

PUBLICLY AVAILABLE SPECIFICATION

PRE-STANDARD



Industrial networks – Wireless communication network and communication profiles – WIA-FA

Withdrawn



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2015 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.

IEC Central Office
3, rue de Varembe
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.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

The advanced search enables 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 It also gives information on projects, replaced and withdrawn publications.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 online 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 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

More than 60 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC 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.

PUBLICLY AVAILABLE SPECIFICATION

PRE-STANDARD



Industrial networks – Wireless communication network and communication profiles – WIA-FA

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40; 35.100.01

ISBN 978-2-8322-2477-9

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD.....	12
1 Scope.....	14
2 Normative references	14
3 Terms, definitions, abbreviations, and conventions	14
3.1 Terms and definitions.....	14
3.2 Abbreviations.....	17
3.3 Conventions.....	19
4 Data coding	20
4.1 Overview.....	20
4.2 Basic data type coding.....	21
4.2.1 Integer coding.....	21
4.2.2 Unsigned coding.....	21
4.2.3 Float coding.....	22
4.2.4 Octetstring coding	23
4.2.5 Bit Field coding.....	23
4.2.6 TimeData coding	23
4.2.7 KeyData coding	23
4.3 Structured data type coding	24
4.3.1 Structure type coding.....	24
4.3.2 List type coding	24
5 WIA-FA overview	24
5.1 Device types.....	24
5.1.1 Host computer.....	24
5.1.2 Gateway device.....	24
5.1.3 Access device	24
5.1.4 Field device.....	25
5.1.5 Handheld device.....	25
5.2 Network topology.....	25
5.3 Protocol architecture.....	26
6 System management	28
6.1 Overview.....	28
6.2 Device Management Application Process.....	28
6.2.1 Network manager	31
6.2.2 Security manager	31
6.2.3 Network management module.....	31
6.2.4 Security management module.....	31
6.2.5 DMAP state machines	31
6.3 Addressing and address assignment.....	42
6.4 Communication resource allocation.....	42
6.4.1 General	42
6.4.2 Communication resource allocation	43
6.5 Joining and leave process of field device	44
6.5.1 Joining process of a field device	44
6.5.2 Communication resource allocation to field device.....	45
6.5.3 Leaving process of a field device	45
6.6 Network performance monitoring.....	46

6.6.1	Device status report.....	46
6.6.2	Channel condition report.....	47
6.7	Management information base and services.....	47
6.7.1	Management information base.....	47
6.7.2	MIB services.....	57
7	Physical layer.....	61
7.1	General.....	61
7.2	General requirements based on IEEE STD 802.11-2012.....	61
7.3	Additional requirements.....	62
7.3.1	General.....	62
7.3.2	Frequency band.....	62
7.3.3	Channel bitmap.....	62
7.3.4	Transmission power.....	63
7.3.5	Data rate.....	63
8	Data Link Layer.....	64
8.1	General.....	64
8.1.1	Protocol architecture.....	64
8.1.2	WIA-FA superframe.....	64
8.1.3	Communication based on multiple access devices.....	67
8.1.4	Time synchronization.....	68
8.1.5	Aggregation/Disaggregation.....	69
8.1.6	Retransmission.....	70
8.2	Data link sub-layer data services.....	73
8.2.1	General.....	73
8.2.2	DLDE-DATA request primitive.....	73
8.2.3	DLDE-DATA indication primitive.....	74
8.2.4	Time sequence of DLL data service.....	75
8.3	Data link sub-layer management services.....	76
8.3.1	General.....	76
8.3.2	Network discovery services.....	76
8.3.3	Time synchronization services.....	78
8.3.4	Device joining services.....	80
8.3.5	Device status report services.....	83
8.3.6	Channel condition report services.....	85
8.3.7	Remote attribute get services.....	86
8.3.8	Remote attribute configuration services.....	90
8.3.9	Device leaving services.....	93
8.4	DLL frame formats.....	94
8.4.1	General frame format.....	94
8.4.2	Data frame format.....	96
8.4.3	Aggregation frame format.....	96
8.4.4	NACK frame format.....	97
8.4.5	GACK frame format.....	97
8.4.6	Beacon frame format.....	97
8.4.7	Join request frame format.....	98
8.4.8	Join response frame format.....	98
8.4.9	Leave request frame format.....	98
8.4.10	Device status report frame format.....	99
8.4.11	Channel condition report frame format.....	99

8.4.12	Time synchronization request frame format	99
8.4.13	Time synchronization response frame format	99
8.4.14	Remote attribute get request frame format	100
8.4.15	Remote attribute get response frame format	100
8.4.16	Remote attribute set request frame format	101
8.4.17	Remote attribute set response frame format	101
8.5	Data link layer state machines	101
8.5.1	DLL state machine of access field	101
8.5.2	DLL state machine of field device	105
8.5.3	Functions used in DLL state transitions	110
9	Wired specifications between GW and AD	111
9.1	Overview	111
9.2	Join process of access device	111
9.3	Frame formats between GW and AD	111
10	Application Layer	113
10.1	Overview	113
10.2	AL protocol stack	114
10.3	AL functions	114
10.3.1	Data function	114
10.3.2	Management function	114
10.3.3	Communication mode	115
10.4	Application data	115
10.4.1	General	115
10.4.2	Process data	116
10.4.3	Event data	117
10.5	User application process	118
10.5.1	General	118
10.5.2	User application object	119
10.5.3	IO data images on gateway device	119
10.5.4	Alarm mechanism	120
10.5.5	Application configuration process	120
10.6	Application services	126
10.6.1	Confirmed services and unconfirmed services	126
10.6.2	READ service	127
10.6.3	WRITE service	128
10.6.4	PUBLISH Service	129
10.6.5	REPORT Service	130
10.6.6	REPORT ACK	131
10.7	Application sublayer	132
10.7.1	Overview	132
10.7.2	ASL data service	132
10.7.3	ASL packet format	135
11	Security	155
11.1	General	155
11.1.1	Security management architecture	155
11.1.2	Security functions	156
11.1.3	Keys	156
11.2	Security services	157
11.2.1	General	157

11.2.2	Key establish service	158
11.2.3	Key update service	160
11.2.4	Security alarm service	162
11.3	Secure join	164
11.3.1	General	164
11.3.2	Secure join process of FD	164
11.4	Key management	165
11.4.1	General	165
11.4.2	Key establish process	165
11.4.3	Key update process	166
11.5	DLL secure communication	168
11.6	Security alarm	169
11.7	Secure frame format	169
11.7.1	General secure DLL frame format	169
11.7.2	Secure aggregation frame format	171
11.7.3	Key establish request frame format	172
11.7.4	Key establish response frame format	172
11.7.5	Key update request frame format	172
11.7.6	Key update response frame format	173
11.7.7	Security alarm request frame format	173
Annex A (informative)	Security strategy for WIA-FA network	174
A.1	Risk analysis for WIA-FA network	174
A.2	Security principles for WIA-FA network	174
A.3	Security objectives for WIA-FA network	174
A.4	Security grade of WIA-FA network	175
Annex B (informative)	Regional modification for compliance with ETSI standards	176
B.1	General	176
B.2	Compliance with ETSI EN 300 440-2 V1.4.1	176
B.3	Compliance with ETSI EN 300 328 V1.8.1	176
Bibliography		180
Figure 1	– Conventions used for state machines	19
Figure 2	– Integer coding	21
Figure 3	– Unsigned coding	21
Figure 4	– Single float coding	22
Figure 5	– Double float coding	22
Figure 6	– WIA-FA enhanced star topology	25
Figure 7	– OSI basic reference model mapped to WIA-FA	26
Figure 8	– Protocol architecture of WIA-FA	27
Figure 9	– Data flow over WIA-FA network	27
Figure 10	– System management scheme	28
Figure 11	– DMAP of management system	29
Figure 12	– DMAP state machine of gateway device	32
Figure 13	– DMAP state machine of gateway device for each field device	33
Figure 14	– DMAP state machine of a field device	37
Figure 15	– Long address structure of device	42

Figure 16 – Joining process of field device	44
Figure 17 – Communication resource allocation process for a field device	45
Figure 18 – Passive leave process of a field device	46
Figure 19 – Device status report process of field device	46
Figure 20 – Channel condition report process of field device	47
Figure 21 – BitMap format.....	62
Figure 22 – WIA-FA DLL protocol architecture	64
Figure 23 – The template of timeslot structure	65
Figure 24 – WIA-FA default superframe	66
Figure 25 – WIA-FA superframe.....	66
Figure 26 – The example of WIA-FA devices multi-channel communication.....	66
Figure 27 – An example of beacon communication based on multiple ADs.....	67
Figure 28 – Process of one-way time synchronization	68
Figure 29 – Process of two-way time synchronization	69
Figure 30 – Aggregation frame payload format.....	70
Figure 31 – Example of retransmission mode based on NACK.....	71
Figure 32 – Example of multi-unicast retransmission mode.....	72
Figure 33 – Example of multi-broadcast retransmission mode.....	72
Figure 34 – Example of GACK-based timeslot backoff mode.....	73
Figure 35 – Time sequence of period data service from FD to GW	75
Figure 36 – Time sequence of other data service from FD to GW	75
Figure 37 – Time sequence of data service from GW to FD.....	76
Figure 38 – Network discovery process.....	78
Figure 39 – Time synchronization process.....	80
Figure 40 – Device join process	83
Figure 41 – Device status report process	84
Figure 42 – Channel condition report process	86
Figure 43 – Remote attribute get process	89
Figure 44 – Remote attribute set process.....	93
Figure 45 – Device leave process	94
Figure 46 – General frame format	95
Figure 47 – DLL frame header	95
Figure 48 – DLL frame control format.....	95
Figure 49 – DLL Data frame format.....	96
Figure 50 – DLL Aggregation frame format	97
Figure 51 – NACK frame format.....	97
Figure 52 – GACK frame format.....	97
Figure 53 – GACK information	97
Figure 54 – DLL Beacon frame format.....	97
Figure 55 – Shared timeslot count	98
Figure 56 – DLL join request frame format	98
Figure 57 – DLL join request frame format	98
Figure 58 – DLL leave request frame format	99

Figure 59 – DLL Device status report frame format	99
Figure 60 – DLL Channel condition report frame format	99
Figure 61 – DLL time synchronization request frame format	99
Figure 62 – DLL time synchronization response frame format	99
Figure 63 – DLL Remote attribute get request frame format	100
Figure 64 – DLL remote attribute get response frame format	100
Figure 65 – DLL Remote attribute set request frame format	101
Figure 66 – DLL remote attribute set response frame format	101
Figure 67 – DLL state machine of access device	102
Figure 68 – DLL state machine of field device	106
Figure 69 – General frame format between GW and AD	111
Figure 70 – AL portions within WIA-FA protocol stack	114
Figure 71 – The relationships between UAPs and DAPs	118
Figure 72 – User application objects	119
Figure 73 – Implementation example of IO data images on the gateway device	120
Figure 74 – C/S VCR relationships between GW and FDs	122
Figure 75 – P/S VCR relationships between GW and FDs	123
Figure 76 – P/S VCR relationships between FDs and GW	123
Figure 77 – R/S VCR relationships between FDs and GW	124
Figure 78 – Configuration process for a field device	125
Figure 79 – UAO aggregation and disaggregation process	126
Figure 80 – READ request message format	127
Figure 81 – READ response(+) message format	127
Figure 82 – READ response(-) message format	127
Figure 83 – READ Service process	128
Figure 84 – WRITE request message format	128
Figure 85 – WRITE response(-) message format	128
Figure 86 – WRITE Service process	129
Figure 87 – PUBLISH request message format	129
Figure 88 – PUBLISH Procedure from Field Device to Gateway Device	130
Figure 89 – PUBLISH Procedure from Gateway Device to Field Device	130
Figure 90 – REPORT request message format	130
Figure 91 – REPORT Service process	131
Figure 92 – REPORT ACK request message format	131
Figure 93 – REPORT ACK response(+) message format	131
Figure 94 – REPORT ACK response(-) message format	131
Figure 95 – REPORT ACK Service process	132
Figure 96 – ASL general packet format	135
Figure 97 – Format of packet control field	135
Figure 98 – Confirmed service primitives exchanged between layers	137
Figure 99 – Unconfirmed service primitives exchanged between layers	138
Figure 100 – Primitives invoking for read/ write MIB between layers	139
Figure 101 – State transition diagram of AMCL	140

