Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse
Science and Technology

CYD
CYBER DEFENCE CAMPUS

Labs and Trust: How to build a successful aviation cybersecurity research programme

Dr. Martin Strohmeier
Cyber-Defence Campus, armasuisse S + T, Switzerland

CYD Campus Research on Aviation

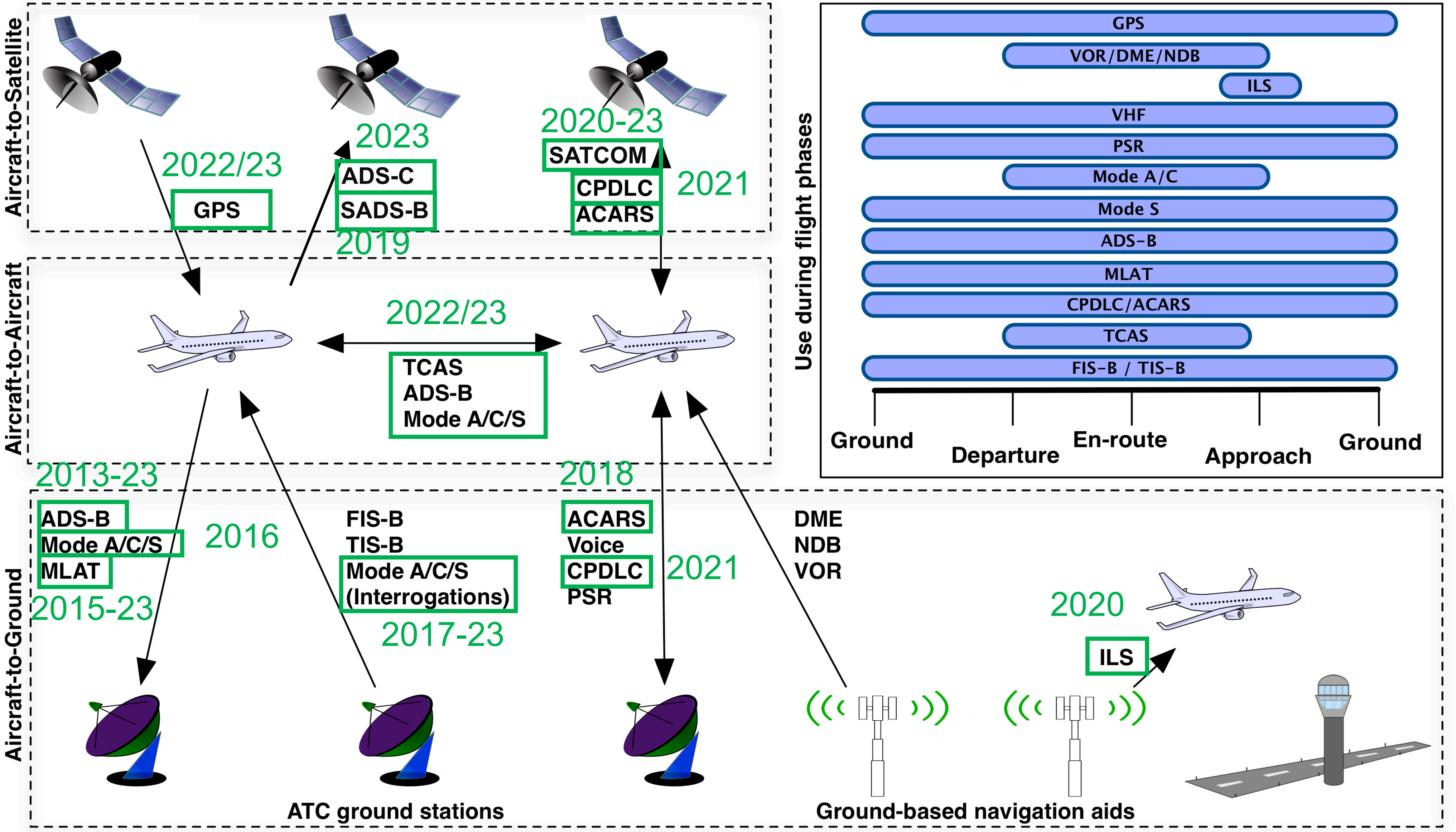
- Three types of partners on this topic
  - Universities – research collaboration
  - Government/Military – stakeholders/users/regulators
  - Industry – research, knowledge exchange, disclosure

- Published over 60 papers in 10 years, with 50 co-authors from more than 20 institutions

- Currently over 10 students working on various aviation security topics this year – stay tuned for exciting practical results on TCAS, CPDLC, ADS-C, MLAT and more!

- **Note: This is a long-term government effort using significant resources, but many lessons should apply across the board.**

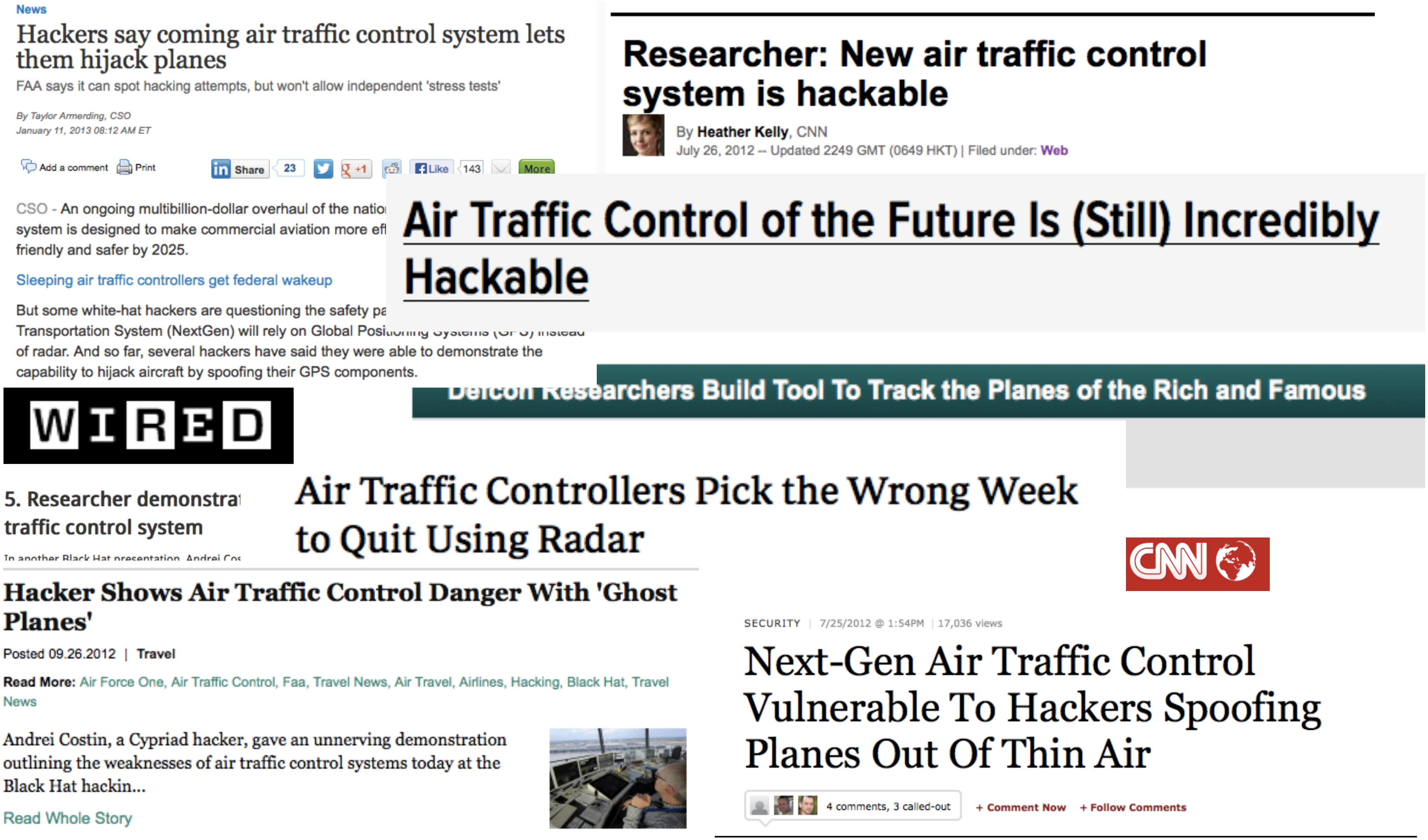
Aviation Comms: Cyber Research



Plus: Privacy research, GPWS, Human Factors…

Trust

Hacker Community: Traditional Security View…or how not to build trust



News

Hackers say coming air traffic control system lets them hijack planes

FAA says it can spot hacking attempts, but won't allow independent 'stress tests'

By Taylor Armerding, CSO
January 11, 2013 08:12 AM ET

CSO - An ongoing multibillion-dollar overhaul of the natio
system is designed to make commercial aviation more ef
friendly and safer by 2025.

Sleeping air traffic controllers get federal wakeup

But some white-hat hackers are questioning the safety pa
Transportation System (NextGen) will rely on Global Positioning Systems (GPS) instead of radar. And so far, several hackers have said they were able to demonstrate the capability to hijack aircraft by spoofing their GPS components.

Researcher: New air traffic control system is hackable

By Heather Kelly, CNN
July 26, 2012 -- Updated 2249 GMT (0649 HKT) | Filed under: Web

Air Traffic Control of the Future Is (Still) Incredibly Hackable

Defcon Researchers Build Tool To Track the Planes of the Rich and Famous

WIRED

5. Researcher demonstrat
traffic control system

In another Black Hat presentation, Andrei Cos

Air Traffic Controllers Pick the Wrong Week to Quit Using Radar

CNN

Hacker Shows Air Traffic Control Danger With 'Ghost Planes'

Posted 09.26.2012 | Travel

Read More: Air Force One, Air Traffic Control, Faa, Travel News, Air Travel, Airlines, Hacking, Black Hat, Travel News

