MASTERING EXCELLENCE

SIMCOM: simulating cyber-attacks on ADS-B protocol

Engage 2 summer school – Braunschweig

Luca Martinoia – Project Engineer

l.martinoia@stamtech.com

25-09-2025

stamtech.com

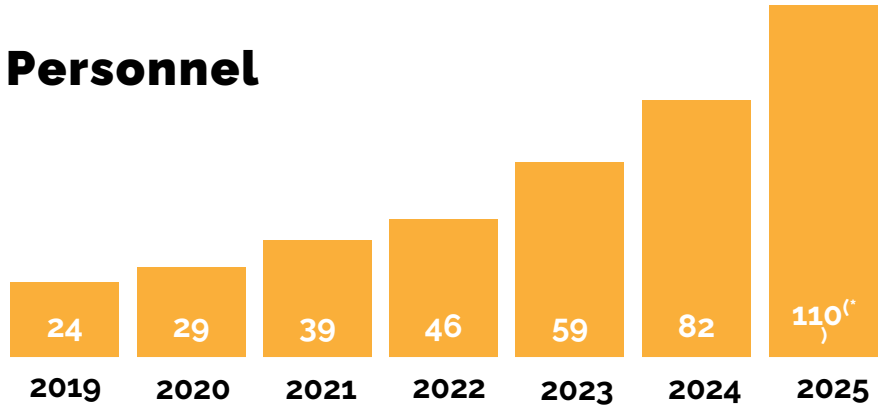
STAM S.r.l.

About me: Ph.D. in theoretical physics (2024). Until recently researcher at university, but in April 2025 I left academia to join STAM as a Project Engineer (Defence and ATM projects).

STAM is a multidisciplinary **consulting engineering** company based in Italy that provides support to clients facing new business and technology challenges.

Core business area:

- Energy & Sustainability
- Digital solutions
- Research & Innovation
- Robotics
- **Engineering solutions**



ATM-EXCITE

ATM-EXCITE[1] is a SESAR JU project to:

- improve **cyber-security** on the ADS-B protocol,
- enhance **civil-military cooperation and coordination**.

The ATM-EXCITE consortium is composed of industrial partners and research institutions: Euro-Funding (PM), INFODAS, INCAS, STAM, UPVISION and TUKE

Each partner develops a possible solution:

- ADVERMA: Collaborative ATC system + ML validation
- SEALD: selective encryption mechanism
- ANYSKY: OSNMA-enabled authentication
- DACSEC ADS-B: Zero Trust Architecture principles
- **SIMCOM**: ATM simulator for cyber-defence on ADS-B protocol

1. atm-excite.eu

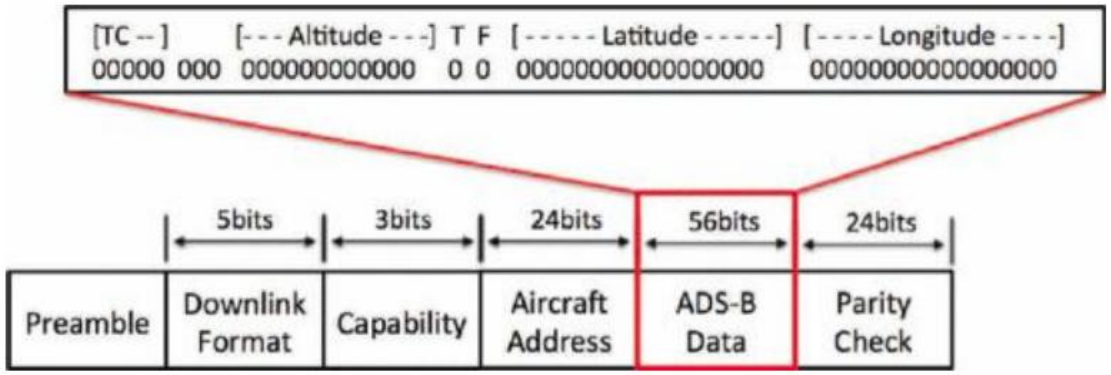
Automatic Dependent Surveillance - Broadcast

