Supporting
European
Aviation

EUROCONTROL

Counter UAS and GNSS RF Interference

High Level Workshop on the current state of C-UAS Systems

Session 2: Challenges and Threats (part 2)

Gerhard BERZ

Head of Navigation and Spectrum

4 Nov 2024

gerhard.berz@eurocontrol.int

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

Counter UAS using GNSS RF Interference

- One potential method to counter UAS is the use of GNSS jammers and spoofers
  - Many products are on the market and may get used during special events by authorities
    - “Jamming by authority action” – ANSP Concern / Uncertainty during consultation
  - Common theoretical approach:
    - First jam COM link. UAS may climb to try and regain COM
    - *What happens next, depends a lot on UAS design*
    - IF UAS attempts to continues trajectory into threat region, navigation jamming or spoofing may be used by authorities
    - *What happens next, depends a lot on UAS design*
    - Today limited feedback on effectiveness of jamming vs spoofing
- Aviation security concerns favour that C-UAS can effectively achieve their missions
  - Especially near airports
  - However, must ensure that safe operations can be maintained
- In cooperation with various partners, EUROCONTROL has sought to find out if **safe coexistence** of C-UAS jammers and aviation ops can be achieved **by producing best practice guidelines?**

Test Plan Phase 1 (EC Joint Research Center - DONE)

- Anechoic Chamber Testing of C-UAS jammers or spoofers
  - Device under test: C-UAS jammer / spoofer
    - No UAS required
  - Measure ACTUAL full 3D radiation pattern of jammer / spoofer, including in particular **any relevant side lobes**
  - Measure and verify manufacturer specifications for device, especially with respect to radiated power and signal characteristics (manufacturer specification are often minimum specifications, where actual device power can be greater)
  - As many devices to be tested as possible – in particular those commonly used by police or military authorities
    - Data can be anonymized if necessary
- Supports theoretical risk assessment of live engagement based on verified data and allows to plan critical encounter scenarios for live tests with UAS

Test Plan Phase 2 (Not completed, still pending)

- Live tests with actual jamming and/or spoofing of UAS with C-UAS device
- Required assets: UAS, C-UAS and authorization to conduct tests at suitable location
  - Note: Multiple UAS with different navigation and recovery capabilities would be ideal. At least some of the C-UAS from phase 1 testing must be available.
- Test environment: Ideally in an open sky environment
  - Considered to be very difficult inside a hangar. Large open pit with sky view could be option
- Test objective: Understand encounter scenarios and likely duration
  - Big difference for managing civil aviation compatibility if jamming lasts a few minutes versus tens of minutes
- Phase 2 not started due to both lack of resources and participation
  - Note: IF sufficient in service or other testing experience is available ➔ Phase 2 testing may not be required?

