Cyber-hijacking Airplanes:

Truth or Fiction?

Dr. Phil of Bloomsburg University

@ppolstra

http://philpolstra.com

Captain Polly of University of <redacted>

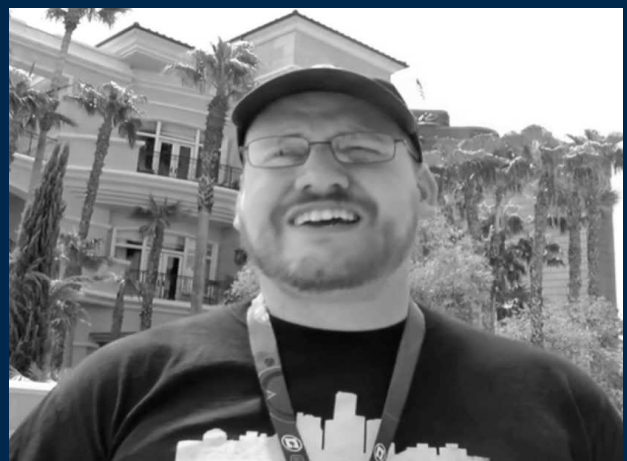
@CaptPolly

Why This Talk?

- Lots of bold claims concerning the feasibility of cyber-hijacking
- Bold claims get lots of press
- Most people don't know enough to evaluate these claims
- Whether you feel safer or even more scared should be based on facts

Who is Dr. Phil

- You may know me as a hardware hacker, but I'm also...
  - Holder of 12 aviation ratings, all current, including:
    - Commercial Pilot
    - Flight Instructor
    - Aircraft Mechanic
    - Inspection Authorization holder
    - Avionics Technician
  - Have thousands of hours of flight time
  - Aircraft builder
  - Have worked on the development of avionics found in modern airliners
  - Have access to airliner manuals, current and former airline pilots



Hacking and Penetration Testing with Low Power Devices

Philip Polstra

SYNGRESS

DEFCON

Who is Captain Polly

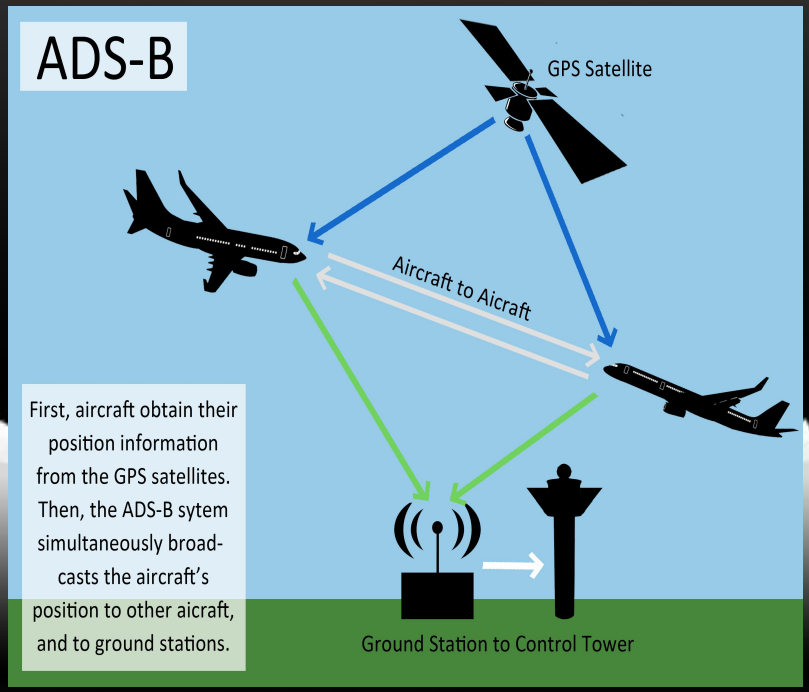
- Former airline pilot for a major US carrier
- Thousands of hours in airliners and small aircraft
- Aviation professor
- Head of college simulator program
- Spouse of a current airline pilot

What you will learn

- How some of the common aircraft systems really work, including:
  - ADS-B
  - ADS-A
  - ACARS
  - Transponders
  - Collision avoidance
  - GPS
  - Autopilots
  - Avionics buses and networks
  - Attacks being presented by others

Some commonly discussed attacks

- Hacking into the avionics via the entertainment network
- Hacking ADS-B
- Hacking engine systems
- Hacking ACARS



Let's get this out of the way to start

- You cannot override the pilot
- All aircraft feature unhackable mechanical backup instruments
- You can affect the autopilot operation
  - If pilot(s) notice they will disconnect
  - Anything you attempt will likely result in alerts

Attacking avionics networks

- Older aircraft use ARINC 429 networks
  - Not connected to anything useful
  - Require specialized hardware
- Newer aircraft use a modified version of Ethernet known as ARINC 664 or AFDX

