IEC/TR 61850-90-5

Edition 1.0 2012-05

TECHNICAL REPORT

colour inside

Communication networks and systems for power utility automation – Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118

IEC/TR 61850-90-5:2012(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC/TR 61850-90-5

Edition 1.0 2012-05

TECHNICAL REPORT

colour inside

Communication networks and systems for power utility automation – Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE XG

ICS 33.200

ISBN 978-2-83220-092-6

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 61850-90-5, which is a technical report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
57/1144/DTR	57/1207/RVC

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This technical report has been prepared in a joint effort between IEC and IEEE. A task force consisting of members from the IEC TC 57 WG 10 as well as the IEEE Power and Energy Society/IEEE Power System Relay Committee has prepared that report with task force meetings both at the regular meetings of IEC TC 57 WG 10 as well as at the regular meetings of the IEEE Power and Energy Society/IEEE Power System Relay Committee. Once the technical report is approved and published, the results will be integrated as amendments into the relevant parts of IEC 61850.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 61850 series, under the general title: *Communication networks and systems for power utility automation*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

A bilingual version of this publication may be issued at a later date.

INTRODUCTION

Synchrophasor data as measured and calculated by PMUs are considered to be useful information to assess the condition of the electrical power network.

The synchrophasors and related message formats to transmit synchrophasor data over long distances are defined in IEEE C37.118.

Even though the communication according to IEEE C37.118 has proven to be usable and work well, there is a desire to have a communication mechanism that is compliant to the concept of IEC 61850. This document lays out how this shall be done.

COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118

1 Scope

This part of IEC 61850 provides a way of exchanging synchrophasor data between PMUs, PDCs WAMPAC (Wide Area Monitoring, Protection, and Control), and between control center applications. The data, to the extent covered in IEEE C37.118-2005, are transported in a way that is compliant to the concepts of IEC 61850.

However, given the primary scope and use cases, this document also provides routable profiles for IEC 61850-8-1 GOOSE and IEC 61850-9-2 SV packets. These routable packets can be utilized to transport general IEC 61850 data as well as synchrophasor data.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61850-2:2003, *Communication networks and systems in substations – Part 2: Glossary*

IEC 61850-6:2009, *Communication networks and systems in substations – Part 6: Configuration description language for communication in electrical substations related to IEDs*

IEC 61850-7-1, *Communication networks and systems for power utility automation – Part 7-1: Basic communication structure – Principles and models*

IEC 61850-7-2, *Communication networks and systems in substations – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI)*

IEC 61850-7-3, *Communication networks and systems for power utility automation – Part 7-3: Basic communication structure – Common data classes*

IEC 61850-7-4:2010, *Communication networks and systems for power utility automation – Part 7-4: Basic communication structure – Compatible logical node classes and data object classes*

IEC 61850-8-1:2011, *Communication networks and systems for power utility automation – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*

IEC 61850-9-2:2010, *Communication networks and systems for power utility automation – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3*

IEC/TR 61850-90-1, *Communication networks and systems for power utility automation – Part 90-1: Use of IEC 61850 for the communication between substations*

IEC/TS 62351-1, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IEC/TS 62351-6:2007, *Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850*

ISO/IEC 8802-3:2000, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

ISO/IEC 19772, *Information technology – Security techniques – Authenticated encryption Also available as: NIST SP 800-38D*

ITU-T X.234, *Information technology – Protocol for Providing the OSI connectionless-mode transport service*
Amendment 1: *Addition of connectionless-mode multicast capability*

IEEE 802.1Q, *Virtual Bridged Local Area Networks*

IEEE C37.118.1, *Standard for Synchrophasor Measurements for Power Systems*

IEEE C37.118.2:2011, *Standard for Synchrophasor Data Transfer for Power Systems*

NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC

RFC 768, User Datagram Protocol

RFC 791, Internet Protocol DARPA Internet Program Protocol Specification

RFC 793, Transmission Control Protocol

RFC 826, An Ethernet Address Resolution Protocol

RFC 894, A Standard for the Transmission of IP Datagrams over Ethernet Networks

RFC 1108, U,S, Department of Defense Security Options for the Internet Protocol

RFC 1240, OSI Connectionless Transport Services on top of UDP Version:1

RFC 2104, HMAC: Keyed-Hashing for Message Authentication

RFC 2406, IP Encapuslating Security Payload (ESP)

RFC 2407, Internet Key Exchange (IKEv1) Protocol

RFC 2474, Definition of Differentiated Services Field (DS Field) in IPv4 and IPv6 Headers

RFC 2991, Multipath Issues in Unicast and Multicast Next-Hop Selection

RFC 3168, The Addition of Explicit Congestion Notification (ECN) to IP

RFC 3246, An Expedited Forwarding PHB (Per-Hop Behavior)

RFC 3376, Internet Group Management Protocol, Version 3

RFC 3547, The Group Domain of Interpretation

RFC 5771, IANA Guidelines for IPv4 Multicast Address Assignments

UCA User's Group 61850-9-2LE- Implementation Guideline for Digital Interface to Instrument Transformers using IEC 61850-9-2

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61850-2, IEC 61850-7-2 and IEEE C37.118.1 as well as the following apply.

3.1
IED tool
short for IED configuration tool or IED configurator in the sense of IEC 61850-6

3.2
nonce
number used once

Note 1 to entry: A nonce is some value that varies with time, although a very large random number is sometimes used.

3.3
part(ial) system
part of a complete system, with a defined, self-consistent part functionality

3.4
project
system part with ownership of a set of IEDs, typically those located in one substation, and handled by one system configuration tool

3.5
gateway
internetworking system capable of allowing communications/information exchange between two networks that use different communication protocols

3.6
system
union of all communicating application-functions performing some overall task like "management of a substation", via logical nodes

Note 1 to entry: The physical system is composed of all devices hosting these functions and the interconnecting physical communication network.

4 Abbreviated terms

The following abbreviations apply to this document.

APDU	Application Protocol Data Unit
A-Profile	Application Profile
CDC	Common Data Class
CID	Configured IED Description
CT	Current Transformer
DA	Data archiver
DNS	Domain Name Service
DSCP	Differentiated Services Code Point
ECN	Explicit Congestion Notification
EF	Expedited Forwarding
ESP	Electronic Security Perimeter
ET	Event Trigger
FACTS	Flexible Alternating Current Transmission Systems
FC	Functional constraint
FCD	Functionally Constrained Data
FCDA	Functionally Constrained Data Attribute
FSS	Functional Software Specification
GCM	Galois Counter Mode
GDOI	Group Domain of Interpretation
GMAC	Galois Message Authentication Code
GoCB	GOOSE Control Block
GOOSE	Generic Object Oriented Substation Event
GW	Gateway
HMI	Human Machine Interface
HW	Hardware
IANA	Internet Assigned Numbers Authority
ID	Identification
IED	Intelligent Electronic Device – any programmable or configurable device in the system
IGMP	Internet Group Management Protocol
IID	IED Instance Description. Describes an IED instance in a project.
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
KDC	Key Distribution Center
LAN	Local area network
LD	Logical Device (IEC 61850)
LI	Length Identifier. This value contains the length of the SI or PI with which it is associated.
LN	Logical Node (IEC 61850)
m	Mandatory – shall be implemented
MAC	Media Access Control
MSV	Multicast Sampled Value
MSVCB	Multicast Sampled Values Control Block
o	Optional – may be implemented

OOS	Out-of-step
ORG	Originator
OSI	Open System Interconnect
PDC	Phasor Data Concentrator
PI	Parameter Identifier. This identifier is used to identify a specific session protocol parameter.
PICS	Protocol Conformance Implementation Statement
PMU	Phasor Measurement Unit
POP	Proof of Possession
PSP	Physical Security Perimeter
r	Readable
RAS	Remedial Action Scheme
SA	Substation Automation
SCD	System Configuration Description in the sense of 61850-6. Output of a system tool of a project to configure the IEDs belonging to the project (imported by IED tools).
SCL	Substation Configuration description Language according to IEC 61850
SDH	Synchronous Digital Hierarchy
SED	System Exchange Description: an SCL file containing a part of a system for exchange of interfacing and responsibility data between projects
SEQ	Sequence
SI	Session Identifier. This identifier is used to identify the session protocol that is in use.
SIPS	System Integrity Protection Scheme
SONET	Synchronous Optical NETwork
SP	Synchrophasor
ssPDC	Substation Phasor Data Concentrator
SPDU	Session Protocol Data Unit
SPS	Special Protection Scheme
SS	Substation System
SSDU	Session Service Data Unit
SV	Sampled Values
SVCB	Sampled Value control block; here used to send synchrophasor data periodically
R-SV	Routable Sampled Value service via UDP
R-GOOSE	Routable GOOSE via UDP
SW	Software
TAI	International Atomic Time (TAI, from the French name Temps Atomique International).
TCI	Tag Control Information
TCP	Transmission Control Protocol
TOS	Type of Service
TPDU	Transport Protocol Data Unit
TPID	Tag Protocol Identifier (for IEEE 802.1Q networks)
T-Profile	Transport Profile
TSAP	Transport Service Access Point
TSDU	Transport Service Data Unit
TSEL	Transport Selector
UDP	User Datagram Protocol
VT	Voltage Transformer. Also known as a Potential Transformer (PT).
w	Writeable
WAMPAC	Wide Area Monitoring, Protection, and Control

WAN	Wide area network
XML	eXtensible Markup Language
XSD	eXtensible Markup Language (XML) Schema Definition
R-MSVCB	Routable Multicast Sampled Value Control Block
R- GoCB	Routable GOOSE Control Block

NOTE Abbreviations used for the identification of the common data classes and as names of the attributes are specified in the specific clauses of this document and are not repeated here.

5 Use cases

5.1 General

Synchrophasor communication can be used within a substation such as for synchrocheck or substation level state estimation, or from several substations to a center which performs regional or network level alarms and stability calculations. Both areas of use are described and delineated in the following subclauses.

In the following use cases, the arrows indicate data flow from one device to another. The solid-like arrows are the basic data flow for all illustrated applications, and the dashed arrows are optional data flow from additional locations. The dashed boxes around groups of objects are co-located equipment as labelled.

5.2 Wide area applications utilizing synchrophasors

In the majority of the applications, the sources and sinks for the synchrophasor data are separated by large distances. In this context, "large" means distances which extend essentially further than a typical local area network (LAN).

One of the options to transmit data over arbitrary large distances is using the Internet Protocol (IP). The IP allows the routing of data packets (IP packets) between different networks over any distance. This document focuses on options that utilize IP.

The use of UDP for the streaming of the synchrophasor data is a proven and functional method. The many working applications of the IEEE C37.118 protocol confirm this. Thus, a method utilizing UDP for streaming the SV data is again required. TCP can also be and has been used but with the reservations outlined in 6.4.

In all use cases, the latency requirement refers to end-to-end communications delay. This is the interval of time from when the message is sent from the measurement device to when it is received by the application. It includes all communication delays including LAN, WAN, and router delays as well as delays in intermediate processing units such at ssPDC and PDC units. It does not include measurement delays from the signal input to synchrophasor calculation. It is specified for each use case as a general guideline for communication planning for the described application. Individual application needs will vary and those particular requirements need to be assessed at the time of implementation.

For an application which takes an action based on data it receives, lost packets effectively increase delay in response. A single lost packet will cause a delay equivalent to the interval between packets set by the data reporting rate. The application can tolerate lost packets up to the allowable delay for response. It can therefore tolerate greater numbers of successive lost packets by using higher data rates. Some applications may be able to estimate values for lost data from previous ones, but even this will result in a delayed action. In all cases, applications dependent on transmitted data require a time out to detect excessive packet loss and a fall back operating mode and/or alarm when this occurs.

Applications that record data or build response curves for calculation or visualisation will usually tolerate some data loss with little problem. They can approximate missing values with various patching techniques. The problem is more in the pattern of loss rather than simply loss. Short loss intervals are much easier to patch with reasonable accuracy than long ones. Loss consisting of short dropouts of a few successive samples is more tolerable than less frequent longer dropouts. Any response will be delayed as previously described. A data loss detection timeout and fall-back operating mode and/or alarms are also required.

Jitter, or variation in delay, will cause a variation in action time of any application that uses the data. As long as the jitter is considerably lower than the data rate interval, it should not have much effect on the application. If it approaches the allowable delay time which could be larger or smaller than the interval between successive data samples, it will have an effect on the response and can be the limiting factor. Data concentration will be delayed by jitter as the process must wait for all data to arrive before assembling a complete packet and forwarding it. In all cases, jitter needs to be included in the worst case delay calculations.

5.3 Synchro-check

In this application, data are sent from one or more PMU devices to a sync check relay. The general information flow is shown in Figure 1. The relay uses this information to assure the phase angles of the voltage on two sides of a breaker are close enough that the breaker can be closed without harm.

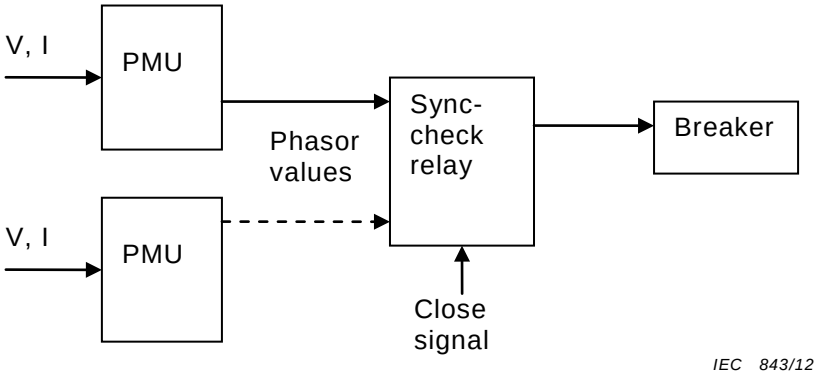


Figure 1 – Use case diagram for Synchro-check

Actors:

Name	Role description
PMU	Computes synchrophasors & frequency
Relay	Checks phase angle between selected inputs
Breaker	Connects/disconnects power line

Operations:

Name	Service or information provided
Data sampling & phasor estimate	PMU estimates synchrophasor and frequency values from voltages and currents
Data sending & receiving	PMU sends values that are received by relay
Relay decision	Checks phase angle between selected inputs and issues a signal to breaker if included angle is within limits

Basic flow:

Data origination & sending

Use case step	Description
Step 1	PMU computes V & I synchrophasors & system frequency
Step 2	PMU selects phasors and frequency at given output rate
Step 3	PMU packages data with appropriate status and time stamp
Step 4	PMU sends data to relay

Data receiving & action

Use case step	Description
Step 1	Relay receives synchrophasor data
Step 2	Relay extracts appropriate phase angle data and checks status flags
Step 3	Relay checks phase angle between selected inputs
Step 4	Relay makes decision & issues command if needed

Constraints:

Synchrophasor measurements can be communicated at a variety of rates and may conform to other standards such as IEEE C37.118.1. The following table summarizes a minimum measurement transmission rate, maximum delay in data transmission, and maximum measurement time error. The measurement timing error contributes directly to error in phase angle measurement which is critical for this application. Such measurement errors are governed by IEEE C37.118.1.

Minimum rate	Maximum communication delay (latency) time	Maximum measurement timing error
4/second	0,1 s	0,05 ms

5.4 Adaptive relaying

In this application, data is sent from one or more PMU devices to a relay supervision function. The general information flow is shown in Figure 2. The receiving device uses this information to adjust relaying parameters or settings so the relay is making optimal decisions based on the actual system configuration. This type of application as currently envisioned is a low-speed application that takes advantage of the precision and wider observability of the phasor measurement system.

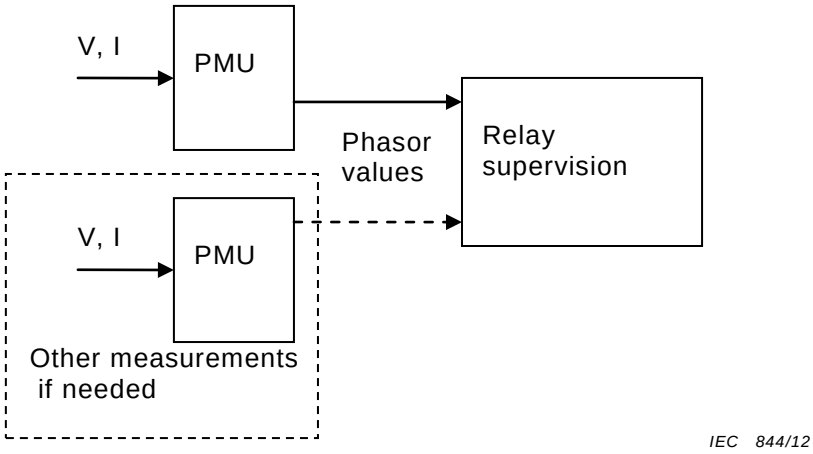


Figure 2 – Use case diagram for adaptive relaying

Actors:

Name	Role description
PMU	Computes synchrophasors & frequency
Relay supervisor	Receives data & makes setting adjustments based on pre-determined algorithm and tables using syncrophasor measurements

Operations:

Name	Service or information provided
Data sampling & phasor estimate	PMU estimates synchrophasor and frequency values from voltages and currents
Data sending & receiving	PMU sends values that are received by relay supervisor
Relay supervisor decision	Compares measurements with reference values using given algorithms; changes relay parameters as needed.

Basic flow:

Data origination & sending

Use case step	Description
Step 1	PMU computes V & I synchrophasors & system frequency
Step 2	PMU selects phasors and frequency at given output rate
Step 3	PMU packages data with appropriate status and time stamp
Step 4	PMU sends data to relay

Data receiving & action

Use case step	Description
Step 1	Relay supervisor receives synchrophasor data
Step 2	Relay supervisor extracts voltage/current angle and magnitude and frequency information as needed
Step 3	Relay supervisor computes settings based on algorithms and measurements
Step 4	Relay supervisor makes changes in relay settings as required

Constraints:

Synchrophasor measurements can be communicated at a variety of rates and may conform to other standards, such as IEEE C37.118.1. Since adaptive relaying is not an established function, actual times and rates may vary considerably from this guideline. These values are estimated to represent the highest data rate, the maximum communication delay, and maximum measurement timing error that will be required by this application.

Minimum rate	Transfer time class	Time synchronization accuracy class
4/second	TT3 0,1 s	T3 0,025 ms

5.5 Out-of-step (OOS) protection

In this application, data is sent from two (or more) PMU devices to a controller that detects out-of-step conditions between substations or system areas. It uses the phase angle and frequency measurements to detect excessive and increasing phase angle, and takes action to reduce the angle or island the system. The general information flow is shown in Figure 3.

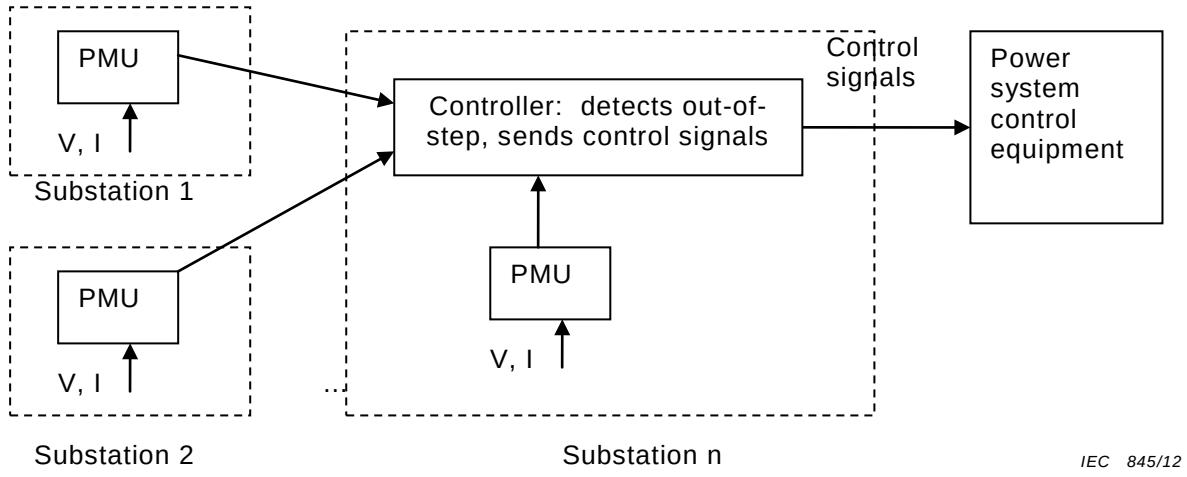


Figure 3 – Use case diagram for out-of-step (OOS) protection

Actors:

Name	Role description
PMU	Computes synchrophasor & frequency
Out-of-step controller	Receive data from the local PDC & perform various processing, alarming, and visualization functions
Power system control equipment	Controls the power system through switching, FACTS power controllers, DC controls, etc.

Operations:

Name	Service or information provided
Data sampling & phasor estimate	PMU estimates synchrophasor and frequency values from voltages and currents
Data sending & receiving	PMU sends values that are received by the controller
Out-of-step protection	The controller compares the data from all PMUs to detect if the protected areas are going out-of-step with each other. If it detects conditions that indicate the areas are going OOS, it initiates control actions

Basic flow:

Data origination & sending

Use case step	Description
Step 1	PMU computes V & I synchrophasors & system frequency
Step 2	PMU selects phasors and frequency at given output rate
Step 3	PMU packages data with appropriate status and time stamp
Step 4	PMU sends data to the controller

Data receiving & action

Use case step	Description
Step 1	Controller receives synchrophasor data
Step 2	Controller selects appropriate data for processing
Step 3	OOS Application compares measurements from indicated PMUs and takes action according to indicated conditions

Constraints:

OOS control actions must take place within a limited time. The measurements must be validated within a short period of time. The data rate has to be rapid enough to support the allowed latency between samples. The following table summarizes the minimum measurement transmission rate, allowable latency range, and maximum measurement timing error that can be tolerated in this application.

Minimum rate	Transfer time class	Time synchronization accuracy class
10/second	TT2 0,5 s	T3 0,025 ms

5.6 Situational awareness

In this application, data is sent from one or more PMU devices to alarm and display applications in a control center. These applications may include processing and alarm functions such as oscillation detection and path loading limits. These applications provide alarms to operations personnel based on information derived from the data and compared with pre-programmed criteria. The general information flow is shown in Figure 4.

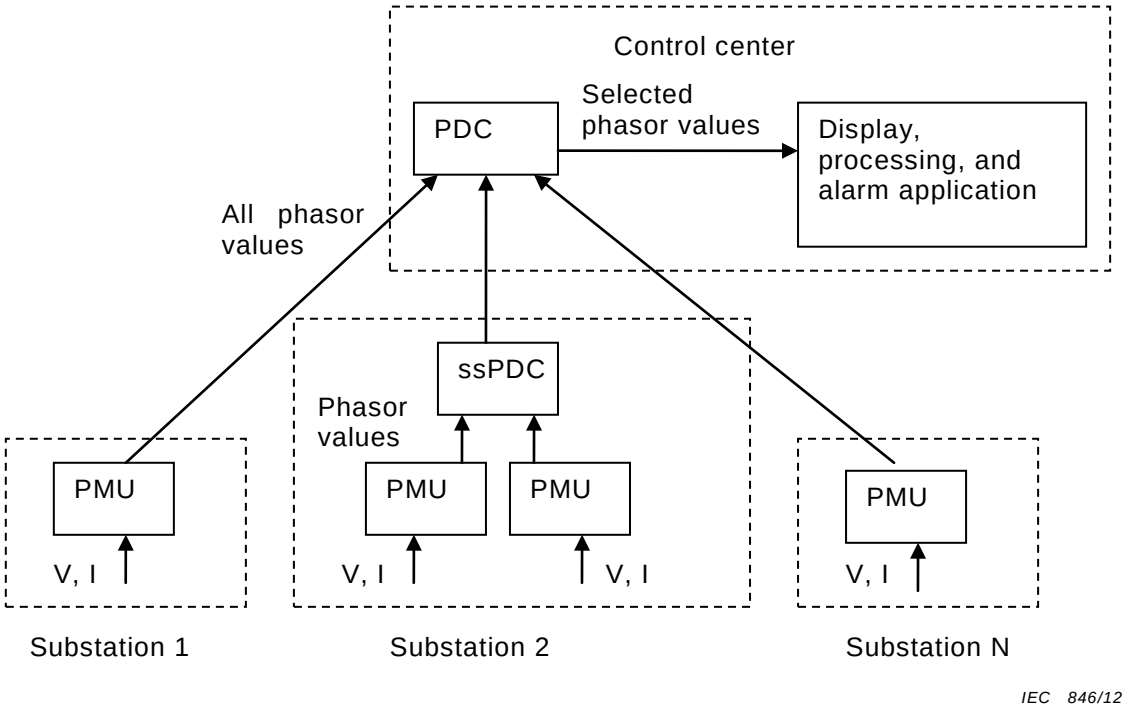


Figure 4 – Use case diagram for situational awareness

Actors:

Name	Role description
PMU	Computes synchrophasors & frequency
ssPDC	Substation Phasor Data Concentrator – collects, aligns, selects & possibly decimates data from several PMUs in the substation
PDC	Phasor Data Concentrator – collects, aligns, selects & possibly decimates data from several PMUs or other PDCs
User applications	Receive data from the local PDC & perform various processing, alarming, and visualization functions

Operations:

Name	Service or information provided
Data sampling & phasor estimate	PMU estimates synchrophasor and frequency values from voltages and currents
Data sending	PMU sends synchrophasor & frequency values
Data receiving/sending	If there is an ssPDC, the data is received in the substation, combined with data from other PMUs, and forwarded to the destination PDC
Data receiving	PDC receives data from PMU or ssPDC, combines with data from other measuring units, and sends on to applications
Situational awareness applications	Applications provide displays of information and process data for more advanced alarms and displays

Basic flow:

Data origination & sending

Use case step	Description
Step 1	PMU computes V & I synchrophasors & system frequency
Step 1	PMU selects phasors and frequency at given output rate
Step 2	PMU packages data with appropriate status and time stamp
Step 3	PMU sends data to the ssPDC or PDC

Data receiving intermediate (alternate path)

Use case step	Description
Step 1	ssPDC receives synchrophasor data
Step 2	ssPDC correlates and selects output data
Step 3	ssPDC resends output data to PDC

Data receiving

Use case step	Description
Step 1	PDC receives synchrophasor data
Step 2	PDC correlates and selects output data
Step 3	PDC resends output data to applications

Applications process data and alert operators

Use case step	Description
Step 1a	Application 1 searches data for system oscillations, sends an alarm to operators when one is located
Step 1b	Application 2 computes system phase angles, computes limit violations, and sends alarm to operators if there are exceptions
Step 1c	Application 3 computes flows (MW & MVAR) at strategic points (flow gates) and reports violations to operators
Step 1d	Application 4 computes system voltages and sends alarms to operators for deteriorating conditions or limit violations
Step 2	Additional displays of processed data results and alarm violation details are made available to operators

Constraints:

Synchrophasor measurements can be communicated under a variety of rates. The measurement may conform to other standards such as IEEE C37.118.1. The following table summarizes the range of required measurement transmission rates, time delays for data delivery, and maximum measurement time errors for the listed applications.

Application type	Minimum rate	Transfer time class	Time synchronization accuracy class
Inter-area oscillation detection	10/second	TT0 >1 s	T3 0,025 ms
Local oscillation detection (up to 10 Hz)	50/second	TT0 >1 s	T3 0,025 ms

Application type	Minimum rate	Transfer time class	Time synchronization accuracy class
Series resonance detection (frequencies < f_0)	Rate > 3x (maximum frequency observed)	TT0 >1 s	T3 0,025 ms
System phase angles	1/second	TT0 >1 s	T3 0,025 ms
Power flow	1/second	TT0 >1 s	T3 0,025 ms
Voltage profiles	1/second	TT0 >1 s	T0 10 ms

5.7 State estimation and on-line security assessment

In this application, data is sent from one or more PMU devices to state estimator and security assessment applications in a control center. The state estimator determines all the voltages and power flows in the grid. Security assessment determines the failure risks by applying various criteria to the state estimate. State estimation will initially use synchrophasor data to supplement traditional SCADA data for added functionality and improved performance since phasor measurements will initially be too sparse to fully support its requirements. Once sufficient measurements are available, state estimation can operate exclusively with phasor data. The general information flow is shown in Figure 5.

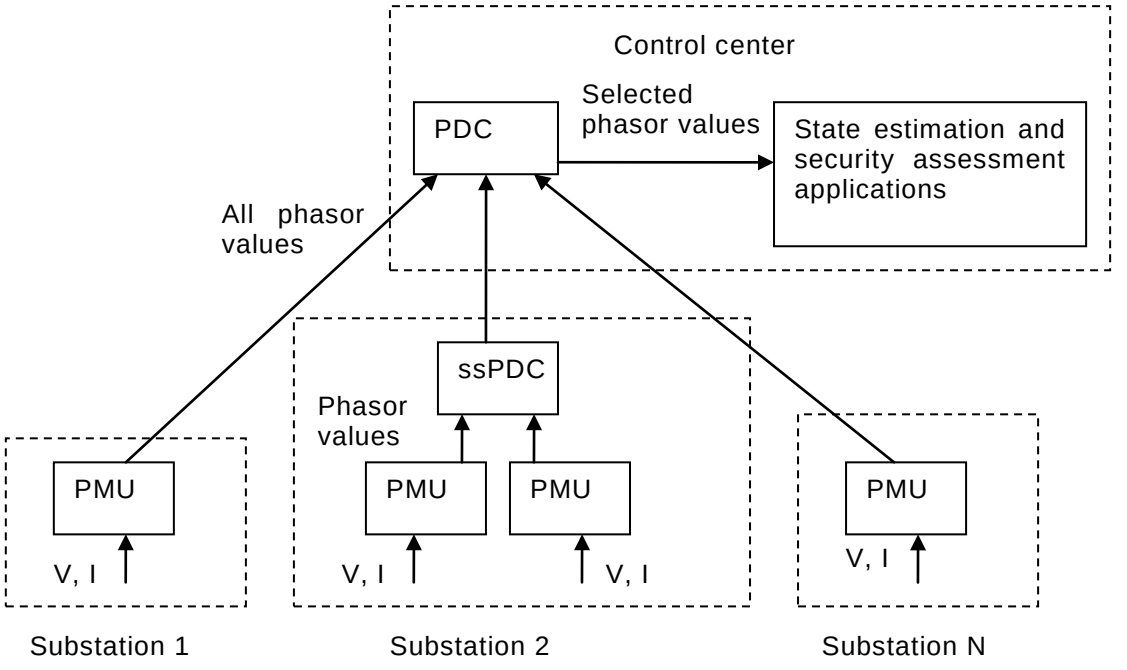


Figure 5 – Use case diagram for state estimation

Actors:

Name	Role description
PMU	Computes synchrophasor & frequency
ssPDC	Substation Phasor Data Concentrator – collects, aligns, selects & possibly decimates data from several PMUs in the substation
PDC	Phasor Data Concentrator – collects, aligns, selects & possibly decimates data from several PMUs or other PDCs
User applications	Receive data from the local PDC, merge with SCADA measurements & perform estimation and assessment functions

Operations:

Name	Service or information provided
Data sampling & phasor estimate	PMU estimates synchrophasor and frequency values from voltages and currents
Data sending	PMU sends synchrophasor & frequency values in continuous data stream
Data receiving/sending	If there is an ssPDC, the data is received in the substation, combined with data from other PMUs, and resent on to the destination PDC
Data receiving	PDC receives data from PMU or ssPDC, combines with data from other measuring units, and sends to state estimator and security assessment functions
State estimation	State estimator combines synchrophasor and SCADA data to create a state estimate
Security assessment	Security assessment uses state estimate and other data as required to perform assessment function

Basic flow:

Data origination & sending

Use case step	Description
Step 1	PMU computes V & I synchrophasors & system frequency
Step 2	PMU selects phasors and frequency at given output rate
Step 3	PMU packages data with appropriate status and time stamp
Step 4	PMU sends data to the ssPDC or PDC

Data receiving intermediate (alternate path)

Use case step	Description
Step 1	ssPDC receives synchrophasor data
Step 2	ssPDC correlates and selects output data
Step 3	ssPDC resends output data to PDC

Data receiving

Use case step	Description
Step 1	PDC receives synchrophasor data
Step 2	PDC correlates and selects output data
Step 3	PDC resends output data to applications

Applications process data and alert operators

Use case step	Description
Step 1	State estimator receives synchrophasor and SCADA data which is uses to produce an estimate of the system state
Step 2	Security assessment functions use the state estimate and other data (synchrophasor and other) to assess system security and report violations to operators

Constraints:

Synchrophasor measurements can be communicated at a rate suitable for the application it serves. Traditional state estimation operates at a rate of seconds to minutes. State estimation using phasor data can operate at sub-second intervals. There is some interest in using high rate state estimation as a filter to provide corrected data for real-time controls, but here it is being considered in the more traditional use for reporting and security assessment. A key point is obtaining measurements that are taken at the same time regardless of the rate. Measurements that conform to IEEE C37.118.1 will have this property. The following table summarizes the required data transmission rates, data transmission delay, and acceptable measurement time error.

Application type	Range of rates	Transfer time class	Time synchronization accuracy class
State estimation	1/(5 min) to 10/second	TT0 >1 s	T3 0,025 ms

5.8 Archive data (event & continuous)

Measurements from PMUs should be archived for system analysis. Archived data should include both continuous measurements and snapshots triggered by anomalous events. These data need to be accessible for later retrieval and analysis. Continuous archiving is accomplished by applications that either have sufficient storage space that they will not run out between scheduled changes, or which utilize size limiting features that delete the oldest data within a time limit. Triggered archive functionality is initiated by an event trigger (ET), here treated as a black box, which sends to one or more data archivers (DAs) an event notification which indicates a need to archive the event data. Data archiving may be a function within PDCs and ssPDCs or may be a stand-alone application. The general information flow is shown in Figure 6.

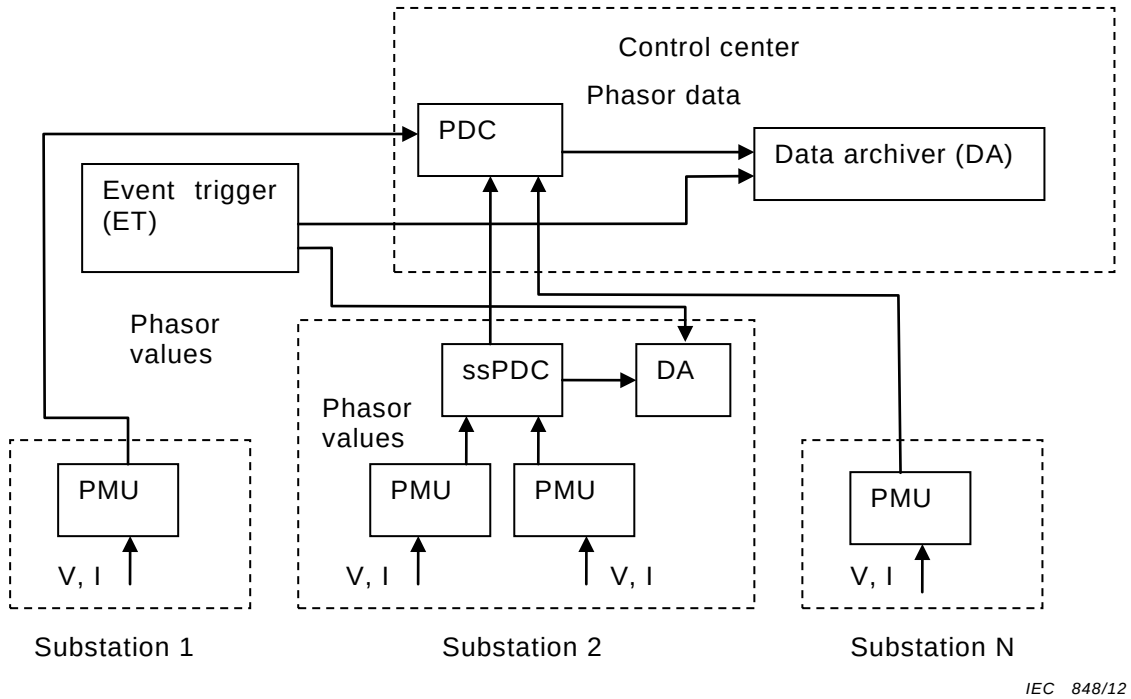


Figure 6 – Use case diagram for archiving data

Actors:

Name	Role description
PMU	Computes synchrophasors & frequency
ssPDC	Substation Phasor Data Concentrator – collects, aligns, selects & possibly decimates data from several PMUs in the substation
PDC	Phasor Data Concentrator – collects, aligns, selects & possibly decimates data from several PMUs or other PDCs
ET	Event trigger – notifies PDCs and ssPDCs to archive data within a particular time frame for later retrieval / analysis
DA	Data archiver – a functional unit with the ability to store continuous or event data from a PDC or ssPDC in non-volatile media for later retrieval and analysis

Operations:

Name	Service or information provided
Data sampling & phasor estimate	PMU estimates synchrophasor and frequency values from voltages and currents
Data sending	PMU sends synchrophasor & frequency values
Data receiving/sending	If there is an ssPDC, the data is received in the substation, combined with data from other PMUs, and forwarded to the destination PDC
Data receiving	PDC receives data from PMU or ssPDC, combines with data from other measuring units, and sends on to applications
Event trigger detection & sending	The ET determines when an event has occurred and sends a trigger that has sufficient information for the Data Archiver to correctly record the event
Event trigger receiving	A DA receives a message from an ET specifying an event to be archived for later retrieval or analysis.
Event data sending	A PDC or ssPDC sends data for the event to a DA.

Basic flow:

Data origination & sending

Use case step	Description
Step 1	PMU computes V & I synchrophasors & system frequency
Step 1	PMU selects phasors and frequency at given output rate
Step 2	PMU packages data with appropriate status and time stamp
Step 3	PMU sends data to the ssPDC or PDC

Data receiving intermediate (alternate path)

Use case step	Description
Step 1	ssPDC receives synchrophasor data
Step 2	ssPDC correlates and selects output data
Step 3	ssPDC resends output data to PDC

Data receiving

Use case step	Description
Step 1	PDC receives synchrophasor data
Step 2	PDC correlates and selects output data
Step 3	PDC resends output data to applications

Event trigger sending & receiving

Use case step	Description
Step 1	ET detects event & sends trigger information to DA
Step 2	DA stores data according to requirements for the specified event

Constraints:

Latency and bandwidth are unlikely to be constraints in the archival process, since it is not a real-time or near-real-time application. The main constraint is that the archival process be lossless, i.e., the measurements generated at the PMUs on the system should be the same measurements stored within the data archive.

Activity	Minimum rate	Maximum communication delay (latency) time	Measurement and timetag accuracy
Event data sending	N/A	N/A	Maximum accuracy of the PMUs used to generate the event data

5.9 Wide area controls

5.9.1 General

There are several different use cases for using synchrophasors in the context of wide area controls. The following subclauses document the related use cases.

5.9.2 Special protection schemes

In this application, data are sent from one or more PMU devices to a controller located at a substation, control center, or other appropriate facility. The data may go directly to the controller or may go through ssPDC or PDC data gathering devices. Using programmed algorithms, the controller will take action based on these measurements. Control functions can include switching capacitors, reactors or lines, generator dropping, SVC damping, and any other action that can be implemented. This action can include both traditional special protection schemes (SPS, SIPS, RAS, etc.) and more sophisticated schemes that are based on measured system responses rather than pre-programmed responses. Synchrophasors provide accurate high speed measurements useful for this purpose. The general information flow is shown in Figure 7.

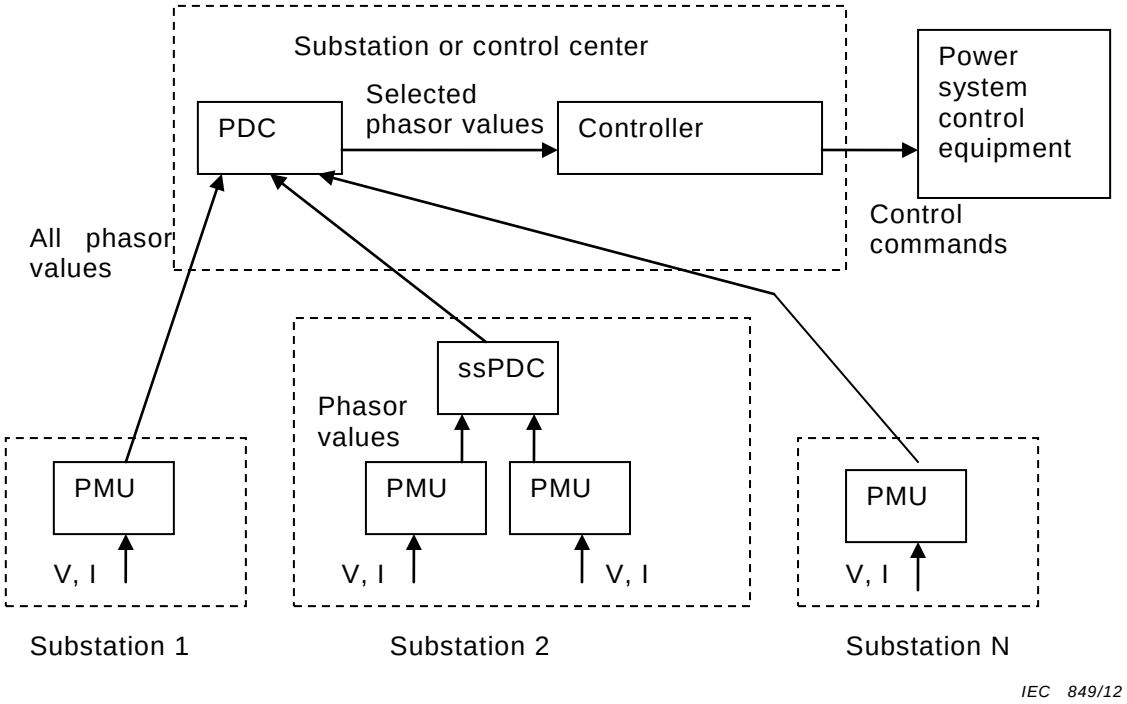


Figure 7 – Use case diagram for wide area controls

Actors:

Name	Role description
PMU	Computes synchrophasors & frequency
ssPDC	Substation Phasor Data Concentrator – collects, aligns, selects & possibly decimates data from several PMUs in the substation
PDC	Phasor Data Concentrator – collects, aligns, selects & possibly decimates data from several PMUs or other PDCs
Controller	Receive data from the local PDC & execute algorithms that implement control functions
System control equipment	Power system control elements including breakers, switches, FACTS power controllers, DC controls, and similar equipment

Operations:

Name	Service or information provided
Data sampling & phasor estimate	PMU samples current and voltage and estimates synchrophasor and frequency values
Data sending	PMU sends synchrophasor & frequency values in continuous data stream or event reporting methods
Data receiving/sending	If there is an ssPDC, the data is received in the substation, combined with data from other PMUs, and forwarded to the destination PDC
Data receiving	PDC receives data from PMU or ssPDC, combines with data from other measuring units, and sends on to a controller
Power system controls	Controllers receive data and determine actions based on data and control algorithms

Basic flow:

Data origination & sending

Use case step	Description
Step 1	PMU computes V & I synchrophasors & system frequency
Step 2	PMU selects phasors and frequency at given output rate
Step 3	PMU packages data with appropriate status and time stamp
Step 4	PMU sends data to the ssPDC or PDC or controller

Data receiving intermediate (alternate path)

Use case step	Description
Step 1	ssPDC receives synchrophasor data
Step 2	ssPDC correlates and selects output data
Step 3	ssPDC resends output data to PDC or controller

Data receiving

Use case step	Description
Step 1	PDC receives synchrophasor data
Step 2	PDC correlates and selects output data
Step 3	PDC resends output data to controller

Controller actions

Use case step	Description
Step 1	Controller receives and validates the data
Step 2	Controller executes control algorithms searching for conditions that require executing control functions
Step 3	If a situation is found that requires a control function, controller sends control command to indicated control equipment

Constraints:

Control actions must take place within a limited time. Some may need to be executed within milliseconds, and some only within seconds. The data rate and latency must support requirements of the particular control action. Control action speed will be limited by how frequently data are sent (data rate) and the time it takes to receive the data after it has been sent (latency). A wide variety of control actions can be implemented using a synchrophasor based wide area system. The following table is only an example for some control actions but by no means covers all situations. It should be used as a guideline for the higher-speed applications regarding measurement transmission rate, timetag error, latency range, and measurement timing error.

