Options for Data Comm Security Roadmap

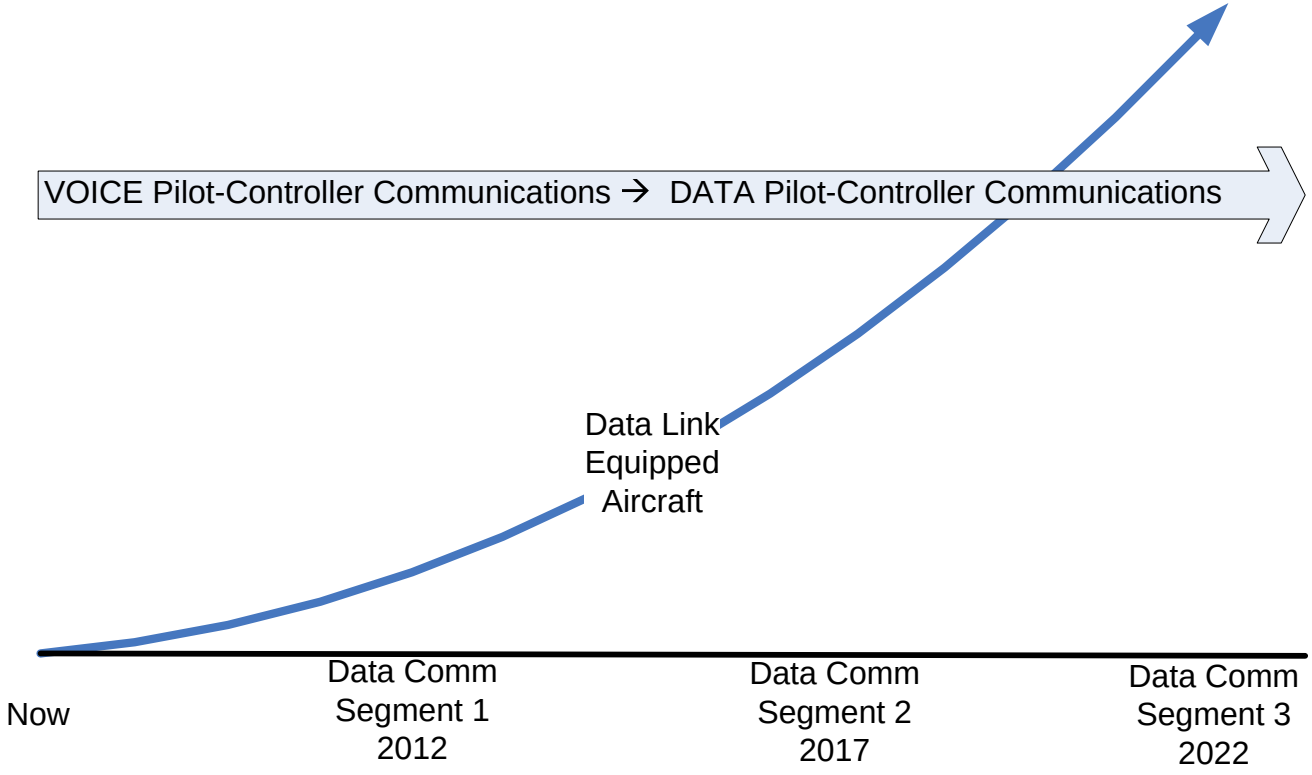
7th Integrated Communications, Navigation and Surveillance (ICNS) Conference
Herndon, VA, May 1-3, 2007