Figure 102 – State transition diagram of AMSV	142
Figure 103 – State transition diagram of AMPB	146
Figure 104 – State transition diagram of AMSB	149
Figure 105 – State transition diagram of AMRS	152
Figure 106 – State transition diagram of AMRK	152
Figure 107 – Security management architecture	155
Figure 108 – Life cycle of keys	157
Figure 109 – Format of NONCE	158
Figure 110 – Time sequence of key establishment	160
Figure 111 – Time sequence of key updating	162
Figure 112 – SecAlarmt_Struct structure	163
Figure 113 – Time sequence of security alarm	163
Figure 114 – Secure join process of field device	165
Figure 115 – Key establish process for field device	166
Figure 116 – Key update state machine for FD	167
Figure 117 – General secure DLL frame format	170
Figure 118 – Secure aggregation frame format	171
Figure 119 – Key establish request frame format	172
Figure 120 – Key establish response frame format	172
Figure 121 – Key update request frame format	172
Figure 122 – Key update response frame format	173
Figure 123 – Security alarm request frame format	173
Figure B.1 – Timeslot timing template	177
Table 1 – Conventions used for state transitions	20
Table 2 – Definition of integer data type	21
Table 3 – Unsigned16 coding	21
Table 4 – Octetstring coding	23
Table 5 – Coding of Bit Field data with one octet	23
Table 6 – Coding of Bit Field data with two octets	23
Table 7 – Coding of Bit Field data with three octet	23
Table 8 – Network management functions	30
Table 9 – Security management functions	30
Table 10 – DMAP state transition of gateway device	32
Table 11 – DMAP state transition of gateway device for each field device	34
Table 12 – DMAP state transition of a field device	38
Table 13 – Functions used in DMAP state transition	41
Table 14 – Unstructured attributes	48
Table 15 – Structured attributes	50
Table 16 – Superframe_Struct structure	50
Table 17 – Link_Struct structure	51
Table 18 – ChanCon_Struct structure	51
Table 19 – Device_Struct	52

Table 20 – Key_Struct structure	53
Table 21 – VcrEP_Struct definition	54
Table 22 – UAOCClassDesc_Struct definition	55
Table 23 – ProDataDesc_Struct definition	56
Table 24 – UAOInstDesc_Struct definition	57
Table 25 – DMAP-MIB-GET.request parameters	58
Table 26 – DMAP-MIB-GET.confirm parameters	59
Table 27 – DMAP-MIB-SET.request parameters	60
Table 28 – DMAP-MIB-SET.confirm parameters	60
Table 29 – PHY protocol selection	61
Table 30 – Coding of Modulation modes	62
Table 31 – Channel indices	63
Table 32 – Data rate	63
Table 33 – Parameters of timeslot template	65
Table 34 – DLDE-DATA.request primitive parameters	74
Table 35 – DLDE-DATA.indication primitive parameters	74
Table 36 – Management services	76
Table 37 – DLME-DISCOVERY.request parameters	77
Table 38 – DLME-DISCOVERY.confirm parameters	77
Table 39 – BeaconDescription_Struct parameters	77
Table 40 – DLME-TIME-SYN.indication parameters	78
Table 41 – DLME-TIME-SYN.response parameters	79
Table 42 – DLME-TIME-SYN.confirm parameters	79
Table 43 – DLME-JOIN.request parameters	81
Table 44 – DLME-JOIN.indication parameters	81
Table 45 – DLME-JOIN.response parameters	82
Table 46 – DLME-JOIN.confirm parameters	82
Table 47 – DLME-DEVICE-STATUS.request parameters	83
Table 48 – DLME-DEVICE-STATUS.indication parameters	84
Table 49 – DLME-DEVICE-STATUS.confirm parameters	84
Table 50 – DLME-CHANNEL-CONDITION.request parameters	85
Table 51 – DLME-CHANNEL-CONDITION.indication parameters	85
Table 52 – DLME-CHANNEL-CONDITION.confirm parameters	86
Table 53 – DLME-INFO-GET.request parameters	87
Table 54 – DLME-INFO-GET.indication parameters	87
Table 55 – DLME-INFO-GET.response parameters	88
Table 56 – DLME-INFO-GET.confirm parameters	89
Table 57 – DLME-INFO-SET.request parameters	90
Table 58 – DLME-INFO-SET.Indication parameters	91
Table 59 – DLME-INFO-SET response parameters	92
Table 60 – DLME-INFO-SET.confirm parameters	92
Table 61 – DLME-LEAVE.request parameters	93
Table 62 – DLME-LEAVE.confirm parameters	94

Table 63 – Frame type coding.....	96
Table 64 – Addressing mode subfields.....	96
Table 65 – DLL state transition of access device	103
Table 66 – DLL state transition of field device.....	107
Table 67 – Functions used in DMAP state transition	110
Table 68 – Wired services between GW and AD	112
Table 69 – Service parameters of AD join request.....	113
Table 70 – Service parameters of AD join response	113
Table 71 – Service parameters of GW requesting AD to send GACK.....	113
Table 72 – Parameters of GACKInfo_Struct structure	113
Table 73 – Service parameters of GW requesting AD to send NACK.....	113
Table 74 – Communication models between gateway device and field devices	115
Table 75 – SingleAnalogData definition.....	116
Table 76 – DoubleAnalogData definition	116
Table 77 – DigitalData8 definition	116
Table 78 – DigitalData16 definition	117
Table 79 – DigitalData32 definition	117
Table 80 – EventData Definition.....	117
Table 81 – UAO events definitions	118
Table 82 – VCR attribute configuration overview.....	121
Table 83 – Application services supported by UAPs.....	126
Table 84 – Error code definition for READ response(-) message.....	127
Table 85 – Error code definition for WRITE response(-)	129
Table 86 – Error code definition for REPORT ACK negative response	132
Table 87 – ASLDE-DATA.request primitive parameter definitions.....	133
Table 88 – ASLDE-DATA.indication primitive parameter definitions	133
Table 89 – ASLDE-DATA.response primitive parameter definition.....	134
Table 90 – ASLDE-DATA.confirmPrimitive Parameters	135
Table 91 – Service Identifier subfield definition.....	135
Table 92 – Message Type subfield definition.....	136
Table 93 –Confirmed service primitives exchanged between ASL and other layers	137
Table 94 – Unconfirmed service primitives exchanged between ASL and other layers.....	138
Table 95 – Primitives for read/ write MIB between layers	139
Table 96 – State transition table of AMCL	140
Table 97 – State transition table of AMSV	142
Table 98 – State transition table of AMPB.....	146
Table 99 – State transition table of AMSB.....	149
Table 100 – State transition table of AMRS.....	152
Table 101 – State transition table of AMRK.....	153
Table 102 – All Functions in ASLM	154
Table 103 – Parameters for KEY-ESTABLISH.request	158
Table 104 – KeyMaterial_Struct structure	158
Table 105 – Parameters for KEY-ESTABLISH.indication.....	159

Table 106 – Parameters for KEY-ESTABLISH.response	159
Table 107 – Parameters for KEY-ESTABLISH.confirm	160
Table 108 – Parameters for KEY-UPDATE.request	160
Table 109 – Parameters for KEY-UPDATE.indication	161
Table 110 – Parameters for KEY-UPDATE.response	161
Table 111 – Parameters for KEY-UPDATE.confirm	162
Table 112 – Parameters for SEC-ALARM.request	162
Table 113 – Parameters for SEC-ALARM.indication	163
Table 114 – Key update states	166
Table 115 – Key update state transition	168
Table 116 – Keys used in DLL secure communication	169
Table 117 – Available security levels for DLL	171
Table A.1 – Security grades for WIA-FA network	175
Table B.1 – Applicable EN 300 440-2 requirements list	176
Table B.2 – Applicable EN 300 328 requirements list	177
Table B.3 – Timeslot timing definitions and calculations	178
Table B.4 – TxMaxPHYPacket of FHSS	178
Table B.5 – TxMaxPHYPacket of DSSS/HR-DSSS	179
Table B.6 – TxMaxMPDU of OFDM	179

Withhold

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL NETWORKS – WIRELESS COMMUNICATION NETWORK AND COMMUNICATION PROFILES – WIA-FA

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.

A PAS is a technical specification not fulfilling the requirements for a standard, but made available to the public.

IEC PAS 62948 has been processed by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this PAS is based on the following document:

This PAS was approved for publication by the P-members of the committee concerned as indicated in the following document

Draft PAS	Report on voting
65C/784/PAS	65C/789/RVD

Following publication of this PAS, which is a pre-standard publication, the technical committee or subcommittee concerned may transform it into an International Standard.

This PAS shall remain valid for an initial maximum period of 3 years starting from the publication date. The validity may be extended for a single period up to a maximum of 3 years, at the end of which it shall be published as another type of normative document, or shall be withdrawn.

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

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.

Withdrawn

INDUSTRIAL NETWORKS – WIRELESS COMMUNICATION NETWORK AND COMMUNICATION PROFILES – WIA-FA

1 Scope

This PAS specifies the system architecture and communication protocol of WIA-FA (Wireless Networks for Industrial Automation – Factory Automation) based on IEEE STD 802.11-2012 Physical Layer (PHY).

This PAS applies to wireless network systems for factory automation measuring, monitoring and control.

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 61588, *Precision clock synchronization protocol for networked measurement and control systems*

IEC 61499, *The industrial process measurement and control system function blocks*

ISO/IEC 7498-1, *Information Technology – Open Systems Interconnection – Basic Reference Model – The Basic model*

IEEE STD 802.11-2012, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*

3 Terms, definitions, abbreviations, and conventions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1

absolute timeslot number

number of timeslots from the start of the network, generally denoting the current timeslot

Note 1 to entry: The value is incremented by one, usually the same with the current timeslot sequence number. Once the maximum value ($2^{48}-1$) is reached, the value is reset to 0.

3.1.2

access device

device installed in the field, which is responsible for forwarding the sensor data, alarm and network management related information of the field device to the gateway device, or forwarding control signals, management information and configuration information of the gateway device to field devices

3.1.3**aggregation**

process of aggregating data from multiple user application objects into one packet, or aggregating several frames into one frame

3.1.4**application configuration**

configuration process for user application processes in field devices to finish certain jobs during the application of factory automation

3.1.5**application sublayer**

protocol sublayer that provides data and management services for the application layer

3.1.6**backoff**

process of retrying a frame in pre-determined retransmission timeslots if the first transmission is failed

3.1.7**beacon**

special frame broadcast by the access device in the WIA-FA network

Note 1 to entry: To join the WIA-FA network, a new field device should first listen to beacons.

3.1.8**channel**

RF medium used to convey a frame from a sender to a receiver

3.1.9**coexistence**

state in which all wireless communication solutions of a plant using shared medium fulfil all their application communication requirements

[SOURCE: IEC 62657-2:2013, 3.1.12]

3.1.10**communication resource**

channels and timeslots used to transport a frame

3.1.11**disaggregation**

process of dividing the aggregated packet into data of multiple user application objects, or dividing the aggregated frame into multiple frames

3.1.12**field device**

device installed in industrial field and connected by sensors and actuators, which is used for transmitting field data and receiving control commands

3.1.13**gateway device**

device that connects the WIA-FA network to other plant networks

3.1.14**handheld device**

portable device used for network provisioning and firmware updating

3.1.15

heartbeat message

signal sent by the working gateway device to the redundant ones, which indicates that the gateway device is working properly

3.1.16

host computer

computer through which operation, maintenance and management personnel interact with the WIA-FA network

Note 1 to entry: Host computer performs functions of configuration, provisioning, and data display.

3.1.17

interoperability

ability of two or more network systems to exchange information and to make mutual use of the information that has been exchanged

[SOURCE: ISO/IEC TR 10000-1:1998, 3.2.1 – modified by replacing “IT systems” with “network systems”]

3.1.18

joining

process in which a WIA-FA device is authenticated and allowed to participate in the WIA-FA network

3.1.19

link

interconnecting path between two neighbouring devices, which consists of a set of parameters

Note 1 to entry: A set of parameters include link identifier, link type, destination address, relative timeslot number, current channel index, and superframe identifier.

Note 2 to entry: A WIA-FA network has only one primary gateway device.

3.1.20

network address

8-bit or 16-bit unsigned integer uniquely identifying the device in the WIA-FA network

Note 1 to entry: It is also called short address.

3.1.21

network configuration

process of configuring parameters for WIA-FA devices to maintain network operation and communication

3.1.22

network manager

logical role responsible for configuring the network, allocating communication resources, monitoring and reporting network performances

Note 1 to entry: There is only one network manager in a WIA-FA network.

3.1.23

passive leaving

process in which an online field device is instructed by the gateway device to leave the WIA-FA network

3.1.24

physical address

EUI-64 bits uniquely identifying the device in the WIA-FA network

Note 1 to entry: : It is also called long address.

Note 2 to entry: : A physical address is assigned by a manufacturer.