Minimum rate	Transfer time class	Time synchronization accuracy class
10/second	TT2 0,5 s	T3 0,025 ms

5.9.3 Predictive dynamic stability maintaining system

When a severe fault occurs in a loop or mesh network connecting two major power systems, an out-of-step condition can occur between the two systems. By checking for a suitable indicator that would denote the occurrence of a disturbance having a gradual onset of between 5 s to 10 s, an out-of-step condition can be detected and by subsequently splitting the system at a specific point it is possible to prevent the out-of-step occurring. The system is composed of PMUs which are used to gather information and are located at each major point of the power system; the IED enables the splitting of the power system. The IED and PMU are connected within a communication network.

Each PMU sends the voltage angle for its own part of the power system to the IED. The IED compares the angles between the PMUs and predicts the future angle. If the predicted angles between the PMUs in system A and the PMUs in system B exceed pre-determined values, the IED determines that an out-of-step condition will occur and trips the CB.

Alternative method: The IED measures the angular difference between PMUs under normal conditions. When a disturbance occurs, the change in angular difference is calculated from the generator rotor angle (speed) or from frequency deviation.

The general information flow is shown in Figure 8.

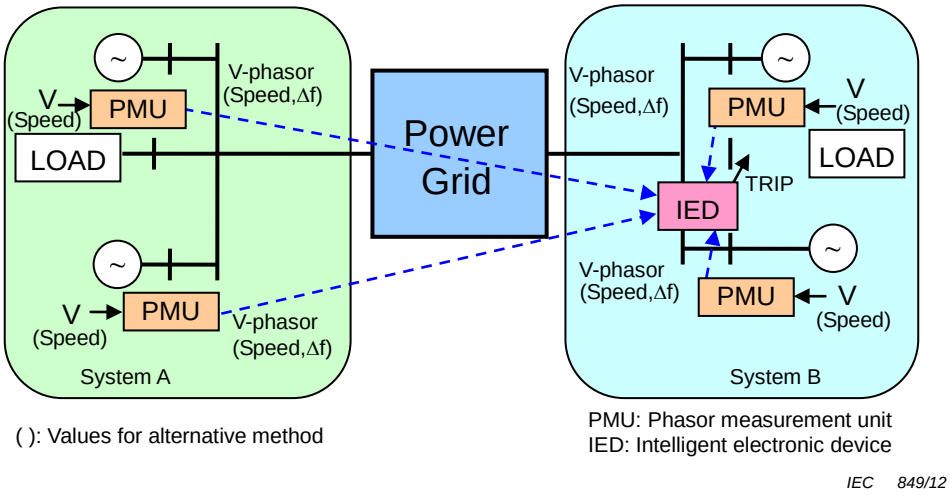


Figure 8 – Use case diagram for predictive dynamic stability

The communication requirements can be summarized as follows:

Actors:

Name	Role description
PMU	Computes synchrophasors
IED	Receives data from PMUs, predicts dynamic stability & power system control

Operations:

Name	Service or information provided
Data sampling & phasor estimate	PMU samples current and voltage and estimates synchrophasor values
Data sending & receiving	PMU sends values that are received by the IED
Power system control	The IED compares the data from all PMUs The IED is able to predict an out of step between two systems, System A and B. When an out of step is predicted, the IED determines to split a part of either system A or B in order to prevent an out of step occurring between System A and B.

Basic flow:

Data origination & sending

Use case step	Description
Step 1	PMU computes V & I synchrophasors
Step 2	PMU selects phasors at given output rate
Step 3	PMU packages data with appropriate status and time stamp
Step 4	PMU sends data to the IED

IED actions

Use case step	Description
Step 1	IED receives synchrophasor data and validates the data
Step 2	IED computes the voltage angular difference between two systems
Step 3	IED predicts the voltage angular difference between two systems 150 ms – 200 ms ahead
Step 4	If the predicted angles exceed the pre-determined values, then the IED judges that an out-of-step between two systems will occur and splits part of either system

Constraints:

Control actions must take place within a limited time. This application predicts the voltage angular difference 150 ms to 200 ms in the future. When the predicted angles exceed pre-determined values, control is executed to split part of the systems.

The requirement for communication delay (latency) time is shown in the following table with consideration being given to the output time of the IED and operation time of CBs; high reliability data communication is also required. Furthermore, high accuracy measurement is required with the maximum timing error permissible shown in the following table so that the IED compares the angles among plural PMUs

Minimum rate	Allowable communication delay (latency) time	Maximum measurement timing error
25/second @ 50 Hz 30/second @ 60 Hz	20 ms	0,05 ms

5.9.4 Under voltage load shedding

Major blackouts such as those that occurred in Tokyo and France in 1987 and those in the North American Eastern interconnections and Southern Europe in 2003 were related to voltage instability.

Since transmission reinforcements are hard to justify as solutions to voltage instability and cascading outages experienced under extreme conditions, under voltage load shedding would seem to be a suitable alternative contingency.

The example system is composed of PMUs installed at four 500 kV substations and IEDs installed at several 275 or 154/66 kV substations. The IEDs are connected to all PMUs.

One of the purposes of the IED is to detect long-term voltage collapse; this is executed at the 500 kV network level as opposed to the 275 kV or lower voltage networks which are automatically regulated by tap changing on the 500/275 kV or 154 kV transformers.

The IED affords high reliability by use of the following procedure. The IEDs detect slow types of voltage collapse, in the range of eight seconds to two minutes, by detecting unusual continuous $\Delta V/\Delta t$ values. Fast voltage collapse can also be detected using a $\Delta V/\Delta t$ calculation with a one second data window. Each IED can trip more than one line. When the IED detects a voltage collapse, it trips each line CB following expiration of an on-delay timer which can be set independently for each line. (Independent time settings are applied for each line.)

The general information flow is shown in Figure 9.

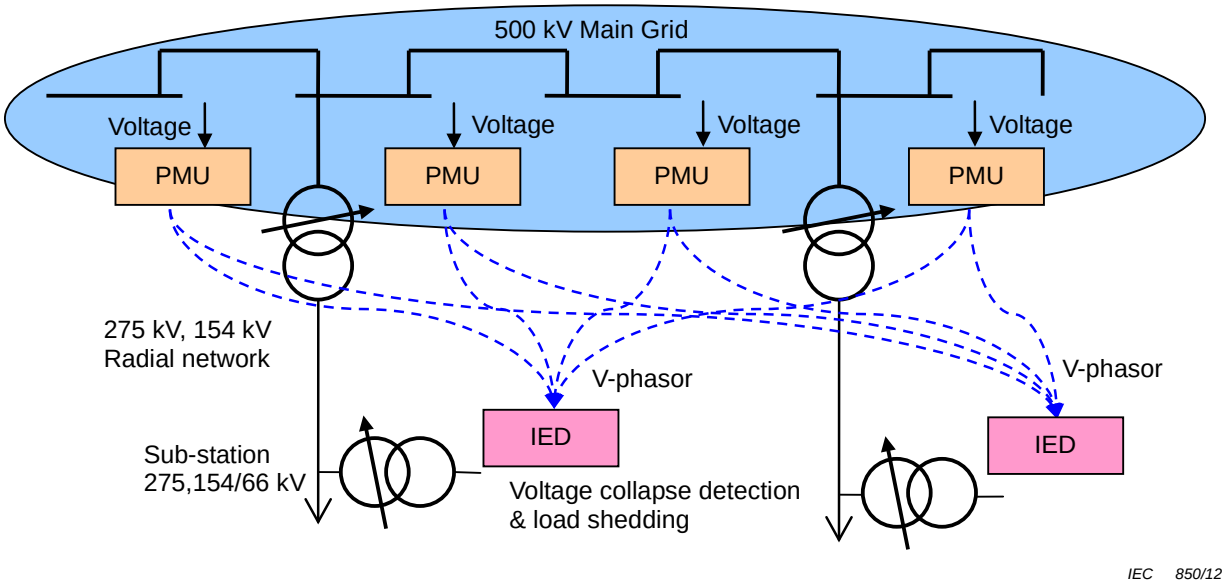


Figure 9 – Use case diagram for under voltage load shedding

The communication requirements can be summarized as follows:

Actors:

Name	Role description
PMU	Computes synchrophasors
IED	Receives data from the PMU, detects voltage collapse & power system control

Operations:

Name	Service or information provided
Data sampling & phasor estimate	PMU samples current and voltage and estimates synchrophasor values
Data sending & receiving	PMU sends values that are received by the IED
Power system control	The IED detects a voltage collapse using data from all PMUs. If the IED detects a voltage collapse, load is shed until the voltage recovers its normal state.

Basic flow:

PMU actions

Use case step	Description
Step 1	PMU computes V & I synchrophasors
Step 2	PMU selects phasors at given output rate
Step 3	PMU packages data with appropriate status and time stamp
Step 4	PMU sends data to the IED

IED actions

Use case step	Description
Step 1	IED receives synchrophasor data and validates the data
Step 2	IED calculates the ratio of the voltage drop using data from each PMU
Step 3	IED will determine that a voltage collapse has occurred, if almost all PMU ratios of voltage drop exceed the pre-determined normal voltage value
Step 4	If the IED detects a voltage collapse, load will be shed by the IED until the pre-determined normal voltage level has been recovered

Constraints:

Control actions must take place within a limited time. This application detects the trend that voltage drops are occurring simultaneously in plural substations, and sheds load successively until the pre-determined normal voltage level has been recovered. The following performance requirements have been determined by considering the period from an initial voltage drop to a volt.

Minimum rate	Allowable communication delay (latency) time	Maximum measurement timing error
25/second @ 50 Hz 30/second @ 60 Hz	100 ms	10 ms

5.9.5 Phenomenon assumption type WAMPAC

When a very severe fault occurs, such as the complete loss of an important power corridor, generators may lose synchronisation with the power network. It may also cause overload of transmission lines or transformers. Imbalance between generation and consumption can occur when a power system network is separated resulting in abnormal frequency conditions.

Phenomenon assumption type WAMPAC (Wide Area Monitoring, Protection and Control) executes generator shedding or load shedding in order to avoid these types of unstable conditions on the power system network based on a pre-fault calculation using on-line power system information.

Phenomenon assumption type WAMPAC is composed of data collecting Terminal Equipment (PMU_M: PMU class M), collecting and Triggering Terminal Equipment (PMU_P: PMU class P), Controller Terminal Unit (IED) and Central Equipment (CE). PMU_M is located at the main substation and the power station. PMU_P is located at the substation in which the detection of the faults predicted (such as line faults) is possible. IED units are located at power stations in which the generators to be shed are located. PDC and CE are typically located in a central control centre where on-line power system information from PMU_M and PMU_P can be obtained.

The general information flow is shown in Figure 10.

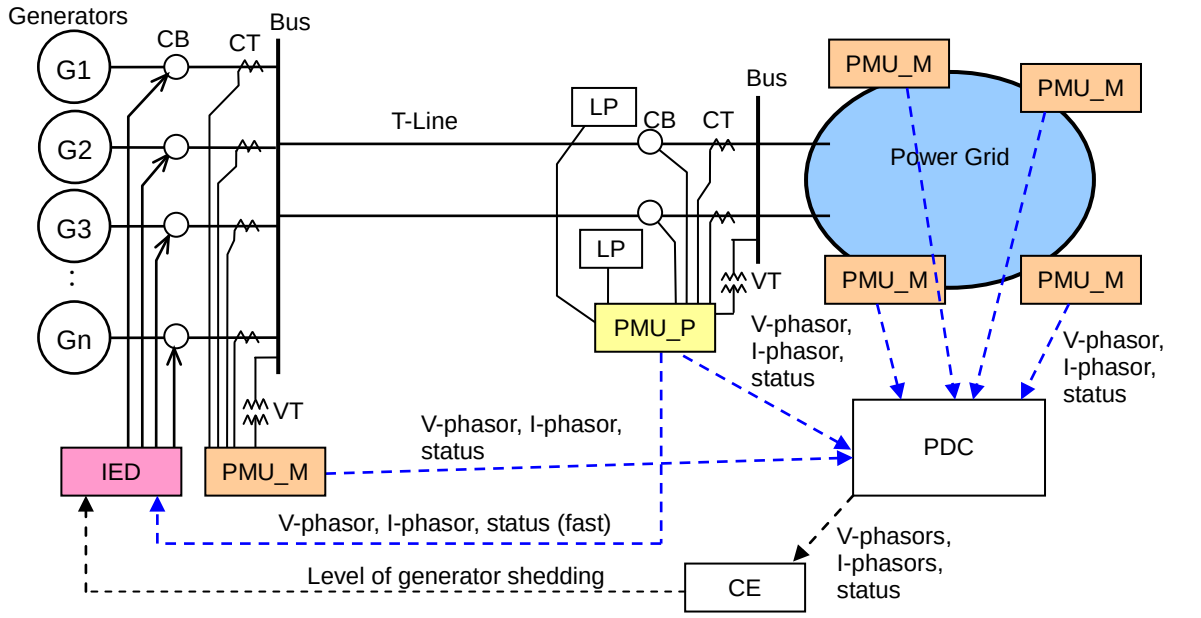


Figure 10 – Use case diagram for WAMPAC

The operating procedure for each equipment type is described as follows:

CE retrieves the operational status of the power system, i.e. connections and topology, etc. and V and I from PMU_M and PMU_P via the PDC in the form of on-line power system information. A power system model representing the current status and the distribution of the flow of power on the grid is generated in CE for analysis from the on-line power system information and stored as system facility data. A transient stability calculation is undertaken for the assumed fault cases using the power system model, and the transient stability is checked for each case. The level of generator shedding required to maintain stability is then calculated. The result is summarised in a tabular format and sent to the IED. CE repeats this process every few tens of seconds. PMU_P detects faults within the power system from information gathered from the operation of protection relays, change of CB status and sends the information to the IED.

Under normal conditions, PMU_P and PMU-M measure V and I and obtain the status of the circuit breakers and line disconnectors, and this information is sent to the PDC. Periodically, the IED detects changes in the information measured by PMU_P which is stored in a tabular format in CE. It contains information identifying which generators are to be tripped to maintain stability for the severe faults predicted.

The communication requirements can be summarized as follows:

Actors:

Name	Role description
PMU	Computes synchrophasors & frequency
PDC	Phasor Data Concentrator collects the computed data from PMUs, and sends power system data to CE
CE	CE estimates the power system state, and selects the target power system primary equipment to be controlled in order to maintain stability for a specific fault, the result of the calculation is transmitted to the IED.
IED	IED receives a list of the power equipment to be controlled for potential specific faults. IED receives notification of a fault occurrence from PMU class P and compares the fault information and the list, the IED transmits a control command to the power equipment to be controlled.

Operations:

Name	Service or information provided
Data sampling & phasor estimate	PMU samples current and voltage and estimates synchrophasor values
Data sending & receiving	Data in PMU is transmitted to PDC Data in PMU class P is transmitted to IED
State estimation	State estimator combines Synchrophasor and SCADA data which are utilized for an estimation of the system status
Creating a list for control table	Based upon the estimation of power system conditions, a list of the power system equipment to be controlled is created that will be used to stabilize the power system in response to specific faults
Power system control	IED compares the list with the actual fault and executes power system control

Basic flow:

Data origination & sending

Use case step	Description
Step 1	PMU computes V & I synchrophasors
Step 2	PMU selects phasors at given output rate
Step 3	PMU packages data with appropriate status and time stamp
Step 4	PMU sends data to the PDC or IED

PDC actions

Use case step	Description
Step 1	PDC receives synchrophasor data
Step 2	PDC correlates and selects output data
Step 3	PDC resends output data to CE

CE actions

Use case step	Description
Step 1	State estimator receives Synchrophasor and SCADA data which are utilized for an estimation of the system status
Step 2	CE calculates the power equipment to be controlled in order to stabilize the power system in respect to t possible specific faults
Step 3	The specific faults and the power equipment to be controlled are listed and transmitted to the IED

IED actions

Use case step	Description
Step 1	IED normally receives and updates a list of the power system equipment to be controlled
Step 2	IED receives fault information from PMUs class P
Step 3	The actual fault information and the list are compared and the relevant power equipment is controlled accordingly

Constraints:

Control actions must take place within a limited time. This application consists of two stages. One is a state estimation and security assessment (PMU to PDC/CE), and the other is a system control as typified in SPS/RAS (PMU to IED). The requirement for “PMU to PDC/CE” and “PMU to IED” is almost the same as those in Subclauses 5.6 and 5.8 respectively. The time constraints for the communication between the IED and PMUs, which have the capability of detecting faults and controlling power equipment, are severe as shown in the following table.

Objects	Minimum rate	Allowable communication delay (latency) time	Maximum measurement timing error
PMU to PDC/CE	1/second to 10/second	5 s	0,05 ms
PMU to IED	50/second @ 50 Hz 60/second @ 60 Hz	20 ms	0,05 ms

5.9.6 Phasor Data Concentrator (PDC)

The Phasor Data Concentrator (PDC) function receives or subscribes to phasor data streams from one or more PMUs and/or other PDCs. The primary purpose of the PDC is to assemble one or more new output data streams from these input data streams. By combining phasor data from many sources into one or a few merged streams, the PDC enables transport of data from many individual PMU sources using a limited number of communications paths and/or or paths of limited data capacity. A PDC can also publish a single phasor data stream for subscription by client functions described in use cases below, including situational awareness, state estimation, on-line security assessment, display, data processing, alarming, archiving, and wide area control. With this PDC function at the input, these subscribing application functions do not require communications connections or management for a long list of individual PMU sources.

The functions within the PDC function that are needed to accomplish this merging are:

a) selection of particular values from input streams;

b) validation of input values, including data presence, test mode, and quality;

c) aggregation of values from input streams to create one or more output streams;

d) decimation or interpolation of input value streams to allow aggregation of data with different sampling rates;

e) time alignment of input values from different streams;

f) protocol conversion in either direction between the IEC 61850-90-5 protocol as specified in other clauses of this document, and the communications protocol formats of IEEE C37.118-2005, C37.118.2-2011, IEEE 1344, or other specified transport protocols;

g) security implementation – authentication and/or encryption for input or output streams;

h) calculation or scaling of derived values from input values, for insertion in an output stream (e.g. insert phase shift, or compute phase angle between input locations).

Functions a) to c) in this list are essential for any PDC. Functions d) and e) are core functions within the PDC function, but may not be needed in every application, and thus may be configured as ‘off’ in a particular case. Functions f) to h) are functions that need not be present in every PDC application; if included, these functions may also be configured as ‘off’.

While the PDC function list is typically provided in one physical equipment unit, some of the functions it performs might also be carried out in other units elsewhere in the system configuration – especially functions f) to h).

By performing communications protocol conversions per f), the PDC enables the integration of legacy data sources or user applications with communications systems based on IEC/TR 61850-90-5 or on other protocols, such as IEEE C37.118-2005. This conversion function thus supports migration towards exclusive use of IEC/TR 61850-90-5.

The use case diagram below shows how a PDC may publish more than one output stream. Furthermore, each output stream may have unique identification, synchrophasor data points listing, sampling rate, communications protocol, or security features configuration.

In the use case diagram and following description, as well as other use cases, show a Substation Phasor Data Concentrator (ssPDC) as a distinct functional entity. ssPDC is described in 6.4.2, as opposed to a PDC at a higher level of the hierarchy as described in 6.4.3. However, the ssPDC is just a specific instance of a PDC and may have any of the eight functions listed above included and enabled.

The general information flow is shown in Figure 11.

Use case diagram

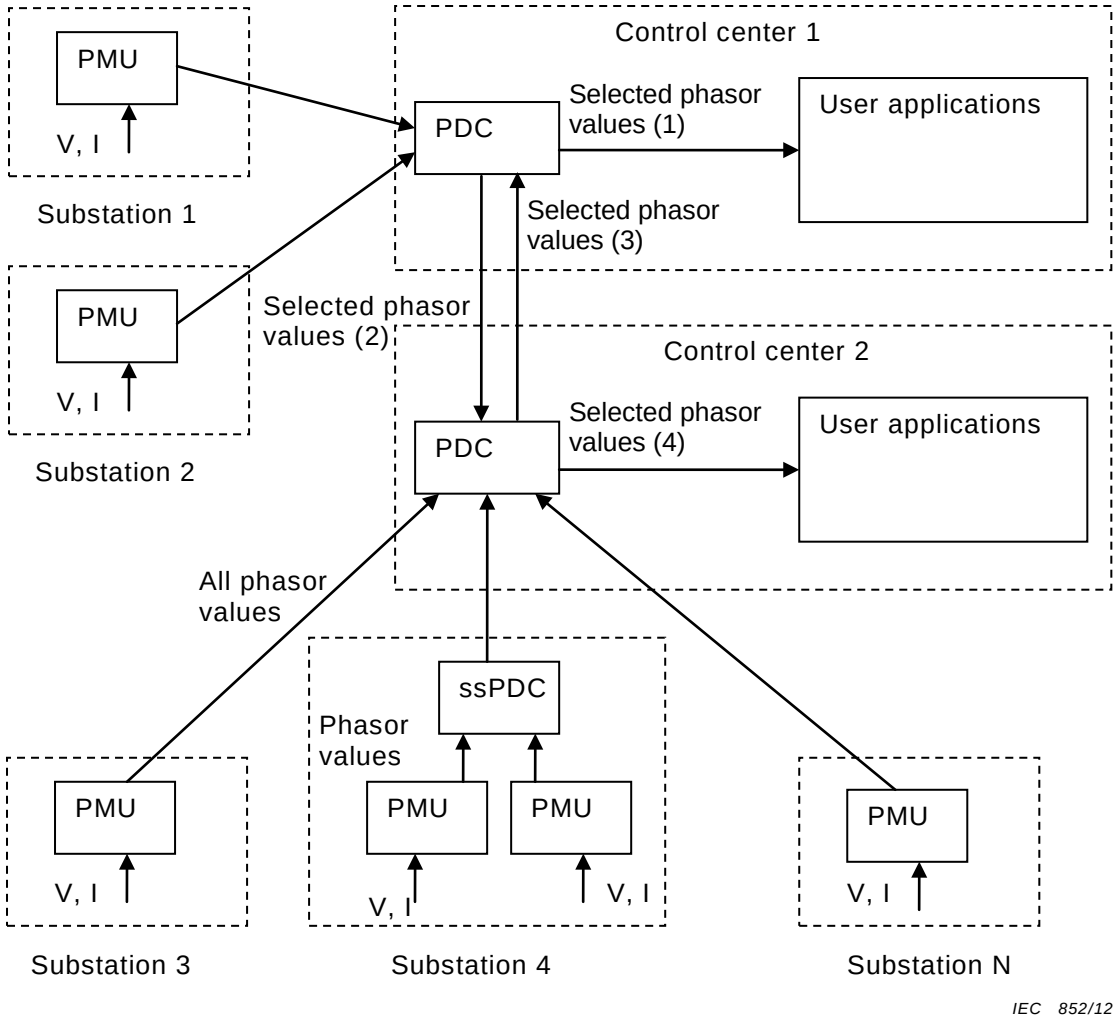


Figure 11 – Use case diagram for phasor data concentrator

Actors:

Name	Role description
PMU	Computes synchrophasor values, frequency, rate of change of frequency, and attaches related measurement and status points in a repetitive stream of output data messages in IEC/TR 61850-90-5 format as specified below, IEEE C37.118.2 format, or other message packet format.
ssPDC	Substation Phasor Data Concentrator - selects, validates, aggregates, and optionally decimates, interpolates, or time aligns data from multiple PMUs in the substation. Optionally converts data to and from IEC/TR 61850-90-5 as required by communications connections, secures data transfer, and calculates or scales derived data values. Special instance of PDC
PDC	Phasor Data Concentrator - selects, validates, aggregates, and optionally decimates, interpolates, or time aligns data from multiple PMUs or PDCs. Optionally converts data to and from IEC/TR 61850-90-5 as required by communications connections, secures data transfer, and calculates or scales derived data values
User applications	Receive collected data from the local PDC & perform various client functions listed in use cases below

Operations:

Name	Service or information provided
Data sampling & phasor estimate	PMU samples input values and computes synchrophasor values, frequency, and rate of change of frequency. PMU attaches related measurement and status points
Data origination & sending	PMU sends a repetitive stream of output data messages in IEC/TR 61850-90-5 format as specified below, IEEE C37.118.2 format, or other message packet format
Data receiving/sending	An ssPDC receives data from within the substation, combines it with data from other PMUs, and forwards merged output stream to the next destination PDC. A PDC receives data from PMUs, ssPDCs, or other PDCs. It selects, validates, aggregates, and optionally decimates, interpolates, or time aligns data from multiple PMUs or PDCs. Optionally it converts data to and from IEC/TR 61850-90-5 as required by communications connections, secures data transfer, and calculates or scales derived data values
Data receiving	A PDC receives data from PMUs, ssPDCs, or other PDCs. It selects, validates, aggregates, and optionally decimates, interpolates, time aligns data, or calculates or scales derived values from multiple PMUs or PDCs. PDC sends output streams to user applications
Data receiving – test mode	One or more input data streams are indicating test mode
Data sending – test mode	One or more output data streams are to be set to indicate test mode
Commissioning	PDC is turned on for the first time, or for the first time with a new configuration
Input change	The configuration of an input stream changes in a way that requires reconfiguration of an output stream
Input failure	PDC stops receiving one or more connected or subscribed data streams completely, or values of input stream have bad quality
Deenergization/energization or fail/replace	PDC is turned off for an arbitrary period and turned back on. Replacement of failed PDC by identically configured unit may occur during time off line. Consider effect of 1 min change flag in IEEE C37.118.2
Data receiving - user applications	Applications provide situational awareness, state estimation, on-line security assessment, display, data processing, alarming, archiving, wide area control, and specific protection or control functions

Basic flow:

Data origination & sending

Use case step	Description
Step 1	PMU measures V & I synchrophasors, power flows, frequency, rate of change of frequency, and other measurement and status points
Step 2	PMU computes data set at configured output rate
Step 3	PMU packages data set with appropriate status flags and time stamp
Step 4	PMU sends data sets to the ssPDC or PDC in a continuous stream and configured data communications protocol

Data receiving/sending – ssPDC

Use case step	Description
Step 1	ssPDC receives synchrophasor data streams from multiple PMU sources
Step 2	ssPDC converts communications protocol of each data input
Step 3	ssPDC validates, selects, combines, and merges data points into output stream
Step 4	ssPDC formats, secures, and sends output data to PDC

Data receiving/sending – PDC

Use case step	Description
Step 1	PDC receives synchrophasor data from multiple PMU, ssPDC, or PDC sources
Step 2	PDC converts communications protocol of each data input
Step 3	PDC validates, aligns, decimates or interpolates data inputs, computes or scales data values, and selects output data for each of multiple output streams
Step 4	PDC formats, secures, and publishes or sends one or more output data streams

Data receiving – test mode

Use case step	Description
Step 1	PDC or ssPDC receives synchrophasor data from multiple PMU, ssPDC, or PDC sources
Step 2	PDC converts communications protocol of each data input
Step 3	PDC determines test mode value for each dataset in each input stream
Step 4	PDC validates, aligns, decimates or interpolates data inputs, calculates or scales values in consideration of test modes, and selects output data for each of multiple output streams
Step 5	PDC maps test mode values as configured to each dataset in each output stream.
Step 6	PDC formats, secures, and publishes or sends one or more output data streams

Data sending – test mode

Use case step	Description
Step 1	PDC receives synchrophasor data from multiple PMU, ssPDC, or PDC sources
Step 2	ssPDC converts communications protocol of each data input
Step 3	ssPDC validates, aligns, decimates or interpolates data inputs, calculates or scales values, and selects output data for each of multiple output streams
Step 4	PDC maps local test mode value to each dataset in each output stream
Step 5	PDC formats, secures, and publishes or sends one or more output data streams

Commissioning

Use case step	Description
Step 1	PDC is configured while off line
Step 2	PDC is energized and applies current input configuration
Step 3	PDC converts communications protocol of each data input
Step 4	PDC validates configuration and ConfRev of each input
Step 5	PDC commences receiving/sending with test modes as selected in PDC or inputs, and with appropriate ConfRev

Input change

Use case step	Description
Step 1	PDC detects change of configuration and ConfRev of each input. A change may be an expected event in an intentional local or wide area updating process, or may be due to a configuration error
Step 2	PDC marks bad quality for changed output data, and inserts null data if source data cannot be identified
Step 3	PDC generates local alarm output until its configuration is updated to recognize new ConfRev of inputs

Input failure

Use case step	Description
Step 1	One or multiple received or subscribed input streams ceases
Step 2	PDC maps bad quality indications to appropriate output message status objects
Step 3	PDC inserts null values as required in output streams
Step 4	PDC generates local alarm output until input stream is restored

Deenergization/reenergization or fail/replace

Use case step	Description
Step 1	PDC is deenergized
Step 2	PDC is reenergized.
Step 3	PDC validates that its own configuration has not changed
Step 4	PDC converts communications protocol of each data input
Step 5	PDC validates configuration and ConfRev of each input
Step 6	PDC commences receiving/sending with test modes as selected in PDC or inputs, and with appropriate ConfRev. Consider effect of one minute change flag in IEEE C37.118.2.

Data receiving – user applications

Use case step	Description
Step 1	User application receives or subscribes to data stream from PDC
Step 2	User application processes synchrophasor data according to specific use cases for respective applications
Step 3	User application processes test modes and quality values in data stream from PDC to yield appropriate outputs or constrained behavior

Constraints:

Synchrophasor measurements can be communicated to and from PDCs at a variety of sampling rates from once every number of minutes to 100 or 120 measurements per second. The measurements may conform to standards such as IEEE C37.118-2005, C37.118.1-2011, or IEC/IEEE 60255-118-1. PDCs are connected in hierarchical architectures in which transfer time delays may accumulate as values pass to applications. The following table presents minimum requirements. The user application installer must ensure that individual PMU delays and errors, as well as the accumulated delays and errors for a sequence of PDCs, are compatible with the requirements of the application. Note that PDCs should be designed not to degrade the accuracy of time stamps applied at the PMU, or the time synchronization accuracy class.

Requirement	Performance class	Transfer time class	Time synchronization accuracy class
Delay acceptable for protection functions	P13	TT6 < 3 ms	T3 < 0,025 ms
Delay acceptable for other functions	P14	TT5 < 10 ms	T3 < 0,025 ms

6 Modelling considerations

6.1 General

To describe a system in IEC 61850, each client and server needs to be modelled as a logical node on some IED. In the case of substation internal synchrophasor applications, probably existing logical nodes can be used, like RSYN for the synchrocheck function and PPAM for generator out-of-step protection. In case that the application itself is outside the IEC 61850 scope, e.g. for pure monitoring and archiving purpose, the ITMI, IHMI or IARC logical nodes can be used. In case any controls are done with classical client server services like Operate, the ITCI logical node can be used as for a network control center. However, there are some wide area control and frequency stability applications, where controls must be given in a time scale for which the classical Operate method might be too slow, so that UDP based GOOSE needs to be used. In this case, a logical node is needed which is able to produce data which can be packed into a GOOSE (command) message. The current IEC 61850-7-4 foresees for this purpose the GAPC logical node. However, to support a better semantic description, e.g. for automated engineering, it might be worthwhile to introduce e.g. generic WAC logical node (e.g. GWAC or CWAN) and a generic WAP logical node (e.g. GWAP or PWAN). In special cases, even the definition of application specific logical nodes might be worthwhile. This needs a more detailed analysis of function implementation and needs to be decided later on a per application base.

A basic logical node based architecture is illustrated in Figure 12.

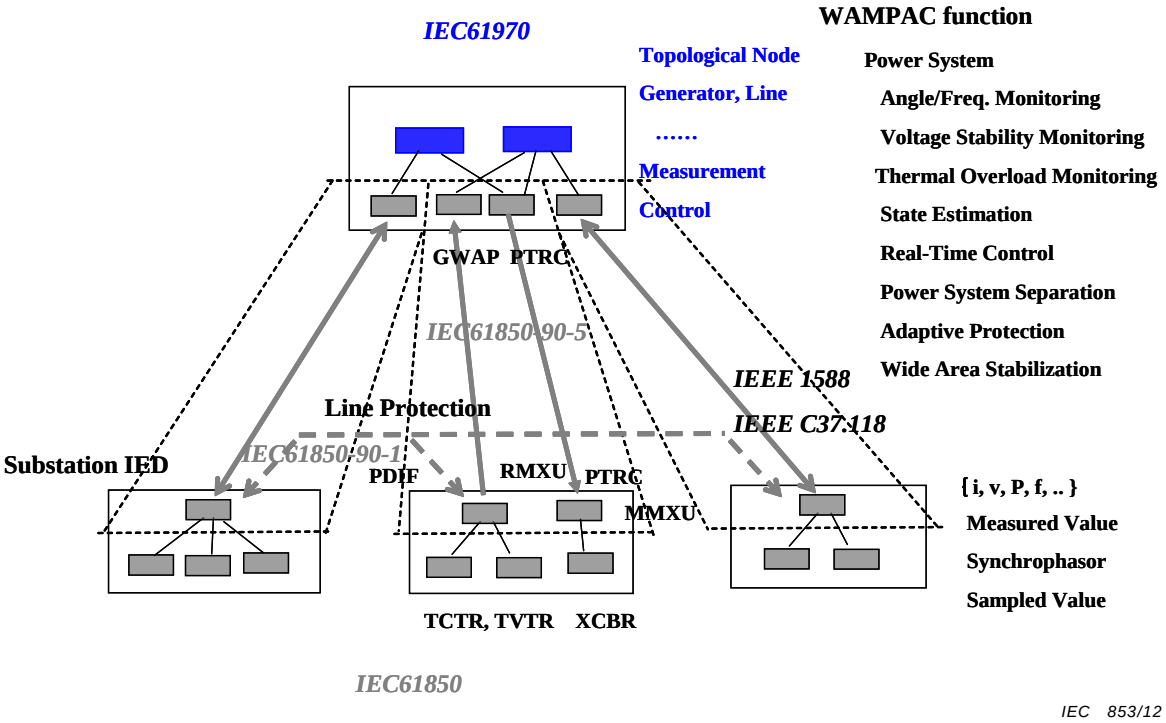


Figure 12 – Basic IEC 61850 model of WAMPAC functions

The following subclauses provide modelling guidance for synchrophasor based devices including PMUs and PDCs.

6.2 System hierarchy

Protection, monitoring and control systems that use synchrophasors are complex hierarchical systems with PMUs at the bottom of the hierarchy and PDCs at the different levels of the hierarchy as shown in Figure 13.

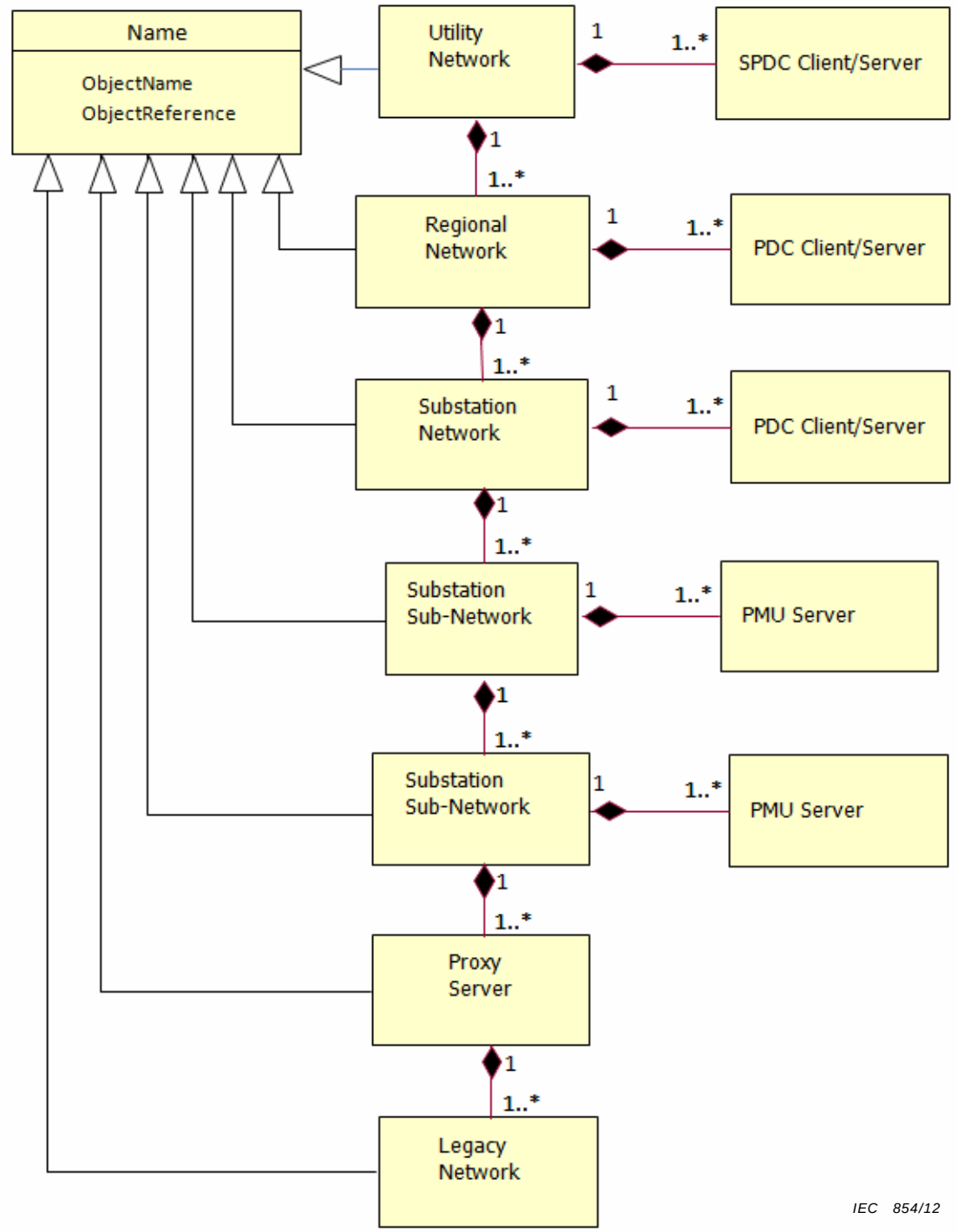


Figure 13 – System hierarchy

6.3 PMU model

The PMU is a function within an IED which is responsible for the calculation and publishing of synchrophasor measurements as defined in IEEE C37.118.1.

These calculations are based on sampled values produced by the analog input module within the IED containing the PMU function or based on streaming sampled values produced by one or more merging units in the substation that the IED containing the PMU function is subscribing to.

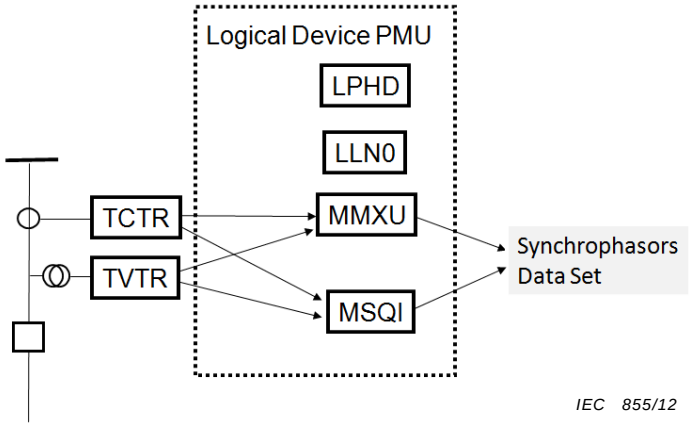


Figure 14 – PMU object model

If the PMU is publishing phase currents and voltages, one or more instances of MMXU will be used as shown in Figure 14.

If the PMU is publishing sequence currents and voltages, one or more instances of MSQI will be used.

6.4 Phasor Data Concentrators (PDCs)

6.4.1 General

There are several recognized deployment options for PDCs: Substation and Regional. The following subclauses give guidance of the modelling of these entities.

6.4.2 Substation PDC model

The substation Phasor Data Concentrator (PDC) is a function that receives over the substation LAN data from multiple PMUs in the substation. The received data are sorted by their time-tags and provided to other applications to use them. If necessary, the PDC may need to perform re-sampling in order to align measurements from devices using different publishing rates.

