Università di Genova | DIBRIS DIPARTIMENTO DI INFORMATICA, BIOINGEGNERIA, ROBOTICA E INGEGNERIA DEI SISTEMI

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung
Bevölkerungsschutz und Sport
armasuisse
Wissenschaft und Technologie

CYD CYBER DEFENCE CAMPUS

On a Collision Course: Unveiling Wireless Attacks to the Aircraft Traffic Collision Avoidance System (TCAS)

Giacomo Longo [1], Martin Strohmeier [2], Enrico Russo [1], Alessio Merlo [3], Vincent Lenders [2]

1 Department of Informatics Bioengineering Robotics and Systems Engineering (DIBRIS), University of Genova, Italy
2 Cyber-Defence Campus, armasuisse Science + Technology, Switzerland
3 Centre for Defense Higher Studies, Ministry of Defence, Italy

Traffic Collision Avoidance System (TCAS)

What

TCAS is the last line of defence against **mid air collisions**

Mandatory in EU & US for practically every* plane

It operates **automatically**, over **radio**

* > 5700 kg or more than 19 passengers

Traffic Collision Avoidance System (TCAS)

Core functions

Surveillance

Surveillance replicates the functionality of a tower to provide situational awareness.

- Aircraft periodically announce their presence via broadcasts

Surveillance

Surveillance replicates the functionality of a tower to provide situational awareness.

- Aircraft periodically announce their presence via broadcasts
- If a new aircraft is found, it is **interrogated** to determine its range, altitude, and capabilities

Surveillance

Surveillance replicates the functionality of a tower to provide situational awareness.

- Aircraft periodically announce their presence via broadcasts
- If a new aircraft is found, it is **interrogated** to determine its range, altitude, and capabilities

Traffic Advisory (TA)

TAs are sent to the cockpit whenever an aircraft comes too close.

Resolution Advisory (RA)

RAs indicate that a TA aircraft is now in a critical position.

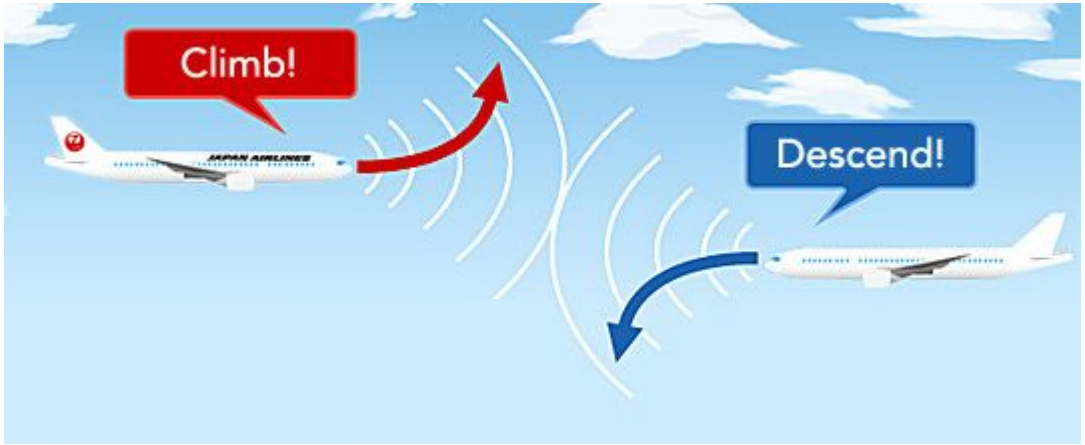
It results in an **advisory**, a command sent to the pilots

The ability to issue RA has been introduced with version II of TCAS

Resolution Advisory (RA)

TCAS II resolves conflicts by ordering **climbs** or **descents.**

Those advisories **must be followed** with some aircrafts even doing so automatically



Security of TCAS

Legacy RF protocol

- Collaborative
- No authentication nor confidentiality measures
- Regulations and standards are available to the public

Università di Genova
DIBRIS DIPARTIMENTO DI INFORMATICA, BIOINGEGNERIA, ROBOTICA E INGEGNERIA DEI SISTEMI

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung Bevölkerungsschutz und Sport
armasuisse
Wissenschaft und Technologie

CYD CYBER DEFENCE CAMPUS

Attacks to TCAS

Inducing a TA

Implementing a transponder

Triggering an RA

Air to Air negotiation

RAs are induced by starting a negotiation.

In case of conflicts the one with the **lowest address wins**.

RAs can be started by any aircraft perceiving another as dangerous

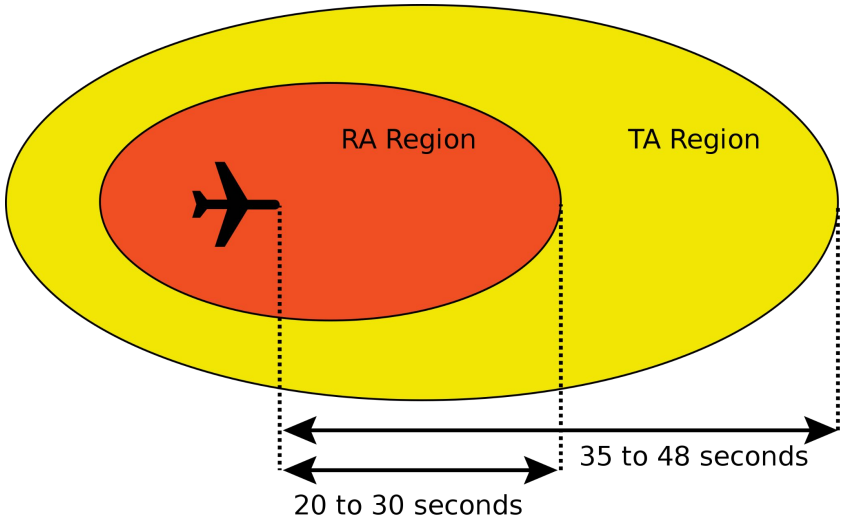
Disabling TCAS remotely

Sensitivity

Each TCAS operates at a given sensitivity level (1-7).

Level is automatically selected depending on **altitude**.

Higher levels increase the protected volume area



Disabling TCAS remotely

Sensitivity Level Command RA DoS

Ground stations can **lower** the sensitivity level, overriding any pre-existing value.