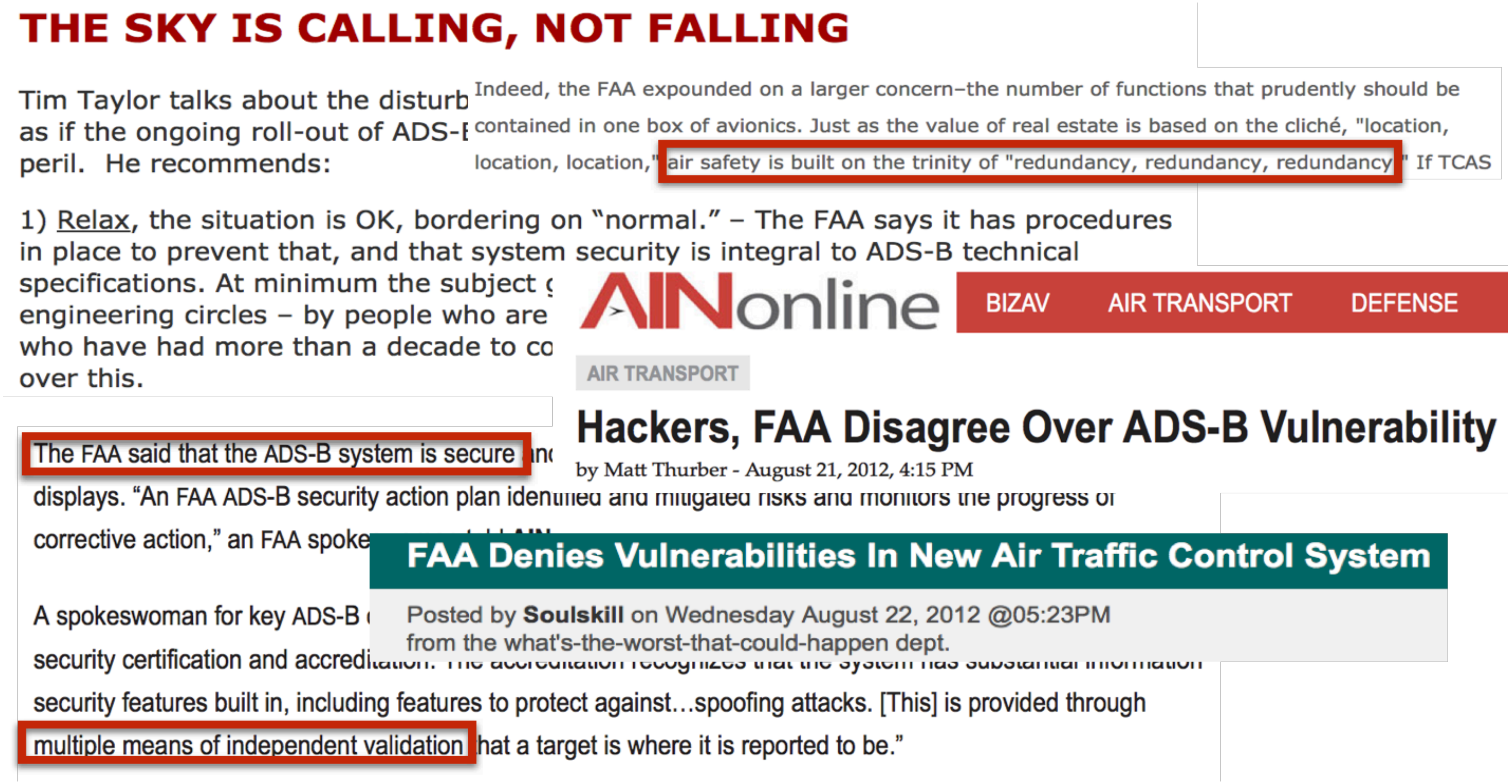
Andrei Costin, a Cypriad hacker, gave an unnerving demonstration outlining the weaknesses of air traffic control systems today at the Black Hat hackin...

Read Whole Story

SECURITY | 7/25/2012 @ 1:54PM | 17,036 views

Next-Gen Air Traffic Control Vulnerable To Hackers Spoofing Planes Out Of Thin Air

Aviation Community: Traditional Safety View …or how not to build trust



THE SKY IS CALLING, NOT FALLING

Tim Taylor talks about the disturb
as if the ongoing roll-out of ADS-I
peril. He recommends:

Indeed, the FAA expounded on a larger concern–the number of functions that prudently should be contained in one box of avionics. Just as the value of real estate is based on the cliché, "location, location, location," air safety is built on the trinity of "redundancy, redundancy, redundancy." If TCAS

1) Relax, the situation is OK, bordering on "normal." – The FAA says it has procedures in place to prevent that, and that system security is integral to ADS-B technical specifications. At minimum the subject g
engineering circles – by people who are
who have had more than a decade to co
over this.

Hackers, FAA Disagree Over ADS-B Vulnerability

by Matt Thurber - August 21, 2012, 4:15 PM

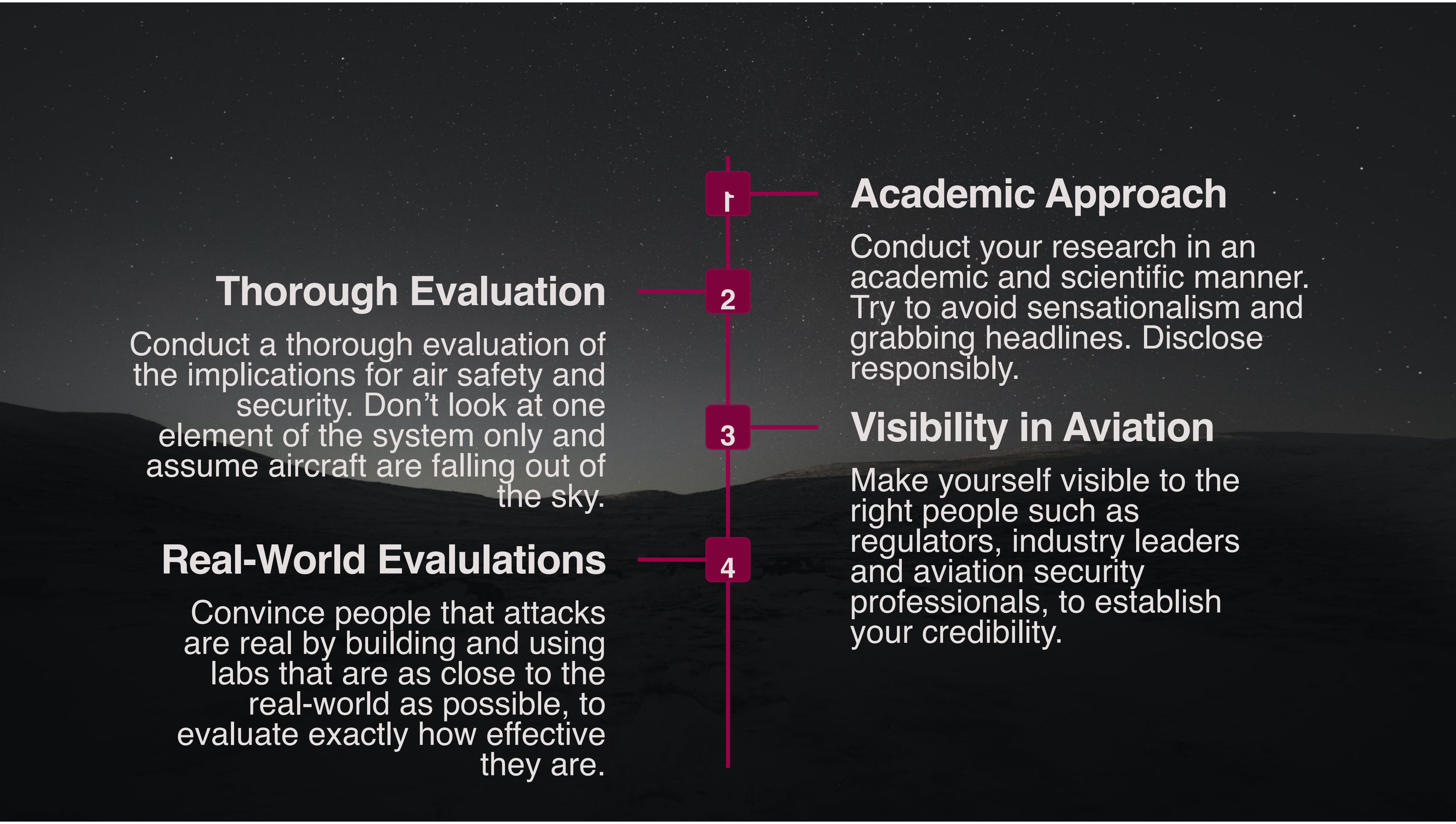
The FAA said that the ADS-B system is secure and displays. "An FAA ADS-B security action plan identified and mitigated risks and monitors the progress of corrective action," an FAA spoke

FAA Denies Vulnerabilities In New Air Traffic Control System

Posted by **Soulskill** on Wednesday August 22, 2012 @05:23PM
from the what's-the-worst-that-could-happen dept.

A spokeswoman for key ADS-B
security certification and accredi
security features built in, including features to protect against…spoofing attacks. [This] is provided through multiple means of independent validation that a target is where it is reported to be."

Building Trust in Aviation Research



Academic Approach

Conduct your research in an academic and scientific manner. Try to avoid sensationalism and grabbing headlines. Disclose responsibly.

Thorough Evaluation

Conduct a thorough evaluation of the implications for air safety and security. Don’t look at one element of the system only and assume aircraft are falling out of the sky.

Visibility in Aviation

Make yourself visible to the right people such as regulators, industry leaders and aviation security professionals, to establish your credibility.

Real-World Evalulations

Convince people that attacks are real by building and using labs that are as close to the real-world as possible, to evaluate exactly how effective they are.

It’s hard!

IT TAKES TIME. A LOT OF TIME.

IT REQUIRES PERSONAL CONNECTIONS.

IT’S EASIER AT THE GOVERNMENT AND MILITARY.

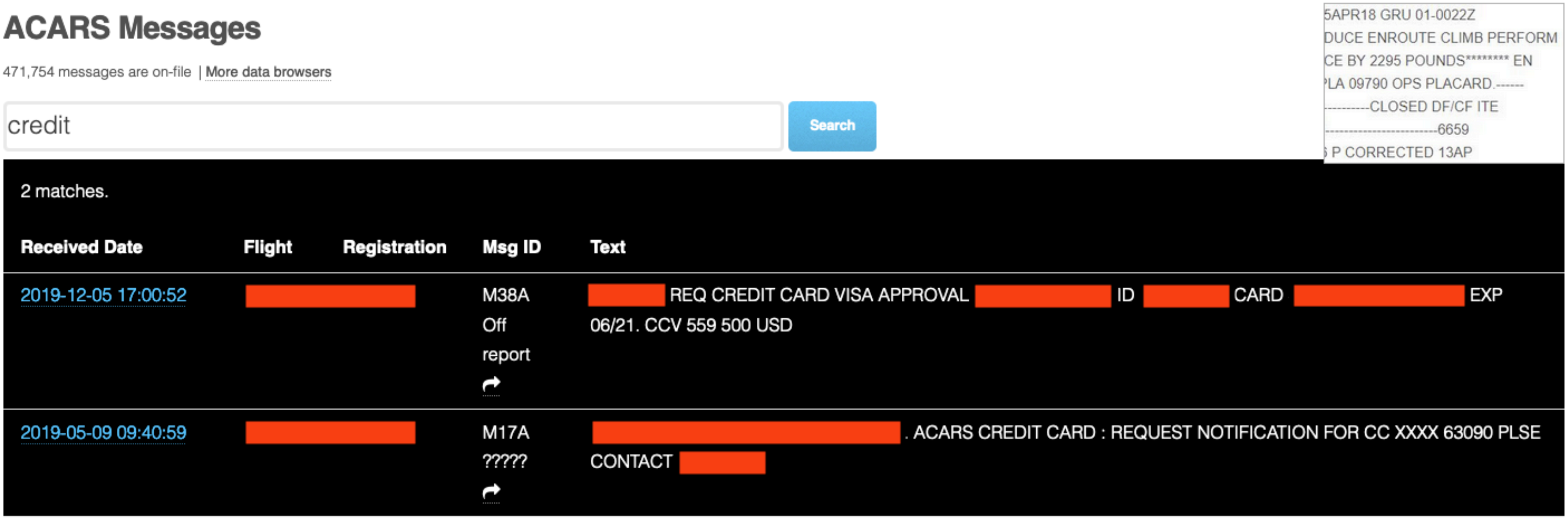
NECESSARY TO SOMEHOW GET AN IN WITH AVIONICS/DEFENCE COMPANIES.

COLLABORATE WIDELY!

GO TO AVIATION CONFERENCES OR RUN YOUR OWN WORKSHOP.

Example Disclosure: Positive Example

Reported credit card issues to several airlines back in 2016.
Successfully fixed (eventually, picture below from 2019)!



ACARS Messages

471,754 messages are on-file | More data browsers

5APR18 GRU 01-0022Z
DUCE ENROUTE CLIMB PERFORM
CE BY 2295 POUNDS******** EN
'LA 09790 OPS PLACARD.------
----------CLOSED DF/CF ITE
-------------------------6659
; P CORRECTED 13AP

2 matches.

