

DIN EN 62601

ICS 35.110; 35.240.50

Einsprüche bis 2015-04-13

Entwurf

**Industrielle Kommunikationsnetze –
Kommunikationsnetze und Kommunikationsprofile –
WIA-PA
(IEC 65C/783/CDV:2014);
Englische Fassung FprEN 62601:2014**

Industrial communication networks –
Wireless communication network and communication profiles –
WIA-PA
(IEC 65C/783/CDV:2014);
English version FprEN 62601:2014

Réseaux industriels de communication –
Réseau de communications sans fil et profils de communication –
WIA-PA
(CEI 65C/783/CDV:2014);
Version anglaise FprEN 62601:2014

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2015-02-13 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 220 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Nationales Vorwort

Die englische Fassung des europäischen Dokuments FprEN 62601:2014 „Industrielle Kommunikationsnetze – Kommunikationsnetze und Kommunikationsprofile – WIA-PA“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (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. Dem entsprechend ist das internationale Dokument IEC 65C/783/CDV:2014 „Industrial communication networks – Wireless communication network and communication profiles – WIA-PA“ unverändert in den Entwurf FprEN 62601:2014 übernommen worden.

Das internationale Dokument wurde vom SC 65C „Industrial networks“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

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 eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

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

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen 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.

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 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 62601 veröffentlicht. Zu 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.

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)

3 Begriffe und Abkürzungen

3.1 Begriffe

3.1.1

absolute Zeitschlitznummer

(en: **absolute timeslot number**)

Nummer der Zeitschlitz, die vom Betriebsbeginn des Netzes an gezählt wird, im Allgemeinen als der aktuelle Zeitschlitz bezeichnet

3.1.2

aktiver Austritt

(en: **active leaving**)

Verfahren, bei dem ein mit dem Netz aktiv verbundenes Feldgerät von seinem Vermittlungsstationsgerät oder ein mit dem Netz aktiv verbundenes Vermittlungsstationsgerät von seinem Gateway-Gerät nach Anforderung die Bestätigung erhält das Netz verlassen zu können

3.1.3

adaptives Frequenzsprungverfahren

(en: **adaptive frequency hopping**)

zustandsbedingter Wechsel der Kommunikationskanäle in jedem Zeitschlitz während der Intra-Cluster-Periode eines WIA-PA-Superrahmens

3.1.4

adaptiver Frequenzschalter

(en: **adaptive frequency switch**)

zustandsbedingter Wechsel der Kommunikationskanäle während des Beacon-Broadcastrahmens und wenn ein Überrahmen aktiv ist, wobei zu den verschiedenen Überrahmen unterschiedliche Kanäle benutzt werden

3.1.5

Aggregation

(en: **aggregation**)

Zusammenführung von Daten aus verschiedenen Benutzer-Anwendungsobjekten oder Zusammenlegung mehrerer Pakete von Cluster-Mitgliedern in einem Paket

3.1.6

Anwendungs-Unterschicht

(en: **application sub-layer**)

Protokoll-Unterschicht, die Daten- und Verwaltungsdienste für die Anwendungsschicht bereitstellt

3.1.7

Beacon

(en: **beacon**)

spezieller von Vermittlungsstationsgeräten oder Gateway-Geräten verwendeter Broadcastrahmen im WIA-PA-Netz

Anmerkung 1 zum Begriff: Um dem WIA-PA-Netz beizutreten, sollten sich eine neues Vermittlungsstationsgerät oder ein Feldgerät zu erst an den Beacons orientieren.

3.1.8**Broadcast****(en: broadcast)**

gleichzeitiges Übertragen eines Pakets an alle WIA-PA-Geräte

3.1.9**Kanal****(en: channel)**

HF-Medium, das verwendet wird, um ein Paket von einem Sender zu einem Empfänger zu übermitteln

3.1.10**Cluster****(en: cluster)**

logische Gruppe von Geräten, die aus einem Vermittlungsstationsgerät und den Feldgeräten besteht

3.1.11**Clusterhead****(en: cluster head)**

Verwaltungsfunktion im Cluster, die von einem Vermittlungsstationsgerät ausgeübt wird

3.1.12**Cluster-Mitglied****(en: cluster member)**

durch ein Feldgerät im Cluster ausgeübte Funktion einer Datenquelle

3.1.13**Koexistenz****(en: coexistence)**

Fähigkeit eines Netzes, seine Aufgabe in einer bestimmten gemeinsamen Umgebung durchzuführen ohne andere Netzwerke zu stören oder durch diese gestört zu werden

Anmerkung 1 zum Begriff: Diese Netzwerke können sowohl nach den gleichen Richtlinien arbeiten als auch nicht.

3.1.14**Kommunikationsbetriebsmittel****(en: communication resource)**

Kanäle und Zeitschlitze, die verwendet werden, um einen Rahmen zu transportieren

3.1.15**WIA-PA-Konfigurationssoftware****(en: WIA-PA configuration software)**

Programmentwicklungssystem für die Konfiguration eines WIA-PA-Netzes und der Geräte

3.1.16**Sicherungs-Unterschicht****(en: data link sub-layer)**

die MAC-Schicht, die obere der Unterschichten des IEEE 802.15.4-Standards, 2011 ist für die Aspekte der Netzwerktopologie und der Kommunikationsbetriebsmittel im WIA-PA-Netz zuständig

3.1.17**Disaggregation****(en: disaggregation)**

Aufteilen der zusammengeführten Pakete in die Daten der Nutzer-Anwendungsobjekte

3.1.18**Feldgerät****(en: field device)**

auf der Feldebene verwendetes Gerät, das in den Prozess eingebunden ist oder diesen kontrolliert

3.1.19

Rahmen

(en: frame)

Format der von der Medienzugriffssteuerung (MAC) aggregierten Bits, die gleichzeitig zusammen übertragen werden

3.1.20

Frequenzsprungverfahren

(en: Frequency hopping)

Wechsel der Sende-/Empfangsfrequenz, um Interferenz und Fading zu verhindern

3.1.21

Gateway-Gerät

(en: gateway device)

Gerät, welches das WIA-PA-Netz mit einem anderen Netzwerktyp verbindet

3.1.22

Handgerät

(en: handheld device)

tragbares Gerät zur Einrichtung, Firmware-Aktualisierung und die Gerätestatusüberwachung

3.1.23

Hop

(en: hop)

Netzwerkvorgang, der bei direkter Übertragung eines Paketes zwischen zwei benachbarten Geräten ohne die Beteiligung von anderen Geräten des WIA-PA-Netzes auskommt

Anmerkung 1 zum Begriff: Multi-Hop-Vorgänge werden angewandt, um Übertragungsstrecken zu verlängern, Störquellen zu umgehen oder Kollisionen zu vermeiden.

3.1.24

Host-Konfigurationsrechner

(en: host configuration computer)

Gerät, mit dem Benutzer und für die Wartung und das Management verantwortliche Personen Transaktionen auf dem WIA-PA-Netz bzw. den Steuerungsnetzwerken durchführen

3.1.25

Verbindbarkeit

(en: interconnectable)

Verwendung gleicher Kommunikationsprotokolle, der gleichen Kommunikationsschnittstelle und des gleichen Datenzugriffs

[Quelle: IEC/TR 62390:2005, 6.2.2, abgewandelt]

3.1.26

Interoperabilität

(en: interoperable)

Fähigkeit zusammenzuarbeiten, um eine spezifische Rolle in einem oder mehreren verteilten Anwendungsprogrammen auszuführen

Anmerkung 1 zum Begriff: In diesem Fall passen die Parameter und ihre anwendungsbezogene Funktionalität sowohl syntaktisch als auch semantisch zusammen. Interoperabilität ist erreicht, wenn die Geräte zusammengehörige Parametersätze und Funktionen unterstützen, die zum gleichen Profil gehören.

[Quelle: IEC/TR 62390:2005, 6.2.2, abgewandelt]

3.1.27

Beitrittsauthentifizierung

(en: joining)

Prozess, durch den ein WIA-PA-Gerät authentifiziert und der Beitritt zum WIA-PA Netz bestätigt wird

3.1.28**Systemverbindung****(en: link)**

bestimmte Kommunikationsparameter, die notwendig sind, einen Rahmen zwischen benachbarten Geräten im Netz zu übertragen

Anmerkung 1 zum Begriff: Darin enthalten sind Quell-/Ziel-Adresse, Zeitschlitz, Kanal, Richtung und Verbindungstyp.

3.1.29**vermaschtes Netz****(en: mesh)**

durch die Vermittlungsstations- und Gateway-Geräte in dem WIA-PA-Netz gebildete Topologie

Anmerkung 1 zum Begriff: Ein Vermittlungsstationsgerät kann mit dem Gateway-Gerät und mit mehreren anderen Vermittlungsstationsgeräten verbunden sein.

3.1.30**Multicast****(en: multicast)**

gleichzeitiges Senden eines Pakets an eine Gruppe von WIA-PA-Geräten

3.1.31**Netzwerkadresse****(en: network address)**

16 Bit lange ganze Zahl ohne Vorzeichen zur eindeutigen Identifizierung des Gerätes im WIA-PA-Netz, die auch als Kurzadresse bezeichnet wird

Anmerkung 1 zum Begriff: Die 8 höchstwertigsten Bits der Netzwerkadresse, die vom Netzmanager zugeordnet sind, kennzeichnen die unterschiedlichen Cluster.

3.1.32**Netzmanager****(en: network manager)**

logische Funktionseinheit zur Konfiguration des Netzes, Zuordnung der Kommunikationsbetriebsmittel, zum Verwalten der Vermittlungstabellen sowie zur Überwachung und Berichterstattung über den Zustand des Netzes

3.1.33**Paket****(en: packet)**

formatierte, aggregierte Bits, die gleichzeitig zusammen über das physikalische Medium übertragen werden

[IEEE STD 802.15.4-2011, 3.31]

3.1.34**Paketlebenszeit****(en: packet lifecycle)**

maximale Lebenszeit des Pakets von der Generierung bis zur Löschung

3.1.35**passiver Austritt****(en: passive leaving)**

Verfahren, bei dem ein mit dem Netz aktiv verbundenes Feldgerät durch sein Vermittlungsstationsgerät oder ein mit dem Netz aktiv verbundenes Vermittlungsstationsgerät durch das Gateway-Gerät angewiesen wird das Netz zu verlassen

3.1.36

physikalische Adresse

(en: **physical address**)

EUI-64-Adresse mit 64 Bits zur eindeutigen Identifizierung des Geräts im WIA-PA-Netz, die auch als lange Adresse bezeichnet wird

Anmerkung 1 zum Begriff: Die Physikalische Adresse wird vom Hersteller zugewiesen.

3.1.37

Vermittlungsstationsgerät

(en: **routing device**)

Gerät, das die Pakete von einem WIA-PA-Gerät zu einem anderen Gerät im WIA-PA-Netz vermittelt

3.1.38

Sicherheitsmanager

(en: **security manager**)

logische Funktionseinheit zur Konfiguration der Sicherheitsstrategien für das gesamte Netz, Verwaltung der Schlüssel und Authentifizierung der Geräte

3.1.39

Überrahmen

(en: **superframe**)

Zuordnung von sich in einem Zeitablauf wiederholenden Zeitschlitz

Anmerkung 1 zum Begriff: Dieser legt die Sende- bzw. Empfangszeit der periodischen Kommunikation fest.

3.1.40

Zeitschlitz

(en: **timeslot**)

Basiszeiteinheit des Datenaustausches

Anmerkung 1 zum Begriff: Deren Dauer ist innerhalb des WIA-PA-Netzwerks konfigurierbar.

3.1.41

Zeitschlitzsprungverfahren

(en: **timeslot hopping**)

regelmäßiges Wechseln der Sende-/Empfangsfrequenz pro Zeitschlitz, um Interferenz und Fading zu vermeiden

3.1.42

Unicast

(en: **unicast**)

senden eines Pakets an ein einzelnes Gerät im WIA-PA-Netz

3.1.43

virtuelle Kommunikationsbeziehung

(en: **virtual communication relation**)

Kommunikationswege und Kommunikationsbetriebsmittel zwischen zwei Benutzer-Anwendungsobjekten

3.1.44

WIA-PA-Gerät

(en: **WIA-PA device**)

Gerät im WIA-PA-Netz

Anmerkung 1 zum Begriff: Zum Beispiel Host-Konfigurationsrechner, Gateway-Gerät, Vermittlungsstationsgerät, Feldgerät oder Handgerät.

– Leerseite –

CONTENTS

FOREWORD.....	13
1 Scope.....	15
2 Normative references	15
3 Terms, definitions and abbreviations	15
3.1 Terms and definitions.....	15
3.2 Abbreviations.....	19
4 Definition of data types.....	21
5 WIA-PA overview.....	21
5.1 Device types	21
5.2 Network topology	21
5.3 Protocol architecture.....	23
5.4 Interconnection	23
6 System management	24
6.1 General.....	24
6.2 Framework of system management.....	26
6.3 Joining process.....	27
6.3.1 Provisioning process	27
6.3.2 Joining process of routing device.....	27
6.3.3 Joining process of field device	28
6.3.4 Addressing and address assignment.....	29
6.4 Virtual Communication Relationship (VCR)	30
6.4.1 Definition	30
6.4.2 Protocol support for VCR	31
6.4.3 VCR establishment	31
6.4.4 VCR release	32
6.5 Routing configuration and communication resource allocation.....	32
6.5.1 Routing configuration.....	32
6.5.2 Framework of communication resource allocation	32
6.5.3 DLPDU priority and scheduling rules	33
6.5.4 Communication resource allocation to routing device.....	33
6.5.5 Communication resource allocation to field device	34
6.6 Aggregation and disaggregation.....	37
6.6.1 Aggregation	37
6.6.2 Disaggregation	39
6.6.3 An example of the two level aggregation process	39
6.6.4 Management of aggregation and disaggregation objects.....	41
6.7 Performance monitoring	43
6.7.1 Path failure report.....	43
6.7.2 Device status report.....	43
6.7.3 Channel condition report.....	44
6.8 Leaving process.....	44
6.8.1 General	44
6.8.2 Leaving process of routing device.....	44
6.8.3 Leaving process of field device	46
6.9 Management information base and services.....	47
6.9.1 Management information base	47

