KOMMISSIONENS FORORDNING (EF) Nr. 482/2008

af 30. maj 2008

om etablering af et softwaresikringssystem, der skal indføres af luftfartstjenesteudøvere, og om ændring af bilag II til forordning (EF) nr. 2096/2005

(EØS-relevant tekst)

KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER HAR —

under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab,

under henvisning til Europa-Parlamentets og Rådets forordning (EF) nr. 550/2004 af 10. marts 2004 om udøvelse af luftfartstjenester i det fælles europæiske luftrum (»luftfartstjenesteforordningen«) ([1]), særlig artikel 4, og

ud fra følgende betragtninger:

(1) I henhold til forordning (EF) nr. 550/2004 skal Kommissionen identificere og vedtage de relevante bestemmelser blandt Eurocontrols sikkerhedskrav (Eurocontrol Safety Regulatory Requirements — ESARR) under hensyn til gældende fællesskabsret. ESARR 6 med overskriften »software i lufttrafikstyringssystemer« indeholder et sæt sikkerhedskrav til indførelsen af et softwaresikringssystem.

(2) Kommissionens forordning (EF) nr. 2096/2005 af 20. december 2005 om fælles krav til udøvelse af luftfartstjenester ([2]) angiver i betragtning 12, sidste punktum, at »de relevante bestemmelser i ESARR 1 om kontrol med flyvesikkerheden i ATM og i ESARR 6 om software i ATM-systemer bør fastlægges og vedtages ved separate fællesskabsretsakter«.

(3) Bilag II til forordning (EF) nr. 2096/2005 pålægger udøvere af lufttrafiktjeneste at indføre et flyvesikkerhedsstyringssystem og flyvesikkerhedsmæssige krav til risikovurdering og -reduktion ved ændringer. Udøvere af lufttrafiktjeneste bør inden for rammerne af deres sikkerhedsstyringssystemer og som led i deres risikovurdering og risikoreduktion ved ændringer fastlægge og indføre et softwaresikringssystem særligt for forhold vedrørende software.

(4) Det vigtigste mål med hensyn til softwaresikkerhed, som skal opfyldes af funktionelle systemer, der indeholder software, er at sikre, at risiciene i forbindelse med brugen af software i systemer i det europæiske lufttrafikstyringsnet (EATMN-software) nedbringes til et tolerabelt niveau.

(5) Denne forordning bør ikke omfatte militære operationer og militær træningsflyvning som omhandlet i artikel 1, stk. 2, i Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004 af 10. marts 2004 om rammerne for oprettelse af et fælles europæisk luftrum (rammeforordningen) ([3]).

(6) Bilag II til forordning (EF) nr. 2096/2005 bør derfor ændres i overensstemmelse hermed.

(7) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelse fra Udvalget for det Fælles Luftrum —

UDSTEDT FØLGENDE FORORDNING:

Artikel 1

Genstand og anvendelsesområde

1. Denne forordning fastsætter kravene til fastlæggelsen og indførelsen af et softwaresikringssystem over for udøvere af lufttrafiktjeneste (ATS), enheder, der leverer lufttrafikregulering (ATFM) og luftrumsregulering (ASM) i forbindelse med almen lufttrafik, og udøvere af kommunikations-, navigations- og overvågningstjenester (CNS).

Forordningen fastlægger og vedtager de bindende bestemmelser i Eurocontrol-sikkerhedskrav — ESARR 6 — med overskriften »Software i lufttrafikstyringssystemer«, der er udstedt den 6. november 2003.

2. Denne forordning gælder for ny software og enhver ændring af softwaren i ATS-, ASM-, ATFM- og CNS-systemerne.

Denne forordning omfatter ikke software til luftbårne komponenter og luftrumsbaseret udstyr.

Artikel 2

Definitioner

Definitionerne i artikel 2 i forordning (EF) nr. 549/2004 finder anvendelse på nærværende forordning.

