

DIN EN 62948

ICS 25.040.40; 35.110

**Industrielle Kommunikationsnetze –
Funk-Kommunikationsnetze und Kommunikationsprofile –
WIA-FA
(IEC 62948:2017);
Englische Fassung EN 62948:2017**

Industrial networks –
Wireless communication network and communication profiles –
WIA-FA
(IEC 62948:2017);
English version EN 62948:2017

Réseaux industriels –
Réseau de communication sans fil et profils de communication –
WIA-FA
(IEC 62948:2017);
Version anglaise EN 62948:2017

Gesamtumfang 204 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2017-08-31 angenommene Europäische Norm als DIN-Norm ist 2018-08-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 62948:2016-05.

Für dieses Dokument ist das nationale Arbeitsgremium K 956 „Industrielle Kommunikation“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom SC 65C „Industrial networks“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu dieser Publikation angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Das Präsidium des DIN hat mit Präsidialbeschluss 1/2004 festgelegt, dass DIN-Normen, deren Inhalt sich auf internationale Arbeitsergebnisse der Informationsverarbeitung gründet, unter bestimmten Bedingungen allein in englischer Sprache veröffentlicht werden dürfen. Diese Bedingungen sind für die vorliegende Norm erfüllt.

Da sich die Benutzer der vorliegenden Norm der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der EN 62948 veröffentlicht. Zu deren Abschnitt 1, Anwendungsbereich, und Unterabschnitt 3.1, der die Begriffe festlegt, wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA der vorliegenden Norm hinzugefügt. Für die meisten der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Diese Norm steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Nationaler Anhang NA (informativ)

Auszugsweise Übersetzung^{N1}

1 Anwendungsbereich

Diese Internationale Norm spezifiziert die Systemarchitektur und das Kommunikationsprotokoll der WIA-FA (en: Wireless Networks for Industrial Automation – Factory Automation; de: drahtloses Netzwerk für die Industrieautomation – Fabrikautomation) auf der Basis der IEEE STD 802.11-2012 Physical Layer (PHY).

Diese Norm gilt für Funk-Netzwerkssysteme für die Messung, Steuerung und Überwachung der Fabrikautomation.

3 Begriffe, Abkürzungen und Konventionen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: unter <<http://www.electropedia.org/>>
- ISO Online Browsing Platform: unter <<http://www.iso.org/obp>>

3.1.1

absolute Zeitschlitznummer

(en: absolute timeslot number)

Anzahl der vom Beginn des Netzwerks gezählten Zeitschlitz

Anmerkung 1 zum Begriff: Der Wert ist die Sequenznummer des aktuellen Zeitschlitzes, die bei jedem Zeitschlitz um eins erhöht wird. Nach Erreichen des höchsten Werts ($2^{48} - 1$) wird der Wert auf 0 zurückgesetzt.

3.1.2

Anschlussgerät

(en: access device)

im Industrie-Feld installiertes Gerät, das Sensordaten, Alarme und auf das Netzwerkmanagement bezogene Informationen der Feldgeräte an Gateway-Geräte weiterleitet oder Steuerungssignale, Managementinformationen und Konfigurationsinformationen des Gateway-Geräts an Feldgeräte weiterleitet

3.1.3

Aggregation

(en: aggregation)

Prozess der Zusammenfassung einer Vielzahl von Benutzeranwendungsobjekten in einem Paket oder der Zusammenfassung mehrerer Rahmen in einem Rahmen

3.1.4

Anwendungskonfiguration

(en: application configuration)

Konfigurationsverfahren für Benutzeranwendungsprozesse in Feldgeräten zur Erfüllung einer Fabrikautomatisierungsaufgabe

^{N1} Nationale Fußnote: Die Nummerierung aus IEC 62948:2017-07 wurde beibehalten.

3.1.5

Anwendungsteilschicht

(en: application sub-layer)

Protokoll-Teilschicht, die Daten- und Managementdienste für die Anwendungsschicht bereitstellt

3.1.6

Backoff

(en: backoff)

Prozess des Wiederholversuchs bei einem Rahmen in einem festgelegten Zeitschlitz für erneute Übertragung, wenn die erste Übertragung fehlschlägt

3.1.7

Warnsignal

(en: beacon)

besondere Rahmen-Rundsendung (en: Broadcast) durch das Anschlussgerät im WIA-FA-Netzwerk

Anmerkung 1 zum Begriff: Um an einem WIA-FA-Netzwerk teilzunehmen, muss ein neues Feldgerät zuerst auf Warnsignale achten.

3.1.8

Kanal

(en: channel)

Medium, das zur Übertragung eines Rahmens vom Absender zu einem Empfänger verwendet wird

3.1.9

Koexistenz

(en: coexistence)

Zustand, in dem alle Funkkommunikationssysteme einer Anlage das gleiche Medium teilen und dennoch alle ihre Anforderungen an die Anwendungskommunikation erfüllen

Anmerkung 1 zum Begriff: Dies stimmt mit der Definition von Koexistenz in IEEE 802.15.2-2003 überein.

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

3.1.10

Kommunikationsressource

(en: communication resource)

Kanäle und Zeitschlitze, die zum Transport eines Rahmens verwendet werden

3.1.11

Disaggregation

(en: disaggregation)

Prozess des Zerlegens des zusammengefassten Paketes in Daten von mehreren Benutzeranwendungsobjekten, oder Zerlegen des zusammengefassten Rahmens in mehrere Rahmen

3.1.12

Feldgerät

(en: field device)

in einem Industriefeld installiertes und mit Sensoren und Aktoren verbundenes Gerät, das für die Übertragung von Felddaten und den Empfang von Steuerungsbefehlen verwendet wird

3.1.13

Gateway-Gerät

(en: gateway device)

Gerät, welches das WIA-FA-Netzwerk mit anderen Anlagennetzwerken verbindet

3.1.14

handgehaltenes Gerät

(en: handheld device)

transportables Gerät, das für die Netzwerkbereitstellung und die Firmware-Aktualisierung verwendet wird

3.1.15**Heartbeat-Signal**

(en: heartbeat signal)

ein vom in Betrieb befindlichen Gateway-Gerät an die redundanten Gateway-Geräte gesendetes Signal, das anzeigt, dass das Gateway-Gerät ordnungsgemäß funktioniert

3.1.16**Host-Computer**

(en: host computer)

Computer für Konfigurations-, Überwachungs- und Steuerungsaufgaben

3.1.17**Verbinden**

(en: join)

Prozess, bei dem ein WIA-FA-Gerät versucht, am WIA-FA-Netzwerk teilzunehmen, und es ihm gestattet wird

3.1.18**Verknüpfung**

(en: link)

Verbindungspfad zwischen zwei benachbarten Geräten in einem WIA-FA-Netzwerk, der aus einem Parametersatz für eine Hop-Kommunikation besteht

Anmerkung 1 zum Begriff: Parameter einer Verknüpfung beinhalten Verknüpfungsbezeichner (en: link identifier), Verknüpfungstyp, Zieladresse, relative Zeitschlitznummer, aktueller Kanalindex und Superrahmen-Bezeichner.

3.1.19**Langadresse**

(en: long address)

EUI-64-Bit, was das Gerät eindeutig im WIA-FA-Netzwerk kennzeichnet

Anmerkung 1 zum Begriff: Eine Langadresse wird vom Hersteller zugewiesen.

3.1.20**Netzwerkadresse**

(en: network address)

vorzeichenlose 8-Bit- oder 16-Bit-Zahl, welche das Gerät im WIA-FA-Netzwerk eindeutig kennzeichnet, auch Kurzadresse genannt

3.1.21**Netzwerkconfiguration**

(en: network configuration)

Prozess des Konfigurierens von Parametern für WIA-FA-Netzwerke zur Aufrechterhaltung von Netzwerkbetrieb und -kommunikation

3.1.22**Netzwerkmanager**

(en: network manager)

logische Rolle für das Konfigurieren des Netzwerks, die Zuweisung von Kommunikationsressourcen, die Überwachung und die Berichterstattung über das Betriebsverhalten des Netzwerks

Anmerkung 1 zum Begriff: Es gibt nur einen Netzwerkmanager in einem WIA-FA-Netzwerk.

3.1.23**passives Verlassen**

(en: passive leaving)

Prozess, bei dem ein mit dem WIA-FA-Netzwerk verbundenes Gerät durch das Gateway-Gerät zum Verlassen des WIA-Netzwerks aufgefordert wird

3.1.24

primäres Gateway-Gerät

(en: primary gateway device)

in einem WIA-FA-Netzwerk in Betrieb befindliches Gateway-Gerät

3.1.25

Bereitstellung

(en: provisioning)

Prozess des Vorkonfigurierens einiger statischer Informationen, welche Netzwerkbezeichner, Sicherheitsstufen, Verbindungsschlüssel und geteilte Schlüssel für WIA-FA-Geräte beinhalten

3.1.26

redundantes Gateway-Gerät

(en: redundant gateway device)

Sicherung für ein in Betrieb befindliches primäres Gateway-Gerät

3.1.27

relative Zeitschlitznummer

(en: relative timeslot number)

Anzahl der vom Beginn eines Superrahmens gezählten Zeitslitze

3.1.28

Sicherheitsmanager

(en: security manager)

logische Rolle für das Konfigurieren der Sicherheitsrichtlinien des gesamten Netzwerks, die Verwaltung von Schlüsseln und die Authentifizierung von Geräten

3.1.29

Superrahmen

(en: superframe)

Sammlung von Zeitslitzen, die gleichmäßig wiederholt auftreten

3.1.30

Zeitschlitz

(en: timeslot)

Basiszeiteinheit für den Datenaustausch in einem WIA-FA-Netzwerk

Anmerkung 1 zum Begriff: Seine Dauer kann im WIA-FA-Netzwerk konfiguriert werden.