6.9.2	MIB services	60
7	Physical Layer	63
7.1	General	63
7.2	General requirements based on IEEE STD 802.15.4-2011	63
7.3	Additional requirements	65
8	Data link layer	67
8.1	General	67
8.2	Protocol stack	67
8.3	MAC overview and function extension	67
8.3.1	MAC overview	67
8.3.2	General requirements based on IEEE STD 802.15.4-2011	68
8.3.3	MAC function extension	71
8.4	DLSL function description	72
8.4.1	General	72
8.4.2	Coexistence	72
8.4.3	Timeslot communication	73
8.4.4	WIA-PA superframe	73
8.4.5	Frequency hopping	74
8.4.6	Transmission of long cycle data	75
8.4.7	Retry strategy	76
8.4.8	Management service	76
8.4.9	Radio link quality and channel condition measurement	76
8.4.10	Security	76
8.4.11	Country code	76
8.4.12	DLSL state machine	77
8.5	Data link sub-layer data services	83
8.5.1	General	83
8.5.2	DLDE-DATA.request	83
8.5.3	DLDE-DATA.confirm	85
8.5.4	DLDE-DATA.indication	86
8.5.5	Time sequence of DSL data service	87
8.6	Data link sub-layer management services	87
8.6.1	General	87
8.6.2	Network discovery services	87
8.6.3	Device joining services	89
8.6.4	Device leaving services	91
8.6.5	DLME-CHANNEL-CONDITION.indication	93
8.6.6	DLME-NEIGHBOUR-INFO.indication	93
8.6.7	DLME-COMM-STATUS.indication	93
8.6.8	Keep-alive services	94
8.6.9	Time synchronization services	95
8.7	DLSL frame formats	96
8.7.1	General frame format	96
8.7.2	Data frame format	96
8.7.3	Command frame format	97
9	Network layer	99
9.1	General	99
9.2	Protocol stack	99
9.3	Function description	99

9.3.1	General	99
9.3.2	Addressing	100
9.3.3	Routing	100
9.3.4	Packet lifecycle management	101
9.3.5	Joining and leaving network of device	101
9.3.6	End-to-end network performance monitoring	101
9.3.7	Fragmentation and reassembly	101
9.3.8	Network layer state machine	101
9.4	Network layer data services	107
9.4.1	General	107
9.4.2	NLDE-DATA.request	107
9.4.3	NLDE-DATA.confirm	108
9.4.4	NLDE-DATA.indication	108
9.4.5	Time sequence of NL data services	109
9.5	Network layer management services	109
9.5.1	General	109
9.5.2	Network communication status report services	109
9.5.3	Network joining services	111
9.5.4	Network leaving services	116
9.5.5	Cluster member report services	120
9.5.6	Neighbour information report services	122
9.5.7	Route allocation services	124
9.5.8	Communication resource allocation services	129
9.5.9	Aggregation and disaggregation services	142
9.5.10	Device status report services	144
9.5.11	Channel condition report services	145
9.5.12	Failure path report services	147
9.5.13	Network attribute getting services	149
9.5.14	Network attribute setting services	152
9.6	Network layer packet formats	154
9.6.1	Common packet format	154
9.6.2	Data packet format	155
9.6.3	Aggregated packet format	155
9.6.4	Command packet format	156
10	Application Layer	173
10.1	Overview	173
10.1.1	General	173
10.1.2	AL structure	173
10.1.3	Functions of UAP	173
10.1.4	Functions of ASL	174
10.2	UAP	174
10.2.1	General	174
10.2.2	UAO	174
10.2.3	Method definition	175
10.3	Application sub-layer	178
10.3.1	General	178
10.3.2	Application sub-layer data entity	178
10.4	Application sub-layer packet formats	183
10.4.1	General	183

10.4.2	ASL general packet format	184
10.4.3	Packet formats	185
11	Security	187
11.1	General	187
11.2	Security management framework	187
11.3	Secure communication protocol stack	189
11.3.1	General	189
11.3.2	Data link sub-layer security	189
11.3.3	Application sub-layer security	191
11.4	Key management	191
11.4.1	Key type	191
11.4.2	Key distribution	193
11.4.3	Key update	193
11.4.4	Key status	193
11.5	Secure joining process	194
11.5.1	Secure joining process of a new WIA-PA device	194
11.5.2	Device security material getting services	195
11.6	Secure transportation	201
11.6.1	Process of secure transportation from field device to host configuration computer	201
11.6.2	Process of secure transportation from host configuration computer to field device	202
Annex A (informative)	Security strategy for WIA-PA network	203
A.1	Risk analysis for WIA-PA network	203
A.2	Security principles for WIA-PA network	203
A.3	Security objectives for WIA-PA network	203
A.4	Graded and layered security system	203
Annex B (informative)	Format description	205
B.1	Time sequence diagram	205
B.2	Packet or frame format	205
Annex C (informative)	Example of UAO	207
C.1	General	207
C.2	Analog input object	207
C.2.1	Overview	207
C.2.2	Class attribute of AIO	207
C.2.3	Instance attribute of AIO	207
Annex D (informative)	Country-specific and region-specific provisions	209
Annex E (informative)	Regional modification for compliance with ETSI standards	210
E.1	General	210
E.2	Compliance with EN 300 440-2 V1.4.1	210
E.3	Compliance with EN 300 328 V1.8.1	210
Bibliography		212
Figure 1	– Example of WIA-PA physical topology (combination of star and mesh)	22
Figure 2	– Example of WIA-PA physical topology (star-only)	22
Figure 3	– OSI basic reference model mapped to WIA-PA	23
Figure 4	– The architecture of WIA-PA gateway	24
Figure 5	– DMAP in system management	

Figure 6 – Hybrid centralized and distributed system management scheme	26
Figure 7 – Joining process of routing device through the gateway device.....	28
Figure 8 – Joining process of routing device through an online routing device	28
Figure 9 – Joining process of field device through a gateway device.....	29
Figure 10 – Joining process of field device through a routing device	29
Figure 11 – Long address structure of device.....	29
Figure 12 – Short address structure of routing device	30
Figure 13 – Short address structure of field device	30
Figure 15 – Allocation process of routing device's communication resources	34
Figure 16 – Allocation process of field device's communication resources	36
Figure 17 – Example of aggregation and disaggregation	40
Figure 18 – Process of path failure report	43
Figure 19 – Device status report process of field device	43
Figure 20 – Device status report process of routing device	43
Figure 21 – Process of channel condition report	44
Figure 22 – Active leaving process of routing device.....	45
Figure 23 – Passive leaving process of routing device	45
Figure 24 – Active leaving process of field device (leaving from gateway device).....	46
Figure 25 – Active leaving process of field device (leaving from routing device).....	46
Figure 26 – Passive leaving process of field device (leaving from gateway device)	47
Figure 27 – Passive leaving process of field device (leaving from routing device)	47
Figure 28 – WIA-PA DLL protocol stack	67
Figure 29 – WIA-PA DLSL reference model	72
Figure 30 – WIA-PA superframe	73
Figure 31 – R1, R2 and R3 superframe structures	75
Figure 32 – An example of long cycle data transmission	75
Figure 33 – DLSL state machine for device joining.....	78
Figure 34 – DLSL state machine for in-network running	80
Figure 35 – Time sequence of data service.....	87
Figure 36 – Time sequence of network discovery.....	89
Figure 37 – General frame format	96
Figure 38 – WIA-PA network layer protocol stack.....	99
Figure 39 – WIA-PA Network layer reference model.....	99
Figure 40 – Network layer state machine	102
Figure 41 – Time sequence of NL data services.....	109
Figure 42 – Time sequence for field device joining through routing device	114
Figure 43 – One-hop joining process for routing device.....	115
Figure 44 – Multi-hop join process of routing device	116
Figure 45 – Active leaving process of field device (leaving routing device).....	119
Figure 46 – Passive leaving of field device	119
Figure 47 – Active leaving process of routing device.....	120
Figure 48 – Passive leaving process of routing device	120
Figure 49 – Cluster member reporting process.....	122

Figure 50 – Neighbour information reporting process	124
Figure 51 – Time sequence for route adding	125
Figure 52 – Time sequence for route updating	127
Figure 53 – Time sequence for route deleting	129
Figure 54 – Adding a link originated from gateway device to routing device	131
Figure 55 – Adding a link originated from routing device to field device.....	132
Figure 56 – Updating a link originated by gateway device to routing device	134
Figure 57 – Updating a link originated from routing device to field device	134
Figure 58 – Releasing a link originated from gateway device to routing device.....	136
Figure 59 – Releasing a link originated from routing device to field device	136
Figure 60 – Adding a superframe originated from gateway device to routing device	138
Figure 61 – Adding a superframe originated from routing device to field device	138
Figure 62 – Updating a superframe originated from gateway device to routing device	140
Figure 63 – Updating a superframe originated from routing device to field device	140
Figure 64 – Releasing a superframe originated from gateway device to routing device	142
Figure 65 – Releasing a superframe originated from routing device to field device.....	142
Figure 66 – Device status reporting process from field device to routing device	145
Figure 67 – Device status reporting process from routing device to gateway device.....	145
Figure 68 – Channel condition reporting process from field device to routing device	147
Figure 69 – Channel condition reporting process from routing device to gateway device.....	147
Figure 70 – Failure path reporting process.....	149
Figure 71 – AL structure	173
Figure 72 – User application process	174
Figure 73 – C/S communication process	182
Figure 74 – P/S communication process (disable aggregation function)	182
Figure 75 – P/S communication process (enable aggregation function).....	183
Figure 76 – R/S communication process	183
Figure 77 – Security management framework of WIA-PA network	188
Figure 78 – Security communication protocol stack.....	189
Figure 79 – Key lifecycle.....	193
Figure 80 – Secure joining process of WIA-PA device.....	194
Figure 81 – Time sequence for field device joining (Field device to routing device).....	197
Figure 82 – Time sequence for field device joining (Routing device to gateway device)	198
Figure 83 – One-hop joining process for routing device.....	199
Figure 84 – Multi-hop join process of routing device (new routing device to routing device).....	200
Figure 85 – Multi-hop join process of routing device (routing device to gateway device)	201
Figure B.1 – Time sequence diagram.....	205
Table 1 – Definition of data types.....	21
Table 2 – Protocol support for VCR.....	31
Table 3 – Relations between VCR and aggregation function	37
Table 4 – Format of aggregated data followed by field device's DAGO	39

Table 5 – Format of aggregated packet followed by routing device's PAGO	39
Table 6 – DAGO class attributes	41
Table 7 – DAGO instance attributes	41
Table 8 – MEM_STRUCT structure	42
Table 9 – PAGO class attributes	42
Table 10 – PAGO instance attributes	42
Table 11 – DGO class attributes	42
Table 12 – DGO instance attributes	43
Table 13 – Unstructured attributes	48
Table 14 – Structured attributes	52
Table 15 – NLRoute_Struct structure	53
Table 16 – Superframe_Struct structure	53
Table 17 – Link_Struct structure	54
Table 18 – Neighbour_Struct structure	55
Table 19 – ChanCon_Struct structure	55
Table 20 – Device_struct structure	56
Table 21 – VCR_Struct structure	58
Table 22 – DevConRep_Struct structure	59
Table 23 – Key_Struct structure	59
Table 24 – ObjList_Struct structure	59
Table 25 – DMAP-MIB-GET.request parameters	60
Table 26 – DMAP-MIB-GET.confirm parameters	62
Table 27 – DMAP-MIB-SET.request parameters	62
Table 28 – DMAP-MIB-SET.confirm parameters	63
Table 29 – PHY protocol selection	64
Table 30 – Frequency band and data rate	65
Table 31 – Frequency assignments	65
Table 32 – PHY PIB attributes	66
Table 33 – MAC protocol selection	68
Table 34 – MAC PIB attributes	70
Table 35 – MAC extendedPIB attributes	71
Table 36 – Beacon payload	71
Table 37 – Format of capability information field	71
Table 38 – Hopping mechanisms	74
Table 39 – DLSSL state transitions for device joining	79
Table 40 – DLSSL state transitions for in-network running	80
Table 41 – DLDE-DATA.request parameters	85
Table 42 – DLDE-DATA.confirm parameters	85
Table 43 – Status table	86
Table 44 – DLDE-DATA.indication parameters	86
Table 45 – DLME-DISCOVERY.request parameters	88
Table 46 – DLME- DISCOVERY.confirm parameters	88
Table 47 – Network descriptor list	88

Table 48 – DLME-JOIN.request parameters	90
Table 49 – DLME-JOIN.indication parameters	90
Table 50 – DLME-JOIN.response parameters	91
Table 51 – DLME-JOIN.confirm parameters	91
Table 52 – DLME-LEAVE.request parameters	92
Table 53 – DLME-LEAVE.indication parameters	92
Table 54 – DLME-LEAVE.confirm parameters	92
Table 55 – DLME-CHANNEL-CONDITION.indicationparameters	93
Table 56 – DLME-NEIGHBOUR-INFO.indication parameters	93
Table 57 – DLME-COMM-STATUS.indication parameters	94
Table 58 – DLME -KEEP-LIVE.confirm parameters	94
Table 59 – DLME -KEEP-LIVE.indication parameters	94
Table 60 – DLME-TIME-SYN.request parameters	95
Table 61 – DLME -TIME-SYN.confirm parameters	95
Table 62 – DLME-TIME-SYN.indication parameters	96
Table 63 – DLSL frame control field	96
Table 64 – Date frame format	97
Table 65 – General command frame format	97
Table 66 – DLSL command frame	97
Table 67 – Format of keep-alive command frame	98
Table 68 – Format of time synchronization command frame	98
Table 69 – Example of a routing table	100
Table 70 – NL state transitions	103
Table 71 – NLDE-DATA.request parameters	108
Table 72 – NLDE-DATA.confirm parameters	108
Table 73 – NLDE-DATA.indication parameters	109
Table 74 – NLME-COMM-STATUS.request parameters	109
Table 75 – NLME-COMM-STATUS.indication parameters	110
Table 76 – NLME-COMM-STATUS.confirm parameters	111
Table 77 – NLME-JOIN.request parameters	111
Table 78 – NLME-JOIN.indication parameters	112
Table 79 – NLME-JOIN.response parameters	112
Table 80 – NLME-JOIN.confirm parameters	113
Table 81 – NLME-LEAVE.request parameters	116
Table 82 – NLME-LEAVE.indication parameters	117
Table 83 – NLME-LEAVE.response parameters	117
Table 84 – NLME-LEAVE.confirm parameters	117
Table 85 – NLME-RPT-CLRMEM.request parameters	121
Table 86 – NLME-RPT-CLRMEM.confirm parameter	121
Table 87 – NLME-RPT-CLRMEM.response parameters	122
Table 88 – NLME-NEIGHBOUR-INFO.request parameters	123
Table 89 – NLME-NEIGHBOUR-INFO.confirm parameter	123
Table 90 – NLME-ADD_ROUTE.request parameters	124