3.1.25

primary gateway device

gateway device working in a WIA-FA network

3.1.26

provisioning

process of pre-configuring some static information that includes network identifier, security level, join key, and shared key

3.1.27

redundant gateway device

hot backup of the primary gateway device

3.1.28

relative timeslot number

timeslot number counted from the start of a superframe

3.1.29

security manager

logical role responsible for configuring the security policies of the whole network, managing keys, and authenticating devices

3.1.30

superframe

collection of channels and timeslots repeatedly appear in one cycle

Note 1 to entry: It specifies the transmitting or receiving time for periodic communication.

3.1.31

timeslot

basic time unit used for data exchange in WIA-FA network

Note 1 to entry: Its duration is configurable in the WIA-FA network.

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

ACK	Acknowledgement
AI	Analog Input
AD	Access Device
AL	Application Layer
ASLDE	Application SubLayer Digital Entity
ASLM	ASL State Machine
AMCTL	ASL State Machine of Client
AMSV	ASL State Machine of Server
AMPB	ASL State Machine of Publisher
AMSB	ASL State Machine of Subscriber
AMRS	ASL State Machine of Report Source
AMRK	ASL State Machine of Report Sink

AO	Analog Output
ASL	Application Sub-layer
ASN	Absolute Slot Number
APDU	Application Protocol Data Unit
ASDU	Application Service Data Unit
C/S	Client/Serve
CCM*	Extension of counter with cipher block chaining message authentication code
DI	Digital Input
DO	Digital Output
DGO	DisaGgregation Object
DLL	Data Link Layer
DLPDU	Data link Layer Protocol Data Unit
DMAP	Device Management Application Process
EIRP	Equivalent Isotropic Radiated Power
ENC	ENCryption
FCS	Frame Check Sequence
FD	Field Device
FDMA	Frequency Division Multiple Access
GW	Gateway Device
HC	Host Computer
HD	Handheld Device
HMAC	keyed-Hash Message Authentication Code
ID	Identifier
KED	Data Encryption Key
KEDB	Broadcast Data Encryption Key
KEDU	Unicast Data Encryption Key
KEK	Key Encryption Key
KJ	Join Key
KS	Shared Key
LSB	Least Significant Bit
LQI	Link Quality Indication
MAC	Medium Access Control
MIB	Management Information Base
MIC	Message Integrity Code
MSB	Most Significant Bit
NACK	Negative Acknowledgement
NRT	Non-Real-Time
NONCE	Number used once, a value that has (at most) a negligible chance of repeating
PAGO	Packet Aggregation Object
PDU	Protocol Data Unit

PHY	PHYSical layer
P/S	Publish/Subscriber
R/S	Report/Sink
SAP	Service Access Point
SM	Security Manager
TDMA	Time Division Multiple Access
UAO	User Application Object
UAP	User Application Process
VCR	Virtual Communication Relationship
WIA-FA	Wireless Network for Industrial Automation – Factory Automation

3.3 Conventions

For the purposes of the state machines and state transitions in this PAS, the following conventions apply.

This PAS uses a diagram to represent a state machine. The conventions used in the state machines are shown in Figure 1.

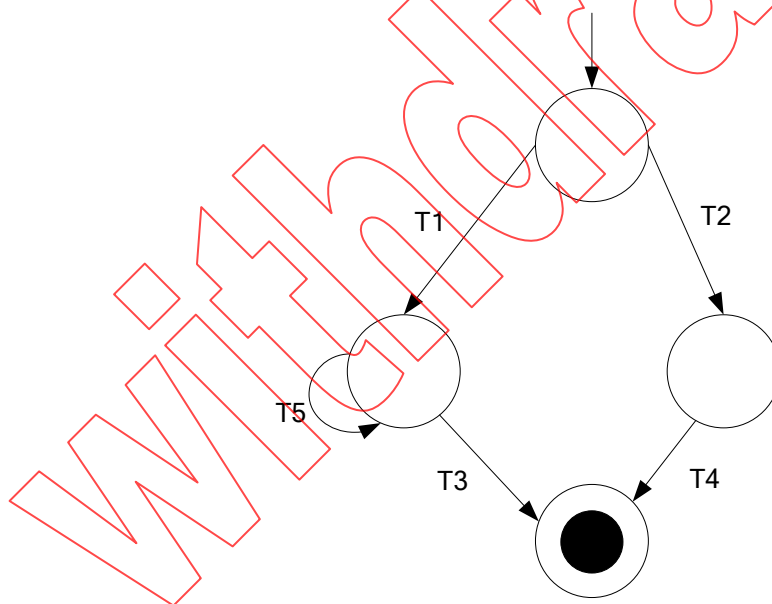


Figure 1 – Conventions used for state machines

The conventions used in the state machines are as follows:

- The labeled circles represent states that a device can be in.
- State transitions are directed lines. They show which state a component leaves and which state it transitions to.
- A transition is labeled by T with the events that caused it and the corresponding actions (this may be empty). The events (above the line) causing the transition is separated from the resulting actions (below the line) by a horizontal line.
- || Logical "OR".

The conventions used in the state transitions are shown in Table 1.

Table 1 – Conventions used for state transitions

#	Current state	Event/conditions =>action	Next state
Name of transition	The current state to which this state transition applies	Events or conditions that trigger this state transaction. => The actions that are taken when the above events or conditions are met. The actions are always indented below events or conditions	The next state after the actions in this transition is taken

The conventions used in the state transitions are as follows:

- = A logical condition to indicate an item on the left is equal to an item on the right.
- := Value of an item on the left is replaced by value of an item on the right. If an item on the right is a parameter, it comes from the primitive shown as an input event.
- == A logical condition to judge an item on the left is equal to an item on the right.
- && Logical "AND".
- || Logical "OR".
- != A logical condition to indicate an item on the left is not equal to an item on the right.

This construct allows the execution of a sequence of actions in a loop within one transition.

The loop is executed for all values from start_value to end_value.

Example:

```
for (Identifier = start_value to end_value)
    actions
end
```

This construct allows the execution of alternative actions depending on some condition (which may be the value of some identifier or the outcome of a previous action) within one transition.

Example:

```
If (condition)
    actions
else
    actions
endif
```

4 Data coding

4.1 Overview

WIA-FA data coding specifies the machine independent syntax for the data conveyed by each layer services. WIA-FA supports the definition and transfer of both basic and struct data types.

Basic types are atomic types that cannot be decomposed into more elemental types. Struct types are types composed of basic types and other struct types. Their complexity and depth of nesting is not constrained by this PAS.

4.2 Basic data type coding

4.2.1 Integer coding

The integer is a signed value, as shown in Figure 2 and Table 2. For this data type, MSB is transmitted first, then the subsequent octets, and finally the LSB.

Notations: Integer8, Integer16, Integer24, Integer32		
Data type	Value range	Length
Integer8	$-128 \leq i \leq 127$	One octet
Integer16	$-32\,768 \leq i \leq 32\,767$	Two octets
Integer24	$-2^{23} \leq i \leq 2^{23} - 1$	Three octets
Integer32	$-2^{31} \leq i \leq 2^{31} - 1$	Four octets
Complement binary notation		
MSB is the bit followed by the first octet (SN)		
SN = 0: positive and 0		
SN = 1: negative		

Figure 2 – Integer coding

Table 2 – Definition of integer data type

octet	bit							
	7	6	5	4	3	2	1	0
1	SN	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^9	2^8
2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

4.2.2 Unsigned coding

The unsigned value is coded as shown in Figure 3 and Table 3. For this data type, MSB is sent first, then the subsequent octets, and finally the LSB.

Notations: Unsigned8, Unsigned16, Unsigned24, Unsigned32, Unsigned40, Unsigned48, Unsigned64, Unsigned80		
Data type	Value range	Length
Unsigned8	$0 \leq i \leq 255$	One octet
Unsigned16	$0 \leq i \leq 65\,535$	Two octets
Unsigned24	$0 \leq i \leq 2^{24} - 1$	Three octets
Unsigned32	$0 \leq i \leq 2^{32} - 1$	Four octets
Unsigned40	$0 \leq i \leq 2^{40} - 1$	Five octets
Unsigned48	$0 \leq i \leq 2^{48} - 1$	Six octets
Unsigned64	$0 \leq i \leq 2^{64} - 1$	Eight octets
Unsigned80	$0 \leq i \leq 2^{80} - 1$	Ten octets

Figure 3 – Unsigned coding

Table 3 – Unsigned16 coding

octet	bit							
	7	6	5	4	3	2	1	0
1	2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^9	2^8
2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

4.2.3 Float coding

The value of floating point is coded as shown in Figure 4 and Figure 5.

The MSB of the sign and the exponent is sent first, and then the remained bits of the exponent and the bits from MSB to LSB of the fraction. If the value of the floating point data is unknown, 0x7F and 0xA0 are firstly sent, followed by 0x00, which means “Not-a-number”.

Notations:	Single Float (four octets)							
Value range	See in IEC 60559, Short Real Number (32 bits)							
coding	See in IEC 60559, Short Real Number (32 bits)							
	MSB Bit 7 6 5 4 3 2 1 0 LSB							
Octet	Exponent (E)							
1	SN	2^7	2^6	2^5	2^4	2^3	2^2	2^1
2	Fraction (F)							
	2^0	2^{-1}	2^{-2}	2^{-3}	2^{-4}	2^{-5}	2^{-6}	2^{-7}
3	Fraction (F)							
	2^{-8}	2^{-9}	2^{-10}	2^{-11}	2^{-12}	2^{-13}	2^{-14}	2^{-15}
4	Fraction (F)							
	2^{-16}	2^{-17}	2^{-18}	2^{-19}	2^{-20}	2^{-21}	2^{-22}	2^{-23}
SN: sign 0 = positive, 1 = negative								

Figure 4 – Single float coding

Notations:	Double Float (eight octets)							
Value range	See in IEC 60559, Short Real Number, 64 bits							
coding	See in IEC 60559, Short Real Number, 64 bits							
	MSB bit 7 6 5 4 3 2 1 0 LSB							
octet	Exponent (E)							
1	SN	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4
2	Exponent (E)				Fraction (F)			
	2^3	2^2	2^1	2^0	2^{-1}	2^{-2}	2^{-3}	2^{-4}
3	Fraction (F)							
	2^{-5}	2^{-6}	2^{-7}	2^{-8}	2^{-9}	2^{-10}	2^{-11}	2^{-12}
4	Fraction (F)							
	2^{-13}	2^{-14}	2^{-15}	2^{-16}	2^{-17}	2^{-18}	2^{-19}	2^{-20}
5	Fraction (F)							
	2^{-21}	2^{-22}	2^{-23}	2^{-24}	2^{-25}	2^{-26}	2^{-27}	2^{-28}
6	Fraction (F)							
	2^{-29}	2^{-30}	2^{-31}	2^{-32}	2^{-33}	2^{-34}	2^{-35}	2^{-36}
7	Fraction (F)							
	2^{-37}	2^{-38}	2^{-39}	2^{-40}	2^{-41}	2^{-42}	2^{-43}	2^{-44}
8	Fraction (F)							
	2^{-45}	2^{-46}	2^{-47}	2^{-48}	2^{-49}	2^{-50}	2^{-51}	2^{-52}
SN: sign 0 =positive, 1=negative								

Figure 5 – Double float coding

4.2.4 Octetstring coding

The Octetstring coding manner is shown Table 4. For the data with N octets, the MSB of the most significant octet of PDU is first sent.

Table 4 – Octetstring coding

octet	bit							
	7	6	5	4	3	2	1	0
1	2^{8N-1}	2^{8N-2}	2^{8N-3}	2^{8N-4}	2^{8N-5}	2^{8N-6}	2^{8N-7}	2^{8N-8}
2	2^{8N-9}	2^{8N-10}	2^{8N-11}	2^{8N-12}	2^{8N-13}	2^{8N-14}	2^{8N-15}	2^{8N-16}
...	...	...	...	...	...	...	...	...
N	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

4.2.5 Bit Field coding

Bit Field data are used to encode objects as single-bit data. The bit coding manner is shown in Table 5, Table 6, and Table 7. This data type is defined as a series of eight bits. For the data with two octets, the most significant octet of PDU is sent first. For each bit of the bit field data type, there is a corresponding definition table.

Table 5 – Coding of Bit Field data with one octet

octet	bit							
	7	6	5	4	3	2	1	0
1	7	6	5	4	3	2	1	0

Table 6 – Coding of Bit Field data with two octets

octet	bit							
	7	6	5	4	3	2	1	0
1	15	14	13	12	11	10	9	8
2	7	6	5	4	3	2	1	0

Table 7 – Coding of Bit Field data with three octet

octet	bit							
	7	6	5	4	3	2	1	0
1	23	22	21	20	19	18	17	16
2	15	14	13	12	11	10	9	8
3	7	6	5	4	3	2	1	0

4.2.6 TimeData coding

This data type is an unsigned integer with a length of 64 bits, indicating time incremented by 1us.

