

## SECTION 2

### CHAPTER 24 (PRELIMINARY DRAFT V0.9 – SUBJECT TO CHANGE)

## FLIGHT AND MISSION PLANNING SYSTEMS

### INTRODUCTION

1. Traditionally, manual methods (e.g. chinagraph pencil routes/notes on maps, manual calculations), rules of thumb (e.g. 220knots, 400lb/hr), and ad hoc computational tools (e.g. spreadsheets) were used for flight and mission planning. However the proliferation of computer-based Flight and Mission Planning Systems (hereafter referred to as MPS) provide substantial efficiencies for aviation flight and mission planning over the traditional approaches to flight planning. MPS also reduce the need to spend precious on-aircraft time manually entering large amounts of flight and mission data into modern Flight Management Systems (FMS) and Mission Computers (MC) by allowing the operator to prepare the data on a desktop computer system in an office environment or operations room beforehand. Some MPS applications are also suitable for use on portable computers and Electronic Flight Bags (EFBs) as discussed in Section 2 Chapter 22.
2. MPS consist of software applications that allow maps, charts, weather, intelligence and aircraft performance data to be used in developing navigation solutions (e.g. routes, approaches, terminal procedures), communication settings, flight/mission calculations (fuel, leg times, etc), and other pertinent aircraft operational data. MPS may include visual software tools optimised for specific aircraft roles, and automate the computations associated with aircraft specific flight/mission planning. Once the mission information has been generated, it is printed (e.g. kneeboards, strip charts), or alternatively written onto a data storage device (e.g. PCMCIA flash disk, or proprietary data transfer module) for transfer to aircraft systems (e.g. FMS, navigation system, EFB). Some modern MPS also include functions to transmit and receive flight/mission information via datalink, either at the commencement of a flight/mission, or as real time updates throughout a flight/mission. MPS may also be used for post-flight/mission debriefing.
3. The advancement of performance based navigation, and the aircraft equipment that supports these types of navigation, are resulting in MPS being used in more challenging and potentially hazardous ways (e.g. aeronautical data supporting required navigation performance). Aircraft equipment approvals underpinning the navigation performance of an aircraft require that valid navigation data, processed using appropriately assured software tools, is sourced from accredited suppliers. Therefore, any MPS applications transferring, translating, manipulating or generating aeronautical information in this context should be designed and assured commensurate with the integrity requirements for the data they process.

### SCOPE AND APPLICABILITY

4. This chapter provides guidance for the technical approval, service release and management of MPS that are used by ADF operators for flight or mission planning off-aircraft. Where MPS applications are hosted on Electronic Flight Bags (EFB) for on-aircraft use, then this chapter should be read in conjunction with Section 2 Chapter 22 *Electronic Flight Bags* and where there are conflicting requirements, the more onerous should be satisfied.
5. The ADF guidance presented in this chapter is based on the aeronautical data tool qualification and management requirements of the Federal Aviation Administration (FAA) framework, although in bringing the guidance into the ADF domain there are a number of important differences. While the guidance primarily focuses on technical issues, it also provides suggestions for operational management of MPS where necessary to complement or supplement the technical requirements.

### FAA FRAMEWORK

6. The FAA's aeronautical data regulations provide a suitable basis for ADF regulation of MPS. A brief understanding of the FAA system therefore provides useful context to the reader of this chapter.
7. The FAA framework relevant to MPS is documented in orders, guidance and standards related to:
  - a. flight planning applications – usually associated with Electronic Flight Bags (EFB), and
  - b. aeronautical data processing applications – usually associated with the development, manipulation and generation of digital aeronautical databases.

8. Note that while the FAA do not use the term MPS to describe these applications, the ADF use of MPS encompasses both flight planning and aeronautical database processing. The FAA has published the following documents relating to the approval of applications typically included in MPS, and the systems on which they are hosted (e.g. desktop PCs and EFBs):

- a. *RTCA/DO-200A – Standards for Processing Aeronautical Data* describes the requirements for the processing of aeronautical data including tool qualification requirements.
- b. *RTCA/DO-201A – Industry Requirements for Aeronautical Information* specifies the aeronautical data elements required by the aviation industry and a standard for the accuracy, resolution, and integrity of the associated values.
- c. *FAA Advisory Circular (AC) AC20-153 – Acceptance of Data Processes and Associated Navigation Databases* describes how to evaluate whether data processes comply with the requirements of RTCA/DO-200A.
- d. *FAA Advisory Circular (AC) 120-76A – Guidelines for the Certification, Airworthiness, and Operational Approval of Electronic Flight Bag Computing Devices* describes the approval criteria for MPS applications hosted on EFBs in civil aviation.

9. The FAA framework can be summarised as consisting of the following key steps:

- a. identify the *aircraft functions* and associated functional *failure conditions* of the data processed by the flight planning / aeronautical database application;
- b. identify which flight planning / aeronautical database application components process the data;
- c. identify the role in the aeronautical data process the flight planning / aeronautical database application components achieve, such as assemble, translate, select, format and distribute (as described in RTCA/DO-200A);
- d. determine the *data criticality* of flight planning / aeronautical database application components based on the severity of aircraft functional *failure conditions* and the role of the application components;
- e. allocate *data assurance levels* to the flight planning / aeronautical database application components based on the *data criticality*; and
- f. assure the design integrity of the flight planning / aeronautical database application components as per the requirements of the *data assurance level*, involving the application of:
  - (1) design features (validation) to assure that the data is applicable to the identity ascribed to it;
  - (2) design features (verification) to detect and handle instances of when the technical content of the data is inadvertently modified; and
  - (3) software design assurance to prevent the technical content of the data being inadvertently modified.

10. Note that FAA terminology for MPS applications hosted on EFBs differs slightly from that used above, however the process and outcomes are consistent. Refer to Section 2 Chapter 22 for further information on how EFB applications are categorised and assurance requirements prescribed.

11. **Relationship to the Safety Assessment.** The *failure condition* definitions used by the FAA for flight planning and aeronautical data are intended to be compatible with the existing aircraft safety assessment process and design assurance requirements of ARP4754/4761 and RTCA/DO-178B, as presented in Table 1. The *data criticality* and *data assurance level* are aligned to the existing *failure condition* definitions, also as shown in Table 1.

ARP4754/4761 and RTCA/DO-178B			RTCA/DO-200A/201A		
Aircraft Functional Failure Condition Category	Effect	Design Assurance Level	Data Criticality for Data Supporting the Aircraft Function	Definition	Data Assurance Level
Catastrophic	Failure condition would prevent continued safe flight and landing.	A	Critical	The data, if erroneous, would prevent continued safe flight and landing or would reduce the ability to cope with adverse operating conditions to the extent that there is a large reduction in safety margins or functional capabilities. There is a high probability when trying to use corrupted critical data that an aircraft would be placed in a life threatening situation.	1
Hazardous / Severe-Major	Failure conditions that would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be: (1) a large reduction in safety margins or functional capabilities, (2) physical distress or higher workload such that the crew could not be relied on to perform their tasks accurately or completely, or (3) adverse effects on occupants including serious or potentially fatal injuries to a small number of those occupants.	B	Critical		1
Major	Failure conditions that would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to occupants, possibly including injuries.	C	Essential	The data, if erroneous, would reduce the ability to cope with adverse operating conditions to the extent that there is a significant reduction in safety margins. There is a low probability when trying to use corrupted essential data that an aircraft would be placed in a life threatening situation.	2
Minor	Failure conditions that would not significantly reduce aircraft safety, and that would involve crew actions that are well within their capabilities. Minor failure conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some inconvenience to occupants.	D	Essential		2
No Safety Effect	Failure conditions that do not affect the operational capability of the aircraft or increase crew workload.	E	Routine	The data, if erroneous, would not significantly reduce aircraft safety. There is a very low probability when trying to use corrupted routine data that an aircraft would be placed in a life threatening situation.	3

**Table 1:** Relationship between Failure Condition Categories and Data Process Assurance Levels

**12.** For example, consider the *aircraft function* ‘Navigation’ for which misleading and/or malfunction without warning is a ‘Hazardous’ *failure condition* for precision approaches. Digital aeronautical data supporting the conduct of the precision approach would be assessed using Table 1 as ‘Critical’ and would require assurance to ‘Data Assurance Level 1’. Any flight planning or aeronautical database application processing this data would require its role in processing the data assessed and its design integrity assured commensurate with ‘Data Assurance Level 1’.

