ILLINOIS
SECURITY LAB

IEC 61850 - Communication Networks and Systems in Substations: An Overview of Computer Science

Jianqing Zhang and Carl A. Gunter
University of Illinois at Urbana-Champaign

Agenda

ILLINOIS SECURITY LAB

- Overview
- Data modeling approach
- Communication model
- Communication service mapping
- Sampled measured values
- Configuration description language
- Conclusion
- Reference

Background I: Power Substation

ILLINOIS SECURITY LAB

Intelligent Electronic Device

- Microprocessor-based controllers of power system equipment
  - e.g. circuit breaker, protective relay…

- Receive digitalized data from sensors and power equipment

- Issue control commands in case of anomalies to maintain the desired status of power grid
  - e.g. tripping circuit breakers

Why Standards Are Needed

- Interoperability and Integration
  - No standard for data representation or how devices should look and behave to network applications
- Intuitive device and data modeling and naming
  - Hierarchical and structured, rather than plain formatted
- Fast and convenient communication
- Lower cost for installation, configuration and maintenance
  - Wire connected legacy devices

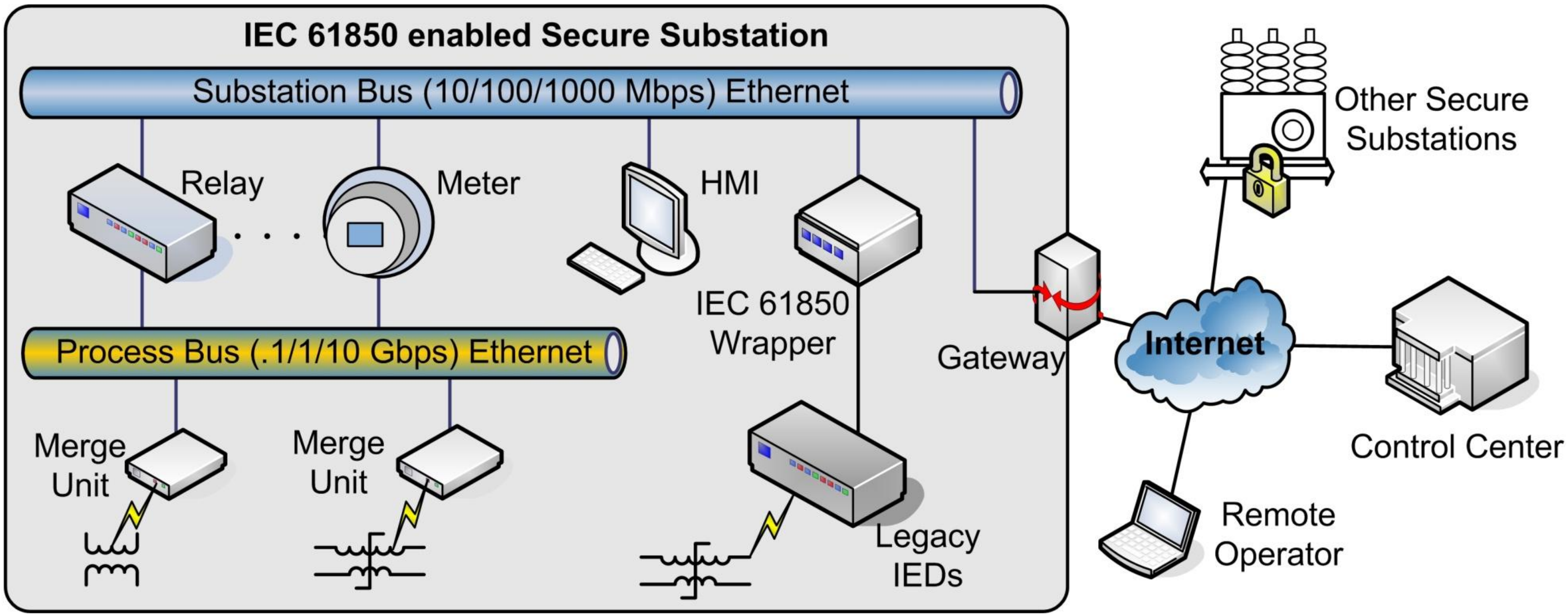
History of IEC 61850

UCA: Utility Communication Architecture
- Protocols
- Data models
- Abstract service definitions

IEC 61850

IEC 60870-5
- A communication profile for sending basic telecontrol messages between two systems
- Based on permanent directly connected data circuits

IEC 61850 Substation Architecture



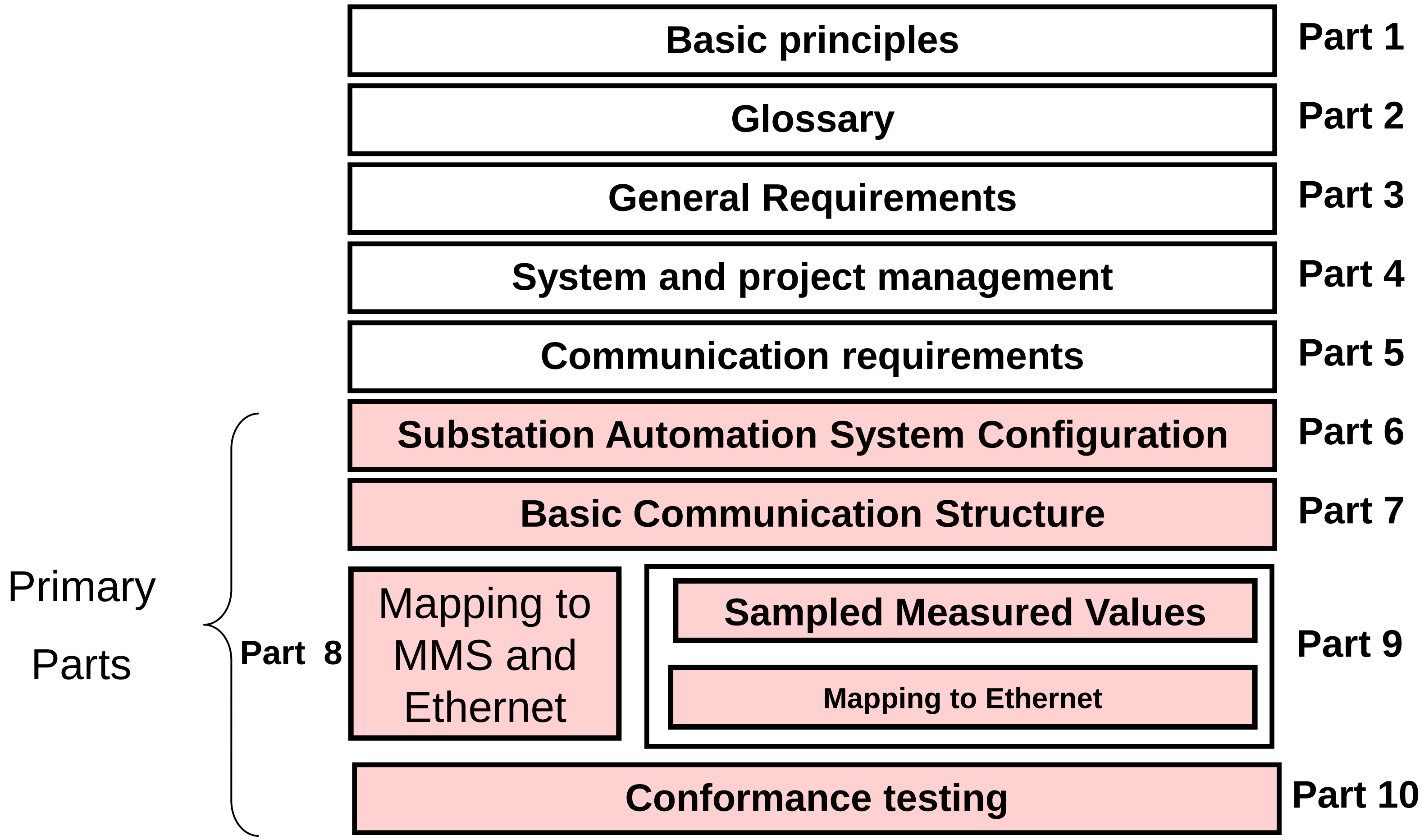
- IEC61850-enabled IEDs get digitalized power grid condition data via process bus and merge units
- IEDs communicate with each other using substation buses
- Legacy devices use IEC61850 wrapper

Core Components of IEC 61850

ILLINOIS SECURITY LAB

- An object model describing the information available from the different primary equipment and from the substation automation functions
  - Abstract definitions of services, data and Common Data Class, independent of underlying protocols
- A specification of the communication between the IEDs of the substation automation system.
  - Maps the services to actual protocols
- A configuration language
  - Exchange configuration information

IEC 61850 Standards



IEC 61850 Primary Parts

ILLINOIS SECURITY LAB

- Part 6-1: Substation Configuration Language (**SCL**)
- Part 7-2: Abstract Communications Service Interface (**ACSI**) and base types
- Part 7-3: Common Data Classes (**CDC**)
- Part 7-4: Logical Nodes
- Part 8-1: Specific Communications Service Mappings (**SCSM**) - MMS & Ethernet
- Part 9-2: SCSM - Sampled Values over Ethernet
- Part 10-1: Conformance Testing

IEC 61850 Is Unique

- Not a recast serial RTU protocol
- Designed specifically for LANs to lower life cycle cost to use a device:
  - Cost to install, configure, and maintain
- Real object-oriented approach for SA:
  - Supports standardized device models using names instead of object/register numbers and indexes.
  - Standardized configuration language (SCL).
  - Feature rich with support for functions difficult to implement otherwise.

Benefits of IEC 61850

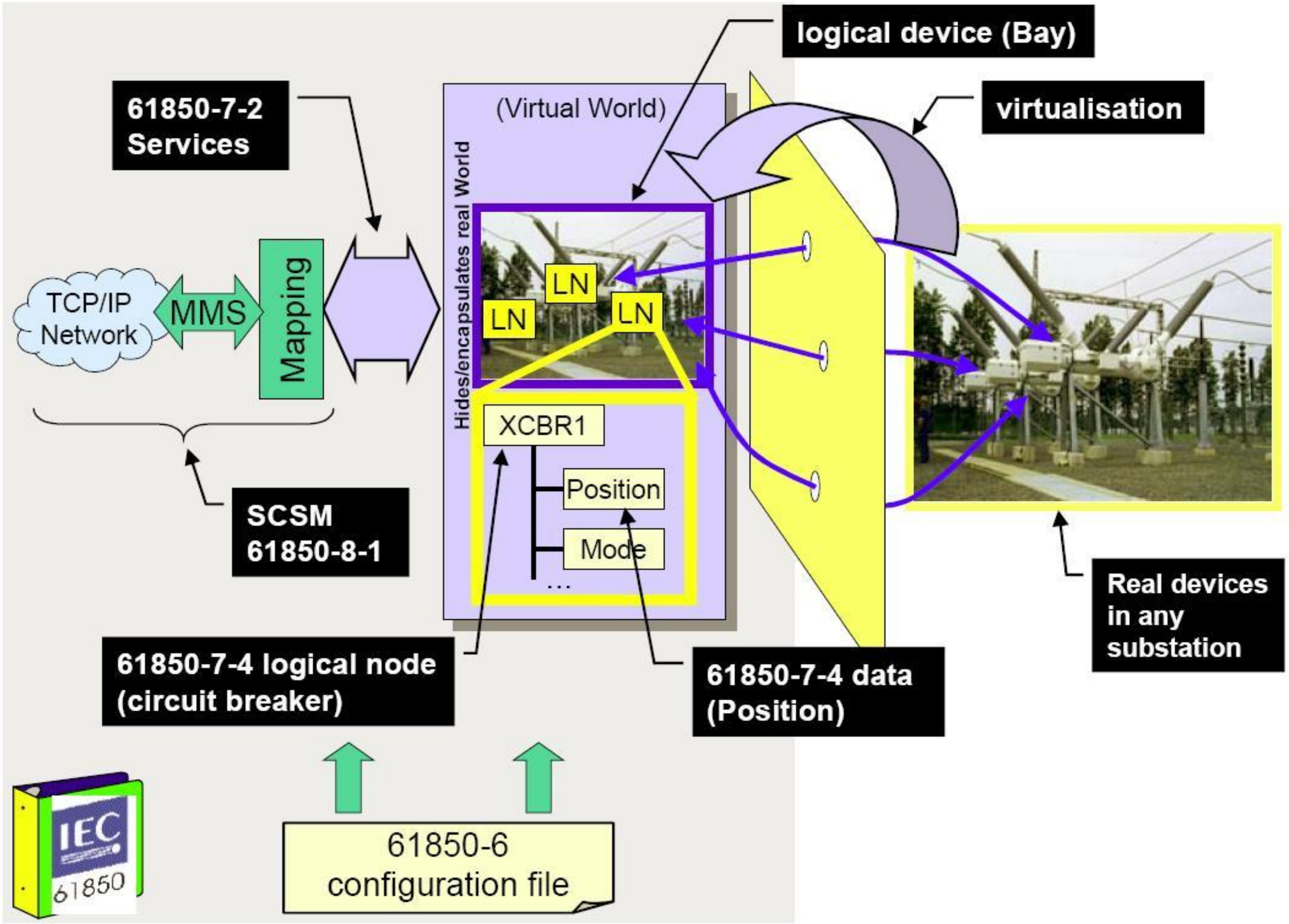
- Supports a comprehensive set of substation functions
- Easy for design, specification, configuration, setup, and maintenance.
  - High-level services enable self-describing devices & automatic object discovery
  - Standardized naming conventions with power system context
  - Configuration file formats eliminate device dependencies and tag mapping and enables exchange of device configuration.
- Strong functional support for substation communication
  - Higher performance multi-cast messaging for inter-relay communications
- Extensible enough to support system evolution