Received Date	Flight	Registration	Msg ID	Text
2019-12-05 17:00:52	[redacted]		M38A Off report ↪	[redacted] REQ CREDIT CARD VISA APPROVAL [redacted] ID [redacted] CARD [redacted] EXP 06/21. CCV 559 500 USD
2019-05-09 09:40:59	[redacted]		M17A ????? ↪	[redacted] . ACARS CREDIT CARD : REQUEST NOTIFICATION FOR CC XXXX 63090 PLSE CONTACT [redacted]

Example Disclosure: Negative Example

Reported ACARS encryption issue [1] on 6th Dec 2016, with a reply on 9th Feb 2017, indicating no further action would be taken

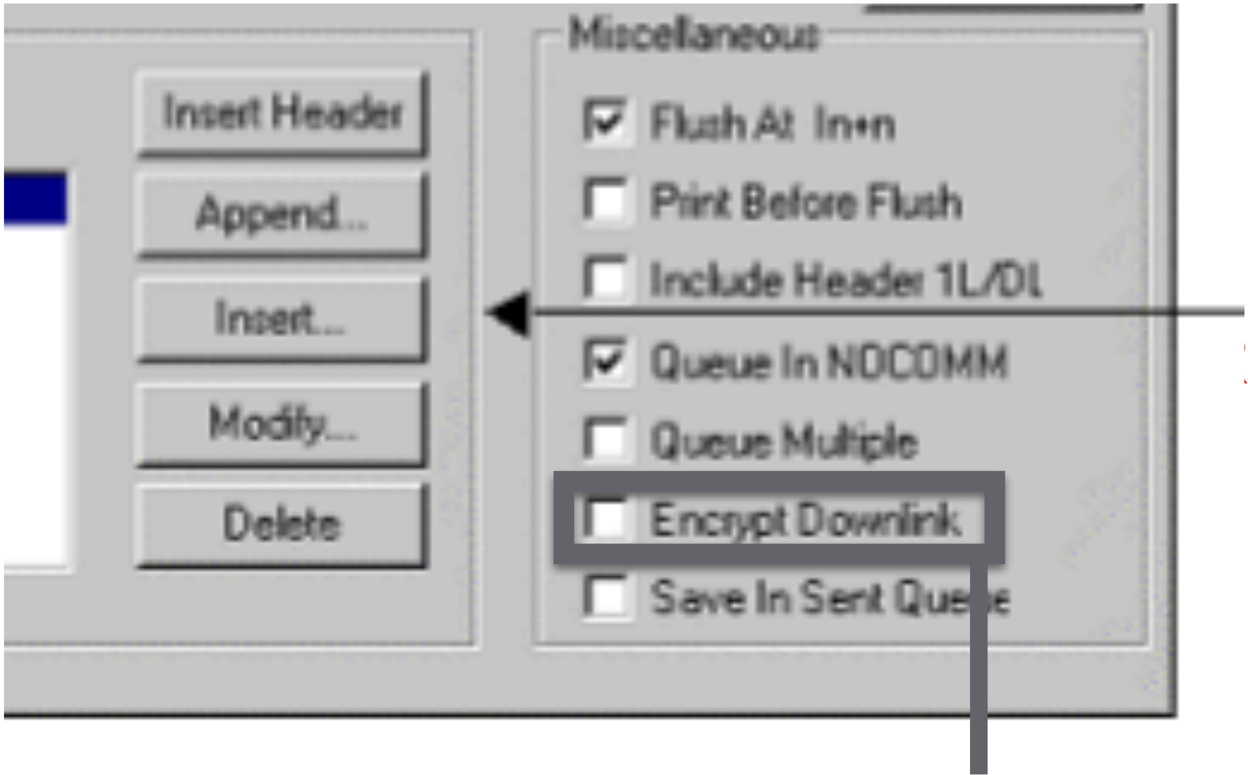
"The obfuscation function described in your research paper does not remediate any of the privacy disclosure observations you claim." - On the claim that this cipher protects sensitive data

"Neither industry standards nor regulations require keys to be recycled" - On the lack of rekeying

[1] **Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS,** *Matthew Smith, Daniel Moser, Martin Strohmeier, Vincent Lenders and Ivan Martinovic.* In *International Conference on Financial Cryptography and Data Security 2017*. Springer. April, 2017.

Example Disclosure: Negative Example

“‘users’
[…] are



☑ Flush At In•n
□ Print Before Flush
□ Include Header 1L/DL
☑ Queue In NDCOMM
□ Queue Multiple
□ Encrypt Downlink
□ Save In Sent Que e

S
RS”

This is the ‘obfuscation’ function as confirmed by vendor in follow up emails

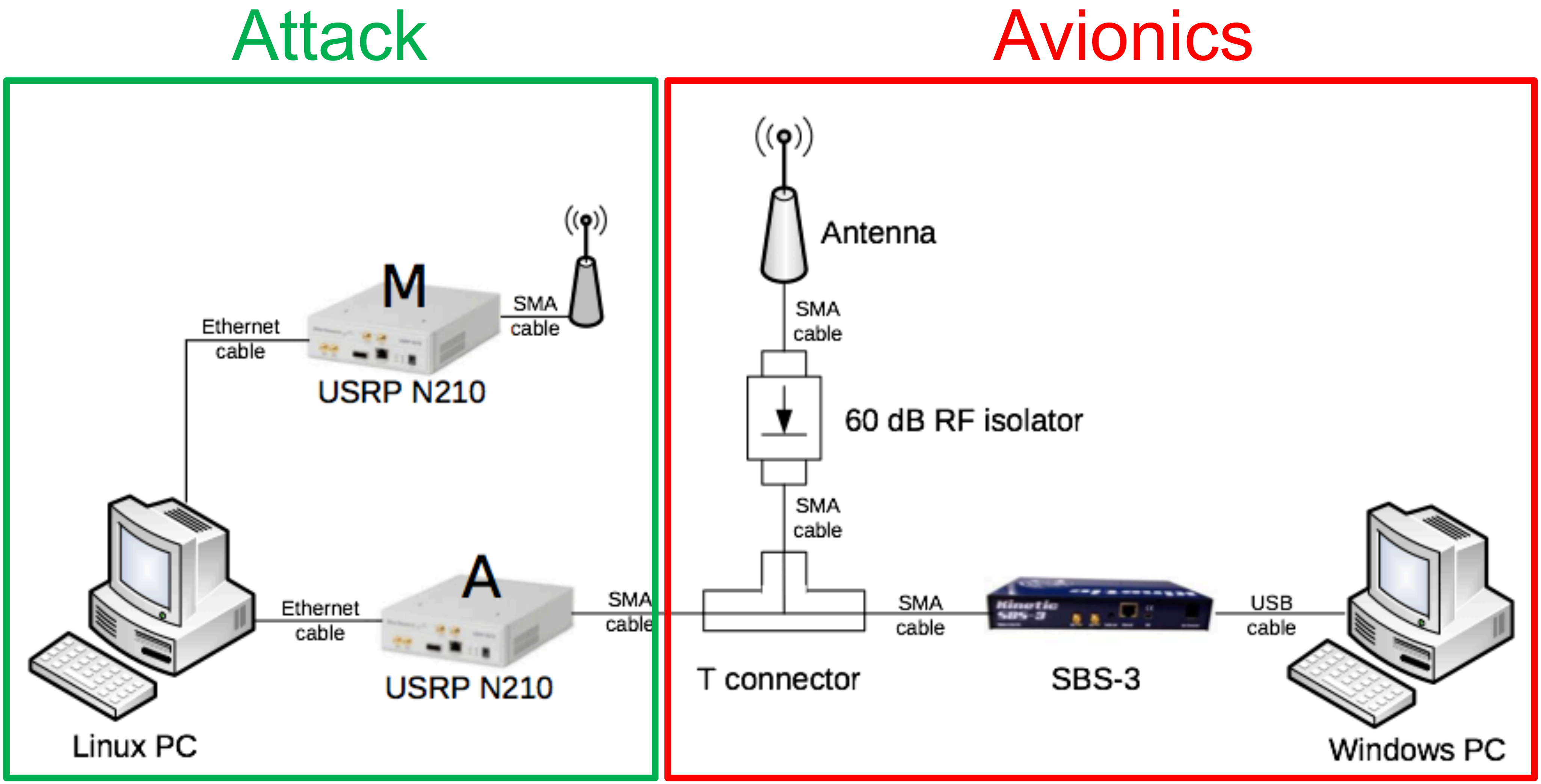
Aviation Security Labs: How To

Original Motivation: Real RF Attacks

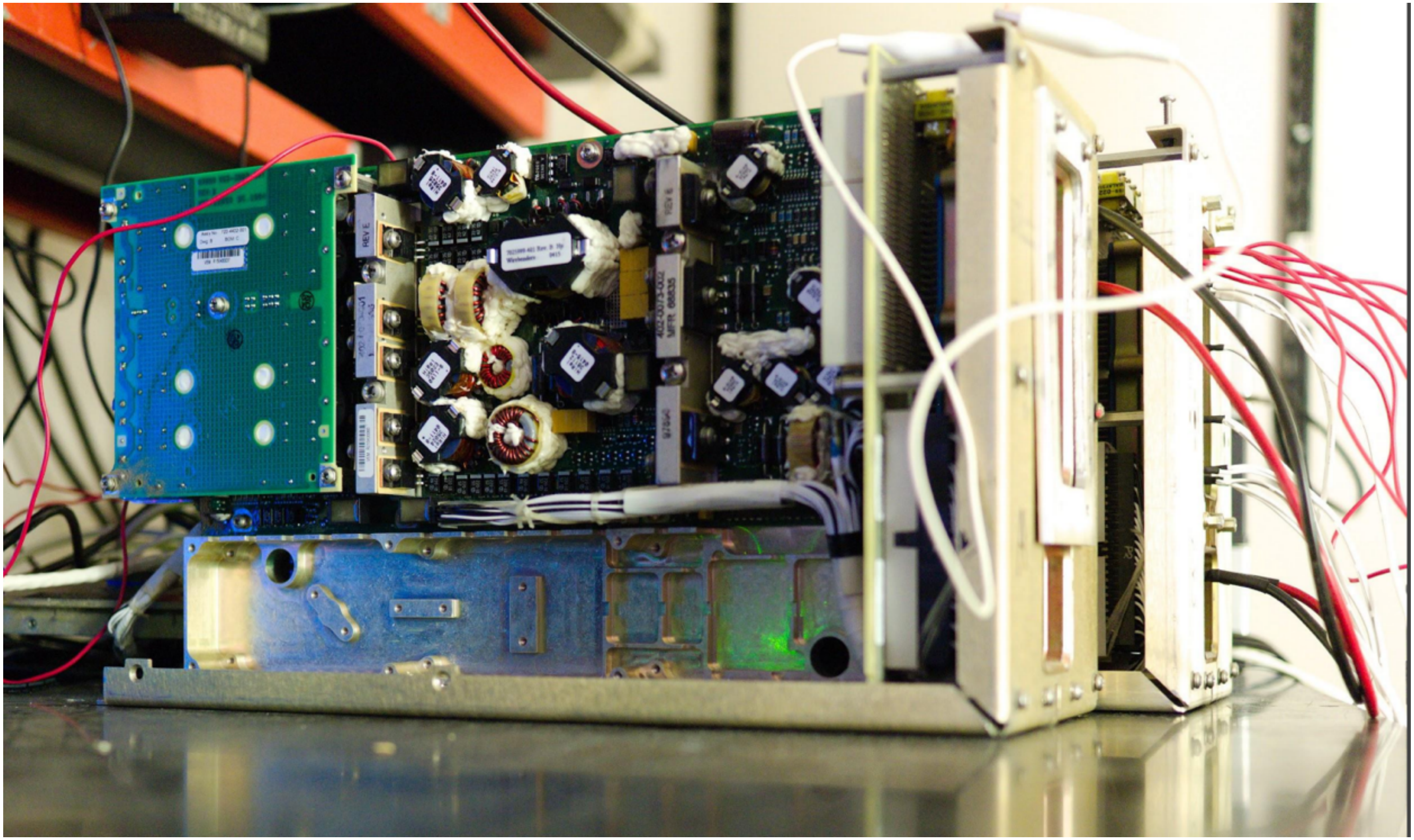
- After a decade of affordable (i.e., non-Electronic Warfare) security research into RF/avionics cyber attacks in aviation
  - ADS-B/Mode S/SSR
  - ACARS
  - MLAT
  - Collision Avoidance
  - …