Table 91 – NLME-ADD_ROUTE.confirm parameters	124
Table 92 – NLME-UPDATE_ROUTE.request parameters	126
Table 93 – NLME-UPDATE_ROUTE.confirm parameter	126
Table 94 – NLME-UPDATE_ROUTE.request parameters	127
Table 95 – NLME-DELETE_ROUTE.confirm parameters	128
Table 96 – NLME-ADD-LINK.request parameters	130
Table 97 – NLME-ADD-LINK.confirm parameters	130
Table 98 – NLME-UPDATE-LINK.request parameters	132
Table 99 – NLME-UPDATE-LINK.confirm parameters	133
Table 100 – NLME-RELEASE-LINK.request parameters	134
Table 101 – NLME-RELEASE-LINK.confirm parameters	135
Table 102 – NLME-ADD-SFR.request parameters	137
Table 103 – NLME-ADD-SFR.confirm parameters	137
Table 104 – NLME-UPDATA-SFR.request parameters	139
Table 105 – NLME-UPDATE-SFR.confirm parameters	139
Table 106 – NLME-RELEASE-SFR.request parameters	141
Table 107 – NLME-RELEASE-SFR.confirm parameters	141
Table 108 – NLME-AGG.indication parameters	143
Table 109 – NLME-AGO-SEND.request parameters	143
Table 110 – NLME-DAG.indication parameter	144
Table 111 – NLME-DEVICE -STATUS.request parameters	144
Table 112 – NLME-DEVICE -STATUS.indication parameters	144
Table 113 – NLME-DEVICE -STATUS.confirm parameter	145
Table 114 – NLME-CHANNEL-CONDITION.request parameters	146
Table 115 – NLME-CHANNEL-CONDITION.indication parameters	146
Table 116 – NLME-CHANNEL-CONDITION.confirm parameter	146
Table 117 – NLME-PATH_FAILURE.request parameters	148
Table 118 – NLME-PATH_FAILURE.indication parameters	148
Table 119 – NLME-PATH_FAILURE.confirm parameters	148
Table 120 – NLME-INFO_GET.request parameters	149
Table 121 – NLME-INFO_GET.indication parameters	150
Table 122 – NLME-INFO_GET.response parameters	150
Table 123 – NLME-INFO_GET.confirm parameters	151
Table 124 – NLME-INFO_SET.request parameters	152
Table 125 – NLME-INFO_SET.indication parameters	152
Table 126 – NLME-SET.response parameters	153
Table 127 – NLME-SET.confirm parameters	154
Table 128 – Network layer common packet format	154
Table 129 – Control field format	154
Table 130 – Network layer data packet format	155
Table 131 – Aggregated packet format	156
Table 132 – Format of NL command packet	156
Table 133 – Network layer command packet	157

Table 134 – Execution results of commands	158
Table 135 – Format of joining request packet.....	158
Table 136 – Format of joining response packet.....	158
Table 137 – Format of communication status report request packet	159
Table 138 – Format of leaving request packet.....	159
Table 139 – Value of Leaving reason	161
Table 140 – Format of leaving response packet	161
Table 141 – Format of cluster member report request packet.....	161
Table 142 – Format of cluster member report response packet	162
Table 143 – Format of neighbour information report request packet.....	162
Table 144 – Format of route adding request packet	162
Table 145 – Format of route adding response packet.....	163
Table 146 – Format of route update request packet	163
Table 147 – Format of route update response packet.....	163
Table 148 – Format of route deleting request packet	164
Table 149 – Format of route deleting response packet.....	164
Table 150 – Format of link adding request packet	165
Table 151 – Format of link adding response packet	165
Table 152 – Format of link update request packet.....	165
Table 153 – Format of link update response packet	166
Table 154 – Format of link release request packet.....	166
Table 155 – Format of link release response packet	166
Table 156 – Format of superframe adding request packet.....	167
Table 157 – Format of superframe adding response packet	167
Table 158 – Format of superframe update request packet.....	168
Table 159 – Format of superframe update response packet	168
Table 160 – Format of superframe release request packet.....	168
Table 161 – Format of superframe release response packet	169
Table 162 – Format of device condition report request packet.....	169
Table 163 – Format of device condition information field.....	169
Table 164 – Format of channel condition report request packet	170
Table 165 – Format of channel quality information field	170
Table 166 – Format of path failure report request packet	171
Table 167 – Format of attribute getting request packet	171
Table 168 – Format of attribute getting response packet.....	171
Table 169 – Format of attribute setting request packet.....	172
Table 170 – Format of attribute setting response packet.....	172
Table 171 – UAO method definition.....	175
Table 172 – Request format of READ method	176
Table 173 – Response format of READ method	176
Table 174 – Request format of WRITE method	176
Table 175 – Response format of WRITE method.....	177
Table 176 – Format of PUBLISH method	177

Table 177 – Format of REPORT method	178
Table 178 – Format of REPORT ACK method	178
Table 179 – ASLDE-DATA.request parameters	179
Table 180 – ASLDE-DATA.confirm parameters	179
Table 181 – ASLDE-DATA.indication parameters	180
Table 182 – ASLDE-AGG.request parameters	180
Table 183 – ASLDE-DAG.indication parameters	181
Table 184 – Application sub-layer general packet format	184
Table 185 – Packet control field format	184
Table 186 – Packet type subfield value	185
Table 187 – ASL data packet format	186
Table 188 – ASL acknowledgement packet format	186
Table 189 – Format of security DLPDU	190
Table 190 – Format of DLSL security header	190
Table 191 – Structure of security control field in DLSL security header	190
Table 192 – Structure of security material control field in DLSL security header	190
Table 193 – Security APDU structure	191
Table 194 – Structure of ASL security header field	191
Table 195 – DLME-SEC.request parameters	195
Table 196 – DLME-SEC.indication parameters	195
Table 197 – DLME-SEC.response parameters	196
Table 198 – DLME-SEC.confirm parameters	196
Table A.1 – Graded and layered security measures for WIA-PA network	204
Table A.2 – Security levels of data packets	204
Table B.1 – Packet or frame format in octet(s)	205
Table B.2 – Subfield format in bit(s)	206
Table C.1 – AIO Class Attribute	207
Table C.2 – AIO Instance Attributes	208
Table E.1 – Applicable EN 300 440-2 requirements list	210
Table E.2 – Applicable EN 300 328 requirements list	210
Table E.3 – Timeslot timing definitions and calculations	211

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**Industrial communication networks –
Wireless communication network and communication profiles –
WIA-PA**

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 62601 has been prepared by subcommittee 65C: Industrial networks, of IEC technical committee 65: Industrial process measurement, control and automation.
- This second edition cancels and replaces the first edition published in 2011. This edition constitutes a technical revision.
- This edition includes the following significant technical changes with respect to the previous edition:
- Changed IEEE STD 802.15.4-2006 to IEEE STD 802.15.4-2011 and added common modification for IEEE STD 802.15.4-2011 MAC profile, PHY profile and IEEE STD 802.15.4-2011 related references.
 - Added common modifications for regional adoption and added Annex D and Annex E.
 - Deleted extended MAC management services and added two DLSS management services.
 - Added specific state machines for DLSS and NL.

- Unified representation of frame format and packet format.
- Changed format of definition of data types.
- Added detailed description of technologies for clearly understanding.
- Provided support for CCA modes 1, 2, and 3.

The reader's attention is drawn to the fact that Annex E lists all of the “in-some-country” clauses on differing practices of a less permanent nature relating to the subject of this standard.

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

FDIS	Report on voting
65C/xxx/FDIS	65C/xxx/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.

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

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

The National Committees are requested to note that for this publication the stability date is 2018.

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

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.

**Industrial communication networks –
Wireless communication network and communication profiles –
WIA-PA**

1 Scope

This International Standard specifies the system architecture and the communication protocol of Wireless networks for Industrial Automation – Process Automation (WIA-PA) that is built on IEEE STD 802.15.4-2011.

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 9899 *Information technology – Programming languages - C*

IEEE STD 802.15.4-2011, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

3.1.1

Absolute timeslot number

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

3.1.2

active leaving

process by which an online field device is allowed to leave the network through applying to its routing device or by which an online routing device is allowed to leave the network through applying to the gateway device

3.1.3

adaptive frequency hopping

change of communication channels according to actual condition of channels in every timeslot during the intra-cluster period of WIA-PA superframe

3.1.4

adaptive frequency switch

change of communication channels according to the actual condition of channels during the beacon frame and active period in a superframe cycle, and using different channels in different superframe cycles

3.1.5

aggregation

merging of data from multiple user application objects or merging of several packets from cluster members into one packet

3.1.6

application sub-layer

protocol sub-layer that provides data and management services for the application layer

- 131 **3.1.7**
132 **beacon**
133 special frame broadcast by the routing devices or the gateway device in the WIA-PA network
- 134 **3.1.8**
135 **broadcast**
136 sending one packet to all WIA-PA devices simultaneously
- 137 **3.1.9**
138 **channel**
139 RF medium used to convey a packet from a sender to a receiver
- 140 **3.1.10**
141 **cluster**
142 logical group of devices that is comprised of a routing device and field devices
- 143 **3.1.11**
144 **cluster head**
145 manager in a cluster, performed by the routing device
- 146 **3.1.12**
147 **cluster member**
148 data source in a cluster, performed by a field device
- 149 **3.1.13**
150 **coexistence**
151 ability of one network to perform its task in a given shared environment without disturbing or
152 being disturbed by other networks
- 153 Note 1 to entry: These networks may or may not have the same set of rules.
- 154 **3.1.14**
155 **communication resource**
156 channels and timeslots used to transport a frame
- 157 **3.1.15**
158 **WIA-PA configuration software**
159 software tool for configuring a WIA-PA network and devices
- 160 **3.1.16**
161 **data link sub-layer**
162 upper layer of the IEEE STD 802.15.4-2011 MAC layer, used to handle the aspects of network
163 topology and communication resources in the WIA-PA network
- 164 **3.1.17**
165 **disaggregation**
166 dividing the merged packet into data of user application objects
- 167 **3.1.18**
168 **field device**
169 device usable in the field, which is connected to or controls the process
- 170 **3.1.19**
171 **frame**
172 format of aggregated bits from the medium access control (MAC) entity that are transmitted
173 together in time
- 174 [SOURCE: IEEE STD 802.15.4-2011]
- 175 **3.1.20**
176 **Frequency hopping**
177 change of transmitting/receiving frequency to combat interference and fading

- 178 **3.1.21**
179 **gateway device**
180 device connecting the WIA-PA network to other plant networks
- 181 **3.1.22**
182 **handheld device**
183 portable device used for provisioning, firmware updating, and device status monitoring
- 184 **3.1.23**
185 **hop**
186 movement of a packet directly between two adjacent neighbour devices in one network
187 transaction without the participation of any other devices in the WIA-PA network
- 188 Note 1 to entry: Multiple hops are used to lengthen the transmission distance, bypass interference sources or
189 avoid obstructions.
- 190 **3.1.24**
191 **host configuration computer**
192 device through which users and maintenance/management personnel perform transactions on
193 the WIA-PA network and the management networks
- 194 **3.1.25**
195 **interconnectable**
196 using the same communication protocols, communication interface and data access
- 197 [SOURCE: IEC/TR 62390:2005, 6.2.2, adapted]
- 198 **3.1.26**
199 **interoperable**
200 able to work together to perform a specific role in one or more distributed application
201 programs
- 202 Note 1 to entry: In this case parameters and their application-related functionality fit together both syntactically
203 and semantically. Interoperability is achieved when the devices support complementary sets of parameters
204 and functions belonging to the same profile.
- 205 [SOURCE: IEC/TR 62390:2005, 6.2.2, adapted]
- 206 **3.1.27**
207 **joining**
208 process by which a WIA-PA device is authenticated and allowed to participate in the WIA-PA
209 network
- 210 **3.1.28**
211 **link**
212 set of communication parameters necessary to transport a frame between adjacent devices in
213 the network
- 214 Note 1 to entry: It includes source/destination address, timeslot, channel, direction, and link type.
- 215 **3.1.29**
216 **mesh**
217 topology formed by routing devices and the gateway device in the WIA-PA network
- 218 Note 1 to entry: One routing device may connect to the gateway device and more than one other routing device.
- 219 **3.1.30**
220 **multicast**
221 sending one packet to a group of WIA-PA devices simultaneously
- 222 **3.1.31**
223 **network address**
224 16-bit unsigned integer uniquely identifying the device in the WIA-PA network; also called
225 short address
- 226 Note 1 to entry: The most significant 8 bits of the network address, assigned by the network manager, identify
227 different clusters.

- 228 **3.1.32**
229 **network manager**
230 logical role for configuring the network, allocating the communication resources, managing the
231 routing tables, and monitoring and reporting the health of the network
- 232 **3.1.33**
233 **packet**
234 formatted, aggregated bits that are transmitted together in time across the physical medium
235 [IEEE STD 802.15.4-2011, 3.31]
- 236 **3.1.34**
237 **packet lifecycle**
238 maximal packet survival time from being generated to being dropped
- 239 **3.1.35**
240 **passive leaving**
241 process by which an online field device is instructed by its routing device to leave the network
242 or by which an online routing device is instructed by the gateway device to leave the network
- 243 **3.1.36**
244 **physical address**
245 EUI-64 bits uniquely identifying the device in the WIA-PA network; also called long address
246 Note 1 to entry: A physical address is assigned by a manufacturer.
- 247 **3.1.37**
248 **routing device**
249 device forwarding packets from one WIA-PA device to another in the WIA-PA network
- 250 **3.1.38**
251 **security manager**
252 logical role for configuring the security strategies of the whole network, managing keys, and
253 authenticating devices
- 254 **3.1.39**
255 **superframe**
256 collection of timeslots repeating over time
257 Note 1 to entry: It specifies the transmitting or receiving time of periodic communication.
- 258 **3.1.40**
259 **timeslot**
260 basic time unit of data exchange
261 Note 1 to entry: Its duration is configurable in the WIA-PA network.
- 262 **3.1.41**
263 **timeslot hopping**
264 regular change of transmitting/receiving frequency per timeslot to avoid interference and
265 fading
- 266 **3.1.42**
267 **unicast**
268 sending one packet to a single device in the WIA-PA network
- 269 **3.1.43**
270 **virtual communication relation**
271 communication paths and communication resources between two user application objects
- 272 **3.1.44**
273 **WIA-PA device**
274 device in the WIA-PA network

275 Note 1 to entry: For example, the host configuration computer, gateway device, routing device, field device or
276 handheld device.

