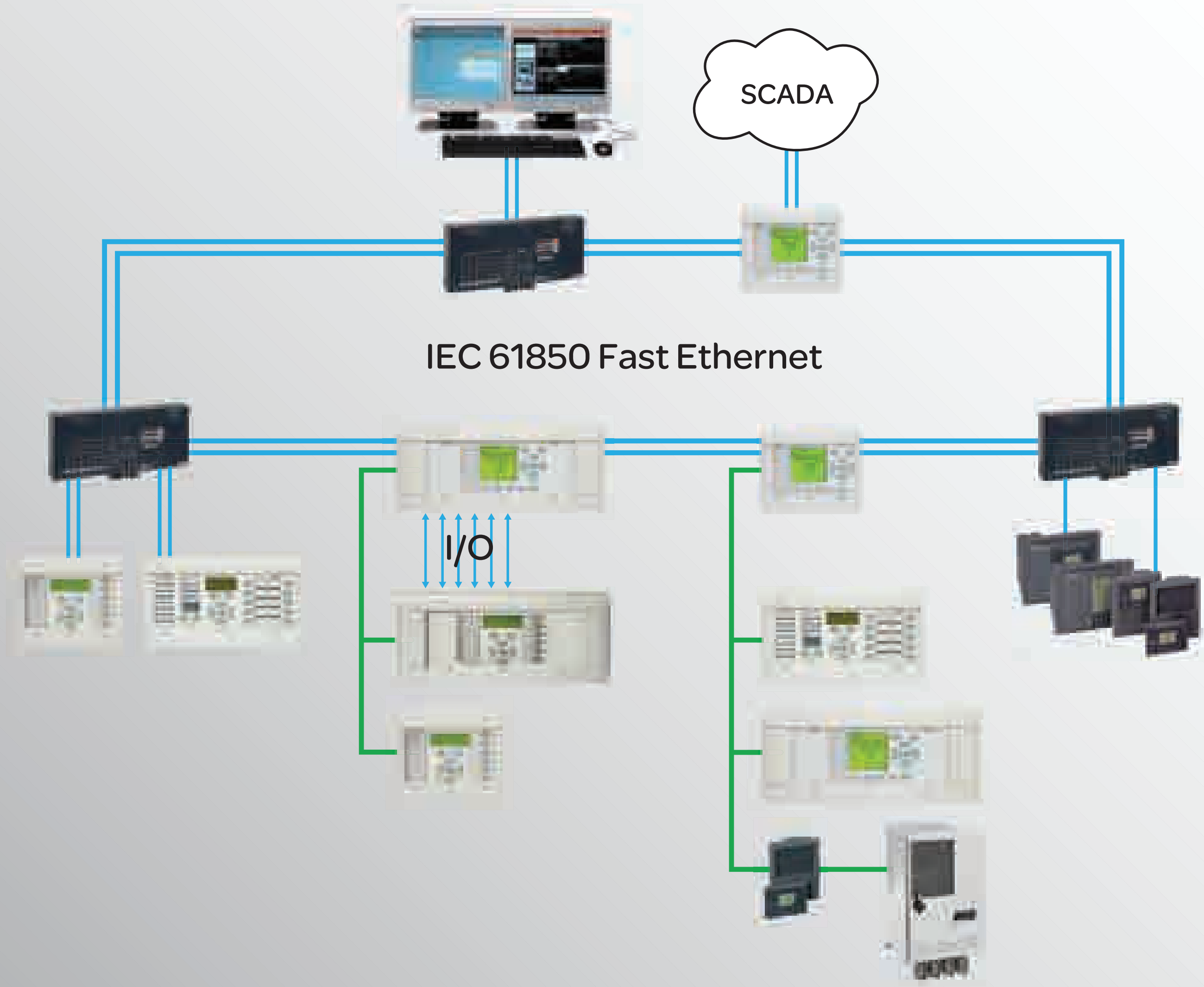

D3

IEC 61850 and Applications

Network Protection & Automation Guide

Life Is On | Schneider Electric

Chapter D3

IEC 61850 and Applications

D3

1. Introduction

IEC 61850 is the international standard for the communication networks and systems for power utility automation. It allows the implementation of distributed application functions, based on Intelligent Electronic Devices (IEDs) from different manufacturers. Initially dedicated to communication inside substations, IEC 61850 is now the one central communication standard of the Smart Grid IEC reference architecture as shown in Figure D3.1.

This chapter presents an overview of IEC 61850 and shows practical applications of this standard in the protective relays domain. A further chapter outlines typical network architecture solutions and related redundancy concepts for Ethernet solutions selected by IEC 61850 as the communication layer.

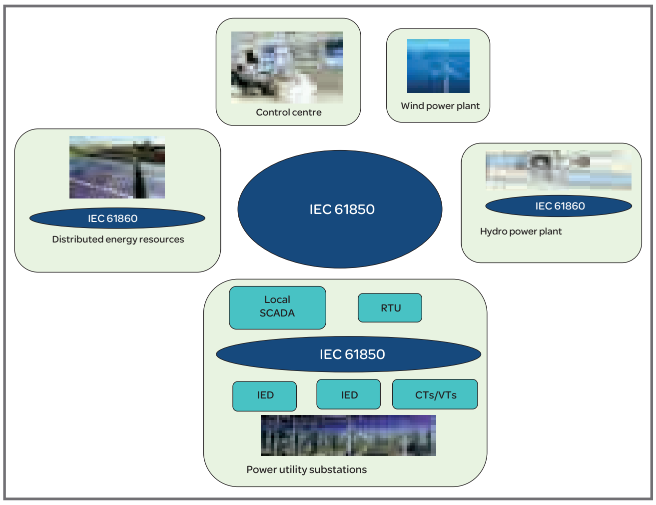

Figure D3.1:
IEC 61850 Smartgrid Architecture

1.1 What is IEC 61850?

The objective of the IEC 61850 standard is to offer a way of exchanging meaningful information between field level devices coming from different vendors in the context of electric utility energy automation.

But IEC 61850 is much more than just a communication protocol. It aims to offer ways to seamlessly and efficiently design an automation system from the very upstream specification part, down to commissioning, operation and maintenance. It has been designed to specifically address the specifics of electricity transmission and distribution such as:

a. The reaction speed: a few milliseconds reaction time is achievable

b. Multicast capabilities: information can be sent by the producer to a group of connected devices

c. EMC performance level: matching the specific electrical environment

The flexible design of the standard allows it to support evolution coping with technology evolutions and domain extensions.

IEC 61850 is based on 3 pillars:

a. A set of dictionaries: the information modelling or data model

b. A set of communication services available on several communication layers

c. A configuration language: the backbone of the engineering workflow.

1.1.1 IEC 61850 as a set of dictionaries

When a device receives an IEC 61850 data item there is no ambiguity in the meaning of this information as it is clearly defined in the dictionary. Every IEC 61850 domain (substation, hydro etc.) shares a common dictionary. But also each IEC 61850 domain can own a specific dictionary for its own definition. The link of data definition is done to create functional bricks used to model typical electrical and non-electrical functions used in an application model.

1.1.2 IEC 61850 as a communication protocol

The communication services have been defined in a generic way in IEC 61850 through an Abstract Communication Service interface (ACSI).

ACSI is independent of any communication method but provides basic functions such as read/write, browsing, event, setting, control, file transfer etc.

This abstract specification is mapped on communication technologies such as:

a. Client-Server over MMS/IP (most common)

b. Client-Server over web services

c. Multicast on Ethernet (most common)

d. Multicast on IP

1.1.3 IEC 61850 as a configuration language

The configuration language defines the structure of the configuration files used by the engineering workflow. This XML based schema (named SCL for System Configuration Language) supports many activities:

a. Specifying system requirements in terms of topology, primary devices and functions

b. Describing a complete system, following the life cycle of this system

c. Describing the functional capabilities of devices (through its communication interface)

The different actors of the engineering workflow exchange data using files based on SCL. These kinds of files are also standardised for specific usage, depending on the associated workflow state. This allows engineering tools to be interoperable regarding system configuration process.

1.2 Why choose IEC 61850?

IEC 61850 seeks to overcome the problem of multiple vendors using multiple protocols or different solutions based on the same protocol to convey essentially the same information.

This is one of the key drivers, however there are many other features and benefits that provide the user with more control and better visibility of the system, maintenance and process:

a. A single configuration file is used to define the system

b. Direct, high speed, peer to peer communications simplifies or replaces wiring schemes (GOOSE)

c. Common data models provide an interoperable solution for data description between vendors

d. The inbuilt engineering process provides standardisation and common structures

e. Cost and delivery can be controlled and long term maintenance is simplified

f. Data integrity built in means that the user understands the status of his communication network and can be assured that only valid signals are acted upon

g. Contextual data allows for more and more automated solutions with products self identifying and describing

h. An open protocol that allows future extensions.

1.3 History of IEC 61850

Development of Substation Automation Systems has been very rapid in the last few decades because of major advances in communication and microprocessor technologies.

In the 1980s, utilities and manufacturers started developing private communication protocols. Rapidly, the lack of compatibility led to the necessity for an international standardisation with the effort to ensure interoperability. Utilities were frustrated with the cost of supporting many device protocols and with the lack of freedom in choosing components within a solution. End-users complained that products and systems were not interoperable and that maintenance, installation and engineering costs were getting higher and higher.

IEC 61850 has been elaborated by the IEC technical committee 57 by merging concepts coming from two preceding standards: UCA2 from Electric Power Research Institute (EPRI) and the IEC 60870-5.

Starting in 2002, IEC has published a list of separate consistent documents establishing the Edition 1 of IEC 61850. Since the introduction of this new standard several thousands of substations were installed all over the world according to this Edition.

The main benefits are not only interoperability, but also a reduction in hardware equipment and its wiring thanks to the substitution by a single Ethernet cable, an enhancement of the maintainability by the increased system observability, an easier way to diagnose and repair and finally an agility increase, so that installations can more easily cope with new functional requirements.

But nevertheless, as usual for such a complex standard, this first version did not solve all potential interoperability problems in one go. Issues have been registered in a web database (http://tissue.iec61850.com/) and solved by extensions or corrections of the standard.

Edition 2 of IEC 61850 was published in 2009. Previous parts have been improved by adding more precise descriptions of ambiguous points and fixing errors. IEC 61850 foundations have been strengthened by various updates.

New parts have been added, so that the scope of the standard is no longer limited to substations, it now includes inter-substation communication, wind farm systems, control centres, distributed energy resources (DER), wide area measurement and protection automation control systems, hydro power systems and power quality.

The standard is giving clear rules using so called “name space” extensions to add manufacturer or domain specific data without a risk of collision or interoperability break.

In addition secured communication over WAN, high availability seamless redundancy protocols (HSR/PRP), mapping IEC 61850/IEC 850-1-101/104 and mapping IEC 61850/DNP3 (IEEE 1815) are now defined to support this standard.

1.4 Evolution of IEC 61850

Evolutions of IEC 61850 will not stop with the Edition 2. On the contrary, IEC 61850 will play a major role in the scope of the smart grid. In 2015, IEC should release an amendment named Ed2.1. The scope and the quality of IEC 61850 quality shall be improved again.

A maintenance process is setup to handle technical issues (called TISSUES) raised after publication. Two categories of TISSUES are defined. The first one, the most critical, called “IntOp” TISSUES must be handled by a vendor as soon as a proposed fix is provided by the IEC committee. TISSUES of the second category are improvement proposals. They are taken into account for future versions of the standard.

The Ed2.1 standard itself will be auto-generated from a database, avoiding any typing or format mistakes. A machine readable data model will be available for engineering tools usage. A web-access will be provided through the IEC web site in future.

New parts are under development to extend the coverage to new actors: feeder automation, power supply, battery storage, FACTS (Flexible Alternative Current Transmission System) etc.

New parts, related to new communication and configuration technologies are also under development: use of wide area networks, use of web services, logic modelling, and statistical calculation capabilities.

D3

2. General philosophy

This chapter covers the main aspect of IEC 61850. The first section gives an overview of the IEC 61850 series, thereby one can go directly to the part of interest. The last three sections explain the three foundations of IEC 61850: the data model, the communication services and the configuration process.

2.1 Global approach

To achieve interoperability between IEDs from different manufacturers, the standard has to specify a very precise definition of both the functions and the communication services, without compromising the needed flexibility.

A function can be defined as a task which has to be performed by the electric utility automation system. A function has a well defined purpose, inputs and outputs. The standard defines many basic functions, named **Logical Node (LN)**. Collectively, LNs define the behaviour of the system. At the end, the real processing is done in physical devices. To achieve flexibility, the standard allows the free allocation of a LN to the physical devices, taking into account availability requirements, performance requirements, cost constraint, and device capabilities etc. Communications services allow exchange of data between LNs which are not located in the same physical devices.

Figure D3.2 shows 4 IEDs that each contain one or more LNs (PTOC, PDIS, PTRC, XCBR). The red lines represent the communication services between IEDs. The black lines represent communications between LNs inside some IEDs, but they are private to the IED and not defined by the standard.

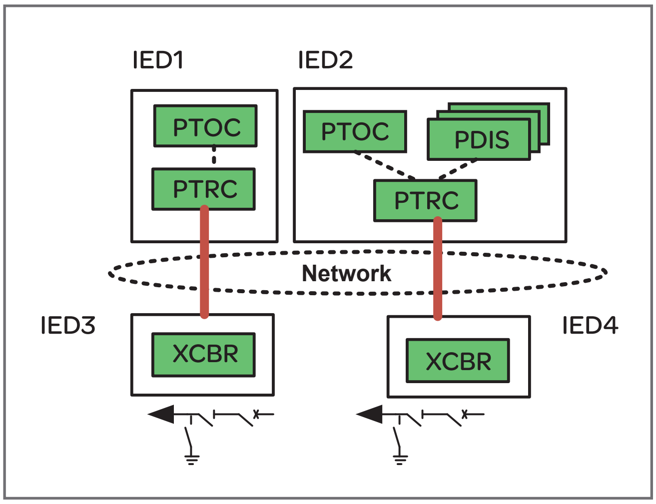

Figure D3.2:
IEC 61850 smartgrid architecture

2.2 Parts of the standard

2.2.1 Documentation structure

IEC 61850 documentation is quite extensive. The documentation is split into several parts. Some of them are normative (International Standard). Others are only informative and can be used as a guideline or overview (for instance part 7-5). Let's describe briefly the documentation structure.

Parts 1 to 5 cover general requirements.

Parts 7-3, 7-4, 7-4xx, describe the set of dictionaries (the first pillar as introduced earlier).

Parts 7-2, 8-1, 9-2 focus on communication services (the second pillar).

Part 6 deals with the configuration language (the third pillar)

Finally, **part 10** specifies the test cases which have to be performed to ensure the conformance of the implementation.

As a summary, the documentation defines how IEDs must be implemented, provides general information and guidelines and specifies how a manufacturer can obtain an IEC 61850 conformance certificate.

The following Figure D3.3 outlines the structure of the documentation with the three pillars. The following Table D3.1 lists the official IEC 61850 parts as of June 2015 (In Pink: Dictionaries, Orange: Communication Protocols, Green: Configuration language).

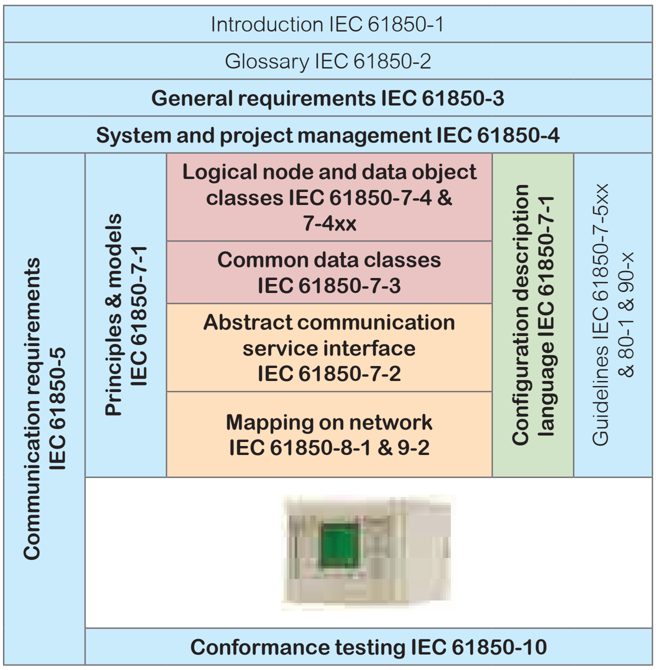

Figure D3.3:
IEC 61850 standard parts overview

2. General philosophy

Part	Title	Latest	Previous
1	Introduction and overview	ed2.0_2013-03	ed1.0_2003-04
2	Glossary	ed1.0_2003-08	
3	**General requirements**	ed2.0_2013-12	ed1.0_2002-02
4	**System and project management**	ed2.0_2011-04	ed1.0_2002-01
5	**Communication requirements for functions and device models**	ed2.0_2013-01	ed1.0_2003-07
6	**Configuration language for communication in electrical substations relate**	ed2.0_2009-12	ed1.0_2004-03
	Basic communication structure		
7-1	**Principles and models**	ed2.0_2011-07	ed1.0_2003-07
7-2	**Abstract communication service interface (ACSI)**	ed2.0_2010-08	ed1.0_2003-05
7-3	**Common Data Classes**	ed2.0_2010-12	ed1.0_2003-05
7-4	**Compatible logical node classes and data classes**	ed2.0_2010-03	ed1.0_2003-05
7-410	Hydroelectric power plants - Communication for monitoring end control	ed2.0_2012-10	ed1.0_2007-08
7-420	Distributed energy resources logical nodes	ed1.0_2009-03	
7-510	Hydroelectric power plants - Modelling concepts and guidelines	ed1.0_2012-03	
	Specific communication service mapping (SCSM)		
8-1	**Mappings to MMS (ISO/IEC9506-1 and ISO/IEC 9506-2)**	ed2.0_2011-06	ed1.0_2004-05
9-1	*Sampled values over serial unidirectional multidrop point to point link*	*withdraw*	*ed1.0_2003-05*
9-2	**Sampled values over ISO/IEC 8802-3**	ed2.0_2011-09	ed1.0_2004-04
10	**Conformance testing**	ed2.0_2012-12	ed1.0_2005-05
80-1	Guideline to exchanging information from a CDC-based data model using IEC 60870-5-101 or IEC 60870-5-104	ed1.0_2008-12	
90-1	Use of IEC 61850 for the communication between substations	ed1.0_2010-03	
90-4	Network engineering guidelines	ed1.0_2013-08	
90-5	Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118	ed1.0_2012-05	
90-7	Object models for power converters in distributed energy resources (DER) system	ed1.0_2013-02	

Table D3.1:
List of IEC 61850 standard parts (published until the 30.04.2015)

If relevant, the reference of the previous version is also mentioned. Some parts are still in the first edition. You will notice that IEC has decided to withdraw the **part 9-1**.

New parts of IEC 61850 are regularly published because of the inclusion of new domains or methods of communication or guidelines.

The main parts are: **6, 7-2, 7-3, 7-4, 8-1, 9-2** and **10** because they provide the foundation of the interoperability characteristic of IEC 61850.

2.2.2 General requirements

IEC 61850-1 provides an introduction and an overview of IEC 61850.

IEC 61850-2 lists a collection of terminology and definitions used within the various part of the standard.

IEC 61850-3 provides general requirements: quality requirements (reliability, maintainability etc.), environmental conditions.

IEC 61850-4 describes the system lifecycle, the engineering requirements and the quality assurance.

IEC 61850-5 defines the communication requirements for functions. Part 5 decomposes the whole system behaviour into the smallest functions, called **Logical Nodes**. All of them are documented and categorised.

2.2.3 Parts linked to data model definition

IEC 61850-7-4 specifies the information model of devices and functions generally related to power utility automation. It also contains the information model of devices and function-related applications in a substation.

IEC 61850-7-410 and **IEC 61850-7-420** have the same part 7-4 objective, but are dedicated respectively to distributed energy resources and hydroelectric power plants.

IEC 61850-7-3 is applicable to the description of device models and functions of substations and feeder equipment.

2. General philosophy

It has a list of commonly used information that is referenced in part 7-4 and 7-4xx. In particular, it specifies common basic information (named Common Data Class or **CDC**) for status, measurement, control, setting and description.

2.2.4 Parts linked to communication services definition

IEC 61850-7-2 applies to the ACSI communication for energy systems providing the following abstract communication service interfaces:

a. Abstract interface describing communications between a client and a remote server

b. Abstract interface for fast and reliable system-wide event distribution between an application in one device and many remote applications in different devices (publisher/subscriber)

c. Abstract interface for transmission of sampled measured values (publisher/subscriber).

IEC 61850-8-1 specifies a method of exchanging time-critical and non-time-critical data through local-area networks according to the abstract specification in IEC 61850-7-2 by mapping ACSI to MMS and ISO/IEC 8802-3 frames. This is often referred to as “System Bus”.

IEC 61850-9-2 defines the specific communication service mapping for the transmission of sampled values according to the abstract specification in IEC 61850-7-2. It defines the concrete means to communicate samples values from sensors to IEDs. This is often referred to as “Process Bus”.

2.2.5 Part linked to the definition of substation communication language

IEC 61850-6 specifies a file format describing communication-related configurations and IED parameters, communication system configurations, switch yard (function) structures, and the relations between them. The main purpose of this format is to exchange IED capability descriptions and SA system descriptions between IED and system engineering tools of different manufacturers in a compatible way. This part also defines the engineering process cycle with tool roles and different file types to reflect the different process phases to be done.

2.2.6 Parts linked to the definition of conformance testing

IEC 61850-10 specifies test-cases which must be passed to prove a certain level of interoperability. It applies both to IEDs and tools. It excludes functional testing. UCA/IEC international users group uses this part as a foundation to establish a conformance test procedure. This allows products to be tested in a uniform way and to obtain a certificate of conformance to the standard.

2.2.7 Guideline parts

IEC 61850-7-1 explains the general concepts and can be used as a tutorial. It’s a good means to acquire a global understanding of the standard.

