Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse
Science and Technology

CYD
CYBER DEFENCE CAMPUS

Building an Avionics Laboratory for Cybersecurity Testing

15th Cyber Security Experimentation and Test Workshop

Martin Strohmeier[1], Leeloo Granger[2], Giorgio Tresoldi[1], Vincent Lenders[1]

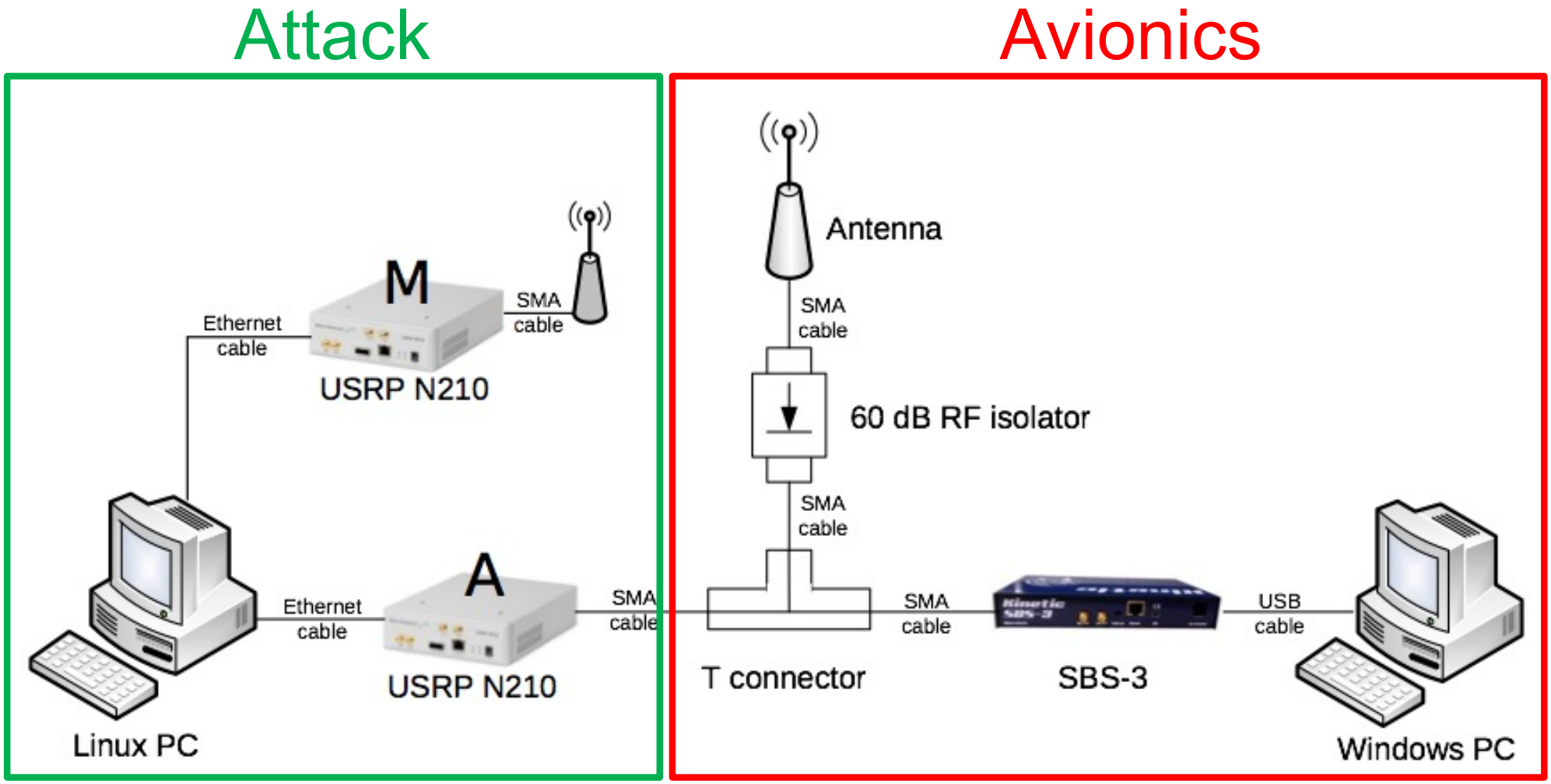