English Version

Industrial networks – Wireless communication network
and communication profiles – WIA-FA
(IEC 62948:2017)

Réseaux industriels – Réseau de communication sans fil
et profils de communication – WIA-FA
(IEC 62948:2017)

Industrielle Kommunikationsnetze –
Funk-Kommunikationsnetze und Kommunikationsprofile –
WIA-FA
(IEC 62948:2017)

This European Standard was approved by CENELEC on 2017-08-31. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 65C/877/FDIS, future edition 1 of IEC 62948, prepared by SC 65C "Industrial networks" of IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62948:2017.

The following dates are fixed:

- latest date by which the document has to be (dop) 2018-06-01
implemented at national level by
publication of an identical national
standard or by endorsement
- latest date by which the national (dow) 2020-12-01
standards conflicting with the
document have to be withdrawn

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62948:2017 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following note has to be added for the standard indicated:

IEC 62657-2	NOTE	Harmonized as EN 62657-2.
-------------	------	---------------------------

CONTENTS

European foreword	2
1 Scope	13
2 Normative references	13
3 Terms, definitions, abbreviated terms, and conventions	13
3.1 Terms and definitions	13
3.2 Abbreviated terms	16
3.3 Conventions	18
4 Data coding	19
4.1 Overview	19
4.2 Basic data type coding	20
4.2.1 Integer coding	20
4.2.2 Unsigned coding	20
4.2.3 Float coding	21
4.2.4 Octetstring coding	22
4.2.5 BitField coding	22
4.2.6 Bitstring coding	23
4.2.7 TimeData coding	23
4.2.8 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 General	24
5.1.2 Host computer	24
5.1.3 Gateway device	24
5.1.4 Access device	25
5.1.5 Field device	25
5.1.6 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	29
6.2.1 General	29
6.2.2 Network manager	31
6.2.3 Security manager	31
6.2.4 Network management module	31
6.2.5 Security management module	31
6.2.6 DMAP state machines	31
6.3 Addressing and address assignment	44
6.4 Communication resource allocation	44
6.4.1 General	44
6.4.2 Communication resource allocation	44
6.5 Joining and leave process of field device	46

6.5.1	Join process of a field device	46
6.5.2	Communication resource allocation to field device	47
6.5.3	Leaving process of a field device.....	48
6.6	Network performance monitoring	49
6.6.1	Device status report.....	49
6.6.2	Channel condition report	49
6.7	Management information base and services	50
6.7.1	Management information base	50
6.7.2	MIB services	60
7	Physical layer	63
7.1	General	63
7.2	General requirements based on IEEE STD 802.11-2012	63
7.3	Additional requirements	64
7.3.1	General	64
7.3.2	Frequency band	64
7.3.3	Channel bitmap.....	64
7.3.4	Transmit power	66
7.3.5	Data rate	66
8	Data Link Layer	66
8.1	General	66
8.1.1	DLL functions	66
8.1.2	Protocol architecture	66
8.1.3	WIA-FA superframe	67
8.1.4	Communication based on multiple access devices	69
8.1.5	Time synchronization	71
8.1.6	Frame aggregation/disaggregation	72
8.1.7	Fragmentation and reassembly	73
8.1.8	Retransmission.....	73
8.2	Data link sub-layer data services	76
8.2.1	General	76
8.2.2	DLDE-DATA.request primitive	76
8.2.3	DLDE-DATA.indication primitive	77
8.2.4	Time sequence of DLL data service.....	78
8.3	Data link sub-layer management services.....	79
8.3.1	General	79
8.3.2	Network discovery services	80
8.3.3	Time synchronization services.....	82
8.3.4	Device joining services	84
8.3.5	Device status report services	87
8.3.6	Channel condition report services	89
8.3.7	Remote attribute get services.....	91
8.3.8	Remote attribute set services	95
8.3.9	Device leaving services.....	99
8.4	DLL frame formats	101
8.4.1	General frame format.....	101
8.4.2	Date frame format.....	102
8.4.3	Aggregation frame format.....	103
8.4.4	NACK frame format.....	103

8.4.5	GACK frame format.....	103
8.4.6	Beacon frame format.....	104
8.4.7	Join request frame format.....	105
8.4.8	Join response frame format.....	105
8.4.9	Leave request frame format.....	105
8.4.10	Leave response frame format.....	105
8.4.11	Device status report frame format.....	105
8.4.12	Channel condition report frame format.....	106
8.4.13	Time synchronization request frame format.....	106
8.4.14	Time synchronization response frame format.....	106
8.4.15	Remote attribute get request frame format.....	106
8.4.16	Remote attribute get response frame format.....	107
8.4.17	Remote attribute set request frame format.....	107
8.4.18	Remote attribute set response frame format.....	108
8.5	Data link layer state machines.....	108
8.5.1	DLL state machine of access device.....	108
8.5.2	DLL state machine of field device.....	116
8.5.3	Functions used in DLL state machines.....	122
9	Wired specifications between GW and AD.....	123
9.1	Overview.....	123
9.2	Join process of access device.....	123
9.3	Frame formats between GW and AD.....	123
9.4	Communication based on multiple access device.....	126
10	Application Layer.....	126
10.1	Overview.....	126
10.2	AL protocol stack.....	126
10.3	AL functions.....	127
10.3.1	Data functions.....	127
10.3.2	Management functions.....	127
10.3.3	Communication models.....	128
10.4	Application data.....	128
10.4.1	General.....	128
10.4.2	Attribute data.....	128
10.4.3	Process data.....	128
10.4.4	Event data.....	129
10.5	User application process.....	130
10.5.1	General.....	130
10.5.2	User application object.....	131
10.5.3	IO data image on gateway device.....	131
10.5.4	Alarm mechanism.....	132
10.5.5	Application configuration.....	133
10.6	Application services.....	139
10.6.1	Confirmed services and unconfirmed services.....	139
10.6.2	Read service.....	140
10.6.3	Write service.....	142
10.6.4	Publish service.....	144
10.6.5	Report service.....	144
10.6.6	Report ACK service.....	145

10.6.7	Start service	147
10.6.8	Stop service	147
10.7	Application sub-layer.....	148
10.7.1	Overview	148
10.7.2	ASL data service.....	148
10.7.3	ASL management service.....	151
10.7.4	ASL message format.....	153
11	Security.....	172
11.1	General	172
11.1.1	Security management architecture	172
11.1.2	Security functions	174
11.1.3	Keys.....	174
11.2	Security services.....	175
11.2.1	General	175
11.2.2	Key establish service	176
11.2.3	Key update service	178
11.2.4	Security alarm service.....	180
11.3	Secure join	182
11.3.1	General	182
11.3.2	Secure join process of FD	182
11.4	Key management.....	183
11.4.1	General	183
11.4.2	Key establish process	183
11.4.3	Key update process	184
11.5	DLL secure communication	186
11.6	Security alarm.....	187
11.7	Secure frame format	187
11.7.1	General secure DLL frame format.....	187
11.7.2	Secure aggregation frame format	188
11.7.3	Key establish request frame format	189
11.7.4	Key establish response frame format.....	189
11.7.5	Key update request frame format	189
11.7.6	Key update response frame format.....	189
11.7.7	Security alarm request frame format.....	190
Annex A (informative)	Security strategy for WIA-FA network	191
A.1	Risk analysis for WIA-FA network.....	191
A.2	Security principles for WIA-FA network.....	191
A.3	Security objectives for WIA-FA network	191
A.4	Security grade of WIA-FA network.....	191
Annex B (informative)	Regional modification for compliance with ETSI standards.....	193
B.1	General	193
B.2	Compliance with ETSI EN 300 440-2 V1.4.1	193
B.3	Compliance with ETSI EN 300 328V1.9.1	193
Bibliography		197
Annex ZA (normative)	Normative references to international publications with their corresponding European publications.....	198

Figure 1 – Conventions used for state machines.....	18
Figure 2 – Integer coding	20
Figure 3 – Unsigned coding	20
Figure 4 – Single float coding.....	21
Figure 5 – Double float coding	22
Figure 6 – WIA-FA redundant star topology	26
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	28
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 sub-state machine of gateway device for each field device.....	32
Figure 14 – DMAP state machine of a field device	36
Figure 15 – DMAP state machine of an access device	39
Figure 16 – Long address structure of device	44
Figure 17 – Join process of field device.....	47
Figure 18 – Communication resource allocation process for a field device.....	48
Figure 19 – Passive leave process of a field device	49
Figure 20 – Device status report process of field device	49
Figure 21 – Channel condition report process of field device.....	50
Figure 22 – BitMap format.....	65
Figure 23 – WIA-FA DLL protocol architecture	67
Figure 24 – The template of timeslot	67
Figure 25 – WIA-FA default superframe.....	68
Figure 26 – WIA-FA superframe	69
Figure 27 – The example of WIA-FA devices multi-channel communication	69
Figure 28 – An example of beacon communication based on multiple ADs	70
Figure 29 – Process of one-way time synchronization	71
Figure 30 – Process of two-way time synchronization	72
Figure 31 – Aggregation frame payload format	73
Figure 32 – Example of NACK-based retransmission mode.....	74
Figure 33 – Example of multi-unicast retransmission mode	75
Figure 34 – Example of multi-broadcast retransmission mode	75
Figure 35 – Example of GACK-based timeslot backoff mode	76
Figure 36 – Time sequence of period data service from FD to GW	78
Figure 37 – Time sequence of other data service from FD to GW.....	79
Figure 38 – Time sequence of data service from GW to FD.....	79
Figure 39 – Network discovery process	81
Figure 40 – Time synchronization process.....	84
Figure 41 – Device join process	87
Figure 42 – Device status report process.....	89