- Typical responses of aviation experts(?), academic reviewers
  - **“Cannot be done in a real aircraft / ground station”**
  - Redundancy, some black (box) magic will prevent attacks

Until Now: Avionics Simulated with SDRs

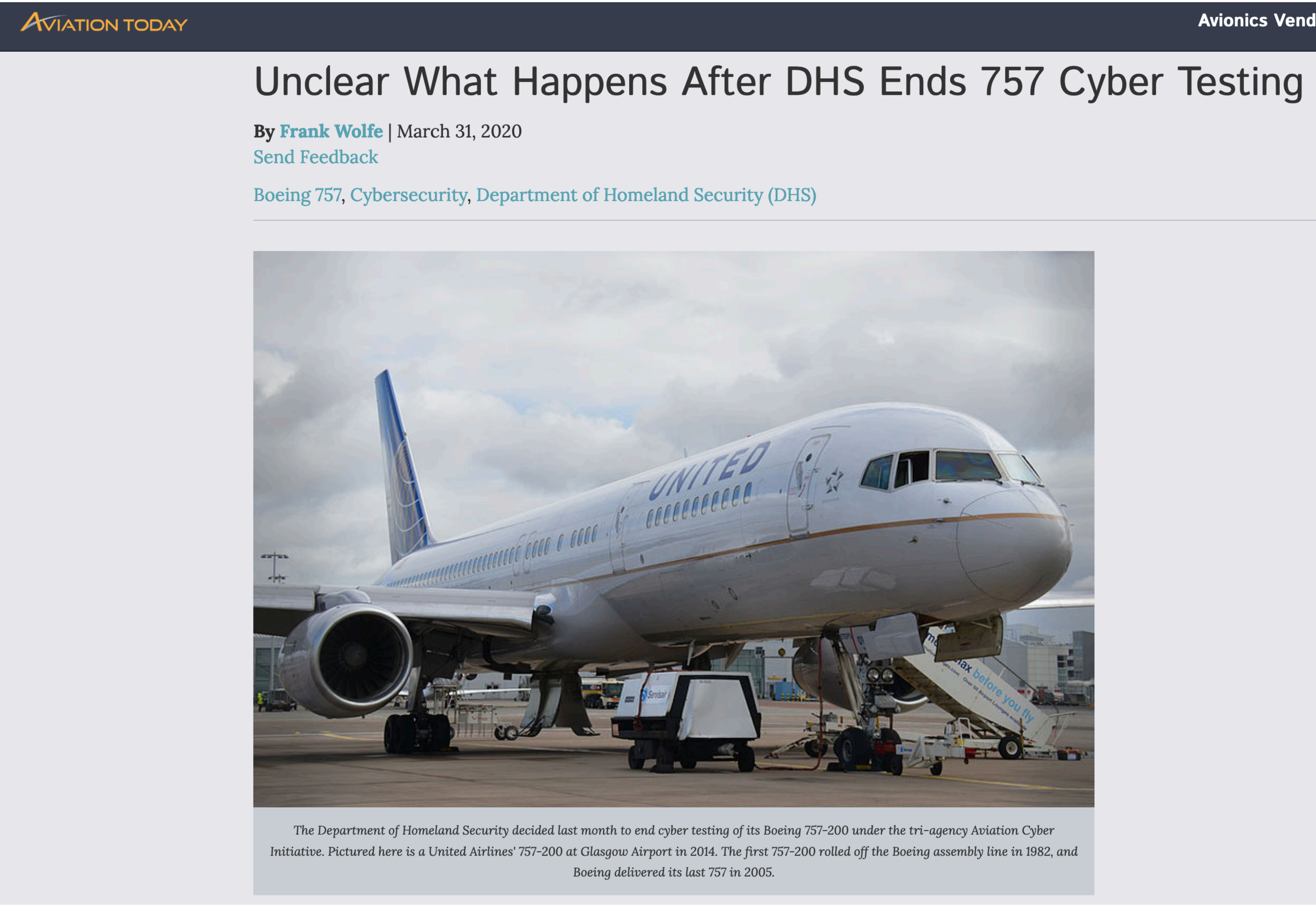


Related Efforts



Crow, Sam, et al. "Triton: A Software-Reconfigurable Federated Avionics Testbed." *12th USENIX Workshop on Cyber Security Experimentation and Test (CSET 19)*. 2019.

Avionics Lab Efforts around the World



Unclear What Happens After DHS Ends 757 Cyber Testing

By Frank Wolfe | March 31, 2020

Send Feedback

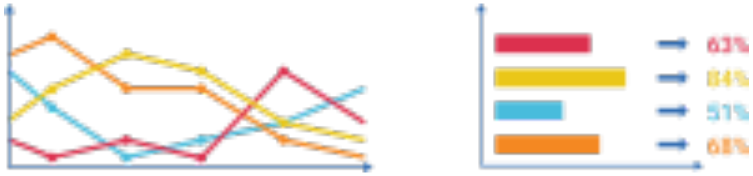
Boeing 757, Cybersecurity, Department of Homeland Security (DHS)

The Department of Homeland Security decided last month to end cyber testing of its Boeing 757-200 under the tri-agency Aviation Cyber Initiative. Pictured here is a United Airlines' 757-200 at Glasgow Airport in 2014. The first 757-200 rolled off the Boeing assembly line in 1982, and Boeing delivered its last 757 in 2005.

Challenges in Building an Avionics Lab

- Novel problem:
  - No references, unchartered (public) research ground
  - Closest similar projects at OEMs such as Airbus, Boeing, Pilatus
    - Not accessible and not really comparable
  - Some avionics manufacturers even boycott testbeds

- Trade-offs:
  - Realism
  - Cost
  - Complexity



- Overall Costs:
  - Quickly in the hundreds of thousands of dollars
  - Serious deliberations to just buy an aircraft…

Martin Strohmeier - Labs and Trust: How to build a successful aviation cybersecurity research programme. Aerospace Village, DEF CON 31.

High-Level Concept of the CYD Lab

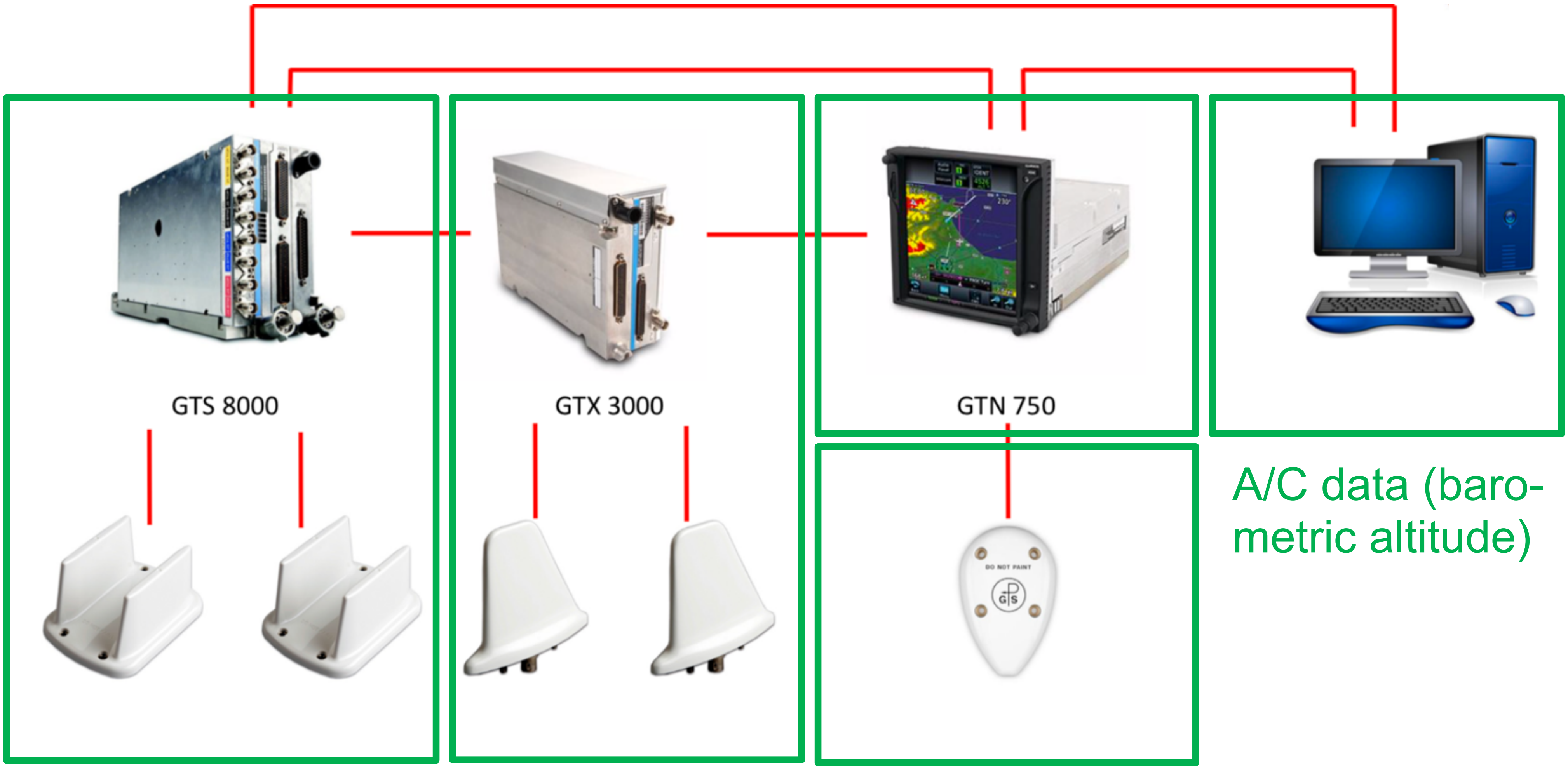
1. **Certified avionics hardware,** believing it is deployed in real aircraft, and conducting real flights

2. **RF interfaces** accessible through antennas

3. **Ability to conduct RF attacks,** including
   - Spoofing, jamming
   - Fuzzy testing of hardware / interfaces

4. **Extensibility**
   - We started with TCAS, ADS-B/SSR transponders, GPS
   - Should be modular, allow for new units/technologies