4.2.7 KeyData coding

This data type is an unsigned integer with a length of 128 bits.

4.3 Structured data type coding

4.3.1 Structure type coding

A structure is made of an ordered set of heterogeneously different typed data called members, which may be basic data type or structured data type. The member of a structure is identified by MemberID. The structure data may be accessed as a whole, or just one of its members may be accessed by specifying the MemberID.

4.3.2 List type coding

A list is composed of an ordered set of homogeneously same typed elements called records, which may be basic data type or structured data type. The record of a list is identified by FirstStoreIndex. The list data may be accessed as a whole, or one or several of its records may be accessed by specifying the starting FirstStoreIndex and the count.

5 WIA-FA overview

5.1 Device types

The document specifies five types of WIA-FA devices:

host computer (HC);
gateway device (GW);
access device (AD);
field device (FD);
handheld device (HD).

To improve availability and reliability, WIA-FA network allows the existence of redundant gateway device as a hot backup, multiple access devices working in parallel.

NOTE 1 In the WIA-FA network, the redundant gateway device (see 3.1.27) and the primary gateway device (see 3.1.25) use the same network address. They adopt wired connection and synchronous update. The redundant gateway device periodically receives the heartbeat signal from the primary gateway device in wired connection manner. If the redundant gateway device does not receive the heartbeat signal in the period of PriGwFailureTime (see Table 14), it will take over all works of the original primary gateway device.

NOTE 2 Access devices connect the gateway device in the wired manner (see Clause 9). Multiple access devices concurrently work.

5.1.1 Host computer

Host computer is the interface for the operation, maintenance and management personnel to execute functions of application configuration, network configuration, and data display. Its specific implementation is beyond the scope of this PAS.

5.1.2 Gateway device

The main functions of the gateway device are listed as follows:

- Providing interconnection interfaces between WIA-FA network and other external networks, such as fieldbus, using data mapping and protocol conversion means;
- Responsible for network management and security management;
- Communicating with other WIA-FA devices through access devices, and exchanging information between devices;
- Acting as the unique clock source in the WIA-FA network for network time synchronization.

5.1.3 Access device

The main functions of the access device are listed as follows:

- Receiving data gathered by field device and forwarding them to the gateway device;
- Forwarding the control command of gateway device to the actuators of field device;
- Forwarding the management information and configuration information of gateway device to the field devices;
- Receiving alarms and network management information of field device and forwarding them to the gateway device.

NOTE The access devices and gateway devices are connected by wire. Their synchronization method is beyond the scope of this PAS.

5.1.4 Field device

Field devices are installed in industrial field and connect sensors and actuators. Field devices collect field application data and control production process. The power supply modes of field devices include wired power supply, battery power supply, etc., which are beyond the scope of this PAS.

5.1.5 Handheld device

Handheld devices are portable devices that used for provisioning field device, access device, and gateway device. A handheld device communicates with its direct connected device, and does not communicate with other WIA-FA devices. Handheld devices use RS-232 maintenance port to provision field device, access device and gateway device and write security level, join keys, shared keys(except security level 0), and network Identifier (ID) for them.

5.2 Network topology

As shown in Figure 6, WIA-FA supports the enhanced star topology, which is comprised of a center and a number of field devices. The center is comprised of one gateway device (redundant gateway device can exist) and one or several access devices.

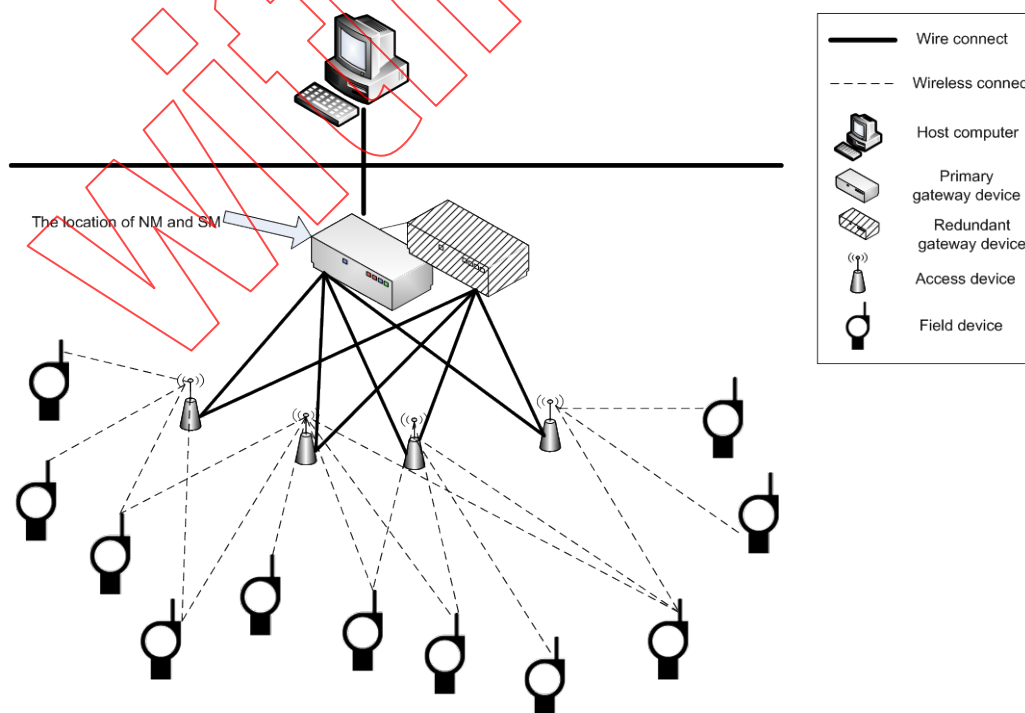


Figure 6 – WIA-FA enhanced star topology

5.3 Protocol architecture

The WIA-FA network protocol follows the ISO/IEC 7498-1 OSI reference model. The WIA-FA network protocol defines the Physical Layer (PHY), Data Link Layer (DLL) and Application Layer (AL). Figure 7 shows the mapping between WIA-FA and OSI basic reference model.

OSI layer	Function	WIA-FA
Application	Provides the user with network capable application	Distributed application services
Presentation	Converts between application layer data and the lower layer data formats	
Session	Connection management services	
Transport	Provides network independent, transparent message transfer	
Network	Resolving network addresses, End- to- end routing of packets.	
Data link	Establishes data packet structure, framing, error detection, bus arbitration	DLL Communication based on multiple AOs, TDMA, FDMA, retransmission, aggregation...
Physical	Mechanical / electrical connection. Transmits raw bit stream	PHY (IEEE STD 802.11-2012 PHY)

Figure 7 – OSI basic reference model mapped to WIA-FA

Figure 8 shows the protocol architecture of WIA-FA. The protocol architecture of WIA-FA includes the following components:

- Protocol layers: including PHY, DLL, AL; AL is comprised of ASL, UAP and DMAP;
- Entities of protocol layers: including data entities (DLDE and ASLDE) and management entities (DLME and ALSME);
- Protocol layer interfaces: including data entities SAPs (DLDE-SAP and ASLDE-SAP) and management entity SAPs (DLME-SAP and ALSME-SAP).

Device Management Application Process (DMAP) includes the network manager/network management module, security manager/security management module, and MIB. DMAP is a special User Application Process (UAP) and uses ASLDE-SAP together with UAP to exchange messages with ASL.

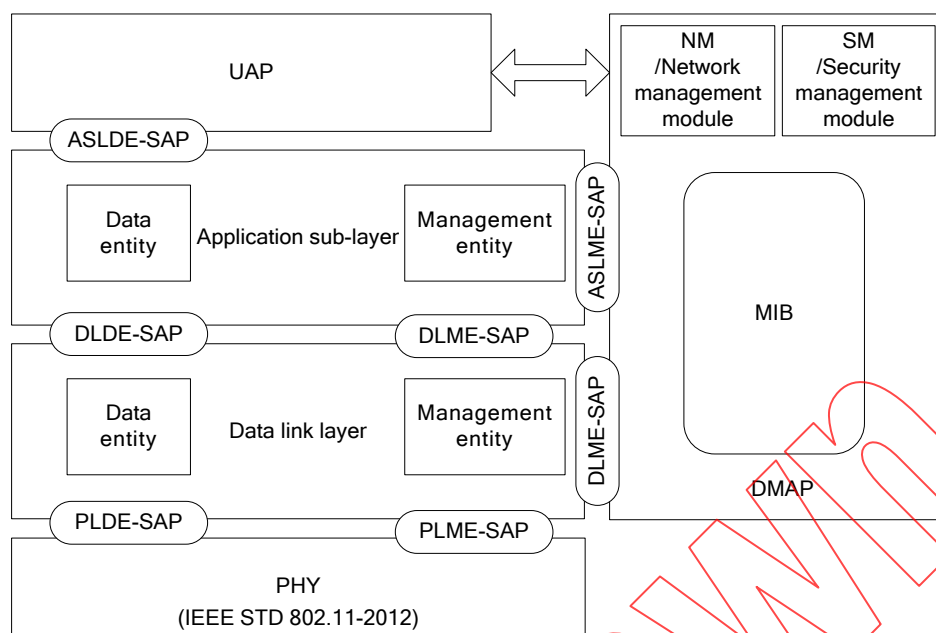


Figure 8 – Protocol architecture of WIA-FA

The data flow over WIA-FA network is shown in Figure 9.

- A field device has PHY, DLL, and AL;
- An access device has PHY and DLL; An access device connects with the gateway device by wires;
- The gateway device only has AL and part of DLL. The application running on the gateway device consists of a component that communicates with the application layer of the WIA-FA network, plus a component that communicates with the application layer of the plant network, plus any components that facilitate translation between the application layer of the WIA-FA network and the application layer of the plant network.

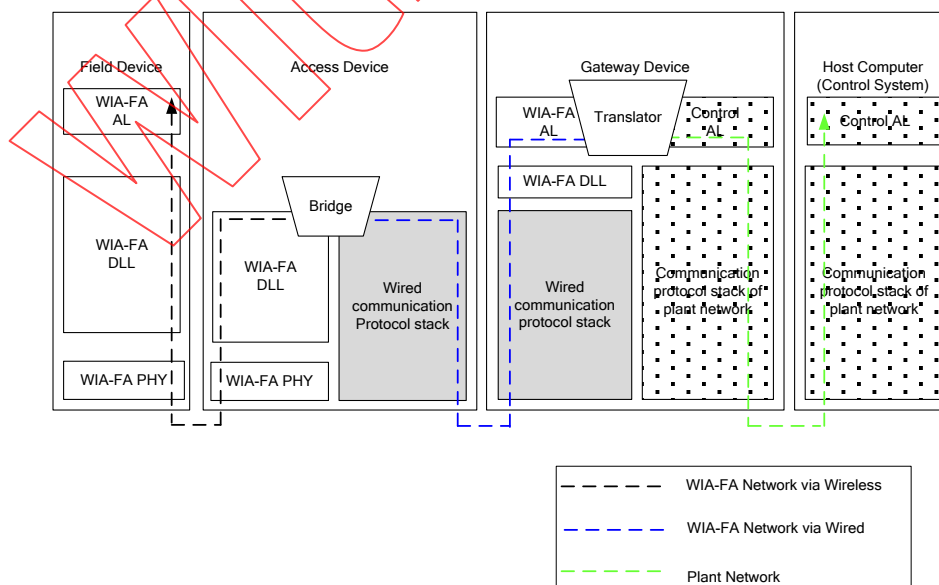


Figure 9 – Data flow over WIA-FA network

6 System management

6.1 Overview

The WIA-FA network adopts centralized management framework, as shown in Figure 10. The system management is implemented by the network manager and security manager in the gateway device, and the network management modules and security management modules in field devices and access devices. The network manager and security manager are responsible for managing the access devices and field devices. Network management modules and security management modules are realized in field devices and access devices, which perform management functions together with the gateway device.