([1]) EUT L 96 af 31.3.2004, s. 10.
([2]) EUT L 335 af 21.12.2005, s. 13. Ændret ved forordning (EF) nr. 1315/2007 (EUT L 291 af 9.11.2007, s. 16).
([3]) EUT L 96 af 31.3.2004, s. 1.

Endvidere forstås ved:

1) »software«: edbprogrammer og tilhørende konfigurationsdata, inklusive tidligere udviklet software, men undtagen elektroniske dele som f.eks. applikationsspecifikke integrerede kredsløb, programmerbare gate arrays eller solid-state logiske controllere

2) »konfigurationsdata«: data, som konfigurerer et generisk softwaresystem til et særligt anvendelsesformål

3) »tidligere udviklet software«: software, der ikke er udviklet inden for den nugældende kontrakt

4) »sikring«: alle planlagte og systematisk udførte handlinger, som er nødvendige for at skabe tilstrækkelig tillid til, at et produkt, en tjeneste, en virksomhed eller et funktionssystem opnår acceptabel eller tolerabel sikkerhed

5) »organisation«: en ATS-udøver, en CNS-udøver eller en enhed, der leverer ATFM eller ASM

6) »funktionssystem«: en kombination af systemer, procedurer og menneskelige ressourcer, der er organiseret med henblik på at udfylde en funktion i lufttrafikstyringen

7) »risiko«: kombinationen af den overordnede sandsynlighed for eller hyppighed af en skadelig virkning, der er forårsaget af en fare, og alvoren af en sådan virkning

8) »fare«: ethvert forhold og enhver begivenhed eller omstændighed, som kan føre til et havari

9) »ny software«: software, som er bestilt efter denne forordnings ikrafttræden, eller som der er underskrevet en bindende kontrakt om efter denne forordnings ikrafttræden

10) »sikkerhedsmål«: en kvalitativ eller kvantitativ opgørelse, som fastlægger den maksimale hyppighed eller sandsynlighed for, at en fare kan forventes at indtræde

11) »sikkerhedskrav«: et middel til risikoreduktion, der er fastlagt på grundlag af strategien for risikoreduktion, og hvorved der opfyldes et særligt sikkerhedsmål, herunder krav, der vedrører organisation, drift, procedurer, funktion, resultater, interoperabilitet eller miljøegenskaber

12) »cutover eller hot swapping«: det at udskifte systemkomponenter eller software i det europæiske lufttrafikstyringsnet (EATMN), medens systemet er i drift

13) »sikkerhedskrav til software«: en beskrivelse af, hvad softwaren skal frembringe på grundlag af input og begrænsninger, og opfyldelsen af disse sikrer, at EATMN-softwaren fungerer sikkert og opfylder det operationelle behov

14) »EATMN-software«: software, som anvendes i EATMN-systemerne i artikel 1

15) »kravvalidering«: en bekræftelse efter undersøgelse og tilvejebringelse af objektiv dokumentation for, at de særlige krav til et specifikt anvendelsesformål følger hensigten

16) »opnå ved uafhængig verifikation«: ved verifikation af software den omstændighed, at verifikationsprocesaktiviteterne udføres af en eller flere personer, som ikke har deltaget i udviklingen af det verificerede objekt

17) »softwarefunktionsfejl«: et programs manglende evne til at udføre en påkrævet funktion korrekt

18) »softwaresvigt«: et programs manglende evne til at udføre en påkrævet funktion

19) »COTS«: (Commercial Off The Shelf) en applikation, som sælges af forhandlere via offentligt tilgængelige katalogvarer, og som normalt ikke skal tilpasses eller forbedres

20) »softwarekomponenter«: moduler, der kan indbygges eller forbindes med andre genanvendelige softwaremoduler for at kombinere og skabe en brugerdefineret softwareapplikation

21) »uafhængige softwarekomponenter«: softwarekomponenter, der ikke sættes ud af drift som følge af den svigttilstand, der forårsager faren

