International Civil Aviation Organization

WORKING PAPER

A39-WP/267
TE/105
25/8/16

ASSEMBLY — 39TH SESSION

TECHNICAL COMMISSION

Agenda Item 36: Aviation safety and air navigation implementation support

A PROPOSAL FOR GUIDANCE MATERIAL TO STANDARD CERTIFICATION & DEVELOPMENT PROCEDURES ON COMMUNICATIONS, NAVIGATION AND SURVEILLANCE/AIR TRAFFIC MANAGEMENT (CNS/ATM) SYSTEMS

(Presented by the Republic of Korea)

EXECUTIVE SUMMARY

With the technology development and diversification of the Communications, Navigation and Surveillance/Air Traffic Management (CNS/ATM) systems, the certification such as safety and compatibility has become important. Therefore, it is recommended that ICAO establish the standardized certification procedures to be acceptable by Member States. In this paper, a certification and development procedure for the international application on the CNS/ATM systems is proposed.

Action: The Assembly is invited to consider if it is necessary for the ICAO to develop guidance materials for standard certification and development procedures on CNS/ATM systems.

Strategic Objectives:	This working paper relates to the Safety Strategic Objective.
Financial implications:	Not applicable
References:	Annex 10 – *Aeronautical Telecommunications*, Volumes I, II and IV Doc 8071, *Manual on Testing of Radio Navigation Aids* SAE ARP-4754 /4761 EUROCAE ED-79A/ ED-135 RTCA DO-278A/178C/254 EUROCAE ED-109/ED-12C/ED-80

1. INTRODUCTION

1.1 It is important to operate the correct and accurate Communications, Navigation and Surveillance/Air Traffic Management (CNS/ATM) systems for the safe navigation of airplanes. Today, ICAO Annex 10 and Doc 8071 address international Standards on the technology and performance test. However, as there are no internationally recognizable development and certification procedures in the CNS/ATM systems like the aircraft certification Standards, the CNS/ATM systems certified in the exporting country should get a new certification for operation in accordance with the certification procedures and criteria of the importing country. Therefore, it is a huge burden for the equipment developer without an internationally standardized development and certification process.

1.2 The conventional CNS/ATM systems were approved for operation without a standardized certification procedure because it was relatively simple. However, it is important for the modern complex and advanced systems to have the safety, consistency and compatibility for the performance certification. Today, United States, Europe, Russia, China, as well as the Republic of Korea are developing their own CNS/ATM systems or importing from other countries and are required to get the certification from their approval authority and only the certified equipment can be installed for operation in a few states.

1.3 Therefore, it is necessary to propose a standardized certification process and internationally recognizable development procedures (excluding ground and flight test) in developer's and authority's point of view, which is acceptable to ICAO. Some countries require the CNS/ATM systems approval of "System Approval," "Facility Approval," finally "Service Approval" step by step from the aviation authority.

2. DISCUSSION

2.1 Purpose

2.1.1 The purpose of this paper proposed that a number of countries all over the world address the standardized and consistent certification system in accordance with the establishment of the internationally standardized approval process for the CNS/ATM systems. And if the CNS/ATM systems among Member States have equal level of the performance and safety certification systems, the other purpose can be established with the simplified certification on the product concerned with the CNS/ATM systems based on the trust among Member States.

2.2 Proposal for ICAO Standard Process to System Approval

2.2.1 The main focus is as follows to certify CNS/ATM systems:

a) design to satisfy requirements for suitable equipment;

b) develop in proportion to design assurance level; and

c) satisfy system performance requirements of developed equipment.

2.3 The system approval processes for the CNS/ATM systems are proposed as follows:

a) safety inspection of equipment;

b) inspection of related matters such as requirement;

c) inspection of the suitability for test procedure, test procedure and test results;

d) inspection of software development and design assurance system;

e) inspection of hardware development and design assurance system;

f) inspection of user manual; and

g) inspection of education, training and data.

3. CONCLUSION

3.1 In standardizing the development and certification process for the CNS/ATM systems internationally, a range of countries all over the world address the standardized and consistent certification systems for the improvement of the aviation safety and reliability.

3.2 If there is equivalent level of development and certification systems with Member States, the products related to the CNS/ATM systems bring the simplification of the certification process and cost and time saving for the certification based on the trust among Member States.

— — — — — — — — —

APPENDIX

DETAILED DESCRIPTION OF PARAGRAPH 2.3 FOR INSPECTION PROCEDURES

Safety inspection of equipment: The certification authority shall confirm safety level by checking its safety assessment process and safety result report submitted by developer.

Inspection Items	Inspection Contents
Hazard evaluation system functions	It should be hazard elements identified and defined for the failure of the system function.
Safety assessment of backup system	Safety requirements for all items constituting a system based on the results of its elements evaluation for system function are identified and defined.
System safety assessment	Developed system should satisfy all safety requirements.
Analysis of failure mode effect	The influences of impact on system configuration and system by failure of function are analysis and quantifiable.
Analysis of common factor	The safety analysis of the failure broken by external factors, independent area and common factor should be analysis.

a) Inspection of items associated requirements: The certification authority shall perform the inspection on document of requirement for equipment, configuration management, validation request, equipment list, development plan, hardware and software composition, result of equipment demonstrated, equipment design and date of production approval.

