



ICAO

*International Civil Aviation Organization***Seventh Meeting of the Surveillance Implementation
Coordination Group (SURICG/7)**

Video Teleconference, 24 – 27 May 2022

Agenda Item 10: Review ADS-B Implementation and Operations Guidance Document (AIGD)**POSITIVE EFFECT OF CPR REASONABLENESS TEST ON ADS-B SECURITY**

(Presented by ENRI, Japan)

SUMMARY

This paper presents reasonableness test for CPR decoding is useful for improving ADS-B security via numerical simulation. Based on the result, this paper also proposes to add a suggestion into ADS-B Implementation and Operation Guidance Document (AIGD).

1. INTRODUCTION

- 1.1 ADS-B is a dependent surveillance and also open system without encryption and authentication. Consequently, there is a possibility of false position information caused by avionics and security issues.
- 1.2 Previous considerations for these issues have been documented in ADS-B Implementation and Operation Guidance Document (AIGD) and the guidance material on security issues associated with ADS-B provided on Secure Portal.
- 1.3 Additionally, in Mode S DAPs WG/5 IP/06 in 2022, China introduced the technique called reasonableness test for CPR Decoding, which was originally written in RTCA-DO260B. China reported that this technique addressed a false position caused by an airborne aircraft transmitting a surface position format.
- 1.4 This paper presents that the reasonableness test also has ability to reduce some of false information that is intentionally transmitted, although the technique was not originally aimed at solving security issue.
- 1.5 Based on the information above, this paper also proposes to add it to AIGD that appropriate implementation of a decoding method is important for security aspect as well.

Agenda Item 10

24-27/05/22

2. REASONABLENESS TEST FOR CPR DECODING

2.1 CPR (Compact Position Reporting) is the format used to encode a latitude and longitude in the ADS-B position report using 1090 Extended Squitter (DF = 17, BDS = 0,5 and 0,6).

2.2 There are two ways of decoding the encoded CPR:

a) globally unambiguous decoding, which requires two signals called “even” and “odd”.

b) locally unambiguous decoding, which requires either even or odd signal plus a reference position.

2.3 The reasonableness test is a technique to verify the decoded position. The basic mechanism of the reasonable test for locally unambiguous decoding is detecting a position jump from previous decoding, for example, 6 NM for airborne positions within 30 seconds. The basic mechanism of the reasonable test for globally unambiguous decoding is decoding an additional pair of signal and use it for verifying the previous decoding.

2.4 The CPR reasonableness test is included in the ADS-B message decoding logic in RTCA DO-260B together with a range test, which checks whether the output of globally unambiguous decoding is within the receiver’s operational coverage. The range test and CPR reasonableness test are included also in EUROCAE ED-129B (Technical Specification for a 1090 MHz Extended Squitter ADS-B Ground System) as follows:

[REQ 47] By default, the ADS-B System shall only output ASTERIX Category 021 reports for targets that have passed the CPR Global Decoding Reasonableness test in 2.2.10.6.2 of ED-102A/DO-260B.

[REQ 48] For position reports that fail the range check test, the CL and RFC bit of the I021/040 shall be 1 (“Report Suspect, Range Check Failed”).

[REC 77] The ADS-B System should be configurable to deliver Target Reports when position messages are received and fail CPR Validation (with the invalid position in the report).

[ORQ 72] If [REC 77] is implemented, the configuration for this recommendation is set to enabled, and the target has failed CPR Validation as described in section 2.2.10.6 in ED-102A/DO-260B, the CL bit of the item I021/040 primary subfield ASTERIX Category 021 shall be 1 (“Report Suspect”).

[ORQ 73] If [REC 77] is implemented, the configuration for this recommendation is set to enabled, and the target has failed CPR Validation as described in section 2.2.10.6 in ED-102A/DO-260B, the CPR bit of the item I021/040 primary subfield ASTERIX Category 021 shall be 1 (“CPR Validation failed”).

2.5 It is noted that the techniques are not intended for security measure. However, they are expected to reduce some of intentional false information, too, in addition to reduce unintentional false information (as demonstrated in Mode S DAPs WG/5 IP/06 in 2022 by China).

3. NUMERICAL SIMULATION

- 3.1 ENRI conducted a numerical simulation. Figure 1 shows the setup; ADS-B airborne position messages were generated for a correct track and a false track. The detail parameters are listed in Table 1.
- 3.2 Then, the decoding method in RTCA DO-260B was applied. The signals passed the range test and reasonableness test for globally unambiguous decoding. However, the false positions did not pass the reasonableness test for locally unambiguous decoding as shown in Figure 2. Position jumps of 13.7 NM, which are larger than 6 NM threshold, were detected.

