

DIN EN 62948

ICS 25.040.01; 35.110

Einsprüche bis 2016-06-01

Entwurf

**Industrielle Kommunikationsnetze –
Kommunikationsnetze und Kommunikationsprofile –
WIA-FA
(IEC 65C/813/CD:2015);
Text in English**

Industrial networks –
Wireless communication network and communication profiles –
WIA-FA
(IEC 65C/813/CD:2015);
Text in English

Réseaux industriels –
Réseau de communications sans fil et profils de communication –
WIA-FA
(IEC 65C/813/CD:2015);
Texte en Anglaise

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2016-04-01 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 175 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Nationales Vorwort

Die englische Originalfassung des internationalen Dokuments IEC 65C/813/CD:2015 „Industrial networks – Wireless communication network and communication profiles – WIA-FA“ (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden.

Das internationale Dokument wurde vom SC 65C „Industrial networks“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

Die IEC und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf prEN nur 2 Monate beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

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

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 den vorliegenden Normentwurf erfüllt.

Da sich die Benutzer des vorliegenden Normentwurfs der englischen Sprache als Fachsprache bedienen, wird die Englische Fassung der IEC 62948 veröffentlicht. Zu deren Abschnitt 1, der den Anwendungsbereich festlegt, und deren Abschnitt 3, der die Begriffe festlegt, wurde eine Übersetzung angefertigt und als informativer Nationaler Anhang NA des vorliegenden Normentwurfs hinzugefügt. Für viele der verwendeten Begriffe existieren keine gebräuchlichen deutschen Benennungen, da sich die deutschen Anwender in der Regel ebenfalls der englischen Benennungen bedienen. Dieser Normentwurf steht nicht in unmittelbarem Zusammenhang mit Rechtsvorschriften und ist nicht als Sicherheitsnorm anzusehen.

Es ist vorgesehen, auch bei der entsprechenden zukünftigen Deutschen Norm auf die deutsche Sprachfassung zu verzichten und diese in der englischsprachigen Fassung zu veröffentlichen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO [und/oder] IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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)

Die deutschen Übersetzungen haben Empfehlungscharakter und können nur die ungefähre Begrifflichkeit in Deutsch wiedergeben. Unter Experten wird empfohlen, ausschließlich die englischen Fachbegriffe zu verwenden, um die Gefahr von Missverständnissen zu reduzieren.

1 Anwendungsbereich

Diese internationale Norm beschreibt die Systemarchitektur und das Kommunikationsprotokoll der WIA-FA (drahtloses Netzwerk für die Industrieautomation – Fabrikautomation) auf Basis der IEEE STD 802.11-2012 Physical Layer (PHY).

Diese Norm bezieht sich auf drahtlose Netzwerksysteme für Mess-, Steuer- und Beobachtung der Fabrikautomation.

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1.1

absolute Zeitschlitznummer

(en: absolute timeslot number)

Nummer von Zeitschlitzten vom Start des Netzwerks, welche im Allgemeinen den aktuellen Zeitschlitz bezeichnen

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

3.1.2

Anschlussgerät

(en: access device)

im Feld installiertes Gerät, welches für die Weiterleitung von Sensordaten, Alarmen und Informationen mit Bezug zum Netzwerkmanagement von Feldgeräten zu Gateway-Geräten verantwortlich ist, oder für die Weiterleitung von Steuerungssignalen, Managementinformationen und Konfigurationsinformationen des Gateway-Geräts an Feldgeräte

3.1.3

Aggregation

(en: aggregation)

Prozess der Zusammenfassung einer Vielzahl von Benutzeranwendungsobjekten in einem Paket oder der Zusammenfassung mehrerer Frames (Rahmen) in einem Frame

3.1.4

Anwendungskonfiguration

(en: application configuration)

Konfigurationsprozess für Benutzeranwendungsprozesse in Felddiensten zum Abschluss bestimmter Aufgaben während der Anwendung von Fabrikautomatisierung

3.1.5

Anwendungsteilschicht

(en: application sublayer)

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

3.1.6**Backoff**

(en: backoff)

Prozess des Versuchs der Wiederholung eines Frames in einem festgelegten Zeitschlitz für erneute Übertragung, wenn die erste Übertragung fehlgeschlagen ist

3.1.7**Warnsignal**

(en: beacon)

besondere Frame-Rundsendung (Broadcast) durch das Anschlussgerät im WIA-FA-Netzwerk

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

3.1.8**Kanal**

(en: channel)

RF-Medium, welches zur Übertragung eines Frames vom Absender zu einem Empfänger verwendet wird

3.1.9**Koexistenz**

(en: coexistence)

Zustand, in dem alle drahtlosen Kommunikationslösungen einer Anlage, die ein gemeinsames Medium nutzen, alle Kommunikationsanforderungen ihrer Anwendung erfüllen

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

3.1.10**Kommunikationsressource**

(en: communication resource)

Kanäle und Zeitschlitze, welche zum Transport eines Frames verwendet werden

3.1.11**Disaggregation**

(en: disaggregation)

Prozess des Zerlegens des zusammengefassten (aggregierten) Paketes in Daten von mehreren Benutzeranwendungsobjekten, oder Zerlegen eines Frames in mehrere Frames

3.1.12**Feldgerät**

(en: field device)

in einem Industriefeld installiertes und mit Sensoren und Aktoren verbundenes Gerät, welches für die Übertragung von Felddaten und zum 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, welches für die Netzbereitstellung und die Firmware-Aktualisierung verwendet wird

3.1.15**Heartbeat-Nachricht**

(en: heartbeat message)

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

3.1.16

Host-Computer

(en: host computer)

Computer, über welchen Betrieb-, Instandhaltungs- und Managementpersonal mit dem WIA-FA-Netzwerk interagieren

Anmerkung 1 zum Begriff: Ein Host-Computer führt Funktionen der Konfiguration, Bereitstellung und Datenanzeige aus.

3.1.17

Interoperabilität

(en: interoperability)

Fähigkeit von zwei oder mehr Netzwerksystemen zum Austausch von Informationen und zur beiderseitigen Verwendung der ausgetauschten Informationen

[QUELLE: ISO/IEC TR 10000-1:1998, 3.2.1 – modifiziert durch Ersatz von „IT-Systeme“ durch „Netzwerk-systeme“]

3.1.18

Verbinden

(en: join)

Prozess, in welchem ein WIA-FA-Gerät authentifiziert wird und ihm die Teilnahme am WIA-FA-Netzwerk gestattet wird

3.1.19

Verknüpfung

(en: link)

Verbindungspfad zwischen zwei benachbarten Geräten, welcher aus einem Parametersatz besteht

Anmerkung 1 zum Begriff: Ein Parametersatz umfasst Verknüpfungsbezeichner (en: link identifier), Zieladresse, relative Zeitschlitznummer, aktuellen Kanalindex und Superframe-Bezeichner.

Anmerkung 2 zum Begriff: Ein WIA-FA-Netzwerk hat nur ein primäres Gateway-Gerät.

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

Netzwerkkonfiguration

(en: network configuration)

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

3.1.22

Netzwerkmanager

(en: network manager)

logische Rolle, welche für das Konfigurieren des Netzwerks, die Zuweisung von Kommunikationsressourcen, die Überwachung und Berichterstattung des Betriebsverhaltens des Netzwerks verantwortlich ist

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

3.1.23

passives Verlassen

(en: passive leaving)

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

3.1.24

physikalische Adresse

(en: **physical address**)

EUI-64-Bit, welcher das Gerät eindeutig im WIA-FA-Netzwerk kennzeichnet; auch Langadresse genannt

Anmerkung 1 zum Begriff: Eine physikalische Adresse wird durch den Hersteller zugewiesen.