Concrete Tech View



ARINC 429 Databus

Flight Management System

GTS 8000

GTX 3000

GTN 750

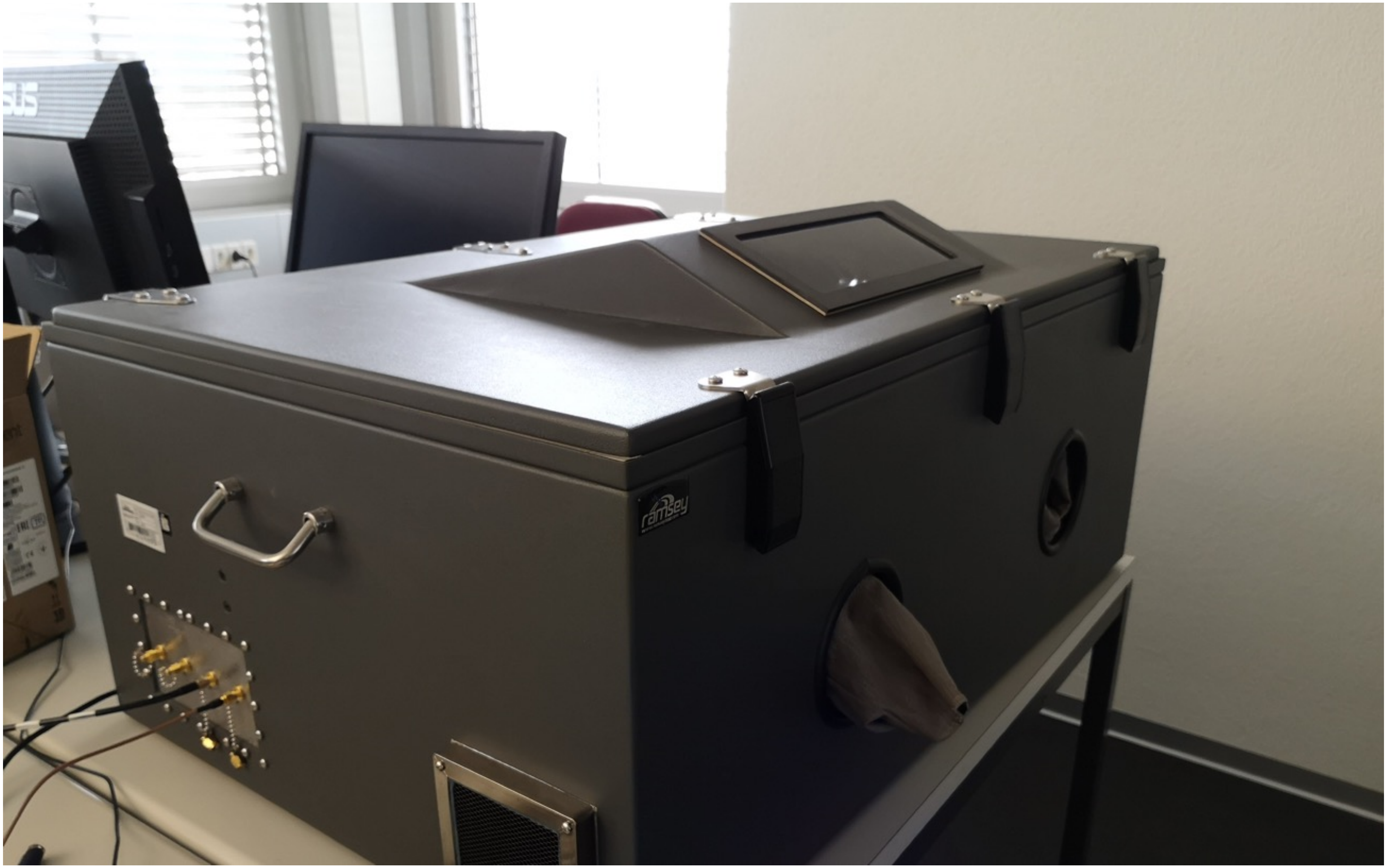
A/C data (barometric altitude)

Collision Avoidance

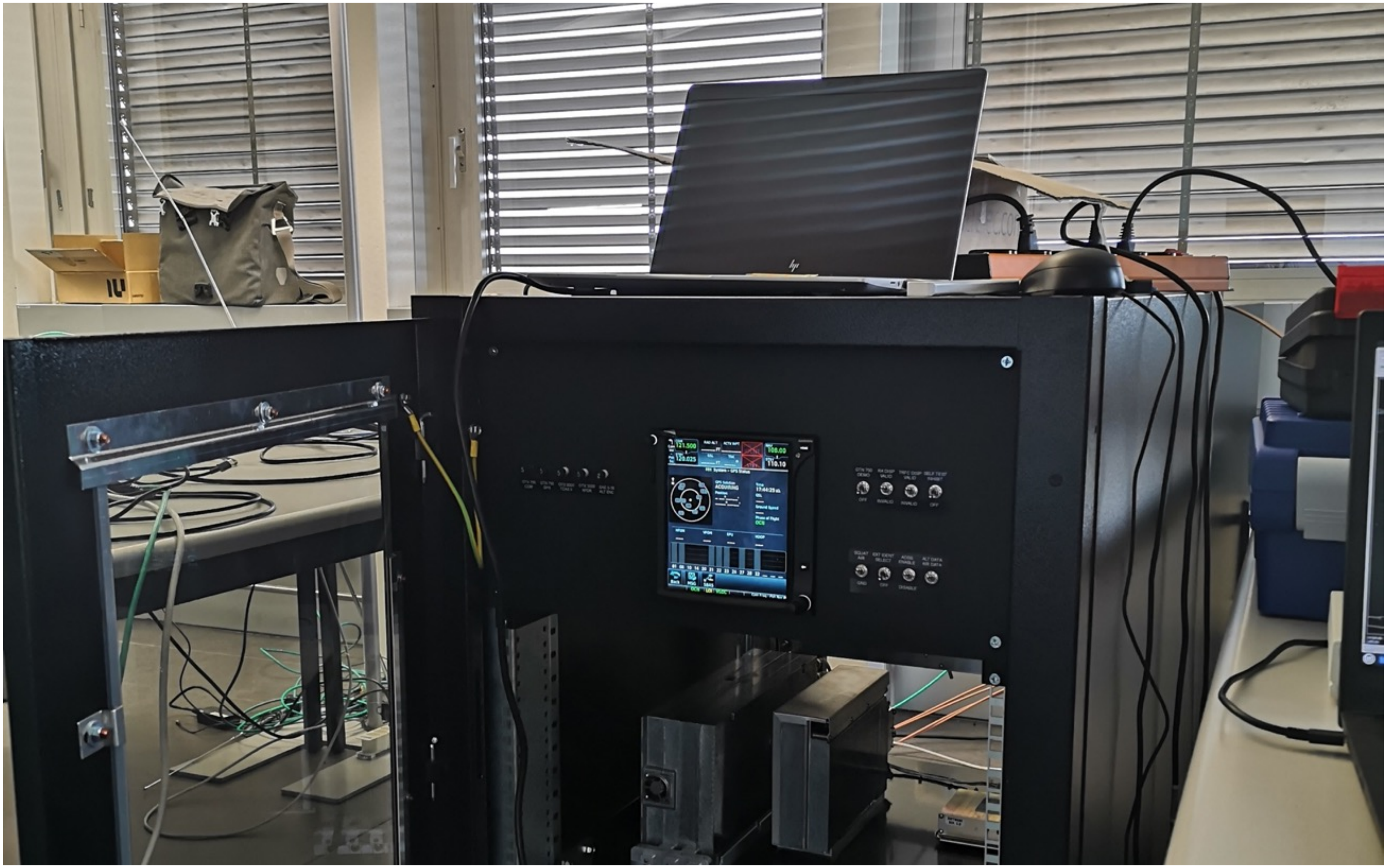
Transponder

GNSS

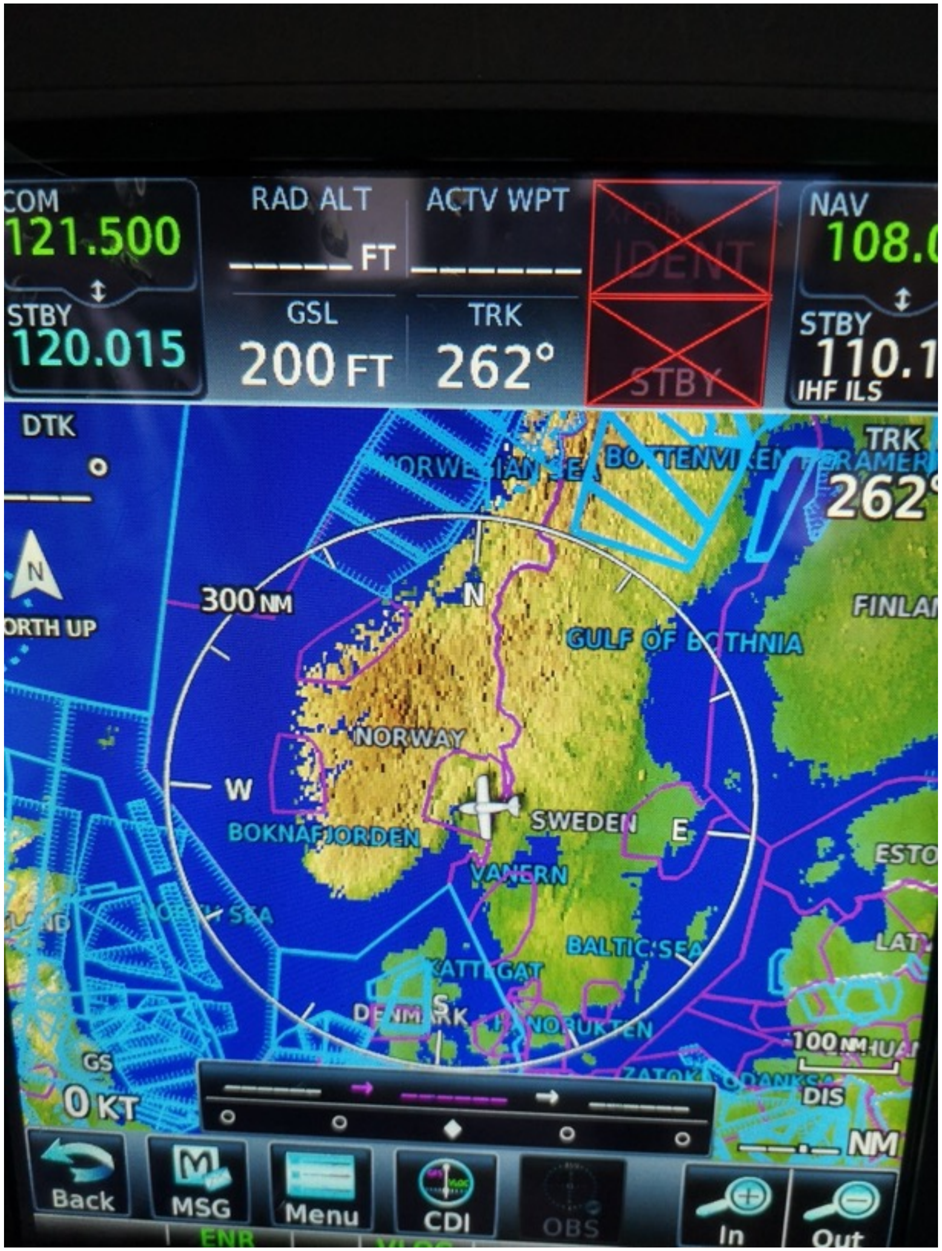
Safety First!