Tom McParland, BCI

Security Roadmap

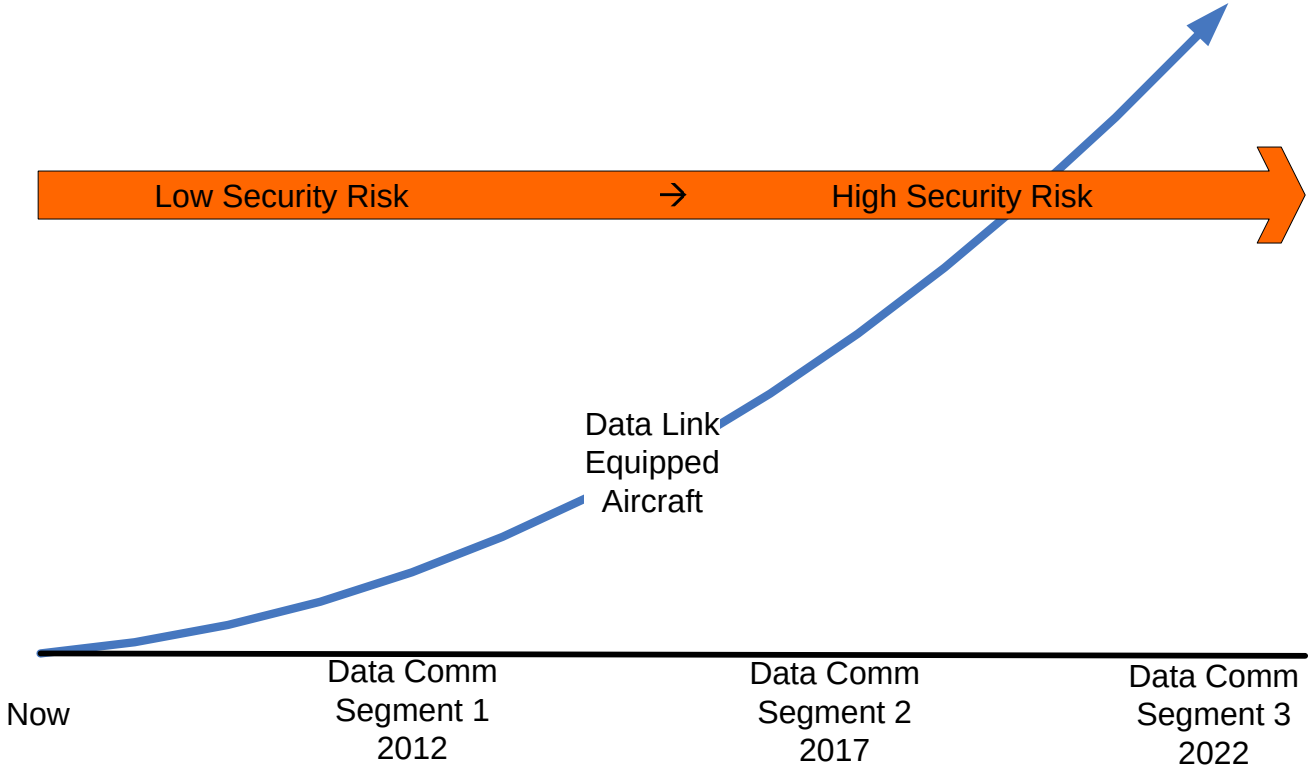
- The current Controller-Pilot Data Link Communications (CPDLC) systems are being implemented without security.
- As dependency on CPDLC increases, so does the need for security.
- A coordinated plan for the introduction of security is needed. This plan is the “Security Roadmap”

Transition from Voice to Data



In the future ATM environment it will no longer be possible to relay exclusively on voice messages for the exchange of information. Transition from voice for pilot-controller communications to a predominance of data communication has been identified as a key goal for Air Traffic Control. (Preliminary Program Requirements for Data com)

Security Risk will Increase



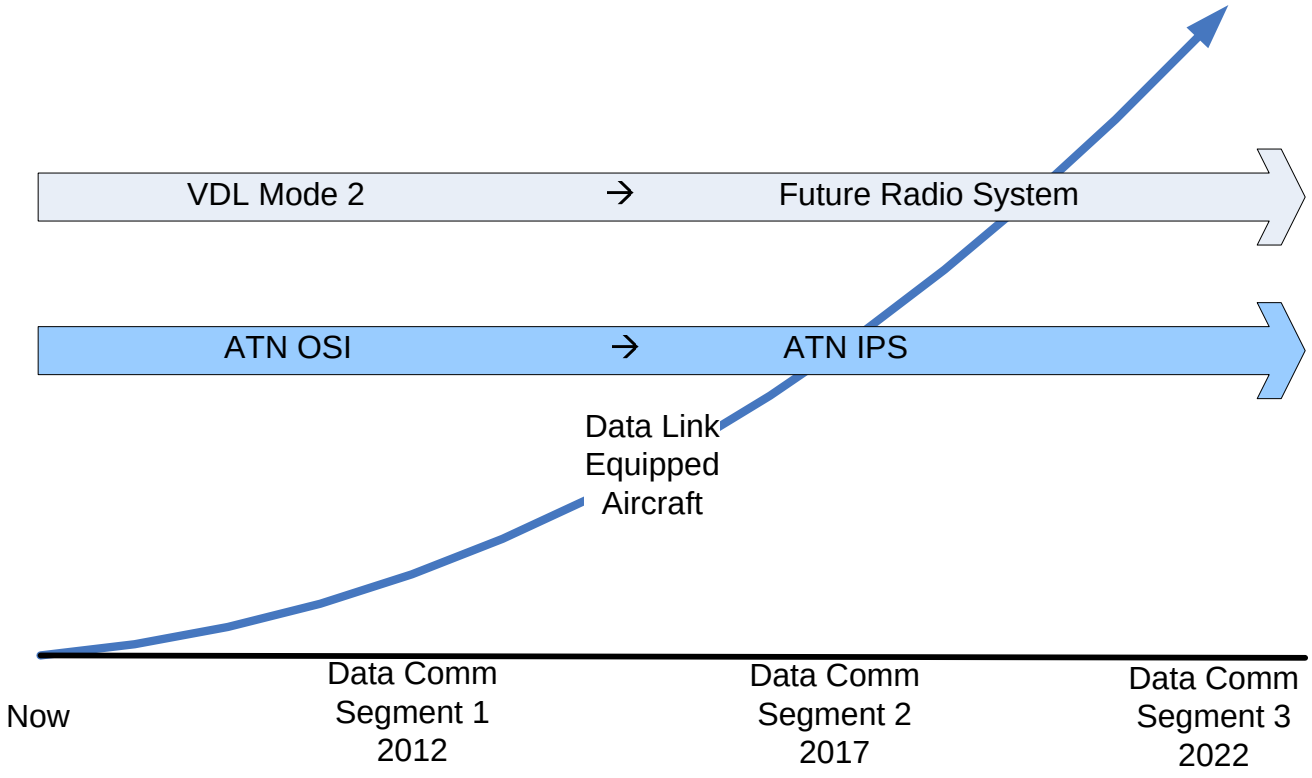
As usage and dependency on Data Comm increase so do security risks in terms of safety and economic impact.