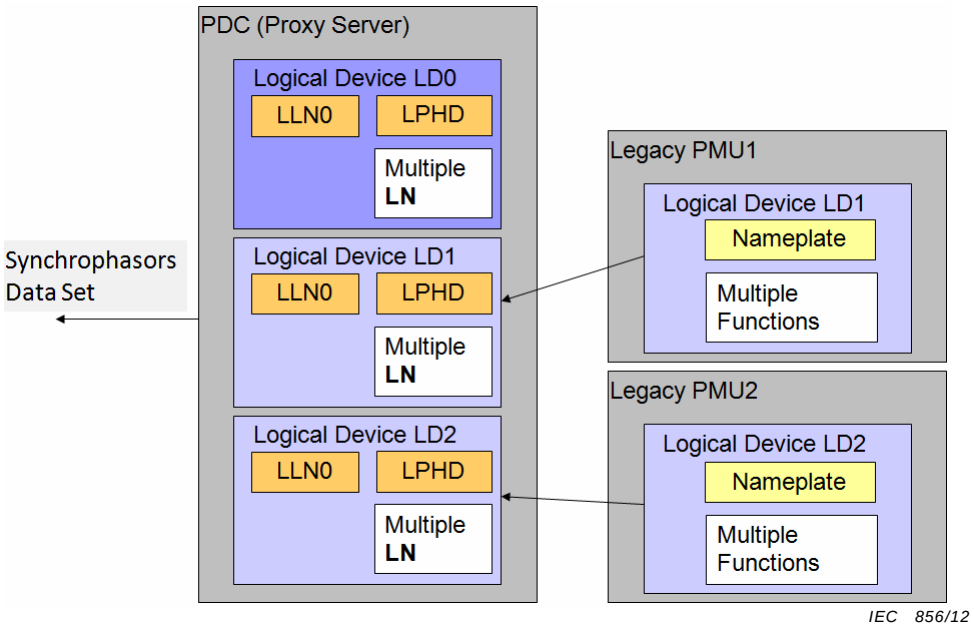


Figure 15 – Substation PDC model with legacy PMUs

A data set containing a representative set of data as required by the upper levels of the system hierarchy is created and published over a wide area interface using UDP multicast.

It is recommended to model the PDC function as a PDC logical device with the Proxy data object in logical node LPHD *Proxy* set to *True*.

The PDC model is based on the nesting of logical devices as defined in IEC 61850-7-1. An example of a possible hierarchy is shown in Figure 15.

6.4.3 Regional or system level PDC

The Regional level Phasor Data Concentrator (PDC) is a function that receives over the wide area network data from multiple PDCs in different substations. The received data are sorted by their time-tags and provided to other applications to use them. If necessary, the PDC may need to perform re-sampling in order to align measurements from devices using different publishing rates.

A data set containing a representative set of data as required by the upper levels of the system hierarchy is created and published over a wide area interface using UDP multicast.

It is recommended to model the PDC function as a PDC logical device with the Proxy data object in logical node LPHD *Proxy* set to *True*.

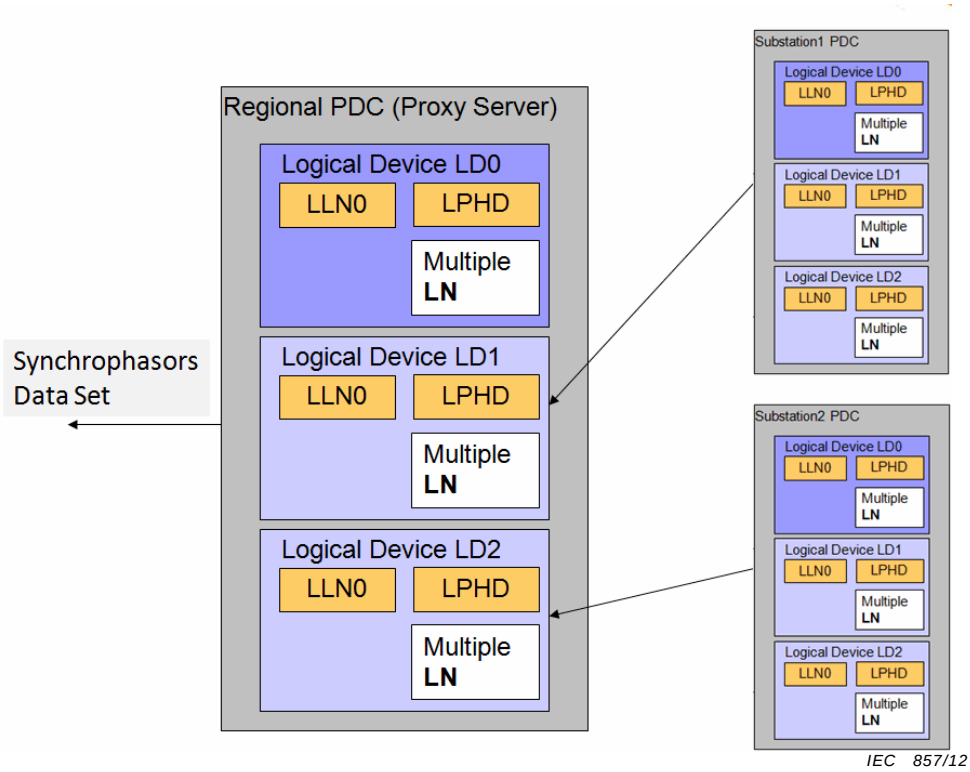


Figure 16 – Regional PDC object model

The Regional PDC model, shown in Figure 16, is based on the nesting of logical devices defined in IEC 61850-7-1.

6.4.4 Quality

Data that have been re-sampled or interpolated shall set their “substituted” quality bit set.

7 Communication requirements

7.1 General

The communication mechanisms laid out in this document shall serve the needs for Wide Area Monitoring, Protection, and Control (WAMPAC) applications utilizing synchrophasors measured according to IEEE C37.118.1.

The fast cyclic communication within the substation in IEC 61850 will typically be based on the sampled value (SV) service, while additional event data can be communicated with GOOSE or by reporting, dependent on its time criticality. Communication to receivers outside a substation can be done either by tunnelling the SV service across some high speed communication network like SDH or SONET, or via IP networks, if their communication delays and delay jitter are acceptable by the application. For the second purpose, the current IEC 61850 has to be enhanced by a mapping of samples and GOOSE messages onto an IP based protocol. Due to the basically periodic nature of these services, UDP with multicast addressing is the transport protocol chosen for this purpose. In the following it is assumed that this new mapping of the SV service will be based on routable UDP, and therefore shortly be called R-SV.

The use of tunnelling Ethernet level messages across some other high speed medium is already described in IEC/TR 61850-90-1. From an engineering point of view, this is similar to engineering within a substation, with additional use of SED files to exchange the phasor related interface definitions between the different substation projects and the center project(s).

The source of periodic data like synchrophasors to be sent across a wide area communication system can reside in an IED near the switch yard, or in a gateway from the substation to the WAN, like a PDC. In the case that R-SV data sources reside within the substation instead of only at its WAN boundary (like a PDC), these sources shall be the only ones visible for engineering of the wide area communication connections. This can be handled from an engineering point of view like the tunnelling of SV services across the WAN, i.e. by exchange of interface definition files (SED) between the source LAN project containing these R-SV sources and the destination LAN project at the other side of the WAN. It is up to this destination project to decide how far routers at the WAN border shall be contained in the system interface exchange description (SED file). This mechanism is called ‘direct connection’ (with or without tunnelling).

Another approach often used for synchrophasors is to assemble different phasor sources into one telegram with synchronised phasor data, possibly even with resampling of the data. This is done by a phasor data concentrator (PDC), which acts like a gateway from different sources of phasor data streams to several sinks, most probably all needing the same now synchronized phasor information (see also 5.6). Such a phasor concentrator acts from an IEC 61850 perspective like a gateway with data selection and possibly a filtering function, however with the additional functionality to forward all received phasor data synchronised and resampled into one telegram to several intended destinations.

7.2 Direct connection with tunnelling or R-SV service

Engineering-wise the interface definitions from several systems to a higher level system have to be defined (e.g. use case in 5.6). For direct connections, these interface descriptions are extracts from the internal interfaces in the source systems. A concrete example is given in Figure 17.

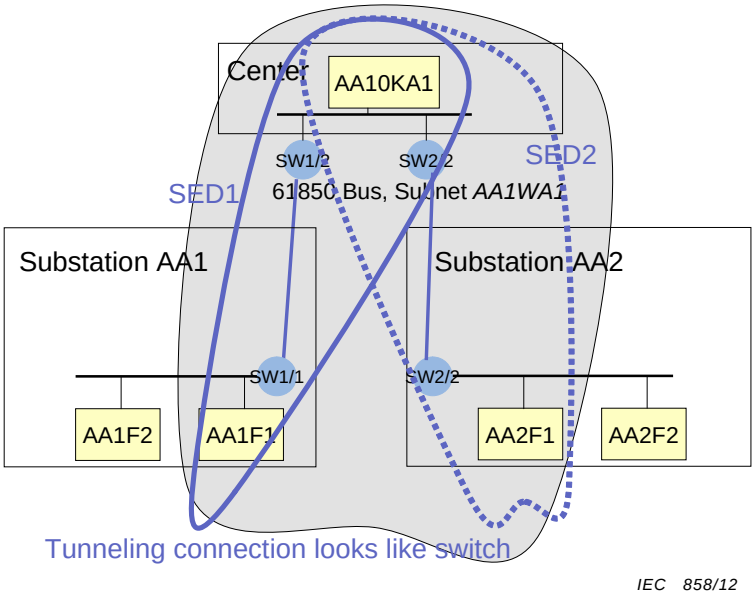


Figure 17 – Synchrophasor communication modelling for direct connection

Figure 17 shows two substations AA1 and AA2, each having a protection device or PMU providing synchrophasor data, namely IED AA1F1 in AA1, and AA2F1 in AA2. To engineer the data flow to the center IED AA10KA1 in the center project, the SED1 file is exchanged between the AA1 project and the center project, and the SED2 interface file is exchanged between the AA2 project and the center project. The result is the center project containing the center IED AA10KA1 as well as the PMUs AA1F1 and AA2F1 (grey area in Figure 17).

For complete engineering, the following should be considered:

- If tunnelling is used, the two interfacing devices SW1/1 and SW1/2 (resp. SW2/1 and SW2/2) look like they provide different ports of the same switch, hiding the tunnel connection (thick blue connecting line between them). In the case of R-SV, these may be routers instead, which could be modelled in the SCD and SED files, if needed.
- The semantics of incoming signals can be kept in data objects of CDC ORG, containing the object reference of the incoming signal source.
- If the SubNetwork identifications within all projects are identical, then the SED files can be directly imported, else the SubNetwork name in the imported SED file has to be adapted before import.
- As the names of the IEDs in the center project must be unique, these should be harmonized across all projects. By using project specific substation designations (e.g. AA1, AA2 in the example) this is automatically fulfilled.
- The semantic related to the power system can be exchanged by keeping the relevant substation parts in the SED files. Again this needs either harmonized power network naming or an appropriate renaming of the substation section elements before import.
- Non-IED related naming is required by many synchrophasor deployments. Therefore, based upon IEC 61850-6, the “ldname” attribute of tLDevice production should be utilized.

More details about the usage of SED files and exchange of engineering rights for this purpose is described in IEC 61850-6:2009.

7.3 The gateway approach

If reduction of connections and synchronised sending of several phasor streams in one message is important, the Phasor Data Concentrator concept comes into play. The PDC device is a client to phasor streams from the PMUs' respective substations, as described for the center IED in 5.6. Further, the PDC might make a protocol translation from substation internal SV service or from C37.118.2 to R-SV service across the WAN.

The PDC approach is illustrated in Figure 18. The PDC AA10TH1 concentrates phasor data streams coming from AA1F1 and AA10F1. The names shall indicate that AA10F1 is a PMU in the same project as AA10TH1 (and possibly even AA10KA1), while the interface to AA1F1 is imported by means of a SED file e.g. as described in 7.2. The solid line ellipse indicates the IEDs which belong to the PDC project, while the dotted ellipse contains the IEDs relevant for the center project. The PDC AA10TH1 is the common connection between them.

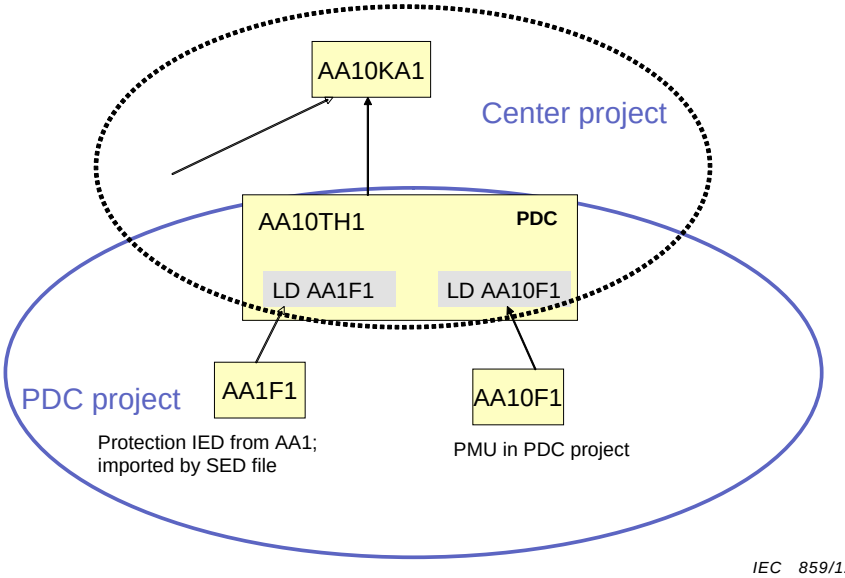


Figure 18 – PDC as phasor concentrator and (proxy) gateway

The engineering of the PDC concerning communication has two sides:

- The PDC is a client to several synchrophasor data streams. The synchrophasor data, provided in the streams, can be provided by different protocols (e.g. IEEE C37.118.2, IEC 61850, and others). This asynchronously delivered data needs to be synchronized and forwarded. If the data is coming directly from substations, this is handled as described in 7.2 for the direct communication. If it is coming from PMUs or other PDCs, this is handled like a normal IEC 61850 project, i.e. ICD and IID files of PMUs and PDCs are needed. In some cases, the PDC may need to provide protocol translation. Within the scope of this document, such translation is considered to be to IEC 61850, and thus the PDC acts like a gateway, being an IEC 61850 device described with an IID file.

- The PDC acts as a server to higher level clients/subscribers. In this view, the PDC is a ‘normal’ IEC 61850 IED in the center project, and is handled together with the client and probably other PDCs and PMUs like a normal IEC 61850 IED.In particular, it needs a formal description in the form of an IID file.

The special point for gateways in general and the PDC in this case is how to come from the step 1 input to the IID file of the PDC needed in step 2 as input for higher level system engineering. As this is from the IEC 61850 perspective IED engineering, it is particular to the implementation/tool of the gateway (PDC). However, as the data semantics, including the connection to the power system, shall be preserved during the engineering, there are recommendations for the gateway engineering, especially those gateways whose primary functionality is not concerned with data concentration but rather with filtering and message bundling.

Recommended rules for creation of PDC IID file:

- Map all LDs of lower level (source) IEDs, whose data shall be forwarded, as Proxy LDs. Optional data objects not needed may be removed.
- Name the proxy LDs according to the source IED, e.g. proxy LD name:= Source IED name + Source LD name (note LD name length restrictions!). Do not forget to state the IED name in the Proxy-LPHD.PhyNam data object.
- Take over all substation sections from the source SED SCD files to which data source LNs are mapped, and replace the link to the source IED logical node by a link to the PDC proxy LD logical node.

7.4 Requirement summary

The requirements for communication of synchrophasor data follow from the applications they serve. These requirements include the rate at which the measurements are sent, the amount of delay from measurement to application, variation in delay (jitter), and the reliability with which they are delivered. The accuracy and precision of the measurement as well as the instrument processing delays are also application requirements, but they are PMU functions and are not addressed in this document.

The following table summarizes the requirements outlined in Clause 5. Columns have been added for sensitivity to transmission jitter, lost data packets, and if the required service is currently covered in IEC 61850 services. The first 3 columns are derived directly from the individual use cases. The jitter and lost packet columns indicate qualitative sensitivity based on the expected operation of the application. The actual requirements will depend on the details of the application and will need to be assessed in each individual case. In this table, jitter is understood to be less than the time interval between successive samples.

Factor		Reporting rate range	End-to-end latency	Measurement timing error	Sensitivity to transmission jitter	Sensitivity to lost packets	Currently covered in 61850
Sync-check		≥ 4/s	100 ms	50 μs	Medium	High	SV service
Adaptive relaying		≥ 10/s	50 ms	50 μs	Low	Medium	SV service
Out-of-step protection		≥ 10/s	50 ms to 500 ms	50 μs	Medium	Medium	SV service
Situational awareness		1/s to 50/s	5 s	50 μs	Low to medium	Low to medium	Periodic reporting, SV service
State-estimation & security assessment		1/300 s to 10/s	5 s	50 μs	Low	Medium	Periodic reporting, SV service
Data archiving		Any	N/A	50 μs	Low	Medium	All as needed
Wide area controls		≥ 10/s	50 ms to 500 ms	50 μs	Medium	High	SV service
Predictive dynamic stability maintaining system		≥ 25/s or 30/s	50 ms	50 μs	Medium	High	SV service
Under voltage load shedding		≥ 25/s or 30/s	100 ms	50 μs	Low	High	SV service
Phenomenon assumption type WAMPAC	PMU to PDC	1/s to 10/s	5 s	50 μs	Low to medium	Low to Medium	Periodic reporting, SV service
	PMU to IED	50/s or 60/s	20 ms	50 μs	Medium	High	SV service

As can be seen, the SV service covers in principle all applications. However, due to its direct mapping to Ethernet, it is not usable across wide area communication systems. Here is where the R-SV mapping can be used. R-SV does not cover the most stringent requirements for sampled values as needed for classical protection. However, it can be used for the application requirements listed above in most cases. Figure 19 gives a rough overview of this. The ‘Sampled value’ range needs the SV service directly mapped to Ethernet, and the ‘Rms’ range is covered with event based or periodic reporting. The UDP based R-SV service roughly covers the ‘Phasor’ range.

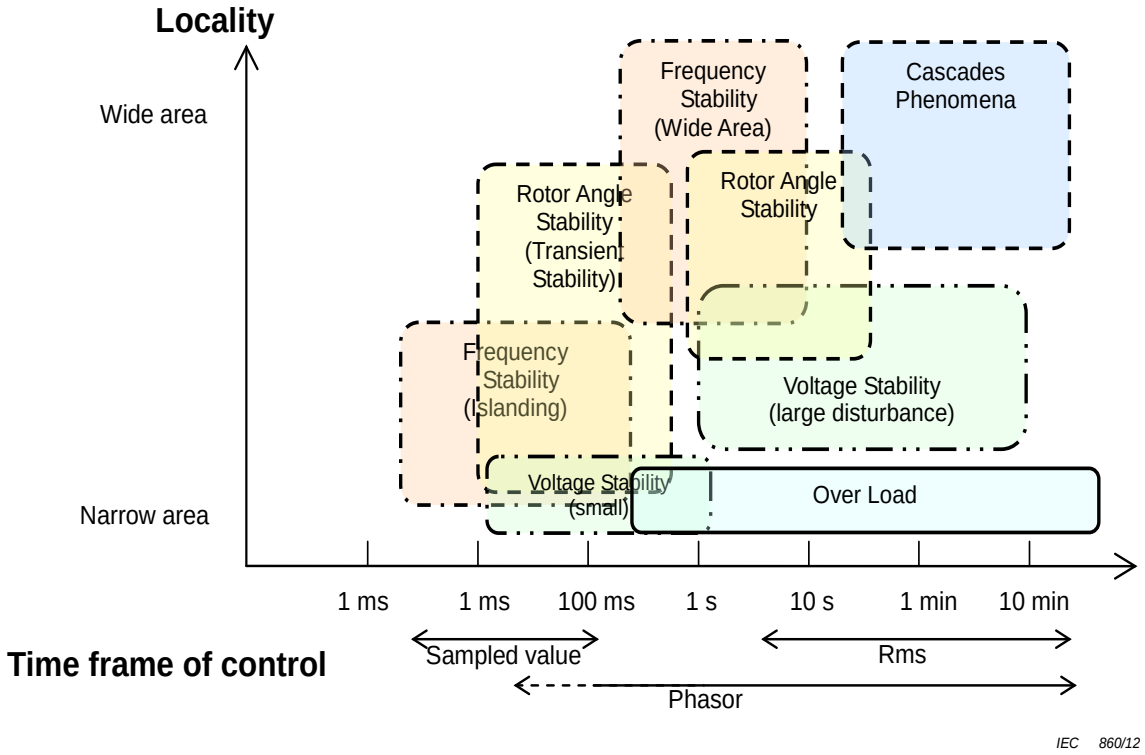


Figure 19 – Application locality and time scale

7.5 TCP use

The SV/R-SV service is based on periodic sending without recovery of lost messages. It is designed for high throughput rates and applications tolerating infrequent losses of single samples. In case that a loss of samples is critical, but the response times need not be deterministic, the following mechanisms can be used: the reporting mechanism of IEC 61850-7-2 and IEC 61850-8-1 can be used; in the case of needed high sample rates around a specific event, the disturbance recording feature with later file transfer, or a retransmission of the original packet (see Annex H) can be utilized. TCP based services are restricted to point-to-point associations between client and servers; however, they allow security by authentication as well as by encryption with existing means as needed.

8 Security model

8.1 General

The security model, for IEC/TR 61850-90-5, provides security functions based upon the security threats and security functions found in IEC/TS 62351-1 and IEC 62351-2.

Several aspects of security are addressed within this document with the following basic assumptions:

- information authentication and integrity (e.g. the ability to provide tamper detection) is needed;
- confidentiality is optional.

Theoretically, information authentication and integrity should be provided in an end-to-end method, regardless of information hierarchies. The typical method to provide this security function is through some type of information/message authentication code.

IEC/TS 62351-6 specifies the use of digital signatures using asymmetric cryptography. However, concerns about the impact of this specific technology in terms of cost and CPU performance given the current class of hardware found in PMUs, Relays and Merging Units today have been expressed. These concerns increase as the messaging rates for Sample Values increases. Therefore, the security model needs to take performance issues into account for use of the profiles/technologies specified within this document. This document provides specifications for both asymmetric and symmetric key authentication/MAC creation as well as symmetric key encryption. The encryption is used to provide optional confidentiality.

There are two explicit uses for the mapping of the SampledValues Application Protocol Data Unit (APDU) within this document. The APDU will be used to carry at least two types of information: CT/PT information per IEC 61850-7-2 and Synchronized Measured Values per IEEE C37.118.1. The messaging rates of these two types of data are different:

- CT/PT Information messaging rates can range from 50-256 messages/cycle and can consume approximately 7,2 to 34,6 Mbits/second, or more, of Local Area Network traffic.
- Synchronized Measured Values messaging rates can range from 1 to 240 messages/second.

Thus CT/PT information/communication requirements are approximately sixty (60) times greater than those of Synchronized Measured Values. This presumes a 50 Hz or 60 Hz nominal system. Based upon the messaging rates and types of information, different security requirements and classes of traffic can be developed:

- Intra-substation (Class A): This class of traffic is characterized by the exchange of high resolution waveform data within a substation. Intra-substation traffic should be capable of supporting both the CT/PT and Synchronized Measured Values. This requires a light-weight mechanism for Authentication and Tamper Detection (e.g. to support the CT/PT maximum messaging rates).
- Inter-substation (Class B): This class of traffic is characterized by the exchange of moderate resolution waveform data between different geographic locations. Inter-substation traffic allows Synchronized Measured Value information to be exchanged between different endpoints. Such endpoints include, but are not limited to, other substations and control centers.
- An optional encryption functionality is specified in order to provide confidentiality for this type of traffic, in addition to the Authentication and Tamper Detection.

Based upon the security requirements defined above, this technical report defines a means of message Authentication and Tamper detection regardless of the route of the message. The base security construct used to provide these types of security functions also provides the integrity of the selected security mechanisms on an end-to-end basis. Within the context of this technical report, several different types of endpoints have been identified:

- IEC 61850-9-2 SV and IEC 61850-8-1 publishers and subscribers: Implementations claiming conformance to these standards send/receive the prescribed messages via protocol profiles that do not provide a Network Layer protocol. As such, these protocols do not inherently provide routing capability and would otherwise be considered ClassA traffic. However, this technical report specifies a mechanism to forward these packets as ClassB traffic. These protocols do not provide the cryptographic integrity required for Authentication or Tamper Detection. However, IEC/TS 62351-6:2007 does specify the required mechanism. As the mechanism specified in IEC/TS 62351-6:2007 is optional, it is possible to use these protocols with or without the needed cryptographic integrity.
- This technical report specifies a standardized mechanism to route IEC 61850-9-2 SV and IEC 61850-8-1 GOOSE packets by forwarding them as ClassB traffic. This report specifies a mandatory mechanism to provide the needed cryptographic integrity. Therefore:
  - For implementations that do not implement IEC/TS 62351-6:2007, cryptographic integrity is provided between the IEC/TR 61850-90-5 implementations and not the original publisher and subscriber.

– For implementations that implement IEC/TS 62351-6:2007, two levels of cryptographic integrity occur: one between the publisher and subscriber and another between the IEC/TR 61850-90-5 implementations. The first level of cryptographic integrity is provided by Ethernet publishers (per IEC/TS 62351-6:2007). The second level of cryptographic integrity is provided by IEC/TR 61850-90-5.

– Figure 20 shows the various cryptographic endpoints, protocols used. Additionally, the figure shows the specifications used to provide the cryptographic integrity between the endpoints.

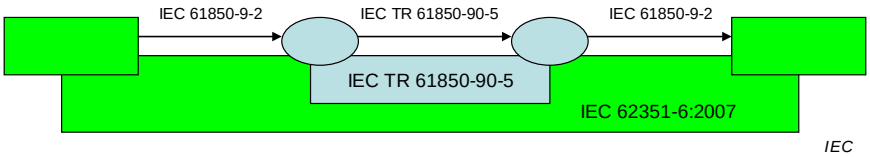


Figure 20 – End-to-end cryptographic integrity for IEC 61850-9-2 implementations

This enveloping approach provides implementations of IEC/TR 61850-90-5 inherent end-to-end cryptographic integrity.

The use of end-to-end cryptographic integrity, within IEC/TR 61850-90-5, allows packets to be sent across multiple Physical Security Perimeters (PSPs) and multiple Electronic Security Perimeters (ESPs). The actual definition of an actual PSP or ESP is established by the governance of the defining utility. However, in general, the following examples of PSPs and ESPs can be shown:

Substation: This would typically not be classified as an ESP or a PSP due to the fact that many utilities do not provide adequate access control/audit facilities that are typically required for a PSP (e.g. a Substation fence does not inherently create a PSP). Note that substation devices located outside the substation control house may need to be considered their own PSP and ESP.

Substation Control House: This would typically be considered a PSP and ESP.

Substation Devices not within the control house: These would typically need to be considered their own PSP and ESP.

Control Center: These would typically need to be considered their own PSP and ESP.

From a security perspective, messages exchanged across PSP/ESP boundaries require end-to-end cryptographic integrity. However, the need for confidentiality is typically determined by the path of the packet transmission/delivery and the sensitivity of the information being conveyed. If the information is accessible at endpoints that have varying levels of trust, the need for confidentiality would be determined based upon the sensitivity of the information.

This standard specifies the use of encryption technology that can be applied within the communicating end systems (e.g. PMUs, relays, PDCs, etc.) and/or between communication intermediate systems (e.g. routers). Although this Technical Report specifies an optional mechanism to provide encryption within the end systems, this document also implements the concept of “edge” security functions that allow intermediate systems to provide communication path selection, but also encryption capability.

In order to provide “edge” security functionality:

- This document will provide a mechanism to authenticate traffic to the intermediate system(s).
- The manager of the intermediate system is assumed to be trusted.

- The intermediate system is capable of adding additional security protection to the traffic (e.g. confidentiality, communication path selection, etc.) based upon the authentication parameters provided.
- An intermediate system that provides this additional security functionality will be referred to as an Edge Security Node.

One additional security protection an Edge Security Node might provide is confidentiality. Although it is up to the manager of the Edge Security Node, there are two recognized mechanisms for an Edge Security Node to provide confidentiality:

- The Edge Security Node can provide encryption of the traffic.
- The security model does not specify the actual mechanism for encryption, rather an authentication mechanism that would allow the Edge Security Node to identify the need for encryption. Thus, as new technologies become available, they can be deployed.
- The Edge Security Node can provide transmission path selection/assurance similar to the red-zone/green-zone paradigms used in the past (e.g. selection of a trusted communication path).

This document provides for APDU authentication and integrity through the use of a digital signature. Although it is desirable to provide end-to-end authentication and integrity protection, such protection cannot be assured if the contents of multiple APDUs are repackaged into another APDU. Such repackaging may occur within Phasor Data Concentrators, Phasor Gateway, or data concentrators, in general. The repackaging of IEC/TS 62351-6:2007 based packets should include the integrity parameters in those packets.

From a security model perspective, it becomes incumbent upon the intermediate systems (e.g. PDC, etc.) to provide an audit trail and chain of trust capability should repackaging occur.

8.2 Key management and cryptographic support

Key management and cryptographic support needs to be designed to provide the following functionality:

- Synchrophasor information needs to be able to be exchanged in an uninterrupted fashion. This continuous delivery needs to be supported even if the digital keys, used for encryption and signatures, are changed.
- Synchrophasor information is delivered using connectionless services/protocols and typically in a multicast environment.
- Both asymmetric and symmetric cryptographic support is desired.

The use of multicast, coupled with the need to support symmetric keys, requires the use of what is known as a Key Distribution Center (KDC). It is the KDC that provides the symmetric key coordination between the publisher and subscribers. Normal implementation practice would have the KDC deployed as a separate standalone node that manages the coordination for multiple publishers and subscribers. However, such a standalone entity raises concerns regarding redundancy. Additionally, the use of separate KDCs can cause issues in providing the un-interrupted delivery of information.

Therefore, the KDC function, for IEC/TR 61850-90-5, shall allow the publishing IED, or equivalent, to be its own KDC or to use an external KDC function. There is a benefit in having the IED providing its own KDC function in that the device can determine when to apply the next key. Given this intelligence, a mechanism for informing the subscribers of an impending key change can allow the subscribers enough time to acquire the new key thereby being prepared for the key change and thus allowing continuous information exchange. In order to accomplish this, the IEC/TR 61850-90-5 protocol needs to:

- Provide a mechanism to inform the subscribers of an impending key change.
- This mechanism is provided through the TimetoNextKey session attribute (see page 75).

- Provide a mechanism to inform the subscribers that a key change has occurred.
- This mechanism is provided through the TimeofCurrentKey session attribute (see page 75).

In order to accommodate the requirement to support symmetric and asymmetric technologies and to allow new mechanisms to be used in the future, a mechanism to convey the encryption and signature algorithms needs to be provided. This mechanism is provided through the SecurityAlgorithms session attribute (see page 75).

The publisher shall be configured to periodically change the symmetric keys used for the signature and optional encryption. It is recommended that symmetric keys be changed at least every forty-eight (48) h. Additionally, the configuration shall allow the definition of the maximum and minimum TimetoNextKey values. The maximum value shall be used for periodic updates of the keys. The minimum value shall be used for updates of the keys in situations where the current key has been compromised. Should no configuration be provided, the default values shall be:

Maximum value: 48 h (e.g. 2 880 min)
Minimum value: 30 min

The values shall be specified in minutes.

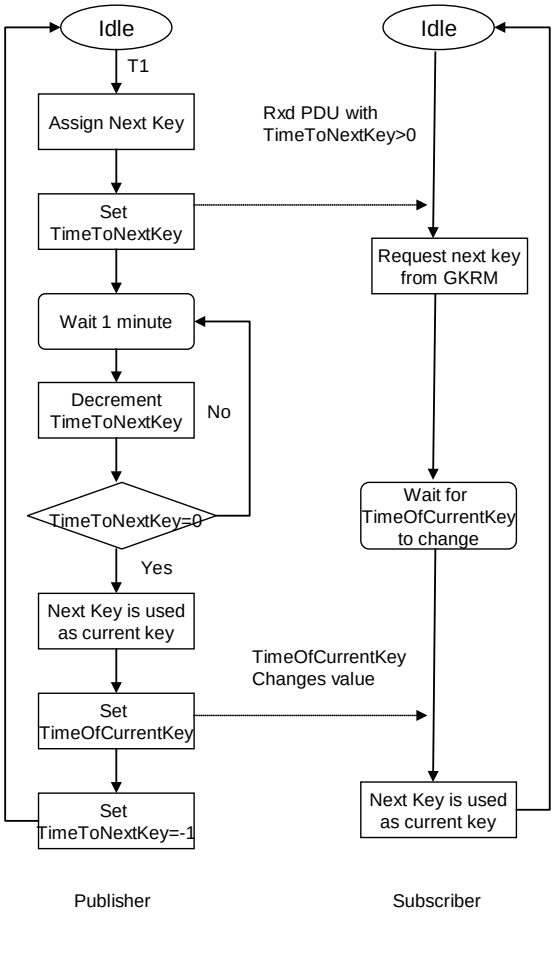


Figure 21 – State transitions for key usage

Figure 21 shows the interaction between the publisher and subscribers regarding key usage. When the publisher starts the update process (T1), a new key is assigned within the KDC function. The publisher sets the TimeToNextKey attribute value. Once a minute, the publisher checks to determine if the TimeToNextKey has reached a value of zero (0). If not, the value is

decremented. If the value is zero, the new key starts being used as the current key and the TimeOfCurrentKey is updated with the current timestamp.

When a subscriber detects a positive TimeToNextKey value, the subscriber interacts with the KDC to obtain the next key. The subscriber then waits until the TimeOfCurrentKey value changes. The PDU that has the changed value shall be the first PDU to use formerly next key as the current key.

8.3 Key Distribution Center (KDC)

There are several aspects to the functionality required by an IEC/TR 61850-90-5 KDC server function. These are the following.

- The KDC must be capable of authenticating KDC clients on a per information stream basis.
- There are several types of information streams within the IEC 61850 domain. These are:
  - Ethernet multicast GOOSE,
  - Ethernet multicast SV,
  - UDP GOOSE (e.g. IEC/TR 61850-90-5),
  - UDP SV (e.g. IEC/TR 61850-90-5),
  - IEC/TR 61850-90-5 Tunnel,
  - The Client/Server profile of IEC 61850-8-1.

  Each information stream type needs to be further constrained in order to allow a more granular authentication/key exchange. As an example, there may be two (2) publishers (e.g. IED1 and IED2) to two (2) different destination multicast addresses (e.g. DMAC1 and DMAC2). A subscriber may be need to be restricted to a group that is only allowed to be a group key member for DMAC1 and not DMAC2. Therefore, the KDC must allow key group management based upon either the destination Ethernet or IP address.

  However, a further restriction is also needed in protection/encryption based upon the contents that are being sent to the destination. It is possible that the same destination address is being used by two different publishers, but protection is needed on both separately. In the case of GOOSE/SV, the content constraint/definition is in relationship to the DataSet being published.
- The KDC shall support clients requesting keys as opposed to publishing keys to an established group. The ability to publish the keys to a key group is out of the scope of this Technical Report.
- The KDC shall allow asymmetric cryptography to be used for identity establishment and authentication of a client requesting a key.
- The KDC deployment architecture shall support KDC functions that are internal or external functions to an IED/Server that is publishing IEC/TR 61850-90-5.

9 Services

9.1 General

IEEE C37.118.2 does not explicitly talk of "services". Instead, it specifies the synchrophasor message format in Chapter 6. It describes four message types (frames types):

- Data frame (see 6.3 of IEEE C37.118.2),
- Configuration frame (see 6.4 of IEEE C37.118.2),
- Header frame (see 6.5 of IEEE C37.118.2),
- Command frame (see 6.6 of IEEE C37.118.2).

The functions performed by exchanging the different frame types from IEEE C37.118.2 have to be mapped to services of IEC 61850.

9.2 Command service

9.2.1 General

This shall be the equivalent to the function performed by the command frame.

The different functions as specified by the command word in IEEE C37.118.2 can be performed by equivalent IEC 61850 actions or services as specified in Table 1:

Table 1 – Equivalent commands

Command word	Definition (IEEE C37.118.2)	Equivalent IEC 61850 action /service
1	Turn off transmission of frames	Disable SVCB (set SvEna in SVCB to False)
2	Turn on transmission of frames	Enable SVCB (set SvEna in SVCB to True)
3	Send header	Read information for FC “DC” and read SvCB (see 9.4)
4	Send CFG-1 information	Obtain data model of PMU related functions (e.g. logical device PMU or LNs representing PMU functions) as well as all other LNs in the device.
5	Send CFG-2 information	Read actual measurements from data model (MMXU, etc.)
8	Extended frame	Out-of-scope

9.2.2 Control blocks

9.2.2.1 General

There are two (2) control blocks that need to be defined. The functions of these control blocks allow:

- the sending of stream information (e.g. Sampled Values),
- the sending of event driven information (e.g. GOOSE).

In order to provide backward compatibility, the currently defined IEC 61850-8-1 GOOSE and SV control blocks will remain unchanged. Therefore, there are two new functional constraints that will be added to LN0:

- RS – Indicates a functional constraint for routable SV packets based upon the profile defined in this document. The control blocks with this constraint will be defined as ROUTABLE-MULTICAST-SAMPLED-VALUE-CONTROL-BLOCK (R-MSVCB).
- RG – Indicates a functional constraint for routable GOOSE packets based upon the profile defined in this document. The control blocks with this constraint will be defined as ROUTABLE-GOOSE-CONTROL-BLOCK (R-GoCB).

The introduction of new control blocks has an impact on several different parts of the IEC 61850 standard. The impacted parts are:

- IEC 61850-8-1: Will need to be updated to:
  - specify the new FCs of RS and RG;
  - specify the mapping of the IEC 61850-7-2 GoCB to the R-GoCB.
- IEC 61850-9-2: Will need to be updated to:
  - specify the mapping of the IEC 61850-7-2 MSVCB to the R-MSVCB.
- IEC 61850-6 will need to be updated to allow the appropriate specification of both the R-GoCB and R-MSVCB.

The following subclauses specify the R-GoCB, R-MSVCB, and the Substation Configuration Language changes that are required.

9.2.2.2 Sampled values over IP control block: R-MSVCB

The synchrophasor stream will be transmitted via the use of Sampled Values, but over a transport profile that utilizes IPv4 or IPv6. In order to accomplish this, and to support the existing Ethernet multicast, the R-MSVCB structure will be similar to the MSVCB, but with the enhancements of a SecurityEnable attribute, and the use UDPCOMADDR.

R-MSVCB control blocks shall have a functional constraint of RS.

Table 2 defines the R-MSVCB.

Table 2 – R-MSVCB class definition

Attribute name		Attribute type	r/w	m	Value/value range/explanation
MsvCBName		ObjectName	-	m	MMS object name: the value of this component shall be of the format of ObjectReference and shall be limited to VMD or Domain scoped NamedVariableLists.
MsvCRef		ObjectReference	-	m	Path-name of an instance of SvCB
SvEna		BOOLEAN	r/w	m	Enabled (TRUE) | disabled (FALSE), DEFAULT FALSE
Resv		BOOLEAN	r/w	m	
MsvID		VISIBLE STRING129	r/w		System wide unique identification****.
DatSet		ObjectReference	r/w	m	
ConfRev		INT32U	r	m	
SmpRate		INT16U	r/w		(0..MAX)
OptFlds		PACKEDLIST		m	
	refresh-time	BOOLEAN	r	m	TRUE = SV buffer contains the attribute "RefrTm" FALSE = attribute "RefrTm" is not available in the SV buffer. Shall be TRUE if TransportinUse is not ETHERNET.
	samplesynchronised	BOOLEAN	r	m	Value will be ignored. Kept to ensure backward compatibility to IEC 61850-9-2 edition 1.0
	sample-rate	BOOLEAN	r	m	TRUE = SV buffer contains the attribute "SmpRate". FALSE = attribute "SmpRate" is not available in the SV buffer.
	data-set	BOOLEAN	r	m	TRUE = SV buffer contains the attribute "DatSet". FALSE = attribute "DatSet" is not available in the SV buffer.
	security	BOOLEAN	r	m	Mapping specific attribute. TRUE = SV buffer contains the attribute "Security".

Attribute name	Attribute type	r/w	m	Value/value range/explanation
				FALSE = attribute “Security” is not available in the SV buffer.
timestamp*	BOOLEAN	r	m	Include a TIMESTAMP if TRUE.
SmpMod	ENUMERATED	r/w	m	samples per nominal cycle (DEFAULT) | samples per second | seconds per sample
DstAddress	UDPCOMADDR***	r	o	
SecurityEnable* **	ENUMERATED	r	o	None, Signature, SignatureAndEncryption

* Additional OptFld added.

** The definition UDPCOMADDR can be found in 9.2.2.4.1.

*** Additional attribute to be added to the control block.

9.2.2.3 GOOSE over IP control block: R-GoCB

In order to send events over IP, the R-GoCB requires the ability to support IPv4 and IPv6 multicast. The R-GoCB will be similar to the GoCB structure but will be enhanced by the SecurityEnable attribute and the UDPCOMADDR.

Table 3 shows the additional attributes that need to be added to the GoCB.

Table 3 – R-GoCB definition

Attribute name	Attribute type	r/w	m	Value/value range/explanation
GoEna	Boolean	rw	m	
GoID	Visible-string	r	m	
DatSet	Visible-string	r	m	
ConfRev	Unsigned	r	m	
NdsCom	Boolean	r	m	
DstAddress	UDPCOMADDR*	r	m	
MinTime	Unsigned	r	o	
MaxTime	Unsigned	r	o	
FixedOffs	Boolean	r	o	
SecurityEnable**	ENUMERATED	r	o	None, Signature, SignatureAndEncryption

* The definition of UDPCOMADDR can be found in Table 5.

** Additional attribute to be added to the control block.

9.2.2.4 Explanation of additional attributes

9.2.2.4.1 UDPCOMADDR

The current definition of PHYCOMADDR, from IEC 61850-8-1, is shown in Table 4.

Table 4 – Current PHYCOMADDR structure

Attribute name	Attribute type	r/w	m	Value/value range/explanation
Addr	OCTET-STRING	r	m	Length is 6 Octets and contains the value of the destination Media Access Control (MAC) address to which the GOOSE message is to be sent. The address shall be an Ethernet address that has the multicast bit set TRUE.
PRIORITY	Unsigned8	r	m	Range of values shall be limited from 0 to 7.
VID	Unsigned16	r	m	Range of values shall be limited from 0 to 4 095.
APPID	Unsigned16	r	m	As defined in Annex C in IEC 61850-8-1

The definition of UDPCOMADDR is similar to PHYCOMADDR and is defined in Table 5.