Inspection Items	Inspection Contents
Verification of system development plan	System development and integration process shall be defines the conditions and verified completion of the criteria and activities.
System requirement	System requirement should be defines the considerations of architecture, software and hardware interface and include all the functional requirements of the subsystems
Definition of safety	The results of the safety assessment should be quantified and analyzed safety assessments consist of FHA, FTA, FMEA, CCA.
Design of system architecture	The design considerations for the configuration of subsystems, interfaces, constraints should be defined and possible to verify.
System implementation	System should be implemented to meet the functional and safety requirements. Also, it should be considered countermeasures for the exception and demonstrated the test procedures.
System safety assessment	SSA should be defined in the procedure and method and analyzed quantifying evaluation results.
Configuration management	Configuration management should be defined configuration item, properly managed baseline and record configuration management history. Also, it should be systematically managed to configuration change, recovery and release.
Operational test and evaluation	The operation testing procedures and standards are developed consistently in the software development life cycle, the verification is possible, quantify the results of the evaluation shall be analyzed.

Access control	The access control should be established policy including access control area, scope, rules and methods. Therefore, the unauthorized access should be controlled.
Audit record	Audit log for access to the track should be recorded
Data management	It should be safely managed data using a technique such as a transport and storage of the encrypted sensitive data.
Integrity	Integrity for the data should be ensured by using a technique such as method of protection data against forgery when data transmission and reception.
Enhanced security	It is should be established security measures for security vulnerabilities.

b) <u>Inspections of the propriety of test results and procedure</u>: The certification authorities should identify Standard test evaluation document, test evaluation document, exemptions and mitigation document, compliance certification document, Flight tests result documents submitted by the applicant.

Inspection Items	Inspection Contents
Interoperability requirements definition	It should be defined the necessary standards and requirements for interoperability with other aircraft or facilities.
Interoperability Test and Evaluation Plan	It should be established the plan of the testing items, environments, schedules, etc. in accordance with the interoperability requirement.
Interoperability Test and evaluation	It should comply with the interoperability tests and conduct an evaluation test in accordance with test and evaluation plan.
Miscellaneous requirements for test evaluation	Test and evaluation of the requirements should be defined in order to properly operate CNS/ATM except for the minimum performance, interoperability, security. Then, the test results should be operating normally.

c) <u>Inspection of software development and design assurance system</u>: The certification authority shall ensure a system of software development and design assurance upon result of standard test evaluation for software approval and standard evaluation for software test and assessment submitted by developer.

Inspection Items	Inspection Contents
Software development process	Software life cycle processes completed by activity, completion conditions and development/verification environment shall be defined.
Software requirements definition	High-level requirements are produced through analysis of system requirements, accuracy, standards compliance, and object equipment can be verified, and algorithm shall be accurate
Software design	The architecture and lower-level requirements correspond to higher-level requirement, accuracy, standards compliance, and object equipment can be verified, algorithm shall be accurate, and architecture shell designed exactly.
Software coding and integration	The source code requirements correspond to lower-level requirements and architecture, accuracy, standards compliance, and object equipment can be verified, and software development file and validated data shall be correct.
Software testing	The file permissions correspond to lower-level and high-level requirements, the test procedure and the results are correct, and test coverage standards for system shall be defined and corrected.
Software configuration management	The configuration is defined, baseline managed properly, the configuration management have recorded, and the systematic control about change, repair and distribution of configuration should be made.
Software quality	The quality assurance activity is carried out as planned, evaluated and

assurance	supplemented to the defined step-by-step completion condition.

d) Inspections of hardware and design assurance: The certification authority shall ensure a system of hardware development and design assurance upon result of standard test evaluation for H/W approval and standard evaluation for hardware test and assessment submitted by developer.

Inspection Items	Inspection Contents
Planning	It should be defined The hardware lifecycle and process-specific activity, step completion conditions, development / verification environment.
Requirements definition	It should be defined only hardware requirements and should be reflected in the safety assessment.
Preliminary design or concept design	It should be verified design and review results based on the requirement and provided with a solution according to the requirements of error and omission.
Critical design	It should be reflected Preliminary design and hardware considerations, and provided with a solution according to the requirements of error and omission and verified design and review results based on the requirement.
Development	It should be reflected sufficient for critical design, and provided in development, installation and assembling the data.
Production conversion	It should be reflected design result of the hardware components, and established sufficiently the production requirements and the manufacturing procedure related to the safety.
Hardware verification	The result of safety analysis should be reflected in the hardware components that is shall be fully. Also. Hardware verification should be defined to develop evidence and arguments that guarantee test criteria based on the requirements.
Configuration management	It should be systematically managed to change shape, recovery and distribution, and defined configuration management item and history record.
Quality Assurance	It should be conducted acceptance test to verify whether the conditions to satisfy the complete step-by-step, maintained the results, and carried out level of quality assurance activities.

e) Inspection of user manual: The certification authority shall ensure a user manual upon instruction manual submitted of installation and operation.

Inspection Item	Inspection Content
Guideline provision	The document such as instructions for use and maintenance instructions should provide for normal operation of CNS/ATM system.

f) Inspection of training and data for education: The certification authority shall ensure appropriate and adequate training has been accomplished upon training data submitted.

Inspection Item	Inspection Content
Guideline provision	The document such as related training materials should provide for normal operation of CNS/ATM system.

— END —