ARINC 628 – Section 17

CABIN WIRELESS ACCESS POINT (CWAP) / CABIN CELL MODEM (CCM)

Change Log

Version	Chapter	Change
Strawman_V1	All	Initial version
Strawman_V2 *Based on May 2019 Fulda CSS Results*	All	Added CWAP interface configurations including A801, EN4531, and MT F/O connectors
Strawman_V3 *Based on Aug 2019 Fremont CSS Results*	All	Added Description and CWAP Reference Scheme Added J7-Jxx Antenna Connections Relocated J4 / J5 next to each other Restructured "Interfaces" Section 17.2. Section 17.3/17.4 not used anymore Added Contact Arrangement for F/O Connector
Strawman_V4 *Based on Oct 2019 Herrsching CSS Results*		Merged CWAP and CCM strawman documents (Section 17/19) Added Referencing Scheme for CCM/CWAP providing information on interface and radio configuration. Re-arranged interfaces to ensure backwards compatibility with current A628 WAP but still have the new F/O interfaces side by side. Added special “copper-only” configuration to cover installations with J7 antenna interfaces at front of the unit. Marked MT Fiber Optic connector definition as “Reserved for future use”. Moved definition details to 5GCN strawman document

Actions from Feb2020 Mobile CSS Meeting		- Check overlap with A763A (ETWLU). A763 defines a network "client" for external communication while 628p1 defines a network "access point". Still both standards may include redundant requirements - Check if reference to A822 (Gate Link) is required - Check all figure and table references - 17.1.3: Referencing Scheme - Add indication for Hybrid unit supporting Cellphone *and* Wi-Fi external communication (CCM+ETWLU) - Check if indication of J7 config and indication of "External Antennas" is redundant - 17.2 Interfaces: - Remove color from Fig 17-2 pin representation - Define max number of J7-Jxx TNC interfaces - Remove representation of MT based configurations - Config E (F/O A801): Add representation of 6 pin A801 EN4165 insert. - Change 10GBASE-F to 10GBASE-SR - Check if J3 definition for CWAP and CCM can be merged? What is the J3 definition for hybrid units? - 17.3.4 Electrical Interfaces: - Add description of optional CWAP/CCM daisy chaining. - Check if third Ethernet port on J3 can be deleted - 17.3.7 RF Interface - Check if note on CCM EIRP is applicable - Check "single antenna operation" requirement - 17.4 Batteries: - Delete section. - Allow interface to external battery pack via J3 - 17.7.5. 802.11 b/g/n mixed clients operation - Delete section as sufficiently covered by latest 802.11 standards. - 17.7.6 Virtual Service Communities: - Check if still applicable - 17.7.7 Security: - Check for required updates - Add WPA3 in addition to WPA2 - Check if new ARINC APIM/standard "Onboard Secure Wi-Fi Network" can be applied

		- 17.8 Data Loading: Check if ARINC667 / 675A is covering this aspect sufficiently - 17.9 Remote Control: - Check if still applicable - Appendix: - Update outline drawing
Strawman_V5 Nov 2020 *Based on Feb2020 Mobile CSS Results*		Urban 19.11.2020.: Incorporated V4 / Feb 2020 comments (to be completed)
Strawman_V6		From Airbus on NOV 23 – Drafting session 24 NOV

Contents

17.0 CABIN WIRELESS ACCESS POINT (CWAP) / CABIN CELL MODEM (CCM)

17.1 OVERVIEW

Section 17 defines the **Cabin Wireless Access Point (CWAP) and the Cabin Cell Modem (CCM)**.

Even though the function of these two types of equipment covers different aspects of passenger entertainment and crew operations, CWAP and CCM are sharing a large number of hardware and interface requirements.

To make CWAP / CCM units clearly identifiable, they should be designated according to the referencing scheme defined in chapter 17.1.3

17.1.1 Description of the CABIN WIRELESS ACCESS POINT (CWAP)

The primary function of the CWAP is to provide wireless connectivity between airlines or passengers-owned mobile computing devices and a network infrastructure within the aircraft environment. Mobile computing devices (clients) may include all wireless equipment passengers can bring aboard commercial aircraft including, but not limited to, laptop computers, smartphones, or tablets.

The CWAP communicates with the host aircraft system (e.g. IFE System) via electrical or fiber optic interfaces.

For extended-length and double-deck aircraft, multiple CWAPs may be used to provide seamless coverage as clients roam throughout the aircraft.

17.1.1.1 CWAP definition scope compared to ARINC 763 CWLU

The Cabin Wireless Access Point (CWAP), though similar to the Cabin Wireless LAN Unit (CWLU) described in ARINC Characteristic 763, provides additional features and focuses operation on passenger wireless access supporting the Passenger Information and Entertainment Services Domain (PIESD) and Passenger Owned Devices Domain (PODD) defined per ARINC Report 821, whereas the CWLU is more airline operation oriented supporting the Airline Information Services Domain (AISD).

Similarly to CWLU, CWAP mobile users may include aircraft flight and cabin crews, maintenance personnel, and cabin passengers within the aircraft, dependent on airline-intended use. This specification does not impose a limit of the type of application the CWAP supports. It is expected that airlines will define what type of data can be made available over the wireless link provided by the CWAP.

There are some major differences between CWAP and CWLU: CWAP is expected to be designed to be a node on the aircraft LAN and for that purpose should be provided with network daisy chaining capability. CWAP extends the capability of the CWLU by providing higher bandwidth wireless connectivity. Finally, CWAP is expected to support for more than one RF antenna thus allowing support of antenna diversity technology such as Multiple Input/Multiple Output (MIMO).

Similarly to CWLU, each CWAP is expected to create one or more RF coverage cell.

17.1.2 Description of the CABIN CELL MODEM (CCM)

The primary function of the Cabin Cell Modem (CCM) is to provide a cellular and/or wireless data connection from the aircraft to the ground network application, while the aircraft is on ground.

The CCM communicates with the host aircraft system (e.g. IFE System) via electrical or fiber optic interfaces.

The radios of the CCM shall operate on ground only.

The CCM can be used to transmit stored data (e.g. BITE messages, performance and statistical data), to receive media content, and to manage Digital Right Management (DRM) keys.

17.1.3 CWAP / CCM Referencing Scheme

A628-P1 – 17 – A10 – I A N – 10.00.00.00

ARINC 628 Part 1

Chapter of Component

Interface Configuration:

Digit 1 (A-G): Main Interface Configuration
A: 2.5Gpbs Eth.
B: 2.5Gbps Eth. / J7 at front side
C: 2.5Gpbs Eth.+ 10Gbps F/O (ARINC 801)
D: 2.5Gpbs Eth.+ 10Gbps F/O (EN4531)
E: 10Gbps F/O (ARINC 801)
F: 10Gbps F/O (EN4531)
G-H: Reserved for future 10Gbps MT F/O

Digit 2 (1/0): 0: J3 not implemented
1: J3 implemented

Digit 3 (0-2): 0: J7..Jxx TNC not implemented
1: J7..Jxx TNC implemented

Equipment Type:
I: Internal Communication (CWAP)
E: External Communication (CCM)
H: Hybrid (CWAP + CCM)

~~**Antenna Configuration:**~~
~~**A**: Integrated Antenna(s) only~~
~~**S**: Separate/External Antenna(s) required~~

~~**Battery Configuration:**~~
~~**B**: Includes Battery Pack~~
~~**N**: No Battery~~

~~**Radio Types:**~~
~~**Digit 1 (4-7):** Wi-Fi Standard 802.11 n, ac, ax, be~~
~~4: Wi-Fi 4 Standard~~
~~5: Wi-Fi 5 Standard~~
~~6: Wi-Fi 6 Standard~~
~~7: Wi-Fi 7 Standard~~
~~**Digit 2 (1/0):** 60Ghz Wi-Gig 802.11 ad, ay~~
~~**Digit 3 (1/0):** Low Rate WPAN 802.15.4~~
~~**Digit 4 (1/0):** WiMAX~~
~~**Digit 5 (1/0):** WAIC~~
~~**Digit 6 (1/0):** *Other (to be sp*~~
~~**Digit 7 (1/0):** *Reserved*~~
~~**Digit 8 (0-6):** Mobile Network~~
~~4: 4G Standar~~
~~5: 5G Standar~~
~~6: 6G Standard~~

~~** e.g. Bluetooth 802.15.1 / BT SIG*~~

Urban / Nov.19:
Proposal: Simplified reference scheme excluding specific communication standards.
Rather refer to frequency ranges / bands?
AI: Airbus to build example

17.2 Installation Locations

17.2.1 CWAP Installation Locations

In a typical CWAP system, several units are installed along the aircraft cabin. (e.g. 3 units for narrow-body aircraft and 6 units for wide-body aircraft),
The exact location and number of CWAPs is depending on aircraft type.

