

An aerial photograph of a university campus. In the foreground, there are several large, modern buildings with dark roofs and glass facades, interspersed with green lawns and trees. A large, multi-story parking lot is visible. In the middle ground, a wide, calm lake reflects the sky and the surrounding landscape. The background features rolling green hills and several prominent, rounded mountains under a clear blue sky. The overall scene is bright and sunny.

# 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

Physical (P)

Cyber (C)

Physical (P)



### PHYSICAL THREATS

- e.g., crew error, sabotage of facilities



### CYBER-PHYSICAL THREATS

- e.g., CNS-ATM data disruption by radio signal jamming



### CYBER-PHYSICAL THREATS

- e.g., pilot/controller distracted by spoofed CNS-ATM message

### CYBER THREATS

- e.g., SWIM data, software, or network compromise, malware, and DoS

Dozens of aircraft VANISH from air-traffic control radars sparking HACKING fears

DOZENS of aircraft VANISHED from Europe's skies in the past month, sparking fears of air-traffic control hacking attacks.

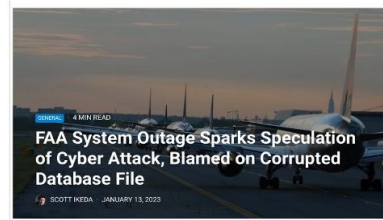
By GREG HEFFNER  
1936, Ft. Lee 13, 2014



After Alaska Airlines planes bump runway, a scramble to 'pull the plug'

Feb. 17, 2023 at 7:59 pm | Updated Feb. 20, 2023 at 3:59 pm

CPO MAGAZINE HOME NEWS INSIGHTS RESOURCES



Increasing Fake GPS Signals Near Iran Prompt FAA Alert

Ops Group has tracked at least 20 such spoofing incidents



By KERRY LYNCH | Editor, Air Investing Magazine  
November 28, 2023

What happened to GPS in Denver?

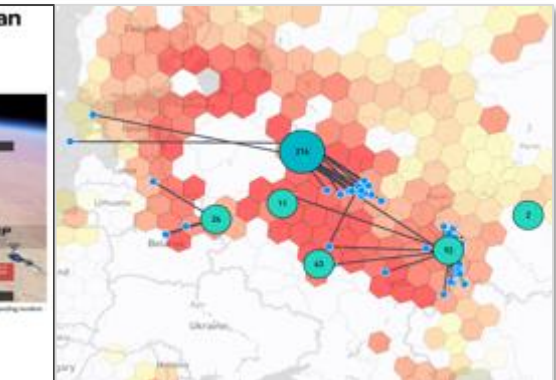
September 21, 2022 - By Dana Goward Est. reading time: 3 minutes