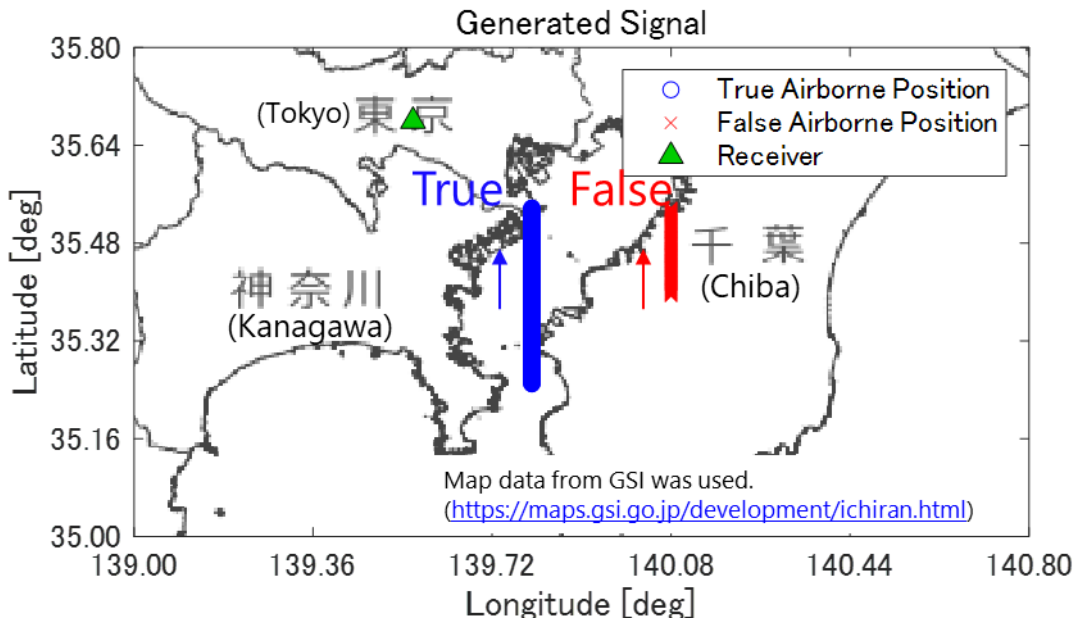


Figure 1. Generated signal in the simulation

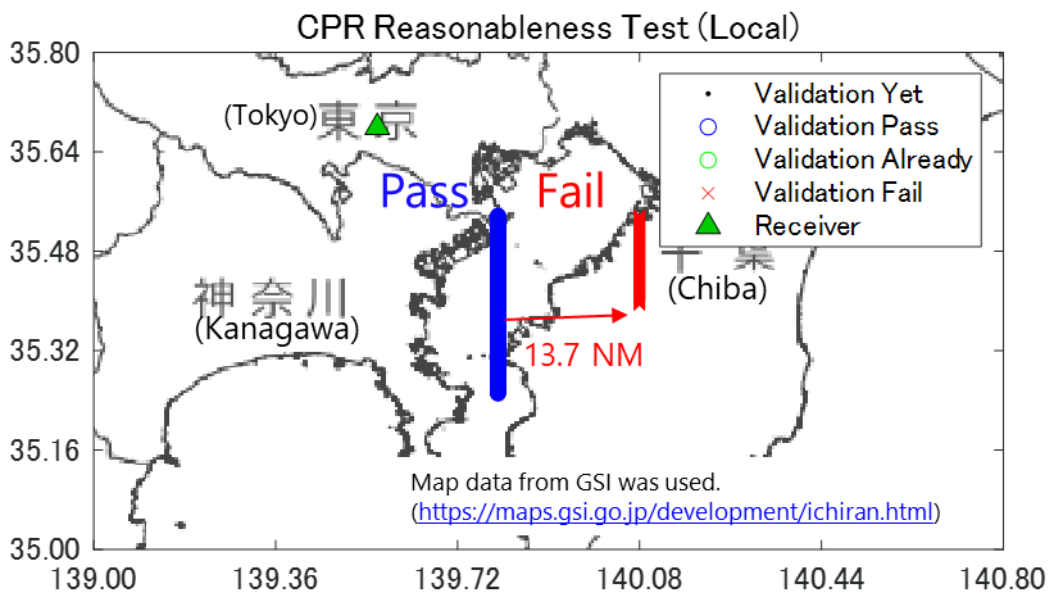


Figure 2. Simulation result of reasonableness test for locally unambiguous decoding

Table 1. Simulation Parameters

Transmission Start	2022.4.1 9:00:00(UTC) ... True signals 2022.4.1 9:02:00(UTC) ... False signals
Transmission Duration	240 seconds ... True signals 120 seconds ... False signals
Transmission Interval	0.4 to 0.6 sec
Velocity	Approx. 260 knot to true north
Address	8520FC
Signal Type	Airborne Position Message ... True/False signals (Type Code = 11) Airborne Velocity Message True signals (Type Code = 19; for invoking state changes of the decoder (Init, Acquisition, and Track) and most content was set empty)
Altitude	8,000 feet

4. PROPOSED MODIFICATION IN AIGD

- 4.1 The simulation result has shown that the reasonableness test for CPR decoding has ability to reduce some of false information that is intentionally transmitted.
- 4.2 Based on the simulation result, international standards, and previous IP, it is proposed to include a suggestion to AIGD as follows:

10.3 MEASURES FOR ENHANCING THE SECURITY OF ADS-B
 10.3.1 TIME DIFFERENCE OF ARRIVAL (TDOA) BASED POSITION
 VERIFICATION METHOD
 10.3.2 APPROPRIATE IMPLEMENTATION OF A DECODING METHOD

Appropriate implementation of a decoding method is important also for security aspect. In the technical standards, there are techniques available for supporting correct decoding, for example, range test and reasonableness test for CPR (Compact Position Reporting) decoding in DO-260B. Although they are not originally intended for security purpose, reduction of false position information is expected.

5. ACTION BY THE MEETING

- 5.1 The meeting is invited to:
 - a) note the information contained in this paper; and
 - b) discuss any relevant matter as appropriate