To support system performance, the CWAPs should be located at equal distances between each unit covering all cabin zones. Obstruction of the wireless signal path between CWAP to the PAX mobile equipment should be avoided as far as possible.

17.2.2 CCM Installation Locations

Typically, one CCM is installed per aircraft. The installation location of the CCM is depending on aircraft type.

To enable wireless communication with external networks, the installation location should be in the proximity of those aircraft doors, which are open during normal boarding / de-boarding process.
Typical installation locations are:

- Ceiling area near LH FWD door (behind cabin lining)
- Inside IFE control center / purser station near LH FWD doors

If the CCM is integrated with antennas external to the aircraft fuselage, the installation location is not depending on proximity to aircraft doors.

One could consider the possibility that more than one cell modem may be installed in an aircraft, albeit used by another system or purpose.

17.3 INTERFACES

The CWAP/CCM connector arrangement is defined to account for:

- Backwards compatibility with former A628 CWAP implementations (J1-J3 located adjacent to each other at venter of LRU)
- Efficient arrangement of J4/J5 Fiber Optic ports side by side
- Reserving space for future interface options (e.g. J6)
- Creating special configuration B to account for installation that do not allow RF interfaces at rear side of LRU.

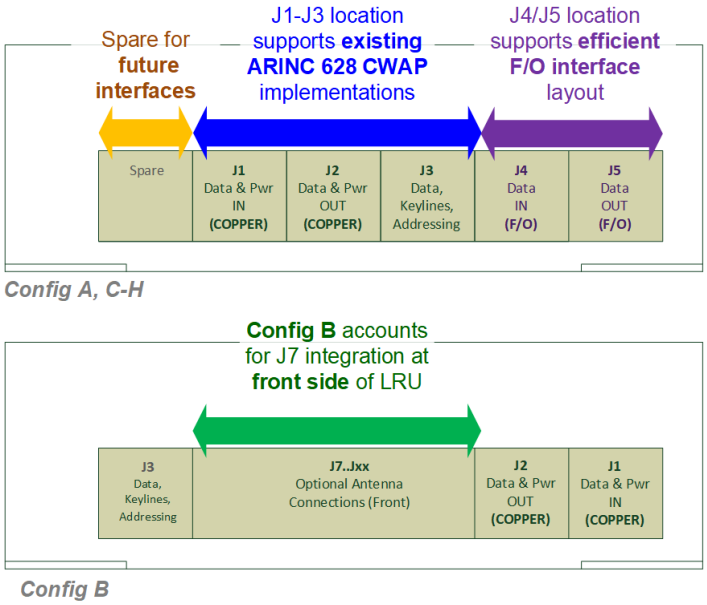


Figure 17-x - CWAP / CCM Interfaces

17.3.1 CONNECTOR DESIGNATIONS AND LOCATIONS

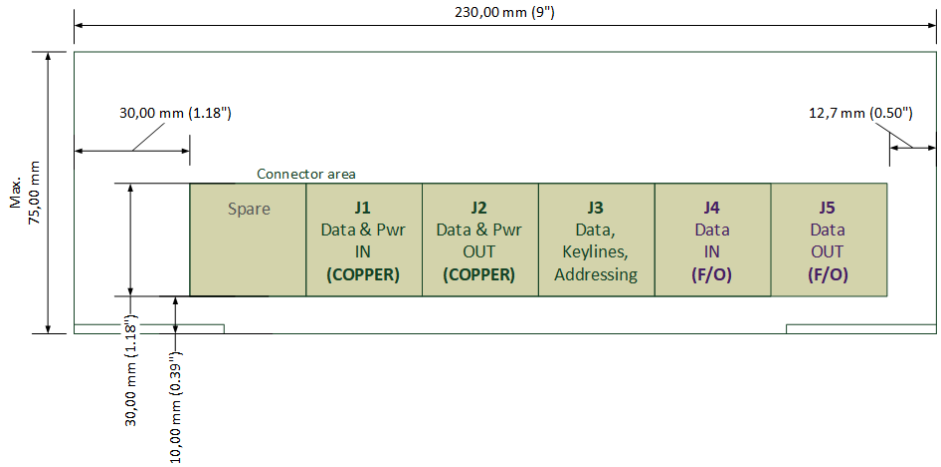


Figure 17-1a - Main Interface (Front Side)

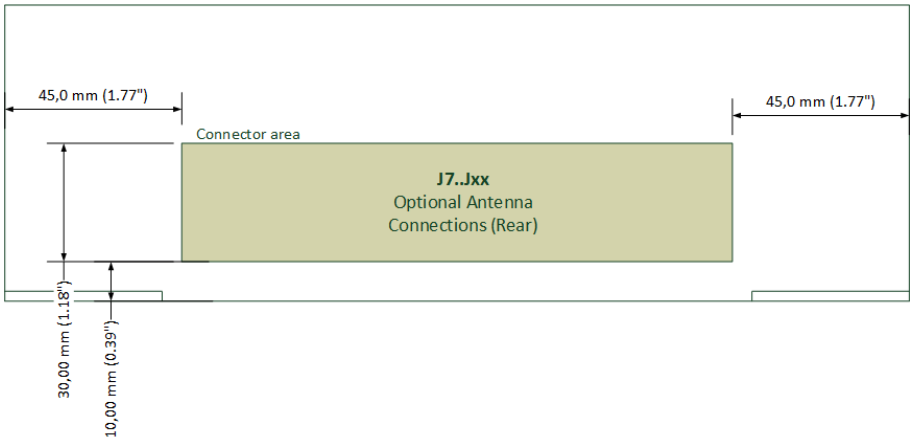


Figure 17-1b - Optional Antenna Interface (Rear Side)

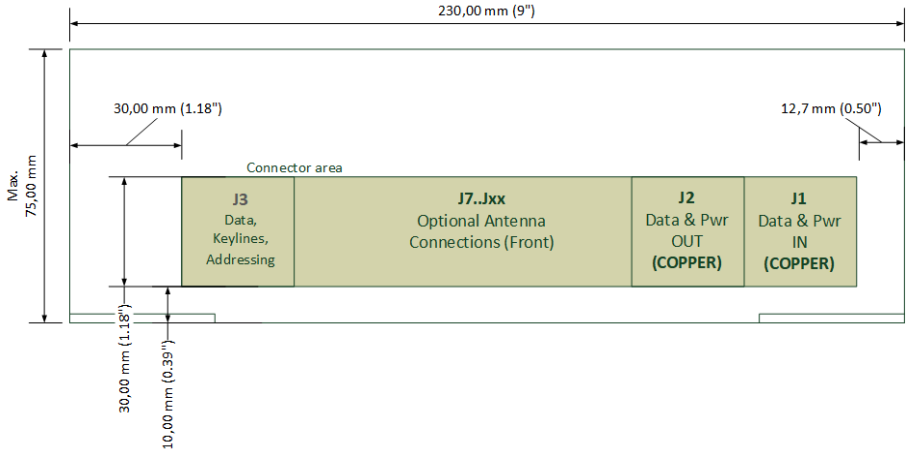


Figure 17-1c - Configuration B with Antenna Interface at Front Side

17.3.2 INTERFACE CONFIGURATION

This standard provides a range of different CWAP and CCM interface configurations covering copper based Ethernet and Fiber Optic data connections. Each configuration is identified by a configuration code ("**A**" through "**H**"). The space envelope, mechanical interface and connector locations are the same for all interface configurations.

AI: More study is needed on power/proximity to higher speed connections (J1..Jx)

The interface configurations include the following variants for **J1-J5 and J7-Jxx**:

A: 2.5Gpbs Ethernet
B: 2.5Gpbs Ethernet *with optional J7 RF interface at front side*
C: 2.5Gpbs Ethernet + 10Gbps Fiber Optic (ARINC 801)
D: 2.5Gpbs Ethernet + 10Gbps Fiber Optic (EN4531)
E: 10Gbps Fiber Optic (ARINC 801)
F: 10Gbps Fiber Optic (EN4531)
G-H: *Reserved for future 10Gbps MT Fiber Optic*

J3 is an optional interface, which may include a 28VDC power input, pin addressing, control keylines and inputs for an external battery pack ~~a third Ethernet Port ETH3~~. The **J3** pin definition varies depending on equipment type (CWAP or CCM)

J7..Jxx are optional antenna interfaces.

J6 is reserved for future use.

The CWAP/CCM shall include one of **interface configurations** listed in Table 17-1.
The CWAP/CCM interfaces shall be **designated and located** as defined in Fig. 17-01a-c

To enable compatibility to existing ARINC 628 p1-17 installations, Configuration A (J1-J3 located side-by-side) should be applied as the preferred solution for new copper-based CWAP/CCM designs.