Figure 43 – Channel condition report process.....	90
Figure 44 – Remote attribute get process.....	95
Figure 45 – Remote attribute set process.....	99
Figure 46 – Device leave process	100
Figure 47 – General frame format	101
Figure 48 – DLL frame header	101
Figure 49 – DLL frame control format.....	101
Figure 50 – DLL Date frame format	102
Figure 51 – DLL Aggregation frame format.....	103
Figure 52 – NACK frame format	103
Figure 53 – NACK information.....	103
Figure 54 – GACK frame format.....	103
Figure 55 – GACK_Struct Structure.....	104
Figure 56 – DLL Beacon frame format.....	104
Figure 57 – Shared timeslot count.....	104
Figure 58 – DLL join request frame format	105
Figure 59 – DLL join request frame format	105
Figure 60 – DLL leave request frame format.....	105
Figure 61 – DLL leave response frame format	105
Figure 62 – DLL Device status report frame format.....	106
Figure 63 – DLL Channel condition report frame format.....	106
Figure 64 – DLL time synchronization request frame format.....	106
Figure 65 – DLL time synchronization response frame format	106
Figure 66 – DLL Remote attribute get request frame format.....	107
Figure 67 – DLL remote attribute get response frame format.....	107
Figure 68 – DLL Remote attribute set request frame format.....	108
Figure 69 – DLL remote attribute set response frame format.....	108
Figure 70 – DLL state machine of access device	109
Figure 71 – DLL state machine of field device	117
Figure 72 – General frame format between GW and AD.....	123
Figure 73 – AL within the protocol architecture of WIA-FA	127
Figure 74 – The relationships between UAPs and DAPs	131
Figure 75 – User application objects in a field device.....	131
Figure 76 – Example of IO data images on the gateway device.....	132
Figure 77 – C/S VCR relationships between GW and FDs.....	135
Figure 78 – P/S VCR relationships between GW and FDs.....	136
Figure 79 – R/S VCR relationships between GW and FDs.....	137
Figure 80 – Application configuration procedure for a field device.....	138
Figure 81 – Example of UAO data aggregation and disaggregation process	139
Figure 82 – Read request message format.....	140
Figure 83 – Read positive response message format.....	141
Figure 84 – Read negative response message format.....	141

Figure 85 – Read service process	142
Figure 86 – Write request message format	142
Figure 87 – Write negative response message format	142
Figure 88 – Write service process	143
Figure 89 – Publish request message format	144
Figure 90 – Publish process from FD to GW	144
Figure 91 – Publish process from GW to FD	144
Figure 92 – Report request message format	145
Figure 93 – Report service process	145
Figure 94 – Report ACK request message format	145
Figure 95 – Report ACK positive response message format	146
Figure 96 – Report ACK negative response message format	146
Figure 97 – Report ACK service process	146
Figure 98 – Start service process	147
Figure 99 – Stop service process	148
Figure 100 – ASL general message format	153
Figure 101 – Format of Message control field	153
Figure 102 – Confirmed application service primitives among layers	155
Figure 103 – Unconfirmed application service primitives among layers	156
Figure 104 – ASL management service primitives between ASL and UAP	156
Figure 105 – State transition diagram of AMCL	157
Figure 106 – State transition diagram of AMSV	159
Figure 107 – State transition diagram of AMPB	162
Figure 108 – State transitions diagram of AMSB	165
Figure 109 – State transitions diagram of AMRS	169
Figure 110 – State transitions diagram of AMRK	170
Figure 111 – Security management architecture	173
Figure 112 – Life cycle of keys	175
Figure 113 – Format of NONCE	176
Figure 114 – Time sequence of key establishment	178
Figure 115 – Time sequence of key updating	180
Figure 116 – SecAlarnt_Struct structure	181
Figure 117 – Time sequence of security alarm	182
Figure 118 – Secure join process of field device	183
Figure 119 – Key establish process for field device	184
Figure 120 – Key update state machine for FD	185
Figure 121 – General secure DLL frame format	187
Figure 122 – Secure aggregation frame format	188
Figure 123 – Key establish request frame format	189
Figure 124 – Key establish response frame format	189
Figure 125 – Key update request frame format	189
Figure 126 – Key update response frame format	190

Figure 127 – Security alarm request frame format	190
Figure B.1 – Timeslot timing template	194
Table 1 – Conventions used for state transitions	19
Table 2 – Integer16 coding	20
Table 3 – Unsigned16 coding	21
Table 4 – Octetstring coding	22
Table 5 – Coding of BitField8 data with one octet	23
Table 6 – Coding of BitField16 data with two octets	23
Table 7 – Coding of BitField24 data with three octets	23
Table 8 – Bitstring coding	23
Table 9 – Network management functions	30
Table 10 – Security management functions	30
Table 11 – DMAP state transition of gateway device	32
Table 12 – DMAP sub-state transition of gateway device for each field device	33
Table 13 – DMAP state transition of a field device	36
Table 14 – DMAP state transition of an access device	40
Table 15 – Functions used in DMAP state machines	42
Table 16 – Unstructured attributes	51
Table 17 – Structured attributes	53
Table 18 – Superframe_StructStructure	53
Table 19 – Link_Struct Structure	54
Table 20 – ChanCon_Struct Structure	54
Table 21 – Device_Struct Structure	55
Table 22 – Key_Struct Structure	56
Table 23 – VcrEP_StructStructure	57
Table 24 – UAOCClassDesc_Struct Structure	58
Table 25 – ProDataDesc_Struct Structure	59
Table 26 – UAOWInstDesc_Struct Structure	60
Table 27 – DMAP-MIB-GET.request parameters	61
Table 28 – DMAP-MIB-GET.confirm parameters	61
Table 29 – DMAP-MIB-SET.request parameters	62
Table 30 – DMAP-MIB-SET.confirm parameters	63
Table 31 – PHY protocol selection	63
Table 32 – Coding of Modulation modes	65
Table 33 – Channel indices	65
Table 34 – Data rate	66
Table 35 – Parameters of timeslot template	68
Table 36 – DLDE-DATA.request primitive parameters	77
Table 37 – DLDE-DATA.indication primitive parameters	78
Table 38 – Management services	80
Table 39 – DLME-DISCOVERY.request parameters	80
Table 40 – DLME-DISCOVERY.confirm parameters	81
Table 41 – BeaconDescription_Struct parameters	81
Table 42 – DLME-TIME-SYN.indication parameters	82

Table 43 – DLME-TIME-SYN.response parameters.....	83
Table 44 – DLME-TIME-SYN.confirm parameters	83
Table 45 – DLME-JOIN.request parameters	85
Table 46 – DLME-JOIN.indication parameters	85
Table 47 – DLME-JOIN.response parameters.....	86
Table 48 – DLME-JOIN.confirm parameters.....	86
Table 49 – DLME-DEVICE-STATUS.request parameters	87
Table 50 – DLME-DEVICE -STATUS.indication parameters	88
Table 51 – DLME-DEVICE -STATUS.confirm parameters.....	88
Table 52 – DLME-CHANNEL-CONDITION.request parameters	89
Table 53 – DLME-CHANNEL-CONDITION.indication parameters	90
Table 54 – DLME-CHANNEL-CONDITION.confirm parameters	90
Table 55 – DLME-INFO-GET.request parameters	91
Table 56 – DLME-INFO-GET.indication parameters	92
Table 57 – DLME-INFO-GET.response parameters.....	93
Table 58 – DLME-INFO-GET.confirm parameters	94
Table 59 – DLME-INFO-SET.request parameters	96
Table 60 – DLME-INFO-SET.indication parameters	97
Table 61 – DLME-INFO-SET.response parameters	97
Table 62 – DLME-INFO-SET.confirm parameters.....	98
Table 63 – DLME-LEAVE.request parameters	99
Table 64 – DLME-LEAVE.confirm parameters.....	100
Table 65 – Frame type coding.....	102
Table 66 – Addressing mode subfields	102
Table 67 – DLL state transition of access device	109
Table 68 – DLL state transition of field device	117
Table 69 – Functions used in DLL state machines	123
Table 70 – Frames between GW and AD	124
Table 71 – Payload of AD join request frame	125
Table 72 – Payload of AD join response frame	125
Table 73 – Payload of GW requesting AD to send GACK	126
Table 74 – Definition of GACKInfo_Struct.....	126
Table 75 – Payload of GW requesting AD to send NACK	126
Table 76 – Communication models between gateway device and field devices	128
Table 77 – EventData definition	129
Table 78 – UAO events definitions	130
Table 79 – VCR attribute configuration for a field device.....	134
Table 80 – Application services used by UAPs	140
Table 81 – Error code definition for Read negative response message.....	141
Table 82 – Error code definition for Write negative response message.....	143
Table 83 – Error code definition for Report ACK negative response	146
Table 84 – ASLDE-DATA.request primitive parameter definitions.....	149
Table 85 – ASLDE-DATA.indication primitive parameter definitions.....	150
Table 86 – ASLDE-DATA.response primitive parameter definitions	150
Table 87 – ASLDE-DATA.confirm primitive parameter definitions	151

Table 88 – ASLME-VcrActive.request primitive parameter definitions	152
Table 89 – ASLME-VcrDeactive.request primitive parameter definitions	152
Table 90 – ASLME-SignalEvent.request primitive parameter definitions	152
Table 91 – Service Identifier subfield definition.....	153
Table 92 – Message Type subfield definition	154
Table 93 – Confirmed service primitives exchanged between ASL and other layers.....	155
Table 94 – Unconfirmed service primitives exchanged between ASL and other layers	156
Table 95 – ASL management service primitives between ASL and UAP	157
Table 96 – State transition table of AMCL	158
Table 97 – State transition table of AMSV	160
Table 98 – State transition table of AMPB	162
Table 99 – State transitions table of AMSB	166
Table 100 – State transitions table of AMRS	169
Table 101 – State transitions table of AMRK	170
Table 102 – All Functions used in ASLM	171
Table 103 – Parameters for KEY-ESTABLISH.request.....	176
Table 104 – KeyMaterial_Struct structure	176
Table 105 – Parameters for KEY-ESTABLISH.indication.....	177
Table 106 – Parameters for KEY-ESTABLISH.response	177
Table 107 – Parameters for KEY-ESTABLISH.confirm	178
Table 108 – Parameters for KEY-UPDATE.request.....	178
Table 109 – Parameters for KEY-UPDATE.indication.....	179
Table 110 – Parameters for KEY-UPDATE.response	179
Table 111 – Parameters for KEY-UPDATE.confirm	180
Table 112 – Parameters for SEC-ALARM.request.....	181
Table 113 – Parameters for SEC-ALARM.indication	181
Table 114 – Key update states.....	184
Table 115 – Key update state transition	185
Table 116 – Keys used in DLL secure communication	187
Table 117 – Available security levels for DLL	188
Table A.1 – Security grades for WIA-FA network	192
Table B.1 – Applicable EN 300 440-2 requirements list.....	193
Table B.2 – Applicable EN 300 328 requirements list.....	194
Table B.3 – Timeslot timing definitions and calculations	195
Table B.4 – TxMaxPHYPacket of FHSS.....	195
Table B.5 – TxMaxPHYPacket of DSSS/HR-DSSS	195
Table B.6 – TxMaxMPDU of OFDM	196

