REGULAMENTUL (CE) NR. 482/2008 AL COMISIEI

din 30 mai 2008

de stabilire a unui sistem de asigurare a siguranței software care urmează să fie pus în aplicare de către furnizorii de servicii de navigație aeriană și de modificare a anexei II la Regulamentul (CE) nr. 2096/2005

(Text cu relevanță pentru SEE)

COMISIA COMUNITĂȚILOR EUROPENE,

având în vedere Tratatul de instituire a Comunității Europene,

având în vedere Regulamentul (CE) nr. 550/2004 al Parlamentului European și al Consiliului din 10 martie 2004 privind prestarea de servicii de navigație aeriană în Cerul Unic European (regulament privind prestarea de servicii) ([1]), în special articolul 4,

întrucât:

(1) În conformitate cu Regulamentul (CE) nr. 550/2004, Comisia trebuie să identifice și să adopte dispozițiile relevante ale cerințelor Eurocontrol pentru reglementarea siguranței („ESARR"), luând în considerare legislația comunitară existentă. ESARR 6 denumit „Sistemele software ale sistemelor ATM" prevede un set de cerințe pentru reglementarea siguranței în vederea punerii în aplicare a unui sistem de asigurare a siguranței software.

(2) În Regulamentul (CE) nr. 2096/2005 al Comisiei din 20 decembrie 2005 de stabilire a unor cerințe comune pentru furnizarea de servicii de navigație aeriană ([2]) se menționează, la ultima propoziție la considerentul 12, următoarele: „Dispozițiile relevante ale ESARR 1 privind controlul siguranței în domeniul ATM și ale ESARR 6 privind sistemele software ale sistemelor ATM ar trebui identificate și adoptate prin acte comunitare separate."

(3) Anexa II la Regulamentul (CE) nr. 2096/2005 solicită furnizorilor de servicii de navigație aeriană să pună în aplicare un sistem de management al siguranței, precum și cerințele de siguranță pentru o strategie de evaluare și reducere a riscurilor în ceea ce privește modificările. În cadrul sistemului de management al siguranței, și ca parte a activităților de evaluare și reducere a riscurilor în ceea ce privește modificările, un furnizor de servicii de trafic aerian ar trebui să definească și să pună în aplicare un sistem de asigurare a siguranței software care să vizeze, în mod specific, aspectele legate de software.

(4) În ceea ce privește siguranța software, principalul obiectiv de îndeplinit în cazul sistemelor funcționale care conțin software este acela de a garanta reducerea la un nivel tolerabil a riscurilor aferente Autilizării software în cadrul sistemelor privind rețeaua europeană de management al traficului aerian („software EATMN").

(5) Prezentul regulament nu ar trebui să vizeze operațiunile și pregătirea militară menționate la articolul 1 alineatul (2) din Regulamentul (CE) nr. 549/2004 al Parlamentului European și al Consiliului din 10 martie 2004 de stabilire a cadrului pentru crearea Cerului Unic European (regulamentul-cadru) ([3]).

(6) Prin urmare, anexa II la Regulamentul (CE) nr. 2096/2005 ar trebui modificată în consecință.

(7) Măsurile prevăzute de prezentul regulament sunt conforme cu avizul Comitetului pentru Cerul Unic,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Obiectul și domeniul de aplicare

(1) Prezentul regulament stabilește cerințele privind definirea și punerea în aplicare a sistemului de asigurare a siguranței software de către furnizorii de servicii de trafic aerian (ATS), de către entitățile responsabile cu gestionarea fluxului de trafic aerian (ATFM) și cu managementul spațiului aerian (ASM) pentru traficul aerian general precum și de către furnizorii de servicii de comunicații, navigație și supraveghere (CNS).

Acesta identifică și adoptă dispozițiile obligatorii ale cerințelor Eurocontrol pentru reglementarea siguranței software – ESARR 6 denumite „Sistemele software ale sistemelor ATM" emise la data de 6 noiembrie 2003.

(2) Prezentul regulament se aplică software-ului nou și tuturor modificărilor aduse software-ului în sistemele ATS, ASM, ATFM, și CNS.

