Formal Methods for Trustworthy Skies: Building Confidence in the Security of Aircraft Assets Distribution

Scott Lintelman, Richard Robinson,
Mingyan Li, Krishna Sampigethaya

Trusted Systems and Software,
Boeing Phantom Works

Outline

- **High assurance for e-distribution of airplane assets**
- **Challenges to using FM for this problem**
- **Our solution approach**
- **Our experiences with using FM**
- **Open problems**

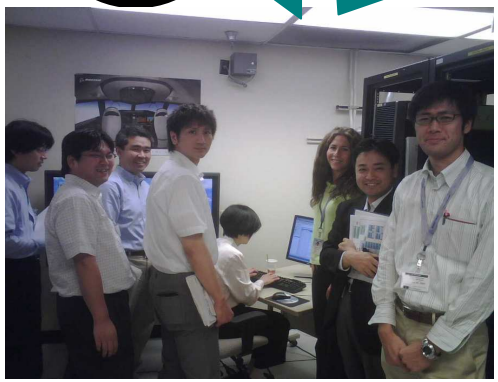
Airplane Assets Distribution System (AADS)

Airframe Manufacturer

Operational Airplane

Shared Networks

Software Suppliers



Airlines

➡ : AADS

Goal : end-to-end integrity & authenticity assured software/data distribution over shared networks

High confidence in AADS required

FM in AADS Development & Assessment: Major Challenges

- **Lack of regulatory guidance for supporting FM application**
  - **Regulations for software development at supplier will use FM**
    - **in DO-178C standard**
  - **No well-established guidance for ground systems connecting to airplane**
- **Inconsistent security requirements for FM application**
  - **Multiple stakeholders**
- **Cost constraints for FM application**
  - **System level evaluation can incur high evaluation cost**
  - **Component level evaluation can levy system maintenance effort**
- **Difficulties with FM integration in design and development**
  - **A dearth of user-friendly tools**
  - **Limited FM expertise**
- **Tradeoff between full formalization and strategic, selective FM**

FM in AADS Development and Assessment: Our Approach

Lack of regulatory guidance → **Assessment: Common Criteria Methodology**
- **Framework for threats, requirements, mitigation**

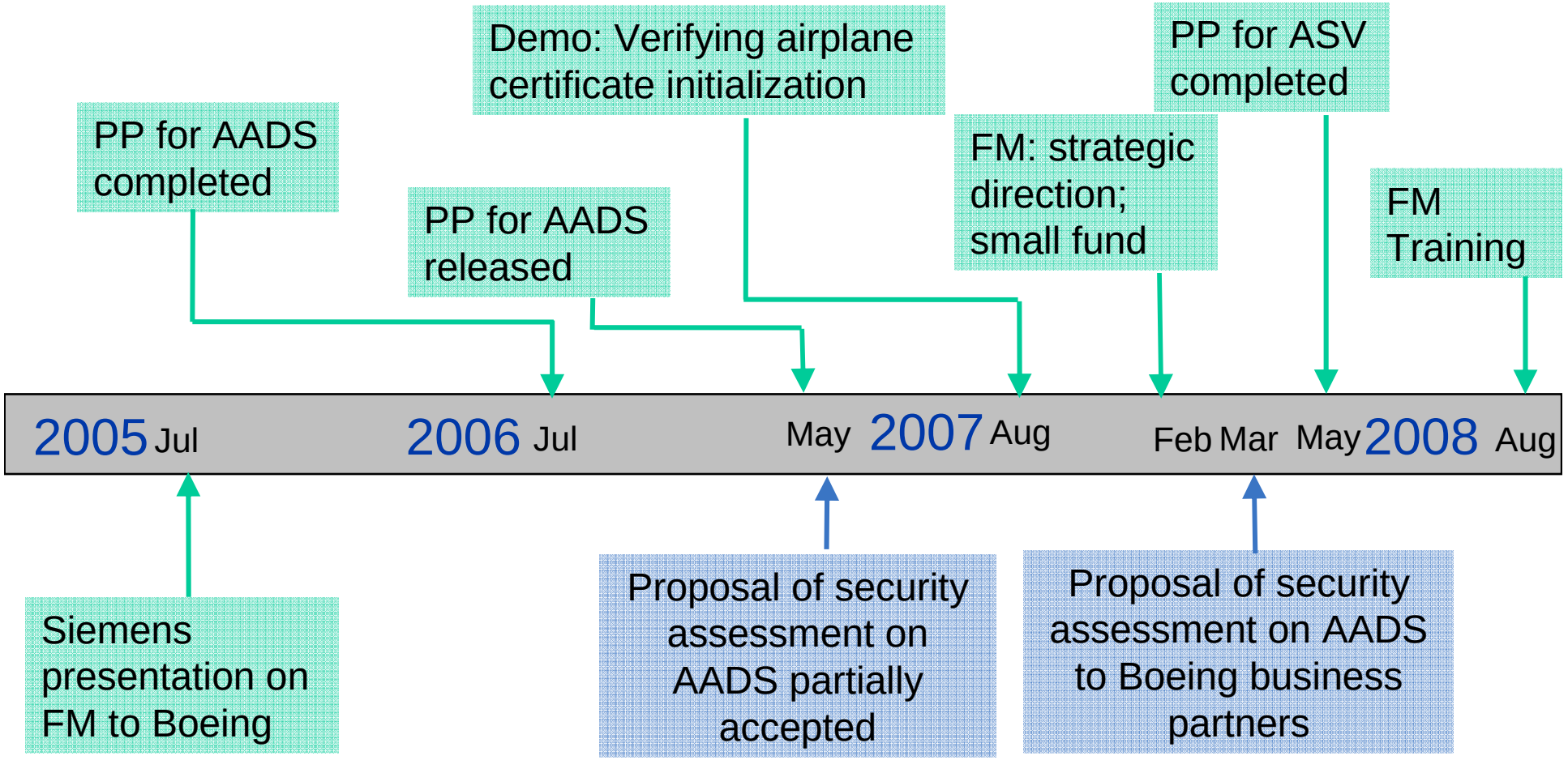
Inconsistent security requirements → **Protection profile (PP) for AADS**
- **Interview and feedback on PP**