	J1	J2	J3 (optional)	J4	J5	J7..Jxx (optional)
A *Copper Only*	*2.5G & PWR*	*2.5G & PWR*	*2.5G & ADDR Keylines*			RF
B *Copper Only*	*2.5G & PWR*	*2.5G & PWR*	*2.5G & ADDR Keylines*			RF *(at front side of LRU)*
C *Copper + A801*	*2.5G & PWR*	*2.5G & PWR*	*2.5G & ADDR Keylines*	*10G F/O (A801)*	*10G F/O (A801)*	RF
D *Copper + EN4531*	*2.5G & PWR*	*2.5G & PWR*	*2.5G & ADDR Keylines*	*10G F/O (EN4531)*	*10G F/O (EN4531)*	RF

E A801	*PWR*	*PWR*		*10G F/O (A801)*	*10G F/O (A801)*	RF
F EN4531	*PWR*	*PWR*		*10G F/O (EN4531)*	*10G F/O (EN4531)*	RF
G-H MT	*PWR*	*PWR*		*10G F/O (MT)*	*10G F/O (MT)*	RF

Table 17-1 – CWAP/CCM Interface Configurations

17.3.2.1 Configuration A (Copper 2.5Gbps)

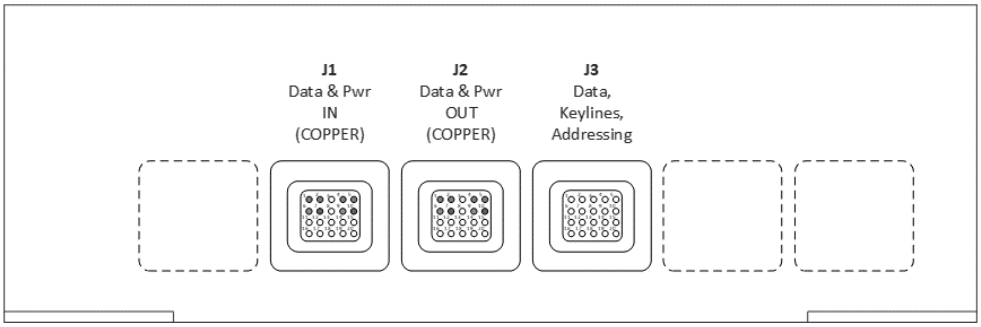


Figure 17-2 – Configuration A

	J1	J2	J3 (optional)	J4	J5
Shell	EN4165M01AA	EN4165M01AB	EN4165M01AC		
Mating Shell	EN4165M61AA	EN4165M61AB	EN4165M61AC		
Module	EN4165A20-22-1NA	EN4165A20-22-1NB	EN4165A20-22-1NA		
Mating Module	EN4165A20-22-1NB	EN4165A20-22-1NA	EN4165A20-22-1NB		

Table 17-2 – Configuration A Connector Definition

17.3.2.2 Configuration B (Copper 2.5Gbps with J7 interface at front side)

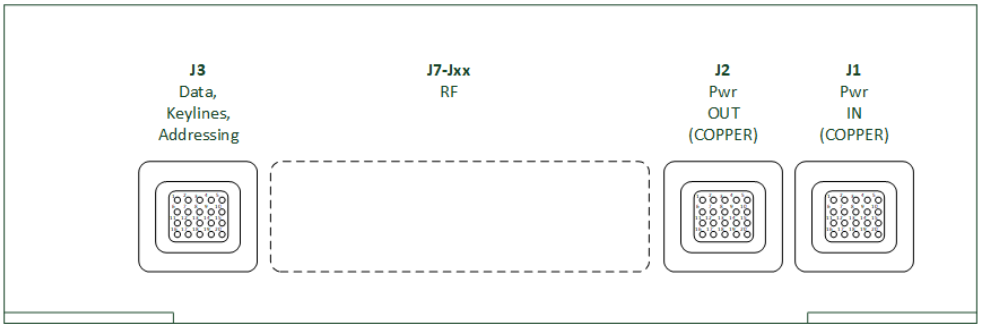


Figure 17-3 – Configuration B

	J1	J2	J3 (optional)	J4	J5
Shell	EN4165M01AA	EN4165M01AB	EN4165M01AC		
Mating Shell	EN4165M61AA	EN4165M61AB	EN4165M61AC		
Module	EN4165A20-22-1NA	EN4165A20-22-1NB	EN4165A20-22-1NA		
Mating Module	EN4165A20-22-1NB	EN4165A20-22-1NA	EN4165A20-22-1NB		

Table 17-3 – Configuration B Connector Definition

17.3.2.3 Configuration C/D (Copper 2.5Gbps + 10Gbps F/O)

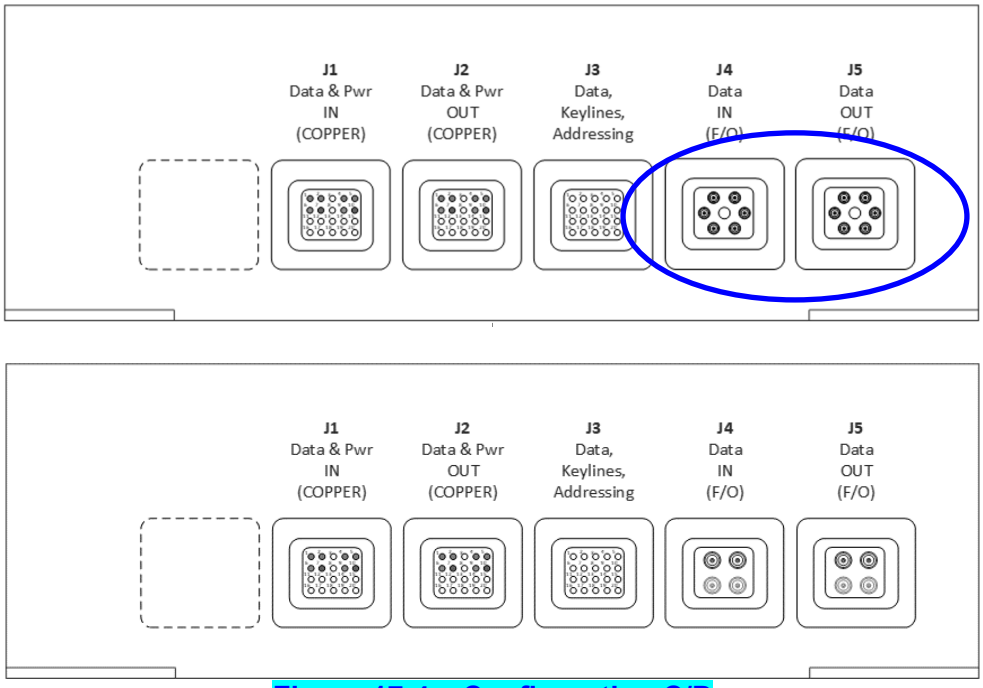


Figure 17-4 – Configuration C/D

	J1	J2	J3 (optional)	J4	J5
Shell	EN4165M01AA	EN4165M01AB	EN4165M01AC	EN4165M01AD	EN4165M01AE
Mating Shell	EN4165M61AA	EN4165M61AB	EN4165M61AC	EN4165M61AD	EN4165M61AE
Config B					
Module	EN4165A20-22-1NA	EN4165A20-22-1NB	EN4165A20-22-1NA	ARINC 801 Insert	ARINC 801 Insert
Mating Module	EN4165A20-22-1NB	EN4165A20-22-1NA	EN4165A20-22-1NB	ARINC 801 Insert	ARINC 801 Insert
Config C					
Module	EN4165A20-22-1NA	EN4165A20-22-1NB	EN4165A20-22-1NA	EN4531 Insert	EN4531 Insert
Mating Module	EN4165A20-22-1NB	EN4165A20-22-1NA	EN4165A20-22-1NB	EN4531 Insert	EN4531 Insert

Table 17-4 – Configuration C/D Connector Definition

17.3.2.4 Configuration E/F (10Gbps F/O)

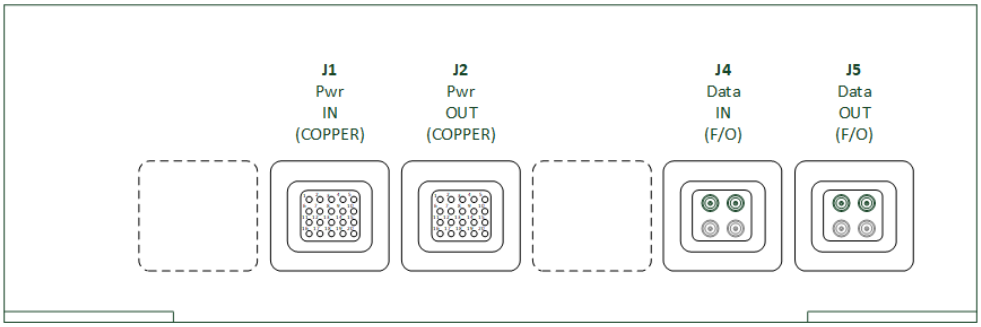


Figure 17-5 – Configuration E/F

	J1	J2	J3	J4	J5
Shell	EN4165M01AA	EN4165M01AB		EN4165M01AD	EN4165M01AE
Mating Shell	EN4165M61AA	EN4165M61AB		EN4165M61AD	EN4165M61AE
Config D					
Module	EN4165A20-22-1NA	EN4165A20-22-1NB		ARINC 801 Insert	ARINC 801 Insert
Mating Module	EN4165A20-22-1NB	EN4165A20-22-1NA		ARINC 801 Insert	ARINC 801 Insert
Config E					
Module	EN4165A20-22-1NA	EN4165A20-22-1NB		EN4531 Insert	EN4531 Insert
Mating Module	EN4165A20-22-1NB	EN4165A20-22-1NA		EN4531 Insert	EN4531 Insert