## ADF APPROACH FOR MISSION PLANNING SYSTEMS

13. Of the recognised civilian and military Airworthiness Authorities, the FAA has the most mature and available policy and guidance on aeronautical data processing functions carried out by aeronautical data process applications. In addition, the FAA policy is consistent with the data classifications and requirements defined by ICAO, and internationally recognised aeronautical data standards such as RTCA/DO-200A and RTCA/DO-201A. For these reasons, the ADF approach to MPS has been developed to address relevant factors relating to aeronautical data processing identified in the FAA policy, ICAO requirements, and the related standards. However, in bringing the guidance into the military domain, recognising that many MPS systems are acquired through the restricted arrangements of United States Foreign Military Sales, and recognising some of the additional functions carried out on military MPS that have no civilian equivalent or do not relate to the processing of aeronautical data, the ADF approach has some specific differences. The ADF approach, and the differences to the FAA approach, are discussed in this section.

14. Perhaps the most significant difference between the FAA approach and the ADF approach is the focus of the assessment. FAA policy focuses on the aeronautical data processing chain from source to use. The ADF, on the other hand, will look to assess an MPS as part of the Design Acceptance process. As such, some aspects of FAA policy are not considered when assessing an MPS, or are only assessed to the extent that they are relevant to the MPS. FAA policy defines a number of data quality attributes, only some of which are directly applicable to an MPS. This chapter focuses on those data quality attributes, such as data assurance, that are most directly influenced by an MPS. An MPS will also have a role in preserving other data quality attributes, such as accuracy, resolution, completeness and format. This role should be defined through functional requirements, the satisfaction of which can be assured through the techniques described in this chapter.

### Acquisition of MPS by the ADF

15. MPS have historically been acquired and modified for the ADF through a number of quite disparate means. The following paragraphs discuss these means and the impact this has on the ADF approach to the assurance and acceptance of MPS.

16. **MPS developed for the ADF.** Where MPS applications/components are being developed specifically for the ADF, it is possible to specify software assurance requirements in the acquisition and sustainment contracts for the development and support of these systems. In these cases the ADF should specify the equivalent benchmarks as used by the FAA as described by paragraphs 6-10 and at annex A of this chapter and where necessary, as adapted by this chapter for applicability to the ADF use of MPS.

17. However, recognising the potential cost of compliance with rigorous software assurance standards, the Commonwealth should be specific, where possible, which software components within the MPS require rigorous software assurance, versus those that simply require a quality development and support process. For example, those MPS components associated with Critical aeronautical data supporting Required Navigation Performance (RNP) should be targeted.

18. **MPS modified for the ADF.** Where existing COTS or MOTS MPS application/components are being modified for ADF purposes, it is highly desirable to apply the standards prescribed for MPS developed specifically for the ADF (paragraphs 16 and 17) to those components modified for the ADF and those containing critical aeronautical data to ensure the MPS products we acquire are of suitable integrity. However, in many cases this may not be possible, particularly if the modifications involve only limited or targeted changes to an existing MPS suite. In these cases, the ADF may be better off conducting a retrospective assessment of the existing MPS product, with consideration for the ADF modifications and critical data elements, using the process described at paragraphs 21 through 38 of this chapter.

19. **MPS Acquired with Airworthiness Authority Oversight.** The two most common MPS in ADF use are the Portable Flight Planning System (PFPS) and Joint Mission Planning System (JMPS). Both of these MPS are acquired and modified through recognised military Airworthiness Authorities (i.e. the USAF and USN respectively). As the ADF is typically not a significant stakeholder in the initial development and ongoing support and evolution of these products, there is often limited opportunity for the ADF to specify design requirements and software assurance requirements for these products.

20. For MPS acquired with Airworthiness Authority oversight, recognition of prior acceptance (RPA) is likely to be sought to the maximum extent possible. In principle, this approach is sound, however a number of important considerations apply. Even when a recognised Airworthiness Authority has accepted an MPS, the ADF should still conduct an assessment of the design features (e.g. means used for digital error detection, etc) against the ADF's intended use of MPS functions, and the target systems or paper products for the data produced by the MPS, to ensure the ADF Configuration, Role and Environment (CRE) has been adequately considered and that the Airworthiness

Authority (particularly military authorities) have not retained intolerable risk any risks which the ADF cannot reasonably tolerate in their approvals. In these cases a combination of RPA coupled with ADF evaluation of the MPS should be used to determine the extent to which the MPS incorporate applicable verification and validation design features, and to determine the extent to which the recognised Airworthiness Authority has assured the MPS. This approach is described at paragraphs 40 through 45.

### RETROSPECTIVE ASSESSMENT OF MPS INTEGRITY

**21.** For some MPS acquisitions it is not possible to inject design and software assurance requirements into the development of the MPS. This may be because the MPS is being acquired via US Foreign Military Sales, or from an existing COTS civil or MOTS military flight/mission planning product. In these situations, a retrospective assessment of the MPS should be conducted to determine the extent to which the MPS design is adequately assured for its intended use. The retrospective assessment approach is only intended for those circumstances where the ADF is not able to inject design requirements into the MPS development.

**22.** The principle behind the ADF retrospective assessment is to establish of the adequacy of MPS design features to provide assurance that the integrity of source data is preserved by the MPS application in producing an on-aircraft data set from the source data; and that data manipulated or generated by the MPS (automatically, or through manual user input, or combination thereof) is valid for its intended use. Software assurance requirements will still be relevant (including benchmarks for adequacy of testing), however, their application will be constrained to relevant functions or applications within the MPS that process critical aeronautical data. The following paragraphs describe the retrospective assessment approach.

**23.** The retrospective assessment approach is based around an evaluation of the following factors affecting the function and application of the MPS:

- a.** how the data is used by the aircraft – to determine the consequence of the failure modes associated with errors or faults in the data;
- b.** the source data used by the MPS – to ensure that the integrity of the data is appropriate (includes data accuracy, format, completeness) for the intended use by the aircraft or aircrew; and
- c.** the functions carried out by the MPS with this data (e.g. transfer, formatting, manipulation, generation) – to ensure that relevant design measures have been implemented to preserve data integrity, or provide validation of data manipulated or generated by the MPS (automated and/or manual entry).

**24.** The goal of the assessment is to determine which design features are in place to detect or handle possible sources of aeronautical data errors, or whether the Commonwealth should pursue evidence of the absence of data processing faults (which may involve specification of software assurance requirements, seeking evidence of rigorous robustness testing, rigorous robustness testing by the ADF acceptance agency (e.g. CISSO-DMO), etc). The following three sections provide guidance on evaluating the three issues identified in paragraph 23.

#### Assessing the Use of Aeronautical Data on the Aircraft

**25.** The first step of the assessment is to determine how the data is used by the aircraft. The data may be used:

- a.** in digital format by aircraft systems such as flight management systems, mission computers, navigation systems, flight directors, autoland systems, etc.; or
- b.** in paper format by aircrew as references throughout the flight, in such formats as printed kneeboards and strip charts.

**26.** For each aircraft system that uses aeronautical data, the assessment should identify which specific data elements are used by the aircraft system, and for what purposes. An error or fault with each of these data elements should then be assessed against the failure conditions presented in Table 1. RTCA/DO-201A provides additional guidance on the integrity classification of aeronautical data elements. For example, RTCA/DO-201 presents the classifications of aeronautical data elements to support RNAV as defined in RTCA/DO-236 and to support GNSS precision approach operations as defined in RTCA/DO229B and RTCA/DO-245. For mission systems, missionised hazard classifications should be used as presented in Section 2 Chapter 7. Table 2 presents an example (extract only) of an aeronautical data use assessment.

Aircraft System / Aircrew Paper Product	Aeronautical Data Element	Minimum Data Accuracy	Failure Condition Category for erroneous data	Data Process Assurance Level
Flight Management System / Autoland System	CAT I/II/III Rwy End and Landing Threshold Location	1m	Major	Essential (Assurance Level 2)
	ILS Glide Slope Antenna Location	3m	Major	Essential (Assurance Level 2)
Flight Management System / GPS Navigation	Threshold Crossing Height (GNSS)	0.05m	Hazardous	Critical (Assurance Level 1)
Flight Management System	Airspace Boundary Points	1sec	No Safety Effect	Routine (Assurance Level 3)
	Terminal / Approach Routes	1deg	No Safety Effect	Routine (Assurance Level 3)
Kneeboard Approach Plate*	VHF Navaid – Terminal Location	30m	Major	Essential (Assurance Level 2)
{etc...}				

**Table 2:** Example Aeronautical Data Use Assessment (Extract Only)

27. The minimum data accuracy requirements and assigned data process assurance levels are then used to determine the adequacy of sourced data, and the appropriateness for the MPS applications, as explained in the next section.