Phase 1 C-UAS Jammers Test Results

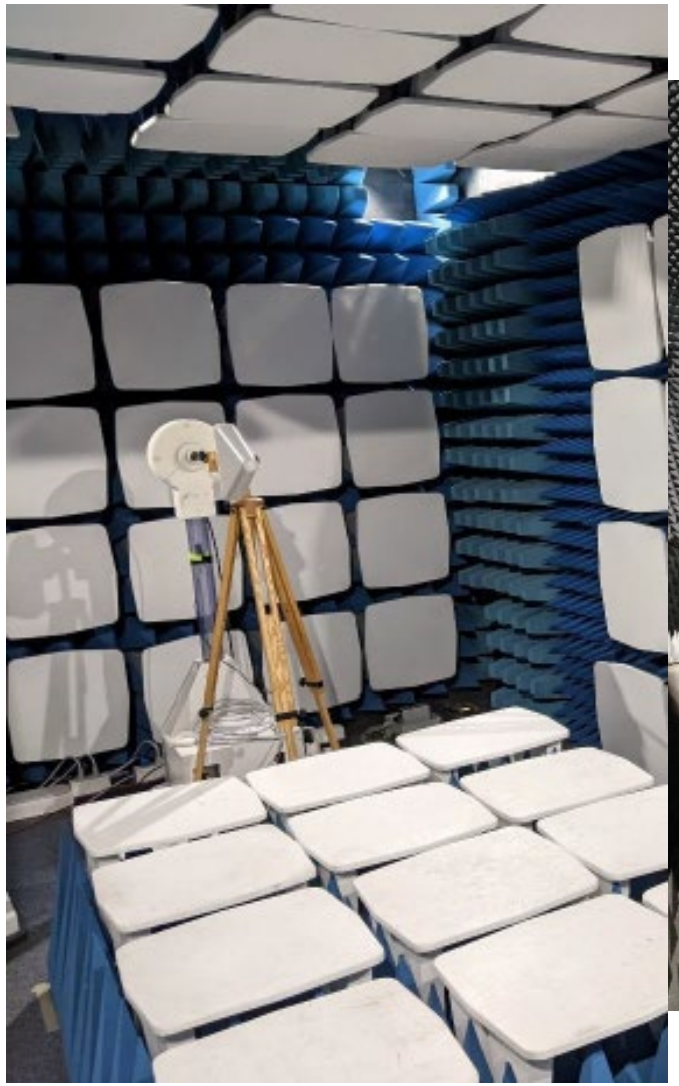
- **Ad hoc group** included EUROCONTROL, EDA, NATO, EC JRC and several European police forces/frequency regulators/military and ENAC

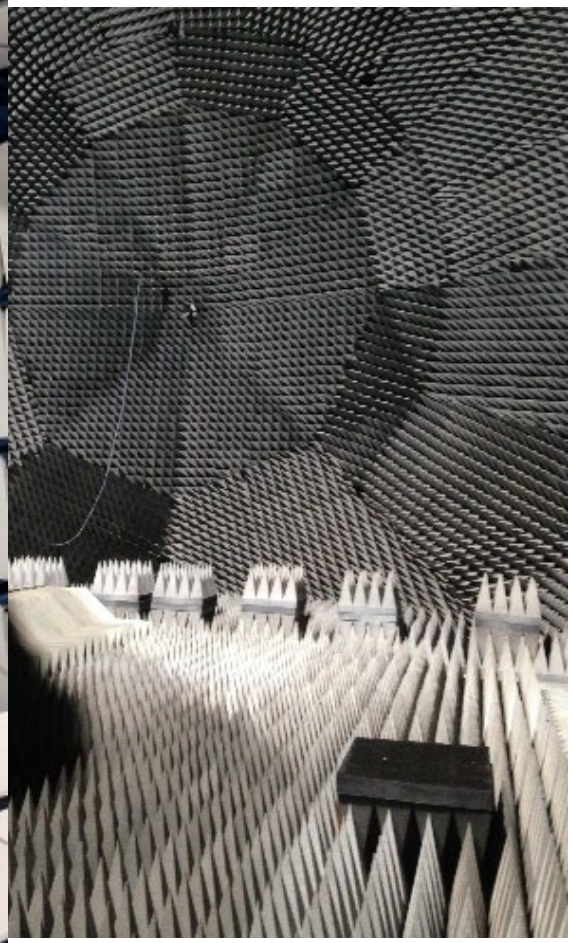
Joint Research Center, Ispra

- Several military or police authorities furnished C-UAS jammers
- JRC facility supports handling classified equipment
- State of the art anechoic chambers and test tools

