# Aviation Cyber-Physical System Security and Resilience: Challenges and Opportunities

**Krishna Sampigethaya, Ph.D., FRAeS**

*Chair and Professor,*

*Department of Cyber Intelligence and Security,*

*Embry-Riddle Aeronautical University, Prescott, AZ, USA*

# Outline

- Classifying security concerns for CNS-ATM
- Assessing and mitigating security risks
- Coverage and gaps in current state
- Future research directions to address the gaps

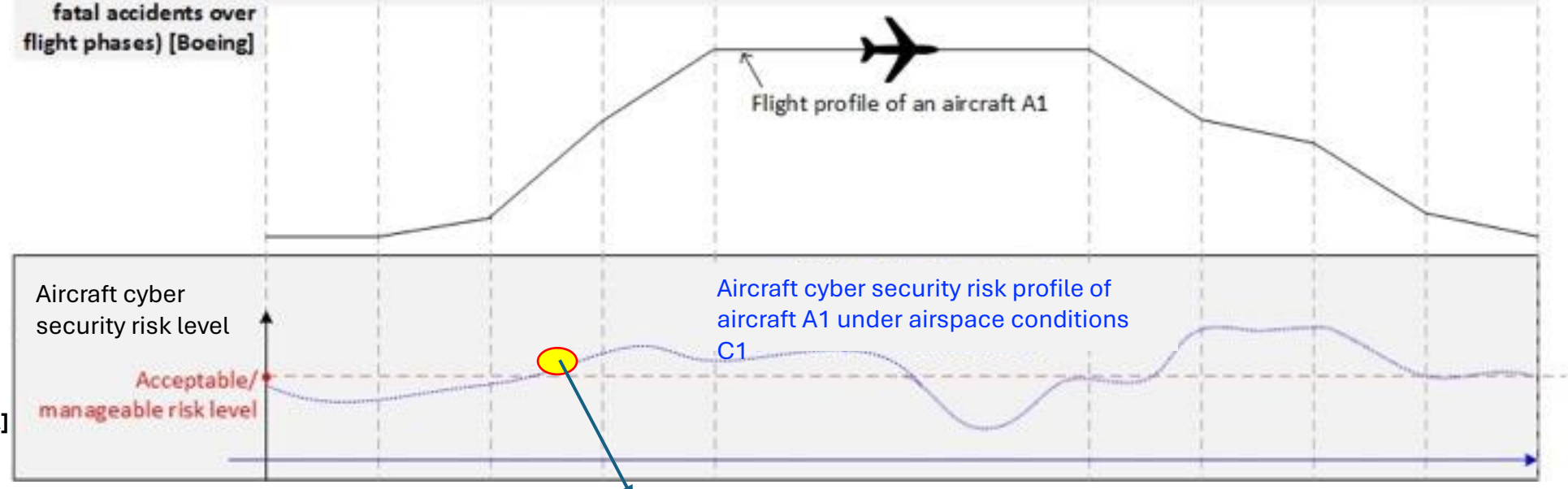
# An Expanding CNS-ATM Threat Surface

**Attacked Asset**

| Attack Type | Physical (P) | Cyber (C) |
|---|---|---|
| Physical (P) | **PHYSICAL THREATS**<br>• e.g., crew error, sabotage of facilities | NEW! **CYBER-PHYSICAL THREATS**<br>• e.g., CNS-ATM data disruption by radio signal jamming |
| Cyber (C) | NEW! **CYBER-PHYSICAL THREATS**<br>• e.g., pilot/controller distracted by spoofed CNS-ATM message | **CYBER THREATS**<br>• e.g., SWIM data, software, or network compromise, malware, and DoS |

# Aviation Cyber-Physical Security Risk Assessment

| Flight Phase | Parked, Tow, Taxi | Takeoff | Initial Climb | Climb | Enroute | Descent | Initial Approach | Final Approach | Landing |
|---|---|---|---|---|---|---|---|---|---|
| Avionics Systems | ACARS, ADS-B, GPS, .... | ACARS, ADS-B, GPS, .... | ACARS, ADS-B, GPS, .... | ACARS, ADS-B, GPS, .... | ACARS, ADS-B, GPS, TCAS, SATCOM .... | ACARS, ADS-B, GPS, .... | ACARS, ADS-B, GPS, .... | ACARS, ADS-B, GPS, .... | ACARS, ADS-B, ILS, GPS, .... |
| Aircraft System Information | weight, balance, position reports, weather reposts, engine data, ..... | | | | | | | | |
| Pilot Workload | | | | | | | | | |
| Safety Statistics (e.g., distribution of fatal accidents over flight phases) [Boeing] | 10% | 7% | 6% | 7% | 13% | 3% | 8% | 24% | 24% |