Table 17-5 – Configuration E/F Connector Definition

17.3.2.5 Configuration G/H (Reserved for future 10Gbps F/O MT Contact)

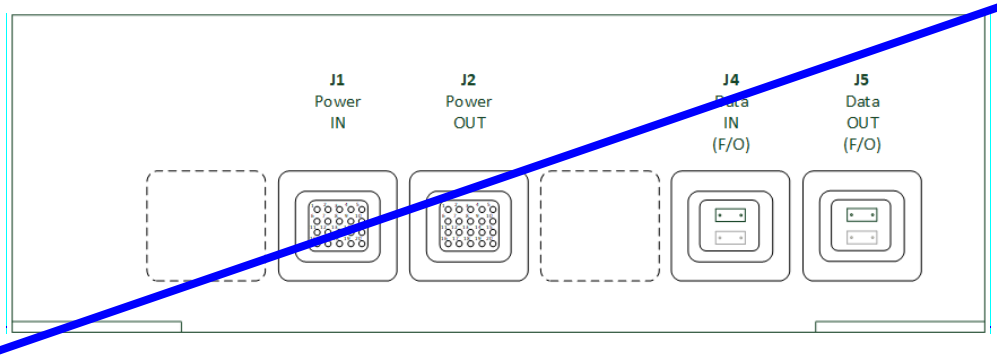


Figure 17-6a – CWAP Configuration G

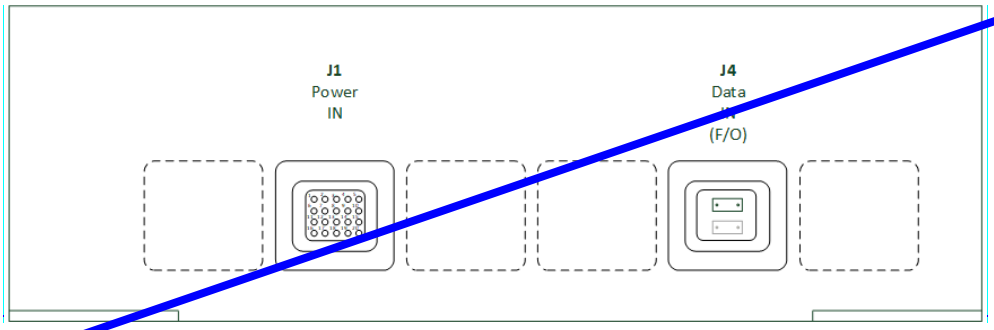


Figure 17-6b – Configuration H

	J1	J2	J3 (optional)	J4	J5
Shell	EN4165M01AA	EN4165M01AB	EN4165M01AC	EN4165M01AD	EN4165M01AE
Mating Shell	EN4165M61AA	EN4165M61AB	EN4165M61AC	EN4165M61AD	EN4165M61AE
Config F					
Module	EN4165A20-22-1NA	EN4165A20-22-1NB	EN4165A20-22-1NA	MT Insert	MT Insert
Mating Module	EN4165A20-22-1NB	EN4165A20-22-1NA	EN4165A20-22-1NB	MT Insert	MT Insert
Config G					
Module	EN4165A20-22-1NA	EN4165A20-22-1NB	EN4165A20-22-1NA	MT Insert	
Mating Module	EN4165A20-22-1NB	EN4165A20-22-1NA	EN4165A20-22-1NB	MT Insert	

Table 17-6 – Configuration F/G Connector Definition

17.3.3 Connector Pin Definition

17.3.3.1 J1 Pin Assignment

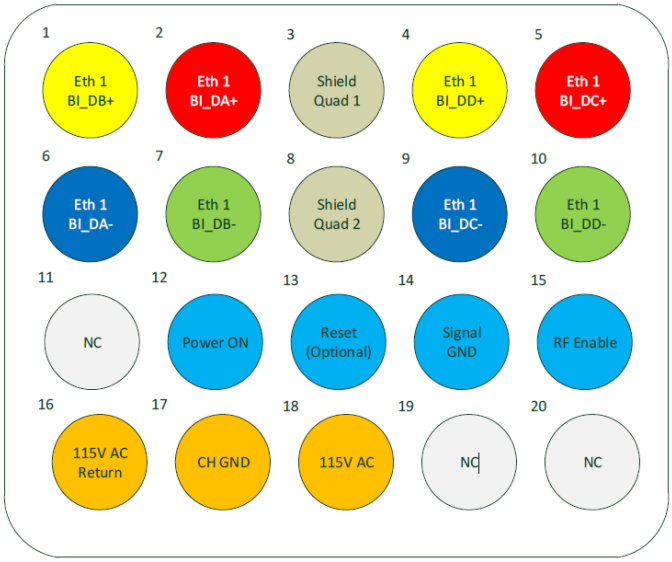


Figure 17-x – Pin Arrangement of Connector J1 (pins)

Pin ID	Signal Name	Description	Config A-D	Config E-H
1	ETH 1 BI_DB+	Ethernet 1 2.5GBase-T (Quad 1)	X	
2	ETH 1 BI_DA+	Ethernet 1 2.5GBase-T (Quad 1)	X	
3	ChGnd	Shield Quad 1	X	
4	ETH 1 BI_DD+	Ethernet 1 2.5GBase-T (Quad 2)	X	
5	ETH 1 BI_DC+	Ethernet 1 2.5GBase-T (Quad 2)	X	
6	ETH 1 BI_DA-	Ethernet 1 2.5GBase-T (Quad 1)	X	
7	ETH 1 BI_DB-	Ethernet 1 2.5GBase-T (Quad 1)	X	
8	ChGnd	Shield Quad 2	X	
9	ETH 1 BI_DC-	Ethernet 1 2.5GBase-T (Quad 2)	X	
10	ETH 1 BI_DD-	Ethernet 1 2.5GBase-T (Quad 2)	X	
11	Discrete GND	Optional for PIN 12	X	X
12	Power ON	GND = power on, OPEN = power off	X	X
13	Not Connected			
14	Signal GND	Reference for discretes	X	X
15	RF Enable	GND = RF on, OPEN = RF off	X	X
16	115 Vac Return	AC Power Return	X	X
17	CH GND	Chassis ground	X	X
18	115 Vac	AC Power input (max. 5A)	X	X
19	Not Connected			
20	Not Connected			

Table 17-x – Pin Definition of Connector J1

17.3.3.2 J2 Pin Assignment

Figure 17-x – Pin Arrangement of Connector J2 (sockets)

Depending on the interface configuration of the CWAP/CCM, J2 is defined with or without Ethernet port (see applicability columns in Table 17-x).

Pin ID	Signal Name	Description	Config A-D	Config E-H
1	ETH 2 BI_DA+	Ethernet 2 2.5GBase-T out (Quad 1)	X	
2	ETH 2 BI_DB+	Ethernet 2 2.5GBase-T out (Quad 1)	X	
3	ChGnd	Shield Quad 1	X	
4	ETH 2 BI_DC+	Ethernet 2 2.5GBase-T out (Quad 2)	X	
5	ETH 2 BI_DD+	Ethernet 2 2.5GBase-T out (Quad 2)	X	
6	ETH 2 BI_DB-	Ethernet 2 2.5GBase-T out (Quad 1)	X	
7	ETH 2 BI_DA-	Ethernet 2 2.5GBase-T out (Quad 1)	X	
8	ChGnd	Shield Quad 2	X	
9	ETH 2 BI_DD-	Ethernet 2 2.5GBase-T out (Quad 2)	X	
10	ETH 2 BI_DC-	Ethernet 2 2.5GBase-T out (Quad 2)	X	
11	Not Connected		X	X
12	Power ON	GND = power on, OPEN = power off	X	X
13	Not Connected			
14	Signal GND	Reference for discretes	X	X
15	RF Enable	GND = RF on, OPEN = RF off	X	X
16	115VAC Return		X	X
17	CH GND		X	X
18	115VAC		X	X
19	Not Connected			
20	Not Connected			