### Assessing the Adequacy of Source Data

28. Having determined the data process assurance levels applicable to the aircraft type being assessed, the next step is to assess whether the source data being used by the MPS meets accuracy and integrity requirements. This may be achieved by sourcing data from an appropriately accredited data provider (i.e. an organisation accredited by the ADF or another airworthiness authority to meet the requirements of RTCA/DO-200A, e.g. RAAF AIS once they are accredited), and assessing that the accredited data supplier, provides data of the appropriate integrity classification.

29. FAA AC20-153 describes two types of data supplier accreditations:

- a. *Type 1 Letter of Acceptance (LOA)* provides recognition of a data suppliers' compliance with RTCA/DO-200A with no identified compatibility with an aircraft system.
- b. *Type 2 Letter of Acceptance (LOA)* provides recognition of a data suppliers' compliance with RTCA/DO-200A and the compatibility of their delivered data with particular avionics systems.

30. If the data is sourced from an accredited data supplier with a Type 1 LOA, then the source data will still require assessment for compatibility with the particular avionics system, and how this contributes to the host platform's navigation performance requirements. If the data is sourced from an accredited data supplier with a Type 2 LOA, then compatibility with the particular avionics system is already assured, provided the ADF installation or use of that system does not vary from the Type 2 LOA's context. If an accredited data provider is not available, then data validation should be undertaken on the source data in accordance with those approaches identified in Annex A of this chapter and Appendix C to RTCA/DO-200A.

### Assessing the MPS Functions

31. Having established that the source data for the MPS is commensurate with the accuracy and integrity requirements of the aircraft use, the next step of the assessment of the MPS applications is three fold. The MPS should be assessed to ensure that:

- a. the accuracy and integrity of data is preserved as it is passed through the MPS applications/components;
- b. the accuracy and integrity of data is preserved as it is translated, reformatted or manipulated by the MPS applications/components; and
- c. any generation of data by the MPS meets the accuracy and validity requirements of the aircraft use.

32. Two sources of hazardous outcomes must be assessed:
- a. those caused by operators inadvertently entering erroneous data, and
  - b. errors caused by system technical aberrations (either an error in the manipulation of trusted data, and/or invalid data in source data).
33. **MPS Functional Guidewords.** To allow an association of relevant design features and assurance requirements with MPS functional components, it is necessary to define a means of categorising MPS functions. In RTCA/DO-200A this is done using the data processing phases of receive, assemble, translate, select, format and distribute. However these terms are defined in the context of the whole aeronautical data process, and not just MPS components. Therefore, the ADF approach defines the following guide words for MPS components:
- a. **Transfer.** The MPS directly transfers the source data to the data transfer device, in the same format, without change. This type of MPS function is suitable for protection using digital error detection mechanisms as described at Annex A.
  - b. **Format.** The MPS takes static source data, and through a set of pre-defined formatting requirements, reformats the source data into a new format for writing to the data transfer device. The extent of changes to the source data is confined to format changes (e.g. DAFIF to ARINC424), including the unit changes, word data type, and frame packing strategy. The unit changes (e.g. meters to feet) will involve some form of calculation. The MPS does not generate any new information as a result of dynamic source data or user input. Feedback and independent redundancy are the most suitable means of MPS components determining if errors have been introduced into the data, as described at Annex A.
  - c. **Manipulation.** The MPS takes a combination of static and dynamic source data, and through a set of pre-defined requirements, manipulates (or translates) the source data for writing to the data transfer device. Manipulation may include the production of new information as a result of calculations based on static source data, but does not include the provision of data input by the user. Feedback and independent redundancy are the most suitable means of MPS components determining if errors have been introduced into the data, as described at Annex A.
  - d. **Generation.** Through a combination of static and dynamic source data, and keyboard input from the user, the MPS generates new data to be loaded onto the data transfer device. The validation methods described at Annex A are the most suitable methods of ensuring the resultant generated data is valid.
34. The guidewords, in conjunction with the data assurance level of the aeronautical data element in question, are used to determine which design features or assurance requirements the assessment requires evidence of (refer Table 3). Refer to Annex A for definitions of these detection and handling design features. The alternative to detection and handling design features identified in Table A-3 is to assure that design faults that could introduce errors are absent. Of course, the absence of design faults cannot be conclusively demonstrated. Software assurance techniques are used to provide confidence, commensurate with the severity of failure, that design faults are absent.

MPS Functional Guideword	Data Assurance Level	Detection and Handling	OR	Absence
Transfer	1 (Critical)	Digital Error Detection <sup>1</sup> OR Feedback / Read back Verify <sup>2</sup>	OR	MPS components that perform the Transfer are qualified commensurate with RTCA/DO-178B Level A or B.
	2 (Essential)	Digital Error Detection <sup>3</sup> OR Feedback / Read back Verify <sup>4</sup>	OR	MPS components that perform the Transfer are qualified commensurate with RTCA/DO-178B Level C or D*.
	3 (Routine)	No detection and handling required	OR	No absence required
Formatting	1 (Critical)	Feedback / Reversibility Check <sup>2</sup> OR Independent Redundancy <sup>5</sup>	OR	MPS components that perform the Formatting/Translation are qualified commensurate with RTCA/DO-178B Level A or B.
	2 (Essential)	Feedback / Reversibility Check <sup>4</sup> OR Independent Redundancy <sup>6</sup>	OR	MPS components that perform the Formatting/Translation are qualified commensurate with RTCA/DO-178B Level C or D*.
	3 (Routine)	No detection and handling required	OR	No absence required
Manipulation / Generation	1 (Critical)	Feedback / Reversibility Check <sup>2</sup> OR Independent Redundancy <sup>5</sup>	OR	MPS components that perform the Manipulation are qualified commensurate with RTCA/DO-178B Level A or B.
		AND Logical Consistency Checks OR Semantic Consistency Checks		
	2 (Essential)	Feedback / Reversibility Check <sup>4</sup> OR Independent Redundancy <sup>6</sup>	OR	MPS components that perform the Manipulation are qualified commensurate with RTCA/DO-178B Level C or D*.
		AND Logical Consistency Checks OR Semantic Consistency Checks		
	3 (Routine)	No detection and handling required	OR	No absence required

Notes:

- 1: MPS components that generates and performs the Digital Error Detection should be qualified commensurate with RTCA/DO-178B Level A/B
- 2: MPS components that perform the Feedback should be qualified commensurate with RTCA/DO-178B Level C
- 3: MPS components that perform the Digital Error Detection OR Feedback / Read back Verify should be qualified commensurate with RTCA/DO-178B Level C or D\*
- 4: MPS components that perform the Feedback should be qualified commensurate with RTCA/DO-178B Level D or Verification Tool Requirements
- 5: At least one of the MPS components that constitute the Independent Redundancy should be qualified commensurate with RTCA/DO-178B Level C or D\*
- 6: At least one of the MPS components that constitute the Independent Redundancy should be qualified commensurate with RTCA/DO-178B Level D or Verification Tool Requirements

\*: Note the different between RTCA/DO-178B Level C and D is notable, and therefore the safety assessment process must make it explicit which severity failure condition the data element relates to. It also means there may be limitations to the extent to which tools used for Essential data in one context may be used in an alternative context.

Note that the Digital Error Detection qualification requirements (e.g. generate and check) are more onerous than the other verification techniques as the generated Digital Error Detection code is typically used by other downstream data processing tools/steps for error detection.

**Table 3:** Design and Assurance Requirements for MPS Functions

**35.** Table 4 provides a template (and limited examples, including an assurance shortfall against MPS Component P) for the purposes of illustrating the conduct and documenting of the MPS design and assurance assessment against the criteria of Table 3. The assessment involves working backwards from the data outputs of the MPS back through the affected MPS components. Annexes B – D provide examples of possible MPS Data Sources, MPS Functions / Applications and MPS Output Data and Formats for consideration in the MPS assessment. Note that Annex D is not a complete list and should be used only as a prompt for possible factors to consider. The MPS data sources, functions, application and output data of the MPS product in question should all be analysed.

**36.** Significant amounts of aeronautical data may be processed by an MPS. In assessing the MPS, this aeronautical data will invariably be grouped to some extent. It is acceptable for a technical assessment to group aeronautical data provided the same criticality can be assigned to each data element in the group and the description of the group is sufficiently accurate for external organisations to validate the criticality. In general, descriptions should link to functions and not to data transfer mediums.