In particular, they can set sensitivity to Level 2 (Disable resolution advisory) inducing a **complete loss of collision avoidance capability**

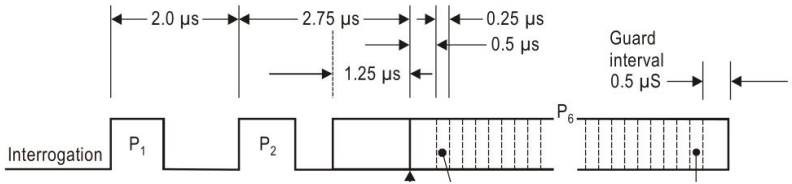
The crew can't restore it without a **power cycle**

Timing is everything

An interrogation cycle

TCAS to TCAS leverages a transport layer called "Mode-S"

Interrogation

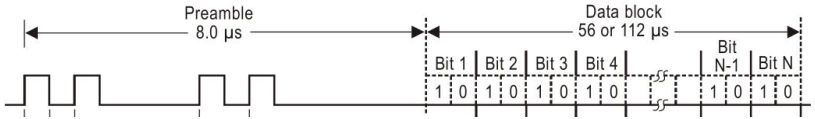


Uplink on 1030MHz (2 MBit/s, 56 or 112 bits)

An interrogation cycle

TCAS to TCAS leverages a transport layer called "Mode-S"

Response



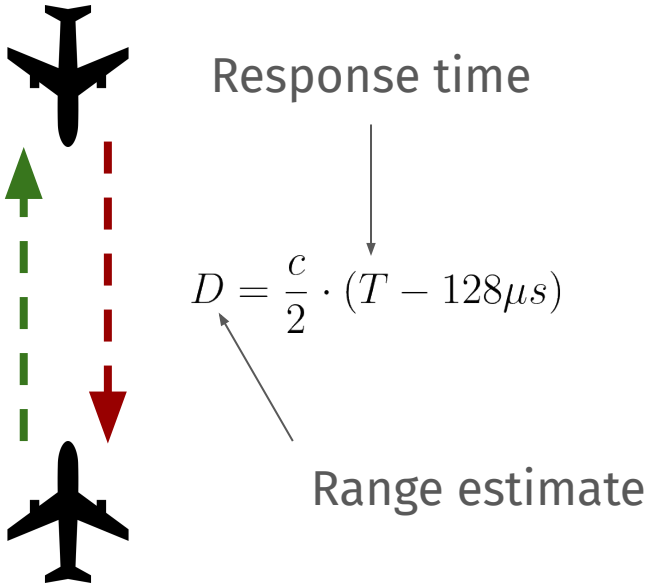
Downlink on 1090MHz (1 MBit/s, 56 or 112 bits)

UniGe | DIBRIS CYD CYBER DEFENCE CAMPUS

An interrogation cycle

Interrogation

Response



An unintentional physical security feature

Range estimation

Range estimation acts as a de-facto physical security feature.

128 microsecond is an extremely short time, **even for a computer**.

Secondary timing problems

Coherence, jitter, and precision

Other than meeting such timing constraint, attackers must

- **Transmit coherently** across two channels
- **Maintain low jitter** (~900ns) across different interrogations
  - I.e. the aircraft should not change its range between interrogations
- **Reply to multiple** interrogations in order to complete the protocol
  - Correct decoding of the received interrogation

Università di Genova
DIBRIS DIPARTIMENTO DI INFORMATICA, BIOINGEGNERIA, ROBOTICA E INGEGNERIA DEI SISTEMI

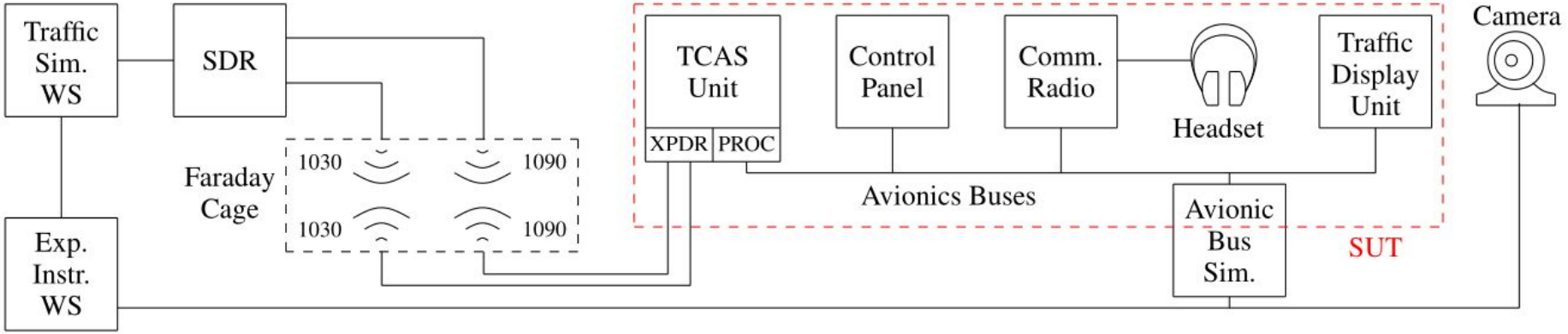
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung Bevölkerungsschutz und Sport
armasuisse
Wissenschaft und Technologie