22) »softwarens responstid«: den tid, softwaren må bruge på at reagere på et givet input eller på periodiske hændelser, og/eller softwarens præstationer målt på antal behandlede transaktioner eller beskeder pr. tidsenhed

23) »softwarekapacitet«: softwarens evne til at håndtere en given datastrøm

24) »nøjagtighed«: kravet til de databeregnede resultaters præcision

25) »softwareressourceudnyttelse«: den mængde ressourcer i computersystemet, som softwareapplikationen kan udnytte

26) »softwarestabilitet«: softwarens respons på uventede input, hardwaresvigt og strømafbrydelser enten i selve computersystemet eller i tilsluttede enheder

27) »overload tolerance«: systemets respons, og særlig dets tolerance, over for input, der forekommer med større intensitet, end det forventes under systemets normale drift

28) »korrekt og komplet verifikation af EATMN-software«: alle sikkerhedskrav til software, som på korrekt vis angiver, hvad der kræves af softwarekomponenten i overensstemmelse med risikovurderings- og risikoreduktionsprocessen, og opfyldelsen af sikkerhedskravene er dokumenteret i henhold til det niveau, der kræves ifølge softwaresikringsniveauet

29) »softwarelivscyklusdata«: data, der frembringes i løbet af softwarens livscyklus for at planlægge, styre, forklare, definere, registrere eller dokumentere aktiviteter. Disse data letter softwarelivscyklusprocesserne og godkendelsen af systemet eller udstyret samt ændringer af softwareproduktet efter godkendelsen

30) »softwarelivscyklus«:

a) en ordnet samling af processer, som en organisation betragter som tilstrækkelig og passende til at frembringe et softwareprodukt

b) en tidsperiode, som begynder med beslutningen om at frembringe eller ændre et softwareprodukt, og som ender, når produktet tages ud af drift

31) »sikkerhedskrav til systemet«: et sikkerhedskrav, der gælder for et funktionssystem.

Artikel 3

Almene sikkerhedskrav

1. Når en organisation skal gennemføre en risikovurderings- og risikoreduktionsproces i henhold til gældende fællesskabslovgivning eller national lovgivning, skal den definere og indføre et softwaresikringssystem særligt for forhold vedrørende EATMN-software, herunder alle online driftsmæssige ændringer af softwaren såsom cutover og hot swapping.

2. Organisationen sikrer som minimum, at dens softwaresikringssystem frembringer dokumentation og argumenter, der viser følgende:

a) sikkerhedskravene til softwaren angiver på korrekt vis, hvad der kræves af softwaren for at opfylde sikkerhedsmålene og -kravene fastlagt i risikovurderings- og risikoreduktionsprocessen

b) der tages højde for sporbarhed i alle sikkerhedskrav til softwaren

c) softwareimplementeringen indeholder ingen funktioner, som indvirker negativt på sikkerheden

d) EATMN-software opfylder kravene med en pålidelighedsgrad, der modsvarer softwarens kritikalitet

e) det er sikret, at de almene sikkerhedskrav i litra a) til d) er opfyldt, og argumenter til støtte for den påkrævede sikkerhed kan til enhver tid udledes af:

i) en kendt eksekverbar version af softwaren

ii) et kendt spektrum af konfigurationsdata

iii) et kendt sæt softwareprodukter og -beskrivelser, herunder specifikationer, der er benyttet til fremstillingen af denne version.

3. Organisationen stiller den påkrævede dokumentation af, at kravene i stk. 2 er opfyldt, til rådighed for den nationale tilsynsmyndighed.