277 3.2 Abbreviations

278	ACK	Acknowledge
279	AFH	Adaptive Frequency Hopping
280	AFS	Adaptive Frequency Switch
281	AIO	Analog Input Object
282	AL	Application Layer
283	AOO	Analog Output Object
284	ASDU	Application Service Data Unit
285	ASL	Application Sub-Layer
286	ASLDE	Application Sub-Layer Data Entity
287	ASLDE-SAP	ASLDE Service Access Point
288	ASLME	Application Sub-Layer Management Entity
289	ASLME-SAP	ASLME Service Access Point
290	ASLPDU	Application Sub-Layer Protocol Data Unit
291	ASN	Absolute timeSlot Number
292	CAP	Contention Access Period
293	CFP	Contention Free Period
294	C/S	Client/Server
295	CSMA	Carrier Sense Multiple Access
296	CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
297	DAGO	Data AggreGation Object
298	DGO	DisaGgregation Object
299	DIO	Digital Input Object
300	DLDE	Data Link Sub-Layer Data Entity
301	DLDE-SAP	DLDE Service Access Point
302	DLL	Data Link Layer
303	DLME	Data Link Sub-Layer Management Entity
304	DLME-SAP	DLME Service Access Point
305	DLPDU	Data Link Sub-Layer Protocol Data Unit
306	DLSL	Data Link Sub-Layer
307	DMAP	Device Management Application Process
308	DOO	Digital Output Object
309	ENC	ENCryption
310	EUI-64	Extended Unique Identifier-64 bits
311	FCS	Frame Check Sequence
312	FDMA	Frequency Division Multiple Access
313	FFD	Full-Function Device
314	FH	Frequency Hopping
315	GTS	Guaranteed Time Slot
316	GW	GateWay device
317	ID	IDentifier

318	IDS	Intrusion Detection System
319	KED	Data Encryption Key
320	KEK	Key Encryption Key
321	KJ	Join Key
322	KS	Share Key
323	LME-SAP	Layer Management Entity Service Access Point
324	LSB	Least Significant Bit
325	LQI	Link Quality Indication
326	MAC	Medium Access Control sub-layer
327	MCPS	MAC Common Part Sub-layer
328	MHR	Medium Access Control Header
329	MIB	Management Information Base
330	MIC	Message Integrity Code
331	MLDE	MAC sub-Layer Data Entity
332	MLDE-SAP	MLDE Service Access Point
333	MLME	MAC sub-Layer Management Entity
334	MLME-SAP	MLME Service Access Point
335	MPDU	MAC Protocol Data Unit
336	MSB	Most Significant Bit
337	NL	Network Layer
338	NLDE	Network Layer Data Entity
339	NLDE-SAP	NLDE Service Access Point
340	NLME	Network Layer Management Entity
341	NLME-SAP	NLME Service Access Point
342	NMNetwork	Manager
343	NPDU	Network Protocol Data Unit
344	NSDU	Network Service Data Unit
345	PAGO	Packet AGgregation Object
346	PAN	Personal Area Network
347	PHY	PHYsical layer
348	PIB	PAN Information Base
349	P/S	Publisher/Subscriber
350	RFD	Reduced-Function Device
351	R/S	Report source/Sink
352	SAP	Service Access Point
353	SMSecurity	Manager
354	TDMA	Time Division Multiple Access
355	TH	Timeslot Hopping
356	UAO	User Application Object
357	UAP	User Application Process
358	UAPME-SAP	UAP Management Entity SAP
359	UTC	Universal Time Coordinated
360	VCR	Virtual Communication Relationship

361 VCR_ID Virtual Communication Relationship Identifier
 362 WIA-PA Wireless network for Industrial Automation – Process Automation

363 4 Definition of data types

364 Table 1 gives the WIA-PA definition of data types.

365 **Table 1 – Definition of data types**

Definition of data types (see ISO/IEC 9899)			
Data type		Range of values	Length
Boolean	Boolean	Non 0: TRUE; 0: FALSE	1 octet
Unsigned integer	Unsigned8	$0 \leq i \leq 2^8 - 1$	1 octet
	Unsigned16	$0 \leq i \leq 2^{16} - 1$	2 octets
	Unsigned24	$0 \leq i \leq 2^{24} - 1$	3 octets
	Unsigned32	$0 \leq i \leq 2^{32} - 1$	4 octets
	Unsigned40	$0 \leq i \leq 2^{40} - 1$	5 octets
	Unsigned48	$0 \leq i \leq 2^{48} - 1$	6 octets
	Unsigned64	$0 \leq i \leq 2^{64} - 1$	8 octets
Octetstring	Octetstring	8-bit string	1 octet
Float	Float	Refer to IEEE STD™ 754-2008	4 octets

366 5 WIA-PA overview

367 5.1 Device types

368 The document specifies five types of WIA-PA devices:

- 369 a) host configuration computer;
- 370 b) gateway device(GW);
- 371 c) routing device;
- 372 d) field device; and
- 373 e) handheld device.

374 To improve reliability, there may be redundant gateway devices and redundant routing
 375 devices in the WIA-PA network. A primary device connects its redundant device in the wired
 376 manner. The wired connection is not defined in this document. The short address (see 6.3.4)
 377 of a redundant device is the same as that of its primary device. The start-up time of a
 378 redundant device is not later than that of the primary device. When primary devices run,
 379 redundant devices do not start up their radio modules. When the information of primary
 380 devices is changed, the primary devices should timely backup the changed information to
 381 their redundant devices in the wired manner. The wired manner is not specified in this
 382 document. If SecEnableFlag is enabled, the redundant devices are authenticated (see 11.2).

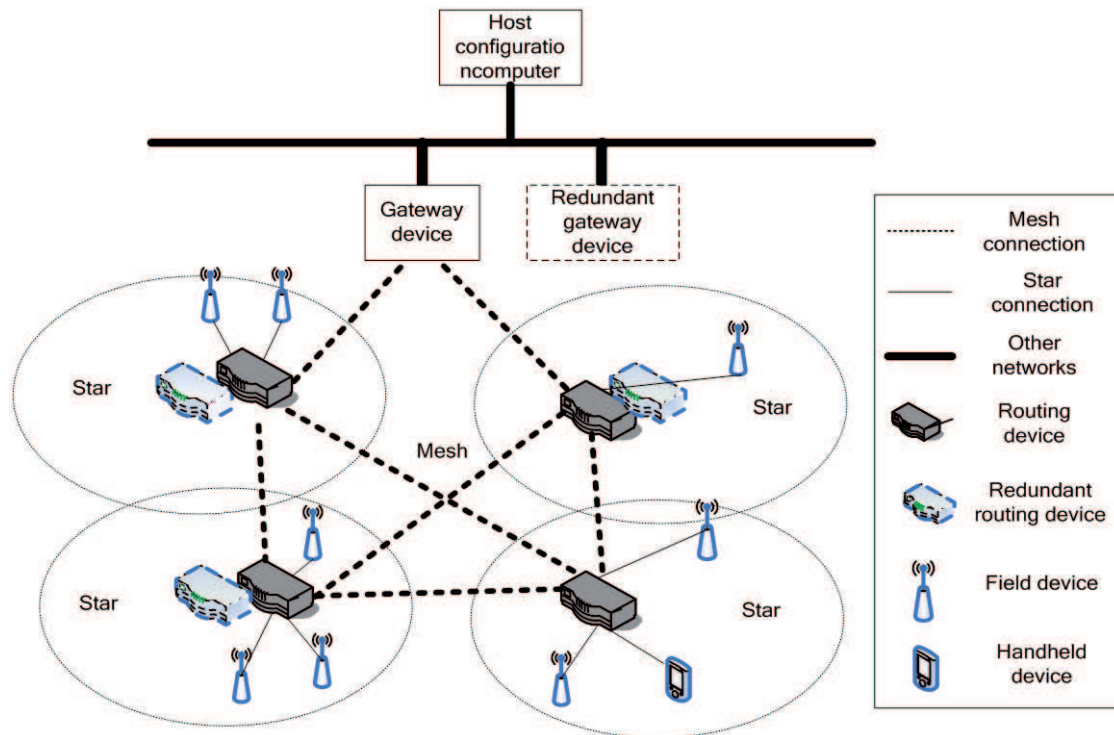
383 5.2 Network topology

384 WIA-PA network supports two different types of network topologies:

- 385 a) a hierarchical network topology that combines star and mesh, and
- 386 b) a star-only network topology.

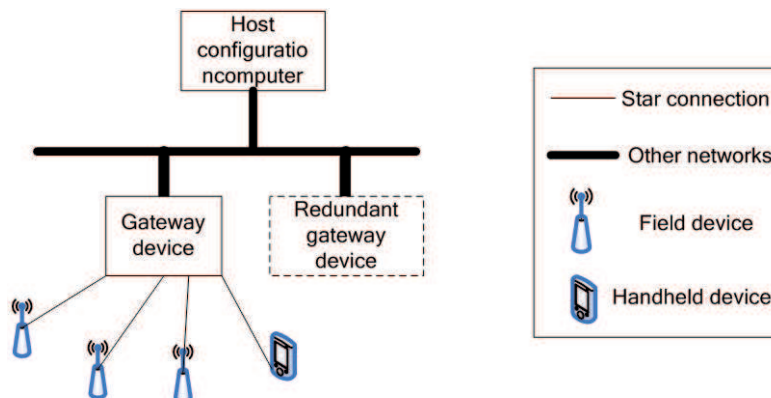
387 The hierarchical network topology that combines star and mesh is illustrated in Figure 1. The
 388 first level of the network is in mesh topology, where routing devices and gateway devices are

389 deployed. The second level of the network is in star topology, where routing devices, field
390 devices, and handheld devices (if they exist) are deployed.



391
392 **Figure 1 – Example of WIA-PA physical topology (combination of star and mesh)**

393 The star-only network is comprised of a gateway device, field devices, and handheld devices
394 (if they exist). The star network topology is illustrated in Figure 2.



395
396 **Figure 2 – Example of WIA-PA physical topology (star-only)**

397 The star-only network is a special case of the hierarchical network. In this document, the
398 specification of the hierarchical network covers the star-only network. Therefore, there is no
399 explicit specification provided for the star-only network.

400 In order to facilitate management, this document specifies five kinds of logical roles:

401 a) Gateway

402 Gateway handles protocol-translation and data-mapping between the WIA-PA network and
403 other networks.

404 b) Network manager

405 Network Manager (NM) manages and monitors the entire network (see 6.2). There should
406 be one and only one network manager per WIA-PA network.

407 c) Security manager

408 Security Manager (SM) deals with security key management and security authentication of
409 gateway devices, routing devices, field devices, and handheld devices (if they exist).

410 d) Cluster head

411 Cluster head manages and monitors field devices and handheld devices (if they exist).
412 Cluster head also merges and securely forwards packets from local cluster members and
413 other cluster heads.

414 e) Cluster member

415 Cluster member collects field data and sends the data to its cluster head.

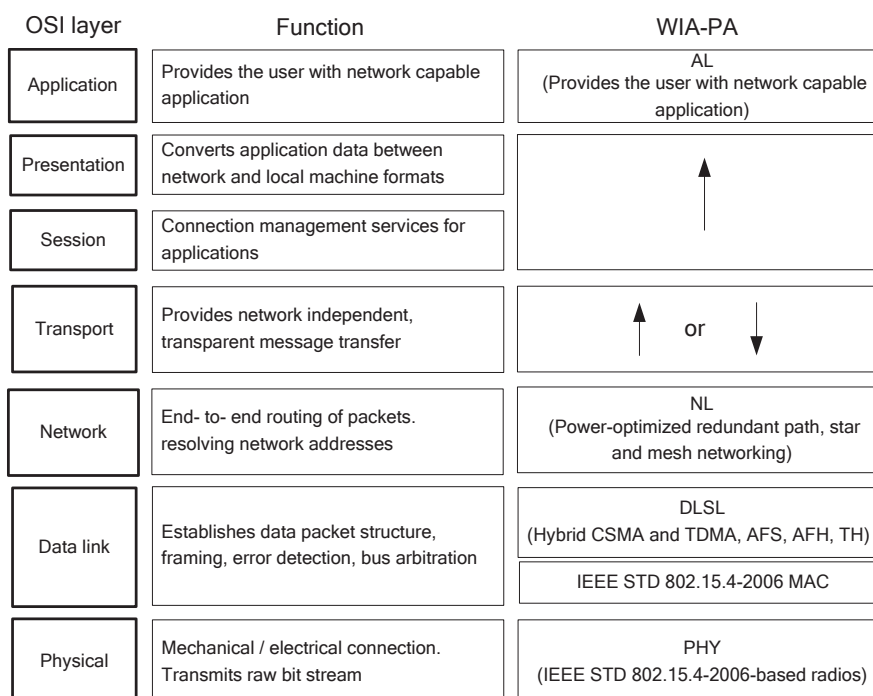
416 The NM and the SM that are used for system management should reside in a gateway device.

417 One physical device may perform the functions of several logical roles. In the hierarchical
418 network that combines star and mesh, a gateway device may perform the logical roles of
419 gateway, NM, SM, and cluster head. A routing device should act as a cluster head. A field
420 device/handheld device should only act as a cluster member.

421 The primary device and the redundant device are marked by the parameter
422 RedundantDevFlag in Table 20.

423 5.3 Protocol architecture

424 The WIA-PA protocol architecture, which is illustrated in Figure 3, is based on ISO/IEC 7498-
425 1. The WIA-PA protocol architecture defines the Data Link Sub-Layer (DLSL), Network Layer
426 (NL) and Application Layer (AL), while its PHYSical layer (PHY) and Medium Access Control
427 sub-layer (MAC) are based on IEEE STD 802.15.4-2011.



428
429 **Figure 3 – OSI basic reference model mapped to WIA-PA**

430 5.4 Interconnection

431 The WIA-PA network interconnects with other networks through the WIA-PA gateway. Besides
432 the communication to the WIA-PA NM and SM, the WIA-PA gateway may communicate with
433 other WIA-PA devices in order to exchange information between devices. Meanwhile, the

WIA-PA gateway may connect other networks, such as wired fieldbuses. The architecture of the WIA-PA gateway is shown in Figure 4.