Acesta nu se aplică software-ului aferent componentelor de bord și amplasat în spațiu.

Articolul 2

Definiții

În sensul prezentului regulament, se aplică definițiile din articolul 2 din Regulamentul (CE) nr. 549/2004.

([1]) JO L 96, 31.3.2004, p. 10.

([2]) JO L 335, 21.12.2005, p. 13. Regulament modificat prin Regulamentul (CE) nr. 1315/2007 (JO L 291, 9.11.2007, p. 16).

([3]) JO L 96, 31.3.2004, p. 1.

De asemenea, se aplică următoarele definiții:

1. „software” înseamnă programe pentru calculator, precum și date de configurare corespunzătoare, inclusiv software comercial, dar excluzând elementele electronice cum ar fi circuitele integrate specifice unei aplicații, rețelele circuit-poartă programabile sau controlerele logice pentru semiconductoare;

2. „date de configurare” înseamnă date care configurează un software generic pentru un caz particular de utilizare;

3. „software comercial” înseamnă software care nu a fost creat pentru actualul contract;

4. „asigurarea siguranței” înseamnă toate acțiunile, planificate și sistematice, necesare pentru a genera încrederea corespunzătoare că un produs, un serviciu, o organizație sau un sistem funcțional atinge un nivel de siguranță acceptabil sau tolerabil;

5. „organizație” înseamnă fie un furnizor de servicii de trafic aerian (ATS), fie un furnizor de comunicare, navigație și supraveghere (CNS), fie o entitate care asigură (ATFM sau ASM);

6. „sistem funcțional” înseamnă o combinație de sisteme, proceduri și resurse umane organizate în scopul îndeplinirii unei funcții în cadrul ATM;

7. „risc” înseamnă combinația între probabilitatea generală sau frecvența de apariție a unui efect dăunător provocat de un pericol și gravitatea acelui efect;

8. „pericol” înseamnă orice situație, eveniment sau circumstanță care ar putea determina un accident;

9. „software nou” înseamnă un software care a fost comandat sau pentru care au fost încheiate contracte ferme după intrarea în vigoare a prezentului regulament;

10. „obiectiv privind siguranța” înseamnă o declarație calitativă sau cantitativă care definește frecvența maximă sau probabilitatea maximă la care poate apărea un pericol;

11. „cerință de siguranță” înseamnă un mijloc de reducere a unui risc, definit în cadrul unei strategii de reducere a riscurilor care permite atingerea unui obiectiv de siguranță specific, incluzând cerințele organizaționale, operaționale, procedurale, funcționale, de performanță, precum și cerințele de interoperabilitate sau caracteristicile de mediu;

12. „tranziție sau transfer în regim operațional” înseamnă modalitatea de înlocuire a componentelor sistemului privind rețeaua europeană de management al traficului aerian (EATMN) sau a software-ului în timp ce sistemul este operațional;

13. „cerință de siguranță software” înseamnă o descriere a ceea ce trebuie să producă software-ul, ținând cont de inputuri și de constrângeri, astfel încât să fie asigurată funcționarea în siguranță a software-ului EATMN și în conformitate cu nevoile operaționale;

14. „software EATMN” înseamnă software utilizat în cadrul sistemelor EATMN menționat la articolul 1;

15. „validarea cerințelor” înseamnă confirmarea prin examinare și furnizare de dovezi obiective că cerințele specifice pentru o anumită utilizare sunt așa cum au fost prevăzute;

16. „realizare în mod independent” înseamnă desfășurarea activităților corespunzătoare procesului de verificare a software-ului de către o persoană (persoane), alta decât cea care a dezvoltat elementul verificat;

17. „defecțiune de software” înseamnă incapacitatea unui program de a efectua, în mod corect, o funcție cerută;

18. „cădere software” înseamnă incapacitatea unui program de a efectua o funcție cerută;

19. „COTS” înseamnă o aplicație disponibilă pe piață, comercializată prin intermediul unor cataloage publice și care nu poate fi personalizată sau îmbunătățită;

20. „componente software” înseamnă un modul care poate fi instalat sau conectat împreună cu alte module software reutilizabile în scopul combinării și al creării unei aplicații software specifice;