AADS cost constraints → **FM evaluation of core component (Safecomp08 paper, PP for Asset Signer Verifier (ASV) module)**

FM integration with design/development → **OPEN problem: a user-friendly modeling and analysis tool**

Tradeoff between full formalization and strategic FM → **Application of FM in most beneficial scenarios in AADS**

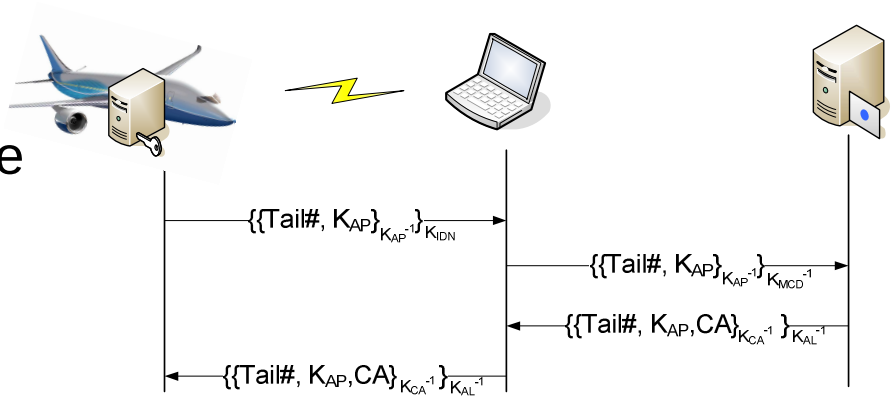
Our FM Experience and Activities

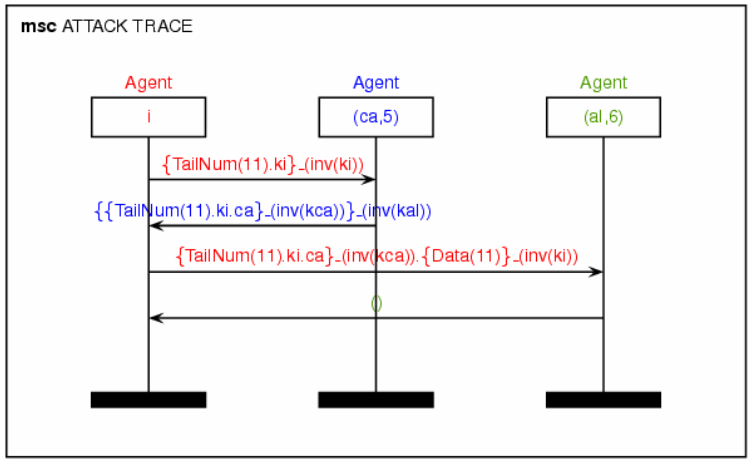


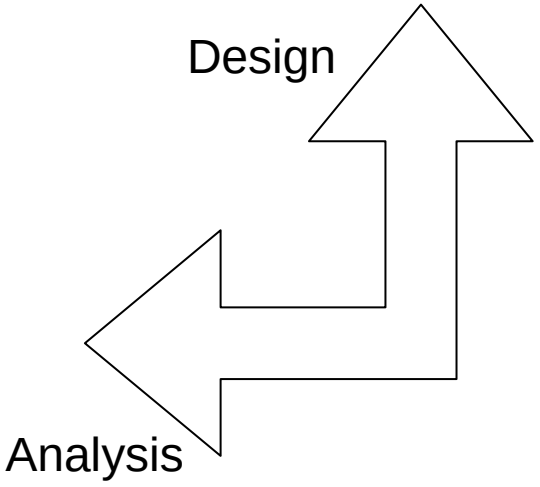
ASV: asset signing and verification module

Case Study: Demonstrating FM Utility, Efficacy

- Opportunity to share methodology with diverse stakeholders
- Goal: Guarantee authentic airplane identity
- Formal protocol analysis elicits required protocol features
- Analysis dictates specific design and implementation requirements

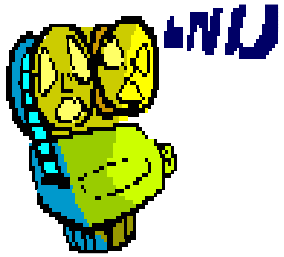






Open Problems

- **Visual representation of FM**
  - **with transparent analysis to demo FM benefits**
- **Accessible formal specification language**
  - **to software developers, customers**
- **Automated FM analysis and modeling tools**
- **Balance between full formalization and cost constraints**



Questions?

scott.a.lintelman@boeing.com
richard.v.robinson@boeing.com