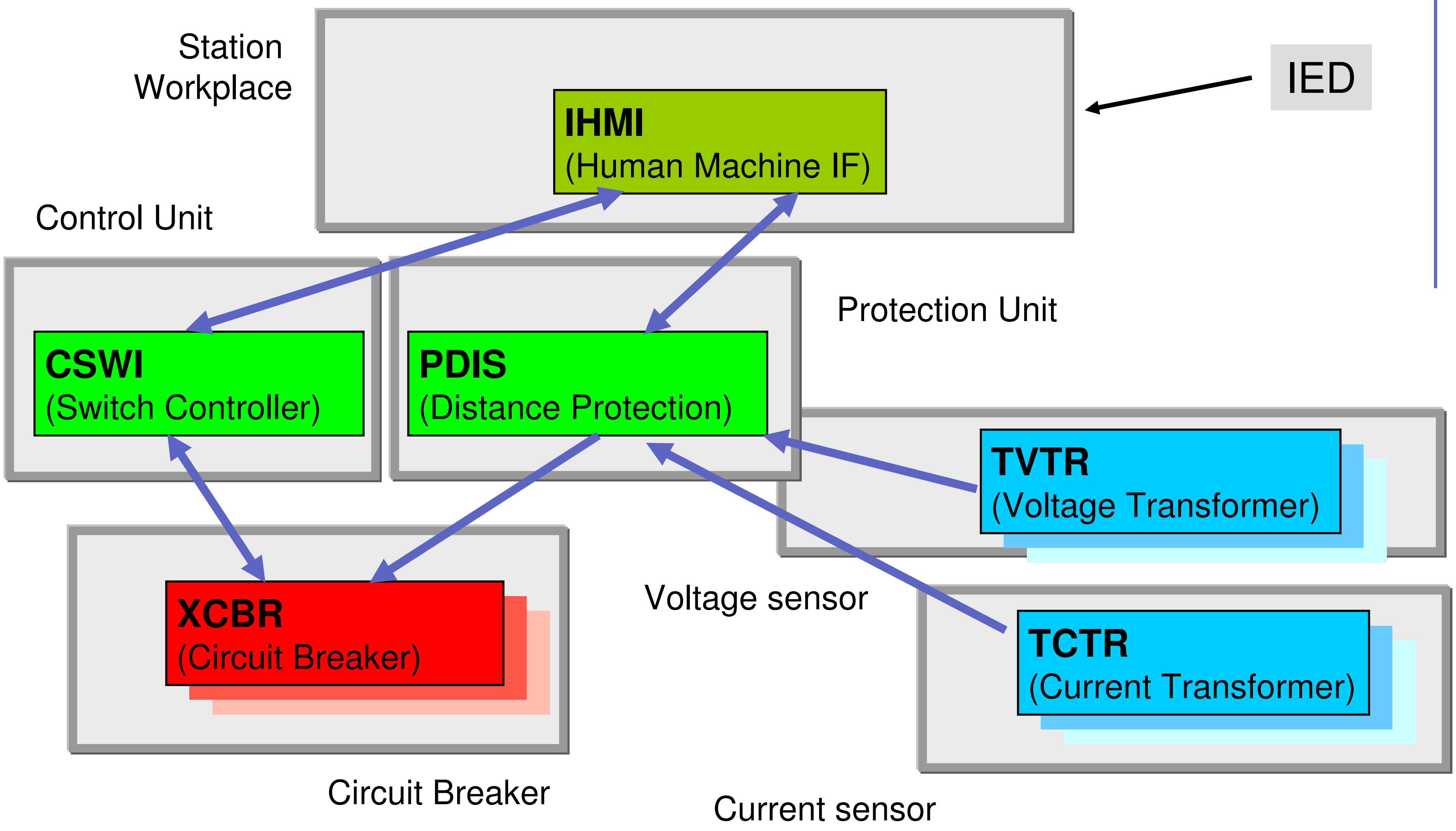
Examples

- *PDIF: Differential protection*
- *RBRF: Breaker failure*
- *XCBR: Circuit breaker*
- *CSWI: Switch controller*
- *MMXU: Measurement unit*
- *YPTR: Power transformer*

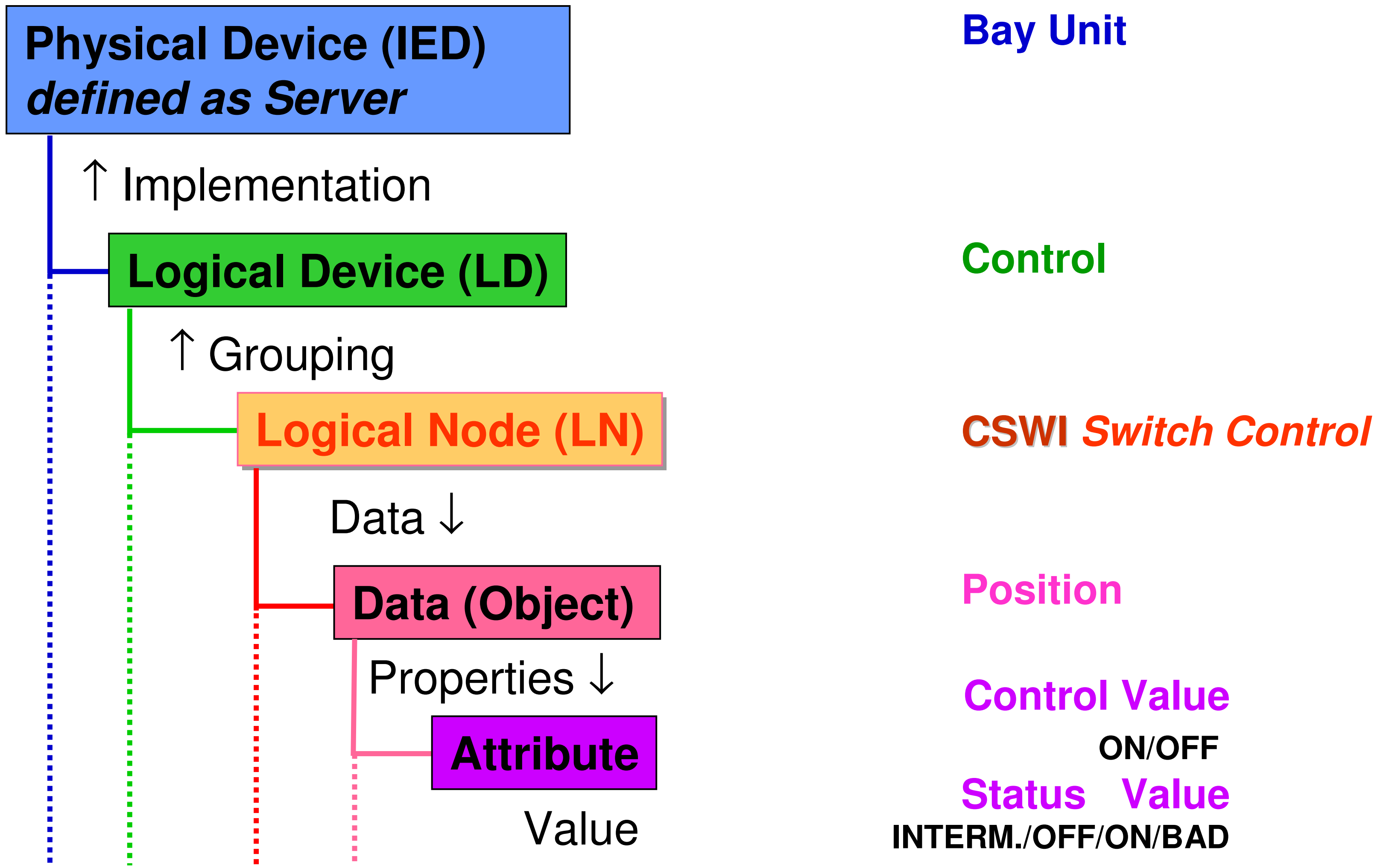
Allocation of LNs to devices (IEDs) – 1



Allocation of LNs to devices (IEDs) - 2

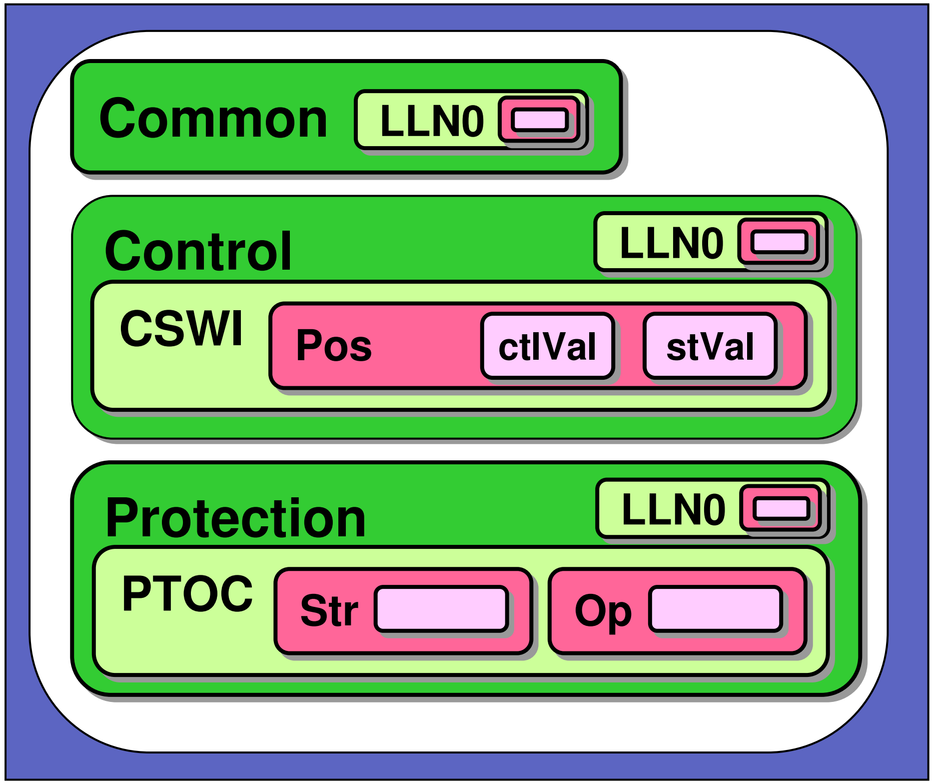


Data Hierarchy



Implementation Example of Data Hierarchy

Bay device (IED) as server for Protection and Control



Common
- LLN0
  - Name plate
    - Vendor
    - etc.

Control
- Switch Control
  - Position
    - Control Value
    - Status Value

Protection
- Overcurrent
  - Start/Pick-up
  - Operate/Trip

Examples for Logical Nodes (1) ref. part 7-4

Common Logical Node class				
Attribute Name	**Attr. Type**	**Explanation**	**T**	**M/O**
LNName		Shall be inherited from Logical-Node Class (see IEC 61850-7-2).		
Data				
Mandatory Logical Node Information (Shall be inherited by ALL LN but LPHD)				
Mod	INC	Mode		M
Beh	INS	Behaviour		M
Health	INS	Health		M
NamPlt	LPL	Name plate		M
Optional Logical Node Information				
Loc	SPS	Local operation		O
EEHealth	INS	External equipment health		O
EEName	DPL	External equipment name plate		O
OpCntRs	INC	Operation counter resetable		O
OpCnt	INS	Operation counter		O
OpTmh	INS	Operation time		O
Data Sets (see IEC 61850-7-2)				
Inherited and specialised from Logical Node class (see IEC 61850-7-2).				
Control Blocks (see IEC 61850-7-2)				
Inherited and specialised from Logical Node class (see IEC 61850-7-2).				
Services (see IEC 61850-7-2)				
Inherited and specialised from Logical Node class (see IEC 61850-7-2).				

M = mandatory, O = optional

Example for Logical Node (2) ref. part 7-4

XCBR class				
Attribute Name	**Attr. Type**	**Explanation**	**T**	**M/O**
LNName		Shall be inherited from Logical-Node Class (see IEC 61850-7-2)		
Data				
Common Logical Node Information **see Example for Logical Node (1)**				
		LN shall inherit all Mandatory Data from Common Logical Node Class		M
Loc	SPS	Local operation (local means without substation automation communication, hardwired direct control)		M
EEHealth	INS	External equipment health		O
EEName	DPL	External equipment name plate		O
OpCnt	INS	Operation counter		M
Controls				
Pos	**DPC**	Switch position		M
BlkOpn	SPC	Block opening		M
BlkCls	SPC	Block closing		M
ChaMotEna	SPC	Charger motor enabled		O
Metered Values				
SumSwARs	BCR	Sum of Switched Amperes, resetable		O
Status Information				
CBOpCap	INS	Circuit breaker operating capability		M
POWCap	INS	Point On Wave switching capability		O
MaxOpCap	INS	Circuit breaker operating capability when fully charged		O

M = mandatory, O = optional

Common Data Class (CDC) DPC ref. part 7-3

DPC class					
Attribute Name	**Attribute Type**	**FC**	**TrgOp**	**Value / Value Range**	**M/O/C**
DataName	Inherited from Data Class (see IEC 61850-7-2)				
DataAttribute					
				control and status	
ctlVal	BOOLEAN	CO		off (FALSE) | on (TRUE)	AC_CO_M
operTim	TimeStamp	CO			AC_CO_O
origin	Originator	CO, ST			AC_CO_O
ctlNum	INT8U	CO, ST		0..255	AC_CO_O
stVal	CODED ENUM	ST	dchg	intermediate-state | off | on | bad-state	M
q	Quality	ST	qchg		M
t	TimeStamp	ST			M
stSeld	BOOLEAN	ST	dchg		AC_CO_O
				substitution	
subEna	BOOLEAN	SV			PICS_SUBST
subVal	CODED ENUM	SV		intermediate-state | off | on | bad-state	PICS_SUBST
subQ	Quality	SV			PICS_SUBST
subID	VISIBLE STRING64	SV			PICS_SUBST
				configuration, description and extension	
pulseConfig	PulseConfig	CF			AC_CO_O
ctlModel	ENUMERATED	CF		status-only | direct-with-normal-security | sbo-with-normal-security | direct-with-enhanced-security | sbo-with-enhanced-security	M
sboTimeout	INT32U	CF			AC_CO_O
sboClass	ENUMERATED	CF		operate-once | operate-many	AC_CO_O
d	VISIBLE STRING255	DC		Text	O
dataNs	VISIBLE STRING255	EX			AC_DLN_M
cdcNs	VISIBLE STRING255	EX			AC_DLNDA_M
tag	Tag	AX			O
Services					
As defined in **Error! Reference source not found.**					