Table 5 – UDPCOMADDR structure

Attribute name	Attribute type	r/w	m	Value/value range/explanation
PRIORITY	Unsigned8	r	m	Range of values shall be limited from 0 to 7.
VID	Unsigned16	r	m	Range of values shall be limited from 0 to 4 095.
APPID	Unsigned16	r	m	As defined in Annex C in IEC 61850-8-1
TransportInUse	Unsigned8	r	o	Is an enumerated value whose values are: IPv4, IPv6, and DNS assigned
IPClassOfTraffic	Unsigned8	r	c	If TransportInUse=IPv4, the value shall represent the IPv4 TypeOfService value. If TransportInUse=IPv6, the value shall be the IPv6 Class of Traffic field.
IPv6FlowLabel	Unsigned32	r	c	If TransportInUse= IPv4, the value shall be zero (0) and shall be ignored. If the TransportInUse= IPv6, the value shall contain the 24 bits of the IPv6 Flow Label field in the least significant part of the unsigned value.
IPAddressLength	Unsigned8	r	c	If TransportInUse= IPv4, the value shall be four (4). If TransportInUse= IPv6, the value shall be sixteen (16). If TransportInUse= DNS, the value shall be the length of the DNS string, not including terminating NULL.
IPAddress	OCTET-STRING	r	c	This attribute shall be 64 octets in size. Any unused octets, based upon the IPAddressLength attribute value, shall be zero (0).

In order to configure the additional information in SCL, the following additions to SCL need to be made. The following “P” types need to be added:

- IPv6FlowLabel,
- DNS String address.

NOTE The addition of the DNS string allows names to be used for addressing in addition to the dotted-decimal notations of IPv4 or IPv6.

Additionally, the IPv6 equivalents of tp_IP, tp_IP-SUBNET, and tp_IP-GATEWAY need to be created to allow IPv6 representations in addition to IPv4 representations. Observe that the values of transportInUse, IPClassOfTraffic and IPAddressLength are implicitly given by the IPv4 respective IPv6 syntax of the IP address in SCL.

9.3 Configuration request service

9.3.1 General

This shall be the equivalent to the functions performed by the configuration frames.

There are three (3) kinds of configuration information in IEEE C37.118.2, named CFG-1, CFG-2, and CFG-3.

9.3.2 CFG-1 Type of configuration data – Capabilities

The capabilities correspond to the data model of the server that provides the SP data.

Getting this configuration information is equivalent to obtaining the data model structure of the server.

For this, IEC 61850 provides standardized methods.

9.3.3 CFG-2 or CFG-3 Type of configuration data – Measurements

The capabilities correspond to acquiring the data set member definitions of a particular control block.

For this, IEC 61850 provides standardized methods (GetDataSetDirectory, and GetGOReference). However, IEC 61850 does not currently define the equivalent of GetSavReference (e.g. for Sampled Values). This document adds the GetSavReference service.

9.3.4 Online access to CFG-1 configuration information

For this, IEC 61850 servers provide the self-description. A client can request information about the control blocks, the assigned datasets and the datasets themselves.

9.3.5 Offline access to CFG-2 and CFG-3 configuration information

The data model of the server, the control blocks, and the datasets are described in SCL (Substation Configuration Language) files that describe the configured IED (SCD, CID).

9.4 Header information service

The header frames in IEEE C37.118.2 are intended to provide information in human readable form.

The defined semantics of the data in IEC 61850 provide a high degree of readability for human users that are familiar with the concept.

Additional description attributes ("d" and dU") can be used to provide further information on the data attributes. This depends on the implementation of the data model. These attributes reside under the functional constraint "DC" (description).

The access methods to the description data are the same as for the other configuration data.

No special methods need to be defined to resemble the functions of the header frames.

9.5 Data transmission service

9.5.1 General

This shall be the equivalent to the functions performed by the data frames.

9.5.2 General

IEEE C37.118.2 allows RS-232 serial or a UDP or TCP protocol for the transmission of the data frames, which hold the actual synchrophasor data. RS-232 is becoming less used in favour of networks, so only network communication will be addressed here. UDP and TCP protocols are in any case IP-based and therefore routable. This property of being routable over wide area IP networks is necessary and suited for a protocol to be used with for wide area applications, where PMUs are applied.

For data with periodic transmission, IEC 61850 provides the sampled value service.

As described in IEC 61850-9-2, this is a layer two protocol, mainly intended for applications within a substation. As a layer two protocol, it is not routable and therefore not suited for wide area applications.

The remarks in IEC/TR 61850-90-1 on Synchrophasors (Subclause 5.1.1) are an approach for exchanging the sampled values between substations, but this is not really a useful option solution for synchrophasor applications.

As far as the TCP option is concerned, IEC 61850 reporting would be an option. It would be imaginable to use integrity reports (with some additional definitions on how data are retrieved and synchronized with the integrity period) for the periodic transmission of the data. But as the applications show, the TCP option in IEEE C37.118.2 is rarely applied in real applications.

For obvious reasons, the bulk of the applications transfer the data frames using UDP, and this document focuses on providing an IEC 61850 mechanism exactly for this case.

9.5.3 Coding synchrophasors data

9.5.3.1 General

For the coding of the values of datasets, there are two options possible: for GOOSE and SV. Neither of these offers the efficiencies of bytes transmitted as IEEE C37.118.2. However, certain efficiencies are available.

9.5.3.2 GOOSE data coding

There are two options provided for the encoding of GOOSE APDUs. One is the generic ASN.1 and the other is Fixed Length Encoding. Although neither mechanism provides any additional significant efficiency of octets transmitted, the Fixed Length encoding option (see IEC 61850-8-1) allows more efficient processing.

9.6 Specific data mapping

The IEC 61850-9-2 encoding rules, for SV, are efficient and are largely optimized for byte efficiency. There is a further optimization available should the synchrophasor information be able to be conveyed in the data mapping of the UCA implementation guideline for sampled values (e.g. UCA User's Group 61850-9-2LE).

9.7 Common data fields

There are some data which must be present in any case to make up a useful synchrophasor protocol. These data shall be arranged at the beginning of the dataset in a defined order.

These fields include, but are not limited to:

- time stamp;
- time source and synchronization status information.

9.8 Time synchronization

UTC time is required for making synchrophasor measurements. Accuracy is dictated by the requirements specified in the IEEE Synchrophasor Measurement Standard, IEEE C37.118.1. The expected accuracy is 1 μs though the measurement can meet required accuracy with a timing error of 26 μs (at 60 Hz) if all other measurements are perfect. The measurement is made continuously and a typical measurement system requires continuous time accuracy at 5 μs or better. Time can be provided by any source that can deliver UTC time at the required accuracy and reliability.

9.9 Redundancy

Based upon the use cases in Clause 5, there is a need to specify mechanisms for redundancy. The necessary availability of synchrophasor information for Wide Area Situational Awareness and Control requires that at least communication redundancy be provided. The implementation of LAN-based redundancy shall be a selected mechanism/architecture from IEC/TR 61850-90-4.

From a wide area communication perspective (e.g. substation-to-substation, substation-to-control center, control center-to-control center, etc.), there are several communication system architectures that need to be considered. These architectures are discussed in the following subclauses.

Communication redundancy:

The architecture uses a single communication node (e.g. router, etc.) to connect to two (2) independent communication media infrastructures (e.g. T1 and Microwave or Sonet Ring with counter rotating tokens).

This architecture provides redundancy protection from communication path failure.

This redundancy mechanism is a system design issue and is out of the scope of this document.

Multi-path delivery:

The architecture uses a single communication node (e.g. router), with a single communication port, to send packets into a mesh network.

The mesh network then provides parallel multi-path delivery of the packets.

For the purposes of communication failure detection, it is the responsibility of the receivers of the communication profile packets, as defined in this document, to enunciate problems when the expected packets are not delivered in a timely manner or based upon protocol expectations (e.g. GOOSE APDUs). Receivers shall mark the quality of the dataset members that have not been delivered within the appropriate time with a quality.validity of “invalid” or “questionable” and a quality.detailedQual of “oldData”.

In the case of the profiles specified in this document, the use of multi-path delivery makes use of IP based facilities to determine the appropriate paths. Such path determination shall be performed per RFC 2991.

In order to provide duplicate packet delivery detection, at the receiving application the combination of source IP address and SPDU number shall be unique. Security authentication must be performed prior to duplicate packet discard.

10 IEC logical node modelling for synchrophasor measurements

Since this standard refers to the measurement techniques and filtering requirements of IEEE C37.118.1, it is the semantics of the performance classes of protection and measurement that shall be expressed.

From IEEE C37.118.1 (Informative):

"P class is intended for applications requiring fast response; it mandates no explicit filtering. M class is intended for applications which could be adversely affected by aliased signals but do not require the fastest reporting speed. “

This standard does not correlate signal filtering with reporting rate. Therefore, this standard defines:

- P-Class mandates no explicit signal filtering and provides the shortest signal response times,
- M-Class requires anti-alias filtering which could result in longer signal response times.

The characteristics of P-Class and M-Class shall be as defined in IEEE C37.118.1.

In order to allow the construct of P-Class and M-Class to be specified within the context of IEC 61850, the IEC 61850-7-4 ClcMth shall be used. The set of allowed values shall be expanded as shown in Table 6.

Table 6 – Extension to ClcMth to allow P-Class and M-Class

<table>
<tr><td>ClcMth</td><td>The calculation method specifies how the Data Attributes that represent analogue values have been calculated. The calculation method shall be the same for all Data Objects of a given logical node instance.

The possible values shall be:
<table><tr><td>Value</td><td>Description</td></tr><tr><td>PRES_OR_UNKNOWN</td><td>Indicates that all analogue values (i.e. all common attributes I and f) are present or, more precisely, actual values.</td></tr><tr><td>TRUE_RMS</td><td>Indicates that all analogue values (i.e. all common attributes I and f) are true r.m.s. values.</td></tr><tr><td>PEAK_FUNDAMENTAL</td><td>Indicates that all analogue values (i.e. all common attributes I and f) are peak fundamental values.</td></tr><tr><td>RMS_FUNDAMENTAL</td><td>Indicates that all analogue values (i.e. all common attributes I and f) are r.m.s. fundamental values.</td></tr><tr><td>MIN</td><td>Indicates that all analogue values (i.e. all common attributes i and f) are minimum values.</td></tr><tr><td>MAX</td><td>Indicates that all analogue values (i.e. all common attributes i and f) are maximum values.</td></tr><tr><td>AVG</td><td>Indicates that all analogue values (i.e. all common attributes i and f) are average values.</td></tr><tr><td>SDV</td><td>Indicates that all analogue values (i.e. all common attributes i and f) are standard deviation values.</td></tr><tr><td>PREDICTION</td><td>Indicates that all analogue values (i.e. all common attributes i and f) are long term changes over time.</td></tr><tr><td>RATE</td><td>Indicates that all analogue values (i.e. all common attributes i and f) are actual changes over time calculated with the actual value and value before.</td></tr><tr><td>P-CLASS</td><td>Indicates that all analogue values (i.e. all common attributes i and f) meet the sampling and filtering characteristics specified in IEEE C37.118.1 for P-class.</td></tr><tr><td>M-CLASS</td><td>Indicates that all analogue values (i.e. all common attributes i and f) meet the sampling and filtering characteristics specified in IEEE C37.118.1 for M-class.</td></tr></table>This DATA OBJECT shall be mandatory for all logical nodes that are intended to represent statistical data, indicated by the common data classes, for example, CDC MV, CMV, WYE, etc.

NOTE 1 If different calculation periods are required for the Data Objects of a logical node, then different logical nodes could be instantiated – with different calculation periods.

NOTE 2 The calculation algorithm and number of samples used for the calculation is an implementation issue.</td></tr>
</table>

It is also recommended that the last character of the LN prefix be utilized to indicate if the LN is M or P class. The character should be ‘M’ or ‘P’ representing the appropriate class of measurement.

For P-CLASS and M-CLASS ClcMth values, the following attribute values shall be:

- ClcMod: Shall be set to a value of PERIOD.
- ClcIntvTyp: Shall be a value of MS, PER-CYCLE, or CYCLE.
- ClcIntvPer: Shall be set appropriately.

11 Synchrophasor profile mappings

11.1 General overview

The control and configuration services use conventional IEC 61850 methods with MMS over TCP/IP. No extensions are required for this.

For data transmission, new UDP mappings are required. However, it is also desirable to be able to utilize/integrate the currently existing GOOSE and SV protocols without change. Therefore, an ability to “tunnel” the currently existing Ethernet bound GOOSE and SV packets over UDP/IP have been identified.

Figure 22 depicts a general overview of the mapping of Synchrophasor Services. The services identified in 9.2 will utilize the client/server A-Profile as specified in IEC 61850-8-1 (Subclause 6.2.2 of IEC 61850-8-1).

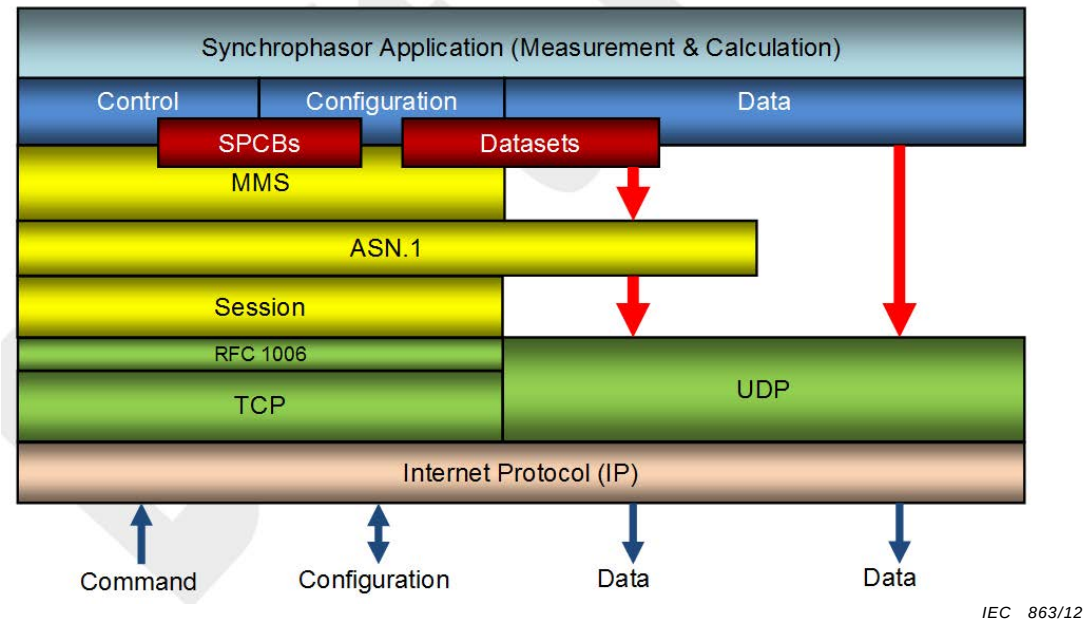


Figure 22 – General service mappings

IEEE C37.118.2 supports the delivery of synchrophasor information using a streaming mechanism. This type of information naturally maps into the IEC 61850-9-2 packet and streaming mechanisms, however utilizing a T-Profile based upon UDP/IP. Analysis of several use-cases has indicated that there is also a need for event driven communications (e.g. for certain critical control applications). Therefore, GOOSE services also need to be supported.

11.2 A-Profiles

In general, the A-Profiles will consist of the current GOOSE and SV Application Protocol Data Units (APDUs) encapsulated or tunnelled using the session protocol that is defined in this document.

In order to reuse port 102 for UDP, RFC 1240 needs to be implemented; this means that ISO Connectionless Transport must be used as well (ITU X.234).

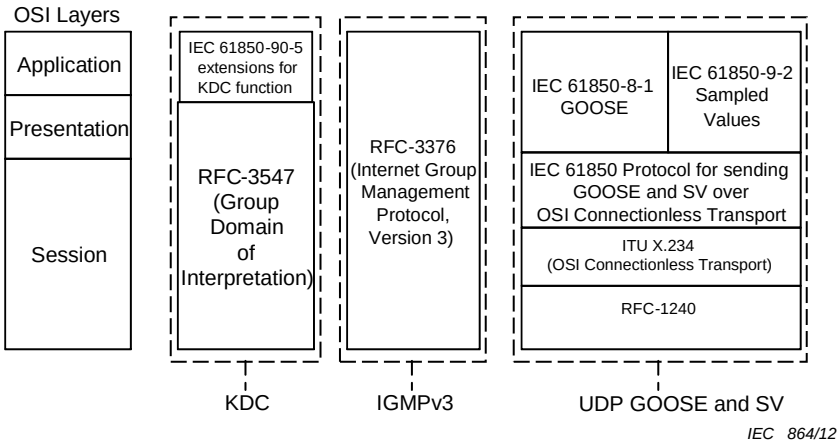


Figure 23 – IEC/TR 61850-90-5 A-Profiles

Figure 23 shows the Application Profile (A-Profile) that will be used to convey synchrophasor information. In general, it uses:

- IEC 61850-8-1 GOOSE and IEC 61850-9-2 as the application and presentation layers. The session protocol consists of:
  - a session protocol detailed in 11.3.2. This protocol is used to convey key parameters that are required in order to satisfy the use cases identified in this document.
  - ITU X.234: OSI Connectionless Transport.
  - RFC 1240: OSI Connectionless Transport over UDP
- RFC 3547 provides the KDC function. The RFC allows extensions to occur in a standardized manner. This capability is used to provide IEC/TR 61850-90-5 extensions.
- RFC 3376 provides the ability to have the routed networks configure IP multicast routing paths based upon detecting client subscriptions.

The A-Profiles will be bound to one of the Transport Profiles (T-Profiles) specified in 11.6 .

11.3 A-Profile GOOSE, SV, and management A-Profile

11.3.1 Application layer

This A-Profile specifies the communication profile that allows GOOSE and SV to be transported over an IP based network in a secure manner. This is called R-GOOSE respective R-SV.

This A-Profile allows for the transport of the GOOSE and SV APDUs, as defined in IEC 61850-8-1 and IEC 61850-9-2, to be sent in a secure and routable manner. It is intended that these APDUs be utilized with a minimum of changes.

The following subclauses detail the changes required to the GOOSE and SV APDUs in order to achieve the functionality required by IEC/TR 61850-90-5.

11.3.1.1 Changes required for IEC 61850-9-2

There are two (2) impacts on IEC 61850-9-2:

- Control block changes are required in order to accommodate the new profile(s). These have been documented in 9.2.2.2.
- There is a need to have an absolute TimeStamp for the streaming data.

Currently, the Sampled Value message header contains the following information:

Abstract Buffer Format according to IEC 61850-7-2		Coding in IEC 61850-9-2	Comments
Attribute name	**Attribute type**	**ASN.1 Basic Encoding Rules (BER)** **SavPdu::=** **SEQUENCE {**	
		noASDU [0] IMPLICIT INTEGER (1..65535),	Mapping specific attribute. Number of ASDUs, which will be concatenated into one APDU.
		security [1] ANY OPTIONAL,	Mapping specific attribute. Reserved for future definition (e.g. digital signature). NOTE Is reserved to provide backward compatibility, but use is deprecated.
		asdu [2] IMPLICIT SEQUENCE OF ASDU,	1 to *n* number of ASDUs as specified before.
		messageAuthentication [3] ANY OPTIONAL }	Mapping specific attribute. Reserved for future definition (e.g. MAC).
		ASDU::= SEQUENCE {	
MsvID	VISIBLE STRING	svID [0] IMPLICIT VisibleString,	Should be a system-wide unique identification.
DatSet	ObjectReference	datset [1] IMPLICIT VisibleString OPTIONAL,	Value from the MSVCB
SmpCnt	INT16U	smpCnt [2] IMPLICIT OCTET STRING (SIZE(2)),	Will be incremented each time a new sampling value is taken. The counter shall be set to zero if the sampling is synchronised by clock signal (SmpSynch = 1 or 2) and the synchronising signal occurs. When sync pulses are used to synchronise merging units, the counter shall be set to zero with every sync pulse. The value 0 shall be given to the data set where the sampling of the primary current coincides with the sync pulse. The OCTET STRING is interpreted as INT16U
ConfRev	INT32U	confRev [3] IMPLICIT OCTET STRING (SIZE(4)),	Value from the MSVCB The OCTET STRING is interpreted as INT32U.

Abstract Buffer Format according to IEC 61850-7-2		Coding in IEC 61850-9-2	Comments
Attribute name	**Attribute type**	**ASN.1 Basic Encoding Rules (BER)** **SavPdu::=** **SEQUENCE {**	
RefrTm	TimeStamp	refrTm [4] IMPLICIT UtcTime OPTIONAL,	RefrTm contains the refresh time of the SV buffer. This is the measurement time of the synchrophasor data as defined in IEEE C37.118.1.
SmpSynch	INT8U	smpSynch [5] IMPLICIT OCTET STRING (SIZE(1)),	2 = SV are synchronised by a global area clock signal. 1 = SV are synchronised by a local area clock signal. 0 = SV are not synchronised by an external clock signal.
SmpRate	INT16U	smpRate [6] IMPLICIT OCTET STRING (SIZE(2)) OPTIONAL,	Value from the MSVCB The OCTET STRING is interpreted as INT16U.
Sample [1..n]	Type depends on the CDC defined in IEC 61850-7-3.	sample [7] IMPLICIT OCTET STRING (SIZE(n))	List of data values related to the data set definition. For the encoding of the Data, the rules for the encoding of IEC 61850-9-2 shall apply. The SIZE(n) is the cumulated size, in octets, of all the data conveyed as defined in the DataSet.
SmpMod	INT16U	smpMod [8] IMPLICIT OCTET STRING (SIZE(2)) OPTIONAL	Value from the MSVCB The OCTET STRING is interpreted as INT16U.
t	TIMESTAMP	timeStamp [9] IMPLICIT UtcTime OPTIONAL }	Absolute timestamp of the transmission time of the packet. Inclusion of this field is controlled by the control block OptFld.timestamp value.

The MsvID attribute could be used to convey IEEE C37.118.2 Station and IDCode information. It is recommended that the following format be utilized: C37-118-<Station Name>-<IDCode>. Where the Station Name and IDCode values are the appropriate VisibleString characters.

11.3.1.1.1 t – Timestamp

There is need, for wide area network communications, to convey an absolute timestamp that represents the contents of the stream. Currently, the only available timestamp is the attribute RefrTm. However, in IEC 61850-9-2, EntryTime is defined as a “48-bit TimeStamp as defined in IEC 61850-8-1”.

In IEC 61850-8-1, EntryTime is defined to be:

“EntryTime shall be mapped to the MMS DataType of BINARY-TIME. The size of the BINARY-TIME value shall be six (6) octets.

The MMS TimeOfDay epoch began at 0 hours on 1 January 1984 (MJD 40 587). Times measured are designated in this standard as MMS TimeOfDay milli-seconds GMT and TimeOfDay days GMT, and represent offets from the epoch. It should be noted that exceptions to this mapping do occur.”

This means that the “absolute timestamp”, of a resolution required for synchrophasors can be calculated for SV:

RefrTm(EntryTime) + SmpCnt/(SmpRate)

Therefore, for synchrophasor information, RefrTm, SmpCnt, and SmpRate shall be sent in a SV message.

For DataSet elements that are not sampled at that time, the DataSet element will need to include its own timestamp. Additionally, the QUALITY for each DataSet element may need to be included. As such, it is recommended that Functionally Constrained Data (FCD) and not Functionally Constrained Data Attributes (FCDA) be utilized as DataSet members.

The timestamp calculation, based upon RefrTm, is valid for PMUs and CTs/VTs where the actual sampling is actually occurring. However, at the Phasor Data Gateway level, the concept of SmpRate and SampleCount are not appropriate. Therefore, the timestamp field (e.g. “t”) has been added to the SV APDU to allow the same PDU structure to be used at any level in the hierarchy.

The value of “t” shall be of the format specified in IEC 61850-8-1. It is recommended that TAI be utilized through having the TimeQuality.LeapSecondsKnown set FALSE.

11.3.1.2 Addition of management services protocol

Currently there is no equivalent to GetGOReferences and GetGOElementNumber services for sampled values. However, in order to support the equivalence of IEEE C37.118.2 CFG-2/CFG-3 commands, and to support run-time verification without SCL, these services shall be added to IEC 61850-7-2. This means that the protocol productions (see 11.3.3.6) will need to be added to IEC 61850-9-2.

11.3.1.3 Changes required for IEC 61850-8-1 and IEC 61850-9-2

It is recommended that the DataSet elements include their own timestamp. Additionally, the QUALITY for each DataSet element may need to be included. As such, it is recommended that Functionally Constrained Data (FCD) and not Functionally Constrained Data Attributes (FCDA) be utilized as DataSet members.

11.3.2 Session layer

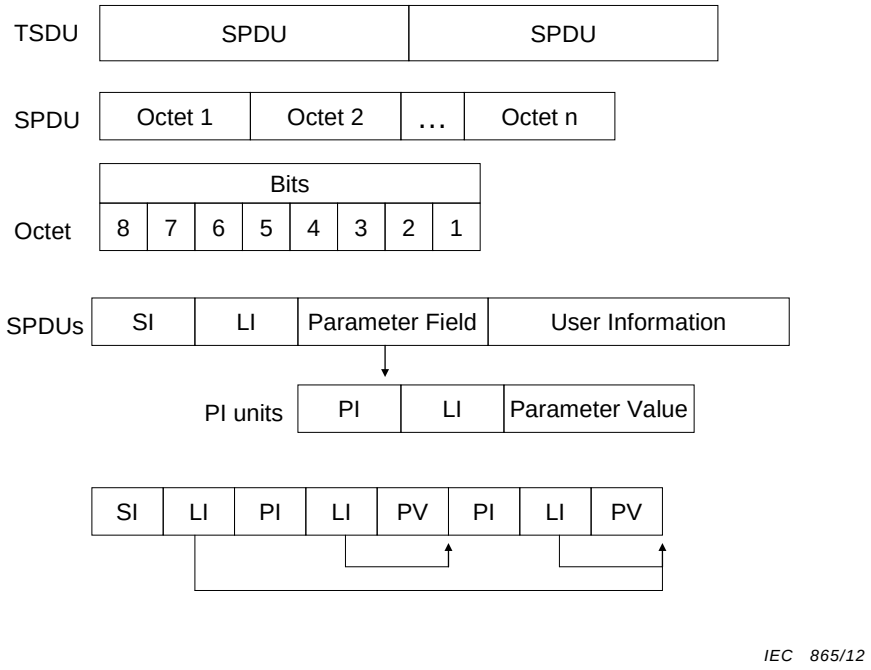


Figure 24 – General byte ordering of session protocol

ITU X.235 reserves a Session Identifier (SI) value of 64 (decimal) to indicate OSI Connectionless Session. Therefore, this value may not be used.

11.3.2.1 General

Figure 24 shows the general construction of the session protocol, and the bit/byte ordering for the protocol for transmission. In general, there will be a Session Identifier (SI) which has a single byte length. This length covers the length of all of the parameter fields for the session header, but not the user data of the session protocol.

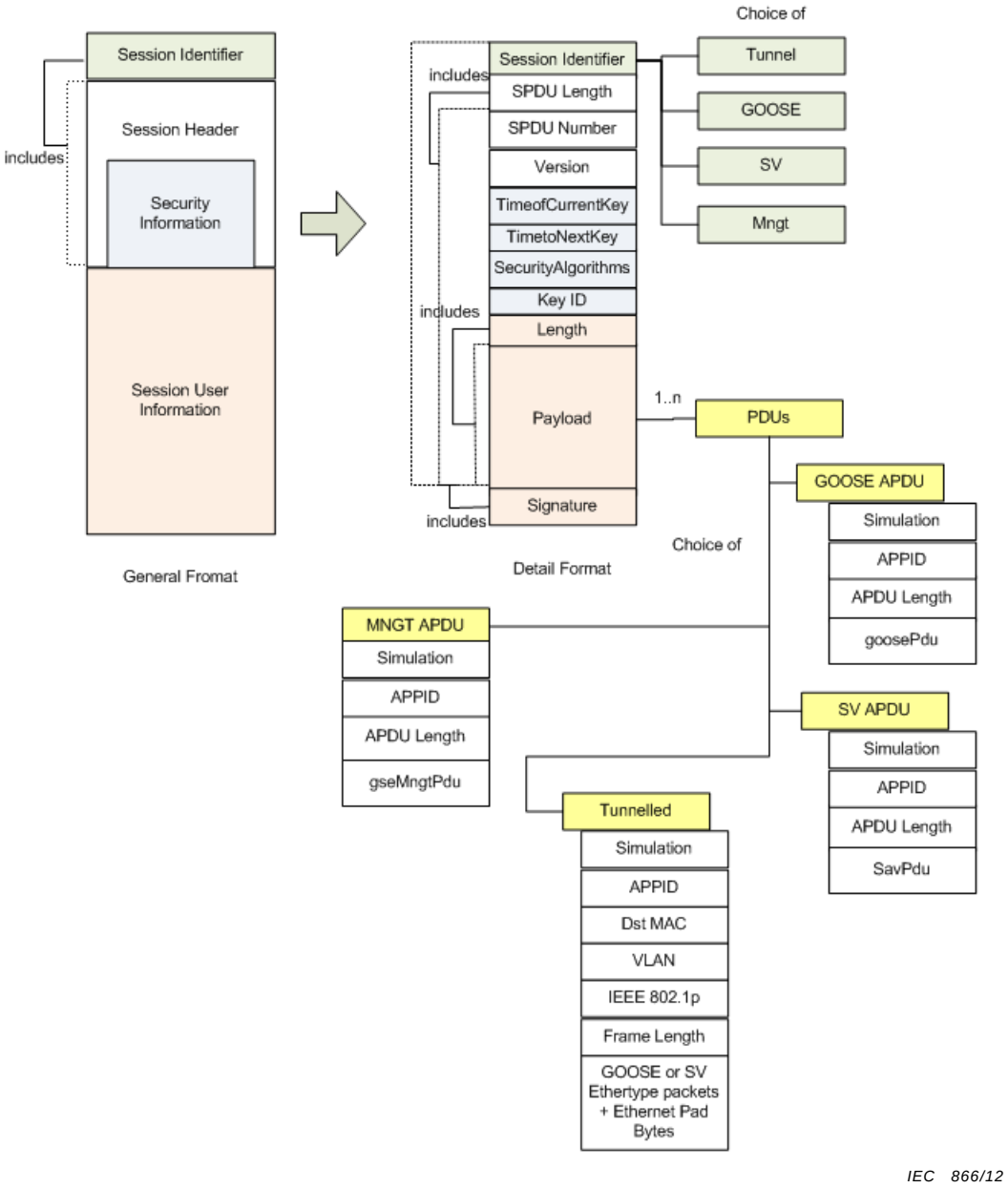


Figure 25 – Structure of IEC/TR 61850-90-5 session protocol

Figure 25 shows that the SI Length (LI) will provide the length of the Session Header. The Session Header shall contain the following information. The order of the information shall be as follows:

- Session Protocol Data Unit (SPDU) Length,
- Session Protocol Data Unit Number,
- Session Protocol Version Number,
- Security Information that contains:
  - TimeofCurrentKey: The time at which the current signature and encryption key was first used.
  - TimetoNextKey: A relative time that indicates the time before another key is put into use for the signature and encryption.
  - SecurityAlgorithms: Used to indicate which cipher suites and algorithms are used to generate the Signature and used to encrypt the user payload.
  - Key ID: Used to provide a reference to the key that is currently in use.

The Session Header is then followed by Session User Information. The user information contains the following sequence:

- Length: This information represents the length of the user payload.
- User Payload: This represents a sequence of GOOSE, SV, or Tunnelled packets. The actual contents are constrained based upon the actual Session Identifier.
- Signature: The contents of this field are calculated based upon the choice of security algorithms specified in the value of the SecurityAlgorithm field. The signature is calculated based upon the SPDU length including the Session Identifier, but not including the Signature itself. Specifics of this will be provided in another clause.

The following ASN.1 production is used to show the structure and future expansion capability of the session protocol, specifically the session identifier and header:

```
sessionIdentifier::= CHOICE {
        tunnelled       [0] IMPLICIT SessionHeader,
        goose           [1] IMPLICIT SessionHeader,
        sv              [2] IMPLICIT SessionHeader,
        mngt            [3] IMPLICIT SessionHeader,
        …,
        }

SessionHeader::= SEQUENCE {
        commonHeader [0] IMPLICIT OCTETSTRING,
        …,
        }
```

11.3.2.1.1 Session identifier

There are four (4) Session Identifiers defined:

- For Tunnelled GOOSE and Sampled Value Packets: The SI shall have a hexadecimal value of A0.

  This SI allows for the Payload to contain both SV and GOOSE packets. However, the Payload shall be constrained to only having a PDU type of Tunnelled.
- For SPDUs that contain non-tunnelled GOOSE APDUs: The SI shall have a hexadecimal value of A1. This SI shall constrain the Payload to contain PDU types of GOOSE APDU.
- For SPDUs that contain non-tunnelled Sampled Value APDU: The SI shall have a hexadecimal value of A2. This SI shall constrain the Payload to contain PDU types of SV APDU.
- For SPDUs that contain non-tunnelled management APDU: The SI shall have a hexadecimal value of A3. This SI shall constrain the Payload to contain PDU types of MNGT APDU.

The associated LI field, for the SI, shall be the length of the entire session header.

The standardized common session header contents shall be indicated by a PI whose value is zero (80 hexadecimal). The PV of the session header shall contain a sequence of the following values:

- SPDU Length,
- SPDU Number,
- Version,
- TimeofCurrentKey,

- TimetoNextKey,
- SignatureAlgorithm,
- Key ID.

The representation and definition of these fields follows.

11.3.2.1.2 SDPU length

The maximum size of the SPDU length is based upon the maximum packet size for UDP. Version 1 of this protocol does not support the IPv6 capability of Jumbograms and therefore the maximum UDP packet size shall be 65,535 octets. However, in future versions of this protocol, Jumbograms may be supported. Therefore, the SPDU Length value shall be a 32-bit unsigned integer value. Therefore, the SPDU Length parameter shall be four (4) octets.

Its maximum allowed value, for this version, shall be: 65,519 octets.

NOTE This maximum value is determined by

Maximum UDP size:	65 535
Number octets in UDP protocol:	- 8
Number octets in X.234:	- 2
Number octets in SI:	- 2
Number octets for common header:	- 2
Number octets for SPDU Length:	- 4
Maximum size:	65 517

Protocol data units received that have a value greater than the maximum value shall be discarded.

Examples of various SPDU length value encodings are provided in Table 7:

Table 7 – Example encodings of SPDU length

Value	Octet 1	Octet 2	Octet 3	Octet 4
1	00	00	00	01
255	00	00	00	FF
32 765	00	00	7F	FD
65 517	00	00	FF	ED

11.3.2.1.3 SPDU number

The SPDU Number is a value that can be used by the subscriber to detect duplicate or out-of-order packet delivery. The SPDU number attribute shall be four (4) octets and represent an Unsigned Integer Value whose range of values is 0 to 4 294 967 295.

The SPDU Number shall be maintained, by the sender, on a per destination basis. The initial SPDU Number sent shall be a value of zero. Subsequent SPDU Number values shall be incremented. When the maximum value is reached, the value shall start at a value of zero (0).

11.3.2.1.4 Version

The Version attribute shall contain the session protocol version number as specified by this document. The attribute value shall be two (2) octets and represent an Unsigned Integer Value.

The value assigned for the Version shall be 1.

11.3.2.2 Security related attributes

The security fields in the Session Header are described in the following subclauses.

11.3.2.2.1 TimeofCurrentKey

The TimeofCurrentKey attribute shall be four (4) octets that represent an Unsigned Integer value. The value of the attribute shall represent the SecondSinceEpoch. SecondSinceEpoch shall be the interval in seconds continuously counted from the epoch 1970-01-01 00:00:00 UTC. The value shall not be adjusted for leap seconds.

NOTE SecondSinceEpoch corresponds to the Unix epoch.

Some operating systems have a 32-bit Signed value that represents SecondsSinceEpoch (e.g. Unix). For implementations in such operating systems, it shall be the implementation's responsibility to provide the appropriate time offsets to allow the full range of the Unsigned Integer value to be used.

11.3.2.2.2 TimetoNextKey

The TimetoNextKey attribute shall be two (2) octets that represent a Signed Integer value. The value of the attribute represents the number of minutes prior to a new key being used. If the Most Significant Bit is a value of one (1), representing a negative value, it shall be used to indicate that no new key has been scheduled to be placed into service. Any positive value shall be used to indicate the number of minutes prior to the new key being placed into service.

Figure 26 shows the encoding of the unsigned integer value.

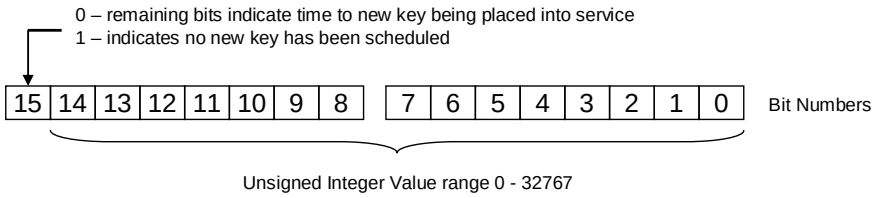


Figure 26 – Encoding of TimetoNextKey

Prior to setting a positive value, the Group Manager (e.g. IED) shall determine the new key that will be applied. This will allow the subscribers to use the Group Key Management Protocol to obtain the new assigned key prior to expiration.

The positive number shall be the relative time until the new key is put into service. Therefore, the number is decremented until the new key is in actual use. When the new key is placed into use, the TimeofCurrentKey attribute value is updated.

11.3.2.2.3 SecurityAlgorithms

The SecurityAlgorithmsN field is a two (2) octet field. The most significant octet shall be reserved to indicate the type of encryption provided.

Octet value	Encryption algorithm
0	None
1	AES-128-GCM
2	AES-256-GCM

The least significant octet shall contain the HMAC algorithm information regarding the signature generation. The value shall be one of the values from Table 9.

11.3.2.2.4 Key ID

The value of Key ID is a four (4) octet value that was assigned by the KDC as a reference to the key that is in use.

The Key ID selection shall be based upon the contents of the User Data:

- For User Data that contains payloads containing a single DataSet of information, the Key ID shall be the Key ID provided by the KDC for the particular DataSet.
- For User Data that contains payloads containing multiple DataSets, the Key ID shall be one of the Key IDs of the DataSets contained. Once the DataSet selection is made locally, the selected DataSet shall not be changed.
- For MNGT payloads, the Key ID shall be the value assigned to the DataSet provided by the KDC.

11.3.2.3 User data

The session user data consists of two fields: Length and Payload.

11.3.2.3.1 Length

The maximum size of the Length is based upon the maximum packet size for SPDU Length. The maximum value may be no greater than the SPDU Length – 14 – Signature Size.

The Length attribute shall be a four (4) octet field that is an Unsigned Integer value.

One-hundred octets shall be reserved for the Signature part of User Data.

Therefore, the allowed maximum value, for this version, is 65 399 octets.

The value shall be the length of all of the octets in the payload. It shall not include the Signature.

11.3.3 Payload

The payload section, as shown in Figure 25, allows multiple user data PDUs to be aggregated within one SPDU. The types of PDUs that can be aggregated are constrained by the Session Identifier (SI) of the SPDU (see page 73).

11.3.3.1 Common payload attributes

The payloads of GOOSE, SV, or Tunnelled have two (2) common attributes: Simulation and APPID.

The common values are part of a sequence that begins with a tag that specifies the type of payload. The values for the different payload_type_tag(s) are:

- GOOSE – shall be indicated by a tag value of 81 hexadecimal.
- SV – shall be indicated by a tag value of 82 hexadecimal.
- Tunnel – shall be indicated by a tag value of 83 hexadecimal.
- MNGT – shall be indicated by a tag value of 84 hexadecimal.

The production for the payload_type is:

```
payload_type::= SEQUENCE {
        payload_type_tag,
        simulation,
         APPID,
        ...}
```

The following subclauses define these common values.

11.3.3.2 Simulation

Simulation shall be a BOOLEAN value (e.g. one octet) and shall be as defined in IEC 61850-8-1.

11.3.3.3 APPID

The APPID shall be a two (2) octet value and shall be as defined in IEC 61850-8-1.

11.3.3.4 GOOSE payload

The GOOSE payload type is defined as:

```
GOOSE_payload_type::= SEQUENCE {
        payload_type_tag,      -- shall be a value of 81 hexadecimal
        simulation,
         APPID,
         APDU Length,
         GOOSE APDU
        }
```

The APDU Length is a two octet value, unsigned integer value, and contains the value of the number of octets of the GOOSE APDU.

A GOOSE APDU is defined as the goosePdu as defined in IEC 61850-8-1.

The normative ASN.1 productions can be found in IEC 61850-8-1 and the following are provided for information only.

```
IEC 61850-8-1 Specific Protocol::= CHOICE {
        gseMngtPdu              [APPLICATION 0] IMPLICIT GSEMngtPdu,
        goosePdu                [APPLICATION 1] IMPLICIT IECGoosePdu,
        ... }

IECGoosePdu::= SEQUENCE {
        gocbRef                 [0]   IMPLICIT VISIBLE-STRING,
        timeAllowedtoLive       [1]   IMPLICIT INTEGER,
        datSet                  [2]   IMPLICIT VISIBLE-STRING,
        goID                    [3]   IMPLICIT VISIBLE-STRING OPTIONAL,
        t                       [4]   IMPLICIT UtcTime,
        stNum                   [5]   IMPLICIT INTEGER,
        sqNum                   [6]   IMPLICIT INTEGER,
        test                    [7]   IMPLICIT BOOLEAN DEFAULT FALSE,
        confRev                 [8]   IMPLICIT INTEGER,
        ndsCom                  [9]   IMPLICIT BOOLEAN DEFAULT FALSE,
        numDatSetEntries        [10]  IMPLICIT INTEGER,
        allData                 [11]  IMPLICIT SEQUENCE OF Data,
        security                [12]  ANY OPTIONAL  -- reserved for digital signature
        }
```

11.3.3.5 Sampled value payload

The Sampled Value payload type is defined as:

```
Sampled_Value_payload_type::= SEQUENCE {
        payload_type_tag,      -- shall be a value of 82 hexadecimal
        simulation,
         APPID,
         APDU Length,
         Sampled Value APDU
        }
```

The APDU Length is a two octet value, unsigned integer value, and contains the value of the number of octets of the Sampled Value APDU.

A Sampled Value APDU is defined as the savPdu as defined in IEC 61850-9-2.