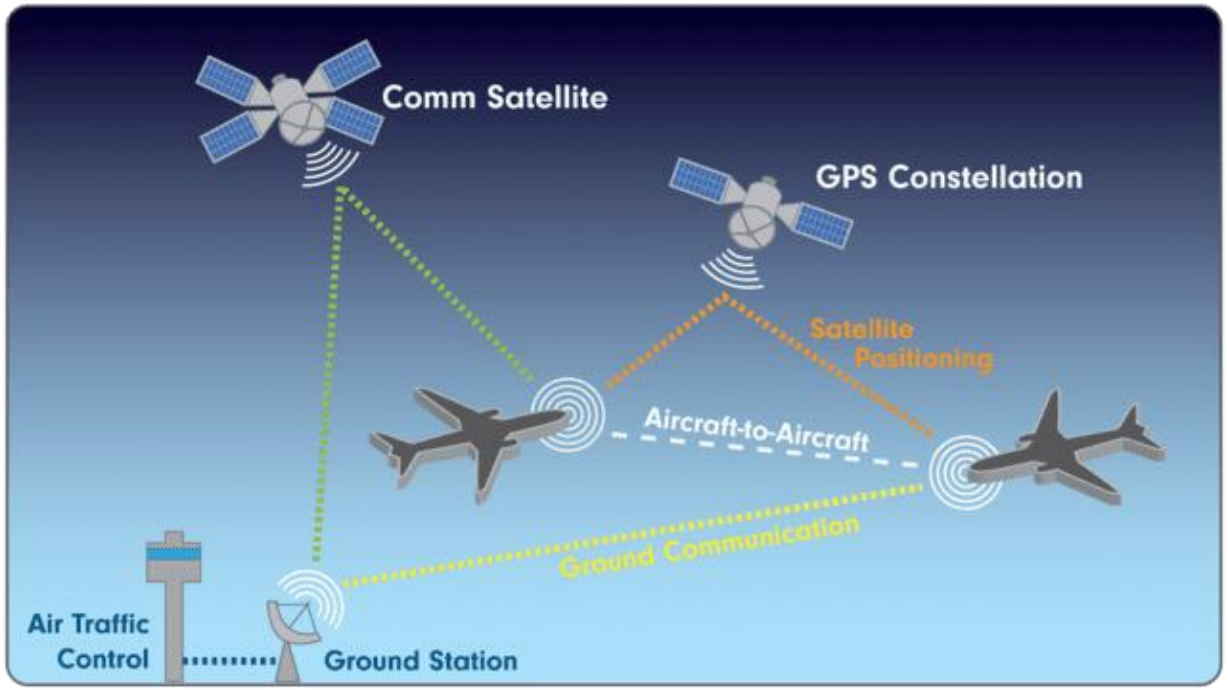
ADS-B (standard RTCA DO-242A) is a core surveillance system that provides ATC and aircraft with **situational awareness**.

Based on the Mode S ES protocol, the system itself is divided into two separate functions: **ADS-B In** and **ADS-B Out**.

It has several advantages compared to traditional surveillance methods (PSR and SSR):

- cheaper,
- easily deployable,
- more precise,
- faster update rate.