[1] Cyber-Defence Campus [2] EPFL

Motivation: (Almost) Real RF Attacks

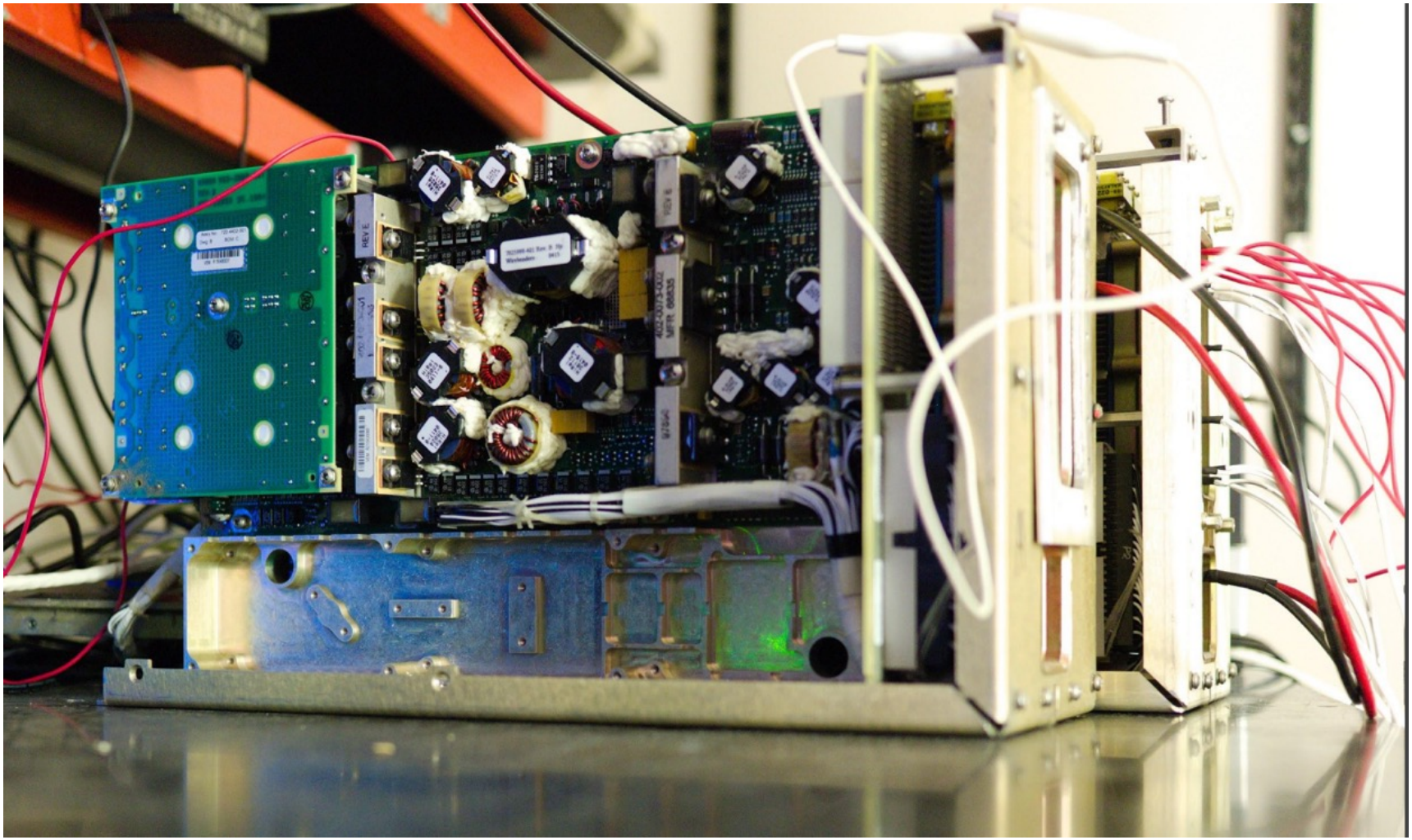
- > Decade of affordable (i.e., non-Electronic Warfare) security research into RF/avionics cyber attacks in aviation
  - ADS-B/Mode S/SSR
  - ACARS
  - MLAT
  - Collision Avoidance
  - …

- 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.