1 Scope

This International Standard 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 document applies to wireless network systems for factory automation measuring, monitoring and control.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. 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

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, abbreviated terms, and conventions

3.1 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1.1

absolute timeslot number

number of timeslots counted from the start of the network

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

3.1.2

access device

device installed in the industrial field, which forwards the sensor data, alarms and network management related information of the field devices to the gateway device, or forwards control signals, management information and configuration information of the gateway device to field devices

3.1.3

aggregation

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

3.1.4

application configuration

configuration procedure for user application processes in field devices to finish a factory automation task

3.1.5

application sub-layer

protocol sub-layer 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 previous transmission fails

3.1.7

beacon

special frame broadcasted by the access devices in the WIA-FA network

Note 1 to entry: To join the WIA-FA network, a new field device has to 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

wireless communication coexistence

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

Note 1 to entry: This is consistent with the definition of coexistence in IEEE 802.15.2-2003.

[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 the industrial field and connected to sensors or 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 signal

signal sent by the primary gateway device to the redundant ones, which indicates the gateway device is operating properly

3.1.16

host computer

computer that is used for configuration, monitoring, and controlling

3.1.17

joining

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

3.1.18

link

interconnecting path between two neighbouring devices in the WIA-FA network, which consists of a set of parameters for one hop communication

Note 1 to entry: Parameters of link include link identifier, link type, active timeslot, peer address, relative timeslot number, current channel index, and superframe identifier.

3.1.19

long address

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

Note 1 to entry: A long address is assigned by a manufacturer.

3.1.20

network address

8-bit or 16-bit unsigned integer uniquely identifying the device in the WIA-FA network, which 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 configuring the network, allocating communication resources, monitoring and reporting network status

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

3.1.23

passive leaving

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

3.1.24

primary gateway device

gateway device currently operating in a WIA-FA network

Note 1 to entry: A WIA-FA network has only one primary gateway device.

3.1.25

provisioning

process of pre-configuring some static information that includes network identifier, security level, join key, and shared key for the WIA-FA devices

3.1.26

redundant gateway device

hot backup of the primary gateway device

3.1.27

relative timeslot number

number of timeslots counted from the start of a superframe

3.1.28

security manager

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

3.1.29

superframe

collection of timeslots cyclically repeating at a constant rate

3.1.30

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 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

ACK	Acknowledgement
AI	Analog Input
AD	Access Device
AL	Application Layer
ASLDE	Application Sub-layer Digital Entity
ASLM	ASL State Machine
AMCL	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 timeSlot Number
APDU	Application Protocol Data Unit
ASDU	Application Service Data Unit
C/S	Client/Server
CCM*	Extension of counter with cipher block chaining message authentication code
DGO	DisaGgregation Object
DI	Digital Input
DLDE	Data Link layer Data Entity

DLL	Data Link Layer
DLME	Data Link layer Management Entity
DLPDU	Data link Layer Protocol Data Unit
DMAP	Device Management Application Process
DO	Digital Output
DoS	Deny of Service
DSSS	Direct Sequence Spread Spectrum
EIRP	Equivalent Isotropic Radiated Power
ENC	ENCryption
EUI-64	Extended Unique Identifier-64 bits
FCS	Frame Check Sequence
FD	Field Device
FDMA	Frequency Division Multiple Access
FHSS	Frequency-Hopping Spread Spectrum
GACK	Group ACK
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
NM	Network Manager
NONCE	Number used once, a value that has (at most) a negligible chance of repeating
NRT	Non-Real-Time
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open System Interconnection
PAGO	Packet Aggregation Object
PDU	Protocol Data Unit
PHY	PHYsical layer

PLCP	Physical Layer Convergence Protocol
P/S	Publisher/Subscriber
R/S	Report/Sink
SAP	Service Access Point
SM	Security Manager
SN	Sign Notation
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 document, the following conventions apply.

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

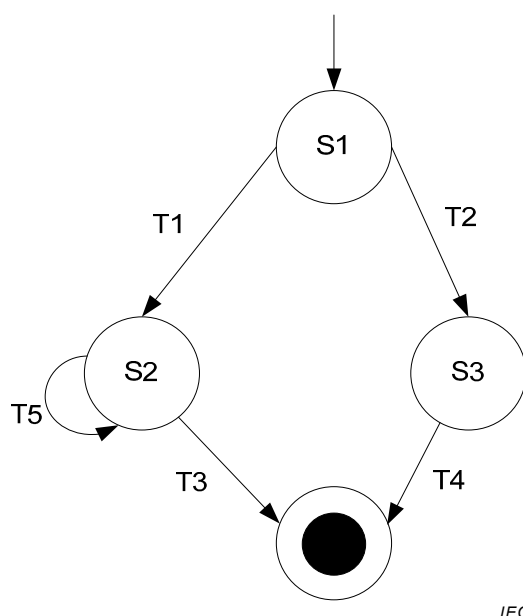


Figure 1 – Conventions used for state machines

The conventions used in the state machines are as follows:

- The labeled circles (S1, S2, ...) represent states that a device can be in; the solid cycle (●) represents the end state in which a device terminates its operations.
- State transitions are directed lines. They show which state a component leaves and which state it enters.
- A transition is labeled by (T1, T2, ...) standing for the events that trigger it and the corresponding actions (if present).

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:

- “:=” represents that 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.
- “==” represents a logical condition indicating that an item on the left is equal to an item on the right.
- “&&” represents logical "AND"
- “||” represents logical "OR"
- “!=” represents a logical condition indicating that 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 1

```
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 2