21. „componente independente software” înseamnă acele componente software care nu sunt scoase din operare de către defecțiunea care a determinat apariția pericolului;

22. „performanțele privind timpul de răspuns al software-ului” înseamnă timpul necesar software-ului de a răspunde unor inputuri date sau unor evenimente periodice, și/sau performanța software în ceea ce privește tranzacțiile sau mesajele prelucrate în unitatea de timp;

23. „capacitate software” înseamnă abilitatea software-ului de a prelucra un anumit volum de flux de date;

24. „acuratețe” înseamnă gradul necesar de precizie pentru rezultatele calculate;

25. „utilizarea resurselor software” înseamnă cantitatea de resurse din cadrul unui sistem de calcul care poate fi utilizată de către aplicația software;

26. „robustețea software" înseamnă comportamentul software-ului în cazul apariției unor inputuri neașteptate, al cedării componentelor hardware și al penelor de curent, fie în cadrul sistemului de calcul, fie în cadrul dispozitivelor conectate la acesta;

27. „toleranță la supraîncărcare" înseamnă comportamentul unui sistem și, în special, toleranța acestuia, atunci când inputurile au loc cu o frecvență mai mare decât cea prevăzută pentru exploatarea normală a sistemului;

28. „verificare completă și corectă a software-ului EATMN" înseamnă că toate cerințele de siguranță software definesc în mod corect exigențele privind componenta software ca urmare a procesului de evaluare și reducere a riscurilor, iar punerea lor în aplicare este dovedită la nivelul cerut de către nivelul de asigurare software;

29. „date privind ciclul de viață software" înseamnă date produse pe perioada ciclului de viață software pentru a planifica, conduce, explica, defini, înregistra sau pentru a furniza dovezi privind activitățile desfășurate; aceste date permit desfășurarea proceselor aferente ciclului de viață software, autorizarea sistemelor sau a echipamentelor și modificarea post-autorizare a produsului software;

30. „ciclu de viață software" înseamnă:

(a) o colecție ordonată de procese stabilite de o organizație ca fiind suficiente și corespunzătoare pentru a produce un produs software;

(b) perioada de timp care începe odată cu decizia de a produce sau de a modifica un produs software și care se termină atunci când produsul respectiv este retras din serviciu;

31. „cerință de siguranță" înseamnă o cerință de siguranță aplicabilă unui sistem funcțional.

Articolul 3

Cerințe generale de siguranță

(1) Atunci când unei organizații i se cere să pună în aplicare un proces de evaluare și reducere a riscurilor, în conformitate cu legislația comunitară sau națională în vigoare, aceasta definește și pune în aplicare un sistem de asigurare a siguranței software care să vizeze, în mod specific, aspectele legate de software EATMN, inclusiv toate modificările on-line aduse software-ului în regim operațional, cum ar fi tranziția sau transferul în regim operațional.

(2) Organizația se asigură, cel puțin, că sistemul său de asigurare a siguranței software produce dovezi și argumente care demonstrează următoarele:

(a) cerințele de siguranță software precizează în mod corect criteriile necesare pentru ca software-ul să îndeplinească obiectivele și cerințele privind siguranța definite în cadrul procesului de evaluare și reducere a riscurilor;

(b) trasabilitatea este avută în vedere în ceea ce privește toate cerințele de siguranță software;

(c) implementarea software-ului nu include funcții care să afecteze grav siguranța;

(d) software-ul EATMN satisface cerințele aplicabile în cazul său, la un nivel de încredere corespunzător nivelului de risc al software-ului;

(e) sunt prevăzute garanții care confirmă respectarea cerințelor generale de siguranță menționate la literele (a)-(d), iar argumentele care demonstrează că garanțiile necesare în acest sens derivă întotdeauna:

(i) dintr-o versiune executabilă cunoscută a software-ului;

(ii) dintr-o gamă cunoscută de date de configurare;

(iii) dintr-un set cunoscut de produse și descrieri software, inclusiv specificații, care au fost utilizate la realizarea acelei versiuni.

(3) Organizația trebuie să furnizeze autorității naționale de supraveghere garanțiile necesare, demonstrând că cerințele prevăzute la alineatul (2) sunt îndeplinite.

