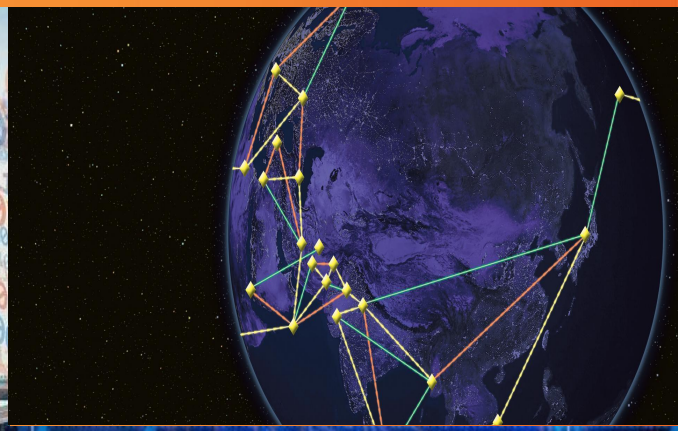


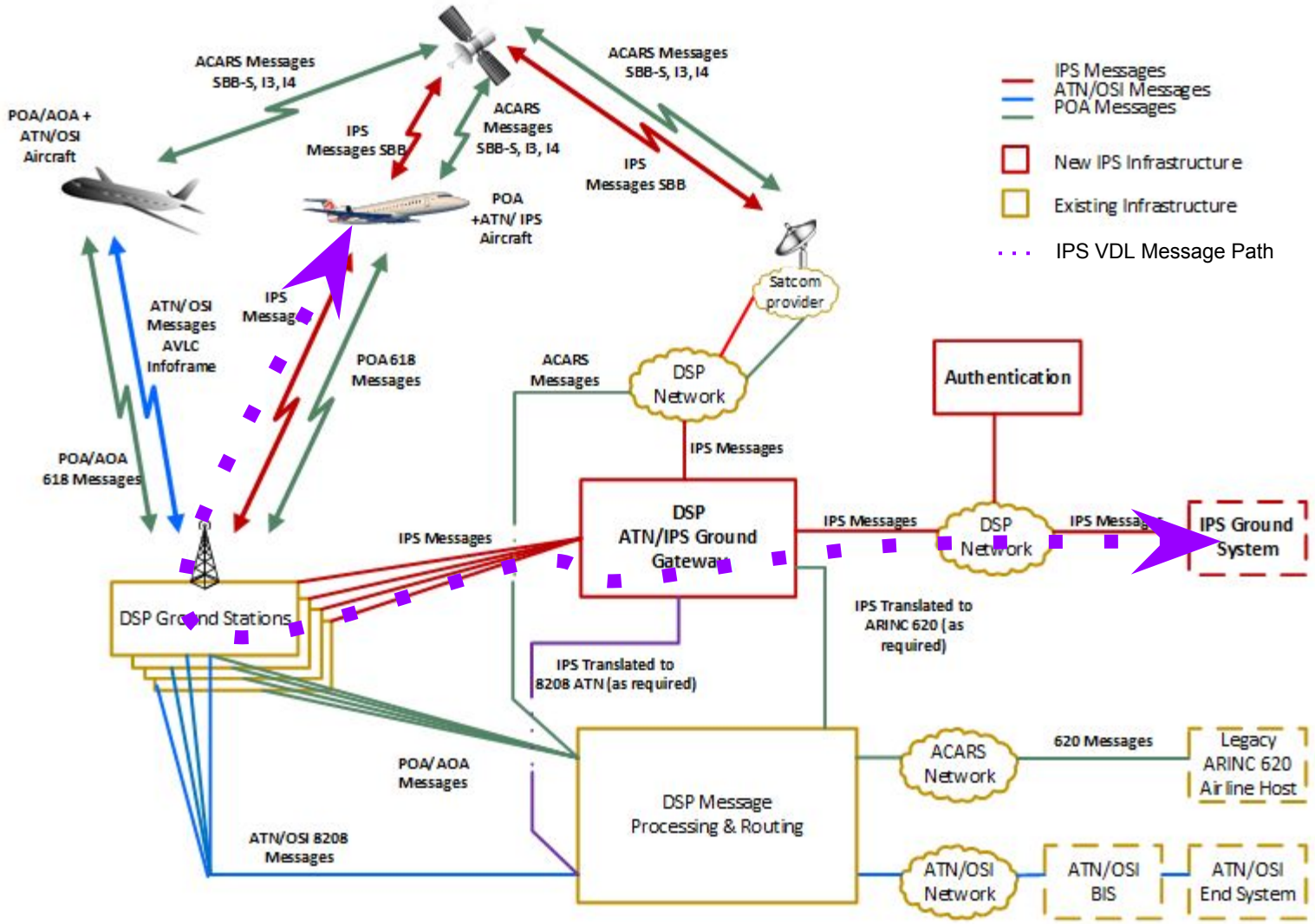
VDL IPS Security Consideration
AEEC IPS Sub-committee