M = mandatory, O = optional

xC_… = conditional

Free allocation of Logical Nodes

Free allocation of Logical Nodes to devices is based on free allocation of functions to devices

- The support of free allocation Logical Nodes (functions and sub-functions) allows an ***optimization*** of of systems today and tomorrow
- The free allocation is controlled by ***strict rules*** and the concept of IEC 61850
- The free allocation does not disturb ***interoperability*** but may increase the requirements for tools
- The free allocation is limited by the device capacities as described in ***data sheets*** same as today

Strict rules for Extensions

- **Existing** Logical Nodes, Data, and Attributes shall be used if applicable
- **Mandatory** data shall be provided if claiming conformance
- Before making any extension, the **Optional** data shall be used if applicable
- If the conditions apply, **Conditional** data get mandatory
- For **Extensions** of Logical Nodes, first data defined for other Logical Nodes shall be used
- In creating data extensions, combinations of well-defined **Terms** shall be used
- **Name spaces** shall be used for any extension referring to some document where the meaning and the use of these extensions is defined

M = mandatory, O = optional

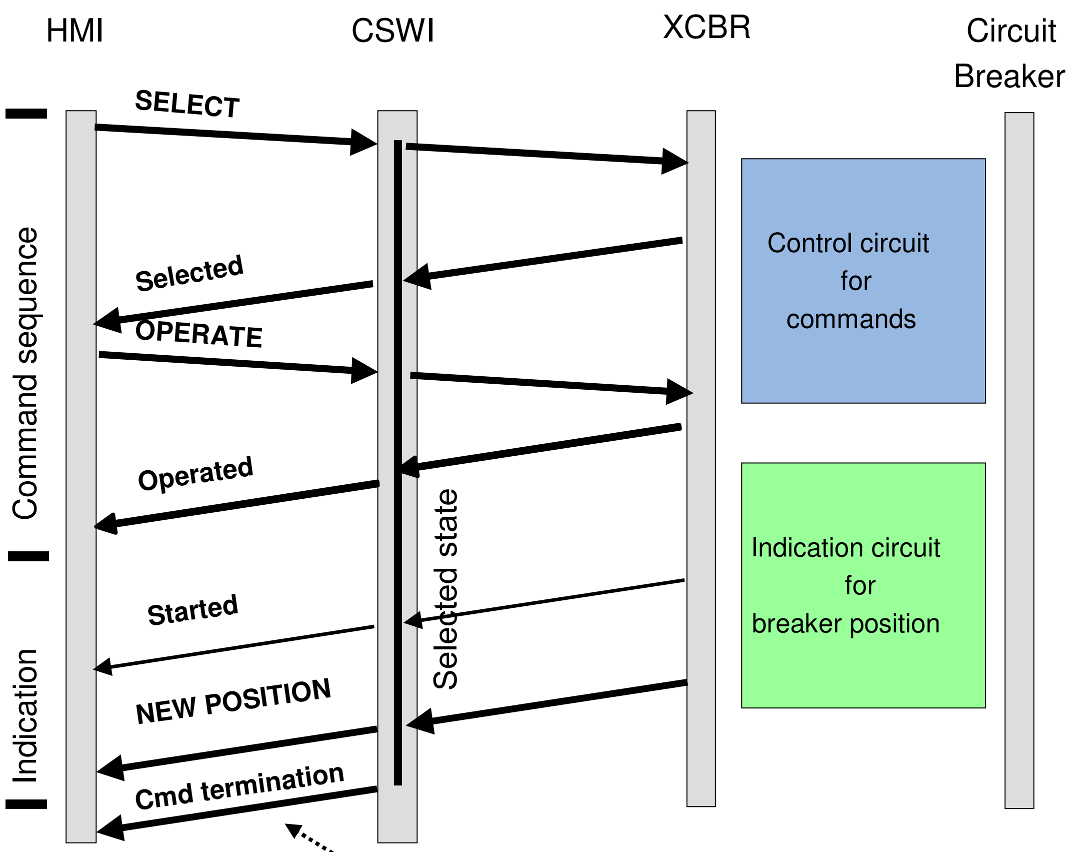
Data access and transfer (Services)

- **read** a value / attribute
- **write** configuration attributes
- **control** a device (direct operate / **s**elect **b**efore **o**perate)
- **event oriented** communication with reporting
- local storage of time-stamped events in a **log**
- get **directory information**
- **file transfer** for e.g.
  - parameter and software download
  - upload from monitoring information like travel curves or history of gas density values
- **Transfer of generic object oriented system events (GOOSE)**
- **Transfer of sampled (analog) values (SV)**

Non time-critical Services

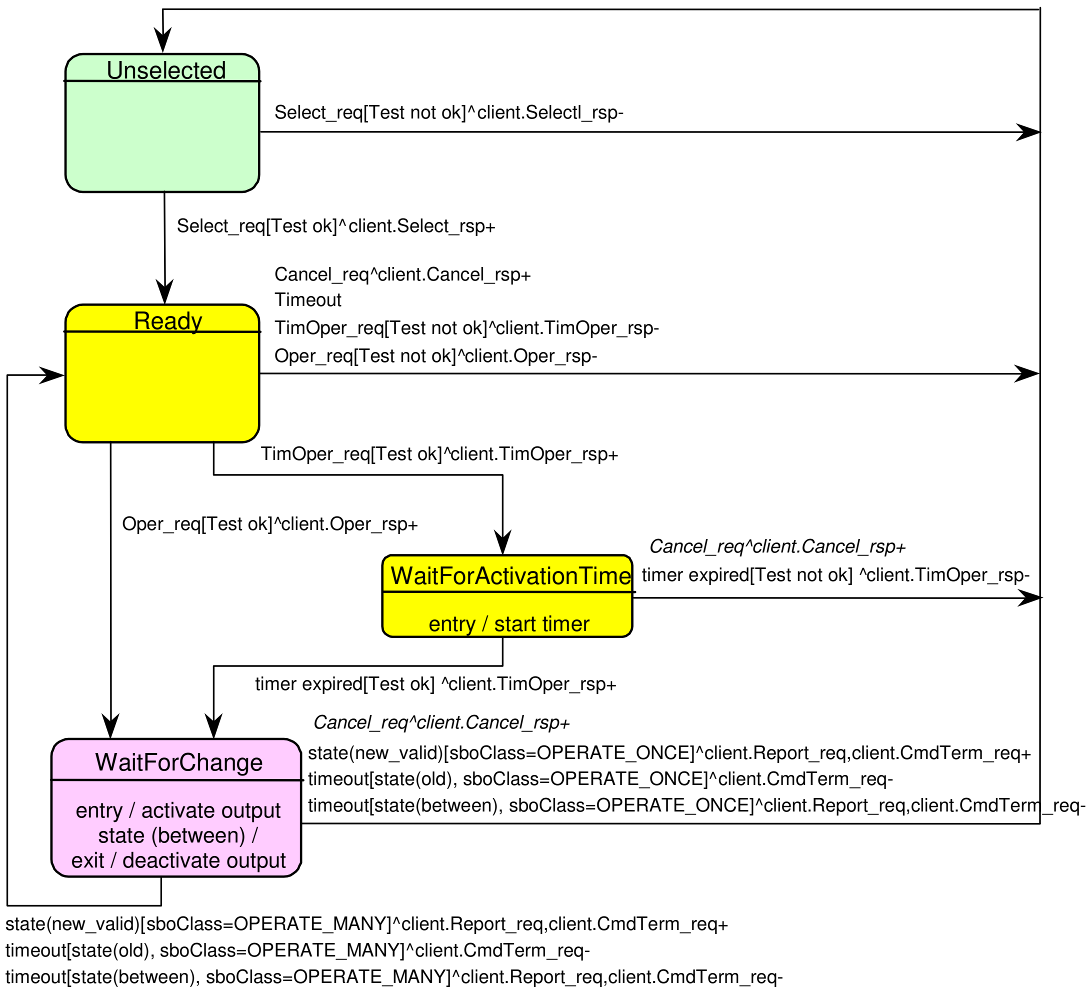
Time-critical Services

Example: Select before Operate



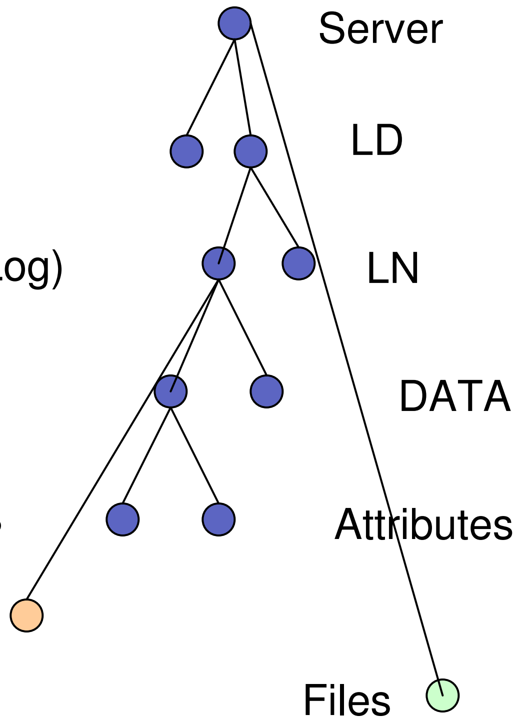
Enhanced security

Select before Operate – state diagram



Example: Directory services

- GetServerDirectory (Files, LDs)
- GetLogicalDeviceDirectory
- GetLogicalNodeDirectory(DATA, DataSet, CBs, Log)
- DATA
  - GetDataDirectory -> List of Attributes
  - GetDataDefinition -> Data/Attribute properties
- GetDataSetDirectory -> Members of DataSet
- GetFileAttributeValues



Common features of Reports, GOOSE and SV

- All these three services send data **spontaneously**, i.e. without being asked from a Master or Client

- For defining the data to be transmitted by these services, a **Data Set** is defined comprising all these data out of the overall data model (for Report, GOOSE or SV)

- The starting event (conditions) when the data transmission is started starts has to be defined in a **Control Block** (for Report, GOOSE or SV)

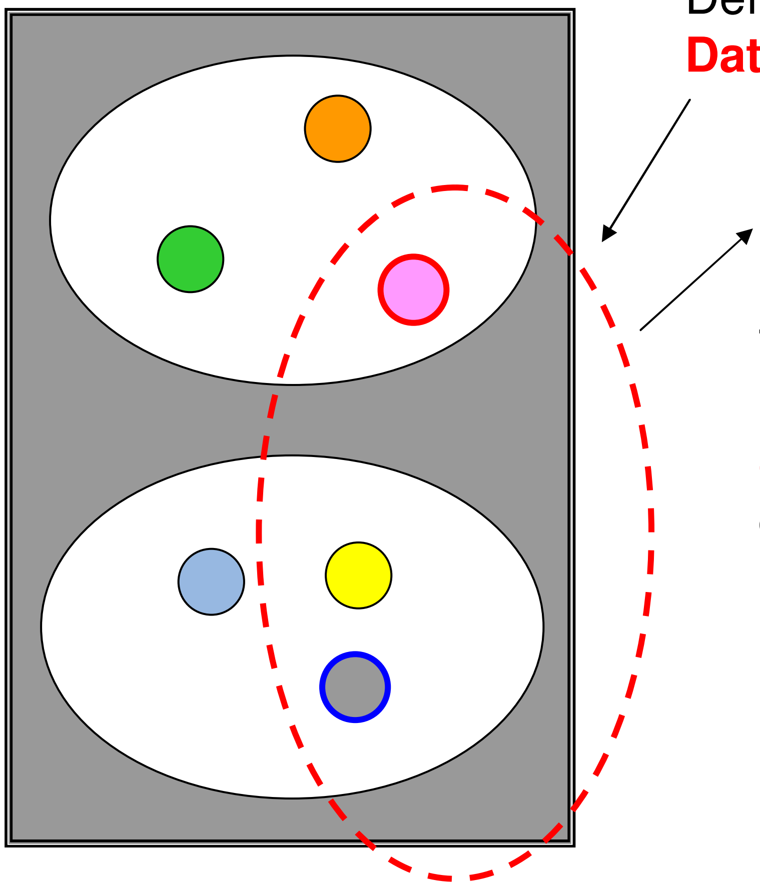
- The starting event for Reporting and GOOSE messages may be a **change of a value**, a crossing of a boundary, etc.

- The starting event of sending synchronous sampled values (SV) is a “**clock event**”

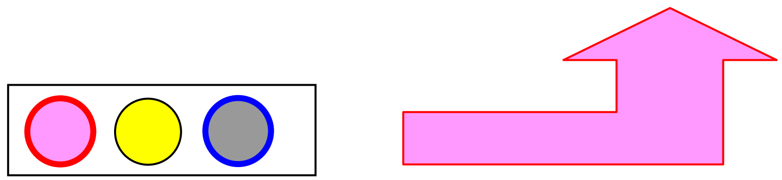
Communication Services

Services with Data Sets and Control Blocks

Logical Device (LD) with two Logical Nodes (LN) containing all Data



Definition of **Data Set**



The configurable Report, GOOSE and SV control block defines, when a report, a GOOSE message, or SV are send based on the Data in the Data Set

No Data avalanche, only predefined data will be send.

Time critical Services

- Transfer of generic object oriented system events (GOOSE)
- Transfer of sampled (analog) values (SV)

To understand how to handle time critical services on Ethernet, some communication Know-how is needed.