The normative ASN.1 productions can be found in IEC 61850-8-1 and the following are provided for information only.

```
IEC 61850-9-2 Specific Protocol::= CHOICE {
9-1-Pdu [0] IMPLICIT OCTET STRING, -- Reserved for 9-1 APDU
savPdu [APPLICATION 0] IMPLICIT SavPdu}

SavPdu::=  SEQUENCE {
        noASDU [0] IMPLICIT INTEGER (1..65535),
        security [1] ANY OPTIONAL,
        asdu [2] IMPLICIT SEQUENCE OF ASDU
        }
```

NOTE The savPdu and gseMngtPdu have the same ASN.1 tag (e.g. APPLICATION 0). There is no conflict since the gseMngtPdu is out of the scope of IEC/TR 61850-90-5. Since the tags for the goosePdu and savPdu are different, no additional tagging is needed for differentiation within the user payload. This is important should the specification ever need to send GOOSE and SV in a single user payload.

11.3.3.6 MNGT payload

The MNGT payload type is defined as:

```
MNGT_payload_type::= SEQUENCE {
        payload_type_tag,      -- shall be a value of 84 hexadecimal
        simulation,
         APPID,
         APDU Length,
         MNGT APDU
        }
```

The APDU Length is a two octet value, unsigned integer value, and contains the value of the number of octets of the MNGT APDU.

A MNGT APDU is defined as the gseMngtPdu.

This clause adds additional service definitions to those defined in IEC 61805-8-1. The ASN.1 productions shall be:

```
IEC 61850-8-1 Specific Protocol::= CHOICE {
        gseMngtPdu          [APPLICATION 0] IMPLICIT MngtPdu,
        goosePdu            [APPLICATION 1] IMPLICIT IECGoosePdu,
        … }

MngtPdu::= SEQUENCE {
        StateID         [0] IMPLICIT INTEGER,
        Security        [3] ANY OPTIONAL, -- reserved for future definition
        CHOICE {
                        requests        [1] IMPLICIT GSEMngtRequests,
                        responses       [2] IMPLICIT GSEMngtResponses
                        }
                }

MngtRequests::= CHOICE {
        getGoReference                  [1] IMPLICIT GetReferenceRequestPdu,
        getGOOSEElementNumber           [2] IMPLICIT GetElementRequestPdu,
        getGsReference                  [3] IMPLICIT GetReferenceRequestPdu,
        getGSSEDataOffset               [4] IMPLICIT GetElementRequestPdu,
        getSavReference                 [5] IMPLICIT GetReferenceRequestPdu,
        getSavElementNumber             [6] IMPLICIT GetElementRequestPdu,
        …
        }

MngtResponses::= CHOICE {
        gseMngtNotSupported             [0] IMPLICIT NULL,
        getGoReference                  [1] IMPLICIT GSEMngtResponsePdu,
        getGOOSEElementNumber           [2] IMPLICIT GSEMngtResponsePdu,
        getGsReference                  [3] IMPLICIT GSEMngtResponsePdu,
        getGSSEDataOffset               [4] IMPLICIT GSEMngtResponsePdu,
        getSavReference                 [5] IMPLICIT GSEMngtResponsePdu,
        getSavElementNumber             [6] IMPLICIT GSEMngtResponsePdu,
        …}

GetReferenceRequestPdu::= SEQUENCE {
        ident       [0] IMPLICIT VISIBLE-STRING,  -- size shall support up to 129 octets
        offset      [1] IMPLICIT SEQUENCE OF INTEGER DEFAULT NULL,
        datSet      [2] IMPLICIT VISIBLE-STRING OPTIONAL DEFAULT NULL,
        …
        }
```

If the offset is NULL, this shall indicate that the response shall contain all of the references if the references are able to fit in the APDU. Otherwise, the error responseTooLarge shall be returned.

If the provided datSet (DataSet Reference) does not correspond to the ident value specified, the response shall be controlBlockConfigurationError.

```
GetElementRequestPdu::= SEQUENCE {
        ident           [0] IMPLICIT VISIBLE-STRING,  -- size shall support up to 129 octets
        references      [1] IMPLICIT SEQUENCE OF VISIBLE-STRING,
        datSet          [2] IMPLICIT VISIBLE-STRING OPTIONAL DEFAULT NULL,
        …}
```

If the provided datSet (DataSet Reference) does not correspond to the ident value specified, the response shall be controlBlockConfigurationError.

```
GSEMngtResponsePdu::= SEQUENCE {
        ident           [0] IMPLICIT VISIBLE-STRING, -- echos the value of the request
        confRev         [1] IMPLICIT INTEGER OPTIONAL,
        CHOICE {
                responsePositive [2] IMPLICIT SEQUENCE {
                        datSet  [0] IMPLICIT VISIBLE_STRING OPTIONAL,
                        result   [1] IMPLICIT SEQUENCE OF RequestResults
                        },
                 responseNegative [3] IMPLICIT GlbErrors
                },
        …
        }

RequestResults::=       CHOICE {
                        offset          [0] IMPLICIT INTEGER,
                        reference       [1] IMPLICIT IA5STRING,
                        error           [2] IMPLICIT ErrorReason
        }


GlbErrors::= INTEGER {
        other(0),
        unknownControlBlock(1),
        responseTooLarge(2),
        controlBlockConfigurationError (3),
        …
        }




ErrorReason::= INTEGER {
        other (0),
        notFound (1),

        …
        }
```

The MNGT APDU shall only be used with unicast addresses (source and destination). It shall contain request/responses for a single DataSet.

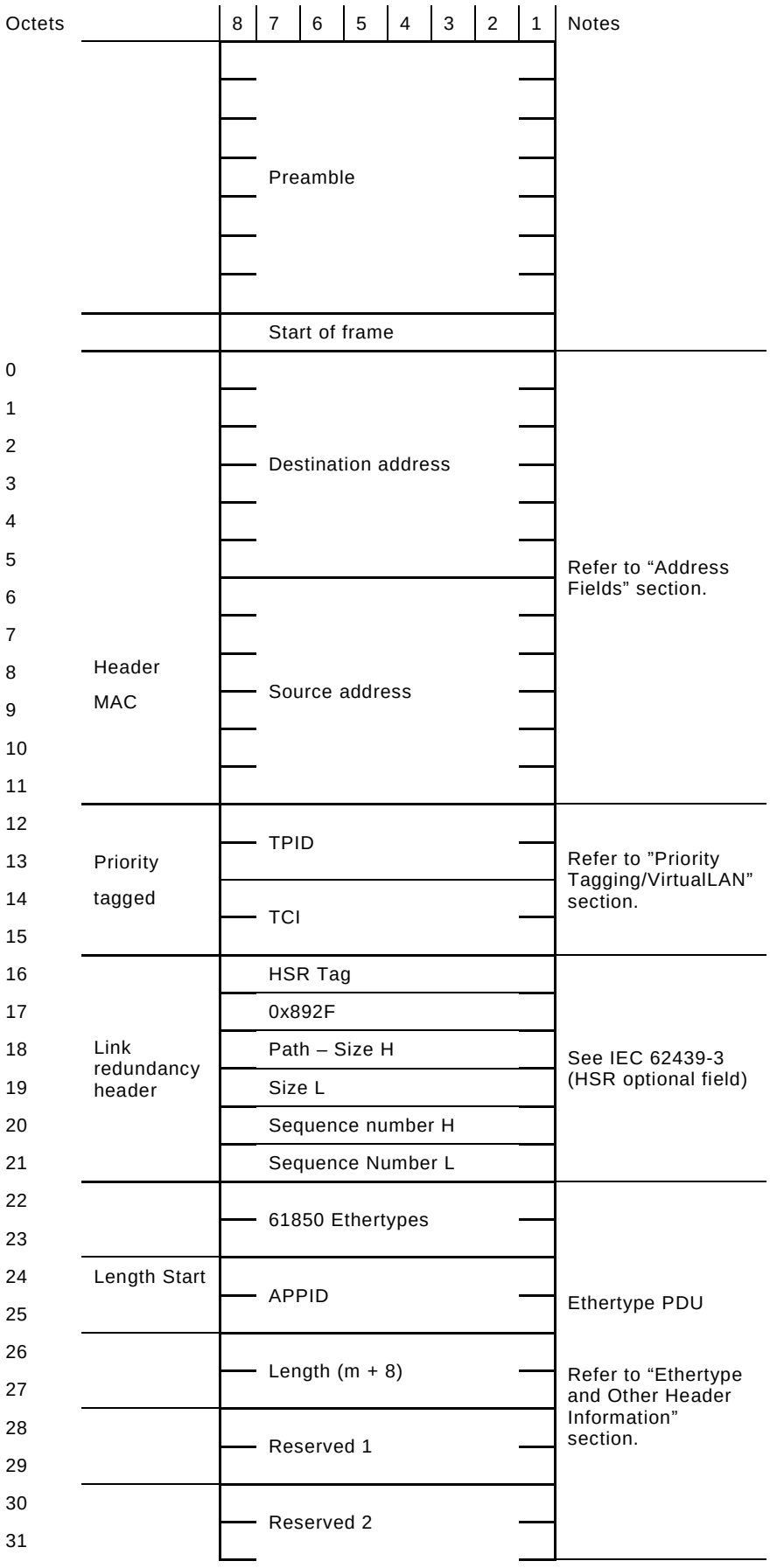
11.3.3.7 Tunnelled

The tunnelled payload PDUs need to provide the key information required to re-emit the appropriate frames at the end of the tunnel(s). In order to accomplish this, the following information needs to be conveyed:

- Destination Address: This is the multicast destination Media Access Control (MAC) address that the original GOOSE or SV message was sent to via Ethernet multicast.
- TPID and TCI: This is the VLAN tagging for VLAN identification as well as IEEE priority tagging.

61850 Ethertype PDU and Ethernet padding: This information represents the Ethernet 61850 Ethertype field and associated information. In addition to the 61850 Ethertype PDUs, the Ethernet padding needs to be included so that IEC/TS 62351-6 security information can be conveyed.

In Figure 27, the Ethertype PDU starts at octet 22 and includes all other octets except the Frame Check Sequence.



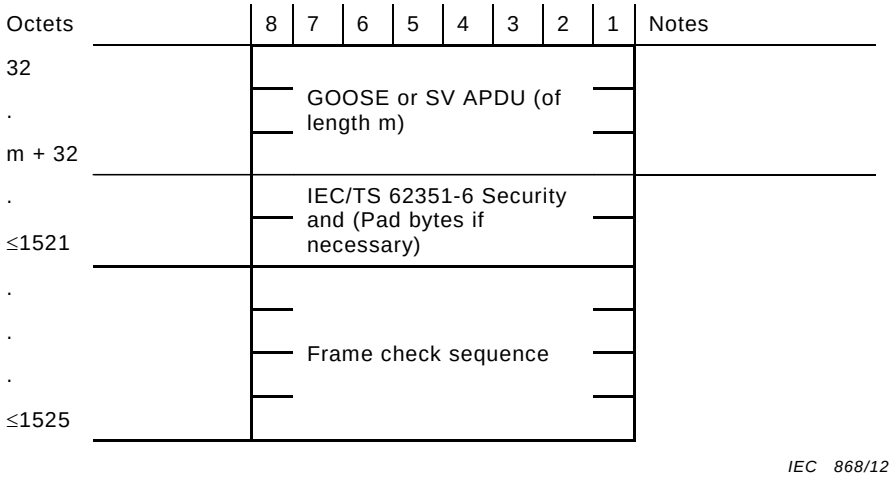


Figure 27 – IEEE 802.3 frame format for SV and GOOSE

The assigned IEC 61850 Ethertype values are shown in Table 8. The Ethertype values for GOOSE Type 1, GOOSE Type 1A, and Sampled Values shall be allowed to be conveyed as part of the tunnel. The GSE Management Ethertype, and its associated PDUs, is excluded from use within the tunnel. Table 8 shows the Ethertype values that are allowed to be tunnelled.

Table 8 – IEC 61850 Ethertype values

Use	Ethertype value (hexadecimal)	Comment
IEC 61850-8-1 GOOSE Type 1	88-B8	
IEC 61850-8-1 GSE Management	88-B9	Out of the scope of this standard
IEC 61850-9-2 Sampled Values	88-BA	
IEC 61850-8-1 GOOSE Type 1A	88-B8	

The tag indicating a tunnelled GOOSE or SV PDU shall be 83 hexadecimal.

The tunnelled payload extends the common payload production to include destinationMACAddress, TPIDandTCI, tunnelledPduLength, and the actual tunnelled PDU.

```
tunnelled_payload::= SEQUENCE {
        payload_type_tag,  -- shall be a value of 83 hexadecimal
        simulation,
        APPID,
        destinationMACAddress,
        TPIDandTCI,,
        tunnelledPduLength,
        tunnelledPdu
}
```

11.3.3.7.1 destinationMACAddress

The destination Media Access Control (MAC) address field shall be six (6) octets in size. It shall contain the original MAC address that the tunnelled PDU was sent to. The value shall be in transmission order as defined by ISO/IEC 8802-3:2000.

11.3.3.7.2 TPID and TCI

The structure of the tag header is defined in Figure 28.

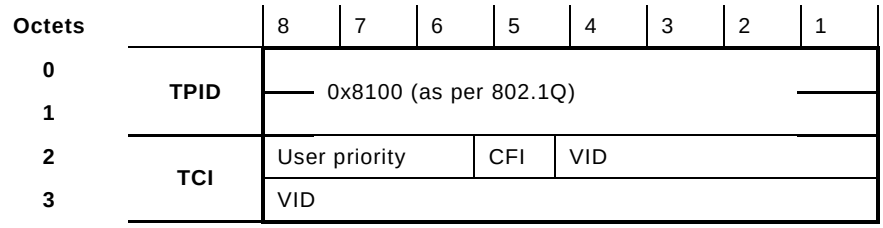


Figure 28 – Virtual LAN Tag

TPID (Tag Protocol Identifier) Field: Indicates the Ethertype assigned for 802.1Q Ethernet encoded frames. This value shall be 0x8100.

TCI (Tag Control Information) Fields: User Priority: BS3; user priority value shall be set by configuration to separate sampled values and time critical protection relevant GOOSE messages from low priority busload. If the priority is not configured, then the default values shall be used.

CFI (Canonical Format Indicator): BS1 [0]; a single bit flag value. For this standard, the CGI bit value shall be reset (value = 0).

NOTE If set (value = 1), an Embedded Resource Identification Field (E-RIF) follows the Length/Type field in the ISO/IEC 8802-3 tagged frame.

VID: The use of Virtual LAN support is optional. If this mechanism is used, the VLAN Identifier (VID) shall be set by configuration; if it is not used, it shall be set to zero (0).

The TPIDandTCI field shall be four (4) octets and shall contain the values received by the subscriber (e.g. publishing end of the tunnel). The Ethernet transmission order, as shown in Figure 28 shall be maintained. However, due to some system designs, the information may not be received by the subscriber. In this case, all octets shall be set to a value of zero (0).

It is recommended that the receiving entity, of a tunneled PDU, has the ability to re-map the TPID and TCI information as needed by the local LAN segment. This mapping should include the capability of mapping zero (0) values. This mapping function is a local issue and out of the scope of this standard.

11.3.3.7.3 tunnelledPduLength

The tunnelledPduLength field shall be an unsigned integer value of two (2) octets. The value shall be the number of octets in the tunnelledPdu. The length shall include the IEC 61850 Ethertype octets through all other octets except the Frame Check Sequence as shown in Figure 27.

11.3.3.7.4 tunnelledPdu

This field is the number of octets specified by the tunnelledPduLength field.

11.3.4 Signature

The Signature production shall start with a one octet tag of a value of 85 hexadecimal. The following octet shall be the length of the calculated signature. The third octet shall be the most significant byte of the calculated signature value.

The calculated signature value shall be used for the authentication/integrity of the octets that include the Session Identifier through the end of the user data payload. The signature.calculations shall not include the Signature production. The value of the parameter shall be calculated based upon the HMAC algorithm in RFC 2104.

The value of the HMAC and Signature production shall be treated as ASN.1 OCTETString values.

The allowed HMAC functions are: H, HMAC-SHA256, and AES-GMAC.

Additionally, the calculated HMAC value may be truncated, per RFC 2104. The allowed truncations are 80, 128, and 256 bits.

Therefore, the HMAC enumerated values, used in the Security Algorithm field (see 11.3.2.2.3) shall be as defined in Table 9.

Table 9 – Allowed values for MAC signature value calculations

Enumerate value	HMAC algorithm	Number of bits	Designation	Mandatory (m), Optional (o)
0	None	None	MAC-None	c1
1	SHA-256	80	HMAC-SHA256-80	m
2	SHA-256	128	HMAC-SHA256-128	m
3	SHA-256	256	HMAC-SHA256-256	m
4	AES-GMAC	64	AES-GMAC-64	m
5	AES-GMAC	128	AES-GMAC-128	m
c1 – Shall only be used when encryption is also in use.				

The MAC-None option is provided for testing and shall not be used in production systems. It indicates that no signature value (e.g. MAC) is being calculated. Therefore, for MAC-None, the length octet of the signature production shall contain a value of zero (0).

When a truncated value is used, the leftmost bytes of the computed value shall be used as the value known as a Message Authentication Code (MAC). The output length shall be no less than eight (8) octets.

The periodicity between rekey is related to the strength of the MAC. In particular, the guidance for AES-GMAC needs to be evaluated. The relevant document is NIST Special Publication 800-38D (http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf) *(website checked 2012-04-02)*.

The action due to detection of an invalid signature being received is a local issue. It is recommended that the information not be processed and that some type of security related event be triggered. The event type is a local issue but could be per IEC/TS 62351-7 and/or the incrementing of AuthFail attribute of a GSAL Logical Node.

11.3.5 ITU X.234 A-Profile options

ITU X.234 defines several transport parameters. Subclause 11.3.5 specifies the parameters that shall be supported and lengths for those parameters.

Transport parameter description	Parameter value (decimal)	LI value	Mandatory/Optional/ eXcluded	Comment
Source TSAP	193	1	X	Used to identify the application emitter within a node.
Destination TSAP	194	1	X	
Checksum	195		X	
User Data			M	

The variable parts of X.234 shall not be used within this standard. Therefore, only the LI and UD fields shall be present (e.g. 2 octets).

11.4 KDC Profile

The IEC/TR 61850-90-5 KDC profile is based upon RFC 3547: Group Domain of Interpretation (GDOI). This RFC makes use of ISAKMP (RFC 2407) as part of the key request and exchange mechanism. RFC 2407 allows user/private extensions in several areas, two of which IEC/TR 61850-90-5 makes use of:

a) The identification payload (5.1 of RFC 3547): The payload identifier indicates the information stream type for which a key is being requested.

b) The identification of the key payload (5.5 of RFC 3547): The Key Payload Type identifier indicates the type of the key being returned.

There are three phases of communication for GDOI for what is known as a GROUPKEY-PULL:

- Phase 1: Connection establishment and Authorization
- Although there are two mechanisms of Authentication allowed by GDOI, IEC/TR 61850-90-5 implementations shall support the ability to use the GDOI client certificate credentials exchanged at connection establishment time.
- Phase 2: Determining the policies in use for the group that is being requested.
- This is accomplished through a GDOI Identification Payload Request. The KDC responds to this request with the policies (e.g. encryption and signature algorithms) that are supported. The policies are returned using GDOI SA which returns a SA KEK payload.
- If the client does not support the policies, the client shall abort (e.g. close the TCP connection). If the client can support the policies, the client will issue the Key Download (KD) payload request.
- Phase 3: Obtain the keys to be utilized.
- This is accomplished through the request of the appropriate KD payload.

The following subclauses detail the IEC/TR 61850-90-5 extensions to RFC 3547 for Phase 2 and Phase 3.

11.4.1 Signature Hash algorithm

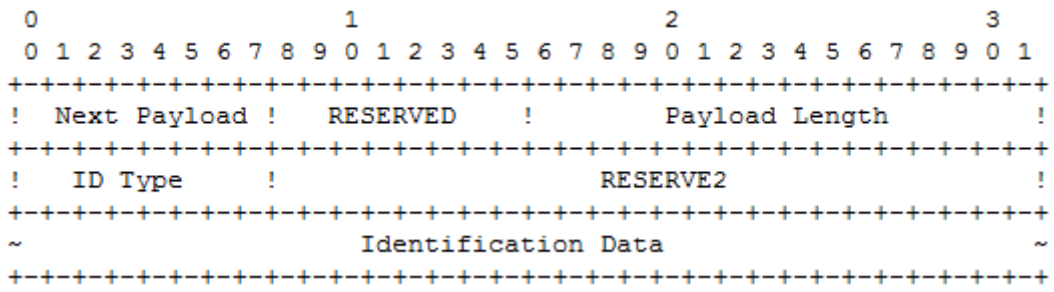
RFC 3547 allows several different signature hash algorithms to be supported (see 5.3.6 of RFC 3547). The RFC 3547 specified algorithms are shown in Table 10.

Table 10 – RFC-3547 assigned Hash identifiers

Algorithm type	Value
RESERVED	0
SIG_HASH_MD5	1
SIG_HASH_SHA1	2
RESERVED	3-127
Private Use	128-255

Implementations claiming conformance with IEC/TR 61850-90-5 shall provide support for SIG_HASH_SHA1 and SIG_HASH_SHA256. The Algorithm Type Value of 192 (decimal) shall be used to indicate SIG_HASH_SHA256.

11.4.2 Identification payload



The GDOI Identification Payload (e.g. Phase 2 request) is shown in IEC/TR 61850-90-5 defines a specific ID Type value and a format of the Identification Data.

Subclause 5.4 of RFC 3547 specifies the following payload identifiers shown in Table 11:

Table 11 – RFC-3547 assigned payload identifiers

Identifier name	Value
Reserved	0-10
ID_KEY_ID	11
RESERVED	12-127
Private Use	128-255

IEC/TR 61850-90-5 shall assign the following additional payload identifier. This identifier shall be 161 (decimal).This identifier shall be used to identify a sequence of octets that define a payload extension. This extension mechanism is designed to allow other protocols or organizations to make use of the IEC/TR 61850-90-5 payload extension. The general sequence for the payload extension is shown in Figure 29.

Octet	Definition/value	Description
0	161 decimal A1 hexadecimal	Identifier for payload extension.
1	Length of payload	
2		
3	80 (hexadecimal)	Tag indicating that the next field is an Object Identifier
4	n	Length of Object Identifier
5...5+n-1		Object Identifier Value encoded per ASN.1
5+n		Length of payload
5+n+1		
5+n+2		Start of Payload

IEC 870/12

Figure 29 – General format for IEC/TR 61850-90-5 payload extensions

The general format consists of:

- Identifier of the payload extension. This shall be 161 decimal.
- Length of the payload extension: This shall be a two (2) octet value. The Most Significant Byte shall be octet number 1. The value shall be an unsigned integer.
- Object Identifer Tag: This octet shall be 80 hexadecimal and shall be used to indicate that the following octets contain the length and value of an ASN.1 encoded Object Identifier.
- Length of Object Identifer: This length shall be an unsigned integer value and shall specify the number of octets of the ASN.1 encoded ObjectIdentifier, whose value follows the length.
- ObjectIdentifer: This set of octets represents an ASN.1 encoded ObjectIdentifier. The value of the identifier defines the payload that follows. It is the use of this ObjectIdentifier that will allow other organizations or standards to utilize this payload extension process without definition collision.

  The ObjectIdentifer values used by IEC/TR 61850-90-5 are defined in Table 12.

  KDCs claiming conformance to this document shall support the identifiers that are marked as mandatory (e.g. m).

Table 12 – IEC/TR 61850-90-5 assigned payload identifiers

Object identifier name	Description	Value	m/o
61850_ETHERNET_GOOSE	Specifies that the payload is requesting a key for an IEC 61850-8-1 GOOSE APDU, with IEC/TS 62351-6 signature, that is being sent to a particular destination Ethernet address.	1.2.840.10070.61850.8.1.1	o
61850_UDP_ADDR_GOOSE	Specifies that the payload is requesting a key for an IEC/TR 61850-90-5 GOOSE APDU that is being sent to a particular destination IP address.	1.2.840.10070.61850.8.1.2	m
61850_UDP _Tunnel	Specifies that the payload is requesting a key for an IEC/TR 61850-90-5 Tunnel APDU that is being sent to a particular destination IP address.	1.2.840.10070.61850.8.1.4	m

Object identifier name	Description	Value	m/o
61850_ETHERNET_SV	Specifies that the payload is requesting a key for an IEC 61850-9-2 SV APDU, with IEC/TS 62351-6 signature, that is being sent to a particular destination Ethernet address.	1.2.840.10070.61850.9.2.1	o
61850_UDP_ADDR_SV	Specifies that the payload is requesting a key for an IEC/TR 61850-90-5 SV APDU that is being sent to a particular destination IP address.	1.2.840.10070.61850.9.2.2	m
61850_IP_ISO9506	Specifies that the payload is requesting a key for an IEC 61850-8-1 ISO 9506 endpoint. This payload definition is out of the scope of this Technical Report.	1.2.840.10070.61850.8.1.4	o

11.4.3 Payload identification

The following subclauses detail the IEC/TR 61850-90-5 payload identification values,

11.4.3.1 Common payload values

In order to achieve common and reusable definitions, each payload may be constructed from the following definitions.

11.4.3.1.1 VERSION

This is a single octet value that represents the version of the particular payload. Unless otherwise specified, the value of the VERSION shall be one (1).

11.4.3.1.2 DEST_MULTICAST_ETHERNET_ADDRESS

This is a value that consists of six (6) octets. The value shall be specified per Ethernet transmission order.

11.4.3.1.3 IP_ADDRESS

This value component allows the specification of either an IPv4 or IPv6 destination address for which a key is being requested. The value component is a structure consisting of:

```
IP_ADDRESS::= {
        type_of_address      TYPE_OF_ADDRESS_ENUMERATION,
        is_DNS_address       BOOLEAN.
        length_of_address    UNSIGNED INTEGER16,
        address              octet[length_of_address]
        }
```

where:

TYPE_OF_ADDRESS_ENUMERATION: has the values of IPv4(0) and IPv6(1).

is_DNS_address: shall be FALSE if the IP address is numeric. The value shall be TRUE if the address represents a DNS string.

length_of_address: specifies the number of octets contained in the address value. If is_DNS_address is TRUE, the length shall not include a terminating NULL character.

address: contains the value of the IP address.

	Bit number									
Octet number	0	1	2	3	4	5	6	7	8	9
0	type_of_address									
1	is_DNS_address									
2	length_of_address(n)									
3										
4	address									
3+n										

11.4.3.1.4 DATASET

The DATASET value component allows the specification of an IEC 61850 DataSet Reference (DSRef), as specified in IEC 61850-7-2.

```
DATASET::={
        length_of_DataSet_Reference     UNSIGNED INTEGER8,
        dataSet_Reference               octet[length_of_DataSet_Reference]
        }
```

11.4.3.2 61850_UDP_ADDR_GOOSE and 61850_UDP_ADDR_SV

The payload for the IP versions of GOOSE and SV are the same. The payload is defined as:

```
Payload Identification::= {
        version         VERSION,
        ip_address      IP_ADDRESS,
        dsRef           DATASET
}
```

11.4.3.3 61850_UDP_Tunnel

The payload for the IEC/TR 61850-90-5 Tunnel session protocol is defined as:

```
Payload Identification::= {
        version         VERSION,
        ip_address      IP_ADDRESS
}
```

The reason that the dsRef is not present is that multiple Ethernet multicast frames (e.g. GOOSE or SV) may be sent in one Tunnel SPDU. Therefore, only the destination IP address allows for differentiation.

11.4.3.4 61850_ETHERNET_GOOSE and 61850_ETHERNET_SV

The payload for the Ethernet versions of GOOSE and SV are the same. The payload identification is defined as:

```
Payload Identification::= {
        version         VERSION,
        dstMAC          DEST_MULTICAST_ETHERNET_ADDRESS,
        dsRef           DATASET
}
```

11.4.3.5 61850_IP_ISO9506

This payload identification is out of the scope of this Technical Report.

11.4.3.6 Common IEC/TR 61850-90-5 payload response field definitions

The IEC/TR 61850-90-5 fields defined, for payload responses, are:

- Protocol ID (Prot-ID): Shall be the value of 161 decimal to indicate the use of IEC/TR 61850-90-5.
- Tag: Is the ASN.1 Tag, specified by IEC/TR 61850-90-5 to represent the Object Identifier that was requested by the client.
- Length of OID: ASN.1 length of the Objective Identifier value.
- ASN.1 for OID: The ASN.1 encoded value for the Object Identifier.
- Current Key ID (Cur KeyID): Shall be one (1).
- SA Life Type ID (RFC 2407): Specifies the time-to-live for the overall security association. When the SA expires, all keys negotiated under the association (AH or ESP) must be renegotiated. The SA Life Type ID field shall be one (1).
- SA Life Type Value: The life type values are:

RESERVED	0
seconds	1
kilobytes	2

The value shall be one (1) indicating the lifetime is specified in seconds.

- Remaining LifeTime Value: shall specify the number of seconds prior to the next scheduled key change. A value of zero (0) shall indicate that no key change has been scheduled.
- Authentication Algorithm ID (RFC 2407): Shall be five (5).
- Authentication Algorithm Value: Shall be one of the following set of values:

  HMAC-SHA256 value of 61440

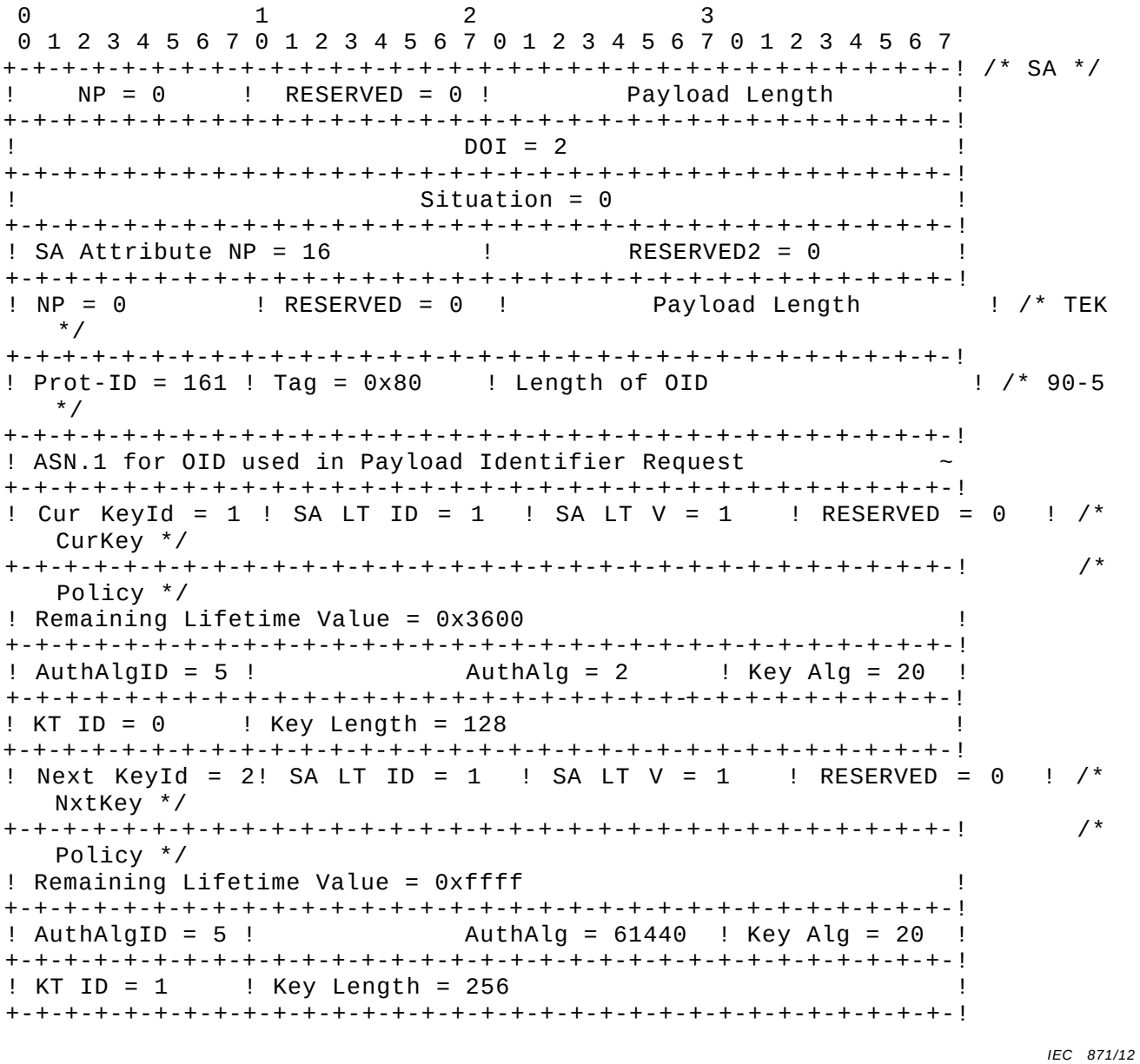
  AES-GMAC-128 value of 61441
- Key Algorithm: Shall be 20 (decimal) and shall be used to indicate that the next octet shall contain the Key Algorithm identification for the current key that is in use.
- Key Type ID: Shall be one of the following values:

  0 – AES 128 1 – AES 256
- Key Length ID: As defined in RFC 2407. Used to indicate the current key length size.
- Next Key Length: number of octets of the key value.
- Current Key Key: The actual key being used currently. The number of octets is governed by the Key Length that was specified.

- Next Key ID: shall be 21 (decimal) and shall indicate that the payload contains another key that should be used when the current key expires.
- Key LifeTime Value: shall specify the number of seconds prior to the next scheduled key change. A value of zero (0) shall indicate that no key change has been scheduled.
- Next Key Key: The next key to be used. The number of octets is governed by the Next Key Length that was specified.

11.4.4 Policy response

The policy response shall be of the template:



IEC 871/12

Figure 30 – Policy response frame

Figure 30 shows the field definitions and example values for a policy response frame.

The RFC 3547 field definitions are as follows:

- Next Payload (NP): Shall be zero (0) as specified as RFC 3547.
- Payload Length: Length of the message as defined in RFC 3547.

- Domain of Information (DOI): Shall be two (2) to specify the GDOI protocol as specified in RFC 3547.
- Situation: Shall be zero (0) as specified in RFC 3547.
- SA Attribute Next Payload: The definition, per RFC 3547, are decimal values:
  - 15 – SAK Payload,
  - 16 – SAT Payload.

The definitions of the IEC/TR 61850-90-5 specific values are defined in 11.4.3.6.

The octets following, and including the Next Key octet, shall not be present in the Key Payload under the following conditions:

a) If the Payload is being pushed to group members.

b) If the authentication credential of the client expires prior to the expiration of the current key.

c) If the next key has not been assigned or computed.

11.4.5 Key download payload

Clause 5.5 of RFC 3547 specifies the general format for the group keys that are to be provided to group members. The key download (KD) Type allows for the definition of private key download formats, the range of allowed values is shown in Table 13. It is this extensibility that IEC/TR 61850-90-5 will utilize.

Table 13 – RFC-3547 key download type identifiers

Identifer name	Value
Reserved	0
TEK	1
KEK	2
LKH	3
RESERVED	4-127
Private Use	128-255

The Key Download (KD) Payload identifiers, for IEC/TR 61850-90-5, shall specify several identifiers. These identifiers will be assigned from the Private Use range of identifiers (128-255). The private use range shall be used as standardized identifiers within the domain of IEC/TR 61850-90-5. The following numbers shall be used, as defined in Table 14:

Table 14 – IEC/TR 61850-90-5 key download type identifiers

KD type identifier name	Value
61850_ETHERENT_GOOSE_OR_SV	192
61850_90_5_SESSION	193
61850_8_1_ISO9506	194
61850_UDP_IP_AGGR	195
61850_UDP_MNGT	196

11.4.5.1 Common key payload for current and next keys

Within the scope of IEC/TR 61850-90-5, there is a recognized need to provide authenticated clients with the current key and the next key that is intended to be used. The payload containing both of these keys shall be:

0								1								2								3							
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
SA Life Type ID								SA Life Type Value								Reserved – shall be zero (0)															
Remaining Lifetime Value																															
Authentication Algorithm ID								Authentication Algorithm																Key Algorithm							
Key Type ID								Key Length ID								Key Length															
Current Key Key																															
Current Key ID																															
Next Key ID								SA Life Type ID								SA Life Type Value								Reserved– shall be zero (0)							
Key Lifetime Value																															
Authentication Algorithm ID								Auth Alg. Value																Key Algorithm							
Key Type ID								Key Length ID								Next Key Length															
Next Key Key																															
Next Key ID																															

IEC 872/12

Figure 31 – Key download response payload definition

Figure 31 depicts the format of an IEC/TR 61850-90-5 Key Download Response Payload. The definitions of the fields can be found in 11.4.3.6.

The octets following, and including the Next Key octet, shall not be present in the Key Payload under the following conditions:

a) If the payload is being pushed to group members.

b) If the authentication credential of the client expires prior to the expiration of the current key.

c) If the next key has not been assigned or computed.

Clients that receive the key download response shall compare the policies of the key download with the actual policy response. If policies do not match, the client shall discard the information.

The Current Key and Next Key ID values are generated by the KDC to identify the key. This value is used in the Session protocol to identify the key that is actually in use. The value is a four (4) octet value and not an integer. The values shall be unique within the lifetime value and download type.

The maximum allowed Lifetime value shall be forty-eight (48) hours. Lifetimes for keys provided by the 61850_UDP_MNGT download type shall have a maximum allowed LifeTime value of thirty (30) minutes.

11.4.5.1.1 62351_ETHERNET_GOOSE_OR_SV key download type

The 62351_ETHERNET_GOOSE_OR_SV shall be present for Payload Identifiers (see Table 12) values 195 or 196.

The Key Payload shall be as specified in 11.4.5.1.

11.4.5.1.2 61850_90_5_SESSION key download type

The 62351_ETHERNET_GOOSE_OR_SV shall be present for Payload Identifiers (see Table 12) values 192, 193, or 194.

The Key Payload shall be as specified in 11.4.5.1.

11.4.5.2 61850_8_1_ISO9506 key download type

The 62351_ETHERNET_GOOSE_OR_SV shall be present for the Payload Identifiers (see Table 12) value 197. The actual format of this payload is out of the scope of this Technical Report.

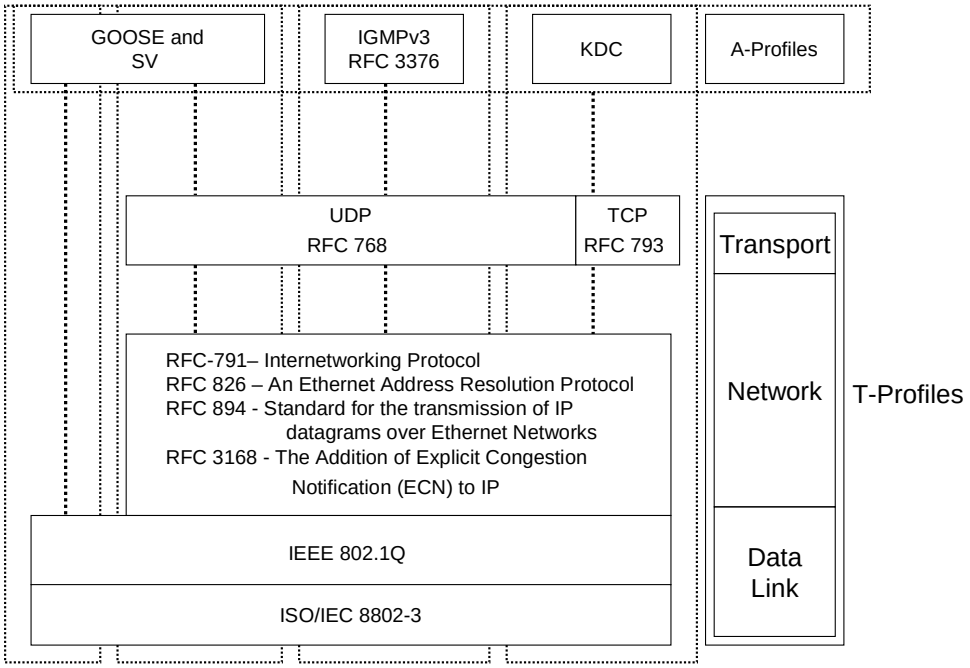
11.5 Internet group management protocol version 3 A-Profile

IGMP version 3 (RFC 3376 shall be supported by implementations that are subscribers for the routable GOOSE and SV as specified in 11.3.

11.6 T-Profiles

11.6.1 General

There are three (3) different A-Profiles, as specified in IEC/TR 61850-90-5. Each of these A-Profiles makes use of three (3) independent Transport Profiles (T-Profiles). The correlation between the A-Profiles and T-Profiles is shown in Figure 32.



IEC 873/12

Figure 32 – A-Profile association to various T-Profiles

Figure 32 shows that the various T-Profiles have common elements for the Network and Layer 2 layers. However, there are some differences within the Transport layer.

The following subclauses detail the differences between the T-Profiles required to support the various A-Profiles.

11.6.2 T-Profile to support GOOSE and SV A-Profile over Ethernet

This T-Profile shall be as specified in IEC 61850-8-1 and IEC 61850-9-2, respectively. This T-Profile is utilized to create an IEC/TR 61850-90-5 Tunnel as specified by the Session layer within this document.

11.6.2.1 T-Profile to support GOOSE and SV A-Profile (UDP)

The T-Profile, supporting the GOOSE and SV A-Profile, includes:

Protocol	Description	m/o
UDP – RFC 768	User Datagram Protocol	m

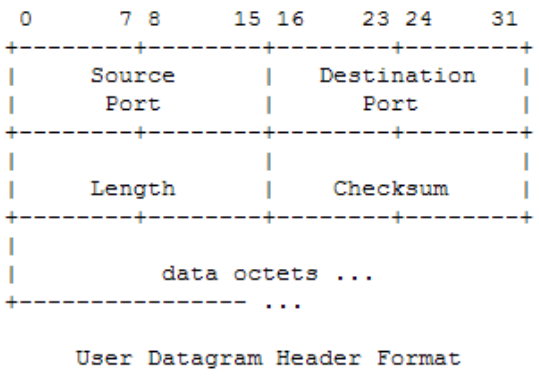


Figure 33 – From RFC 768

Figure 33 is a normative extract from the UDP specification (RFC 768). The Destination Port shall be port 102 as prescribed by RFC 1240. The source port shall be locally assigned and the specification of these is out of the scope of this Technical Report.

Table 15 – UDP field implementation requirements

UDP	Mandatory/Optional/ eXcluded
Source Port	M
Destination Port	M
Length	M
Checksum	M

Table 15 specifies that all of the RFC 768 fields shall be implemented and transmitted.