IEC 61850-7-510 explains the modelling of hydroelectric power plants. There are other parts planned in this area as following:

a. 7-5: Application guide

b. 7-500: Use of logical nodes for modelling applications and related concepts and guidelines for substations.

IEC 61850-80-x and **IEC 61850-90-x** series deal with communication mapping with other technologies. The parts **80-x** are mainly “Technical Specifications” (**TS**) which are used as amendments to the IEC 61850 standard, e.g. mapping of other standards like IEC 60870 series/DNP3/Modbus/web protocols or IEEE C34.94). The parts **90-x** are used for “Technical Reports” (**TR**), which are mostly definitions of new features which could be integrated in any future major edition of the standard (like communication between Substations, Substations and Network Centres, LAN (Local Area Network) and WAN (Wide Area Network) etc.). These parts can be seen as extensions to the standard with all requirements to be added in each pillar of the IEC 61850.

2.3 Abstract service interface

To prepare the standard for future usage, the part IEC 61850-7-2 defines an abstract communication service interface (ACSI) for the link between the communication hardware and driver software to the application. Figure D3.4 illustrates the principle based on the OSI (Open Systems Interconnection) communication layer model.

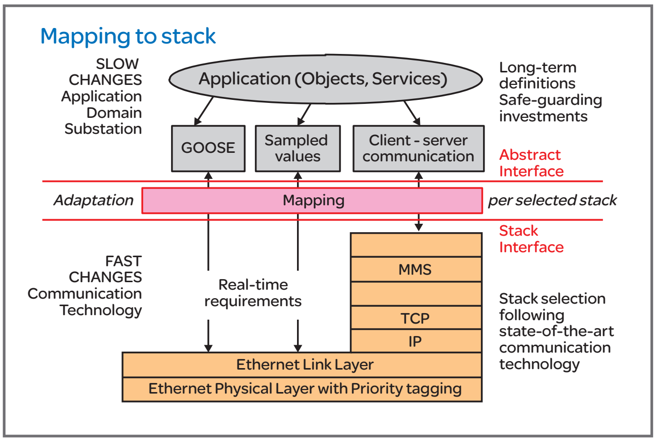

Figure D3.4:
Abstract communication interface

The ACSI allows the development of hardware independent software structures at the application level. This is done by using a communication stack for the connection to the hardware technology selected. As it is expected that the hardware technology is continuously changing in future, e.g. from today’s 100MBit Ethernet to e.g. 1GBit Ethernet, the software part can be kept unchanged as the adaptation to the new hardware is managed by a new or updated

2. General philosophy

communication stack. The stack software itself has to provide an interface to different layers and protocols to support the different services used for IEC 61850. IEC 61850-8-1 and IEC 61850-9-2 currently define the communication media (Hardware level). Table D3.2 details the selected protocols for each category of service with standard part name.

Sampled values	GOOSE	Time synchronisation	Client/server services	Category
IEC 61850 -9-2	IEC 61850-8-1			Standard
SV	GOOSE	Time sync (SNTP)	MMS protocol suite	Application, presentation, session layers
		UPD/IP	TCP/IP T-PROFILE	Transport network, data link layers
SMV	GOOSE			
HSR/PRP (optional)				
802.1Q		802.1Q (optional)		
1 Gb fibre	100 Mb fibre or copper			Physical layer

Table D3.2:
Network mapping for IEC 61850

For "Sampled Values" (see section 3.4) according to part 9-2 and "GOOSE communication" (see section 3.3) according to part 8-1, the data is transported on a low communication layer as multicast on the MAC address level with its own defined data structure and content.

Time Synchronisation is managed by SNTP (Simple Network Time Protocol). IEEE Std1588:2009 can also be used when higher precision is required.

For "Client-Server communication", MMS (Manufacturing Messaging Specification) is used. It was initially designed for the manufacturing industry and it has been chosen, because it is able to support the complex naming and service model of IEC 61850 and the event reporting mechanism. Mapping of the Client-Server services from part 7-2 onto MMS is relatively straightforward. TCP/IP is not the only transport option, but today every device uses it.

A mapping of Client-Server services of part 7-2 using Web-Services is coming and foreseen as the future part 8-2.

2.4 Data modelling

Data modelling allows real world objects to be represented in a virtual world, allowing information to be exchanged digitally. Data is grouped in a structured way allowing a semantic to be applied to give a strong meaning to their virtual representation. The semantic is represented by standardised names listed in part 7-2, 7-3,7-4 and 7-4xx series of the IEC 61850 standard.

The data model of a device is the description of all of its data and their organisation. There is a minimum of 5 nested layers used to define the structure of a data model of the device. All upper levels are used to structure the information and as a container for data of a lower level. Figure D3.5 illustrates this principle. At the lowest level, the data values are managed by Data Attributes (DA). Those are grouped to build Data Objects (DO). At the next level DO are also grouped to build Logical Nodes (LN). LN again are grouped to Logical Devices (LD) and LD to Physical devices. The standard allows two levels of DO or several levels of DA. These sub level elements are named as SDO (Sub Data Object) and SDA (Sub Data Attribute). They are used when the element needs a deeper, more detailed differentiation.

The standard defines the most typical objects which could be added to the data model. Nevertheless this collection of standard objects cannot contain elements for all available information provided by the functionality of an IED. By adding private elements to the data model, it can be extended so that manufacturer specific data can be included as manufacturer specific LN or DO at the right level, without breaking the interoperability.

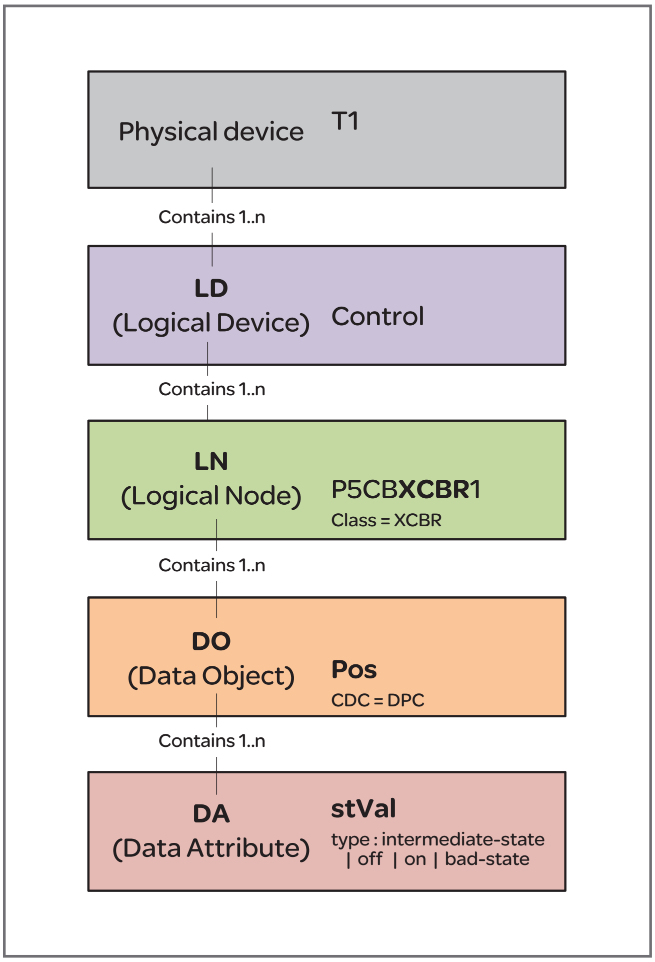

Figure D3.5:
Hierarchy of data model objects

2. General philosophy

2.4.1 Logical devices

A physical device is split into several **Logical Devices (LD)** to allow the structuring of different independent functional groups of functions. A typical bay unit could contain a LD for protection, control or measurements. The grouping and structure depends strongly on the applications for which the physical device is made. An IED hosts one or multiple communication access points and related communication services with one or multiple LDs inside. With Edition 2 of the standard it is also possible to cascade multiple levels of LD.

2.4.2 Logical nodes

Each LD is a collection of **Logical Nodes (LN)**. Each LN is an instance of a Logical Nodes class. Logical Node classes are defined in part 7-4 or part 7-4xx. A Logical Node class represents a well defined autonomous function. For example, class XCBR always represents a circuit breaker and class PDIS a single zone element of the distance protection. LN class names are always built with 4 letters. This first letter is used to categorise the LN class. For example, **P**TOC, **P**DIS, **P**TRC are all LN classes related to protection functions. Table D3.3 shows the different categories available. The standard gives a specific LN class for each dedicated type of application function to define its mandatory or optional DOs. All LNs instantiated from a given Logical Node class are not necessarily identical in terms of DO composition. The presence of some DOs is mandatory. For others, the presence is optional or depends on a set of well defined rules. That means that two LNs built upon the same LN class can be composed of two different DO sets. LNs can exchange information to each other by using embedded DOs or DAs.

2.4.3 Data objects

Each DO is an instance of a **Common Data Class (CDC)**. CDCs are defined in part 7-3. Table D3.4 shows all the available CDCs. CDCs are categorised into 7 categories: status information, measured information, controls, status settings, analogue settings, description information and service tracking. A CDC is a defined class for a DO to list all data attributes required to support all access services. Similar to LN, DO instantiated from a given CDC can be different when additional DA gets added to the collection of DA given by the template.

An example of a DO in LN class XCBR is the DO “Pos”, which contains mainly the DA “stVal” for the position of the circuit breaker, the “t” for the timestamp and the “q” for quality. DA “stVal” is an enumeration with the four states “on”, “off”, “intermediate-state” and “bad state”. “Pos” is based on the CDC class “DPC” which can be controlled and monitored. This is based on the two wires used for the control and two others for the status of a switching device.

The distance LN PDIS itself contains a DO “Str” for the starting information and an “Op” for the trip (Operate) information for the distance element. The DO “Str” and “Op” are based on CDC “SPS” as binary “Single Pole Status”.

LN class first letter / Category	
A	Automatic control
C	Supervisory control
D	Distributed energy resources
F	Functional blocks
G	Generic function references
H	Hydro power
I	Interfacing and archiving
K	Mechanical and non-electrical primary equipment
L	System logical nodes
M	Metering and measurement
P	Protection functions
Q	Power quality events detection related
R	Protection related functions
S	Supervision and monitoring
T	Instrument transformer and sensors
W	Wind power
X	Switchgear
Y	Power transformer and related functions
Z	Further (power system) equipment

Table D3.3:
LN class categories overview

Category	
Status information	SPS,DPS,INS,ENS,ACT,ACD,SEC,BCR,HST, VSS
Measured information	MV,CMV,SAV,WYE,DEL,SEQ,HMV,HWYE,HDEL
Controls	SPC,DPC,INC,ENC,BSC,ISC,APC,BAC
Status settings	SPG,ING,ENG,ORG,TSG,CUG,VSG
Analogue settings	ASG,CURVE,CSG
Description information	DPL,LPL,CSD
Service tracking	CST,BTS,UTS,LTS,GTS,MTS,NTS,STS,CTS,OT, VSD

Table D3.4:
CDC class overview

2.4.4 Data attributes

Each DO is a collection of **Data Attributes (DA)**. A DA is linked to each single information element of the DO and provides information such as the value, its time stamp, its quality and other required information defined for each DO. DA definition can be retrieved by looking inside the CDC definition linked to the DO. DA is mainly defined by its standardised name and its type. The type of DA can by basic (integer, float, string etc.) or already structured (Quality, Range, Unit, Vector etc.). Basic types are defined in part 7-2. Structured types are named 'Constructed attribute classes' and defined in part 7-3. Also standardised enumerations are defined in 7-3 and 7-4. They make use of standardised names.

2.4.5 Data reference

All data owned by a given device has a standardised reference: a name built according to a rule and with standardised names. Physical Device, LD, LN, DO and DA build together as string to create a unique reference. Table D3.5 shows several examples of DA references. For the DO and SDO part, the associated CDC is mentioned. For the DA and SDA, the associated format type is also mentioned.

In example Ex1 (see 1st column in Table D3.5), **T1Control/P5CBXCMB1.Pos.stVal** represents the position of the breaker. Example Ex2 is more complex. It involves 3 levels of DA.

T1Measurement/P5VECAMMXU1.A.phsA.cVal.mag.f represents the current measurement of the Phase A of a measurement unit.

The last example Ex3 represents a setting of an overcurrent protection. **T1Protection/P5PHPTOC1.OpDlTmms.setVal** represents the Operate delay time duration.

The value **T1Protection/P5PHPTOC1.OpDlTmms.units.multiplier** makes it possible to know if the value is in seconds, in milliseconds, or in any other unit.

2.4.6 Communication modelling

The LD/LN/DO/DA hierarchy isn't sufficient to model objects for use by communication services. This section goes deeper into the data model description, so that communication services can be more easily understood.

From a network communication point of view, a system is a set of communicating physical devices connected together using communication networks. IEC 61850 models the system using "Sub Network" and "Access Point" entities.

Sub Network is a logical, visible subdivision of an IP network. Each device on the subnet has a common subnet IP address allowing simple segregation by creating a subnet mask to isolate specific devices assigned.

Access Point represents a network interface of a physical device connected to one as used above to highlight that it is a special expression "Sub Network".

IEC 61850 reference for DA										
	LDName		LNName			DataName[.DataName[. ...]]				
	IEDname (Physical Device Name)	**Ldinst**	**LN Prefix**	**LN Class** defined in part 7-4	**LN Suffix**	**DO** defined in part 7-3	**SDO** defined in part 7-3	**DA** defined in part 7-3	**SDA** defined in part 7-3	**SDA** defined in part 7-3
Ext1	T1	Control	P5CB	XCMB	1	Pos CDC: DPC		stVal Type : intermediate-state | off | on | bad-state		
Ext2	T1	Measurement	P5VECA	MMXU	1	A CDC: WYE	phsA CDC: CMV	cVal Type: Vector	mag Type : AnalogueValue	f Type: float
Ext3	T1	Protection	P5PH	PTOC	1	OpDlTmms CDC: ING		units Type:Unit	multiplier Type: enum	

Table D3.5:
Reference overview for DA

D3

2. General philosophy

Server is the logical grouping of Logical Devices. It controls the access to the whole set of data exposed by a given physical device through a given Access Point. Dedicated Authentication mechanisms could be described at that level. Server is the owner of the data. A physical device can own several access points and so it can communicate on several networks. Facilities are provided, so that the same Server is exposed to manage this multiple network access. Figure D3.6 outlines all entities required for communication purpose. The picture introduces the new "Control Block", "Data Set" and "LOG" entities.

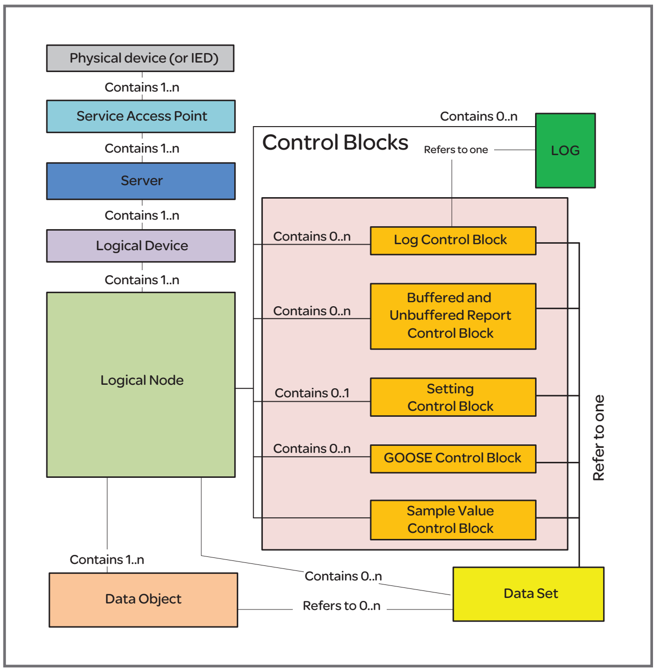

Figure D3.6:
Data model for communication services

A Data Set is an ordered group of DO and DA references called the members of the data set. The membership and order of the references in a data set shall be known to both the client/subscriber and the server/publisher, therefore it is included as a list in the data model and the ICD file. This capability avoids the transmission of many references in the messages and permits more efficient use of the communications bandwidth. Data Set can be usually pre-defined at configuration, but can also be dynamically created or modified using a dedicated communication services model. This feature provides a lot of flexibility.

Control blocks are used for Logging, Reporting, Setting Group management, GOOSE and Sampled Values services to configure the transmission networks. Facilities are provided, so that the same Server is exposed to work on several networks.

LOG is the data base where events are stored. The client can later retrieve them by using the logging services.

Figure D3.6 outlines all entities required for communication purpose with properties and runtime behaviour of the associated communication services. For the data transmission each control block gets a data set assigned defining the data content behind it. When an event-triggered transmission for the control block is configured, a report will only happen, when one of the references in the assigned Data Set has changed its status. Similarly to data set, control blocks can be defined dynamically (during operation).

2.5 Engineering process

2.5.1 Substation configuration language

Based on the very widely used **eXtensible Markup Language** (**XML**) as the exchange data format, IEC 61850 provides a configuration language, the **System Configuration Language** (**SCL**). SCL defines how the data is structured inside the file to allow an interoperable way to import and export data between the different tools from possibly different vendors.

The SCL is used to store all relevant information objects such as the data model, the supported services and the communication parameters of an IED in one common file. Secondly at a higher hierarchy level, an SCL file is used to describe the whole substation system with all its primary and secondary equipment. It contains the collection of IEDs including the links between them and the primary equipment.

SCL is defined in IEC 61850-6. SCL benefits from the XML format as it allows a deep control of the content through a normalised schema definition file (XSD files) specifically for IEC 61850.

The SCL file contains the following sub-sections:

a. The definition of the primary power system structure (transformers, breakers, etc.) and how the apparatus is connected. The functional specification of the power system switchyard equipment, and how it relates to the communication system and IEDs

b. The communication system: how IEDs are connected to networks and sub-networks, the IP addresses, multicast addresses, VLAN definition and other communication network parameters

c. For each IED: the logical devices configured on the IED, the logical nodes, off-line configuration values, the configuration of control blocks and data sets, supported ACSI services

d. A Data Type Template section with definition of LN, DO, DA types and used format (e.g. list of enumeration types)

Subsection (**a**) helps LNs to perform their processing. Subsection (**b**) allows the binding to the network. With the contents of subsection (**c**) and (**d**) the IED can build and initialise its runtime data model.

All this information is stored in various types of file with different subsets of data, described in Table D3.6.

2. General philosophy

SCL file	File extension	Description
IED capability description	ICD	The ICD contains a description of the functional capabilities of a specific IED type. It acts as an un-configured template to be configured in a System or IED Configuration Tool.
Instantiated IED description	IID	The IID contains a configured instance for a single IED for a specific IED of a project. It may have some components already configured such as project addresses or data sets. This data can be imported to a System Configuration Tool.
System specification description	SSD	The SSD describes the system specification including the single line diagram of the substation, the required substation switchyard equipment, their functions and all its required Logical Nodes. It can also contain specification of virtual IEDs which can be used to adapt the modelling to a profile.
Substation configuration description	SCD	The SCD contains the complete system configuration including the substation specification, all configured IED instances and the communication configurations.
Configured IED description	CID	The CID file is meant to be sent directly to the IED for configuration. It contains information related to configuring the communications for a specific IED. It can contain standardised or private data in an interoperable description.
System exchange description	SED	The SED describes interfaces for data that needs to be exchanged between different systems or projects. The SED gets exchanged between different System Configuration Tools (SCT) or different projects managed by the same SCT.

Table D3.6:
File types according IEC 61850-6

All these files allow data transfer between different engineering tools and devices independent of vendor. This eliminates some of the intermediate steps that are required when using more traditional tools for substation engineering in projects and helps to maintain data consistency.

2.5.2 The engineering cycle

The IEC 61850 standard defines a methodology for engineering a substation automation system in an object-oriented, multi-vendor environment. Two main tools are used to achieve the configuration process.

The **System Specification Tool** (**SST**) is used to specify a system with all primary and secondary equipment of the substation on the basis of the functional topology and required logical nodes. The tool is able to:

a. Model a substation

b. Export an SSD file with the substation specification

The **System Configuration Tool** (**SCT**) is an IED independent tool to specify a system. The tool is able to:

a. Import an ICD/IID files for the various IEDs used in the system

b. Configure communication parameters and dataflow (configuration, data sets, control blocks, external references etc.,) for IEDs

c. Export an SCD file with the modelling of the whole substation and used IEDs

d. Import a specification by mean of an SSD

e. Exchange with other system configuration tools by import/export an SED (optional)

The **IED Configuration Tool** (**IET**) is a manufacturer specific or at least IED specific tool. It is able to:

a. Create an ICD file as IED template

b. Configure a linked IED using private means

c. import an SCD file to get data for an IED from the SCT

d. Export (IID) SCL files

e. Export a CID file or any other manufacturer specific format to configure the real IED (CID capability is not mandatory)

Figure D3.7 shows the data flow for a usual “Top Down configuration process”. The following list gives the detailed description for each step marked with a number, the red and green colour shows the engineering for two different vendor IEDs:

1 Availability of ICD or IID files

Most organisations have a process to choose the standard IEDs used in their substations, based on their specific protection and control philosophies and the required logical nodes for their power system. This allows a pre-selection of the ICD files required for the system configuration.

Native IED configuration tools contain a mechanism to export ICD files which act as a template for a specific IED containing the logical nodes supported by the device and its capabilities. In some cases, an organisation may have standardised configuration parameters such as network addresses or preconfigured data sets. In this case an IID file can be used. The IID file would contain the same data as the ICD file, plus it would also contain additional parameters regarding the configuration for a specific IED. The objects in an IID can already be reduced to those ones used in the dedicated substation system.