Agenda

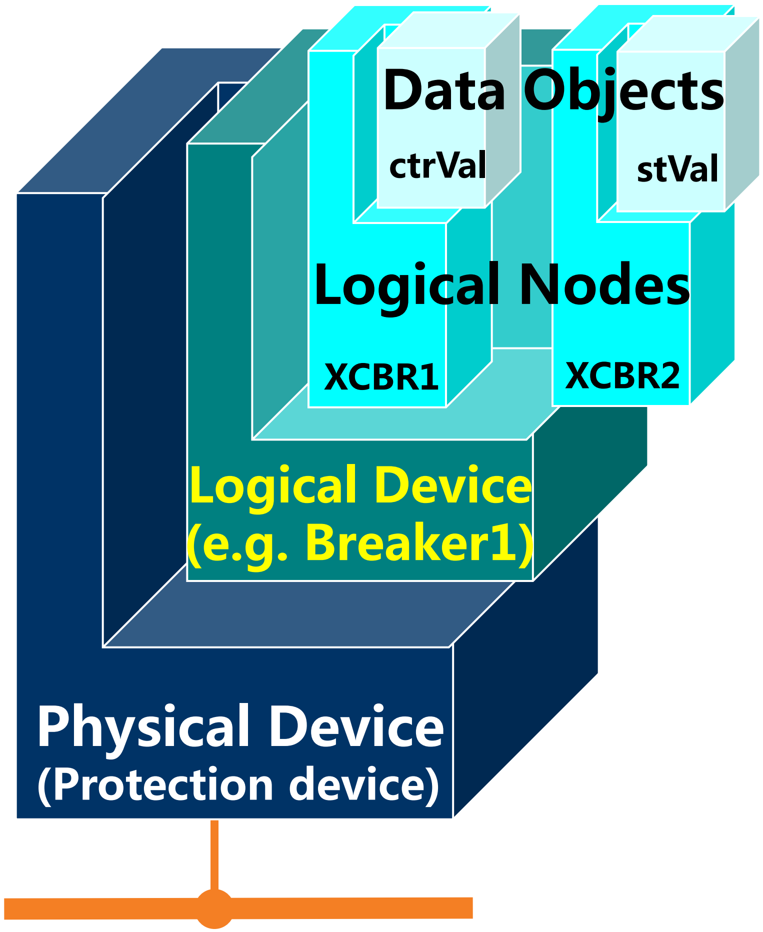
ILLINOIS SECURITY LAB

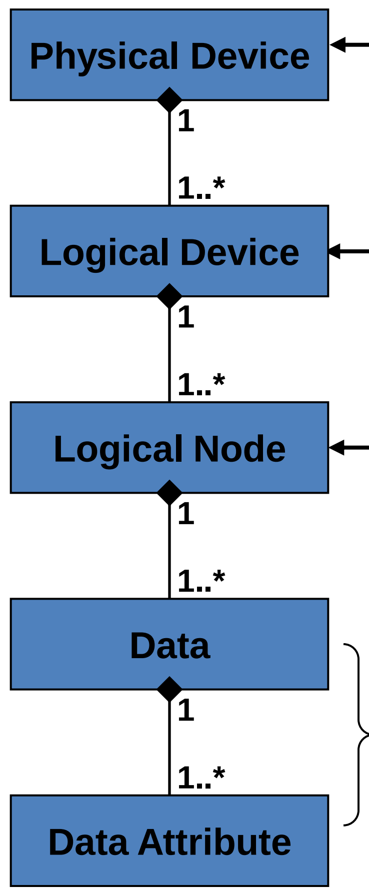
- Overview
- Data modeling approach
- Communication model
- Communication service mapping
- Sampled measured values
- Configuration description language
- Conclusion
- Reference

IEC 61850 Modeling Approach



IEC 61850 Class Model





Access by network address

Collections of logical nodes, implemented in one IED, i.e. not distributed

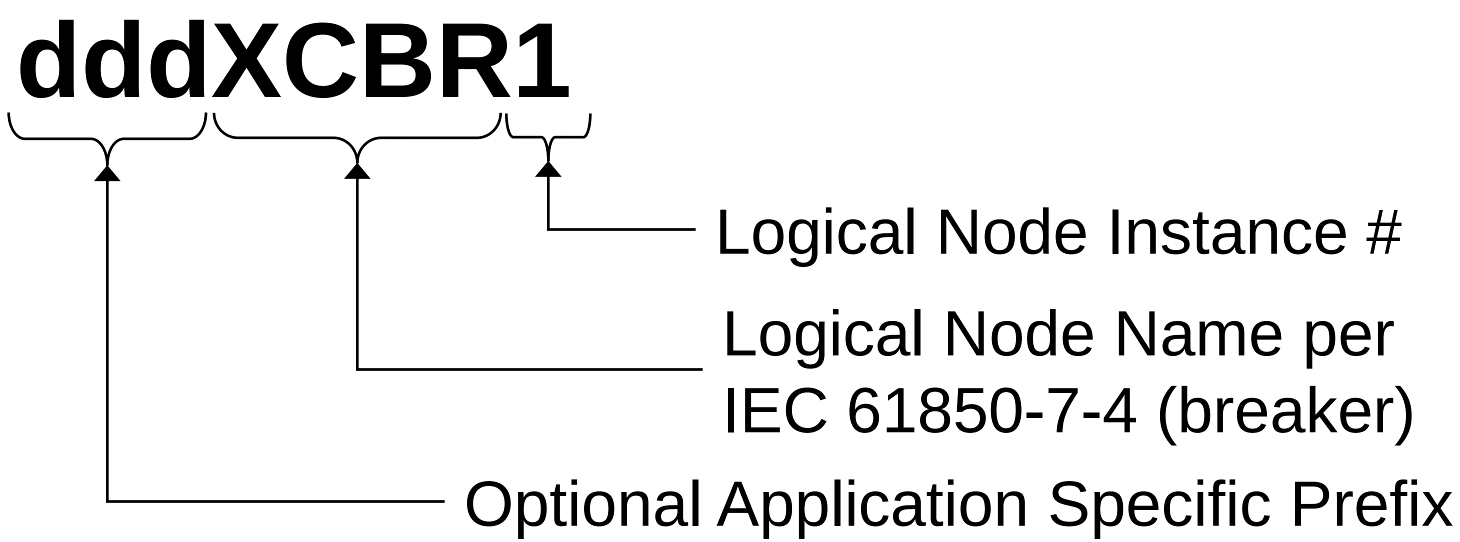
Functions in the real devices e.g. XCBR: circuit breaker

Properties of logic nodes e.g. Position

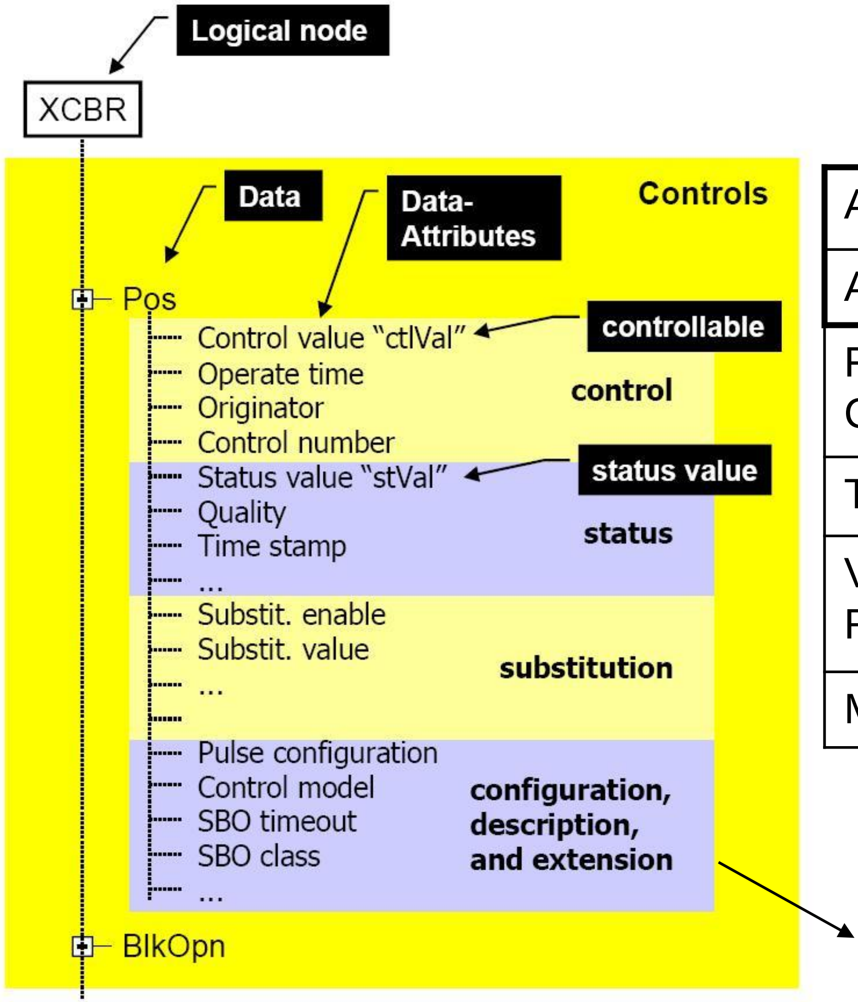
- Dedicated data values
- Structured and well-defined semantic
- Exchanged according to well-defined rules and performance
- Configuration: assign selected values and exchange mechanisms

Logical Node

- A named grouping of data and associated services that is logically related to some power system function.



Data Example of Logical Node



Attr. Name	ctrVal	stVal
Attr. Type	BOOLEAN	CODED ENUM
Functional Constraint	CO	ST
TrgOp		dchg
Value/Value Range	OFF (False) | ON (True)	off | on | bad-state
M/O/C	O	M

Common Data Class: Double Points Control

Logical Nodes Information Categories

- **Common logical node information**
  - Information independent from the dedicated function represented by the LN, e.g., mode, health, name plate, ...
- **Status information**
  - Information representing either the status of the process or of the function allocated to the LN, e.g., switch type, switch operating capability
- **Settings**
  - Information needed for the function of a logical node, e.g., first, second, and third reclose time
- **Measured values**
  - Analogue data measured from the process or calculated in the functions like currents, voltages, power, etc., e.g., total active
  - power, total reactive power, frequency
- **Controls**
  - Data, which are changed by commands like switchgear state (ON/OFF), resetable counters, e.g., position, block opening
- **88 pre-defined logical nodes and extensible**

Logical Node Class Example - XCBR

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				
		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

Single Point Status (SPS) CDC (e.g. Loc)

SPS class					
Attribute Name	**Attribute Type**	**FC**	**TrgOp**	**Value/Value Range**	**M/O/C**
DataName	Inherited from Data Class (see IEC 61850-7-2)				
DataAttribute					
				status	
stVal	BOOLEAN	ST	dchg	TRUE | FALSE	M
q	Quality	ST	qchg		M
t	TimeStamp	ST			M
				substitution	
subEna	BOOLEAN	SV			PICS_SUBST
subVal	BOOLEAN	SV		TRUE | FALSE	PICS_SUBST
subQ	Quality	SV			PICS_SUBST
subID	VISIBLE STRING64	SV			PICS_SUBST
				configuration, description and extension	
d	VISIBLE STRING255	DC		Text	O
dU	UNICODE STRING255	DC			O
cdcNs	VISIBLE STRING255	EX			AC_DLNDA_M
cdcName	VISIBLE STRING255	EX			AC_DLNDA_M
dataNs	VISIBLE STRING255	EX			AC_DLN_M