Related Efforts

Martin Strohmeier - Building an Avionics Labora

Hackers just found serious vulnerabilities in F-15 fighter jet

An F-15C fighter jet on a runway in Keflavik, Iceland, Wednesday, Aug. 15, 2018.
MARTIN EGNASH/STARS AND STRIPES

BUY PHOTO

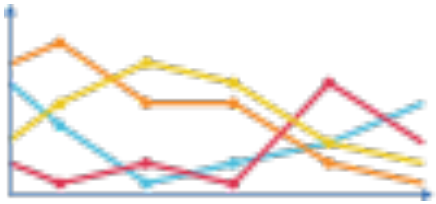
By JOSEPH MARKS | The Washington Post | Published: August 14, 2019

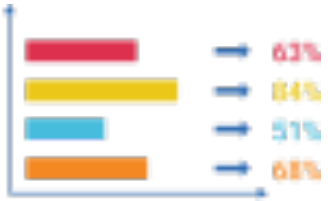
LAS VEGAS — In a Cosmopolitan hotel suite 16 stories above the Def Con cybersecurity conference, a team of highly vetted hackers tried to sabotage a vital flight system for a U.S. military fighter jet. And they succeeded.

Building the Cyber Avionics Lab

Challenges

- Novel problem:
  - No references, unchartered 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…

High-Level Concept

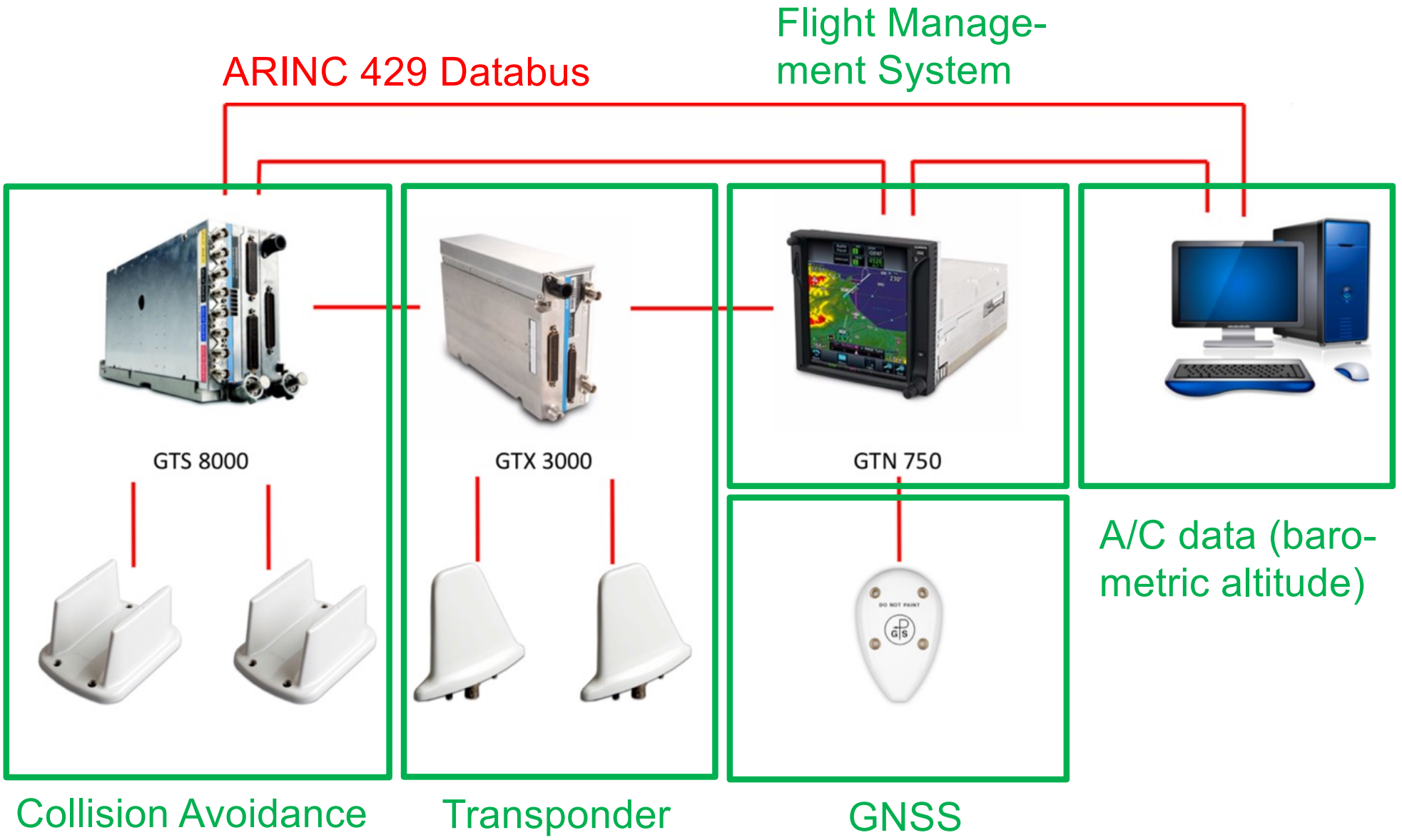
1. **Certified avionics hardware,** believing it is deployed in real aircraft, and conducting real flights