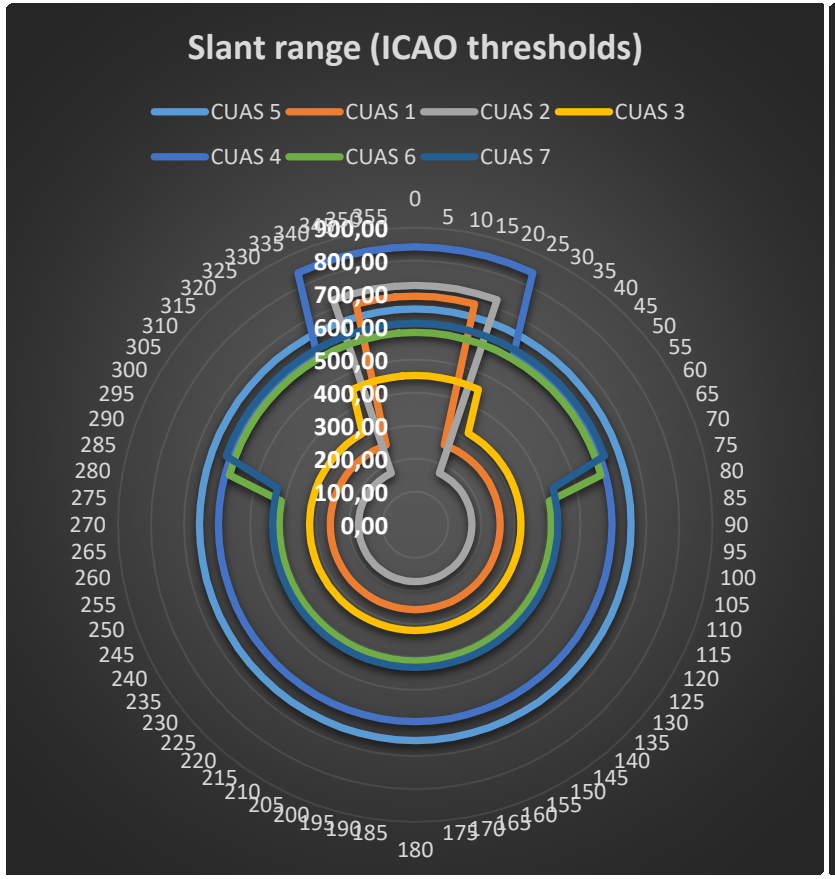
Test Reports

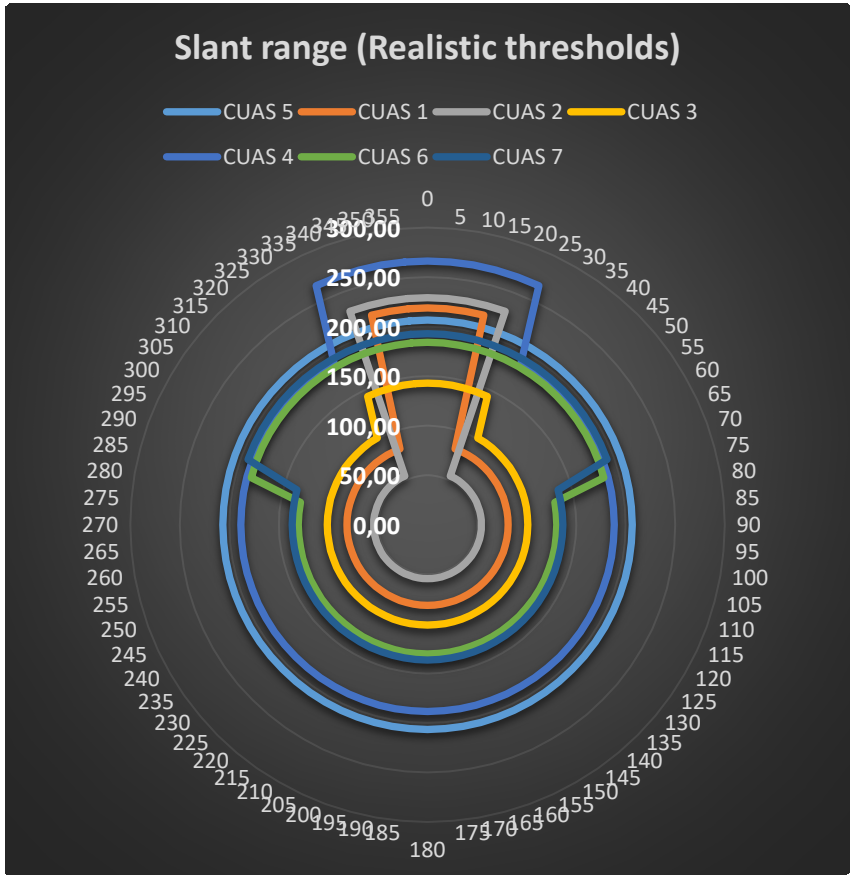
- Available on request basis only
- State authority which furnished tested equipment needs to provide agreement
- **Note:** EGITF, EU GNSS Interference Task Force, may continue some activities, in cooperation with JRC and ENAC

