Organisation de l'aviation civile internationale

NOTE DE TRAVAIL

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

ASSEMBLÉE — 39e SESSION

COMMISSION TECHNIQUE

Point 36 : Sécurité de l'aviation et soutien à la mise en œuvre de la navigation aérienne

PROPOSITION D'ÉLÉMENTS D'ORIENTATION POUR DES NORMES DE CERTIFICATION ET DES PROCÉDURES DE DÉVELOPPEMENT DES SYSTÈMES DE COMMUNICATIONS, NAVIGATION ET SURVEILLANCE/GESTION DE LA CIRCULATION AÉRIENNE (CNS/ATM)

(Note présentée par la République de Corée)

RÉSUMÉ ANALYTIQUE

Avec le développement et la diversification technologiques des systèmes de communications, navigation et surveillance/gestion de la circulation aérienne (CNS/ATM), la certification sur le plan de la sécurité et de la compatibilité est devenue un aspect important. Il est donc recommandé que l'OACI établisse des procédures de certification normalisées pour l'acceptation de ces systèmes par les États membres. La présente note propose donc une procédure de certification et de développement en vue d'une application internationale des systèmes CNS/ATM.

Suite à donner : L'Assemblée est invitée à considérer que l'OACI devrait, selon les besoins, établir des éléments d'orientation pour les normes de certification et les procédures de développement des systèmes CNS/ATM.

Objectifs stratégiques :	La présente note de travail concerne l'objectif stratégique Sécurité.
Incidences financières :	Sans objet.
Références :	Annexe 10 –*Télécommunications aéronautiques,* Volumes I, II et IV Doc 8071, *Vérification des systèmes terrestres de radionavigation* 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 Pour la sécurité de la navigation des avions, il est important qu'ils soient équipés de systèmes adéquats et précis de communications, de navigation et de surveillance/gestion du trafic aérien (CNS/ATM). Actuellement, l'Annexe 10 de l'OACI et le Doc 8071 définissent les normes internationales de technologies et d'essais fonctionnels. Toutefois, il n'existe pas de procédures de développement et de certification reconnues à l'échelle internationale pour les systèmes CNS/ATM, comme c'est le cas pour les normes de certification des aéronefs, les systèmes certifiés dans les pays exportateurs devraient faire l'objet d'une nouvelle certification fonctionnelle, conforme aux procédures et aux critères de certification du pays importateur. Ces exigences représentent un fardeau considérable pour le développeur de l'équipement qui ne peut s'appuyer sur un processus de développement et de certification normalisés et reconnu au plan international.

1.2 Les systèmes classiques CNS/ATM étaient jusqu'ici approuvés sans procédures de certification normalisées car il s'agissait de systèmes relativement simples. Cependant, il devient important pour les systèmes les plus modernes et les plus complexes de faire l'objet d'une certification fonctionnelle du point de vue de la sécurité, de la cohérence des indications et de la compatibilité. Aujourd'hui, les États-Unis, l'Europe, la Russie, la Chine, ainsi que la République de Corée, développent leurs propres systèmes CNS/ATM, ou les importent d'autres pays, et doivent obtenir la certification de leurs autorités approbatrices car seuls les équipements certifiés peuvent être installés pour une utilisation aéronautique dans quelques États.

1.3 Il est donc nécessaire de proposer un processus de certification normalisé et des procédures de développement reconnues au plan international (à l'exclusion des essais au sol et en vol) selon les points de vue du développeur et des autorités, ce qui est acceptable pour l'OACI. Dans certains pays, l'approbation des systèmes CNS/ATM doit se faire par étape : « Approbation du système », « Approbation des installations » et « Approbation pour le service de la part des autorités de l'aviation ».

2. ANALYSE

2.1 Objet

2.1.1 L'un des buts de la présente note de travail est de proposer qu'un certain nombre de pays dans le monde cherchent à encadrer un système de certification normalisé et cohérent, basé sur l'établissement d'un processus d'approbation normalisé à l'échelle internationale pour les systèmes CNS/ATM. Si les systèmes CNS/ATM d'autres États membres répondent aux mêmes certifications de performance et de sécurité, l'autre but de la note peut être atteint par une certification simplifiée du produit dans le domaine des systèmes CNS/ATM, basée sur la confiance entre les États membres.

2.2 Proposition d'un processus normalisé de l'OACI pour l'approbation des systèmes

2.2.1 Les principaux aspects de la certification des systèmes CNS/ATM sont les suivants :

a) conception selon des exigences applicables à l'équipement concerné ;

b) développement en proportion du niveau d'assurance de la conception ;

c) respect des exigences de performance de système pour l'équipement développé.

2.3 Les processus proposés d'approbation des systèmes CNS/ATM comprendraient les activités suivantes :

a) inspection de sécurité de l'équipement ;

b) inspection des aspects liés en tant que spécification ;

c) inspection de conformité des procédures et des résultats des essais ;

d) inspection du développement du logiciel et système de conception ;

e) inspection du développement du matériel et système d'assurance de conception ;

f) inspection de la documentation de l'utilisateur ;

g) inspection des aspects éducation, formation et données.

3. CONCLUSION

3.1 Pour la normalisation du processus de développement et de certification des systèmes CNS/ATM au plan international, un certain nombre de pays dans le monde entier se préoccupent d'élaborer un système de certification normalisé et cohérent, visant l'amélioration de la sécurité et de la fiabilité de l'aviation.

3.2 S'il existe un niveau équivalent de systèmes de développement et de certification dans les États membres, les produits liés aux systèmes CNS/ATM pourraient faire l'objet d'une simplification du processus de certification et d'une réduction des coûts et des délais de certification nationale sur la base de la confiance entre États membres.

– – – – – – – – – – – –

APPENDICE

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.

— FIN —