Международная организация гражданской авиации

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

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 39-Я СЕССИЯ

ТЕХНИЧЕСКАЯ КОМИССИЯ

Пункт 36 повестки дня. Безопасность полетов и поддержка внедрения в области аэронавигации

ПРЕДЛОЖЕНИЕ В ОТНОШЕНИИ ИНСТРУКТИВНОГО МАТЕРИАЛА В ЦЕЛЯХ СТАНДАРТИЗАЦИИ ПОРЯДКА СЕРТИФИКАЦИИ И РАЗВИТИЯ СИСТЕМ СВЯЗИ, НАВИГАЦИИ И НАБЛЮДЕНИЯ/ОРГАНИЗАЦИИ ВОЗДУШНОГО ДВИЖЕНИЯ (CNS/ATM)

(Представлено Республикой Кореей)

КРАТКАЯ СПРАВКА

В условиях развития и роста количества систем связи, навигации и наблюдения/организации воздушного движения (CNS/ATM) большое значение приобретает сертификация в сфере безопасности полетов и функциональной совместимости. В связи с этим рекомендуется, чтобы ИКАО установила стандартизированные процедуры сертификации, приемлемые для государств-членов. В настоящем документе предлагается порядок сертификации систем CNS/ATM, предназначенных для международного применения.

Действия: Ассамблее предлагается рассмотреть вопрос о необходимости разработки в ИКАО инструктивного материала для стандартизации порядка сертификации и разработки систем CNS/ATM.

Стратегические цели	Данный рабочий документ связан со стратегической целью "Безопасность полетов"
Финансовые последствия	Неприменимо
Справочный материал	Приложение 10, *Авиационная электросвязь*, тома I, II и IV Doc 8071, *Руководство по испытаниям радионавигационных средств* SAE ARP-4754 /4761 EUROCAE ED-79A/ ED-135 RTCA DO-278A/178C/254 EUROCAE ED-109/ED-12C/ED-80

1. ВВЕДЕНИЕ

1.1 Для обеспечения безопасной навигации самолетов важно эксплуатировать правильные и точные системы связи, навигации и наблюдения/организации воздушного движения (CNS/ATM). В настоящее время в Приложении 10 и документе Doc 8071 ИКАО содержатся международные Стандарты по испытаниям техники и характеристик. Однако в связи с отсутствием признанных в международном плане норм в отношении разработки и сертификации систем CNS/ATM, аналогичных Стандартам на сертификацию воздушных судов, системы CNS/ATM, сертифицированные в стране-экспортере, должны вновь сертифицироваться для эксплуатации в соответствии с процедурами и критериями страны-импортера. Поэтому в связи с отсутствием международного стандартизированного процесса разработки и сертификации разработчик оборудования несет огромную нагрузку.

1.2 Традиционные системы CNS/ATM утверждались для эксплуатации в отсутствие стандартизированной процедуры сертификации, потому что они были сравнительно простыми. Однако с точки зрения безопасности полетов, стабильности и совместимости современных сложных и продвинутых систем важно осуществлять сертификацию их характеристик. В настоящее время Соединенные Штаты Америки, государства Европы, Россия, Китай и Республика Корея разрабатывают свои собственные системы CNS/ATM или импортируют их из других стран и должны получать сертификат от своего полномочного органа прежде, чем оборудование будет установлено для эксплуатации в нескольких государствах.

1.3 Поэтому необходимо предложить приемлемый для ИКАО стандартизированный процесс сертификации и международно признанный порядок разработки (исключая наземные и летные испытания) с точки зрения разработчика и полномочного органа. В некоторых странах требуется, чтобы системы CNS/ATM утверждались авиационным полномочным органом в порядке "утверждение системы", затем "утверждение средства" и, наконец, "допуск к эксплуатации".

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Цель

2.1.1 В настоящем документе содержится предложение установить для всего мира стандартизированную и последовательную систему сертификации на основе создания международного стандартизированного процесса утверждения для систем CNS/ATM. В случае, если системы CNS/ATM государств-членов имеют аналогичные характеристики и системы сертификации аспектов безопасности полетов, можно установить упрощенный процесс сертификации соответствующих компонентов систем CNS/ATM, основанный на взаимном доверии государств-членов.

2.2 Предложение в отношении разработки в ИКАО стандартизированного процесса утверждения систем

2.2.1 При сертификации систем CNS/ATM основное внимание уделяется следующим моментам:

a) конструкция должна отвечать требованиям к соответствующему оборудованию;

b) разработка должна вестись в соответствии с уровнем гарантии проектирования;

c) разработанное оборудование должно соответствовать требованиям к характеристикам системы.

2.3 Предлагается следующий процесс утверждения систем CNS/ATM:

a) проверка оборудования на соответствие требованиям безопасности полетов;

b) проверка смежных вопросов, например на соответствие требованиям;

c) проверка готовности к проведению испытаний, проведение испытаний и результаты испытаний;

d) проверка системы разработки и гарантии проектирования программного обеспечения;

e) проверка системы разработки и гарантии проектирования аппаратного оборудования;

f) проверка руководства пользователя;

g) проверка образования, подготовки и данных.

3. ВЫВОД

3.1 Для международной стандартизации процесса разработки и сертификации систем CNS/ATM ряд стран мира создают стандартизированные и последовательные системы сертификации для повышения уровня безопасности полетов и надежности.

3.2 Если в государствах-членах существуют эквивалентные системы разработки и сертификации, можно добиться упрощения процесса сертификации компонентов систем CNS/ATM, сокращения расходов и уменьшения затрат времени на сертификацию на основе взаимного доверия между государствами-членами.

— — — — — — — —

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.

— КОНЕЦ —