CYD CYBER DEFENCE CAMPUS

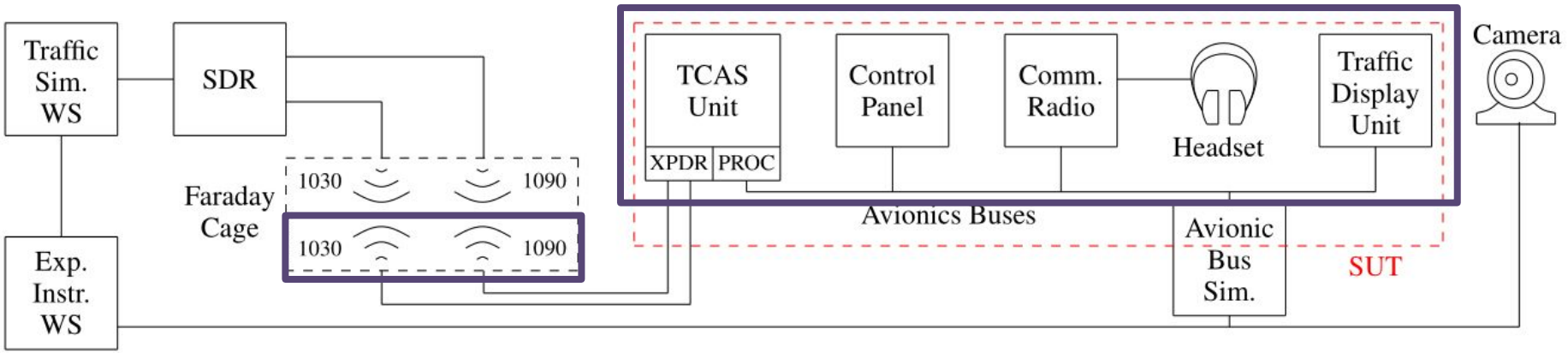
A TCAS Testbed

Generic testbed architecture



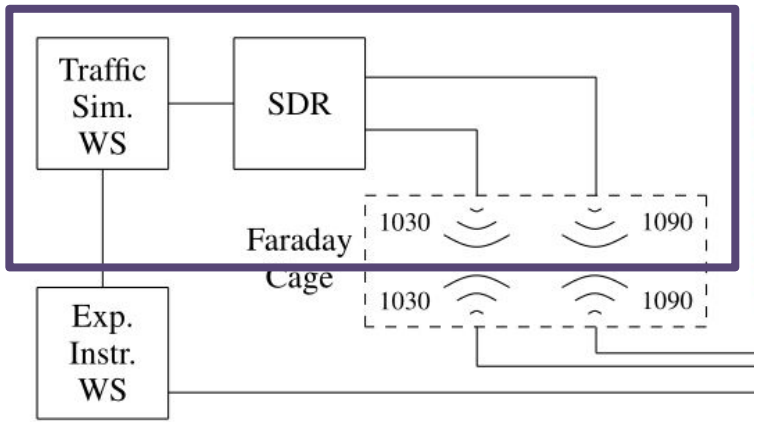
Testbed architecture

TCAS



Testbed architecture

Attacker

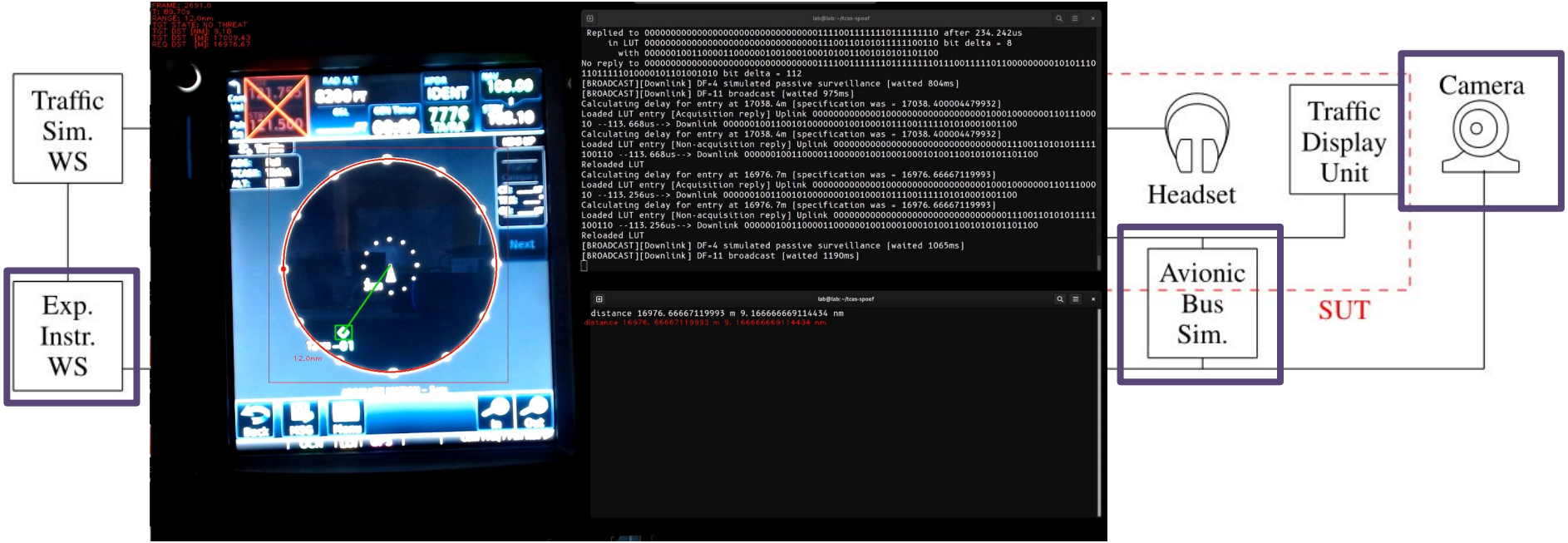


Software Defined Radio (SDR)

- ~10000 EUR
- COTS devices
- Can be programmed by people with mixed Electrical+Computer engineering background
- Going to get cheaper in the future