D3

2. General philosophy

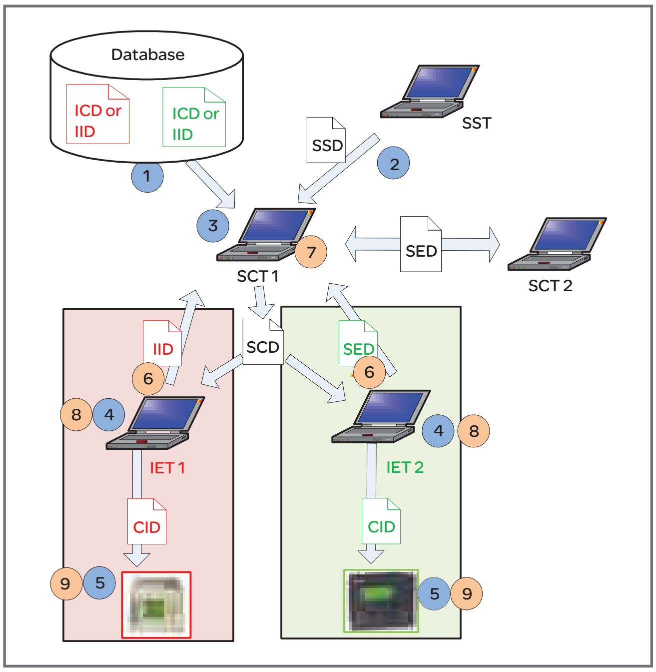

Figure D3.7:
Top Down Cycle

2 SSD file setup

In parallel, substation engineers define the substation specification based on their operating methodologies. This includes defining the primary switchyard equipment, their functions, the single line diagram and choosing the necessary logical nodes. This data contains a substation section of the project.

3 System engineering

Once the group of IEDs and the system specification have been defined, they can be imported into a system configuration tool. Within the system configuration tool the engineer can define specific instances from the different IED templates and link them to the electrical process. The engineer can then define project-specific addressing and configure the data model by defining the data sets for Reporting and GOOSE publishing/subscribing amongst the various IEDs. The complete substation description, all IEDs and communications configuration can be exported then as an SCD file.

4 IED configuration level engineering

The SCD file can be imported to various vendor specific ICTs to complete the protection, control, and device-specific configuration. The IED configuration tool is fully aware of the data available to it from the system and can make use of this data in the protection logic.

5 IED download of configuration file

When the IED specific configuration is completed, the configuration can be downloaded to the IED through a proprietary way or by transferring a CID file with standardised objects to the IED. In real life, this Top Down configuration process is not sufficient. Often, during the process, changes are made at the communication level. A further “Round Trip” of the configuration process needs to be performed.

6 The impacted **IED configurator exports** its IID files for a next “Round Trip” cycle.

7 System configurator import

An SCD file is rebuilt by importing the IID file back into the system configuration tool. All related IED sections at the substation level will be updated accordingly. A further repeat of the top down cycle (steps 4 & 5) ensures that any IEDs impacted by the IID are updated with new information.

8 Repetition of step 4 (2nd loop of the Top Down Cycle)

9 Repetition of step 5 (2nd loop of the Top Down Cycle)

Several further cycles could be required to complete the configuration process ending up at system configuration level as final system documentation.

2.6 Documentation

For the engineering and testing of IEDs the user needs sufficient documentation of the supported services and data. The standard specifies the IED file described in the engineering process in section 2.5. This file contains the whole data model and object classes in a structured ASCII format. In addition the standard specifies the following text files which each vendor has to provide on request to the user:

A “Protocol Implementation Conformance Statement” **(PICS)** lists all supported services with Yes/No statements so that a user or tester understands the IED capabilities.

A “Model Implementation Conformance Statement” **(MICS** lists all used object classes which are given in the ICD file in the type template section.

A “Protocol Implementation eXtra Information for Testing” **(PIXIT)** provides additional information on possible restrictions and predetermined boundary conditions of the IED on the supported services and available data which is relevant for the conformance testing (e.g. a functional limitation or a remark to a special setting or configuration).

A “Technical Issue Conformance Statement“ **(TICS)** provides a statement to each Tissue raised at the standardisation committee, if the IED already supports the corrected subject of the standard or not. With each new conformity test this document has to be updated to include all Tissues known at the moment of testing. For Tissues with relevance to the interoperability, it is essential for the conformity tester to evaluate the impact when the IED is not designed according the latest definitions.

All these documents are mandatory for a vendor IED to get a conformity certificate by any test institute.

2.7 Interoperability vs. interchangeability

One of the main disadvantages of conventional communication standards was always the limitations on the compatibility between devices from different vendors to provide sufficient system functionality by exchanging data in the right form and content and to use similar procedures to transmit them. The IEC 61850 standard has addressed this topic as a central requirement under the heading of "Interoperability".

Interoperability is the ability of two or more intelligent electronic devices from the same vendor, or different vendors, to exchange information and to use that information for correct co-operation.

To achieve this goal the standard provides the following key elements:

a. Open modelling method to describe each possible data object in its functional context in such a way that each tool and component in the system can understand and process this data

b. Standardised file format to exchange the data description and device capabilities between tools of different vendors without limitations

c. Standardised communication procedures called "services" to allow system wide interaction between components of different vendors as a complete system

d. Standardised mapping on a network to use unique communication and hardware layers

e. Test method definition to confirm interoperable behaviour of all system components

For the last topic part 10 called "Conformance Testing" was added to ensure that each vendor or third party can execute a test of a product or system component to confirm its level of interoperability to the standard. The main topic of the defined testing is the proof of the correct implementation of data modelling, services, description files and documentation. This testing only proves that there is no inconsistency between the data model, description file and documentation.

For the services all the different procedures and their use cases including fault reaction behaviour are validated.

The validation of which functional objects are modelled and how they are structured is out of scope of this conformance testing. This can lead to differences between the communication partners and results in an issue around the "interchangeability".

Interchangeability is the possibility to replace one intelligent electronic device by another one without additional modifications of the equipment around it. This possibility is normally only given when the same type of IED or system component from the same vendor on the same product platform is used as a replacement.

In terms of a communication protocol, it can only be said that full interchangeability occurs when the IEDs or system components from different vendors can provide the full collection of services and similar data content for the specific substation in which it is installed. As the standard offers a very flexible way of data modelling and a lot of space for interpretation of it, the data modelling for each vendor IED is quite different. The related data model of an IED is known in IEC 61850 as "Product Naming".

Product Naming (PN) is the fixed or default data model of the IED reflecting the complete hierarchy/structure of the functions inside an IED. IEC 61850 also provides a user view looking more from the substation and primary equipment side called "Functional Naming".

Functional Naming (FN) is the reflection of the functional application view (like in a substation) in the naming of the structural elements of an IED data model as LDname (IEDname+LDInst) and LN pre/suffix. To reach any kind of interchangeability, it is required to modify the data model in the IED in such a way, that all data exchanged has the same naming with same function behind it. IEDs that provide this capability provide "Flexible Product Naming" functionality.

Flexible Product Naming (fPN) allows the data model of an IED to be modified to reflect the hierarchy/structure defined by the overall scheme. This means that, from the communication point of view, any IED can be remodelled to comply with the overall substation control scheme structure and thus the IED data definition can become vendor independent. Figures D3.8 and D3.9 show two examples for the fPN remodelling.

There are of course other criteria for the interchangeability such as the different hardware solutions, e.g. case and mounting, power supply, wiring for CT/VT and I/O will be different as well as the tools used for its configuration. Therefore a communication standard can only provide a general basis to reach compatibility without standardisation of the products and system components.

FN - Functional naming (Customer substation view)

Station	Vtg Lvl	Bay	Function	IED	Subf	LN	Suffix	DO	DA
IEDName (Server)			PROT		Prefix	LN	Suffix	DO Name	DA Name
Frankfurt	110 kV	E2	Protection	1	Dtoc	PTOC	2	Str	stVal

PN - Fix product naming (IED address mapping for device "P139")

Station	Vlt Lvl	Bay	Function	Subf	Prefix	LN	Suffix	DO	DA
IEDName (Server)			LDinst		Präfix	LN	Suffix	DO Name	DA Name
P139			Protection		DtpPhs	PTOC	1	Str	stVal

fPN - Flexible product naming (After remodelling by an IED configurator)

Station	Vtg Lvl	Bay	Function	IED	Subf	LN	Suffix	DO	DA
IEDName (Server)			LDinst		Prefix	LN	Suffix	DO Name	DA Name
Frankfurt	110 kV	E2	Protection	1	Dtoc	PTOC	2	Str	stVal

Figure D3.8:
Example for fPN on protection elements

D3

2. General philosophy

FN - Functional naming (Customer substation view)

Station	Vtg Lvl	Bay	Function	IED	Subf	LN	Suffix	DO	DA
IEDName (Server)			PROT		Prefix	LN	Suffix	DO Name	DA Name
Frankfurt	110 kV	E2	Control	1	QA1	XCBR	1	Pos	stVal

PN - Fix product naming (IED address mapping for device "P139")

Station	Vlt Lvl	Bay	Function	Subf	Prefix	LN	Suffix	DO	DA
IEDName (Server)		LDinst			Präfix	LN	Suffix	DO Name	DA Name
P139			Control			XCBR	1	Str	stVal

fPN - Flexible product naming (After remodelling by an IED configurator)

Station	Vtg Lvl	Bay	Function	IED	Subf	LN	Suffix	DO	DA
IEDName (Server)			LDinst		Prefix	LN	Suffix	DO Name	DA Name
Frankfurt	110 kV	E2	Control	1	QA1	XCBR	1	Pos	stVal

Figure D3.9:
Example for fPN on control elements

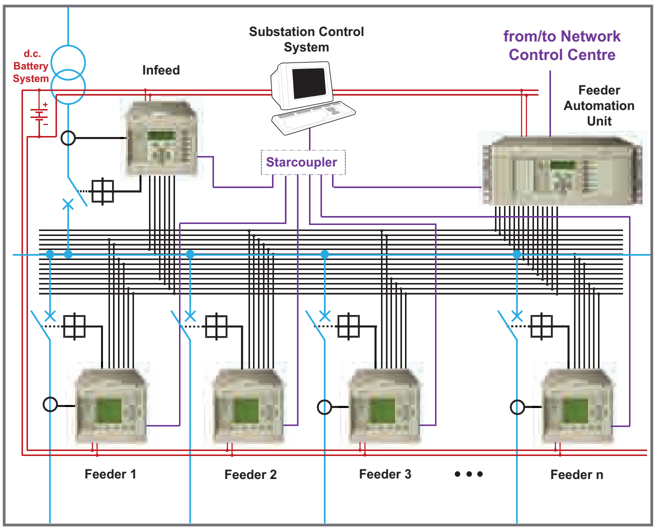

Figure D3.10:
Conventional I/O wiring with feeder automation unit and serial bus system

2.8 Advantages vs. conventional hard-wiring

IEC 61850 provides a lot of areas for optimisation. One specific area is the concept to use one single bus system, such as the Ethernet protocol and related network equipment, to communicate between IEDs and all other system components in a substation and beyond. In parallel with conventional protocol links there are conventionally a considerable amount of electrical wires installed in a substation to exchange binary signals between all IEDs and system components. IEC 61850 provides the opportunity to save cost by the reduction of the required amount of wiring, binary inputs and outputs in the IED. It can do this by the use of client-server or GOOSE communication, which supports the high speed exchange of binary data equivalent to the hardwire signals. By using GOOSE the system is not only cheaper to install but it facilitates testing, post design modifications and commissioning.

For illustration Figure D3.10 shows a typical wiring plan for a complete substation with related I/O wiring. Here we show a bay unit and feeder automation units collecting all signals and providing them to the network control system using a conventional 60870-5-103 bus in star whereas Figure D3.11 shows the optimised solution with an Ethernet redundant ring and Gateway to the network control system.

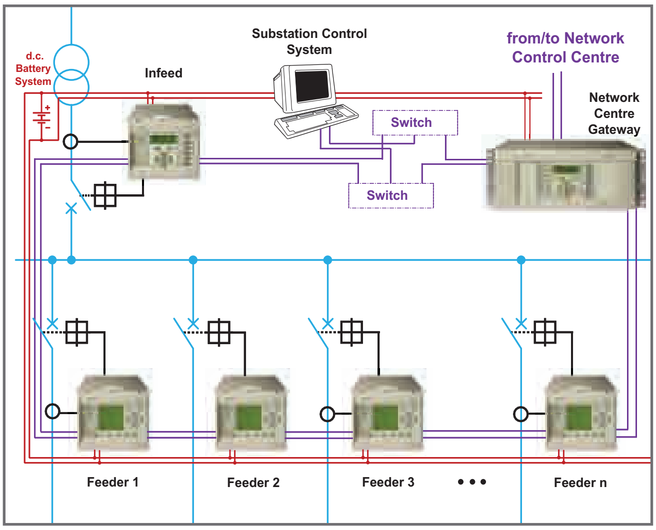

Figure D3.11:
Modern redundant ethernet installation

3. Communication services

This section describes the fundamental "Substation Communication Architecture", which outlines the usage of four communication models. The second section follows with the Client-Server related communication services. The last three sections deal with GOOSE, Sampled Values and finally the Time Synchronisation.

Part 7-2 defines an abstract communication services interface (ACSI) for a compatible exchange of information among all available communication partners and IEDs in a substation. The standard offers the following four types of communication models:

a. Classical Client-Server services model

b. GOOSE (Generic Object Oriented Substation Event) communication with fast and reliable distribution of DO and DA references based on Communication Publisher/Subscriber model

c. Sampled values distribution model based on Communication Publisher/Subscriber model

d. Time synchronisation protocols

3.1 General communication architectures

Today, three communication levels are considered in IEC 61850: "station level", "bay level" and "process level". Figure D3.12 shows the related substation network architecture.

The Station Bus is dedicated to a substation, or power system or more globally, management system for control and protection. The communication at this level is a mix of fast data exchange for protection and automation and of data reporting with less time constraints but with more detailed information flow.

On the lower level, the "Process Bus" is dedicated to the exchange of data between primary devices and the control and protection IEDs.

(1) Represents substation data exchange between the bay units at bay level and the substation control equipment at station level. The criticality of the data allows usage of the Client-Server service model (green marked lines). The same applies for data exchange within the station level **(2)**.

(3) and **(4)** shows the data exchange within the bay level between the bay units (so called "IED to IED communication"). GOOSE is used for that purpose (blue marked lines).

From the bay level down to the process bus level **(5)**, control-data is sent from bay units to the process using GOOSE. Often hardwires are still used here instead of a real process bus (dotted black lines on the right bay level part).

(6) represents the exchange of instantaneous data from the process to the bay level, e.g. analogue values from current and voltage transformers or status of sensors or switches.

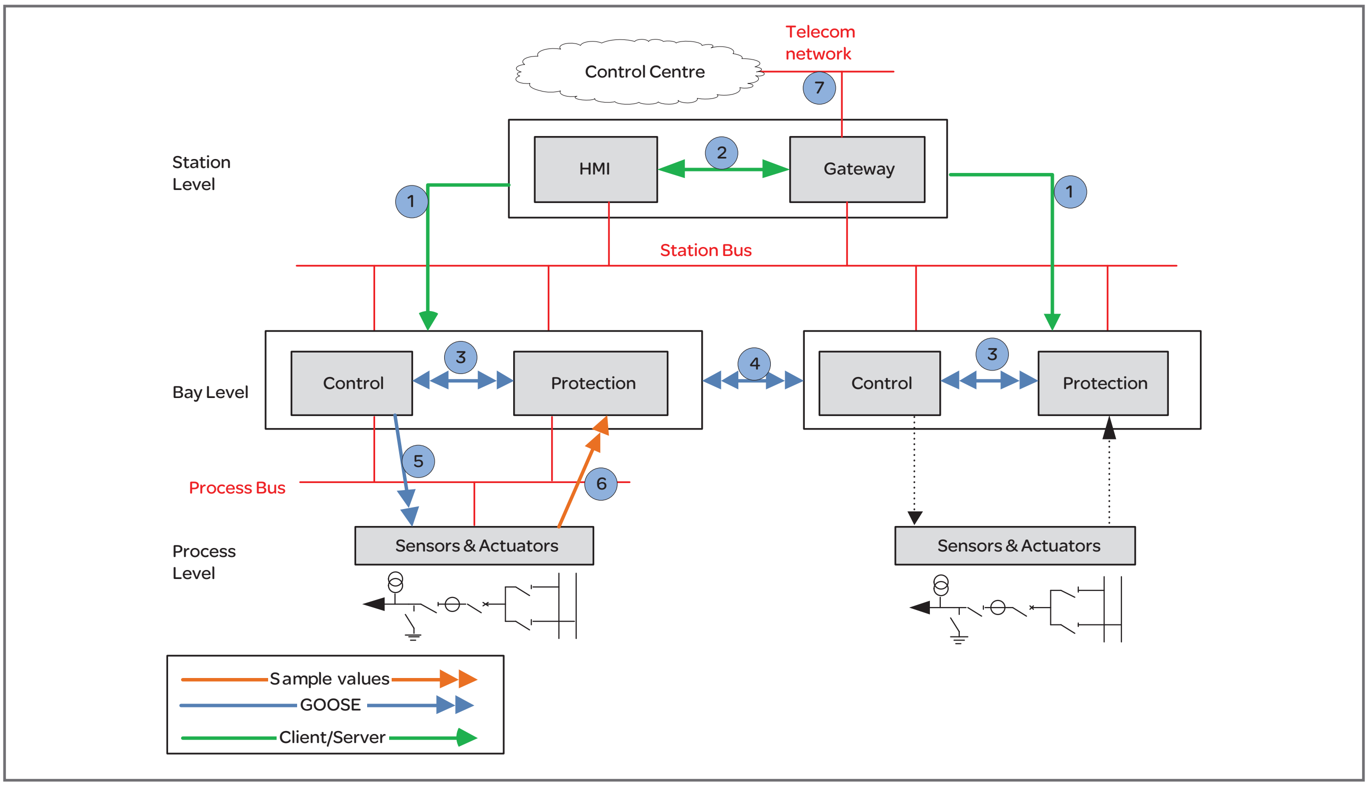

Figure D3.12:
Communication architecture

D3

3. Communication services

Analogue values are time critical and they need to be transferred in a precise and chronological order. Sampled values distribution model is used (orange marked lines). For the binary information the usage of GOOSE is usual.

The telecontrol network is used to report data from the substation to other network systems. Traditionally, this level **(7)** is based on SCADA protocols like DNP3, T101 or T104. Part 90-2 is under preparation to define the link between a station bus and a control centre using IEC 61850 services.

The Station and Process Bus shown in Figure D3.12 can be carried out as a separate physical network or on basis of the same physical network by using virtual addressing to filter and separate data at the network switch level.

3.2 Client-server communication

In software engineering a server is an entity that provides information to other communication partners. All entities who are interested in receiving this information are called clients. Each client can request the server to open a continuous connection to subscribe information. During the startup of the connection the client can configure how the information has to be transmitted. When a connection has been established, the server sends all upcoming information to the client and handles and responds to the requests from all the clients connected to it. A server can manage simultaneous connections to several clients as shown in Figure D3.13. A client can also connect to several servers.

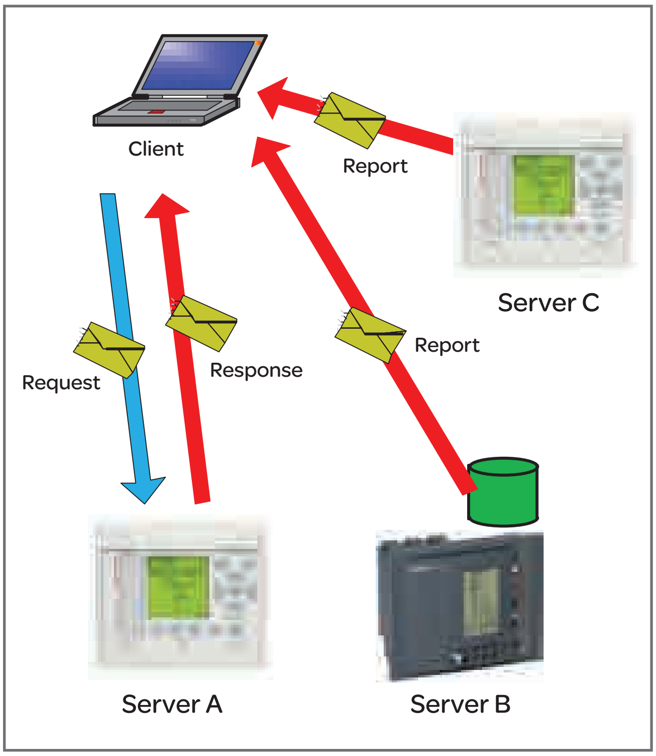

Figure D3.13:
Client-Server communication

Figure D3.14 illustrates the basics of the Client-Server communication services. The communication starts by the establishment of a connection using the “Associate” service. The Associate request message is sent by the client to the server and contains input parameters. The response message is sent by the server to the client and contains output parameters. Often a Control Block or LN, DO or DA reference is used as input or output parameter, just to identify which part of the model the service acts upon. The response message contains the result of the processing of the input parameters. This can be an error code if a failure occurs, the requested information for a simple reading request or simply an acknowledgement of the right command execution.

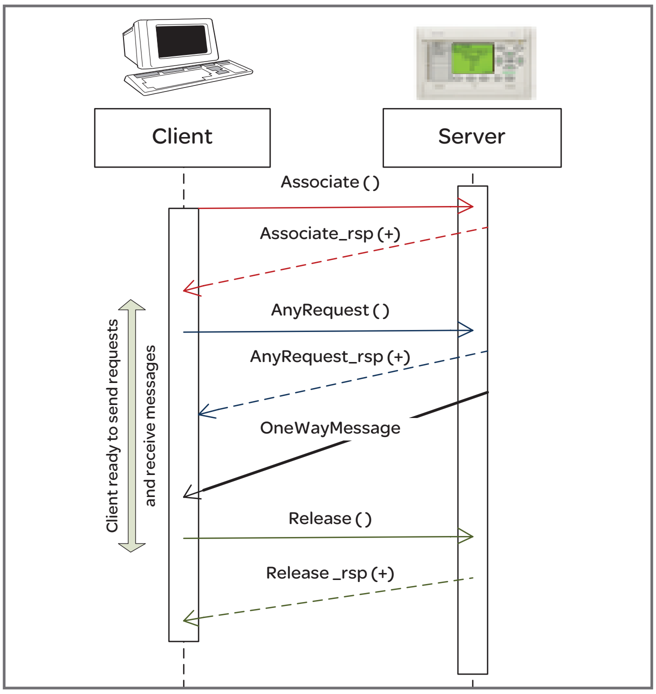

Figure D3.14:
Procedures for Client-Server communication

Two communication services are unidirectional, that means a message is sent, but no response is expected. One is the “Command Termination” service used in the “control model”. Second is the “Report” service defined in the information “Report model”. Finally, the client ends the data exchange with the server by using a “Release” communication service.