11.6.2.2 IEEE quality of service (IEEE 802.1Q)

Implementations claiming conformance to this standard shall provide a transport service data interface that allows for the Destination IP Address, VLAN, and the Ethernet Class of Service to be specified.

11.6.3 T-Profile to support KDC (TCP and UDP)

The T-Profile, supporting the GOOSE and SV A-Profile, includes:

Protocol	Description	m/o
TCP – RFC 793	Transmission Control Protocol	m
UDP – RFC 768	User Datagram Protocol	m

The destination port, for GDOI requests, shall be 898 as assigned by IANA. The source ports shall be locally assigned and the specification of these is out of the scope of this Technical Report.

11.6.4 T-Profile to support IGMPv3

The T-Profile, supporting the GOOSE and SV A-Profile, includes:

Protocol	Description	m/o
UDP – RFC 768	User Datagram Protocol	m

The Destination Port shall be port 465 as prescribed by RFC 1240. The source port shall be locally assigned and the specification of these is out of the scope of this Technical Report.

11.6.5 Common T-Profile standards

11.6.5.1 General

The following subclauses describe the common set of T-Profile standards that are to be utilized.

11.6.5.2 IPv4 based network layer (mandatory)

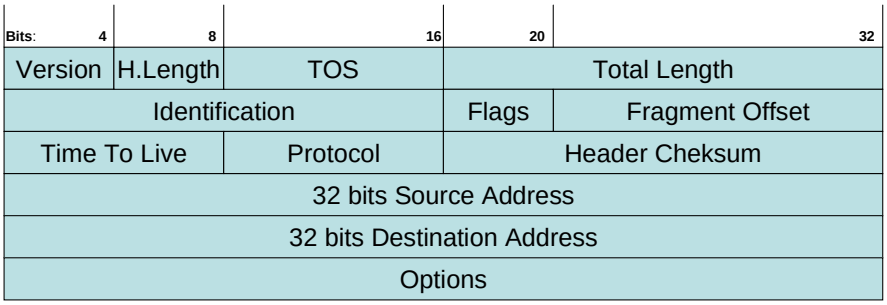
The Network Layer protocols are common between the T-Profiles. However, the network layer may be differentiated into support for IPv4 and IPv6 (see Annex D). Implementations claiming conformance to this Technical Report shall support IPv4 at a minimum.

Implementations claiming conformance to this Technical Report shall implement the network layer protocols shown in Table 16.

Table 16 – Network protocol conformance implementation statement (PICS) for IPv4 based T-Profiles

Protocol	Description	m/o
RFC 791	Internetworking Protocol	m
RFC 826	An Ethernet Address Resolution Protocol	m
RFC 894	Standard for the transmission of IP datagrams over Ethernet Networks	m
RFC 3168	The Addition of Explicit Congestion Notification (ECN) to IP	m

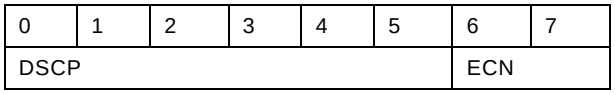
The following subclauses specify additional constraints based upon that shall be implemented for by implementations claiming conformance to this Technical Report.



IEC 875/12

Figure 34 – Format of IP header

The fields of the IP Header, as defined in RFC 791, are shown Figure 34. Treatment of packets under congestion can be signalled using information contained in what was originally referred to as the TOS (Type of Service) field (8-bits in length). This field is now treated as consisting of two sub-fields, DSCP (Differentiated Services Code Point) and ECN (Explicit Congestion Notification). The format for the TOS field is shown in Figure 35.



IEC 876/12

Figure 35 – ToS byte field definition RFC-2474 and RFC-3168

The DSCP field can be used to signal a particular treatment for a specific packet along its end-end path through the network. At each hop, or router, the DSCP can be used to implement a particular per-hop-behaviour (PHB) for the packet. The DSCP field can be set when the packet is first transmitted by the originating host or it can be changed at any hop in the network, depending on the implementation, in order to change the relevance of a particular packet with regard to other packets (or traffic) at different points in the network (e.g. at edge-core boundary within a domain or at a domain boundary).

How different types of traffic are treated within a particular domain must be relevant to the policy set forth in the domain. Recommendations are available from various router vendors regarding baseline settings for DSCP values for particular traffic classes (e.g. VoIP, Video, Data, Best Effort Traffic and others).

It is recommended that ECN bits are set per RFC 3168 by the intermediate systems. Furthermore, it is recommended that IP packets, delivered to a subscriber, indicating congestion should provide a notification to the application of packet loss. The actual notification mechanism is out of the scope of this Technical Report.

Both T- and A-Profiles merit are marked as Expedited Forwarding (EF), described in RFC 3246. Additionally, scheduling of this traffic into Low Latency Queues in order to expedite its handling versus other types of traffic is indicated.

The actual specifics for classification will depend on the particular implementation and specific mix of A- and T-Profile traffic within a utility network domain and their relative importance to problem resolution. How traffic is handled in cross-domain situations will need to be negotiated between the various domain administrations.

Additionally, RFC 791 includes the provision of an optional Security Field (e.g. one of the IP Option fields). However, the format and use of this field has been superseded by RFC 1108. Although this field is optional in RFC 791, implementations claiming conformance to this Technical Report shall implement and send this field per RFC 1108, as shown in Figure 36.

Type=130	Length	Classification Level	Protection Authority Flags

IEC 877/12

Figure 36 – Security field definition from RFC 1108

Implementations should be able to be configured with a range of values for the security field. However, the default values shall be:

- Classification Level: Confidential,
- Protection Authority Bits: Field Termination Indicator (7).

Implementations claiming conformance to this Technical Report shall be able to support unicast and multicast IP addresses. The support of IP multicast addresses shall conform to RFC 5771.

NOTE Some operating systems default the UDP/IP Time to Live (TTL) parameter value to a value of one (1) that prevents the packet from being routed. Since the intent is to have routable packets, the minimum allowed TTL needs to be specified.

The Time to Live parameter shall be set to a value of thirty-two (32), or greater, to allow the routing of the UDP/IP packets. The value of 255 shall not be used. The value shall be specified in the implementation's PIXIT.

11.6.5.3 Data link layer

Shall be as specified in IEC 61850-8-1.

Additionally, the T-Profile supporting the GOOSE and SV A-Profile shall implement IEEE 802.1Q per IEC 61850-8-1.

11.6.5.4 Physical layer

Shall be as specified in IEC 61850-8-1.

12 Effects on IEC 61850-5

The current IEC 61850-5 standard does not have sufficient time class definitions to support the synchrophasor use cases set forth within this document. Therefore, the following performance classes should be added to IEC 61850-5.

This message type includes the output data from synchronized measuring devices independent from the calculation and synchronization methods. The data will consist of continuous streams of synchronized measurements from each IED, interleaved with data from other IEDs.

Transfer time means for the stream of synchronized measurements a constant delay resulting in a delay for the functions using the measurements (e.g. for protection, visualization or other). Therefore, this transfer time shall be dependent on the requirements of the application. For protection applications, it should be small, so no negative impact on an application function is experienced.

Performance class	Requirement	Transfer time class	Transfer time	Typical for interface (IF)
P13	Delay acceptable for protection functions using the measurements in the substation	TT6	< 3 ms	IF8
P14	Delay acceptable for other functions using the measurements in the substation	TT5	< 10 ms	IF8
P15	Delay acceptable for protection functions using the measurements between substations	TT6	< 3 ms	IF11
P16	Delay acceptable for other functions using the measurements between substations	TT5	< 10 ms	IF11

13 Effects on the IEC 61850-6 (SCL)

13.1 General

There are three (3) major identified impacts on the Substation Configuration Language (SCL) as defined in IEC 61850-6. The extensions of IEC 61850-6 are required due to the need to:

- express the new IEC 61850 UDP/IP profile, as defined in this document, and the new synchrophasor functions,
- provide a mechanism to express IEEE C37.118.2 packet information configuration via SCL. This is needed to allow IEEE C37 migration to the use of IEC 61850,
- provide a mechanism to express the configuration of Phasor Data Concentrators.

Additionally, the creation of routable profiles has an impact on SCL. The following subclauses detail the extensions/changes needed.

13.2 SCL extensions to support IEC/TR 61850-90-5 defined profiles

For the purpose defined above, the following SCL enhancements are suggested:

- Indication of new SV service mapping R-SV as a sub element (Protocol) at the SV control block respective GOOSE control block (Protocol R-GOOSE) with mustUnderstand property. This allows running SV and R-SV service in parallel on the same IED, and both as a part of the IEC 61850 protocol without needing a new protocol type. The implementation as an element with mustUnderstand property prohibits usage of this control block by ‘old’ tools and IEDs which do not know the R-SV mapping.
- R-SV and R-GOOSE client capability shows that a client is able to receive appropriate messages.
- The use of IPv4 or IPv6 in the profiles also requires extensions. These additions can be found in 9.2.2.2 and 13.2.4.

The exchange of SED files and the connected engineering rights is already defined in IEC 61850-6:2009.

The description of routers and physical connections to switches and other IEDs is already defined in IEC 61850-6:2009.

See Annex B for example SCL XML.

13.2.1 General engineering process

Independent from the basic scenario (SED or IID import), the general engineering flow always contains the steps described below (side A = source substation, or PMU / protection IED; the receiving client is a PDC or an application IED in a center project):

a) identify the signals at side A to be transferred to PDC respective to center IED,

b) generate side A image in SCL (SED, IID, ICD),

c) import side A image at PDC/Center project,

d) marshall incoming signals to clients,

e) identify signals from PDC/Center to side A (if needed at all),

f) generate PDC/center IED & signal image in SCL (SED),

g) Import SED back to side A, and wire PDC/Center signals to A destinations (if needed at all).

NOTE Steps e), f), g) can be skipped, if there are no signals going down from the higher level to the source substation (side A), and can be replaced by providing a client IED file to side A for correct data flow presentation in step a) and performing step d) after step a) with the side A system tool.

13.2.2 Control block extensions

The following subclauses detail the extensions needed, within the Substation Configuration Language, to support the R-GoCB and R-MSVCB.

13.2.2.1 SV control block extensions

The SCL XSD for a SV needs to be extended to include the security field and the new R-SV service mapping, as shown in Figure 37:

```
<xs:complexType name="tSampledValueControl">
  <xs:complexContent>
    <xs:extension base="tControlWithIEDName">
      <xs:sequence>
        <xs:element name="SmvOpts">
          <xs:complexType>
            <xs:attributeGroup ref="agSmvOpts"/>
          </xs:complexType>
        </xs:element>
        <xs:element name="Protocol" fixed="R-SV" minOccurs="0">
          <xs:complexType>
            <xs:simpleContent>
              <xs:extension base="xs:normalizedString">
                <xs:attribute name="mustUnderstand"
  type="xs:boolean" use="required"
  fixed="true"/>
              </xs:extension>
            </xs:simpleContent>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
      <xs:attribute name="smvID" type="tMessageID" use="required"/>
      <xs:attribute name="multicast" type="xs:boolean" default="true"/>
      <xs:attribute name="smpRate" type="xs:unsignedInt" use="required"/>
      <xs:attribute name="nofASDU" type="xs:unsignedInt" use="optional" default="1"/>
      <xs:attribute name="smpMod" type="tSmpMod" use="optional" default="SmpPerPeriod"/>
      <xs:attribute name="securityEnable" type="scl:tPredefinedTypeOfSecurityEnum"
use="optional"
  default="None"/>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

IEC 878/12

Figure 37 – Extension to tSampledValueControl

The Protocol element may only be used with multicast SV control blocks.

NOTE that agSmvOpts needs to be extended as follows:

```
<xs:attributeGroup name="agSmvOpts">
  <xs:attribute name="refreshTime" type="xs:boolean" use="optional" default="false"/>
  <xs:attribute name="sampleSynchronized" type="xs:boolean" use="optional"
fixed="true"/>
  <xs:attribute name="sampleRate" type="xs:boolean" use="optional" default="false"/>
  <xs:attribute name="dataSet" type="xs:boolean" use="optional" default="false"/>
  <xs:attribute name="security" type="xs:boolean" use="optional" default="false"/>
  <xs:attribute name="timestamp" type="xs:boolean" use="optional" default="false"/>
</xs:attributeGroup>
```

IEC 879/12

Figure 38 – Extension to agSmvOpts

In order to utilize SV over wide areas, the timestamp attribute, shown in Figure 38, shall be True.

13.2.2.2 GSE control block extensions

The SCL XSD for a GSE Control block needs to be extended to allow for the security attribute and the new R-GOOSE service mapping. The revised XSD is shown in Figure 39:

```
<xs:complexType name="tGSEControl">
  <xs:complexContent>
    <xs:extension base="tControlWithIEDName">
      <xs:sequence>
        <xs:element name="Protocol" fixed="R-GOOSE" minOccurs="0">
          <xs:complexType>
            <xs:simpleContent>
              <xs:extension base="xs:normalizedString">
                <xs:attribute name="mustUnderstand" type="xs:boolean" use="required"
fixed="true"/>
              </xs:extension>
            </xs:simpleContent>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
      <xs:attribute name="type" type="tGSEControlTypeEnum" use="optional"
default="GOOSE"/>
      <xs:attribute name="appID" type="tMessageID" use="required"/>
      <xs:attribute name="fixedOffs" type="xs:boolean" use="optional" default="false"/>
      <xs:attribute name="securityEnable" type="scl:tPredefinedTypeOfSecurityEnum"
use="optional"
    default="None"/>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>
```

Figure 39 – Extension of tGSEControl *IEC 880/12*

13.2.2.2.1 SecurityEnable

This attribute, if present, allows an IEC 61850 client to read the current usage of security. The attribute may have the following enumerated values:

- None: No security mechanisms are in use.
- Signature: This value indicates that the Session Security Parameter will be present.
- SignatureAndEncryption: This value indicates that both Signature and Encryption is in use.

Implementations claiming conformance to this document shall support the Signature value.

If the attribute is not present in the control block(s), then there shall be no security used.

Additionally, if the attribute value of DstAddress.TransportinUse is ETHERNET, the value of the SecurityEnabled attribute shall be None.

In order to provide the proper enumeration, the SCL XSD needs to be extended with the following new enumeration. The revised XSD is shown in Figure 40:

```
<xs:simpleType name="tPredefinedTypeOfSecurityEnum">
    <xs:restriction base="xs:normalizedString">
        <xs:enumeration value="None"/>
        <xs:enumeration value="Signature"/>
        <xs:enumeration value="SignatureAndEncryption"/>
    </xs:restriction>
</xs:simpleType>
```

Figure 40 – Definition of tPredefinedTypeOfSecurityEnum *IEC 881/12*

13.2.3 KDC access point

The IEC 61850-6 SCL shall be extended to indicate if an Access Point contains a KDC function. This shall be accomplished through the addition of the “kdc” attribute as shown in Figure 41.

```
<xs:complexType name="tAccessPoint">
        <xs:complexContent>
            <xs:extension base="tUnNaming">
                <xs:sequence>
                    <xs:choice minOccurs="0">
                        <xs:element name="Server" type="scl:tServer">
                            <xs:unique name="uniqueAssociationInServer">
                                <xs:selector xpath="./scl:Association"/>
                                <xs:field xpath="@associationID"/>
                            </xs:unique>
                        </xs:element>
                        <xs:element ref="scl:LN" maxOccurs="unbounded"/>
                        <xs:element name="ServerAt" type="tServerAt"/>
                    </xs:choice>
                    <xs:element name="Services" type="scl:tServices"
minOccurs="0"/>
                    <xs:element name="GOOSESecurity" type="tCertificate"
minOccurs="0"
                                maxOccurs="7"/>
                    <xs:element name="SMVSecurity" type="tCertificate"
minOccurs="0"
                                maxOccurs="7"/>
                </xs:sequence>
                <xs:attribute name="name" type="tAccessPointName" use="required"/>
                <xs:attribute name="router" type="xs:boolean" use="optional"
default="false"/>
                <xs:attribute name="clock" type="xs:boolean" use="optional"
default="false"/>
                <xs:attribute name="kdc" type="xs:boolean" use="optional"
default="false"/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
```

IEC 882/12

Figure 41 – AccessPoint SCL production indicating a KDC function

SCL shall further be extended to indicate the KDC(s) that an IED will use. This shall be accomplished through the addition of any number of KDC elements as shown in Figure 42.

```
<xs:complexType name="tIED">
    <xs:complexContent>
      <xs:extension base="tUnNaming">
        <xs:sequence>
          <xs:element name="Services" type="tServices" minOccurs="0"/>
          <xs:element name="AccessPoint" type="tAccessPoint" maxOccurs="unbounded">
            <xs:unique name="uniqueLNInAccessPoint">
              <xs:selector xpath="./scl:LN"/>
              <xs:field xpath="@inst"/>
              <xs:field xpath="@lnClass"/>
              <xs:field xpath="@prefix"/>
            </xs:unique>
          </xs:element>
          <xs:element name="KDC" type="tKDC" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="name" type="tIEDName" use="required"/>
        <xs:attribute name="type" type="xs:normalizedString" use="optional"/>
        <xs:attribute name="manufacturer" type="xs:normalizedString" use="optional"/>
        <xs:attribute name="configVersion" type="xs:normalizedString" use="optional"/>
        <xs:attribute name="originalSclVersion" type="tSclVersion" use="optional"/>
        <xs:attribute name="originalSclRevision" type="tSclRevision" use="optional"/>
        <xs:attribute name="engRight" type="tRightEnum" use="optional" default="full"/>
        <xs:attribute name="owner" type="xs:normalizedString" use="optional"/>
      </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

IEC 883/12

Figure 42 – IED SCL XSD indicating the KDC(s) to be used

The tKDC type of Figure 43 needs to be added:

```
<xs:complexType name="tKDC">
        <xs:attribute name="iedName" type="tIEDName" use="required"/>
        <xs:attribute name="apName" type="tAccessPointName" use="required"/>
</xs:complexType>
```

Figure 43 – SCL tKDC type

13.2.4 Addressing extensions

In order to allow IPv4 and IPv6 addressing, as part of the tConnectedAP, the appropriate enumerations must first be added to the tPredefinedPTypeEnum, as shown in Figure 44:

```
<xs:simpleType name="tPredefinedPTypeEnum">
        <xs:restriction base="xs:Name">
                <xs:enumeration value="IP"/>
                <xs:enumeration value="IP-SUBNET"/>
                <xs:enumeration value="IP-GATEWAY"/>
                <xs:enumeration value="OSI-NSAP"/>
                <xs:enumeration value="OSI-TSEL"/>
                <xs:enumeration value="OSI-SSEL"/>
                <xs:enumeration value="OSI-PSEL"/>
                <xs:enumeration value="OSI-AP-Title"/>
                <xs:enumeration value="OSI-AP-Invoke"/>
                <xs:enumeration value="OSI-AE-Qualifier"/>
                <xs:enumeration value="OSI-AE-Invoke"/>
                <xs:enumeration value="MAC-Address"/>
                <xs:enumeration value="APPID"/>
                <xs:enumeration value="VLAN-PRIORITY"/>
                <xs:enumeration value="VLAN-ID"/>
                <xs:enumeration value="SNTP-Port"/>
                <xs:enumeration value="MMS-Port"/>
                <xs:enumeration value=”DNSName”/>
                <xs:enumeration value=”C37-118-IP-Port”/>
        </xs:restriction>
</xs:simpleType>
```

IEC 885/12

Figure 44 – Extension to tPredefinedPTypeEnum

The extensions are DNSName, and IPv6 syntax for the IP element. For describing the mapping of C37.118.2 IEDs, additionally, the corresponding IP port needs to be configurable as C37-118-IP-Port. The extensions result in new P-Types needing to be defined. These definitions are found in the following subclauses.

13.2.4.1 IPv6 addresses

In order to allow IPv6 addresses to be configured, the abstract type tP_IPbase needs to be extended with a pattern for IPv6. The definition is found in Figure 45. This definition supports only the standard presentation without suppression of zero fields.

```
<xs:complexType name="tP_IPbase" abstract="true">
        <xs:simpleContent>
                <xs:restriction base="tP">
                        <xs:pattern value="([0-9]{1,2}|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.([0-9]{1,2}|1[0-
9]{2}|2[0-4][0-9]|25[0-5])\.([0-9]{1,2}|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.([0-9]{1,2}|1[0-9]{2}|2[0-4][0-9]|25[0-5])"
id="IPv4"/>
                        <xs:pattern value="([0-9,a-f,A-F]{1,4}:){7}[0-9,a-f,A-F]{1,4}" id="IPv6"/>
                </xs:restriction>
        </xs:simpleContent>
</xs:complexType>
```

IEC 886/12

Figure 45 – tP_IPbase extension for IPv6 addresses

This modification will then be automatically propagated to the concrete P-Types tP_IP, tP_IP-GATEWAY, and tP_IP-SUBNET.

The default “id” type shall be IPv4 if the “id” is not present.

13.2.4.2 String representation of IP address (DNSName)

In order to provide wide area addressability between multiple addressing domains, as may be required for Wide Area Measurement systems or exchanges between utilities, a DNS string representation of an IP address may allow easier coordination between systems.

An xsi:type of tP_DNSName is shown in Figure 46. The purpose of this definition is to allow for XML tools to validate the format of the value. The definition is:

```
<xs:complexType name="tP_DNSName">
    <xs:simpleContent>
        <xs:restriction base="tP">
            <xs:pattern value="\S*"/>
            <xs:attribute name="type" type="tPTypeEnum" use="required"
fixed="DNSName"/>
        </xs:restriction>
    </xs:simpleContent>
</xs:complexType>
```

IEC 887/12

Figure 46 – Definition of tP_DNSName

13.2.4.3 IEEE C37.118 IP port definition (C37-118-IP-Port)

The implementations of IEEE C37.118.2 do not have a specified IP Port address. The general practice, in the industry, has been that each vendor/installation assigns its own destination port addresses. In order to allow IEEE C37.118.2 to be able to be represented in SCL, the P-Type of C37-118-IP-Port has been added. This P-Type shall not be used for any configuration other than IEEE C37.118.2.

The SCL type definition is found in Figure 47.

```
<xs:complexType name="tP_C37-118-IP-Portl">
  <xs:simpleContent>
    <xs:restriction base="xs:integer">
      <xs:minInclusive value="1025"/>
      <xs:maxInclusive value="65535"/>
      <xs:attribute name="type" type="tPTypeEnum" use="required" fixed=" C37-118-IP-Portl"/>
    </xs:restriction>
  </xs:simpleContent>
</xs:complexType>
```

IEC 888/12

Figure 47 – Definition tp_ C37-118-IP-Port

IANA has no defined port address for C37.118.2; only private port numbers may be used.

13.3 SCL extensions to support the configuration of IEEE C37.118.2

The C37.118.2 application level can be mapped to different lower level protocols. The mapping defined here restricts itself to a mapping onto TCP and UDP. Further mappings might be added later.

This mapping restricts on mapping process data to the IEC 61850 data model. Configuration data is not mapped, but replaced by the IEC 61850 model itself respective its SCL description. Due to the specific nature of the telegrams, which is similar to sampled value telegrams in IEC 61850, the mapping is done only to the process data values of the C37.118.2 telegrams. Any time stamped IEC 61850 data needs to derive the time from the common time stamp of the telegram, and the value quality from the appropriate quality bits as described in C37.118.2.

The mapping to the IEC 61850 vector data can be naturally made for the polar representation of phasors. If the phasor data within the telegram is rectangular, AND it shall be converted to an IEC 61850 based access model, it has to be converted by the receiving client to polar representation. If only the semantics of the data shall be communicated to the application, this is not necessary, i.e. the application must then directly handle the rectangular representation, and the SCL description is only used to transfer the semantics to the application.

The phasor data and the frequency contained in the telegram map directly to data objects of a logical node of LN class MMXU within IEC 61850. The unspecified analog and digital data in a C37.118.2 telegram can be mapped to any IEC 61850 data object fitting to the appropriate data type and carrying the needed semantic. The appropriate IEC 61850 logical node class and data object name has to be chosen to document the semantics of the value.

The IEC 61850 data object for rate of frequency needs to be defined. This definition is found in 15.4. It is modelled by an extension of the LNs PFRC, MMXU or MMXN e.g. by a data object HzRte. This is simpler to use than the first recommended method, however needs to be standardized in IEC 61850-7-4.

NOTE This version does not support the mapping of binary status data to switch positions (IEC 61850 attribute type Dbpos).

13.3.1 The underlying protocol

This mapping supports UDP and TCP as underlying protocol. All IEDs communicating with the same protocol are connected with their appropriate access point to a SubNetwork defining this protocol. The following SubNetwork types are defined for this purpose:

Protocol type	Address parameters	Remarks
C37-118-UDP	IP, IP-SUBNET, IP-GATEWAY, C37-118-IP-Port	GOOSE and SV addresses not allowed, the IP address can be a multicast address The definition of C37-118-IP-Port is found in 13.2.4.3.
C37-118-TCP	IP, IP-SUBNET, IP-GATEWAY	GOOSE and SV addresses not allowed

13.3.2 The data values

The mapping of data values shall create a relation between the values in the C37.118.2 telegram and the IEC 61850 data model. To create this relation, two options are possible:

- use the sAddr attribute at the data attribute level to map them to the telegram,
- define a Private address type which may be allocated to the needed level of the data model.

Within IEEE C37.118.2, the identification of a telegram source is done by its IP source address, and the values within the telegram are identified only by their location in the telegram. Based upon this analysis, a more hierarchical addressing scheme, other than attribute level, is not needed. For Phasor Data Concentrator (PDC) telegrams, which might have a repeating structure, it is optionally allowed to specify the repetition identification at the logical device level, i.e. above the data attribute level.

Values map to the C37.118.2 data telegram only. The configuration telegrams are not mapped, as their information respective equivalent information will be supplied by the IEC 61850 data model itself. E.g. if the values of a PDC telegram belong to different PMUs, each one shall be modelled by a different logical device.

The sAddr string shall have the following syntax:

[<repeatno>], <118Type>,<count> [,<bitoffs>]

with the following meaning:

Syntax element	Range	Meaning
repeatno	0..n	Repetition number of the data value structure part (ASDU). If repeatno is missing, its value is either stated at the LDevice level, or is zero.
118Type	PHASORS, ANALOG, DIGITAL, FREQ, DFREQ, STAT	The type of data as described in C37.118.2
Count	0..n	The value of n depends on the 118 type. It is the relative offset of the data value within all data elements of the same type. For PHASORS, the offset of the data per phasor.
Bitoffs	0..15	The bit within the 16 bit value identified by count. Each bit maps to an IEC61850 data attribute of type BOOLEAN, or a health respective alarm Enum , where bit value 0 is mapped to OK (1), and bit value 1 to Alarm (3). Only needed for 118Type = DIGITAL or STAT.

To specify the repeatno at LDevice level, the following **Private** type is introduced:

C37.118-repeatno

Example:

<LDevice inst=”LD0”>

<Private type=”C37.118-repeatno”>5</Private>

<LN0>

…

</LN0>

….

</LDevice>

13.3.3 SCL example

The following example illustrates the usage at the data object instance on the IED.

Observe that sAddr attributes can be attached at IED instance level as well as at DataTypeTemplate level. The last choice might need more data type template definitions, however saves the definition at instance level, if several PMUs of the same type (with same address values) are in the same SCD file.

```
<IED name=”MyPMU” ...>
....
        <LN lnClass=”MMXU” ....>
           <DOI name=”PhV”>
                <SDI name=”phsA”>
                    <SDI name=”cVal”>
                        <SDI name=”mag”>
                            <DAI name=”f” sAddr=”0,PHASORS,2” />
<!-- floating point value of voltage phasor phase A amplitude is the second phasor value in the first ASDU -->
                        </SDI>
                        <SDI name=”ang”>
                            <DAI name=”f” sAddr=”,PHASORS,2” />
<!-- floating point value of voltage phasor phase A angle is found at the same place; this part or this sAddr might therefore be skipped; missing repeatno indicates value 0, as no repeatno is defined at LDevice level -->
                        </SDI>
                    </SDI>
                </SDI>
           </DOI>
        </LN>
</IED>
....
```

For a full SCL example, see Annex A.

14 Effect on IEC 61850-7-2

In order to provide the equivalent of the IEEE C37.118.1 CFG-2 and CFG-3 configuration commands, GetSavReference and GetSavElementNumber service shall be added.

15 Effect on IEC 61850-7-4

15.1 General

This document specifies several modifications needed to IEC 61850-7-4. These modifications/extensions shall be designated by a well-defined namespace.

The following subclauses detail the changes and namespace definition.

15.2 Namespace definition

The namespace used to identifying the definition additions to IEC 61850-7-4, and potentially other parts of IEC 61850, shall be: “IEC/TR 61850-90-5”.

15.3 Extension of ClcMth

The extension to the ClcMth enumerated set of definitions to include P-CLASS and M-CLASS (see Table 6).

15.4 Addition of rate of change of frequency (ROCOF) DataObject

IEEE C37.118.1 defines the estimation technique for the value representing the Rate of Change of Frequency (ROCOF).

The normative estimation method is defined in IEEE C37.118.1. The following text is an extract from IEEE C37.118.1 and shall be considered informative:

> "A PMU shall calculate and be capable of reporting frequency and rate of change of frequency (ROCOF). For this measurement, the following standard definitions shall be used. Given a sinusoidal signal:
>
> $$X(t) = X_m \cos [\underline{\Psi}(t)]$$
>
> Frequency is defined by:
>
> $$f(t) = \frac{1}{2\pi} \cdot \frac{d\underline{\Psi}(t)}{dt}$$
>
> and the rate of change of frequency ROCOF = df(t)/dt
>
> Synchrophasors are always computed in relation to the system nominal frequency (f_0). If the cosine argument is represented as $\underline{\Psi}(t) = \omega_0 t + \varphi(t) = 2\pi f_0 t + \varphi(t) = 2\pi [f_0 t + \varphi(t)/2\pi]$, the formula for frequency becomes
>
> $$f(t) = f_0 + d[\varphi(t)/2\pi]/dt = f_0 + \Delta f(t)$$
>
> where $\Delta f(t)$ is the deviation of frequency from nominal and
>
> $$ROCOF = d^2[\varphi(t)/2\pi]/dt^2 = d(\Delta f(t))/dt$$
>
> Frequency in phasor measurements may be reported as the actual frequency f(t) or the deviation of frequency from nominal, $\Delta f(t)$. In steady-state conditions, $\Delta f(t)$ can be represented as a scalar number Δf."

For the purposes of IEC 61850, a conditional DataObject shall be added to the MMXU and/or MMXN Logical Node definition in IEC 61850-7-4. The DataObject name shall be "HzRte" indicating the rate of change of the frequency. "HzRte" shall be of the Common Data Class (CDC) MV. The HzRte DataObject value shall be floating point.

The units shall be Hz/second as specified IEC 61850-7-3. It is recommended that the multiplier be "none" as defined in IEC 61850-7-3.

15.5 Modifications to the LTIM logical node class

The following Data Object semantic shall be added to Clause 6, Table 10 of IEC 61850-7-4:

TmLeaps	Indicates if a leap second is currently active. A value of TRUE shall indicate that there is a leap second that is active. A value of FALSE shall indicate that no leap second is active.

The TmLeaps Data Object shall be added to the LTMS Logical Node Class as shown in Table 17.

Table 17 – Addition of TmLeaps in LTIM

LTIM class				
Data object name	**Common data class**	**Explanation**	**T**	**M/O/C**
LNName				
Data Objects				
Status Information				
TmDT	SPS	Indicates if for this location daylight saving time is in effect now		M
TmLeaps	SPS	Indicates if a leap second is currently active. A value of TRUE shall indicate that there is a leap second that is active. A value of FALSE shall indicate that no leap second is active.		O

15.6 Modifications to the LTMS logical node class

The following Data Object semantic shall be added to Clause 6, Table 10 of IEC 61850-7-4:

TmLok	Shows if synchronisation is locked respective how long it is unlocked. The state is 'Locked' only if the IED is synchronised globally (LTMS.TmSyn is not LocalAreaClock), and Unlocked state is against loss of global clock.

TmLok	Value
UnlockedMoreThan1000s	5
Unlocked1000s	4
Unlocked100s	3
Unlocked10s	2
Locked	1

The TmLok Data Object shall be added to the LTMS Logical Node Class as shown in Table 18.

Table 18 – Addition of TmLok in LTMS

LTMS class				
Data object name	**Common data class**	**Explanation**	**T**	**M/O/C**
LNName				
Data Objects				
Status Information				
TmAcc	INS	Number of significant bits in the Fraction Of Second in the time accuracy part of the time stamp. See IEC 61850-7-2.		O
TmSrc	VSS	Current time source		M
TmSyn	ENS	Time synchronized according to IEC 61850-9-2		O
TmChSt1	SPS	Time channel status (up/down)		O
TmLok	ENS	Unlock Time		O
Settings				
TmSrcSet1	VSG	Time source setting (“1588” in case the time source is a IEEE 1588 source or dotted IP-address)		O

The values of the enumerations for TmLok shall be:

```
<EnumType id="TmLokKind">
        <EnumVal ord="1">Locked</EnumVal>
        <EnumVal ord="2">Unlocked10s</EnumVal>
        <EnumVal ord="3">Unlocked100s</EnumVal>
        <EnumVal ord="4">Unlocked1000s</EnumVal>
        <EnumVal ord="5">UnlockedMoreThan1000s</EnumVal>
</EnumType>
```

Annex A
(informative)

Full SCL example for C37.118.2 configuration

To make the example shorter, all address mappings are in the instance part, and the DataTypeTemplate definitions are removed. Observe that the semantic is carried at two levels: first the data model of the IED, second the allocation of IED logical nodes to the substation single line.

This example is based on the bay single line shown in Figure A.1, and describes one PMU named AA1FP1, sending phasor data of this bay to a client AA1KA1.