Rockwell Collins
Building trust every day

Main Topic

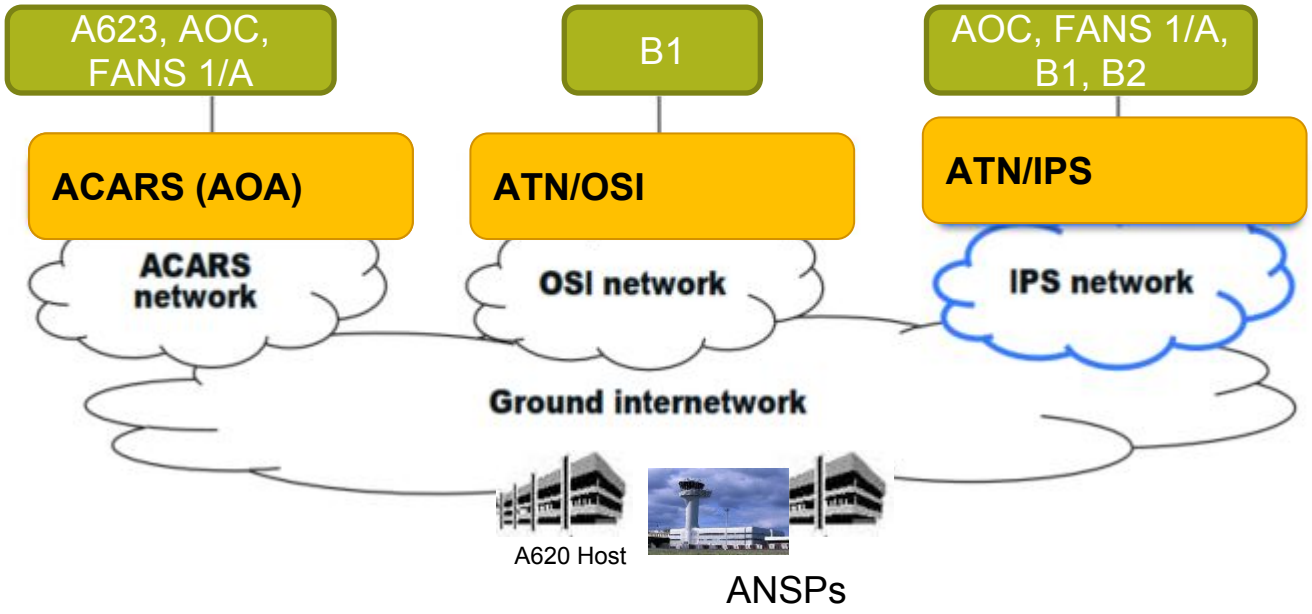
- VDL architecture and Security Considerations
- Securing the AVLC Layer for IPS
- Propose Security provision
- IPS Gateway
- Summary
- Q&A

IPS Message Path - VDL IPS Message Path



VDL and ATS, AOC and ATC applications Systems

- VDL supports ATC (FANS1/A, B1, B2) and AOC over AOA or ATN/OSI (Baseline 1 [Link2000+]), Baseline 2)
- ATN OSI, currently only B1 is deployed
- B2 may or may not be deployed over ATN/OSI



Current VDL Message Path (1/2)

FMS and other Aircraft Safety Critical System

ATC and ATS applications Systems

AOC Applications Systems

VDR

A429

CMU/ ATSU

Aircraft

Ground

Enhanced GSIF
w/ AOA, ATN, and IPS

Radio

GS

GS RTR
RTR

0x8E IPI for IPS
(AOA, 8208 ATN OSI)

8028 ATN
AVLC Handoff

AOA

OSI Msg Processor

BIS

ATN OSI ES

ATN/OSI Legacy

ACARS MSG Processor

MATIP

A620 Host

AOC and FANS 1/A legacy

AVLC XID, CMD and Info Frame

Current VDL Message Path (2/2)

FMS and other Aircraft Safety Critical System

ATC and ATS application Systems

AOC Applications

Aircraft Local Network

Protocol Bridge

ACARS ATN OSI Message Router

A429

VDR

Aircraft

Ground

Enhanced GSIF w/ AOA, ATN, and IPS

Radio

GS

GS RTR RTR

0x8E IPI for IPS (AOA, 8208 ATN OSI)