3.2.1 Self-description of device

To work properly, clients e.g. a Human Machine Interface (HMI) need to be configured by an ICD file, to understand and visualise all information received by the servers. During the opening of the connection the client often sends a self-description service, to check that his configuration is in line with the server data model.

Some clients, for example Operating or Test Software, can perform tasks without any pre-configuration. In this case, self-description services are used to acquire the server data model to understand the available services and information.

3.2.2 Real-time data access and retrieval

The data provided by a Server can be static with no change expected during operation (e.g. a serial number) or change slowly or rarely, dependent on the process behind it. Real-time data access and retrieval services deal with data that is static or is changing slowly or not time-critical. The client can read this data from time to time to get an update by "Polling". The data object retrieval services shall be used only when the data change isn't time-critical for the client. If a fast data update is required, the client has to use the event reporting services described in the next section. The typical service used to read data from a server is "GetDataValues". Figure D3.15 illustrates how a client retrieves information about the vendor and software version of an IED. Reading DA NamPlt in the LN LLN0 of the LD Measurement.

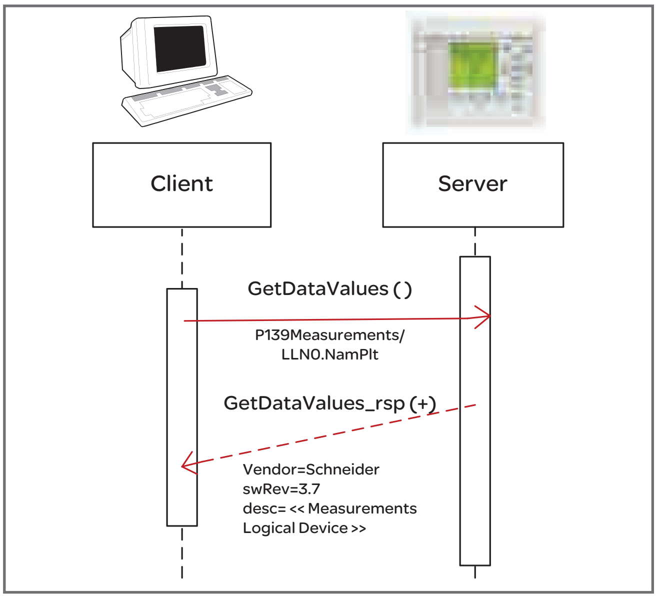

Figure D3.15:
GetDataValues service

Using the service "SetDataValues", a client can overwrite the value of a data object on server side, when this capability is offered by the server. This is described in the IED configuration file (ICD/IID).

3.2.3 Event reporting and logging

The "Reporting" services are used to fulfill the requirement of event-driven information exchange. Event reporting is useful to save network bandwidth and is much more efficient in comparison to the traditional "Polling" procedure reading cyclic data. As long as no data change happens, no data transmission takes place. When one or multiple data objects are changing their value and/or quality status, a report is sent by the server using the service "Reporting", to update all clients subscribing to the related data objects.

The "Logging" services are provided when the event reporting is not required as the information is not time-critical, but the changes should be traced and no data change should be lost. The client can request the data from time to time to collect in a central long term storage.

Reports and logs are both controlled by a control block linked to a Data Set. The data management behind both is very similar. When a data change occurs, each active report or log control block evaluates if the change must generate an event based on its current configuration.

Two kinds of reports are available, the "Unbuffered Reports" and the "Buffered Reports". Related control blocks are named as URCB (Unbuffered Report Control Block) and BRCB (Buffered Report Control Block). With an Unbuffered Report a data change will get lost by a client, if the change happens when the link is disconnected. In the case of Buffered Reports, the server keeps a queue of the events. After a link recovery, the affected client is able to retrieve older events from this data queue.

Report control blocks provide a lot of flexibility with configuration parameters to define the content of the sending message, sending cycle, deadbands for measurements, behaviour during integrity scan or general interrogation.

Figure D3.16 illustrates the basic usage of event reporting services with buffered reports. Behind the pre-configuration by the service "SetBRCBValues" the server is starting to send reports in a pre-defined sending cycle. Other services are for example "GetURCBValues" to read a control block configuration or "QueryLogAfter" to get data from the Logging queue.

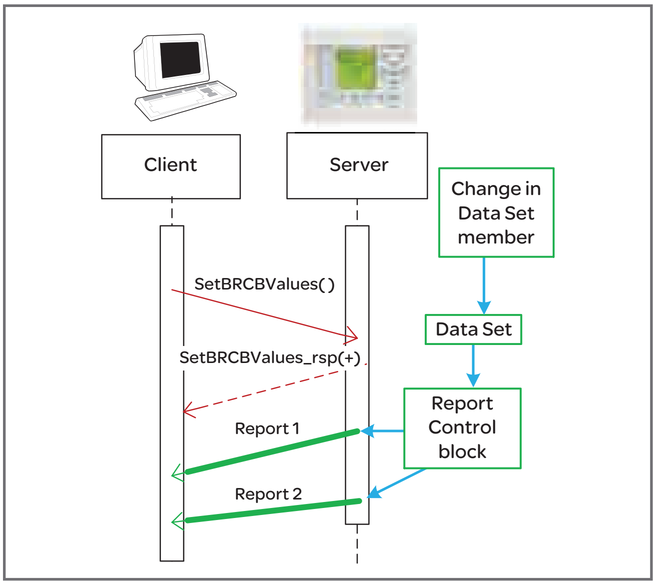

Figure D3.16:
Procedure for reporting

D3

3. Communication services

3.2.4 Device control

For control the following services are available:

a. Direct control with normal security

b. Direct control with enhanced security

c. SBO control with normal security

d. SBO control with enhanced security

e. Status-only (for manual operation) only

"Direct control" is used when no pre-selection of the equipment is required, whereas "SBO control" require operator to first select a control to ensure that no other process will execute the control at the same time. Control with "normal security" does not respond to the client with a value check result after operate. Control "with enhanced security" is always sending a "command termination" at the procedure completion to confirm if the demanded state/position has been reached or not.

For the control of objects in the LN classes, e.g. the control of DO "Mod" to change the operating mode of a logical node, a direct control with normal or enhanced security is usually used.

For the control of switchgear equipment in substations it is strongly recommended to use only the "SBO with enhanced security". The typical sequences for an SBO control with enhanced security are illustrated in Figures D3.17 to D3.20 showing each single process step for understanding.

Figure D3.17 shows the enhanced select and operate procedure with successful termination. At first the client sends a "Select Value Request" for an open (on) or a close (off). When receiving a positive "Select Value Response" back from the IED the same client sends an "Operate Request" for the open/close operation. Now the switch controller sends an "Activate Output Request" to the logical node representing the switching device (XCBR, XSWI). Directly afterwards it responds to the client with a positive "Operate Response" to confirm the start of a switch actuation. While the primary device is moving, the logical node representing the switching device first sends an intermediate-state and then the new on/off position as requested. As soon as the end position gets returned, the switch controller sends a positive "Report Request" independent of the validation followed afterwards.

If the new status value is the one requested by the client, a positive "Command Termination" is sent to close the sequence.

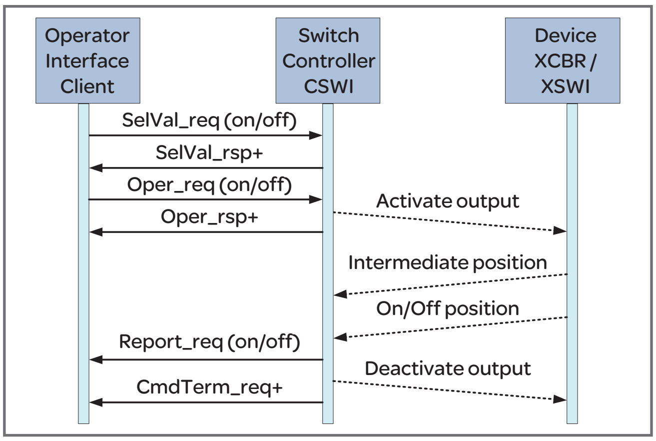

Figure D3.17:
SBO control with enhanced security
Positive command response and termination

Figure D3.18 shows a select with unsuccessful selection. At first the client sends a "Select Value Request" for on/off. If another device has already been selected or is in operation, the switch controller returns a negative "Select Value Response" to abort the sequence.

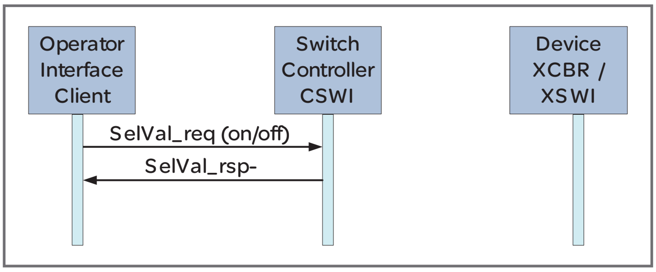

Figure D3.18:
SBO control with enhanced security
Negative select response

Figure D3.19 shows a select and an operate with successful cancellation by the client. At first the client sends a "Select Value Request" for on/off. When receiving a positive "Select Value Response" the same client operator decides that the wrong device has been selected or the switching does not make sense anymore. Then a "Cancel Request" can be sent to stop the procedure. Now the switch controller sends a positive "Cancel Response" to close the sequence.

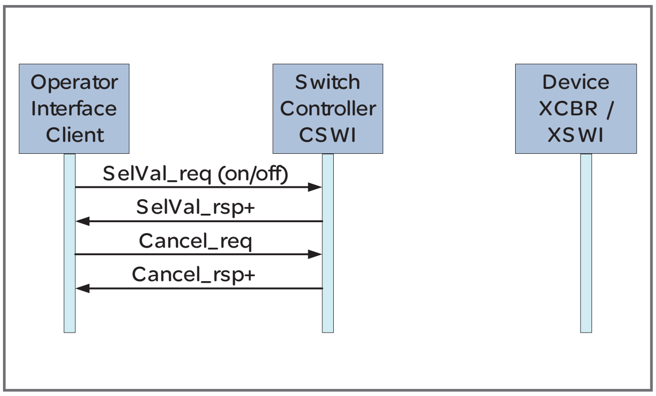

Figure D3.19:
SBO control with enhanced security
Cancel command response

Figure D3.20 shows a select and operate with time-out. The first part of the sequence is similar to the first case with positive select and operate, but when activating the output, the position signals of the device are not changing. A possible reason for this could be that the switching device did not start to operate or that it did not reach the final position due to a mechanical error. With an expired supervision time the switch controller sends a negative command termination as a result of the validation test.

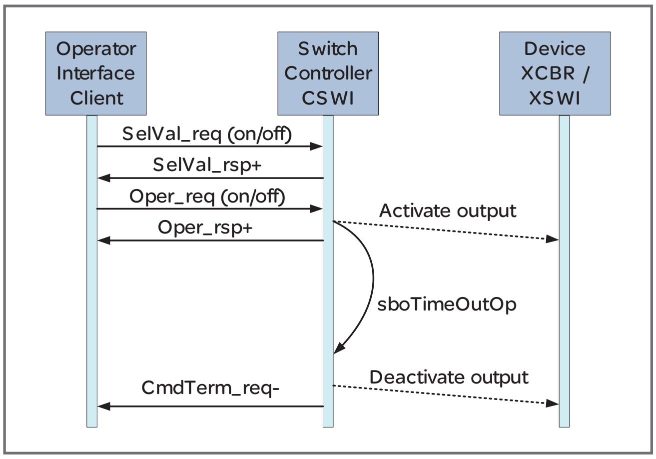

Figure D3.20:
SBO control with enhanced security
Negative command termination

All shown sequences are similar for a direct control procedure except that the select request and response at the beginning are not used.

3.2.5 Setting and setting group management

The initial physical device behaviour is defined by its setting and configuration. During operation it can be useful to allow adjustments of setting and configuration parameters in order to adapt them to changing circumstances. Providing an interoperable changing capability on parameters during operation brings a lot of flexibility. Settings and setting groups are defined in IEC 61850 for that purpose. They offer a standardised way to adjust the behaviour of a device. Adjustments can be done either on a single parameter ("Setting Management") or on sets of parameters ("Setting Group Management"). A given parameter is managed either in standalone or through a set, but not both.

For Setting Management, a client uses the service "SetDataValues" to change parameters one by one. Setting Group Management allows consistent management of a set of parameters. Setting groups are managed using a Setting Group Control Block (SGCB).No data set is needed, because the definition of the set of parameters is defined by the standard as DOs for each LN. The initial values of those parameters are defined during the engineering phase.

During operation a client may use "SetEditSGValue" to change parameters of a setting group during operation or "SelectActiveSG" to switch from a group of parameters to another one. For example, a group of parameters can be used during summer and another during winter.

3.2.6 File transfer

IEC 61850 provides basic file management facilities. A server (IED) has to manage this with a real or virtual file system. File transfer is used to upload files from a client to the server or to download files from the server to the client. Typical files transmitted from the client to the server are configuration or setting files. In the opposite direction recordings, loggings or documentation files can be sent from the server to the client. The services used are "GetFile" for file retrieval as illustrated in Figure D3.21 to retrieve a fault recording. In the opposite direction, the "SetFile" service can be used to send e.g. a CID file for the configuration to the server. Finally, a client can have access to some file attributes using "GetFileAttributeValues" or delete a file using "DeleteFile".

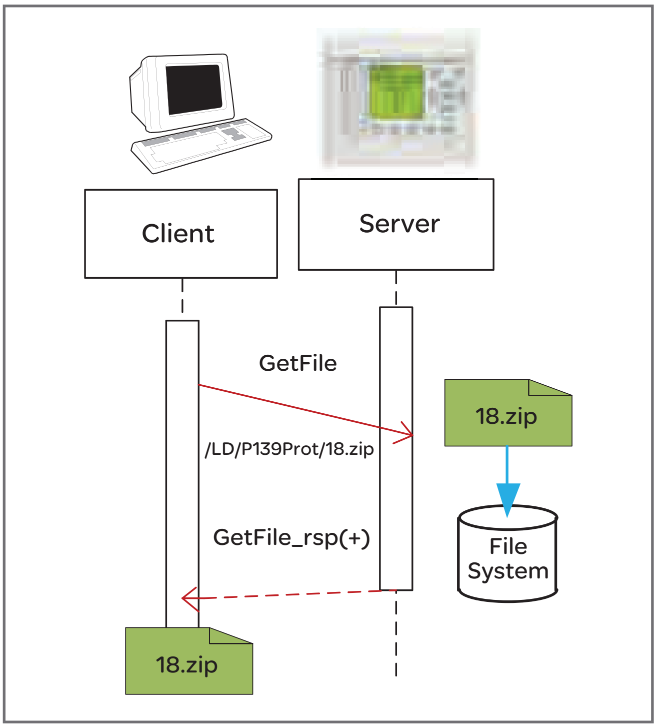

Figure D3.21:
File transfer for fault recording

3.2.7 Substitution

Clients can request the server to replace a process value by a fixed one. It can be useful in case of acquisition failure of external equipment, e.g. a sensor which moves out of order. In IEC 61850, this mechanism to replace a process value for a dedicated time is called 'Substitution'. The service "SetDataValues" is used for that purpose. The substitution

3. Communication services

mechanism is optional and is handled only on server side. The clients handle the 'substituted' process value as a normal value. The only difference is on the quality of the value: a dedicated field indicates that the value has been substituted.

3.3 GOOSE communication

Publish/Subscribe communication is used for the transmission of a "GOOSE" (Generic Object Oriented Substation Event) message. GOOSE communication is used for the fast and reliable distribution of DO or DA reference from one IED to other IEDs. In comparison to Client-Server communication, no dedicated link connection is required. As illustrated in Figure D3.22, a "Publisher" posts a message to all IEDs in the same network using a multicast address as destination address. All subscribers (here "Subscriber A" and "Subscriber B") in the network receive this message and identifies if it contains the same multicast address as if pre-configured in their subscription. If this is the case, the IED processes the data of this GOOSE to its internal function. If not, the message will be ignored.

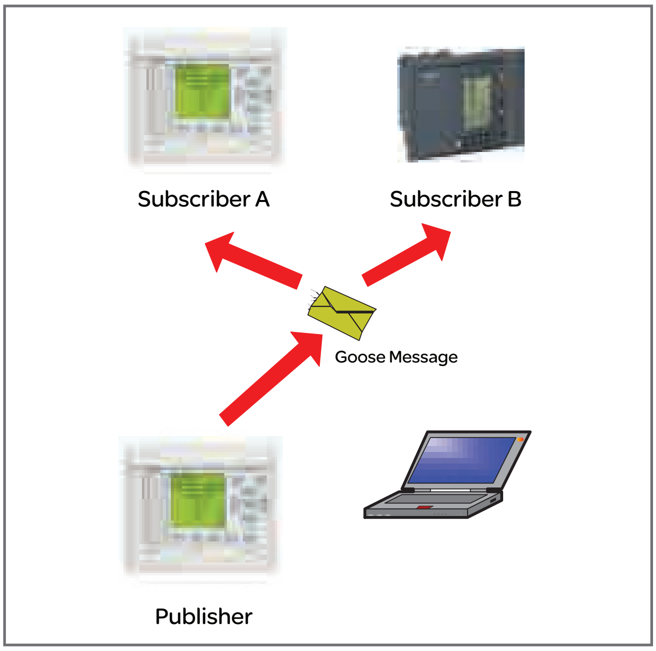

Figure D3.22:
Configuration for GOOSE communication

An IED usually receives GOOSE messages from different IEDs as well as over several different multicast addresses. An example is shown in Figure D3.23, where a "Message A" is received only by "Subcriber2", as "Subscriber1" isn't subscribing to the same multicast address. "MessageB & C" are both received at the same time by both "Subscriber1 and 2". "MessageD"again is received only by "Subscriber1" as it will be ignored by "Subscriber2" due to the unsubscribed multicast address.

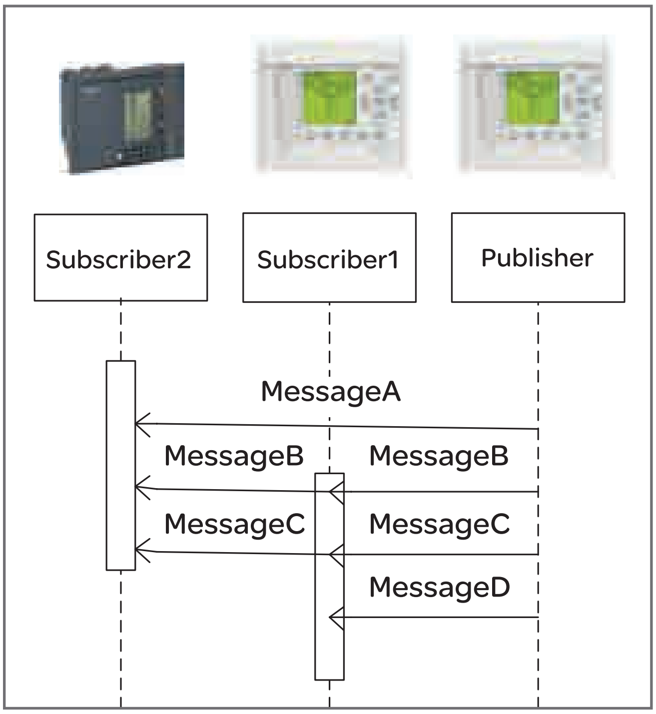

Figure D3.23:
Procedures for GOOSE communication

From a high level perspective, GOOSE fulfills the same requirement as a Report, as it provides an event based distribution of information. As the GOOSE model is designed for high performance, it offers much less flexibility than report mode but can transmit information to other devices in a few milliseconds. To achieve the performance requirements, it is mandatory that the GOOSE message fits inside a single Ethernet frame.

GOOSE behaviour is managed by a GOOSE control block (GCB) and some communication parameters. As for Reporting, a data set is linked to the GCB to list the published and subscribed data.

The GOOSE message includes standard Ethernet fields, VLAN flags (used to virtually isolate part of the communication network), specific GOOSE related fields for identification and timestamp and the values of each member of the data set.

Table D3.7 provides more details on typical GOOSE message with the following colour marking:

a. Green: Identification field to filter on the communication level

b. Purple: Identification field to filter on data model level and other general message information

c. Blue: Data values of DO and DA references

d. Orange: Security or redundancy field

3. Communication services

Field name	Typical value
Multicast MAC address	01:0c:cd:01:00:02
Sender MAC address	00:80:f4:78:88:76
VLAN id and priority	0,4
Ethertype	IEC 61850/GOOSE (0x88b8)
PDU Length	420
APPID	2
Reserved1; Reserved2	Reserve for security
Control block reference	P544System/LLN0GOgcb02
Time allowed to live	2010
Data set reference	P544System/LLN0$DS07
GOOSEID	P544System/LLN0GOgcb02
Event Timestamp	2014-12-18 23:04.8,972000
stNum	10
SqNum	240
Simulation bit	0
Config revision	10
Needs commissioning	FALSE
Number data set entries	15
First data	Depend of data set definition
…	
Last data	Depend of data set definition
Optional security fields	
Optional PRP fields	

Table D3.7:
Structure of a GOOSE frame

Loss of multicast messages can happen on an Ethernet network. Subscribers are able to detect the loss of a message or the whole link because a special repetition mechanism is used as illustrated in Figure D3.24. The message is sent in a slow cycle (“MaxTime”), with each repetition a counter value (“sqNum”) gets incremented. The “TimeAllowedToLive” sets the validity time of the last message. If the subscriber receives an invalid “sqNum” or doesn’t receive a message before the “TimeAllowedToLive” has expired, the GOOSE monitoring indicates a loss of one of the subscribed message.

