

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Electricity metering data exchange – The DLMS/COSEM suite –
Part 8-3: Communication profile for PLC S-FSK neighbourhood networks**

**Échange des données de comptage de l'électricité – La suite DLMS/COSEM –
Partie 8-3: Profil de communication pour réseaux de voisinage CPL S-FSK**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2013 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

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It also gives information on projects, replaced and withdrawn publications.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.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,...).

Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Electricity metering data exchange – The DLMS/COSEM suite –
Part 8-3: Communication profile for PLC S-FSK neighbourhood networks**

**Échange des données de comptage de l'électricité – La suite DLMS/COSEM –
Partie 8-3: Profil de communication pour réseaux de voisinage CPL S-FSK**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XA

ICS 17.220; 35.110; 91.140.50

ISBN 978-2-83220-807-6

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	4
1 Scope.....	6
2 Normative references	6
3 Terms, definitions and abbreviations	7
3.1 Terms and definitions	7
3.2 Abbreviations	8
4 Targeted communication environments.....	9
5 Reference model	11
6 The physical layer (PhL).....	11
7 The data link layer.....	12
7.1 General.....	12
7.2 The MAC sublayer.....	12
7.3 The connectionless LLC sublayer	12
7.4 The HDLC based LLC sublayer	13
7.5 Co-existence of the connectionless and the HDLC based LLC sublayers.....	13
8 The application layer (AL).....	14
9 The application process (AP).....	14
10 The Configuration Initiation Application Service Element (CIASE)	14
10.1 Overview	14
10.2 The Discover service.....	14
10.3 The Register service	15
10.4 The Ping Service.....	15
10.5 The RepeaterCall service	17
10.6 The ClearAlarm service	19
10.7 The Intelligent Search Initiator process	21
10.7.1 General	21
10.7.2 Operation	21
10.8 The Discovery and Registration process.....	24
10.9 Abstract and transfer syntax.....	28
11 Addressing	28
11.1 General.....	28
11.2 IEC 61334-5-1 MAC addresses	28
11.3 Reserved special LLC addresses	28
11.3.1 General	28
11.3.2 Reserved addresses for the IEC 61334-4-32 LLC sublayer	29
11.3.3 Reserved addresses for the HDLC based LLC sublayer.....	29
11.3.4 Source and destination APs and addresses of CI-PDUs	30
12 Specific considerations / constraints for the IEC 61334-4-32 LLC sublayer based profile.....	31
12.1 Establishing application associations.....	31
12.2 Application association types, confirmed and unconfirmed xDLMS services	33
12.3 xDLMS client/server type services.....	33
12.4 Releasing application associations	33
12.5 Service parameters of the COSEM-OPEN / -RELEASE / -ABORT services.....	34
12.6 The EventNotification service and the TriggerEventNotificationSending service	34

12.7	Transporting long messages.....	35
12.8	Broadcasting	35
13	Specific considerations / constraints for the HDLC LLC sublayer based profile	35
13.1	Establishing Application Associations	35
13.2	Application association types, confirmed and unconfirmed xDLMS services	36
13.3	xDLMS client/server type services	37
13.4	Correspondence between AAs and data link layer connections, releasing AAs	37
13.5	Service parameters of the COSEM-OPEN/ -RELEASE/ -ABORT services.....	37
13.6	The EventNotification service and protocol.....	37
13.7	Transporting long messages.....	37
13.8	Broadcasting	37
14	Abstract syntax of CIASE APDUs	37
	Annex A (informative) S-FSK PLC encoding examples.....	39
	Bibliography.....	51
	Index	52
	Figure 1 – Communication architecture.....	10
	Figure 2 – The DLMS/COSEM S-FSK PLC communication profile.....	11
	Figure 3 – Co-existence of the connectionless and the HDLC based LLC sublayers.....	13
	Figure 4 – Intelligent Search Initiator process flow chart	22
	Figure 5 – The Discovery and Registration process	25
	Figure 6 – MSC for the discovery and registration process.....	32
	Figure 7 – MSC for successful confirmed AA establishment.....	32
	Figure 8 – MSC for releasing an Application Association	34
	Figure 9 – MSC for an EventNotification service	35
	Figure 10 – MSC for the Discovery and Registration process	36
	Figure 11 – MSC for successful confirmed AA establishment and the GET service	36
	Table 1 – Service parameters of the Discover service primitives	15
	Table 2 – Service parameters of the Register service primitives	15
	Table 3 – Service parameters of the PING service primitives	16
	Table 4 – Service parameters of the RepeaterCall service primitives	17
	Table 5 – Service parameters of the ClearAlarm service primitives	20
	Table 6 – MAC addresses.....	28
	Table 7 – Reserved IEC 61334-4-32 LLC addresses on the client side	29
	Table 8 – Reserved IEC 61334-4-32 LLC addresses on the server side	29
	Table 9 – Reserved HDLC based LLC addresses on the client side	29
	Table 10 – Reserved HDLC based LLC addresses on the server side.....	29
	Table 11 – Source and Destination APs and addresses of CI-PDUs.....	31
	Table 12 – Application associations and data exchange in the S-FSK PLC profile using the connectionless LLC sublayer	33

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**ELECTRICITY METERING DATA EXCHANGE –
THE DLMS/COSEM SUITE –****Part 8-3: Communication profile for PLC S-FSK neighbourhood networks**

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 International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this International Standard may involve the use of a maintenance service concerning the stack of protocols on which the present standard IEC 62056-8-3 is based.

The IEC takes no position concerning the evidence, validity and scope of this maintenance service.

The provider of the maintenance service has assured the IEC that he is willing to provide services under reasonable and non-discriminatory terms and conditions for applicants throughout the world. In this respect, the statement of the provider of the maintenance service is registered with the IEC. Information may be obtained from:

DLMS¹ User Association
Zug/Switzerland
www.dlms.ch

¹ Device Language Message Specification.

International Standard IEC 62056-8-3 has been prepared by technical committee 13: Electrical energy measurement, tariff- and load control.

The text of this standard is based on the following documents:

FDIS	Report on voting
13/1526/FDIS	13/1544/RVD

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

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

A list of all the parts in the IEC 62056 series, published under the general title *Electricity metering data exchange – The DLMS/COSEM suite*, can be found on the IEC website.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

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.

ELECTRICITY METERING DATA EXCHANGE – THE DLMS/COSEM SUITE –

Part 8-3: Communication profile for PLC S-FSK neighbourhood networks

1 Scope

This part of IEC 62056 specifies the DLMS/COSEM PLC S-SFK communication profile for neighbourhood networks.

It uses standards established by IEC TC 57 in the IEC 61334 series, *Distribution automation using distribution line carrier systems* and it specifies extensions to some of those standards.

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 60050 (all parts), *International Electrotechnical Vocabulary* (available at <http://www.electropedia.org>)

IEC 61334-4-1:1996, *Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 1: Reference model of the communication system*

IEC 61334-4-32:1996, *Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 32: Data link layer – Logical link control (LLC)*

IEC 61334-4-511:2000, *Distribution automation using distribution line carrier systems – Part 4-511: Data communication protocols – Systems management – CIASE protocol*

IEC 61334-5-1:2001, *Distribution automation using distribution line carrier systems – Part 5-1: Lower layer profiles – The spread frequency shift keying (S-FSK) profile*

IEC/TR 62051:1999, *Electricity metering – Glossary of terms*

IEC/TR 62051-1:2004, *Electricity metering – Data exchange for meter reading, tariff and load control – Glossary of terms – Part 1: Terms related to data exchange with metering equipment using DLMS/COSEM*

IEC 62056-46:2002, *Electricity metering – Data exchange for meter reading, tariff and load control – Part 46: Data link layer using HDLC protocol*
Amendment 1:2006

IEC 62056-5-3:—, *Electricity metering data exchange – The DLMS/COSEM suite – Part 5-3: DLMS/COSEM application layer*²

² To be published simultaneously with this part of IEC 62056.

IEC 62056-6-2:—, *Electricity metering data exchange – The DLMS/COSEM suite – Part 6-2: COSEM interface classes*³

ISO/IEC 8802-2:1998, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 2: Logical link control*

NOTE See also the Bibliography.

3 Terms, definitions and abbreviations

For the purposes of this document, the terms and definitions given in IEC 60050-300, IEC/TR 62051 and IEC/TR 62051-1 and the following apply.

Where there is a difference between the definitions in the glossary and those contained in product standards produced by TC 13, then the latter shall take precedence in applications of the relevant standard.

3.1 Terms and definitions

3.1.1

initiator

user-element of a client System Management Application Entity (SMAE). It uses the CIASE and xDLMS ASE and it is identified by its system title

[SOURCE: IEC 61334-4-511:2000, 3.8.1, modified]

3.1.2

active initiator

initiator, which issues or has last issued a CIASE Register request when the server is in the unconfigured state

[SOURCE: IEC 61334-4-511:2000, 3.9.1]

3.1.3

new system

server system, which is in the unconfigured state: its MAC address equals "NEW-address"

[SOURCE: IEC 61334-4-511:2000, 3.9.3]

3.1.4

new system title

system-title of a new system

Note 1 to entry: This is the system title of a system, which is in the new state.

[SOURCE: IEC 61334-4-511:2000, 3.9.4, modified]

3.1.5

registered system

server system, which has an individual, valid MAC address

Note 1 to entry: Therefore, this MAC address is different from "NEW Address", see IEC 61334-5-1: Medium Access Control.

[SOURCE: IEC 61334-4-511:2000, 3.9.5, modified]

³ To be published simultaneously with this part of IEC 62056.