OSI MSG Processor

BIS

ATN OSI ES

ATN/OSI Legacy

8028 ATN AVLC Handoff

AOA

ACARS MSG Processor

MATIP

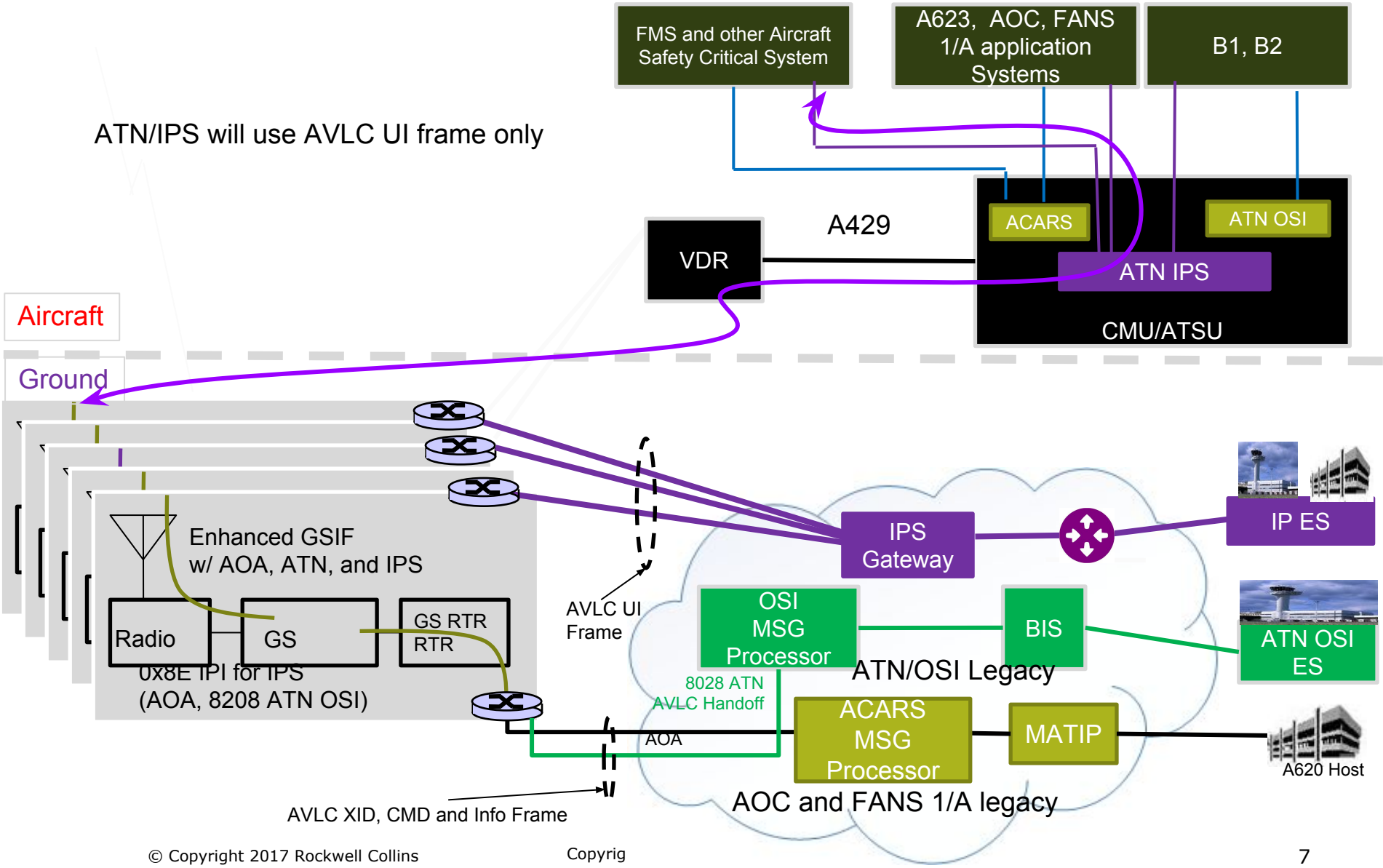
A620 Host

AOC and FANS 1/A legacy

AVLC XID, CMD and Info Frame

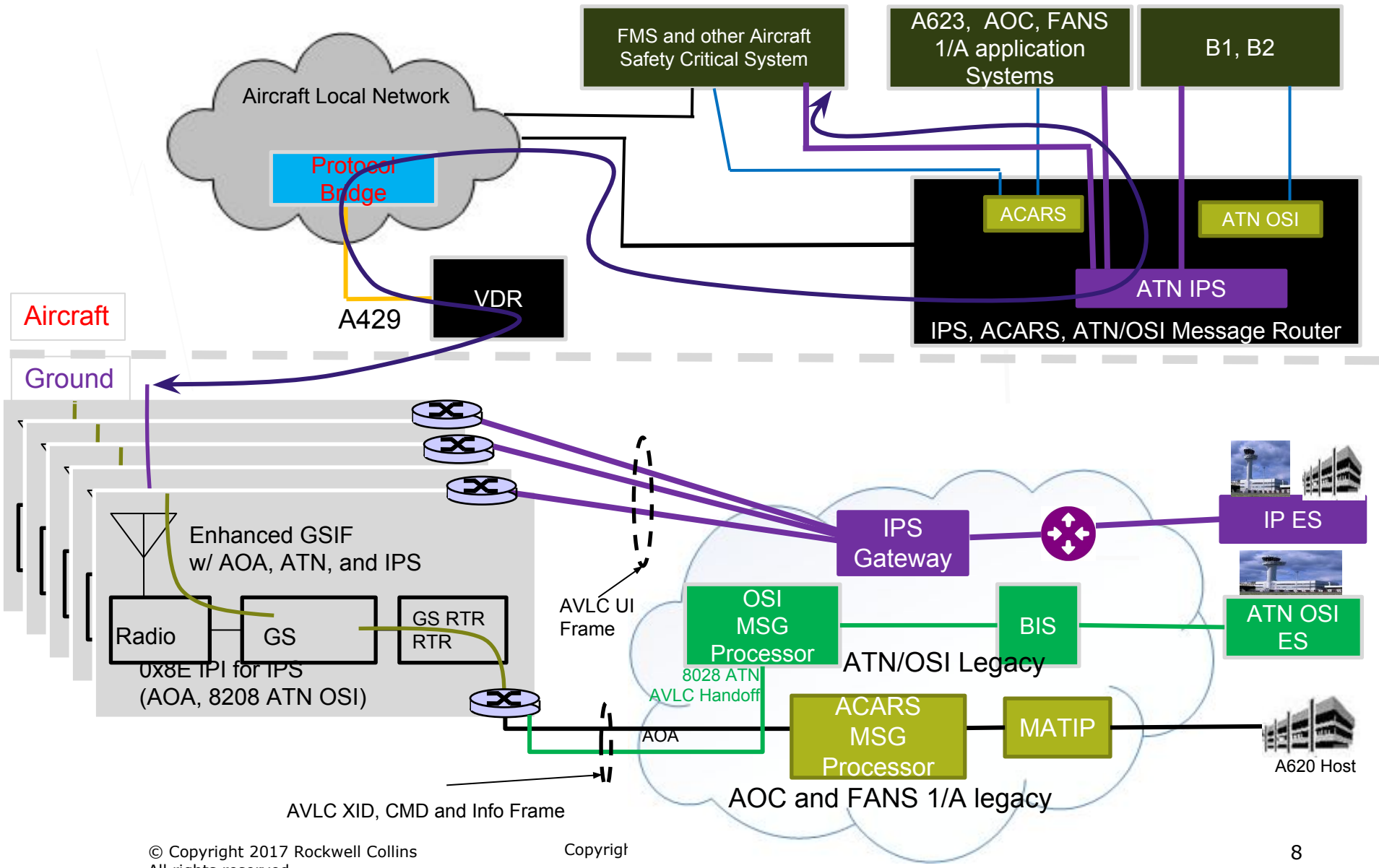
Message Transfer Process with ATN/IPS (1/2)