ARINC 664 and AFDX

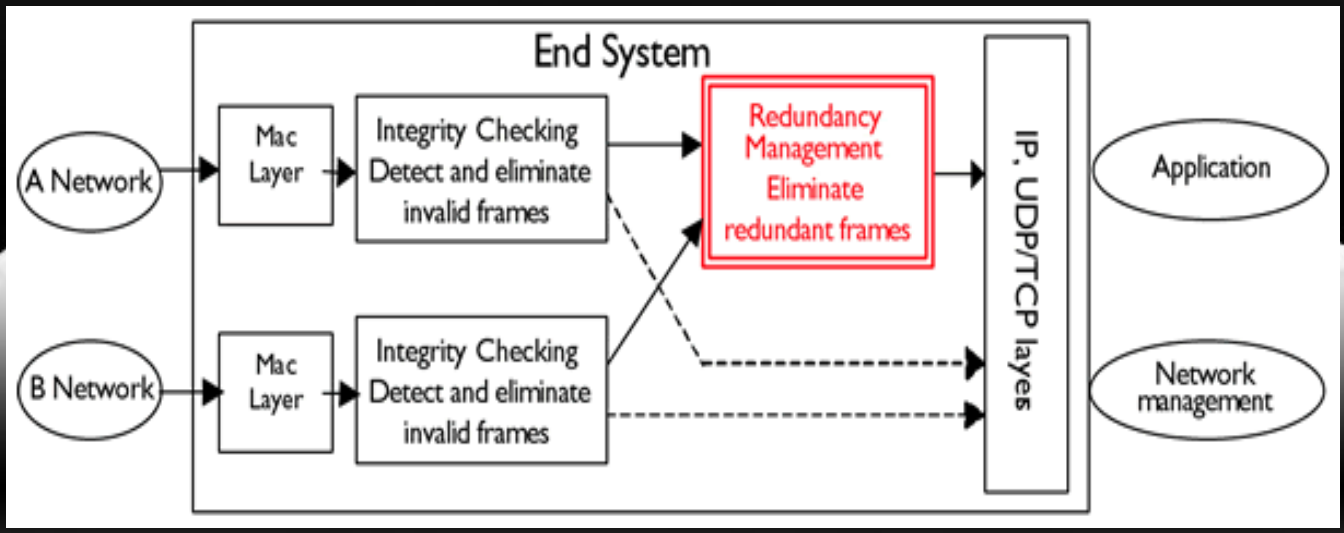
- Built on Ethernet, but...
  - Can't just start sending packets
  - Never wireless
  - Some security in place
- Not connected to entertainment system
- Not connected to in-flight wifi

Meet ARINC 664 aka AFDX

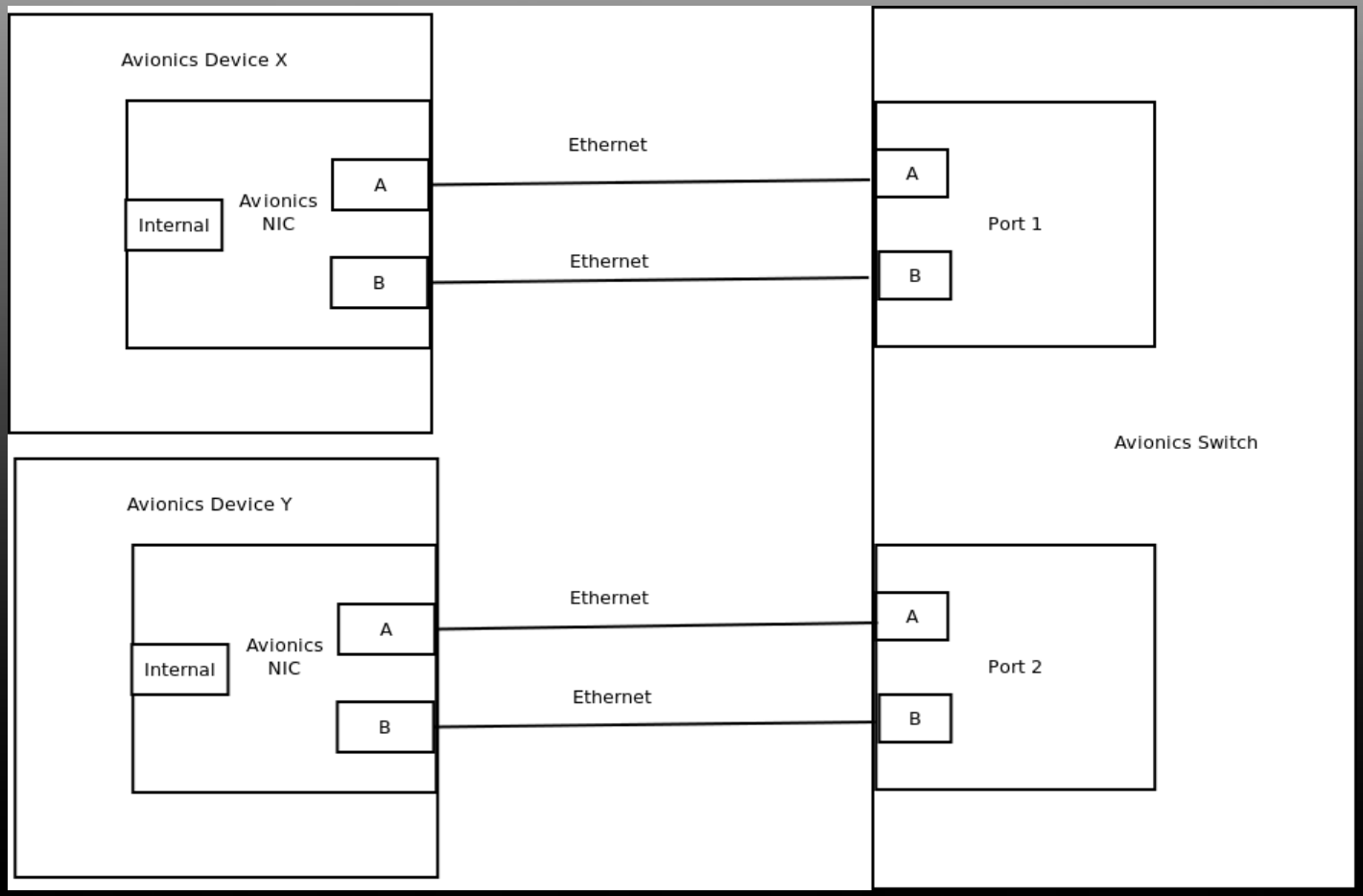
- Based on ARINC 629
  - First created by Boeing for 777
- Allows the use of common off the shelf (COTS) components vs ARINC 429 which is proprietary
- Built on Ethernet, but not the same
  - Uses redundant channels
  - Assigns time slices to avoid collisions and make it deterministic

ARINC 664 Virtual Links

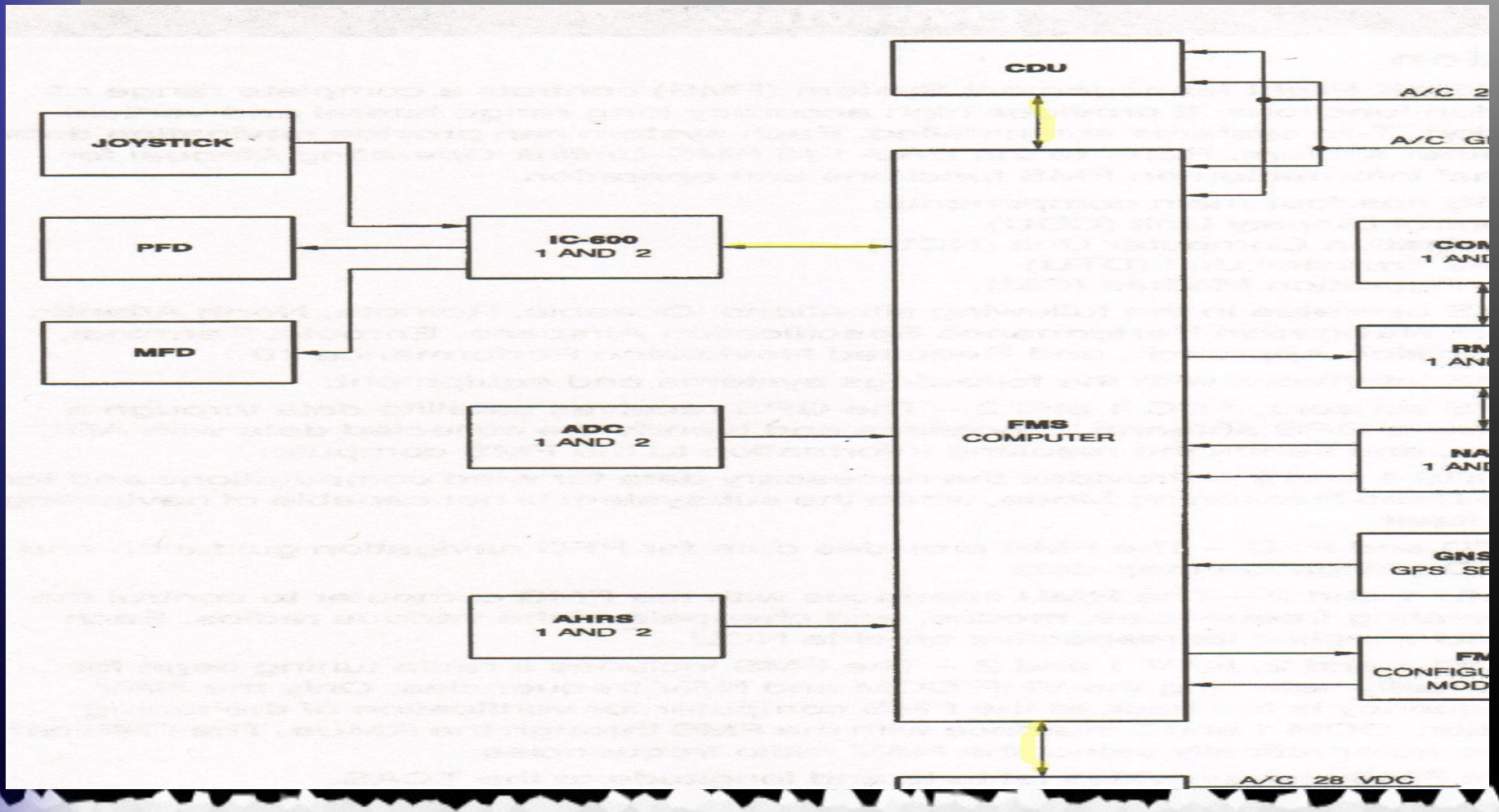
- Unidirectional logical pipe
- 1 and only 1 sender
- 1 or more receiver
- Timeslicing is used to avoid collisions
  - Bandwidth Allocation Gap (BAG) determines size of timeslice
  - Jitter (max latency – min latency) determined by number of VL and BAG



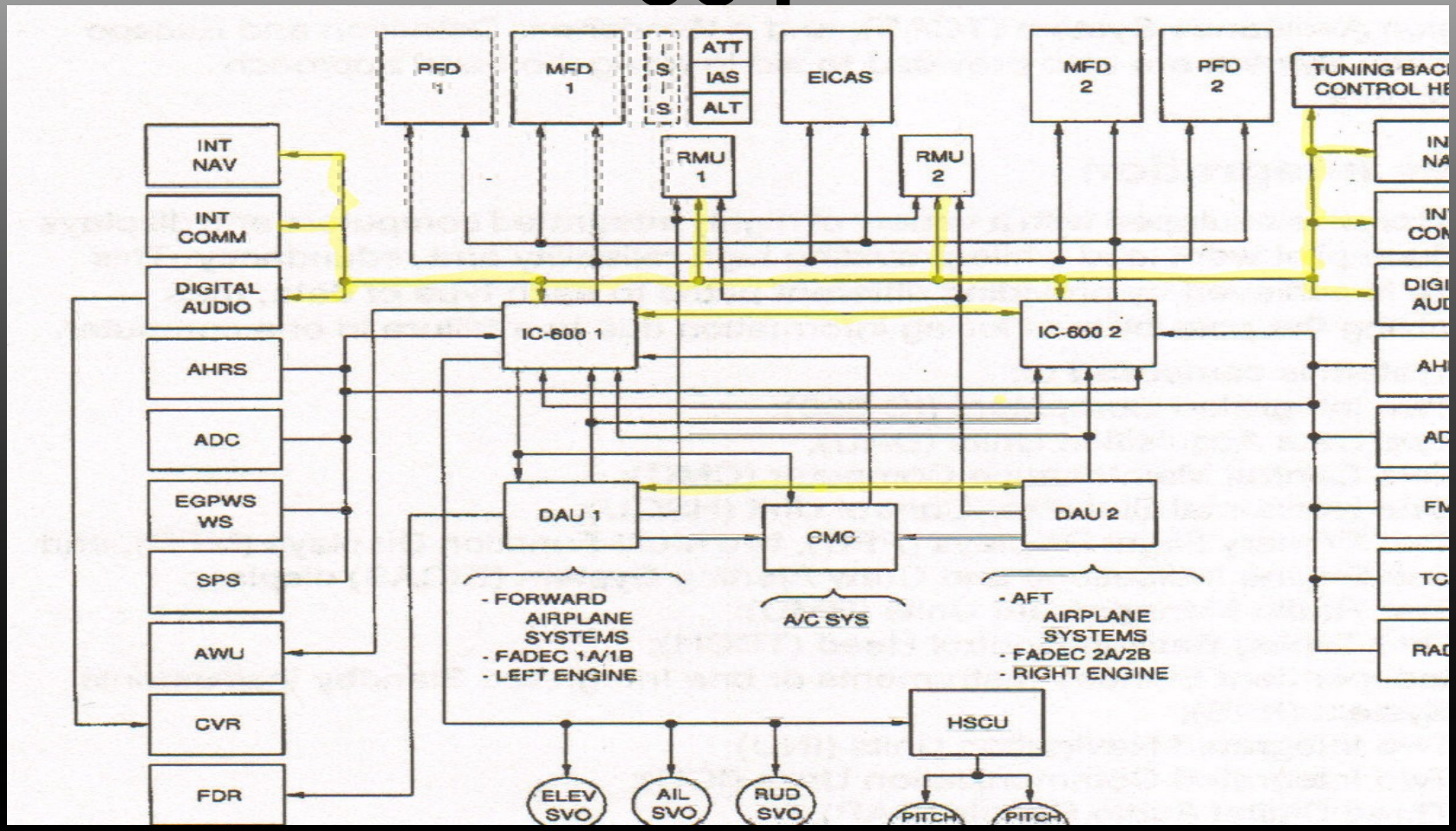
AFDX Connections



ARINC 664 in real life



Tight Integration with ARINC 664



Entertainment Systems

- Connected to output ports on GPS and FMS or through a Network Extension Device (NED)
- Never connected to ARINC 429/629/664
- Remember that the avionics network is never wireless and not compatible with your friendly TCP/IP

In-flight Entertainment

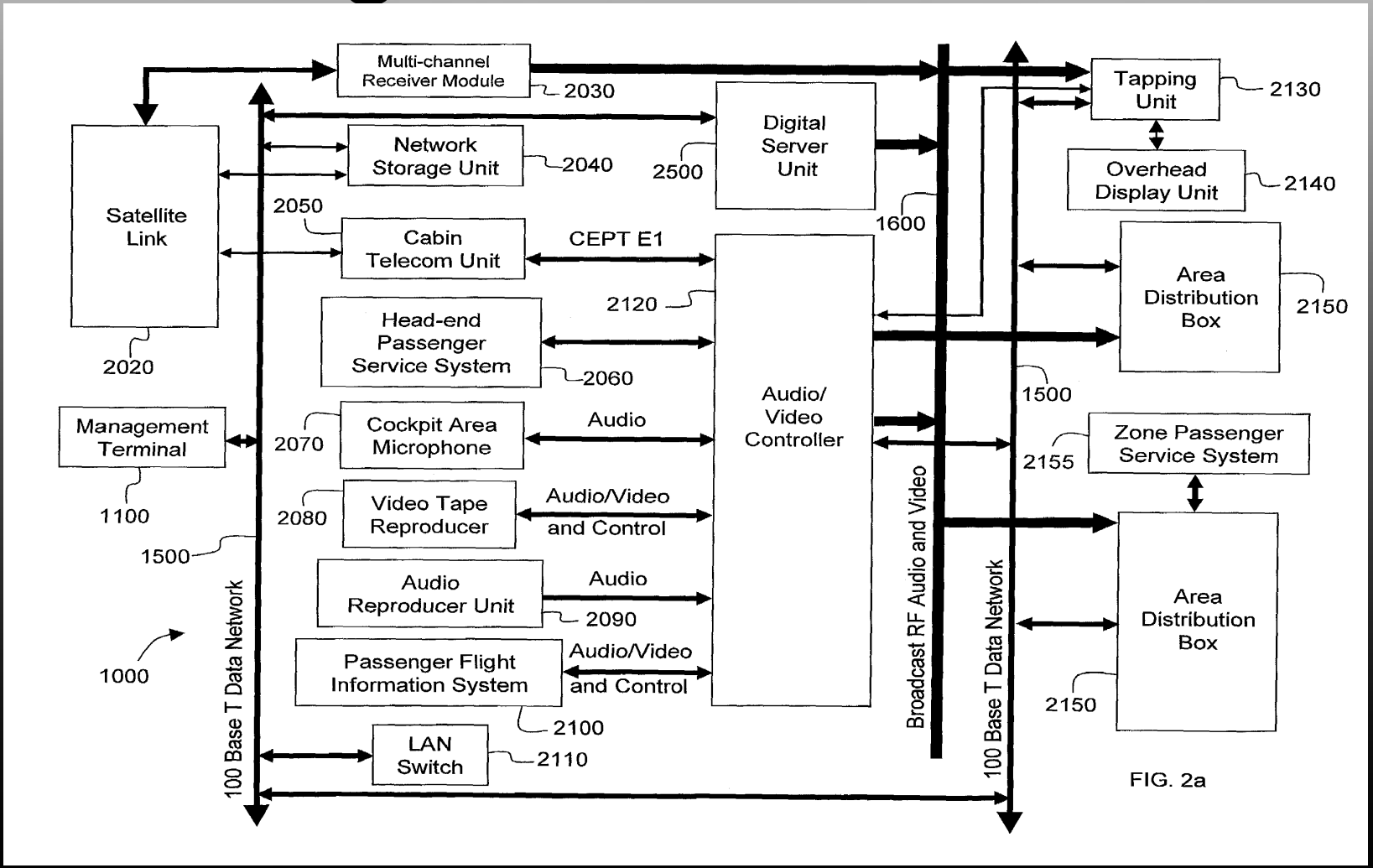


FIG. 2a

Boeing 777 Confusion

- Boeing asked for a special condition to allow the passenger information network to be connected to other networks such as the aircraft information network
- FAA granted this special condition on 11/18/13 provided that a network extension device (NED) was used and certain conditions were met

777 Confusion (contd)

FAA specified:

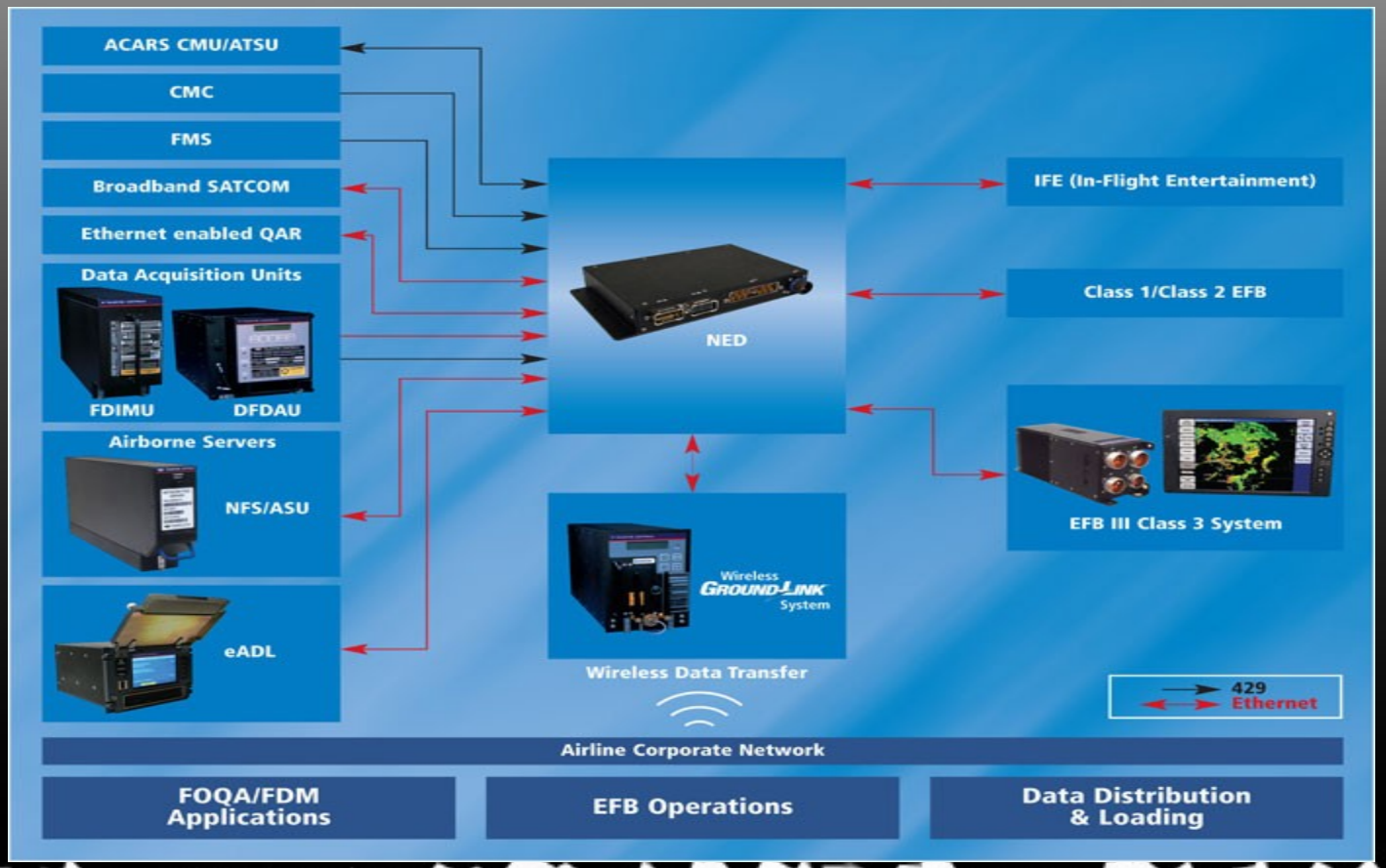
- The applicant must ensure that the design provides isolation from, or airplane electronic system security protection against, access by unauthorized sources internal to the airplane. The design must prevent inadvertent and malicious changes to, and all adverse impacts upon, airplane equipment, systems, networks, or other assets required for safe flight and operations.

Meet NED the Network Extension Device

- Essentially a gateway that goes between ARINC 429/629/664 and IP
- Like any gateway each path must be programmed
- FMS does not receive input from NED
  - Cannot send bogus commands to FMS
  - If NED is compromised may be possible to impersonate another device

Example NED implementation

- Shameless used from http://www.teledynecontrols.com/productsolution/ned/blockdiagram.asp



MH370?

- A Boeing 777
- Uses ARINC 629
  - Not 664 we've been discussing
  - *Really* not Ethernet
- The 777 is essentially the only plane to use ARINC 629
  - Harder to hack than ARINC 664

Airliner Entertainment System Connection

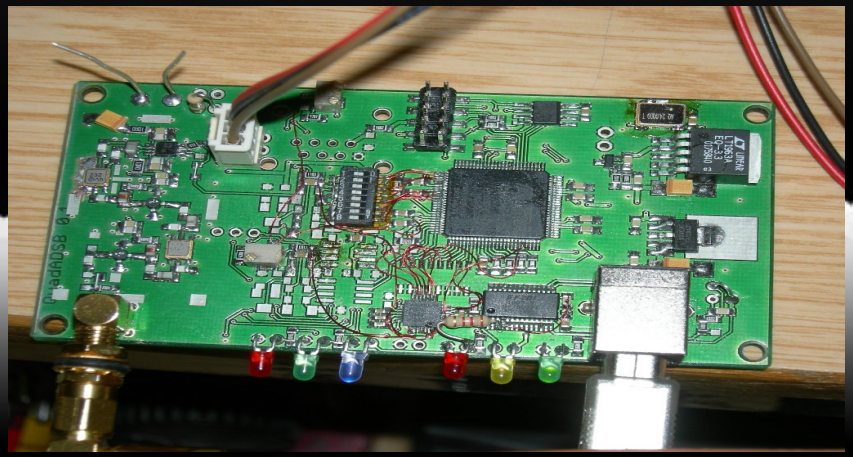
Redacted

Sorry, we really tried to put a schematic on this slide, but couldn't get approval from manufacturers

Hacking In-flight Wireless

Attacking ADS-B/ADS-A

- Can create phantom aircraft
- No security in protocol
- Could create fake weather reports
- Could be jammed
- Not likely to affect TCAS



ADS-B (broadcast)

- Piloted in Alaska
- Intended to improve flying where RADAR coverage is limited
- Part of a Free Flight system planned for the future
- Provides traffic and weather where available
- Used by small planes to broadcast position information

ADS-A (addressable)

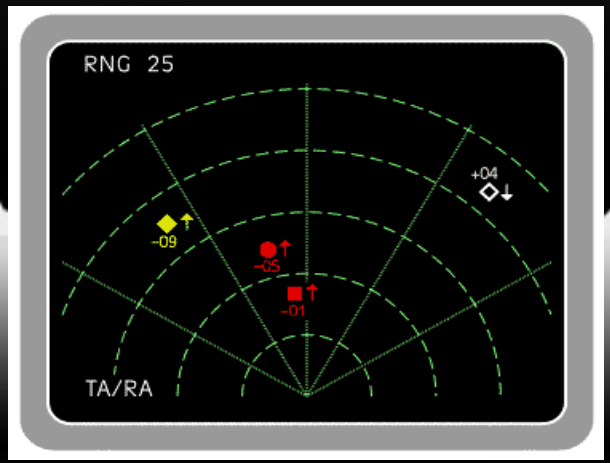
- What the airlines use (contrary to what you may have heard)
- Related to ACARS
- ADS-B == cable-ready TV
- ADS-A == addressable cable box with pay-per-view, etc
  - Allows specific airplanes to send/receive messages
  - Allows lower separation outside of RADAR coverage (FANS)
  - Airliners use neither ADS-B or ADS-A for collision avoidance
  - Can be VHF, HF, or Satellite based

Collision Avoidance

- TIS-B
  - Provided by ATC
  - Requires a mode S transponder (ADS-B in)
  - Only available in some areas
  - Not authoritative
  - Does not use ADS-B signals
  - ATC does not automatically relay every ADS-B signal they receive

Collision Avoidance (contd)

- TCAD
  - Used in small planes
  - Provides information
  - Not authoritative
- TCAS
  - What the big boys (biz jet and up) use

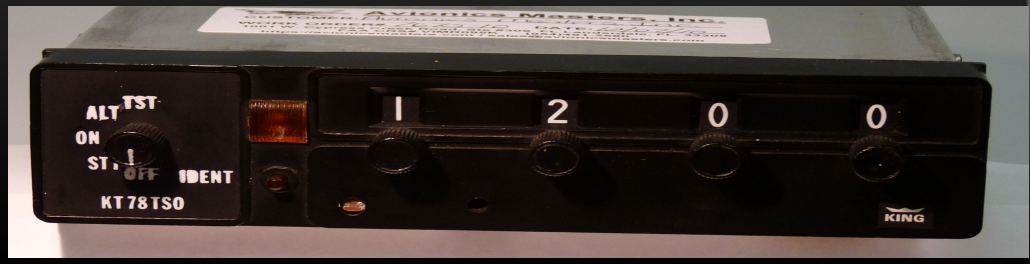


TCAS

- Uses transponders in the area
- Can actively interrogate other transponders
- Authoritative
- Pilot can use even if other aircraft not in sight

Transponders

- Supplement primary RADAR
- Mode S used in ADS-B
- Airliners have at least 2
- Signals are used for collision avoidance



Attacking ADS-B

ADS-B ATTACK

Attacking engine systems

Engine monitors are output only

- Information is recorded for maintenance
- Some information may be sent via ACARS to airline and/or manufacturer