In order to effectively deal with the increased risk a roadmap for the introduction of security is needed.

Security Roadmap Dependencies

- Availability of ATN Internet Protocol Suite (IPS) Mobility (TCP/IP for air-ground)
- IPS Mobility Applied to VDL-2 or Only Applied to FRS

Radio System and Protocol Suite Transition



Eventually the VDL Mode 2 radio system will be supplemented by a Future Radio System (FRS).

ICAO is developing Air-Ground SARPs and Technical Provisions for an Aeronautical Telecommunications Network based on the Internet Protocol Suite (ATN IPS).

Options for Cryptographic Protection of Messages

- ATN (Edition 3) Security implemented in the Upper Layer Communication Service (ULCS). **[ATN-CP-ULCS**].
- Direct invocation of the ATN Security Protocol as defined in the Edition 3 System Security Object. **[ATN-CP-SSO].**
  - When Protected-Mode Applications were developed, direct invocation of the SSO by the application or as a separate sub-layer (called the “security shim”) were considered
  - ACARS Message Security approach described in AEEC PP 823 invokes the SSO directly
- The IETF Authentication Header (AH) protocol or the Encapsulating Security Payload (ESP) protocol defined in the Internet Protocol Security (IPsec) could be used. **[IPsec]**.

Options for Key Establishment

- The currently specified (Edition 3) mechanism for key establishment performs this process during Context Management. **[ATN-KE-CM**].
- ATN Security Key Establishment could be performed independent of Context Management as a separate application or at application start. **[ATN-KE-nonCM].**
  - ATN Security Key Establishment with Pre-shared aircraft keys could be performed. The concept is to introduce ATN key establishment initially without a full PKI for aircraft keys
- AEEC DSEC has defined an option for key establishment with pre-shared aircraft and ground keys. **[AEEC-KE-Preshared**].
  - This option was introduced by Airbus in AEEC PP 823
- The method of key establishment planned for future use with IPsec is the Internet Key Exchange Protocol version 2. **[IKEv2].**

IPS Mobility Not Applied to VDL-2

- Cryptographic protection may be [ATN-CP-ULCS] or [ATN-CP-SSO].
- Key establishment may be [ATN-KE-CM] or [ATN-KE-nonCM].
  - Either may be applied using preshared aircraft keys.
- Alternatively the [AEEC-KE-Preshared] approach may be used at least for initial deployment.

IPS Mobility Applied to VDL-2

- The ATN security options for cryptographic protection of messages may be applied.
- IPsec may also be used

- The ATN or AEEC key establishment methods may be used.
- In principle, IKEv2 could also be used; however, it may not be practical due to VDL-2 bandwidth limitations.