3.1.25

primäres Gateway-Gerät

(en: primary gateway device)

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

3.1.26

Bereitstellung

(en: provisioning)

Prozess des Vorkonfigurierens einiger statischer Informationen, welche Netzwerk-Identifizier, Sicherheitsstufen, Verbindungsschlüssel und geteilte Schlüssel umfassen

3.1.27

redundantes Gateway-Gerät

(en: redundant gateway device)

Sicherung für ein in Betrieb befindliches primäres Gateway-Gerät

3.1.28

relative Zeitschlitznummer

(en: relative timeslot number)

vom Beginn eines Superframes gezählte Zeitschlitznummer

3.1.29

Sicherheitsmanager

(en: security manager)

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

3.1.30

Superframe

(en: super frame)

Sammlung von Kanälen und Zeitschlitzten, welche wiederholt in einem Zyklus auftreten

Anmerkung 1 zum Begriff: Er legt die Übertragungs- oder Empfangszeit für periodische Kommunikation fest.

3.1.31

Zeitschlitz

(en: timeslot)

grundlegende Zeiteinheit, die für den Datenaustausch in einem WIA-FA-Netzwerk verwendet wird

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

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.....	20
4 Data coding	22
4.1 Overview	22
4.2 Basic data type coding	22
4.2.1 Integer coding	22
4.2.2 Unsigned coding.....	23
4.2.3 Float coding.....	23
4.2.4 Octetstring coding	24
4.2.5 BitField coding.....	24
4.2.6 Bitstring coding.....	25
4.2.7 TimeData coding	25
4.2.8 KeyData coding	25
4.3 Structured data type coding	26
4.3.1 Structure type coding.....	26
4.3.2 List type coding	26
5 WIA-FA overview	26
5.1 Device types	26
5.1.1 Host computer	26
5.1.2 Gateway device	26
5.1.3 Access device	27
5.1.4 Field device	27
5.1.5 Handheld device.....	27
5.2 Network topology	27
5.3 Protocol architecture	28
6 System management	30
6.1 Overview	30
6.2 Device Management Application Process.....	31
6.2.1 Network manager	32
6.2.2 Security manager	33
6.2.3 Network management module.....	33
6.2.4 Security management module.....	33
6.2.5 DMAP state machines	33
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	46
6.6	Network performance monitoring.....	47
6.6.1	Device status report.....	47
6.6.2	Channel condition report.....	47
6.7	Management information base and services.....	48
6.7.1	Management information base	48
6.7.2	MIB services	57
7	Physical layer	60
7.1	General.....	60
7.2	General requirements based on IEEE STD 802.11-2012	60
7.3	Additional requirements	61
7.3.1	General	61
7.3.2	Frequency band.....	61
7.3.3	Channel bitmap	61
7.3.4	Output power	62
7.3.5	Data rate	62
8	Data Link Layer	63
8.1	General.....	63
8.1.1	Protocol architecture.....	63
8.1.2	WIA-FA superframe	63
8.1.3	Communication based on multiple access devices	66
8.1.4	Time synchronization.....	67
8.1.5	Frame aggregation/disaggregation	68
8.1.6	Fragmentation and reassembly.....	69
8.1.7	Retransmission.....	69
8.2	Data link sub-layer data services	72
8.2.1	General	72
8.2.2	DLDE-DATA.request primitive.....	72
8.2.3	DLDE-DATA.indication primitive	73
8.2.4	Time sequence of DLL data service	73
8.3	Data link sub-layer management services	75
8.3.1	General	75
8.3.2	Network discovery services	75
8.3.3	Time synchronization services	77
8.3.4	Device joining services	79
8.3.5	Device status report services.....	81
8.3.6	Channel condition report services	83
8.3.7	Remote attribute get services	84
8.3.8	Remote attribute configuration services	87
8.3.9	Device leaving services	91
8.4	DLL frame formats	93
8.4.1	General frame format.....	93
8.4.2	Date frame format.....	94
8.4.3	Aggregation frame format	94
8.4.4	NACK frame format	95
8.4.5	GACK frame format	95
8.4.6	Beacon frame format	95
8.4.7	Join request frame format	96
8.4.8	Join response frame format	96

8.4.9	Leave request frame format.....	96
8.4.10	Leave response frame format	97
8.4.11	Device status report frame format.....	97
8.4.12	Channel condition report frame format.....	97
8.4.13	Time synchronization request frame format	97
8.4.14	Time synchronization response frame format.....	97
8.4.15	Remote attribute get request frame format.....	98
8.4.16	Remote attribute get response frame format	98
8.4.17	Remote attribute set request frame format.....	98
8.4.18	Remote attribute set response frame format	99
8.5	Data link layer state machines	99
8.5.1	DLL state machine of access device	99
8.5.2	DLL state machine of field device	103
8.5.3	Functions used in DLL state machines.....	106
9	Wired specifications between GW and AD	107
9.1	Overview	107
9.2	Join process of access device.....	107
9.3	Frame formats between GW and AD	108
10	Application Layer	110
10.1	Overview	110
10.2	AL protocol stack	110
10.3	AL functions.....	111
10.3.1	Data functions	111
10.3.2	Management functions.....	111
10.3.3	Communication models.....	111
10.4	Application data	112
10.4.1	General	112
10.4.2	Process data	112
10.4.3	Event data	112
10.5	User application process.....	113
10.5.1	General	113
10.5.2	User application object	113
10.5.3	IO data images on gateway device	114
10.5.4	Alarm mechanism	115
10.5.5	Application configuration process	115
10.6	Application services	120
10.6.1	Confirmed services and unconfirmed services	120
10.6.2	READ service	121
10.6.3	WRITE service.....	122
10.6.4	PUBLISH Service	123
10.6.5	REPORT Service.....	124
10.6.6	REPORT ACK	125
10.7	Application sublayer.....	126
10.7.1	Overview	126
10.7.2	ASL data service	126
10.7.3	ASL packet format	128
11	Security.....	147
11.1	General.....	147
11.1.1	Security management architecture.....	147

11.1.2	Security functions	149
11.1.3	Keys	149
11.2	Security services	150
11.2.1	General	150
11.2.2	Key establish service	150
11.2.3	Key update service	153
11.2.4	Security alarm service	155
11.3	Secure join	156
11.3.1	General	156
11.3.2	Secure join process of FD	156
11.4	Key management	157
11.4.1	General	157
11.4.2	Key establish process	157
11.4.3	Key update process	158
11.5	DLL secure communication	160
11.6	Security alarm	160
11.7	Secure frame format	161
11.7.1	General secure DLL frame format	161
11.7.2	Secure aggregation frame format	162
11.7.3	Key establish request frame format	162
11.7.4	Key establish response frame format	162
11.7.5	Key update request frame format	163
11.7.6	Key update response frame format	163
11.7.7	Security alarm request frame format	163
Annex A (informative)	Security strategy for WIA-FA network	164
A.1	Risk analysis for WIA-FA network	164
A.2	Security principles for WIA-FA network	164
A.3	Security objectives for WIA-FA network	164
A.4	Security grade of WIA-FA network	164
Annex B (informative)	Regional modification for compliance with ETSI standards	166
B.1	General	166
B.2	Compliance with ETSI EN 300 440-2 V1.4.1	166
B.3	Compliance with ETSI EN 300 328 V1.8.1	166
Bibliography		170
Figure 1	– Conventions used for state machines	21
Figure 2	– Integer coding	22
Figure 3	– Unsigned coding	23
Figure 4	– Single float coding	23
Figure 5	– Double float coding	24
Figure 6	– WIA-FA enhanced star topology	28
Figure 7	– OSI basic reference model mapped to WIA-FA	28
Figure 8	– Protocol architecture of WIA-FA	29
Figure 9	– Data flow over WIA-FA network	30
Figure 10	– System management scheme	30
Figure 11	– DMAP of management system	31
Figure 12	– DMAP state machine of gateway device	