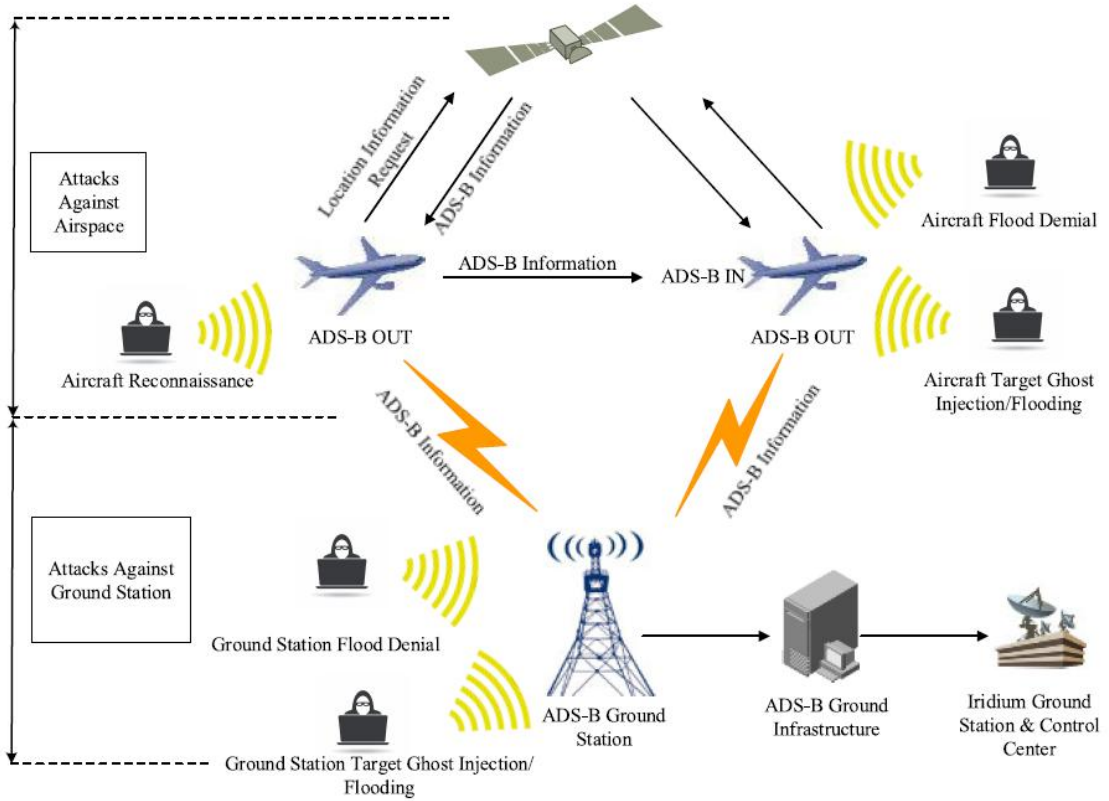
ADS-B cyber-security

Despite the advantages, **ADS-B was not designed with security considerations in mind**:

- Open-text
- Unencrypted
- Unauthenticated
- No anti-jamming

Cheap hardware + software defined radio enable a wide variety of **cyber-attacks on ADS-B**[2]:

- Passive attack (eavesdropping, like FlightRadar)
- Authentication (message injection)
- Integrity (message deletion, message modification)
- Availability (jamming, DoS)



2. Costin, 2013, Schäfer 2013, etc…

Cyber-attacks ADS-B simulators

ATM simulators with a focus on ADS-B cyber attacks have already been considered in the past.
Always based on OpenScope[3], most notably:

- Gurtov's group (Linköping University) from 2020 to 2024,
- Cestaro's OpenScope-sec (University of Padova) in 2024

E.g., OpenScope-sec attack taxonomy:

- Non-responsive aircraft
- Jumping aircraft
- False information
- Virtual trajectory modification
- False alarm
- Aircraft spoofing
- Ghost injection
- Message delay
- Aircraft standing still

3. openscope.io

SIMCOM

SIMCOM plans to expand BlueSky with cyber-threat and cyber-defence specific modules:

- ADS-B protocol encoding-decoding (pyModeS)
- cyber-attacks implementations (jamming, ICAO spoofing, trajectory modification, ghost aircraft, etc…)
- template cyber-defence strategies (simple encryption/authentication mechanisms)
- potentially, a new conflict detection module

In the (hopefully near) future:

- merging and synergizing with other ATM-EXCITE solutions
- civil-military shared airspace scenarios

STAM
MASTERING EXCELLENCE

Thank you for your attention!

STAM
MASTERING EXCELLENCE

CONTACTS

Luca Martinoia – Project Engineer

l.martinoia@stamtech.com

stamtech.com

stamtech.com

STAM S.r.l

Stam_Tech

stam_tech