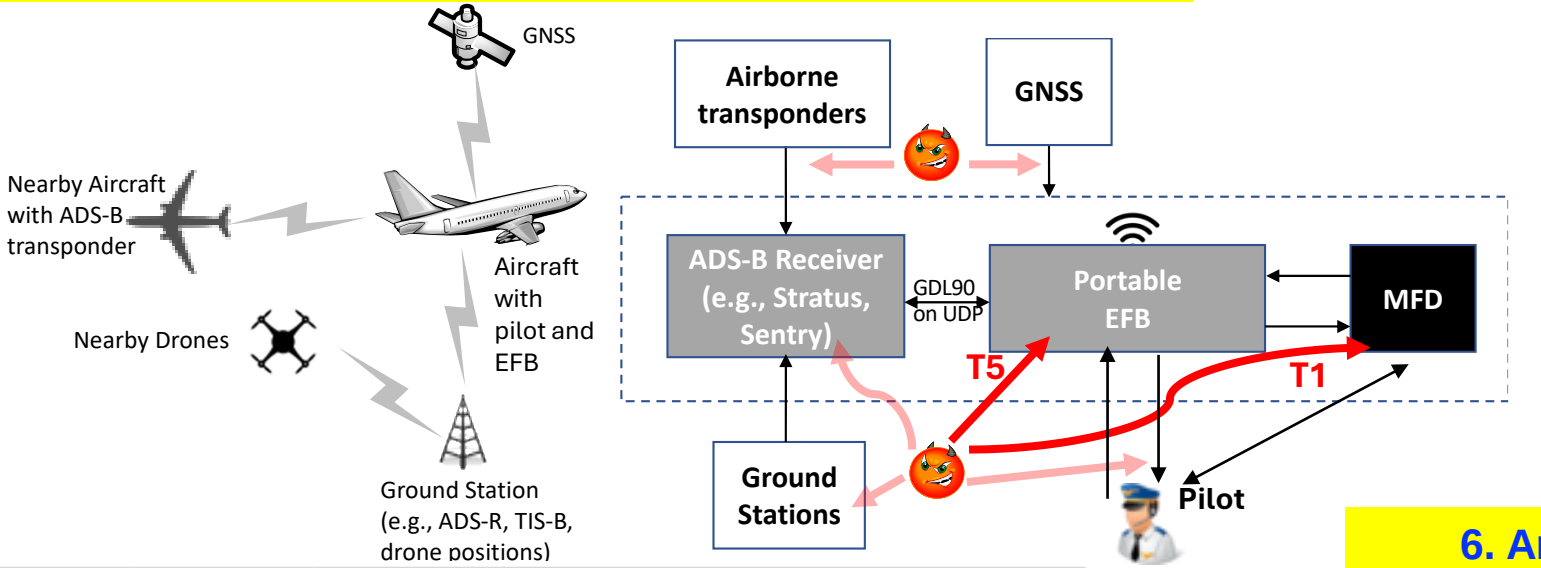



[Sampigethaya, AIAA]

**If security risk is unacceptable, mitigate it!**

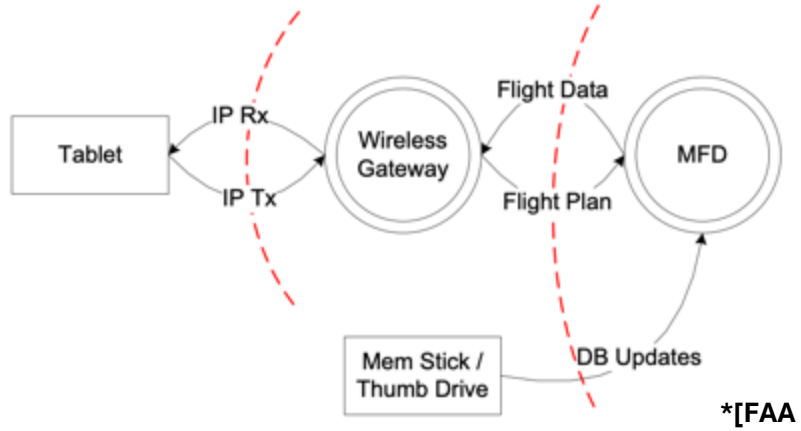
# Best Practice to Assess and Mitigate Risks: EFB Case Study