Figure 13 – DMAP state machine of gateway device for each field device.....	34
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	45
Figure 17 – Communication resource allocation process for a field device	46
Figure 18 – Passive leave process of a field device	47
Figure 19 – Device status report process of field device	47
Figure 20 – Channel condition report process of field device	48
Figure 21 – BitMap format.....	61
Figure 22 – WIA-FA DLL protocol architecture	63
Figure 23 – The template of timeslot structure	64
Figure 24 – WIA-FA default superframe	65
Figure 25 – WIA-FA superframe.....	65
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	67
Figure 29 – Process of two-way time synchronization	68
Figure 30 – Aggregation frame payload format.....	69
Figure 31 – Example of retransmission mode based on NACK.....	71
Figure 32 – Example of multi-unicast retransmission mode	71
Figure 33 – Example of multi-broadcast retransmission mode	71
Figure 34 – Example of GACK-based timeslot backoff mode	72
Figure 35 – Time sequence of period data service from FD to GW	74
Figure 36 – Time sequence of other data service from FD to GW	74
Figure 37 – Time sequence of data service from GW to FD.....	74
Figure 38 – Network discovery process.....	76
Figure 39 – Time synchronization process	79
Figure 40 – Device join process	81
Figure 41 – Device status report process	82
Figure 42 – Channel condition report process	84
Figure 43 – Remote attribute get process	87
Figure 44 – Remote attribute set process.....	91
Figure 45 – Device leave process	92
Figure 46 – General frame format	93
Figure 47 – DLL frame header	93
Figure 48 – DLL frame control format.....	93
Figure 49 – DLL Data frame format.....	94
Figure 50 – DLL Aggregation frame format	94
Figure 51 – NACK frame format	95
Figure 52 – GACK frame format.....	95
Figure 53 – GACK information	95
Figure 54 – DLL Beacon frame format.....	95
Figure 55 – Shared timeslot count	95

Figure 56 – DLL join request frame format	96
Figure 57 – DLL join request frame format	96
Figure 58 – DLL leave request frame format	96
Figure 59 – DLL leave response frame format.....	97
Figure 60 – DLL Device status report frame format	97
Figure 61 – DLL Channel condition report frame format	97
Figure 62 – DLL time synchronization request frame format.....	97
Figure 63 – DLL time synchronization response frame format	97
Figure 64 – DLL Remote attribute get request frame format	98
Figure 65 – DLL remote attribute get response frame format.....	98
Figure 66 – DLL Remote attribute set request frame format	99
Figure 67 – DLL remote attribute set response frame format.....	99
Figure 68 – DLL state machine of access device	100
Figure 69 – DLL state machine of field device.....	103
Figure 70 – General frame format between GW and AD	108
Figure 71 –AL portions within WIA-FA protocol stack	110
Figure 72 –The relationships between UAPs and DAPs	113
Figure 73 – User application objects	114
Figure 74 – Implementation example of IO data images on the gateway device	115
Figure 75 – C/S VCR relationships between GW and FDs.....	117
Figure 76 – P/S VCR relationships between GW and FDs	117
Figure 77 – P/S VCR relationships between FDs and GW	118
Figure 78 – R/S VCR relationships between FDs and GW.....	118
Figure 79 – Configuration process for a field device.....	119
Figure 80 – Example of UAO data aggregation and disaggregation process.....	120
Figure 81 – READ request message format	121
Figure 82 – READ response(+) message format	121
Figure 83 – READ response(-) message format	121
Figure 84 – READ Service process	122
Figure 85 – WRITE request message format.....	122
Figure 86 – WRITE response(-) message format.....	122
Figure 87 – WRITE Service process	123
Figure 88 – PUBLISH request message format	123
Figure 89 – PUBLISH Procedure from Field Device to Gateway Device	124
Figure 90 – PUBLISH Procedure from Gateway Device to Field Device	124
Figure 91 – REPORT request message format.....	124
Figure 92 – REPORT Service process	125
Figure 93 – REPORT ACK request message format.....	125
Figure 94 – REPORT ACK response(+) message format.....	125
Figure 95 – REPORT ACK response(-) message format	125
Figure 96 – REPORT ACK Service process	126
Figure 97 – ASL general packet format	129
Figure 98 – Format of packet control field	129

Figure 99 – Confirmed service primitives exchanged between layers	130
Figure 100 – Unconfirmed service primitives exchanged between layers.....	131
Figure 101 – Primitives invoking for read/ write MIB between layers	132
Figure 102 – State transition diagram of AMCL	133
Figure 103 – State transition diagram of AMSV	135
Figure 104 – State transition diagram of AMPB.....	139
Figure 105 – State transition diagram of AMSB.....	142
Figure 106 – State transition diagram of AMRS.....	145
Figure 107 – State transition diagram of AMRK.....	145
Figure 108 – Security management architecture	148
Figure 109 – Life cycle of keys.....	150
Figure 110 – Format of NONCE	151
Figure 111 – Time sequence of key establishment.....	153
Figure 112 – Time sequence of key updating	155
Figure 113 – SecAlarnt_Struct structure.....	155
Figure 114 – Time sequence of security alarm	156
Figure 115 – Secure join process of field device	157
Figure 116 – Key establish process for field device.....	158
Figure 117 – Key update state machine for FD	159
Figure 118 – General secure DLL frame format.....	161
Figure 119 – Secure aggregation frame format	162
Figure 120 – Key establish request frame format	162
Figure 121 – Key establish response frame format.....	163
Figure 122 – Key update request frame format	163
Figure 123 – Key update response frame format.....	163
Figure 124 – Security alarm request frame format.....	163
Figure B.1 – Timeslot timing template	167
Table 1 – Conventions used for state transitions	21
Table 2 – Definition of integer16 data type	22
Table 3 – Unsigned16 coding.....	23
Table 4 – Octetstring coding	24
Table 5 – Coding of BitField8 data with one octet	25
Table 6 – Coding of BitField16 data with two octets	25
Table 7 – Coding of BitField24 data with three octets.....	25
Table 8 – Bitstring coding	25
Table 9 – Network management functions.....	31
Table 10 – Security management functions.....	32
Table 11 – DMAP state transition of gateway device	34
Table 12 – DMAP state transition of gateway device for each field device.....	34
Table 13 – DMAP state transition of a field device	37
Table 14 – Functions used in DMAP state machines	40
Table 15 – Unstructured attributes	49