```
If (condition)
  actions
else if (condition)
  actions
else
  actions
```

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 structured data types.

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

4.2 Basic data type coding

4.2.1 Integer coding

The integer is a signed value, as shown in Figure 2. An example of Integer16 coding is shown in Table 2. For this data type, the MSB of the most significant octet is transmitted first.

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
Two's complement binary notation MSB is the bit followed by the first octet (SN) SN = 0: positive and 0 SN = 1: negative		

IEC

Figure 2 – Integer coding

Table 2 – Integer16 coding

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. An example of Unsigned16 coding is shown in Table 3. For this data type, the MSB of the most significant octet is sent first.

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

IEC

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		Short Real Number (32bits), see ISO/IEC/IEEE 60559							
coding		Short Real Number (32bits), see ISO/IEC/IEEE 60559							
		MSB LSB							
Bit		7	6	5	4	3	2	1	0
Octet		Exponent (E)							
1		SN	2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹
		Fraction (F)							
2		2 ⁰	2 ⁻¹	2 ⁻²	2 ⁻³	2 ⁻⁴	2 ⁻⁵	2 ⁻⁶	2 ⁻⁷
		Fraction (F)							
3		2 ⁻⁸	2 ⁻⁹	2 ⁻¹⁰	2 ⁻¹¹	2 ⁻¹²	2 ⁻¹³	2 ⁻¹⁴	2 ⁻¹⁵
		Fraction (F)							
4		2 ⁻¹⁶	2 ⁻¹⁷	2 ⁻¹⁸	2 ⁻¹⁹	2 ⁻²⁰	2 ⁻²¹	2 ⁻²²	2 ⁻²³
		SN: sign 0 =positive, 1=negative							

IEC

Figure 4 – Single float coding

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

IEC

Figure 5 – Double float coding

4.2.4 Octetstring coding

The Octetstring coding method is shown in Table 4. For the data with N octets, the MSB of the most significant octet 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 BitField coding

BitField data are used to encode single-bit data with fixed length. BitFieldn indicates BitField with n-bit length. The bit coding method 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 more than one octet, the most significant octet is first sent. There is a corresponding definition table for each bit of the data with BitField data type.

Table 5 – Coding of BitField8 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 BitField16 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 BitField24 data with three octets

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 Bitstring coding

Bitstring data are used to encode single-bit data with flexible length. The bit coding method is shown in Table 8. This data type is defined as a sequence of bits, and its bit length shall be specified concomitantly. Bitstring data are packed into octets and transferred as an octet sequence over network. The amount of octets is the maximum number of octets that can contain all bit values. For the data with more than one octet, the most significant octet of data is first sent.

Table 8 – Bitstring coding

octet	bit							
	7	6	5	4	3	2	1	0
1	X ^a	X	X	X	X	X	X	X
2	X	X	X	X	X	X	X	X
3	X	X	X	X	X	X	X	X
... ^b	... ^c							
^a MSB of the Bitstring data								
^b the amount of octets is the maximum number of octets that contain all bit values.								
^c the position of last bit (LSB) = 8 – bit length % 8								

4.2.7 TimeData coding

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

4.2.8 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 index. 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 Count.

5 WIA-FA overview

5.1 Device types

5.1.1 General

This document specifies five types of WIA-FA devices:

- a) host computer (HC);
- b) gateway device (GW);
- c) access device (AD);
- d) field device (FD);
- e) handheld device (HD).

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

NOTE Redundant gateway device is out of the scope of this document.

5.1.2 Host computer

Host computer is used to configure and monitor WIA-FA network for the operation, maintenance and management personnel. In addition, host computer may carry out controlling functions. Its implementation is out of the scope of this document.

5.1.3 Gateway device

The main functions of the gateway device shall be as follows:

- Providing interconnection interface 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 field devices through access devices, and exchanging information between field devices;
- Acting as the unique clock source in the WIA-FA network for network time synchronization;
- There is only one gateway device in one WIA-FA network with the unique NetworkID (see Table 16 for NetworkID).

5.1.4 Access device

The main functions of the access device shall be as follows:

- Receiving data from field devices and forwarding them to the gateway device;
- Forwarding the control commands of gateway device to field devices;
- Forwarding the management information and configuration information of the gateway device to field devices;
- Receiving alarms and network management information of field devices and forwarding them to the gateway device.

NOTE Access devices and the gateway device are connected by wire (see Clause 9). Their synchronization method is out of the scope of this document .

5.1.5 Field device

Field devices shall be installed in industrial field and connect sensors and actuators. Field devices shall send field application data and alarms to the gateway device, as well as receive configuration information, management information and control commands from the gateway device. The power supply modes of field devices include wired power supply, battery power supply, etc., which are out of the scope of this document.

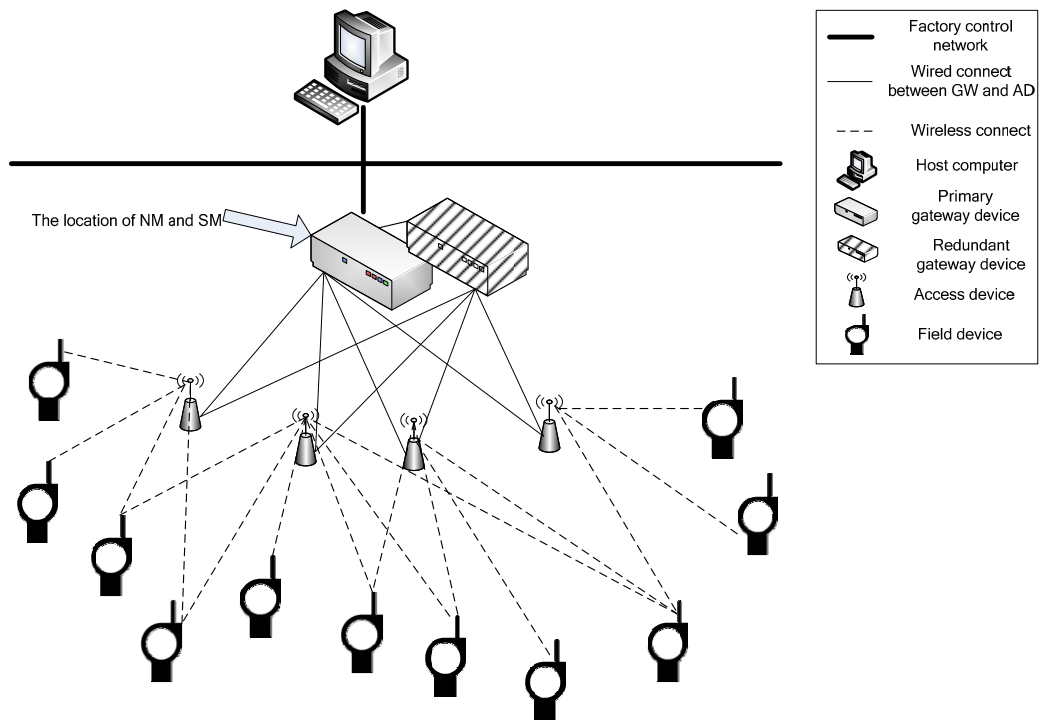
5.1.6 Handheld device

Handheld devices are portable devices that shall be used for provisioning field devices, access devices and the gateway device. A handheld device shall communicate only with its direct connected device using wired maintenance port. Provision parameters may include security level, join keys, shared keys (except security level 0), and network Identifier (ID).

NOTE Wired maintenance ports used by a handheld device could be RS232, RS485, USB, etc.

5.2 Network topology

As shown in Figure 6, WIA-FA supports redundant star topology. The center is comprised of one gateway device (redundant gateway device may exist) and one or several access devices, which means multiple access devices may communicate with the field devices in parallel and form multiple star topologies. These access devices shall have the same address (see 6.3) and are transparent for the field devices. Each access device forms a star topology with the field devices. See 8.1.4 for communication details of redundant star topology.



IEC

Figure 6 – WIA-FA redundant star topology

5.3 Protocol architecture

The WIA-FA network protocol is based on 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	↓ and ↑ ↓ and ↑ DLL Communication based on multiple ADs, TDMA, FDMA, retransmission, aggregation...
Network	Resolving network addresses, End- to- end routing of packets.	
Data link	Establishes data packet structure, framing, error detection, bus arbitration	
Physical	Mechanical / electrical connection. Transmits raw bit stream	PHY (IEEE STD 802.11-2012 PHY)

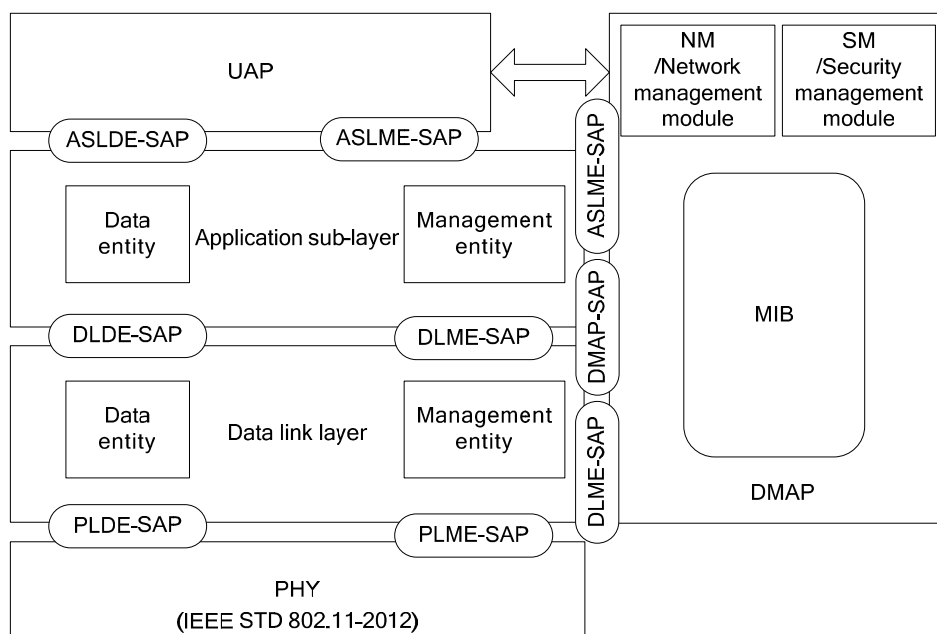
NOTE ↓ and ↑ indicate that the functionality of this layer, when present, can be included in the protocol layer that is nearest in the direction of the arrow. Thus network and transport functionality can be included in data link layer or application layer, while session and presentation functionality can be included in application layer, not in data link layer.

IEC

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 shall include 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 ASLME);
- Protocol layer interfaces: including data entity SAPs (DLDE-SAP and ASLDE-SAP) and management entity SAPs (DLME-SAP and ASLME-SAP).

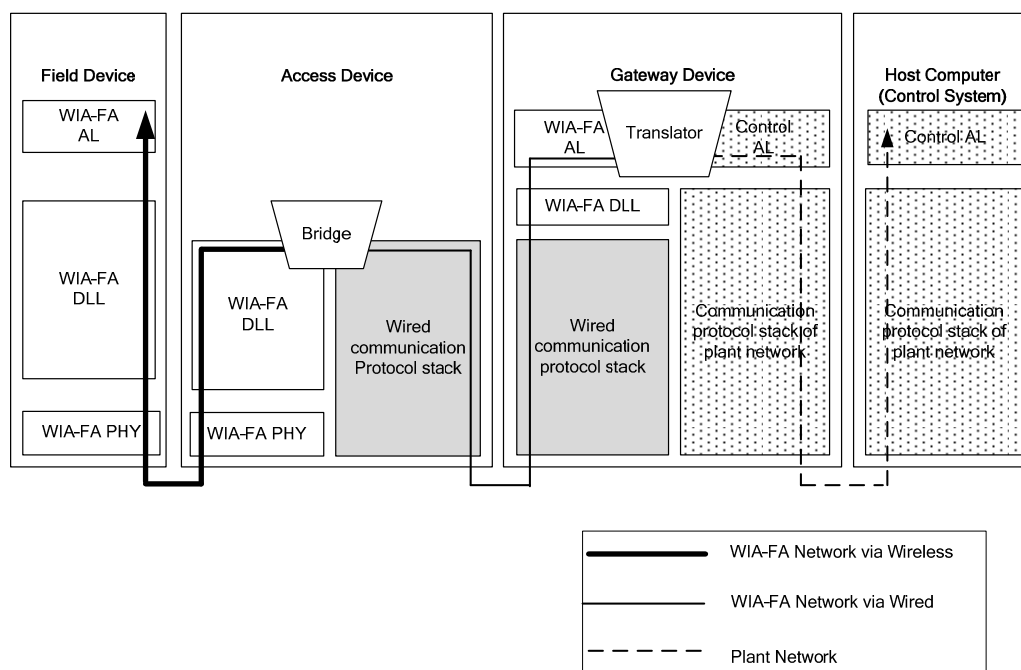


IEC

Figure 8 – Protocol architecture of WIA-FA

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

- A field device shall have PHY, DLL, and AL;
- An access device shall have PHY and DLL; an access device shall connect with the gateway device by wires;