↑ Attribute Name

↑ Type

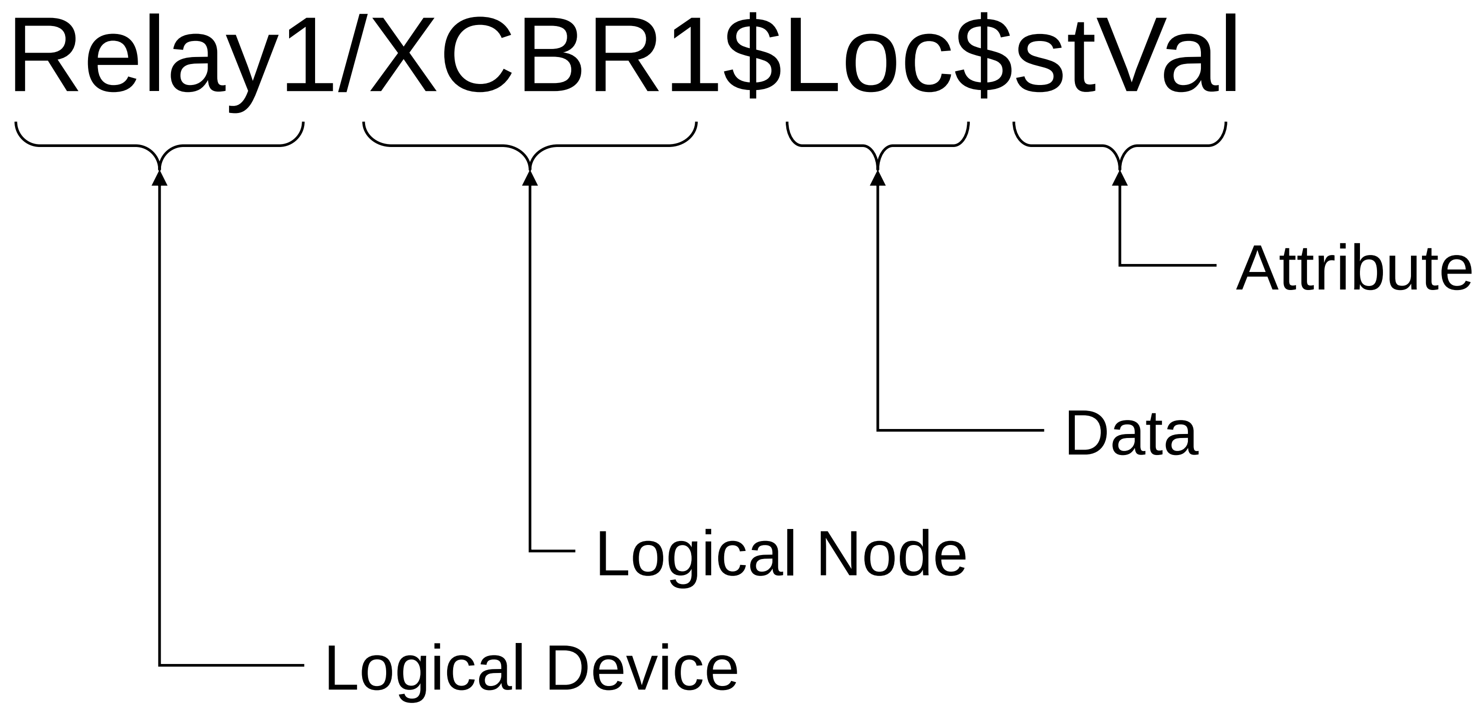
↑ Functional Constraint

↑ Range of Values

↑ Mandatory/ Optional

Object Name Structure

ILLINOIS SECURITY LAB

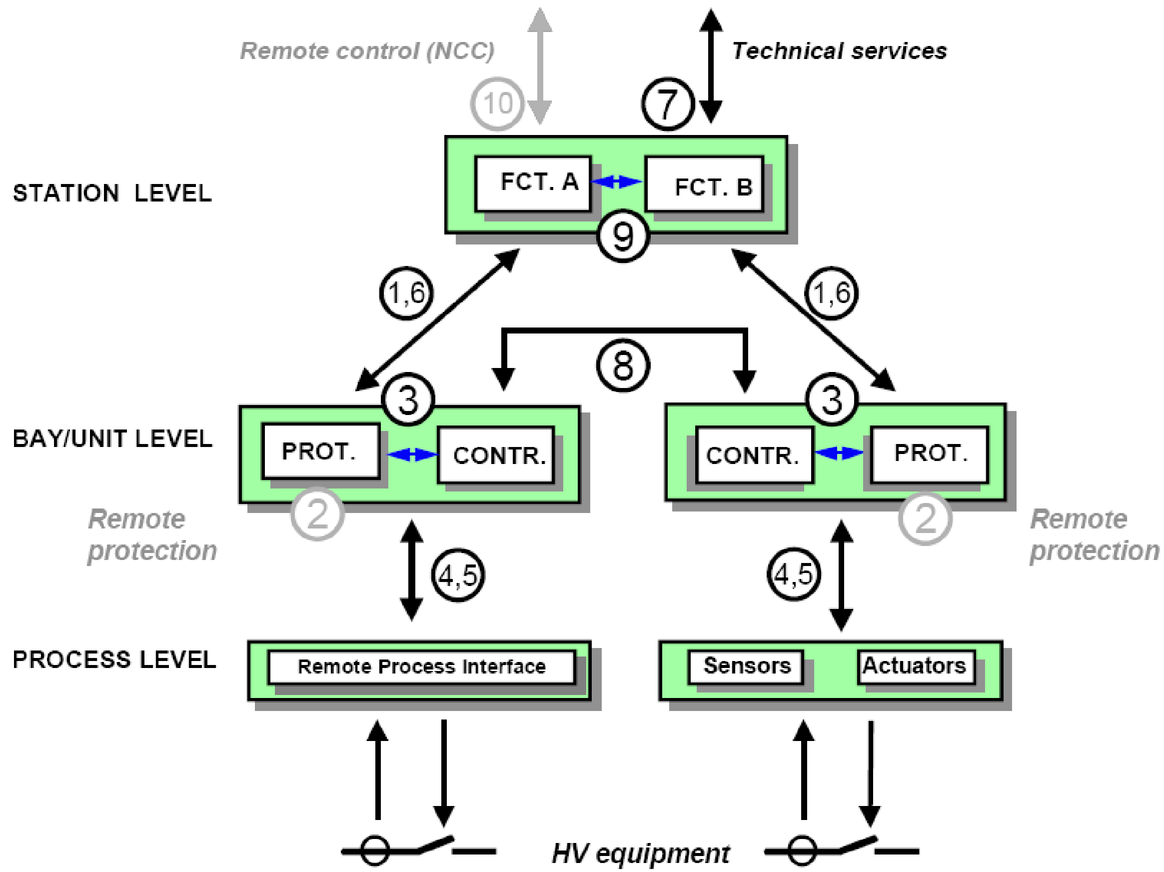


Agenda

- Overview
- Data modeling approach
- Communication model
- Communication service mapping
- Sampled measured values
- Configuration description language
- Conclusion
- Reference

IEC 61850 Communication Scope

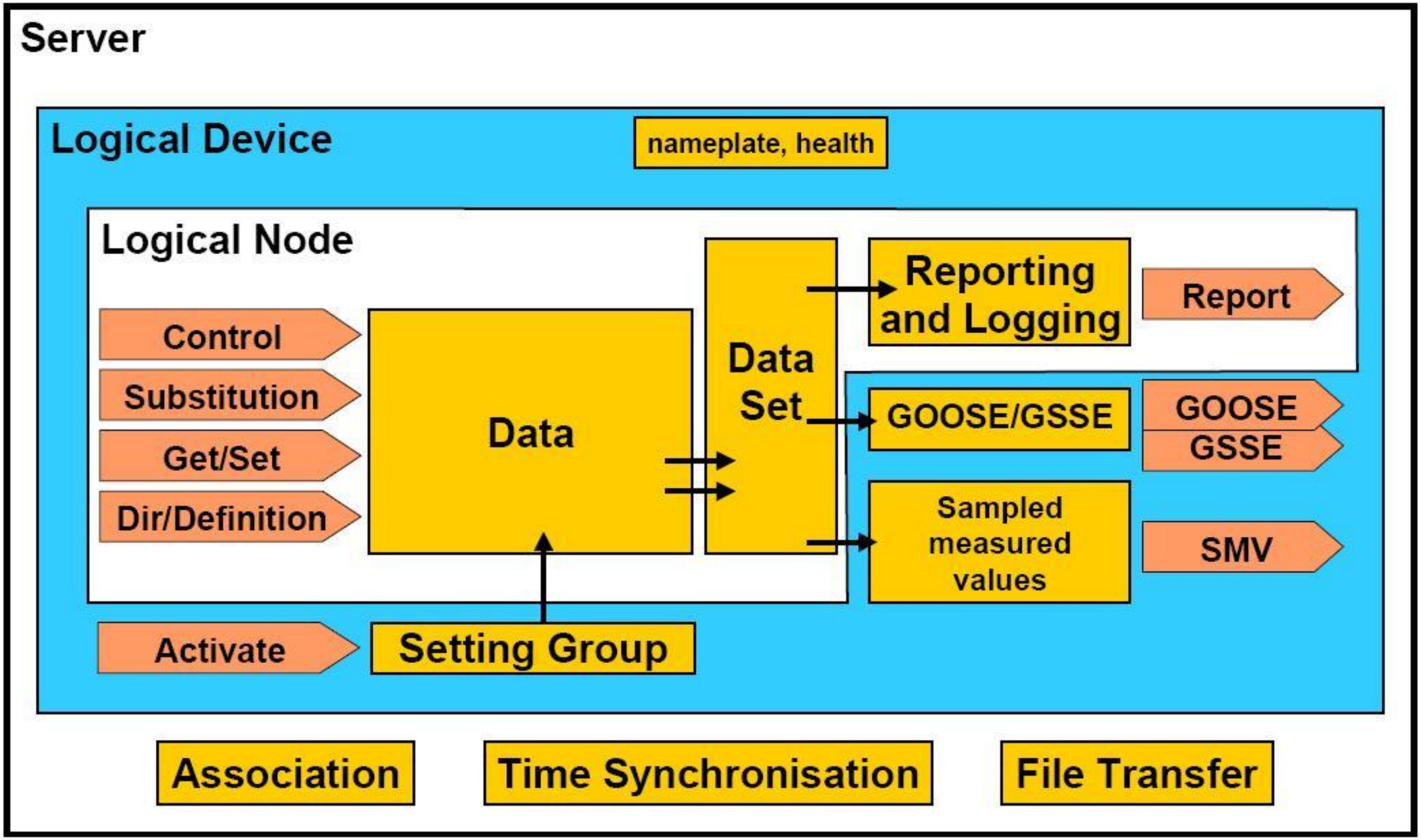
1. Protection-data exchange between bay and station level
2. Protection-data exchange between bay level and remote protection
3. Data exchange within bay level
4. CT and VT instantaneous data exchange between process and bay levels
5. Control-data exchange between process and bay level
6. Control-data exchange between bay and station level
7. Data exchange between substation and remote engineer’s workplace
8. Direct data exchange between the bays especially for fast functions like interlocking
9. Data exchange within station level
10. Control-data exchange between substation (devices) and a remote control center



ACSI: Abstract Communications Service Interface

- None timing critical message transmitting
- Used for configuration, maintenance, log…
- Three basic components
  - A set of objects
  - A set of services to manipulate and access those objects
  - A base set of data types for describing objects

ACSI Server Building Block



Basic Information Models

- SERVER
  - Represents the external visible behavior of a (physical) device
  - Communicate with a client
  - Send information to peer devices

- LOGICAL-DEVICE (LD)
  - Contains the information produced and consumed by a group of domain-specific application functions, which are defined as LOGICAL-NODEs

- LOGICAL-NODE (LN)
  - Contains the information produced and consumed by a domain specific application function

- DATA
  - Status and meta-information of object it presents in substation
  - Provide means to specify typed information

Services Operating on Data

- DATA-SET
  - The grouping of data and data attributes
  - A view of DATA
- SETTING-GROUP
  - How to switch from one set of setting values to another one
  - How to edit setting groups
- REPORT and LOG
  - Describe the conditions for generating reports and logs based on parameters set by the client
  - Reports may be sent immediately or deferred
  - Logs can be queried for later retrieval
- Generic Substation Event (GSE) control block (GSSE/GOOSE)
  - Supports a fast and reliable system-wide distribution of input and output data values
- Sampled Values Transmission control block
  - Fast and cyclic transfer of samples

Services Operating on Data (cont.)

ILLINOIS SECURITY LAB

- Control
  - Provide client mechanisms to control the DATA related to external devices, control outputs, or other internal functions
- Substitution
  - Support replacement of a process value (measurands of analogue values or status values) by another value
- Get/Set
  - Retrieve or write particular DataAttribute Values
- Dir/Definition
  - Retrieve ObjectReferences and definitions of all sub-objects.

Other Services

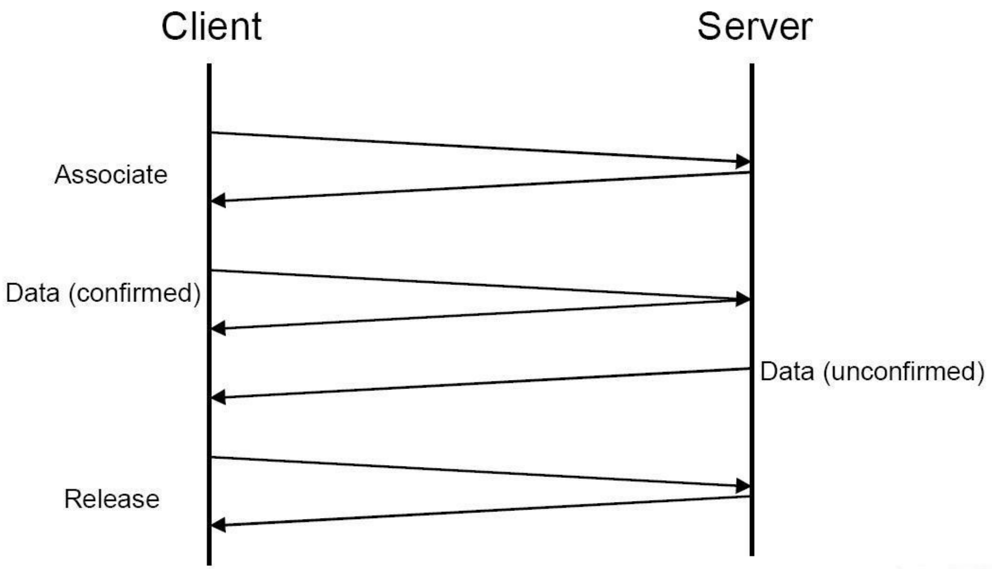
- Association
  - How the communication between the various types of devices is achieved
  - Two-party and Multicast
  - Access Control
- Time Synchronization
  - Provide the UTC synchronized time to devices and system
- File Transfer
  - Defines the exchange of large data blocks such as programs

Communication Model

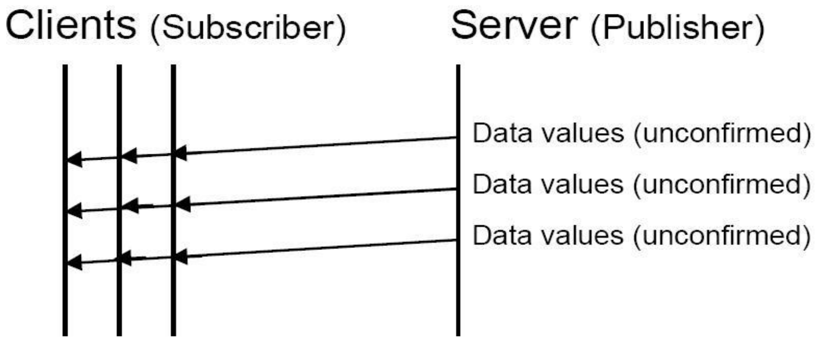
- Two-Party-Application-Association (TPAA)
  - A bi-directional connection-oriented information exchange
  - Reliable and end-to-end flow control

