

Comments and questions on
« Proposed Revisions to ADS-B MASPS :
Integrity and Accuracy Monitoring
SC 186 WG-6, August 2001 »

by Pierre GAYRAUD
(THALES Avionics, formerly SEXTANT)
Tel +33(0) 5 61 19 77 87
@email : pierre.gayraud@thales-avionics.com

This paper provides with some comments to the above referenced RTCA White paper. As I didn't participate in the preparation of this document some comments or questions may not be appropriate.

1 – Integrity

I agree that integrity is a very important parameter. The integrity risk is the probability to have an error greater than a specified value without annunciation for a period longer than a specified time-to-alert.

As a consequence it is generally characterised by three figures:

- A probability (with respect to a given exposure time);
- A maximum error value (the containment bound);
- A maximum time to alert.

For example according to the different phases, ICAO defines various time to alert:

- En route oceanic: 5 min.;
- En route continental : 15 sec;
- CAT I operations: 6 sec...

I imagine that specified values of time to alert associated to Surveillance integrity levels could be necessary for the safety assessment.

2 – Continuity

I am surprised that no continuity requirements are used for surveillance. Generally safety assessments need to know what is the continuity of the parameters.

For example the JAA is in the process to establish requirements for the data that are transmitted by airborne ATC Transponder for Elementary Surveillance with SSR Mode S. Only two kind of events are specified for the different parameters :

- Loss of Parameter (i.e. continuity),
- Erroneous Parameter (i.e. integrity).

In the case where it is confirmed that a Continuity requirement is needed, I do not know if the Continuity level has to be transmitted within an ADS-B message or if it has only to be demonstrated during the certification process and required by Airspace regulation.

3 – Accuracy

Generally accuracy is a secondary requirement because it is superseded by the integrity requirement.

The weakness of an accuracy figure stated as à 95 % value is that it doesn't allow to derive the probability that during an exposure time the error becomes greater than a given threshold. Actually, an additional knowledge of the spectral or temporal behaviour of the error is necessary (the probability could be totally different whether the error is a constant one or is a high frequency error).

4 – Navigation or Position?

Required Navigation Performance (RNP) is really relative to Navigation because it characterises the way the aircraft follows a given track. As a consequence the RNP values include (cf. ED-75A/DO-236A):

- Position estimation;
- Path definition;
- Path Steering (or Flight Technical Error).

Conversely, ADS-B objective is not to transmit how accurately or how safely the aircraft follows a given track (navigation) but how accurate or how safe are the Position data.

(Note that RNP levels and ADS-B integrity, accuracy or continuity categories cannot be directly compared because they do not address the same concept.)

As a consequence I think ADS-B should characterise the Position Integrity, Position Continuity and Position Accuracy instead of the Navigation Integrity, Navigation Continuity and Navigation Accuracy.

5 – Criticality or severity or occurrence rate?

I am surprised by the use of criticality levels (Non-essential, Essential and Critical) because as far as I know these terms are only used by Airworthiness authorities to characterise the Assurance level used during the qualification process of a given equipment.

Of course I agree that this level is related to the most serious failure condition that can be generated by the equipment in the system concerned:

- Non-essential: Equipment whose malfunction or loss of function may play a significant part in a major failure condition.
- Essential: Equipment whose malfunction or loss of function may play a significant part in a hazardous failure condition.
- Critical: Equipment whose malfunction or loss of function may play a significant part in a catastrophic failure condition.

(note that the failure condition severities in this definitions are different from the one in the White paper).

If it is considered that the consequence of a given malfunction is assessed at the aircraft level, the usual severity terms used within the framework of Airworthiness Catastrophic, Hazardous/Severe Major, Major, Minor could be used because the Airworthiness regulation associates to each of them a maximum allowable occurrence rate.

