RSAC Sandbox

RSAConference2020

HUMAN ELEMENT

SESSION ID: **SBX1-R9**

Aviation Cybersecurity: Technology and Teamwork

Pete Cooper
MD
Aerospace Sandbox

Patrick Kiley
Principal Security Consultant
Rapid7

Ken Munro
Partner
Pen Test Partners

Talk objectives

Aviation security primer.

Share experiences.

Contribute to future aviation safety.

Caveat: you're more likely to be pwned through your business network and supply chain than through your planes & airports

Responsible disclosure

Aircraft are hard to fix if an issue is found.

We, and our friends and families, fly.

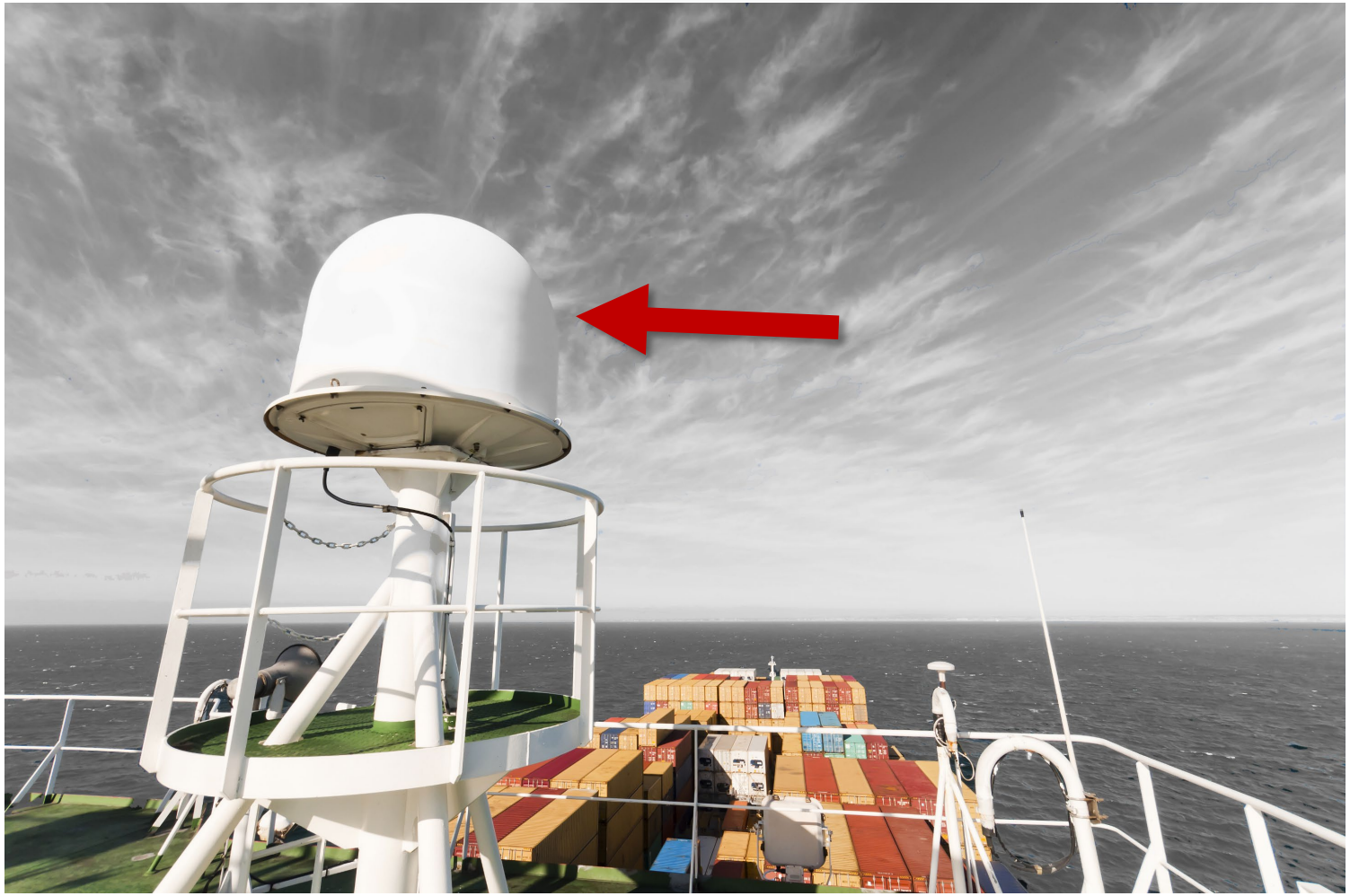
Disclose to vendors and regulators.