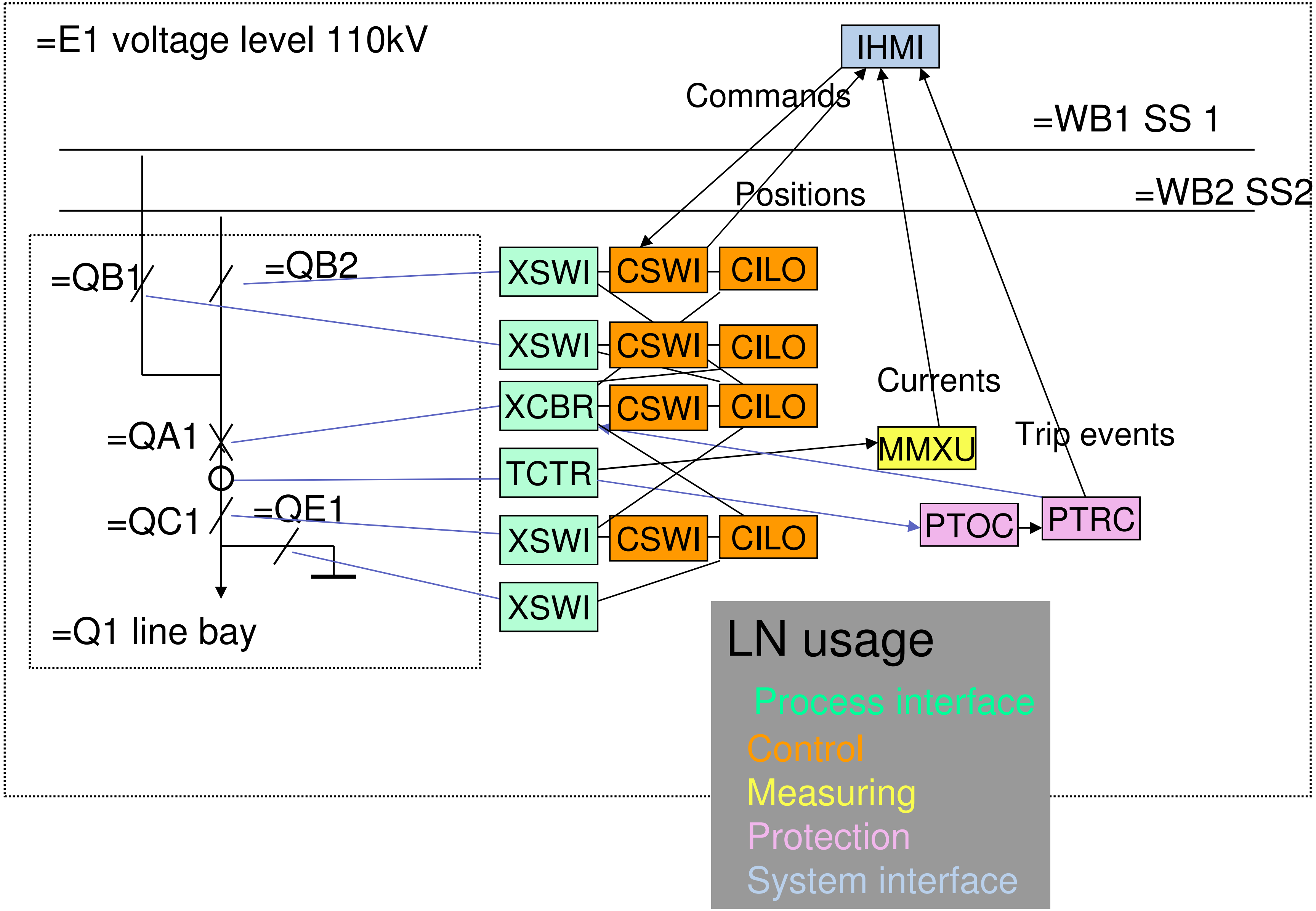
Will be explained later !

Content

IEC 61850
Application of Data Model
Refers to IEC 61850-7-y

- Application of data model

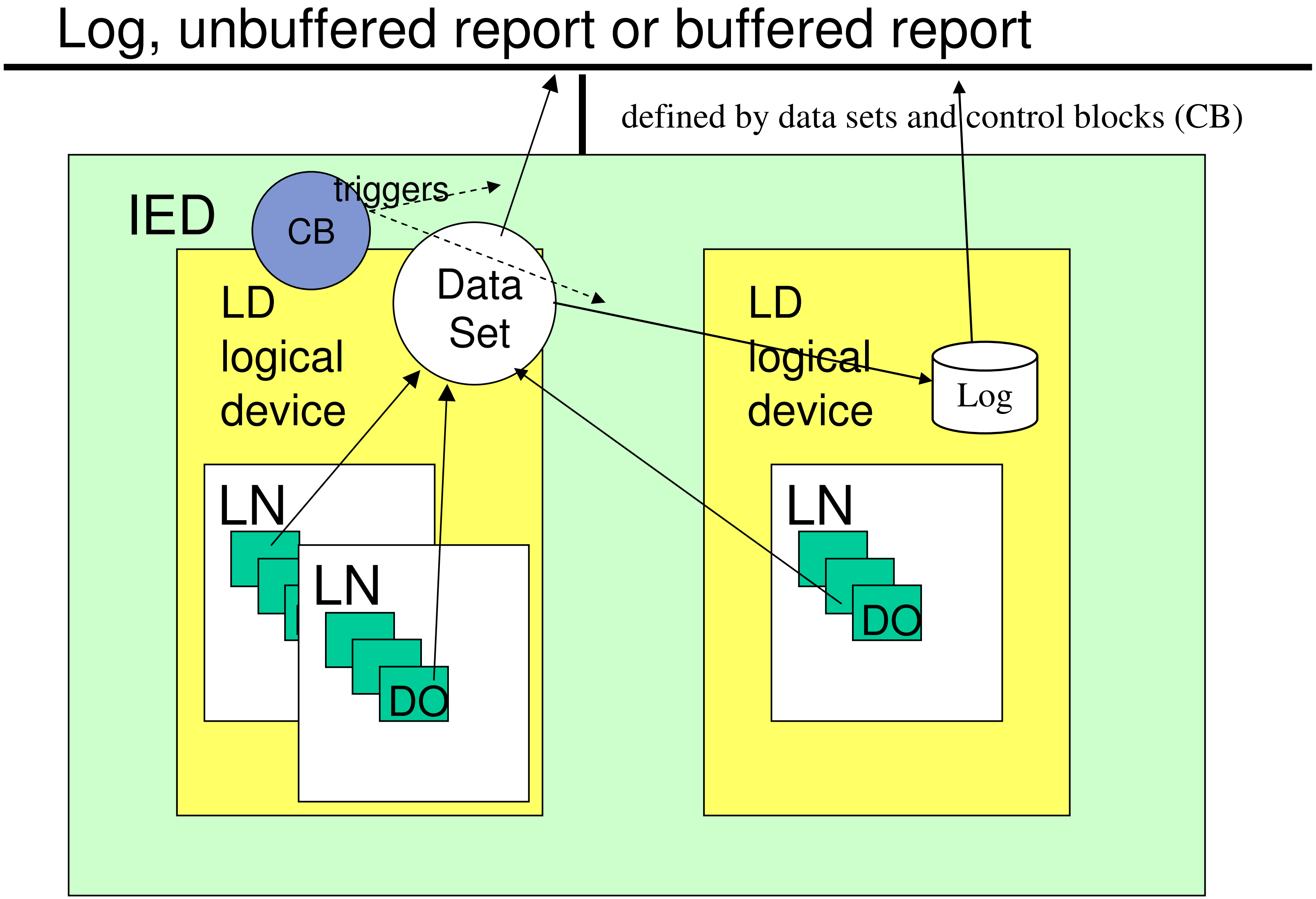
Function modeling – general principle



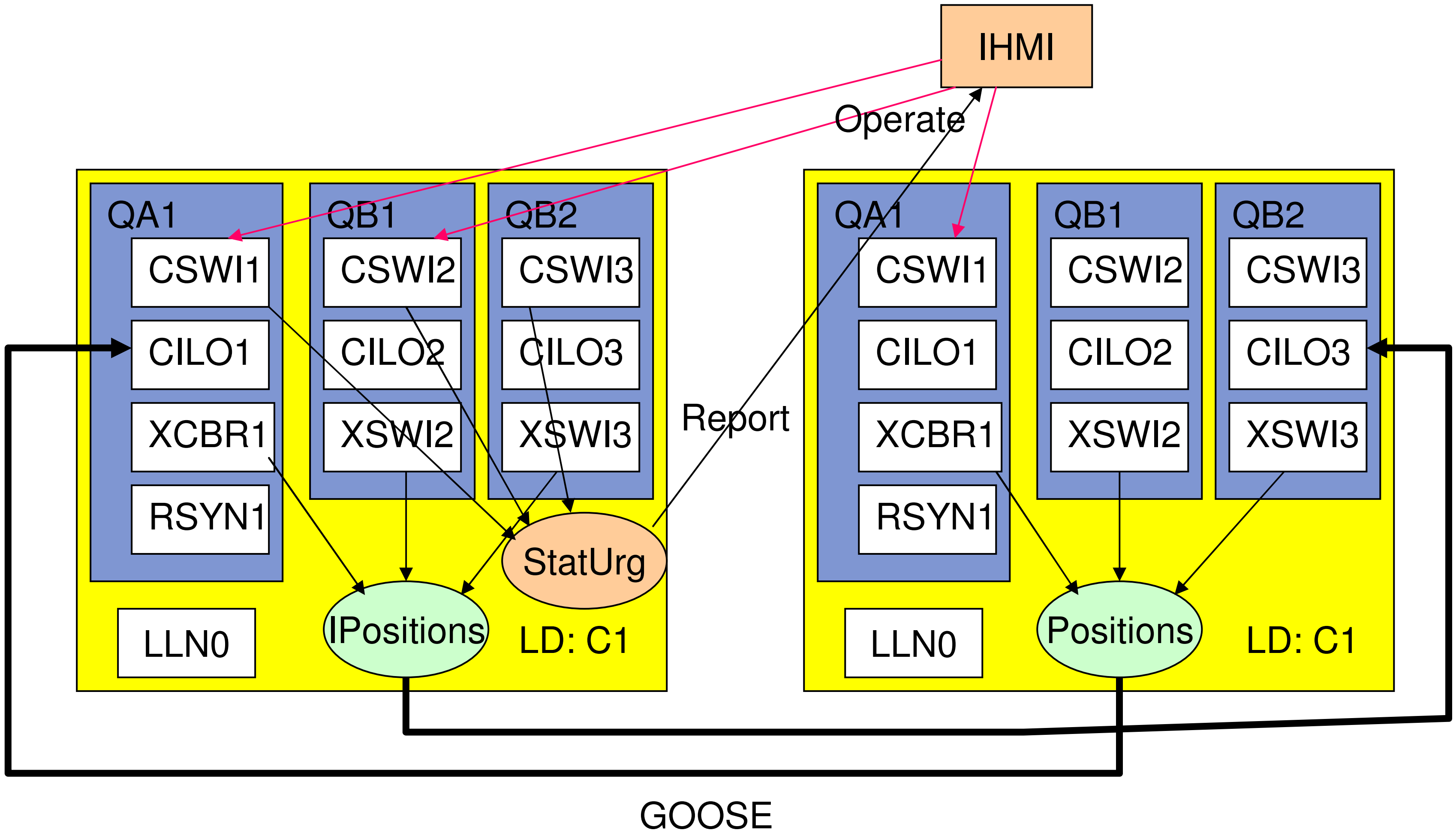
Function modeling - principles

- Process interface – function (– system interface)
  - At least **two** LNs per function
- Protection
  - Trip by **XCBR**
  - Trip conditioning by **PTRC**
  - One **PDIS** instance per zone
  - **PSCH** / **MDIF** hide communication with other line side (to be standardized)
- Disturbance recorder
  - All LNs belonging to one disturbance recorder must form one LD with **one RDRE** and one LLN0