When a change occurs in a member of the data set, a new GOOSE message is sent by the Publisher as soon as possible. In this message, “sqNum” is set to zero and “stNum” is incremented. Based on this indication, the subscriber knows that an event has occurred. This message is then repeated again much quicker and several times with increasing cycle time. After several retransmissions, the message is sent again in the “MaxTime” cycle.

There are several other identification elements in addition to the multicast MAC address, to group GOOSE messages. Examples are the VLAN address which can be filtered by the network switches to reduce the traffic or the “AppID” to separate GOOSEs per application.

The GOOSE and Report models are very different but complementary ways to manage events. Depending on the performance or flexibility requirements, either one or other can be chosen.

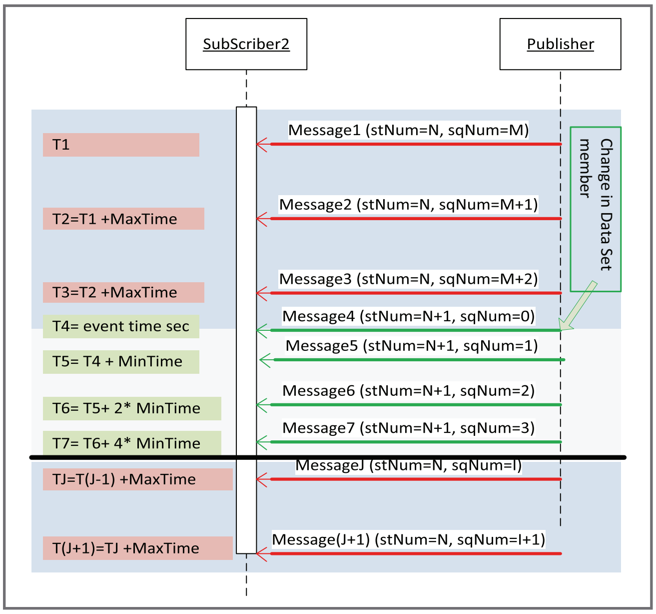

Figure D3.24:
GOOSE publishing mechanism

3.4 Sampled values

Sampled Values (SV) are defined in part 9-2. The goal of SVs is to send sampled Current and Voltage data in a very precise and regular way from an intelligent transformer IED with Ethernet interface called a “Merging Unit” (MU) to other units.

The communication services for SV and GOOSE are very similar. Both use the Publish/Subscribe model and send multicast messages from one publisher MU to one or multiple subscribing IEDs which can use them for further processing. Figure D3.25 illustrates the principle. SV generate a continuous data stream on the Ethernet and consume a significant bandwidth of the network traffic. Especially if multiple MUs are running in the system, it is recommended to use a separate bus system. As the SV are near to the process this separated bus system is called in the standard “Process Bus” as shown in Figure D3.25.

The IEDs themselves no longer need their own CT/VT interface hardware as they receive the sampled data over an Ethernet interface. With respect to the synchronicity and precision of the received sampled data the IED can use them for its protection, control, measurement or power quality purpose. This can reduce the number of transformers and power leading hard-wiring, when the data sent by SV can satisfy the specification of all connected IEDs.

D3

3. Communication services

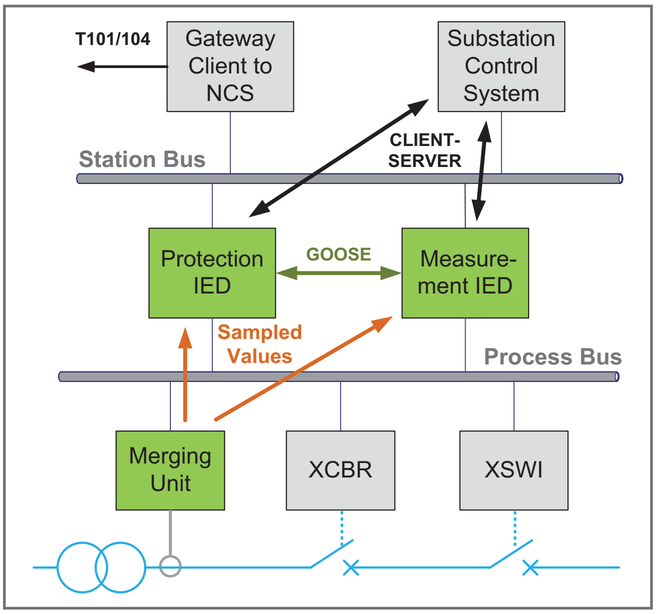

Figure D3.25:
Sampled values via process bus

Typical sampling rates for SV in a 50Hz network:

a. Protection 4 kHz - 80 samples/period

b. Measurement 12.8 kHz - 256 samples/period

A key requirement of the MU is to ensure the synchronisation of the sampling using time synchronisation over IEEE1588. Especially on sampled data for protection devices, a slight slippage in the sampling time leads to a high error on the phase angle between the voltages and currents of the 3 phases. This may have a negative impact to the measurements for the evaluation of the impedance phasors of the distance protection or can generate a delta of the current phasors between the ends of the differential protection.

3.5 Time synchronisation

In IEC 61850 the information data has to be time-stamped when a change occurs. Each device embeds a clock to take the time stamp precisely. To generate a timestamp synchronously to other IEDs, a central time synchronisation of this clock should happen.

IEC 61850 refers to generally available time synchronisation protocols such as the following:

a. 1 PPS

b. IRIG-B

c. SNTP

d. PTP (IEEE1588)

Figure D3.26 shows a classical time synchronisation architecture.

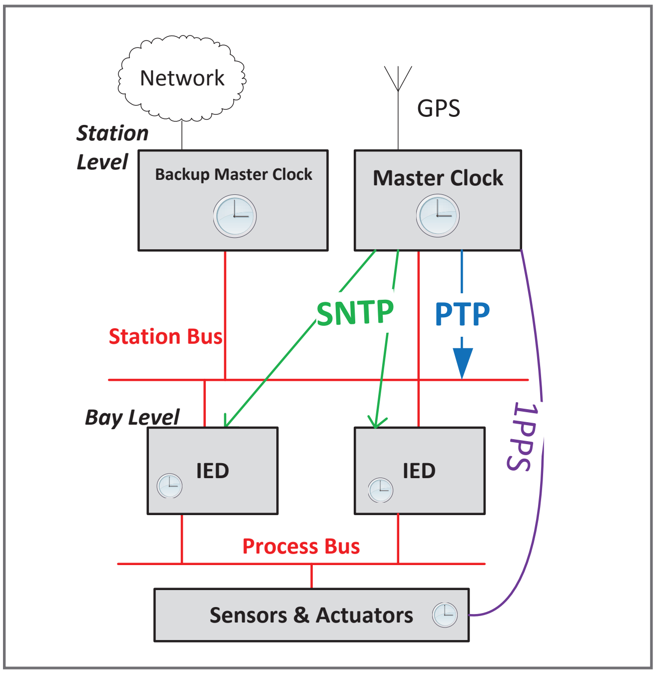

Figure D3.26:
Time synchronisation in IEC 61850

At the top level, a GPS receiver acts as a time server and indicates the absolute time. As time synchronisation is critical, a backup time server should be available, in best case using a different type of media to the first one. It can be based on a network or on a long wave radio (DCF77, MSF-60 etc.). The time server generates a 1 PPS or IRIG-B signal over a dedicated wiring or sends time information on the Ethernet Station Bus using a SNTP or PTP protocol.

1 PPS is referenced by IEC 61850-LE and is mainly used at the merging unit level. Data can be time-stamped with an accuracy of four microseconds. Like 1 PPS, IRIG-B is also based on a pulse, but it also transmits the time data by a real message.

IEC 61850-8.1 specifies SNTP as the synchronisation protocol. SNTP uses a classical Client-Server mechanism. The central time server takes as well the server role for SNTP. All communication devices (IEDs, HMI, Gateway) are working as clients. Each client opens a separate client channel and requests the new time information in a periodic cycle. Devices using SNTP can offer a clock accuracy of about one millisecond.

A new part of IEC 61850 is in progress to define the PTP profile for the substation usage (Part 9-3 - Precision Time Protocol Profile for Power Utility Automation). Contrary to SNTP, PTP acc. IEEE 1588/IEC 61588 relies on the master-slave scheme. The time server broadcasts a sync message periodically containing the reference time. PTP allows much better performance than SNTP with an accuracy in the microsecond area.

On applications with normal up to low time requirements the IEC 61850 standard provides the "client-server communication" i.e. the Reporting. The services behind get transported via the MMS stack on a higher application layer. Application examples, where client-server communication is the preferred method for transmission, are following in the next sections 4.1.

On applications with higher time constraints the normal client-server communication over MMS is not fast enough to be usable. For this a dedicated service was foreseen in IEC 61850 which is the GOOSE communication. All information exchanged over GOOSE is transmitted on the TCP Ethernet communication layer. Application examples where GOOSE communication is the main preferred method for transmission follow in section 4.2.

All data objects shown in the several tables of application sections contain only the part of LN/DO/DA information used in the application, the tables cannot be seen as a complete picture of all DO/DA of the related LN classes. The tables include a T/R column which show the direction to (R = Receive) and from (T = Transmit) the IED to the client or other IEDs. The IED name can be found in the related figure of the substation configuration. Names used for "LDInst" in the tables are examples only.

4.1 Applications with client-server communication

4.1.1 Substation control

Controlling of switchgear equipment in an electrical substation is a safety-related operating area. In modern substation control networks there are mostly multiple operator interfaces as communication clients which have the capability and in most cases the authority to control switching devices. To ensure that only one client is able to initiate a control activation at the same time, the IEC 61850 standard provides a well defined "Select-Before-Operate" (SBO) procedure as a common service. SBO allows an exclusive reservation of substation equipment by a pre-selection named in IEC 61850 as "SelectWithValue", before sending the real open or close command as "Operate" to actuate the control action. A second switching command coming from another client will be normally rejected as long as the object is selected, if there is no other principle used to allow multiple switching commands in parallel. The decision on how to handle switching commands in a limited network section or in the entire substation is managed by the "Substation Interlocking" as described in section 1.2.2.

The SBO principle can be explained with help of Figure D3.27. The substation shown has one infeed bay T1 and several feeder bays F1 to Fn. There are two substation control clients S1 & S2 as Operator Interface (OI) from where control commands can be initiated. If OI S1 requests a Select at bay F2 in step "1", feeder bay unit F2 responds to this client with a "switch selected" message in step "2". As soon as the switch of F2 is selected to execute a control command, any further select or operate request will be rejected as shown in step "3".

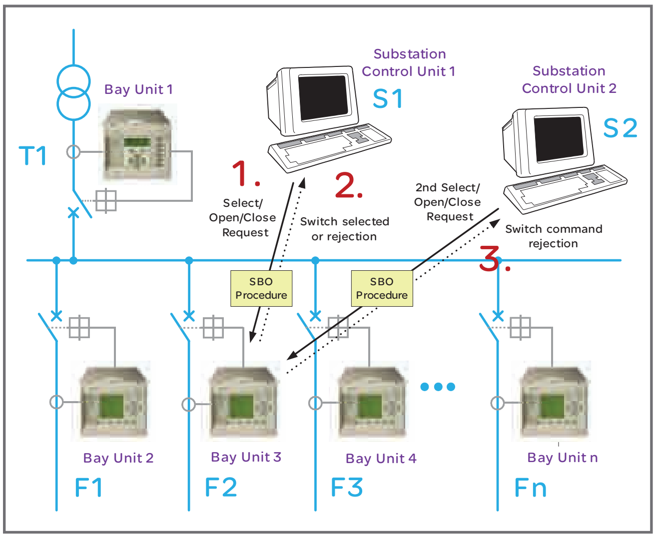

Figure D3.27:
Select-Before-Operate principle in IEC 61850

In IEC 61850 there are several logical nodes defined to model the different functional elements to manage switchgear control. There are two main different kinds of switching devices in a substation:

a. Circuit Breaker with fast switching speed and the capabilities to interrupt load currents and fault currents

b. Disconnector with slow switching speed and low switching capabilities to connect substation parts or to create an earth connection for safety reason during maintenance.

The logical node which is directly connected to the primary process part is called "XCBR" for the circuit breaker and "XSWI" for the disconnector. According to the standard a switchgear position can have four different states for which it is modelled with common data class "Double Pole Control" (DPC) for the control and for the feedback of the state as shown in Table D3.9. Double pole stands here for the 2 wire control of the process, the IED has normally a binary output for the close (switch on) command and a 2nd one for the open (switch off) command. For the feedback of the switch position there are two binary inputs providing the signals from the switch end contact for open and for close ("off" or "on"). If a switch moves from open to close or close to open, there is an "intermediate-state" detectable when both inputs are de-energised as the switch is moving from one end position to the other. When both switch signals are high it is seen as a "bad-state", as it must be an error in the wiring or the position feedback contacts of the switch. In addition, this state is used to indicate that the switch is found in an abnormal status.

In future the Logical Node to represent a circuit breaker or a disconnector can be hosted in an intelligent switch. A further logical node called switch controller "CSWI", is located in the communication server itself, controlling the primary equipment interface nodes XCBR and XSWI. The position signals are

D3

4. Typical applications

using the same model. Where the XCBR and the XSWI do provide the actual position signals following the primary equipment, the CSWI may perform a suppression of the intermediate-state, if required. The detailed data information transmitted between client and IED server is shown in Table D3.8 and D3.9. Bay F2 receives a control from the client via CSWI.Pos.ctlVal (LN.DO.DA). The status response is sent using CSWI.Pos.stVal.

T/R	IED	LDInst	LN	DO	DA
->R	F2	Control	CSWI	Pos	ctlVal
T->	F2	Control	CSWI	Pos	stVal, q

Table D3.8:
Transmitted data for substation control

LN	DO	CDC	DA	Values
CSWI	Pos	DPC	ctlVal stVal	0 = intermediate- state 1 = off 2 = on 3 = bad-state
CSWI	Pos	DPC	stSeld	0 = false 1 = true
XCBR XSWI	Pos	DPC	stVal	0 = intermediate state 1 = off 2 = on 3 = bad-state
CILO	EnaOpn	SPS	stVal	0 = false 1 = true
CILO	EnaCls	SPS	stVal	0 = false 1 = true

Table D3.9:
Modelled objects for substation control

For the safe and reliable switching in a bay or entire substation there is a need to realise an interlocking. Most of the switches can be opened or closed only with respect to the positions of other switches. A dedicated logic is built as a control element which is called in IEC 61850 "interlocking" (CILO). See Figure D3.28 for the illustration of all control nodes according to the standard. We distinguish between bay interlocking, which is always part of the bay unit in the communication server, and the system interlocking, which is normally outside the bay equipment, controlling the entire substation or a selected part of it. The CILO manages the monitoring and the release of all controls of switches in the bay, whereas the system interlocking monitors and releases the control of switches. How the substation interlocking works in an IEC 61850 environment is described in section 4.2.2. For the control of switchgear equipment in substations it is strongly recommended to use the service "SBO with enhanced security" only. Refer to section 3.2.4 for detailed description of this service.

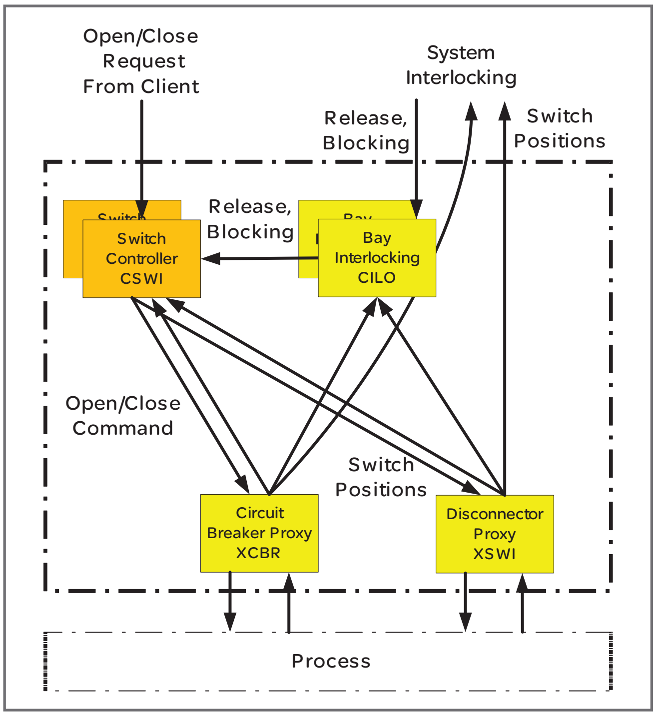

Figure D3.28:
Logical nodes for control in IEC 61850

4.1.2 Local/remote control

Switching devices of a substation as described in the previous section can be controlled from different locations. Each location is assigned a hierarchical level, following the principle 'the closer to the switchgear, the lower the hierarchy'. Typically, "local" is understood if the control happens from the "local" position inside the substation and in front of the control bay unit, and "remote" as issued from a substation control system or a network control centre in another room, floor, building or region. To co-ordinate between control actuations from different sources at the same time, the control device performs a local/remote validation of the control commands against its status before an SBO procedure is accepted. On the bay level, differentiation can be made between controls issued via the Human Machine Interface (HMI) on the front panel of the bay unit and control equipment connected via binary inputs to the bay unit and controls issued directly via push buttons on the switchgear equipment as emergency control without consideration of any interlocking.

Sometimes the local/remote switching is locked by a key switch on the bay unit HMI or by a separate one wired to a binary input of the bay unit. So it is ensured that local control is only activated when the operator with related switch authority uses this key.

4. Typical applications

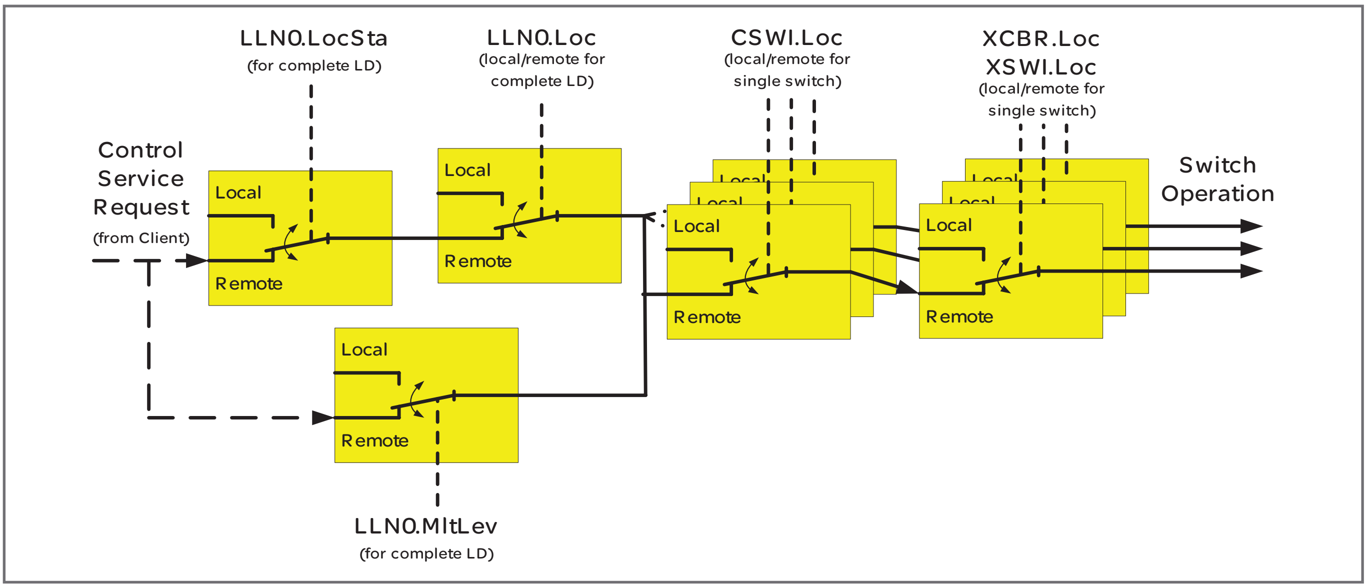

Figure D3.29:
Local/Remote control behaviour

The standard defines a dedicated data object "Loc" on different hierarchical node levels, which each shows the current state and behaviour of the individual switching devices or of the whole logical device or of the bay unit (see Figure D3.29). As the IED cannot know whether a control command received via IEC 61850 is issued from the operator control system location or from the network control centre, all controls which are not issued locally (i.e. from IED level) are dealt with as 'remote'. There is an additional information 'originator.orCat' provided with each control command which helps the IED to decide whether the control hierarchy of the control command received matches the control authority the IED is set to. So, if Loc = false, control commands other than local are rejected. The data object "LocKey" provided on the IED level and with logical nodes hosting controllable objects can be used to set Loc to either 'local' or 'remote'. On the switchgear level, LocKey is typically representing the status of a physical local/remote switch. Another data object object "LocSta" represents the control authority set to substation control system (LocSta = true) or remote via Network Control Centre (LocSta = false). The object "MltLev" defines whether a bay unit will accept a control command from different sources . With MltLev = false the IED only accepts control commands of the given level. With MltLev = true control commands of hierarchical levels closer to the switchgear are also accepted. Table D3.10 and D3.11a summarises all relevant data objects of the local/remote switching.

For safety reasons, a local/remote switchover is always activated via operation at the bay device or at the switchgear via a binary contact and never via communication (therefore SPS, not SPC). For this reason there is no control of any 'Loc' element from an OI client, the various states are only reported from the bay unit to the client when changing.