Articolul 4

Cerințe privind sistemul de asigurare a siguranței software

Organizația se asigură, cel puțin, că sistemul de asigurare a siguranței software:

1. este documentat, în mod specific ca parte a documentației generale de evaluare și reducere a riscurilor;

2. alocă niveluri de asigurare software tuturor aplicațiilor software EATMN operaționale, în conformitate cu cerințele prevăzute în anexa I;

3. include asigurări privind:

(a) validitatea cerințelor de siguranță software, în conformitate cu cerințele prevăzute în anexa II partea A;

(b) verificarea software, în conformitate cu cerințele prevăzute în anexa II partea B;

(c) managementul configurației software, în conformitate cu cerințele prevăzute în anexa II partea C;

(d) trasabilitatea cerințelor de siguranță software în conformitate cu cerințele prevăzute în anexa II, partea D;

4. determină gradul de rigoare pentru stabilirea garanțiilor; gradul de rigoare trebuie definit pentru fiecare nivel de asigurare software și crește pe măsură ce crește nivelul de risc al software-ului, în acel sens:

(a) variația gradului de rigoare a garanțiilor per nivel de asigurare software trebuie să includă următoarele criterii:

(i) obligația realizării în mod independent;

(ii) obligația realizării;

(iii) nicio obligație;

(b) garanțiile corespunzătoare fiecărui nivel de asigurare software trebuie să ofere suficientă încredere că software-ul EATMN poate fi operat în condiții tolerabile de siguranță;

5. utilizează rezultatele experienței utilizării software-ului EATMN pentru a confirma faptul că sistemul de asigurare a siguranței software și alocarea nivelurilor de asigurare software sunt corespunzătoare. În acel scop, efectele unei căderi sau ale unei defecțiuni a software-ului, notificate în conformitate cu cerințele relevante privind notificarea și evaluarea evenimentelor legate de siguranță, se evaluează în comparație cu efectele asupra sistemului în cauză identificate conform schemei de clasificare a gravității prevăzută în anexa II secțiunea 3.2.4 la Regulamentul (CE) nr. 2096/2005.

Articolul 5

Cerințe privind modificările de software și pentru tipuri specifice de software-uri specifice

(1) În cazul oricăror modificări aduse software-ului sau pentru tipuri specifice de software cum ar fi COTS, software comercial sau software reutilizat cărora nu se pot aplica unele cerințe prevăzute la articolul 3 alineatul (2) litera (d) sau (e) sau la articolul 4 punctul 2, 3, 4 sau 5, organizația se asigură că sistemul de asigurare a siguranței software prevede, prin intermediul altor mijloace alese și convenite împreună cu autoritatea națională de supraveghere, același nivel de încredere ca și nivelul relevant de asigurare software care a fost definit.

Aceste mijloace trebuie să ofere suficientă încredere că software-ul îndeplinește obiectivele și cerințele de siguranță definite în cadrul procesului de evaluare și reducere a riscurilor pentru siguranță.

(2) În vederea evaluării mijloacelor menționate la alineatul (1), autoritatea națională de supraveghere poate utiliza o organizație recunoscută sau un organism autorizat.

Articolul 6

Modificarea Regulamentului (CE) nr. 2096/2005

În anexa II la Regulamentul (CE) nr. 2096/2005, se adaugă următoarea secțiune:

„3.2.5 Secțiunea 5

Sistem de asigurare a siguranței software

În cadrul exploatării sistemului de management al siguranței, un furnizor de servicii de navigație aeriană pune în aplicare un sistem de asigurare a siguranței software în conformitate cu Regulamentul (CE) nr. 482/2008 al Comisiei din 30 mai 2008 de stabilire a unui sistem de asigurare a siguranței software care urmează să fie pus în aplicare de către furnizorii de servicii de navigație aeriană și de modificare a anexei II la Regulamentul (CE) nr. 2096/2005 (*).

(*) JO L 141, 31.5.2008, p. 5."

Articolul 7

Intrarea în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Se aplică începând cu 1 ianuarie 2009 pentru software-ul nou al sistemelor EATMN prevăzut la articolul 1 alineatul (2) primul paragraf.