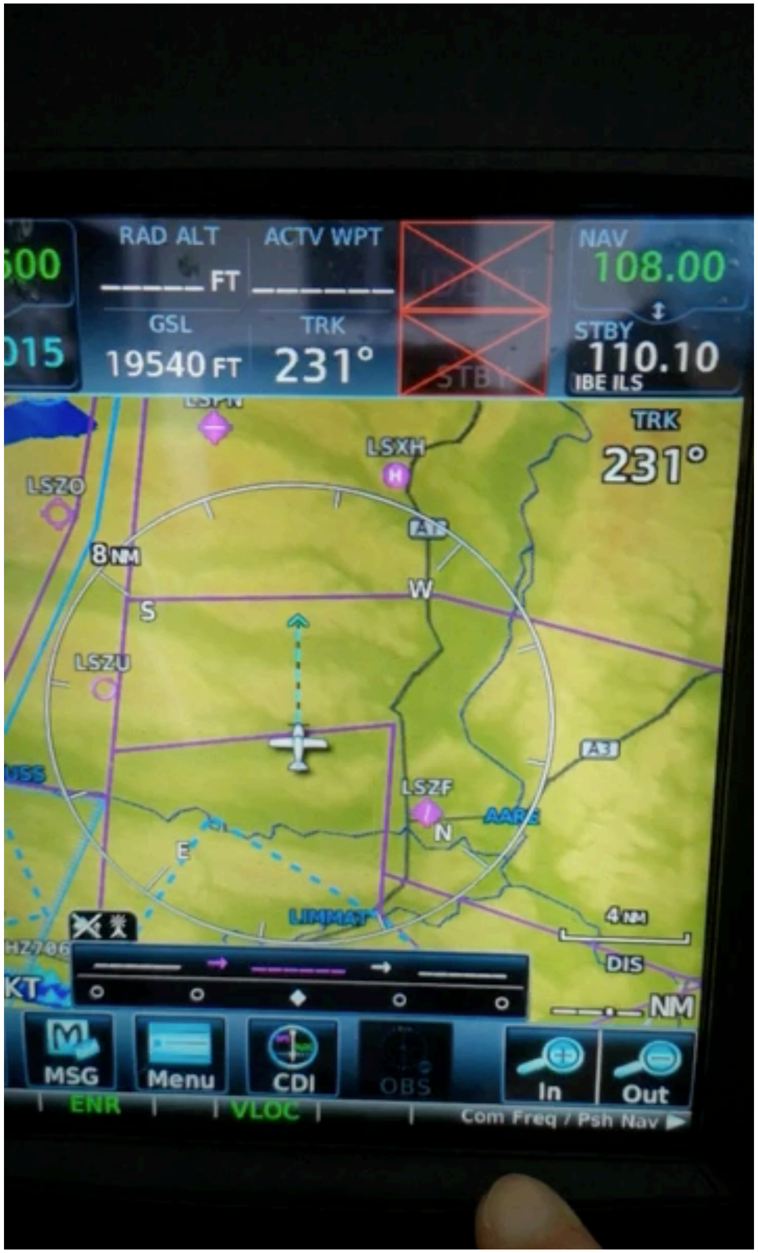


The Original Lab Assembled

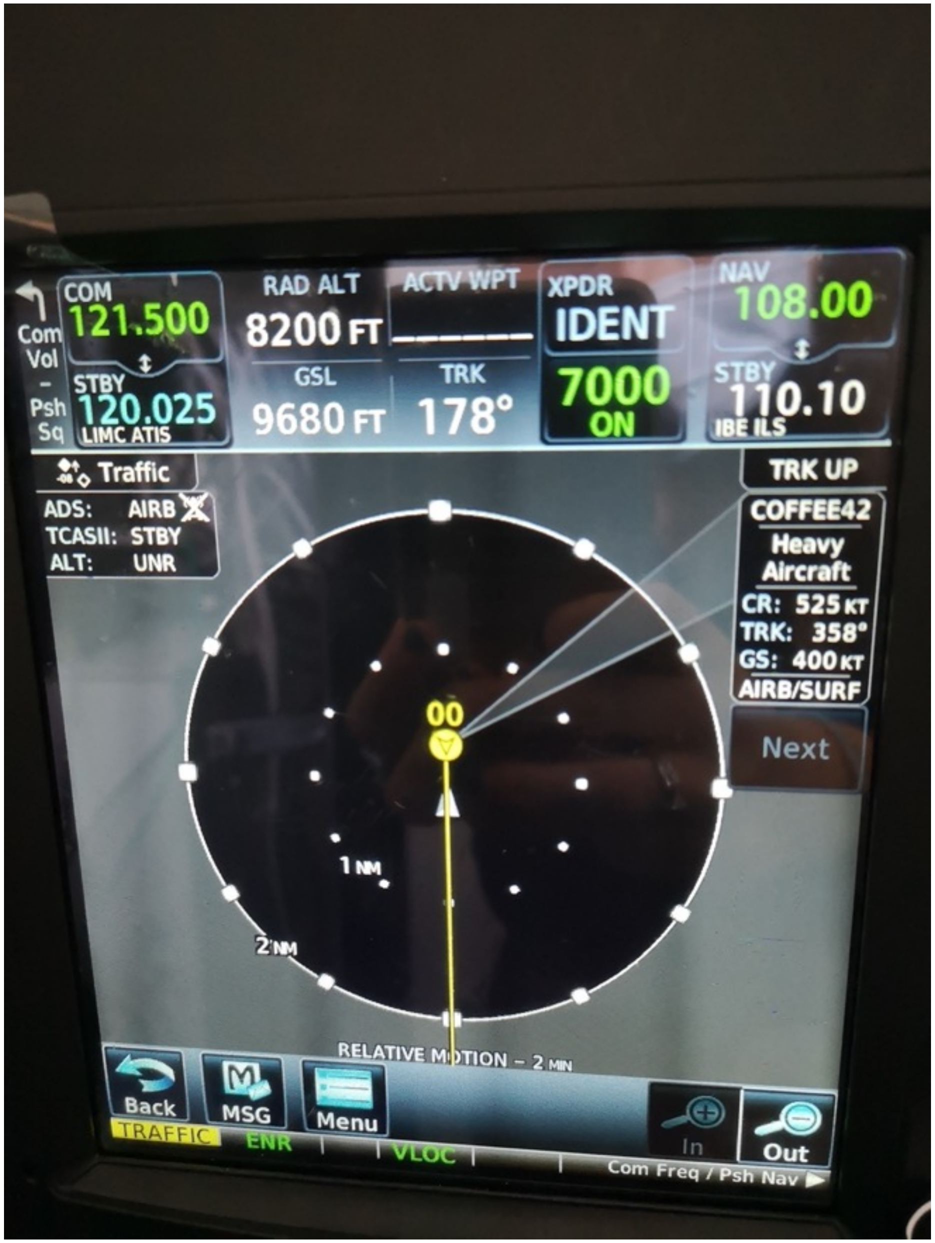


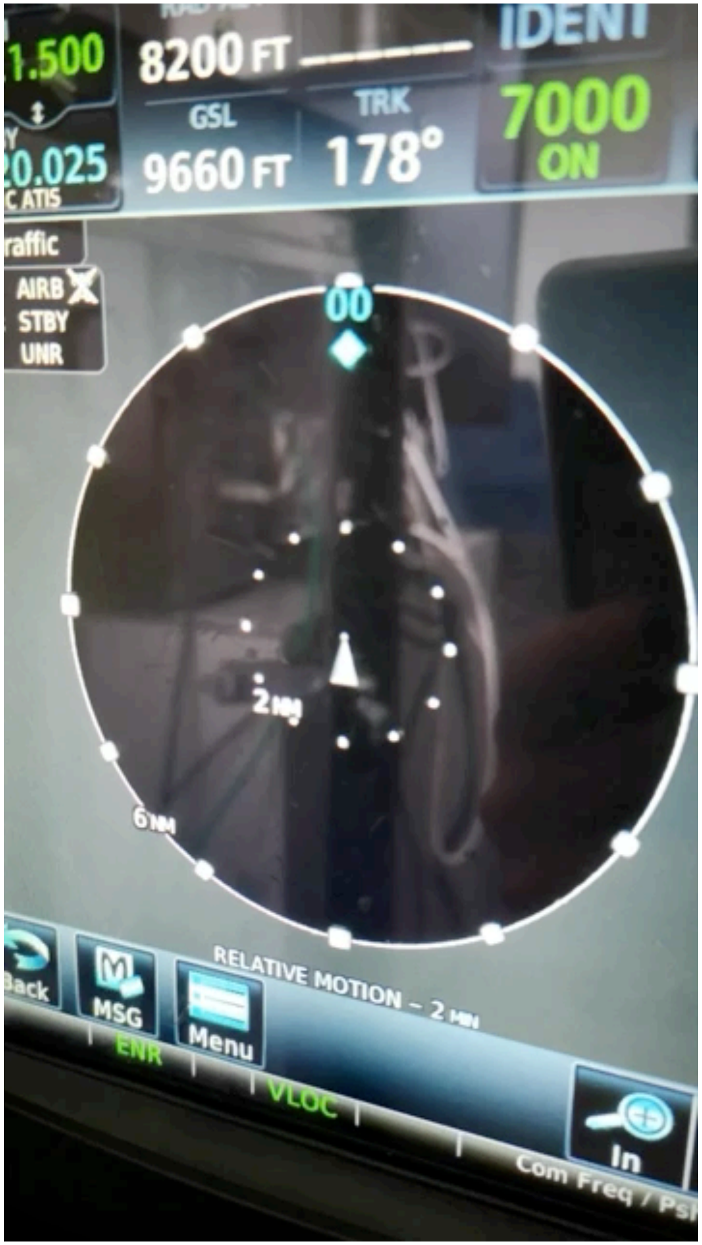
Preliminary Evaluation: GPS Spoofing



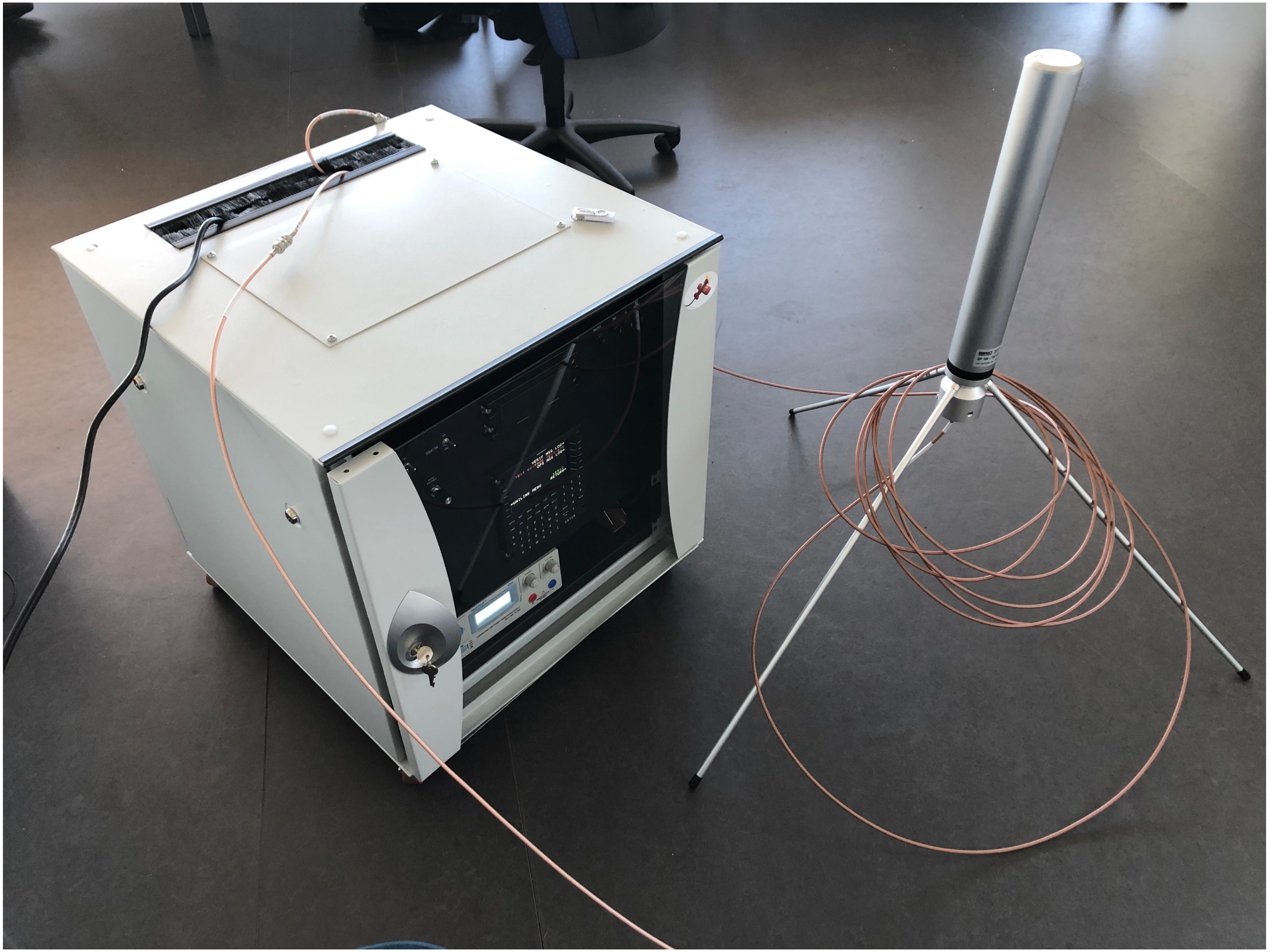


Prelim. Evaluation: ADS-B/TCAS Spoofing