Aircraft System Data Element <i>{list each data element, starting with the most Critical, followed by Essential and then Routine}</i>	Data Criticality / Data Assurance Level <i>{Critical – Assurance Level 1, Essential – Assurance Level 2, Routine – Assurance Level 3}</i>	MPS Components and Functions		Detection/Handling OR Absence <i>{identify the detection / handling mechanisms or software assurance evidence relevant to assuring the integrity of the data element}</i>
		MPS Component <i>{list each MPS Component that processes the Data Element}</i>	MPS Functional Guideword <i>{record the functional guideword for the MPS component}</i>	
Data Element A	Critical – Assurance Level 1	MPS Component X	Transfer	<u>Detection:</u> Digital Error Detection using a CRC check. CRC Generator assured commensurate with RTCA/DO-178B Level A – reference to Level A assessment.
		MPS Component Y	Translation	<u>Detection:</u> Feedback / Reversibility Check
		MPS Component Z	Manipulation	<u>Absence:</u> MPS Component Z assured commensurate with RTCA/DO-178B Level B – reference to Level B assessment.  Semantic Consistency Check – reasonability (range, resolution)
Data Element B	Essential – Assurance Level 2	MPS Component P	Transfer	**No evidence of Detection/Handling or Absence**
		MPS Component Q	Manipulation	<u>Detection:</u> Independent Redundancy with Component R  Logical Consistency Check using Component R and alternative data source XY
{etc. ...}				

**Table 4:** Template/Examples for MPS Component Functional Assessment

**Managing Deficiencies Identified in the Assessment**

37. When assessing an MPS retrospectively, the assessor will inevitably identify deficiencies against the aforementioned criteria. If the MPS is relatively robust, these deficiencies should be isolated. On the other hand if the MPS is being used for more critical data than what it was originally designed for, then the shortfalls may be more widespread.
38. Once the deficiencies are identified, the assessor should determine how to treat the deficiencies. Deficiencies may be treated in one of the following ways (with precedence for the treatments listed first over those listed last).
  - a. **Design Assurance.** Produce or acquire the additional analysis and test evidence to satisfy the prescribed assurance requirements. This may even involve a design change where the assurance shortfalls are substantial.
  - b. **Detection and Handling Mechanisms.** Introduce additional MPS design features (*Digital Error Detection, Feedback, Independent Redundancy*) to provide detection and handling of any errors caused from the design assurance shortfalls. Ensure that any of these mechanisms introduced are adequately assured.
  - c. **Operational Limitations.** Propose operational limitations and procedures to reduce the criticality of the associated data element, such that the design assurance shortfalls are no longer shortfalls at the revised data criticality level. For example, many of the critical data elements in RTCA/DO-201 are associated with GNSS based precision approaches, and thus limiting aircraft operation to non-precision approaches may be a suitable limitation in this case.
  - d. **Independent Verification.** In some cases, it may be possible to treat shortfalls in the assurance of an MPS. Rather than relying on the output of the MPS being correct, operators may independently verify each data element each and every time the MPS is used. As manually inspecting data is a notoriously unreliable means of detecting errors, independent verification may only be a suitable treatment where the amount of data to be inspected is not extensive and the expected data values can easily be

determined. As this is a procedural control, independent verification may not be a suitable treatment for shortfalls in the assurance of Critical data.

- e. **Risk Retention.** Refer risk to the OAA via an issue paper through the TAA, disclosing why the preferable options above were not pursued and quantify this in AVRVM risk terms.

**39.** A period of operational use is not a suitable substitute for design assurance unless structures are put in place to compare the extent of operational use against design assurance goals. Even if such structures are put in place, operational use of an MPS can only ever provide confidence at the lowest level of safety-related functions (i.e. operational use could only ever satisfy the DO-178B Level D software assurance objectives). There are two primary reasons why a period of operational use is not a suitable substitute for design assurance:

- a. Design assurance concepts provide confidence in the correct operation of a system not only through verification of correct functionality for the range of expected use, but also through verification that system responses to unexpected usage are appropriate. Verifying system response to unexpected inputs is critical to assuring safe operation as, while every effort is made to assure correlation, there is often a difference between the expected range of use and the actual range of use. Furthermore, the most common cause for systematic failure condition contributions to accidents is exposure to unexpected inputs or usage. A period of operational use early in the MPS lifecycle is unlikely to expose the MPS to the same range of unexpected inputs that would be seen through application of design assurance concepts.
- b. MPS usage early in the lifecycle is likely to differ from MPS usage later in the lifecycle. There are a number of potential reasons for this difference, including expansion of the types of mission plans, optimisation of operational processes, increased operator familiarity with the system and so on. Any confidence that can be obtained through the initial phase of use cannot be extended to latter phases as it is possible that the different usage later in the lifecycle may expose faults that were not seen for the limited range of use early in the lifecycle.

#### MPS DESIGN ACCEPTANCE USING RECOGNITION OF PRIOR ACCEPTANCE

**40.** The intent of informed RPA by a recognised Military Airworthiness Authority (MAA) as defined in accordance with TAREG 2.2.7 is that their products can be considered acceptable for the ADF provided:

- a. the ADF can determine that the elements of the MAA involved in the development and release of the product have acted in the capacity as an airworthiness authority (and not just a project/contract management authority);
- b. the ADF can determine that the products intended for the ADF have been exposed to an equivalently broad suite of design assurance, verification and validation activities as normally applied to products used by the MAA, else there are obligations on the ADF to address the shortfalls;
- c. the ADF comprehensively understands any risks that the MAA may have retained in their acceptance and release to service of the product, such that the ADF can determine if the risks are tolerable; and
- d. the products are comprehensively assessed as appropriate for the relevant ADF MPS and associated aircraft CRE, including any specific differences between ADF navigation authorisations and the MAA's.

**41.** In order for the Design Acceptance Strategy (DAS) for a MPS to utilise RPA, additional assessments are required to confirm the appropriateness of RPA, and to treat any shortfalls in the scope of MAA acceptance as applicable to the ADF products. The following paragraphs identify the key elements that should constitute the DAS for the MPS using RPA. These paragraphs reflect those assessments required to establish and address limitations in the applicability of RPA, as well as those assessments to address MPS specific issues.

**42. Involvement as an Airworthiness Authority.** The assessment should establish the role that each of the MAA agencies has played in the release of each MPS component (ADF common and non-common), and how these agencies have acted in the capacity as an airworthiness authority. The assessment should be cognisant of the differences in role between project management authority activities, and those activities addressing technical airworthiness outcomes. Any substantial shortfalls identified will require treatment by the ADF.

**43. Common MPS Components.** For MPS components that are entirely common between the ADF and MAA configuration, the ADF should conduct the following activities:

- a. **Prior Acceptance.** The assessment should obtain evidence of MAA acceptance of the MPS components that specifically includes relevant engineering acceptance and release to service activities. The assessment should ensure that the MPS components/modules to which the MAA acceptance/release applies to are clearly identified and what the scope of acceptance/release is.
- b. **ADF Configuration, Role and Environment.** For common MPS components, the ADF should determine whether there are any role or environment differences that would alter the reliance that is placed on the MPS. Where the ADF, through conduct of a different role or operation in a different environment, places greater reliance on the MPS than the MAA, the ADF must determine whether the integrity of the MPS is commensurate with that reliance. Where it is not, the ADF may need to conduct additional verification activities or engage the MAA to provide additional oversight.
- c. **Retention of Risk.** The assessment should obtain evidence that the MAA has not retained risks associated with any MPS design or assurance shortfalls, defects or deficiencies that might be unacceptable to the ADF. The assessment should:
  - (1) obtain the MAA certification and verification reports for each MPS component;
  - (2) assess the problem reports raised/issues identified to determine the status of resolution, fix implemented or work around recommended;
  - (3) establish if the fix or workaround is acceptable to the ADF; and
  - (4) establish that the relevant workarounds have been incorporated into ADF instructions and procedures.