2. **RF interfaces** accessible through antennas

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

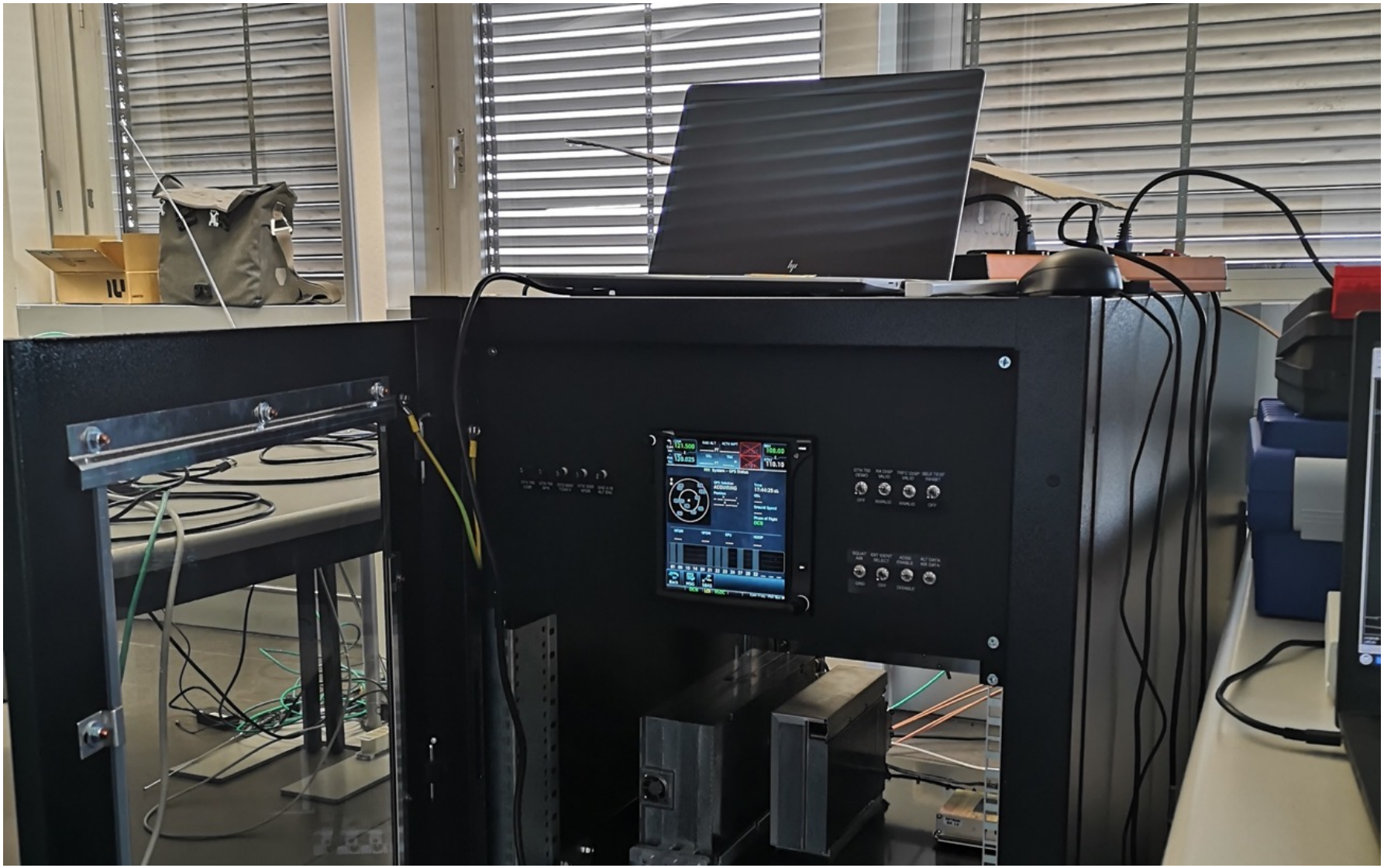
4. **Extensibility**
   - We started with TCAS, ADS-B/SSR transponders, GPS
   - Current extensions include CPDLC, Electronic Flightbags, Satellite Internet/Phone