Artikel 4

Krav til softwaresikringssystemet

Organisationen sørger som minimum for, at softwaresikringssystemet:

1) er dokumenteret, især som en del af dokumentationen vedrørende den overordnede risikovurdering og -reduktion

2) tildeler softwaresikringsniveauer til al operationel EATMN-software i overensstemmelse med kravene i bilag I

3) omfatter godtgørelse af, at:

a) sikkerhedskravene til softwaren er valideret i overensstemmelse med kravene i bilag II, del A

b) softwaren er verificeret i overensstemmelse med kravene i bilag II, del B

c) softwarens konfigurationsstyring er i overensstemmelse med kravene i bilag II, del C

d) sikkerhedskravene til softwaren er sporbare i overensstemmelse med kravene i bilag II, del D

4) fastsætter, med hvilken grad af strenghed sikringen er godtgjort; strengheden af kravene, der stilles til godtgørelsen, defineres for hvert softwaresikringsniveau og skærpes, når softwarens kritikalitet øges; i den forbindelse gælder følgende:

a) afhængig af softwaresikringsniveauet stilles der forskellige krav til godtgørelsens strenghed på grundlag af følgende kriterier:

i) skal opnås ved uafhængig verifikation

ii) skal opnås

iii) skal ikke opnås

b) den godtgørelse, som kræves ved hvert softwaresikringsniveau, skal give tilstrækkelig tillid til, at EATMN-software kan benyttes med en tolerabel sikkerhedsrisiko

5) anvender feedback fra erfaringer med EATMN-software til at bekræfte, at softwaresikringssystemet og tildelingen af sikringsniveauer er hensigtsmæssige. Virkningerne af en softwarefunktionsfejl eller et softwaresvigt, der indberettes i henhold til de relevante krav om indberetning og vurdering af sikkerhedsmæssige hændelser, skal vurderes til dette formål sammenholdt med de virkninger, der er påpeget for det pågældende system i henhold til alvorsklassifikationsskemaet i afsnit 3.2.4 i bilag II til forordning (EF) nr. 2096/2005.

Artikel 5

Krav, der gælder for ændringer af software og specifik software

1. For ændringer af software eller specifikke softwaretyper såsom COTS, tidligere udviklet software eller tidligere benyttet software, hvor nogle af kravene i artikel 3, stk. 2, litra d) eller e), eller artikel 4, stk. 2, 3, 4 eller 5, ikke kan anvendes, sørger organisationen for, at softwaresikringssystemet med andre midler, der udvælges og aftales med de nationale tilsynsmyndigheder, skaber samme pålidelighedsgrad som for det pågældende softwaresikringsniveau, når et sådan er defineret.

Disse midler skal skabe tilstrækkelig tillid til, at softwaren opfylder sikkerhedsmålene og -kravene i overensstemmelse med risikovurderings- og risikoreduktionsprocessen.

2. Ved vurderingen af midlerne i stk. 1 kan den nationale tilsynsmyndighed benytte en anerkendt organisation eller et bemyndiget organ.

Artikel 6

Ændring af forordning (EF) nr. 2096/2005

I bilag II til forordning (EF) nr. 2096/2005 indsættes følgende afdeling:

»3.2.5. Afdeling 5

Softwaresikringssystem

Inden for rammerne af flyvesikkerhedsstyringssystemet indfører luftfartstjenesteudøvere et softwaresikringssystem i overensstemmelse med Kommissionens forordning (EF) nr. 482/2008 af 30. maj 2008 om etablering af et softwaresikringssystem, der skal indføres af luftfartstjenesteudøvere, og om ændring af bilag II til forordning (EF) nr. 2096/2005 (*).

(*) EUT L 141 af 31.5.2008, s. 5.«

Artikel 7

Ikrafttrædelse

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Fra den 1. januar 2009 finder forordningen anvendelse på ny software inden for de i artikel 1, stk. 2, første afsnit, nævnte systemer i det europæiske lufttrafikstyringsnet.

Fra den 1. juli 2010 finder forordningen anvendelse på alle ændringer af softwaren i de i artikel 1, stk. 2, første afsnit, nævnte systemer i det europæiske lufttrafikstyringsnet, der er i drift på denne dato.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 30. maj 2008.