**44. Non-Common MPS Components.** For MPS components that are not common to the MAA's configuration including Australian unique, Australian modified or other custom components, the assessment should include the following activities:

- a. **Equivalent Rigour.** The assessment should obtain evidence that the MAA attests that the products would be suitable for release to the MAA – i.e. the products have been developed, verified and assessed as rigorously as the work done directly for the MAA for use by their own units. Any shortfalls compared with the MAA's benchmark, will require specific treatment by the assessment.
- b. **ADF Configuration, Role and Environment.** The assessment should obtain evidence that the Non-Common components have been developed cognisant of the ADF CRE. The assessment should assess the MPS application suite (including all components) paying specific attention to how the ADF intends to use it, compared with the MAA use of the application. This assessment should consider the role of MPS in the ADF mission planning process, processing of aeronautical information including data loaded digitally onto aircraft, and critical decisions involved in flight planning (e.g. vertical clearances, air routes, precision approaches, etc). The assessment should also consider the navigation authorisations in place for the ADF aircraft. One of the following approaches may be employed:
  - (1) **MAA understands ADF CRE.** Provided the assessment can establish that the MAA comprehensively understands the ADF CRE, and this knowledge has been robustly applied to their oversight of Non-Common components, then no further assessment is required by the ADF. This approach may be impractical for some elements of MPS, such as Flight Performance Models pertaining specifically to ADF aircraft.
  - (2) **ADF assesses CRE.** Alternatively, the assessment should obtain the relevant requirements documentation and test reports to make an explicit assessment of the behaviour of these products against the ADF's intended use. The CRE assessment of each should assess the MPS components should be based on against how the ADF intends to use the MPS, including compatibility with our aircraft configuration, other MPS components (common and ADF unique), and the target computer used to host the MPS. The problem reports raised should also be assessed to determine their status of resolution including the fix implemented or work around recommended; establish if the fix or workaround is acceptable to the ADF; and establish that the relevant workarounds have been incorporated into ADF instructions and procedures.

45. **Additional Factors.** The assessment should consider the following additional factors:
- a. **Compliance Assurance.** If there are any shortfalls in the MAA's execution of its responsibilities as an airworthiness authority for the MPS, then more substantial compliance assurance activities will be required. In this case, the assessment should establish whether the MAA has appropriate oversight of the MPS design agency contractors they employed to develop or modify MPS. This may entail involvement in relevant MPS working groups and project review boards. The assessment should also establish a documented understanding of the software development process employed by MPS design agency contractors to assess ongoing consistency in the application of development processes to builds for the ADF.
  - b. **Processing of Critical Aeronautical Data.** The PO should undertake an assessment (as per paragraphs 21 through 38 of this chapter) to establish whether new or modified MPS components process data that that would be considered Critical (in accordance with RTCA/DO-201), vice Essential or Routine, when used by the target ADF platform. For any data assessed as Critical, the assessment must ensure that the contractor and MAA has been comprehensive in their design assurance, verification and validation of impacted MPS components versus a benchmark commensurate with the Aeronautical Tool Qualification requirements as summarised in this chapter and described by RTCA/DO-200A, or that appropriate fault tolerance features are employed to reduce the need for a higher degree of design assurance. Any shortfalls should be communicated to the TAA/OAAR through an issue paper. As there are often shortfalls in meeting the design assurance requirements of RTCA/DO-200A for applications certified by MAAs, the assessment should pay particular attention to assessing what fault tolerant features are employed by the MPS. Such fault tolerance features should include those discussed at Annex A of this chapter.

### MPS DESIGN CONSIDERATIONS

46. The following paragraphs provide guidance on general design considerations for MPS. These design considerations are not intended to be a complete list of design considerations for MPS development; instead they are intended to highlight several key factors which have considerable potential to impact airworthiness.

47. **Human Machine Interface (HMI).** The MPS interface should provide a consistent and intuitive user interface within and across the various MPS functions and applications. The interface design, including but not limited to data entry methods, colour coding philosophies, and symbology, should be consistent across the MPS functions and applications. These applications should also be compatible with the aircraft systems in terms of data entry units, and calculation units, to avoid potential errors due to unit mismatch or conversion. Consideration should also be given to storing data internal to the MPS in the same format as either the source database or the target aircraft system to maximise opportunities for operator to detect errors in displayed or stored values. The HMI should be resistant to the operator inadvertently importing or using stale data from previous flights or aircraft. This is a known contributor to a number of accidents and incidents involving MPS applications such as the Boeing Laptop Tool (BLT) and other operator's/manufacture's MPS flight planning applications (e.g. 14 Oct 2004 Boeing 747-244B crash at Halifax International Airport, and 20 Mar 09 Emirates A340-500 tail strike at Melbourne Airport). While it is recommended to introduce reasonability checking into the software applications, MPS designers should be aware that such features may only provide a coarse value check, and often do not provide complete detection of stale data scenarios. A standardised methodology should be established for explicit default or starting values, with explicit indication or warning when data from other sources (previous flights, other aircraft, or alternative aircraft configurations) is used. Note that such methodologies may be required to span various MPS applications to avoid scenarios such as the use of weight and balance data from alternate aircraft configurations when performing performance calculations in another MPS module. For further information on HMI considerations, see Section 2 Chapter 13 of this publication.

48. **Target Computer.** Most MPS applications are hosted on COTS PC computing hardware, either configured as a stand-alone workstation, or as part of ADF network infrastructure. For MPS hosted on Defence networks, the applications are also required to meet relevant security policy for those environments. Some MPS applications are hosted on EFBs for use during flight. For requirements relating to hosting applications on EFBs refer to Section 2 Chapter 22.

49. When relying on Recognition of Prior Acceptance, the ADF will rely on civil or military airworthiness authority oversight of MPS verification activities. These verification activities will seek to confirm that the MPS operates as intended on the target hardware. The value of these verification activities may be diminished if the ADF employs the MPS on different hardware, which will often be the case when the MPS is hosted on a Defence network. The ADF must assure that the MPS is compatible with the target hardware upon which it is hosted. It is not necessary that the hardware be identical, but any differences must be analysed for impacts on the relevance of the prior

certification. Where there are configuration differences that may have an impact, additional verification activities may be required.

**50.** While this chapter has identified RTCA/DO-178B software assurance requirements for the MPS components, it is rarely possible to assure the target computer and associated software components (e.g. COTS OS, other MPS components) to the same level of assurance as is required for the MPS components. COTS operating systems such as Windows XP, Mac OS X, Linux, Solaris, etc., are generally considered Level D software in accordance with FAA CAST 14 *Use of a Level D Commercial Off-the-Shelf Operating System in Systems with Other Software of Levels C and/or D*. CAST 14 identifies that COTS operating systems, such as Windows XP, could be used in a Level C or D system provided the issues listed in CAST 14 are addressed. These issues include assuring that the system architecture prevents the COTS operating system negatively affecting the operation of critical functions. Note that the list of issues in CAST 14 is not all-inclusive, and addressing these issues is not a trivial undertaking and requires extensive analysis, and knowledge of the system and software. Addressing the requirements of CAST 14 is also unlikely to be possible on the DRN and DSN configurations. Fortunately, these measures are usually only required if the MPS applications are hosted on an EFB (refer to Section 2 Chapter 22). For pre-flight MPS software, a standard COTS operation system can be used, provided the verification of the MPS components, accounted for the configuration of the COTS OS (refer paragraph 55).

**51.** Robust partitioning between MPS software components is rarely possible using COTS OS's. However, to ensure that common mode failures do not undermine the assurance of individual software components, coupling between MPS components (particularly between those assured for processing critical data and those that are not assured) should be avoided.

**52. Receiving Data from Suppliers of Aeronautical Data.** The integrity of aeronautical data must be assured from source to use. In addition to being assured for the functions performed, an MPS may also play a role in assuring that errors are not introduced into the aeronautical data in the transfer from the supplier of aeronautical data. In particular, the MPS may be required to implement digital error detection in order to protect the transfer which in all probability will be over unassured mediums such as Defence networks or the Internet.

**53. Loading Data onto the Aircraft.** Data product being loaded onto Data Load Devices should be checked using digital error detection techniques such as checksums (e.g. CRC checks), file format checks or read-back verify techniques of loaded data. Data exchanged by datalink should be checked for correct format at the application layer and by packet digital error detection at the transport layer.

**54. Flight Performance Models.** Some MPS use flight performance models to calculate various aircraft parameters, including fuel usage, route times, etc. There are two aspects relevant to flight performance models: verification and validation.

- a. **Verification of Flight Performance Model.** The flight performance model implemented within the MPS should be verified against the flight manual (or associated flight test reports associated with the aircraft certification basis) using software assurance practices. The required level of assurance will be determined by the criticality of the functions that the flight performance model contributes to.
- b. **Validation of Flight Performance Model.** Where the flight manual and associated flight test reports do not contain sufficient information to develop a complete set of requirements for the flight performance model, or are overly conservative, then additional flight performance characterisation may be required. The flight performance model only requires validation where this new information has been introduced in writing software requirements for the specification of the MPS flight performance model, or in developing the design and implementation of the MPS flight performance model. Validation is not required if a complete set of software requirements has been developed from the aircraft flight manual (and associated flight test reports associated with the aircraft certification basis). Validation may involve modelling, simulation or flight trials to establish the correctness of the requirements for the flight performance model.