ATN/IPS will use AVLC UI frame only

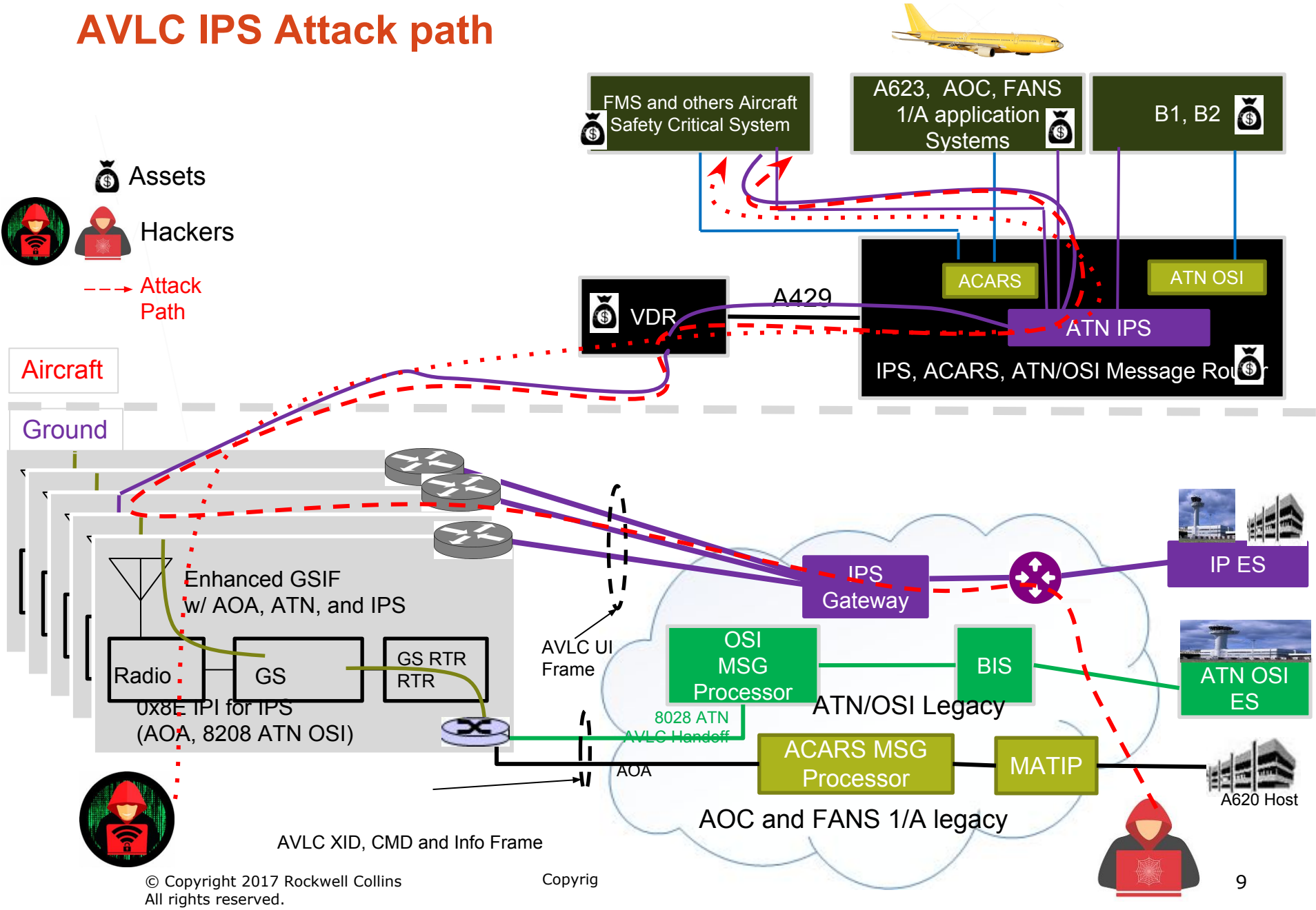


Copyrig

Message Transfer Process with ATN/ IPS (2/2)