- MultiCast-Application-Association (MCAA)
  - A unidirectional information exchange
  - Between one source (publisher) and one or many destinations (subscriber)
  - The subscriber shall be able to detect loss and duplication of information received
  - The receiver shall notify the loss of information to its user and shall discard duplicated information

Principle of TPAA and MCAA



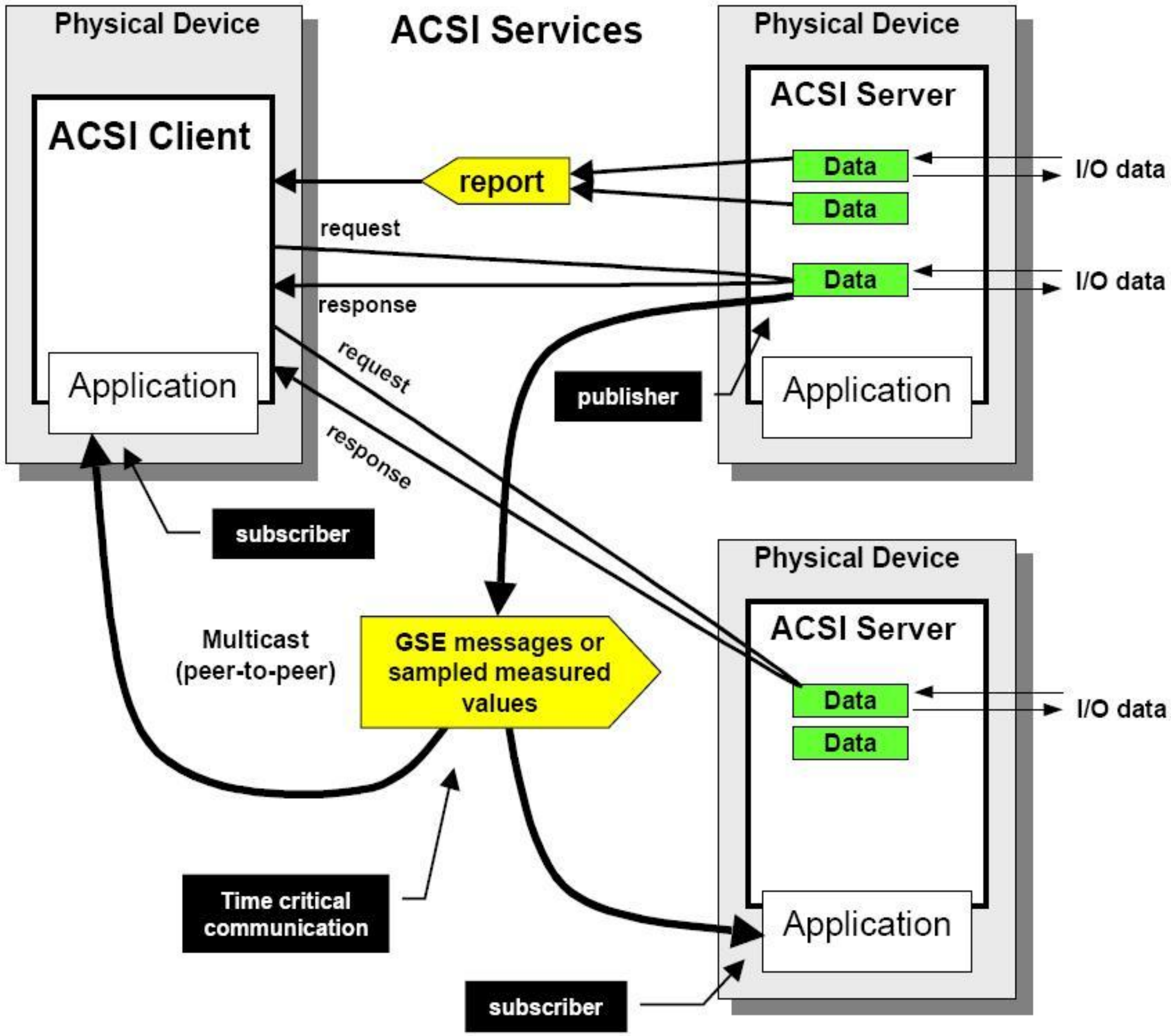
Two-Party-Application-Association



MultiCast-Application-Association

ACSI Communication Model

ILLINOIS SECURITY LAB



Generic Substation Event (GSE) Model

ILLINOIS SECURITY LAB

- A fast and reliable system-wide distribution of input and output data values
- Based on a publisher/subscriber mechanism
- Simultaneous delivery of the same generic substation event information to more than one physical device through the use of multicast/broadcast services
- GSSE/GOOSE

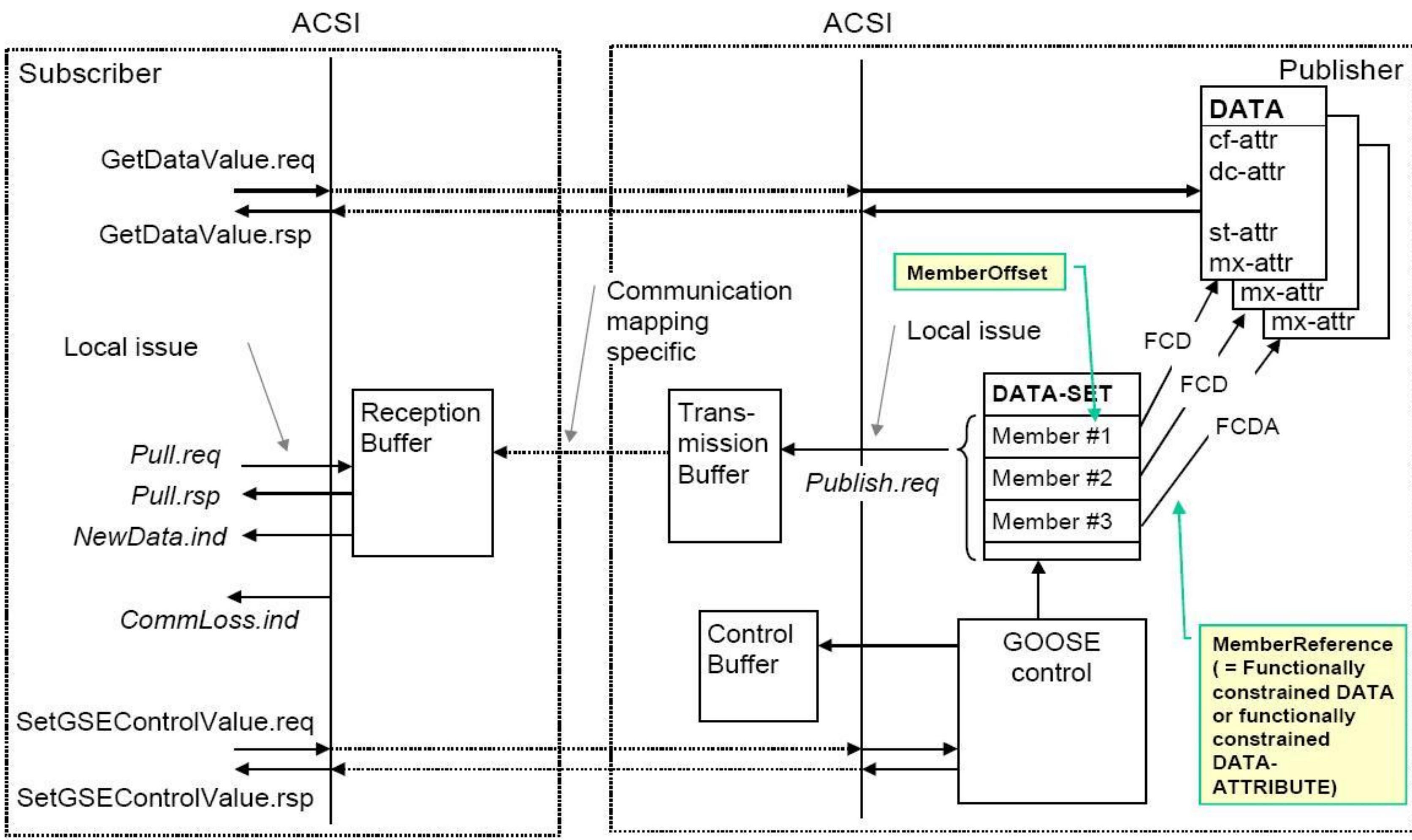
GOOSE: Generic Object Oriented Substation Event

- Used for fast transmission of substation events, such as commands, alarms, indications, as messages
- A single GOOSE message sent by an IED can be received several receivers
- Take advantage of Ethernet and supports real-time behavior
- Examples:
  - Tripping of switchgear
  - Providing position status of interlocking

Generic Object Oriented Substation Event (GOOSE)