**55. Software Verification Guidance.** For MPS components that require assurance commensurate with RTCA/DO-178B, the verification objectives of RTCA/DO-178B should be used to establish verification criteria for MPS components. The following MPS component specific criteria should also be included in satisfying the verification objectives of RTCA/DO-178B:

- a. Normal and robustness testing conducted on MPS components should take into account the following types of test cases most pertinent to aeronautical data.
  - (1) testing of system limits,

- (2) testing of data storage capacity,
  - (3) co-ordinate system formats, storage/transfer data types and conversions,
  - (4) co-ordinate system ranges and limits, and
  - (5) aeronautical database format and data element type limitations.
- b. The verification of MPS components requiring Assurance Levels 1 and 2 should focus on directly establishing the compatibility of the subject MPS component with the:
- (1) Target Hardware,
  - (2) COTS Operating Systems, and
  - (3) other MPS components and applications hosted on the COTS OS on the target hardware

### SERVICE RELEASE GUIDELINES FOR MPS

**56. MPS Design Approval and Acceptance.** Design approval and acceptance of the MPS should take into account the proposed navigations operations of the target platform, as these are fundamental to the determination and assessment of the design assurance of the MPS. Design approval and acceptance should be given on the basis that the criteria in this chapter have been addressed. Any changes or updates to the MPS components, or changes in operational use of MPS produced aeronautical data will require reassessment against the criteria of this chapter and be subject to further design approval and acceptance activities.

**57. MPS Configuration Control.** The MPS should be subject to configuration control and configuration status accounting by the relevant SPO including:

- a. operating system to include version control – for the DRN and DSN this is performed by CIOG and not by the SPO directly;
- b. MPS and additional application program version control;
- c. approved and accredited source for database updates; and
- d. make and model of MPS hardware, including a tracking process for major internal subcomponents whose replacement/upgrade may necessitate additional non-interference testing.

**58. Aeronautical Data Configuration Control.** Procedures and design features should be put in place to assure configuration control of aeronautical data, particularly for those sources that are subject to regular or frequent updates. The level at which aeronautical data is controlled should enable two versions, that may differ by no more than a single bit, to be distinguished based solely on the unique identifier (such as a version or part number) alone.

**59. Instructions for Continued Airworthiness.** On-going maintenance and support of MPS should be considered in maintaining the continued airworthiness of the capability, and may be an explicit requirement on certain navigation performance authorisations. A maintenance or inspection program should be defined to identify inspection items, establish time-in-service intervals for maintenance and inspections, and provide details of the methods and procedures. COTS operating systems and MPS applications should be managed using a problem reporting and management system as described in Section 2 Chapter 17.

### Operational Considerations

**60. Operational Considerations.** It is vital that the operators of the MPS have a clear understanding on how their actions contribute to the integrity of the data the MPS produces in support of the flight or mission. This section provides basic operational approval guidelines.

**61.** The operational aspects of service release should at least address the following issues:

- a. Training development should reflect the level of functionality and complexity of using the MPS. Training should ensure operators have a clear understanding of what the MPS is, its capabilities, and the applications for which the operator will use the MPS system and its components and peripherals.
- b. Training should particularly emphasise the any features of the MPS for checking the validity of the data and for checking for data errors.
- c. Any workarounds resulting from design or assurance shortfalls should be documented in operating procedures.
- d. A scheme for assessing and tracking operator currency with MPSs should be developed, particularly for the processing of critical data.
- e. Human factors (HMI) should be assessed to ensure use of the MPS is at least as safe as under the paper based system.
- f. Procedures should be developed and approved prior to use of the MPS. These are described in further detail in the following paragraph.

**62. Procedures.** Operational procedures should be developed and approved prior to recommendation for Service Release for MPS. Procedures should be developed for:

- a. use of the MPS;
- b. authorised methods for managing inoperative or erroneous MPS applications or equipment;
- c. confirming the revision numbers and/or dates of MPS flight databases and software installed on their MPS prior to using;
- d. ensuring database accuracy and currency, and the completeness of data loaded and maintained in each installation;
- e. any roles that aircrew may have in creating, reviewing and using performance calculations performed by MPS;
- f. enforcing security measures to prevent introduction of unauthorised modifications to the MPS operating system, its hosted applications, and any of the databases, or data links used to enable hosted applications;
- g. initial operational test and evaluation or trial, leading to full service release / navigation authorisation.

**63. Validation by Application.** For data elements assessed as Critical in accordance with RTCA/DO-200A, the civilian benchmark is to validate that data by application. Validation by application involves applying the data under controlled flight test conditions to assess its validity (e.g. flight inspection of final approach segment data prior to widespread release of the data to aircraft operators). This is particularly relevant for GNSS based approaches and navigation authorisations such as Required Navigation Performance Authorisation Required (RNP) where Critical data is commonplace. Operational authorities should establish procedures to ensure that any Critical data used to support navigation operations has been validated by application prior to blanket authorisation of navigation operations conducted using the data, and that MPS components are re-evaluated in this context prior to authorisation. Validation by application is not required where it can be demonstrated that an update to a database does not affect Critical data elements.

#### **Annexes:**

- A. Summary of Application of FAA Framework
- B. Example MPS Data Sources
- C. Example MPS Functions / Applications
- D. Example MPS Output Data and Formats



**Summary of Application of the FAA Framework**

1. This Annex provides a summary of the application of RTCA/DO-200A in the context of MPS application. Readers are referred to the original standards for complete requirements of these standards.
2. As summarised in the main body of this chapter, the FAA framework consists of the following key steps:
  - a. identify the *aircraft functions* and associated functional *failure conditions* of the data processed by the flight planning / aeronautical database application;
  - b. identify which flight planning / aeronautical database application components process the data;
  - c. identify the role in the aeronautical data process the flight planning / aeronautical database application components achieve, such as assemble, translate, select, format and distribute (as described in RTCA/DO-200A);
  - d. determining the *data criticality* of flight planning / aeronautical database application components based on the severity of aircraft functional *failure conditions* and the role of the application components;
  - e. allocate *data assurance levels* to the flight planning / aeronautical database application components based on the *data criticality*; and
  - f. assure the design integrity of the flight planning / aeronautical database application components as per the requirements of the *data assurance level*, involving the application of:
    - (1) design features (validation) to assure that the data is applicable to the identity ascribed to it;
    - (2) design features (verification) to detect and handle instances of when the technical content of the data is inadvertently modified; and
    - (3) software design assurance to prevent the technical content of the data being inadvertently modified.
3. The *failure condition*, *data criticality*, and *data assurance level* definitions are presented in Table 1 of the main body of this chapter. Using the safety assessment process defined in ARP4754 and ARP4761, and additional guidance such as presented in FAA AC25.1309-1A and AC23.1309-1C, the severity of aircraft failure conditions dependent on aeronautical data can be determined. Several examples for generic transport or commuter category aircraft are presented in Table A-1.

Aircraft Function	Failure Condition	Severity / Consequence
Display of Navigation Information	Total Loss of Function	Major
	Loss of Primary Means of Providing Function	Major, Minor if multiple systems installed
	Misleading and/or Malfunction without Warning	Major, may be Hazardous for precision approaches
Communication	Total Loss of Function	Minor – total loss of communication and navigation is Hazardous/Catastrophic
	Loss of Primary Means of Providing Function	Minor
	Misleading and/or Malfunction without Warning	Major if datalink, otherwise Minor
Autopilot – Outer Loop Flight Guidance Flight Director {etc...}	Misleading and/or Malfunction without Warning	Major – Catastrophic, depending on phase of flight, RNP airspace, etc.

**Table A-1:** Example Navigation and Communication Failure Conditions Associated with Aeronautical Data

4. As per the taxonomy of failure conditions presented in Table A-1, aeronautical data can potentially contribute to these failure conditions in the following ways, and these potential contributions should be analysed in the safety assessment.

- a. *Loss of Function (Total Loss, Sole or Primary means)*. It may contribute to loss of a function when the aeronautical data is either not available, or not accessible (in whole or in part), depending on how the data is being used.
- b. *Misleading and/or Malfunction without warning*. The data is available, but is either not valid, contains errors or faults, presents misleading information, or contributes to a malfunction of a system without warning.

5. In addition to the safety assessment process, RTCA/DO-201A provides specific identification of the criticality of each aeronautical data element in the context of civil transport category aircraft operations, an extract from which is presented in Table 3. These standardised criticalities are a useful benchmark when establishing the contribution of particular aeronautical data elements to aircraft level failure conditions.