3.1.6

reporting system

server system, which issues a DiscoverReport

[SOURCE: IEC 61334-4-511:2000, 3.9.6, modified]

3.1.7

sub-timeslot

the time needed to transmit two bytes by the physical layer

Note 1 to entry: Timeslots are divided to sub-slots in the RepeaterCall mode of the physical layer.

3.1.8

timeslot

the time needed to transmit a physical frame

Note 1 to entry: As specified in IEC 61334-5-1:2001, 3.3.1, a physical frame comprises 2 bytes preamble, 2 bytes start subframe delimiter, 38 bytes PSDU and 3 bytes pause.

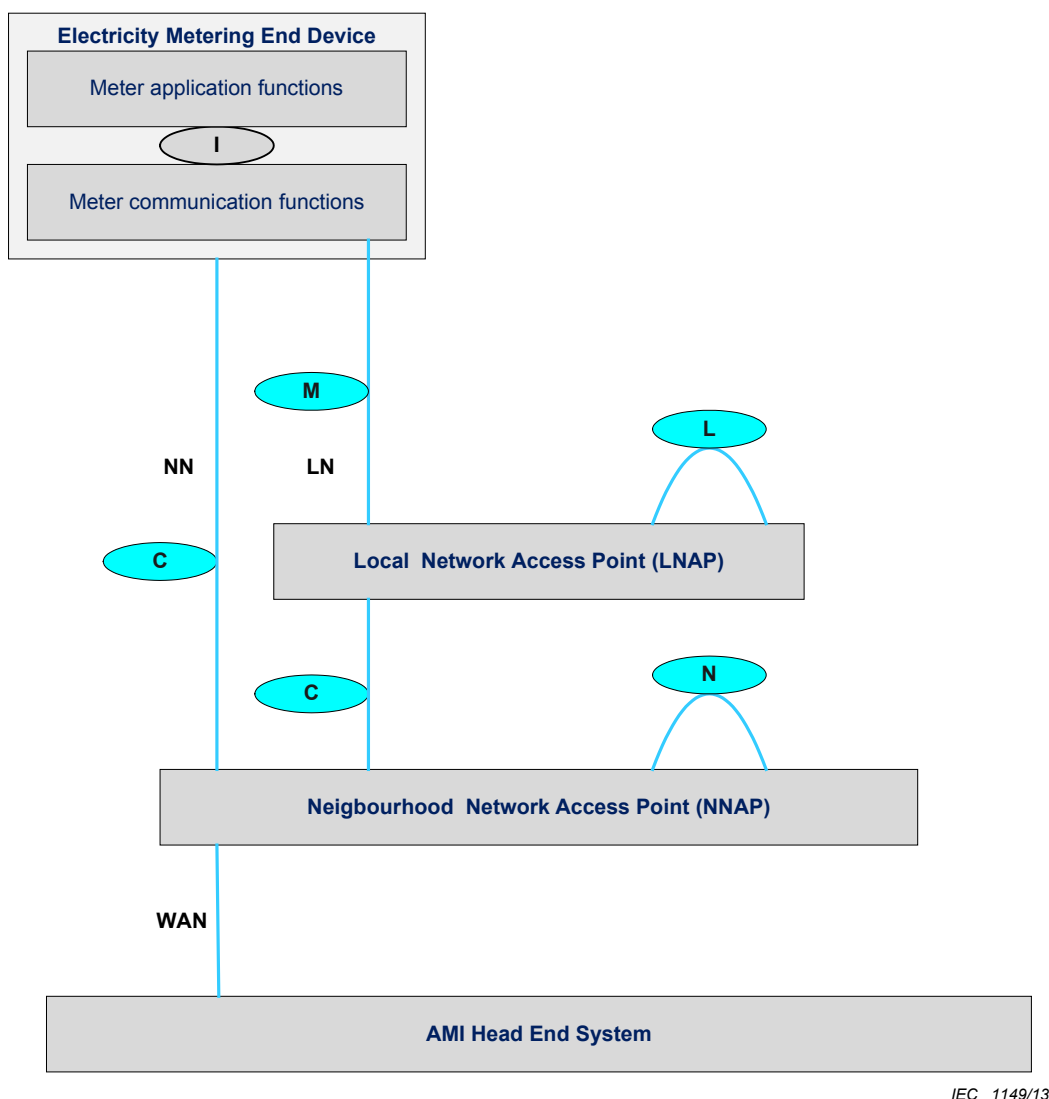
3.2 Abbreviations

.cnf	.confirm service primitive
.ind	.indication service primitive
.req	.request service primitive
.res	.response service primitive
AA	Application Association
AARE	A-Associate Response – an APDU of the ACSE
AARQ	A-Associate Request – an APDU of the ACSE
ACSE	Association Control Service Element
AES	Advanced Encryption Standard
AL	Application Layer
AP	Application Process
APDU	Application Layer Protocol Data Unit
ASE	Application Service Element
ASO	Application service Object
A-XDR	Adapted Extended Data Representation
CIASE	Configuration Initiation Application Service Element
CI-PDU	CIASE PDU
Client	A station, asking for services. In the case of the 3-layer, CO HDLC based profile it is the master station
COSEM	Companion Specification for Energy Metering
DA	Destination Address
DLMS	Device Language Message Specification
DLMS UA	DLMS User Association
FCS	Frame Check Sequence
GCM	Galois/Counter Mode, an algorithm for authenticated encryption with associated data
HCS	Header Check Sequence
HDLC	High-level Data Link Control
HES	(Metering) Head End System
ISO	International Organization for Standardization

LLC	Logical Link Control (Sublayer)
LN	Local Network
LNAP	Local Network Access Point
L-SAP	LLC sublayer Service Access Point
LSDU	LLC Service Data Unit
LV	Low voltage
MAC	Medium Access Control (sublayer)
MPDU	MAC Layer Protocol Data Unit
MSC	Message Sequence Chart
NN	Neighbourhood Network
NNAP	Neighbourhood Network Access Point
NS	Number of subframes (S-FSK MAC sublayer)
OSI	Open System Interconnection
PDU	Protocol Data Unit
PhL	Physical Layer
PLC	Power Line Carrier
PSDU	Physical Layer Service Data Unit
RDR	Reply Data on Request (used in IEC 61334-4-32)
RLRE	A-Release Response – an APDU of the ACSE
RLRQ	A-Release Request – an APDU of the ACSE
SA	Source Address
SAP	Service Access Point
SDN	Send Data Non-acknowledged (used in IEC 61334-4-32)
SDU	Service Data Unit
SMAE	Systems Management Application Entity
SMAP	Systems Management Application Process
SNRM	Set Normal Response Mode (a HDLC frame type)

4 Targeted communication environments

The DLMS/COSEM PLC S-FSK communication profile is intended for remote data exchange on Neighbourhood Networks (NN) between Neighbourhood Network Access Points (NNAP) *and* Local Network Access Points (LNAPs) or End Devices using S-FSK power line carrier technology over the low voltage electricity distribution network as a communication medium. The functional reference architecture is shown in Figure 1.



IEC 1149/13

Figure 1 – Communication architecture

End devices – typically electricity meters – comprise application functions and communication functions. They may be connected directly to the NNAP via the C interface, or to an LNAP via an M interface, while the LNAP is connected to the NNAP via the C interface. The LNAP function may be co-located with the metering functions.

A NNAP comprises gateway functions and it may comprise concentrator functions. Upstream, it is connected to the Metering Head End System (HES) using suitable communication media and protocols.

End devices and LNAPs may communicate to different NNAPs, but to one NNAP only at a time. From the PLC communication point of view, the NNAP acts as an initiator while end devices and LNAPs act as responders.

NNAPs and similarly LNAPs may communicate to each other, but this is out of the scope of this standard, which covers the C interface only.

When the NNAP has concentrator functions, it acts as a COSEM client. When the NNAP has gateway functions only, then the HES acts as a COSEM client. The end devices or the LNAPs act as COSEM servers.

5 Reference model

NOTE This clause is partly based on IEC 61334-4-1:1996, Clause 3.

The reference model of the *DLMS/COSEM PLC S-FSK communication profile* is shown in Figure 2. It is based on a simplified – or collapsed – three-layer OSI architecture. The layers are the *physical layer*, the *data link layer* and the *application layer*. The data link layer is split to the *MAC sublayer* and the *LLC sublayer*.