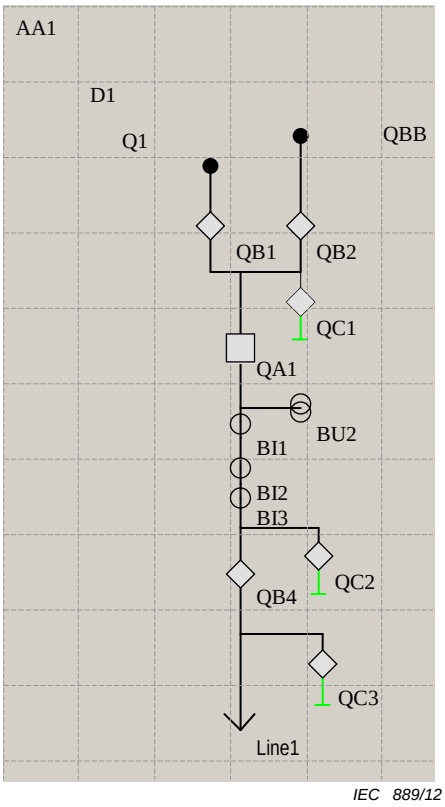


Figure A.1 – Single line for SCL example

```
<?xml version="1.0"?>
<SCL xmlns:sxy="http://www.iec.ch/61850/2003/SCLcoordinates" xmlns="http://www.iec.ch/61850/2003/SCL" version="2007" revision="B"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.iec.ch/61850/2003/SCL
C:\Data\sdps\SCL3.1\SCL.xsd">
    <Header id="SynchroPhasor AA1 SED" toolID="SSI-Tool"/>
    <Substation name="AA1" desc="Substation">
        <VoltageLevel name="D1" desc="Voltage Level">
            <Bay name="Q1" desc="Bay" sxy:x="55" sxy:y="62" sxy:dir="vertical">
                <LNode iedName="AA1FP1" ldInst="PMU" lnClass="MMXU" lnInst="1"/>
                <ConductingEquipment name="BI1" desc="Current Transformer" type="CTR"
                    sxy:x="8" sxy:y="15" sxy:dir="vertical">
                    <LNode iedName="AA1FP1" ldInst="PMU" lnClass="TCTR" lnInst="1"/>
                    <Terminal name="AA1D1Q1N2" connectivityNode="AA1/D1/Q1/N2"
                        substationName="AA1" voltageLevelName="D1" bayName="Q1"
                        cNodeName="N2"/>
<Terminal name="AA1D1Q1N3" connectivityNode="AA1/D1/Q1/N3" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="N3"/>
                </ConductingEquipment>
                <ConductingEquipment name="QC2" desc="Isolator" type="DIS" sxy:x="10"
sxy:y="21" sxy:dir="vertical">
                    <Terminal name="AA1D1Q1N6" connectivityNode="AA1/D1/Q1/N6" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="N6"/>
                    <Terminal name="grounded" connectivityNode="AA1/D1/Q1/grounded" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="grounded"/>
                </ConductingEquipment>
                <ConductingEquipment name="BU2" desc="Voltage Transformer 3Phase" type="VTR" sxy:x="12" sxy:y="14" sxy:dir="vertical">
                    <LNode iedName="AA1FP1" ldInst="PMU" lnClass="TVTR" lnInst="1"/>
                    <Terminal name="AA1D1Q1N3" connectivityNode="AA1/D1/Q1/N3" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="N3"/>
                </ConductingEquipment>
                <ConductingEquipment name="QB2" desc="Isolator" type="DIS" sxy:x="12" sxy:y="4" sxy:dir="vertical">
                    <Terminal name="AA1D1QBBN4" connectivityNode="AA1/D1/QBB/N4" substationName="AA1" voltageLevelName="D1"
bayName="QBB" cNodeName="N4"/>
                    <Terminal name="AA1D1Q1N5" connectivityNode="AA1/D1/Q1/N5" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="N5"/>
                </ConductingEquipment>
                <ConductingEquipment name="QC1" desc="Isolator" type="DIS" sxy:x="10" sxy:y="8" sxy:dir="vertical">
                    <Terminal name="AA1D1Q1N5" connectivityNode="AA1/D1/Q1/N5" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="N5"/>
                    <Terminal name="grounded" connectivityNode="AA1/D1/Q1/grounded" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="grounded"/>
                </ConductingEquipment>
                <ConductingEquipment name="BI3" desc="Current Transformer" type="CTR" sxy:x="8" sxy:y="19" sxy:dir="vertical">
                    <Terminal name="AA1D1Q1N6" connectivityNode="AA1/D1/Q1/N6" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="N6"/>
```

```
                                        <Terminal name="AA1D1Q1N4" connectivityNode="AA1/D1/Q1/N4" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="N4"/>
                                </ConductingEquipment>
                                <ConductingEquipment name="QA1" desc="Circuit Breaker" type="CBR" sxy:x="8" sxy:y="11" sxy:dir="vertical">
                                        <Terminal name="AA1D1Q1N3" connectivityNode="AA1/D1/Q1/N3" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="N3"/>
                                        <Terminal name="AA1D1Q1N5" connectivityNode="AA1/D1/Q1/N5" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="N5"/>
                                </ConductingEquipment>
                                <ConductingEquipment name="BI2" desc="Current Transformer" type="CTR" sxy:x="8" sxy:y="17" sxy:dir="vertical">
                                        <Terminal name="AA1D1Q1N2" connectivityNode="AA1/D1/Q1/N2" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="N2"/>
                                        <Terminal name="AA1D1Q1N4" connectivityNode="AA1/D1/Q1/N4" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="N4"/>
                                </ConductingEquipment>
                                <ConductingEquipment name="QB1" desc="Isolator" type="DIS" sxy:x="6" sxy:y="4" sxy:dir="vertical">
                                        <Terminal name="AA1D1Q1N5" connectivityNode="AA1/D1/Q1/N5" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="N5"/>
                                        <Terminal name="AA1D1QBBN1" connectivityNode="AA1/D1/QBB/N1" substationName="AA1" voltageLevelName="D1"
bayName="QBB" cNodeName="N1"/>
                                </ConductingEquipment>
                                <ConductingEquipment name="QB4" desc="Isolator" type="DIS" sxy:x="8" sxy:y="23" sxy:dir="vertical">
                                        <Terminal name="AA1D1Q1N1" connectivityNode="AA1/D1/Q1/N1" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="N1"/>
                                        <Terminal name="AA1D1Q1N6" connectivityNode="AA1/D1/Q1/N6" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="N6"/>
                                </ConductingEquipment>
                                <ConductingEquipment name="QC3" desc="Isolator" type="DIS" sxy:x="10" sxy:y="35" sxy:dir="vertical">
                                        <Terminal name="AA1D1Q1N1" connectivityNode="AA1/D1/Q1/N1" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="N1"/>
                                        <Terminal name="grounded" connectivityNode="AA1/D1/Q1/grounded" substationName="AA1" voltageLevelName="D1" bayName="Q1"
cNodeName="grounded"/>
                                </ConductingEquipment>
                                <ConnectivityNode name="N1" pathName="AA1/D1/Q1/N1" sxy:x="8" sxy:y="31"/>
                                <ConnectivityNode name="N2" pathName="AA1/D1/Q1/N2" sxy:x="8" sxy:y="16"/>
                                <ConnectivityNode name="N3" pathName="AA1/D1/Q1/N3" sxy:x="9" sxy:y="13"/>
                                <ConnectivityNode name="N6" pathName="AA1/D1/Q1/N6" sxy:x="8" sxy:y="21"/>
                                <ConnectivityNode name="N5" pathName="AA1/D1/Q1/N5" sxy:x="9" sxy:y="6"/>
                                <ConnectivityNode name="N4" pathName="AA1/D1/Q1/N4" sxy:x="8" sxy:y="18"/>
                        </Bay>
                        <Bay name="QBB" desc="Bay" sxy:x="63" sxy:y="36" sxy:dir="vertical">
                                <ConnectivityNode name="N3" pathName="AA1/D1/QBB/N3" sxy:x="48" sxy:y="12"/>
                                <ConnectivityNode name="N2" pathName="AA1/D1/QBB/N2" sxy:x="47" sxy:y="17"/>
                                <ConnectivityNode name="N4" pathName="AA1/D1/QBB/N4" sxy:x="25" sxy:y="18"/>
                                <ConnectivityNode name="N1" pathName="AA1/D1/QBB/N1" sxy:x="22" sxy:y="20"/>
                        </Bay>
```

```
        </VoltageLevel>
    </Substation>
    <Communication>
        <SubNetwork name="AA1WA1" desc="C37.118 UDP network" type="C37.118-UDP">
            <ConnectedAP iedName="AA1KA1" apName="S1" desc="the client receiving the messages >
                <Address>
                    <P type="IP">172.16.0.100</P>
                    <P type="IP-SUBNET">255.255.0.0</P>
                    <P type="C37-118-IP-Port">110</P>
                </Address>
            </ConnectedAP>
            <ConnectedAP iedName="AA1FP1" apName="S1">
                <Address>
                    <P type="IP">172.16.1.3</P>
                    <P type="IP-SUBNET">255.255.0.0</P>
                </Address>
            </ConnectedAP>
        </SubNetwork>
    </Communication>
    <IED name="AA1KA1" desc="Client receiving Synchrophasor data" type="OPCServer" manufacturer="ME" configVersion="1.0" >
        <AccessPoint name="S1">
            <LN inst="1" lnClass="IHMI" lnType="IHMI_OPCServer_IEC61850"/>
            <!-- shall receive the phasor data from the PMU -->
        </AccessPoint>
    </IED>
    <IED name="AA1FP1" type="PMU" manufacturer="Whatever" configVersion="1.0">
        <Services>
            <DynAssociation/>
            <ConfDataSet max="50" maxAttributes="240"/>
            <ReadWrite/>
            <SMVSettings datSet="Conf">
                <SmpRate>2</SmpRate>
            </SMVSettings>
        </Services>
        <AccessPoint name="S1">
            <Server>
                <Authentication none="true"/>
                <LDevice inst="PMU">
                    <LN0 inst="" lnClass="LLN0" lnType="LLN0_RELx_IEC61850">
                        <!-- SMV data set and control block definitions are optional. They might be used to define the logical data flow (i.e. to the
clients) in case this is not defined at the clients itself as incoming data. The link to the C37.118 message is done by means of the sAddr definitions at the data objects -->
                        <DataSet name="PMUdata">
                            <FCDA ldInst="PMU" prefix="" lnClass="MMXU" lnInst="1" doName="A.phsA" fc="MX"/>
                            <FCDA ldInst="PMU" prefix="" lnClass="MMXU" lnInst="1" doName="A.phsB" fc="MX"/>
                            <FCDA ldInst="PMU" prefix="" lnClass="MMXU" lnInst="1" doName="A.phsC" fc="MX"/>
                            <FCDA ldInst="PMU" prefix="" lnClass="MMXU" lnInst="1" doName="Health" fc="ST"/>
```

```
                <FCDA ldInst="PMU" prefix="" lnClass="LPHD" lnInst="1" doName="PhyHealth" fc="ST"/>
            </DataSet>
            <SampledValueControl name="SyPh_SVCB1" desc="Phasor SVCB" datSet="PMUdata" confRev="1" smvID="MyPhasors AA1"
smpRate="2" nofASDU="1">
                <IEDName>AA1OPC1</IEDName>
            </SampledValueControl>
        </LN0>
        <LN inst="1" lnClass="LPHD" lnType="Physical Device_RELx_IEC61850">
            <DOI name="PhyHealth">
                <DAI name="stVal" sAddr="0, DIGITAL, 0,0" />
            </DOI>
        </LN>
        <LN inst="1" lnClass="TCTR" lnType="CT_RELx_IEC61850"/>
        <LN inst="1" lnClass="TVTR" lnType="VT_RELx_IEC61850">
            <DOI name="FuFail">
                <DAI name="stVal" sAddr="0, DIGITAL, 0,1" />
            </DOI>
        </LN>
        <LN inst="1" desc="Synchrophasor measurements" lnClass="MMXU" lnType="Syph_RELx_IEC61850">
            <DOI name="PhV">
                <DAI name="angRef">
                    <Val>Synchrophasor</Val>
                </DAI>
                <SDI name="phsA">
                    <SDI name="cVal" >
                        <SDI name="mag" >
                            <DAI name="f" sAddr="0,PHASORS,0" />
                        </SDI>
                    </SDI>
                </SDI>
                <SDI name="phsB">
                    <SDI name="cVal" >
                        <SDI name="mag" >
                            <DAI name="f" sAddr="0,PHASORS,1" />
                        </SDI>
                    </SDI>
                </SDI>
                <SDI name="phsC">
                    <SDI name="cVal" >
                        <SDI name="mag" >
                            <DAI name="f" sAddr="0,PHASORS,2" />
                        </SDI>
                    </SDI>
                </SDI>
            </DOI>
            <DOI name="A">
```

```
                                        <DAI name="angRef">
                                                <Val>Synchrophasor</Val>
                                        </DAI>
                                        <SDI name="phsA">
                                                <SDI name="cVal" >
                                                        <SDI name="mag" >
                                                                <DAI name="f" sAddr="0,PHASORS,3" />
                                                        </SDI>
                                                </SDI>
                                        </SDI>
                                        <SDI name="phsB">
                                                <SDI name="cVal" >
                                                        <SDI name="mag" >
                                                                <DAI name="f" sAddr="0,PHASORS,4" />
                                                        </SDI>
                                                </SDI>
                                        </SDI>
                                        <SDI name="phsC">
                                                <SDI name="cVal" >
                                                        <SDI name="mag" >
                                                                <DAI name="f" sAddr="0,PHASORS,5" />
                                                        </SDI>
                                                </SDI>
                                        </SDI>
                                </DOI>
                                <DOI name="Hz">
                                        <SDI name="mag">
                                                <DAI name="f" sAddr="0,FREQ" />
                                        </SDI>
                                </DOI>
                        </LN>
                </LDevice>
        </Server>
    </AccessPoint>
</IED>
<DataTypeTemplates>
        <LNodeType id="IHMI_OPCServer_IEC61850" lnClass="IHMI">
                <DO name="Beh" type="aIns_OPCServer_IEC61850"/>
                <DO name="Health" type="aIns_OPCServer_IEC61850"/>
                <DO name="Mod" type="aInc_OPCServer_IEC61850"/>
                <DO name="NamPlt" type="aLpl_OPCServer_IEC61850"/>
                <DO name="EEHealth" type="aIns_OPCServer_IEC61850"/>
                <DO name="EEName" type="aDpl_OPCServer_IEC61850"/>
                <DO name="Loc" type="aSps_OPCServer_IEC61850"/>
                <DO name="OpCnt" type="aIns_OPCServer_IEC61850"/>
                <DO name="OpCntRs" type="aInc_OPCServer_IEC61850"/>
```

```
        <DO name="OpTmh" type="aIns_OPCServer_IEC61850"/>
    </LNodeType>
    <LNodeType id="LLN0_RELx_IEC61850" lnClass="LLN0">
        <DO name="Beh" type="tcBeh_RELx_IEC61850"/>
        <DO name="Health" type="tcHealth_RELx_IEC61850"/>
        <DO name="LEDRs" desc="LED Reset" type="tcSPCRO_RELx_IEC61850"/>
        <DO name="Mod" type="tcROMod_RELx_IEC61850"/>
        <DO name="NamPlt" type="tcLPLIdNs_RELx_IEC61850"/>
    </LNodeType>
    <LNodeType id="Syph_RELx_IEC61850" lnClass="MMXU">
        <DO name="Beh" type="tcBeh_RECx_IEC61850"/>
        <DO name="Health" type="tcHealth_RECx_IEC61850"/>
        <DO name="Mod" type="tcROMod_RECx_IEC61850"/>
        <DO name="NamPlt" type="tcLPL_RECx_IEC61850"/>
        <DO name="PhV" desc="Voltage phasors" type="tcSyphWYE"/>
        <DO name="A" desc="Current phasors" type="tcSyphWYE"/>
    </LNodeType>
    <LNodeType id="CT_RELx_IEC61850" lnClass="TCTR">
        <DO name="Beh" type="tcBeh_RECx_IEC61850"/>
        <DO name="Health" type="tcHealth_RECx_IEC61850"/>
        <DO name="Mod" type="tcROMod_RECx_IEC61850"/>
        <DO name="NamPlt" type="tcLPL_RECx_IEC61850"/>
    </LNodeType>
    <LNodeType id="VT_RELx_IEC61850" lnClass="TVTR">
        <DO name="Beh" type="tcBeh_RECx_IEC61850"/>
        <DO name="Health" type="tcHealth_RECx_IEC61850"/>
        <DO name="Mod" type="tcROMod_RECx_IEC61850"/>
        <DO name="NamPlt" type="tcLPL_RECx_IEC61850"/>
        <DO name="FuFail" desc="VT supply failure (MCB)" type="tcSPS_RECx_IEC61850"/>
    </LNodeType>
    <LNodeType id="Physical Device_RELx_IEC61850" lnClass="LPHD">
        <DO name="PhyNam" type="tcDPL_RELx_IEC61850"/>
        <DO name="Beh" type="tcBeh_RELx_IEC61850"/>
        <DO name="PhyHealth" desc="Relay ready" type="tcHealth_RELx_IEC61850"/>
        <DO name="Proxy" type="tcSPS_RELx_IEC61850"/>
    </LNodeType>
    ..... <!-- other data type definitions removed -->
    <EnumType id="ctlModel">
        <EnumVal ord="0">status-only</EnumVal>
        <EnumVal ord="1">direct-with-normal-security</EnumVal>
        <EnumVal ord="2">sbo-with-normal-security</EnumVal>
        <EnumVal ord="3">direct-with-enhanced-security</EnumVal>
        <EnumVal ord="4">sbo-with-enhanced-security</EnumVal>
    </EnumType>
    <EnumType id="Beh">
        <EnumVal ord="1">on</EnumVal>
```

```
                <EnumVal ord="2">blocked</EnumVal>
                <EnumVal ord="3">test</EnumVal>
                <EnumVal ord="4">test/blocked</EnumVal>
                <EnumVal ord="5">off</EnumVal>
            </EnumType>
            <EnumType id="Health">
                <EnumVal ord="1">Ok</EnumVal>
                <EnumVal ord="2">Warning</EnumVal>
                <EnumVal ord="3">Alarm</EnumVal>
            </EnumType>
            <EnumType id="Mod">
                <EnumVal ord="1">on</EnumVal>
                <EnumVal ord="2">blocked</EnumVal>
                <EnumVal ord="3">test</EnumVal>
                <EnumVal ord="4">test/blocked</EnumVal>
                <EnumVal ord="5">off</EnumVal>
            </EnumType>
            <EnumType id="dir">
                <EnumVal ord="0">unknown</EnumVal>
                <EnumVal ord="1">forward</EnumVal>
                <EnumVal ord="2">backward</EnumVal>
                <EnumVal ord="3">both</EnumVal>
            </EnumType>
            <EnumType id="angid">
                <EnumVal ord="0">Va</EnumVal>
                <EnumVal ord="1">Vb</EnumVal>
                <EnumVal ord="2">Vc</EnumVal>
                <EnumVal ord="3">Aa</EnumVal>
                <EnumVal ord="4">Ab</EnumVal>
                <EnumVal ord="5">Ac</EnumVal>
                <EnumVal ord="6">Vab</EnumVal>
                <EnumVal ord="7">Vbc</EnumVal>
                <EnumVal ord="8">Vca</EnumVal>
                <EnumVal ord="9">Vother</EnumVal>
                <EnumVal ord="10">Aother</EnumVal>
                <EnumVal ord="11">Synchrophasor</EnumVal>
            </EnumType>
        </DataTypeTemplates>
</SCL>
```

Annex B
(informative)

SCL examples for direct PMU and PDC-oriented communication

B.1 Direct PMU communication example

This describes an example SED file from the source substation AA1 to the center system project (see Figure 17 for the communication configuration, and Figure A.1 for the bay single line). It just contains the phasor related interface information of the source substation, and the internal reporting client needed to allocate correct report control blocks in case reporting shall also be used to the center. The SV control block indicates UDP based service (<Protocol>R-SV</Protocol>). Observe the transfer of data flow engineering right at AA1FP1 to the center project.

```
<?xml version="1.0"?>
<SCL xmlns:sxy = "http://www.iec.ch/61850/2003/SCLcoordinates" xmlns:xsi = "http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation = "http://www.iec.ch/61850/2003/SCL;C:\Data\data\IECTC57\SCL-XML\Schema2007\SCL2.0\SCL.xsd" xmlns = "http://www.iec.ch/61850/2003/SCL">
 <Header id = "SynchroPhasor AA1 SED" toolID = "SSI-Tool" nameStructure = "IEDName"/>
 <Substation name = "AA1" desc = "Substation">
  <VoltageLevel name = "D1" desc = "Voltage Level">
   <Bay name = "Q1" desc = "Bay" sxy:x = "55" sxy:y = "62" sxy:dir = "vertical">
    <LNode iedName = "AA1FP1" ldInst = "PMU" lnClass = "MMXU" lnInst = "1"/>
    <ConductingEquipment name = "BI1" desc = "Current Transformer" type = "CTR" sxy:x = "8" sxy:y = "15" sxy:dir = "vertical">
     <LNode iedName = "AA1FP1" ldInst = "PMU" lnClass = "TCTR" lnInst = "1"/>
     <Terminal name = "AA1D1Q1N2" connectivityNode = "AA1/D1/Q1/N2" substationName = "AA1" voltageLevelName = "D1" bayName = "Q1" cNodeName = "N2"/>
     <Terminal name = "AA1D1Q1N3" connectivityNode = "AA1/D1/Q1/N3" substationName = "AA1" voltageLevelName = "D1" bayName = "Q1" cNodeName = "N3"/>
    </ConductingEquipment>
    <ConductingEquipment name = "QC2" desc = "Isolator" type = "DIS" sxy:x = "10" sxy:y = "21" sxy:dir = "vertical">
     <Terminal name = "AA1D1Q1N6" connectivityNode = "AA1/D1/Q1/N6" substationName = "AA1" voltageLevelName = "D1" bayName = "Q1" cNodeName = "N6"/>
     <Terminal name = "grounded" connectivityNode = "AA1/D1/Q1/grounded" substationName = "AA1" voltageLevelName = "D1" bayName = "Q1" cNodeName = "grounded"/>
    </ConductingEquipment>
    <ConductingEquipment name = "BU2" desc = "Voltage Transformer 3Phase" type = "VTR" sxy:x = "12" sxy:y = "14" sxy:dir = "vertical">
     <LNode iedName = "AA1FP1" ldInst = "PMU" lnClass = "TVTR" lnInst = "1"/>
     <Terminal name = "AA1D1Q1N3" connectivityNode = "AA1/D1/Q1/N3" substationName = "AA1" voltageLevelName = "D1" bayName = "Q1" cNodeName = "N3"/>
    </ConductingEquipment>
    <ConductingEquipment name = "QB2" desc = "Isolator" type = "DIS" sxy:x = "12" sxy:y = "4" sxy:dir = "vertical">
     <Terminal name = "AA1D1QBBN4" connectivityNode = "AA1/D1/QBB/N4" substationName = "AA1" voltageLevelName = "D1" bayName = "QBB" cNodeName = "N4"/>
     <Terminal name = "AA1D1Q1N5" connectivityNode = "AA1/D1/Q1/N5" substationName = "AA1" voltageLevelName = "D1" bayName = "Q1" cNodeName = "N5"/>
    </ConductingEquipment>
    <ConductingEquipment name = "QC1" desc = "Isolator" type = "DIS" sxy:x = "10" sxy:y = "8" sxy:dir = "vertical">
     <Terminal name = "AA1D1Q1N5" connectivityNode = "AA1/D1/Q1/N5" substationName = "AA1" voltageLevelName = "D1" bayName = "Q1" cNodeName = "N5"/>
     <Terminal name = "grounded" connectivityNode = "AA1/D1/Q1/grounded" substationName = "AA1" voltageLevelName = "D1" bayName = "Q1" cNodeName = "grounded"/>
    </ConductingEquipment>
    <ConductingEquipment name = "BI3" desc = "Current Transformer" type = "CTR" sxy:x = "8" sxy:y = "19" sxy:dir = "vertical">
     <Terminal name = "AA1D1Q1N6" connectivityNode = "AA1/D1/Q1/N6" substationName = "AA1" voltageLevelName = "D1" bayName = "Q1" cNodeName = "N6"/>
```

```
      <Terminal name = "AA1D1Q1N4" connectivityNode = "AA1/D1/Q1/N4" substationName = "AA1"
voltageLevelName = "D1" bayName = "Q1" cNodeName = "N4"/>
    </ConductingEquipment>
    <ConductingEquipment name = "QA1" desc = "Circuit Breaker" type = "CBR" sxy:x = "8" sxy:y = "11" sxy:dir =
"vertical">
      <Terminal name = "AA1D1Q1N3" connectivityNode = "AA1/D1/Q1/N3" substationName = "AA1"
voltageLevelName = "D1" bayName = "Q1" cNodeName = "N3"/>
      <Terminal name = "AA1D1Q1N5" connectivityNode = "AA1/D1/Q1/N5" substationName = "AA1"
voltageLevelName = "D1" bayName = "Q1" cNodeName = "N5"/>
    </ConductingEquipment>
    <ConductingEquipment name = "BI2" desc = "Current Transformer" type = "CTR" sxy:x = "8" sxy:y = "17"
sxy:dir = "vertical">
      <Terminal name = "AA1D1Q1N2" connectivityNode = "AA1/D1/Q1/N2" substationName = "AA1"
voltageLevelName = "D1" bayName = "Q1" cNodeName = "N2"/>
      <Terminal name = "AA1D1Q1N4" connectivityNode = "AA1/D1/Q1/N4" substationName = "AA1"
voltageLevelName = "D1" bayName = "Q1" cNodeName = "N4"/>
    </ConductingEquipment>
    <ConductingEquipment name = "QB1" desc = "Isolator" type = "DIS" sxy:x = "6" sxy:y = "4" sxy:dir =
"vertical">
      <Terminal name = "AA1D1Q1N5" connectivityNode = "AA1/D1/Q1/N5" substationName = "AA1"
voltageLevelName = "D1" bayName = "Q1" cNodeName = "N5"/>
      <Terminal name = "AA1D1QBBN1" connectivityNode = "AA1/D1/QBB/N1" substationName = "AA1"
voltageLevelName = "D1" bayName = "QBB" cNodeName = "N1"/>
    </ConductingEquipment>
    <ConductingEquipment name = "QB4" desc = "Isolator" type = "DIS" sxy:x = "8" sxy:y = "23" sxy:dir =
"vertical">
      <Terminal name = "AA1D1Q1N1" connectivityNode = "AA1/D1/Q1/N1" substationName = "AA1"
voltageLevelName = "D1" bayName = "Q1" cNodeName = "N1"/>
      <Terminal name = "AA1D1Q1N6" connectivityNode = "AA1/D1/Q1/N6" substationName = "AA1"
voltageLevelName = "D1" bayName = "Q1" cNodeName = "N6"/>
    </ConductingEquipment>
    <ConductingEquipment name = "QC3" desc = "Isolator" type = "DIS" sxy:x = "10" sxy:y = "35" sxy:dir =
"vertical">
      <Terminal name = "AA1D1Q1N1" connectivityNode = "AA1/D1/Q1/N1" substationName = "AA1"
voltageLevelName = "D1" bayName = "Q1" cNodeName = "N1"/>
      <Terminal name = "grounded" connectivityNode = "AA1/D1/Q1/grounded" substationName = "AA1"
voltageLevelName = "D1" bayName = "Q1" cNodeName = "grounded"/>
    </ConductingEquipment>
    <ConnectivityNode name = "N1" pathName = "AA1/D1/Q1/N1" sxy:x = "8" sxy:y = "31"/>
    <ConnectivityNode name = "N2" pathName = "AA1/D1/Q1/N2" sxy:x = "8" sxy:y = "16"/>
    <ConnectivityNode name = "N3" pathName = "AA1/D1/Q1/N3" sxy:x = "9" sxy:y = "13"/>
    <ConnectivityNode name = "N6" pathName = "AA1/D1/Q1/N6" sxy:x = "8" sxy:y = "21"/>
    <ConnectivityNode name = "N5" pathName = "AA1/D1/Q1/N5" sxy:x = "9" sxy:y = "6"/>
    <ConnectivityNode name = "N4" pathName = "AA1/D1/Q1/N4" sxy:x = "8" sxy:y = "18"/>
   </Bay>
   <Bay name = "QBB" desc = "Bay" sxy:x = "63" sxy:y = "36" sxy:dir = "vertical">
    <ConnectivityNode name = "N3" pathName = "AA1/D1/QBB/N3" sxy:x = "48" sxy:y = "12"/>
    <ConnectivityNode name = "N2" pathName = "AA1/D1/QBB/N2" sxy:x = "47" sxy:y = "17"/>
    <ConnectivityNode name = "N4" pathName = "AA1/D1/QBB/N4" sxy:x = "25" sxy:y = "18"/>
    <ConnectivityNode name = "N1" pathName = "AA1/D1/QBB/N1" sxy:x = "22" sxy:y = "20"/>
   </Bay>
  </VoltageLevel>
 </Substation>
 <Communication>
  <SubNetwork name = "AA1WA1" desc = "IEC61850 through both stations" type = "8-MMS">
   <ConnectedAP iedName = "AA1OPC1" apName = "S1">
    <Address>
     <P type = "SA">0</P>
     <P type = "IP">172.16.0.100</P>
     <P type = "IP-SUBNET">255.255.0.0</P>
     <P type = "OSI-AP-Title">1,3,9999,23</P>
     <P type = "OSI-AE-Qualifier">23</P>
     <P type = "OSI-TSEL">0001</P>
     <P type = "OSI-PSEL">00000001</P>
     <P type = "OSI-SSEL">0001</P>
    </Address>
   </ConnectedAP>
   <ConnectedAP iedName = "AA1FP1" apName = "S1">
    <Address>
     <P type = "SA">0</P>
     <P type = "IP">172.16.1.3</P>
     <P type = "IP-SUBNET">255.255.0.0</P>
```

```
        <P type = "OSI-AP-Title">1,3,9999,23</P>
        <P type = "OSI-AE-Qualifier">23</P>
        <P type = "OSI-TSEL">0001</P>
        <P type = "OSI-PSEL">00000001</P>
        <P type = "OSI-SSEL">0001</P>
      </Address>
      <SMV desc = "Phasor SVCB" ldInst = "PMU" cbName = "SyPh_SVCB1">
        <Address>
            <P type="VLAN-ID">004</P>
            <P type="VLAN-PRIORITY">4</P>
            <P type="APPID">3001</P>
             <P type = "IP">172.16.0.100</P>
             <P type = "IP-SUBNET">255.255.0.0</P>
        </Address>
      </SMV>
    </ConnectedAP>
  </SubNetwork>
 </Communication>
 <IED name = "AA1OPC1" desc = "OPC Server" type = "OPCServer" manufacturer = "Whatever" configVersion =
"1.0" engRight = "fix" owner = "AA1">
  <AccessPoint name = "S1">
   <LN inst = "1" lnClass = "IHMI" lnType = "IHMI_OPCServer_IEC61850"/>
  </AccessPoint>
 </IED>
 <IED name = "AA1FP1" type = "PMU" manufacturer = "Whatever" configVersion = "1.0"
engRight = "dataflow" owner = "AA1">
  <Services>
   <DynAssociation/>
   <SettingGroups>
    <SGEdit/>
   </SettingGroups>
   <GetDirectory/>
   <GetDataObjectDefinition/>
   <DataObjectDirectory/>
   <GetDataSetValue/>
   <ConfDataSet max = "50" maxAttributes = "240"/>
   <ReadWrite/>
   <ConfReportControl max = "100"/>
   <GetCBValues/>
   <ReportSettings datSet = "Conf" rptID = "Dyn" optFields = "Dyn" bufTime = "Dyn" trgOps = "Dyn" intgPd =
"Dyn"/>
   <SMVSettings datSet = "Conf"/>
  </Services>
  <AccessPoint name = "S1">
   <Server>
    <Authentication none = "true"/>
    <LDevice inst = "PMU">
     <LN0 inst = "" lnClass = "LLN0" lnType = "LLN0_RELx_IEC61850">
      <DataSet name = "PMUdata">
       <FCDA ldInst = "PMU" prefix = "" lnClass = "MMXU" lnInst = "1" doName = "A.phsA" fc = "MX"/>
       <FCDA ldInst = "PMU" prefix = "" lnClass = "MMXU" lnInst = "1" doName = "A.phsB" fc = "MX"/>
       <FCDA ldInst = "PMU" prefix = "" lnClass = "MMXU" lnInst = "1" doName = "A.phsC" fc = "MX"/>
       <FCDA ldInst = "PMU" prefix = "" lnClass = "MMXU" lnInst = "1" doName = "Health" fc = "ST"/>
       <FCDA ldInst = "PMU" prefix = "" lnClass = "LPHD" lnInst = "1" doName = "PhyHealth" fc = "ST"/>
      </DataSet>
      <DataSet name = "StatUrgentA" desc = "Status Data used to update process pictures and to generate
alarms.">
       <FCDA ldInst = "PMU" prefix = "" lnClass = "LPHD" lnInst = "1" doName = "PhyHealth" fc = "ST"/>
       <FCDA ldInst = "PMU" prefix = "" lnClass = "TVTR" lnInst = "1" doName = "FuFail" fc = "ST"/>
       <FCDA ldInst = "PMU" prefix = "" lnClass = "LLN0" doName = "Mod" fc = "ST"/>
      </DataSet>
      <ReportControl name = "rcb_A" datSet = "StatUrgentA" confRev = "2" bufTime = "100" buffered = "true">
       <TrgOps dchg = "true" qchg = "true"/>
       <OptFields/>
       <RptEnabled max = "5">
        <ClientLN iedName = "AA1OPC1" ldInst = "none" lnInst = "1" lnClass = "IHMI"/>
       </RptEnabled>
      </ReportControl>
      <SampledValueControl name = "SyPh_SVCB1" desc = "Phasor SVCB" datSet = "PMUdata" confRev = "1"
smvID = "MyPhasors AA1" smpRate = "2" nofASDU = "1">
            <Protocol mustUnderstand="true">R-SV</Protocol>
```

```
        <SmvOpts refreshTime = "true" sampleRate = "true"/>
          <IEDName>AA1OPC1</IEDName> <!-- the destination IED -->
        </SampledValueControl>
      </LN0>
      <LN inst = "1" lnClass = "LPHD" lnType = "Physical Device_RELx_IEC61850"/>
      <LN inst = "1" lnClass = "TCTR" lnType = "CT_RELx_IEC61850"/>
      <LN inst = "1" lnClass = "TVTR" lnType = "VT_RELx_IEC61850"/>
      <LN inst = "1" desc = "Synchrophasor measurements" lnClass = "MMXU" lnType = "Syph_RELx_IEC61850">
        <DOI name = "PhV">
          <SDI name = "phsA">
            <DAI name = "angRef">
              <Val>Synchrophasor</Val>
            </DAI>
          </SDI>
          <SDI name = "phsB">
            <DAI name = "angRef">
              <Val>Synchrophasor</Val>
            </DAI>
          </SDI>
          <SDI name = "phsC">
            <DAI name = "angRef">
              <Val>Synchrophasor</Val>
            </DAI>
          </SDI>
        </DOI>
        <DOI name = "A">
          <SDI name = "phsA">
            <DAI name = "angRef">
              <Val>Synchrophasor</Val>
            </DAI>
          </SDI>
          <SDI name = "phsB">
            <DAI name = "angRef">
              <Val>Synchrophasor</Val>
            </DAI>
          </SDI>
          <SDI name = "phsC">
            <DAI name = "angRef">
              <Val>Synchrophasor</Val>
            </DAI>
          </SDI>
        </DOI>
      </LN>
    </LDevice>
  </Server>
 </AccessPoint>
</IED>
<DataTypeTemplates>
                ...
 <LNodeType id = "Syph_RELx_IEC61850" lnClass = "MMXU">
  <DO name = "Beh" type = "tcBeh_RECx_IEC61850"/>
  <DO name = "Health" type = "tcHealth_RECx_IEC61850"/>
  <DO name = "Mod" type = "tcROMod_RECx_IEC61850"/>
  <DO name = "NamPlt" type = "tcLPL_RECx_IEC61850"/>
  <DO name = "PhV" desc = "Voltage phasors" type = "tcSyphWYE"/>
  <DO name = "A" desc = "Current phasors" type = "tcSyphWYE"/>
 </LNodeType>
 <LNodeType id = "CT_RELx_IEC61850" lnClass = "TCTR">
  <DO name = "Beh" type = "tcBeh_RECx_IEC61850"/>
  <DO name = "Health" type = "tcHealth_RECx_IEC61850"/>
  <DO name = "Mod" type = "tcROMod_RECx_IEC61850"/>
  <DO name = "NamPlt" type = "tcLPL_RECx_IEC61850"/>
 </LNodeType>
 <LNodeType id = "VT_RELx_IEC61850" lnClass = "TVTR">
  <DO name = "Beh" type = "tcBeh_RECx_IEC61850"/>
  <DO name = "Health" type = "tcHealth_RECx_IEC61850"/>
  <DO name = "Mod" type = "tcROMod_RECx_IEC61850"/>
  <DO name = "NamPlt" type = "tcLPL_RECx_IEC61850"/>
  <DO name = "FuFail" desc = "VT supply failure (MCB)" type = "tcSPS_RECx_IEC61850"/>
 </LNodeType>
 <LNodeType id = "Physical Device_RELx_IEC61850" lnClass = "LPHD">
  <DO name = "PhyNam" type = "tcDPL_RELx_IEC61850"/>
```

```
    <DO name = "Beh" type = "tcBeh_RELx_IEC61850"/>
    <DO name = "PhyHealth" desc = "Relay ready" type = "tcHealth_RELx_IEC61850"/>
    <DO name = "Proxy" type = "tcSPS_RELx_IEC61850"/>
  </LNodeType>
                    ...
  <DOType id = "ABB_aWYECMV" cdc = "CMV">
    <DA name = "cVal" fc = "MX" dchg = "true" bType = "Struct" type = "ABB_aVector"/>
    <DA name = "q" fc = "MX" qchg = "true" bType = "Quality"/>
    <DA name = "t" fc = "MX" bType = "Timestamp"/>
    <DA name = "angRef" fc = "CF" bType = "Enum" type = "angid"/>
  </DOType>
  <DOType id = "tcSyphWYE" cdc = "WYE">
    <SDO name = "phsA" type = "ABB_aWYECMV"/>
    <SDO name = "phsB" type = "ABB_aWYECMV"/>
    <SDO name = "phsC" type = "ABB_aWYECMV"/>
  </DOType>
  <DAType id = "ABB_aVector">
    <BDA name = "mag" bType = "Struct" type = "ABB_aAnalogueValue"/>
    <BDA name = "ang" bType = "Struct" type = "ABB_aAnalogueValue"/>
  </DAType>
  <DAType id = "ABB_aAnalogueValue">
    <BDA name = "f" bType = "FLOAT32"/>
  </DAType>
  <EnumType id = "ctlModel">
    <EnumVal ord = "0">status-only</EnumVal>
    <EnumVal ord = "1">direct-with-normal-security</EnumVal>
    <EnumVal ord = "2">sbo-with-normal-security</EnumVal>
    <EnumVal ord = "3">direct-with-enhanced-security</EnumVal>
    <EnumVal ord = "4">sbo-with-enhanced-security</EnumVal>
  </EnumType>
  <EnumType id = "Beh">
    <EnumVal ord = "1">on</EnumVal>
    <EnumVal ord = "2">blocked</EnumVal>
    <EnumVal ord = "3">test</EnumVal>
    <EnumVal ord = "4">test/blocked</EnumVal>
    <EnumVal ord = "5">off</EnumVal>
  </EnumType>
  <EnumType id = "Health">
    <EnumVal ord = "1">Ok</EnumVal>
    <EnumVal ord = "2">Warning</EnumVal>
    <EnumVal ord = "3">Alarm</EnumVal>
  </EnumType>
  <EnumType id = "Mod">
    <EnumVal ord = "1">on</EnumVal>
    <EnumVal ord = "2">blocked</EnumVal>
    <EnumVal ord = "3">test</EnumVal>
    <EnumVal ord = "4">test/blocked</EnumVal>
    <EnumVal ord = "5">off</EnumVal>
  </EnumType>
  <EnumType id = "angid">
    <EnumVal ord = "0">Va</EnumVal>
    <EnumVal ord = "1">Vb</EnumVal>
    <EnumVal ord = "2">Vc</EnumVal>
    <EnumVal ord = "3">Aa</EnumVal>
    <EnumVal ord = "4">Ab</EnumVal>
    <EnumVal ord = "5">Ac</EnumVal>
    <EnumVal ord = "6">Vab</EnumVal>
    <EnumVal ord = "7">Vbc</EnumVal>
    <EnumVal ord = "8">Vca</EnumVal>
    <EnumVal ord = "9">Vother</EnumVal>
    <EnumVal ord = "10">Aother</EnumVal>
    <EnumVal ord = "11">Synchrophasor</EnumVal>
  </EnumType>
 </DataTypeTemplates>
</SCL>
''
```