ILLINOIS SECURITY LAB

- Exchange of a wide range of possible common data organized by a DATA-SET

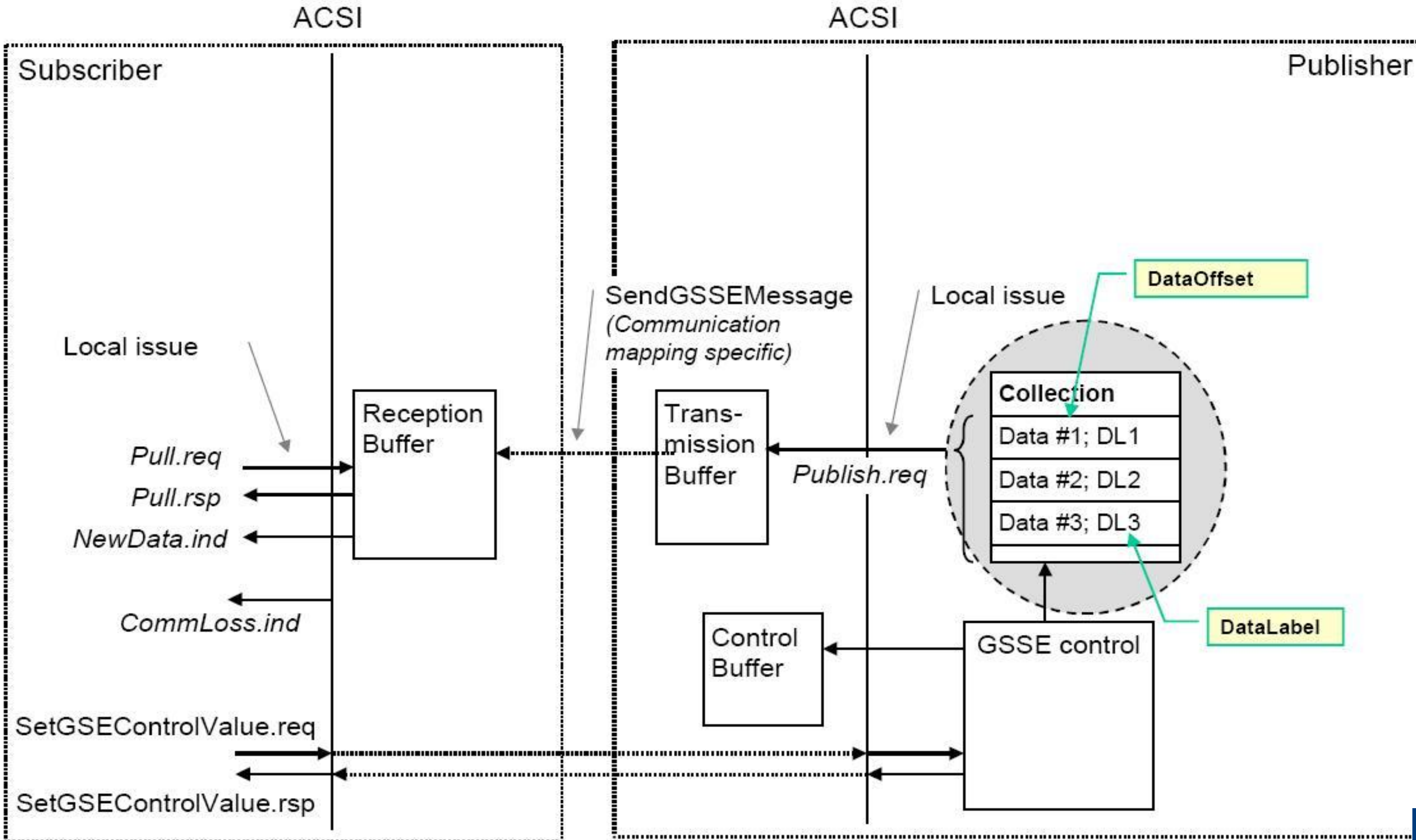


GSSE: Generic Substation Status Event

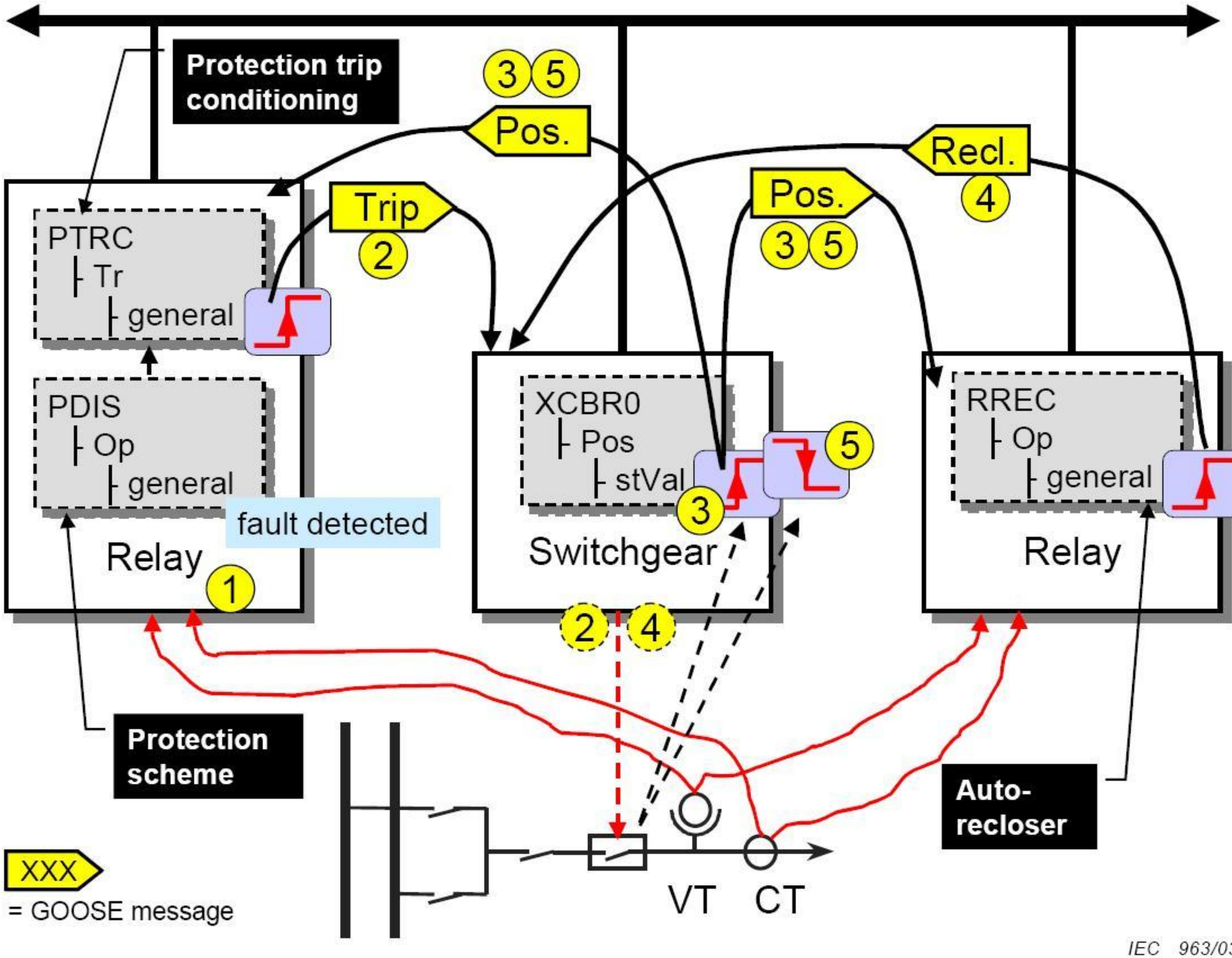
- Provide backward compatibility with the UCA GOOSE
- Just support a fixed structure of the data to be published
- Based on multicast

Generic Substation State Event (GSSE)

- Convey state change information (a simple list of status information)



Application Of GSE Model



Application of GSE Model (cont.)

1. PDIS (distance protection) detects a fault
2. PTRC issues a <Trip> command to XCBR0 (circuit break); the switchgear opens the circuit breaker;
3. The new status information is immediately sent; the reporting model may report the change;
4. RREC (auto-reclosing) issues <Reclose> to XCBR0 according to the configured behavior;
5. XCBR0 receives the GOOSE message with the value <Reclose>; the switchgear closes the circuit breaker. XCBR0 issues another GOOSE message with the new position value

Agenda

- Overview
- Data modeling approach
- Communication model
- Communication service mapping
- Sampled measured values
- Configuration description language
- Conclusion
- Reference

Mapping To Real Communication Systems

- IEC 61850 is just a high level description of substation automation
- Use MMS to implement IEC61850
- Map each IEC 61850 object to a MMS object
- Map each IEC 61850 service to a MMS operation
- All but GOOSE messages and transmission of sampled values are mapped to MMS protocol stack

MMS: Manufacturing Message Specification

ILLINOIS SECURITY LAB

- ISO 9506 standard used in Control Networks
- A reduced OSI stack with the TCP/IP protocol in the transport/network layer
- Ethernet and/or RS-232C as physical media
- Defines communication messages transferred between controllers as well as between the engineering station and the controller (e.g. downloading an application or reading/writing variables)

ACSI Objects Mapping

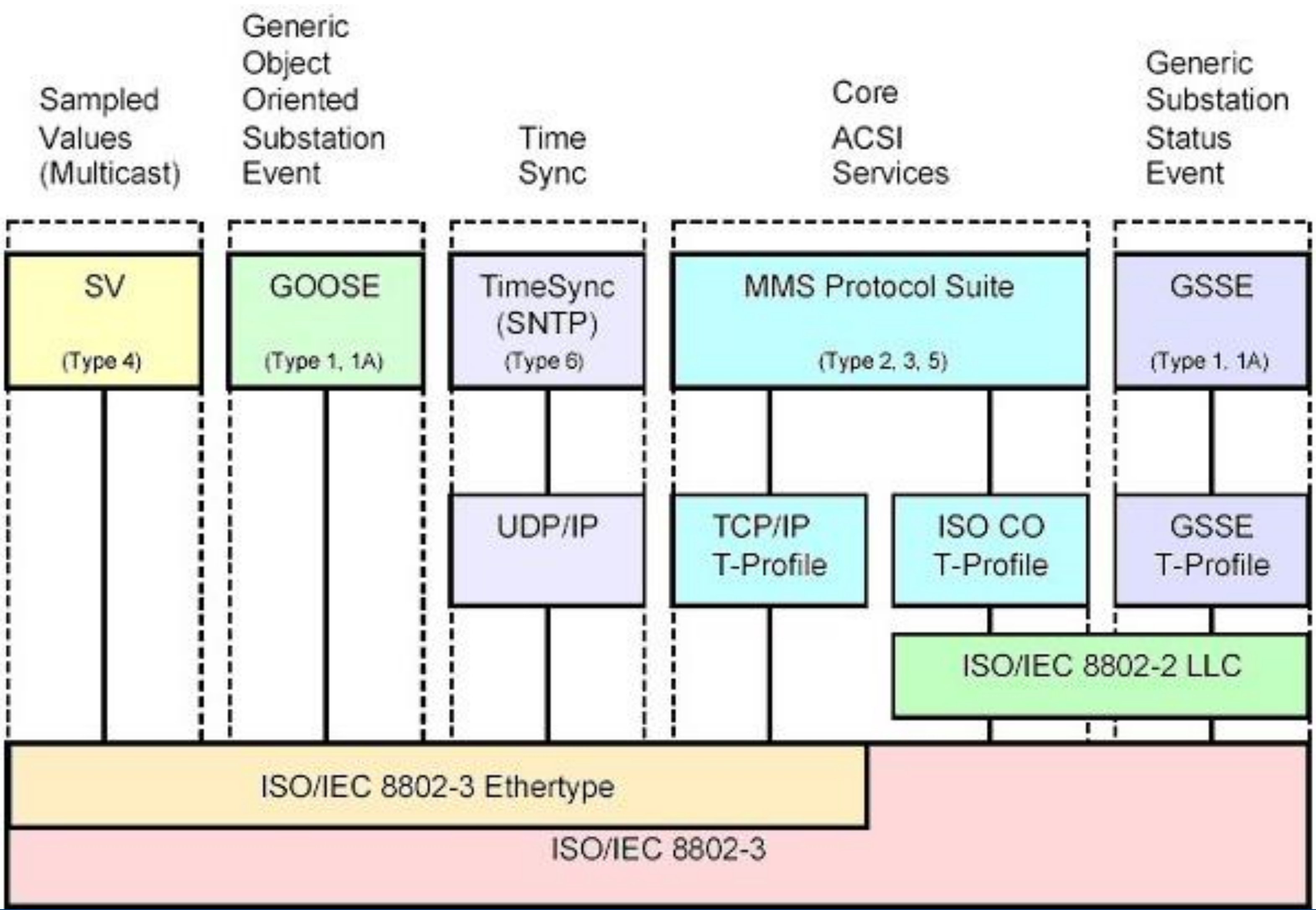
ACSI Object Class (7-2)	MMS Object (8-1)
SERVER class	Virtual Manufacturing Device (VMD)
LOGICAL DEVICE class	Domain
LOGICAL NODE class	Named Variable
DATA class	Named Variable
DATA-SET class	Named Variable List
SETTING-GROUP-CONTROL-BLOCK class	Named Variable
REPORT-CONTROL-BLOCK class	Named Variable
LOG class	Journal
LOG-CONTROL-BLOCK class	Named Variable
GOOSE-CONTROL-BLOCK class	Named Variable
GSSE-CONTROL-BLOCK class	Named Variable
CONTROL class	Named Variable
Files	Files

ACSI Services Mapping

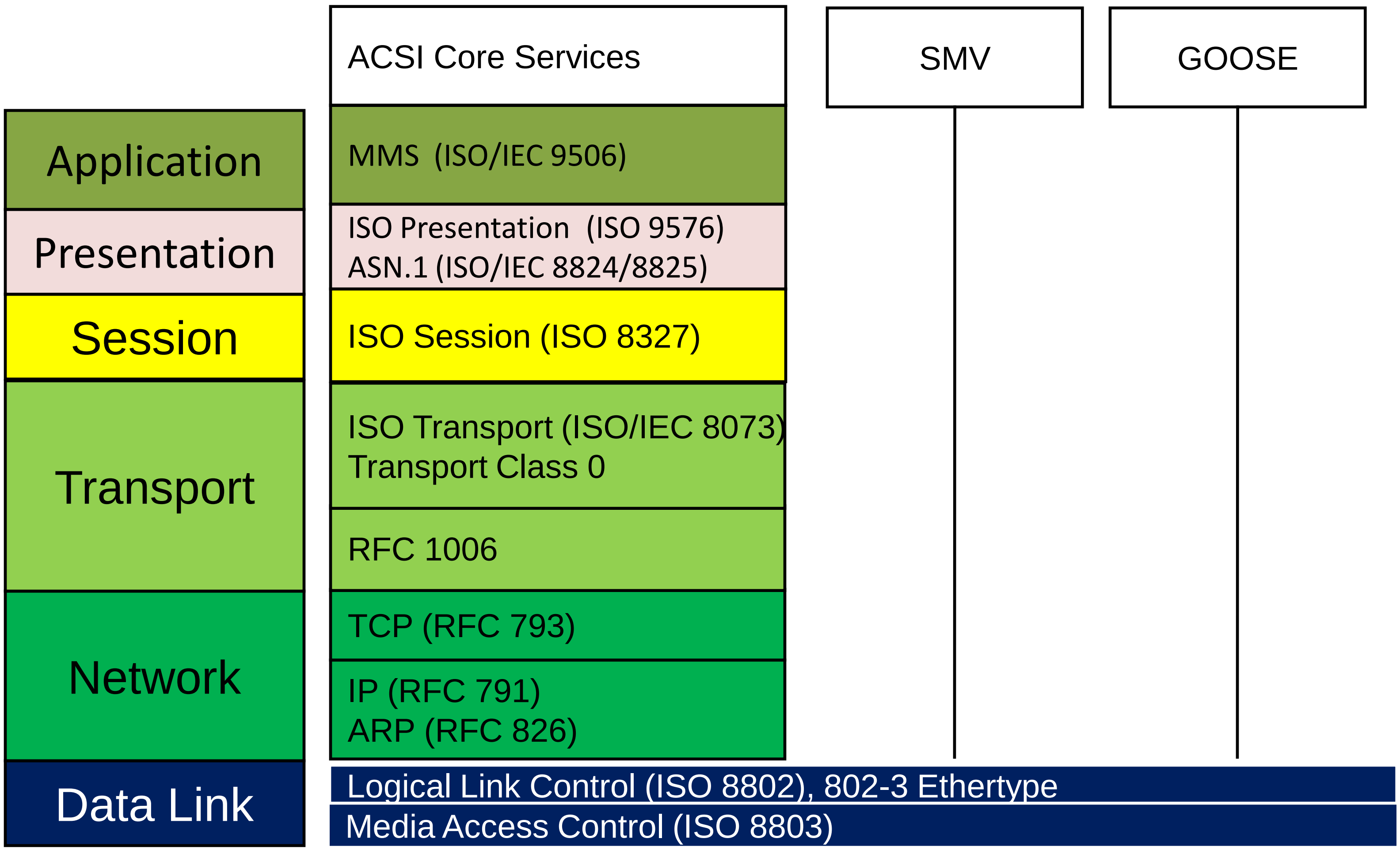
ILLINOIS SECURITY LAB

ACSI Services (7-2)	MMS Services (8-1)
LogicalDeviceDirectory	GetNameList
GetAllDataValues	Read
GetDataValues	Read
SetDataValues	Write
GetDataDirectory	GetNameList
GetDataDefinition	GetVariableAccessAttributes
GetDataSetValues	Read
SetDataSetValues	Write
CreateDataSet	CreateNamedVariableList
DeleteDataSet	DeleteNamedVariableList
GetDataSetDirectory	GetNameList
Report (Buffered and Unbuffered)	InformationReport
GetBRCBValues/GetURCBValues	Read
SetBRCBValues/SetURCBValues	Write
GetLCBValues	Read
SetLCBValues	Write
QueryLogByTime	ReadJournal
QueryLogAfter	ReadJournal
GetLogStatusValues	GetJournalStatus
Select	Read/Write
SelectWithValue	Read/Write
Cancel	Write
Operate	Write
Command-Termination	Write