Aeronautical Data Element	Integrity Classification of Data per RTCA/DO-201A
VHF Navaid – En Route - Location	Essential
VHF Navaid – Terminal - Location	Essential
ILS Localizer Antenna - Location	Essential
ILS Glide Slope Antenna - Location	Essential
Precision Approach Rwy LTP and FPAP	Critical
CAT I/II/III Rwy End and Landing Threshold	Critical
Aerodrome Reference Point	Routine
{etc...}	

**Table A-2:** Extract from RTCA/DO-201A of Aeronautical Data Element Integrity Classifications

6. For example, using the information presented at Tables A-1 and A-2, erroneous aeronautical data (e.g. CAT I/II/III Runway End and Threshold) supporting display of aircraft navigation information related to a precision approach is Hazardous. This equates to Essential (Critical) data and Assurance Level 1 using information presented in Tables 1 of the main body.

#### Data Assurance Level

7. The Assurance Level determines the robustness of the validation and verification that must be applied to processing of aeronautical data; and the extent to which software tools and applications are assured. There are three steps in determining the requirements of the Assurance Level.

8. The first is to determine which phase of the aeronautical data processing process the software tool applies to. RTCA/DO-200A defines the following terminology for expressing the phases of how data is being processed or manipulated.

- a. *Receive* – accepting input data from a supplier.
- b. *Assemble* – merging or compiling aeronautical data from multiple sources into a single database, including checking the data and ensuring that detected errors and omissions are rectified.
- c. *Translate* – changing how information is expressed.
- d. *Select* – extracting a subset of data applicable to the period of its intended use.
- e. *Format* – converting, arranging, packing and compressing a selected set of data for distribution to a specific target system.

- f. *Distribute* – duplication of formatted aeronautical data into a database and the shipping and loading of the database into the target system for application.

9. The second step is to determine which validation features are being applied (or should be applied). Validation is the activity where a data element is checked as having a value that is fully applicable to the identity ascribed to the data element. The following approaches are permitted:

- a. *Validation by Application* – validates by applying data under test conditions (e.g. flight inspection of final approach segment data prior to publishing).
- b. *Logical Consistency* – validates by comparing the relationship between two different datasets (e.g. the primary data source against an alternative data source).
- c. *Semantic consistency* – validates by comparing data to an expected value or range of values for the data characteristics (e.g. reasonability checks – range, resolution, relationships to adjacent data, etc).

10. Table A-3 describes the relationship between the Data Assurance Level and the application of these aforementioned Validation approaches.

Data Process Assurance Level	Validation Requirements
1	<i>Validation by Application</i> is required. <i>Validation by Application</i> is typically accomplished by the originator of the data, provided the originator is aware of the intended application of the data. Once the data is validated, verification techniques must be used to ensure that the technical content of the data is not modified at any stage of the process.
2	<i>Validation by Application</i> is not required. However, <i>Validation by Application</i> remains the most effective means of validation and is recommended. <i>Logical Consistency</i> and <i>Semantic Consistency</i> may alternatively be used as components of the overall validation where <i>Validation by Application</i> is not practicable.
3	Validation is recommended, but is not required.

**Table A-3: Validation Requirements**

11. The third step is to determine which verification features are being applied (or should be applied) to prevent the technical content of the data being modified. Verification is the means of ensuring that the technical content of the data is not modified at any stage of the process. One or more of the following approaches are typically employed:

- a. *Digital Error Detection Techniques* can be used to detect errors during the transfer and storage of data (e.g. cyclic redundancy checks (CRCs), parity, Hamming codes, and Reed-Solomon codes).
- b. *Feedback* is the comparison of a data set between its output and input state – independent reverse data process (e.g. reversibility check, read back verify, etc)
- c. *Independent Redundancy* involves making a comparison of data processing the same data through two or more independent processes or tools.
- d. *Update Comparison* is the comparison of data to its previous version to identify and verify all data elements that have changed.

12. Table A-4 describes the relationship between the data processing phase and the applicability of the verification techniques. This table provides a guide when selecting the appropriateness of available verification techniques for the applicable phase of the aeronautical data processing phase. As expressed in Table A-4, the verification techniques are independent of the data assurance level, however Table A-5 defines additional requirements for qualification of these mechanisms which is dependant on the data assurance level.

Verification Technique  Data Processing Phase	Digital Error Detection	Feedback	Independent Redundancy	Update Comparison
Applications to: <i>Receive Phase, Assemble Phase, Select Phase, Distribute, Phase</i>	Effective assurance can be numerically demonstrated through the probability of undetected error given the digital error detection technique.	Feedback is an effective means of verifying data after moving/storing.  Manual feedback can be used as part of a Level 2 process.	Independent redundancy is an effective means of verifying data during moving/storing.	Update comparison is an effective means of verifying data during moving or storing.
Application to: <i>Translate Phase, Format Phase</i>	Not applicable as the data undergoes technical change.	Feedback can be used when transforming data.  In order to compare the output of the transformation to the input, it's necessary to transform one or both to a common form, usually involving a reversibility check.  Therefore, feedback provides verification only if the means of transformation for the verification is independent of the means of transformation that is being verified.	Independent redundancy is an effective means of verifying manual transformations.  For automated transformations, the tool that performs the transformation should be qualified.	Update comparison is not an effective means of verifying transformation, as the transformation could introduce the same error in both updates, and technical changes to the data are difficult to resolve using this method.  However, use of update comparison can provide some assurance provided the prior update has been validated (by application).

Table A-4: Processing Phases and Verification Design Features

13. Once the verification techniques have been proposed for a given aeronautical data application, the qualification requirements for any tools associated with the processing of aeronautical data can be determined, as per Table A-5.

Data Assurance Level	Data Processing - Tool Qualification Requirements
1	<p>Tools that have the potential to modify the data in an undetected manner must be qualified to a level consistent with the <i>Hazardous</i> or <i>Catastrophic</i> failure conditions (i.e. RTCA/DO-178B Level A or B). However, the precise requirements for tool qualification are based on the tool’s involvement in the data process, as follows:</p> <ul style="list-style-type: none"> <li>• The tool that generates the Digital Error Detection code (e.g. CRC), and the tool that verifies the Digital Error Detection code (e.g. CRC) value should be qualified to RTCA/DO-178B Level A or B. This is because the Digital Error Detection code is the only means of detection additional errors downstream of this immediate process.</li> <li>• Tools that <i>translate</i> or <i>format</i> the data do not need to be qualified as long as the subsequent participant can recover the original format and verify the source data CRCs against the recovered format using the qualified tool from above (RTCA/DO-178B Level A or B). If there is no means to recover the original format, then the tool that performs the <i>translate</i> or <i>format</i> should be qualified to RTCA/DO-178B Level A or B.</li> <li>• Tool qualification (as per RTCA/DO-178B Verification Tool requirements) of any tools used to accomplish the <i>feedback comparison</i>, <i>independent redundancy comparison</i>, or <i>update difference comparison</i>.</li> </ul>
2	<p>Tools that have the potential to modify the data in an undetected manner must be qualified to a level consistent with the <i>Major</i> or <i>Minor</i> failure conditions (i.e. RTCA/DO-178B Level C or D respectively), depending on the specific aircraft level failure condition to which the data related. However, the precise requirements for tool qualification are based on the tool’s involvement in the data process, as follows:</p> <ul style="list-style-type: none"> <li>• The tool that generates the Digital Error Detection code (e.g. CRC), and the tool that verifies the Digital Error Detection code (e.g. CRC) value should be qualified to RTCA/DO-178B Level C or D.</li> <li>• Tools that translate or format the data do not need to be qualified as long as the subsequent participant can recover the original format and verify the source data CRCs against the recovered format using a qualified tool from above (RTCA/DO-178B Level C or D). If there is no means to recover the original format, then the tool should be qualified to RTCA/DO-178B Level C or D.</li> <li>• Tool qualification (RTCA/DO-178B Verification Tool) of any tools used to accomplish the <i>feedback comparison</i>, <i>independent redundancy comparison</i>, or <i>update difference comparison</i></li> </ul> <p>Note the different between RTCA/DO-178B Level C and D is notable, and therefore the safety assessment process must make it explicit which severity failure condition the data element relates to. It also means there may be limitations to the extent to which tools used for <i>Essential</i> data in one context may be used in an alternative context.</p>
3	Tools are not required to be qualified.

**Table A-5:** Tool Qualification Requirements for RTCA/DO-200A Aeronautical Data Process

14. Provided the tools used to process aeronautical data have been qualified, then those tools are suitable for use in their specified role as flight planning applications or aeronautical database applications. Any changes to the role of the tool or the data processed by the tool will require re-evaluation against these criteria to determine the ongoing suitability of the tool.