T/R	IED	LDInst	LN	DO	DA
T->	F2	Control	CSWI	Loc	stVal, q

Table D3.10:
Transmitted data for local/remote control

LN	DO	CDC	DA	Values
LLN0	LocKey	SPS	stVal	0 = false (remote active) 1 = true (local active)
LLN0	Loc	SPS	stVal	0 = false (remote control accepted) 1 = true (local control accepted)
LLN0	LocSta	SPC	stVal	0 = false (remote control from network level accepted) 1 = true (control from station level accepted)
LLN0	MltLev	SPG	stVal	0 = false (single control level acceptable) 1 = true (multiple control levels acceptable)
CSWI	LocKey	SPS	stVal	0 = false (remote active) 1 = true (local active)
CSWI	Loc	SPS	stVal	0 = false (remote control accepted) 1 = true (local control accepted)
CSWI	Pos	DPC	originator	See table D3.11b

Table D3.11a:
Modelled objects for local/remote control

4. Typical applications

Each client initiating a control command has to provide his own "originator" information in the control request message. This information comprises the hierarchical level (helping the IED to decide on acceptance), categories of reasons and the name of the issuing client. The bay unit has to copy the originator information into any responses following the control command. As on bay unit level a control command can be created via local HMI, binary input or related communication interface, 'Originator' has to be configured for all of these command sources. The possible order categories are shown in Table D3.11b.

LN	DO	CDC	DA	Values
CSWI	Pos	originator	orCat	0 = not supported 1 = bay-control 2 = station-control 3 = remote-control 4 = automatic-bay 5 = automatic-station 6 = automatic-remote 7 = maintenance 8 = process
CSWI	Pos	originator	orIdent	String with control source identification

Table D3.11b:
Originator sub data attributes

4.1.3 Control with synchrocheck

If network areas with different power infeeds have to be connected, an additional function for switchgear control called "synchronism check", or abbreviated to "synchrocheck", is used. This function tests before connection if both network sections are synchronous to each other or the deviation is within defined limits. The synchrocheck function measures if the following conditions are met:

a. Difference of voltages $|\Delta U| < \Delta U\ max$

b. Difference of frequencies $\Delta f < \Delta f\ max$

c. Difference of angles $\Delta\alpha < \Delta\alpha\ max$

A closing of the related switch can be only allowed if the limits are not exceeded. The synchrocheck function is sometimes provided by a separate device but very often as an additional function inside a control device.

The synchrocheck can be requested as a first check prior to the decision to do a network connection or directly before the related circuit breaker would be closed. For the second case the request can be combined with the control command of the switch.

The synchrocheck can be managed either centrally or distributed. With the central concept, a dedicated IED performs the synchrocheck for the entire substation. Here a scheme needs to ensure that this IED is provided the necessary measurands. With the distributed concept, the synchrocheck is carried out by each of the bay units where the networks can be connected.

The substation control system uses the client-server communication from IEC 61850 as a service for request and reporting as there are low timing requirements (reaction < 2 seconds). For control commands the typical client supports the differentiation between control modes "with synchrocheck" and "without synchrocheck". If the control with synchrocheck is selected, the IED performs the check of the network synchronism after having checked the bay and system-wide interlocking. Once the conditions for synchronism have been checked successfully, the close command is released and carried out. If the check fails, the command is blocked and a corresponding message is generated.

The bay unit can report the successful or unsuccessful switch actuation and the measured values for voltage, frequency and phase angle difference, in parallel to the new switch position using the logical Node RSYN for the synchronism check. The detailed data is shown in Tables D3.12 and D3.13. Figure D3.30 illustrates the interactions between the different logical nodes in the bay unit. For the measurement acquisition the nodes TVTR for the voltage transformers are involved to retrieve the required measurement values.

T/R	IED	LDInst	LN	DO	DA
->R	T1	Control	CSWI	Pos	ctlVal check
T->	T1	Control	CSWI	Pos	stVal, q
T->	T1	Control	RSYN	Rel, VInd, AngInd, HzInd	stVal, q
T->	T1	Control	RSYN	DifVClc, DifHzClc, DifAngClc	mag, q

Table D3.12:
Transmitted data for control with synchrocheck

LN	DO	CDC	DA	Values
RSYN	Rel	SPS	stVal	0 = false (blocked) 1 = true (released)
RSYN	VInd	SPS	stVal	0 = false (met) 1 = true (violated)
RSYN	HzInd	SPS	stVal	0 = false (met) 1 = true (violated)
RSYN	AngInd	SPS	stVal	0 = false (met) 1 = true (violated)
CSWI	LocKey	SPS	stVal	0 = false (remote) 1 = true (local)
RSYN	DifVClc	MV	mag	Voltage Difference
RSYN	DifHzClc	MV	mag	Frequency Difference
RSYN	DifAngClc	MV	mag	Angle Difference

Table D3.13:
Used IEC 61850 objects for synchrocheck

4. Typical applications

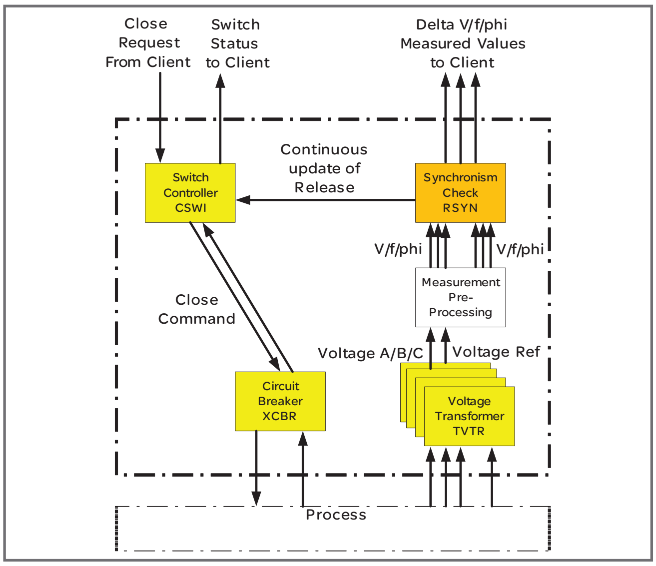

Figure D3.30:
Logical nodes used for synchrocheck

4.1.4 Selection of the parameter subset

In some application cases, the protection settings have to be adjusted when network conditions change during operation. Such a change could happen when additional loads or infeeds are connected, or the settings are changed under different environmental conditions. To satisfy such requirements, modern protection devices offer a certain number of parameter subsets, most of the common protection devices offer 4, 6 or 8 parameter subsets (PS). Typically the first PS considers the normal protection settings, whereas the other ones provide different setting values for the interim network conditions. Parameter subsets can be swapped during operation without interrupting the protection function. The selection of the related PS happens via HMI, binary input or the communication link from the substation control system. Proprietary protocols like IEC 60870-5-103 already provide dedicated definitions to support PS selection with adequate status and control command telegrams. IEC 61850 supports this use case by the services of the Setting Group Control Block (SGCB). The standard defines a control instance SGCB located in the common node LLN0 of a LD, in this example the LD Protection (see Table D3.14, LD name is an example only as it is not defined in the standard). Table D3.15. shows the application relevant attributes of SGCB.

T/R	IED	LDInst	LN	CB	Attribute
->R	F2	Protection	LLN0	SGCB	NumOfSG ActSG LActTm

Table D3.14:
Transmitted data for setting group selection

LN	CB	CDC	Attribute	Values
LLN0	SGCB	INS	NumOfSG	Integer value of max. available SG
LLN0	SGCB	INC	ActSG	Identification number of the active SG
LLN0	SGCB		LActTm	Time of the last SG change

Table D3.15:
Modelled objects for setting group selection

In conformance with the IEC 61850 standard, a client shall use the service SelectActiveSG to activate any of the available PSs. A service request is acknowledged with a positive response (write operation succeeded) if the service was used with valid SGCBReference (System/LLN0.SGCB) and a valid SettingGroupNumber (1 to NumOfSG). The attributes of SGCB are not available for reporting. The identification number of the active PS can be obtained by reading the value of the attribute ActSG or by using a private DO in a data set.

4.1.5 Transmission of disturbance recordings

In cases when a fault occurs in the electrical network, the related protection device detects this fault by its algorithm and clears the fault by issuing a CB trip. A modern protection device generates in parallel to the fault clearance a disturbance recording of the analogue values retrieved during the fault, together with the most important binary signals, to allow a protection engineer to investigate the root cause of the fault afterwards. This disturbance recording can be retrieved from the protection IED in different ways. To simplify the access to disturbance recordings in the devices and to manage an autonomous archiving of all disturbances centrally in a substation, a dedicated disturbance analysis & archiving system can be set up in a communication system. Figure D3.31 illustrates such a disturbance recording system in a typical substation network with file transfer for F2.

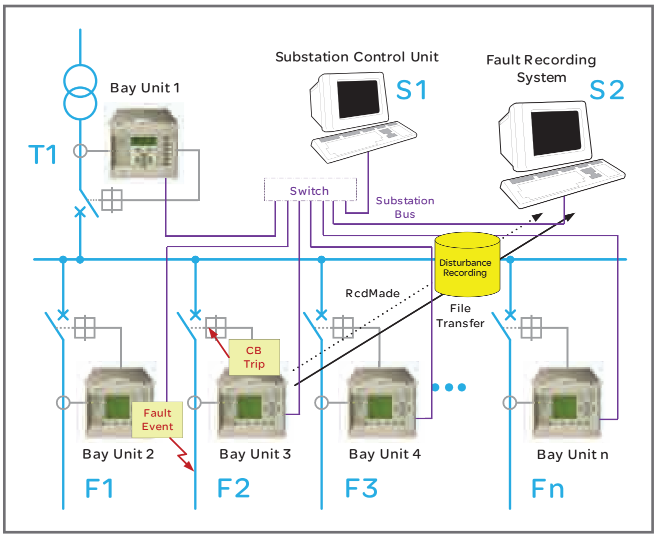

Figure D3.31:
Principle of fault recording retrieval

D3

4. Typical applications

By reporting “RcdMade” the protection relay indicates that a disturbance recording was made and that a file can be retrieved. Any subscriber to this information may now use file transfer routines to receive a copy of this file. Proprietary protocols like IEC 60870-5-103 already provide dedicated telegrams to support disturbance recording signalling and download. IEC 61850 supports this use case by file transfer services. The disturbance recording function of an IED is represented by the following LN classes:

a. RDRE – Disturbance recorder function

b. RADR – Disturbance recorder channel analogue

c. RBDR – Disturbance recorder channel binary

RDRE is the function to manage the disturbance recording. The information (header, data values) is stored in a COMTRADE file. Some devices allow to configure whether the COMTRADE file is exposed as ASCII or as binary data. If IEC 61850 is used to configure the disturbance recording function, RADR is the node to configure the analogue channels, RBDR is the node to configure the binary channels. The most important objects required to handle recordings are shown in Tables D3.16 and D3.17. Figure D3.32 illustrates the sequence of messages used to trigger, download and archive the files.

T/R	IED	LDInst	LN	DO	DA
T->	F2	Records	RDRE	RcdStr RcdMade FltNum GriFltNum	stVal, q stVal, q stVal, q stVal, q

Table D3.16:
Transmitted data for fault recordings

LN	DO	CDC	DA	Values
RDRE	RcdStr	SPS	stVal	0 = false (no recording) 1 = true (record started)
RDRE	RcdMade	SPS	stVal	0 = false (no new record) 1 = true (new record made
RDRE	FltNum	INS	stVal	Integer value of fault number
RDRE	GriFltNum	INS	stVal	Integer value of grid fault number

Table D3.17:
Modelled objects for fault recordings

4.1.6 Characteristics switching

For a few applications, the protection functions have to be dynamically adapted to the situation of the electrical network or modus of the electrical objects protected. IEC 61850 provides a couple of different solutions to satisfy this requirement.

One practical example is the distance protection function for an electrical catenary network for railways. Very often the catenary is not organised into one single long feeder line per train direction, but it is a combination of multiple catenary segments for both directions and alternative tracks in parallel, especially near to railway stations. For modern high speed trains there is as well in parallel to the feeder catenary a return conductor to support an auto-transformer solution (see Chapter [C10: A.C. Railway Protection]).

The distance protection device protecting the catenary network is located in each substation over the long railway track between the different railway stations. The protection detects the faults by measuring the impedances of the lines. Dependent on the actual network connections, the impedance changes and the protection has to be adapted to protect the line in the most reliable way.

Figure D3.33 shows an example of the electrical network of a typical railway track under normal conditions. All segments of the catenary are in operation, the distance protection works with an impedance threshold Z1 in both substations.

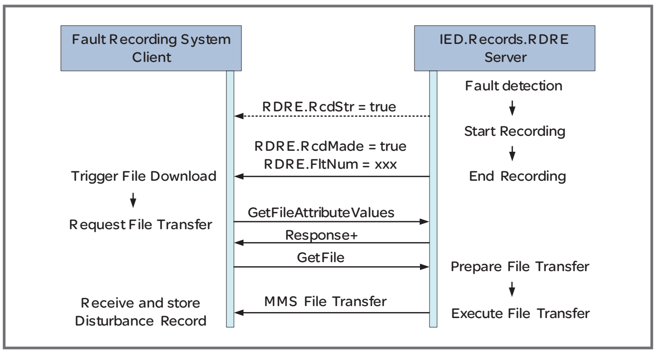

Figure D3.32:
File transfer to download fault records

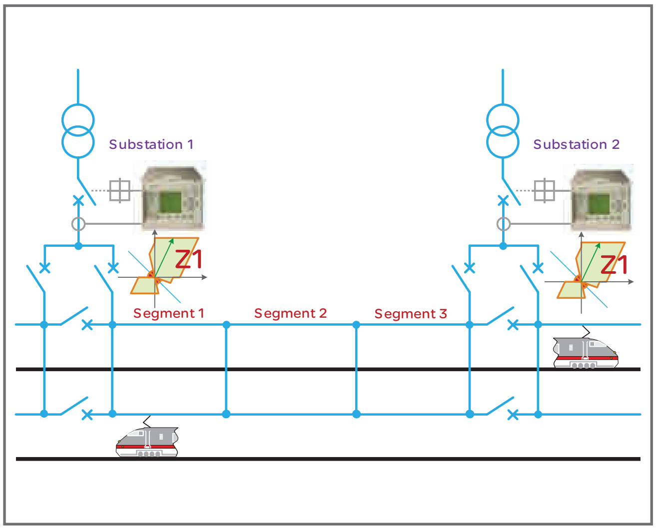

Figure D3.33:
Rail catenary impedance - normal mode

If one of the catenary segments is now switched off for segment 2, as shown in Figure D3.34, the current flow is different and the impedance of the remaining network system changes. To adapt the protection device to the new arrangement of the catenary the impedance threshold needs to be adjusted to Z1´.

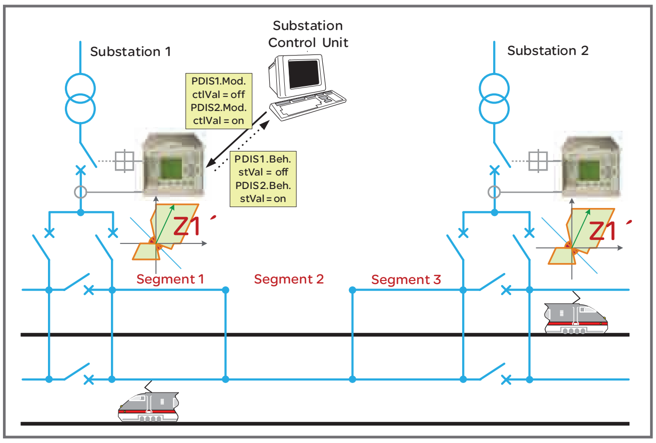

Figure D3.34:
Rail catenary impedance – one segment lost

The change-over is initiated by an operator using the device HMI or via the substation control system, which holds an image of the network configuration. With a switching of a circuit breaker there could be as well an automated change-over made to keep the protection up to date.

The IEC 61850 standard provides two main solutions to manage this kind of application:

a. Selection of the Parameter Subset

b. Enabling/Disabling of Logical Nodes

For the selection of the parameter subset refer to section 4.1.4. Most of the common protection devices offer 4, 6 or 8 parameter subsets. Very often they are already used for other reasons, in the case of the distance for railways for example to manage alternative infeed operation modes and for the adjustment of the impedance levels during train starts or their acceleration. Using the variation of the setting groups for another adaptation, the Enable/ Disable of Logical Nodes is therefore the preferred solution by the railway utility companies.

The timing requirements are not high at all, if the change-over happens in about 1 second, it is sufficient. The selected communication method over IEC 61850 is therefore chosen with client-server communication. The recommended mode is the "Direct control with enhanced security". For the status return it is recommended to use Reporting with spontaneous transmission. For the change of the impedance the substation control system first sends a disable (blocking) of the related distance logical node PDIS1 with impedance threshold value Z1 and directly afterwards an enable of the logical node PDIS2 with impedance threshold value Z1´ to take over. The IED reacts with related response reports to confirm the change of the LN states. The required data element is the data object "Mod" with data attribute "ctlVal" for the control of the LN and the data object "Beh" with the data attribute "stVal" for the status returned (see Table D3.18, D3.19). The disabled LN will be changed to state "off" and the enabled one from "off" to "on". "Beh" represents the real state of the LN. It's computed based on its own Mod value and the Mod of the LLN0 of its LD. If the LLN0 Mod is set to off, all LN of the LD have their Beh also set to off and so, the LNs are disabled by a higher hierarchical level.

T/R	IED	LDInst	LN	DO	DA
->R	S1	Protection	PDIS1 PDIS2	Mod	ctlVal
T->	S1	Protection	PDIS1 PDIS2	Beh	stVal, q

Table D3.18:
Transmitted data for characteristic switching

LN	DO	CDC	DA	Values
PDIS1 PDIS2	Mod	ENC	ctlVal	1 = on 2 = on-blocked 3 = test 4 = test/blocked 5 = off
PDIS1 PDIS2	Beh	ENS	stVal	1 = on 2 = on-blocked 3 = test 4 = test/blocked 5 = off

Table D3.19:
Detailed data for characteristic switching

The IED obviously has to secure that at no time can it happen that both PDIS nodes are in the "on" state at the same time. The best implementation would be to automatically change the one to state "off" when the other is changed to state "on" and vice-versa.

4.2 Applications with GOOSE communication

4.2.1 Reverse interlocking

Reverse interlocking can be used in radial networks with a single infeed, to set up a simple busbar protection scheme. Figure D3.35 shows a simple busbar scheme with a transformer bay T1 as infeed and Feeder bays F1 to Fn for the several outgoing bays in a substation. In our example the highset overcurrent stage I>> of the definite time overcurrent device of T1 is set to a short tripping time of 0.1 seconds. Additionally, this stage is configured to be blocked via a binary input. The first overcurrent

D3

4. Typical applications

stage I> of the outgoing feeder bays F1 to Fn are set to a tripping time of 0.3 seconds. The pickup signal of the I> stage or the general pickup signal are configured to a binary output. The binary outputs of all the outgoing protection devices in F1 to Fn are connected as a ring wire to the same blocking input of the infeed protection (see red line in Figure D3.35).

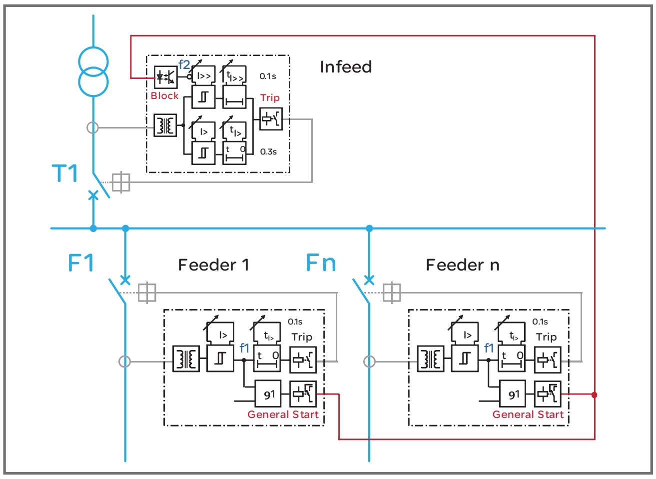

Figure D3.35:
Signal path reverse interlocking by wire

When a fault occurs at one of the outgoing feeders F1 to Fn, the pickup of the protection instantaneously generates a blocking signal to the protection device of the incoming feeder T1 via the configured output and its I>> stage is blocked to prevent a trip condition (e.g. < 0.1 seconds). The outgoing feeder protection in F1 to Fn generates a trip selectively to its circuit breaker which is connected to the faulty outgoing feeder line to clear the fault. The busbar and all other connected loads can remain operational.

When a fault occurs on the busbar itself, the I>> stage of the infeed protection in T1 picks up but none of the outgoing feeder protection units F1 to Fn generate the blocking signal since the affected protection devices of the outgoing feeders do not pick up. Thus, the infeed protection switches off the infeed after 0.1 seconds.

When all protection devices of the busbar are connected via IEC 61850 communication to the Ethernet network of the substation, the GOOSE services can be used to transmit the blocking signals from the feeder bays to the transformer bay without the need of any additional electrical wires. The information is transmitted in one direction only, i.e. to the virtual inputs of the incoming feeder protection (see Figure D3.36).

The use of Ethernet communication thus replaces the ring wire circuits and the required binary outputs of the outgoing feeder protection units and the binary input at the incoming feeder protection unit for blocking the trip. This is saving cost for I/O hardware, wiring and documentation.