FAA Warns Airline Pilots as GPS Signals Disrupted Around Dallas - Bloomberg

by Editor | Oct 18, 2022 | Blog

NASA report: Passenger aircraft nearly crashes due GPS disruption

July 8, 2019 - By Dana Goward Est. reading time: 1 minute



# Aviation Cyber-Physical Security Risk Assessment

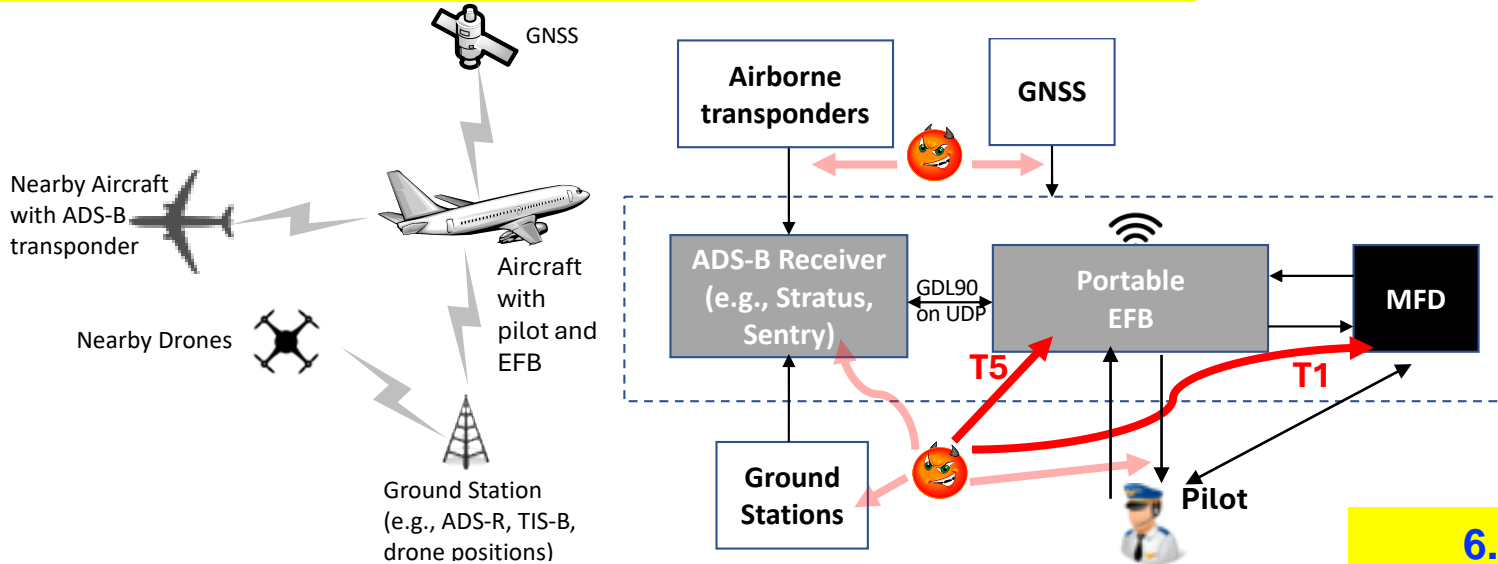


**If security risk is unacceptable, mitigate it!**

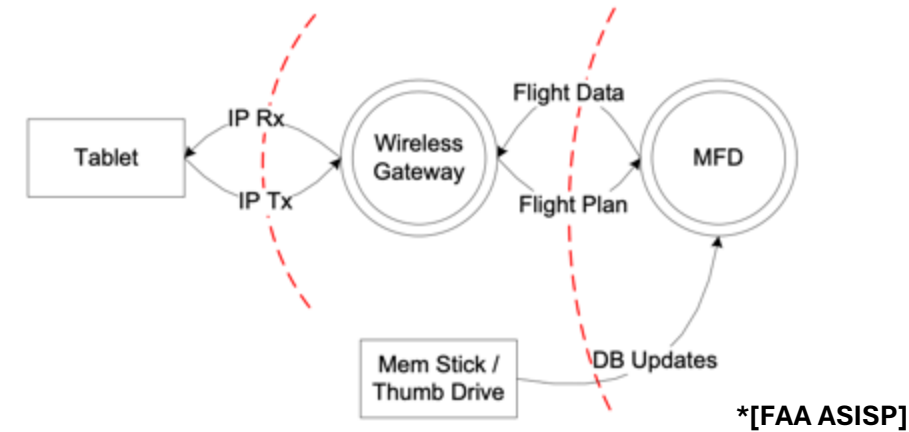
[Sampigethaya, AIAA]

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

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



## 3. Draw Data Flow Diagram



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

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

Red circles with 'T5' and 'T1' are placed over the 'Acceptable' cells in the 'High' and 'Low' rows respectively. Red arrows labeled 'MITIGATION' point from these cells towards the 'Acceptable' cells in the 'Extremely Low' row.

## 4, 5. Identify and Document Threats

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
---	-----	------	-----------------------------------

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
---	------	-----	---	----------------------------