På Kommissionens vegne

Antonio TAJANI

Medlem af Kommissionen

BILAG I

Krav vedrørende det i artikel 4, stk. 2, omhandlede softwaresikringsniveau

1. Softwaresikringsniveauet skal stå i forhold til graden af strenghed for softwaresikringen med hensyn til EATMN-softwarens kritikalitet under anvendelse af alvorsklassifikationsskemaet i afsnit 3.2.4, afdeling 4, i bilag II til forordning (EF) nr. 2096/2005, sammenholdt med sandsynligheden for, at en given negativ virkning forekommer. Der opstilles som minimum fire softwaresikringsniveauer, hvor softwaresikringsniveau 1 står for det mest kritiske niveau.

2. Et tildelt softwaresikringsniveau skal stå i forhold til de mest alvorlige virkninger, som softwarefunktionsfejl eller -svigt kan afstedkomme, jf. bilag II, afsnit 3.2.4, afdeling 4, i bilag II til forordning (EF) nr. 2096/2005. Der skal navnlig tages hensyn til risiciene i forbindelse med softwarefunktionsfejl eller -svigt og de fundne arkitektur- eller proceduremæssige modforanstaltninger.

3. EATMN-softwarekomponenter, som det ikke kan påvises er indbyrdes uafhængige, tildeles softwaresikringsniveauet for den mest kritiske af de indbyrdes afhængige komponenter.

BILAG II

Del A: Krav vedrørende den i artikel 4, nr. 3, litra a), omhandlede sikring af, at sikkerhedskravene til software er valideret

1. I sikkerhedskravene til softwaren specificeres EATMN-softwarens funktionelle respons ved nominelt og nedsat funktionsniveau, dvs. responstid, kapacitet, nøjagtighed, softwareressourceudnyttelse af den dertil bestemte hardware, stabilitet over for unormale driftsforhold og overloadtolerance, når dette er relevant.

2. Sikkerhedskravene til softwaren skal være komplette og korrekte og være i overensstemmelse med sikkerhedskravene til systemet.

Del B: Krav vedrørende den i artikel 4, nr. 3, litra b), omhandlede sikring af, at softwaren er verificeret

1. EATMN-softwarens funktionelle respons, responstid, kapacitet, nøjagtighed, softwareressourceudnyttelse af den dertil bestemte hardware, stabilitet over for unormale driftsforhold og overload tolerance skal opfylde kravene til softwaren.

2. EATMN-softwaren skal verificeres i tilstrækkelig grad med analyse og/eller afprøvning og/efter tilsvarende midler efter aftale med den nationale tilsynsmyndighed.

3. EATMN-softwaren skal verificeres på korrekt og komplet vis.

Del C: Krav vedrørende den i artikel 4, nr. 3, litra c), omhandlede sikring af softwarens konfigurationsstyring

1. Konfigurationsidentifikation, sporbarhed og tilstandsregistrering skal forefindes, således at det kan påvises, at softwarelivscyklusdata er under konfigurationskontrol under EATMN-softwarens samlede livscyklus.

2. Der foretages indberetning og sporing af problemer samt korrigerende handlinger, således at det kan påvises, at sikkerhedsrelaterede problemer ved softwaren er imødegået.

3. Procedurer for retrieval og release skal forefindes, således at softwarelivscyklusdata kan genoprettes og leveres i EATMN-softwarens samlede livscyklus.

Del D: Krav vedrørende den i artikel 4, nr. 3, litra d), omhandlede sikring af sporbarheden af sikkerhedskravene til software

1. Hvert sikkerhedskrav til software skal føres tilbage til det samme designniveau, hvor det er påvist at være tilfredsstillende.

2. Hvert sikkerhedskrav til software på hvert designniveau, hvor det er påvist at være tilfredsstillende, skal føres tilbage til et sikkerhedskrav til systemet.