- The gateway device shall only have AL and part of DLL. The AL of the gateway device shall communicate with AL of WIA-FA field devices. The AL of the gateway device may also communicate with AL of the plant network and translate ALs between the WIA-FA network and the plant network.



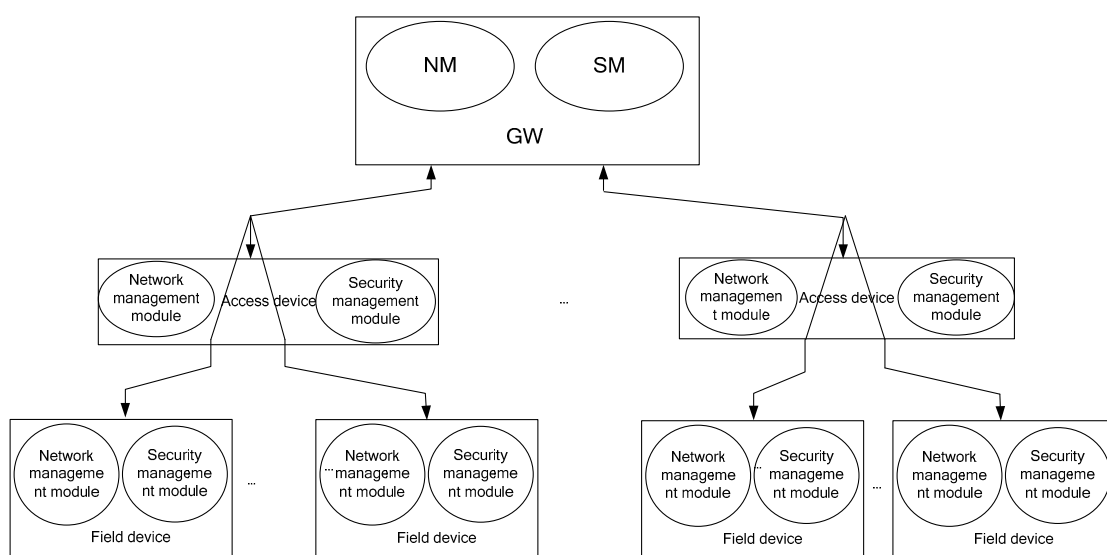
IEC

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 shall be 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 shall be implemented in field devices and access devices, which perform management functions together with the gateway device.



IEC

Figure 10 – System management scheme

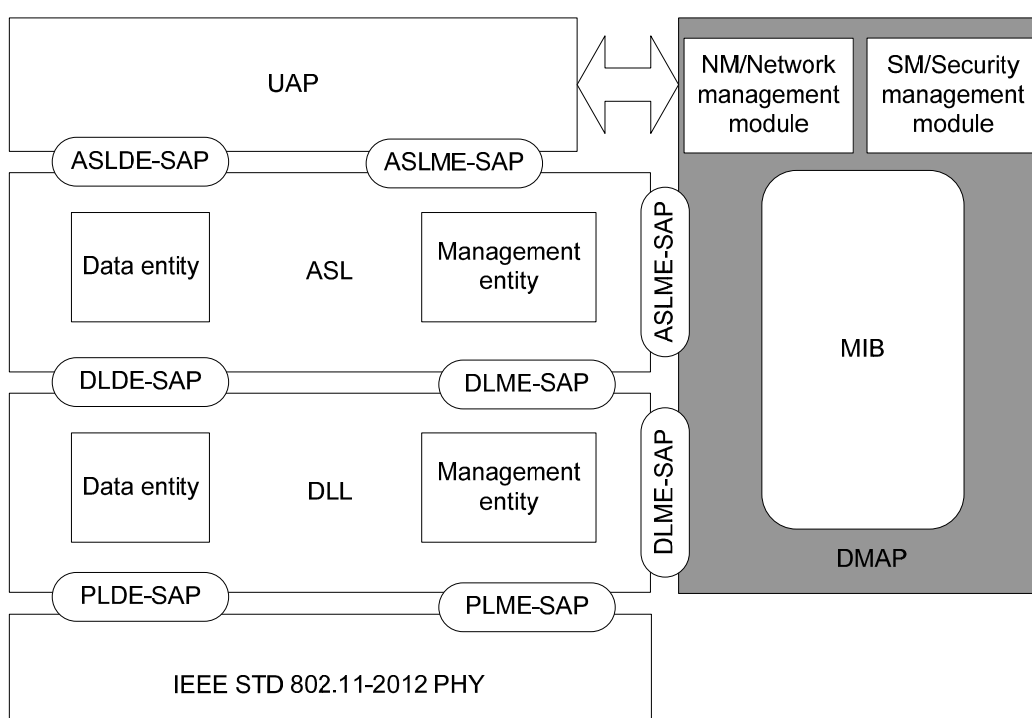
6.2 Device Management Application Process

6.2.1 General

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

- Network Manager (NM) of GW or the network management modules of ADs and FDs;
- Security Manager (SM) of GW or the security management modules of ADs and FDs;
- Management Information Base (MIB), storing all the attributes for network management and security management in WIA-FA network.

DMAP shall use ASLME-SAP and DLME-SAP to interact with ASL and DLL respectively, as shown in Figure 11.



IEC

Figure 11 – DMAP of management system

The network management and security management functions implemented in WIA-FA network are shown in Table 9 and Table 10.

Table 9 – Network management functions

Network management functions	Descriptions
Network establishment	Initialization: initializing the NM/network management modules and starting the network
	Clock source configuration and time synchronization service; the WIA-FA network shall set up one reference clock source, which is performed by the gateway device. Devices in the network synchronize with the gateway device.
	Device join process management: the devices need NetworkID (see Table 16) before joining. A new device invokes the join process by sending a join request; after the authentication of SM, the NM returns the join response.
	Network address allocation: Each device in the WIA-FA network shall have 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 redundant star topology as shown in Figure 6.
	Network configuration management: configuring the information of all network devices by the NM, including the communication resources, network address and other network attributes.
Network scheduling and communication resource allocation	Superframe establishment: establishing the superframes for communication according to the application configuration.
	Communication resource allocation: allocating the communication resources to the links.
	Activation/deactivation: activating and deactivating the superframes and links according to application process.
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.
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; the gateway device releases the communication resources of field devices. The abnormal leaving is detected and processed by the gateway device.

Table 10 – Security management functions

Security management functions	Descriptions
Secure network establishment and configuration	Initially key 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 shall return a join response carrying the authentication result.
	Key establishment: after FD secure joining, SM shall generate and distribute keys including KEK, KEDB, and KEDU to make secure operation during normal operating process.
Key updating	Key update: SM shall update the keys in use before the ends of their lifetime, including KEK, KEDB, and KEDU.
Security performance monitoring	Security alarm: monitoring the update status of keys and attacked counts of keys.

6.2.2 Network manager

Network Manager (NM) shall implement network management function in the gateway device. One WIA-FA network has only one NM.

NM shall mainly perform 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 redundant star topology;
- allocating communication resources for communications of WIA-FA devices;
- monitoring the status of the WIA-FA network, including device status and channel condition.

6.2.3 Security manager

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

SM shall mainly perform 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.

6.2.4 Network management module

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

The main functions of the network management module shall be as follows:

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

6.2.5 Security management module

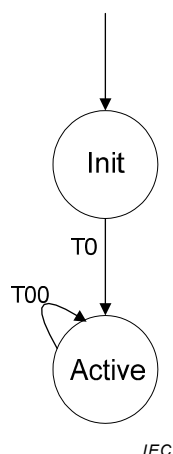
Security management modules in field devices and access devices shall maintain the information for security management functions, and implement the following security management functions:

- coordinating with SM to handle secure joining (field devices only);
- coordinating with SM to manage keys;
- coordinating with SM to report security alarm.

6.2.6 DMAP state machines

6.2.6.1 DMAP state machine of gateway device

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



IEC

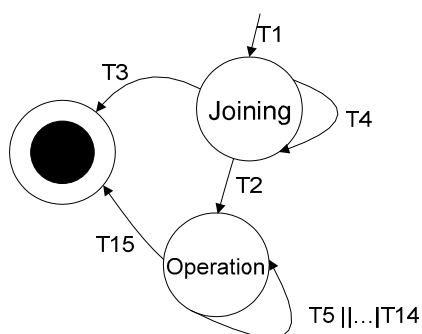
Figure 12 – DMAP state machine of gateway device

The DMAP state transitions of gateway device are shown in Table 11.

Table 11 – DMAP state transition of gateway device

#	Current State	Event or condition => action	Next state
T0	Init	IsDMAPInitializationDone() == TRUE => ;	Active
T00	Active		Active

When the DMAP of gateway device is in Active state and receives a join request from a new field device, it shall create and maintain a sub-state machine for this field device, as shown in Figure 13, so as to process multiple packets from multiple field devices concurrently.



IEC

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

The DMAP sub-state transition of gateway device for each field device is listed in Table 12.

Table 12 – DMAP sub-state transition of gateway device for each field device

#	Current State	Event or condition => action	Next state
T1		PrimitiveType == DLME-JOIN.indication => JoinResult:= HandleFieldJoinRequest(); If (JoinResult == SUCCESS) { ShortAddrResult:= AllocateShortAddr(Addr); DLME-JOIN.response(Status:= SUCCESS, ShortAddr); Delay(DefaultSuperFrameTime); DLME-INFO-GET.request(DeviceStatus); Start DeviceStatusConfirmTimer; } 	Joining
T2	Joining	PrimitiveType == DLME-INFO-GET.confirm &&Status == SUCCESS &&DeviceStatus == Operation => If(SECLEVEL != 0) { KEY-ESTABLISH.request(DstAddr, KeyMaterial); } 	Operation
T3	Joining	JoinResult != SUCCESS (DeviceStatusTimer expires)&&(No DLME-INFO-GET.confirm) ((PrimitiveType =DLME-INFO-GET.confirm) &&((Status != SUCCESS) (DeviceStatus != Operation))) => If (JoinResult != SUCCESS) { DLME-JOIN.response(JoinResult, ShortAddr); } 	End
T4	Joining	PrimitiveType != DLME-INFO-GET.confirm => Ignore;	Joining
T5	Operation	IsHostComputerConfigureDone() == TRUE => ResAllocAgrithm (SuperframeList, LinkList); If (AllocResult == SUCCESS) { DLME-INFO-SET.request(VCR_ID); DLME-INFO-SET.request(SuperframeList); DLME-INFO-SET.request(LinkList); } 	Operation

#	Current State	Event or condition => action	Next state
T6	Operation	IsHostComputerSet MIB() == TRUE => DLME-INFO-SET.request(Handle, DstAddr, AttributeOption, AttributeID, MemberID, FirstStoreIndex, Count, AttributeValue);	Operation
T7	Operation	PrimitiveType ==DLME-INFO-SET.confirm => IndicateSetMIBResult(Handle, Status);	Operation
T8	Operation	IsHostComputerGet MIB() == TRUE => DLME-INFO-GET.request(Handle, DstAddr, AttributeID, MemberID, FirstStoreIndex, Count);	Operation
T9	Operation	PrimitiveType ==DLME-INFO-GET.confirm => IndicateGetMIBResult(Handle, Status);	Operation
T10	Operation	PrimitiveType == DLME-CHANNEL-STATUS.indication => HandleChannelStatusReport(Addr, ChannelConditonInfo);	Operation
T11	Operation	PrimitiveType == DLME-DEVICE-STATUS.indication => HandleDeviceStatusReport(PowerSupplyStatus);	Operation
T12	Operation	IsHostComputerRequestDeviceLeave() == TRUE => DLME-LEAVE.request(DeviceAddr); IndicateHostComputerLeaveResult(Addr);	Operation
T13	Operation	PrimitiveType ==DLME-LEAVE.confirm && Status == FAILURE =>	Operation
T14	Operation	PrimitiveType != DLME-INFO-SET.confirm && PrimitiveType != DLME-INFO-SET.confirm && PrimitiveType != DLME-CHANNEL-STATUS.indication && PrimitiveType !=DLME-LEAVE.confirm && PrimitiveType != DLME-DEVICE-STATUS.indication =>	Operation
T15	Operation	((PrimitiveType ==DLME-LEAVE.confirm)&&(Status == SUCCESS)) ((LossConnectDuration time out) &&(receive no frame from this field device)) => ReleaseResources(Addr); IndicateHostComputerLeaveResult(Addr);	End

– Joining state

In Joining state, the DMAP of the gateway device shall handle join request received from the field device, which includes authentication and assignment of short address for the device. If authentication or short address assignment fails, DMAP shall invoke DLME-JOIN.response to notify the field device of the failure result, then the DMAP sub-state machine shall enter to End state; if authentication and short address assignment succeeds, the DMAP of the gateway device shall invoke DLME-JOIN.response to notify the field device that the join process is successful; then remotely get DeviceStatus in the device if DeviceStatus is equal to Operation, the DMAP sub-state machine shall enter to Operation state.

– Operation state

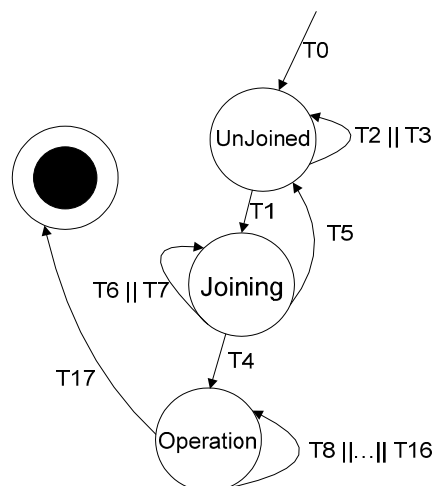
In Operation state, the following events and responding actions may occur:

- If host Computer finishes Configuration, DMAP of the gateway device shall allocate communication resources to field devices; DMAP shall invoke DLME-INFO-SET.request to remotely write VCR_ID, superframes and links to field devices.
- If it is necessary to remotely set the field device's MIB attributes, DMAP shall invoke DLME-INFO-SET.request to request DLL generating a Remote attribute set request frame (see 8.4.17).
- If DLL invokes DLME-INFO-SET.confirm, DMAP shall handle the result of remote attribute set operation.
- If it is necessary to remotely get the field device's MIB attributes, DMAP shall invoke DLME-INFO-GET.request to request DLL generating a Remote attribute get request frame (see 8.4.15).
- If DLL invokes DLME-INFO-GET.confirm, DMAP shall get and handle the returned MIB attributes of a field device.
- If DLL invokes DLME-DEVICE-STATUS.indication, DMAP shall handle the device status report from a field device.
- If DLL invokes DLME-CHANNEL-STATUS.indication, DMAP shall handle the channel condition report from a field device.
- If it is necessary to request a field device to leave WIA-FA network. DMAP shall invoke DLME-LEAVE.request to indicate DLL to generate a Leave command frame (see 8.4.9).

If DLL invokes DLME-LEAVE.response with Status, DMAP shall handle the result of requesting a field leaving WIA-FA network. If Status is equal to SUCCESS, or LossConnectDuration times out and the abnormal leaving of a field is detected, DMAP shall release all MIB attributes and communication resources that are occupied by a leaving field device, then the DMAP sub-state machine enters to End state.

6.2.6.2 DMAP state machine of field device

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



IEC

Figure 14 – DMAP state machine of a field device

The DMAP state transition of a field device is shown in Table 13.

Table 13 – DMAP state transition of a field device

#	Current State	Event or condition => action	Next state
T0	-	IsDMAPInitializationDone() == TRUE => DLME-DISCOVERY.request(ScanChannels, ProbeTime);	UnJoined
T1	UnJoined	PrimitiveType == DLME-DISCOVERY.confirm && Status == SUCCESS => DeviceStatus:= Joining; DLME-JOIN.request(NetworkID, Channel, PhyAddr, SecMaterial);	Joining
T2	UnJoined	PrimitiveType == DLME-DISCOVERY.confirm &&Status == NO_BEACON => DLME-DISCOVERY.request(ScanChannels, ProbeTime);	UnJoined
T3	UnJoined	PrimitiveType != DLME-DISCOVERY.confirm => Ignore;	UnJoined
T4	Joining	PrimitiveType == DLME-JOIN.confirm && Status == SUCCESS => DeviceStruct.ShortAddr:= ShortAddr; DeviceStatus:= Operation; If (TwoWayTimeSyn == TRUE) { DLME-TIME-SYN.request(); }	Operation

#	Current State	Event or condition => action	Next state
T5	Joining	PrimitiveType == DLME-JOIN.confirm && Status != SUCCESS => DeviceStatus:= UnJoined; DLME-DISCOVERY.request(ScanChannels, ProbeTime);	UnJoined
T6	Joining	PrimitiveType ==DLME-INFO-GET.indication => DMAP-MIB-GET.request (Handle, AttributeID, MemberID, FirstStroeIndex, Count, AttributeValue); DMAP-MIB-GET.confim(Handle, Status, Count, AttributeValue); DLME-INFO-GET.response(DstAddr, Status, Count, FirstStoreIndex, Count, AttributeValue);	Joining
T7	Joining	PrimitiveType != DLME-JOIN.confirm &&PrimitiveType !=DLME-INFO-GET.indication => Ignore;	Joining
T8	Operation	PrimitiveType == DLME-TIME-SYN.confirm && Status == SUCCESS => HandleTwoWaySyn();	Operation
T9	Operation	PrimitiveType == DLME-TIME-SYN.confirm && Status != SUCCESS => DLME-TIME-SYN.request();	Operation
T10	Operation	PrimitiveType == DLME-INFO-SET.indication => DMAP-MIB-SET.request (Handle, AttributeOption, AttributeID, MemberID, FirstStoreIndex, Count, AttributeValue); DMAP-MIB-SET.confim(Handle, Status); DLME-INFO-SET.response(SrcAddr , AttributeOption, AttributeID, MemberID, FirstStoreIndex, Count, Status);	Operation
T11	Operation	PrimitiveType ==DLME-INFO-GET.indication => DMAP-MIB-GET.request (Handle, AttributeID, MemberID, FirstStroeIndex, Count, AttributeValue); DMAP-MIB-GET.confim(Handle, Status, Count, AttributeValue); DLME-INFO-GET.response(DstAddr, Status, Count, FirstStoreIndex, 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

#	Current State	Event or condition => action	Next state
T15	Operation	PrimitiveType == DLME-CHANNEL-STATUS.confirm =>	Operation
T16	Operation	PrimitiveType != DLME-INFO-SET.indication && PrimitiveType != DLME-INFO-GET.indication && PrimitiveType != DLME-CHANNEL-STATUS.confirm && PrimitiveType != DLME-DEVICE-STATUS.confirm && PrimitiveType != DLME-LEAVE.indication && PrimitiveType != DLME-TIME-SYN.confirm => Ignore;	Operation
T17	Operation	PrimitiveType == DLME-LEAVE.indication => DLME-LEAVE.response(); ReleaseResources(Addr); DeviceStatus:= End;	End

– UnJoined state

After the DMAP of field device finishes initialization, the state machine shall enter to UnJoinedstate. The DMAP of the field device shall invoke 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 Joining state; otherwise, the DMAP state machine of a field device still stays in UnJoined state and restarts the network discovery.

– Joining state

In Joining state, the DMAP of a field device shall invoke 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 UnJoinedstate.

– Operation state

In Operation state, the following events and responding actions may occur:

- If the state machine is entering to Operation State, DMAP of the field device shall invoke DLME-TIME-SYN.request to request a two way synchronization.
- If DLL invokes DLME-TIME-SYN.confirm after it receives a two way synchronization response frame, and if the status is SUCCESS, the DMAP of the field device shall handle the two way synchronization, otherwise, the DMAP of the field device invoke DLME-TIME-SYN.request to restart the two way synchronization procedure.
- If DLL invokes DLME-INFO-SET.indication after it receives a Remote attribute set request frame (see 8.4.17). The DMAP of the field device shall invoke DMAP-MIB-SET.request to locally set the MIB attributes properly and invoke DLME-INFO-SET.response with the set result which is indicated by DMAP-MIB-SET.confim.
- If DLL invokes DLME-INFO-GET.indication after it receives a remote attribute get request frame (see 8.4.15). The DMAP of the field device shall invoke DMAP-MIB-GET.request to locally get the MIB attributes properly and invoke DLME-INFO-GET.response with the requested MIB attributes which are indicated by DMAP-MIB-GET.confim.
- If the DevStaRptCycle (see 6.7.1.2.1) timer expires, the DMAP of the field device shall invoke DLME-DEVICE-STATUS.request to send the device status report.

- If DLL invokes DLME-DEVICE-STATUS.confirm, DMAP shall handle the result of sending device status report.
- If the ChaStaRptCycle (see 6.7.1.2.1) timer expires, the DMAP of the field device shall invoke DLME-CHANNEL-STATUS.request to send channel condition report.
- If DLL invokes DLME-CHANNEL-STATUS.confirm, DMAP shall handle the result of sending channel condition report.

If DLL invokes DLME-LEAVE.indication after receiving a Leave request frame from the gateway device; the DMAP of the field device shall invoke DLME-LEAVE.response and release all MIB attributes and communication resources, then enters to End state.

6.2.6.3 DMAP state machine of access device