Table 17-x – Pin Definition of Connector J2

17.3.3.3 CWAP J3 Pin Assignment

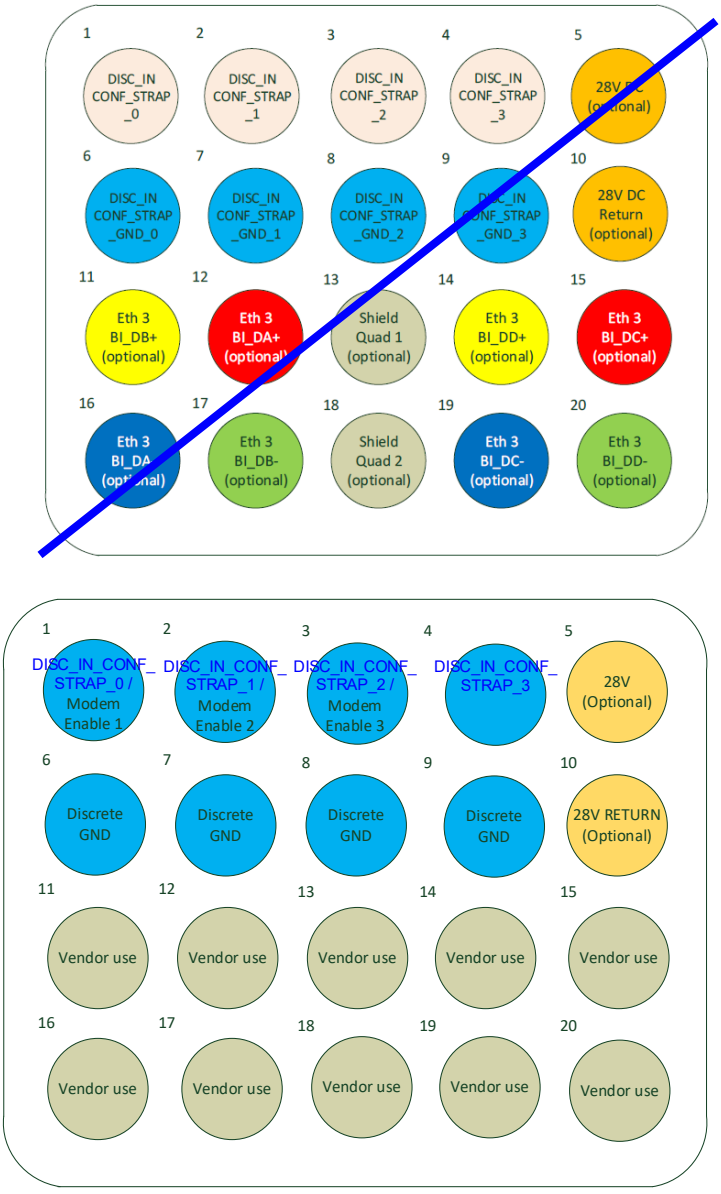


Figure 17-x – CCM/CWAP J3 (pins)

Pin ID	Signal Name	Description
1 (CWAP)	DISC_IN_CONF_STRAP_0	Address pin 1 (See Note)
2 (CWAP)	DISC_IN_CONF_STRAP_1	Address pin 2 (See Note)
3 (CWAP)	DISC_IN_CONF_STRAP_2	Address pin 3 (See Note)
4 (CWAP)	DISC_IN_CONF_STRAP_3	Address pin 4 (See Note)
1 (CCM + Hybrid)	Modem enable 1	GND = Modem on, OPEN = Modem off
2 (CCM + Hybrid)	Modem enable 2	GND = Modem on, OPEN = Modem off
3 (CCM + Hybrid)	Modem enable 3	GND = Modem off, OPEN = Modem on
4 (CCM + Hybrid)	Not connected	
5	28V	Optional 28V Interface
6	Discrete GND	Ground reference for pin 1..4
7	Discrete GND	Ground reference for pin 1..4
8	Discrete GND	Ground reference for pin 1..4
9	Discrete GND	Ground reference for pin 1..4
10	28V Return	Optional 28V Interface
11	Vendor use	Vendor use
12	Vendor use	Vendor use
13	Vendor use	Vendor use
14	Vendor use	Vendor use
15	Vendor use	Vendor use
16	Vendor use	Vendor use
17	Vendor use	Vendor use
18	Vendor use	Vendor use
19	Vendor use	Vendor use
20	Vendor use	Vendor use

Figure 17-x – Pin Arrangement of Connector J3 (pins)

Note: See Table 17-x for Addressing.

Add pins for Battery Pack?

~~Depending on the interface configuration of the CWAP/CCM, J1 is defined with or without Ethernet port (see applicability columns in Table 17-x).~~

Pin	Function	Remark
1	DISC_IN_CONF_STRAP_0	Address Pin 1 (see note)
2	DISC_IN_CONF_STRAP_1	Address Pin 2 (see note)
3	DISC_IN_CONF_STRAP_2	Address Pin 3 (see note)
4	DISC_IN_CONF_STRAP_3	Address Pin 4 (see note)
5	28 Vdc	Optional
6	DISC_IN_CONF_STRAP_GND_0	Signal Ground
7	DISC_IN_CONF_STRAP_GND_1	Signal Ground
8	DISC_IN_CONF_STRAP_GND_2	Signal Ground
9	DISC_IN_CONF_STRAP_GND_3	Signal Ground
10	28 Vdc return	Optional
11	ETH 3 BI_DB+	Ethernet 3 2.5GBase-T out (Quad 1)
12	ETH 3 BI_DA+	Ethernet 3 2.5GBase-T out (Quad 1)
13	ChGnd	Shield Quad 1
14	ETH 3 BI_DD+	Ethernet 3 2.5GBase-T out (Quad 2)
15	ETH 3 BI_DC+	Ethernet 3 2.5GBase-T out (Quad 2)
16	ETH 3 BI_DA-	Ethernet 3 2.5GBase-T out (Quad 1)
17	ETH 3 BI_DB-	Ethernet 3 2.5GBase-T out (Quad 1)
18	ChGnd	Shield Quad 2
19	ETH 3 BI_DC-	Ethernet 3 2.5GBase-T out (Quad 2)
20	ETH 3 BI_DD-	Ethernet 3 2.5GBase-T out (Quad 2)

~~Figure 17-x – CWAP Pin Arrangement of Connector J3~~

DISC_IN_CONF_STRAP_3 (MSB)	DISC_IN_CONF_STRAP_2	DISC_IN_CONF_STRAP_1	DISC_IN_CONF_STRAP_0 (LSB)	CWAP No.
open	open	open	open	1
open	open	open	ground	2
open	open	ground	open	3
open	open	ground	ground	4
open	ground	open	open	5
open	ground	open	ground	6
open	ground	ground	open	7
open	ground	ground	ground	8
ground	open	open	open	9
ground	open	open	ground	10
ground	open	ground	open	11
ground	open	ground	ground	12
ground	ground	open	open	13
ground	ground	open	ground	14
ground	ground	ground	open	15
ground	ground	ground	ground	Supplier Specific

Table 17-x – CWAP Addressing

17.3.3.4 CCM J3 Pin Assignment

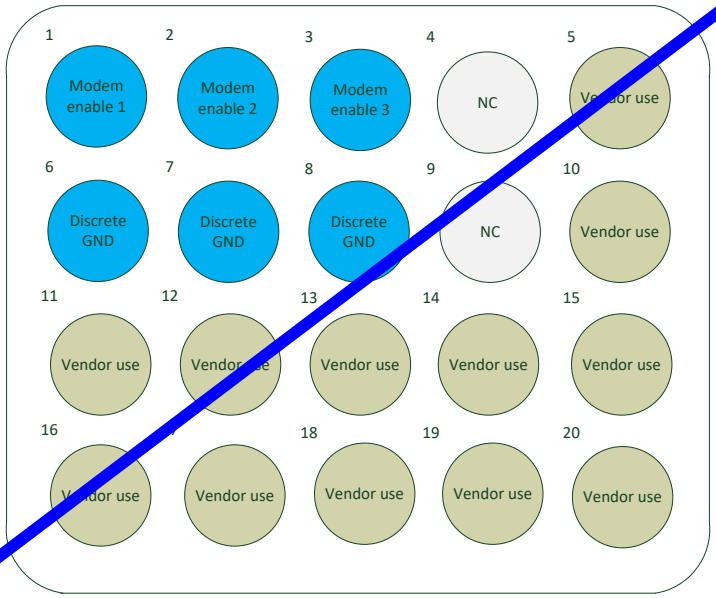


Figure 17-x – CCM J3 (pins)

Pin ID	Signal Name	Description
1	Modem enable 1	GND = Modem on, OPEN = Modem off
2	Modem enable 2	GND = Modem on, OPEN = Modem off
3	Modem enable 3	GND = Modem off, OPEN = Modem on
4	Not connected	
5	Reserved	Vendor use
6	Discrete GND 1	
7	Discrete GND 2	
8	Discrete GND 3	
9	Not connected	
10	Reserved	Vendor use
11	Reserved	Vendor use
12	Reserved	Vendor use
13	Reserved	Vendor use
14	Reserved	Vendor use
15	Reserved	Vendor use
16	Reserved	Vendor use
17	Reserved	Vendor use
18	Reserved	Vendor use
19	Reserved	Vendor use
20	Reserved	Vendor use

Table 17-x – CCM Pin Arrangement of Connector J3

17.3.3.5 J4 / J5 F/O Contact Assignment in I/F Configuration E

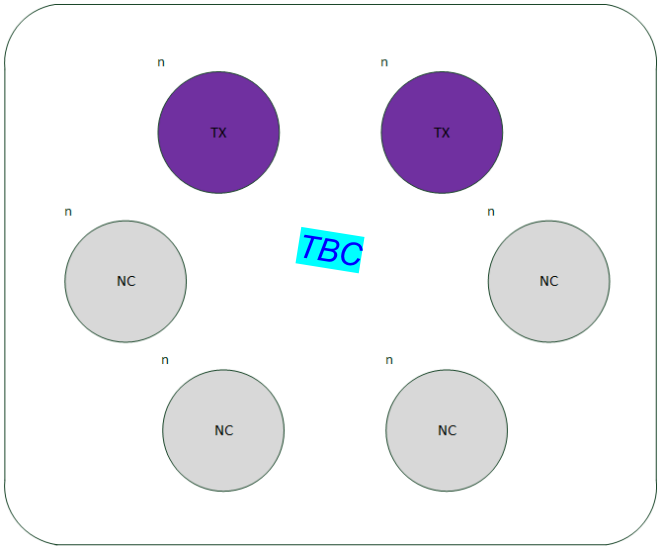


Figure 17-x – F/O Contact Arrangement of Connector J4/J5

Pin	Function	Remark
1	FO_1_TX	Fiber Optic Port 1 TX
2	FO_1_RX	Fiber Optic Port 1 RX
3	Not Connected TBC	
4	Not Connected	
5	Not Connected	
6	Not Connected	

Table 17-x- F/O Contact Definition of Connector J4

Pin	Function	Remark
1	FO_2_TX	Fiber Optic Port 2 TX
2	FO_2_RX	Fiber Optic Port 2 RX
3	Not Connected TBC	
4	Not Connected	
5	Not Connected	
6	Not Connected	

Table 17-x - F/O Contact Definition of Connector J5

17.3.3.5 J4 / J5 F/O Contact Assignment in I/F Configuration F

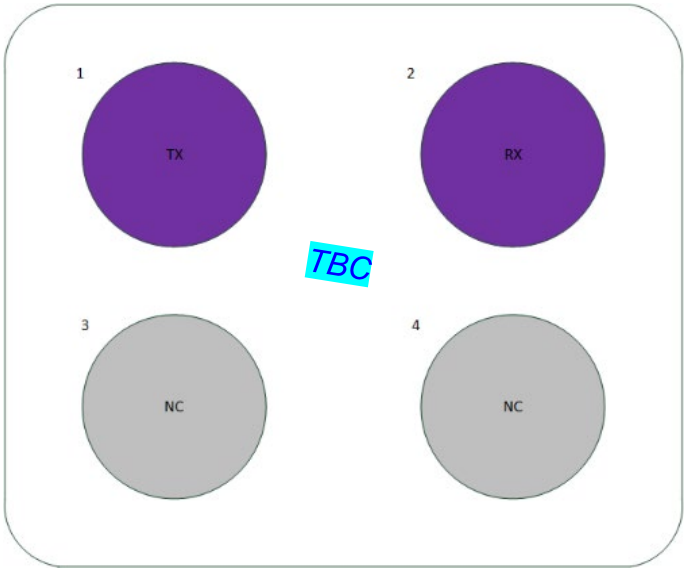


Figure 17-x – F/O Contact Arrangement of Connector J4/J5

Pin	Function	Remark
1	FO_1_TX	Fiber Optic Port 1 TX
2	FO_1_RX TBC	Fiber Optic Port 1 RX
3	Not Connected	
4	Not Connected	

Table 17-x- F/O Contact Definition of Connector J4

Pin	Function	Remark
1	FO_2_TX	Fiber Optic Port 2 TX
2	FO_2_RX	Fiber Optic Port 2 RX
3	Not Connected TBC	
4	Not Connected	

Table 17-x - F/O Contact Definition of Connector J5

~~17.3.3.6 J4 / J5 F/O Contact Assignment in I/F Configuration G-H~~

~~Reserved for future use~~

17.3.3.7 J7-Jxx Optional Antenna Interfaces

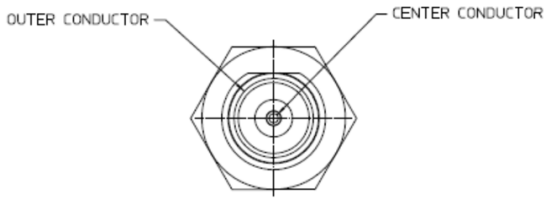


Figure 17-10 – CWAP J7-Jxx

The J7-Jxx connector type is supplier specific.

In case the CWAP/CCM requires separate antennas, the CWAP/CCM supplier shall coordinate the J7-Jxx configuration with the airframe manufacturer to ensure compatibility with airframe electrical integration standards.

Depending on the general interface configuration, the optional external antenna J7-Jxx may be located at the front or the rear side of the unit.

17.3.4 Electrical Interface

Input Power:

- 115 Vac Variable Frequency single phase or 28 Vdc.
- ~~If the CWAP is not daisy-chained, it is expected to get its power locally from the aircraft power distribution system.~~
- The CWAP/CCM should be designed to operate normally through power interruptions of up to 200 milliseconds duration for 115 Vac installations and 28 Vdc installations.

COMMENTARY

CWAP/CCM may provision for both AC and DC power supplies. However, it is not expected to operate from both supplies connected at the same time.

Power Consumption

- 25W maximum

COMMENTARY

This maximum is based on the assumption of a passively cooled LRU. Power consumption in excess of this value will require additional cooling considerations.

Ethernet I/Os in **Interface Configuration A-D**

- Two gigabit Ethernet (2.5GBase-T) switched ports should be provided.
- ~~A third gigabit Ethernet (2.5GBase-T) port may be provided via optional connector J3. This Ethernet port can support functions like Airline Information Services Domain (AISD) connectivity.~~
- The Ethernet ports should support pass-through of Ethernet data at 2500 Mbps.

Discrete input signals:

- One low-current discrete for CWAP/CCM power control should be provided: a POWER ON signal that turns on internal power to the unit upon assertion. This signal should also be used to connect or disconnect the optional CCM internal battery pack.
- One (CWAP) / Three (CCM) low current discretes should be provided for an RF Enable signal which enables all controlled radio-frequency emissions from the CWAP upon assertion.
- These signals should comply with Section 2.2.1 of this Specification.

COMMENTARY

Discrete input signals can be controlled remotely allowing installations where the CWAP is in an overhead location in the cabin, whereas the controlling equipment may be installed in an electronic bay. Distances of up to 150 ft. (50 m) are not uncommon for such installations.

Configuration Signals:

- Four optional pin straps should be provided by the CWAP intended to define internal IP operation of the unit. Such things as static IPs or DHCP IP assignment could be controlled via these signals.
- These signals should comply with Section 2.2.1 of this Specification.

17.3.5 Optical Interface

Fiber Optic I/Os in **Interface Configuration C-F** (ARINC 801 / EN4531 contact)

- Two Fiber Optic (10GBASE-SR) switched ports should be provided.

~~Fiber Optic I/Os in **Interface Configuration G-H** (future MT contact)~~

- ~~Two Fiber Optic (10GBase-F) switched ports should be provided.~~
- ~~A third Fiber Optic (10GBase-F) switched port is optional.~~

The Fiber Optic ports should support pass-through of Ethernet data at 10 Gbps.

17.3.6 RF Interface (CWAP)

The CWAP should be fitted with one or more radios capable of transmitting data using the IEEE 802.11 family of standards.

The CWAP should be able to operate in either the 2.4 GHz or the 5 GHz bands or both at the same time (requiring more than one radio).

When equipped with more than one radio, each radio should be controllable independently. In particular, transmit power levels, operating channels, mode of operation and hosted VSC (see Section 17.6.6) should be independently controllable per radio.

During normal operation and in any case of failure of the radio transmitter system inside the aircraft, no single radio inside the aircraft shall transmit power levels (EIRP) higher than 100 mW (20 dBm) for pulsed levels and 100 mW (20 dBm) for continuous wave levels. If multiple radios operating on the same frequency band are embedded into one CWAP, the total transmit power levels (EIRP) of all embedded radios shall not exceed the above limits on the same frequency band.

Application of WiFi7 IEEE 802.11be standard is reserved for future use.
Account for WiFi 6E?

17.3.7 RF Interface (CCM)

The CCM should be fitted with one or more radios capable of transmitting data

using the 4G LTE as a minimum.