## 1, 2. Identify Assets and Draw Architecture Diagram




| Asset ID | Name | A,I,C | Description |
|---|---|---|---|
| 1 | MFD | A, I | The MFD is used for primary instrumentation and considered critical to aircraft operation. |
| 2 | EFB | A, I | EFB is used for minor safety apps |

## 3. Draw Data Flow Diagram




*[FAA ASISP]

## 4, 5. Identify and Document Threats

| Threat ID | Source | Asset | A,I,C Property | Description |
|---|---|---|---|---|
| 1 | USB | MFD | A, I | An USB drive hosting malicious software is inserted into the USB port of the MFD. |
| 5 | WiFi | EFB | A | Malicious packet injection |

## 6. Analyze and Rate Threats on a Risk Matrix

| Level of Threat | No Safety Effect | Minor | Major | Hazardous | Catastrophic |
|---|---|---|---|---|---|
| Very High | Acceptable | Acceptable | Unacceptable | Unacceptable | Unacceptable |
| High | Acceptable | Acceptable | Unacceptable | Not acceptable | Unacceptable |
| Moderate | Acceptable | Acceptable | Acceptable | Unacceptable | Unacceptable |
| Low | Acceptable | Acceptable | Acceptable | Acceptable | Unacceptable |
| Extremely Low | Acceptable | Acceptable | Acceptable | Acceptable | Acceptable* |

T5 MITIGATION T1 MITIGATION

Severity of the Threat Condition Effect

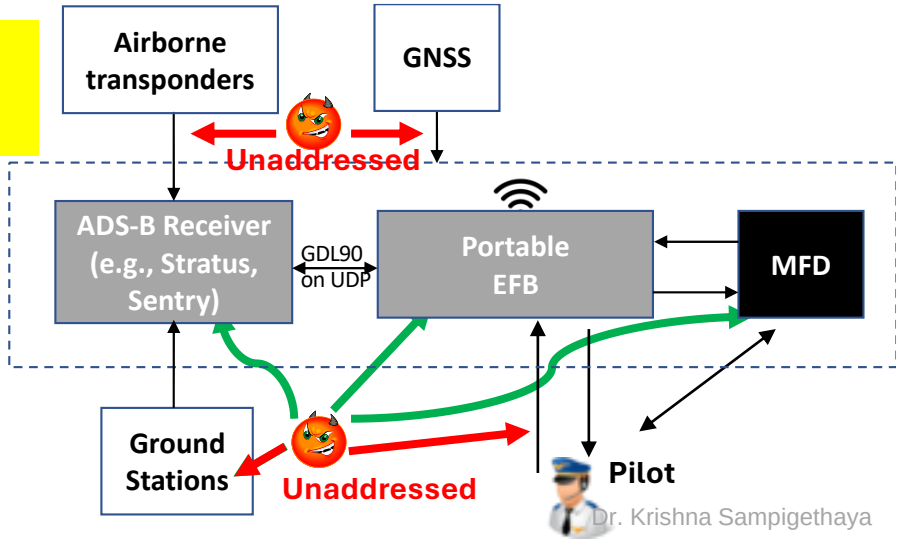
[RTCA SC-216 DO-356A], [Sampigethaya, RSAC]

# Coverage and Gaps in Best Practice

| Organization | Standard(s) | Aircraft | ATC/ATM Ground System | Aircraft CNS-ATM Dependency | Airline/Airport Information System | Cyber Threat Focus | Cyber-Physical Threat Focus |
|---|---|---|---|---|---|---|---|
| RTCA | DO-326A, 355A, 356A, 391, 392, 393 | x | x | | x | x | |
| EUROCAE | ED-201A-205A, 206 | x | x | | | x | |
| ARINC | 811, 823, 830, 835, 842,… | x | x | | x | x | |
| NIST | SP 800-30/37/39/53/160, CSF…. | | | | x | x | |
| ISO | 27000-27006, 27032,.. | | | | x | x | |