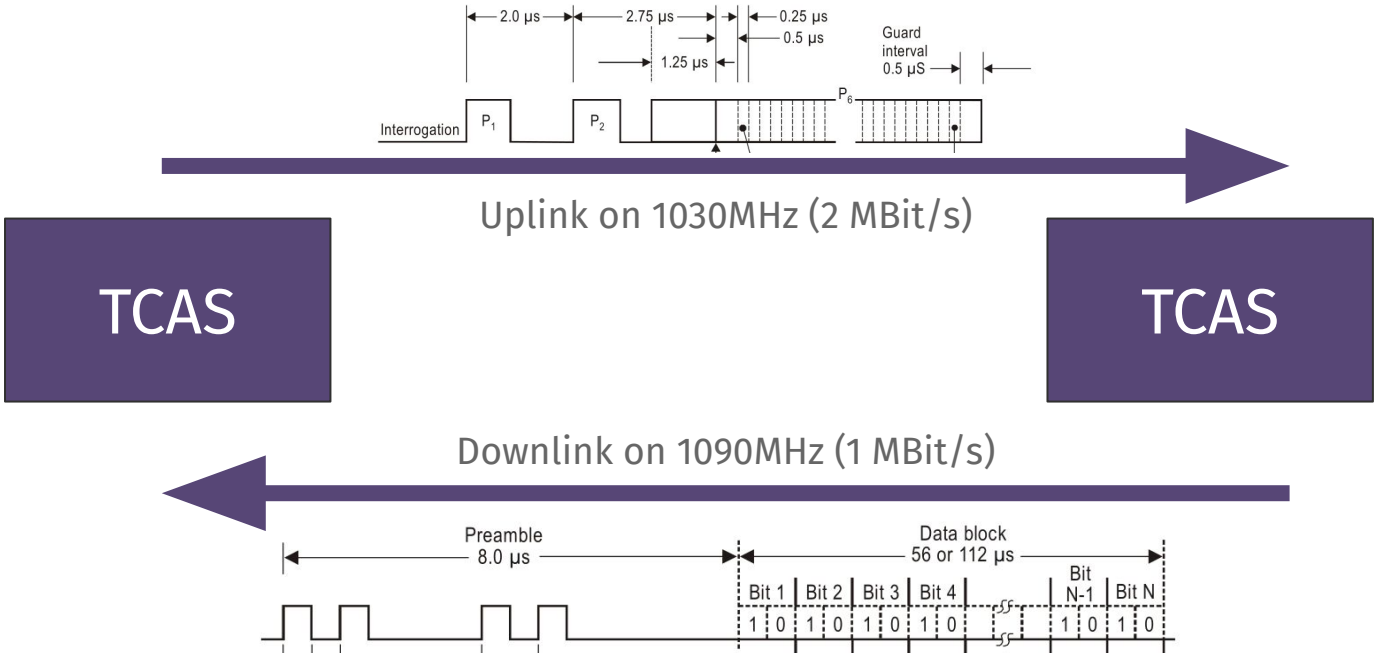
Testbed architecture

Instrumentation



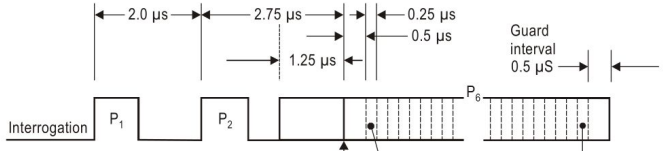
Implementing an attack

Mode-S Physical Implementation



Mode-S Physical Implementation

No publicly available **realtime** TX implementation



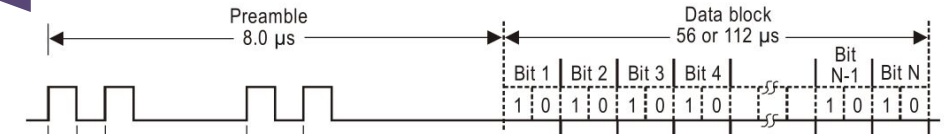
No publicly available **realtime** RX implementation

Uplink on 1030MHz (2 MBit/s)

TCAS

TCAS

Downlink on 1090MHz (1 MBit/s)

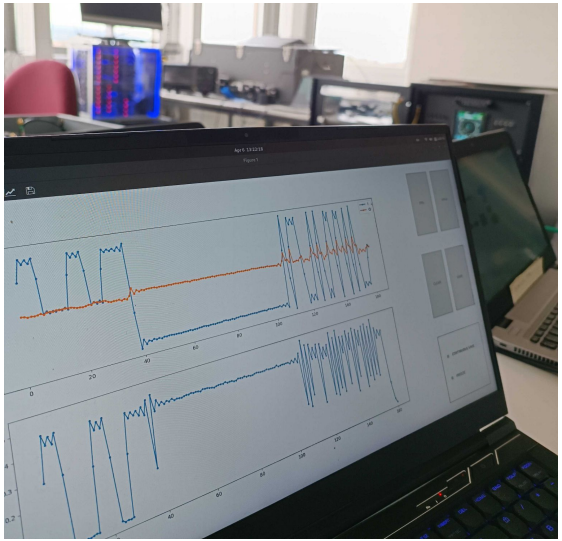


No publicly available **realtime** TX implementation

No publicly available **multichannel coherent** implementation

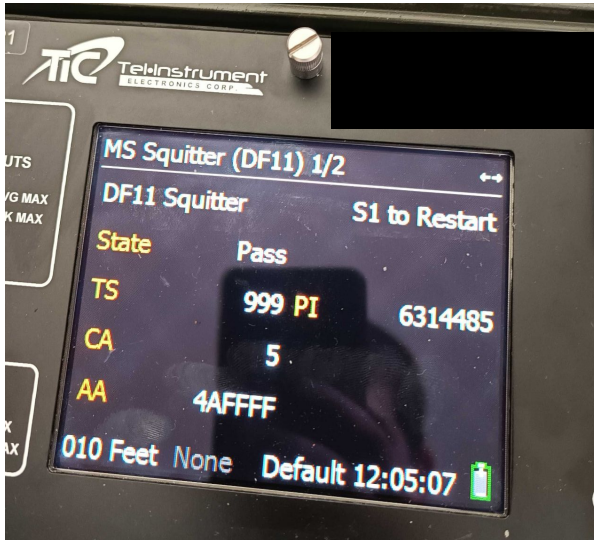
Mode-S

A full SDR chain



Laboratory testing

We implemented a bespoke Mode-S realtime coherent multichannel SDR chain.
Focusing on its latency