B.2 PDC communication example

This example SCD file describes the center project of Figure 18 with IED AA1TH1 as PDC for AA1F1 and AA10F1. The synchrphasor data belongs to bay AA1D1Q1, whose single line is shown in Figure A.1. From this, it is easily seen how the IID file for AA1TH1 would look like (just remove AA10KA1 and all references to it).

```
<?xml version="1.0"?>
<SCL xmlns:sxy="http://www.iec.ch/61850/2003/SCLcoordinates"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.iec.ch/61850/2003/SCL&#xD;&#xA;C:\Data\data\IECTC57\SCL-
XML\Schema2007\SCL2.0\SCL.xsd" xmlns="http://www.iec.ch/61850/2003/SCL">
 <Header id="SynchroPhasor AA1 SED" toolID="SSI-Tool" nameStructure="IEDName" />
 <Substation name="AA1" desc="Substation">
  <VoltageLevel name="D1" desc="Voltage Level">
   <Bay name="Q1" desc="Bay" sxy:x="55" sxy:y="62" sxy:dir="vertical">
    <LNode iedName="AA10TH1" ldInst="AA1F1PMU" lnClass="MMXU" lnInst="1" />
    <ConductingEquipment name="BI1" desc="Current Transformer" type="CTR" sxy:x="8"
sxy:y="15" sxy:dir="vertical">
     <LNode iedName="AA10TH1" ldInst="AA1F1PMU" lnClass="TCTR" lnInst="1" />
     <Terminal name="AA1D1Q1N2" connectivityNode="AA1/D1/Q1/N2" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N2" />
     <Terminal name="AA1D1Q1N3" connectivityNode="AA1/D1/Q1/N3" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N3" />
    </ConductingEquipment>
    <ConductingEquipment name="QC2" desc="Isolator" type="DIS" sxy:x="10" sxy:y="21"
sxy:dir="vertical">
     <Terminal name="AA1D1Q1N6" connectivityNode="AA1/D1/Q1/N6" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N6" />
     <Terminal name="grounded" connectivityNode="AA1/D1/Q1/grounded"
substationName="AA1" voltageLevelName="D1" bayName="Q1" cNodeName="grounded" />
    </ConductingEquipment>
    <ConductingEquipment name="BU2" desc="Voltage Transformer 3Phase" type="VTR"
sxy:x="12" sxy:y="14" sxy:dir="vertical">
     <LNode iedName="AA10TH1" ldInst="AA1F1PMU" lnClass="TVTR" lnInst="1" />
     <Terminal name="AA1D1Q1N3" connectivityNode="AA1/D1/Q1/N3" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N3" />
    </ConductingEquipment>
    <ConductingEquipment name="QB2" desc="Isolator" type="DIS" sxy:x="12" sxy:y="4"
sxy:dir="vertical">
     <Terminal name="AA1D1QBBN4" connectivityNode="AA1/D1/QBB/N4"
substationName="AA1" voltageLevelName="D1" bayName="QBB" cNodeName="N4" />
     <Terminal name="AA1D1Q1N5" connectivityNode="AA1/D1/Q1/N5" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
    </ConductingEquipment>
    <ConductingEquipment name="QC1" desc="Isolator" type="DIS" sxy:x="10" sxy:y="8"
sxy:dir="vertical">
     <Terminal name="AA1D1Q1N5" connectivityNode="AA1/D1/Q1/N5" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
     <Terminal name="grounded" connectivityNode="AA1/D1/Q1/grounded"
substationName="AA1" voltageLevelName="D1" bayName="Q1" cNodeName="grounded" />
    </ConductingEquipment>
    <ConductingEquipment name="BI3" desc="Current Transformer" type="CTR" sxy:x="8"
sxy:y="19" sxy:dir="vertical">
     <Terminal name="AA1D1Q1N6" connectivityNode="AA1/D1/Q1/N6" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N6" />
```

```
        <Terminal name="AA1D1Q1N4" connectivityNode="AA1/D1/Q1/N4" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N4" />
      </ConductingEquipment>
      <ConductingEquipment name="QA1" desc="Circuit Breaker" type="CBR" sxy:x="8" sxy:y="11"
sxy:dir="vertical">
        <Terminal name="AA1D1Q1N3" connectivityNode="AA1/D1/Q1/N3" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N3" />
        <Terminal name="AA1D1Q1N5" connectivityNode="AA1/D1/Q1/N5" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
      </ConductingEquipment>
      <ConductingEquipment name="BI2" desc="Current Transformer" type="CTR" sxy:x="8"
sxy:y="17" sxy:dir="vertical">
        <Terminal name="AA1D1Q1N2" connectivityNode="AA1/D1/Q1/N2" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N2" />
        <Terminal name="AA1D1Q1N4" connectivityNode="AA1/D1/Q1/N4" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N4" />
      </ConductingEquipment>
      <ConductingEquipment name="QB1" desc="Isolator" type="DIS" sxy:x="6" sxy:y="4"
sxy:dir="vertical">
        <Terminal name="AA1D1Q1N5" connectivityNode="AA1/D1/Q1/N5" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
        <Terminal name="AA1D1QBBN1" connectivityNode="AA1/D1/QBB/N1"
substationName="AA1" voltageLevelName="D1" bayName="QBB" cNodeName="N1" />
      </ConductingEquipment>
      <ConductingEquipment name="QB4" desc="Isolator" type="DIS" sxy:x="8" sxy:y="23"
sxy:dir="vertical">
        <Terminal name="AA1D1Q1N1" connectivityNode="AA1/D1/Q1/N1" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N1" />
        <Terminal name="AA1D1Q1N6" connectivityNode="AA1/D1/Q1/N6" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N6" />
      </ConductingEquipment>
      <ConductingEquipment name="QC3" desc="Isolator" type="DIS" sxy:x="10" sxy:y="35"
sxy:dir="vertical">
        <Terminal name="AA1D1Q1N1" connectivityNode="AA1/D1/Q1/N1" substationName="AA1"
voltageLevelName="D1" bayName="Q1" cNodeName="N1" />
        <Terminal name="grounded" connectivityNode="AA1/D1/Q1/grounded"
substationName="AA1" voltageLevelName="D1" bayName="Q1" cNodeName="grounded" />
      </ConductingEquipment>
      <ConnectivityNode name="N1" pathName="AA1/D1/Q1/N1" sxy:x="8" sxy:y="31" />
      <ConnectivityNode name="N2" pathName="AA1/D1/Q1/N2" sxy:x="8" sxy:y="16" />
      <ConnectivityNode name="N3" pathName="AA1/D1/Q1/N3" sxy:x="9" sxy:y="13" />
      <ConnectivityNode name="N6" pathName="AA1/D1/Q1/N6" sxy:x="8" sxy:y="21" />
      <ConnectivityNode name="N5" pathName="AA1/D1/Q1/N5" sxy:x="9" sxy:y="6" />
      <ConnectivityNode name="N4" pathName="AA1/D1/Q1/N4" sxy:x="8" sxy:y="18" />
    </Bay>
    <Bay name="QBB" desc="Bay" sxy:x="63" sxy:y="36" sxy:dir="vertical">
      <ConnectivityNode name="N3" pathName="AA1/D1/QBB/N3" sxy:x="48" sxy:y="12" />
      <ConnectivityNode name="N2" pathName="AA1/D1/QBB/N2" sxy:x="47" sxy:y="17" />
      <ConnectivityNode name="N4" pathName="AA1/D1/QBB/N4" sxy:x="25" sxy:y="18" />
      <ConnectivityNode name="N1" pathName="AA1/D1/QBB/N1" sxy:x="22" sxy:y="20" />
    </Bay>
  </VoltageLevel>
 </Substation>
 <Substation name="AA2" desc="Substation" sxy:x="120" sxy:y="62">
  <VoltageLevel name="D1" desc="Voltage Level">
    <Bay name="Q1" desc="Bay" sxy:x="55" sxy:y="62" sxy:dir="vertical">
      <LNode iedName="AA10TH1" ldInst="AA10F1PMU" lnClass="MMXU" lnInst="1" />
```

```
      <ConductingEquipment name="BI1" desc="Current Transformer" type="CTR" sxy:x="8"
sxy:y="15" sxy:dir="vertical">
        <LNode iedName="AA10TH1" ldInst="AA10F1PMU" lnClass="TCTR" lnInst="1" />
        <Terminal name="AA1D1Q1N2" connectivityNode="AA2/D1/Q1/N2" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N2" />
        <Terminal name="AA1D1Q1N3" connectivityNode="AA2/D1/Q1/N3" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N3" />
      </ConductingEquipment>
      <ConductingEquipment name="QC2" desc="Isolator" type="DIS" sxy:x="10" sxy:y="21"
sxy:dir="vertical">
        <Terminal name="AA1D1Q1N6" connectivityNode="AA2/D1/Q1/N6" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N6" />
        <Terminal name="grounded" connectivityNode="AA2/D1/Q1/grounded"
substationName="AA2" voltageLevelName="D1" bayName="Q1" cNodeName="grounded" />
      </ConductingEquipment>
      <ConductingEquipment name="BU2" desc="Voltage Transformer 3Phase" type="VTR"
sxy:x="12" sxy:y="14" sxy:dir="vertical">
        <LNode iedName="AA10TH1" ldInst="AA10F1PMU" lnClass="TVTR" lnInst="1" />
        <Terminal name="AA1D1Q1N3" connectivityNode="AA2/D1/Q1/N3" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N3" />
      </ConductingEquipment>
      <ConductingEquipment name="QB2" desc="Isolator" type="DIS" sxy:x="12" sxy:y="4"
sxy:dir="vertical">
        <Terminal name="AA1D1QBBN4" connectivityNode="AA2/D1/QBB/N4"
substationName="AA2" voltageLevelName="D1" bayName="QBB" cNodeName="N4" />
        <Terminal name="AA1D1Q1N5" connectivityNode="AA2/D1/Q1/N5" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
      </ConductingEquipment>
      <ConductingEquipment name="QC1" desc="Isolator" type="DIS" sxy:x="10" sxy:y="8"
sxy:dir="vertical">
        <Terminal name="AA1D1Q1N5" connectivityNode="AA2/D1/Q1/N5" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
        <Terminal name="grounded" connectivityNode="AA2/D1/Q1/grounded"
substationName="AA2" voltageLevelName="D1" bayName="Q1" cNodeName="grounded" />
      </ConductingEquipment>
      <ConductingEquipment name="BI3" desc="Current Transformer" type="CTR" sxy:x="8"
sxy:y="19" sxy:dir="vertical">
        <Terminal name="AA1D1Q1N6" connectivityNode="AA2/D1/Q1/N6" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N6" />
        <Terminal name="AA1D1Q1N4" connectivityNode="AA2/D1/Q1/N4" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N4" />
      </ConductingEquipment>
      <ConductingEquipment name="QA1" desc="Circuit Breaker" type="CBR" sxy:x="8" sxy:y="11"
sxy:dir="vertical">
        <Terminal name="AA1D1Q1N3" connectivityNode="AA2/D1/Q1/N3" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N3" />
        <Terminal name="AA1D1Q1N5" connectivityNode="AA2/D1/Q1/N5" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
      </ConductingEquipment>
      <ConductingEquipment name="BI2" desc="Current Transformer" type="CTR" sxy:x="8"
sxy:y="17" sxy:dir="vertical">
        <Terminal name="AA1D1Q1N2" connectivityNode="AA2/D1/Q1/N2" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N2" />
        <Terminal name="AA1D1Q1N4" connectivityNode="AA2/D1/Q1/N4" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N4" />
      </ConductingEquipment>
      <ConductingEquipment name="QB1" desc="Isolator" type="DIS" sxy:x="6" sxy:y="4"
sxy:dir="vertical">
```

```
        <Terminal name="AA1D1Q1N5" connectivityNode="AA2/D1/Q1/N5" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N5" />
        <Terminal name="AA1D1QBBN1" connectivityNode="AA2/D1/QBB/N1"
substationName="AA2" voltageLevelName="D1" bayName="QBB" cNodeName="N1" />
      </ConductingEquipment>
      <ConductingEquipment name="QB4" desc="Isolator" type="DIS" sxy:x="8" sxy:y="23"
sxy:dir="vertical">
        <Terminal name="AA1D1Q1N1" connectivityNode="AA2/D1/Q1/N1" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N1" />
        <Terminal name="AA1D1Q1N6" connectivityNode="AA2/D1/Q1/N6" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N6" />
      </ConductingEquipment>
      <ConductingEquipment name="QC3" desc="Isolator" type="DIS" sxy:x="10" sxy:y="35"
sxy:dir="vertical">
        <Terminal name="AA1D1Q1N1" connectivityNode="AA2/D1/Q1/N1" substationName="AA2"
voltageLevelName="D1" bayName="Q1" cNodeName="N1" />
        <Terminal name="grounded" connectivityNode="AA2/D1/Q1/grounded"
substationName="AA2" voltageLevelName="D1" bayName="Q1" cNodeName="grounded" />
      </ConductingEquipment>
      <ConnectivityNode name="N1" pathName="AA2/D1/Q1/N1" sxy:x="8" sxy:y="31" />
      <ConnectivityNode name="N2" pathName="AA2/D1/Q1/N2" sxy:x="8" sxy:y="16" />
      <ConnectivityNode name="N3" pathName="AA2/D1/Q1/N3" sxy:x="9" sxy:y="13" />
      <ConnectivityNode name="N6" pathName="AA2/D1/Q1/N6" sxy:x="8" sxy:y="21" />
      <ConnectivityNode name="N5" pathName="AA2/D1/Q1/N5" sxy:x="9" sxy:y="6" />
      <ConnectivityNode name="N4" pathName="AA2/D1/Q1/N4" sxy:x="8" sxy:y="18" />
    </Bay>
    <Bay name="QBB" desc="Bay" sxy:x="63" sxy:y="36" sxy:dir="vertical">
      <ConnectivityNode name="N3" pathName="AA2/D1/QBB/N3" sxy:x="48" sxy:y="12" />
      <ConnectivityNode name="N2" pathName="AA2/D1/QBB/N2" sxy:x="47" sxy:y="17" />
      <ConnectivityNode name="N4" pathName="AA2/D1/QBB/N4" sxy:x="25" sxy:y="18" />
      <ConnectivityNode name="N1" pathName="AA2/D1/QBB/N1" sxy:x="22" sxy:y="20" />
    </Bay>
  </VoltageLevel>
 </Substation>
 <Communication>
  <SubNetwork name="AA1WA1" desc="IEC61850in center project" type="8-MMS">
   <ConnectedAP iedName="AA10KA1" apName="S1">
    <Address>
     <P type="SA">0</P>
     <P type="IP">172.20.0.100</P>
     <P type="IP-SUBNET">255.255.0.0</P>
     <P type="OSI-AP-Title">1,3,9999,23</P>
     <P type="OSI-AE-Qualifier">23</P>
     <P type="OSI-TSEL">0001</P>
     <P type="OSI-PSEL">00000001</P>
     <P type="OSI-SSEL">0001</P>
    </Address>
   </ConnectedAP>
   <ConnectedAP iedName="AA10TH1" apName="S1">
    <Address>
     <P type="SA">0</P>
     <P type="IP">172.20.1.3</P>
     <P type="IP-SUBNET">255.255.0.0</P>
     <P type="OSI-AP-Title">1,3,9999,23</P>
     <P type="OSI-AE-Qualifier">23</P>
     <P type="OSI-TSEL">0001</P>
     <P type="OSI-PSEL">00000001</P>
     <P type="OSI-SSEL">0001</P>
```

```
      </Address>
      <SMV desc="Phasor SVCB" ldInst="PDC" cbName="SyPh_SVCB1" />
     </ConnectedAP>
    </SubNetwork>
  </Communication>
  <IED name="AA10KA1" desc="OPC Server" type="OPCServer" manufacturer="Whatever"
configVersion="1.0">
    <AccessPoint name="S1">
     <LN inst="1" lnClass="IHMI" lnType="IHMI_OPCServer_IEC61850" />
    </AccessPoint>
  </IED>
  <IED name="AA10TH1" type="PDC" manufacturer="Whatever" configVersion="1.0">
    <Services>
     <DynAssociation />
     <GetDirectory />
     <GetDataObjectDefinition />
     <DataObjectDirectory />
     <GetDataSetValue />
     <ConfDataSet max="50" maxAttributes="240" />
     <ReadWrite />
     <ConfReportControl max="100" />
     <GetCBValues />
     <ReportSettings datSet="Conf" rptID="Dyn" optFields="Dyn" bufTime="Dyn" trgOps="Dyn"
intgPd="Dyn" />
     <SMVSettings datSet="Conf" />
    </Services>
    <AccessPoint name="S1">
     <Server>
      <Authentication none="true" />
      <LDevice inst="PDC">
       <LN0 inst="" lnClass="LLN0" lnType="LLN0_RELx_IEC61850">
        <DataSet name="PMUdata" desc="Common Synchrophasor message" >
         <FCDA ldInst="AA1F1PMU" prefix="" lnClass="MMXU" lnInst="1" doName="A.phsA"
fc="MX" />
          <FCDA ldInst="AA1F1PMU" prefix="" lnClass="MMXU" lnInst="1" doName="A.phsB"
fc="MX" />
          <FCDA ldInst="AA1F1PMU" prefix="" lnClass="MMXU" lnInst="1" doName="A.phsC"
fc="MX" />
          <FCDA ldInst="AA1F1PMU" prefix="" lnClass="MMXU" lnInst="1" doName="Health"
fc="ST" />
          <FCDA ldInst="AA1F1PMU" prefix="" lnClass="LPHD" lnInst="1" doName="PhyHealth"
fc="ST" />
          <FCDA ldInst="AA10F1PMU" prefix="" lnClass="MMXU" lnInst="1" doName="A.phsA"
fc="MX" />
          <FCDA ldInst="AA10F1PMU" prefix="" lnClass="MMXU" lnInst="1" doName="A.phsB"
fc="MX" />
          <FCDA ldInst="AA10F1PMU" prefix="" lnClass="MMXU" lnInst="1" doName="A.phsC"
fc="MX" />
          <FCDA ldInst="AA10F1PMU" prefix="" lnClass="MMXU" lnInst="1" doName="Health"
fc="ST" />
          <FCDA ldInst="AA10F1PMU" prefix="" lnClass="LPHD" lnInst="1" doName="PhyHealth"
fc="ST" />
         </DataSet>
         <DataSet name="StatUrgentA" desc="Status Data used to update process pictures and to
generate alarms.">
          <FCDA ldInst="AA1F1PMU" prefix="" lnClass="LPHD" lnInst="1" doName="PhyHealth"
fc="ST" />
```

```
          <FCDA ldInst="AA1F1PMU" prefix="" lnClass="TVTR" lnInst="1" doName="FuFail"
fc="ST" />
          <FCDA ldInst="AA1F1PMU" prefix="" lnClass="LLN0" doName="Mod" fc="ST" />
          <FCDA ldInst="AA1F1PMU" prefix="" lnClass="LPHD" lnInst="1" doName="PhyHealth"
fc="ST" />
          <FCDA ldInst="AA1F1PMU" prefix="" lnClass="TVTR" lnInst="1" doName="FuFail"
fc="ST" />
          <FCDA ldInst="AA1F1PMU" prefix="" lnClass="LLN0" doName="Mod" fc="ST" />
          <FCDA ldInst="PDC" prefix="" lnClass="LPHD" lnInst="1" doName="PhyHealth" fc="ST"
/>
          <FCDA ldInst="PDC" prefix="" lnClass="LLN0" doName="Mod" fc="ST" />
         </DataSet>
         <ReportControl name="rcb_A" datSet="StatUrgentA" confRev="2" bufTime="100"
buffered="true">
          <TrgOps dchg="true" qchg="true" />
          <OptFields />
          <RptEnabled max="5">
           <ClientLN iedName="AA10KA1" ldInst="none" lnInst="1" lnClass="IHMI" />
          </RptEnabled>
         </ReportControl>
         <SampledValueControl name="SyPh_SVCB1" desc="Phasor SVCB" datSet="PMUdata"
confRev="1" smvID="MyPhasors AA1+ AA2" smpRate="1" nofASDU="1" >
     <Protocol mustUnderstand=”true”>R-SV</Protocol>
  </SampledValueControl>
          <IEDName>AA10KA1</IEDName>
          <SmvOpts refreshTime="true" sampleRate="true" />
         </SampledValueControl>
        </LN0>
        <LN inst="1" lnClass="LPHD" lnType="Physical Device_RELx_IEC61850">
         <DOI name="Proxy">
          <DAI name="stVal" valKind="RO">
           <Val>0</Val>
          </DAI>
         </DOI>
        </LN>
       </LDevice>
       <LDevice inst="AA1F1PMU">
        <LN0 inst="" lnClass="LLN0" lnType="LLN0_RELx_IEC61850" />
        <LN inst="1" lnClass="LPHD" lnType="Physical Device_RELx_IEC61850">
         <DOI name="Proxy">
          <DAI name="stVal" valKind="RO">
           <Val>1</Val>
          </DAI>
         </DOI>
        </LN>
        <LN inst="1" lnClass="TCTR" lnType="CT_RELx_IEC61850" />
        <LN inst="1" lnClass="TVTR" lnType="VT_RELx_IEC61850" />
        <LN inst="1" desc="Synchrophasor measurements" lnClass="MMXU"
lnType="Syph_RELx_IEC61850">
         <DOI name="PhV">
          <SDI name="phsA">
           <DAI name="angRef">
            <Val>Synchrophasor</Val>
           </DAI>
          </SDI>
          <SDI name="phsB">
           <DAI name="angRef">
            <Val>Synchrophasor</Val>
```

```
            </DAI>
           </SDI>
           <SDI name="phsC">
            <DAI name="angRef">
             <Val>Synchrophasor</Val>
            </DAI>
           </SDI>
          </DOI>
          <DOI name="A">
           <SDI name="phsA">
            <DAI name="angRef">
             <Val>Synchrophasor</Val>
            </DAI>
           </SDI>
           <SDI name="phsB">
            <DAI name="angRef">
             <Val>Synchrophasor</Val>
            </DAI>
           </SDI>
           <SDI name="phsC">
            <DAI name="angRef">
             <Val>Synchrophasor</Val>
            </DAI>
           </SDI>
          </DOI>
         </LN>
        </LDevice>
        <LDevice inst="AA10F1PMU">
         <LN0 inst="" lnClass="LLN0" lnType="LLN0_RELx_IEC61850" />
         <LN inst="1" lnClass="LPHD" lnType="Physical Device_RELx_IEC61850">
          <DOI name="Proxy">
           <DAI name="stVal" valKind="RO">
            <Val>1</Val>
           </DAI>
          </DOI>
         </LN>
         <LN inst="1" lnClass="TCTR" lnType="CT_RELx_IEC61850" />
         <LN inst="1" lnClass="TVTR" lnType="VT_RELx_IEC61850" />
         <LN inst="1" desc="Synchrophasor measurements" lnClass="MMXU"
lnType="Syph_RELx_IEC61850">
          <DOI name="PhV">
           <SDI name="phsA">
            <DAI name="angRef">
             <Val>Synchrophasor</Val>
            </DAI>
           </SDI>
           <SDI name="phsB">
            <DAI name="angRef">
             <Val>Synchrophasor</Val>
            </DAI>
           </SDI>
           <SDI name="phsC">
            <DAI name="angRef">
             <Val>Synchrophasor</Val>
            </DAI>
           </SDI>
          </DOI>
          <DOI name="A">
```

```
            <SDI name="phsA">
              <DAI name="angRef">
                <Val>Synchrophasor</Val>
              </DAI>
            </SDI>
            <SDI name="phsB">
              <DAI name="angRef">
                <Val>Synchrophasor</Val>
              </DAI>
            </SDI>
            <SDI name="phsC">
              <DAI name="angRef">
                <Val>Synchrophasor</Val>
              </DAI>
            </SDI>
          </DOI>
        </LN>
      </LDevice>
    </Server>
  </AccessPoint>
 </IED>
 <DataTypeTemplates>
          …. Same as in previous example
 </DataTypeTemplates>
</SCL>
```

Annex C
(informative)

Migration from IEEE C37.118 to IEC 61850

C.1 General

In 2005, IEEE C37.118 – Synchrophasors for Power Systems was published. The scope of this standard was:

> "This is a standard for synchronized phasor measurement systems in power systems. It addresses the definition of a synchronized phasor, time synchronization, application of timetags, method to verify measurement compliance with the standard, and message formats for communication with a phasor measurement unit (PMU). In this context, a PMU can be a stand-alone physical unit or a functional unit within another physical unit. This standard does not specify limits to measurement response time, accuracy under transient conditions, hardware, software, or a method for computing phasors." [From IEEE C37.118.1]

Based upon the scope, there are two aspects to the standard:

a) measurement and time tagging specifications that allow for the creation of a synchronized phasor measurement;

b) a message format to convey the measured information.

   This message format specifies a packet structure, but does not standardize a communication profile over which to exchange the packet.

   During the standardization process, the use of IEC 61850 was discussed as an alternative to the "packet" structure. However, due to time constraints and industry pressures, the inclusion of IEC 61850 did not occur for the first publication of the standard.

In the late 2008-early 2009, IEEE requested IEC for a joint logo regarding IEEE C37.118. However, with the scope defined in IEEE C37.118, such a request needed to be coordinated between two different IEC Technical Committees (TCs).

> TC95 Scope: Standardization of measuring relays and protection equipment used in the various fields of electrical engineering covered by the IEC, taking into account combinations of devices to form schemes for power system protection including the control, monitoring and process interface equipment used with those systems.
>
> TC57 Scope: To prepare international standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA (Supervisory Control And Data Acquisition), distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information, used in the planning, operation and maintenance of power systems. Power systems management comprises control within control centres, substations and individual pieces of primary equipment including telecontrol and interfaces to equipment, systems and databases, which may be outside the scope of TC 57.

In order to accommodate IEEE coordination with the two (2) IEC TCs, and to allow synchrophasor information to be exchanged via IEC 61850, IEEE issued a Project Authorization Requests (PAR) in 2010 to split the IEEE C37.118 standard into two distinct parts.

> IEEE C37.118.1 – Measurement and time tagging specifications for synchronized phasors, frequency, and rate of change of frequency. This part deals with the measurements only and is intended to be coordinated for dual logo status through IEC TC95.
>
> IEEE C37.118.2 – A message format to convey the measured information. This part supports the legacy C37.118 formats and will remain an IEEE standard.

The intent of the two standards is to provide as much backward compatibility as possible with the IEEE C37.118:2005 standard, but to provide some enhancements. In the case of IEEE C37.118.1, substantial enhancements are ongoing to provide dynamic performance/measurement standardization as well as providing standardization for testing and calibration.

In regard to IEEE C37.118.2, there was a substantial set of requested enhancements as well as a limited set of problem resolutions. Upon evaluation of the enhancement requests, it was recognized that an equivalent protocol suite to IEC 61850 would need to be developed and that interoperability would probably not be able to be maintained should all of the enhancements be implemented. A decision was made that the IEEE C37.118.2 should standardize the current packet specification of IEEE C37.118:2005 with the resolution to several of the problematic issues. It was further decided that IEC 61850 should be used to provide the enhanced functionality.

The question became how to provide discrete and manageable steps from IEEE C37.118.2 into IEC 61850 for users/vendors that desired to use IEC 61850 or the enhanced functionality. The sequence of “manageable steps” constitutes a migration strategy. As such, the starting and end points of the strategy are readily understood. The starting point is IEEE C37.118:2005 and soon IEEE C37.118.2. The end point, for synchrophasors, would be IEC 61850 as modified by IEC/TR 61850-90-5 (this document). For both endpoints, the measurement techniques referenced would be IEEE C37.118.1.

The steps in the migration strategy can be summarized.

Starting Point: IEEE C37.118:2005 or IEEE C37.118.2.

This starting point provides the industry with the capability to proceed with projects and deployments using internationally recognized and stable standards.

Step 1: Provide standardized configuration capability for C37.118.1 communicating entities.

One of the major enhancement requests for C37.118 has been to provide a mechanism to configure a Phasor Measurement Unit (PMU) or Phasor Data Concentrator (PDC) to provide a subset the information available in the unit (e.g. PMU or PDC) for communication within the C37.118 Data packet.

NOTE In essence, this represents the ability to define the contents of IEEE C37.118 CFG-2 responses based upon a subset of the IEEE C37.118 CFG-1 response.

In the world of IEC 61850, the Substation Configuration Language (SCL) is used to define the overall information contents of a unit (e.g. CFG-1) and to define a subset of the information to be communicated (e.g. CFG-2) via a construct called a DataSet. Therefore, in order to provide the aforementioned configuration capability, Step 1 makes use of SCL to configure a C37.118 device.

Although the communication packet definition, via the creation of subsets/DataSets, is the primary focus of this migration step, there are other benefits as well.

There are several types of SCL files that are applicable for use: Instantiated IED Description (IID) or IED Capability Description (ICD) SCL files. It is preferable to utilize the IID file due to the fact that the file reflects the configuration of the communication parameters as well as user definitions for the DataSet configurations. The ICD file is provided by the vendor of the unit and represents a default configuration.

Step 2: Provide a first step to using the IEC 61850 protocol.

This step provides a user with the functionality for using the protocol, models, security, etc. as published within IEC/TR 61850-90-5 (this document) without the requirement of using ISO 9506 (e.g. the MMS profile in IEC 61850-8-1). This step basically provides a more enhanced protocol and service capability (e.g. supports events in addition to streams) as well as security. In essence, this step utilizes GOOSE and SV over a new routable profile. The configuration of the communication streams is still performed via SCL (same as in Step 1). However, without using ISO 9506, the enabling and disabling of the streams also needs to be performed in the SCL file.

End Point: Full IEC 61850 capability.

The end point provides the capabilities of Step 2 and adds the full capabilities of the other services and features of IEC 61850. As an example, this allows the Control blocks to be enabled/disabled dynamically (e.g. via communication and not just through SCL) as well as dynamic creation of DataSets.

In general, the steps can be represented in tabular form as shown in Table C.1:

Table C.1 – Migration steps from C37.118 to IEC 61850

Capability	Starting Point	Step 1 – adds to Starting Point	Step 2	End Point – adds to Step 2
Enable/Disable of synchrophasor data exchange	IEEE C37.118.2 Enable/Disable commands	SCL CID File could be used to automatically enable/disable.	Same as Step 1's use of SCL.	IEC 61850 control blocks provide the equivalent functionality of C37.118.2 commands for enabling/disabling as well.
Header exchange – obtaining descriptive information	IEEE C37.118.2 Header Exchange Command	SCL CID would be used to configure the descriptive information as well as being able to be used to retrieve it. This would be accomplished through the use of the description fields defined in the object model.	Same as Step 1's use of SCL.	Provides file transfer possibility as well as dynamic query capability similar (e.g. allows for descriptions to be retrieved via communication and not file exchange).
Provide a description of the capabilities of the device	IEEE C37.118.2 CFG-1	SCL CID file would be used.	Same as Step 1's use of SCL. or the extended 61850 GOOSE/Sav management services.	Adds ability to browse and validate via communications.
Provide a description of the configuration of the information being sent in the data exchange	IEEE C37.118.2 CFG-2	SCL CID file would be used. Additionally, multiple stream definition capability would be available due to the ability to configure DataSets and ControlBlocks.	Same as Step 1's use of SCL or the extended 61850 GOOSE/Sav management services.	Adds ability to browse, validate, and create additional DataSets dynamically.

Annex D
(informative)

Open system interconnect (OSI) model

The Open System Interconnect (OSI) model is a layered representation of the communication functionality required to implement communication interchange in an interoperable manner. The model is often referred to as the 7-layer model, because it describes seven (7) layers of functionality.

In general, the layers of functionality are recognized to be: Application; Presentation; Session; Transport; Network; Datalink; and Physical Layers. Each layer can be considered to "answer" a different set of questions about how to communicate with another device, as illustrated in Figure D.1.

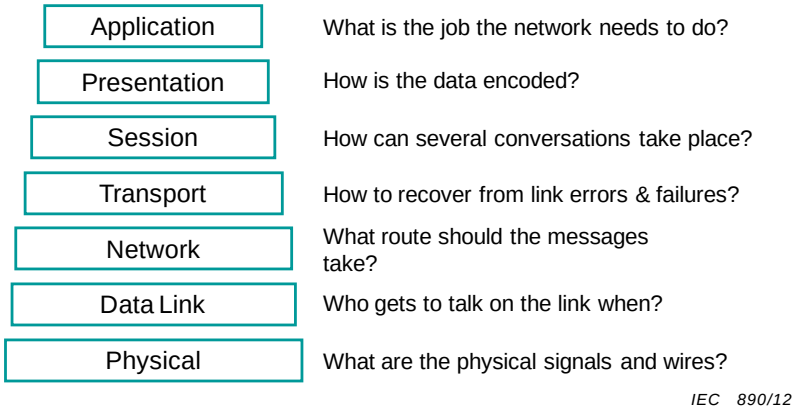


Figure D.1 – Tasks of the OSI model layers

Together, the seven layers are often known as a "stack". The software at each layer of the stack has its own address, its own data header that it adds to a message (an "envelope"), and its own processing rules.

It is important to note that while the OSI model was developed to describe the International Standards Organization (ISO) suite of protocols, it can be used to describe communications using any set of protocols. Figure D.2 shows roughly how OSI terminology corresponds to Internet Protocol (IP) terminology for naming layers.

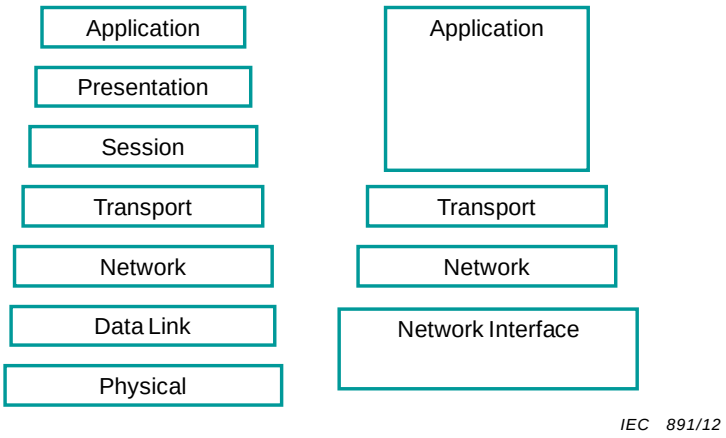
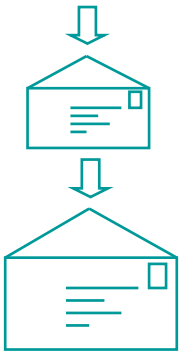


Figure D.2 – Comparison between OSI model and Internet models

To send data, a message must travel to the bottom of the stack, across to another device at the physical layer, and back up to the top of the stack. Moving down the stack, headers are added to a message. It is useful to think of encapsulating a mail envelope in a larger envelope with a different address on the outside, as shown in Figure D.3. Moving up the stack, the “envelopes” or headers are read, opened and removed.

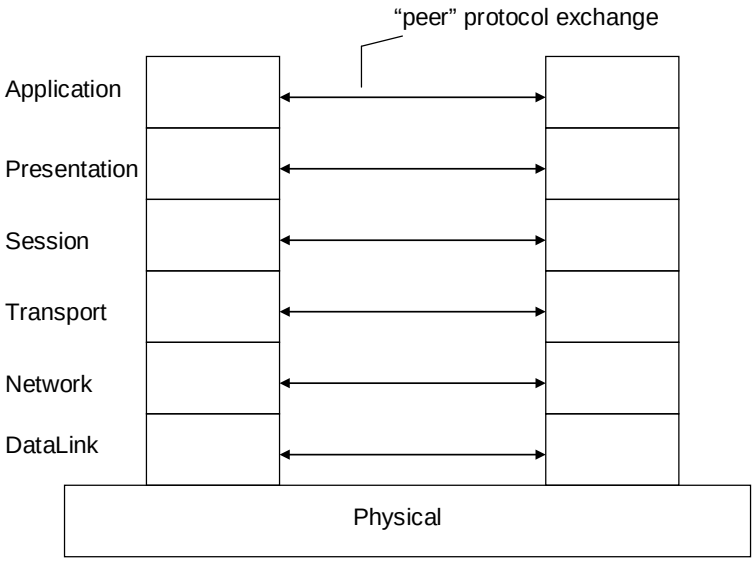


IEC 892/12

Figure D.3 – Visualizing adding layer headers

Each layer knows only its own addressing. As shown in Figure D.4, each layer communicates only with its peer layer on other devices and the layer immediately above and below.

In order to achieve interoperability, the software implementing each layer on a given device must be the “peer” of the equivalent layer software on the remote device (i.e. both peers must agree to use the same choices for protocols and implementation parameters).



IEC 893/12

Figure D.4 – Peer-to-peer data exchange in the OSI model

Each layer must pass information between the local layers. There is a convention for describing what the message is called as it is passed between the layers, as shown in Figure D.5.

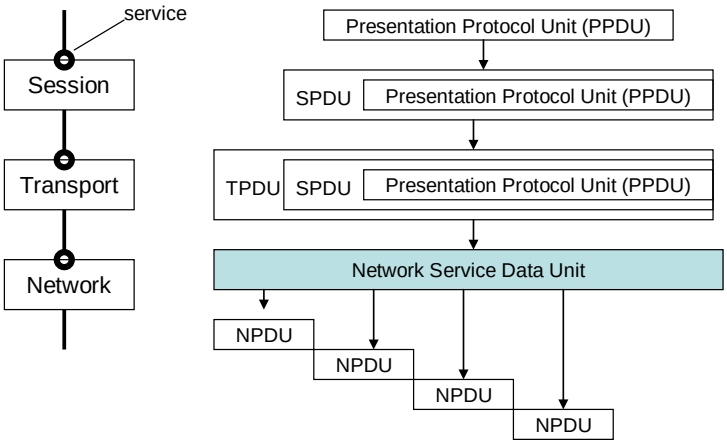


Figure D.5 – Relationship of OSI services to protocol data units (PDUs)

Each layer offers a communications service interface to the layer above it. These interfaces are standardized so that one layer may use the services of a variety of different underlying layers. This permits the underlying layers to be “mixed and matched” in an interoperable manner. For instance, an Internet Protocol (IP) network layer may use an Ethernet data link layer or a Point-to-Point Protocol (PPP) serial data link layer.

A message is called a Protocol Data Unit, or PDU. The diagram shows that a Presentation Protocol Data Unit (PPDU) is passed to the Session layer. The session layer adds additional information to the PPDU, and the combination is called a Session Protocol Data Unit (SPDU). This is in turn passed onto the Transport layer, etc. as was previously described in the “envelope” analogy.

It is the layer’s PDUs that are used to create the “peer” relationships that allow for information to be exchanged.

In some cases, one service provided by a layer may be the ability to segment or re-assemble information. Two good examples of this are the Transport and Network layers. In particular, the Network layer is responsible for segmenting the information sent to it by the Transport layer so that the packet size does not exceed the maximum packet size for the Data Link layer. In this case, sending one TPDU can cause multiple Network Protocol Data Units (NPDUs) to be transmitted.

A special naming convention is used to discuss this capability. While the name PDU is used for the message produced out the “bottom” of a layer, the name “Service Data Unit” is used for the data presented at the “top” of the next layer. Thus the concept of a Network Service Data Unit (NSDU) is used to represent the entire TPDU that causes multiple NPDUs to be sent. The service concept applies to other layers, particularly the Transport layer, where segmentation can also occur. For layers that do not segment, the PDU produced by a layer is equivalent to the Service Data Unit (SDU) it received with the header for that layer added.

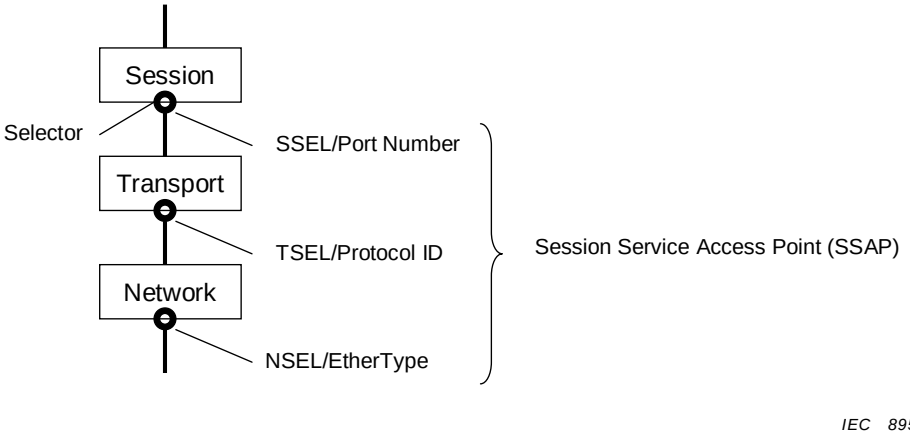


Figure D.6 – OSI model addressing

At each layer of the OSI Model, it is possible to use more than one different protocol. The OSI Model describes the use of special addresses called “selectors” to choose which protocol is going to be utilized at a given layer. Figure D.6 depicts the model and shows there is a selector (SEL) that specifies which protocol is to be utilized.

In the case of an incoming message arriving at the Network Layer from an Ethernet Data Link layer, the selection of the use of RFC 791 (IP) is designated by the EtherType ID of 800 hex. A message to be processed by a different network layer (say, the ISO connectionless network layer, or Novell IPX) would be labelled with a different EtherType. Therefore, The EtherType is the equivalent of an ISO Network Selector (NSEL).

The transport protocol to be used is chosen via a Transport Selector (TSEL). The equivalent of a TSEL, in the IP world, is the Protocol Identifier used to differentiate between UDP and TCP.

The next level protocol would be specified by a Session Selector (SSEL). In the Internet world, the SSEL is the IANA TCP Port Number that specifies the actual application protocol to be used (e.g. Port 80 for HTTP, Port 21 for FTP).

The total address information, including all of the selectors, is known as a Service Access Point. As an example, the addressing information needed to locate a particular Session protocol is known as a Session Service Access Point (SSAP). The SSAP includes all of the lower layer selectors.

Annex E
(informative)

IPv6

E.1 General

This annex provides the information needed to use/specify the use of Internet Protocol version 6 (IPv6). It is anticipated that an IPv6 T-Profile will be used in parallel to the IPv4 T-Profile initially. Additionally, it is the IPv6 T-Profile that will allow more wide area routing ability for larger scale integration/information exchange.

E.2 Additions to references needed for IPv6 support

The following should be added to the normative references:

RFC 2460 Internet Protocol, Version 6 (IPv6) Specification

RFC 2147 TCP and UDP over IPv6 Jumbograms

RFC 2461 Neighbour Discovery for IPv6

RFC 2464 Transmission of IPv6 Packets over Ethernet Networks

RFC 2375 IPv6 Multicast Address Assignments

RFC 3697 IPv6 Flow Label Specification

RFC 5095 Deprecation of Type 0 Routing Headers in IPv6

RFC 5722 Handling of Overlapping IPv6 Fragments

RFC 5871 IANA Allocation Guidelines for the IPv6 Routing Header

E.3 A-Profile

Shall be the same as in 11.1.

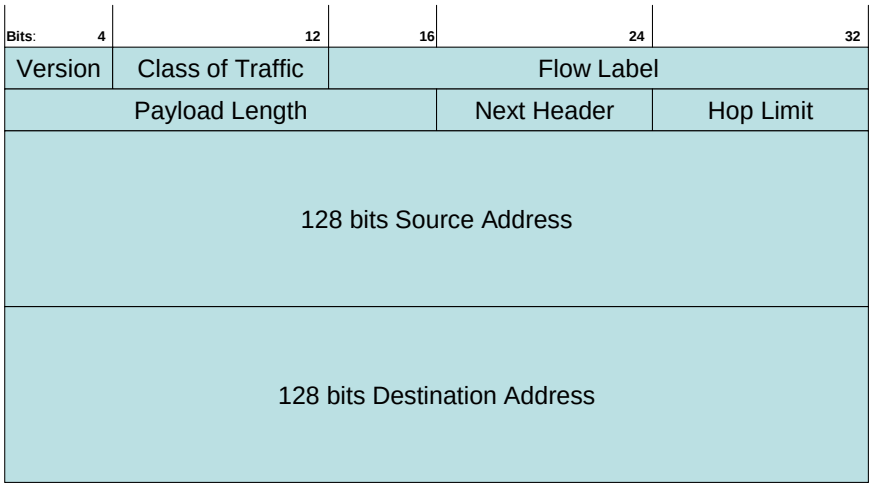
However, with the use of IPv6, there is a potential to send UDP packets that exceed a length supported by IPv4. These are called Jumbo Datagrams and shall not be used. This means that the use of RFC 2147 is excluded.

E.4 T-Profile

RFC-768 UDP
RFC-2326 – IP Authentication Header*
RFC-2460– Internetworking Protocol version 6 RFC 2461 – Neighbor Discovery for IPv6 RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks RFC 2375 - IPv6 Multicast Address Assignments RFC 1108 – U.S. Department of Defense Security options for the Internet Protocol
IEEE 802.1Q
ISO/IEC 8802-3 Ethertype
ISO/IEC 8802-3

E.4.1 IPv6 Options

The implementation of IPv6 shall support both unicast and multicast addressing.



Additionally, the ClassOfTraffic and FlowLabel fields shall be configurable. The recommendations found in RFC 3697 and RFC 2474 shall be followed.

E.5 SCL modifications

The current SCL definitions in IEC 61850-6 do not support the expression of an IPv6 address, subnets, or gateways. Therefore, it will eventually be necessary to add a mechanism to express this address.

These extensions are found in 13.2.4.

Annex F
(informative)

Edge authentication

Edge Authentication is typically a local issue. However, this Technical Report recommends that such authentication be performed using RFC 2406 – IP Encapsulating Security Payload.

The key negotiations, needed to support this protocol, are supported by the KDC mechanism (e.g. RFC 3547).

Annex G
(informative)

Example of A-Profile encodings

Figure G.1 shows an example encoding of the GOOSE and SV A-Profile.

Example of Single GOOSE APDU

LI							Hex Data example	SIG	For Entire Packet	RFC 1240
TI							40			ITU **X**.234 Connectionless Transport
LI							00			
SI							A1			IEC/TR 61850-90-5
LI							13			
							80			commonHeader
LI							12			
							00 00 FF ED		Doesn't support jumbo packets for now	SPDU User Data Length
							00 10 00 00		For duplicate packet delivery and OOD	SPDU Number
							00 01			Version Number
							4C F6 D9 FE		Seconds Since Epoch: 1970-01-01 00:00:00 UTC (value = December 1, 2010 23:27:58 UTC)	TimeOfCurrentKey
							00 10		Minutes until key change	TimeToNextKey
							00		High byte = Encryption information (**none**, AES-128, AES-256)	Security Algorithms
							02		Low byte = HMAC algorithm (none, , SHA256-80, **SHA256-128**, SHA256-256, MD5-80, MD5-128, MD5-256)	Security Algorithms
							00 00 01 00		Key ID assigned from KDC	
							xx xx xx xx			User Data Length
							81			GOOSE Payload type
							00		Simulation is FALSE	Simulation
							00 01		APPID is a value of 1	APPID
							yyyy+ 3		APDU Length	
							61 yyyy			GOOSE PDU
							85			Signature
LI							10			Length of HMAC
							16 octets		For SHA1-128	HMAC

IEC 896/12

Figure G.1 – Example encoding of GOOSE A-Profile

Annex H
(informative)

Improving reliability of R-SV transmissions

The use of multicast (UDP or Ethernet) does not guarantee message/data delivery. In most multicast protocols, a lost packet is not automatically detected and re-transmitted.

The GOOSE send service and message, as specified in IEC 61850-8-1, addresses this issue through a repeat mechanism where the transmitted dataset is repeated several times after the initial changed data packet is sent. As such, there is a very high probability, given that the network is intact, that a lost GOOSE message will eventually be received. The R-GOOSE, in that it inherits the operational characteristics of the GOOSE, will possess this message repeat function.

Sample Values, on the other hand, do not possess a repeat mechanism. In certain circumstances (especially at low message send rates), it may be desirable to increase the reliability of the received data. This can be achieved through a re-transmit of the R-SV data packet. In as much as the subscriber is designed to identify and reject duplicate packets, re-sending the exact same data packet is an effective way to achieve higher-reliability when desired. The re-launch mechanism, number of re-tries, and time between retries is a local issue.

For such re-transmissions, the SPDU Number needs to be identical to the original packet. This is required in order to allow the subscriber to detect duplicate delivery should the original packet have been received. It is further recommended that the contents of the entire SPDU be a duplicate of the original packet that is being repeated.

Annex I
(informative)

Guidance on HMAC and truncation

HMAC is a standard approach for achieving two-party authentication via shared symmetric keys. The HMAC standards and guidelines [6], [4], [5], [8], [9] [1] provide techniques and protocols to use HMAC such that the resulting authentication protocol is secure and resistant to replay attacks. One effective approach for dealing with replay attacks is to ensure that there is either a unique sequence number or a nonce for each message for any given shared key. This can be achieved by using either sequence numbers or nonces [8]. When HMAC is used for authentication, truncation of the output is an option occasionally used to conserve bandwidth. Truncation is considered reasonable in HMAC standards [4], [9] and is also used in practice; e.g., in TLS [7].

The following are some guidelines regarding the use of truncation from HMAC standards and guidelines.

- “The results in this area are not absolute as for the overall security advantages of truncation. ... Applications of HMAC can choose to truncate the output of HMAC by outputting the t leftmost bits of the HMAC computation for some parameter t ... We recommend that the output length t be not less than half the length of the hash output (to match the birthday attack bound) and not less than 80 bits.” [6]
- “When a truncated HMAC is used, the leftmost bytes of the HMAC computation shall be used as the MAC. The output length, shall be no less than four bytes ... However, t shall be at least L/2 bytes unless an application or protocol makes numerous trials impractical” [1]. Note that FIPS 198 [1] has been superseded by FIPS 198-1 [5], which defers to NIST-SP800-107 for truncation [6].
- “The length of a MacTag shall be sufficiently long to prevent false acceptance of forged data. For most applications, a length of 64 to 96 bits is sufficient.” [9]

As a practical example, TLS recommends a 96 bit truncated output [7].

---

1 Figures in square brackets refer to the Bibliography.

Bibliography

[1] "Undervoltage load shedding protection", IEEE Power System Relaying Committee, C13 Working Group Report (available in http://www.pes-psrc.org/c/) *(website checked 2012-04-02)*

[2] IMAI, S., "Undervoltage load shedding improving security as reasonable measure for extreme contingencies", IEEE Power Engineering Society General Meeting, 2005, IEEE

[3] OHURA Y., SUZUKI M., YANAGIHASHI K., YAMAURA M., OMATA K., NAKAMURA T., MITAMURA S. & WATANABE H., "A Predictive Out-of-step Protection Based on Observation of the Phase Difference between Substations", IEEE Trans. Power Delivery, PWRD-5. No.4 Nov.1990

[4] National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), (Standard, 2002). Available at http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf. *(website checked 2012-04-02)*

[5] National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), (July, 2008)

[6] KRAWCZYK, H., BELLARE, M., and CANETTI, R., 1997 Hmac: Keyed-Hashing for Message Authentication. RFC. RFC Editor

[7] BLAKE-WILSON S. et. al., RFC 4336 Transport Layer Security (TLS) Extensions, Network Working Group (IETF 2006). Available at http://www.ietf.org/rfc/rfc4366.txt. *(website checked 2012-04-02)*

[8] International Standards Organization, International Electrotechnical Commission, ISO/IETF 9798-4:1999, *Information technology Security techniques Entity authentication – Part 4: Mechanisms using a cryptographic check function*, (Standard, 1999). Available at http://www.iso.org.

[9] National Institute of Standards and Technology, Recommendation for Applications Us- ing Approved Hash Algorithms, (Special Publication 800-107, 2009). Available at http://csrc.nist.gov/publications/nistpubs/800-107/NIST-SP-800-107.pdf *(website checked 2012-04-02)*

[10] IEC/TR 61850-90-4, *Communication networks and systems for power utility automation – Part 90-4: Network engineering guidelines for substations*[2]

[11] IEC/TS 62351-2:2008, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

[12] IEC 62351-7:2010, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and system management (NSM) data object models*

2 Under consideration.

[13] IEC 62439-3, *Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)*[3]

[14] ISO 9506-1:2003, *Industrial automation systems, Manufacturing Message Specification – Part 1: Service Definition*

[15] ISO 9506-2:2003, *Industrial automation systems, Manufacturing Message Specification – Part 1: Protocol Specification*

[16] IEC/IEEE 60255-118-1, *Measuring relays and protection equipment – Part 118-1 Synchrophasor for power system – Measurements*

[17] IEEE 1344:1995, *IEEE Standard for Synchrophasors for Power Systems*

[18] IEEE C37.238: 2011, *IEEE Standard Profile for Use of IEEE Std. 1588 Precision Time Protocol in Power System Applications*

_____

3 To be published.

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch