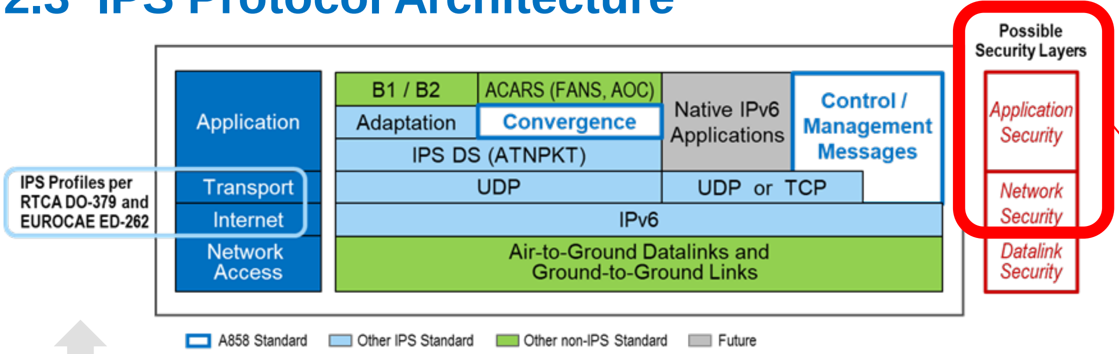
PP858 –
Section 2 & Section 5 Comment Disposition Discussion

21 April 2020

PP858 Section 2 Comment Disposition [#1, #2]

2.3 IPS Protocol Architecture



Possible Security Layers

Application Security

Network Security

Datalink Security

Application | B1 / B2 | ACARS (FANS, AOC) | Native IPv6 Applications | Control / Management Messages

Adaptation | Convergence

IPS DS (ATNPKT)

Transport | UDP | UDP or TCP

Internet | IPv6

Network Access | Air-to-Ground Datalinks and Ground-to-Ground Links

IPS Profiles per RTCA DO-379 and EUROCAE ED-262

□ A858 Standard 🟦 Other IPS Standard 🟩 Other non-IPS Standard ⬜ Future

***COMMENT*: Pre-M13 (Timo Warns) –** *Depending on the discussion on Section 2.3.2 below, the figure may need to be updated regarding the "Possible Security Layers" column.*

***COMMENT*: Pre-M13 (Timo Warns) –** *This section requires discussion by the working group. My understanding today is that we have DTLS for end-to-end security and datalink (radio-level) security, but no network security.*

Discussion

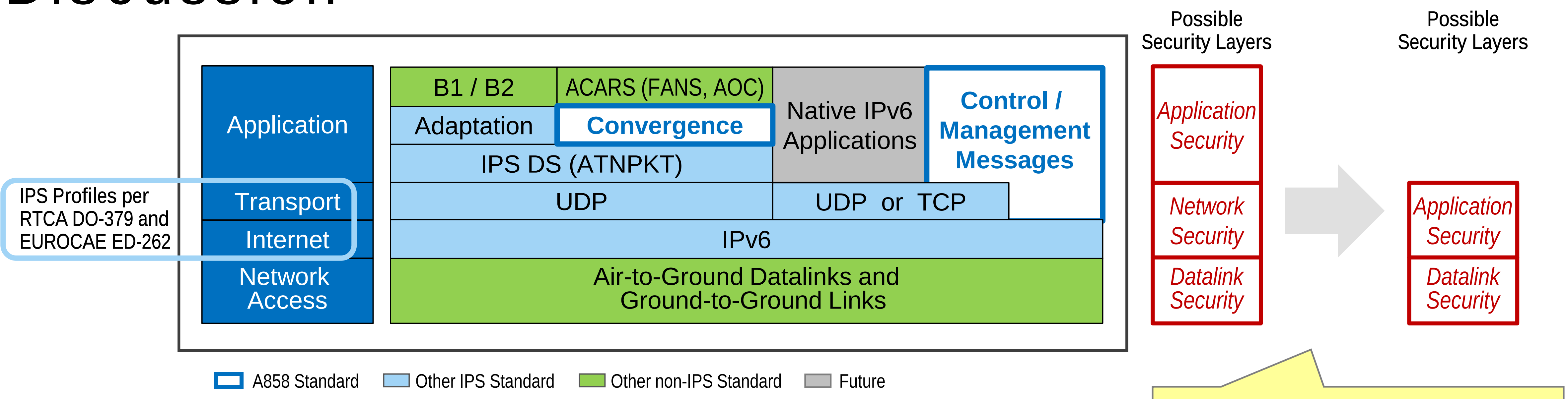
- (see next slide)

2.3.2 Security Layers

The IPS System envisages different layers of security, including:

- Application Security: Application layer security protects the data transmitted between the airborne applications and the ground applications. This is end-to-end security and is further described in Section 4.3.
- Network Security: Network security operated between hosts, which may be the hosts on which the applications are run or ground IPS Gateways if present for protocol conversion. It is important to note that in such cases the security is not end-to-end as the security endpoints are located somewhere in the network. This is described in Section 4.3.
- Datalink (i.e., radio-level) Security: Air-to-ground subnetwork security protects data over the air between the airborne radio and the CSP's ground access network. This layer protects data in flight over the radio channel and typically provides integrity protection. Security mechanisms provided here are under the control of the CSP and may vary between CSPs. As such they are not described further in this document. For ground-to-ground links, link layer security may be used, although it is possible that the physical protection surrounding these links is deemed sufficient.