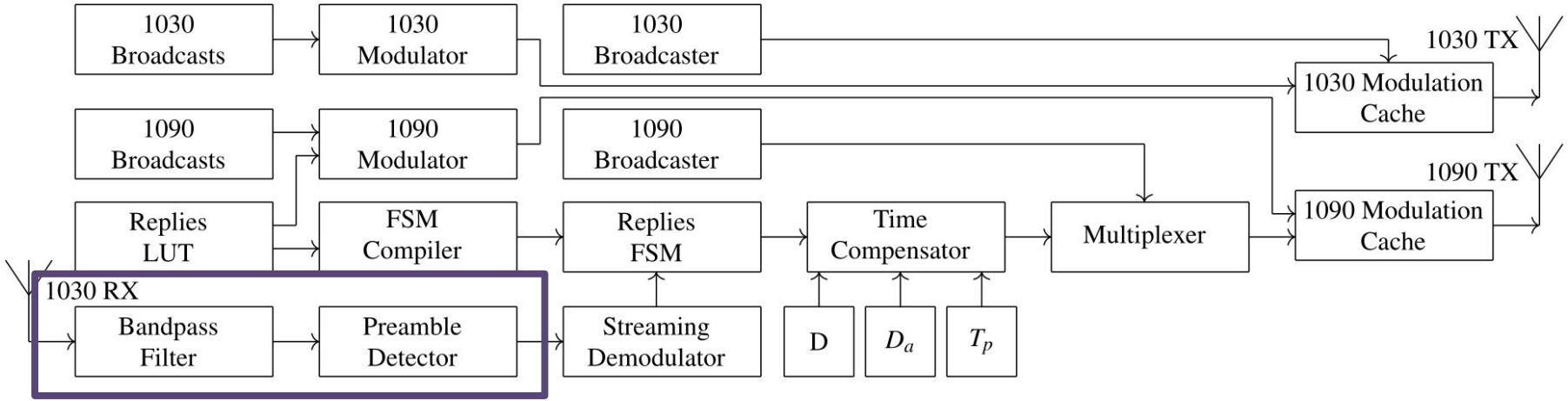


Compliance checking

UniGe | DIBRIS CYD CYBER DEFENCE CAMPUS

Our SDR chain

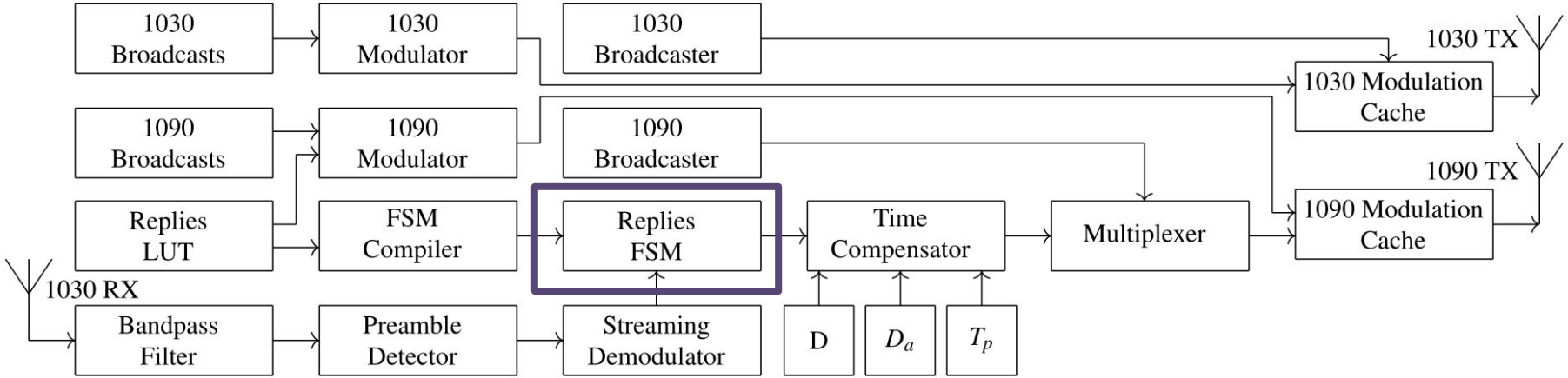
A minimal latency software architecture



Convolution theorem, Fourier transforms, Symmetries, ...

