International Civil Aviation Organization

THE TENTH MEETING OF AUTOMATIC DEPENDENT SURVEILLANCE – BROADCAST (ADS-B) STUDY AND IMPLEMENTATION TASK FORCE (ADS-B SITF/10)

Singapore, 26 -29 April 2011

Agenda Item 8: **Any other business**

GUIDANCE REGARDING RELIABILITY AND AVAILABILITY OF ADS-B SYSTEMS

(Presented by Australia)

SUMMARY

This paper discusses some recommended approaches for ongoing support of ADS-B ground stations and related systems.

1. Background

1.1 The ADS-B IMPLEMENTATION AND OPERATIONS GUIDANCE DOCUMENT (AIGD) maintained by APANPIRG provides guidance to States wishing to implement ADS-B.

1.2 The current version has no guidance regarding Reliability and Availability.

1.3 The provision of a high reliability ADS-B service depends significantly on the approach taken by the Air Navigation Service Provider regarding acquisition, design and ongoing support.

1.4 The attached proposed modification to the AIGD adds guidance regarding this topic.

2. Recommendation

2.1 It is recommended that the meeting adopt the attachment as an amendment to the AIGD.

– – – – – – – – – – – – – –

ATTACHMENT A

PROPOSED ADDITION TO AIGD

SECTION 9 : RELIABILITY & AVAILABILITY CONSIDERATIONS

Reliability and Availability of ADS-B systems should normally be equivalent or better than the reliability and availability of radar systems.

9.1 Reliability

9.1.1 Reliability is a measure of how often a system fails and is usually measured as Mean Time Between Failure (MTBF) expressed in hours. Continuity is a measure equivalent to reliability, but expressed as the probability of system failure over a defined period. In the context of this document,, failure means inability to deliver ADS-B data to the ATC centre. Ie: Failure of the ADS-B system rather than an equipment or component failure.

9.1.2 Poor system MTBF has a safety impact because typically it causes unexpected transition from one operating mode to another. For example, aircraft within surveillance coverage that are safely separated by a surveillance standard distance (say, 5 NM) are unexpectedly no longer separated by a procedural standard distance (say 15 mins), due to an unplanned surveillance outage.

9.1.3 In general, reliability is determined by design (see para 9.3 B below)

9.2 Availability

9.2.1 Availability is a measure of how often the system is available for operational use. It is usually expressed as a percentage of the time that the system is available.

9.2.2 Poor availability usually results in loss of economic benefit because efficiencies are not available when the ATC system is operating in a degraded mode (eg using procedural control instead of say 5 NM separation).

9.2.3 Planned outages are often included as outages because the efficiencies provided to the Industry are lost, no matter what the cause of the outage. However, some organisations do not include planned outages because it is assumed that planned outages only occur when the facility is not required.

9.2.4 Availability is calculated as

Availability (Ao) = MTBF/(MTBF+MDT)

where MTBF= Mean Time Between SYSTEM Failure
MDT = Mean Down Time for the SYSTEM

The MDT includes Mean Time To Repair (MTTR), Turn Around Time (TAT) for spares, and Mean Logistic Delay Time (MLDT)

NB: This relates to the failure of the system to provide a service, rather than the time between individual equipment failures. Some organisations use Mean Time Between Outage (MTBO) rather than MTBF.

9.2.5 Availability is directly a function of how quickly the SYSTEM can be repaired. Ie: directly a function of MDT. Thus availability is highly dependent on the ability & speed of the support organisation to get the system back on-line.

9.3 Recommendations for high reliability/availability ADS-B systems

A : System design can keep system failure rate low with long MTBF. Typical techniques are

- to duplicate each element and minimise single points of failure. Automatic changeover or parallel operation of both channels keeps system failure rates low. Ie: the system keeps operating despite individual failures. Examples are :
  - Separate communication channels between ADS-B ground station and ATC centre preferably using different technologies or service providers eg one terrestrial and one satellite
- Consideration of Human factors in design can reduce the number of system failures due to human error. Eg inadvertent switch off, incorrect software load, incorrect maintenance operation.
- Take great care with earthing, cable runs and lightning protection to minimise the risks of system damage
- Take great care to protect against water ingress to cables and systems
- Establish a system baseline that documents the achieved performance of the site that can be later be used as a reference. This can shorten troubleshooting in future.
- System design can also improve the MDT by quickly identifying problems and alerting maintenance staff. Eg Built in equipment test (BITE) can significantly contribute to lowering MDT.