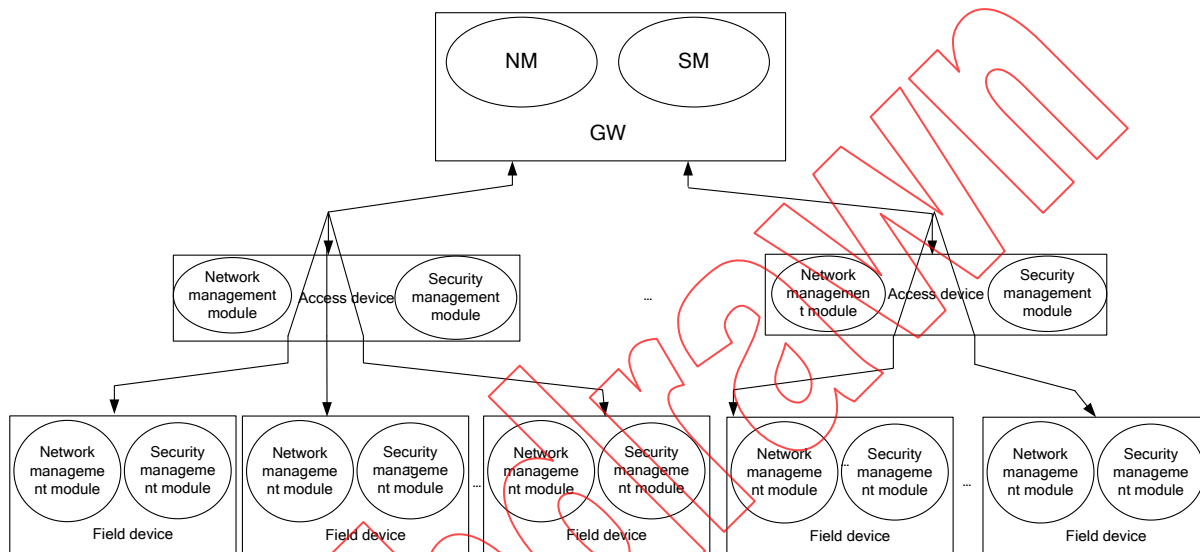


Figure 10 – System management scheme

6.2 Device Management Application Process

The functions of system management in WIA-FA network are implemented by the Device Management Application Process (DMAP) in each device. The DMAP is a particular User Application Process (UAP), responsible for managing devices and providing MIB access services. The position and component of the DMAP in the protocol architecture are shown in Figure 11. The grey part is the DMAP, and the white parts are function modules in DMAP, including:

- Network Manager (NM) of Gateway Device (GW), the network management modules of Access Devices (AD) and Field Device (FD);
- Security Manager (SM) of GW, the security management modules of AD and FD;
- Management Information Base (MIB), saving all the attributes for network management and security management in WIA-FA network.

DMAP is a special User Application Process (UAP) and uses ASLDE-SAP together with UAP to exchange messages with ASL, as shown in Figure 11.

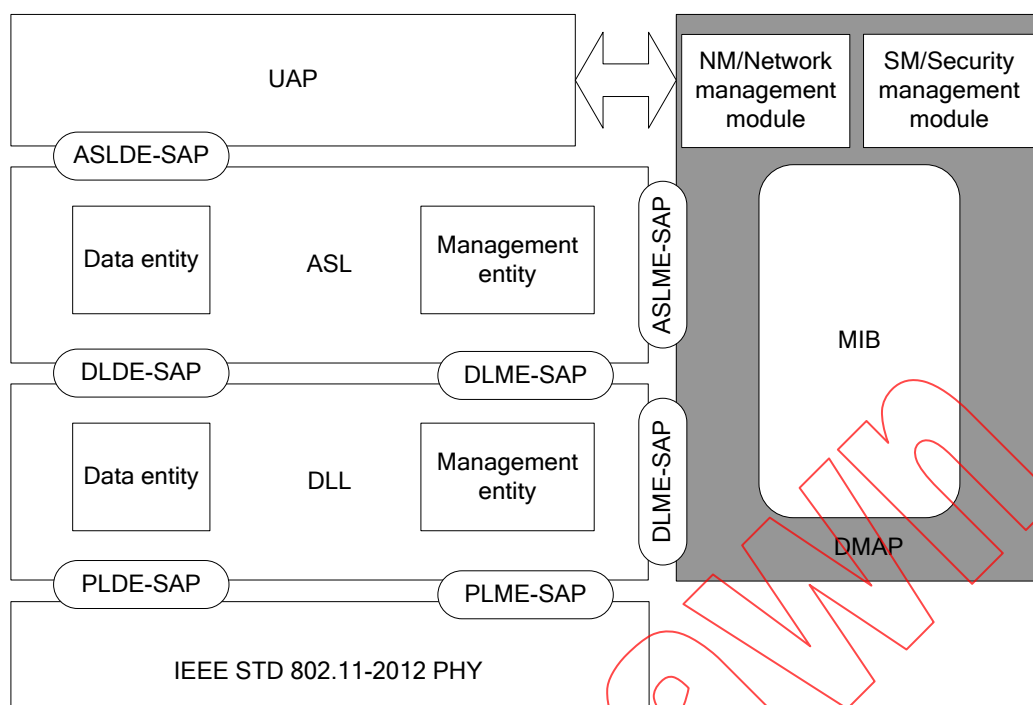


Figure 11 – DMAP of management system

The network management functions implemented in WIA-FA network are shown in Table 8 and Table 9.

Table 8 – Network management functions

Network management functions	Requirement
Network establishment	Initialization: initializing the NM/network management modules and starting the network
	Time source configuration and system time service; the WIA-FA network should set up one reference time source, which is performed by the gateway device. Devices in the network should only synchronize with gateway device.
	Device join process management: the devices need NetworkID (see Table 14) before joining. The joining devices invoke the join process, after the authentication of SM, the NM returns the join response.
	Network address allocation: Each device in the WIA-FA network has a global unique 64-bit address which is called long address and an 8-bit or 16-bit network address which is called short address. The long address of each device is assigned by vendors according to the 64-bit Extended Unique Identifier (EUI-64). The short address of each network device is assigned by the NM.
	Topology management: forming and maintaining the enhanced star topology as shown in Figure 6.
	Network configuration management: maintaining the communication resources, network address, network attributes, including the information of all network devices distributed by the NM, finishing the configuration of MIB.
Network scheduling and Communication resource allocation	Superframe establishment: establishing the superframe for communication according to the application requirement.
	Communication resource allocation: allocating the communication resources in superframe to the links.
	Activation/deactivation: activating and deactivating the superframe according to application process.
Channel Network diagnosis and performance monitoring	Channel management: monitoring and maintaining the channel list and condition.
	Device health status management: monitoring and maintaining the health status of each device.
	Network performance monitoring
Leaving	Device leave process management: the leave process of field devices and access devices includes passive leaving and abnormal leaving. The passive leaving is invoked by the gateway device, the field devices and access devices leave the network after receiving the leave request, and the gateway device releases the communication resources of field devices; The abnormal leaving is detected and processed by the gateway device.

Table 9 – Security management functions

Security management functions	Requirement
Secure network establishment and configuration	Secure join process: when a new field device invokes the secure join process, SM shall authenticate the field device and return the result to NM; NM returns a join response considering the authentication result.
	Key establishment: after FD secure joining, SM generates and distributes keys used to make secure operation during normal operating process, including KEK, KEDB, and KEDU.
Key updating	Key update: SM updates the keys in use before the ends of their lifetime, including KEK, KEDB, and KEDU.
Security performance monitoring	Security alarm: monitoring the update status and attacked counts of keys.

6.2.1 Network manager

Network Manager (NM) realizes network management function in the gateway device, which manages the information of all devices in the network. One WIA-FA network has only one NM.

NM mainly performs the following functions:

- Allocating the unique 8-bit or 16-bit short address for all devices in the network (see 6.3);
- Constructing and maintaining the enhanced star topology;
- Allocating communication resources for communications of WIA-FA devices;
- Monitoring the performance of the WIA-FA network, including device status, and channel condition, etc.

6.2.2 Security manager

Security Manager (SM) realizes the function of security in the gateway device, and one WIA-FA network has only one SM. SM communicates directly with NM.

SM mainly performs the following functions:

- Authenticating the field devices attempting to join the WIA-FA network;
- Managing keys in the WIA-FA network, including key establishment and update (see 11.4).
- Handling security alarm.

6.2.3 Network management module

Network management modules in the field device and access device maintain the information needed for communication.

The main functions of the network management module are as follows:

- Coordinating with NM to construct and maintain the enhanced star topology;
- Coordinating with NM to allocate communication resources for devices;
- Coordinating with NM to monitor the performance of the WIA-FA network, including device status, and channel condition, etc.

6.2.4 Security management module

Security management modules in the field device and access device maintain the information for security management functions, and realize following security management functions:

- Coordinating with SM to conduct secure joining (field device only);
- Coordinating with SM to manage keys;
- Coordinating with SM to report security alarm.

6.2.5 DMAP state machines

6.2.5.1 DMAP state machine of gateway device

The DMAP state machine of the gateway device is shown in Figure 12, which includes Init and Idle states. The gateway device enters into Active state if it finishes initializations.

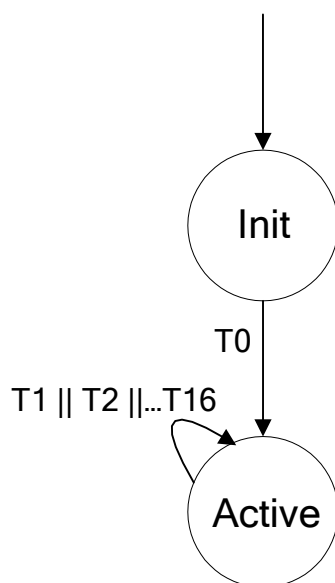


Figure 12 – DMAP state machine of gateway device

The DMAP state transition of gateway device is listed in Table 10.

Table 10 – DMAP state transition of gateway device

#	Current State	Event or condition => action	Next state
T0	Init	IsDMAPInitializationDone() == TRUE => ;	Active
T1 T2 ... T16	Active	T1 T2 ... T16 => See Table 11	Active

The DMAP of gateway device maintains a state machine for each field device, as shown in Figure 13. The gateway device can process multiple packets from multiple field devices in parallel. The triggering condition from Init state to Active state in Figure 11 is one of T1 to T16 (see Table 11).

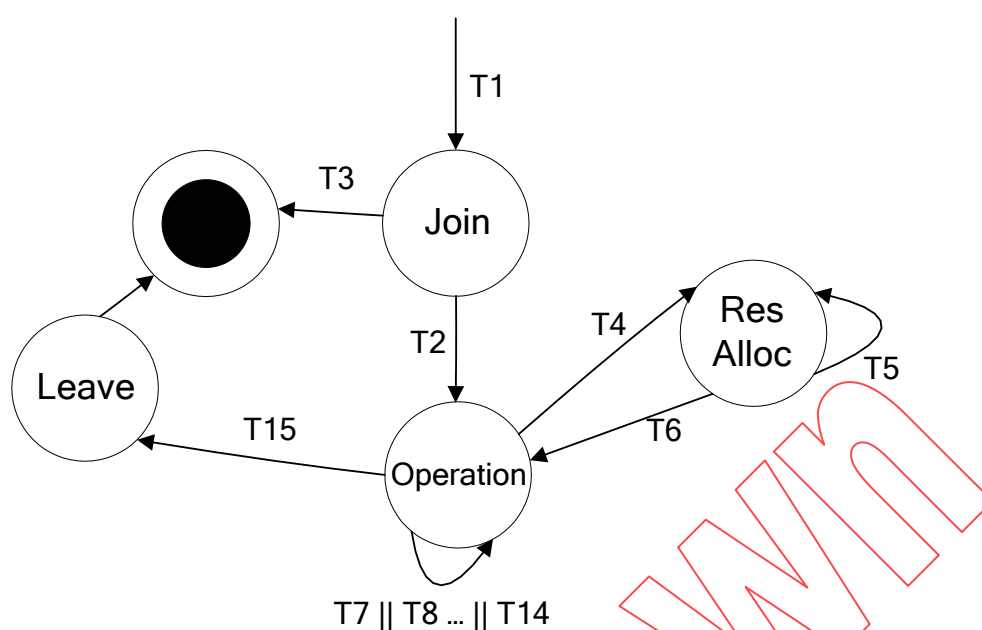


Figure 13 – DMAP state machine of gateway device for each field device

The DMAP state transition of gateway device for each field device is listed in Table 11.