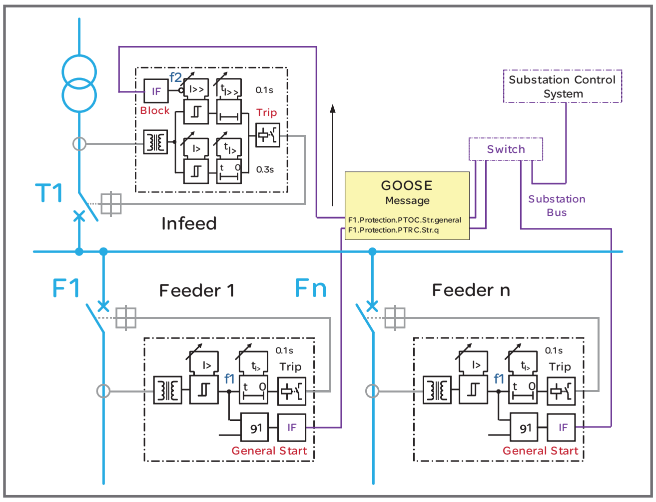

Figure D3.36:
Signal path reverse interlocking by GOOSE

The pickup message of I> as PTOC/Str or the general starting signal as PTRC/Str from the trip Conditioner has to be transmitted by a GOOSE publishing channel from bay F1 to bay T1 (see Figure D3.37). The related IEC 61850 model object is shown in line T-> of Table D3.20. In T1 itself the information out of the subscribed GOOSE messages have to be assigned to the related blocking signal of the I>> stage. The related IEC 61850 model object to indicate that a blocking is affected also is shown in Table D3.20). As IED T1 "collects" all GOOSE information from the different bays F1 to Fn, it has to form a common blocking signal before connecting this to the I>> PTOC function. An internal programming logic is required to combine the virtual inputs by an OR logic. Other possible internal blocking criteria can be integrated as well. The detailed model information is shown in Table D3.21.

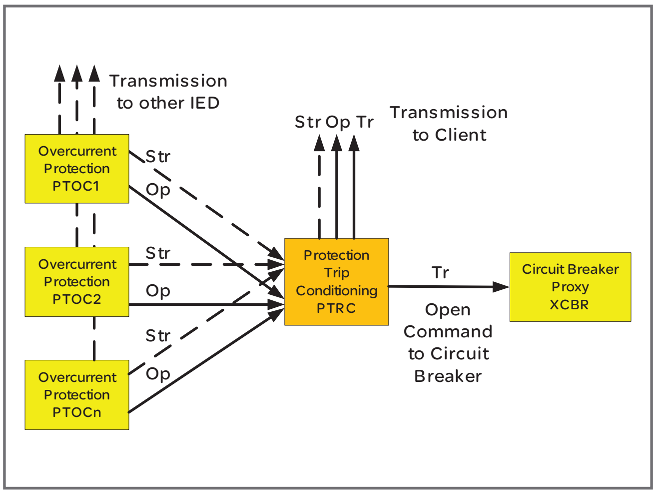

Figure D3.37:
Nodes involved for protection signalling
(Str = Starting, Op = Operate, Tr = Trip)

T/R	IED	LDInst	LN	DO	DA
T->	F1	Protection	PTOC	Str	general, q
T->	F1	Protection	PTRC	Str	general, q
T->	T1	Protection	PTOC	Blk	stVal, q

Table D3.20:
Transmitted data for reverse interlocking

LN	DO	CDC	DA	Values
PTRC	Str	ACD	general	0 = false 1 = true
PTOC	Blk	SPS	stVal	0 = false 1 = true

Table D3.21:
Details on data modelling

For all information submitted via GOOSE, the quality attributes .q have to be transmitted and evaluated on subscriber side to ensure that the blocking is carried out correctly. The blocking may only be activated as long as .q.validity is not marked as "invalid". The transmission must be completed within less than the set command time tI>> of the incoming feeder protection, which is 0.1 seconds in our example. The time requirement applies here for the transmission path from generation of the pickup $f1$ until the actual blocking takes effect $f2$ (see Figure D3.36) according to IEC 61850 part 5, Edition 2, page 62. The transmission must take place without delay, i.e. a spontaneous transmission is an absolute precondition.

Thus data can be transmitted reliably within a few milliseconds. The reverse interlocking is a part of the protection system and as such is on a high safety level. This is why GOOSE services are especially suitable for this application.

4.2.2 System-wide interlocking

The interlocking function in a substation serves to block the operation of switching devices, if this is hazardous for humans, devices or the whole substation equipment during active service. The decision whether a switchgear actuation is blocked or released requires an evaluation of logical equations from the topological environment of the device in the form of a relevant process information of active and inactive parts of the electrical network. A differentiation is made between the bay-related interlocking and system-wide substation interlocking.

Bay-related interlocking considers the switch positions within in a bay and also the conditions of the switchgear primary equipment such as "spring/drive ready" or "pressure/insulation monitoring" and auxiliary equipment like "MCB Trip".

System-wide interlocking considers the positions and conditions of all switching devices and their auxiliary equipment within the entire substation or at least a part of it seen as an isolated system.

For a safe system-wide interlocking the following information has to be collected by the interlocking logic:

a. Position indications of all switching devices in the entire substation

b. Warning and alarm messages of the auxiliary equipment (if bay-related interlocking included)

c. Initiation of the interlocking check

d. Release from the interlocking to the IED controlling the switching devices

There are generally three different implementation concepts possible for a substation interlocking as illustrated in Figures D3.38, D3.39, D3.40:

a. Central interlocking by the substation control unit

b. Central interlocking by a dedicated bay unit

c. Distributed interlocking by the bay units

The request for the switching can originally come from the substation control system, the network control centre or locally on the front panel HMI or the binary inputs on the bay unit wired from a remote terminal unit (RTU). The IED can only execute a switching control command when it receives a release by the interlocking unit, otherwise it has to respond to the initiator with a rejection.

The concepts differ depending on which IEDs status indications are exchanged, in which IEDs the interlocking conditions are checked and from where the release signals are generated. If the substation control system is not involved in the interlocking procedure, it only receives updated status information from each IED about the new position of the switching devices.

In the concepts **a** "Central interlocking by the substation control unit" (Figure D3.38) and **b** "Central interlocking by a dedicated bay unit" (Figure D3.39) the interlocking logic is integrated in one central unit. The central unit holds a process image that comprises all information relevant for the all-embracing interlocking conditions.

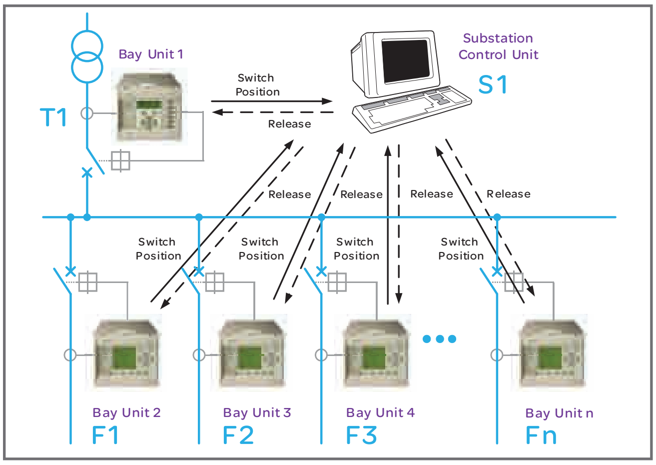

Figure D3.38:
Central interlocking by the substation control unit

4. Typical applications

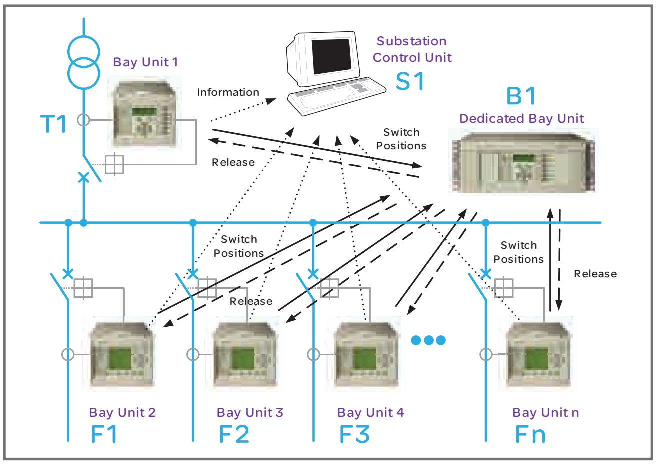

Figure D3.39:
Central interlocking by a dedicated bay unit

All bay units have to transmit the relevant switchgear positions to the central unit either continuously or for each status change. The release information calculated as a result of the central interlocking is sent to the corresponding bay units. This release information is the basis for executing or blocking an open or close control command by the bay units. Additionally it needs to be distinguished whether the interlocking for the bays is integrated in the logic of the central interlocking unit or whether the bay unit manages its own bay-related interlocking. Dependent on this the number of interlocking equations in the central unit may be quite different.

With the concept **c** "Distributed interlocking by the bay units" (Figure D3.40), the all-embracing interlocking logic is distributed among all participating bay units in the substation. The interlocking logic of each bay unit calculates the interlocking conditions autonomously. Moreover, each bay unit provides the status information required by other bay units for calculating the interlocking conditions in a continuous way.

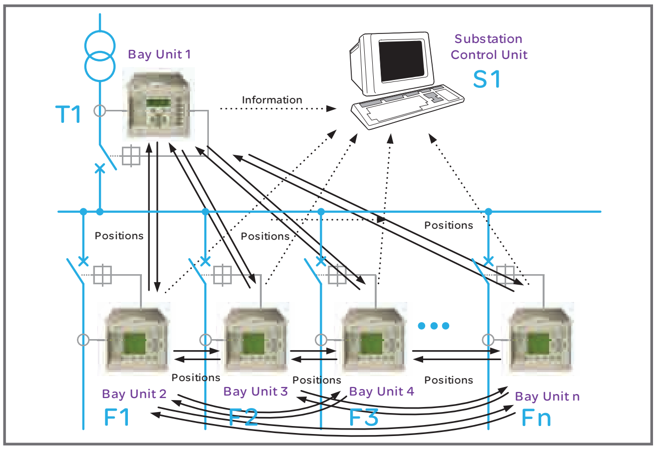

Figure D3.40:
Distributed interlocking by the bay units

With an IEC 61850 network all three concepts can be used. Nevertheless not all concepts can be realised in an interoperable way. For the communication from bay unit to bay unit the GOOSE communication has to be used (so-called "horizontal communication") which provides a fast transmission time and cyclical status update, whereas the communication between the bay units and the substation control system uses event-triggered reporting via the client-server communication ("vertical communication"). With typically one publishing GOOSE message the bay unit sends a multicast message to all other bays at the same time for subscribing the data. With the client-server reporting the bay sends each data change by a separate message per client connected.

In case of the concept **a** the whole communication would happen via client-server communication as a substation control system has typically no GOOSE subscription capabilities. The status reporting for switching devices is defined in IEC 61850 and this works fully interoperable. But for the send message from the system interlocking to release switch executions, dedicated new procedures and objects have to be defined, as the standard is currently not offering any standardised service. As this extension would be not interoperable, it is not recommended to use the concept **a** for system-wide interlocking. Due to this a further description is not added to this document.

For the two other concepts **b** and **c** the main transmission uses GOOSE communication as bay units typically have no client functionalities. A simple exchange of binary information is made by sending the bay status information and control release information in case of concept **b**. The only case using client-server communication is the status update information to the substation control system, which is unidirectional.

There are arguments in favour of concept **b**:

a. For large substations the number of configurable GOOSE virtual inputs could be exceeded, as each bay unit has to subscribe to the appropriate position signals of other bay units

b. Maintenance of the system interlocking is easier, as not all changes affect all the bay units

In the opposite, the concept **c** provides:

a. The most interoperable solution, as no additional signals need to be defined. Concept **c** is therefore the closest solution to the IEC 61850 standard

b. Testing is much simpler as it is bay-oriented

c. Maintenance is higher than in concept **b** as for each new or changed bay unit the interlocking equations in all other bay units need to be updated

As an example Figure D3.41 shows the communication in the network for concept **b**. For the transmission of the switchgear positions and the open/close release information the horizontal communication via GOOSE is used. Additional reports will be transmitted via vertical client-server communication to update the status in the operator workstation and in the network control centre.

4. Typical applications

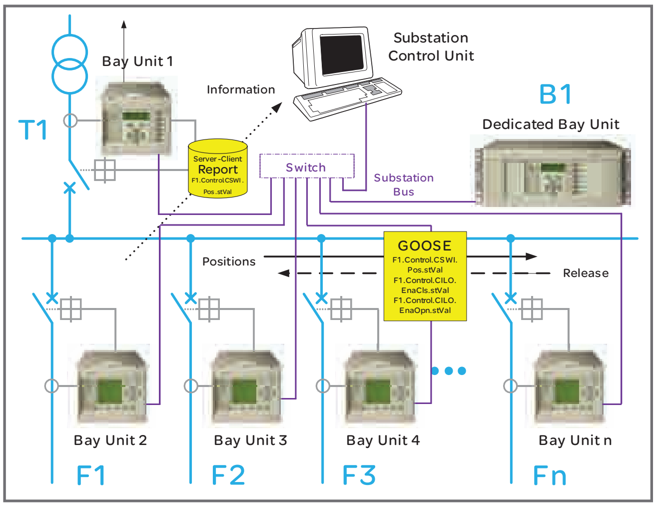

Figure D3.41:
Interlocking communication via IEC 61850

The related objects which are transmitted in concepts **b** and **c** are shown in Tables D3.22 and D3.23. The position indications of the switching devices are modelled in IEC 61850 using the Logical Node (LN) "XCBR" for a circuit breaker and "XSWI" for a disconnector. The data object (DO) "Pos" contains the status information. The position details of a switching device are given by the data attributes (DA) "stVal" for the status value itself and "q" for the quality (e.g. "valid" or "invalid"). As the position

T/R	IED	LDInst	LN	DO	DA
T->	F1	Control	XCBR XSWI	Pos	stVal, q stSeld
T->	F1	Control	CWSI	Pos	stVal, q stSeld
->R	F1	Control	CILO	EnaOpn EnaCls	stVal, q stVal, q

Table D3.22:
Transmitted data for substation interlocking

LN	DO	CDC	DA	Values
XCBR XSWI	Pos	DPC	stVal	0 = intermediate-state 1 = off 2 = on 3 = bad-state
CSWI	Pos	DPC	stSeld	0 = false 1 = true
CILO	EnaOpn	SPS	stVal	0 = false 1 = true
CILO	EnaCls	SPS	stVal	0 = false 1 = true

Table D3.23:
Transmitted data for substation interlocking

status value stVal is a double pole signal, it can take four different values which are "intermediate-state", "off", "on" and "bad-state". For the indication of the switch "selected" state, the switch controller LN CSWI contains the DA "stSeld".

The release signals needed for concept **b** are modelled in the LN CILO (control interlocking logic). The CILO contains DO "EnaOpn" and "EnaCls" to enable (release) or not of the respective open and close controls of the switching device. The internal functional blocks in an IED for control according to IEC 61850 are shown in Figure D3.42.

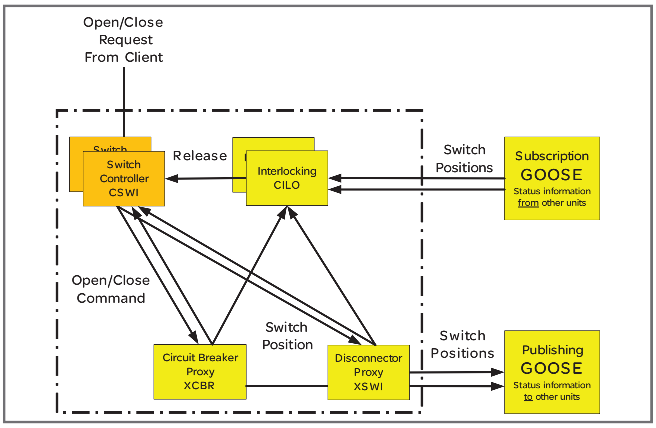

Figure D3.42:
Interaction bay with interlocking unit

For all concepts **a**, **b**, **c** all bay units send their status update via report to the clients connected.

In the case of concept **b** each bay unit continuously sends its switchgear position information and warning GOOSE messages to the interlocking bay unit. The dedicated interlocking bay unit continuously generates the corresponding EnaOpn and EnaCls signals based on the overall substation situation within its interlocking logic and publishes GOOSE messages to return this information to all bay units in charge of their switching devices. If a client requests a select or an operate for a circuit breaker or a disconnector, the corresponding bay unit considers the EnaCls and EnaOpn release status from the interlocking unit in its checks. If the switching control action is permitted, then the command will be executed. If it is not allowed, then the command will not be executed and a rejection message is returned to the client.

In case of concept **c**, each bay unit continuously sends its switchgear position information via a GOOSE message to all other bay units. Each other bay unit has to subscribe to the status GOOSE messages from the other bay units needed for its system-wide interlocking checking. If a client requests a select or an operate for a circuit breaker or a disconnector, the corresponding bay unit when receiving the command initiates an internal interlocking check and evaluates the interlocking status on basis of the received states from the

4. Typical applications

GOOSEs of other bays involved. If the switching control action is permitted, then the command will be executed. If it is not allowed, then the command will not be executed and a rejection message is returned to the client.

Figure D3.43 and D3.44 illustrate the interaction between the different logical parts for both cases.

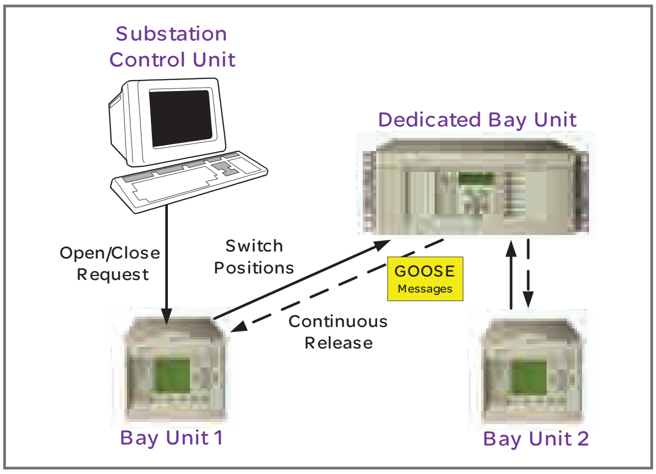

Figure D3.43:
Interaction bay with interlocking unit

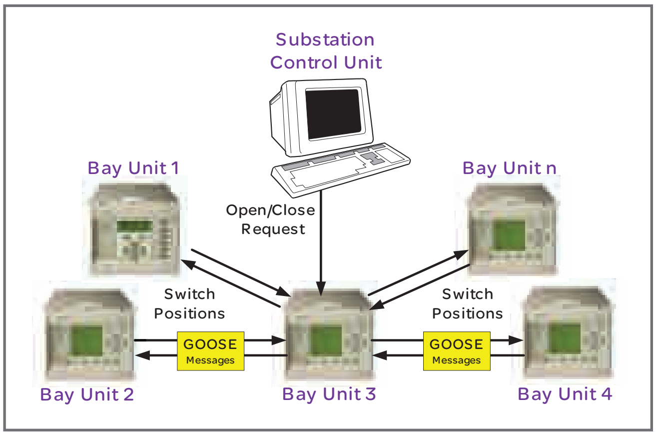

Figure D3.44:
Interaction bay to bay unit

4.2.3 Uniqueness of control

A 1-of-n control logic has to ensure that only one switching control operation can occur at a given time in a pre-defined section of an electrical network. This means that only one switching device (circuit breaker or disconnector) can be opened or closed at the same time. All other switch commands need to be rejected. This function is very important in networks where more than one substation or network control system have the authority to execute operations.

The 1-of-n logic works for a defined substation or network area or possibly a whole substation. The pre-definition of the network sections has to happen at the same time when the concept of the substation interlocking is chosen.

The 1-of-n logic is possible in all three concepts of the system-wide interlocking:

a. Central interlocking by the substation control unit

b. Central interlocking by a dedicated bay unit

c. Distributed interlocking by the bay units

As the concept **a** is currently not feasible in an interoperable way it is not considered in this section.

For the explanation of the 1-of-n logic, the interlocking concept **c** is used. All bay units execute the interlocking by themselves. For that each IED publishes GOOSE messages with the positions of all switching devices. The modelling information transmitted is given in Table D3.24.

LN	DO	CDC	DA	Values
XCBR XSWI	Pos	DPC	stVal	0 = intermediate-state 1 = off 2 = on 3 = bad-state
XCBR XSWI	Pos	DPC	stSeld	0 = false (unselected) 1 = true (selected)

Table D3.24:
Transmitted data for substation interlocking with 1-of-n logic

Each bay unit sends the positions of its primary equipment with the data object “Pos” with an “on”, “off”, “intermediate-state” or “bad-state”. If a switching control operation has been started the position moves from “on” or “off” into the “intermediate-state” until it reaches the opposite state with “off” or “on”. As described in section 4.1.1 “substation control”, the switching control operation is prepared by a “Select” before the real operation.

For the indication that a switch has been selected, an additional status information “stSeld” can be modelled and set from “unselected” to “selected” state. This state will be kept until the final switch position is reached. Adding this object to the GOOSE data set allows other bays to subscribe and to consider it in their bay control logic to be aware of any upcoming and later running switch operations in other bays. The bay control logic of these bays can reject any control request until at least one of the subscribed GOOSE messages from all the other bays signals “Selected” by “stSeld”.

As an example for concept **c** the first step for a close or open command is the operator’s initiation of the operation via the device front panel HMI on bay level or via the Operator Interface (OI) of the substation control system. Figure D3.45 shows in Step “1” a request coming from the OI ‘Select’ as part of an SBO (Select-Before-Operate) command. The control procedure for SBO triggers the interlocking check and responds in Step “2” with a positive confirmation that this switchgear device was now selected. In the next important step “3” in Figure D3.46 the bay unit changes the status of the “stSeld” of the chosen switchgear device to “selected”. If a second control command is initiated during the whole operation by the same or another front panel HMI or by the same or another OI client, in Figure D3.47 shown in Step “4”, the related bay unit can reject the control request directly, in this example by a negative response to the SBO ‘Select’ command to the second OI as illustrated by Step “5”.