**Example MPS Data Sources**

- Manuals and Procedures (electronic format)
  - Aircraft Flight Manuals and Aircraft Flight Manual Supplements, including performance information, weight and balance, limitations, emergency procedures, etc.
  - Operational Policy, Regulations, Manuals and Procedures
  - Technical Policy and Regulations
  - Aircraft Performance Data (Static, non interactive material for planning purposes)
  - Aircraft Maintenance Manuals
  - Aircraft Parts Manuals and Illustrated Parts Breakdown (IPB)
  - Noise abatement procedures for arriving and departing aircraft
  - Flight attendant manuals
- References
  - Airport Rules and Regulations
  - Minimum Equipment Lists (MEL)
  - Published (graphical) pilot Notices to Airmen (NOTAM)
  - Aeronautical Information Publications (AIP)
  - Aeronautical Information Manual (AIM)
  - Medical emergency reference library
  - Material Safety Data Sheets
  - Emergency response guidance for aircraft incidents involving dangerous goods
  - Fuel prices at various airports
  - Electronic checklists, including normal, abnormal and emergency.
  - Terminal Procedures
- Forms (Look-up and Completion of)
  - Customs declaration and quarantine inspection/declaration forms
  - Special reporting forms, such as ASORS, MASORS, etc.
- Logs
  - Aircrew Logbooks and qualification logs (such as aircraft qualifications, Class II flightcrew qualifications, Category (CAT) III qualifications, high minimums logs, night currency logs, etc.)
  - Flight and duty time logs
  - Required rest logs
  - Incidents of interference to aircraft electronic equipment from devices carried on board
  - Aircraft's CAT II/CAT III landing records
- Maps and Charts
  - Electronic aeronautical charts (e.g. en route, area, approach, and airport surface maps)
  - Mapping / GIS
  - Raster maps (scanned in paper maps)
  - Compressed arc digital raster graphic (CADRG) – MIL-PRF 89038, STANAG-7098
  - Satellite imagery (e.g. Controlled Image Base (CIB) – orthographic photos made from rectified greyscale aerial images – MIL-PRF-89041A, registered resolutions in MIL-STD-2411-1, raster product format (RPF) standard).
  - Aerial photograph (GeoTIFF)
  - Vector Maps (VMAP, Digital Nautical Charts) – mapping or overlay
  - Gazetteer data for geographic feature names
  - Drawing files (boundaries, obstacles, etc)
- Terrain Data
  - Digital Terrain Elevation Data (DTED) – level 1 (3 arc seconds – approx 100m), level 2 (1 arc second – approx 30m), level 3 (10m). MIL-PRF-89020A
- Databases
  - Digital Aeronautical Flight Information File (DAFIF) containing airspace boundaries, airport boundaries, airport locations and their characteristics and arrival/departure information.
  - Australian DAFIF
  - Automated Air Facilities Intelligence File (AAFIF) airfield database

- Digital Vertical Obstruction File (DVOF) for vertical obstructions
- Regional data – wire maps, low flying areas, noise avoid areas, local points database
- Drop Zone and Landing Zone database
- Aircraft default settings database
- Routes (waypoints, navpoints)
- Local points
- Threat files / battlefield data
- GPS track files
- Obstacle Data
- Navpoint Data
- Waypoint Data
- Tasking (Air Task Orders (ATO)/ Airspace Control Orders (ACO))
- Coordinate / Deconflict
- Weapons Data
- FLIP
- Threat / Intel
  
- Internet Data Services
  - Weather and climate data
  - National Aeronautical Information Processing System (NAIPS) system provides NOTAMS, MET and Location briefings, and allows electronic flight plan submission
  
- Video
  - Digital video files
  
- Real Time Monitoring via Data-link – VMF
  - Aircraft position

**Example MPS Functions / Applications**

- Component Types
  - Common Components
  - Unique Planning Components
  - Core Functions
  - Aircraft Specific Modules
  
- Functions
  - Map selection
    - 2D mapping – displaying mapping, imagery and overlays
  - Flight planning
    - waypoints & route/flight plans
    - directly plot flight paths onto a digitised map; or enter the key points by reference into flight routes
    - view multiple routes
    - route analysis and de-confliction (distance, altitude and time criteria)
  - Met planning
  - Comm. Planning
    - Communications frequencies
  - Mission planning
    - Weapon parametrics
    - Threat
    - Intervisibility tools, range and bearing tools
    - Checklists
  - Crew brief prep
  - Data upload
  - Calculation of mission specific parameters
  - Calculations
    - Performance calculations for takeoff, en route, approach and landing, missed approach, go-around
    - Hover and cruise data
    - Single and multi engine performance
    - Manoeuvre calculations for fighter aircraft
    - Take-off / landing data (TOLD)
    - Power settings for reduced thrust settings
    - Fuel usage and leg times
    - Runway limiting performance calculations
    - Weight and balance calculations
  - Tabular information about planned routes
    - calculated distances
    - timings
    - fuel consumption between waypoints
  - Mission and C2 Visualisation
    - Threat data and overlays
    - Improved Many on Many EW Simulation
    - Order of Battle Management Tools
    - Detection range, identification range, engagement range
  - Mission Rehearsal / Play-back functionality
    - 2D and 3D flythrough
    - 3D visualisation by using DTED and mapping or imagery surface texture
  - Mission monitoring
  - Mission debrief
  - View ATOs and ACOs (tabular – and overlay on maps)
  - War gaming
  - Mission resourcing and objectives planning
  - Aircraft configuration and payload planning
  - Decision aids – furthest on circle, bearing distance time, course and speed made good, dead reckoning, line of sight, sun moon almanac, weapon safety templates, deconfliction

- Role Specific Software Applications
  - Weapons Release (stores parameters and weapon delivery)
  - Parachute Tools - parachute parameters, drop zone / landing zone
  - Hover performance
  - Combat airdrop planning software (CAPS)
  - Electronic Warfare,
  - Compute airdrop release points (CARP)
- Flight Performance Models
- Aircraft Interfaces (known as Aircraft/Weapons/Electronics)
- Data Transfer
  - Transfer data to/from GPS receivers – waypoints, track points, configuration settings
  - Transfer data to/from flight management systems and mission computers
- Aeronautical databases import and export
- GPS almanac
- Imagery management
  - Import of imagery
  - Scanning in of imagery
  - Geo-rectification
- Aircraft configuration settings (a/c type, departure location and a/c configuration)
- Real Time Data Exchange
  - position request
  - live mission overlays
  - live mission routes
  - live mission
  - live mission images to and from
  - text messages
    - free text
    - assault support request
    - mayday
    - observation report
    - obstacle report
    - basic weather report
    - observed weather information and effects
    - position report
    - movement command/response
    - CASEVAC request
    - emergency resupply request
    - emergency resupply request response.

**Example MPS Output Data and Formats****Output Data**

- Flight Route
  - Routes (Location, Bearing, Flight Level, RNP requirements, etc)
  - Waypoints
- Communications Data
  - Channel Identifiers
  - Band (HF, VHF, UHF, etc)
  - Frequencies
- Weapons Data
  - Weapon Release Points
  - Weapon User Modifiable Data
- Mission / Intelligence Data
  - Locations of Friendly and Enemy Forces
  - EW Data (Threat Rings, Radar Coverage, etc)
  - Intelligence Reports
  - Still Images
  - Pre-recorded Video Files
- Aircraft Performance
  - Predicted Fuel Usage
  - Predicted Leg Times
- Maps
  - Map Base Sets
  - Map Overlays
- Flight Notification to ATM
  - A/C ID or Flight Number
  - Flight rules: IFR/VFR/IFR then VFR/VFR then IFR
  - Type of Flight: scheduled, non-schedule, general aviation, military
  - Aircraft type
  - Wake turbulence category (Low, Medium, high)
  - NAV/COM equipment: DME, ADF, GNSS, INS, ILS, VOR, RNP, TACAN – VHF/ADF/ILS/VOR
  - COM equipment: HF, datalink, UHF, VHF
  - SSR equipment: None, Mode A, Mode A+C, Mode S (including a/c id and/or alt)
  - Departure location
  - Destination
  - Estimated Time of Departure (ETD)
  - Speeds and Flight Levels
  - ATS route

**Output Formats**

- Kneeboards – including paper charts, reports and references.
- Digital Media (e.g. Flash Card, Floppy Diskette, Hard Disk, etc) for aircraft transfer
- Datalink for aircraft transfer
- Flight-line Requests