Time stamped events & Status information



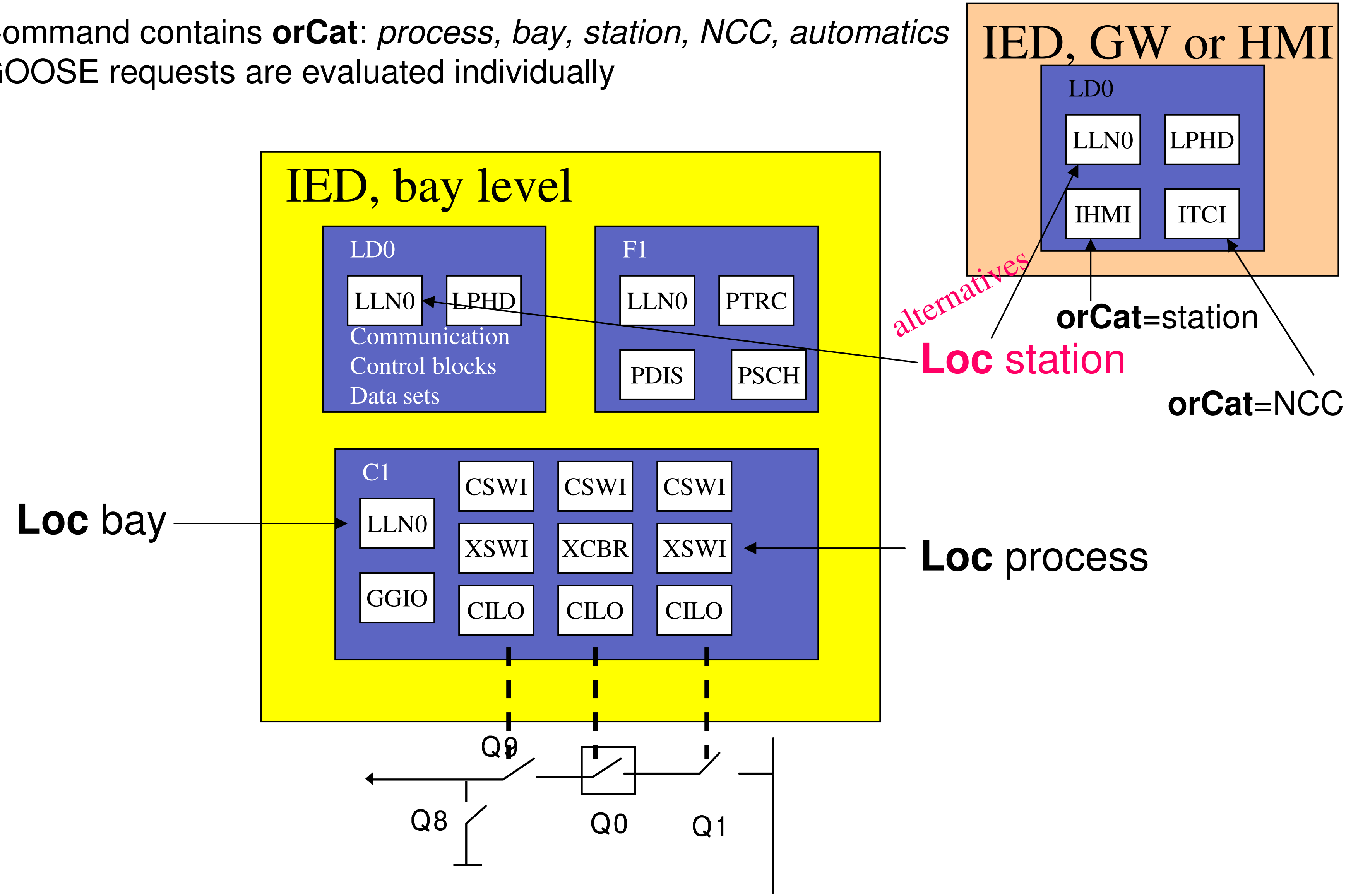
Control application



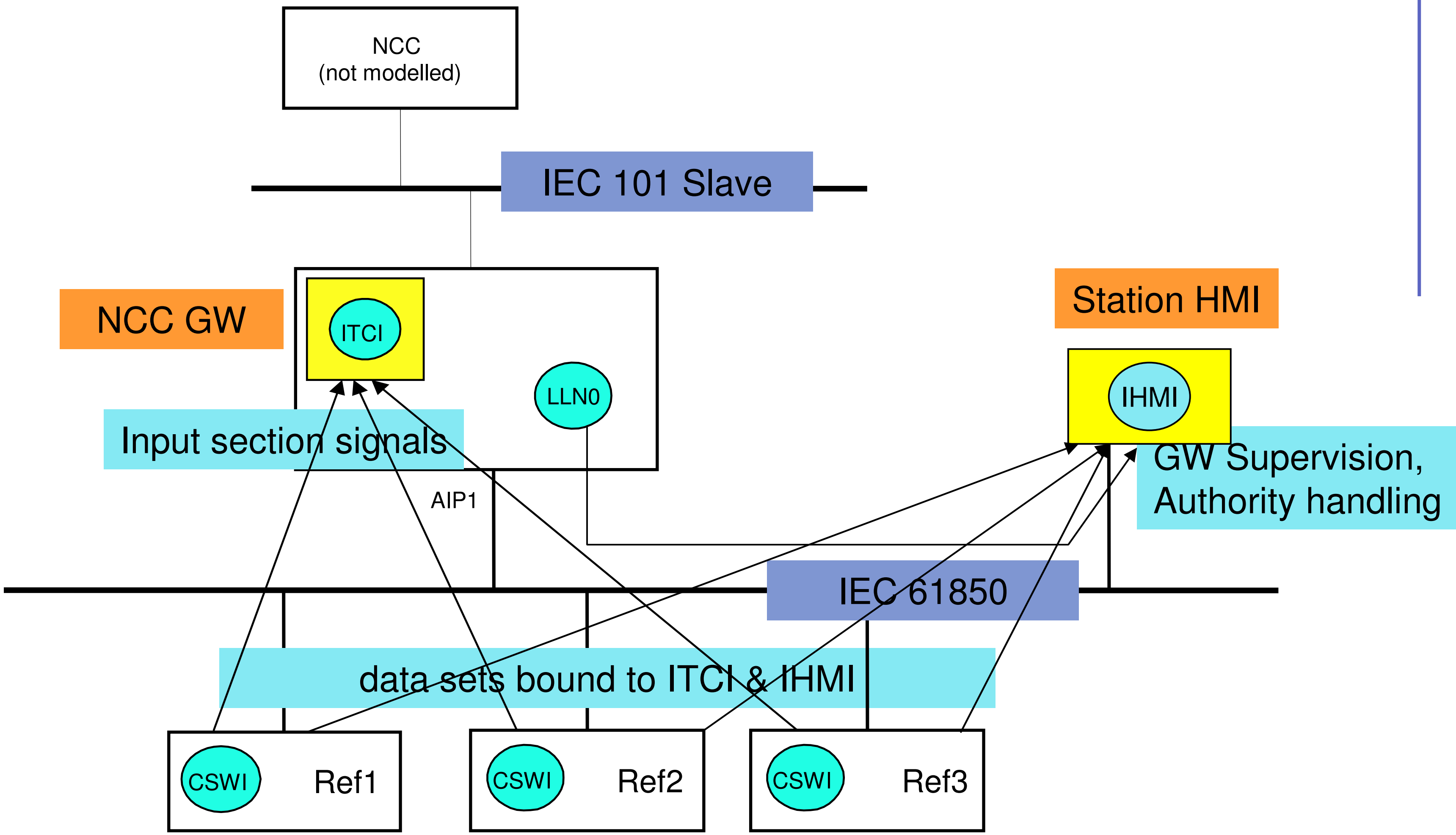
Note: for command reservation also CSWIx.stSeld is in GOOSE

Access hierarchy

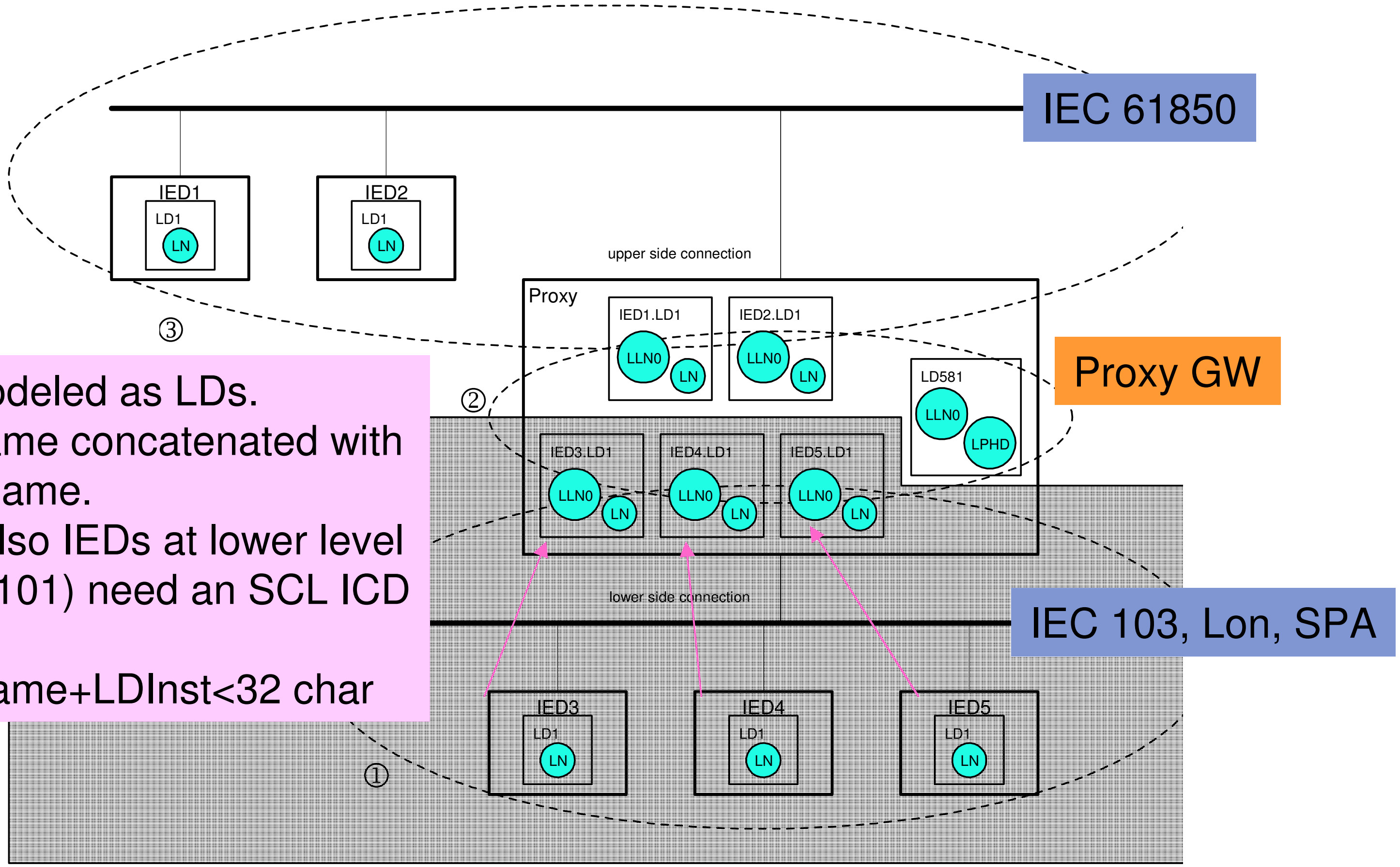
Command contains **orCat**: *process, bay, station, NCC, automatics*
GOOSE requests are evaluated individually



Gateway from IEC 61850 to NCC



Gateway as Proxy to IEC 61850



IED LDs are modeled as LDs.
Name is IED name concatenated with lower level LDName.
Prerequisite: also IEDs at lower level Bus (Lon, 103, 101) need an SCL ICD File!
Caution: IEDName+LDInst<32 char