Optionally the CCM may support the 5G standard and/or IEEE 802.11 family of standards.

The EIRP of each radio may exceed 100mW if the antennas are located outside the aircraft fuselage or if the CCM radios are disabled during flight.

When equipped with more than one radio, each radio should be controllable independently. In particular, transmit power levels, operating channels, mode of operation and hosted VSC (see Section 17.6.6) should be independently controllable per radio.

Application of 6G and WiFi7 IEEE 802.11be standards is reserved for future use. *Account for WiFi 6E?*

17.3.8 Antenna Interfaces

The CWAP/CCM can be fitted with internal or separate (remote) antennas or both.

Separate antennas may be located within the same ARINC 836 space envelope as the CWAP/CCM itself or installed remotely in their own ARINC 836 space envelope.

If they are sharing the same space envelope as the CWAP/CCM, the combined assembly of CWAP/CCM, antenna, and antenna mounting bracket (if any) should fit within the ARINC 836 envelope defined for the CWAP/CCM in Section 17.5.1.

If separate antennas are mechanically adjustable then the CWAP/CCM should fit in the ARINC 836 envelope defined in Section 17.5.1 with all antennas fully deployed (largest occupied volume).

COMMENTARY

Although integrated antennas are preferred for ease of installation, they may limit the installation location and orientation of the CWAP/CCM to provide adequate RF coverage to its intended clients.

The CWAP should have the necessary antenna interfaces to be capable to operate in ~~, in IEEE 802.11ac, ax, n~~ 2x2 MIMO diversity mode at a minimum.

When supporting separate/remote antenna connections, the CWAP/CCM should provide at least two RF TNC coax connectors for connection of coax cable feeds to remote antennas. ~~The two (or more) antennas enable the use of antenna diversity for increased bandwidth.~~

The CWAP~~/CCM~~ should also be operable with a single antenna connection only, without requiring modification of the CWAP~~/CCM~~ (other than a possible configuration setting change)

For IEEE 802.11, 3G and 4G operations in the 2.4 GHz and 5 GHz bands, the input impedance at any antenna interface should be 50 ohms nominal.

COMMENTARY

To provide optimal RF performance it is recommended that a maximum Voltage Standing Wave Ratio (VSWR) of 4.0:1 be achieved over the 2.39-2.49 GHz and 4.9-5.9 GHz frequency ranges.

17.3.9 RF emissions containment

The primary method of emissions containment is accomplished by connecting the cable shield(s) to the connector back shell.
Secondary shielding can be accomplished by also connecting the cable shield to the identified Chassis Ground pins.

~~17.4 BATTERIES~~

~~The CCM may contain an optional rechargeable lithium battery pack. If a battery pack is installed inside the CCM, it has to be tested in accordance to RTCA-DO-347 or RTCA DO-311A requirements.~~

~~The CCM shall provide means to disconnect / isolate the battery.~~

17.5 BITE

The CWAP/CCM should perform self-test functions at Power ON. The units should verify the status of the following items in automatic sequence:

- Correct operation of unit
- I/O modules (including radios)
- Processing
- Memory
- Internal power supply
- External CCM battery pack interface

Relevant hardware resources should be monitored during operation e.g. Commanded Built In Test (CBIT). The CWAP/CCM should be capable of being remotely queried by the host system to provide a detailed health status. SNMPv3 should be used for such a feature.

COMMENTARY

A MIB based on those that are readily available in the commercial industry should be implemented. For that purpose, use of IEEE 802.11 Annex D MIB and its amended version in IEEE 802.11n Annex D are recommended. In addition, control MIBs defined in IETF RFC 5833 and RFC 5834 should also be supported. Commercial MIBs that are based on these standard MIBs, but modified to account for the features that the commercial product supports, are considered as meeting the goal of this specification. This allows CWAP/CCM manufacturers to embed consumer electronics wireless technology, as is, into their design.

17.6 DESIGN GUIDELINES

This section provides guidelines regarding key physical and operational aspect of the CWAP/CCM.

17.6.1 Size

The CWAP/CCM should fit into an envelope per ARINC Specification 836. The size is defined to be A836-1-7 in length and width.

However, CWAP/CCM height should be minimized and should be no greater than 2.95 in (75 mm) including mounting flange, ~~external~~ antenna mounting, and ARINC Specification 836 adapter plate, if required.

The CWAP/CCM should allow close connection of the transceiver to the antennas to reduce the signal power loss from the antenna cables.

17.6.2 Weight

5.51 lbs. (2.5 kg) maximum.

17.6.3 Environmental Conditions

The equipment should meet the environmental requirements of Section 10.

17.6.4 Cooling

The equipment should be designed to perform without forced air cooling.

17.6.5 Grounding and Bonding

Grounding and bonding should be as defined in ARINC Specification 836, Section 4.1.2

17.6.6 On/Off Control and Status

This specification defines a CWAP/CCM interface to control the on/off mode of the CWAP/CCM.

The CWAP/CCM should incorporate one low current input discrete as defined in Section 2.2.1 for use in remotely controlling CWAP/CCM power. The CWAP/CCM should be commanded to the “on” state only when the on/off control discrete input is in the grounded state.

There may be situations when it is beneficial to keep the non RF emitting part of the CWAP/CCM powered and depower the radios. For that purpose, the CWAP/CCM should incorporate one (CWAP) / three (CCM) low current input discrete as defined in Section 2.2.1 for use in
remotely controlling CWAP/CCM transmitters. The CWAP/CCM’s transmitters should be

commanded to the “on” state only when the on/off control discrete input is in the grounded state. CWAP/CCM transmitters’ control should also be available from the remote control (see Section 17.9 for details).

The same capabilities should be available over the CWAP/CCM network interface using one of the protocols defined in Section 17-8.

17.7 FUNCTIONAL DESCRIPTION

17.7.1 Network Protocol Transparency

As a minimum, the CWAP/CCM should be compliant with the IEEE 802.11 standard.

IEEE 802.11 defines the Physical (PHY) and Media Access Control (MAC) portion of the data link layer of the ISO 7-layer protocol stack model. The Logical Link Control (LLC) portion of the data link layer is defined by IEEE 802.2.

Any network protocol that can interface with an IEEE 802.2 layer will operate over an IEEE 802.11 standard LAN. Virtually all network protocols are supported. Applications that use a wired network for inter-process communications or shared resource access will operate unmodified over a combination wired and wireless LAN. Compliance with IEEE 802.3x interface options should also be considered.

17.7.2 CWAP Cabin Roaming

The CWAP should support seamless connection while the clients are moving throughout the aircraft cabin.

Multiple CWAPs may be used to provide complete coverage on large aircraft, including double-deck aircraft. Coverage overlaps of the CWAPs should provide seamless coverage, allowing the clients the ability to roam about the aircraft without loosing connection.

17.7.3 Compliance to national regulations

All CWAP/CCM wireless communication should be compatible with the operational needs of airlines operating between airports located in different countries.

To support such operations, the CWAP/CCM should be capable of adapting the RF configuration (channel and power) to the local regulations of each country. This document does not specify these local regulations, which may include specific spectrum management (frequency utilization) as well as transmitting power control.
The CWAP/CCM is expected to comply with ~~both~~ the transmitted power limits defined by applicable standards (e.g. IEEE 802.11) as well as potentially more stringent requirements imposed by country specific regulations.

COMMENTARY

When an airplane is on the ground, the applicable regulations are those of the country the airplane is located in. When an airplane is in flight, in most cases, the applicable regulations are those of the country of registration of the airplane and in some situations the airplane’s country of overflight.

Special attention should be given when operating in the 5 GHz UNII band. When using this band, the recommendations of IEEE 802.11h should be followed, in particular, Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC).

When the CWAP/CCM operates in channels that require DFS/TPC, it should select a set of fallback frequencies, based on its geographic location, to be available in case the CWAP/CCM detects an event that forces it to switch to another frequency.

COMMENTARY

When operating in certain ranges of frequencies, variable by country, subject to radar signal exposure, the CWAP/CCM is required to switch channels (i.e., dynamically select another frequency, i.e., DFS, and control its transmit power, i.e., TPC) when it detects a radar signal.

The CWAP/CCM should be delivered with the required set of compliance certificates covering national safety and radio-frequency standards. These certificates should be available in English and in the native language of countries requiring it. Certificates are not required to be printed on the CWAP itself. However, the CWAP label should list, in English, the regulations with which the CWAP is compliant.

17.7.4 CWAP Inter-channel Interference

Inter-channel interference may exist when more than one CWAP is installed in the cabin.

COMMENTARY

When multiple CWAPs are operating in the 2.4 GHz band, special care should be given to the channel allocation of each CWAP as there are only three non-overlapping frequency channels available in this band. If more than three CWAPs are installed, suppliers and integrators are encouraged to verify that inter-channel interference is minimized or mitigated.