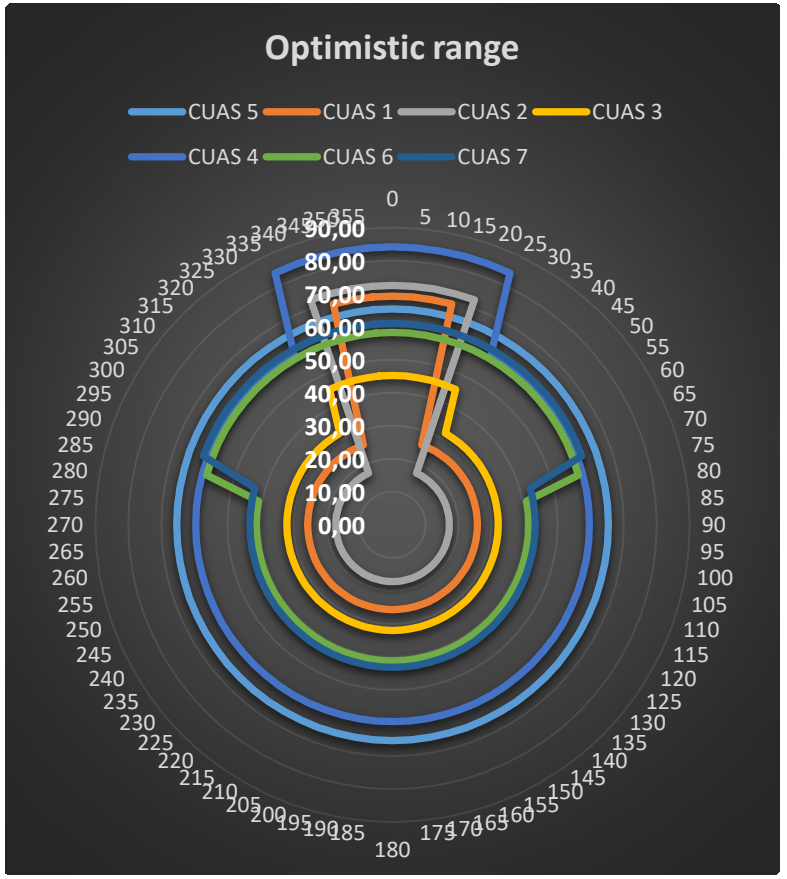




C-UAS Impact: Test Results







- Aviation GNSS receiver impact range derived from a previous EUROCONTROL test campaign which assessed a variety of aeronautical receivers vulnerability to a variety of jamming waveforms
- **Even when using realistic thresholds, BACK LOBE IMPACT in a realistic case on the order of 50NM+!**

C-UAS RF Jamming Solutions – Do they work?

- C-UAS Testing shows that avoiding airport impact even in back lobe is not possible / unlikely
  - Various C-UAS capabilities shown in the past to be effective only against slow rotary wing drones
- IF C-UAS jammers are effective, only two solutions to minimize impact
  - Broadcast less power?
    - Ramp up – should be effective against hobby drones
    - **Can it be taken into account in procurement specifications?**
  - Limit time exposure
- Still need more work on encounter scenarios near airports
  - Difficult / impossible to say today how much of a short duration impact could be tolerable
- The only recipe – we have to talk!
  - Make sure each party understands the needs and constraints of the other
  - Reasonable “use of force” only when required
  - Ensure confidential communication channels for tactical coordination
  - Suitable training, gain experience through exercise, **then exchange experience**!

Spoofing is the new Jamming…

- C-UAS Spoofers are being advertised as having less collateral impact and being more effective against the target threat
- **Is that so???**
- MIL Capabilities evolve much faster than aviation can