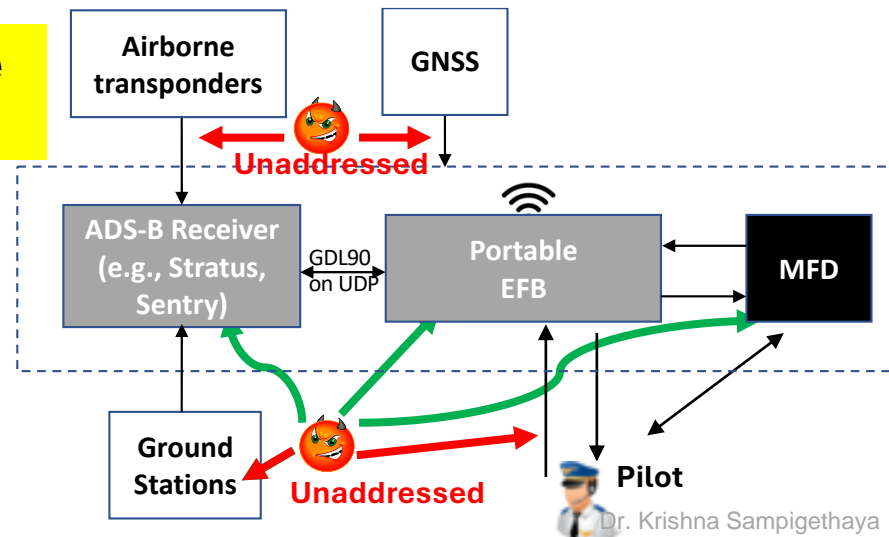
[RTCA SC-216 DO-356A], [Sampigethaya, RSAC]

# 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]

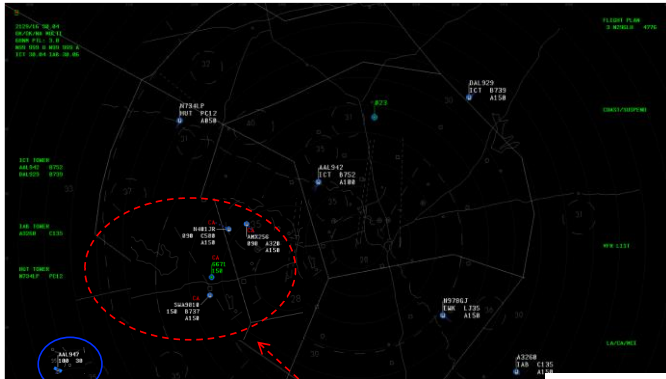
In the context of the example system



## Major Gaps

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

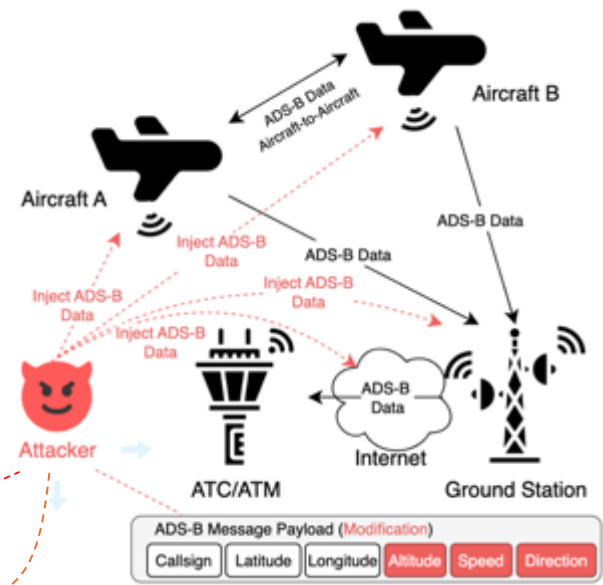
# CNS-ATM Cyber-Physical Security Considerations: ADS-B



Present false scenario to ATCO



ATCO

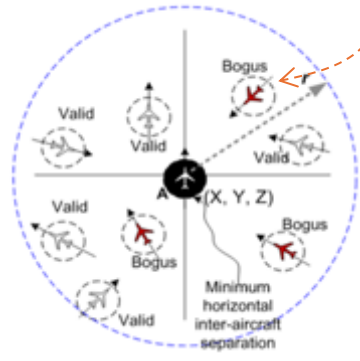


ADS-B Message Payload (Modification)

Callsign	Latitude	Longitude	Altitude	Speed	Direction
----------	----------	-----------	----------	-------	-----------



PILOT



ADS-B Applications	Industry focus	Threat mitigations
	Ground Surveillance	Airborne Surveillance
Security Property		
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 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**