Table 16 – Structured attributes	51
Table 17 – Superframe_Struct structure	51
Table 18 – Link_Struct structure	51
Table 19 – ChanCon_Struct structure	52
Table 20 – Device_Struct	53
Table 21 – Key_Struct structure	53
Table 22 – VcrEP_Struct definition	54
Table 23 – UAOCClassDesc_Struct definition	55
Table 24 – ProDataDesc_Struct definition	56
Table 25 – UAOInstDesc_Struct definition	56
Table 26 – DMAP-MIB-GET.request parameters	57
Table 27 – DMAP-MIB-GET.confirm parameters	58
Table 28 – DMAP-MIB-SET.request parameters	59
Table 29 – DMAP-MIB-SET.confirm parameters	59
Table 30 – PHY protocol selection	60
Table 31 – Coding of Modulation modes	61
Table 32 – Channel indices	62
Table 33 – Data rate	62
Table 34 – Parameters of timeslot template	64
Table 35 – DLDE-DATA.request primitive parameters	72
Table 36 – DLDE-DATA.indication primitive parameters	73
Table 37 – Management services	75
Table 38 – DLME-DISCOVERY.request parameters	75
Table 39 – DLME-DISCOVERY.confirm parameters	76
Table 40 – BeaconDescription_Struct parameters	76
Table 41 – DLME-TIME-SYN.indication parameters	77
Table 42 – DLME-TIME-SYN.response parameters	77
Table 43 – DLME-TIME-SYN.confirm parameters	78
Table 44 – DLME-JOIN.request parameters	79
Table 45 – DLME-JOIN.indication parameters	79
Table 46 – DLME-JOIN.response parameters	80
Table 47 – DLME-JOIN.confirm parameters	80
Table 48 – DLME-DEVICE-STATUS.request parameters	81
Table 49 – DLME-DEVICE -STATUS.indication parameters	82
Table 50 – DLME-DEVICE -STATUS.confirm parameters	82
Table 51 – DLME-CHANNEL-CONDITION.request parameters	83
Table 52 – DLME-CHANNEL-CONDITION.indication parameters	83
Table 53 – DLME-CHANNEL-CONDITION.confirm parameters	84
Table 54 – DLME-INFO-GET.request parameters	84
Table 55 – DLME-INFO-GET.indication parameters	85
Table 56 – DLME-INFO-GET.response parameters	86
Table 57 – DLME-INFO-GET.confirm parameters	86
Table 58 – DLME-INFO-SET.request parameters	86

Table 59 – DLME-INFO-SET.Indication parameters	89
Table 60 – DLME-INFO-SET response parameters	90
Table 61 – DLME-INFO-SET.confirm parameters	90
Table 62 – DLME-LEAVE.request parameters.....	91
Table 63 – DLME-LEAVE.confirm parameters.....	92
Table 64 – Frame type coding.....	93
Table 65 – Addressing mode subfields.....	94
Table 66 – DLL state transition of access device	100
Table 67 – DLL state transition of field device.....	103
Table 68 – Functions used in DLL state machines	106
Table 69 – Wired services between GW and AD	108
Table 70 – Service parameters of AD join request	109
Table 71 – Service parameters of AD join response.....	109
Table 72 – Service parameters of GW requesting AD to send GACK	109
Table 73 – Parameters of GACKInfo_Struct structure	110
Table 74 – Service parameters of GW requesting AD to send NACK.....	110
Table 75 –Communication models between gateway device and field devices	111
Table 76 – EventData Definition.....	112
Table 77 – UAO events definitions	112
Table 78 – VCR attribute configuration overview.....	116
Table 79 – Application services supported by UAPs.....	120
Table 80 – Error code definition for READ response(-) message.....	121
Table 81 – Error code definition for WRITE response(-)	123
Table 82 – Error code definition for REPORT ACK negative response	125
Table 83 – ASLDE-DATA.request primitive parameter definitions.....	127
Table 84 – ASLDE-DATA.indication primitive parameter definitions	127
Table 85 – ASLDE-DATA.response primitive parameter definitions	128
Table 86 – ASLDE-DATA.confirm primitive parameter definitions.....	128
Table 87 – Service Identifier subfield definition.....	129
Table 88 – Message Type subfield definition.....	129
Table 89 –Confirmed service primitives exchanged between ASL and other layers	130
Table 90 – Unconfirmed service primitives exchanged between ASL and other layers	131
Table 91 –Primitives for read/ write MIB between layers	132
Table 92 – State transition table of AMCL.....	133
Table 93 – State transition table of AMSV.....	135
Table 94 – State transition table of AMPB.....	139
Table 95 – State transition table of AMSB.....	142
Table 96 – State transition table of AMRS.....	145
Table 97 – State transition table of AMRK.....	146
Table 98 – All Functions in ASLM	146
Table 99 – Parameters for KEY-ESTABLISH.request.....	151
Table 100 – KeyMaterial_Struct structure	151
Table 101 – Parameters for KEY-ESTABLISH.indication.....	151

Table 102 – Parameters for KEY-ESTABLISH.response	152
Table 103 – Parameters for KEY-ESTABLISH.confirm	152
Table 104 – Parameters for KEY-UPDATE.request	153
Table 105 – Parameters for KEY-UPDATE.indication	153
Table 106 – Parameters for KEY-UPDATE.response	154
Table 107 – Parameters for KEY-UPDATE.confirm	154
Table 108 – Parameters for SEC-ALARM.request	155
Table 109 – Parameters for SEC-ALARM.indication	156
Table 110 – Key update states	158
Table 111 – Key update state transition	159
Table 112 – Keys used in DLL secure communication	160
Table 113 – Available security levels for DLL	161
Table A.1 – Security grades for WIA-FA network	165
Table B.1 – Applicable EN 300 440-2 requirements list	166
Table B.2 – Applicable EN 300 328 requirements list	167
Table B.3 – Timeslot timing definitions and calculations	167
Table B.4 – TxMaxPHYPacket of FHSS	168
Table B.5 – TxMaxPHYPacket of DSSS/HR-DSSS	168
Table B.6 – TxMaxMPDU of OFDM	169

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.

International Standard IEC 62948 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation. The text of this standard is based on the following documents:

FDIS	Report on voting
XX/XX/FDIS	XX/XX/RVD

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

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

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

- 54 • reconfirmed,
- 55 • withdrawn,
- 56 • replaced by a revised edition, or
- 57 • amended.

58

59 The National Committees are requested to note that for this publication the stability date
60 is

61 THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE
62 DELETED AT THE PUBLICATION STAGE.

63

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.

64

65

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

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 standard 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.

ISO/IEC 7498-1, *Information technology, open systems, interconnection, basic reference model – Part 1: Basic model*

IEC 61588-2004, IEEE Standard for a 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*

IETF RFC 1321, The MD5 Message-Digest Algorithm. <http://tools.ietf.org/html/rfc1321>

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 denote 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 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; 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; also called long address

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

196 **3.1.25**

197 **primary gateway device**

198 gateway device working in a WIA-FA network

199 **3.1.26**

200 **provisioning**

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

203 **3.1.27**

204 **redundant gateway device**

205 hot backup of the primary gateway device

206 **3.1.28**

207 **relative timeslot number**

208 timeslot number counted from the start of a superframe

209 **3.1.29**

210 **security manager**

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

213 **3.1.30**

214 **superframe**

215 collection of channels and timeslots repeatedly appear in one cycle

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

217 **3.1.31**

218 **timeslot**

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

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

221 **3.2 Abbreviations**

222 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
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

223 **3.3 Conventions**

224 For the purposes of the state machines and state transitions in this document, the following
225 conventions apply.

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

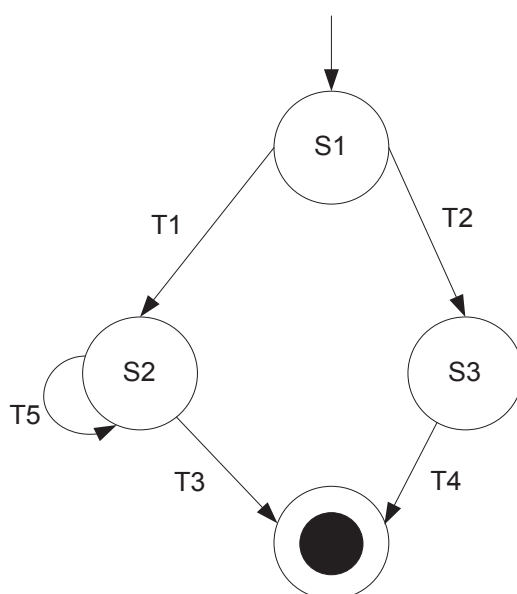


Figure 1 – Conventions used for state machines

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  is the end state in which a device ends its operations.
- 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.

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:

- := 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 indicate 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.