The DMAP state machine of access device is shown in Figure 15.

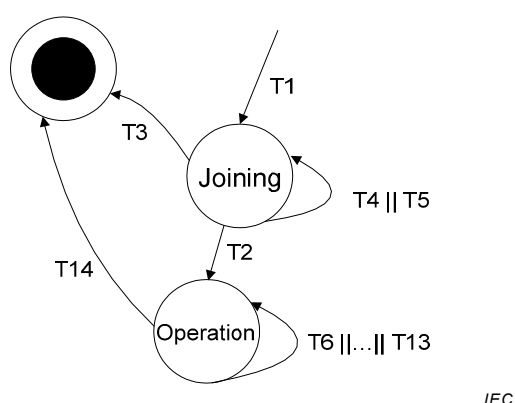


Figure 15 – DMAP state machine of an access device

The DMAP state transition of an access device is shown in Table 14.

Table 14 – DMAP state transition of an access device

#	Current State	Event or condition => action	Next state
T1	-	IsDMAPInitializationDone() == TRUE => DLME-JOIN.request(NetworkID, Channel, PhyAddr, SecMaterial);	Joining
T2	Joining	PrimitiveType == DLME-JOIN.confirm && Status == SUCCESS => DeviceStruct.ApId:= ApId; DeviceStatus:= Operation;	Operation
T3	Joining	PrimitiveType == DLME-JOIN.confirm && Status != SUCCESS => DeviceStatus:= End;	End
T4	Joining	PrimitiveType ==DLME-INFO-GET.indication => DMAP-MIB-GET.request (Handle, AttributeID, MemberID, FirstStoreIndex, Count, AttributeValue); DMAP-MIB-GET.confim(Handle, Status, Count, AttributeValue); DLME-INFO-GET.response(DstAddr, Status, Count, FirstStoreIndex, Count, AttributeValue);	Joining
T5	Joining	PrimitiveType != DLME-JOIN.confirm && PrimitiveType !=DLME-INFO-GET.indication => Ignore;	Joining
T6	Operation	PrimitiveType == DLME-TIME-SYN.indication => DLME-TIME-SYN.response(DstAddr, FieldDeviceTimeValue, ReceiveTimeValue);	Operation
T7	Operation	PrimitiveType == DLME-INFO-SET.indication => DMAP-MIB-SET.request (Handle, AttributeOption, AttributeID, MemberID, FirstStoreIndex, Count, AttributeValue); DMAP-MIB-SET.confim(Handle, Status); DLME-INFO-SET.response(SrcAddr, AttributeOption, AttributeID, MemberID, FirstStoreIndex, Count, Status);	Operation
T8	Operation	PrimitiveType ==DLME-INFO-GET.indication => DMAP-MIB-GET.request (Handle, AttributeID, MemberID, FirstStoreIndex, Count, AttributeValue); DMAP-MIB-GET.confim(Handle, Status, Count, AttributeValue); DLME-INFO-GET.response(DstAddr, Status, Count, FirstStoreIndex, Count, AttributeValue);	Operation
T9	Operation	DevStaRptCycle timeout => DLME-DEVICE-STATUS.request(PowerSupplyStatus);	Operation

#	Current State	Event or condition => action	Next state
T10	Operation	PrimitiveType == DLME-DEVICE-STATUS.confirm =>	Operation
T11	Operation	(ChaStaRptCycle timeout) => DLME-CHANNEL-STATUS.request(ChannelConditionInfo);	Operation
T12	Operation	PrimitiveType == DLME-CHANNEL-STATUS.confirm =>	Operation
T13	Operation	PrimitiveType != DLME-TIME-SYN.indication && PrimitiveType != DLME-INFO-SET.indication && PrimitiveType != DLME-INFO-GET.indication && PrimitiveType != DLME-CHANNEL-STATUS.confirm && PrimitiveType != DLME-DEVICE-STATUS.confirm && PrimitiveType != DLME-LEAVE.indication => Ignore;	Operation
T14	Operation	PrimitiveType == DLME-LEAVE.indication => DLME-LEAVE.response(); ReleaseResources(Addr); DeviceStatus:= End;	End

– Joining state

After the DMAP of access device finishes initialization, the state machine shall enter to Joining state, the DMAP of an access device shall invoke 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.

– Operation state

In Operation state, the following events and responding actions can occur:

- If DLL invokes DLME-TIME-SYN.indication after it receives a two way Time synchronization request frame, the DMAP of the access device shall invoke DLME-TIME-SYN.response.
- If DLL invokes DLME-INFO-SET.indication after it receives a Remote attribute set request frame (see 8.4.17). The DMAP of the access device shall invoke DMAP-MIB-SET.request to locally set the MIB attributes properly and invoke DLME-INFO-SET.response with the set result which is indicated by DMAP-MIB-SET.confim.
- If DLL invokes DLME-INFO-GET.indication after it receives a Remote attribute get request frame (see 8.4.15). The DMAP of the access device shall invoke DMAP-MIB-GET.request to locally get the MIB attributes properly and invoke DLME-INFO-GET.response with the requested MIB attributes which are indicated by DMAP-MIB-GET.confim.
- If the DevStaRptCycle (see 6.7.1.2.1) timer expires, the DMAP of the access device shall invoke DLME-DEVICE-STATUS.request to report the device status.
- If DLL invokes DLME-DEVICE-STATUS.confirm, DMAP shall handle the result of sending device status report.

- If the ChaStaRptCycle (see 6.7.1.2.1) timer expires, the DMAP of the access device shall invoke DLME-CHANNEL-STATUS.request to report channel condition.
- If DLL invokes DLME-CHANNEL-STATUS.confirm, DMAP shall handle the result of sending channel condition report.

If DLL invokes DLME-LEAVE.indication after receiving a Leave request frame from the gateway device; the DMAP of the access device shall invoke DLME-LEAVE.response and release all MIB attributes and communication resources, then enters to End state.

6.2.6.4 Functions used in DMAP state machines

The functions used in DMAP state machines of the gateway device are listed in Table 15.

Table 15 – Functions used in DMAP state machines

Function	Input	Output	Description
AllocateShortAddr()	Addr	AllocateShortAddrResult	Allocating short address for a field device The values of AllocateShortAddrResult include: SUCCESS; FAILURE
HandleFieldJoinRequest()		JoinResult	Handle the join request from device. The value of JoinResult includes: SUCCESS NetworkID mismatched; Authentication failure; Network overload;
HandleTwoWaySyn();			Handle two way synchronization.
IsHostComputerConfigureDone()		HCCDResult	Judging whether the application configuration of the host computer is finished The values of HCCDResult include: TRUE; FALSE
ResAllocAgrithm()	SuperframeList LinkList	ResAllocResult	Allocating communication resources The values of ResAllocResult include: SUCCESS; NO_RESOURCE

Function	Input	Output	Description
IsHostComputerRequestDeviceLeave()		DeviceLeaveResult	Judging whether the host computer requests a field device leave WIA-FA network The values of DeviceLeaveResult include: TRUE; FALSE
IsHostComputerSet MIB()		HostComputerSetMIBResult	Judging whether the host computer remotely request setting the attributes of a field device The values of HostComputerSetMIBResult include: TRUE; FALSE
IndicateSetMIBResult()	Handle Status		Indicating the results of the remote attribute set operation to the host computer
HandleChannelStatusReport()	Addr ChannelConditonInfo		Processing the channel condition report
HandleDeviceStatusReport()	PowerSupplyStatus		Process the device status report
IsHostComputerGet MIB()		HostComputerGetMIBResult	Judging whether the host computer remotely request getting the MIB attributes The values of HostComputerGetMIBResult include: TRUE; FALSE
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
IsDMAPInitializationDone()		DMAPInitializationResult	Judging whether the DMAP initialization is finished The values of DMAPInitializationResult include: TRUE; FALSE
SendWiredFrameToGW();	FrameName		Send wired frames between AD and GW, detail format see 9.3 for frame formats between GW and AD.

6.3 Addressing and address assignment

Each WIA-FA network device shall have a global unique 64-bit long address and an 8-bit or 16-bit short address (indicated by AddressTypeFlag in Table 16). 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 16, shall be assigned by manufacturers according to the EUI-64. The least significant octet of DeviceShortAddress (see Table 21 in 6.7.1.2.2) is valid if the network uses 8-bit short address.

Gateway device shall use AdID (see Table 21 in 6.7.1.2.2) to distinguish different access devices.

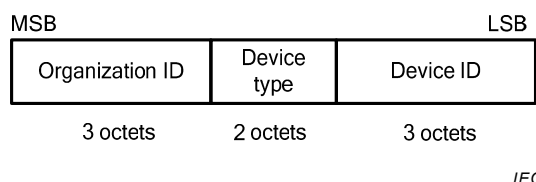


Figure 16 – Long address structure of device

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

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

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

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

The default short address of a WIA-FA device shall be 0x00 or 0x0000, which means the device hasn't been assigned a short address.

6.4 Communication resource allocation

6.4.1 General

Communication resources consist of channels (see 3.1.8) and timeslots (see 3.1.30). 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 shall include LinkID, LinkType, PeerAddr, RelativeSlotNumber, ChannelIndex, and SuperframeID (see Table 19 in 6.7.1.2.2).

6.4.2 Communication resource allocation

6.4.2.1 Data priorities

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

- Urgent data (RT0)

RT0 data shall have 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