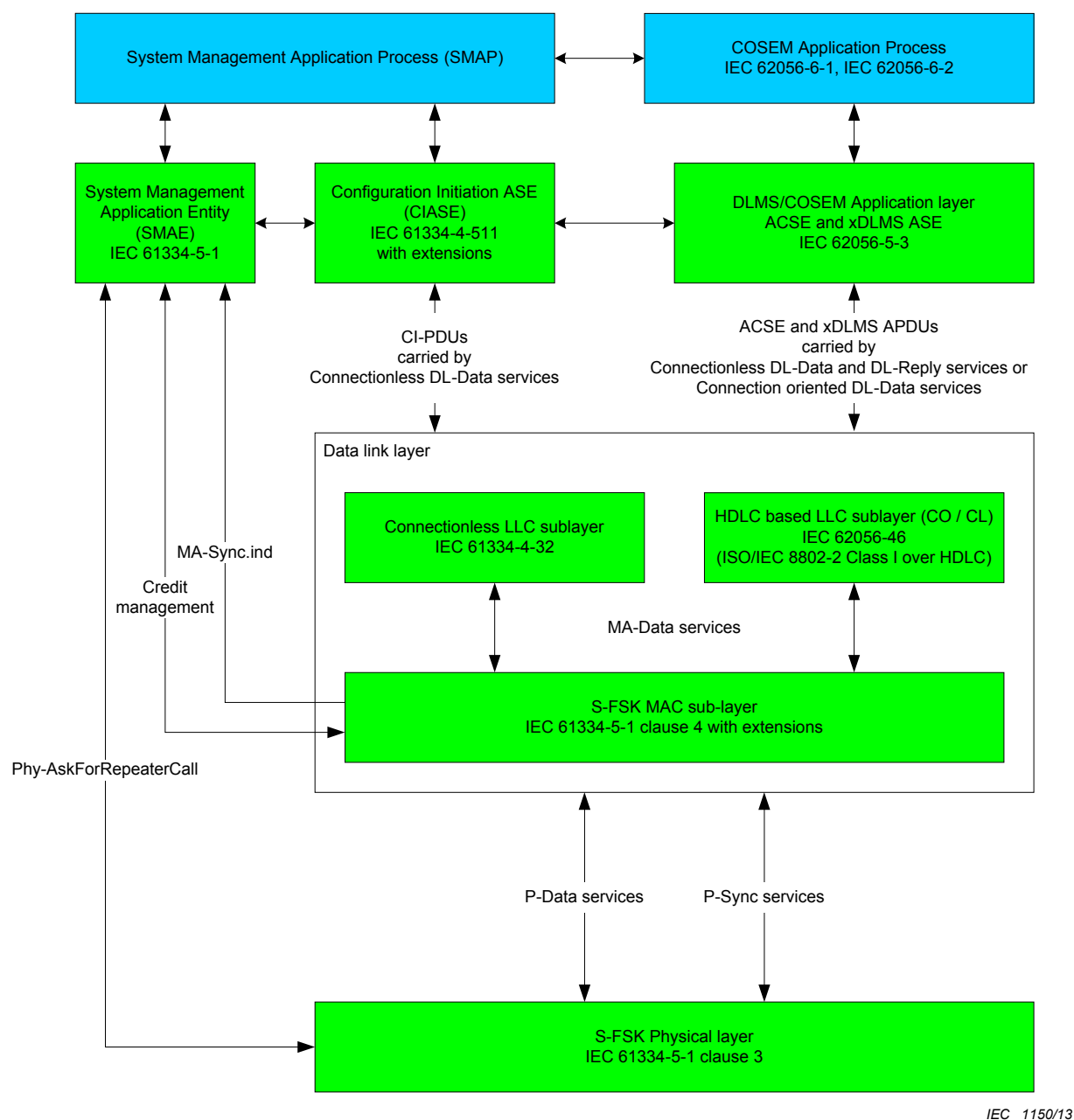


Figure 2 – The DLMS/COSEM S-FSK PLC communication profile

6 The physical layer (PhL)

The PhL provides the interface between the equipment and the physical transmission medium that is the distribution network. It transports binary information from the source to the destination.

The PhL in this profile is as specified in IEC 61334-5-1:2001, Clause 3. It provides the following services to its service user MAC sublayer:

- P-Data services to transfer MPDUs to (a) peer MAC sublayer entity(ies) using the LV distribution network as the transport medium;
- P-Sync services to allow the MAC sublayer entity to ask for a new synchronization and to be informed of a change in the synchronization state of the PL. These services are used locally by the MAC sublayer.

See IEC 61334-5-1:2001, 3.4.

7 The data link layer

7.1 General

The data link layer consists of two sublayers: the Medium Access Control (MAC) and the Logical Link Control (LLC) sublayer.

The MAC sublayer handles access to the physical medium and provides physical device addressing. The decision to access the medium is made by the initiator, directly for its own MAC sublayer, or indirectly for other MAC sublayers that are requested to transmit a response to a request sent previously by the initiator.

The LLC sublayer controls the logical links.

There are two LLC sublayer alternatives available:

- the connectionless LLC sublayer, as specified in IEC 61334-4-32;
- the LLC sublayer using the HDLC based data link layer, as specified in IEC 62056-46.

7.2 The MAC sublayer

The MAC sublayer of the DLMS/COSEM S-FSK PLC communication profile is as specified in IEC 61334-5-1:2001, Clause 4. It provides the following services to its service user LLC sublayer:

- the MA-Data services. These services allow the LLC sublayer entity to exchange LLC data units with peer LLC sublayer entities. See IEC 61334-5-1:2001, 4.1.3.1;
- the MA-Sync.indication service. This allows the SMAE entity to be informed of the synchronization and configuration status of the device. See IEC 61334-5-1:2001, 4.1.3.2.

7.3 The connectionless LLC sublayer

The connectionless LLC sublayer is as specified in IEC 61334-4-32. It is derived from ISO/IEC 8802-2 – similar to Class III operation – and it performs the following functions:

- addressing of application entities within the equipment;
- sending data with no acknowledgement (SDN);
- reply data on request (RDR).

It provides the following services:

- DL-Data services for transporting CI-PDUs, ACSE APDUs and client-server type xDLMS APDUs;
- DL-Reply services for asking the remote LLC sublayer entity to send a previously prepared LSDU;
- DL-Update-Reply services to prepare the LSDUs to be transferred using the DL-Reply services.

For more details, see IEC 61334-4-32:1996, 2.1.

7.4 The HDLC based LLC sublayer

The HDLC based LLC sublayer is as specified in IEC 62056-46.

As explained in IEC 62056-46:2002, 4.1 and 4.2, this sublayer can also be divided to two sublayers:

- the LLC sublayer based on ISO/IEC 8802-2. Here, it is used in an extended Class I operation. The only role of this sublayer is to select the DLMS/COSEM Application layer by using a specific LLC address. The LLC services are provided by the HDLC based MAC sublayer;
- the MAC sublayer, based on the HDLC protocol. It provides addressing of application entities within the equipment.

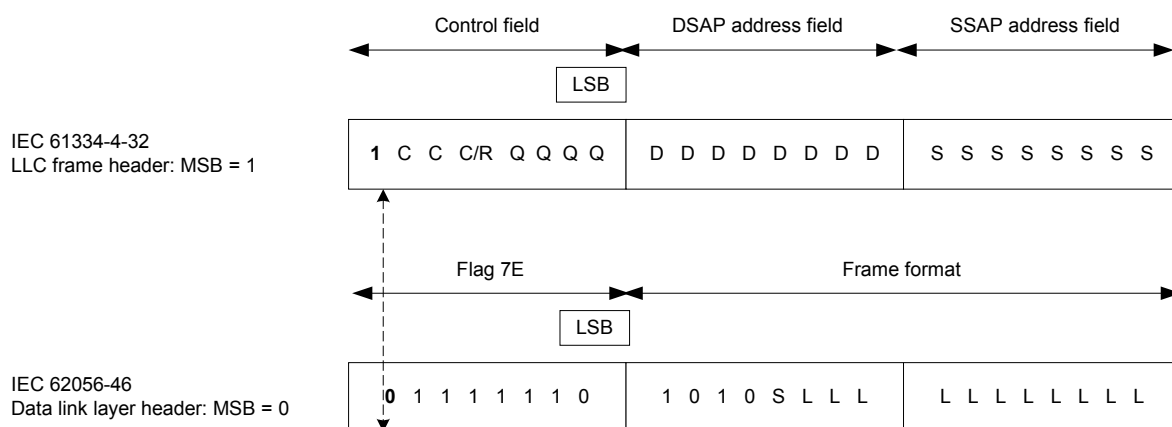
NOTE In this profile, there are two MAC sublayers. The HDLC MAC sublayer provides reliable LLC data transport and segmentation. The Medium Access Control functionality is provided by the S-FSK MAC sublayer specified in 7.2.

The HDLC based LLC sublayer provides the following services:

- DL-Connect services to connect and to disconnect the data link layer;
- connectionless DL-Data services for transporting CI-PDUs, ACSE APDUs and xDLMS APDUs;
- connection oriented DL-Data services for transporting ACSE APDUs and xDLMS APDUs. These services provide reliable data transport and support segmentation to carry long messages, in a transparent manner for the application layer.

7.5 Co-existence of the connectionless and the HDLC based LLC sublayers

The frames of the connectionless LLC sublayer and the HDLC based LLC sublayer can be distinguished from each other as shown in Figure 3. This allows systems using the two profiles to co-exist on the same network.



Legend:
 C: Command subfield
 C/R: Command / response bit
 QQQQ: Qualifier subfield
 DDDDDDD: Destination address
 SSSSSSSS: Source address
 S: Segmentation
 L: Length

IEC 1151/13

Figure 3 – Co-existence of the connectionless and the HDLC based LLC sublayers

8 The application layer (AL)

Concerning the application layer, the DLMS/COSEM Application layer as specified in IEC 62056-5-3 applies. It provides services to the COSEM application process (AP) and uses the services of the connectionless or the HDLC based LLC sublayer.

9 The application process (AP)

On the server side, the COSEM device- and object model – as specified in IEC 62056-6-2 – applies. Each logical device represents an AP.

The client side APs make use of the resources of the server side AP. A physical device may host one or more client APs.

10 The Configuration Initiation Application Service Element (CIASE)

NOTE This clause is based on IEC 61334-4-511 and constitutes an extension to it.

10.1 Overview

One of the activities of systems management is open system initialisation and / or modification. This is provided by the Configuration Initiation ASE (CIASE). It is specified in IEC 61334-4-511 with the extensions specified below.

The CIASE services are the following:

- the Discover service;
- the Register service;
- the PING service;
- the RepeaterCall service; and
- the ClearAlarm service.

The three latter services, together with the Intelligent Search Initiator process specified in 10.7, constitute upper compatible functional extensions to IEC 61334-4-511.

The CIASE uses the connectionless DL-Data services of the LLC sublayer.