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

249 Example:
 250 for (Identifier = start_value to end_value)
 251 actions
 252 end

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

256 Example:
 257 if (condition)
 258 actions
 259 else
 260 actions
 261 endif

262 4 Data coding

263 4.1 Overview

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

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

269 4.2 Basic data type coding

270 4.2.1 Integer coding

271 The integer is a signed value, as shown in Figure 2. An example of Integer16 coding is shown
 272 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	$-32768 \leq i \leq 32767$	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		

273 Figure 2 – Integer coding

274 Table 2 – Definition of integer16 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. 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	$0 \leq i \leq 65535$	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		Short Real Number (32 bits), see ISO/IEC/IEEE 60559							
coding		Short Real Number (32 bits), see ISO/IEC/IEEE 60559							
Octet	Bit	MSB				LSB			
		7	6	5	4	3	2	1	0
1	Exponent (E)								
		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	Short Real Number, 64 bits, see ISO/IEC/IEEE 60559							
coding	Short Real Number, 64 bits, see ISO/IEC/IEEE 60559							
bit	MSB				LSB			
	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
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 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 1µs.

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 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:

- 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, 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 15), it will take over all works of the original primary gateway device.

NOTE 2 A redundant gateway device has its own NM and SM acting as backups of primary NM and SM. Suppliers should implement this functionality on their own.

NOTE 3 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. In addition, host computer carries out the control functions. Its specific implementation is beyond the scope of this standard.

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 commands 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 standard.

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 standard.

5.1.5 Handheld device

Handheld devices are portable devices that are used for provisioning field device, access device, and gateway device. A handheld device communicates with its direct connected device, and does not communication with other WIA-FA devices. Handheld devices use wired 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.

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 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.

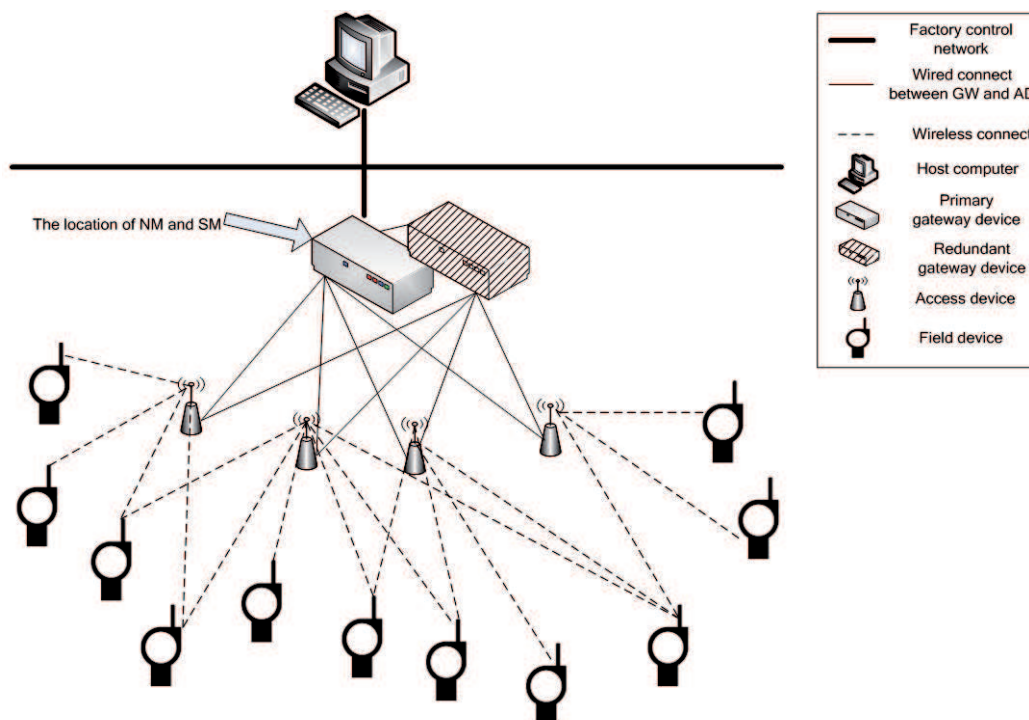


Figure 6 – WIA-FA enhanced star topology

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.	DLL Communication based on multiple ADs, TDMA, FDMA, retransmission, aggregation... PHY (IEEE STD 802.11-2012 PHY)
Data link	Establishes data packet structure, framing, error detection, bus arbitration	
Physical	Mechanical / electrical connection. Transmits raw bit stream	

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);

399 – Protocol layer interfaces: including data entities SAPs (DLDE-SAP and ASLDE-SAP) and
400 management entity SAPs (DLME-SAP and ASLME-SAP).

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

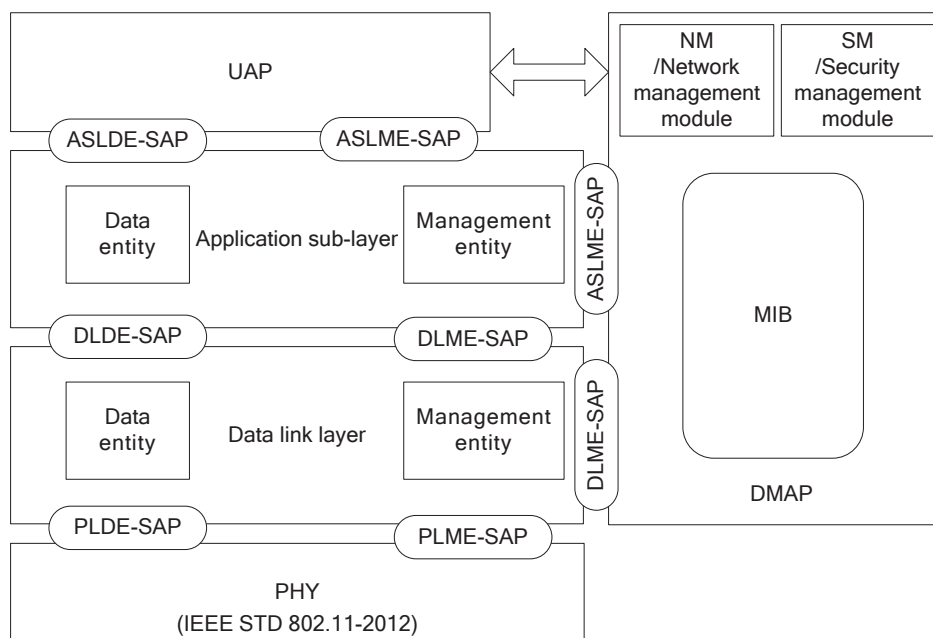


Figure 8 – Protocol architecture of WIA-FA

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

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

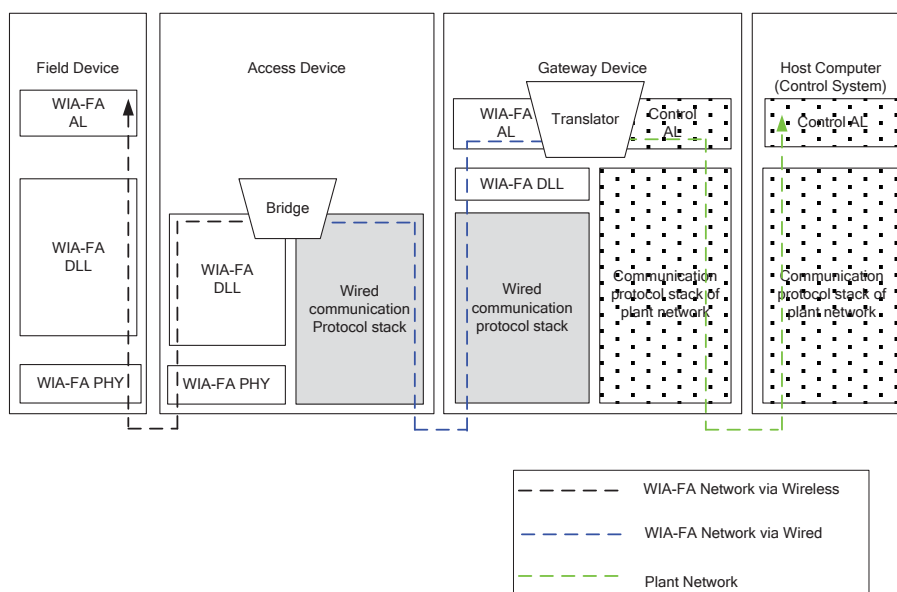


Figure 9 – Data flow over WIA-FA network

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.