Protocol Mapping Profile



IEC61850 Protocol Stack



Agenda

ILLINOIS SECURITY LAB

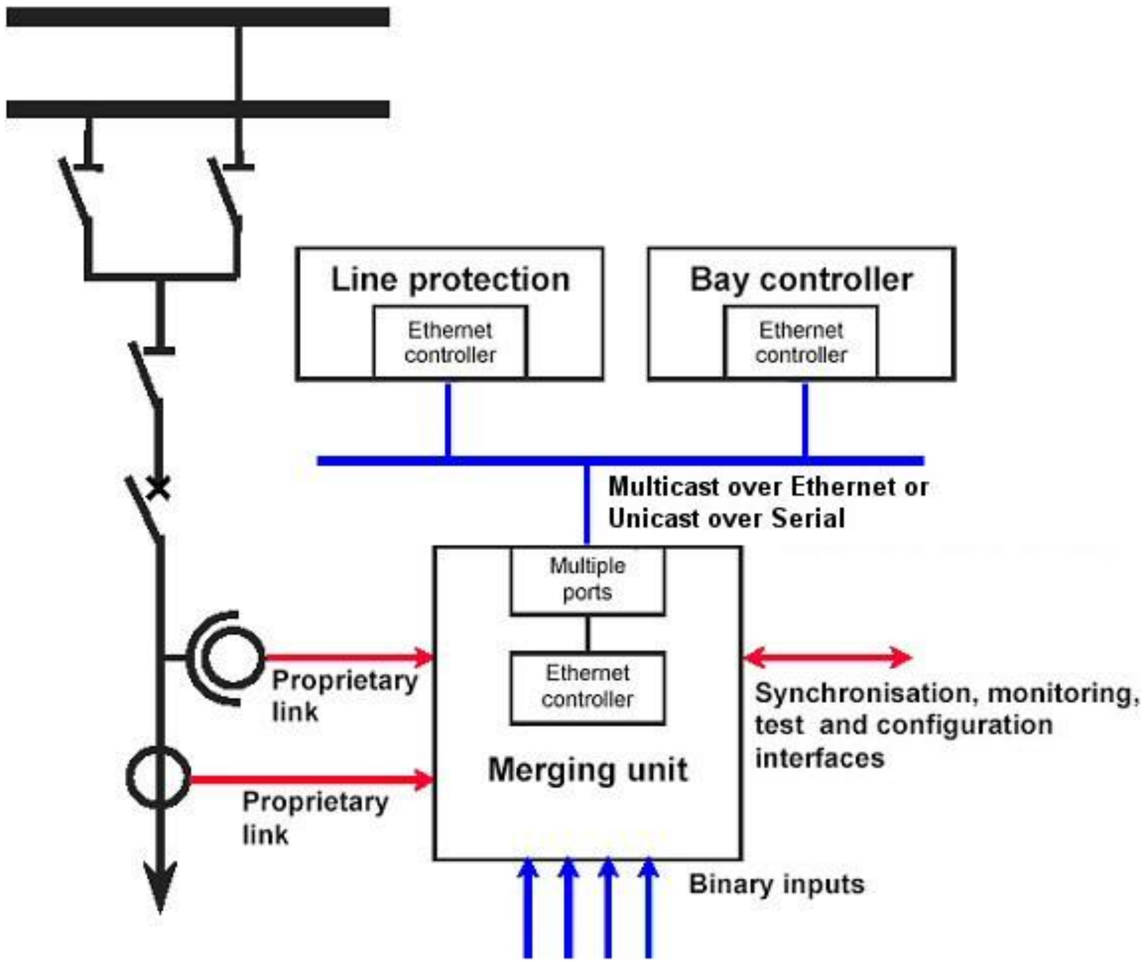
- Overview
- Data modeling approach
- Communication model
- Communication service mapping
- Sampled measured values
- Configuration description language
- Conclusion
- Reference

Sampled Measured Values

ILLINOIS SECURITY LAB

- A method for transmitting sampled measurements from transducers such as CTs, VTs, and digital I/O.
- Enables sharing of I/O signals among IEDs
- Supports 2 transmission methods:
  - Multicast service (MSVC) over Ethernet
  - Unicast (point-to-point) service (USVC) over serial links.

SMV Application



Agenda

ILLINOIS SECURITY LAB

- Overview
- Data modeling approach
- Communication model
- Communication service mapping
- Sampled measured values
- Configuration description language
- Conclusion
- Reference

SCL: Substation Configuration Language

- Purpose: interoperable exchange of communication system configuration data between an IED configuration tool and a system configuration tool from different manufacturers.
- A formal description of
  - Relations between substation automation system and the switchyard
  - Relations of the switchyard structure to the SAS functions (logical nodes) configured on the IEDs

Intended Engineering Process With SCL

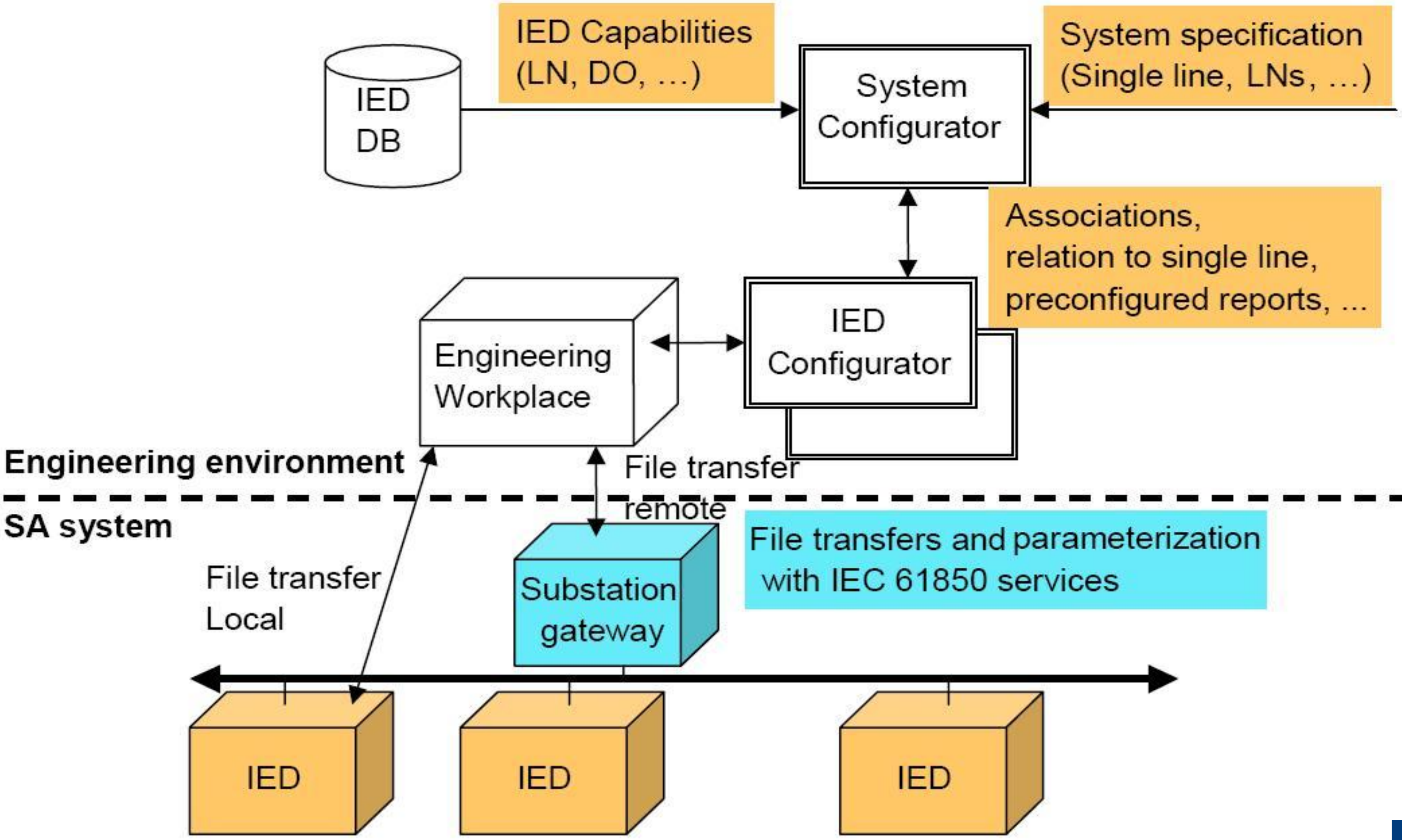
1. Functional specification input to SAS engineering
   - A system specification in terms of the single line diagram, and allocation of logical nodes (LN) to parts and equipment of the single line to indicate the needed functionality.
2. IED capability description – results after IED pre-engineering
   - Pre-configured IEDs with a fixed number of logical nodes (LNs), but with no binding to a specific process . may only be related to a very general process function part.
   - Pre-configured IEDs with a pre-configured semantic for a process part of a certain structure, for example a double bus-bar GIS line feeder.
3. SA system description - result after SAS engineering
   - Complete process configuration with all IEDs bound to individual process functions and primary equipment, enhanced by the access point connections and possible access paths in sub-networks for all possible clients.
   - As item d) above, but additionally with all predefined associations and client server connections between logical nodes on data level. This is needed if an IED is not capable of dynamically building associations or reporting connections (either on the client or on the server side).

Approach

ILLINOIS SECURITY LAB

- Define an object model describing the IEDs, their communication connections, and their allocation to the switchyard (Part 7)
- Describe how this model shall be represented in a file to be exchanged between engineering tools in a standardized way (Part 6)

Information Flow in the Configuration Process



Information Flow in the Configuration Process (cont.)

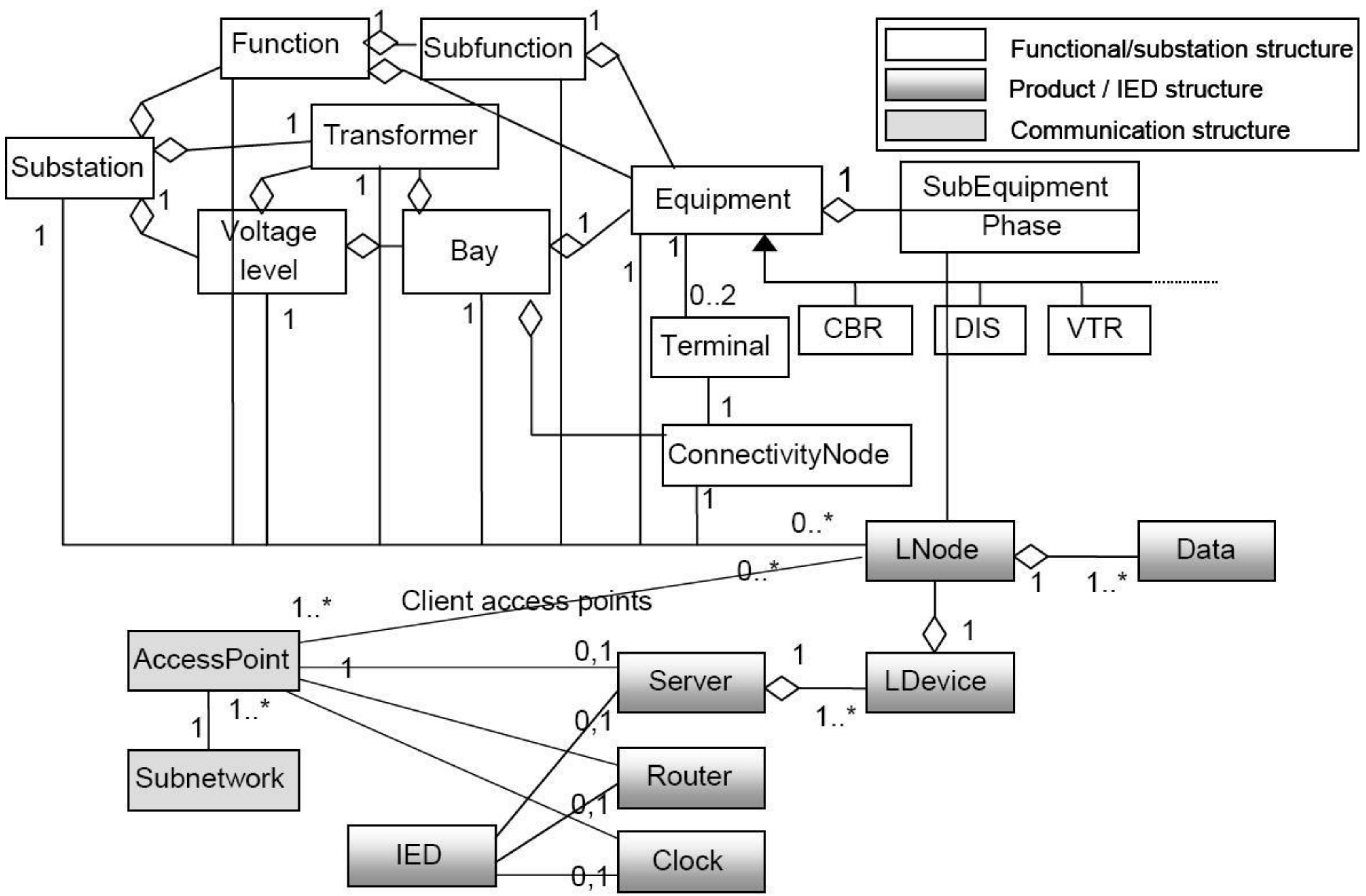
ILLINOIS SECURITY LAB

- IED Configurator
  - A manufacturer-specific tool used to import or export SCL files
  - Provides IED-specific settings and generates IED specific configuration files
  - Loads the IED configuration into the IED
- System Configurator
  - An IED independent system level tool used to import or export SCL files
  - Imports configuration files from several IEDs, as needed for system level engineering
  - Adds system information shared by different IEDs (by the configuration engineer)
  - Generates a substation related configuration file, which may be fed back to the IED Configurator for system related IED configuration
  - Reads a system specification file for example as a base for starting system engineering, or to compares it with an engineered system for the same substation.