10.2 The Discover service

NOTE In this document, the description of the CIASE services follows the presentation style used for the DLMS/COSEM services. For the notation used, see IEC 62056-5-3:—, 6.1.

The Discover service is used to discover new systems or systems, which are in alarm state. It is specified in IEC 61334-4-511:2000, 7.1. The Discover service primitives shall provide the parameters as shown in Table 1.

Table 1 – Service parameters of the Discover service primitives

	Discover		DiscoverReport	
	.request	.indication	.response	.confirm
Argument	M	M (=)	–	–
Response_Probability	M	M (=)		
Allowed_Time_Slots	M	M (=)		
DiscoverReport_Initial_Credit	M	M (=)		
IC_Equal_Credit	M	M (=)	–	–
Result (+)			S	S (=)
System_Title {System_Title}	–	–	M	M (=)
Alarm_Descriptor			C	C (=)
Result (-)			S	S (=)
Argument_Error(s)	–	–	M	M (=)
NOTE This Table 1 is included here for completeness and to correct some editorial errors in IEC 61334-4-511:2000, 7.1. For the description of the service parameters, see the clause referenced here.				

10.3 The Register service

The Register service is used to perform system configuration. It assigns a MAC address to a new system identified by its system title. It is specified in IEC 61334-4-511:2000, 7.2. The Register service primitives shall provide the parameters as shown in Table 2.

Table 2 – Service parameters of the Register service primitives

	.request	.indication
Argument		
Active_Initiator_System_Title	M	M (=)
List_Of_Correspondence	M	M (=)
New_System_Title	M	M (=)
MAC_Address	M	M (=)
Result (+)	S	S
Result (-)	S	S
Argument_Error(s)	M	M (=)
NOTE This Table 2 is included here for completeness. For the description of the service parameters, see IEC 61334-4-511:2000, 7.2.		

NOTE 1 If a server in NEW state receives a correct Register service with its own server system title in it, it will be registered, even if it did not receive a Discover service before.

NOTE 2 Only those servers in the NEW state can be registered.

10.4 The Ping Service

Function

The Ping service is used to check that a server system already registered is still present on the network. It also allows verifying that the right physical device is linked to the right MAC address. It also allows preventing the *time_out_not_addressed* timer to expire.

The process begins with a Ping.request service primitive issued by the active initiator. The service contains the system title of the physical device pinged. The PingRequest CI-PDU is carried by a DL-Data.request service primitive and it is sent to the MAC address assigned to this system and to the server CIASE L-SAP.

If the system title carried by the Ping.indication service primitive is equal to the system title of the server, the server shall respond with a Ping.response service primitive, carrying the system title of the server. It is sent to the initiator CIASE L-SAP.

Semantics

The PING service primitives shall provide parameters as shown in Table 3.

Table 3 – Service parameters of the PING service primitives

	.request	.indication	.response	.confirm
Argument System_Title_Server	M	M (=)	-	-
Result (+) System_Title_Server	–	–	S M	S (=) M (=)
Result (–) Argument_Error(s)	–	–	S M	S M (=)

The System_Title_Server service parameter allows identifying a physical device concerned by the Ping service. The destination MAC address in the DL-Data.request service primitive is equal to the MAC address that has been assigned to this system using the Register service.

The Ping.response service primitive returns with « Result (+) » if the Ping.request service has succeeded, i.e. the system title of the physical device at the given MAC address is equal to the “System_Title_Server” carried by the Ping.request service primitive.

Otherwise, no response is sent by the server.

Use – Client side

The Ping.request service primitive is issued by the active initiator.

If the “System_Title_Server” service parameter is not valid, a local confirmation is sent immediately with a negative result indicating the problem encountered (Ping-system-title-nok).

Otherwise, the CIASE forms a DL-Data.request PDU containing a PingRequest CI-PDU that carries the System_Title_Server requested. It is sent to the physical device concerned by the request.

Once the transmission of the PingRequest CI-PDU is over, the CIASE waits for a DL-Data.indication service primitive containing a PingResponse CI-PDU from the physical device pinged, during the necessary time that depends on the initial credit of the request.

If the CIASE receives a DL-Data.indication service primitive containing a PingResponse CI-PDU before this delay is over, it sends to the initiator a confirmation with a positive result, containing the service parameter returned by the server system.

If no DL-DATA.indication service primitive is received, the CIASE sends to the initiator a confirmation with a negative result pointing out the absence of an answer (Ping-no-response).

Use – Server side

On the reception of a DL-Data.indication service primitive containing a PingRequest CI-PDU, the CIASE checks that the System_Title_Server service parameter is correct and that it is equal to its own system title.

If so, it invokes a Ping.response service primitive that includes its system title. The PingResponse CI-PDU is carried by a DL-Data.request service primitive.

If the service parameter of the Ping.indication service primitive is not correct, no response is sent.

Finally, if the System_Title_Server service parameter in the Ping.indication service primitive is correct, but not equal to the system title of the physical device, no response is sent.

10.5 The RepeaterCall service

Function

The purpose of the RepeaterCall service is to adapt the repeater status of server systems depending on the topology of the electrical network. It allows the automatic configuration of the repeater status on the whole network.

In the RepeaterCall mode, the client and the servers transmit short frames – two bytes long each – and measure the level of the signal to determine if a server system should be a repeater or not.

Semantics

The RepeaterCall service primitives shall provide parameters as shown in Table 4.

Table 4 – Service parameters of the RepeaterCall service primitives

	. request	. indication
Arguments		
Max_Adr_MAC	M	M (=)
Nb_Tslot_For_New	U	U (=)
Reception_Threshold	M	M (=)
Result (+)	S	S
Result (-)	S	S
Argument_Error(s)	M	M

The Max_Adr_MAC service parameter allows calculating the number of timeslots used in the RepeaterCall mode by the physical layer of the server systems registered to an initiator. It corresponds to the largest server system MAC address that is stored by the initiator.

NOTE 1 The largest allowable server MAC address is 3071 (BFF), as the range C00...DFF is reserved for the initiator, as specified in IEC 61334-5-1:2001, 4.3.7.7.1.

The value of Nb_Tslot is calculated from this information:

$$Nb_Tslot = \lfloor MaxAdrMax / 21 \rfloor + 1$$

where $\lfloor x \rfloor$ means the floor of x , the nearest integer $\leq x$.

EXAMPLE 1

Max_Adr_MAC = 20 (20 servers on the network)

$$Nb_Tslot = \lfloor 20/21 \rfloor + 1 = 1$$

Nb_Tslot = 1, with 1 sub-timeslot for the NNAP (concentrator) and 20 sub-timeslots for the servers.

EXAMPLE 2

Max_Adr_MAC = 21 (21 servers on the network)

$$Nb_Tslot = \lfloor 21/21 \rfloor + 1 = 2$$

Nb_Tslot = 2:

1 timeslot with 1 sub-timeslot for the NNAP (concentrator) and 20 sub-timeslots for 20 servers;

1 timeslot with 1 sub-timeslot for one server.

The Nb_Tslot_For_New service parameter defines the number of timeslots used in the RepeaterCall mode by the physical layer of the server systems in NEW state. If the value of this service parameter is 0 (or not present) then the systems in NEW state are not allowed to participate in the Repeater Call process.

The maximum number of timeslots used by the physical layer is equal to the sum of the number of timeslots for the server systems registered and the number of timeslots for the server systems in NEW state.

The Reception_Threshold service parameter defines the threshold of the signal level in dBμV, necessary to validate a physical pattern in a Sub_Tslot when the physical layer is in the RepeaterCall mode.

The Result (+) service parameter (positive result) indicates that the requested service has succeeded.

The Result (–) service parameter (negative result) indicates that the requested service has failed.

The “Arguments Error” indicates that at least one argument has a wrong value.

Use – Client side

The RepeaterCall service of the CIASE is invoked by the SMAP.

If any of the arguments is not valid, a confirmation is sent immediately with a negative result indicating the problem encountered.

Otherwise, the CIASE forms a DL-Data.request service primitive containing a RepeaterCall CI-PDU carrying the parameters requested. This request is sent to all server systems.

A positive confirmation is passed to the CIASE upon the reception of a DL-Data.cnf(+).

When this confirmation is received, the CIASE sends the Phy_AskForRepeaterCall.request primitive allowing the activation of the RepeaterCall mode of the physical layer. The parameters of this primitive are the following:

- Sub_Tslot position: on the client (initiator) side its value is 0;
- Reception_Threshold.

NOTE 2 On the client side, the Reception_Threshold parameter has no significance.

Use – server side

On the server side, on the reception of a DL-Data.indication service primitive containing a RepeaterCall CI-PDU, the CIASE verifies that the service parameters are correct.

If this is the case, it sends the Phy_AskForRepeaterCall.request primitive to activate the RepeaterCall mode of the physical layer. The parameters of this primitive are the following:

- Sub_Tslot position: A number expressed on two octets, between 0 and 65 535. The value 0 is reserved for the configuration of the NNAP (concentrator). The other values are available for the configuration of server systems.

In the case of server systems registered by a NNAP (concentrator), Sub-Tslot takes the value of the local MAC address of the server system, between 1 and Max_Adr_MAC. For the server systems not registered, Sub_Tslot takes a random value between Max_Adr_MAC and Max_Adr_MAC + (Nb_Tslot_For_New * 21).

NOTE 3 Max_Adr_MAC and Nb_Tslot_For_New are the service parameters of the RepeaterCall.request service.

- Reception_Threshold: This represents the signal level in dBμV. The default value is 104.

If the response to this request is negative, the command is cancelled. The following cases lead to a failure:

- the state of the physical layer is not correct (there is no physical synchronization);
- the repeater status is never_repeater;
- the parameters are incorrect.

The participation of the servers in the repeater call process and the effect of the process on their repeater status depend on the *repeater* management variable (attribute 10 of the S-FSK Phy&MAC setup object, see IEC 62056-6-2:—, 5.8.4) and the signal level heard:

- servers configured as never repeater do not participate: they do not transmit during their sub-timeslot and their repeater_status (attribute 11 of the S-FSK Phy&MAC setup object) is not affected;
- servers configured as always repeater participate: they transmit during their timeslot but their repeater_status is not affected;
- servers configured as dynamic repeater participate: they transmit during their sub-timeslot, if they have not heard a signal before from the client or from any servers, which is above the reception threshold. If during the whole repeater call process, a server does not hear a signal from the client or from other servers, which is above the reception threshold, then its repeater status will be TRUE: the server will repeat all frames. If a server hears a signal from the client or from other servers, which is above the reception threshold, then its repeater status will be FALSE: the server won't repeat any frames.

NOTE 4 If each server configured as dynamic repeater hears a signal, which is above the reception threshold, this means that they are all close to a client, and no repetition is needed. So, none of them will become a repeater.

10.6 The ClearAlarm service

Function

The ClearAlarm service allows clearing the alarm state in (a) server system(s), in a point-to-point or in a broadcast mode.

Semantics

The ClearAlarm service primitives shall provide parameters as shown in Table 5.

Table 5 – Service parameters of the ClearAlarm service primitives

	.request	.indication
Arguments		
Alarm_Descriptor	S	S (=)
Alarm_Descriptor {Alarm_Descriptor}	S	S (=)
Alarm_Descriptor_List_And_Server_List	S	S (=)
System_Title {System_Title}	M	M (=)
Alarm_Descriptor {Alarm_Descriptor}	M	M (=)
Alarm_Descriptor_By_Server {Alarm_Descriptor_By_Server}	S	S (=)
System_Title	M	M (=)
Alarm_Descriptor	M	M (=)
Result (+)	S	S
Result (-)	S	S
Arguments Error	M	M

This service provides four different possibilities:

- the Alarm_Descriptor choice allows clearing a single alarm in all server systems. The value of the Alarm_Descriptor parameter identifies the alarm to be cleared;
- the Alarm_Descriptor {Alarm_Descriptor} choice allows clearing a list of alarms in all server systems. The value of the Alarm_Descriptor {Alarm_Descriptor} parameter identifies the list of alarms to be cleared;
- the Alarm_Descriptor_List_And_Server_List choice allows clearing a common list of alarms specified in the list of server systems specified. The System_Title {System_Title} parameter identifies the list of server systems in which the alarms have to be cleared. The value of the Alarm_Descriptor {Alarm_Descriptor} parameter identifies the list of alarms to be cleared;
- the Alarm_Descriptor_By_Server {Alarm_Descriptor_By_Server} choice allows clearing one alarm specified in each server specified. The System_Title parameter identifies the server system in which the alarm has to be cleared. The value of the Alarm_Descriptor parameter identifies the alarm to be cleared.

As specified in IEC 61334-4-511:2000, 6.2.2, alarm descriptors should be specified in companion specifications.

The Result (+) argument (positive result) indicates that the requested service has succeeded.

The Result (–) argument (negative result) indicates that the requested service has failed.

The “Argument Error(s)” indicates that at least one argument has a wrong value.

Use

The ClearAlarm CIASE service is invoked by the initiator.

If any of the service parameters is not valid, a confirmation is sent immediately with a negative result indicating the problem encountered.

Otherwise, the CIASE forms a DL-Data.request service primitive containing a ClearAlarm CI-PDU containing the parameters requested. This request is sent to the server system(s) concerned by the request. A positive confirmation is sent upon the reception of a DL-Data.cnf(+) service primitive.

On the server side, on the reception of a DL-Data.indication service primitive containing a ClearAlarm CI-PDU, the CIASE verifies that the arguments are correct. If this is the case, it clears the alarms corresponding to the list of alarms. Otherwise, the service is ignored.

10.7 The Intelligent Search Initiator process

10.7.1 General

The objective of the Intelligent Search Initiator process is to improve plug&play installation of server systems, by ensuring that each server system is registered by the correct initiator.

When a new server system is placed on the network, it will be discovered and registered by the first initiator it hears talking. It remains registered by that initiator as long as it keeps receiving correct frames (the `time_out_not_addressed` timer does not expire). If there is cross-talk on the network, the server system may be registered by the wrong initiator, i.e. one, which is “heard” by the server system due to cross-talk.

When the Intelligent Search Initiator process is implemented in the server system, it is capable to establish a list of all initiators it can “hear”, and to lock on the initiator with the best signal level.

10.7.2 Operation

10.7.2.1 Flow chart

The intelligent search initiator process comprises two phases:

- the *Search Initiator* phase;
- the *Check Initiator* phase.

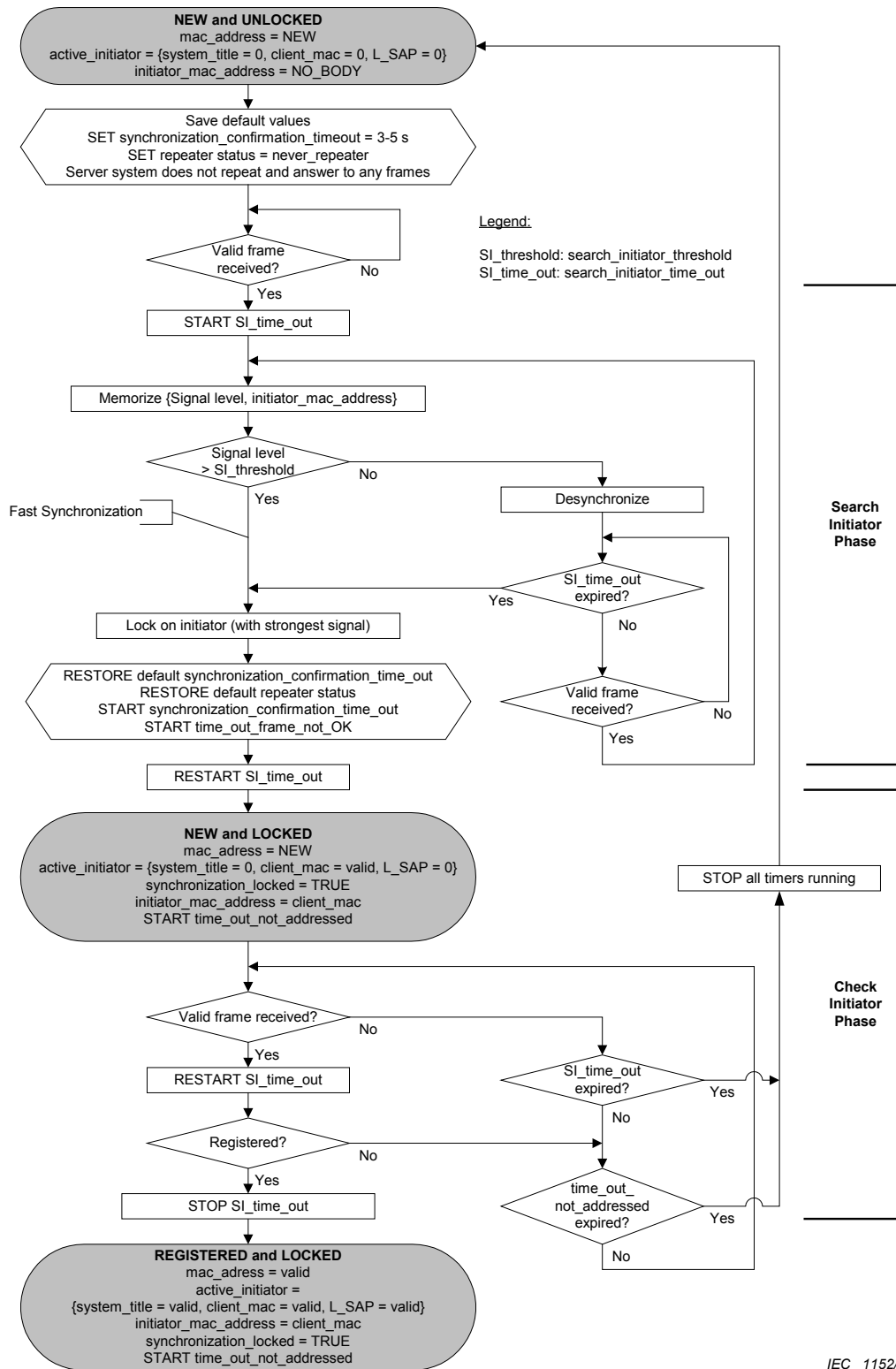
The Intelligent Search Initiator process is shown in Figure 4. See also Figure 5 showing the complete discovery and registration process.

10.7.2.2 Process parameters

The Intelligent Search Initiator process is characterized by two parameters:

- The `search_initiator_time_out`, defining the duration of the Search Initiator Phase. This timeout is also used during the Check Initiator Phase, see 10.7.2.4;
The Search Initiator Phase shall be long enough to allow the server systems to hear all the initiators around them and, when needed, to let sufficient time to start all the initiators by the Head End System. However, this time should not be too long either, so that the discovery phase could be executed correctly. The recommended value for this timeout is 10 minutes;
- The `search_initiator_threshold`, defining the minimum signal level allowing a fast synchronization.

The value of the `search_initiator_threshold` should be chosen so that the server systems next to an initiator lock on it immediately, but the server systems a bit further away (maybe on another network) do only lock on it after the `search_initiator_time_out` timer expires. The default value is 98 dBμV.



IEC 1152/13

NOTE A valid frame is a frame in which either the source or the destination address is an initiator address, and otherwise correct.

Figure 4 – Intelligent Search Initiator process flow chart

10.7.2.3 Search Initiator Phase

Initially, the server system is in the NEW and UNLOCKED state waiting to receive a valid frame.

For the Search Initiator Phase, the `synchronization_confirmation_time_out` shall be reduced to 3-5 s. Otherwise, a server system would remain synchronized too long on a bad frame.

During this phase, a server system shall not repeat any frames. This is because if repetition was allowed, it would have to repeat all frames, not only the frames from the closest initiator, and so the other server systems next to it would listen to frames from a bad initiator with a strong signal level. Therefore, the Intelligent Search Initiator algorithm can only be efficient if all the server systems on a network have the algorithm implemented (otherwise, other server systems could repeat frames and foul the signal level).

For the same reasons, a server system shall not transmit any frames during the Search Initiator Phase:

- it should not answer to a Discover request (It should be desynchronised before, except if the signal level is good enough to allow fast synchronization. But in this case, the server system is not in the Search Initiator Phase anymore but in the Check Initiator Phase);
- it should not answer to a Register request either;
- and in particular, it should not answer any ACSE or xDLMS service requests (this is obvious because the server system is in the NEW state).

Notice that as soon as a server system becomes locked, it can repeat frames since it will only accept frames from the good initiator. (It is even advised that it repeats frames, since it will shorten the Search Initiator Phase for the other server systems).

Each time that the server system receives a frame, it checks the signal level and the MAC addresses in it:

- if none of the MAC addresses – source or destination – is an initiator MAC address, the frame is considered as invalid; the server system immediately desynchronises in order to listen to another frame;
- if one of the MAC addresses is an initiator MAC address, and the signal level is good enough ($\text{signal level} > \text{search_initiator_threshold}$ – see 10.7.2.2) the server system locks on that initiator. This is called Fast Synchronization. This occurs when the server system is next to an initiator or to a server system that is already registered to that initiator. The server system enters the Check Initiator Phase;
- if one of the MAC addresses is an initiator MAC address but the signal level is not good enough ($\text{signal level} < \text{search_initiator_threshold}$), the server system memorizes the signal level and the MAC address, then desynchronizes immediately in order to listen to another frame;
- when the `search_initiator_time_out` expires, the server system locks to the initiator having provided the best signal level.

At this point:

- the default values of the `synchronization_confirmation_time_out` and the repeater status are restored;
- the `synchronization_confirmation_time_out` and the `time_out_frame_not_OK` timers are initialised;
- the `search_initiator_time_out` is restarted.

The server is in the NEW and LOCKED state and enters the Check Initiator Phase.

10.7.2.4 Check Initiator Phase

Once the server system is locked, it can be discovered and registered. The process is the following:

- the `time_out_not_addressed` timer is started;

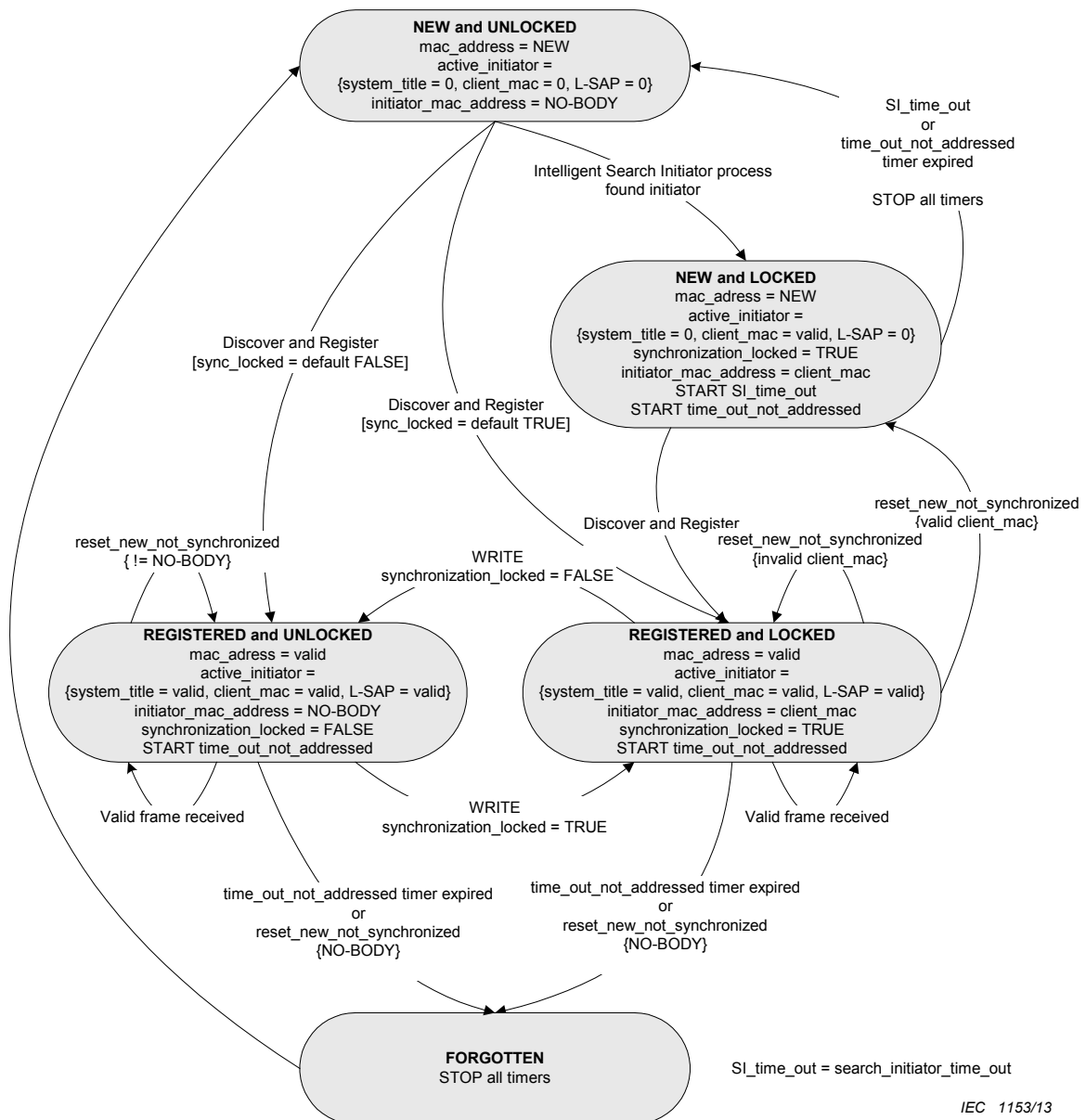
- the server waits then to be discovered and registered;
- the search_initiator_time_out timer is restarted each time a valid frame is received;
- when the server system is registered (valid frame carrying a Register CI-PDU received):
 - the search_initiator_time_out timer is stopped;
 - the active_initiator variable is set;
- if either the search_initiator_time_out or the time_out_not_addressed timer expires, it means that the server system did not receive a frame from or to its initiator for a long time: all timers are stopped then and the server system returns to the initial state: NEW and UNLOCKED.

10.7.2.5 Remarks

The Intelligent Search Initiator process has to be used cautiously. If a server system hears a frame with a wrong MAC address, it will lock on it and won't unlock until the search_initiator_time_out is over. It is advised not to change the initiator MAC address of an NNAP (concentrator) unless it can be made sure that all the server systems on the network are in the unconfigured state: NEW and UNLOCKED.

10.8 The Discovery and Registration process

The Discovery and Registration process, including the Intelligent Search Initiator process, is summarized in Figure 5.



NOTE The state transitions caused by writing the mac-address and initiator-mac-address variables are not shown.

Figure 5 – The Discovery and Registration process

The process is the following.

Initially, the server is in the NEW and UNLOCKED (UNCONFIGURED) state. In this state:

- mac_address = NEW;
- active_initiator: default value, with all three elements set to 0:
 - system_title = octet string of 0;
 - (client_)mac_address = NO-BODY;
 - L-SAP_selector = 0;
- initiator_mac_address = NO-BODY.

The default value of the synchronization_locked variable is as specified in the companion specification:

- a) FALSE: the value of `initiator_mac_address` variable is always NO-BODY;
- b) TRUE: the value of the `initiator_mac_address` variable follows the value of the `(client_)mac_address` element of the `active_initiator` variable;
- c) The Intelligent Search Initiator process is used. In this case, the value of the `search_initiator_time_out` variable shall be different from 0. The server moves from the NEW and UNLOCKED state to the NEW and LOCKED state at the end of the Search Initiator Phase.

NOTE This third possibility is an extension to IEC 61334-4-511.

When a server is installed, it has to be discovered and registered.

In case a), upon the reception of a valid Register CIASE PDU the server moves to the REGISTERED and UNLOCKED state:

- the `mac_address` variable is set to the value allocated by the initiator;
- the elements of the `active_initiator` variable are set to the values contained in the Register CIASE PDU and the DL-Data.indication LLC PDU:
 - `system_title`: system title of the initiator;
 - `(client_)MAC_address`: MAC address of the initiator;
 - `L-SAP_selector`: the L-SAP used by the initiator;
- the `initiator_MAC_address` remains at NO-BODY;
- the `synchronization_locked` variable remains at FALSE;
- the `time_out_not_addressed` timer is started.