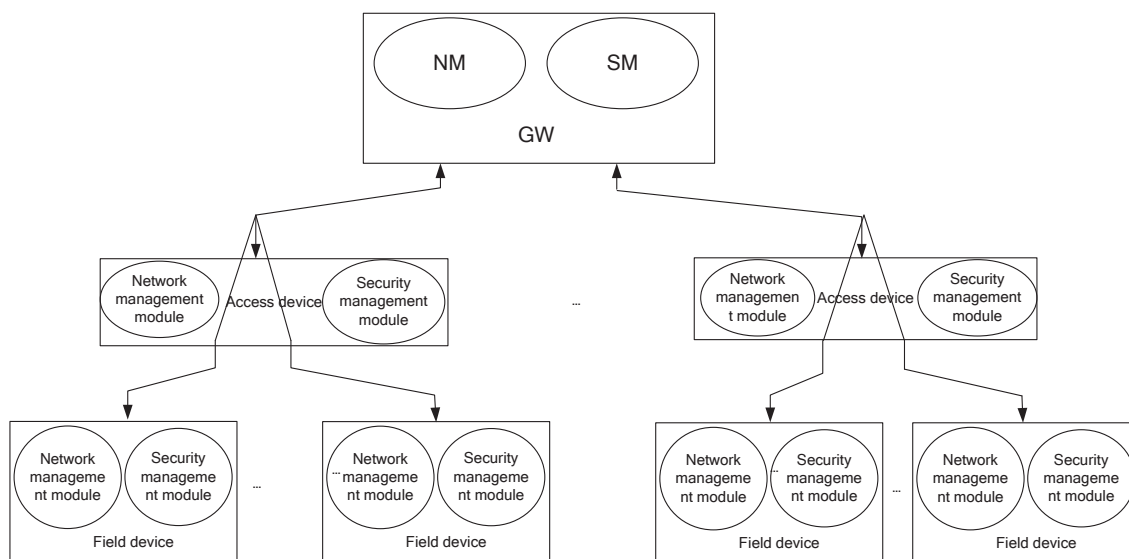


Figure 10 – System management scheme

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 gray 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 it uses ASLDE-SAP and ASLME-SAP with UAP to exchange messages with ASL, as shown in Figure 11.

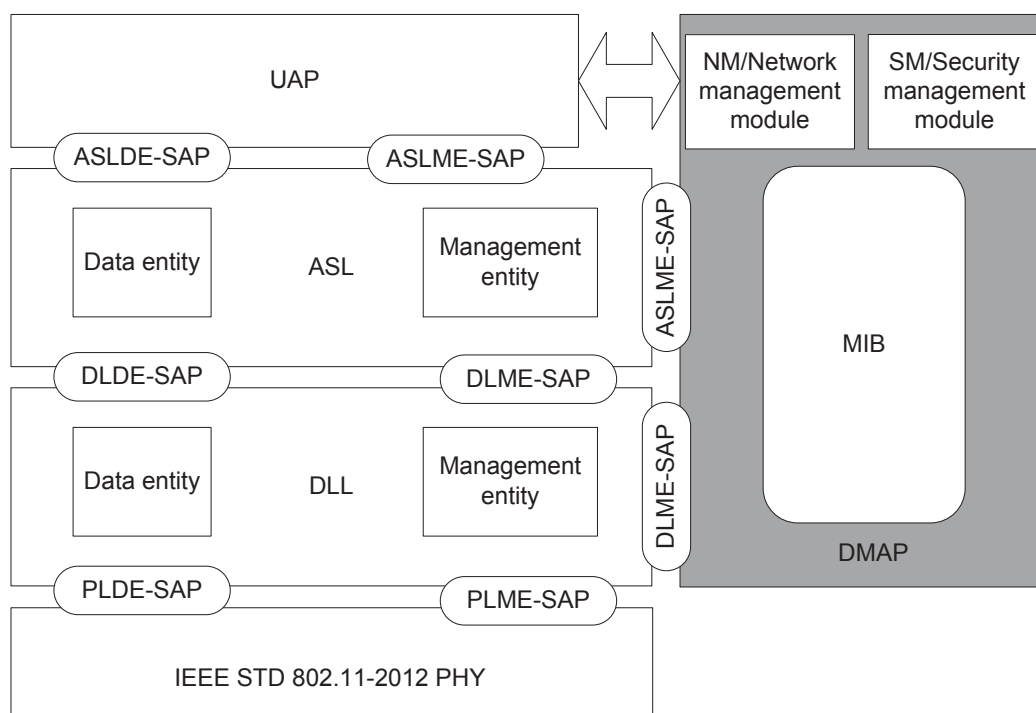


Figure 11 – DMAP of management system

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	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 15) 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.

449

Table 10 – 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.

450

6.2.1 Network manager

451

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.

452

NM mainly performs the following functions:

453

- 454 – Allocating the unique 8-bit or 16-bit short address for all devices in the network (see 6.3);
- 455 – Constructing and maintaining the enhanced star topology;
- 456 – Allocating communication resources for communications of WIA-FA devices;
- 457 – Monitoring the performance of the WIA-FA network, including device status, and channel
- 458 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 Active states. The gateway device enters into Active state if it finishes initializations.

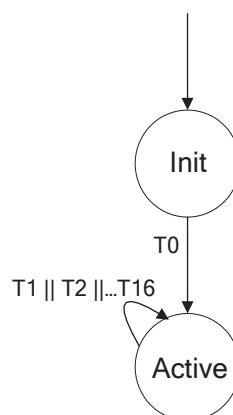


Figure 12 – DMAP state machine of gateway device

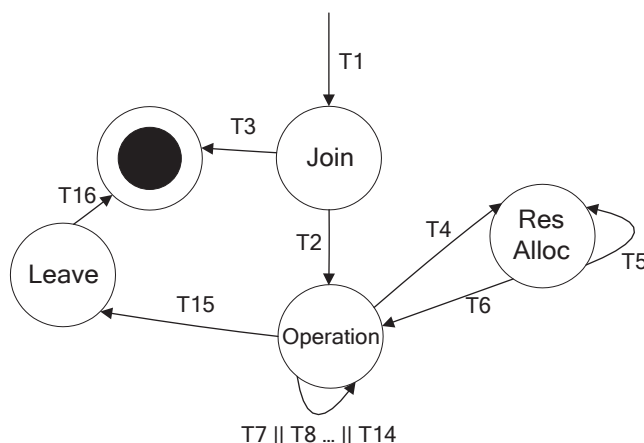
The DMAP state transition of gateway device is listed in Table 11.

487

Table 11 – 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 12	Active

488 The DMAP of gateway device maintains a state machine for each field device, as shown in
 489 Figure 13. The gateway device can process multiple packets from multiple field devices in
 490 parallel. The triggering condition from Init state to Active state in Figure 11 is one of T1 to T16
 491 (see Table 12).