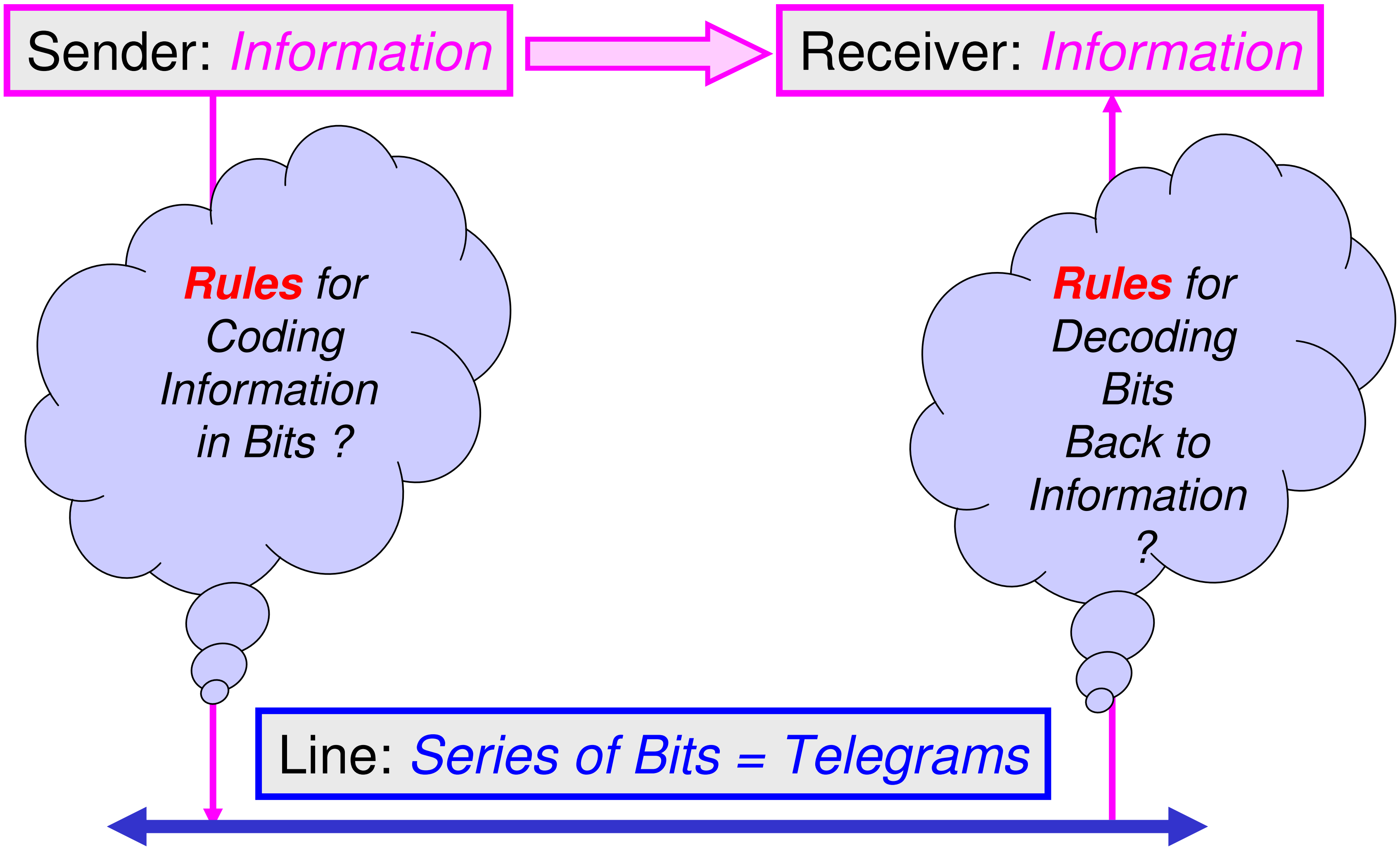
Content

IEC 61850
The Communication Principles

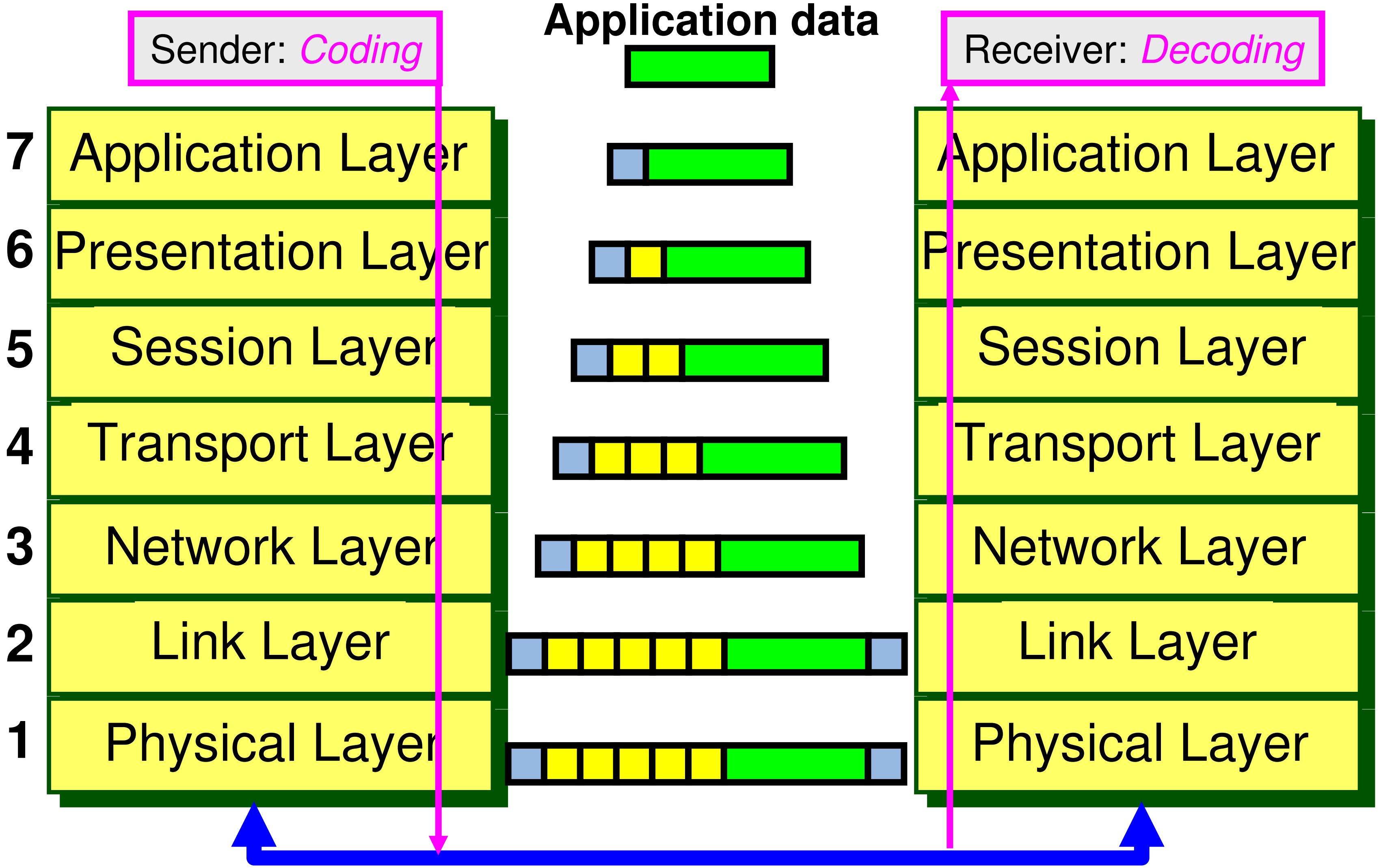
General Information and
references to IEC 61850-7-2 and IEC 61850-8-1 and 9-2

- ISO/OSI Model
- The stack of IEC 61850
- Event driven and time critical services

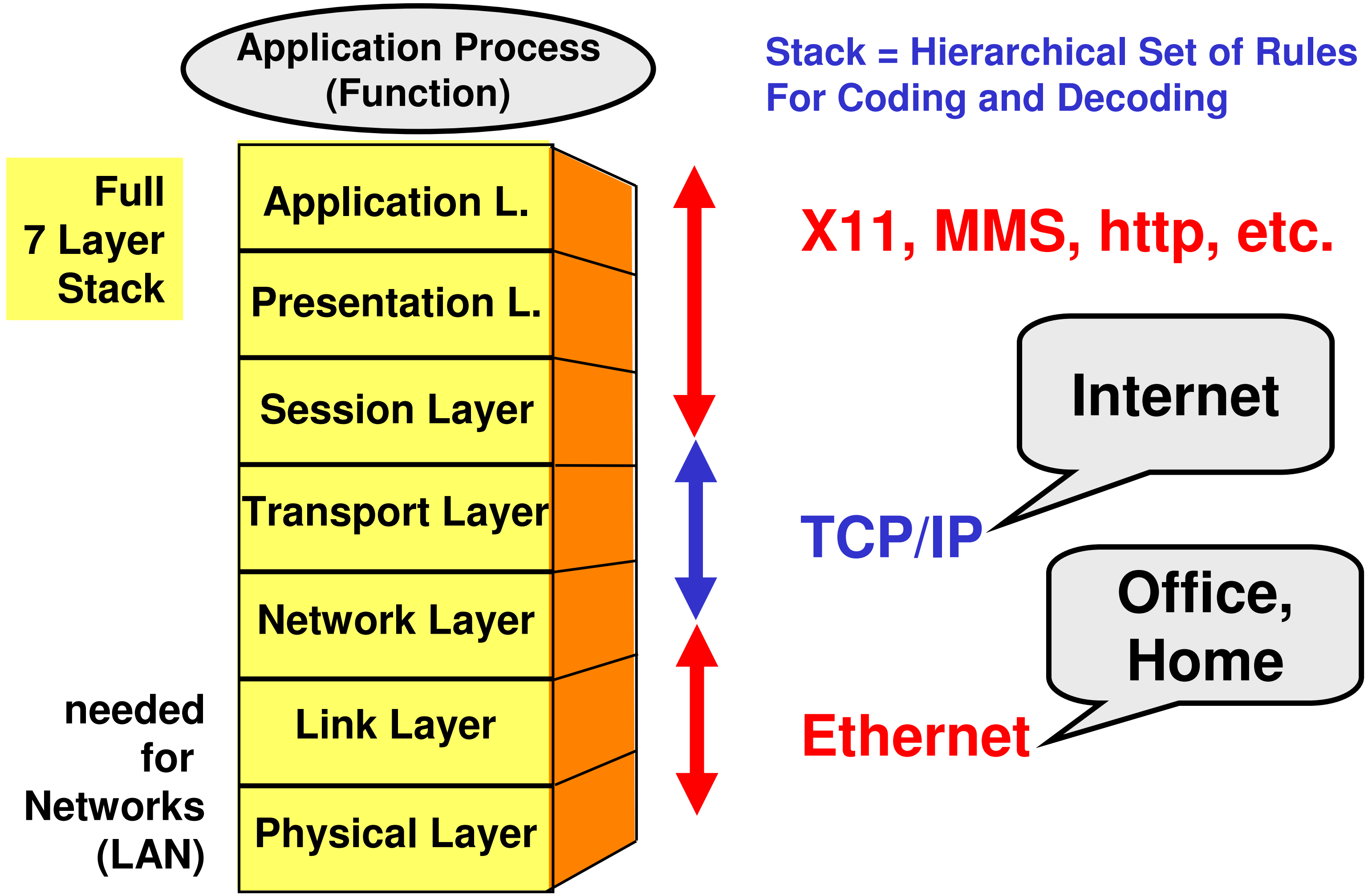
Exchange of data by serial communication



Coding/decoding acc. to the ISO/OSI model



The 7 layers of the ISO/OSI Model

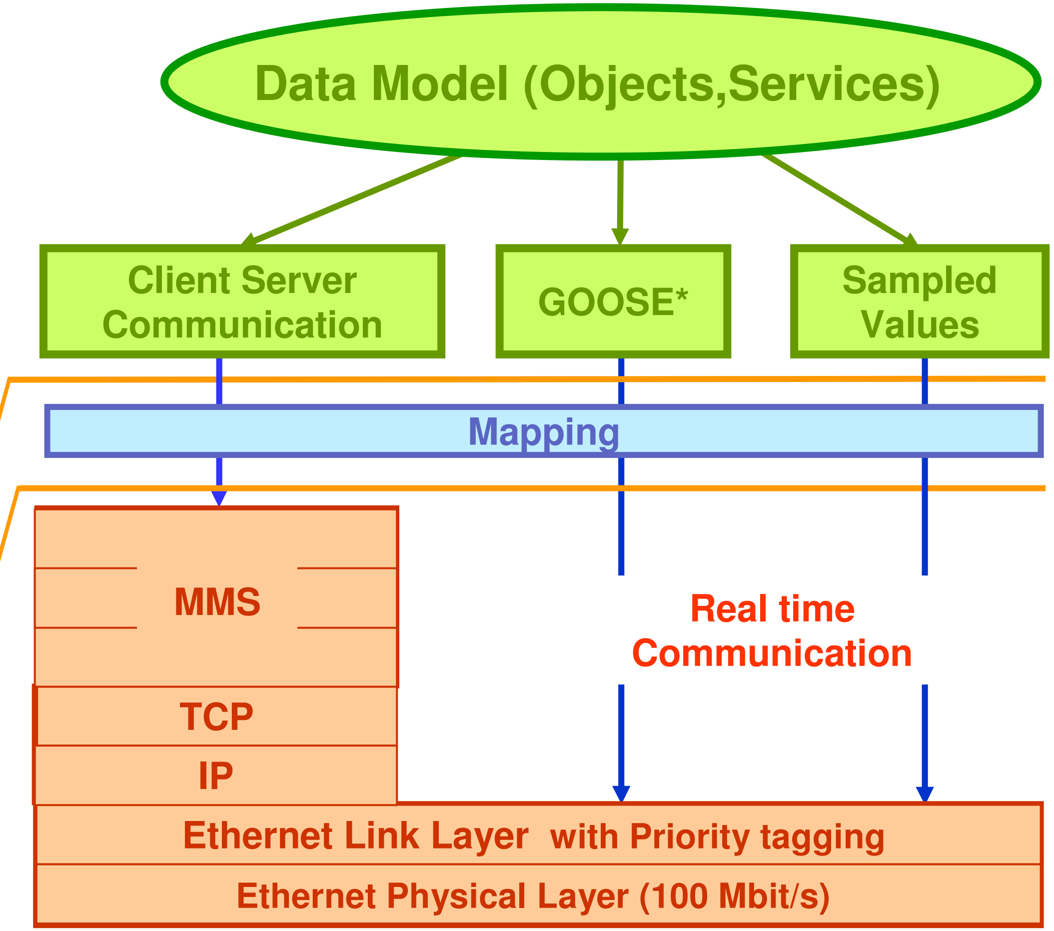


MMS Manufacturing Message Specification
TCP Transport Control Protocol
IP Internet Protocol

The Stack of IEC 68150 and Model Mapping

- SA specific data model evolves slowly
- Communication technology changes quickly
- Splitting of SA specific data model from communication technology

- *Model according to state-of-the-art SA technology*



Abstract Communication Services Interface (ACSI)

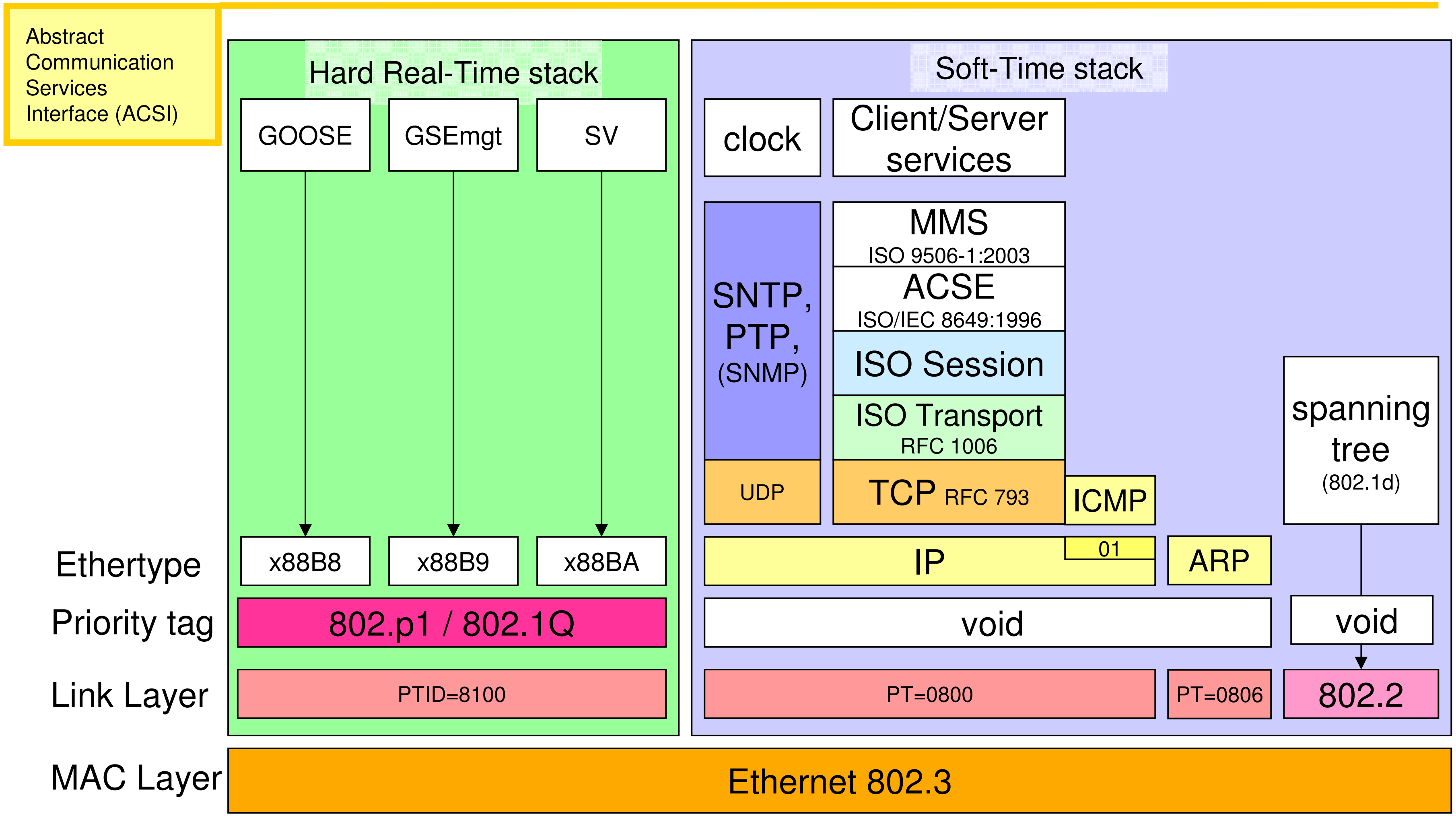
Stack Interface

ISO/OSI – Stack
Hierarchical set of Rules how information is coded for transmission
According to state-of-the art communication technology

Stack selection according to the state-of-the-art Communication technology

* **G**eneric **O**bject **O**riented **S**ubstation **E**vent

IEC 61850 Stack: Technical Details



Time critical Services

- **Transfer of generic object oriented system events (GOOSE)**
  - Some few data like blockings, releases, position, trips, etc. have to be transmitted very fast and reliable.
  - Therefore, the transmission is time critical (highest demand 4 ms)
- **Transfer of sampled (analog) values (SV)**
  - **The samples have to be precisely synchronized depending on the demanding functions.**
  - **Therefore, the synchronization is time critical (highest demand 1 µs). If the sampling is not synchronized the samples have to be tagged with a time of the same accuracy to compare sinusoidal waves or to to calculate phasors.**
  - **In addition, the stream of samples has to be transmitted fast enough that the fast reaction time e.g. of protection in not more delayed than with hardwired connections.**

Time-critical Services using only the 2 Lowest Layers of the stack

For comparison: Client-Server Communication

Used for non time-critical services only !