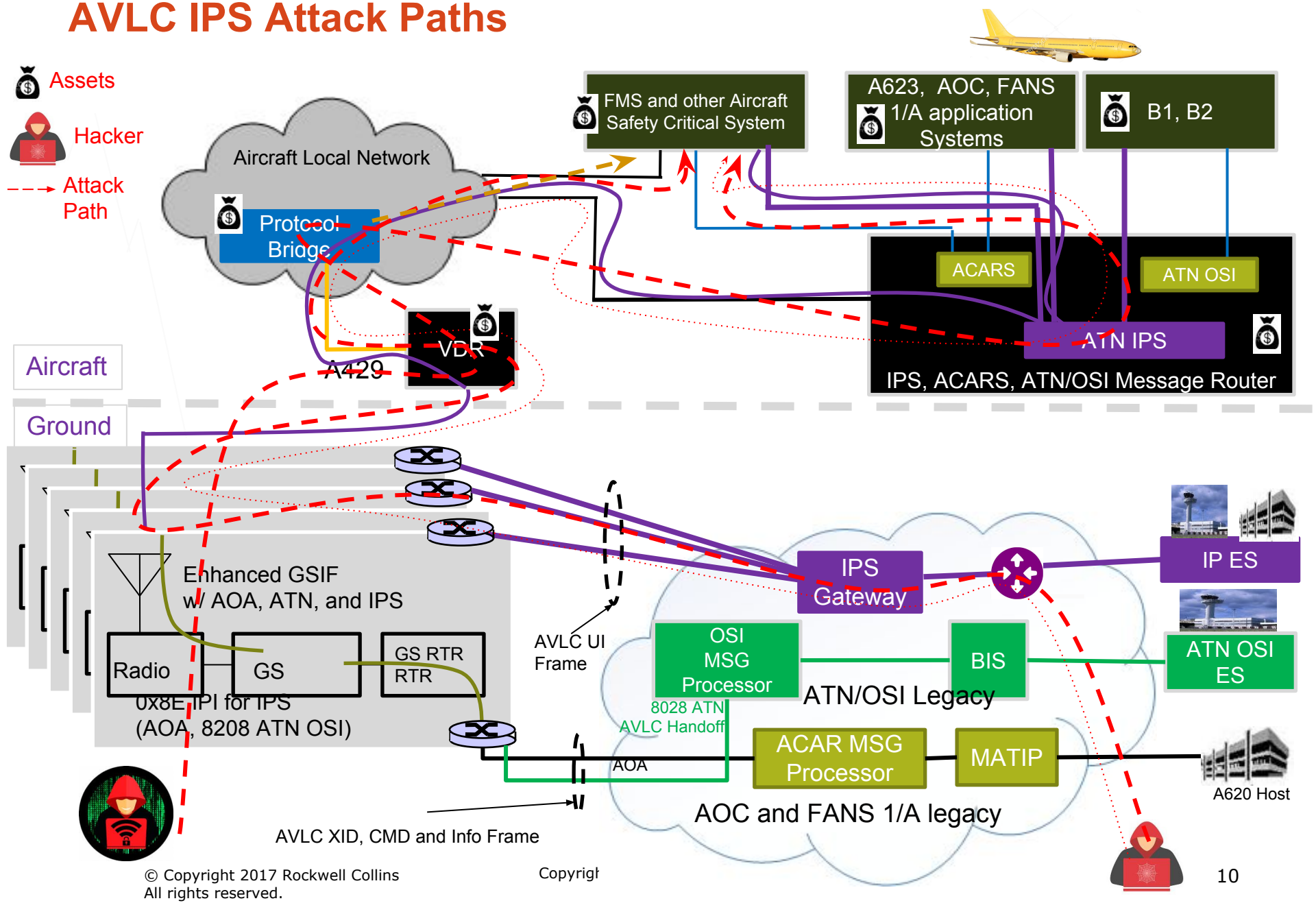


AVLC IPS Attack path



Copyrig

AVLC IPS Attack Paths



Attack Paths

- Based on the specific aircraft architecture one or more attack paths can be exploited by hackers with VDL access subnetwork
  - The potential VDL access subnetwork security related issues need to be resolved for IPS
  - Issue remains open for the ACARS and ATN/OSI and outside the scope of this presentation

Securing the AVLC Layer for IPS

- Access network (VDL) Security
  - We propose using Datagram Transport Layer Security (RFC 6347 DTLS 1.2) over AVLC to ensure mutual authentication and data integrity. Allowing customers to choose to encrypt the data as per their wishes in accordance with the jurisdiction having authority.
  - Each message is protected with message integrity code (MIC) which is derived from the 32bits of SHA384 Message Authentication Code
  - DTLS is used to establish the MIC write keys that will be used to validate the message source and message integrity
  - Implement DTLS with mandatory replay attack detection and logging
  - It supports SCVP server interface for efficient certificate path discovery and validation
  - Make solution independent from CA provider (which I know it is)

DTLS Provides

- Authentication of service provider to avionics
- Authentication of avionics to service provider
- Authentication independent of communications provider.
- Message Integrity Checks to verify the authenticity of messages
- Ability to allow higher layer encryption if desired
- Higher layer agnostic, ATN, ACARS, IPv6, UDP, TCP

