

Appendix 1

RTCA/DO-178B AUDIT CHECKLIST & REPORT		
CHECKLIST DATE: Feb 25, 2008		
AUDIT DATE: 15 December	Auditor: Ali	AUDIT PURPOSE: DO-178B Objective Compliance

REQUIREMENTS	COMPLIANCE & ASSESSMENT			
Section 4.0 <u>Software Planning Process</u>	P&WC ASSESSMENT			
	YES	NO	N/A	REFERENCES AND REMARKS
No specific requirements. 4.1 <u>S/w Planning Process Objectives</u> No specific requirements.	Y			
4.2 <u>Software Planning Process Activities</u>	Y			
➤ R4.1 Is there a procedure that requires s/w plans be developed at a time in the life cycle to provide appropriate direction to personnel?	Y			
➤ R4.2 Is there a procedure that requires s/w standards used for the project be defined or selected?	Y			
➤ R4.3 Is there a procedure that requires methods and tools be chosen to provide error prevention in development process?	Y			Misra, CTC++, CPPCHECK
➤ R4.4 Is there a procedure that requires the s/w planning process provide coordination between the s/w development and integral processes to provide consistency among strategies in the s/w plans?	Y			
➤ R4.5 Is there a procedure that requires a means to update the s/w plans be defined?	Y			
➤ R4.6 Is there a procedure that requires when multiple version dissimilar s/w is used in a system, the s/w planning process chooses the methods and tools to achieve the error avoidance or detection necessary to satisfy the system safety objectives?		N		

REQUIREMENTS	COMPLIANCE & ASSESSMENT				
Section 4.0 <u>Software Planning Process</u>	P&WC ASSESSMENT				
	YES	NO	N/A	REFERENCES AND REMARKS	
➤ R4.7 Is there a procedure that requires s/w plans and s/w development standards be under change control, and reviews of them be completed?	Y				
➤ R4.8 Is there a procedure that requires the planning process define how deactivated code will be defined, verified and handled?	Y				
➤ R4.9 Is there a procedure that requires the process, tools, environment and data items associated with user modifiable code development be defined in the plans and standards	Y				
R4.3 <u>Software Plans</u>		N			
➤ R4.10 Is there a procedure that requires s/w plans comply with DO/178B.					
➤ R4.11 Is there a procedure that requires definition of the transition between s/w life cycles be specified by inputs to the process, any integral process activities to act on the inputs and availability of tools, methods, plans and procedures?		N			
➤ R4.12 Is there a procedure that requires s/w change procedure be defined prior to the use of the change on a certified engine /aircraft			N/A		
4.4 <u>Software Life Cycle Environment Planning</u> No specific requirements			N/A		
4.4.1 <u>Software Development Environment (SDE)</u>			N/A		
➤ R4.20 Is there a procedure that requires SDE be chosen to minimise potential risk to s/w product?			N/A		
➤ R4.21 Is there a procedure that requires the necessary confidence level in the use of tools be such that errors introduced by one part be detected by another?			N/A		
➤ R4.22 Is there a procedure that requires s/w development and verification activities and standards be defined to minimise potential SDE related errors?			N/A		
➤ R4.23 Is there a procedure that requires when certification credit is sought for tool use that the sequence of use is defined?			N/A		
➤ R4.24 Is there a procedure that requires when optional features of a tool are chosen that the effects of the option are			N/A		

REQUIREMENTS	COMPLIANCE & ASSESSMENT				
Section 4.0 <u>Software Planning Process</u>	P&WC ASSESSMENT				
	YES	NO	N/A	REFERENCES AND REMARKS	
defined?					
4.4.2 <u>Language and Compiler Considerations</u>	Y				
➤ R4.25 Is there a procedure that requires the effect on structural coverage of compiler optimisers be defined?					
➤ R4.26 Is there a procedure that requires the means to detect and verify coverage of object code that is not traceable to source be defined?		N			
➤ R4.27 Is there a procedure that requires when compiler, linker, loader or compiler options are changed re-verification is defined?		N			
4.4.3 <u>Software Test Environment</u>			N/A		
➤ R4.28 Is there a procedure that requires an emulator or simulator may need to be qualified?					
➤ R4.29 Is there a procedure that requires the functional and error detection differences between the target and the emulator/simulator be analysed?			N/A		
4.5 <u>Software Development Standards</u>					
➤ R4.30 Is there a procedure that requires software standards comply with DO/178B?	Y				
➤ R4.31 Is there a procedure that requires components are uniformly designed and implemented?	Y				
➤ R4.32 Is there a procedure that requires standards disallow use of constructs or methods that produce output that cannot be verified or incompatible with safety requirements?	Y				
4.6 <u>Review and Assurance of the Software Planning Process</u>					
➤ R4.33 Is there a procedure that requires the software quality system must enable ISO-26262 objectives be met?	Y				
➤ R4.34 Is there a procedure that requires the software life cycle processes be consistently applied?		N			
➤ R4.35 Is there a procedure that requires each process produces evidence that outputs are traceable to the activity and inputs?	Y				
R4.36 Is there a procedure that requires the software planning outputs be consistent and comply with DO/178B?	Y				