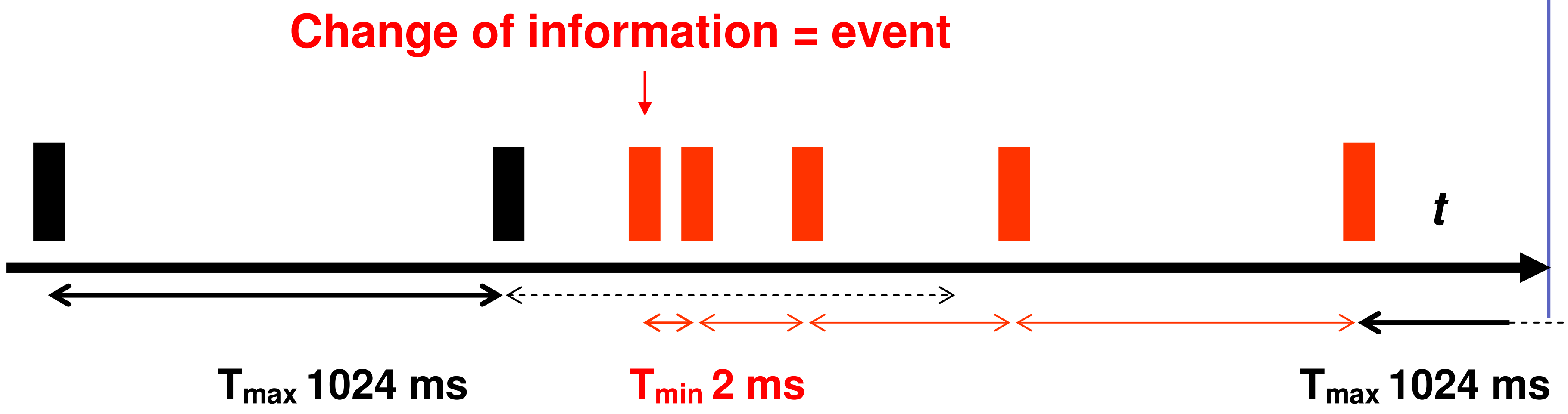
Client – Server services using all 7 layers of the ISO/OSI stack

- A point – point association is established and supervised and may be terminated: Associate / Release / Abort
- MMS: Dynamically built (server addresses, authentication)
- Maximum number is IED implementation dependent
- The mechanism is very reliable
- Telegrams are “acknowledged” on a low level
- Normally, no data are lost since telegrams with errors may be resend again
- Comfortable mechanism – you now it from your office and from the Internet - but time consuming, i.e. not suited for time-critical communication

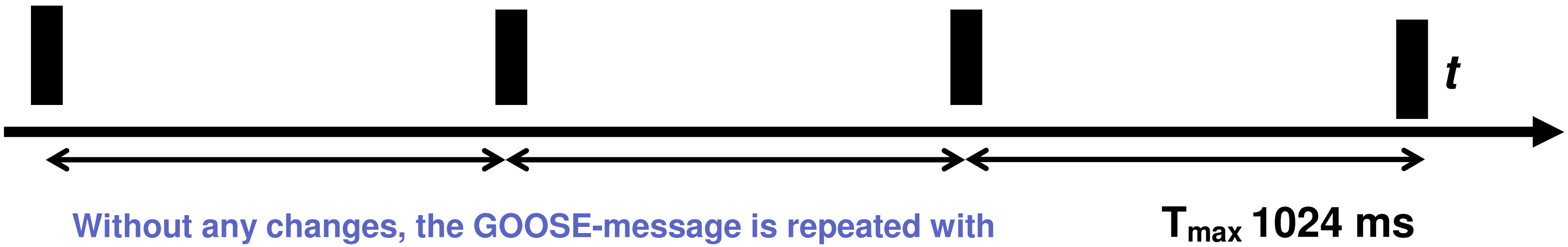
Confirmation of spontaneous messages ?

- The reception of a **report** may be confirmed and in case of losses repeated. Using the full stack and takes some time.
- The data stream of **sampled values (SV)** is not confirmed but losses of some samples are handled without problems by the receiving functions, e.g. by a protection algorithm.
- The unconfirmed **GOOSE messages** may transport important time critical information like a block or a trip. Therefore, a special repetition mechanism has to guarantee a reliable transfer without losses of these data (see next page).

The mechanism GOOSE messages



In case of a information- change, the GOOSE-message will be repeated within T_{min}.
The repetition frequency is lowered until T_{max} is reached.



Without any changes, the GOOSE-message is repeated with T_{max} until the next event / change.

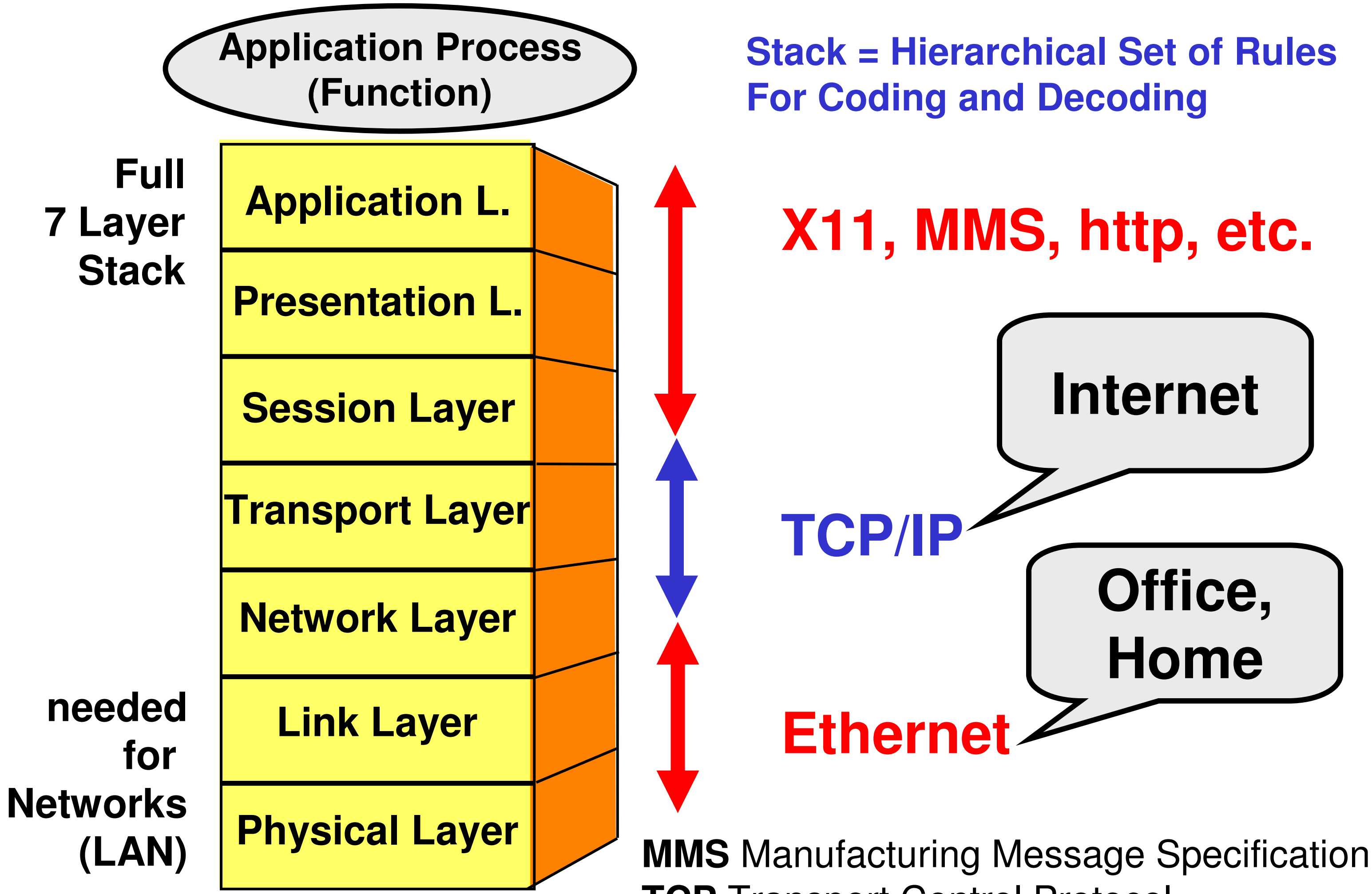
Content

IEC 61850
The Communication Architectures

General Information about Ethernet and references to IEC 61850-8-1 and 9-2

- Basics about Ethernet
- Switches
- Architectures
- Process bus

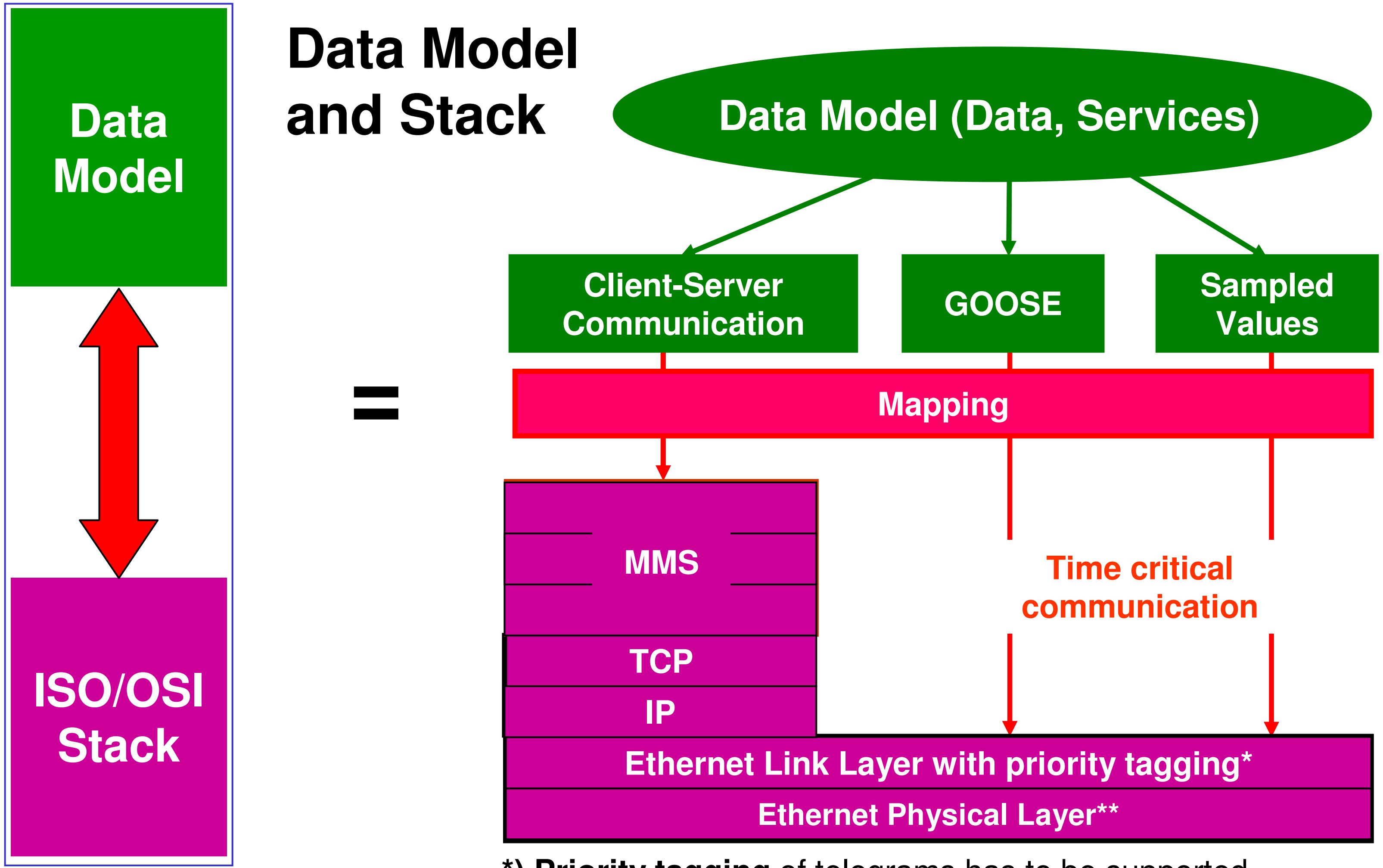
The 7 layers of the ISO/OSI Model



MMS Manufacturing Message Specification
TCP Transport Control Protocol
IP Internet Protocol

Communication Stack of IEC 61850

Data Model and Stack



*) **Priority tagging** of telegrams has to be supported
) **Speed 100 Mbit/s

Access methods

For serial communication, not only

- the Coding according to the ISO/OSI stack

but also

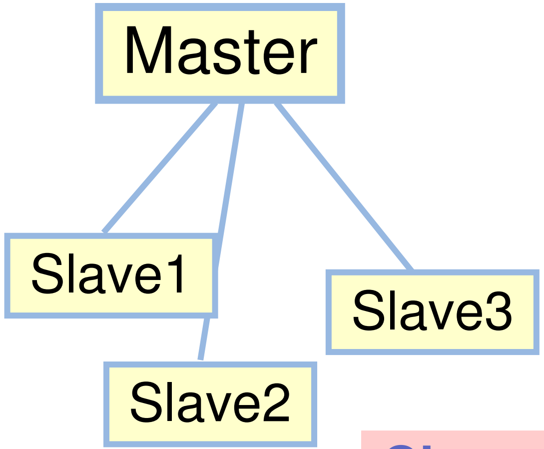
- the Access to and the use of the communication medium

has to be defined.