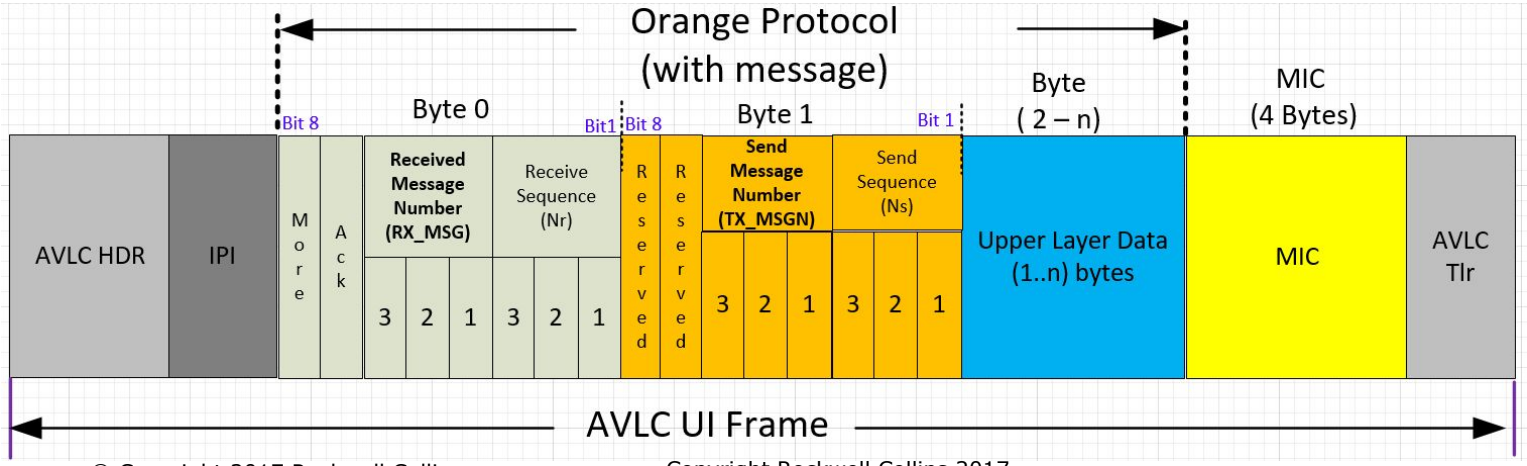
Authentication / Key Management

- ECDSA keys pairs will be provided by the primary service provider for each aircraft subscribed
- Keys will be signed by the primary service provider's own or designate's certificate authority (CA) key and be verifiable by any entity possessing the service provider's or designate's public key
- Each aircraft will receive a public key and a private key. The public key is used for authentication with the IPS Gateway(s) and the private key is kept secret with the aircraft
- To minimize the size of the public keys, suggest encoding in X.509 certificate DER format. The private keys are never transmitted
- Each service provider or designate will maintain a service key directory of X.509 certificates for all aircraft for which they are the primary service provider. Each primary service provider to maintain a valid public CA X.509 certificate in DER encoding with all other trusted companion service providers for which a trusted relationship is established
- Any key generated by the primary service provider that is later compromised, other than by expiration shall be listed in a certificate revocation list until the certificate expires. This list is to be shared no less than daily with all trusted companion service providers, even if no changes are recorded.

AVLC message with MIC

AVLC UI Frame with segmentation support

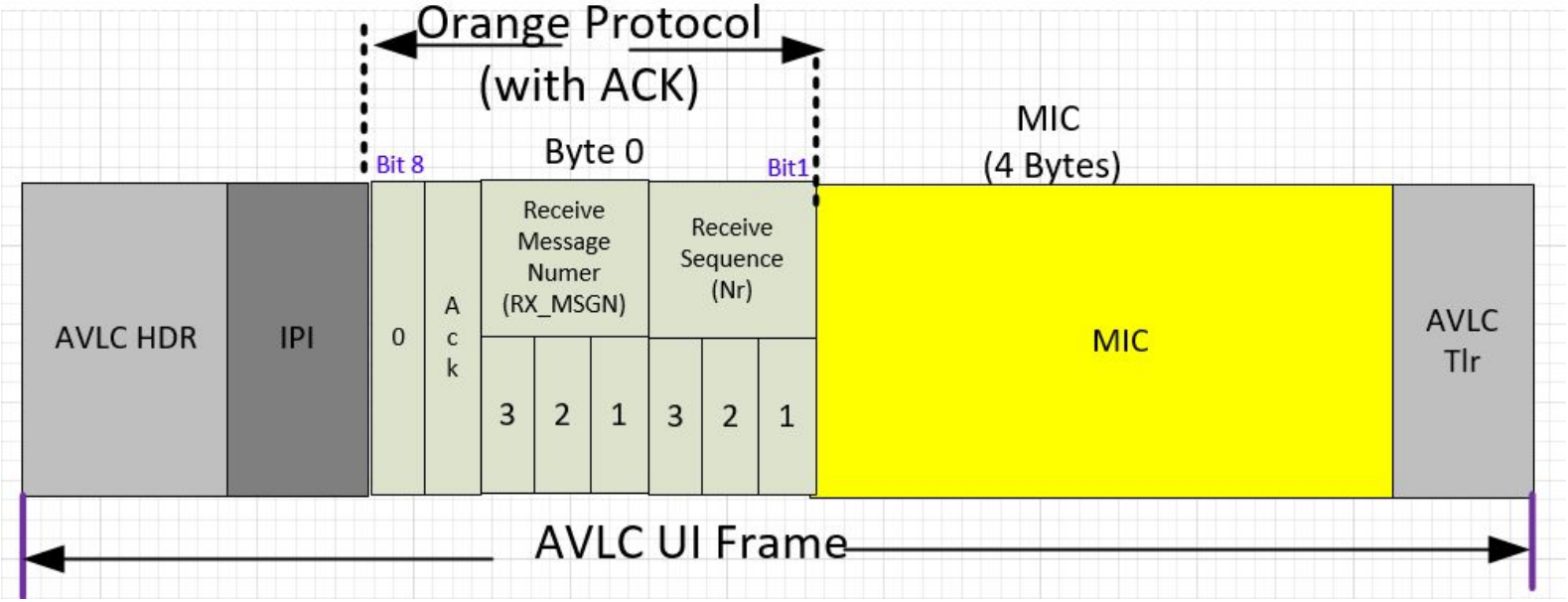
- IPS only use UI frame
- For downlink Source AVLC address contains the aircraft address and Destination address contains the any valid ground address of the target DSP.
- Layer 2 segmentation protocol is added to support RFC 8200 minimum MTU limit of 1280 octets
- Sequence Number: Segment sequence number of this segment
- When message is not segmented, message number shall set to zero (0)
- Each segmented message contains a unique message number, when the message is segmented the message number indicates each segment that belongs to the specific message. Message number is incremented from 1 to 7 for the segmented message. The lowest available message number should be used for segmented messages.
- MIC is calculated and authenticated for each frame after the mutual authentication is done. For the DTLS handshake MIC is not included.
- MIC includes AVLC header as well as last octet of user data
- Retransmit timer at orange protocol layer is 3 seconds, up to 3 attempts only for fragmented messages (non message 0) based on high water mark ACK.
- If no acks are received at Layer 2 then retransmission will be handled by upper layer(s)