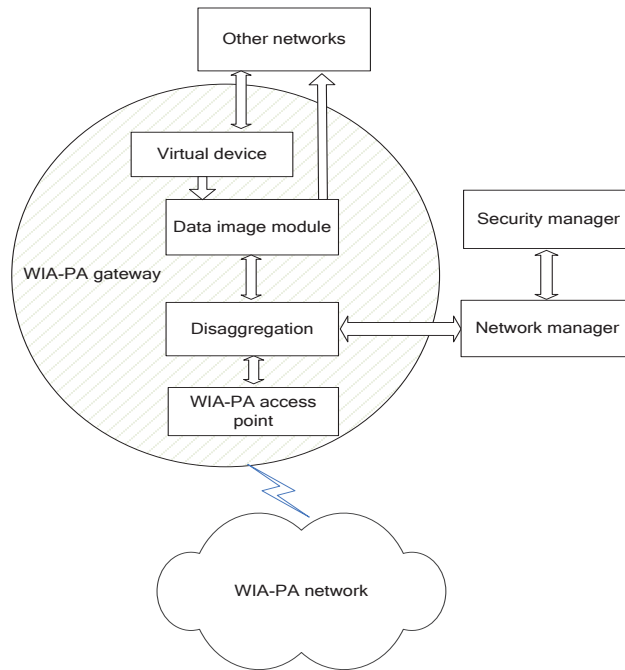


Figure 4 – The architecture of WIA-PA gateway

The WIA-PA gateway includes the following components:

a) WIA-PA access point

The WIA-PA access point realizes the physical connections of the WIA-PA network and transmission of the management information and data.

b) Virtual device

The virtual device defines a communication interface for other networks. The interface is used to map a data source from other networks into a WIA-PA device in order to fulfil communication between the WIA-PA network and other networks.

c) Disaggregation object

This object is used to disaggregate the packets that are aggregated within routing devices and field devices.

d) Dataimage module

The data image module stores the data of devices in the WIA-PA network and provides an access interface for other networks.

The Virtual Device and the Data Image Module are optional and implementation-specific, which are not defined in this document.

6 System management

6.1 General

The system management in the WIA-PA network includes both network management and security management. The functions of system management are implemented by the Device Management Application Process (DMAP) in each device. The DMAP, as a system management entity, includes the network management module, the security management module, and the Management Information Base (MIB) module. DMAP is shown as the grey area in Figure 5. The white blocks within the grey area are the function components in the DMAP.

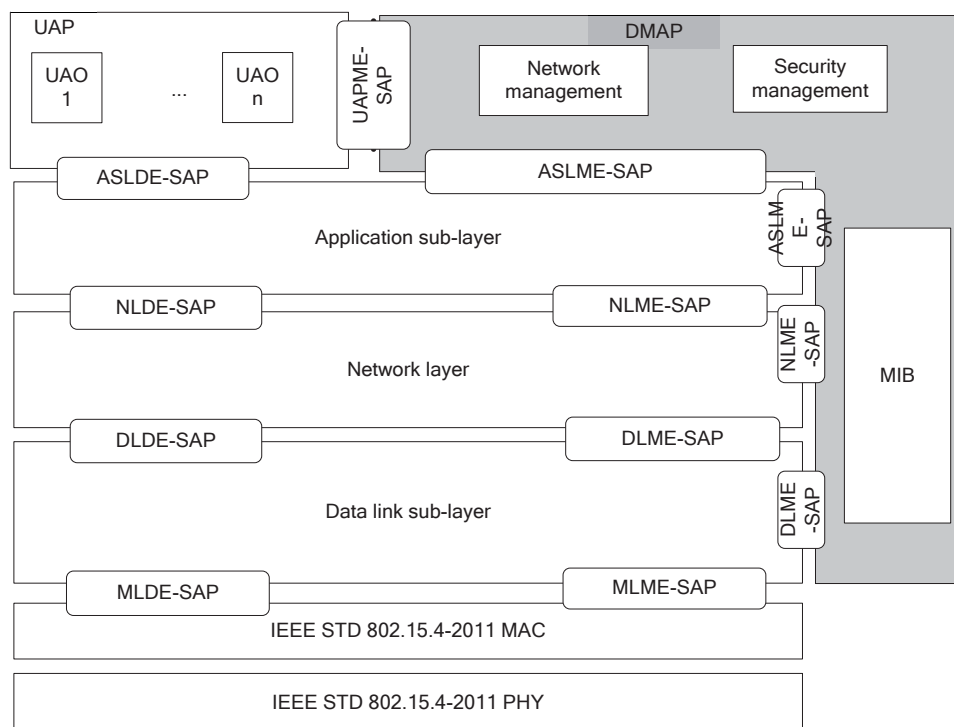


Figure 5 – DMAP in system management

The network management specifies the management of device attributes and attributes that are related to communication and network configuration. The network management functions are accomplished by the DMAPs in the NM, cluster heads, and cluster members. The network management functions include the following actions:

a) Joining and leaving the network

A routing device should join or leave the network through the gateway device or an online routing device. A field device should join or leave the network through an online routing device or the gateway device. The new joining device should be authenticated by the SM.

b) Network address allocation

Each device in the WIA-PA network has a 64-bit Extended Unique Identifier (EUI-64) address and a 16-bit network address. The EUI-64 address is also called long address. The long address of each device is assigned by vendors according to the IEEE EUI-64 address. The 16-bit network address is also called short address. The short address of each network device is assigned by the NM.

c) Routing configuration

Static routing is implemented in the WIA-PA network. The routing table in each routing device is configured by the NM.

d) Communication resource configuration

Communication resources of the WIA-PA network are organized as superframes (see 8.4.4). When a routing device has successfully joined the network, it should be allocated communication resources by the NM. After a field device has successfully joined a cluster, the cluster head should allocate communication resources to it.

e) Time source configuration and services of system time

The WIA-PA network sets only one base time source, which is performed by the gateway device. In order to recognize the order of occurring events, the WIA-PA devices relatively synchronize with the gateway device.

f) Performance monitoring

Performance monitoring is necessary to collect the performance of the WIA-PA network, which includes device status, path failure, and channel condition.

- 494 g) MIB maintenance
 495 The MIB module should configure the MIB of the WIA-PA protocol stack.
 496 h) Interfaces for plant operators and maintenance personnel
 497 The NM should provide an interface to allow plant operators and maintenance personnel
 498 to monitor and control the performance/activities of the network and devices. The
 499 definition of this interface is out of the scope of the current WIA-PA standard.
 500 i) Firmware upgrading
 501 Firmware upgrading should update the protocol stack of WIA-PA devices. Because on-line
 502 firmware upgrading is a power-hungry operation, WIA-PA does not recommend this mode
 503 and does not specify it in this document. WIA-PA recommends off-line firmware upgrading
 504 through handheld devices. Handheld devices connect devices that are to be upgraded by
 505 wire or wireless connections. Wired connections may use the serial communication
 506 methods. Wireless connections are not specified in this document.
 507 The security management should manage the attributes associated with network security. The
 508 security management is performed by the SM and by the security management modules in
 509 cluster heads and cluster members. The SM handles the centralized authentication of the
 510 whole network, and needs coordination with the NM. See 11.1 for the functions of security
 511 management.
 512 The MIB module stores all attributes used in the WIA-PA network, including both structured
 513 attributes and unstructured attributes (see 6.9).
 514 **6.2 Framework of system management**
 515 The WIA-PA network supports the hybrid centralized and distributed management scheme.
 516 The hybrid centralized and distributed management framework is illustrated in Figure 6. The
 517 system management is implemented by the NM, the SM, and cluster heads. Cluster heads are
 518 directly managed by the NM and the SM. In addition, they are provisioned with the privilege of
 519 managing cluster members.

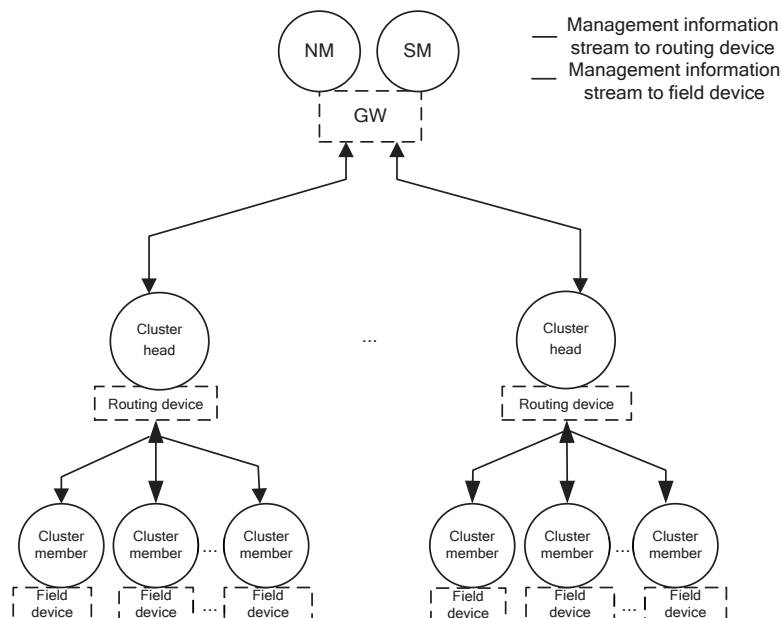


Figure 6 – Hybrid centralized and distributed system management scheme

- 522 The NM should perform the following tasks:
 523 a) Constructing and maintaining the mesh topology comprised of cluster heads, and star
 524 topology comprised of cluster heads and cluster members;

- 525 b) Allocating communication resources for cluster heads in mesh topology, and allocating
526 communication resources for cluster members to the cluster heads in star topology;
527 c) Monitoring the performance of the WIA-PA network, including device status, path failure,
528 and channel condition.

529 The SM should perform the following tasks:

- 530 a) Authorizing the cluster heads and cluster members that are attempting to join the WIA-PA
531 network;
532 b) Managing keys in the entire network, including key generation, key distribution, key
533 recovery, and key revocation;
534 c) Authorizing the relationship of the end-to-end communication.
535 a) The cluster head should perform the following tasks:
536 a) Constructing and maintaining the star topology; allocating communication resources that
537 are allocated to the star topology by the NM to cluster members in the cluster; providing
538 the monitoring results of the star topology to the NM;
539 b) Storing and forwarding keys used in the star topology; authorizing the communication
540 relationship among cluster heads; authorizing the communication relationship between a
541 cluster head and cluster members.

542 6.3 Joining process

543 6.3.1 Provisioning process

544 When a WIA-PA device intends to join the network, it should be provisioned by a handheld
545 device via wired manner.

546 A new device should have 64-bit long address before joining the WIA-PA network. First, the
547 CountryCode value (see 6.9.1.2.1 and 8.4.11) of a new device shall be set, which reflects the
548 regulatory constraints in the region where it might be deployed. The NetworkTopology value
549 (see 6.9.1.2.1) shall be set, which indicates the type of the network topology. The
550 SecEnableflag value (see 6.9.1.2.1) shall be set, which indicates whether the authentication is
551 enabled over the network. If authentication is enabled, KJ shall also be set (see 11.2).

552 To join the WIA-PA network, a new routing device or field device should first listen to beacons.

553 6.3.2 Joining process of routing device

554 When a routing device intends to join the network, it should be provisioned a Join Key by a
555 handheld device. See Clause 11 for the detailed provisioning process.

556 The joining process of a routing device includes the following actions:

- 557 a) A routing device scans the available channels to get beacons from either the online
558 routing devices or the gateway device.
559 b) The routing device chooses an online routing device or the gateway device as the
560 temporal parent and synchronizes with the network according to the received beacon.
561 c) The routing device sends a joining request to its temporal parent, which will then forward
562 the request to the NM.
563 d) When receiving a joining request, the NM should communicate with the SM to complete
564 the authentication process. Then the NM returns a joining response.
565 e) The routing device receives the joining response relayed by its temporal parent. If the
566 response is negative, the routing device should restart this joining process; otherwise, the
567 joining process should be finished.

568 The joining process of a routing device through the gateway device is shown in Figure 7.

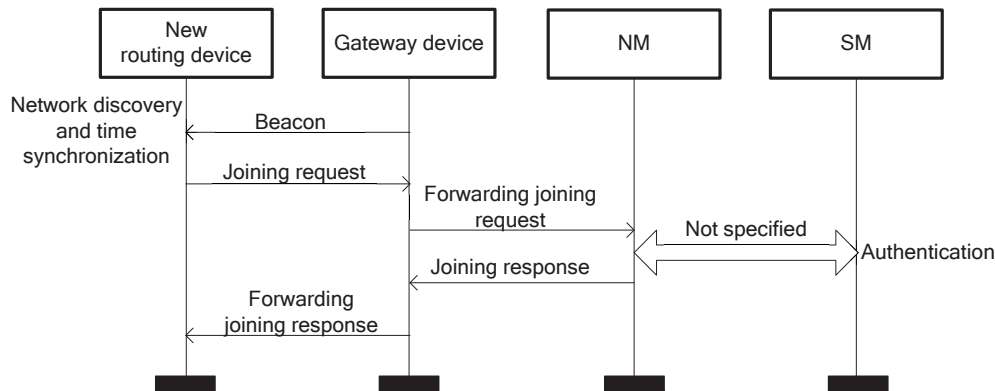


Figure 7 – Joining process of routing device through the gateway device

The joining process of a routing device through an online routing device is shown in Figure 8.

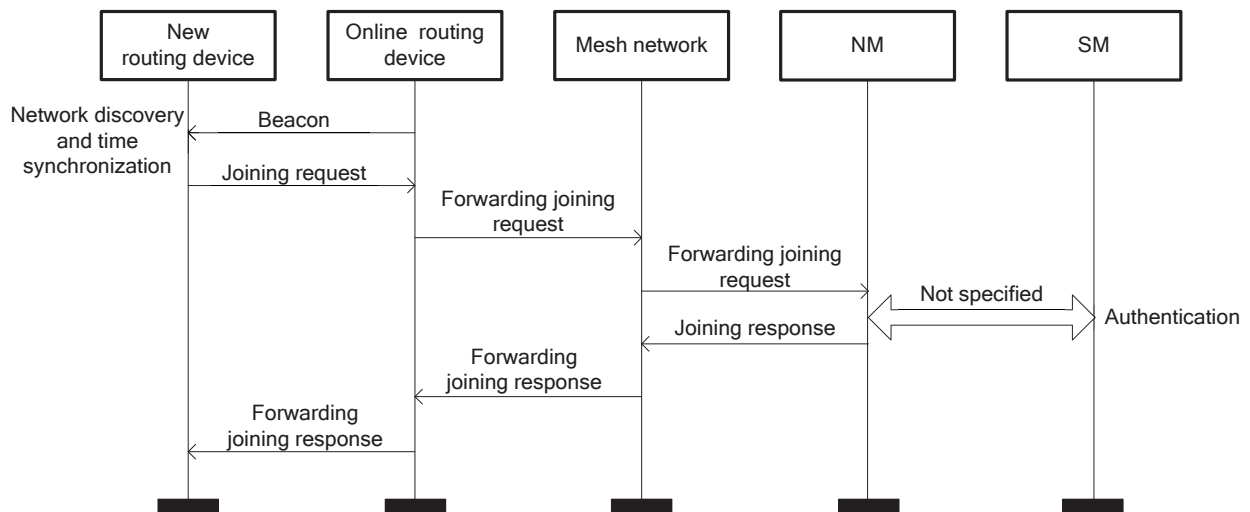


Figure 8 – Joining process of routing device through an online routing device

See 9.5.8 for the allocation of communication resources.