Our SDR chain

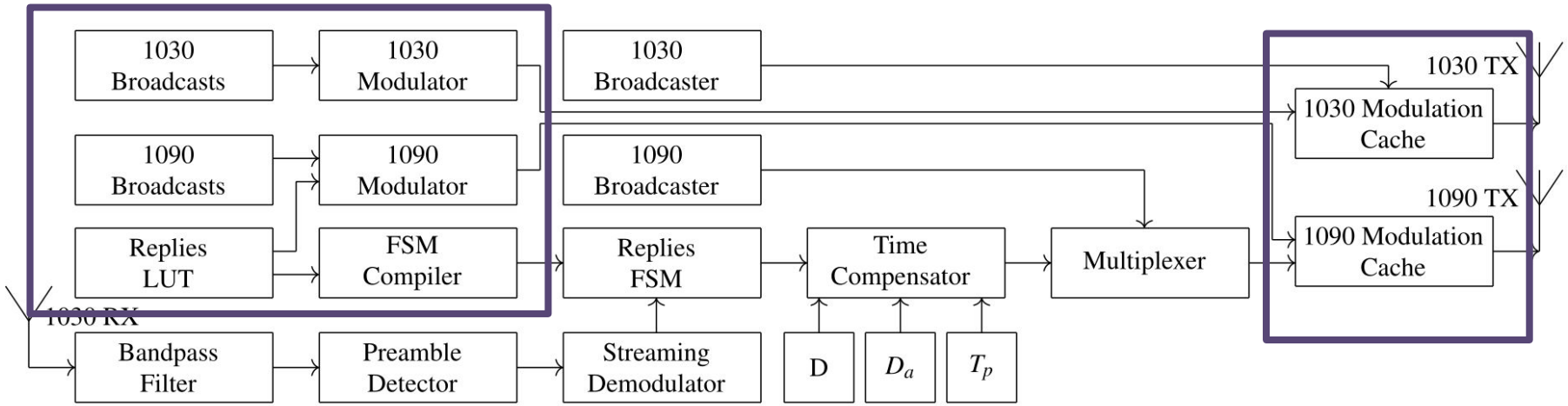
A minimal latency software architecture



Reply as soon as possible once an interrogation is identified

Our SDR chain

A minimal latency software architecture

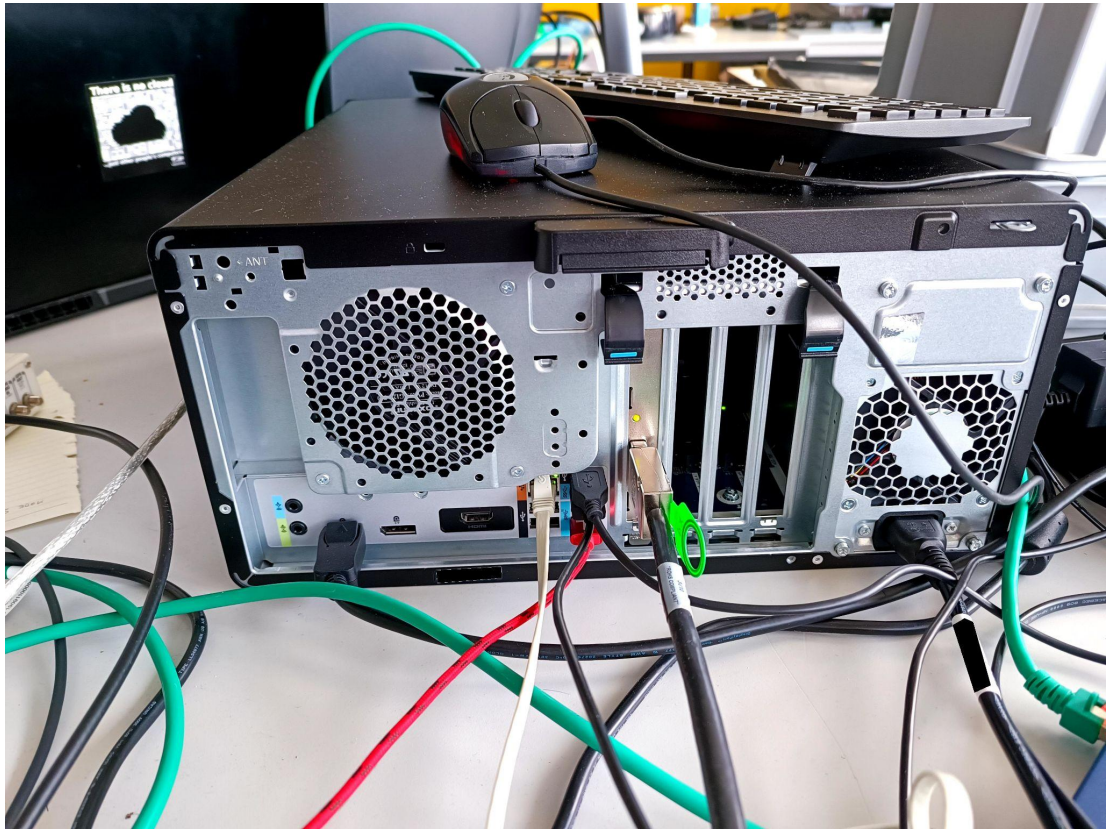


Heavy memoization and pre-computation of modulated responses

Reducing latency

Hardware tricks

- No power saving
- No hyperthreading
- No E-cores
- No GPU
- No security mitigations / DMA protections



Reducing latency

OS / configuration tricks

- Linux RT
- Pin OS/application to different cores
- Busy polling
- Compiler tweaks
  - Optimize for target microarchitecture
  - Profile Guided Optimization
  - Link Time Optimization

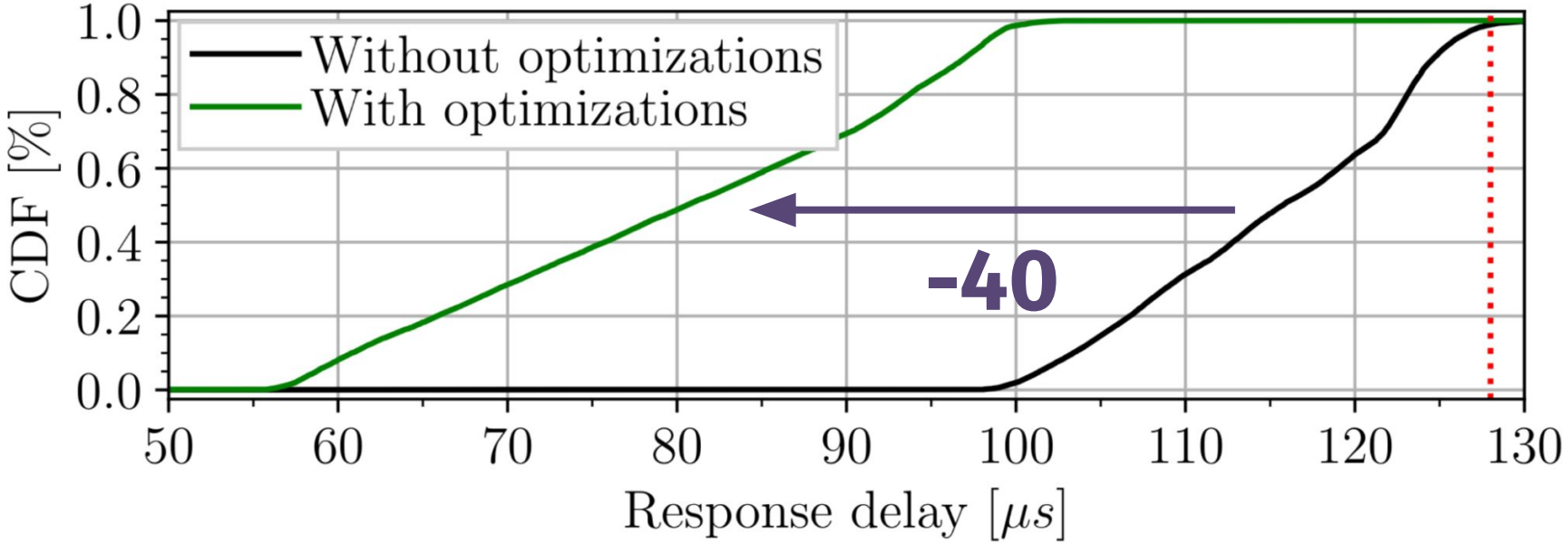
Reducing latency

Software engineering

- Single Instruction Multiple Data (SIMD) DSP processing
- Lockless programming / atomics
- No memory allocations
  - Custom 1GB hugepages allocator to minimize TLB misses
- Threading

