国 际 民 用 航 空 组 织

工 作 文 件

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

大会 — 第39届会议

技术委员会

议程项目36：航空安全和空中航行实施支助

关于通信、导航和监视/空中交通管理（CNS/ATM）系统标准认证和开发程序指导材料的建议

（由大韩民国提交）

执行摘要

随着通信、导航和监视/空中交通管理（CNS/ATM）系统的技术开发及多样化，对安全和兼容性等方面进行认证已经变得十分重要。因此，建议国际民航组织制定成员国可接受的标准化认证程序。在本文件中，建议为进行国际实施，制定关于通信、导航和监视/空中交通管理系统的认证及开发程序。

行动:请大会审议国际民航组织是否需要制定关于通信、导航和监视/空中交通管理系统标准认证及开发程序的指导材料。

战略目标：	本工作文件涉及安全的战略目标。
财务影响：	不适用
参考文件：	附件10 —《航空电信》第 I 卷、第 II 卷和第 IV 卷 Doc 8071号文件：《无线电助航设备检测手册》 汽车工程师学会 ARP-4754 / 4761号文件 欧洲民用航空设备组织 ED-79A/ ED-135号文件 航空无线电技术委员会 DO-278A/178C/254号文件 欧洲民用航空设备组织ED-109/ED-12C/ED-80号文件

1. 引言

1.1 为飞机开展安全航行，运行准确无误的通信、导航和监视/空中交通管理(CNS/ATM)系统十分重要。目前，国际民航组织附件 10 和 Doc 8071 号文件处理了关于技术和性能检测的国际标准。但是，在通信、导航和监视/空中交通管理系统当中，由于没有像航空器认证标准那样可以被国际公认的开发及认证程序，出口国家所认证的通信、导航和监视/空中交通管理系统，应当根据进口国家的认证程序和标准进行新的运行认证。因此，这对不具备国际标准化开发和认证过程的设备开发商而言是一个巨大的负担。

1.2 常规的通信、导航和监视/空中交通管理系统因其相对简单，是在没有标准化认证程序的情况下被批准投入运行的。但是，就现代精密且先进的系统而言，具有安全性、一致性和兼容性，对于性能认证十分重要。目前，美国、欧洲、俄罗斯、中国以及大韩民国，正在开发或者通过其他国家进口其各自的通信、导航和监视/空中交通管理系统，并且需要得到其各自审批机关的认证，而且在一些国家只有经过认证的设备才可以安装投入运行。

1.3 因此，从开发商和当局的角度来看，必须提出一个标准化的认证过程以及可以被国际认可、能够被国际民航组织接受的开发程序(不包括地面和飞行检测)。一些国家要求航空当局按照“系统审批”、“设备验收”、最后 “批准运行”的步骤，对通信、导航和监视/空中交通管理进行系统审批。

2. 讨论

2.1 目的

2.1.1 本文件的目的是建议世界各国按照国际上既定的通信、导航和监视/空中交通管理系统的标准化批准过程，制定标准划一的认证系统。如果成员国之间的通信、导航和监视/空中交通管理系统具有相同水准的性能及安全认证系统，便可以确立另外一重目的，即成员国之间在信任的基础上，制定与通信、导航和监视/空中交通管理系统相关的产品简化认证。

2.2 关于国际民航组织系统批准的标准过程的建议

2.2.1 对通信、导航和监视/空中交通管理系统进行认证的主要重点如下:

a) 设计方面，以满足适当的设备要求；

b) 根据设计的保证水平按比例开发；和

c) 满足所开发设备的系统性能要求。

2.3 建议有关通信、导航和监视/空中交通管理系统的系统批准过程如下:

a) 对设备进行安全检查；

b) 检查要求等方面的相关事项；

c) 检查检测程序的适当性、检测程序及检测结果；

d) 检查软件开发和设计保证系统；

e) 检查硬件开发和设计保证系统；

f) 检查使用手册；和

g) 检查教学、培训和数据。

3. 结论

3.1 在对通信、导航和监视/空中交通管理系统的开发和认证过程实行国际标准化时，世界范围内许多国家都为加强航空安全和可靠性处理了标准划一的认证系统。

3.2 如果成员国之间具有相同水准的开发及认证系统，便可以在成员国当中以信任为基础，简化与通信、导航和监视/空中交通管理系统相关产品的认证过程，并节省认证的费用和时间。

— — — — — — — — —

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 assurance	The quality assurance activity is carried out as planned, evaluated and 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 —