Table 11 – DMAP state transition of gateway device for each field device

#	Current State	Event or condition => action	Next state
T1	Active	PrimitiveType == DLME-JOIN.indication =>	Join
T2	Join	Authentication(PhyAddr, SecMaterial) == SUCCESS && AllocateShortAddr(Addr) == SUCCESS => DLME-JOIN.response(Status:= SUCCESS, ShortAddr);	Operation
T3	Join	Authentication(PhyAddr, SecMaterial) != SUCCESS AllocateShortAddr(Addr) != SUCCESS => If ((Authentication(PhyAddr, SecMaterial) != SUCCESS) { DLME-JOIN.response(Status := AUTH_FAILURE, ShortAddr); }else if(AllocateShortAddr(Addr) != SUCCESS) { DLME-JOIN.response(Status:= NETWORK_SCALE_ERROR, ShortAddr); }	End
T4	Operation	IsHostComputerConfigureDone() == TRUE => AllocResult:= ResAllocAgrithm (SuperframeList,LinkList); If (AllocResult == SUCCESS) DLME-INFO-SET.request(AttributeOption:= 2, AttributeID:= 131, AttributeMemID:= 12, AttributeValue:= ALLOCATION); DLME-INFO-SET.request(AttributeOption:= 0, (AttributeID:= 128) (AttributeID:= 129)); }	Res Alloc
T5	Res Alloc	PrimitiveType ==DLME-INFO-SET.confirm && (AttributeID == 128 AttributeID == 129) => DLME-INFO-SET.request(AttributeOption:= 0, (AttributeID:= 128) (AttributeID:= 129));	Res Alloc
T6	Res Alloc	IsAllResAllocateDone() == TRUE => DLME-INFO-SET.request(AttributeOption:= 2, AttributeID:= 131, AttributeMemID:= 12, AttributeValue:= OPERATION);	Operation
T7	Operation	PrimitiveType == DMAP-MIB-SET.request => Status = WriteToMIB(Handle, AttributeOption, AttributeID, AttributeMemID, FirstStoreIndex, Count, AttributeValue); DMAP-MIB-SET.confim(Handle, Status);	Operation
T8	Operation	PrimitiveType == DMAP-MIB-GET.request => Status := ReadFromMIB(Handle, AttributeID, AttributeMemID, FirstStroeIndex, Count, AttributeValue); DMAP-MIB-GET.confim(Handle, Status, Count, AttributeValue);	Operation

#	Current State	Event or condition => action	Next state
T9	Operation	IsHostComputerSet MIB() == TRUE => DLME-INFO-SET.request(Handle, DstAddr, AttributeOption, AttributeID, AttributeMemID, FirstStoreIndex, Count, AttributeValue);	Operation
T10	Operation	PrimitiveType ==DLME-INFO-SET.confirm => IndicateSetMIBResult(Handle, Status);	Operation
T11	Operation	IsHostComputerGet MIB() == TRUE => DLME-INFO-GET.request(Handle, DstAddr, AttributeID, AttributeMemID, FirstStoreIndex, Count);	Operation
T12	Operation	PrimitiveType ==DLME-INFO-GET.confirm => IndicateGetMIBResult(Handle, Status);	Operation
T13	Operation	PrimitiveType == DLME-CHANNEL-STATUS.indication => HandleChannelStatusReport(Addr, ChannelConditionInfo);	Operation
T14	Operation	PrimitiveType == DLME-DEVICE-STATUS => HandleDeviceStatusReport(PowerSupplyStatus);	Operation
T15	Operation	IsHostComputerRequestDeviceLeave() == TRUE => DLME-LEAVE.request(DeviceAddr); ReleaseResources(Addr); IndicateHostComputerLeaveResult(Addr);	Leave

– Join state

In Join state, the DMAP of the gateway device handles join request received from field devices and performs authentication. If a field device is authenticated successfully, the NM in the DMAP assigns short address for the field device. If authentication or short address assignment fails, DMAP invokes DLME-JOIN.response to notify the field device the failure result. After the DMAP state machine enters to End State; if authentication and short address assignment succeeds, the DMAP of the gateway device invokes DLME-JOIN.response to notify the field device that the join process is successful; then, the DMAP state machine enters to Operation state.

– Operation state

In Operation state, the following events shall occur:

- Host compute remotely sets the field device's MIB attributes; DMAP invokes DLME-INFO-SET.request to request DLL generating a remote attribute set request frame (see 8.4.16).
- DLL invokes DLME-INFO-SET.confirm and returns the result of remote attribute set operation to DMAP.
- Host compute remotely gets the field device's MIB attributes; DMAP invokes DLME-INFO-GET.request to request DLL generating a remote attribute get request frame (see 8.4.14).
- DLL invokes DLME-INFO-GET.confirm and returns the related MIB attributes of a field device to DMAP.

- e) Host computer invokes DMAP-MIB-SET.request to locally set the gateway's MIB attributes; DMAP sets its MIB attributes and invokes DMAP-MIB-SET.confirm to return the result of local attribute set operation to the host computer.
 - f) Host computer invokes DMAP-MIB-GET.request to locally get the gateway's MIB attributes; DMAP returns its MIB attributes and invokes DMAP-MIB-GET.confirm to return related MIB attributes to the host computer.
 - g) DLL invokes DLME-DEVICE-STATUS.indication to DMAP after it receives the device status report from a field device.
 - h) DLL DLME-CHANNEL-STATUS.indication to DMAP after it receives the channel condition report from a field device.
 - i) Host computer requests a field device leaving WIA-FA network. DMAP invokes DLME-LEAVE.request to request DLL generating a leave command frame (see 8.4.9).
- Res Alloc State

In Res Alloc state, the DMAP of the gateway device allocates communication resources to a field device; DMAP invokes DLME-INFO-SET.request to remotely writing superframes or links to the field device. If the communication resource allocating process is completed or failure, DMAP remotely sets the field device's DeviceState (see Table 19) attribute to Operation; then, the DMAP state machine enters to Operation State.
 - Leave State

In Leave state, DMAP releases all MIB attributes and communication resources that are occupied by a leaving field device; then, the DMAP state machine enters to End state.

6.2.5.2 DMAP state machine of field device

The DMAP state machine of field device is shown in Figure 14.

Withdrawn

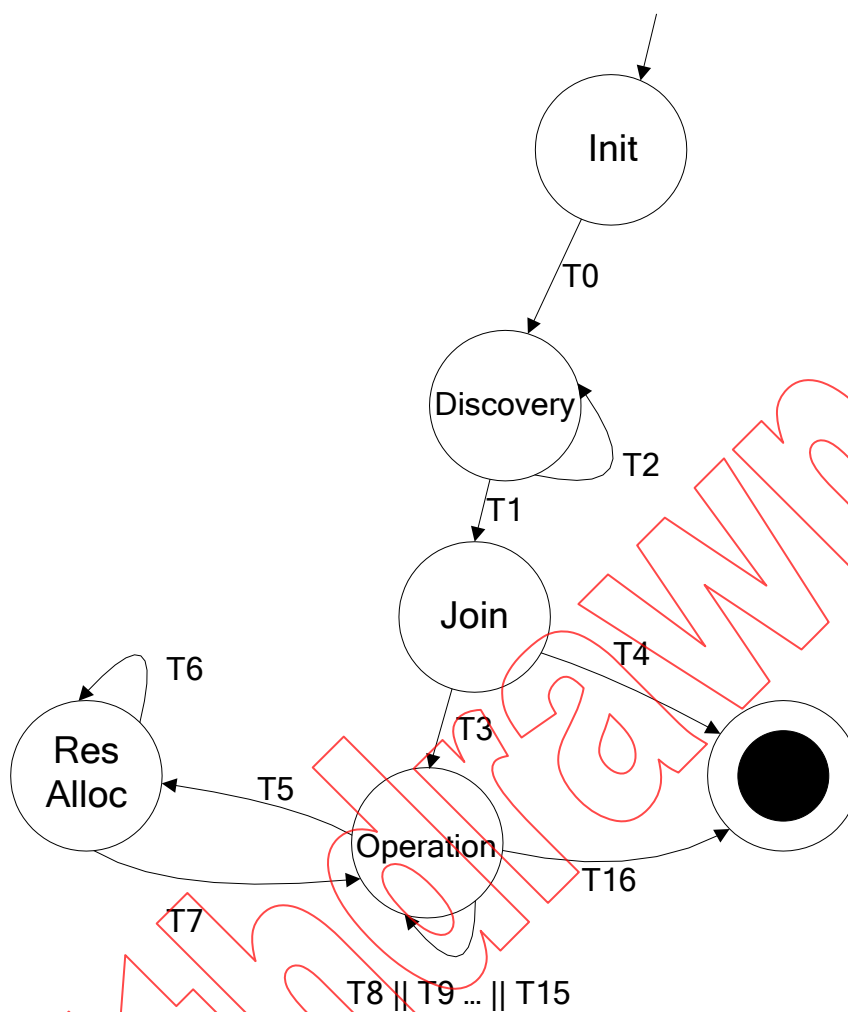


Figure 14 – DMAP state machine of a field device

The DMAP state transition of a field device is shown in Table 12.

Table 12 – DMAP state transition of a field device

#	Current State	Event or condition => action	Next state
T0	Init	IsDMAPInitializationDone() == TRUE => DLME-DISCOVERY.request(ScanChannels, ProbeTime);	Discovery
T1	Discovery	PrimitiveType == DLME-DISCOVERY.confirm && Status == SUCCESS => DLME-JOIN.request(NetworkID, Channel, PhyAddr, SecMaterial);	Join
T2	Discovery	PrimitiveType == DLME-DISCOVERY.confirm && Status == NO_BEACON => DLME-DISCOVERY.request(ScanChannels, ProbeTime);	Discovery
T3	Join	PrimitiveType == DLME-JOIN.confirm && Status == SUCCESS => DeviceStruct.ShortAddr = ShortAddr;	Operation
T4	Join	PrimitiveType == DLME-JOIN.confirm && Status != SUCCESS =>	End
T5	Operation	PrimitiveType == DLME-INFO-SET.indication && (AttributeID == 131 && AttributeMemID == 12) && AttributeValue == ALLOCATION => Status = WriteToMIB(Handle, AttributeOption, AttributeID, AttributeMemID, FirstStoreIndex, Count, AttributeValue); DLME-INFO-SET.response(Handle, Status);	Res Alloc
T6	Res Alloc	PrimitiveType == DLME-INFO-SET.indication && (AttributeID == 128 AttributeID == 129) => Status = WriteToMIB(Handle, AttributeOption, AttributeID, AttributeMemID, FirstStoreIndex, Count, AttributeValue); DLME-INFO-SET.response(Handle, Status);	Res Alloc
T7	Res Alloc	PrimitiveType == DLME-INFO-SET.indication && (AttributeID == 131 && AttributeMemID == 12) && AttributeValue == OPERATION => Status = WriteToMIB(Handle, AttributeOption, AttributeID, AttributeMemID, FirstStoreIndex, Count, AttributeValue); DLME-INFO-SET.response(Handle, Status);	Operation
T8	Operation	PrimitiveType == DLME-INFO-SET.indication => Status = WriteToMIB(Handle, AttributeOption, AttributeID, AttributeMemID, FirstStoreIndex, Count, AttributeValue); DLME-INFO-SET.response(Handle, Status);	Operation
T9	Operation	PrimitiveType == DLME-INFO-GET.indication => Status = ReadFromMIB(Handle, AttributeID, AttributeMemID, FirstStoreIndex, Count, AttributeValue); DLME-INFO-GET.response(Handle, Status, Count, FirstStoreIndex, Count, AttributeValue);	Operation

#	Current State	Event or condition => action	Next state
T10	Operation	PrimitiveType == DMAP-MIB-SET.request => Status = WriteToMIB(Handle, AttributeOption, AttributeID, AttributeMemID, FirstStoreIndex, Count, AttributeValue); DMAP-MIB-SET.confirm(Handle, Status);	Operation
T11	Operation	PrimitiveType == DMAP-MIB-GET.request => Status = ReadFromMIB(Handle, AttributeID, AttributeMemID, FirstStoreIndex, Count, AttributeValue); DMAP-MIB-GET.confirm(Handle, Status, Count, AttributeValue);	Operation
T12	Operation	DevStaRptCycle timeout => DLME-DEVICE-STATUS.request(PowerSupplyStatus);	Operation
T13	Operation	PrimitiveType == DLME-DEVICE-STATUS.confirm =>	Operation
T14	Operation	(ChaStaRptCycle timeout) => DLME-CHANNEL-STATUS.request(ChannelConditionInfo);	Operation
T15	Operation	PrimitiveType == DLME-CHANNEL-STATUS.confirm =>	Operation
T16	Operation	PrimitiveType == DLME-LEAVE.indication => ReleaseResources(Addr);	End

– Init state

In Init state, the field device initializes itself and enters to Discovery state.

– Discovery state

In Discover state, the DMAP of a field device invokes DLME-DISCOVERY.request to scan WIA-FA network. DLL invokes DLME-DISCOVERY.confirm to return the result of network scanning. If the result is successful, the DMAP state machine of a field device enters to Join state; otherwise, the DMAP state machine of a field device stays in Discovery state and restarts the network discovery.

– Join state

In Join state, the DMAP of a field device invokes DLME-JOIN.request to try to join the network; DLL invokes DLME-JOIN.confirm to return the joining results. If the result indicates the join process is successful, the state machine enters to Operation state; otherwise, the state machine enters to End state.