6.3.3 Joining process of field device

The joining process of a field device includes the following actions:

- A field device scans the available channels to get beacons from the online routing devices or the gateway device;
- The field device chooses one online routing device or the gateway device as the cluster head and synchronizes with the network according to the received beacon;
- The field device sends the joining request to the cluster head;
- When receiving the joining request, the cluster head forwards it to the NM;
- After receiving the joining response from the NM, the cluster head returns the joining response to the field device according to the type of network topology and the available communication resources of the cluster head. If the network topology is mismatched, the status in the response is set to FAILURE_TOP_DISMATCH; if there are other types of failures, the status in the response is set to FAILURE_ELSE; if the joining is successful, the status in the response is set to SUCCESS. See 8.6.3.4 for definition of Status;
- The field device receives the joining response from the cluster head. If the status in the response is FAILURE_TOP_DISMATCH, the field device will choose another routing device as its cluster head and restart the joining process as above; if status in the

593 response is FAILURE_ELSE, the field device will restart this joining process; otherwise, if
594 status in the response is SUCCESS, the field device has joined in the network.
595 The joining processes of a field device through the gateway device and through a routing
596 device are shown in Figure 9 and Figure 10 respectively. See 9.5.8 for the allocation of
597 communication resources.

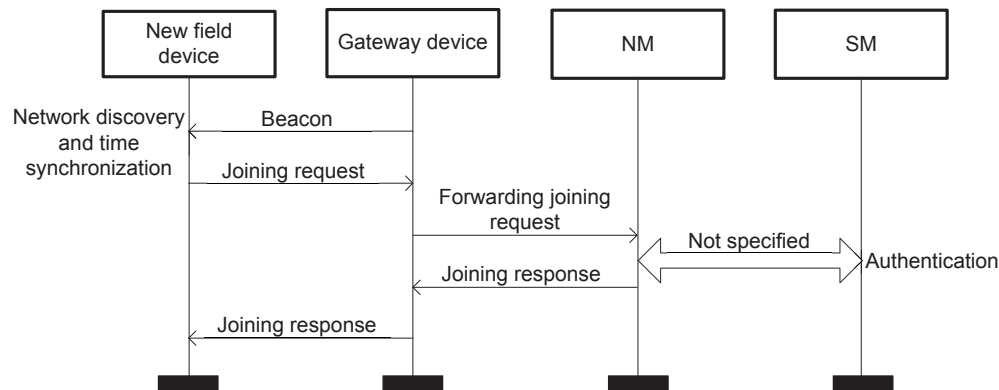


Figure 9 – Joining process of field device through a gateway device

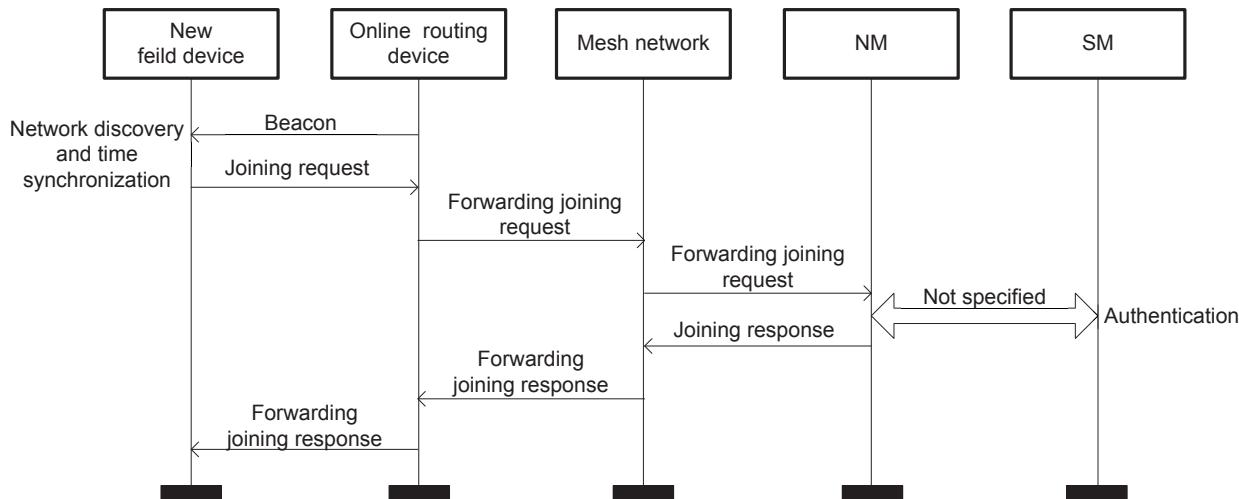


Figure 10 – Joining process of field device through a routing device

602 A WIA-PA handheld device connects to the WIA-PA network via the gateway device or a
603 routing device. The joining process of the handheld device is the same as other WIA-PA
604 devices. After joining in the network, the WIA-PA handheld device configures the WIA-PA
605 devices and collects the network performance/health information during the Contention
606 Access Period (CAP) period of the WIA-PA superframe.

607 See Clause 11 for detailed information about security.

608 **6.3.4 Addressing and address assignment**

609 In the WIA-PA network, each WIA-PA device (GW, routing device or field device) has a global
610 unique 64-bit long address and a 16-bit short address. The long address, as shown in Figure
611 11, is set by manufacturers according to the IEEE EUI-64 address.

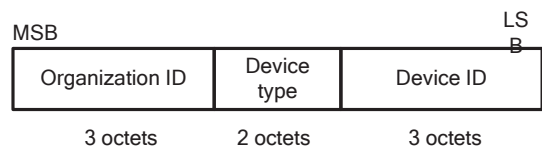
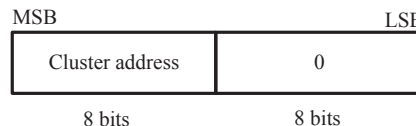


Figure 11 – Long address structure of device

614 The short address is 16-bit long. The most significant 8 bits of the short address that are
615 assigned by the NM are used to identify different clusters. If the value of the parameter
616 NetworkTopology (see 6.9.1.2.1) is 1, that is the network topology is star-only, the address of
617 the gateway device is also the address of the cluster head.

618 The short address of GW is allocated by the NM. The NM resides in a gateway device (see
619 5.2). The address allocation process of the GW is an internal operation, which is not specified
620 in this specification.

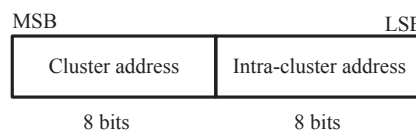
621 The short address of a routing device is shown in Figure 12. For the short address of the
622 routing device, the least significant 8 bits are set to 0.



623

624 **Figure 12 – Short address structure of routing device**

625 The short address of a field device is shown in Figure 13. The least significant 8-bit part of the
626 field device's short address is the intra-cluster address.



627

628 **Figure 13 – Short address structure of field device**

629 **6.4 Virtual Communication Relationship (VCR)**

630 **6.4.1 Definition**

631 Access to the User Application Objects (UAOs) is defined by the VCRs and the endpoints of a
632 VCR are two UAOs. VCRs distinguish the routing and communication resources among
633 different UAOs. Each VCR is identified by a VCR Identifier (VCR_ID). The attributes of a VCR
634 include UAO ID at source side, destination UAO ID, addresses of source device/destination
635 device, VCR type, valid scope, etc (see Table 20).

636 VCRs are classified into three types according to the application modes:

- 637 a) Publisher/Subscriber(P/S) VCR, which is used to publish periodic data;
- 638 b) Report source /Sink(R/S) VCR, which is used to support aperiodic events and trend
639 reports;
- 640 c) Client/Server(C/S) VCR, which is used to transfer aperiodic and dynamic paired unicast
641 messages.

642 VCRs are classified into three types according to its aggregation functions:

- 643 a) Non-aggregation VCR

644 If the aggregation is not supported by a cluster member, the non-aggregation VCR is used
645 by the cluster member to send non-aggregation packets to its cluster head. If the cluster
646 head does not support the aggregation function, it will forward the non-aggregation
647 packets to the gateway through the non-aggregation VCR.

- 648 b) Data aggregation VCR

649 If the aggregation is supported by a cluster member, the data aggregation VCR is used by
650 the cluster member to send the aggregated data from the UAOs to its cluster head. If the
651 cluster head does not support the aggregation function, it will forward the aggregated data
652 to the gateway through the data aggregation VCR. The effective interval of the data

653 aggregation VCR originates from the Data Aggregation Object (DAGO) of the cluster head
 654 to the DisaGgregation Object (DGO) of the gateway.

655 c) Packet aggregation VCR

656 If the aggregation is supported by a cluster head, the packet aggregation VCR is used by
 657 the cluster head to send aggregated packets to the gateway. The effective interval of the
 658 packet aggregation VCR originates from the Packet Aggregation Object (PAGO) of the
 659 cluster head to the DisaGgregation Object (DGO) of the gateway.

660 PAGOs, DGOs, and DAGOs (see 6.6.1) are three special UAOs.

661 6.4.2 Protocol support for VCR

662 The protocol supports for VCRs are listed in Table 2.

663 **Table 2 – Protocol support for VCR**

Protocol layer support			VCR types		
			P/S VCR	R/SVCR	C/S VCR
AL	User applications		Periodic data transmission of UAO	Aperiodic report e.g. alarm or event	Attribute getting and setting operation in UAO
	Communication modes in Application Sub-Layer (ASL)		P/S	R/S	C/S
	Bidirectional		No	No	Yes
	End-to-end retransmission		No	Optional	Yes
	Packet aggregation supporting		Yes	No	No
NL	Redundant path supporting	Intra-cluster	No	No	No
		Inter-cluster	Yes	Yes	Yes
	Unicast/Broadcast		Broadcast/Unicast	Broadcast/Unicast	Unicast
DLSL	Periodic		Yes	No	No
	Real-time		Yes	Optional	No
	Communication resource	Intra-cluster	Contention Free Period (CFP), exclusive timeslots in intra-cluster communication period	CAP	CAP
		Inter-cluster	Exclusive timeslots in inter-cluster communication period	Shared timeslots	Shared timeslots

664 6.4.3 VCR establishment

665 The processes of R/S VCR and C/S VCR establishment are as follows:

666 a) The NM obtains the UAOs of the field devices when they have joined the WIA-PA network.
 667 The UAOs are obtained by the NLME-INFO_GET primitives during the CAP (see 9.5.13
 668 and 9.6.4).

669 b) Once the NM obtains the UAOs, it allocates reserved R/S VCRs and C/S VCRs for each
 670 UAO to field devices.

671 The process of P/S VCR establishment (if it is needed) is as follows:

672 a) The NM establishes one P/S VCR for each UAO by using the NLME-INFO_SET primitives
 673 (see 9.5.14 and 9.6.4). If a field device does not support the data aggregation, each UAO
 674 has one non-aggregation P/S VCR, and different VCRs may use the same routing paths.
 675 Otherwise, each field device has one data aggregation VCR. If the routing device
 676 supports packet aggregation, one packet aggregation VCR is established for the routing
 677 device.

678 See Table 21 for the VCR information.

679 **6.4.4 VCR release**

680 VCRs are released when routing devices and field devices leave the network (see 6.8).

681 **6.5 Routing configuration and communication resource allocation**

682 **6.5.1 Routing configuration**

683 Routing devices use static routing that is configured by the NM. The concrete routing
684 algorithms are not specified in this standard. The details of routing paths are shown in
685 Table 15. The redundant paths are supported and use the same RouteID. The routing
686 configuration is realized by Route allocation services (see 9.5.7).

687 **6.5.2 Framework of communication resource allocation**

688 Communication resources consist of timeslots and channels. Allocation of communication
689 resources should be considered in two dimensions: time and channel.

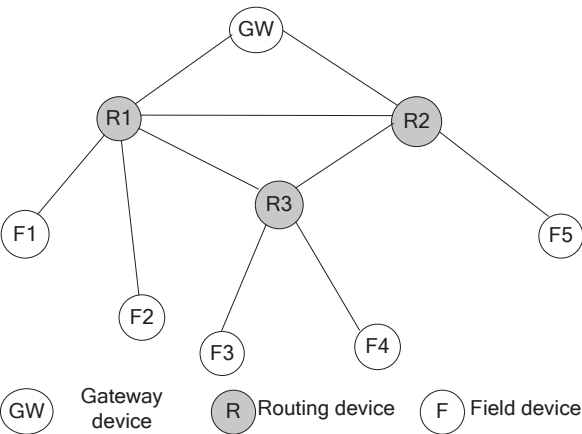
690 The process of communication resource allocation is as follows:

- 691 a) In the mesh network, the communication resources of the cluster heads are allocated by
692 the NM. The communication resources consist of those used by cluster heads in the
693 mesh network and those allocated by cluster heads to cluster members.
- 694 b) In the star network, the communication resources are allocated by cluster heads to
695 cluster members. That is, communication resources are bound to cluster members.

696 An example of the resource allocation in the hierarchical network topology that combines star
697 and mesh is shown in Figure 14. First, the NM residing in the GW allocates communication
698 resources to the routing devices R1, R2 and R3. These communication resources are used for
699 communication among R1, R2 and R3, for communication between routing devices and the
700 GW, and for communication between intra-cluster field devices and routing devices. Second,
701 after receiving communication resources from the NM, routing devices allocate some of the
702 communication resources to their intra-cluster field devices, which are used for intra-cluster
703 communications among field devices and their corresponding routing devices. As shown in
704 Figure 14, after the NM allocates communication resources for R1, R2 and R3, R1 allocates
705 communication resources for F1 and F2; R2 allocates communication resources for F5; and
706 R3 allocates communication resources for F3 and F4.

707

708



709

Communication resource allocation

Timeslot										
Channel	R1=>F1	R1=>F2	F1=>R1	F2=>R1	GW=>R1	GW=>R2	R2=>R3	R2=>GW	R3=>R2	R2=>GW
	R3=>F3	R3=>F4	F3=>R3	F4=>R3	R2=>R3	R1=>R3	R1=>GW			
	R2=>F5	F5=>R2								
Communication resource allocation in Star topology					Communication resource allocation in Mesh topology					Sleeping

710

711

Figure 14 – An example of resource allocation

712

6.5.3 DLPDU priority and scheduling rules

713

Four priority levels of DLPDUs are defined:

714

- a) Command (highest priority)

715

Any packet containing a payload with network-related diagnostics, configuration, control information, or emergent alarms should be classified with a priority of Command.

716

717

- b) Process data (secondary priority)

718

Any packet containing process data should be classified as secondary priority level, Process Data.

719

720

- c) Normal (third priority)

721

DLPDUs that do not meet the criteria of Command, Process data, or Alarm should be classified as Normal priority.