Low-Level Tech View

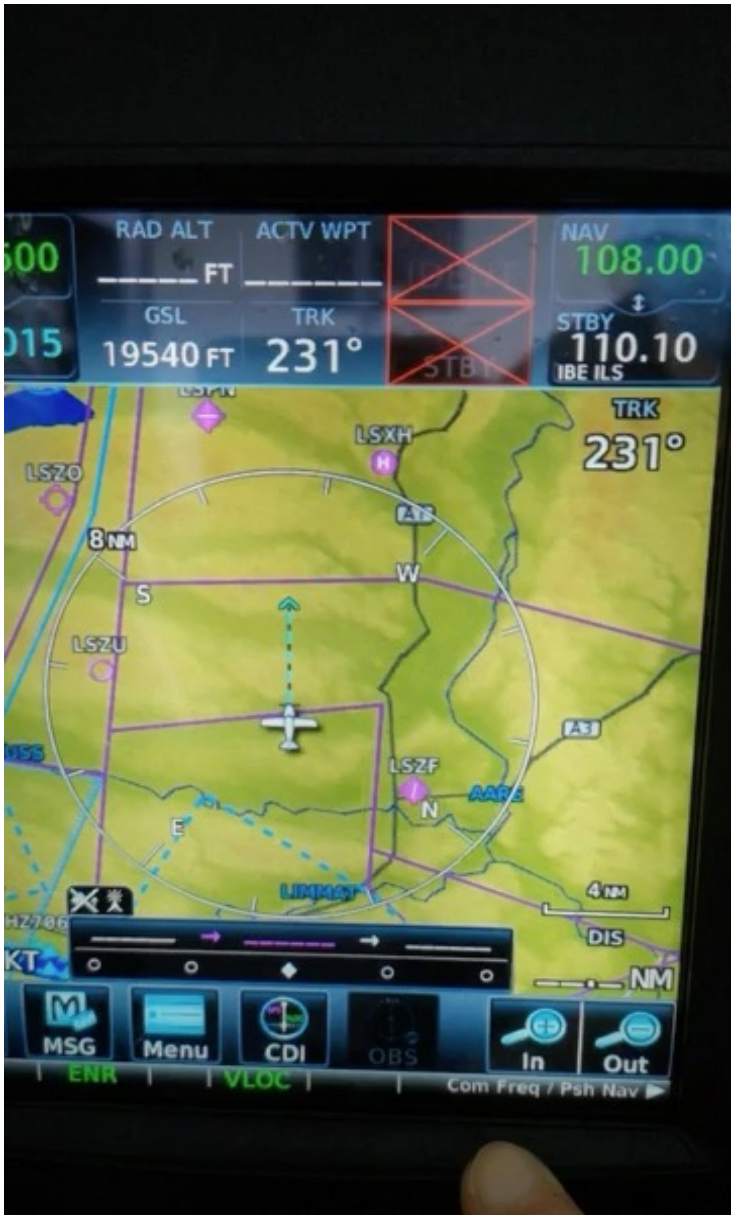


Safety First!

The Assembled Lab



Preliminary Evaluation: GPS Spoofing



Prelim. Evaluation: ADS-B/TCAS Spoofing

Takeaways

1 **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.

2 **It's certified and supports radio communication!**

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

3 **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