Hacking Satcom Terminals

Do you have any control over the smart devices your crews bring on board?

How secure are the wireless networks on board your vessels?

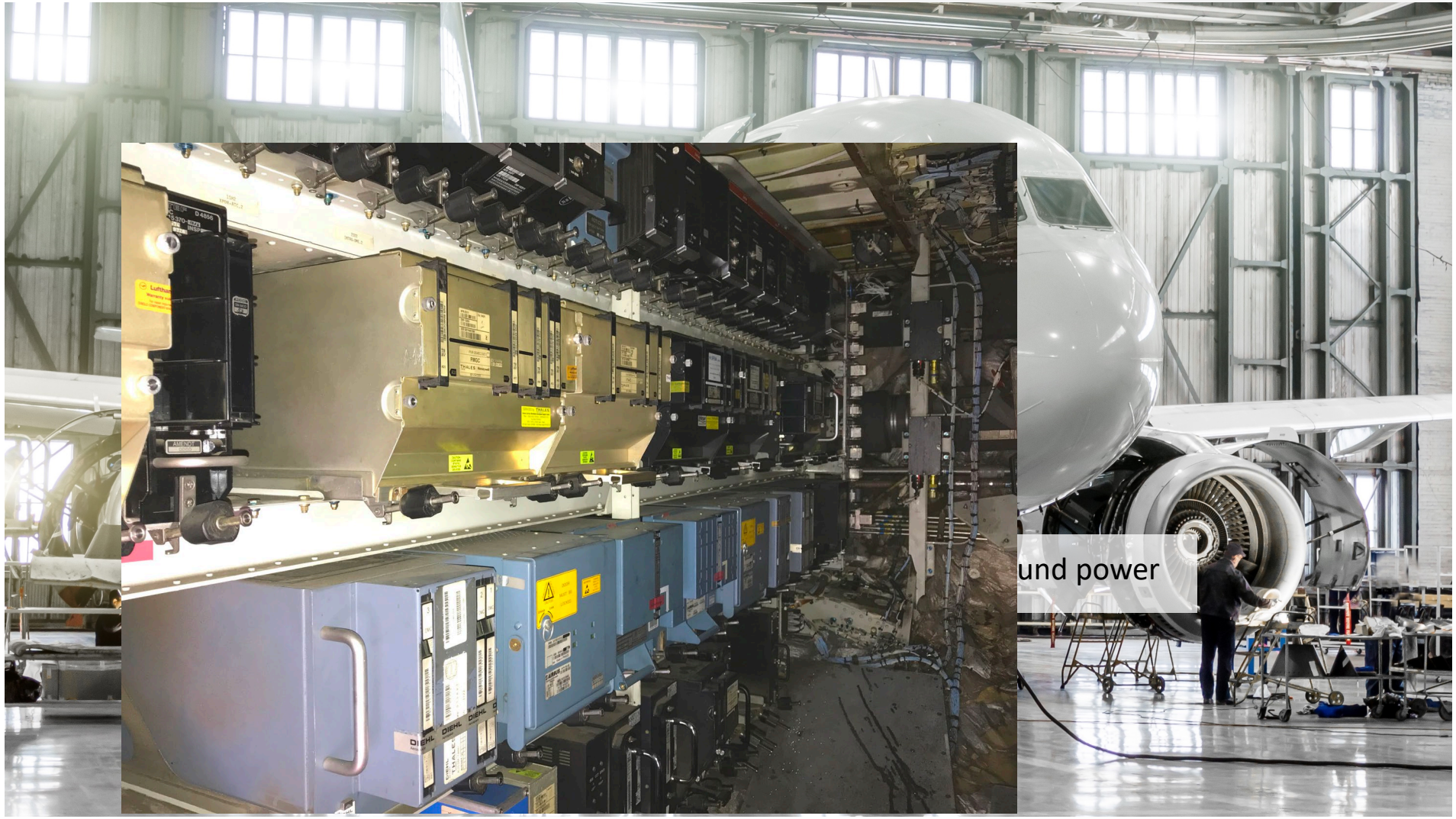
Have you checked the separation of your on-board networks?



How did we get started?

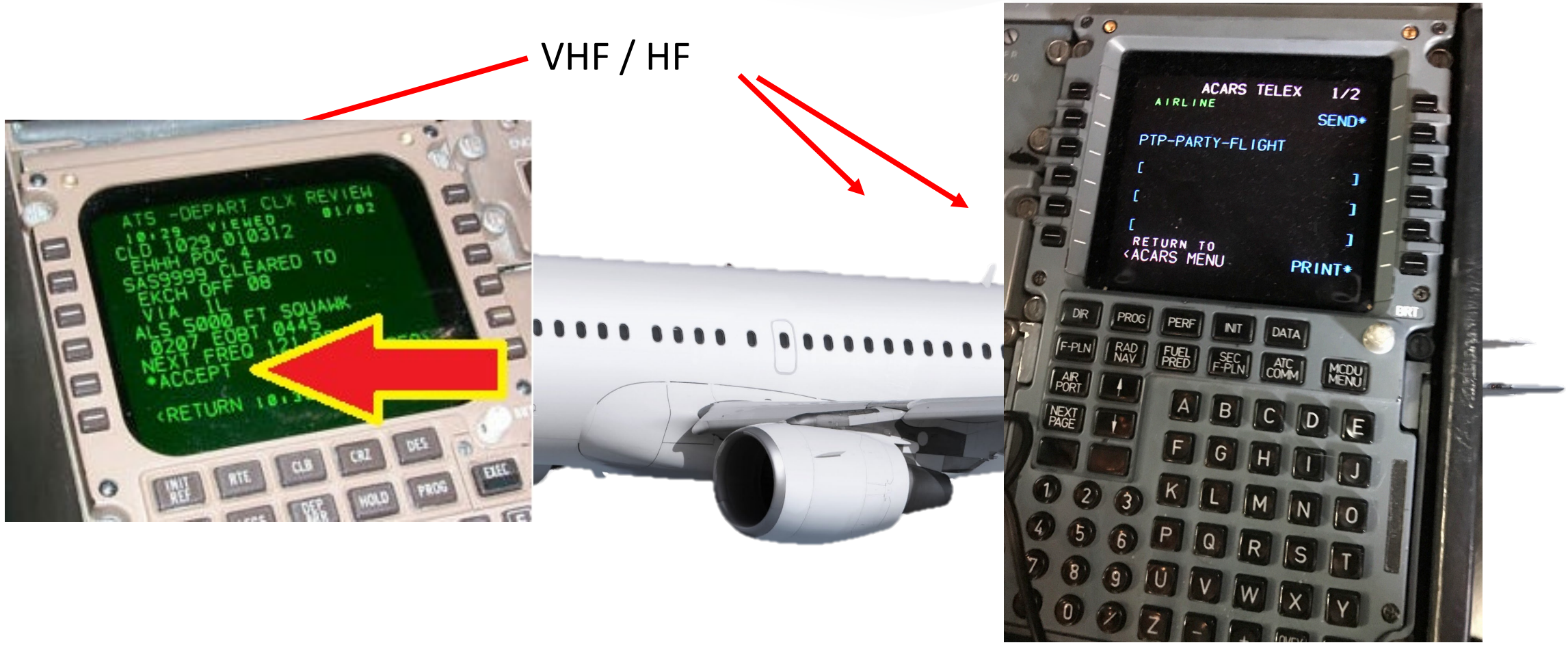
RSAC Sandbox

Aircraft access

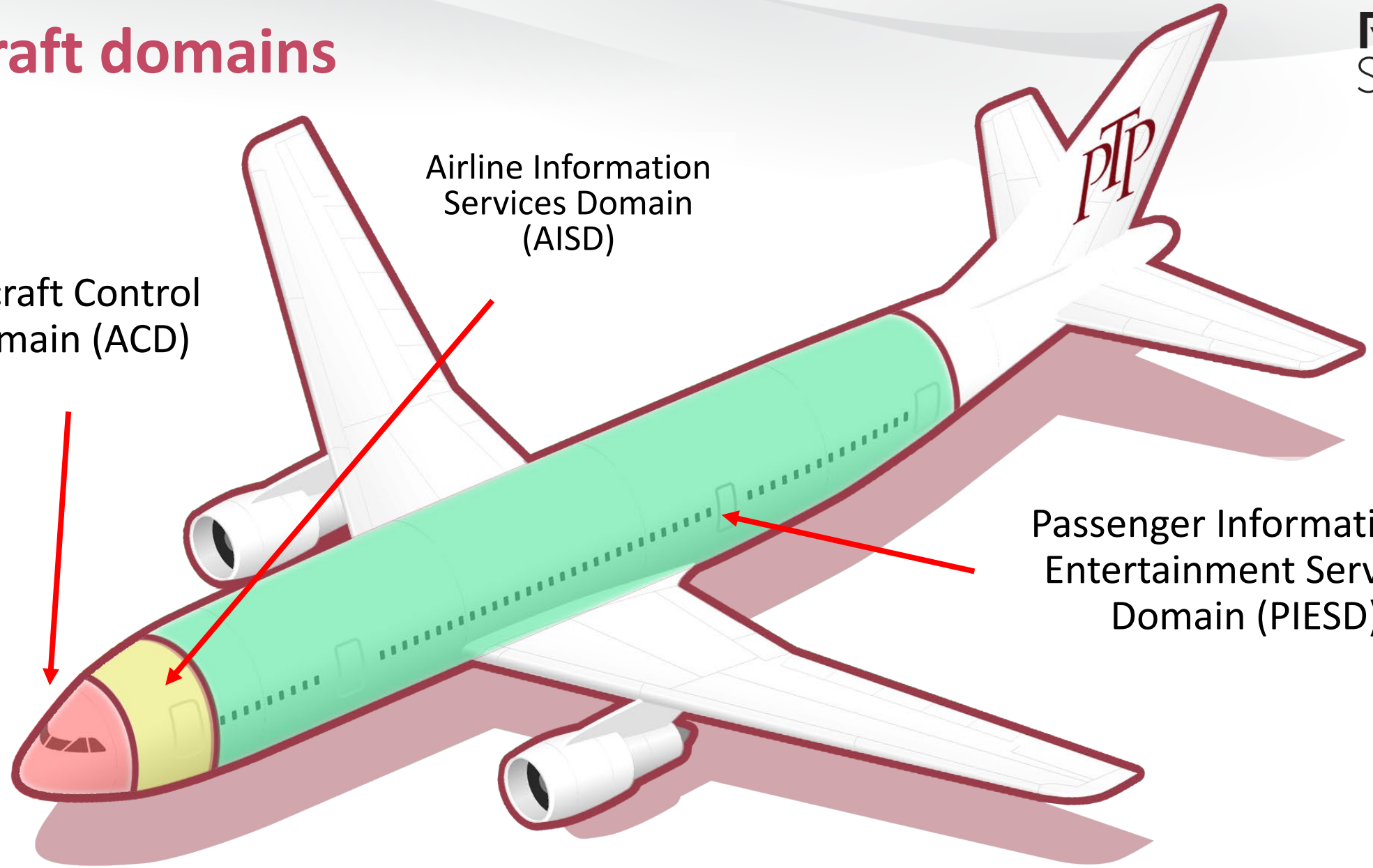


Aircraft connectivity

RSAC Sandbox

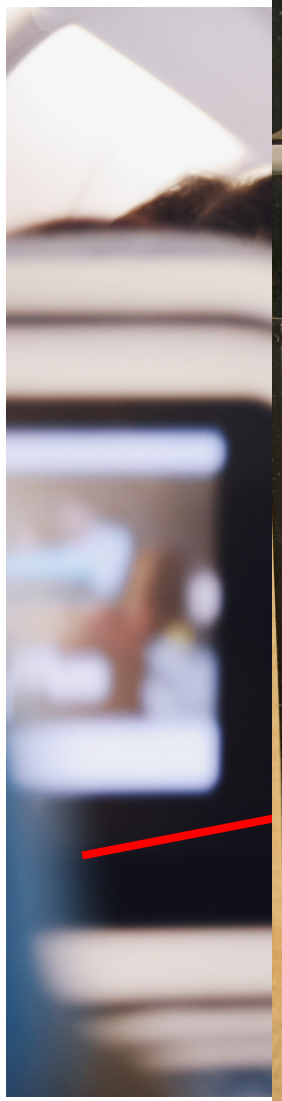


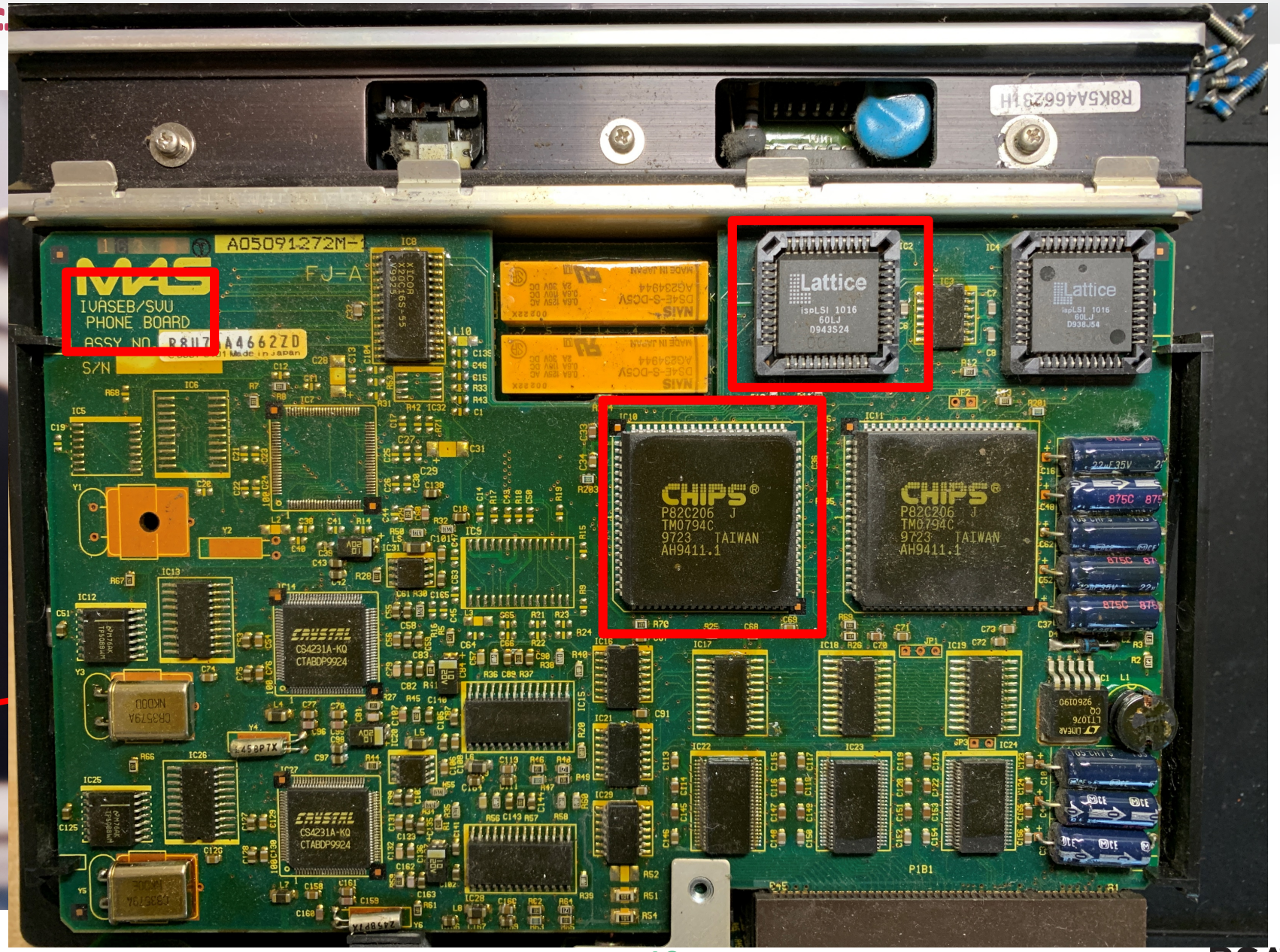
Aircraft domains



Aircraft connectivity

Aircraf





RSAC Sandbox

ACD Connectivity

RSAC Sandbox

ACD Connectivity

RSAC Sandbox

EFBs (Often iPads)

AIDS

PDL

PMAT

Aircraft control databuses – ARINC 429

RSAC Sandbox

Legacy, point-to-point, one source, multiple recipients

+/- 10v differential pairs

12/100kbps

32bit words
Source/sink/data

Odds parity check

Aircraft buses – AFDX (ARINC 664)

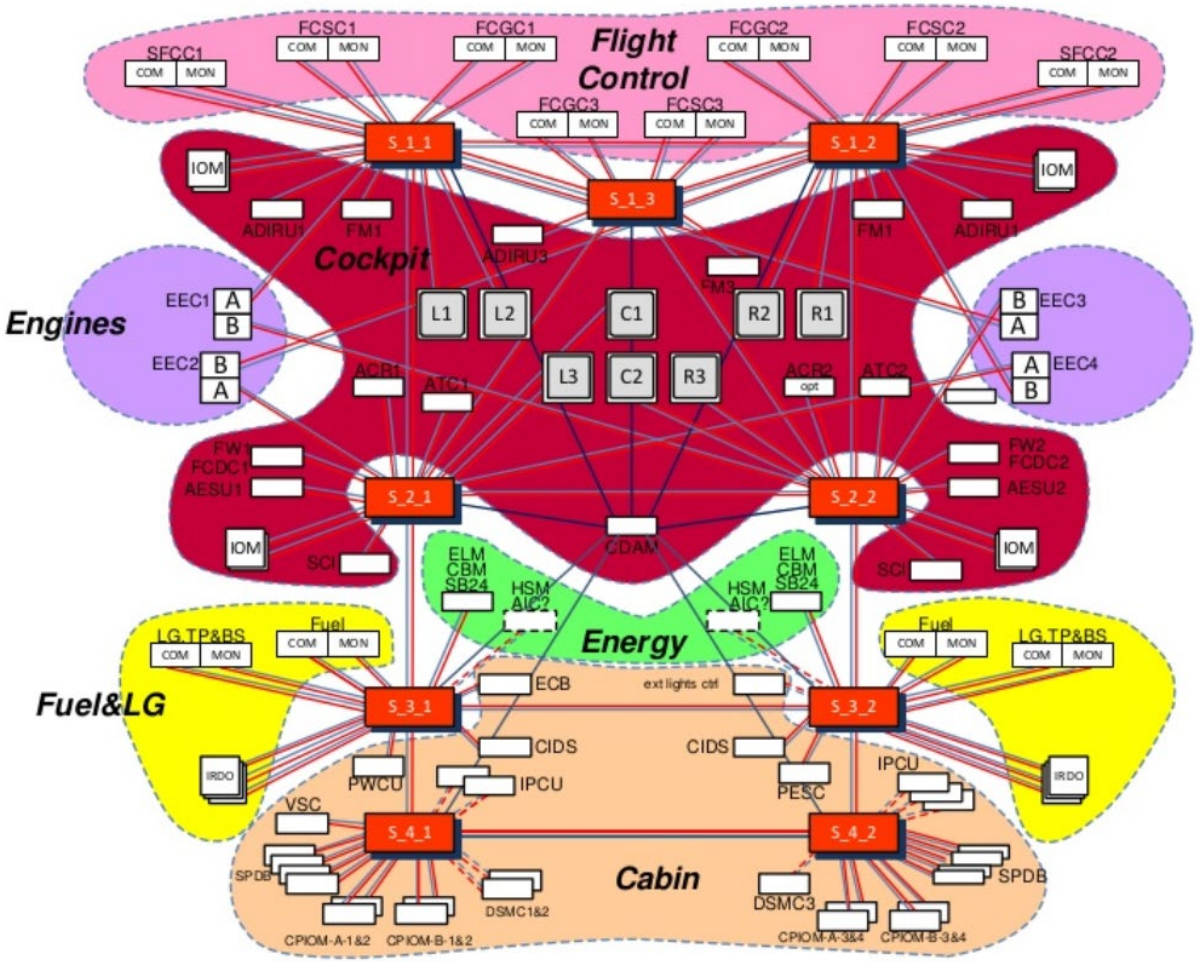
Ethernet

787 / A350 / A380+

MACs / Virtual Links

UDP/ICMP/SNMP(!)