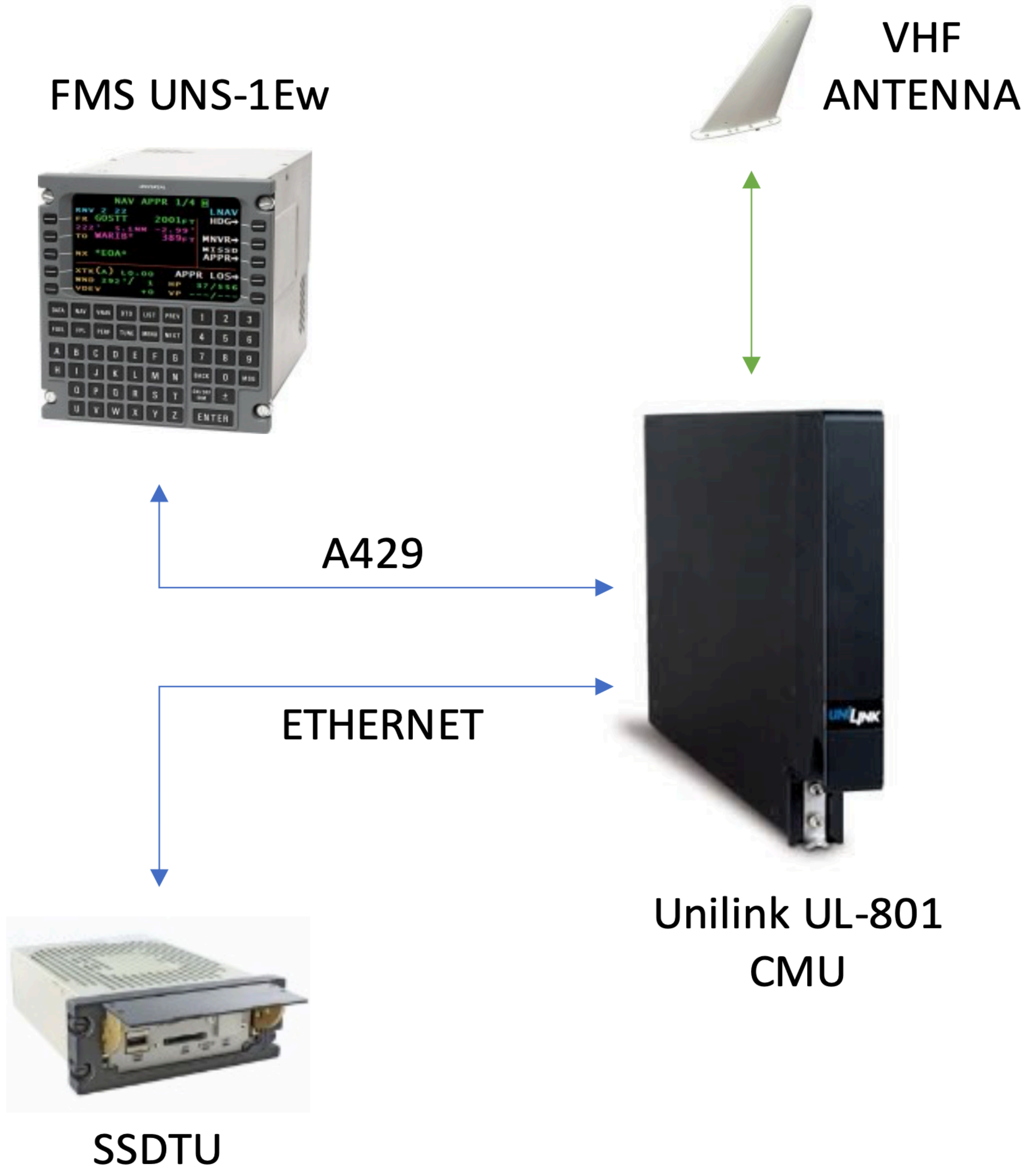


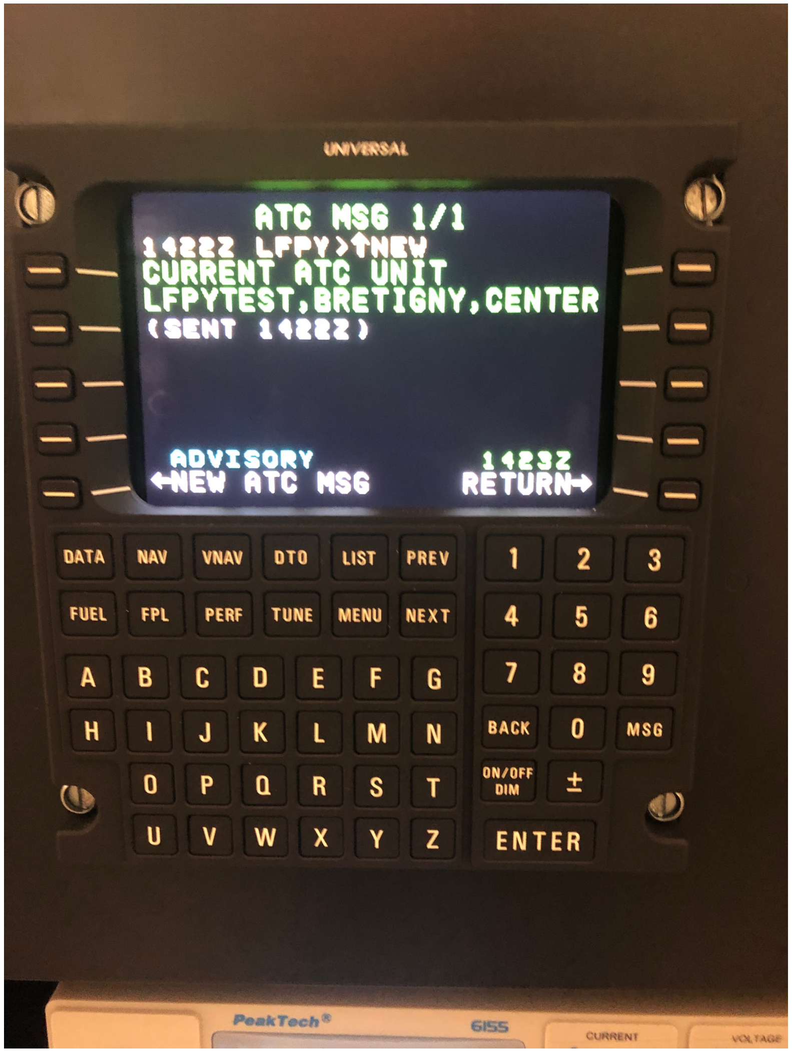


Extension 1: CPDLC



Extension 1: CPDLC

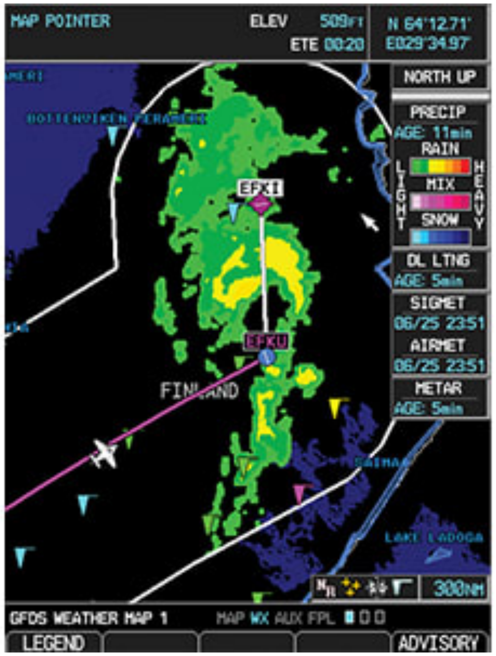


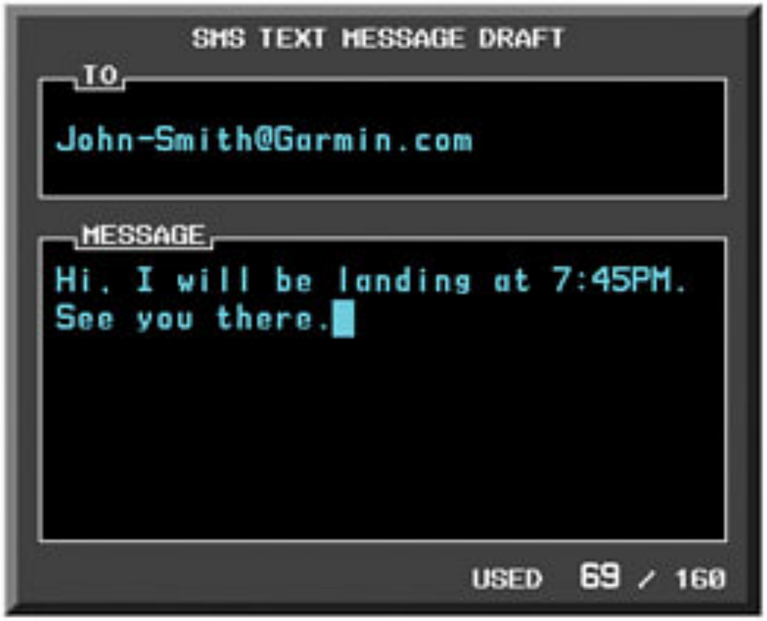

ATC MSG 1/1
1422Z LFPY>↑NEW
CURRENT ATC UNIT
LFPYTEST,BRETIGNY,CENTER
(SENT 1422Z)