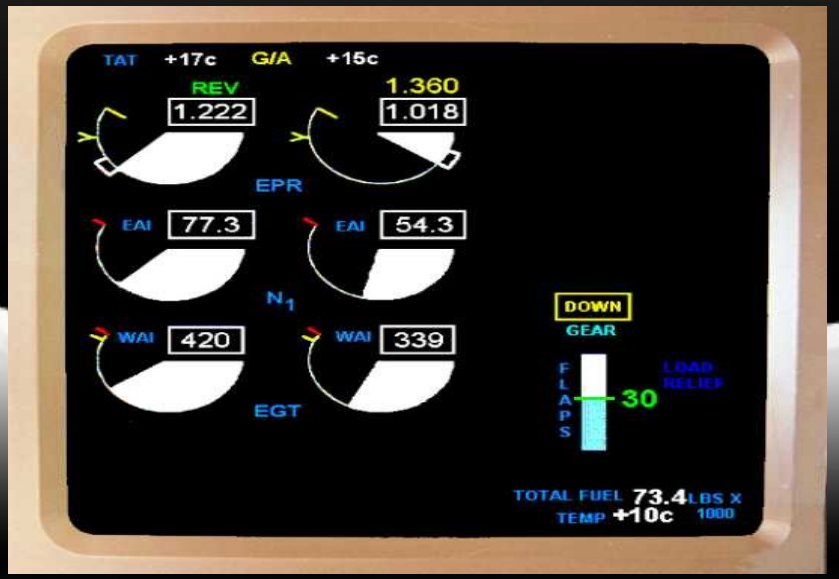
- Some engine control systems are electronic
  - All have purely mechanical backup
  - Most only trim mechanical system electronically

ACARS

- Can be used to send messages to/from ground
- Messages to/from people or systems
- Used for
  - Weather
  - Delays
  - Updated flight plans
  - Maintenance information

Attacking ACARS

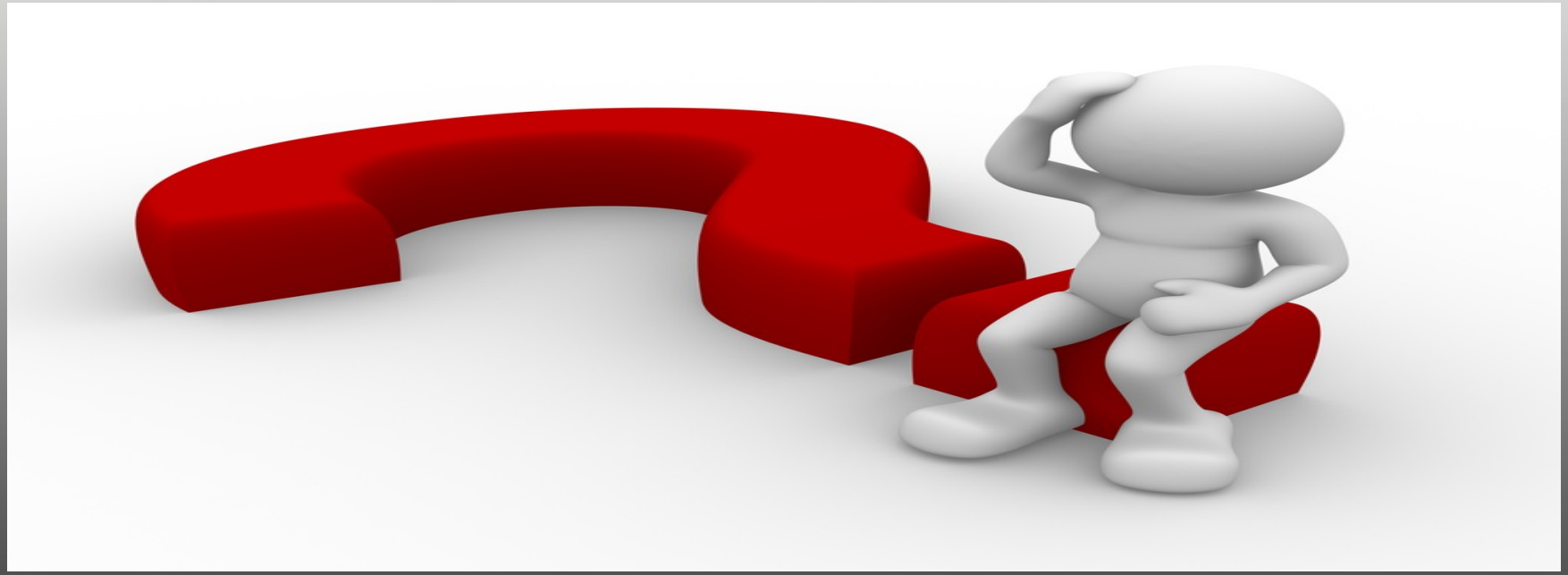
- Could create a bogus flight plan update
- Could create bogus weather
- Hypothetically could create fake messages from plane to ground
- Not a practical way to take over an airplane



ACARS Attack

Closing Thoughts

- Nearly every protocol used in aviation is unsecured
- There is certainly the potential to annoy ATC and/or small aircraft
- Increasing automation while continuing with unsecured protocols is problematic
- Airliners are relatively safe (for now)



Questions?

Come see us after or hit us on Twitter at @ppolstra or @CaptPolly