IPS Mobility Only Applied to FRS

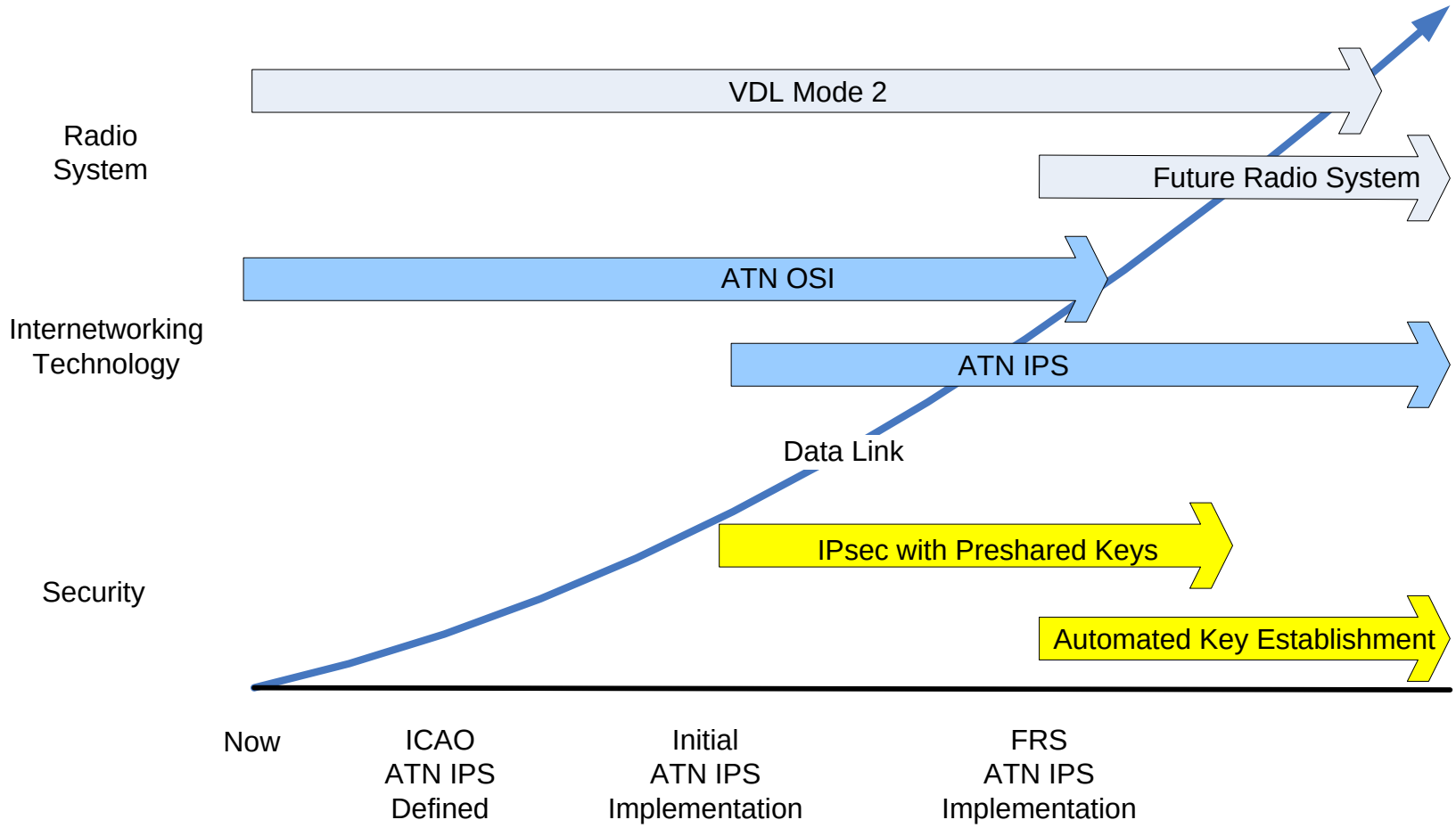
- If IPS Mobility is only applied to the FRS, then the ATN Security solution variants ([ATN-CP-ULCS] or [ATN-CP-SSO]) could be used, but [IPsec] could also be applied.

- Similarly, any of the ATN Security solution variants for key establishment could be applied, but [IKEv2], possibly with mobility extensions could also be used.

Considerations

- It is desirable to have one security solution
  - At a minimum use the same cryptographic techniques
- VDL-2 will likely be in use even when the FRS is available
  - VDL-2 will eventually need to be secured
- A PKI-based key establishment solution is perceived to be a significant undertaking

An Example Security Roadmap



An Example Security Roadmap

- Add IPS mobility to VDL-2
  - Due to its similarity to IDRP, BGP may be a leading candidate for an IPS mobility solution
- Use **[IPsec]** for cryptographic protection of messages
  - Use same cryptography as ACARS message security,
    - Derived from Edition 3 ATN security solution
- Start with Preshared Aircraft and Ground Keys **[AEEC-KE-Preshared]** and evolve to Automated Key Establishment such as **[ATN-KE-nonCM]**

- Adopt additional mobility solution(s) for FRS
  - A possible candidate is an enhanced version of the IETF Network Mobility (NEMO) approach
- Use **[IPsec]** for cryptographic protection of messages
- Use Automated Key Establishment such as **[ATN-KE-nonCM]** or **[IKEv2]**