SCL Object Model

- The primary (power) system structure
  - Which primary apparatus functions are used
  - How the apparatus are connected
- The communication system
  - How IEDs are connected to subnetworks and networks
  - And at which of their communication access points (communication ports)
- The application level communication
  - How data is grouped into data sets for sending
  - How IEDs trigger the sending and which service they choose, which input data from other IEDs is needed
- Each IED
  - The logical devices configured on the IED
  - The logical nodes with class and type belonging to each logical device
  - The reports and their data contents
  - Logged data
  - The (pre-configured) associations
- Instantiable logical node (LN)
  - Mandatory, optional and user defined DATA (here abbreviated DO) as well as optional services

SCL Object Model (cont.)



Substation Model

- **Substation**: the object identifying a whole substation.
- **VoltageLevel**: an identifiable, electrically connected substation part having an identical voltage level.
- **Bay**: an identifiable part or sub-function of the switchyard (substation) within one voltage level.
- **Equipment**: an apparatus within the switchyard. The single line diagram of a switchyard shows the electrical connections between these primary devices.
- **SubEquipment**: a part of an Equipment, which might especially be one phase of a three phase equipment.
- **ConnectivityNode**: the (electrical) connectivity node object connecting different primary devices. Typical connectivity node examples are: connecting nodes within a bay, bus bars connecting several bays in the same voltage level, lines connecting bays in different substations
- **Terminal**: an electrical connection point of a primary apparatus at single line level. A terminal can be connected to a ConnectivityNode. Within SCL terminals can be explicitly named, or exist implicitly.

Product (IED) Model

ILLINOIS SECURITY LAB

- **IED**: a substation automation device performing SA functions by means of logical nodes (LNs).
- **Server**: a communication entity within an IED. It allows access via the communication system and its only access point to the data of the logical devices and logical nodes contained in the server.
- **LDevice**: logical device (LD)
- **LNode**: logical node (LN)
- **DO**: the DATA contained in the LNs

Communication System Model

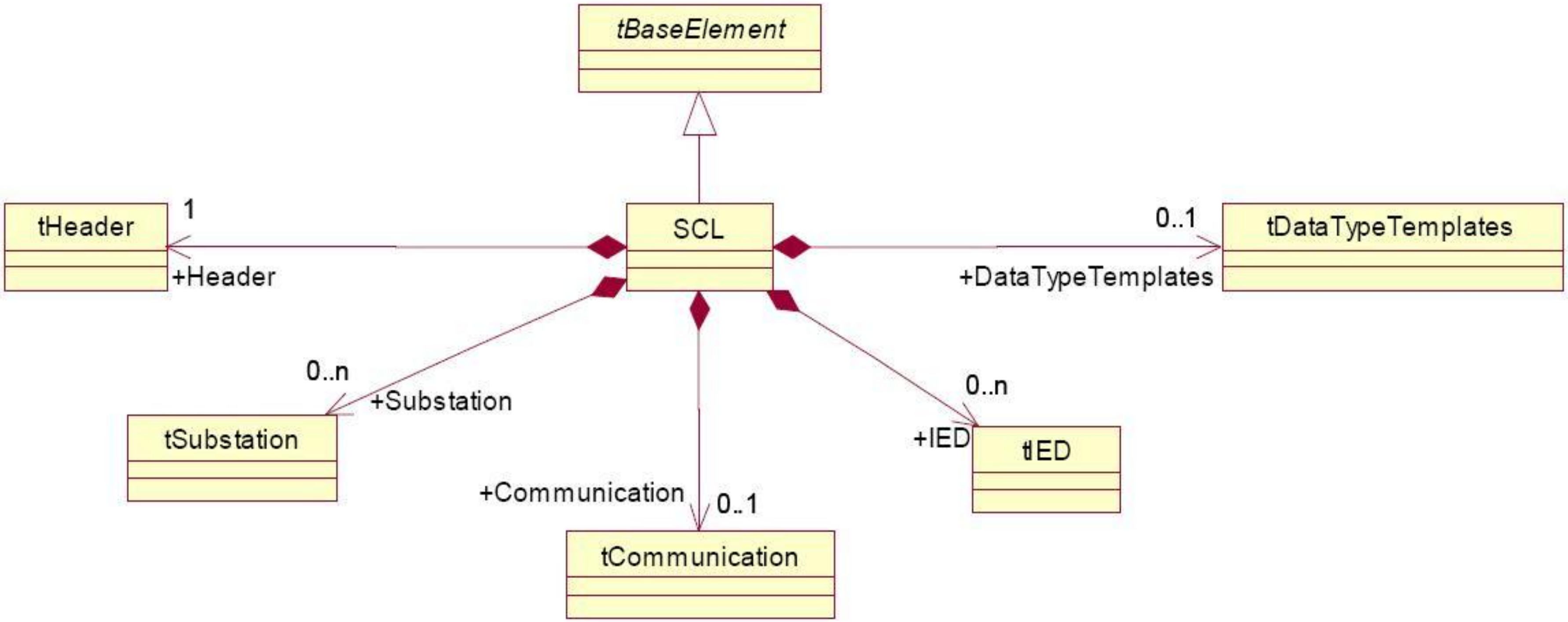
ILLINOIS SECURITY LAB

- **Subnetwork**: a connecting node for direct (link layer) communication between access points.
  - One LD should have at most one connection to a subnetwork
- **Access point**: a communication access point of the LD(s) of an IED to a sub-network.
  - One access point can serve multiple LDs
  - LNs on one LD can access different subnetworks via APs on different LDs
- **Router**: a function hosted on an IED which extends access to servers connected to another subnetwork at another access point of the hosting IED
- **Clock**: a master clock used to synchronize the internal clocks of all (other) IEDs connected to this ubnetwork.

SCL File Types

- SSD: System Specification Description
  - Data exchange from a system specification tool to the system configuration tool.
  - Describes the single line diagram of the substation and the required logical nodes.
- ICD: IED Capability Description
  - Data exchange from the IED configuration tool to the system configuration tool.
  - Describes the capabilities of an IED.
- SCD: Substation Configuration Description
  - Data exchange from the system configuration tool to IED configuration tools.
  - Describes all IEDs, a communication configuration section and a substation description section.
- CID: Configured IED Description
  - Data exchange from the IED configuration tool to the IED.
  - Describes an instantiated IED within a project.
    - The communication section contains the current address of the IED.
    - The substation section related to this IED may be present and then shall have name values assigned according to the project specific names.
    - Possibly a stripped-down SCD file to what the concerned IED shall know.

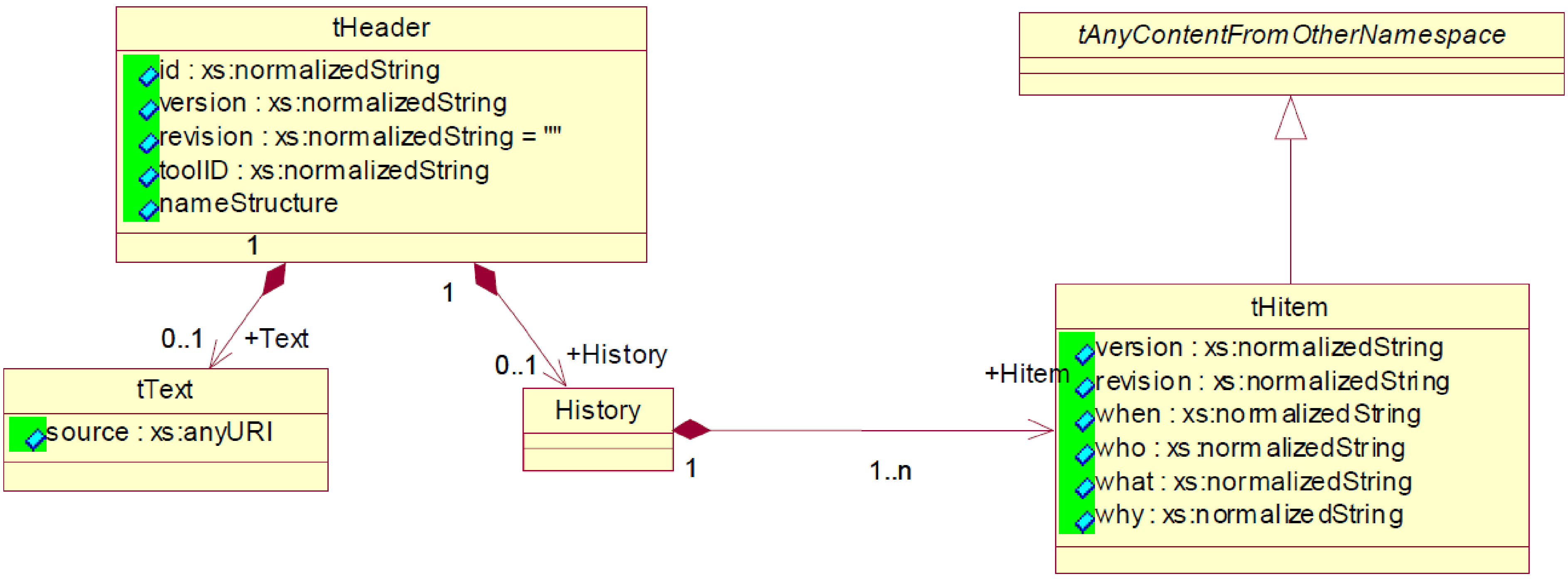
SCL UML Diagram Overview



SCL Syntax Elements: Header

- Header: identify an SCL configuration file and its version
  - Text
  - History
    - Hitem

Header UML Diagram

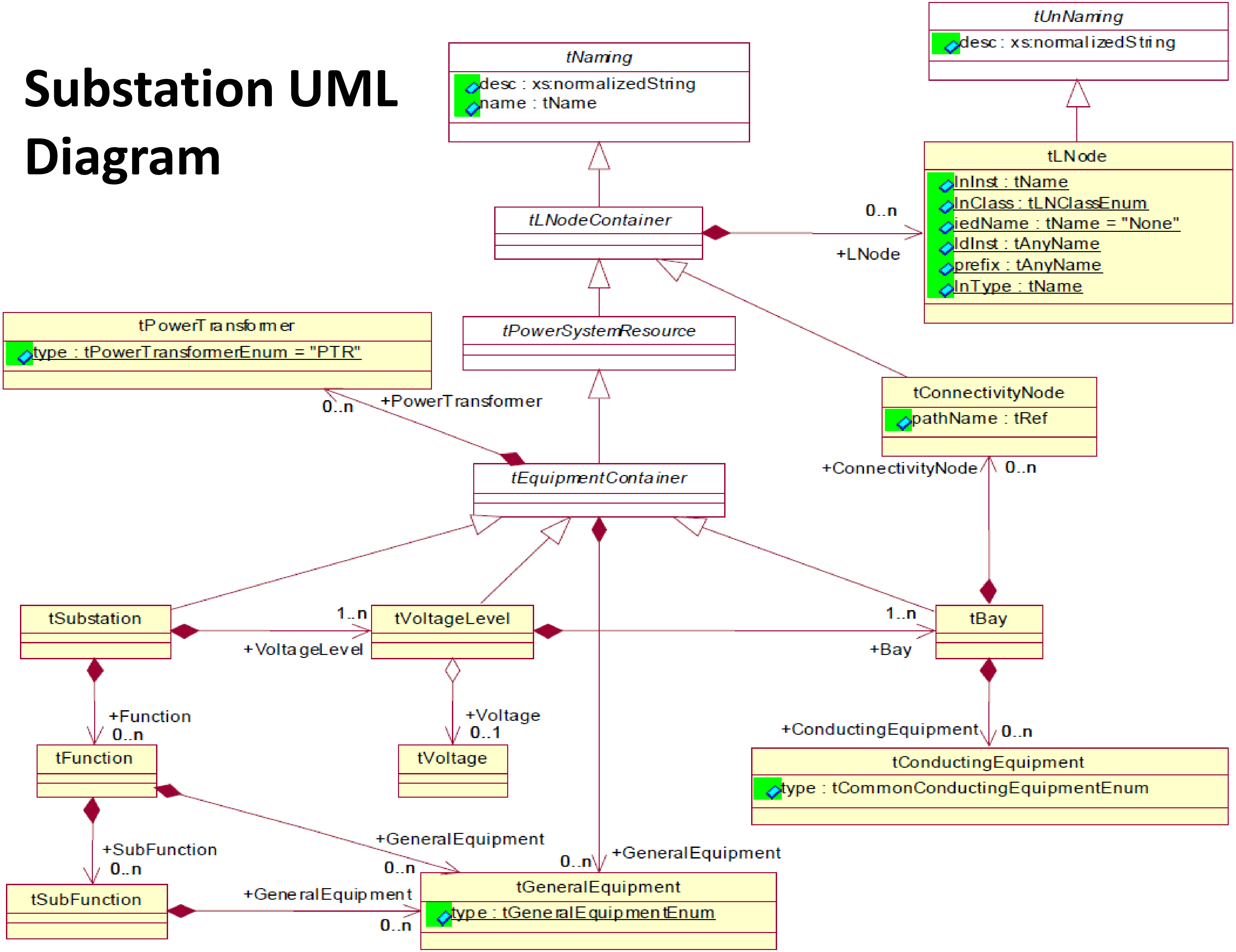


SCL Syntax Elements: Header and Substation

ILLINOIS SECURITY LAB

- Substation: describes the functional structure of a substation; identifies the primary devices and their electrical connections