Data concentrators



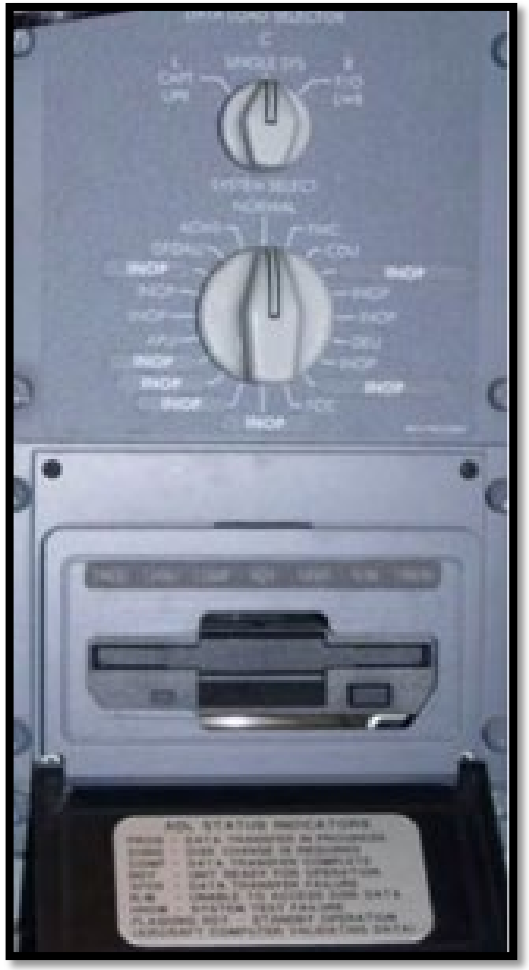
Updates

Dataloaders typically run ARINC 615, layered over 429

Primarily nav databases, but also avionics software

Manual installation overhead, code rarely signed

Desire to update OTA



Hardware RE Strategy

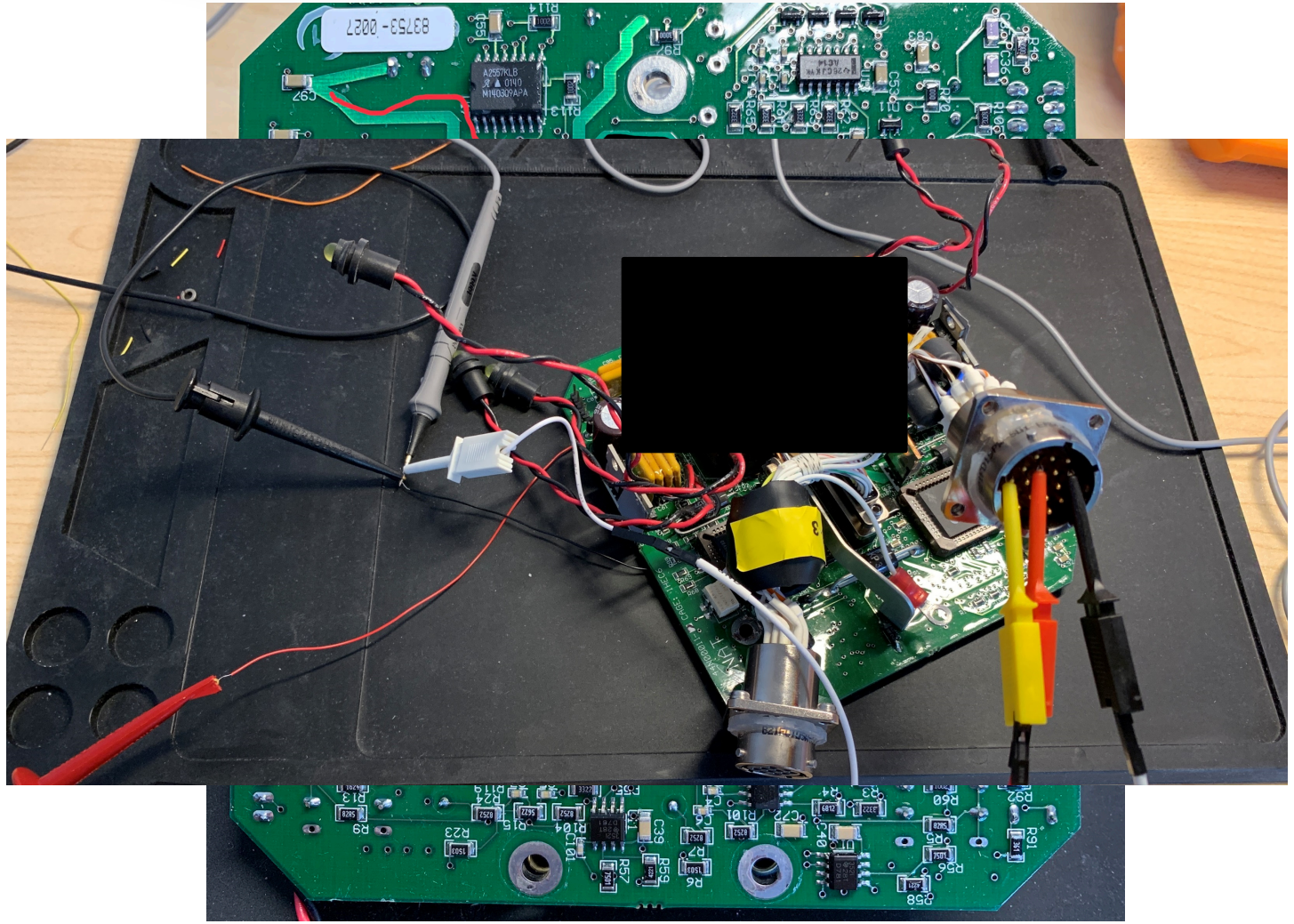
Search for datasheets (often very old)

Trace / buzz out pins (gah, conformal coating)

Saleae

Dataman / firmware binary dump

RO protection uncommon



The future (is now…)

Common core system

VxWorks

LSAP

The Airport

Airport Building

- Briefing Systems
- Baggage
- Check-In Desks
- Departure Boards
- Airside Concessions / Duty Free
- Airside Systems
- CCTV
- Building Management
- Wi-Fi
- Airside Security
- Access Control
- Airside RF
- HVAC
- Gatelink

Pushback Tugs

Airside Vehicles

Docking System