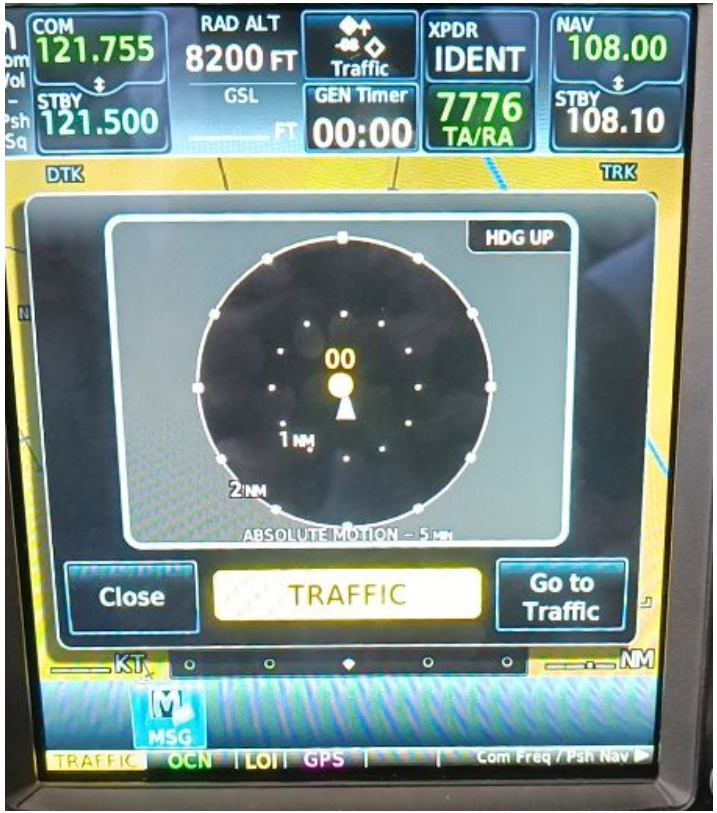
Reducing latency

Engineering matters



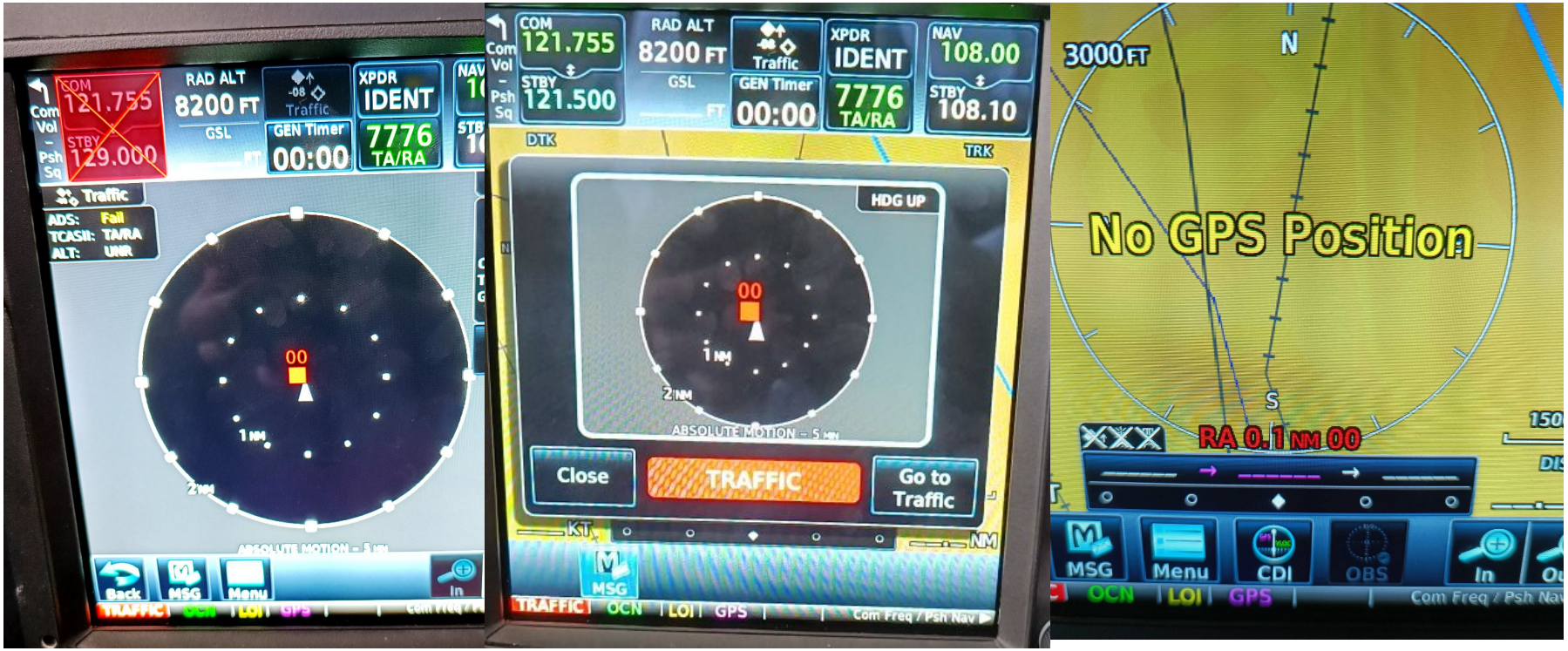
Qualitative results

Triggering a TA



UniGe | DIBRIS CYD CYBER DEFENCE CAMPUS

Triggering a RA



TCAS deactivation

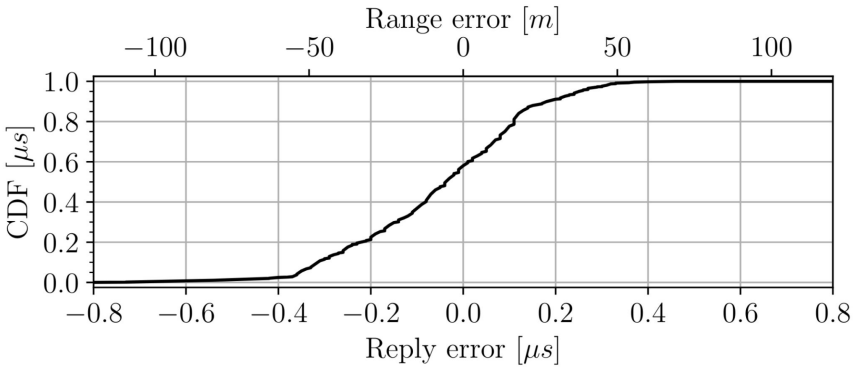

```
(DF0 { df: 0, vertical_status: Airborne, crosslink_capability: Yes, sensitivity_level: L3, reply_information: AirspeedGT75LE150KN,
(DF0 { df: 0, vertical_status: Airborne, crosslink_capability: Yes, sensitivity_level: L3, reply_information: AirspeedGT75LE150KN,
(DF0 { df: 0, vertical_status: Airborne, crosslink_capability: Yes, sensitivity_level: L2, reply_information: AirspeedGT75LE150KN,
```

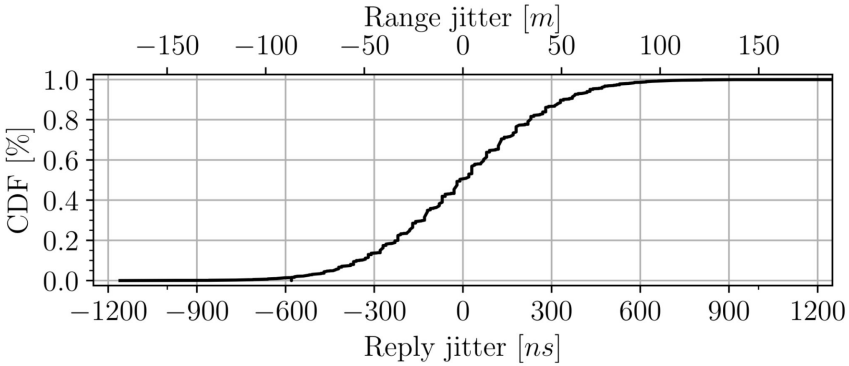
Is it reliable?