722

723

- d) Alarm (lowest priority)

724

Packets containing only non-emergent alarm and event payload should assume a priority of Alarm. Devices should buffer no more than one DLPDU having Alarm priority.

725

726

The following scheduling rules are orderly recommended for allocating communication resources:

727

728

- a) Allocating channels to the beacon frame and active period;

729

- b) Allocating timeslots to the devices with the fastest update rate;

730

- c) Allocating resources to the packet with the earliest generating time in multi-hop situations;

731

- d) Allocating resources to the highest priority packet prior to other packets.

732

6.5.4 Communication resource allocation to routing device

733

The WIA-PA network applies the integrated management strategy of centralized and distributed schemes. After the routing device joins the network, it should scan its neighbour devices on each channel and report the neighbour information to the NM. After receiving the neighbour information, the NM should allocate paths, a superframe, and a block of time slots.

734

735

736

737 routing device by using the communication resource allocation services (see 9.5.8). The
738 information of every routing device superframe is broadcast to its field devices in the beacon
739 frame. The allocation process of routing device communication resources is illustrated in
740 Figure 15.

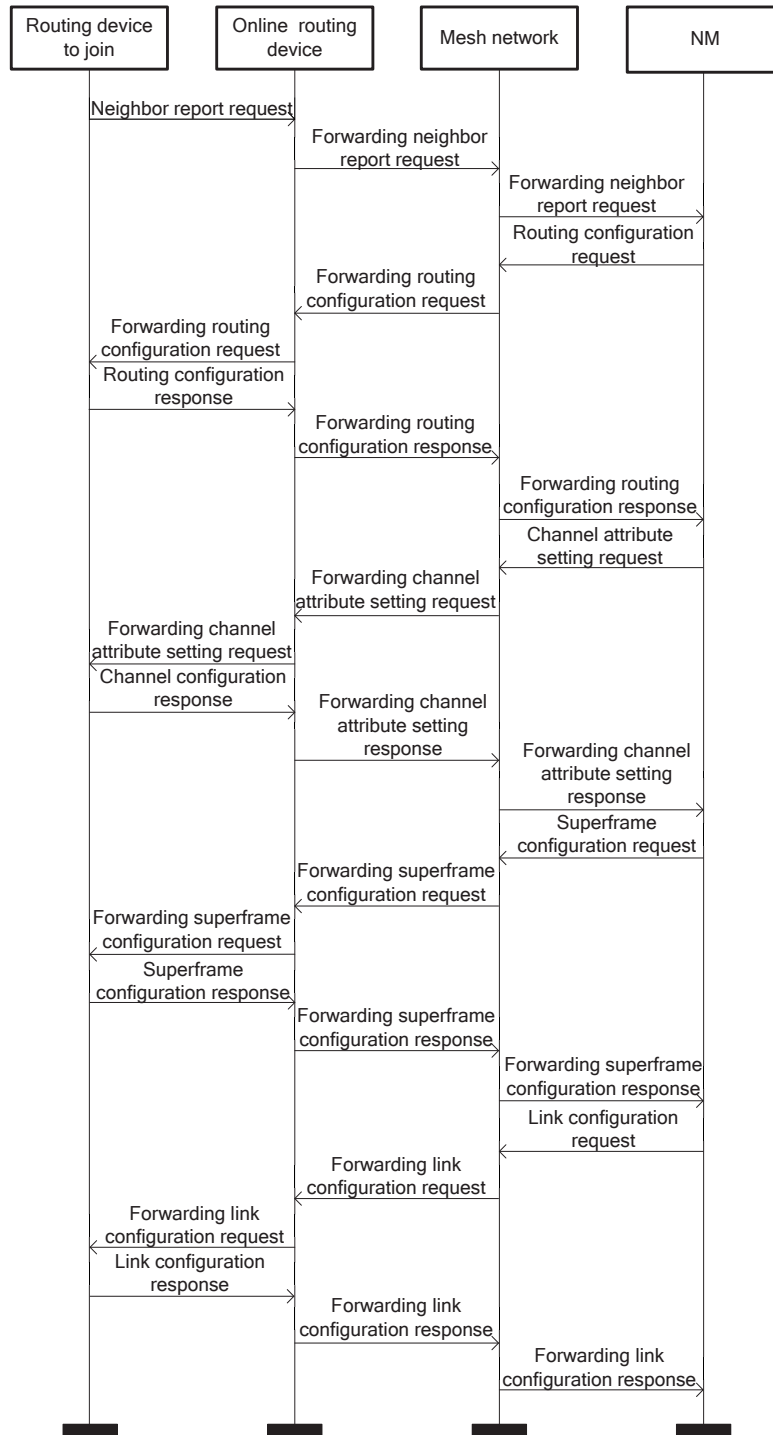


Figure 15 – Allocation process of routing device's communication resources

6.5.5 Communication resource allocation to field device

After VCRs of a field device are established successfully, either the routing device or the gateway device allocates timeslots to its field devices by using the communication resource allocation services (see 9.5.8), which are used in communication between the routing device and the field devices or between the gateway device and the field devices. If the superframes of the routing device and the gateway device are affected by the joining field devices, the

- 749 routing device and the gateway device should update their RouteTable, Superframe and Link
750 attributes (see 6.9.1.2.2 and 9.5.8).
- 751 When a field device joins the network through an online routing device, the communication
752 resource allocation process of the field device is illustrated in Figure 16.

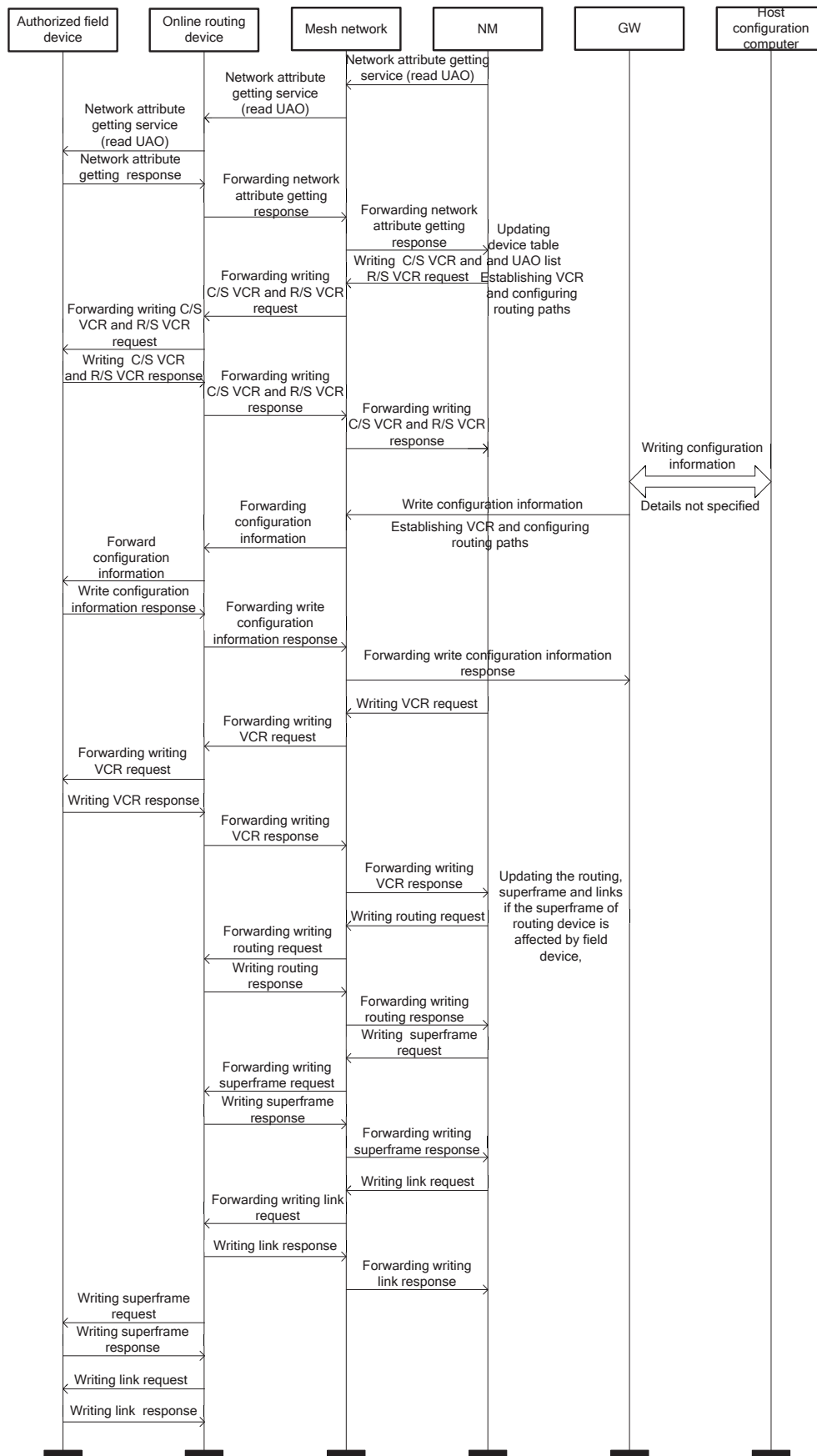


Figure 16 – Allocation process of field device's communication resources

6.6 Aggregation and disaggregation

6.6.1 Aggregation

The aggregation function is optional for field devices and routing devices and is indicated by the aggregation and disaggregation support flag AGGSupportFlag (see Table 19). If the field devices or the routing devices support the aggregation mechanism, the NM sets the aggregation and disaggregation enable flag AGGEnableFlag to 1 (see Table 19).

The WIA-PA network supports a two-level aggregation mechanism in order to reduce the number of the forwarding packets.

a) Data aggregation. If a field device has more than one User Application Object (UAO), it should decide whether or not to invoke the data aggregation mechanism according to the AGGEnableFlag. This mechanism should reduce the data communication frequency and enhance network efficiency.

b) Packet aggregation. If a routing device receives packets from more than one field device, it should decide whether invoking packet aggregation mechanism or not according to the AGGEnableFlag. This mechanism should reduce the number of packets from the routing device to the gateway device and enhance network efficiency.

The aggregation function is implemented by the DAGOs in field devices and PAGOs in routing devices. The operation parameters of DAGOs and PAGOs are configured by the NM.

The aggregation function supported by the WIA-PA network includes the following four situations:

a) A field device supports the aggregation function, while its routing device does not.

b) A routing device supports the aggregation function, while its field device does not.

c) Both, a field device and its routing device support the aggregation function.

d) Neither a field device nor its routing device supports the aggregation function.

Relations between the VCRs and the aggregation functions supported by field device, routing device and gateway device are shown in Table 3.

Table 3 – Relations between VCR and aggregation function

	Field device DAGO (Aggregation function)			Routing device PAGO (Aggregation function)			Gateway device DGO (Disaggregation function)	
	Support	Disable	Enable	Support	Disable	Enable	Disable	Enable
Non-aggregation VCR	NO	X		NO	X		—	—
Data aggregation VCR	YES		X	NO	X ^a			X
	YES		X	NO		X ^b		X
Packet aggregation VCR	NO	— ^c	— ^c	YES		X		X
X indicates the aggregation/disaggregation function in the corresponding device is enabled or disabled. — indicates the VCR is independent of the aggregation/disaggregation function. ^a The data aggregation VCR starts with DAGO of a field device and ends at DGO of the gateway device. ^b The data aggregation VCR starts with DAGO of a field device and ends at PAGO of a routing device. ^c Field devices have no packet aggregation function.								

The aggregation configuration process is listed as follows:

a) NM should read the AGGSupportFlag to verify whether devices support the aggregation function.

b) NM should set the value of the AGGEnableFlag attribute to 1 in the MIB if the routing devices support the aggregation function. The NM should allocate packet aggregation

VCRs to the routing devices. The aggregation duration of a routing device should be indicated by attribute AggPeriod (see 6.9.1.2.1) and set to the minimum Dataupdate rate attribute (see Table 20) of its field devices in the cluster. When aggregation duration expires, the routing device aggregates all its packets and sends the aggregated packet out.

- c) NM should set the value of the AGGEnableFlag attribute to 1 in the MIB if the field devices support the aggregation function. The NM should allocate the data aggregation VCRs to the field devices. The aggregation duration of a field device should be indicated by attribute AggPeriod (see 6.9.1.2.1) and set to the minimum Datadaterate attribute (see Table 20) of its UAOs. When the aggregation duration expires, the field device aggregates all its packets and sends the aggregated packet to the routing device.

According to whether the aggregation is embedded or not, a field device or a routing device operates as follows:

- a) If the AGGEnableFlag attribute of a field device is set to 0, this field device does not support the aggregation function. Field devices that have no aggregation function send their data to the routing device through the non-aggregation VCR and the related RouteID (see Table 20). If the aggregation flag AGGEnableFlag attribute of the routing device is also set to 0, the routing device should forward this aggregated packet to the DGO of the gateway device through the original RouteID.
- b) If a field device has more than one UAO and its AGGEnableFlag attribute is set to 1, the DAGO of the field device calculates the length of the P/S data from the UAOs and aggregates these data. The format of the aggregated data is shown in Table 4. The aggregated data is sent to the ASL by the DAGO and is encapsulated with the ASL header. The field of the packet type in the ASL header is set to 0b11, which is used to indicate the aggregated packet (see 10.4.2). The aggregation packet in the ASL is sent to the routing device through the data aggregation VCR and the related RouteID; if the AGGEnableFlag attribute of the routing device is 0, the routing device should forward this aggregated packet to the DGO of the gateway device through the original RouteID.
- c) If the aggregation function embedded in a routing device is enabled (AGGEnableFlag = 1) and receives packets from its field devices, it reads the NL packet headers. The routing device should aggregate the packet according to the P/S flags and the Fragment flag in the NL packet headers (see 9.6.3). The aggregation rules are as follows:
- If the received packet is P/S type and the Fragment flag is 0, the packet should be aggregated.
 - Other types should not be aggregated.

If the packet can be aggregated, its source address and NL payload are sent to the PAGO of the DMAP. The PAGO uses the time when the first packet comes (required to be aggregated) as the start time of an aggregation cycle PagoPeriod (see Table 10). Once PagoPeriod expires, the PAGO aggregates the packets according to the format that is shown in F, and searches the related to the packet aggregation VCR. The aggregated packet, packet aggregation VCR, and the related are then sent to the NL; the NL should send this aggregated packet to the gateway device through the related. The format of the aggregated packet in NL is shown in 9.6.3. If the length of the aggregated packet is longer than the maximum length allowed by the NL, the NL should fragment the packet and send the packet to the gateway device by using the packet aggregation VCR and the related.