REQUIREMENTS	COMPLIANCE & ASSESSMENT			
Section 6.0 <u>Software Verification Processes</u>	P&WC ASSESSMENT			
	YES	NO	N/A	REFERENCES AND REMARKS
No specific requirements. 6.1 <u>Software Verification Process Objectives</u> No specific requirements			NA	
6.2 <u>Software Verification Process Activities</u> ➤ R6.1 Are the inputs to the software verification process defined?	Y			
➤ R6.2 Have the high level requirements (HLR) and the traceability to them from system level (SLR) and low-level requirements (LLR) been verified?	Y			
➤ R6.3 Do the traceability, requirements-based and structural coverage based analyses show that each software requirement is traceable to the code that implements it and to the activities that verify it?	Y			
➤ R6.4 Have the differences between the code tested and the airborne software been specified and justified?			N/A	
➤ R6.5 For any software requirements that cannot be verified using a realistic test environment, have other means been provided and specified and justified in the Software Verification Plan?		N		
➤ R6.6 Have any deficiencies or errors discovered during the software verification process been reported for corrective action?		N		
6.3 <u>Software Reviews and Analyses.</u> No specific requirements.				
6.3.1 <u>Reviews and Analyses of the High Level Requirements</u> ➤ R6.7 Is the target HLR compliant with a system requirement been confirmed?	Y			
➤ R6.8 Has the HLR accuracy and consistency been confirmed?	Y			
➤ R6.9 Has compatibility of the HLR with the target computer been confirmed?	Y			
➤ R6.10 Is there confirmation that the target HLR is verifiable?	Y			

REQUIREMENTS	COMPLIANCE & ASSESSMENT			
Section 6.0 <u>Software Verification Processes</u>	P&WC ASSESSMENT			
	YES	NO	N/A	REFERENCES AND REMARKS
➤ R6.11 Has HLR conformance to the Software Requirements Standards been confirmed?	Y			
➤ R6.12 Has the HLR traceability to the SLR been confirmed?		N		
➤ R6.13 Has the HLR algorithm accuracy and behavior be confirmed?		N		
6.3.2 <u>Reviews and Analyses of the Low Level Requirements</u>	Y			
➤ R6.14 Is the target LLR compliant with the software high level requirement?				
➤ R6.15 Has the LLR accuracy and consistency been confirmed?	Y			
➤ R6.16 Has compatibility of the HLR with the target computer been confirmed?			N/A	
➤ R6.17 Is there confirmation that the target LLR is verifiable?	Y			
➤ R6.18 Has LLR conformance to the Software Design Standards been confirmed?	Y			
➤ R6.19 Has the LLR traceability to the HLR been confirmed?	Y			
➤ R6.20 Has the LLR algorithm accuracy and behaviour been confirmed?	Y			
6.3.3 <u>Reviews and Analyses of the Software Architecture</u>	Y			
➤ R6.21 Has compliance with the HLR been confirmed?				
➤ R6.23 Has compatibility with the target computer been confirmed?			N/A	
6.3.4 <u>Reviews and Analyses of the Source Code</u>	Y			
➤ R27 Is the target source code compliant with the LLR?				
➤ R28 Is the source code compliant with the software architecture?			N/A	
➤ R29 Is there confirmation that the source code is verifiable?	Y			

REQUIREMENTS	COMPLIANCE & ASSESSMENT			
Section 6.0 <u>Software Verification Processes</u>	P&WC ASSESSMENT			
	YES	NO	N/A	REFERENCES AND REMARKS
➤ R30 Has conformance to the Software Code Standards been confirmed?	Y			
➤ R31 Has traceability to the LLR been confirmed?	Y			
➤ R32 Has the source code accuracy and consistency been confirmed?	Y			
6.3.5 <u>Reviews and Analyses of the Outputs of the Integration Process</u>			N/A	
➤ R6.33 Is there confirmation that incorrect h/w addresses are not present?				
➤ R6.34 Is there confirmation that there are no memory overlaps?			N/A	
➤ R6.35 Is there confirmation that there are no missing software components?			N/A	
6.3.6 <u>Reviews and Analyses of the Test Cases, Procedures and Results</u> Are there test cases, procedures and results for the all the elements of the requirement trace?	Y			
➤ R6.36 Is there confirmation that the test cases have been verified?	Y			
➤ R6.37 Is there confirmation that the test cases have been developed into test procedures and expected results?	Y			
6.4 <u>Software Testing</u> No specific requirements.				
6.4.2 <u>Requirements Based Test Case Selection</u>		N		
➤ R6.40 Are there test cases for normal range and robustness?				
6.4.2.1 <u>Normal Range Test Cases</u>	Y			
➤ R6.42 Are there test cases for real and integer input variables to be exercised using valid equivalence classes and boundary values?				
➤ R6.43 Are there test cases for multiple iterations of the code for time related functions?	Y			
➤ R6.44 Are there test cases that exercise state transitions	Y			