In case b), upon the reception of a valid Register CIASE PDU, the server moves to the REGISTERED and LOCKED state:

- the `mac_address` variable is set to the value allocated by the initiator;
- the elements of the `active_initiator` variable are set to the values contained in the Register CIASE PDU and the DL-Data.indication LLC PDU:
 - `system_title`: system title of the initiator;
 - `(client_)mac_address`: MAC address of the initiator;
 - `L-SAP_selector`: the L-SAP used by the initiator;
 - the `initiator_MAC_address` is updated to be equal to the `(client_)MAC_address` element of the `active_initiator`;
 - the `synchronization_locked` attribute remains at TRUE;
 - the `time_out_not_addressed` timer is started.

In case c), the server searches first for the initiator providing the strongest signal; see Figure 4. At the end of Search Initiator Phase, the `search_initiator_time_out` is re-started, the `time_out_not_addressed` timer is started, and the server locks on the initiator chosen:

- the `(server_)mac_address` variable is still at NO-BODY (server is in NEW state);
- the `synchronization_locked` variable is set to TRUE;
- the `(client_)MAC_address` element of the `active_initiator` variable takes the `MAC_address` of the initiator chosen. The other elements of the `active_initiator` variable remain at their default value;
- the `initiator_MAC_address` is updated to be equal to the `(client_)MAC_address` element of the `active_initiator` variable.

The server is in the NEW and LOCKED state and enters the Check Initiator Phase.

The server can only be registered by the initiator chosen. This takes place exactly as in case b). If the server is not registered before either the `search_initiator_time_out` or the `time_out_not_addressed` timer expires, it returns to the NEW and UNLOCKED state. All timers are stopped.

In the REGISTERED state, the server may receive frames addressed to it and respond to them. The `time_out_not_addressed` timer is restarted with each frame addressed to the server.

The server may also move from the REGISTERED and UNLOCKED state to the REGISTERED and LOCKED state and vice versa by writing the value of the `synchronization_locked` variable.

The server may leave the REGISTERED state either:

- by the expiration of the `time_out_not_addressed` timeout; or
- by writing the `reset_new_not_synchronized` variable.

In the first case, the server becomes “FORGOTTEN”: it loses its MAC address and its active initiator: the `mac_address`, the `initiator_mac_address` and the `active_initiator` variables are all reset. The server returns to the NEW and UNLOCKED state.

In the second case, the server checks first the value of the `client_mac_address` submitted as a parameter of the `reset_new_not_synchronized` request:

- if the value is not equal to a valid client address, or the pre-defined NO-BODY address, the writing is refused;
- if the value is NO-BODY, it has the same effect as the expiration of the `time_out_not_addressed` timer: the server returns to the NEW and UNLOCKED state;
- if the value is a valid client address, then the value of the `synchronization_locked` variable is checked:
 - if it is FALSE – the server is in the REGISTERED and UNLOCKED state – the writing is refused;
 - if it is TRUE – the server is in the REGISTERED and LOCKED state – the `(client_)mac_address` element of the active initiator variable is set to the value submitted, the `system_title` and the `L-SAP_selector` elements are reset to 0. The `initiator_mac_address` variable is also set to the value submitted. The `time_out_not_addressed` timer is stopped. The server returns to the NEW and LOCKED state, where it waits to be registered again by the initiator it has been reset to.

When the server leaves the REGISTERED state, all AAs are aborted.

If a power failure occurs, it is managed as follows:

- if the server is in the NEW and UNLOCKED state, it will stay there when the power returns;
- if the server is in the Search Initiator Phase, then it moves back to the NEW and UNLOCKED state when the power returns. The `search_initiator_time_out` timer is stopped and all data concerning the initiators heard so far (signal level and MAC address) are lost;
- if the server is in the NEW and LOCKED state, it will stay there when the power returns. The `search_initiator_time_out` and the `time_out_not_addressed` timers are restarted;
- if the server is in the REGISTERED (LOCKED or UNLOCKED) state, it will stay there when the power returns. The `time_out_not_addressed` timer is restarted. The Application Associations open before the power failure are locally re-established.

10.9 Abstract and transfer syntax

As specified in IEC 61334-4-511:2000, 7.3.1, the CIASE uses the ASN.1 abstract syntax. See also Clause 14. The transfer syntax is A-XDR.

11 Addressing

11.1 General

In the DLMS/COSEM S-FSK PLC profile, two levels of addresses are defined:

- at the MAC sublayer that processes MAC addresses to access an LLC entity;
- at the LLC sublayer that processes LLC addresses to access application entities.

11.2 IEC 61334-5-1 MAC addresses

A physical client or server – initiator or responder – system may be accessed using a MAC address specific to the system or by using one of the group MAC addresses (see Table 6).

Table 6 – MAC addresses

Address	Value	Reference
NO-BODY	000	IEC 61334-4-1:1996 4.3.2.6, IEC 61334-5-1:2001 4.3.7.5.1
Local MAC	001...FIMA-1	IEC 61334-4-1 :1996 4.3.2.5
Initiator	FIMA...LIMA	IEC 61334-4-1:1996 4.3.2.4
MAC group address	LIMA + 1...FFB	
All-configured	FFC	IEC 61334-4-1:1996 4.3.2.1, IEC 61334-5-1:2001 4.3.7.5.2
NEW	FFE	IEC 61334-4-1:1996 4.3.2.2, IEC 61334-5-1:2001 4.2.3.2
All Physical	FFF	IEC 61334-4-1:1996 4.3.2.3, IEC 61334-5-1:2001 4.3.7.5.3
NOTE MAC addresses are expressed on 12 bits. FIMA = First initiator MAC address; C00 LIMA = Last initiator MAC address; DFF		

11.3 Reserved special LLC addresses

NOTE Subclause 11.3 is based on IEC 61334-4-1:1996, 4.4.

11.3.1 General

Each application process within the physical device is bound to a data link layer address that consists of the doublet {MAC-address, L-SAP}. The following LLC addresses (L-SAPs) are specified:

- All-L-SAP: designates the group consisting of all L-SAPs actively serviced by the underlying MAC layer (with its specified MAC address);
- system management L-SAP (M-L-SAP): there is only one M-L-SAP in a physical system;
- initiator L-SAPs (I-L-SAP): These are defined in a specific range;
- individual LLC addresses: These are defined in a specific range;
- CIASE L-SAP (C-L-SAP).

11.3.2 Reserved addresses for the IEC 61334-4-32 LLC sublayer

The reserved LLC addresses for the IEC 61334-4-32 LLC sublayer on the client side and the server side are shown in Table 7 and

Table 8 respectively.

Table 7 – Reserved IEC 61334-4-32 LLC addresses on the client side

Address	L-SAP	Meaning
0x00		No-station
0x01	M-L-SAP I-L-SAP	Client management process. The CIASE is also bound to this address.
0x10		Public client (lowest security level)

Table 8 – Reserved IEC 61334-4-32 LLC addresses on the server side

Address	L-SAP	Meaning
0x00	I-L-SAP	CIASE
0x01	M-L-SAP	Management logical device
0x02...0x0F		Reserved for future use
0xFF	All-L-SAP	All-station (Broadcast)

11.3.3 Reserved addresses for the HDLC based LLC sublayer

The reserved LLC addresses for the HDLC based LLC sublayer on the client side and the server side are shown in Table 9 and

Table 10 respectively.

Table 9 – Reserved HDLC based LLC addresses on the client side

Address	L-SAP	Meaning
0x00		No-station
0x01	M-L-SAP I-L-SAP	Client management process. The CIASE is also bound to this address.
0x10		Public client

Table 10 – Reserved HDLC based LLC addresses on the server side

One byte address	Two bytes address	Meaning
0x00	0x0000	No-Station. The CIASE is also bound to this address.
0x01	0x0001	Management logical device
0x02...0x0F	0x0002...0x000F	Reserved for future use
0x7E	0x3FFE	Calling physical address, not used in the PLC S-FSK HDLC based profile.
0x7F	0x3FFF	All-station (Broadcast)

11.3.4 Source and destination APs and addresses of CI-PDUs

The Source and destination APs and addresses of CI-PDU requests are shown in Table 11.

Table 11 – Source and Destination APs and addresses of CI-PDUs

CI-PDU	Source AP	Destination AP	MAC SA	MAC DA	D-L-SAP	S-L-SAP
Discover	Initiator	AIISMAE	Initiator	FFF All-Physical	0x00 CIASE	0x01 CIASE ^a
DiscoverReport	Manager	AIISMAE	NEW FFE ^b or individual server MAC	FFF ^c All-Physical or Initiator	0xFD	0x00 CIASE
Register	Initiator	AIISMAE	Initiator	FFF All-Physical	0x00 CIASE	0x01 CIASE ^d
PingRequest	Initiator	Individual	Initiator	Individual	0x00 CIASE	0x01 CIASE ^d
PingResponse	Individual	Initiator	Individual	Initiator	0x01 CIASE ^d	0x00 CIASE
RepeaterCall	Initiator	AIISMAE	Initiator	FFF All-Physical	0x00 CIASE	0x01 CIASE ^d
ClearAlarm	Initiator	AIISMAE	Initiator	FFF All-Physical	0x00 CIASE	0x01 CIASE ^d
NOTE 1 In the MAC frame, the order of the addresses is Source Address – Destination Address.						
NOTE 2 In the IEC 61334-4-32 LLC frame, the order of the addresses is Destination Address – Source Address.						
NOTE 3 In the HDLC frame, the order of the addresses is Destination Address – Source Address.						
^a Could be a different value.						
^b FFE if the server is in the NEW state. Individual MAC address if the server is in ALARM state.						
^c If the reporting system list feature is used, then the Destination Address is All-Physical. Otherwise, it is the Initiator address.						
^d Could be a different value, but shall be the same as in the Discover CI-PDU.						