There exist basically 4 Access Methods, i.e.

- Master-slave
- Time division multiplex
- Token passing
- Carriers sense multiple access

Master-Slave Access



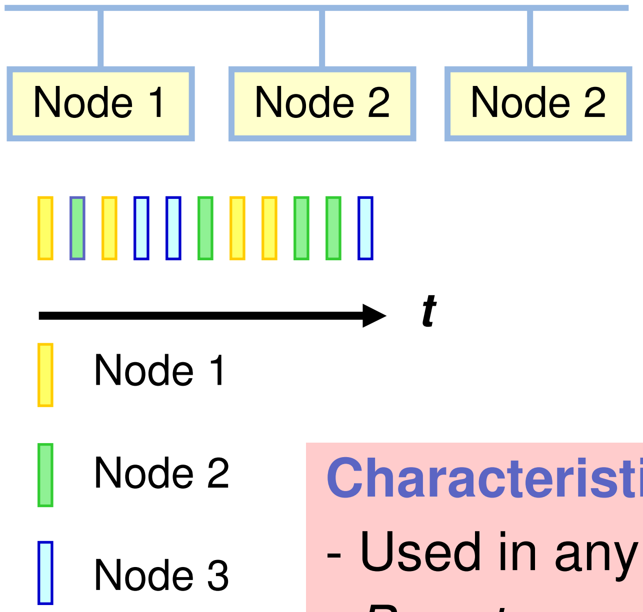
- The master has always access to the bus
- Slaves are polled in a fixed sequence by the master
- Slaves may respond by sending data

Examples: IEC 60870-5 (-101, 103), DNP3, etc. (Layers 1, 2, 7)

Characteristics

- Used in any topology
- No direct slave to slave communication
- Polling rate *depending on master*/transport media
- *Deterministic* response time
- Centralized transport media arbitration (bus administrator)

Time Divison Multiplex Media Access



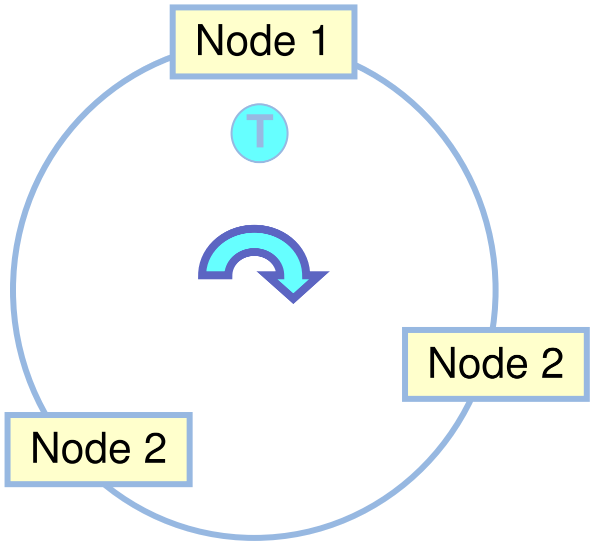
- Each node has its own time slot
- Node may send during this time

Examples: IEC 61375 (MVB) (Layers 1, 2, 7+)

Characteristics

- Used in any topology
- *Peer-to-peer* communication
- Fixed time slot *independent of the network load*
- *Deterministic* response time (no collisions)
- Centralized transport media arbitration (bus administrator)

Token Passing



- Token circulates around ring
- Any node may take the token as it passes by
- Take token, send data, pass token

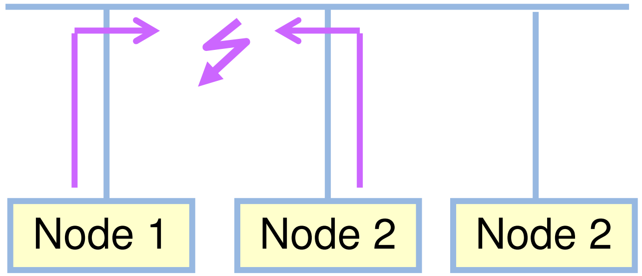
Examples: PROFIBUS (Layers 1, 2, 7)

Characteristics

- Used in any topology
- *Semi-deterministic* response time (no collisions, but token)
- Unnecessary *waiting times* with low network load
- Decentralized, token dependent transport media arbitration

CSMA/CD Media Access

Carrier Sense Multiple Access / Collision Detection



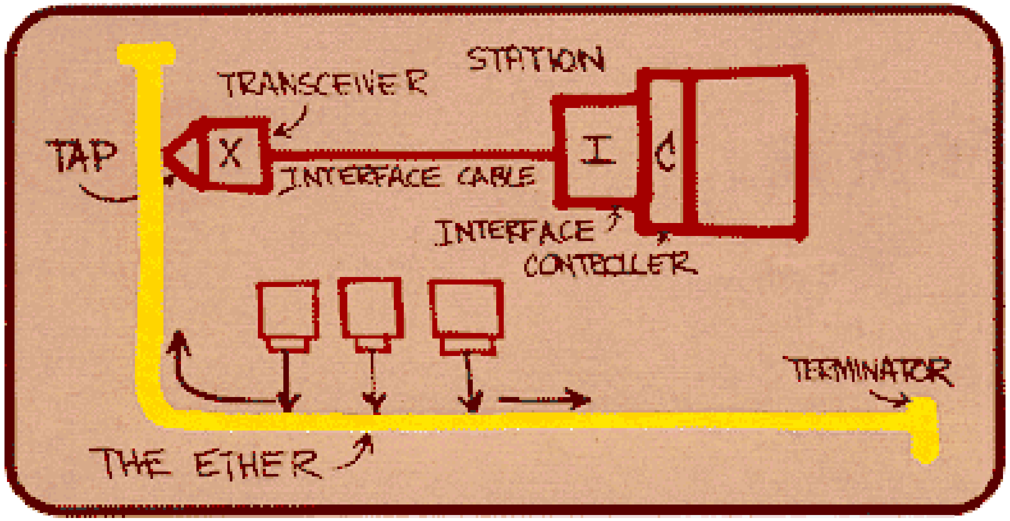
Ethernet Principle

- Each node listens to bus
- If bus is idle try to send
- If collision, try again :
  - stop transmission
  - send jamming signal
  - wait

Characteristics

- Used in bus topology
- Equal access rights for every node
- Response time *not determinable*
- No transport media arbitration (no bus administrator)

The First Ethernet



Bob Metcalfe, 1976

- 1976: Ethernet developped in Xerox Labs
- 1982: First Ethernet Specification from Digital, Intel, Xerox (DIX)
- 1985: First **IEEE 802.3** standard published

Features of Ethernet

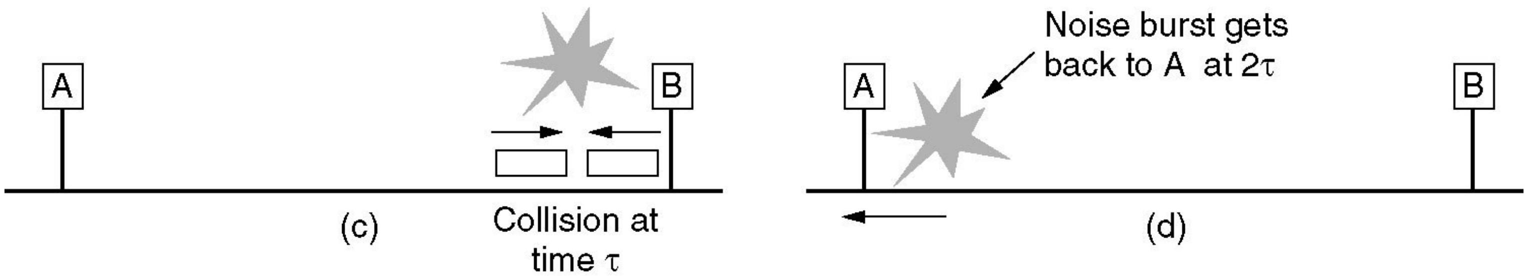
- Ethernet uses multiple access algorithm 1-persistent CSMA/CD
  - Easy decentralized algorithm
  - Very cheap implementations available
  - Ideal for transportation of best-effort traffic
- Ethernet communicates unacknowledged and connectionless
  - Ideal for transmission of IP-packets
- Ethernet is continuously improved regarding performance
  - ~3 MBit/s → 10 MBit/s → 100 MBit/s → 1.000 MBit/s → 10.000 MBit/s → ?
- Ethernet is standardized with IEEE 802.3
  - in IEEE 802 lots of Protocols for physical und data link layer are standardized
- Ethernet is the dominating LAN technology since years
- Ethernet is the communication technology where the most money is put in

Ethernet Problems by definition

- Ethernet's peak utilization is pretty low
  - Collisions limit the utilization of full bandwidth
- Peak throughput gets more worst with
  - more hosts
    - More collisions needed to identify single sender
  - smaller packet sizes
    - More frequent arbitration
  - longer links
    - Collisions take longer to observe, more wasted bandwidth
- Efficiency is improved by avoiding these problems

Collisions are causing the problems

- Collisions are caused when two nodes/adaptors try to transmit at the same time (adaptors sense collision based on voltage differences)
  - Both found line to be idle
  - Both had been waiting to for a busy line to become idle x



Collision detection can take as long as 2τ.

Content

IEC 61850 Engineering

Reference to IEC 61850-6

- SCL
- Engineering process
- Tools

Formal description of system structure

To provide interoperability

- a **formal** description of the Substation Automation System with all *communication links* is needed
- all *IED capabilities* have to be described **formally** in an unambiguous way
- all *communication services* applicable have to be described **formally** in an unambiguous way
- the relationship between the switchgear (*single line*) and the functions of the substation automation system represented by objects (LD, LN, etc.) have to be described **formally** in an unambiguous way

Formal description means SCL

The formal description is provided by the
Substation Configuration description Language (SCL)

- based on XML
- defined in part 6 of the standard (IEC 61850-6)
- usable for

  - IED Capability Description (ICD) files

  - System Configuration Description (SCD) file

  System functional specification (SSD)

The engineering information

is exchangeable between tools,

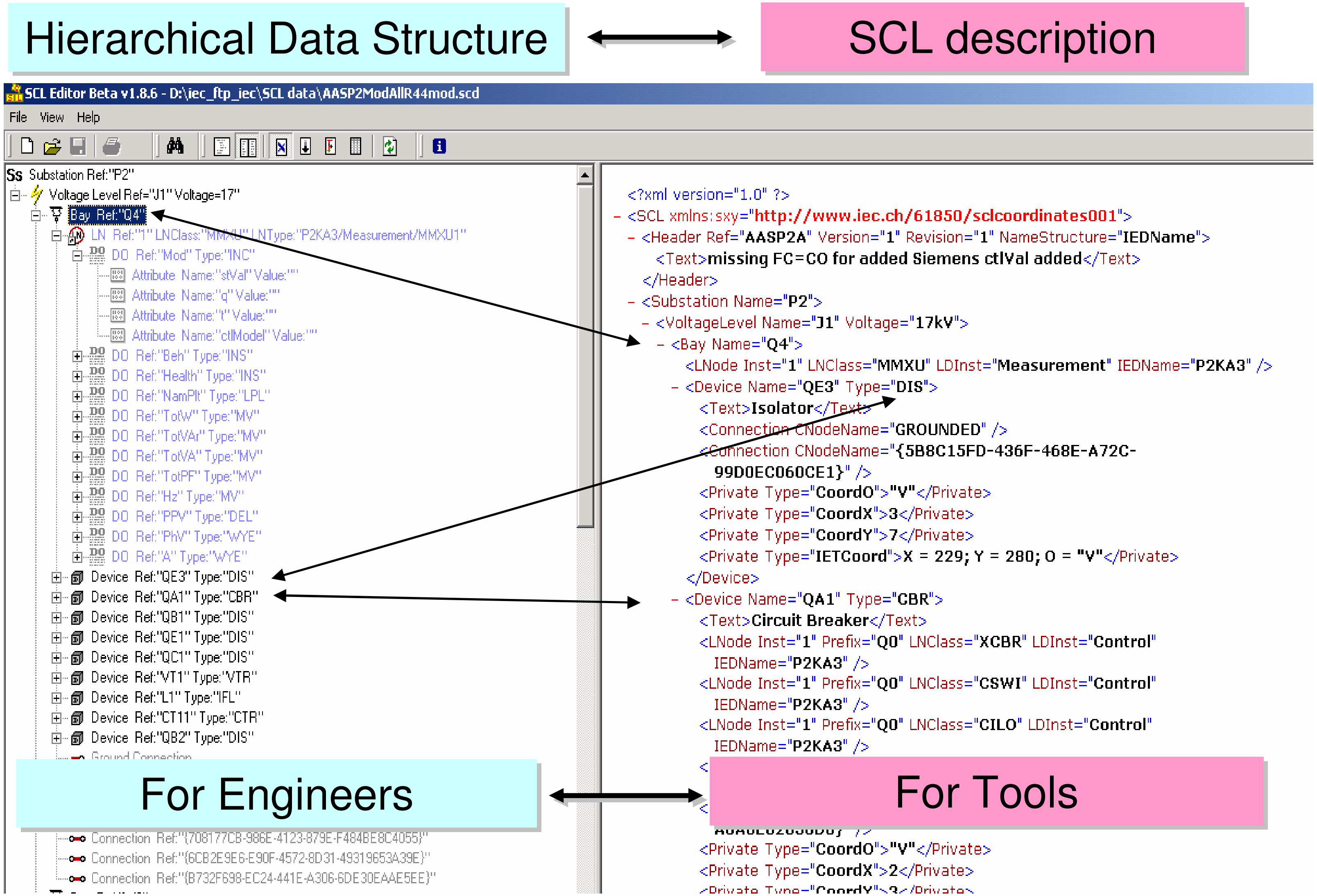
the tools get interoperable !!!bb

Example for SCL

```
<Substation Ref="">
   <VoltageLevel Ref="E1">
      <Bay Ref="Q1">
         <Bfunction Ref="">
            <Device Ref="QA1" Type="CBR">
               <Connection NodeRef="L1"/>
               <LNode Ref="1"
LNClass="CSWI"/>
            </Device>
            <Device Ref="QB1" Type="DIS">
               <Connection NodeRef="L1"/>
               <LNode Ref="2"
LNClass="CSWI"/>
            </Device>
         </Bfunction>
      </Bay>
   </VoltageLevel>
</Substation>
```

Described is a substation with the **bay E1Q1**, the **Circuit breaker QA1** and the **Isolator QB1**, both electrical connected in **Connection Node L1**. The Controller is represented by - **LN CSWI** controls both switches.