REQUIREMENTS	COMPLIANCE & ASSESSMENT			
Section 6.0 <u>Software Verification Processes</u>	P&WC ASSESSMENT			
	YES	NO	N/A	REFERENCES AND REMARKS
during normal operation?				
➤ R6.45 Are there test cases to verify the variable usage and Boolean operators for software requirements expressed by logic equations?	Y			
6.4.3 Requirements Based Testing Methods			N/A	
➤ R6.53 Are there test cases for requirements based h/w-s/w integration testing for error sources?				
➤ R6.54 Are there test cases for requirements based software integration testing?	Y			
➤ R6.55 Are there test cases for requirements based low level testing?	Y			
6.4.4 Test Coverage Analysis	Y			
➤ R6.56 Is there requirements based and structural based test coverage?				
6.4.4.1 Requirements Based Test Coverage Analysis	Y			
➤ R6.57 Are there test cases for each requirement?				
➤ R6.58 Are there test cases to satisfy the criteria of normal and robustness testing?	Y			
6.4.4.2 Structural Coverage Analysis		N		Because code was not executable
➤ R6.59 Is there an analysis to confirm the degree of structural coverage?				
➤ R6.60 Is there a procedure that requires structural coverage analysis on source code be restricted to Levels lower than A unless the object code is directly traceable to the source?	Y			
➤ R6.61 Is there an analysis to confirm the data and control coupling between code components?		N		
➤ Is there tools to perform automated structural coverage (branch, statement, MC/DC)?		N		Manual structural coverage was done

REQUIREMENTS	COMPLIANCE & ASSESSMENT			
Section 7.0 <u>Software Configuration Management Process</u>	P&WC ASSESSMENT			
	YES	NO	N/A	REFERENCES AND REMARKS
No specific requirements. 7.1 <u>Software Configuration Management Process Objectives</u> No specific requirements. 7.2 <u>Software Configuration Management Activities</u> No specific requirements.				
7.2.1 <u>Baselines (b/l) and Traceability</u> ➤ R7.6 Is there a procedure that requires baselines be established for configuration items used for certification credit?	Y			
➤ R7.7 Is there a procedure that requires a s/w product baseline be established and defined in the S/w Configuration Index ?	Y			
➤ R7.8 Is there a procedure that requires b/l's be established in controlled s/w libraries and protected from change?	Y			
➤ R7.9 Is there a procedure that requires change control (CC) activities be followed for derivatives from an established b/l?			N/A	Not in ISO-26262
➤ R7.10 Is there a procedure that requires a b/l to be traceable to the b/l from which it is derived if certification credit is sought for artifacts from the previous b/l?		N		
➤ R7.11 Is there a procedure that requires a configuration item to be traceable to the configuration item from which it is derived if certification credit is sought for artifacts from the previous configuration item?		N		
➤ R7.12 Is there a procedure that requires a b/l or configuration item be traceable to the output it identifies or the process with which it is associated?		N		
7.2.4 <u>Change Control (CC)</u> ➤ R7.16 Does the CC protect the integrity of the configuration item and b/l's from unauthorised change?	Y			
➤ R7.17 Is the change to the configuration item accompanied by a change to its CI?	Y			

REQUIREMENTS	COMPLIANCE & ASSESSMENT			
Section 7.0 <u>Software Configuration Management Process</u>	P&WC ASSESSMENT			
	YES	NO	N/A	REFERENCES AND REMARKS
➤ R7.18 Is the change to the b/l's and to the configuration item under CC recorded?				
➤ R7.19 Has the s/w change been traced to the origin and the life cycle processes repeated from the point at which the change affects the outputs?	Y			
➤ R7.20 Has the s/w life cycle data affected by the change been updated and records maintained for the CC activity?	Y			
7.2.5 Change Review	Y			
➤ R7.21 Are all affected configuration items under CI?				
➤ R7.22 Is there an assessment of the impact on safety-related requirements and feedback to the safety assessment process?		N		
➤ R7.23 Is there an assessment of the problem or change with decisions for actions to be taken?		N		
➤ R7.24 Is there feedback of the problem report or change impact to the affected process?	Y			
➤ R7.26 Is the definition of the data maintained and the means of recording and reporting status of the data per the procedure?		N		
7.2.8 Software Load Control	Y			
➤ R7.37 Is there a procedure that requires part numbering and media identification for s/w configurations intended to be approved for loading into the airborne system or equipment?				
➤ R7.38 Is there a procedure that requires records be kept to confirm s/w compatibility with the airborne system or equipment h/w?	Y			