Se aplică începând cu 1 iulie 2010 pentru noile modificări de software al sistemelor EATMN menționate la articolul 1 alineatul (2) primul paragraf care sunt operaționale la acea dată.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 30 mai 2008.

Pentru Comisie
Antonio TAJANI
Membru al Comisiei

ANEXA I

Cerințe privind nivelul de asigurare software menționat la articolul 4 alineatul (2)

1. Nivelul de asigurare software asociază gradul de rigoare a garanțiilor software cu nivelul de risc al software-ului EATMN prin utilizarea schemei de clasificare a gravității prevăzută în anexa II punctul 3.2.4 secțiunea 4 la Regulamentul (CE) nr. 2096/2005 coroborată cu probabilitatea apariției unui anumit efect advers. Se identifică cel puțin 4 niveluri de asigurare software, nivelul de asigurare software 1 reprezentând nivelul cel mai critic.

2. Un nivel alocat de asigurare software este proporțional cu cel mai grav efect pe care defecțiunile sau căderile de software îl pot cauza, în conformitate cu anexa II punctul 3.2.4 secțiunea 4 la Regulamentul (CE) nr. 2096/2005. Acesta ia în considerare, în special, riscurile asociate cu defecțiunile sau căderile de software, precum și cu metodele de apărare arhitecturale și/sau procedurale identificate.

3. Componentelor de software EATMN, a căror independență una față de alta nu poate fi dovedită, li se alocă nivelul de asigurare software aferent componentei dependente cu cel mai mare grad de pericol.

ANEXA II

Partea A: Cerințe pentru garanțiile privind validitatea cerințelor de siguranță software prevăzute la articolul 4 alineatul (3) litera (a)

1. Cerințele de siguranță software precizează comportamentul funcțional, în regim nominal și degradat, al software-ului EATMN, performanțele privind timpul de răspuns, capacitatea, acuratețea, utilizarea resurselor software pe hardware-ul pe care acesta urmează să fie instalat, robustețea în condiții de operare anormale, precum și toleranța la supraîncărcare, după caz.

2. Cerințele de siguranță software sunt complete, corecte și conforme cu cerințele de siguranță a sistemului.

Partea B: Cerințe pentru garanțiile privind verificarea software prevăzute la articolul 4 alineatul (3) litera (b)

1. Comportamentul funcțional al software-ului EATMN, performanțele privind timpul de procesare, capacitatea, acuratețea, utilizarea resurselor software pe hardware-ul pe care acesta urmează să fie instalat, robustețea în condiții de operare anormale, precum și toleranța la supraîncărcare sunt conforme cu cerințele software.

2. Software-ul EATMN este verificat în mod corespunzător prin analize și/sau teste și/sau mijloace echivalente, conform celor convenite cu autoritatea națională de supraveghere.

3. Verificarea software-ului EATMN trebuie să fie corectă și completă.

Partea C: Cerințe pentru garanțiile privind managementul configurației software prevăzute la articolul 4 alineatul (3) litera (c)

1. Există proceduri de identificare a configurației, de trasabilitate și de înregistrare a statutului configurației, care permit să se demonstreze că datele privind ciclul de viață software se află sub controlul configurației pe tot parcursul ciclului de viață al software-ului EATMN.

2. Există proceduri de notificare și de urmărire a problemelor, precum și măsuri corective, care permit să se demonstreze că problemele de siguranță software au fost diminuate.

3. Există proceduri de recuperare și de accesare care permit ca datele privind ciclul de viață software să poată fi regenerate și furnizate pe tot parcursul ciclului de viață al software-ului EATMN.

Partea D: Cerințe pentru garanțiile privind trasabilitatea cerințelor de siguranță software prevăzute la articolul 4 alineatul (3) litera (d)

1. Fiecare cerință de siguranță software este trasabilă până la nivelul de proiectare la care este demonstrată îndeplinirea acesteia.

2. Fiecare cerință de siguranță software, la fiecare nivel de proiectare la care este demonstrată îndeplinirea acesteia, este trasabilă la o cerință de siguranță a sistemului.