492

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

493

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

495

Table 12 – 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, MemberID := 12, AttributeValue := ALLOCATION); } else { 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, MemberID := 12, AttributeValue := OPERATION);	Operation
T7	Operation	PrimitiveType == DMAP-MIB-SET.request => Status = WriteToMIB(Handle, AttributeOption, AttributeID, MemberID, FirstStoreIndex, Count, AttributeValue); DMAP-MIB-SET.confim(Handle, Status);	Operation
T8	Operation	PrimitiveType == DMAP-MIB-GET.request => Status := ReadFromMIB(Handle, AttributeID, MemberID, FirstStroeIndex, Count, AttributeValue); DMAP-MIB-GET.confim(Handle, Status, Count, AttributeValue);	Operation
T9	Operation	IsHostComputerSet MIB() == TRUE => DLME-INFO-SET.request(Handle, DstAddr, AttributeOption, AttributeID, MemberID, 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, MemberID, FirstStoreIndex, Count);	Operation
T12	Operation	PrimitiveType ==DLME-INFO-GET.confirm => IndicateGetMIBResult(Handle, Status);	Operation
T13	Operation	PrimitiveType == DLME-CHANNEL-STATUS.indication => HandleChannelStatusReport(Addr, ChannelConditonInfo);	Operation
T14	Operation	PrimitiveType == DLME-DEVICE-STATUS => HandleDeviceStatusReport(PowerSupplyStatus);	Operation

T15	Operation	IsHostComputerRequestDeviceLeave() == TRUE => DLME-LEAVE.request(DeviceAddr); IndicateHostComputerLeaveResult(Addr);	Leave
T16	Leave	PrimitiveType ==DLME-LEAVE.response => ReleaseResources(Addr)	End

496 – Join state

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

505 – Operation state

506 In Operation state, the following events shall occur:

- 507 • Host computer remotely sets the field device's MIB attributes; DMAP invokes DLME-INFO-
 508 SET.request to request DLL generating a remote attribute set request frame (see 8.4.17).
- 509 • DLL invokes DLME-INFO-SET.confirm and returns the result of remote attribute set
 510 operation to DMAP.
- 511 • Host computer remotely gets the field device's MIB attributes; DMAP invokes DLME-INFO-
 512 GET.request to request DLL generating a remote attribute get request frame (see 8.4.15).
- 513 • DLL invokes DLME-INFO-GET.confirm and returns the related MIB attributes of a field
 514 device to DMAP.
- 515 • Host computer invokes DMAP-MIB-SET.request to locally set the gateway's MIB attributes;
 516 DMAP sets its MIB attributes and invokes DMAP-MIB-SET.confirm to return the result of
 517 local attribute set operation to the host computer.
- 518 • Host computer invokes DMAP-MIB-GET.request to locally get the gateway's MIB attributes;
 519 DMAP returns its MIB attributes and invokes DMAP-MIB-GET.confirm to return related MIB
 520 attributes to the host computer.
- 521 • DLL invokes DLME-DEVICE-STATUS.indication to DMAP after it receives the device
 522 status report from a field device.
- 523 • DLL DLME-CHANNEL-STATUS.indication to DMAP after it receives the channel condition
 524 report from a field device.
- 525 • Host computer requests a field device leaving WIA-FA network. DMAP invokes DLME-
 526 LEAVE.request to request DLL generating a leave command frame (see 8.4.9).

527 – Res Alloc State

528 In Res Alloc state, the DMAP of the gateway device allocates communication resources to a
 529 field device; DMAP invokes DLME-INFO-SET.request to remotely write superframes or links
 530 to the field device. If the communication resource allocating process is completed or failure,
 531 DMAP remotely sets the field device's DeviceState (see Table 20) attribute to Operation; then,
 532 the DMAP state machine enters to Operation State.

533 – Leave State

534 In Leave state, DMAP releases all MIB attributes and communication resources that are
 535 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.

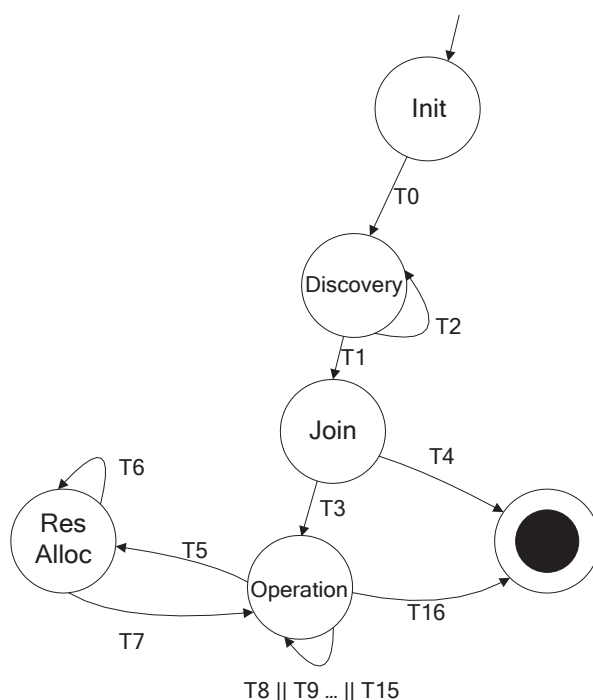


Figure 14 – DMAP state machine of a field device

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	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 && MemberID == 12) && AttributeValue == ALLOCATION ==> Status = WriteToMIB(Handle, AttributeOption, AttributeID, MemberID, 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, MemberID, FirstStoreIndex, Count, AttributeValue); DLME-INFO-SET.response(Handle, Status);	Res Alloc
T7	Res Alloc	PrimitiveType == DLME-INFO-SET.indication && (AttributeID == 131 && MemberID == 12) && AttributeValue == OPERATION ==> Status = WriteToMIB(Handle, AttributeOption, AttributeID, MemberID, FirstStoreIndex, Count, AttributeValue); DLME-INFO-SET.response(Handle, Status);	Operation
T8	Operation	PrimitiveType == DLME-INFO-SET.indication ==> Status = WriteToMIB(Handle, AttributeOption, AttributeID, MemberID, FirstStoreIndex, Count, AttributeValue); DLME-INFO-SET.response(Handle, Status);	Operation
T9	Operation	PrimitiveType == DLME-INFO-GET.indication ==> Status = ReadFromMIB(Handle, AttributeID, MemberID, FirstStoreIndex, Count, AttributeValue); DLME-INFO-GET.response(Handle, Status, Count, FirstStoreIndex, Count, AttributeValue);	Operation
T10	Operation	PrimitiveType == DMAP-MIB-SET.request ==> Status = WriteToMIB(Handle, AttributeOption, AttributeID, MemberID, FirstStoreIndex, Count, AttributeValue); DMAP-MIB-SET.confim(Handle, Status);	Operation
T11	Operation	PrimitiveType == DMAP-MIB-GET.request ==> Status = ReadFromMIB(Handle, AttributeID, MemberID, FirstStoreIndex, Count, AttributeValue); DMAP-MIB-GET.confim(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
-----	-----------	---	-----

542 – Init state

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

544 – Discovery state

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

550 – Join state

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

555 – Res Alloc state

556 In Res Alloc state, DLL invokes DLME-INFO-SET.indication after it receives a remote attribute
557 set request from the gateway device to write superframes or links. The DMAP of the field
558 device writes superframes or links into MIB, and invokes DLME-INFO-SET.response to return
559 the result. If the DeviceState (see Table 20) in MIB is set to Operation by the gateway device,
560 the state machine enters to Operation state.