It could also be considered that ADS-B is not related to only one aircraft but to a number of aircraft that are involved in a given manoeuvre. Then the concepts defined for ATM could be used. For example ED-78A/DO-254 defines five Hazard Classes from 1 (the most severe) to 5 (the less severe) based upon the operational consequences that are no more assessed at the aircraft level but at the Air Traffic level (all

the involved aircraft and ATM). In the same way maximum allowable occurrence rates are defined for each levels but they are also at Air Traffic level and an allocation is to be done in order to define them at sub-system level (aircraft, ATC, communication system if it is under a distinct institution...).

Conclusion: I agree with the White Paper that the most appropriate is the maximum allowable rate. It should be derived from an analysis at the Air Traffic system level and subsequently allocated to each aircraft.

The reference to the equipment criticality classification should be avoided.

6 – Common Failure causes

It is usually considered that the failures are independent from an aircraft to another. Airworthiness regulations considered each aircraft in isolation (it is perfectly true when aircraft position determination is based on Inertial systems for example).

The problem is now different because the Aircraft Position Estimation of several Aircraft involved in the same manoeuvre can rely on GPS or they can share a common centralised communication means.

For example the impact of a loss of continuity of 100 aircraft flying in the same Airspace and complying with a 10-5/hour continuity risk figure is totally different whether the Aircraft failures are independent or have a common cause (in this last case a potential Hazard could be the loss of the Position data for all the aircraft in the Airspace).

Ways will have to be found in order to establish requirements that take into account potential common failure causes.

7 – Common Design errors

ED-79/ARP-4754 explains how the Development Assurance Levels (DALs) shall be allocated to each part of a given system (for example an aircraft avionics system). The process is quite different than the process used to allocate the maximum allowable occurrence rate of hardware failures because hardware failures are random and not correlated from an avionics piece to the other. It is totally different for design errors because if the dissimilarity is not used the same design error could happen simultaneously in several units contributing to the same function. Methods like Functional Failure Path analysis are proposed. The drawback is that the DAL allocation process is more complex: the different avionics parts can not be considered separately because the DAL allocation is different whether the same design is used or not in the different parts.

ED-12B/DO-178B and ED-80/DO-254 give subsequent guidance respectively for software and hardware.

As a consequence for ADS-B, DALs should be allocated to aircraft taking into account the fact that aircraft or ATM or communication components could share the same design (software and/or hardware).

8 – Conclusions

My personal feeling is that we cannot answer to the above interrogations before having performed a number of safety analysis as well as safety and performance allocations for some applications in typical environments.

There are ongoing activities on this subject. They follow the ED78A/DO-264 methodology:

- Operational Services and Environment Definition (OSED);
- Operational Safety Hazard (OHA): identification of the Operational Hazards and assessment of they consequences.
- Allocation of Safety Objectives and Requirements (ASOR) based on a correspondence between the operational consequences and the maximum allowable occurrence rate.
- Operational Performance Assessment (OPA) and Interoperability Assessment (IA) where the technical, functional, and interface requirements are reviewed and allocated to the different sub-systems.

In the end two documents are produced :

- Safety and Performances Requirements (SPR) ;
- INTEROP.

They gather all the functional, performance and safety requirements and their allocation to each subsystem (aircraft, ATM, communication means...).

I recommend waiting in order to have a number of SPRs available for some applications to be operated within a number of typical environments.

Based on the content of this set of SPRs, we will really be in a position to answer to the above questions:

- 1 - Is the Time to Alert parameter required?
- 2 - Is an accuracy category required?
- 3 - Is a continuity category required?
- 4 - What parameters have to be transmitted by each aircraft to the surrounding aircraft and what parameters have to be demonstrated during the Certification process and then required by Airspace regulations?
- 5 - Is it necessary to take into account the potential common failure causes? If yes How?
- 6 - Is it necessary to take into account the potential common design errors? If yes How?

The consideration of the performances required by this set of SPRs will also allow to define for each parameters the different categories or level.

The consideration of their most current combinations (what integrity requirement is generally associated to what continuity requirement...) will allow to regroup them.