– Res Alloc state

In Res Alloc state, DLL invokes DLME-INFO-SET.indication after it receives a remote attribute set request from the gateway device to write superframes or links. The DMAP of the field device writes superframes or links into MIB, and invokes DLME-INFO-SET.response to return the result. If the DeviceState (see Table 19) in MIB is set to Operation by the gateway device, the state machine enters to Operation state.

– Operation state

In Operation state, the following events shall occur:

- a) DLL invokes DLME-INFO-SET.indication after it receives a remote attribute set request frame (see 8.4.16), which indicates DMAP to set MIB attributes. The DMAP of a field device sets the MIB attributes properly and invokes DLME-INFO-SET.response to return the result.
- b) DLL invokes DLME-INFO-GET.indication after it receives a remote attribute get request frame (see 8.4.14), which indicates DMAP to get MIB attributes. The DMAP of a field device gets the related MIB attributes properly and invokes DLME-INFO-GET.response to return the requested MIB attributes.
- c) APP/DLL invokes DMAP-MIB-GET.request to locally get MIB attributes. The DMAP invokes DMAP-MIB-GET.response to return the related MIB attributes.
- d) APP/DLL invokes DMAP-MIB-SET.request to locally set the MIB attributes. The DMAP invokes DMAP-MIB-GET.response to return the result of DMAP-MIB-SET.request.
- e) If the timer for device status report expires every DevStaRptCycle (see 6.7.1.2.1) time, the DMAP of a field device invokes DLME-DEVICE-STATUS.request to send the device status report to the gateway device.
- f) DLL invokes DLME-DEVICE-STATUS.confirm to DMAP, which returns the result of sending device status report.
- g) If the timer for the channel condition report expires every ChaStaRptCycle (see 6.7.1.2.1) time, the field device DMAP invokes DLME-CHANNEL-STATUS.request to returns the result of sending channel condition report.
- h) DLL invokes DLME-CHANNEL-STATUS.confirm to DMAP, which returns the result of sending channel condition report.
- i) DLL invokes DLME-LEAVE.indication after receiving a leave request frame from the gateway device; the field device releases all MIB attributes and communication resources, and enters to End state.

6.2.5.3 Functions used in DMAP state transitions

The functions used in DMAP state transitions of the gateway device are listed in Table 13.

Table 13 – Functions used in DMAP state transition

Function	Input	Output	Description
Authentication()	PhyAddr	SUCCESS FAILURE	Authenticating a joining field device
AllocateShortAddr()	Addr	SUCCESS FAILURE	Allocating short address for a field device
IsHostComputerConfigureDone()		TRUE FALSE	Judging whether the application configuration of the host computer is finished
ResAllocAgrithm()	SuperframeList LinkList	SUCCESS NO_RESOURCE	Allocating communication resources
IsHostComputerRequestDeviceLeave()		TRUE FALSE	Judging whether the host computer request a field device leave WIA-FA network
IsHostComputerSet MIB()		TRUE FALSE	Judging whether the host computer remotely request setting the attributes of a field device
IndicateSetMIBResult()	Handle Status		Indicating the results of the remote attribute set operation to the host computer
HandleChannelStatusReport()	Addr ChannelConditionInfo		Processing the channel condition report
HandleDeviceStatusReport()	PowerSupplyStatus		Process the device status report
IsHostComputerGet MIB()		TRUE FALSE	Judging whether the host computer remotely request getting the MIB attributes
IndicateGetMIBResult()	Handle Status		Indicating the results of the remote attribute get operation to the host computer
ReleaseResources()	Addr		Releasing communication resources occupied by a field device
IndicateHostComputerLeaveResult()	Addr		Indicating the leave of a field device to the host computer
WriteToMIB();	Handle AttributeOption AttributeID AttributeMemID FirstStoreIndex Count AttributeValue	SUCCESS INVALIDATTRIBUTE INVALIDATTRIBUTE_MEMBER INVALID VALUE	Locally writing MIB attributes
ReadFromMIB()	Handle AttributeID AttributeMemID FirstStroeIndex Count AttributeValue	SUCCESS INVALIDATTRIBUTE INVALIDATTRIBUTE_MEMBER INVALID RANGE	Locally reading MIB attributes

Function	Input	Output	Description
IsDMAPInitializationDone()		TRUE FALSE	Judging whether the DMAP initialization is finished
IsAllResAllocateDone()		TRUE FALSE	Judging whether all communication resources are allocated

6.3 Addressing and address assignment

Each WIA-FA network (field device, access device, and gateway device) has a global unique 64-bit long address and an 8-bit or 16-bit short address (indicated by AddressTypeFlag in Table 14). When the number of field devices in the network is less than 252, 8-bit short address should be adopted; Otherwise, the 16-bit short address should be adopted. The long address, shown in Figure 15, is assigned and set by manufacturers according to the EUI-64. The least significant octet of DeviceShortAddress (see Table 9 in 6.7.1.2.2) is valid if the network uses 8-bit short address.

Gateway device uses AdID to distinguish different access devices.

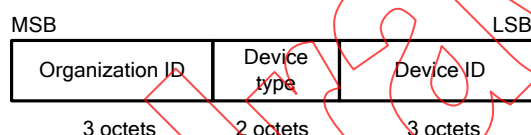


Figure 15 – Long address structure of device

In the WIA-FA network, the 8-bit short address of a WIA-FA device is set as follows:

- The short address of gateway device is 0x01;
- The short address of access device is 0x02;
- The value range of field device short address is 0x03 to 0xFE;
- The broadcast address in WIA – FA network is 0xFF.

In the WIA-FA network, the 16-bit short address of a WIA-FA device is set as follows:

- The short address of gateway device is 0x0001;
- The short address of access device is 0x0002;
- The value range of field device short address is 0x0003 to 0xFFFF;
- The broadcast address in WIA – FA network is 0xFFFF.

The default short address of a device is 0x00 or 0x0000, and it means the device hasn't been allocated short address.

6.4 Communication resource allocation

6.4.1 General

Communication resources consist of channels (see 3.1.8) and timeslots (see 3.1.31). Allocation of communication resources means allocating channels and timeslots in superframe to access devices and field devices for creating links according to data priorities and resource occupation methods. LinkList attributes include LinkID, LinkType, PeerAddr, RelativeSlotNumber, ChannelIndex, and SuperframeID (see 6.7.1.2.2).

6.4.2 Communication resource allocation

6.4.2.1 Data priorities

According to the functions and requirements of data in industrial fields, the data is set to different priorities. WIA-FA defines the following five data priorities:

- Emergent data (RT0)
RT0 data has the highest priority. It refers to the data that plays a key role to application behaviours and requires being timely transferred. RT0 data includes: command from the host computer to brake the actuator; emergent alarm of failure/error notification; critical network management services from the host computer, such as start/stop command. The transmission of RT0 data uses R/S communication mode (see 10.5.5.3.3).
- Periodic process data (RT1)
RT1 data has the second highest priority. It refers to the periodically transmitted process data that has strict real-time requirement. RT1 data mainly includes the physical measurement and control data of a control system. The transmission of RT1 data uses P/S communication mode (see 10.5.5.3.2).
- Aperiodic non-urgent data (RT2)
RT2 data has the third highest priority. It refers to the aperiodically transmitted data triggered by events, such as the non-urgent alarm data. The transmission of RT2 data uses R/S communication mode (see 10.5.5.3.3).
- Periodic management data (RT3)
RT3 data has the fourth highest priority. It refers to the periodically transmitted monitoring data of device and network status, which has certain real-time requirements. RT3 data mainly includes the device status, channel state, etc. The transmission of RT3 data uses P/S communication mode (see 10.5.5.3.2).
- Non-real-time data (NRT)
NRT data has the lowest priority. It refers to data that is generated by network operation and has no strict real-time requirement. In the industrial field, NRT data usually includes parameter configuration and management data. The NRT data transmission should not interfere with transmissions of real-time data. The transmission of NRT data uses C/S communication mode (see 10.5.5.3.1).

The transmission of data with one of above five priorities uses different communication modes and different VCRs. The definition of communication modes, VCR, and the corresponding relationship between VCR and data are shown in 10.5.5.3.

6.4.2.2 Occupation method of communication resources

For transmitting data with different priorities, the occupation methods of communication resources include scheduling, preemption, and competition.

- Scheduling
Scheduling is used for transmitting RT1 data and RT3 data. Network manager schedules all communication resources for whole WIA-FA network. After field devices and access devices joining the network, the network manager allocates fixed timeslots to periodically transmit and retransmit RT1 and RT3 data.
- Preemption
Preemption is used to transmit RT0 data. The gateway device and field devices can utilize timeslots original for periodic data to transmit RT0 data, which defers the transmission of the periodic data.
- Competition
Competition refers to using shared transmitting link to transmit RT2 data and NRT data.

6.5 Joining and leave process of field device

6.5.1 Joining process of a field device

The handheld device provisions a field device through RS232 maintenance port when this field device attempts to join WIA-FA network. The provisioning information includes:

- NetworkID;
- SecLevel;
- KJ (when the security level is not 0);
- KS (when the security level is not 0).

The join process of a provisioned field device is shown in Figure 16. The join process is listed as follows.

- Access devices periodically broadcast beacons;
- A field device with attempt to join the WIA-FA network continually scans available channels to get beacons from access devices and synchronizes with gateway device by using one-way time synchronization method (see 8.1.4);
- The field device chooses a channel on which field device receives beacon frame and utilizes the shared timeslots for sending the join request; the shared timeslot is determined by the "First shared timeslot number" and the "Shared timeslot count" (see 8.4.6) in the beacon frame; the field device competes for transmitting join request utilizing timeslot based backoff method (see 8.1.6.5) on the channel used by the beacon;
- An access device transfers the join request received from a field device to the gateway device;
- The NM residing on the gateway device returns the join response; if the joining is approved, the value of Status in the join response is set to SUCCESS; otherwise, the value of the Status should be set according to error reasons (See Status in 8.3.4.3);
- An access device forwards the join response to the corresponding field device;
- The field device receives the join response from an access device; if the value of Status in the join response is not SUCCESS, the field device should restart or terminate the join process; if the value of Status in the join response is SUCCESS, the join process is completed.

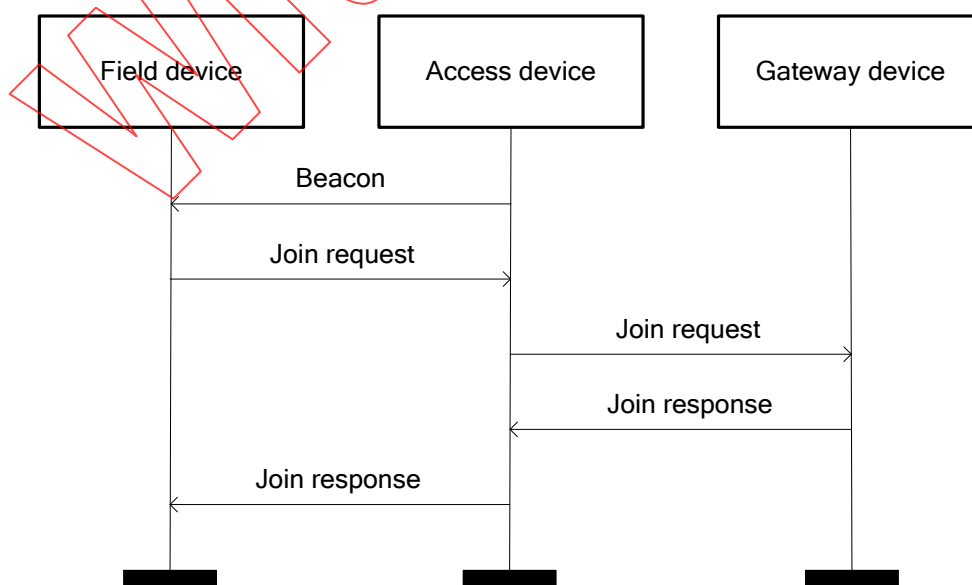


Figure 16 – Joining process of field device

NOTE See Clause 10 for security.

6.5.2 Communication resource allocation to field device

After a new field device joins WIA-FA network, the host computer requests the gateway device to read UAOs of the field device by using the remote attribute get services (see 8.3.7), and to write application configuration information/VCRs (see 10.5.5.3 and 10.5.5.4) for the field device by using the remote attribute configuration services (see 8.3.8).

The NM residing on the gateway allocates communication resources for new joined field device by utilizing the remote attribute configuration services (see 8.3.8). These communication resources are used for communication between field devices and access devices. If the new joined field device influences the superframe structures of access devices (see 8.1.2), the corresponding access device should update its own SuperframeList and LinkList attributes of itself and update SuperframeList and LinkList attributes between it and field devices.