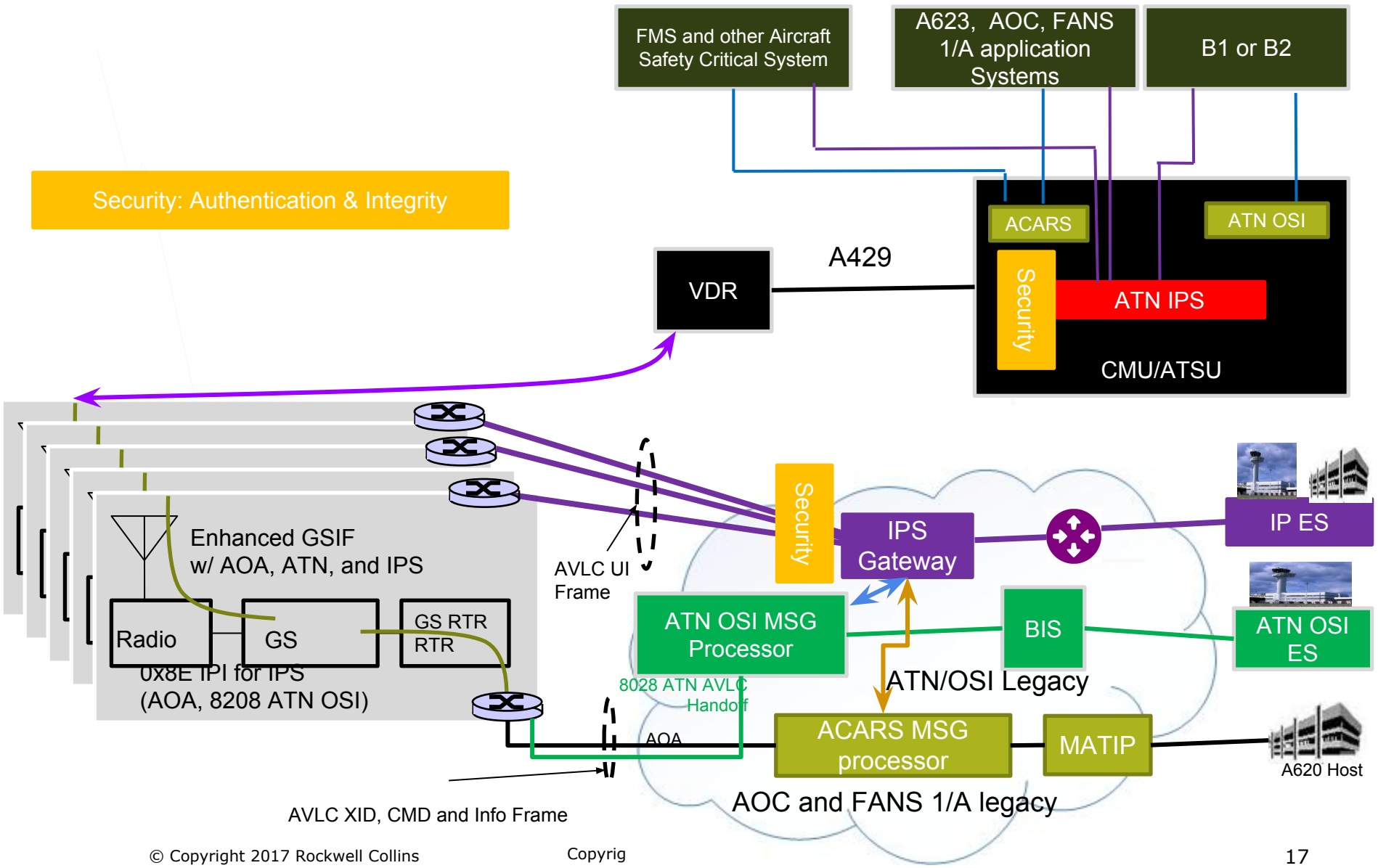
AVLC ACK message with MIC

AVLC UI Frame with segment Ack

- IPI = 0x8E
- ACK bit is set to 1
- Sequence number: Next expected segment (note if there is multiple segment and missed the first segment, sequence number is set to 0). ACKs are high water mark based
- Message number (RX_MSGN) this segment is ACKed for
- Ack is only sent for the segmented message (not message number 0)
- MIC cover AVLC UI frame header to the Message number
- For authentication DTLS handshake, MIC is not included