ADVISORY 1423Z
←NEW ATC MSG RETURN→

Extension 2: SATCOM/Iridium

GSR 56





SMS TEXT MESSAGE DRAFT

TO

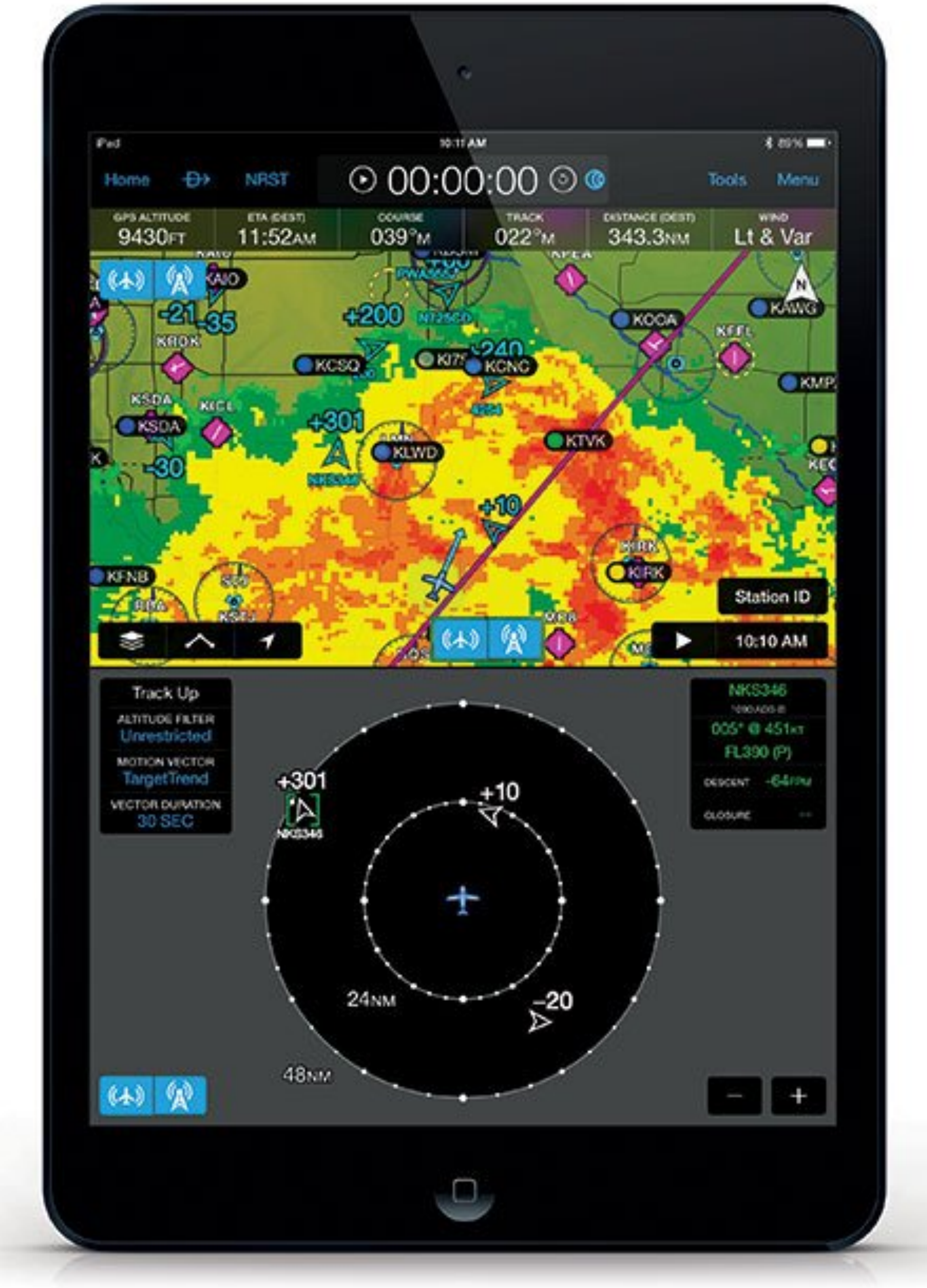
John-Smith@Garmin.com

MESSAGE

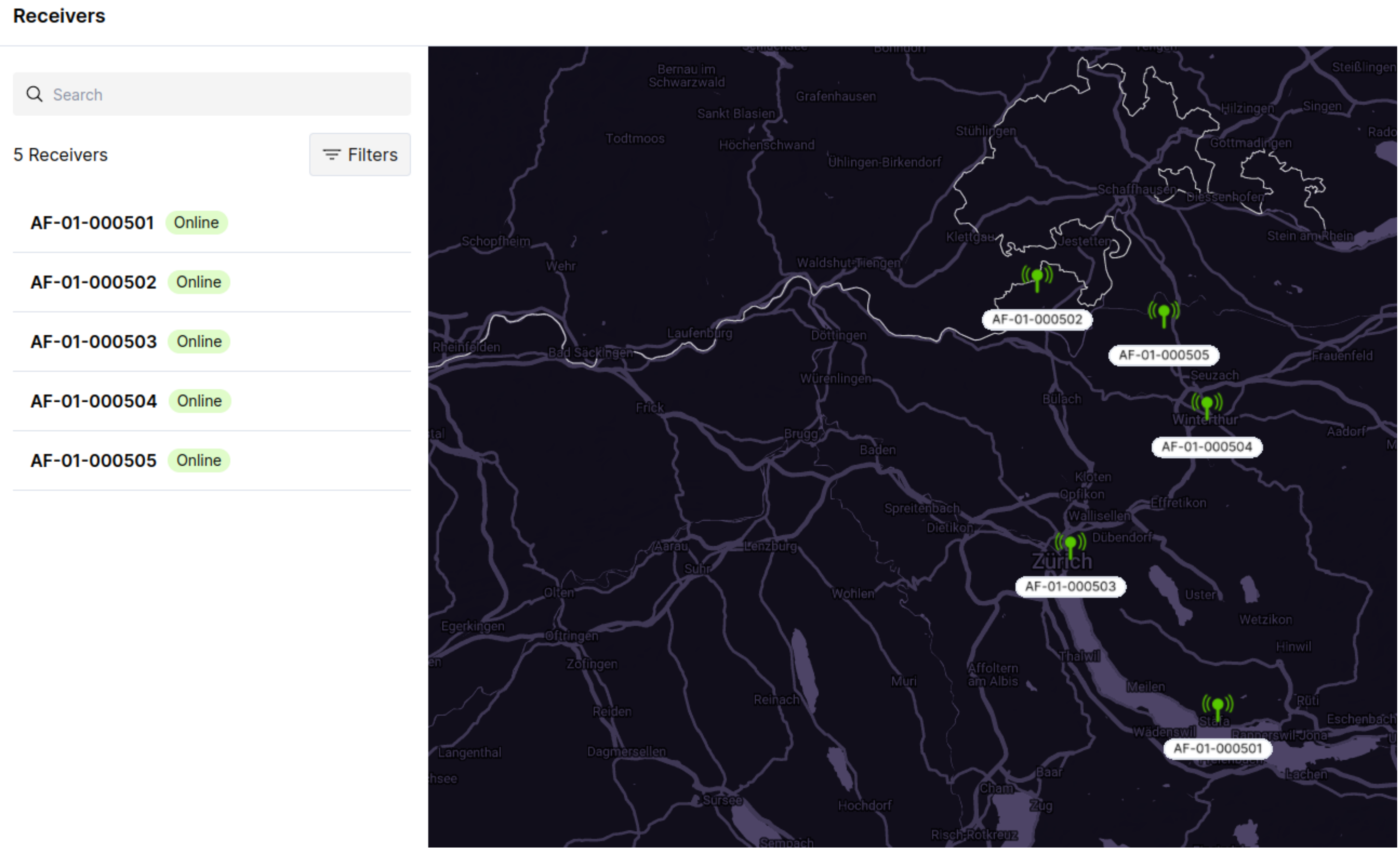
Hi. I will be landing at 7:45PM.
See you there.

USED 69 / 160

Extension 3: Bluetooth/WiFi EFB



Extension 4: MLAT



Receivers

Search

5 Receivers

Filters

AF-01-000501	Online
AF-01-000502	Online
AF-01-000503	Online
AF-01-000504	Online
AF-01-000505	Online

Avionics Lab in Practice

- Used in person already by researchers from
  - University of Genoa (Italy)
  - ENS Lyon (France)
  - Northeastern (US)
  - Many Swiss students (EPFL, ETH, ZHAW)
  - **You?**

- Forthcoming results on all supported technologies
  - CPDLC
  - TCAS
  - ARINC 429
  - Iridium
  - MLAT

Takeaways

1 **Building trust is hard but necessary and worth it**

Do good work, build and leverage personal connections (e.g., those made at the village) to produce meaningful and impactful research.

2 **Simulations are great but we need to take the leap!**

Lots of radio-frequency security research has been conducted in simulated hardware/software but no (public) real-world tests are available.

3 **Our lab is certified and supports radio communication!**

To overcome the doubters, our lab supports real-world RF research (and more) with certified avionics hardware.

4 **It’s for research - contact us!**

It is available for collaboration and we would love to do research with you.

Contact: Martin.Strohmeier@armasuisse.ch

References (1)

Building an Avionics Laboratory for Cybersecurity Testing, *Martin Strohmeier, Leeloo Granger, Giorgio Tresoldi and Vincent Lenders.* In *15th ACM Workshop on Cyber Security Experimentation and Test (CSET)*. August, 2022.

Security and Privacy Issues of Satellite Communication in the Aviation Domain, *Georg Baselt, Martin Strohmeier, James Pavur, Vincent Lenders and Ivan Martinovic.* In *Cyber Conflict (CYCON), 2022 14th International Conference on*. May, 2022.

On the Security of the FLARM Collision Warning System, *Boya Wang, Giorgio Tresoldi, Martin Strohmeier and Vincent Lenders.*In *Proceedings of the 2022 ACM Asia Conference on Computer and Communications Security*. May, 2022.

You talkin' to me? Exploring Practical Attacks on Controller Pilot Data Link Communications, *Joshua Smailes, Daniel Moser, Matthew Smith, Martin Strohmeier, Vincent Lenders and Ivan Martinovic.* In *Proceedings of the 7th ACM Cyber−Physical System Security Workshop (CPSS 2021)*. June, 2021.

A Tale of Sea and Sky: On the Security of Maritime VSAT Communications, *James Pavur, Daniel Moser, Martin Strohmeier, Vincent Lenders and Ivan Martinovic.* In *2020 IEEE Symposium on Security and Privacy (S&P)*. IEEE. May, 2020.

A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems, *Matthew Smith, Martin Strohmeier, Jon Harman, Vincent Lenders and Ivan Martinovic.* In *The Network and Distributed System Security Symposium (NDSS)*. February, 2020.

Crowdsourcing Security for Wireless Air Traffic Communications, Martin Strohmeier, Matthew Smith, Matthias Schäfer, Vincent Lenders and Ivan Martinovic. In *Cyber Conflict (CYCON), 2017 9th International Conference on*. IEEE. June, 2017.

References (2)

On Perception and Reality in Wireless Air Traffic Communications Security, Martin Strohmeier, Matthias Schäfer, Rui Pinheiro, Vincent Lenders, and Ivan Martinovic. In IEEE Transactions on Intelligent Transportation Systems. June, 2017.

On the Security and Privacy of ACARS. Matt Smith, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. *Integrated Communications Navigation and Surveillance (ICNS)*. 2016.

Intrusion Detection for Airborne Communication using PHY−Layer Information, Martin Strohmeier, Vincent Lenders and Ivan Martinovic. In *Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)*. July, 2015.

On the Security of the Automatic Dependent Surveillance−Broadcast Protocol. Martin Strohmeier, Vincent Lenders and Ivan Martinovic. *IEEE Communications Surveys & Tutorials*. 2015.

Realities and Challenges of NextGen Air Traffic Management: The Case of ADS−B. Martin Strohmeier, Matthias Schäfer, Vincent Lenders and Ivan Martinovic. In *IEEE Communications Magazine.* Vol. 52. No. 5. 2014.

Bringing Up OpenSky: A Large−scale ADS−B Sensor Network for Research. Matthias Schäfer, Martin Strohmeier, Vincent Lenders, Ivan Martinovic and Matthias Wilhelm. In *ACM/IEEE International Conference on Information Processing in Sensor Networks* (IPSN). April, 2014.

Experimental Analysis of Attacks on Next Generation Air Traffic Communication. Matthias Schaefer, Vincent Lenders and Ivan Martinovic.
In Proceedings of the *11th International Conference on Applied Cryptography and Network Security* (ACNS). 2013.