Discussion



Application

Transport

Internet

Network Access

IPS Profiles per RTCA DO-379 and EUROCAE ED-262

B1 / B2

ACARS (FANS, AOC)

Adaptation

Convergence

IPS DS (ATNPKT)

Native IPv6 Applications

Control / Management Messages

UDP

UDP or TCP

IPv6

Air-to-Ground Datalinks and Ground-to-Ground Links

Possible Security Layers

Application Security

Network Security

Datalink Security

Possible Security Layers

Application Security

Datalink Security

▭ A858 Standard 🟦 Other IPS Standard 🟩 Other non-IPS Standard ▨ Future

"Application (end-to-end) security" and "datalink (radio-level) security" are consistent with terms used in Section 4.

2.3.2 Security Layers

The IPS System envisages different layers of security, including:

- Application Security: Application layer security protects the data transmitted between the airborne applications and the ground applications. This is end-to-end security and is further described in Section 4.3.
- Network Security: Network security operated between hosts, which may be the hosts on which the applications are run or ground IPS Gateways if present for protocol conversion. It is important to note that in such cases the security is not end-to-end as the security endpoints are located somewhere in the network. This is described in Section 4.3.
- Datalink (i.e., radio-level) Security: Air-to-ground subnetwork security protects data over the air between the airborne radio and the CSP's ground access network. This layer protects data in flight over the radio channel and typically provides integrity protection. Security mechanisms provided here are under the control of the CSP and may vary between CSPs. As such they are not described further in this document. For ground-to-ground links, link layer security may be used, although it is possible that the physical protection surrounding these links is deemed sufficient.

PP858 Section 5 Comment Disposition [#1]

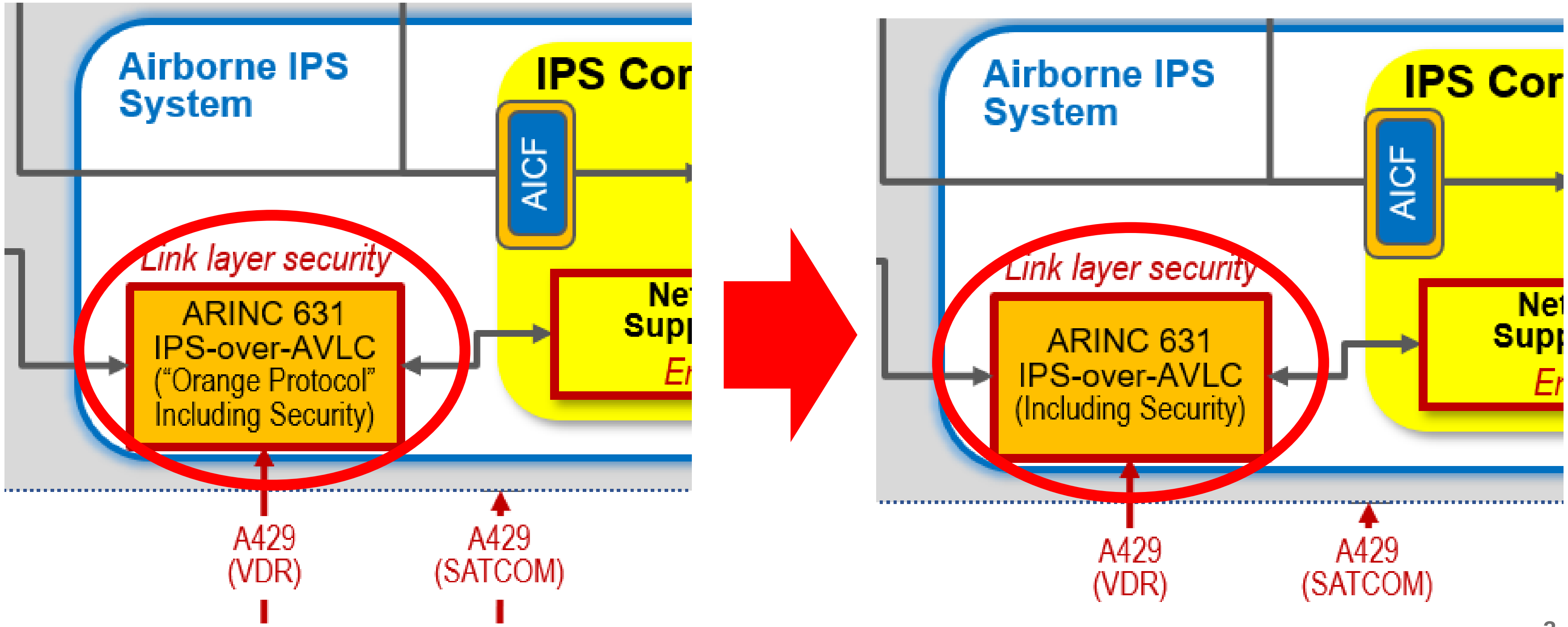
***COMMENT*: Pre-M13 (Fryd Wrobel-Airtel) –** *In Figures 5-1, 5-2, 5-3: Is "Orange Protocol including security" the official solution for IPS over VDLm2? If not, I suggest removing this phrase.*