Table 4 – Format of aggregated data followed by field device's DAGO

	Format of aggregated data followed by field device's DAGO					
Length in octet(s)	1	1	Variable length	...	1	Variable length
Field name	Number of aggregated data	Data length	Data	...	Data length	Data

Table 5 – Format of aggregated packet followed by routing device's PAGO

	Format of aggregated data followed by routing device's PAGO							
Length in octet(s)	1	2	1	Variable length	...	2	1	Variable length
Field name	Number of aggregated packet	Source address	Data length	Data	...	Source address	Data length	Data

6.6.2 Disaggregation

The disaggregation function is optional for the gateway device and is indicated by the aggregation and disaggregationsupport flag AGGSupportFlag (see Table 19). If the gateway device supports the disaggregation mechanism, the NM sets the aggregation and disaggregation enable flag AGGEnableFlag to 1 (see Table 19).

The disaggregation function is implemented by the DGO in the gateway device. The gateway device decides whether to disaggregate the received packet according to the NL header and the ASL header. If the value of packet type in the NL header is 1, the gateway device disaggregates the NL aggregated packet; if the value of the packet type in the ASL header is 0b11, the gateway device continues disaggregating the ASL aggregated packet.

The operation parameters of the DGO are configured by the NM.

The process of disaggregation is as follows:

- a) After the gateway device receives the aggregated packets from field devices and routing devices, it will notify the DGO in its DMAP to disaggregate the packets.
- b) The DMAP sends the disaggregated packets to UAOs.

6.6.3 An example of the two level aggregation process

The following example illustrates the aggregation and disaggregation processes. The example is based on a network that consists of two field devices, one routing device, the GW, and the host configuration computer. As shown in Figure 17, the routing device R acts as the cluster head of field device A and field device B; there are two UAOs named a1 and a2 residing in field device A and two UAOs named b1 and b2 residing in field device B.

This example supposes that field device A does not support the aggregation function, while field device B and routing device R do. The data update rates of a1 and a2 are configured to 1s, and the data update rates of b1 and b2 are configured to 4s. The DAGO of the field device B is responsible for aggregating the packets from b1 and b2, and generates packet p_b. The routing device R has one PAGO and the aggregation duration is the minimum data update rates of a1, a2, b1, and b2, whose value is 1s. The routing device R has a PAGO, which aggregates the packets from a1, a2 and packet p_b. The gateway device has a DGO, which disaggregates packets from field device A and B.

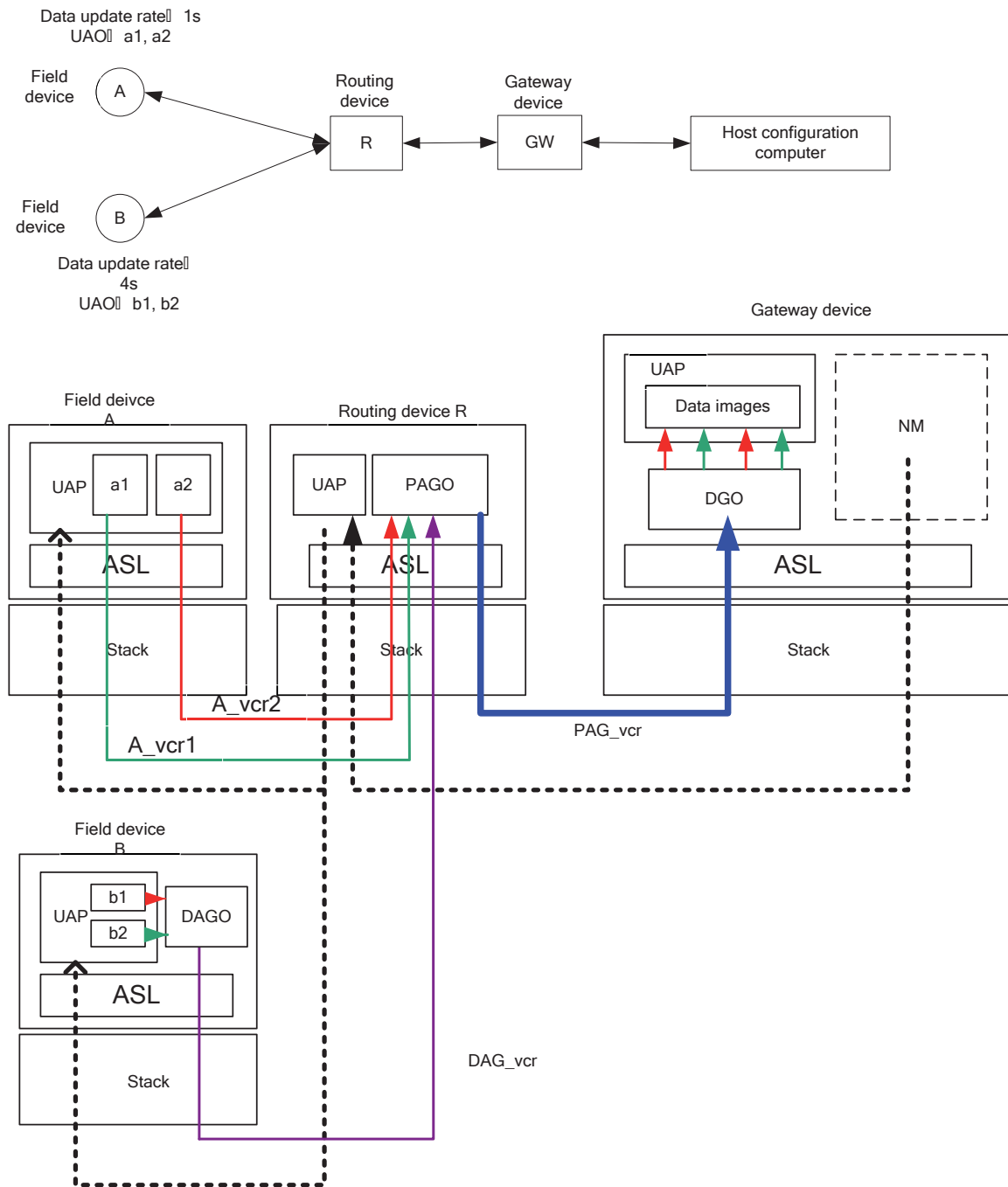


Figure 17 – Example of aggregation and disaggregation

The aggregation and disaggregation process is listed below:

- After the network is established, the NM allocates the non-aggregation VCRs to a1, a2, b1, and b2 for the transmissions of non-aggregation packets. The non-aggregation VCRs of a1 and a2 in field device A are indicated by A_vcr1 and A_vcr2. The endpoints of A_vcr1 are a1 and the UAP of the GW, and the endpoints of A_vcr2 are a2 and the UAP of the GW. Because the data transmissions of field device B do not use the non-aggregation VCRs, the non-aggregation VCRs of b1 and b2 in field device B are not indicated in this example.
- After constructing the non-aggregation VCRs, the NM configures the aggregation duration and data aggregation VCR for field device B and configures the aggregation duration and packet aggregation VCR for routing device R. The aggregation durations are the minimum data update rate among all UAOs in a field device or the minimum data update rate

among all field devices for a routing device. Because the data update rates of b1 and b2 are 4s, the aggregation duration of DAGO in field device B is four seconds; the data aggregation VCR of field device B is indicated by DAG_vcr and its endpoints are DAGO in field device B and the DGO in the GW. The aggregation duration of routing device R is set to the minimum data update rate in a cluster. Because the minimum data update rate among a1, a2, b1, and b2 is one second, the aggregation duration of routing device R is set to 1s. The packet aggregation VCR of routing device R is indicated by PAG_vcr and its endpoints are PAGO in the routing device R and DGO in the GW.

c) After A_vcr1, A_vcr2, DAG_vcr, and PAG_vcr are established, the DAGO, PAGO and DGO begin to work. The DAGO in field device Buses the time when the first packet comes (required to be aggregated) as the start time, and aggregates the packets and sends them to routing device R through DAG_vcr at the configured aggregation timeslot. The PAGO in routing device R uses the time when the first packet comes (required to be aggregated) as the start time, and aggregates the packets in DMAP and sends them to the DGO through PAG_vcr in the GW at the configured aggregation timeslot.

d) After the DGO of the GW receives the aggregated packets, it disaggregates the packets and finds the corresponding UAOS according to the packet source address and UAO identifiers.

e) The DMAP in GW sends the disaggregated packets to the corresponding UAOS.

6.6.4 Management of aggregation and disaggregation objects

The attributes of the DAGO class are shown in Table 6.

Table 6 – DAGO class attributes

Attribute ID	Name	Data type	Default value	Usage	Description	Supporting method
0	DagoID	Unsigned8	0	Mandatory	The identifier of the DAGO	READ
1	DagoRevision	Unsigned8	0	Optional	The version defined by the DAGO	READ

The attributes of the DAGO instance are shown in Table 7.

Table 7 – DAGO instance attributes

Attribute ID	Name	Data type	Default value	Usage	Description	Supporting method
0	DagoInsID	Unsigned8	0	Mandatory	The identifier of the DAGO instance	READ
1	DagoPeriod	Unsigned8	1	Mandatory	The aggregation cycle (in seconds)	READ/WRITE
2	DagoMemNum	Unsigned8	1	Mandatory	Count of the aggregated UAOS	READ/WRITE
3	DagoMemLst	MEM_STRUCT structure (see Table 8)		Optional	List of the aggregated UAOS	READ/WRITE
4	DagoMemData Size	Unsigned8	0	Optional	Length of the aggregated data DagoMemData (in octets)	READ/WRITE
5	DagoMemData	Octetstring		Mandatory	Data of the aggregated UAOS	READ/WRITE

The methods supported by the DAGOs are shown in Table 171.

The definition of the MEM_STRUCT structure is shown in Table 8.

903 **Table 8 – MEM_STRUCT structure**

Attribute ID	Name	Data type	Description
0	AppObjID	Unsigned8	The identifier of the UAO
1	AppObjInsID	Unsigned8	The identifier of the UAO instance
2	AppObjAttrID	Unsigned8	The attribute identifier of the UAO instance

904 The attributes of the PAGO class are shown in Table 9.

905 **Table 9 – PAGO class attributes**

Attribute ID	Name	Data type	Default value	Usage	Description	Supporting method
0	PagoID	Unsigned8	1	Mandatory	The identifier of the PAGO	READ
1	PagoRevision	Unsigned8	0	Optional	The version defined by the PAGO	READ

906 The attributes of the PAGO instance are shown in Table 10.

907 **Table 10 – PAGO instance attributes**

Attribute ID	Name	Data type	Default value	Usage	Description	Supporting method
0	PagoInsID	Unsigned8	0	Mandatory	The identifier of the aggregation object instance	READ
1	PagoPeriod	Unsigned8	1	Mandatory	The aggregation cycle (in seconds)	READ/WRITE
2	PagoMemNum	Unsigned8	1	Mandatory	Count of the aggregated cluster members	READ/WRITE
3	PagoMemLst	Octetstring		Optional	List of the aggregated cluster members	READ/WRITE
4	PagoDataSize	Unsigned8	0	Optional	Length of the aggregated packet (in octets)	READ/WRITE
5	PagoMemData	Octetstring		Mandatory	Data of the aggregated cluster members	READ/WRITE

908 The methods supported by the PAGOs are shown in Table 171.

909 The attributes of the DGO class are shown in Table 11.

910 **Table 11 – DGO class attributes**

Attribute ID	Name	Data type	Default value	Usage	Description	Supporting method
0	DgoID	Unsigned8	2	Mandatory	The identifier of the DGO	READ
1	DgoRevision	Unsigned8	0	Optional	The revision defined by the DGO	READ

911 The attributes of the DGO instance are shown in Table 12.

912 **Table 12 – DGO instance attributes**

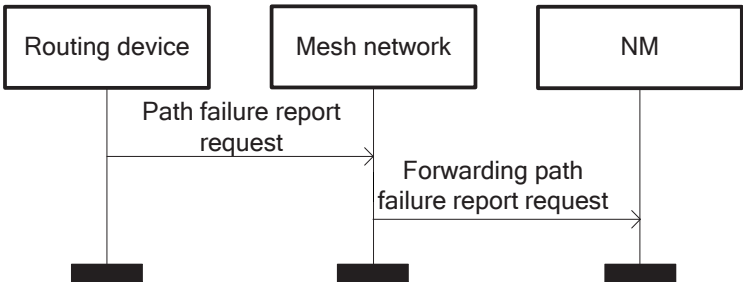
Attribute ID	Name	Data type	Default value	Usage	Description	Supporting method
0	DgoInsID	Unsigned8	0	Mandatory	The identifier of the DGO instance	READ

913 The methods supported by the DGOs are shown in Table 171.

914 **6.7 Performance monitoring**

915 **6.7.1 Path failure report**

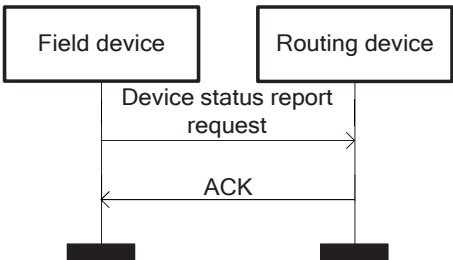
916 The path failure report is used by routing devices to report path failure events to the NM
917 through the redundant paths. The process of path failure report is shown in Figure 18 (see
918 9.5.12).



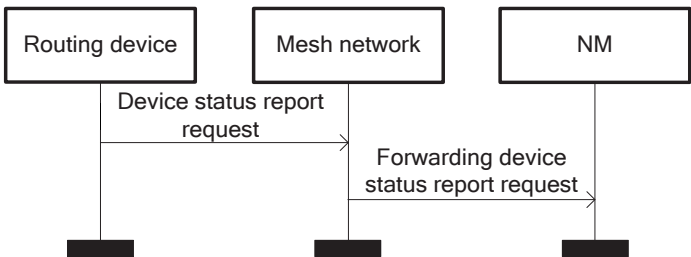
919
920 **Figure 18 – Process of path failure report**

921 **6.7.2 Device status report**

922 After receiving device status reports from intra-cluster field devices, a routing device
923 reports its own health and the health of its field devices to the NM periodically. The
924 NM appraises and diagnoses the network performance according to health information,
925 and replies to the change of network environment timely. The NM should detect abnormal
926 conditions in the WIA-PA device, such as low level of battery power and disconnection
927 from neighbouring devices. This is realized by setting alarm levels to the WIA-PA devices. The
928 device status report processes of the field device and the routing device are shown in Figure
929 19 and Figure 20 (see 9.5.10).



930
931 **Figure 19 – Device status report process of field device**



932
933 **Figure 20 – Device status report process of routing device**