12 Specific considerations / constraints for the IEC 61334-4-32 LLC sublayer based profile

12.1 Establishing application associations

AAs can only be established with server systems properly registered by the initiator. The MSC for the discovery and registration process is shown in Figure 6.

NOTE In the following examples, the NNAP acts as a COSEM client.

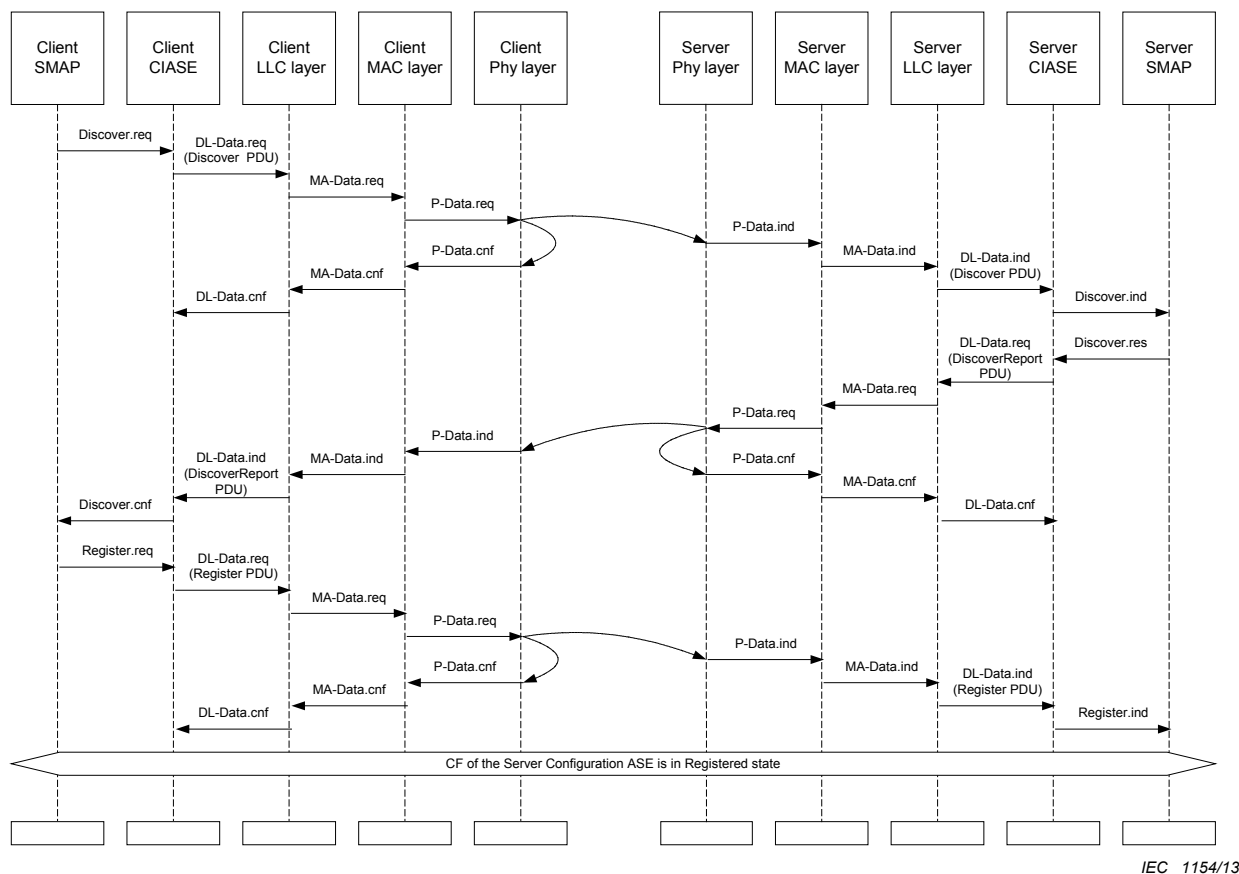


Figure 6 – MSC for the discovery and registration process

The MSC for the establishment of a confirmed AA establishment is shown in Figure 7.

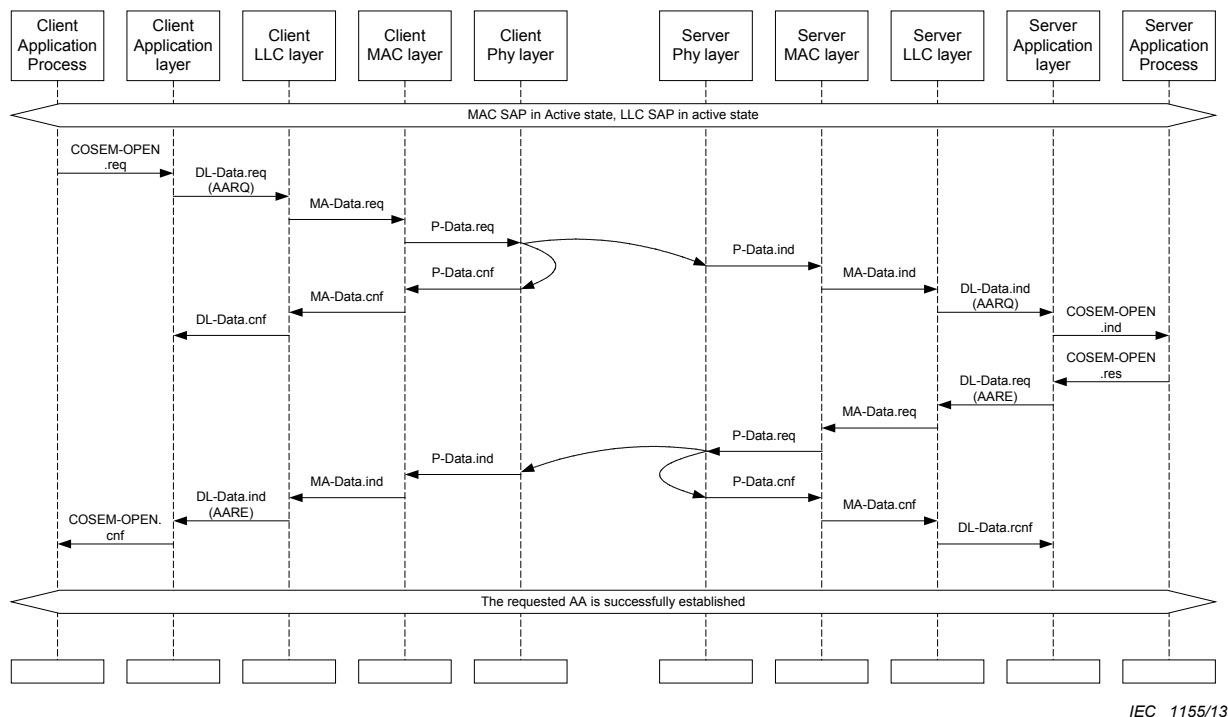


Figure 7 – MSC for successful confirmed AA establishment

12.2 Application association types, confirmed and unconfirmed xDLMS services

Table 12 shows the rules for establishing confirmed and unconfirmed AAs. In this table, grey areas represent cases, which are out of the normal operating conditions: either not allowed or have no useful purpose. According to this:

It is not allowed to request an xDLMS service in a confirmed way (Service_Class = Confirmed) within an unconfirmed AA. This is prevented by the Client AL. Servers receiving such APDUs shall simply discard them, or shall send back a ConfirmedServiceError APDU or – if the feature is implemented – send back the optional ExceptionResponse APDU.

In this profile, the Service_Class parameter of the COSEM-OPEN service is linked to the response-allowed parameter of the xDLMS InitiateRequest APDU. If the COSEM-OPEN service is invoked with Service_Class == Confirmed, the response-allowed parameter shall be set to TRUE. The server is expected to respond. If it is invoked with Service_Class == Unconfirmed, the response-allowed parameter shall be set to FALSE. The server shall not send back a response.

The Service_Class parameter of the GET, SET and ACTION services is linked to the service-class bit of the Invoke-Id-And-Priority byte. If the service is invoked with Service_Class = Confirmed, the service-class bit shall be set to 1, otherwise it shall be set to 0.

Table 12 – Application associations and data exchange in the S-FSK PLC profile using the connectionless LLC sublayer

Application association establishment				Data exchange	
Protocol connection parameters	COSEM-OPEN service class	Use	Type of established AA	Service class	Use
Id: LLC addresses, MAC addresses	Confirmed	Exchange AARQ/AARE APDU-s transported by DL-Data services	Confirmed	Confirmed	DL-Data services
				Unconfirmed	DL-Data services
	Unconfirmed	Send AARQ transported by DL-Data services	Unconfirmed	Confirmed (not allowed)	–
				Unconfirmed	DL-Data services

12.3 xDLMS client/server type services

No specific features / constraints apply related to the use of client/server type services.

The MSC is essentially the same as for establishing confirmed AAs, except that instead of the COSEM-OPEN service primitives, the appropriate xDLMS service primitives are used.

12.4 Releasing application associations

As the LLC sublayer supporting the COSEM Application layer is connectionless, the COSEM-Release service may be invoked with the Use_RLRQ_RLRE option = TRUE to release an AA.

To secure the RLRQ APDU against denial-of-service attacks – executed by unauthorized releasing of the AA – the user-information field of the RLRQ APDU may contain the xDLMS InitiateRequest APDU, authenticated and encrypted using the AES-GCM-128 algorithm, the global unicast encryption key and the authentication key (the same as in the AARQ APDU).

The MSC for releasing an AA is shown in Figure 8.