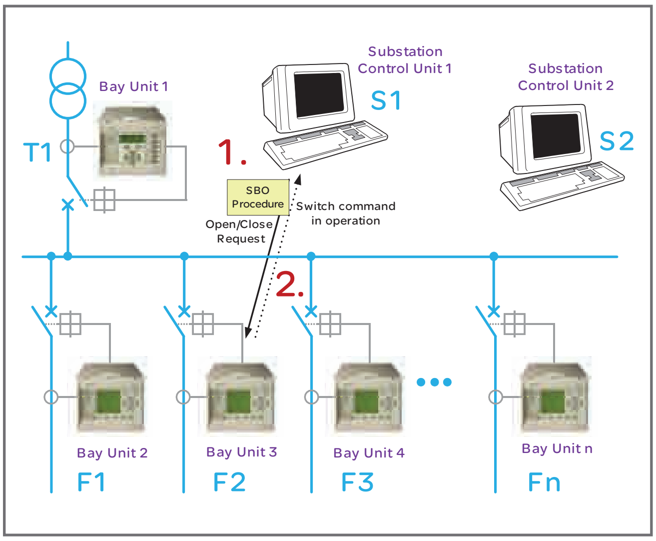

Figure D3.45:
1-of-n logic - step 1 & 2

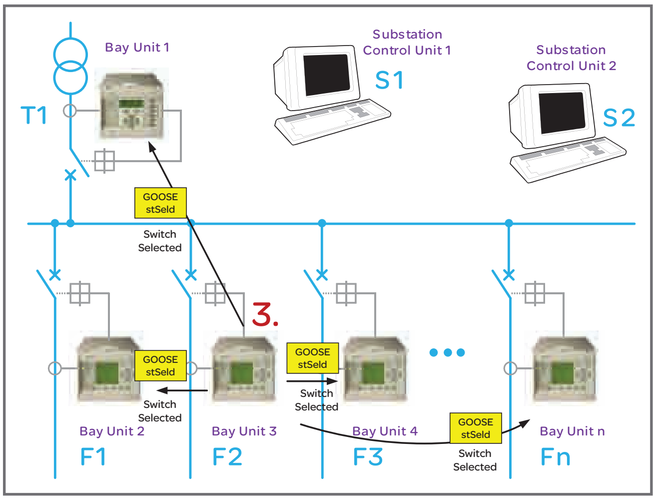

Figure D3.46:
1-of-n logic - step 3

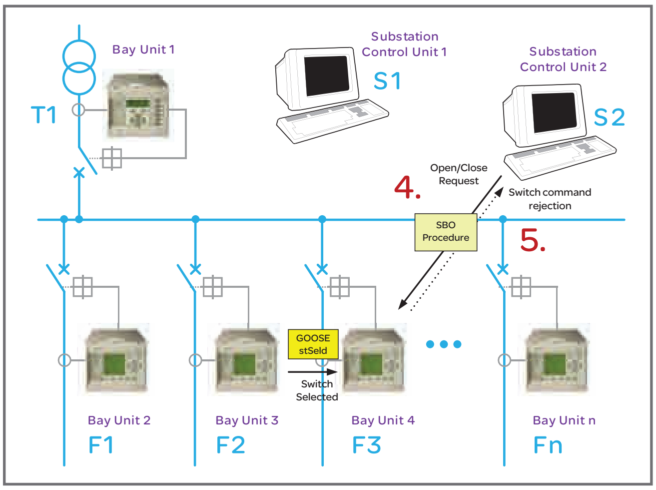

Figure D3.47:
1-of-n logic - step 4 & 5

Figure D3.48 shows the example for concept **b** for the data flow which is much simpler in terms of configuration. The operator initiates a switching control via the Operator Interface (OI) of the substation control system. As shown in Step “1” a SBO request is transmitted from the OI to the bay unit F3. The control procedure for SBO reacts by performing a system-wide interlocking check and responds in Step “2” with a positive confirmation that a switch is now selected. In the next step “3” the bay unit changes the status of the “stSeld” of the chosen switch as “selected” and updates immediately the GOOSE content to the interlocking bay unit. The interlocking bay unit reacts with an immediate update on the release GOOSE messages back to all bay units of the affected system to block further switching operations by setting CILO EnaCls and EnaOpn signals for all other switches to false state (see Table D3.25).

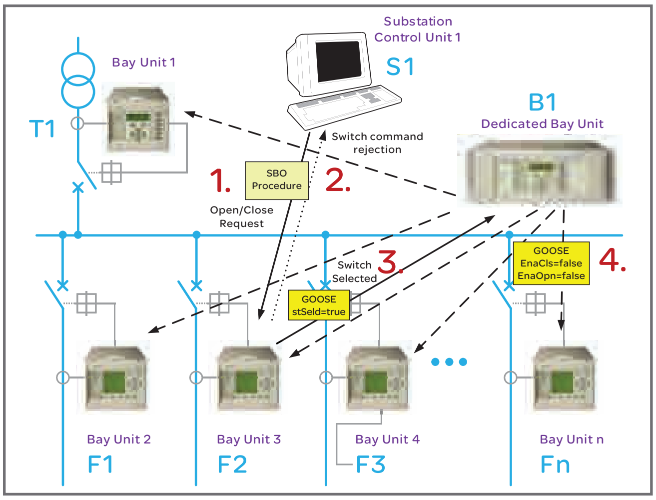

Figure D3.48:
1-of-n logic with dedicated interlocking unit

4. Typical applications

LN	DO	CDC	DA	Values
XCBR XSWI	Pos	DPC	stVal	0 = intermediate-state 1 = off 2 = on 3 = bad-state
XCBR XSWI	Pos	DPC	stSeld	0 = false 1 = true
CILO	EnaOpn	SPS	stVal	0 = false 1 = true
CILO	EnaCls	SPS	stVal	0 = false 1 = true

Table D3.25:
Transmitted data for substation interlocking

If a second control command is initiated during the whole switch operation time by the HMI or a second OI client, the related bay unit can directly reject the control request, as the incoming system-wide interlocking GOOSE from the dedicated interlocking bay unit is blocking it by false states of the related EnaOpn and EnaCls signals.

For the 1-of-n control logic application the same recommendations related to communication interruptions are valid as mentioned in section 4.2.1 "Reverse Interlocking". Dependent on the location of the interruption, a control command can be executed without problem or will be rejected. The most critical case is when a bay unit no longer receives any release signals from the dedicated interlocking bay unit (concept **b**) while a system OI still receives updates over client-server communication. Dependent on the GOOSE default definitions it could happen that a second bay unit accepts a switching command in parallel when not receiving the stSeld information (concept **c**) or EnaOpn/EnaCls information (concept **b**). To prevent this case, it would be useful to report GOOSE error information using LN LGOS to each OI to signify that the system-wide interlocking is not fully operational. For further consideration of fault conditions refer to section 4.2.5 "General Requirements".

4.2.4 Bay unit testing

Before the first operation of a bay unit in a substation, or at regular intervals after commissioning, the functionality of that bay unit needs to be validated. During such tests the system and operators need to be aware that testing is in progress or test actions need to masked from the operators as not relevant information.

As an example a substation control log should not include test messages and test values as they are not relevant for the normal operation. On the other hand, it is important to block commands from external communications during the ongoing testing if they are not sent specifically for testing purposes.

Conventional serial standard protocols like IEC60870-5-103 provide a solution "monitor direction blocked" to satisfy this requirement. Such a solution cannot be used in the scope of IEC 61850 since there are typically not just two communication partners (in -103 master and slave) but rather a larger number of controlling and monitoring communication clients that can have access to the bay units as servers.

While testing a protection and/or control bay unit in a system environment, a test engineer may have to test one or more functions, an IED or an application scheme. Dependent on the scope of work, the test engineer has to define the structure of functions which have to be put in functional isolation. Resulting from this definition one or more Logical Nodes (LN), one or more Logical Devices (LD), one IED or a number of IEDs must be set to test mode. The strict subordination of the behaviour of Logical Nodes under the behaviour of Logical Devices allows a structured intervention into the IED concerning the LN mode:

a. One or more LN:
access of LNxx.Mod controls this LN

b. One or more LD:
access of LDxx.LLN0.Mod controls all subordinate LD and LN (LLN0 is the central LN of each LD)

c. One complete IED:
access of LD0.LLN0.Mod controls all LD of this IED (Remark: LD0 is the central Logical Device for non-functional LN of a Physical Device, if it exists)

The most common way of testing today is to set a complete bay unit to the test mode. Because of that further description is given for this use case only. If the feature is supported in the IED, the activation of the test mode can be triggered by a binary input stimulated from the insertion of the test plug into the secondary circuits. It is very usual to set the IED into test mode directly via front panel or the operating program.

In a substation which is usually kept in operation during bay unit testing, the IED becomes isolated. This means that some analogue and binary inputs and outputs have to be disconnected or changed over to safe state values to have no negative influence to the other equipment remaining in active operation. On the communication link to the substation control system or network control centre a dedicated message has to be communicated to inform about the unavailability for normal operation. Figure D3.49 illustrates how this information is provided in the client-server communication. In IEC 61850 the test mode information is included in the data object "Beh" of each logical node, including LLN0 which represents the global state of the parent logical device. Tables D3.26 and D3.27 show the details of the related data object which changes its status for IED F2. The data attribute "stVal", normally in "on" state, changes to the state "test", if the binary outputs are still connected during the testing to the primary equipment. If they are isolated for the testing which is very usual, the state changes to the "test/blocked" mode accordingly. If the output isolation and test mode changes in two individual steps, the mode first moves from "on" to "on-blocked" and then to "test/blocked" or from "on" to "test" and then to "test/blocked".

4. Typical applications

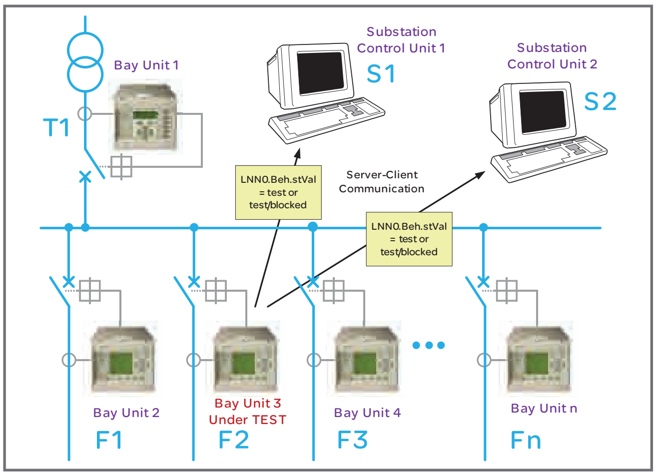

Figure D3.49:
IED in test mode with related indication to the outside equipment in a substation

T/R	IED	LDInst	LN	DO	DA
T->	F2	Various	LLN0 others	Beh	stVal, q

Table D3.26:
Transmitted data for signalling test mode

LN	DO	CDC	DA	Values
LLN0 Others e.g. CSWI PTOC	Beh	ENS	stVal	1 = on 2 = on-blocked 3 = test 4 = test/blocked 5 = off

Table D3.27:
Detailed data for signalling test mode

For each LD the central node "LLN0" changes "Beh" when its state gets modified by the "Mod", to signal the state change for the LD itself. If so, each LN in this LD, e.g. CSWI for control or PTOC for protection, will change the state of "Beh" as well. As this information is usually an element of all data sets, spontaneous reports of all related nodes, which change their states to test mode, are sent to all clients accordingly. This and all further reports to these clients will have data marked as produced while in test mode (data attribute .q as shown in Table D3.28 and D3.29).

T/R	IED	LDInst	LN	DO	DA
T->	F2	Control	CSWI	Pos	q

Table D3.28:
Signalling of messages for testing

LN	DO	CDC	DA	SDA	Values
CSWI	Pos	DPC	q	test	0 = false (off) 1 = true (on)

Table D3.29:
Client message with marking of test mode

The connected clients of the substation and network control system have to react by highlighting this state change of the IED to test mode on their Operator Interface. Furthermore they may ignore all further incoming messages from the IED under test to avoid misinterpretation or malfunction of the equipment not considered as in test mode.

In the opposite case, a client could be used to support the testing by generating special control commands to the IED. In IEC 61850 such test commands are sent with a dedicated marking "Test" in each message to this IED. The IED itself must react only to those messages which are sent with marking "Test".

When a bay unit is placed in Test mode then each of its GOOSE messages must also reflect this by modifying DA. This marking uses the quality DA .q.test = true similar to that used for reporting. The subscribing IED has to react by considering the received data as no longer relevant for its operation whilst the publisher remains in test mode. The detection is only possible when the quality DA for each signal is configured to the GOOSE data set. See also the section 4.2.5 "General Requirements" describing a concept to handle this use case. Figure D3.50 illustrates the example of an IED F2 under test in a complete substation sending its "test mode" information to the other IEDs. The annex of part 7-4 defines how each communication partner should handle each kind of element in test or normal mode.

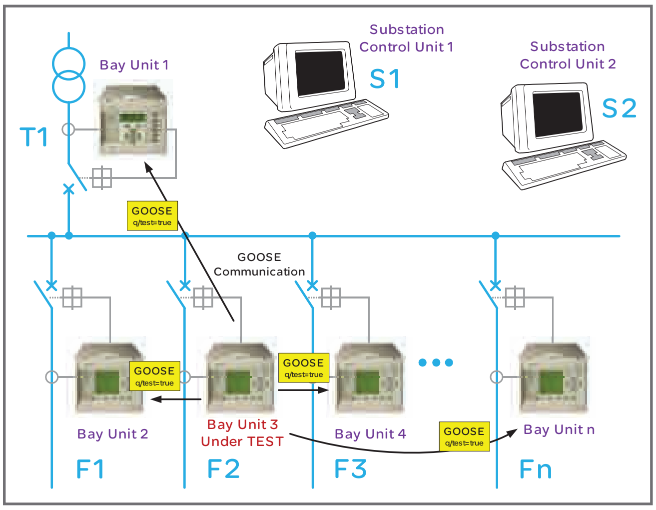

Figure D3.50:
IED in test mode with related indication to the outside equipment in a substation

4. Typical applications

There are several functions of a bay unit to be tested in a substation, the most common test cases are:

a. Primary switchgear testing

b. Isolated protection function testing of a bay unit

c. Isolated control function testing of a bay unit with or without switchgear consideration

d. Client-server communication testing of a bay unit to the substation control system

e. GOOSE communication testing of a bay unit

f. Protection scheme testing of multiple bay units with or without GOOSE communication

For the primary switchgear testing it makes sense to switch the related bay unit to test mode beforehand. Then the operator is informed that a test is ongoing. An IED which is set to test mode is still connected to the primary equipment and thus the control testing typically is made directly via front panel HMI of the bay unit.

For the isolated protection function testing the entire device has to be switched into "test/blocked" mode. Normally a test plug is used to disconnect the CT/VT and to short-circuit the CT connections to the primary substation transformers and to connect the analogue inputs and some of the binary in/outputs to a secondary injection test set.

For the isolated control function testing the IED is set into the same mode as for the protection testing ("test/blocked"). To test the whole chain of control function, a test client is required to send control commands with the test attribute activated. If the connection to the switchgear has to be included in the testing, the binary control outputs have to be kept connected to the primary to initiate a real circuit breaker or disconnector activation ("test"only).

To test the client-server communication to a client, the bay unit should be switched to the "test-blocked" mode and the affected clients to a dedicated test mode. From then on, each message sent from or to the bay unit is then only to be used for testing. In principle a client could possibly work for equipment under test and equipment in operation marking its controls with or without test information. However for unintentional wrong actions during testing it might be in too dangerous in practice.

For the GOOSE communication testing more and more test equipment provides test features over Ethernet. Testing is facilitated for instance by simulating the GOOSE messages published by other IEDs or by checking the content of the GOOSE received which is marked with test attributes. IEDs which support the simulation functionality indicate this with the DO "Sim" in the LN "LPHD" of related LD.

To test a complete application of multiple bay units using GOOSE, all affected IEDs have to be switched into the "test" mode. Dependent on the test attribute received, the subscriber can differentiate between GOOSE messages coming from IEDs in test mode and from those which remain in normal operation. Once this complex testing is made, the communication loss test (fall-back to a default value) should also be tested to check the right behaviour in a complex network.

The testing capabilities in an IEC 61850 network environment are manifold as the standard provides a comprehensive functionality around this. This can be seen as one of the key advantages of this standard. At least when the bay units work on sampled values over Ethernet from Merging Units transformers, the testing equipment can simulate every analogue signal over the same Ethernet as the Merging Units. Only the 'Sim' indication is recognized by the IED under test which analogue values have to be processed. If all binary inputs and outputs are processed by GOOSE messages, the data exchange with information marked 'test' prevents misinterpretation. When switching an IED to the test mode, no test plug is required, as all information goes over Ethernet and all the partners know which information is based on test and which on operation. Testing equipment installed at a central place where it is connected to the substation Ethernet will make it perfect. The user will benefit from accessing all devices from one workplace, saving the time to move from one device to the other. Figure D3.51 illustrates this highly sophisticated test method of the future.

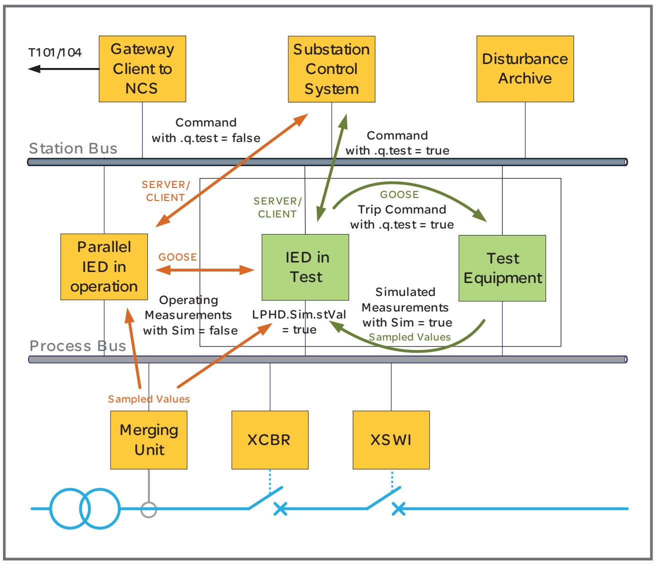

Figure D3.51:
IED in test mode with related indication to the outside equipment in a substation

4.2.5 General requirements

When using GOOSE for data transmission, the quality attribute shall be always evaluated. The possibilty to convey information about the data quality of each information value is a key feature of IEC 61850. On the publisher side it has to be assured that each information value is accompanied by its data attribute ‘q’, to allow the subscriber run a data quality dependent processing. The GOOSE monitoring on the subscriber side must inform the processing functions whether the information received can be used for processing. In case of missing GOOSE messages, the subscriber may modify the data quality attributes of each affected piece of information. In devices which support the change-over to default value/ quality upon the detection of the loss of a GOOSE message the subscriber function can substitute the last received information by pre-configured values and qualities. (see example for a system-wide interlocking logic in Figure D3.52). These defaults should be defined carefully to prevent malfunctions in the application. The data evaluated is shown in Table D3.30 and D3.31. IED F2 continuously receives GOOSE messages from IEDs T1 and F1 containing their switch positions, for an interlocking logic. If the data attribute “q” shows e.g. a validity of “invalid”, the latest received switch position can no more be used.

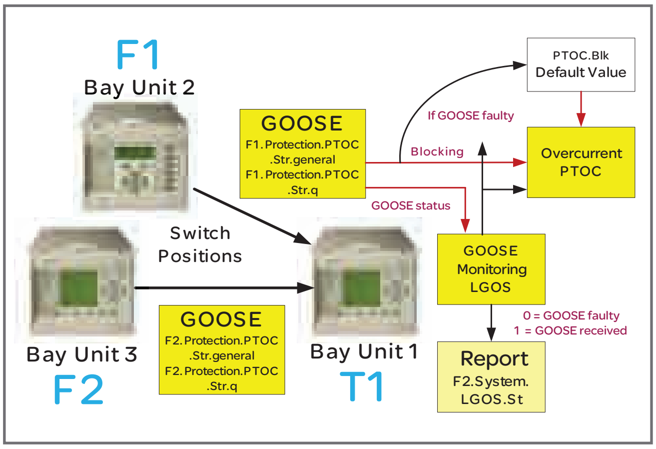

Figure D3.52:
GOOSE monitoring with LGOS

T/R	IED	LDInst	LN	DO	DA
->R	F2	Control	XCBR XSWI	Pos	stVal, q
T->	F2	System	LGOS	St	stVal, q

Table D3.30:
Transmitted data for GOOSE monitoring

LN	DO	CDC	DA	SDA	Values
XCBR XSWI	Pos	DPC	q	validity test	0 = good 1 = invalid 2 = reserved 3 = questionable 0 = false (off) 1 = true (on)
LGOS	St	SPS	stVal		0 = GOOSE inactive 1 = GOOSE active

Table D3.31:
Transmitted data for GOOSE monitoring

Another use case is the activation of the test mode of a publishing IED described in section 4.2.4 “Bay Unit Test”. In this case the quality sub attribute “test” should be evaluated as not relevant for the normal operation if the subscribing IED is not in test mode as well.

To prevent data being lost when (due to frame collisions in the Ethernet network), a GOOSE message is repeated subsequently in increasing time intervals until its normal slow sending cycle (without status change) has been restored. To detect a GOOSE communication interrupt, the IED should provide a monitoring function. The standard provides a dedicated Logical Node LGOS with a status value “St” for the indication of the communication status (see Figure D3.52). The data transmitted is shown in Table D3.30 and D3.31.

The number of GOOSE messages or sampled values in the affected network should not become too high (-> e.g. no merging unit on the same bus as substation control system) to ensure the high demands on the transmission time.

A significant improvement of the GOOSE transmission time can be achieved if all network components (IEDS and switches) support ‘VLAN’ so that GOOSE messages can be prioritised. If such a method is required due to the network load conditions, all corresponding IEDs have to provide this configuration capability - which might not be the case as this is an optional function in IEC 61850.

Using redundancy protocols to improve the availability and reliability of the communication links is very useful. But for protection applications special attention has to be paid. Protocols like RSTP e.g. are not recommended, as the reconfiguration time for the network after any failure in the system takes up to several seconds, which means that applications such as reverse interlocking are not operable during this interruption time. There are other protocols to choose from, like HSR or PRP, which are able to manage a reconfiguration in a few milliseconds.