Quantitative Results

TA & RA injection

Attacker has a range accuracy of around 25 meters, consistent over multiple interrogations





1.7 million samples

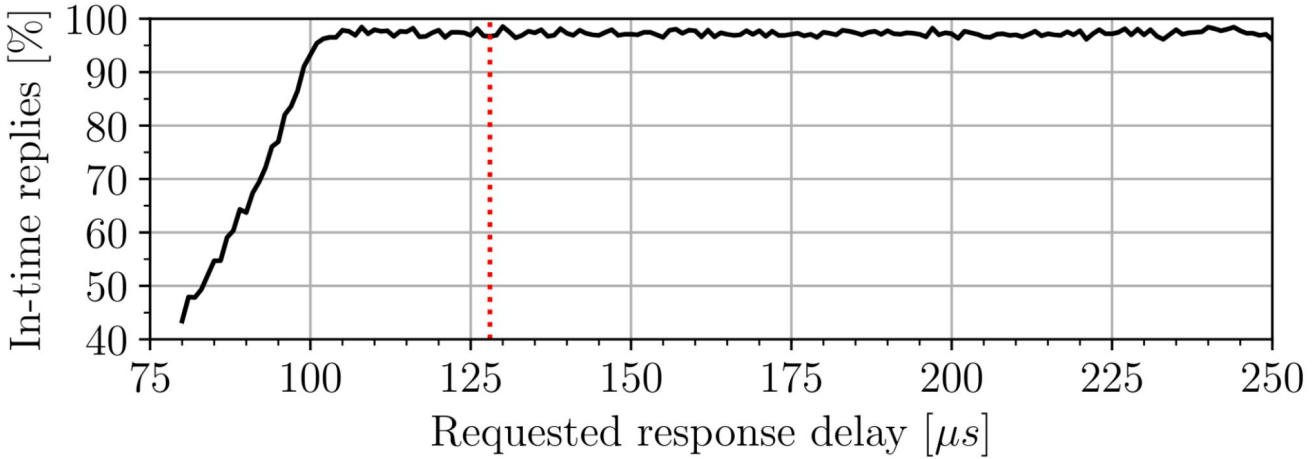
UniGe | DIBRIS

CYD | CYBER DEFENCE CAMPUS

TA & RA injection

Attack replies successfully to around 98% of interrogations.

Can manage around 30+ us of spare delay



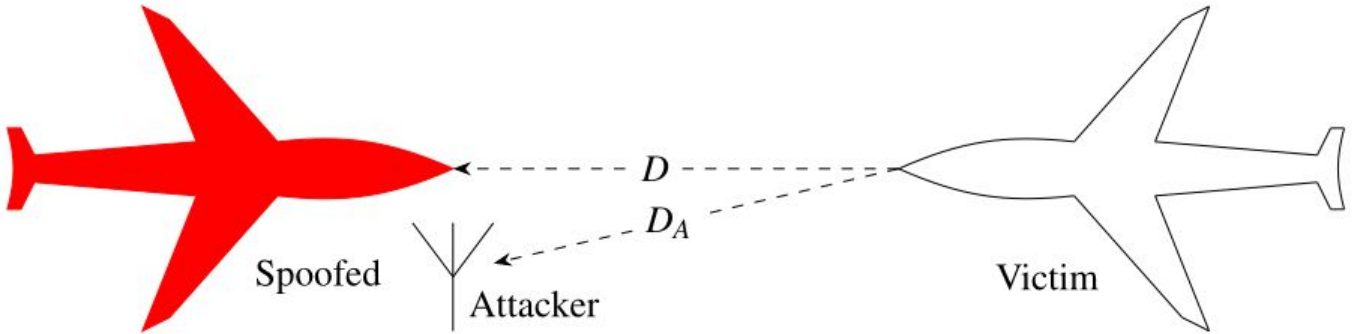
1.7 million samples

30us

Attacker capabilities

The attacker wants to spoof an aircraft at a distance D, **inferior** to its own

We call this the "*range spoofing capability*"



30us

Attacker capabilities

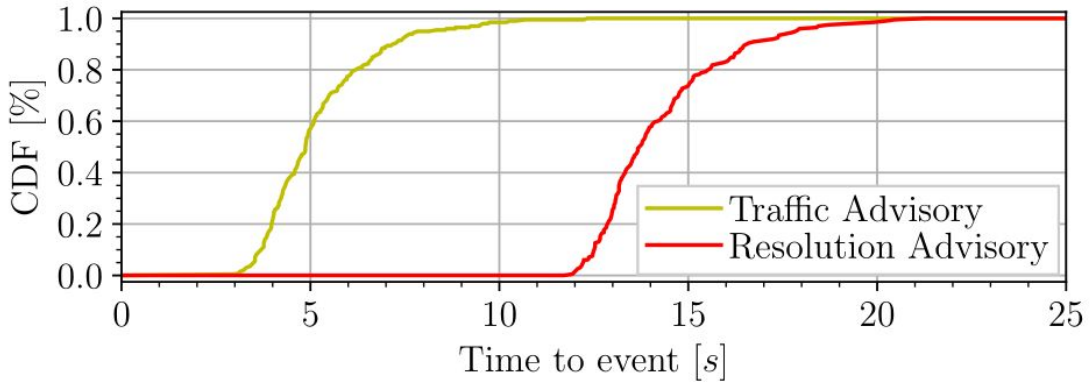
The **current** capabilities allow to place an aircraft at distance 0

If the attacker is within ~4.2km

Theoretical limit (zero processing time): 19.186 km

Capabilities, continued

The current capabilities allow an attacker to induce a RA to an airliner flying at 950km/h with a probability of 80%



25 encounters, 222936 data points, 127 minutes

RA DoS

Works, **always**

Conclusion

Conclusions

What are you doing about it?

1. It's a **systemic** problem within a **standard** on a **delicate topic**
2. We have disclosed to
   a. Manufacturers
      (**A** Airbus, Garmin, Leonardo Elettronica, **U** Boeing, Pilatus Aircraft, Thales)
   b. Authorities
      (**A** EASA NoCA, Italian ENAC, Swiss FOCA, US CISA CVD, **U** FAA)
3. Our artifacts do not contain any code enabling these attacks

A with acknowledgement **U** without yet

UniGe | DIBRIS CYD | CYBER DEFENCE CAMPUS

Thanks

UniGe
DIBRIS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung
Bevölkerungsschutz und Sport
armasuisse
Wissenschaft und Technologie

CYD | CYBER DEFENCE CAMPUS

Qs?