Data structure and SCL



Engineering and IEC 61850

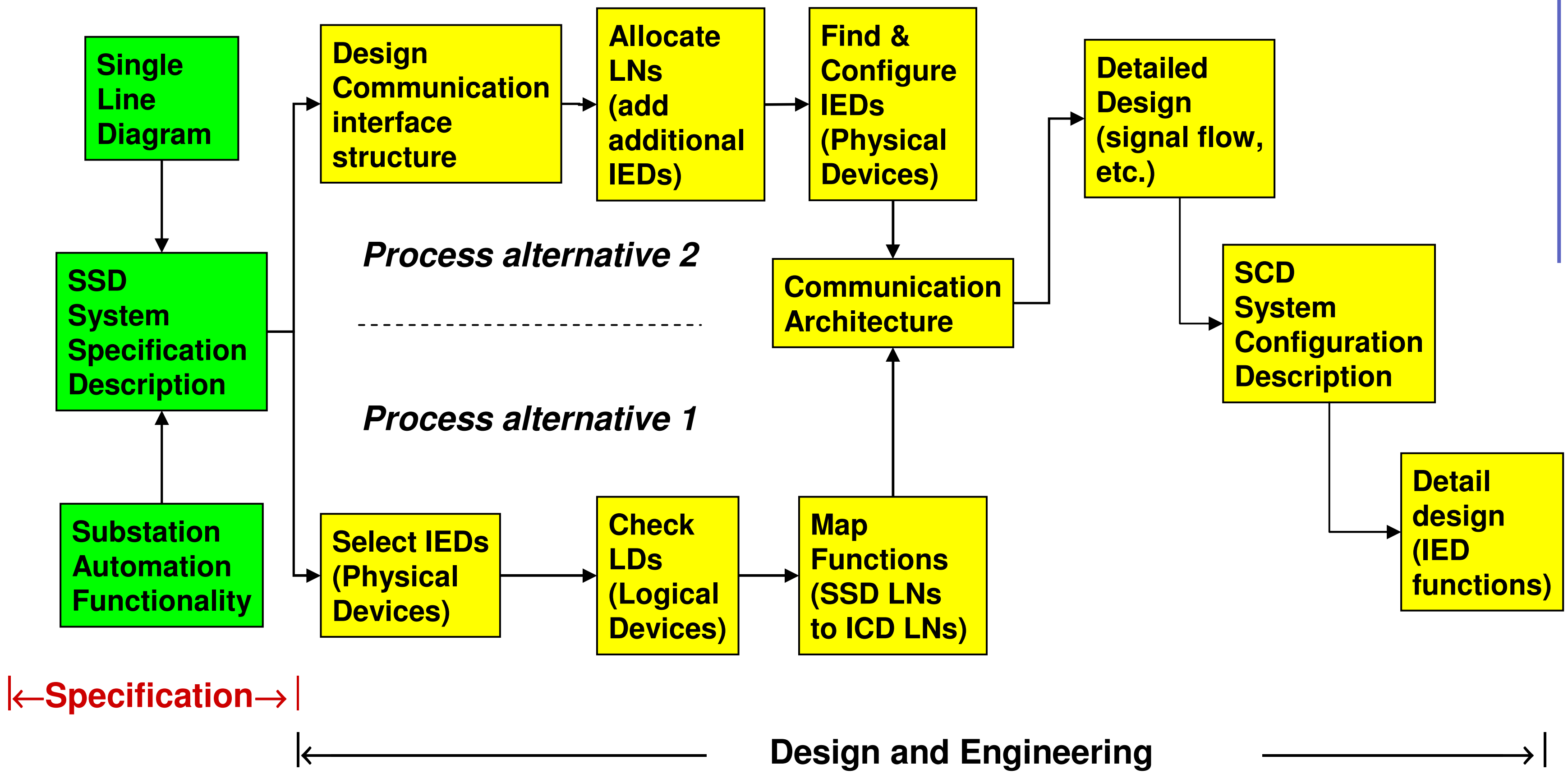
Reminder:

- **The SA functions and devices are not standardized**
- **The SA architecture is not standardized**
- **Data and data exchange is standardized**

Note:

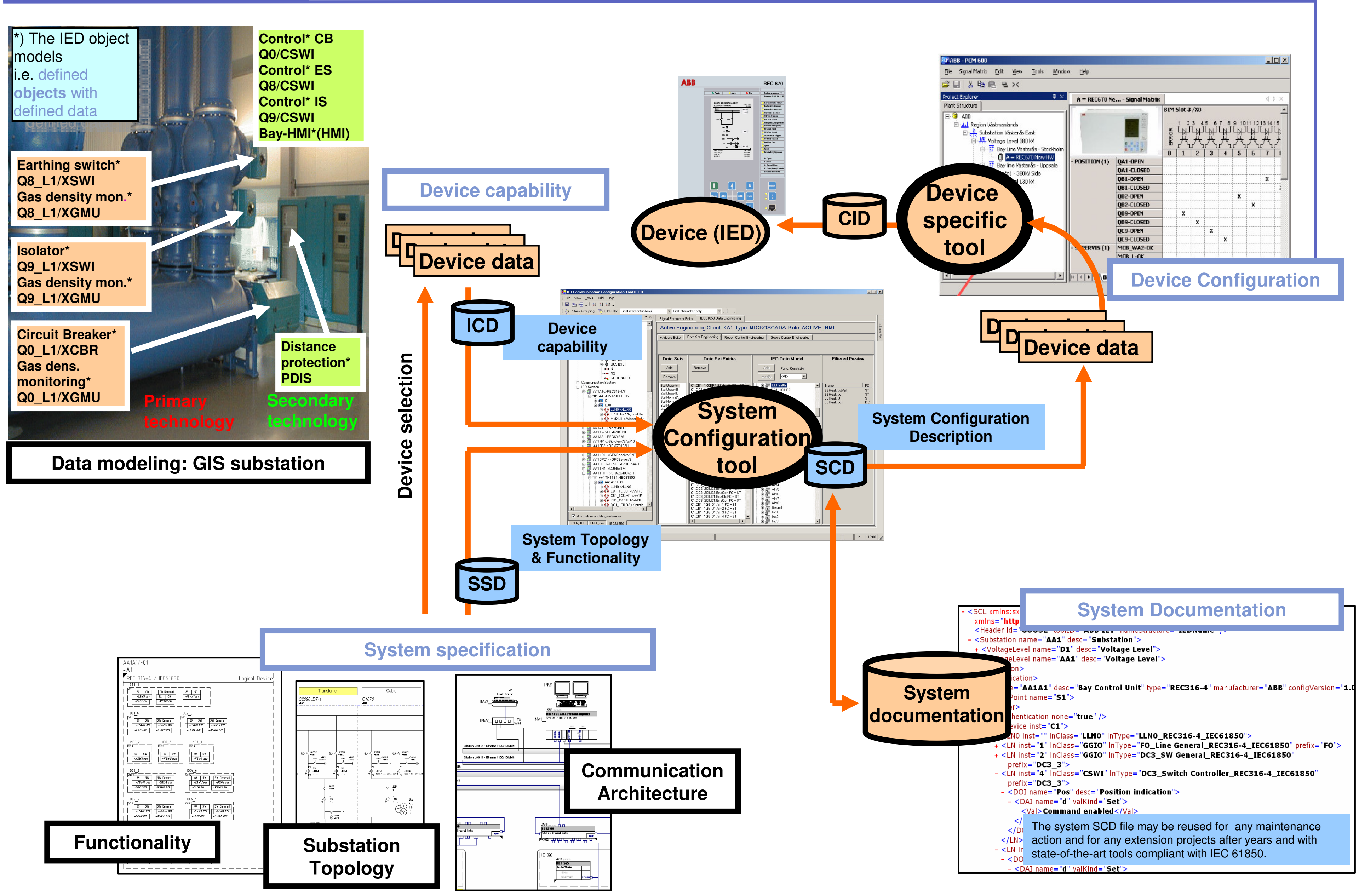
- **The engineering tools are not standardized**
- **The engineering process is not standardized**
- **The configuration description is standardized (SCL)**

Process from Specification to Solution



Engineering Process

Engineering according to IEC 61850



Engineering according to IEC 61850

ICD

IED Capability Description file
Device on the shelf - mandatory

SSD

System Specification Description file
Single line and function allocation

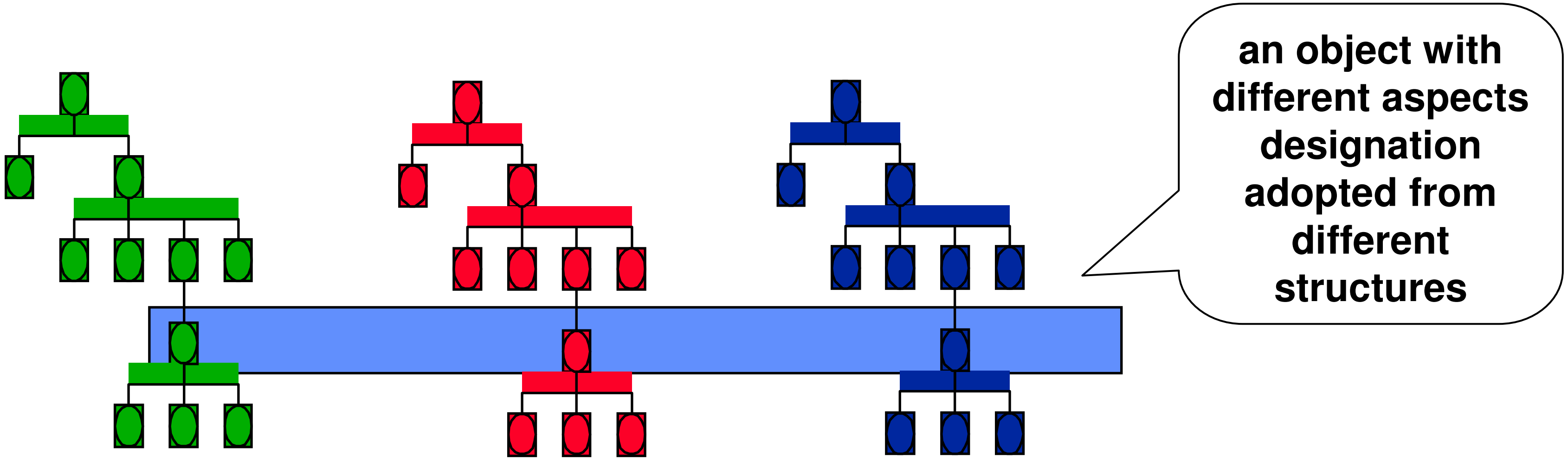
SCD

System Configuration Description file
Configured system description

CID

Configuration IED Description file
Configured IED description incl.
device specific data beyond IEC 61850

Project Structures / Engineering Aspects



Geographic, Location, Placement structure

Function, Software, Data (Product) structure

Devices / Physics, Hardware (Product) structure

Interface to environment or external world

- **Seguridad en las comunicaciones IEC 61850**

  - ***Incidentes recientes de seguridad***: como BlackEnergy y CrashOverride (malware con un módulo exclusivo para comunicaciones IEC 61850) dejan claro que las **empresas de distribución eléctrica no están libres de ser objetivo de ataques.**

  - ***Se han visto involucrados ciertos protocolos industriales, incluido el IEC 61850***, (necesidad de aumentar el conocimiento y la seguridad sobre estas comunicaciones).

- ***Las debilidades de seguridad fueron abordadas dentro del estándar IEC 62351***, en el que se presentan las medidas y mecanismos a seguir para solucionar o mitigar estos problemas y evitar o paliar la mayoría de estos ataque.

- ***El estándar IEC 62351*** establece el uso de las siguientes ***medidas para garantizar la seguridad de las comunicaciones***:
  - Cifrado
  - Autenticación
  - Los mensajes deberán soportar el uso de etiquetas VLAN.
  - Protección frente a retransmisión de paquetes GOOSE
  - Protección frente a retransmisión de paquetes SMV

- **Herramientas de seguridad adicionales**

➢ Un ***NIDS*** (*Network Intrusion Detection System*) con inspección profunda de paquetes (Deep Packet Inspection, DPI) permite realizar una monitorización del tráfico de la subestación eléctrica y detectar posibles anomalías en la red.