Ed. Recommendation:

- Use generic term "IPS-over-AVLC" (i.e., similar to ACARS-over-AVLC) throughout document
- Remove specific references to Orange Protocol and Connectionless VDLm2 since those are details subject to further discussion in AEEC DLK.
  - That specific detail does not add technical value to 858, and using a generic term makes the document more future-proof.
- Update all Section 5 figures as shown to remove "Orange Protocol" reference
- Open action – need to revisit Section 3.4.2

Discussion

- …



PP858 Section 5 Comment Disposition [#2]

COMMENTARY

Publication of ARINC Specification 631-9, which includes the VDLM2-specific enhancements to support ATN/IPS, is expected in early 2023.

In addition to IPS, the subnetwork-level security measures may be leveraged by the legacy ACARS system to provide a first layer of protection for communications over the ACARS network.

<u>COMMENT</u>*: *M12 (Michal Skorepa) *– As noted in the commentary above, Is this required? It introduces additional changes compared to an approach where DTLS would be used only for the IPS traffic.*

Disposition Options

1. Remove the last sentence
2. Move the sentence into the commentary
3. Keep the last sentence but add some additional observations/guidance

Discussion

- …

PP858 Section 5 Comment Disposition [#3]

5.3.2.3 Air-Ground Datalink Security Considerations

***COMMENT*: Pre-M13 (Timo Warns) –** *This subsection may be moved to Section 4.*

Ed. Note - background:

- This material was originally in Section 4, but it was a “dangling” section without a clear linkage to the rest of Section 4.
- The material was moved to Section 5 (Implementation Guidance) since the text does not describe security mechanisms but rather the datalink security implementation options:
  - Secure the radio system itself,
  - Ensure that all of the radio traffic is protected by security measures hosted by the Airborne IPS System.

Ed. Recommendation: Keep as-is, rename to “**Air-Ground Datalink Security Implementation Considerations**”

Discussion

- …

PP858 Section 5 Comment Disposition [#4, #5]

5.3.4 Interface with Redundant Airborne IPS Systems [IF-6]

This interface is located between two Airborne IPS Systems to support the exchange of status and synchronization information between master and standby systems in a redundant configuration. While shown as a single interface in Figure 5-5, multiple physical ports may be necessary to achieve functional and performance requirements.

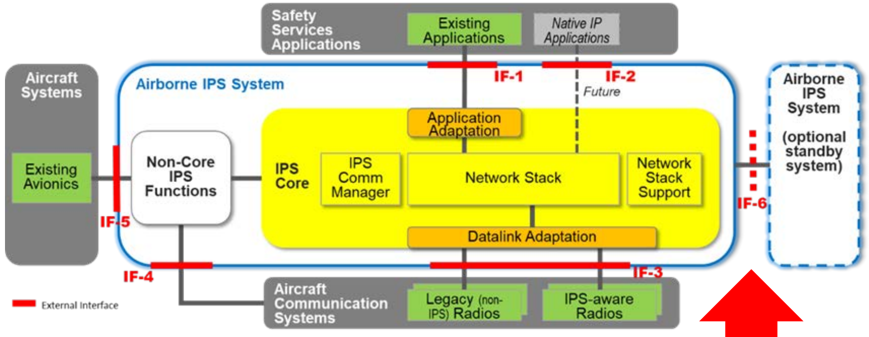


Figure 5-5

<u>COMMENT</u>: ***M12 (Michal Skorepa) –*** *I think this should be addressed from the point of view of IF-1, 2, 3, 4.*

<u>COMMENT</u>: ***Paul P. –*** *Madhu to expand section.*

Discussion

- …

PP858 Section 5 Comment Disposition [#6]

5.5 IPS Host versus IPS Router Considerations ← ***New section***

Section 3.0 comments regarding “multi-homed host versus router” to be addressed in Section 5.0 per Meeting 11 discussion.

Ed. Note - background:

- This section contains a collection of comments and observations dating back to Nov-2018 discussions regarding multi-homed IPS host vs. airborne IPS router. Note that this led to the decision to use the term “system” in Airborne IPS System.

Disposition Options

1. Remove the section
2. Keep the section – who would like to provide material??

Discussion

- …