Potential ways to mitigate interferences include, but are not limited to, installation of overlapping channel CWAPs on different decks, separation of interfering CWAPs by RF power management or physical separation of overlapping cells.

~~17.7.5 IEEE 802.11ac, 802.11ax, 802.11n, and IEEE 802.11b/g Interference~~

~~When fitted with more than one radio, the CWAP/CCM should be capable of operating in IEEE 802.11ac, ax, and n mode only on one of its radios. That implies multiple external antenna connections to that radio are needed to support at least 2x2 MIMO while other radios could be linked to only one external antenna connection.~~

~~COMMENTARY~~

~~In order to get the full benefits of IEEE 802.11ac, ax, or n, it is necessary for all clients of a CWAP to operate in IEEE 802.11ac, ax, or n mode. If a CWAP is configured to support 802.11ac, ax, or n and IEEE 802.11b/g/a on the same radio then, the CWAP bandwidth performance will degrade if at least one client operates in IEEE 802.11b/g/a. One way to mitigate this is to restrict the CWAP~~

~~to operate in 802.11ac, ax, or n on one of its radios (IEEE 802.11b/g/a clients will not be able to connect) and operate in IEEE 802.11a/b/g on another radio. This, however, forces the CWAP to be fitted with two separate radios.~~

17.7.6 Virtual Service Communities (IEEE 802.11 operation)

CWAPs should be capable to create multiple Virtual Service Communities (VSC). Each VSC should have its own configuration setting making it a distinct entity with its own Service Set Identifier (SSID), user authentication, data rates controls, etc.

COMMENTARY

With multiple VSC, a single CWAP could support a larger variety of user class such as, for example, airline personnel, maintenance technicians, and passengers, all on separate dedicated virtual networks.

If the CWAP is fitted with more than one radio, the CWAP should support VSC spanning over multiple radios

COMMENTARY

For example, if a CWAP has two radios, it should be possible to host VSC1 on radio 1 and 2 and VSC2 on radio 1 only or any other combination.

17.7.7 Security (IEEE 802.11 operation)

When operating in IEEE 802.11 mode, the CWAP/CCM should support the following security features:

- Wireless network name: Assigning a unique name to a wireless network (e.g., SSID) enables connection of clients providing the correct network name. The CWAP/CCM should have the capability to not broadcast the network name for added privacy.
- Wi-Fi Protected Access (WPA3): WPA3 is an enhanced Wi-Fi security standard compared to legacy WPA2 and Wired Equivalent Privacy (WEP). The CWAP/CCM should support WPA2 (IEEE 802.11i).

COMMENTARY

Although the CWAP/CCM may support a wide variety of other security features, it is up to the airline customer to define the mode of operation of their wireless LAN. It may be beneficial in certain cases to not implement any of the protection described above and let users use their own security solutions such as VPN. Additional security measures may also be implemented in the host system which is outside the scope of this specification. Additional security guidance is available in US NIST documents SP800-48, *Guide to Securing Legacy IEEE 802.11 Wireless Networks* and SP800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*.

- Network interface – Access to the management interface should be password protected. Default manufacturer credentials should be changed prior to field deployment.

- Running Configuration – The CWAP/CCM should support saving the running configuration to non-volatile memory when commanded. The CWAP/CCM should initialize the running configuration from non-volatile memory at each power-up.
- Logging – The CWAP/CCM should have logging capability for security events, e.g., failed authentication.
- Packet filtering – The CWAP/CCM should be able to filter packets on the incoming wireless interface based on operator-defined rules.
- Address Resolution Protocol (ARP) spoofing – The CWAP/CCM should employ methods to prevent or detect ARP spoofing.
- Ad-hoc client to client communication – The CWAP/CCM should be able to block wireless clients from cross-communicating between one another over the CWAP/CCM Virtual Service Communities (VSCs).
- Rate Limiting – The CWAP/CCM should support rate limiting on a per-client basis.
- Segregation using Virtual LANs – The CWAP should be able to support segregation for wireless LAN access of crew or passenger services by VLANs based on the IEEE 802.1q standard.

COMMENTARY

VLANs based on IEEE 802.1q can be used for logical segregation standard. A different VLAN, other than the Crew or PAX network, should be used for the management of the CWAP. The different SSIDs (Crew and Passenger) can also be bridged to the different VLANs to secure the management of the CWAP.

- Maintenance operations – Software and configuration updates should only be possible over the CWAP/CCM's wired interfaces. Access to the management interfaces should be prohibited from the wireless interface. Software must only be writable while in Dataload mode.

- Situation Awareness – The CWAP/CCM should be able to detect rogue access points in its vicinity and report them via the security log.

COMMENTARY

The usually-accepted meaning of the term "rogue access point" describes an access point connected to a wired network and not controlled by the owner of this network. In the case of an airplane installation, the wired network is physically and procedurally protected and the installation of such rogue access point is considered unlikely, so the term "rogue access point" is used here to described an access point that is not connected to the airplane wired network but advertises itself as a CWAP/CCM.

ARINC Specification 822 provides more detailed information on securing wireless networks for aircraft-ground communications. Most of these recommendations also apply to the type of networks for which the CWAP is intended.

17.8 SOFTWARE AND CONFIGURATION LOADING AND CONFIGURATION CHECK

The CWAP/CCM should include the capability to remotely preposition its own software and configuration via the host system LAN.

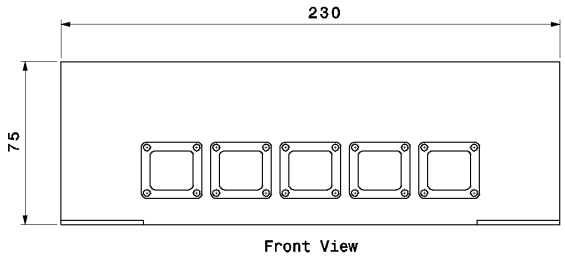
Consistent with this capability, the CWAP/CCM should be capable of reporting its current

firmware, software, and configuration on demand from the host system.

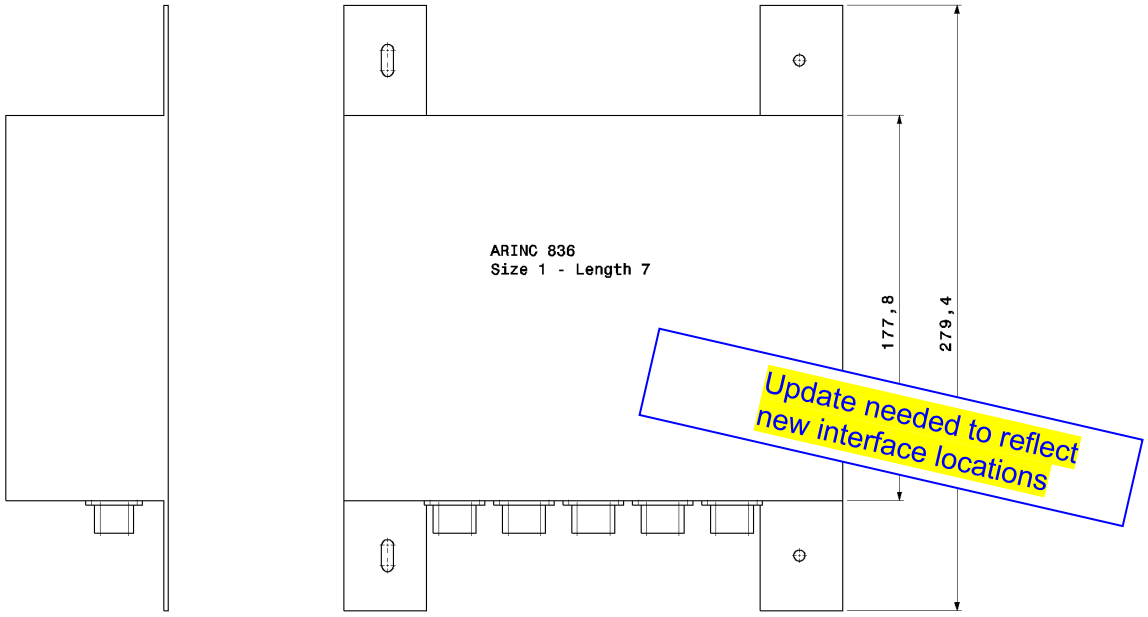
17.9 REMOTE CONTROL

In addition to Simple Network Management Protocol (SNMP), the CWAP/CCM should include the capability to be controlled remotely via a Command Line Interface (CLI) over its Ethernet wired interface. Secure protocols such as Secure Shell – RFC4250-56 (SSH) are recommended for such operation. Alternate means of control over Hypertext Transfer Protocol – IEEE RFC2616 (HTTP), potentially with Transport Layer Security – IEEE RFC5246 and 6176 (TLS) support, e.g., Simple Object Access Protocol (SOAP), are also possible.

ATTACHEMENT – CWAP/CCM OUTLINE DRAWING



Front View



Side View

Top View