[Sampigethaya, AIAA]

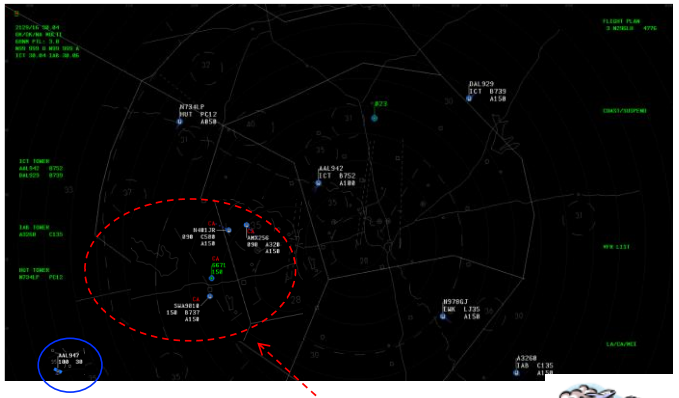
**In the context of the example system**

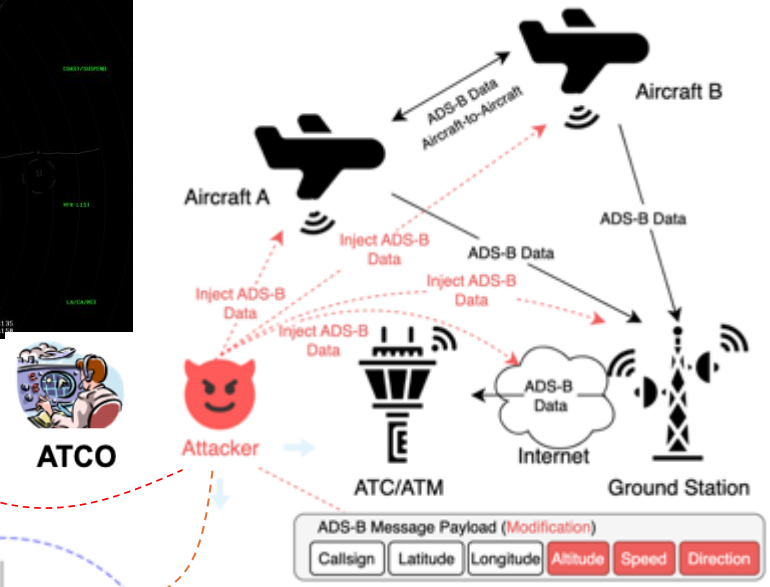



Major Gaps

1. **CNS-ATM security**
2. **Cyber-physical threats**

# CNS-ATM Cyber-Physical Security Considerations: ADS-B



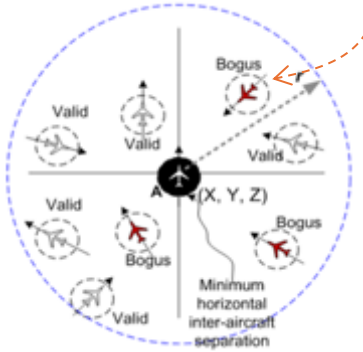





ATCO

Present false scenario to ATCO

PILOT




| | Industry focus | Threat mitigations |
|---|---|---|
| **ADS-B Applications**<br>**Security Property** | **Ground Surveillance** | **Airborne Surveillance** |
| **Integrity and Authenticity** | **Ranging, multilateration, surveillance data fusion, encryption, keyed hash** | **Signal-based/Group navigation (proposed)** |
| **Availability** | **Surveillance radars, APNT** | **Signal-based/Group navigation (proposed)** |
| **Flight Privacy/ Airspace Security** | **Symmetric encryption; LADD, PIA**<br>**Location tracking mitigation (proposed)** | **Location tracking mitigation (proposed)** |
| **Cyber-Physical Resilience** | **Crew readiness and aids (proposed)** | **Crew readiness and aids (proposed)** |

**Need innovative, practical cyber-physical security solutions for CNS-ATM**