561 – Operation state

562 In Operation state, the following events shall occur:

- 563 • DLL invokes DLME-INFO-SET.indication after it receives a remote attribute set request
564 frame (see 8.4.17), which indicates DMAP to set MIB attributes. The DMAP of a field
565 device sets the MIB attributes properly and invokes DLME-INFO-SET.response to return
566 the result.
- 567 • DLL invokes DLME-INFO-GET.indication after it receives a remote attribute get request
568 frame (see 8.4.15), which indicates DMAP to get MIB attributes. The DMAP of a field
569 device gets the related MIB attributes properly and invokes DLME-INFO-GET.response to
570 return the requested MIB attributes.
- 571 • APP/DLL invokes DMAP-MIB-GET.request to locally get MIB attributes. The DMAP
572 invokes DMAP-MIB-GET.response to return the related MIB attributes.
- 573 • APP/DLL invokes DMAP-MIB-SET.request to locally set the MIB attributes. The DMAP
574 invokes DMAP-MIB-SET.response to return the result of DMAP-MIB-SET.request.
- 575 • If the timer for device status report expires every DevStaRptCycle (see 6.7.1.2.1) time, the
576 DMAP of a field device invokes DLME-DEVICE-STATUS.request to send the device status
577 report to the gateway device.
- 578 • DLL invokes DLME-DEVICE-STATUS.confirm to DMAP, which returns the result of
579 sending device status report.
- 580 • If the timer for the channel condition report expires every ChaStaRptCycle (see 6.7.1.2.1)
581 time, the field device DMAP invokes DLME-CHANNEL-STATUS.request to return the
582 result of sending channel condition report.
- 583 • DLL invokes DLME-CHANNEL-STATUS.confirm to DMAP, which returns the result of
584 sending channel condition report.

- 585 • DLL invokes DLME-LEAVE.indication after receiving a leave request frame from the
 586 gateway device; the field device releases all MIB attributes and communication resources,
 587 and enters to End state.

588 6.2.5.3 Functions used in DMAP state machines

589 The functions used in DMAP state machines of the gateway device are listed in Table 14.

590 **Table 14 – Functions used in DMAP state machines**

Function	Input	Output	Description
Authentication()	PhyAddr	AuthenResult	Authenticating a joining field device The values of AuthenResult include: SUCCESS; FAILURE
AllocateShortAddr()	Addr	AllocateShortAddrResult	Allocating short address for a field device The values of AllocateShortAddrResult include: SUCCESS; FAILURE
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
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 ChannelConditionInfo		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
WriteToMIB();	Handle AttributeOption AttributeID MemberID FirstStoreIndex Count AttributeValue	WriteToMIBResult	Locally writing MIB attributes The values of WriteToMIBResult include: SUCCESS; INVALIDATTRIBUTE INVALIDATTRIBUTE_ MEMBER; INVALID VALUE
ReadFromMIB()	Handle AttributeID MemberID FirstStoreIndex Count AttributeValue	ReadFromMIBResult	Locally reading MIB attributes The values of ReadFromMIBResult include: SUCCESS; INVALIDATTRIBUTE INVALIDATTRIBUTE_ MEMBER; INVALID RANGE
IsDMAPInitializationDone()		DMAPInitializationResult	Judging whether the DMAP initialization is finished The values of DMAPInitializationResult include: TRUE; FALSE

IsAllResAllocateDone()		AllResAllocateResult	Judging whether all communication resources are allocated The values of AllResAllocateResult include: TRUE; FALSE
------------------------	--	----------------------	--

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 15). 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 20 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.

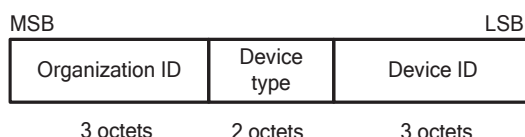


Figure 15 – Long address structure of device

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 0xFFFFE;
- 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 a short address.

6.4 Communication resource allocation

6.4.1 General

Communication resources consist of channels (see 3.1.8) and timeslots (see 3.1.31). 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 Table 18 in 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 model (see 10.5.5.3.4).

– 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 model (see 10.5.5.3.3).

– 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 model (see 10.5.5.3.4).

– 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 model (see 10.5.5.3.3).

– 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 model (see 10.5.5.3.2).

The transmission of data with one of above five priorities uses different communication models and different VCRs. The definition of communication models, 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

663 Preemption is used to transmit RT0 data. The gateway device and field devices can utilize
664 timeslots original for periodic data to transmit RT0 data, which defers the transmission of the
665 periodic data.

666 – Competition

667 Competition refers to using shared transmitting link to transmit RT2 data and NRT data.

668 **6.5 Joining and leave process of field device**

669 **6.5.1 Joining process of a field device**

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

672 – NetworkID;

673 – SecLevel;

674 – KJ (when the security level is not 0);

675 – KS (when the security level is not 0).

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

678 – Access devices periodically broadcast beacons;

679 – A field device with attempt to join the WIA-FA network continually scans available
680 channels to get beacons from access devices and synchronizes with gateway device by
681 using one-way time synchronization method (see 8.1.4);

682 – The field device chooses a channel on which field device receives beacon frame and
683 utilizes the shared timeslots for sending the join request; the shared timeslot is determined
684 by the "First shared timeslot number" and the "Shared timeslot count" (see 8.4.6) in the
685 beacon frame); the field device competes for transmitting join request utilizing timeslot
686 based backoff method (see 8.1.7.5) on the channel used by the beacon;

687 – An access device transfers the join request received from a field device to the gateway
688 device;

689 – The NM residing on the gateway device returns the join response; if the joining is
690 approved, the value of Status in the join response is set to SUCCESS; otherwise, the
691 value of the Status should be set according to error reasons (See Status in 8.3.4.3);

692 – An access device forwards the join response to the corresponding field device;

693 – The field device receives the join response from an access device; if the value of Status in
694 the join response is not SUCCESS, the field device should restart or terminate the join
695 process; if the value of Status in the join response is SUCCESS, the join process is
696 completed.

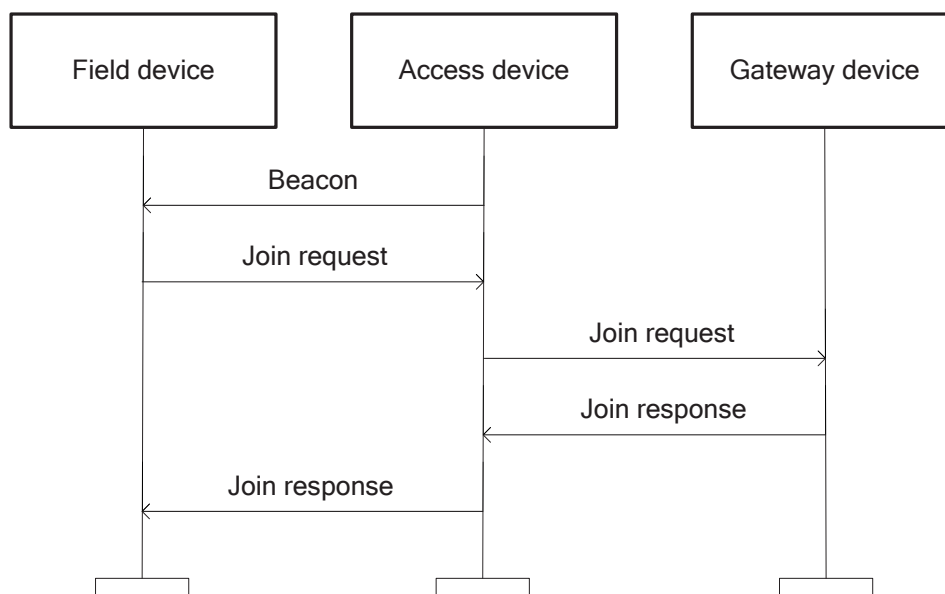


Figure 16 – Joining process of field device

NOTE See clause 11 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.