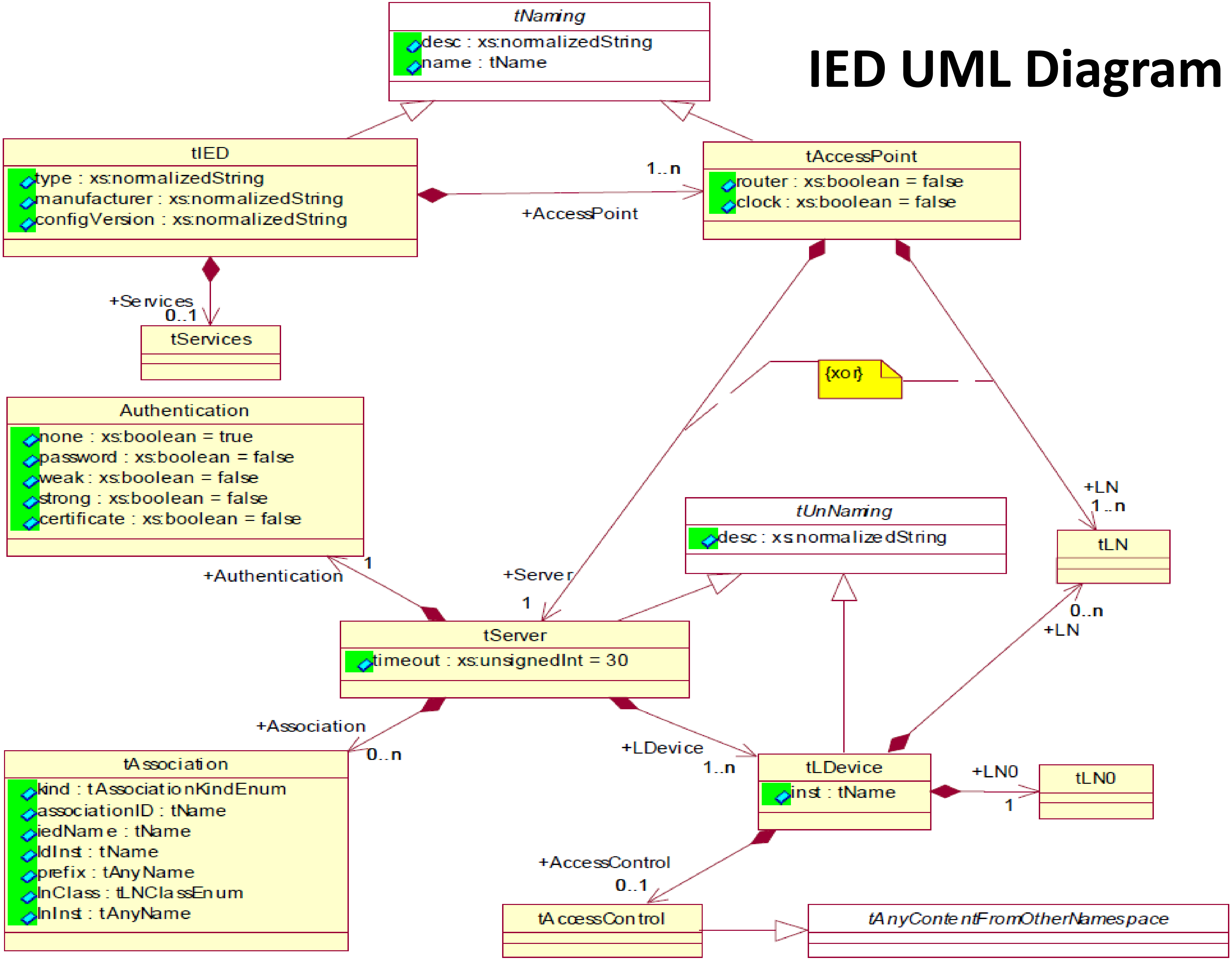
Substation UML Diagram



SCL Syntax Elements - IED

- IED: describes the (pre-) configuration of an IED: access points, the logical devices, and logical nodes.
  - Services (ACSI services)
  - AccessPoint
    - Server xor LN (LN0)
- Server
  - Authentication
  - LDevice
  - Association
- LN
  - DataSet
  - ReportControl
  - LogControl
  - DOI
  - Inputs
- LN0 (extends LN)
  - GSEControl
  - SampledValueControl
  - SettingControl
  - SCLControl
  - Log

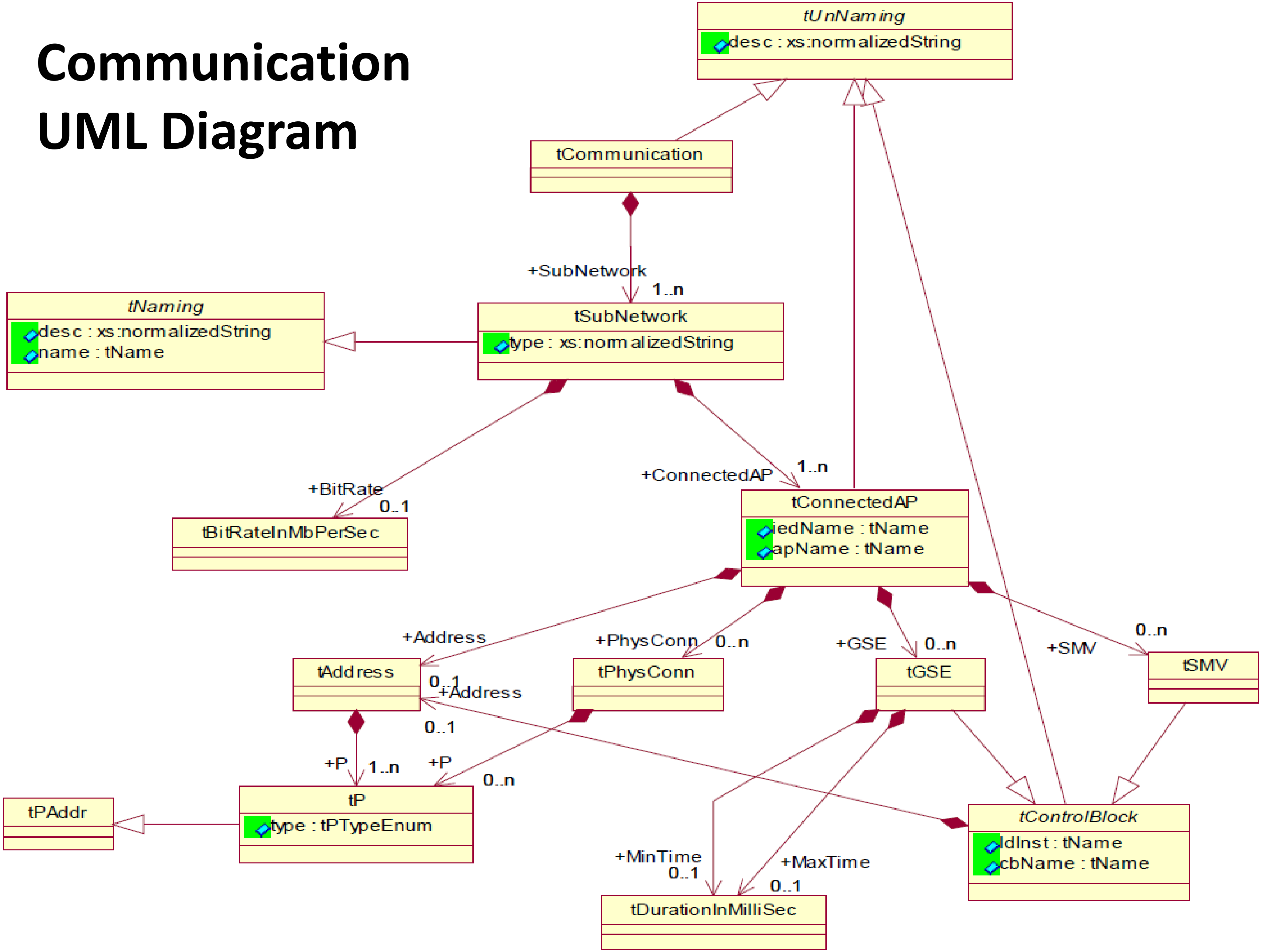
IED UML Diagram



SCL Syntax Elements - Communication

- Communication
  - SubNetwork
    - BitRate
    - ConnectedAP
      - Address
      - GSE
      - SMV
      - PhysConn

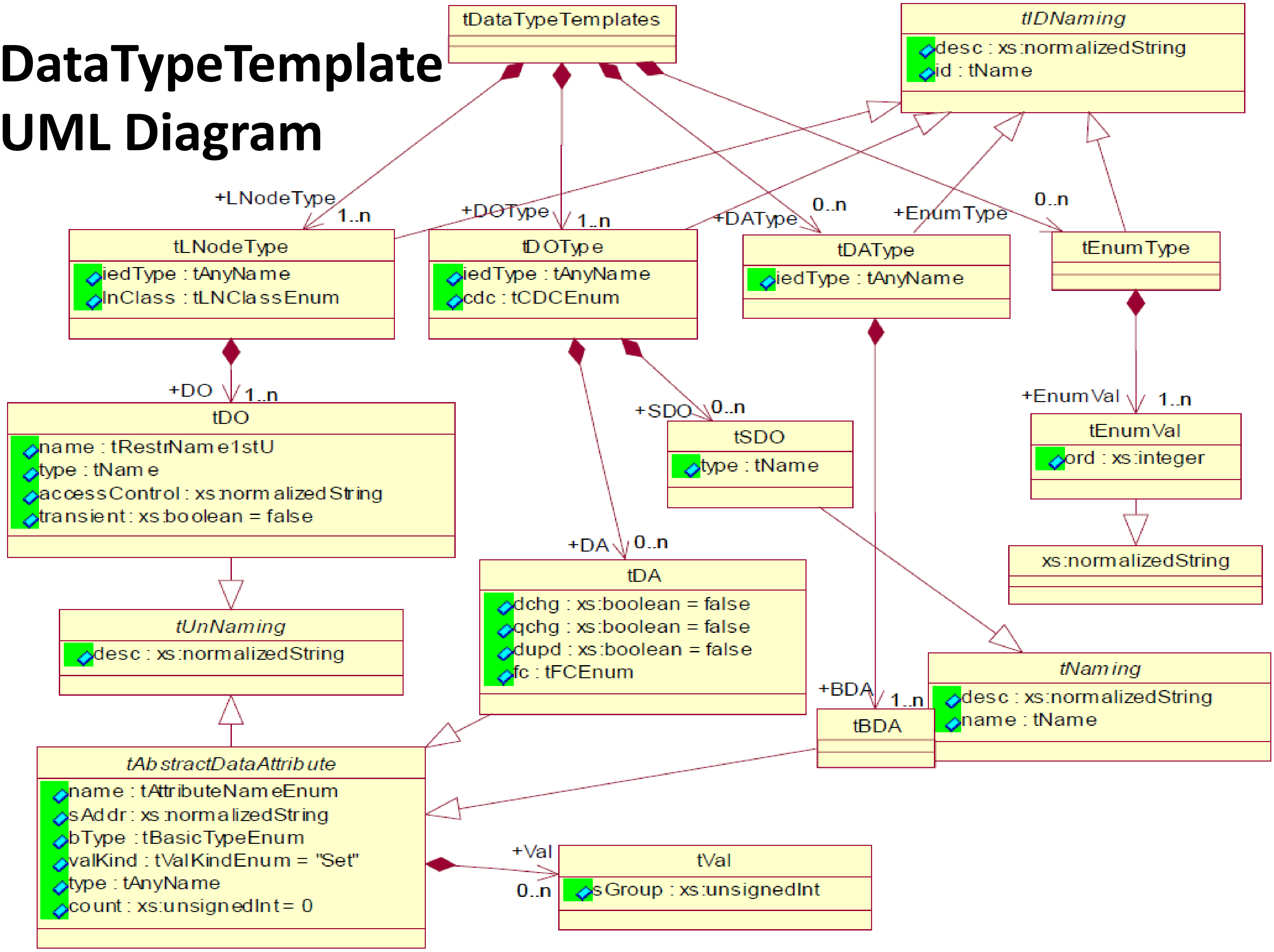
Communication UML Diagram



SCL Syntax Elements - DataTypeTemplate

- DataTypeTemplate
  - LNodeType: an instantiable logical node type
    - DO
  - DOType: an instantiable DATA type
    - SDO xor DA
  - DAType: an instantiable structured attribute type
  - EnumType: An enumeration type
    - EnumVal

DataTypeTemplate UML Diagram



Agenda

- Overview
- Data modeling approach
- Communication model
- Communication service mapping
- Sampled measured values
- Configuration description language
- Conclusion
- Reference

Conclusion

- IEC 61850 is a migration from the analog world to the digital world for substation
  - Standardization of data names
  - Creation of a comprehensive set of services
  - Implementation over standard protocols and hardware
  - Definition of a process bus.
- Multi-vendor interoperability has been demonstrated
- Discussions are underway to utilize IEC 61850 as the substation to control center communication protocol
- IEC 61850 will become the protocol of choice as utilities migrate to network solutions for the substations and beyond.

Reference

ILLINOIS SECURITY LAB

- IEC 61850 Communication Networks and Systems In Substations, Technical Committee 57, International Electrotechnical Commission,
- Secure Intelligent Electronic Devices (SIEDs). C. A. Gunter, S. T. King, J. Zhang. PSERC 2007
- Overview of IEC 61850 and Benefits, R. E. Mackiewicz. PES TD 2005/2006
- IEC 61850 Communication Networks and Systems In Substations: An Overview for Users. D. Baigent, M. Adamiak and R. Mackiewicz. SIPSEP 2004

ILLINOIS SECURITY LAB

4309 Siebel Center for Computer Science
201 N Goodwin Ave
Urbana, IL 61801
Phone: (217)265-6758
http://seclab.illinois.edu

Jianqing Zhang: jzhang24@cs.illinois.edu

Carl A. Gunter: cgunter@cs.illinois.edu