RTCA Special Committee 186, Working Group 3

ADS-B 1090ES MOPS Maintenance

Meeting #24

Honeywell Aerospace, Phoenix, AZ
13 – 15 January 2009

Proposed Redefinition of the SIL Parameter

Prepared originally by: Tony Warren, Boeing
Presented by: Dean Miller, Boeing

Summary
The following was originally prepared by Tony Warren of Boeing as input to the RTCA/Eurocae Requirements Focus Group (RFG) Ground Surveillance Applications Subgroup as they review the requirements for the ADS-B RAD application.

CHANGE ISSUE

ASA MASPS REV -

Tracking Information (committee secretary only)	
Change Issue Number	
Submission Date	
Status (open/closed/deferred)	
Last Action Date	

Short Title for Change Issue:	Revise Surveillance Integrity Level (SIL) Definition and Expand SIL Field

MASPS Document Reference:		Originator Information:	
Entire document (y/n)		Name	Tony Warren
Section number(s)		Phone	425-266-0894
Paragraph number(s)		E-mail	Anthony.w.warren@boeing.com
Table/Figure number(s)		Other	

Proposed Rationale for Consideration (originator should check all that apply):	
x	Item needed to support of near-term MASPS/MOPS development
x	DO-260, 1090 MHz Link MOPS Rev A / ED-102
x	ADS-B MASPS
x	UAT MASPS, MOPS
x	STP MOPS
x	FAA NPRM
x	Item needed to support applications that have well defined concept of operation
	Has complete application description
	Has initial validation via operational test/evaluation
x	Has supporting analysis, if candidate stressing application
x	Item needed for harmonization with international requirements
x	Item identified during recent ADS-B development activities and operational evaluations
	MASPS clarifications and correction item
	Validation/modification of questioned MASPS requirement item
	Military use provision item
	New requirement item (must be associated with traffic surveillance to support ASAS)

Nature of Issue:		Editorial		Clarity		Performance		Functional

Issue Description (attach additional sheets if necessary):

The SIL definition for ADS-B transmit of position quality in DO-242A was originally proposed to cover two functions:

(1) the position source (signal-in-space) containment integrity risk level associated with the broadcast of containment integrity as encoded in the NIC parameter, and
(2) the functional integrity of the source position avionics, e.g., GPS receiver.

Later definitions of SIL included yet more functions, i.e. (3) SIL could represent the functional integrity of the entire transmit avionics chain from the position source to the ADS-B out transmit function including the broadcast message function of the ADS-B transponder. Under this definition, the SIL value is the minimum integrity indicator of any of the above functions. The issue is that the SIL parameter has become badly overloaded and the receiver cannot tell which of the above functions is the basis of the SIL value transmitted.

From the viewpoint of the RAD and NRA ADS-B Out Applications, the SIL parameter is inadequate to be used as the basis of received containment integrity. For these applications, the certification basis is that the containment integrity for Radar-like surveillance standards needs to be equivalent to that of a RAIM GPS

unit, i.e. certified to 10^{-7} per hour level or equivalent to SIL=3 level, whereas the functional integrity of the avionics hardware only needs to be SIL=2 level, i.e. certified to major hazard level or 10^{-5} per hour level. The reason for the difference in integrity requirements is that for radar-like separation standards, a 10^{-7} integrity level in position containment is needed to protect against area-wide failures in position integrity affecting more than one aircraft, whereas the avionics integrity level is only needed to protect against integrity failures affecting a single aircraft. As a result, the SIL parameter is inadequate by itself to certify that an aircraft broadcasting a SIL=2 level in fact meets the 10^{-7} integrity level for source position integrity containment, equivalent to that of a RAIM GPS receiver certified to DO-208 standards or better.

Originator's proposed resolution if any (attach additional sheets if necessary):
The proposed resolution is to redefine the SIL parameter for DO-260A Change 3, DO-242A, and later ADS-B avionics standards to contain two separate subfields for SIL(of two bits each or more), that would independently represent the position source (signal-in-space) containment integrity level, and the functional integrity of the ADS-B transmit domain avionics:

(1) SILc subfield (two bits or more) to represent the containment integrity hazard risk level of the position source (signal-in-space) or of the containment integrity avionics if no signal-in-space is available. For example, the containment integrity of tightly coupled GPS-IRS systems may be 10^{-7} per hour, equivalent to that of a RAIM based GPS system even when the GPS signal is temporarily not available. The proposed definition of this subfield is similar to that of the original DO-242A MASPS:

SILc =	0	Containment integrity risk unknown or greater than 10^{-3} per hour
	1	Containment integrity risk < 10^{-3} per hour
	2	Containment integrity risk < 10^{-5} per hour
	3	Containment integrity risk < 10^{-7} per hour.

(2) SILa subfield (two bits or more) to represent the integrity risk level of the transmit domain avionics
including the position source, STP and ADS-B Transmit functions (interfaces A1 to D in ADS-B MASPS). The proposed definition of this subfield is to represent the functional hazard level as a probability of position data corruption by the underlying avionics. Some avionics systems such as FMS based position sources distinguish the integrity risk level depending on whether the risk is based on faulted or fault free operations. If the fault free operation is limited to an instantaneous probability of data corruption <= 10^{-5}, then SILa is limited to SIL<= 2. Otherwise, the SILa subfield is defined similar to SILc above, except that the integrity risk is for the entire Aircraft Transmit domain, i.e.:

SILa =	0	functional integrity risk unknown or greater than 10^{-3} per hour
	1	functional integrity risk (A1 to D) < 10^{-3} per hour
	2	functional integrity risk (A1 to D) < 10^{-5} per hour
	3	functional integrity risk (A1 to D) < 10^{-7} per hour.

It is possible to consider a simplified one-bit version for SILa also, e.g.,. SILa =0 if functional integrity risk is unknown or greater than 10^{-5}, and SILa=1 if functional integrity risk < 10^{-5}.

Note: Attach additional sheets to capture supporting discussion with source and date.