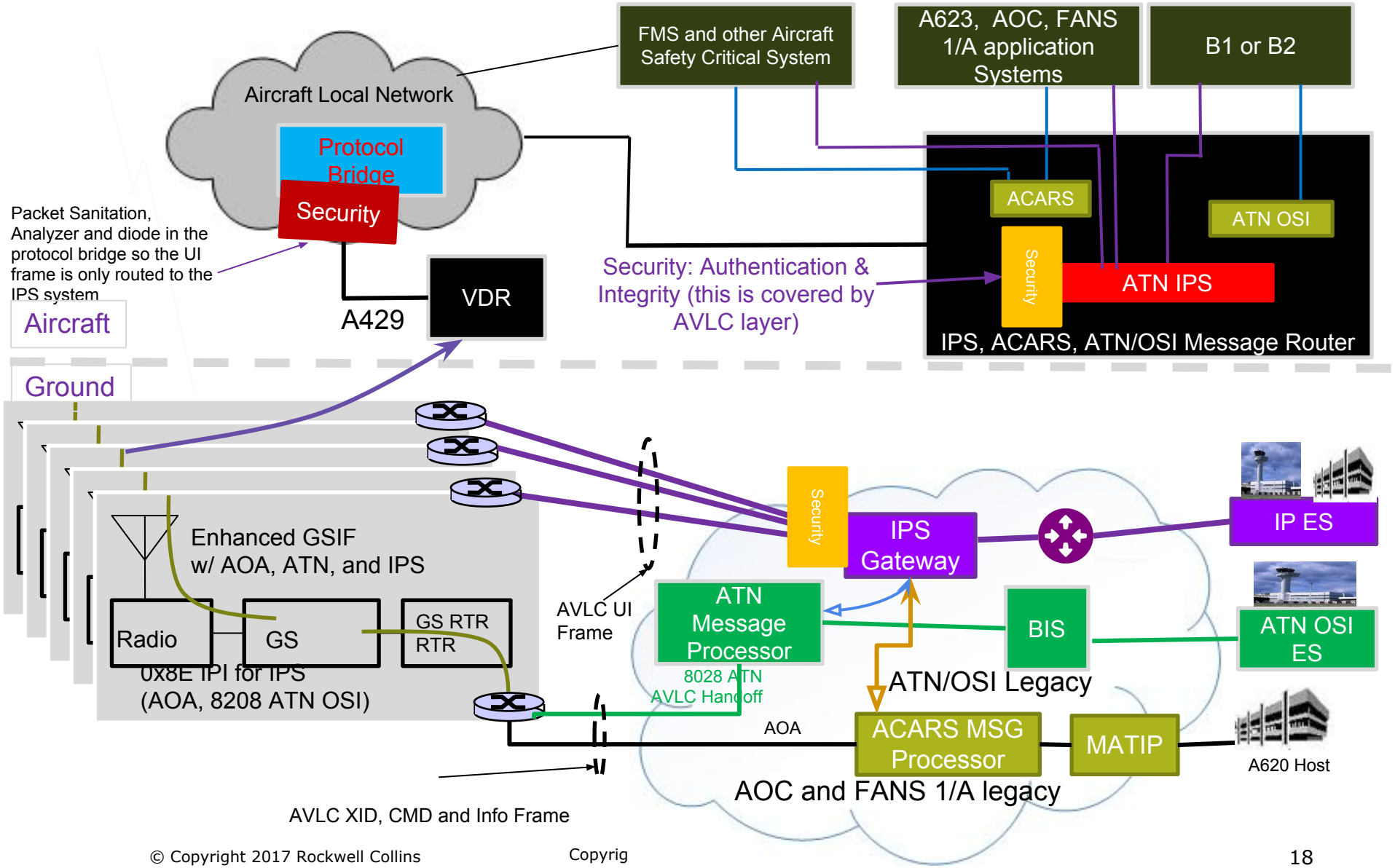


VDL Security Provision



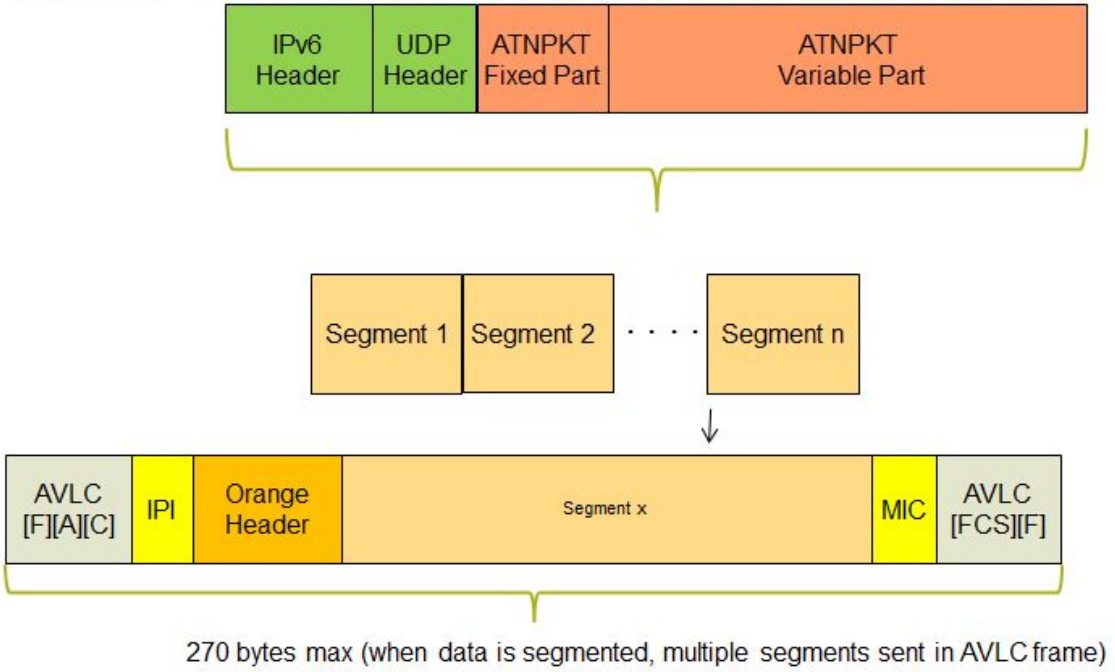
Copyrig

Message Transfer Process with IPS



Copyrig

VDL2 Link layer segmentation for IPS



The IPv6 packet (1280 bytes max) will be segmented as needed for VDL

The number of segments generated will depend on the size of the IPv6 packet and the maximum AVLC frame size (270 for IMS)
Each segments will be in a AVLC frame with the IPS IPI, the 'orange' protocol header and a MIC.

When the IPv6 packet is small, it will be contained in a single AVLC frame

Summary

- Existing and current ARINC AEEC spec indicates that VDL M2 radio will only be equipped with A429 connection to the aircraft systems
- IPS to be used only with AVLC UI frame
- Aircraft potentially could have two architecture for VDL Radio
- Attack path Depends on Aircraft specific architecture
- Proposed provision will mitigate RISK and protect the VDL access network
- FANS and AOC traffic should also be routed through the IPS over AVLC so that they can get same level of security

AEEC members to ask to provide comments feedback

Q & A