B: Logistics strategy aims to keep MDT very low. Typical strategies are :

- Establish availability and reliability objectives that are agreed organisation wide. In particular agree System response times (SRT) for faults and system failure to ensure that MDT is achieved. An agreed SRT can help organisations to decide on the required logistics strategy including number, location and skills of staff to support the system.
- Having appropriate maintenance support contracts in place so that faulty modules are repaired within contractually defined times – preferably with contractual incentives/penalties for compliance. Such support contracts are best negotiated as part of the acquisition contract when competition between vendors is at play to keep costs down. Sometimes it is appropriate to demand that the support contractor also keep a certain level of buffer stock of spares “in country”.

It is strongly recommended that maintenance support is purchased under the same contract as the acquisition contract.

- Establish baseline preventative maintenance regimes including procedures and performance inspections in conjunction with manufacturer recommendations for all subsystems
- Use remote control & monitoring systems to identify faulty modules before travel to site. This can avoid multiple trips to site and reduce the repair time
- Have handbooks, procedures, tools available at the site or a nearby depot so that travel time does not adversely affect down time
- Have adequate spares and test equipment ready at a maintenance depot near the site or at the site itself. Vendors can be required to perform analysis of the number of spares required to achieve low probability of spare "stock out"
- Have appropriate plans to cope with system and component obsolescence. It is possible to contractually require suppliers to regularly report on the ability to support the system and supply components.
- Have ongoing training programs and competency testing to ensure that staff are able to perform the required role

The detailed set of operational and technical arrangements in place and actions required to maintain a system through the lifecycle are often documented in a Integrated Logistics Support Plan.

C: Configuration Management aims to ensure that the configuration of the ground stations is maintained with integrity. Erroneous configuration can cause unnecessary outages. Normally configuration management is achieved by :

- Having clear organizational & individual responsibilities and accountabilities for system configuration.
- Having clear procedures in place which define who has authority to change configuration and records of the changes made including, inter alia
  - The nature of the change including the reason
  - Impact of the change & safety assessment
  - An appropriate transition or cutover plan
  - Who approved the change
  - When the change was authorized and when the change was implemented
- Having appropriate test and analysis capabilities to confirm that new configurations are acceptable before operational deployment.
- Having appropriate methods to deploy the approved configuration (Logistics of configuration distribution). Suggested methods;

- Approved configuration published on intranet web pages
- Approved configuration distributed on approved media

D: Training & Competency plans aim to ensure that staff have the skills to safety repairs Normally this is achieved by :

- Conduct of appropriate Training Needs Analysis (TNA) to identify the gap between trainee skill/knowledge and the required skill/knowledge.
- Development and delivery of appropriate training to maintainers
- Competency based testing of trainees
- Ongoing refresher training to ensure that skills are maintained even when fault rates are low

E: Data collection & Review :

Regular and scheduled review should be undertaken to determine whether reliability/availability objectives are being met. These reviews need to consider :

- Reports of actual achieved availability & reliability
- Data regarding system failures including "down time" needs to be captured and analysed so the ANSP actually knows what is being (or not being) achieved.
- Any failure trends that need to be assessed. This requires data capture of the root cause of failures
- Any environmental impacts on system performance, such coverage obstructions such as trees, planned building developments, corrosion, RFI etc. Changes in infrastructure may also be relevant including airconditioning (temperature/humidity etc) and power system changes.
- System problem reports especially those that relate to software deficiencies (design)
- System and component obsolescence
- Staff skills and need for refresher training

– – – – – – – – – – – –