The communication resource allocation process for a field device is illustrated in Figure 17:

- The network manager sends the "remote attribute configuration" request;
- Access devices forward the "remote attribute configuration" request to the field device;
- After receiving the "remote attribute configuration" request, the field device returns the "remote attribute configuration" response;
- Access devices forward the "remote attribute configuration" response to the gateway device.

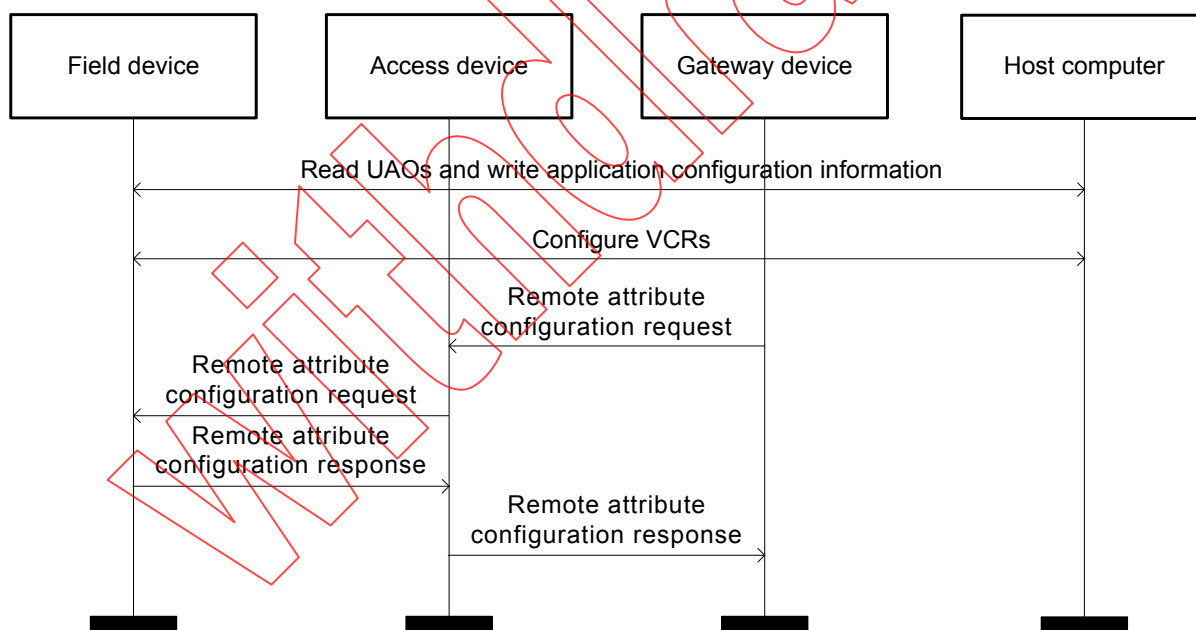


Figure 17 – Communication resource allocation process for a field device

6.5.3 Leaving process of a field device

The leave process of field devices includes abnormal leaving and passive leaving.

- Abnormal leaving: devices can not communicate with other devices because of failure, invalidation, or energy depletion. If the gateway device does not receive any packet from a field device during LossConnectDuration (see 6.7.1.2.1), it shall judge that the field device has left the WIA-FA network abnormally. The gateway device releases the short address and communication resources of the field device. If the field device does not receive any packet from access devices during LossConnectDuration (see 6.7.1.2.1), it shall judge that its connection with access devices is lost. The field device shall handle it as abnormal leaving and restart itself.

- Passive leaving: the gateway device requests a field device to leave the WIA-FA network. The passive leave process of a field device is shown in Figure 18, which includes the following procedures.
 - The gateway device sends the leave request to a field device (see 8.4.9) through the access device;
 - After receiving the leave request, the field device returns a leave response;
 - After the gateway device receiving the leave response forwarded by access devices from a field device, the network manager on the gateway device handles the leave response, updates the device list, and releases the short address and communication resources of the leaving field device; and the access device updates its MIB accordingly.

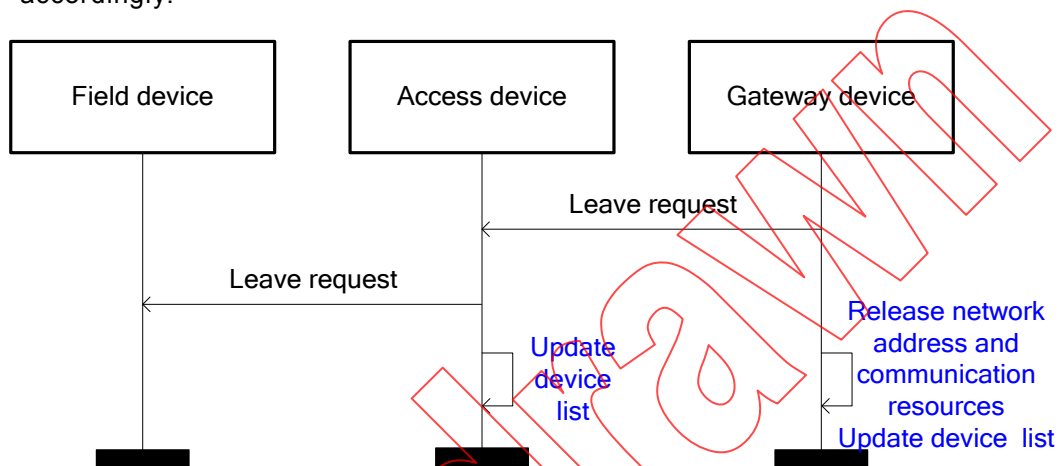


Figure 18 – Passive leave process of a field device

6.6 Network performance monitoring

6.6.1 Device status report

The field device periodically reports its device status to the gateway device (see DeviceList in 6.7.1.2.2 for the detailed device status). After the gateway device receives the device status report of a field device, the NM evaluates and diagnoses the device status. The device status report is used to detect abnormal status of a field device, such as low battery power, etc. The status report process of a field device is shown in Figure 19.

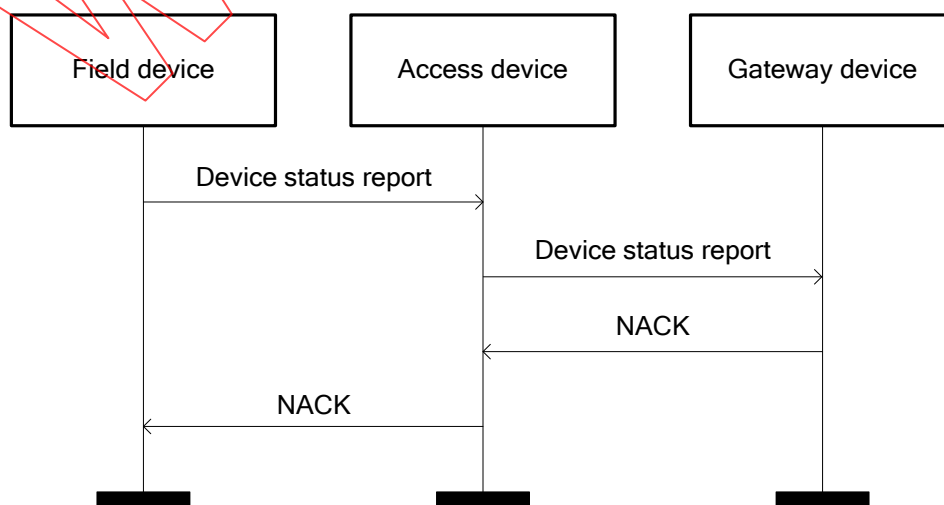


Figure 19 – Device status report process of field device

6.6.2 Channel condition report

The channel condition report is used for a field device to remotely report the channel condition to the NM (see ChannelConditionList in 6.7.1.2.2 for the detailed channel condition). The process of the channel condition report is shown in Figure 20.

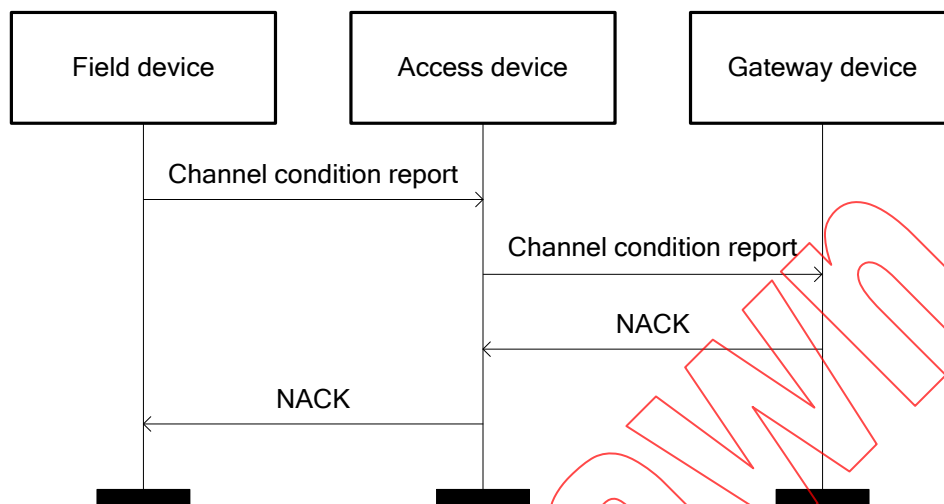


Figure 20 – Channel condition report process of field device

6.7 Management information base and services

6.7.1 Management information base

6.7.1.1 General

Items stored in the MIB are called attributes and are used for monitoring and configuring the WIA-FA network parameters. These attributes can be configured, accessed and updated by the NM.

According to the storage types, the attributes in the MIB are classified into three categories:

- Constant attribute: is unchangeable with time, such as the global unique 64-bit address. The constant attribute is set by manufacturer and should not be modified.
- Static attribute: is changed infrequently during the process of device operation, and can only be modified by NM, such as the period of reporting device status. The static attribute shall hold the previous setting value after the power-down/reboot.
- Dynamic attribute: its value is changed frequently without any external command. The dynamic attribute shall recover to the default value set by manufacturer after the power-down/reboot.

According to the attribute data types, the attributes in the MIB are divided into unstructured attributes and structured attributes.

There are two types of access control to attributes in the MIB:

R (Read), which means the value of the attribute can be read by other devices in WIA-FA network; and

W (Write), which means that the value of attribute can be modified by other devices in WIA-FA network.

According to the implementation requirements, the attributes in the MIB are divided into mandatory attributes and optional attributes.

Attributes in MIB are identified by AttributeID.

6.7.1.2 MIB attributes

6.7.1.2.1 Unstructured attributes

Unstructured attributes are listed in Table 14. Unstructured attributes are unique in whole WIA-FA network.

Table 14 – Unstructured attributes

Attribute ID	Attribute name	Data type	Valid range	Access type	Storage type	Default value	Device type	Description
0	PriGwFailureTime	TimeData	0 to $(2^{64}-1)$	R/W	S	10	Gateway device	The maximal duration without heartbeat signal (in μ s)
1	AddressTypeFlag	Unsigned8	0 to 255	R/W	S	0	All devices	0 = 8-bit short address; 1 = 16-bit short address
2	MaxPayloadLength	Unsigned16	0 to $(2^{16}-1)$	R/W	S	1000	All devices	Maximum length of the DLL payload (in octet)
3	NACKCount	Unsigned8	0 to 255	R/W	S	1	All devices	Number of broadcast NACKs
4	NetworkID	Unsigned8	0 to 255	R/W	S	0	All devices	Network identifier, used for identifying multiple coexisting networks
5	BitMap	Bit Field	0 to $(2^{24}-1)$	R/W	S	0	All devices	Channel bitmap, indicating used modulation mechanism and channel states: bit 0 to 3: modulation mechanism; bit 4 to 17: channel state, 0 stands for unavailable channel, 1 stands for available channel; others are reserved. See 7.3.3 for details of BitMap coding.
6	DevStaRptCycle	Unsigned16	0 to 65 535	R/W	S	10	Gateway devices and field devices	Cycle of device status report (in length of default superframe)
7	ChaStaRptCycle	Unsigned16	0 to 65 535	R/W	S	10	Gateway devices and field devices	Cycle of channel status report (in length of default superframe)
8	LossConnectDuration	Unsigned24	0 to $(2^{24}-1)$	R/W	S	30	Gateway device and field devices	If a WIA-FA device does not receive any packet from a neighbour device during LossConnectDuration, it shall judge that the neighbour device has abnormally left the WIA-FA network (in length of default superframe)
9	KeyupdateDuration	Unsigned8	0 to 255	R/W	S	24	All devices	Cycle of key update (in hour)
10	TimeSlotDuration	Unsigned16	0 to 65 535	R/W	S	200	All devices	Timeslot length (in μ s)