KOMMISJONSFORORDNING (EF) nr. 482/2008

2014/EØS/21/22

av 30. mai 2008

om opprettelse av et system for sikkerhetsbekreftelse av programvare, som skal gjennomføres av ytere av flysikringstjenester, og om endring av vedlegg II til forordning (EF) nr. 2096/2005(*)

KOMMISJONEN FOR DE EUROPEISKE FELLESSKAP HAR —

under henvisning til traktaten om opprettelse av Det europeiske fellesskap,

under henvisning til europaparlaments- og rådsforordning (EF) nr. 550/2004 av 10. mars 2004 om yting av flysikringstjenester i Det felles europeiske luftrom (tjenesteytingsforordningen)([1]), særlig artikkel 4, og

ut fra følgende betraktninger:

1) I henhold til forordning (EF) nr. 550/2004 skal Kommisjonen bestemme og vedta de relevante bestemmelser i Eurocontrols regelverksbaserte sikkerhetskrav (Eurocontrol Safety Regulatory Requirements, ESARR), idet det tas hensyn til Fellesskapets eksisterende regelverk. ESARR 6 med tittelen «Programvare i ATM-systemer» inneholder en samling regelverksbaserte sikkerhetskrav til gjennomføringen av et system for sikkerhetsbekreftelse av programvare.

2) I kommisjonsforordning (EF) nr. 2096/2005 av 20. desember 2005 om fastsettelse av felles krav til yting av flysikringstjenester([2]) er det i siste punktum i betraktning 12 fastsatt at «de relevante bestemmelser i ESARR 1 om tilsyn med sikkerheten innen lufttrafikkstyring, og i ESARR 6 om programvare i ATM-systemer, bør bestemmes og vedtas i egne fellesskapsrettsakter.»

3) I henhold til vedlegg II til forordning (EF) nr. 2096/2005 skal ytere av lufttrafikktjenester innføre et sikkerhetsstyringssystem samt sikkerhetskrav som gjelder risikovurdering og –reduksjon ved endringer. Yteren av lufttrafikktjenestene bør innenfor rammen av sitt sikkerhetsstyringssystem, og som en del av sine risikovurderings- og risikoreduksjonstiltak ved endringer, utarbeide og gjennomføre et system for sikkerhetsbekreftelse av programvare som særlig skal omfatte forhold knyttet til programvare.

4) Når det gjelder programvare, er det viktigste sikkerhetsmålet som skal oppfylles av funksjonssystemene som inneholder programvare, å sikre at risikoene forbundet med bruken av programvare i systemer i Det europeiske nett for lufttrafikkstyring (EATMN-programvare) er redusert til et akseptabelt nivå.

5) Denne forordning bør ikke omfatte militære operasjoner og militær trening som nevnt i artikkel 1 nr. 2 i europaparlaments- og rådsforordning (EF) nr. 549/2004 av 10. mars 2004 om fastsettelse av rammeregler for opprettelse av et felles europeisk luftrom (rammeforordningen)([3]).

6) Vedlegg II til forordning (EF) nr. 2096/2005 bør derfor endres.

7) Tiltakene fastsatt i denne forordning er i samsvar med uttalelse fra Komiteen for det felles luftrom —

VEDTATT DENNE FORORDNING:

Artikkel 1

Formål og virkeområde

1. I denne forordning fastsettes kravene til utarbeiding og innføring av et system for sikkerhetsbekreftelse av programvare, som skal gjennomføres av ytere av lufttrafikktjenester (ATS), enheter for trafikkflytstyring (ATFM) og styring av luftrommet (ASM) i forbindelse med allmenn lufttrafikk, og av ytere av kommunikasjons-, navigerings- og overvåkingstjenester (CNS).

Ved forordningen bestemmes og vedtas de obligatoriske bestemmelsene i Eurocontrols regelverksbaserte sikkerhetskrav — ESARR 6 — med tittelen «Programvare i ATM-systemer», som ble utgitt 6. november 2003.

2. Denne forordning får anvendelse på ny programvare og på alle endringer av programvare i ATS-, ASM-, ATFM- og CNS-systemene.

Den får ikke anvendelse på programvaren i luftbårne komponenter eller på rombasert utstyr.

Artikkel 2

Definisjoner

I denne forordning får definisjonene fastsatt i artikkel 2 i forordning (EF) nr. 549/2004 anvendelse.

(*) Denne fellesskapsrettsakten, kunngjort i EUT L 141 av 31.5.2008, s. 5, er omhandlet i EØS-komiteens beslutning nr. 8/2009 av 5. februar 2009 om endring av EØS-avtalens vedlegg II (Tekniske forskrifter, standarder, prøving og sertifisering) og XIII (Transport), se EØS-tillegget til *Den europeiske unions tidende* nr. 16, 19.3.2009, s. 13.

([1]) EUT L 96 av 31.3.2004, s. 10.

([2]) EUT L 335 av 21.12.2005, s. 13. Forordningen endret ved forordning (EF) nr. 1315/2007 (EUT L 291 av 9.11.2007, s. 16).

([3]) EUT L 96 av 31.3.2004, s. 1.

Videre menes med:

1. «programvare» dataprogrammer og tilhørende konfigurasjonsdata, herunder standardprogramvare, men ikke elektroniske deler som f.eks. programspesifikke integrerte kretser, programmerbare portmatriser eller faste logiske styringsenheter,

2. «konfigurasjonsdata» data som konfigurerer et generisk programvaresystem til et særlig bruksformål,

3. «standardprogramvare» programvare som ikke er utviklet for den gjeldende kontrakt,

4. «sikkerhetsbekreftelse» alle planlagte og systematiske handlinger som er nødvendige for å skape tilstrekkelig tillit til at et produkt, en tjeneste, en organisasjon eller et funksjonssystem oppnår et sikkerhetsnivå som kan aksepteres eller tolereres,

5. «organisasjon» en yter av lufttrafikktjenester (ATS), en yter av kommunikasjons-, navigerings- og overvåkingstjenester (CNS) eller en enhet for styring av lufttrafikkbevegelser eller styring av luftrommet,

6. «funksjonssystem» en kombinasjon av systemer, framgangsmåter og menneskelige ressurser, organisert for å utføre en funksjon innenfor lufttrafikkstyring,

7. «risiko» kombinasjonen av samlet sannsynlighet for, eller hyppighet av, en skadelig virkning forårsaket av en fare samt virkningens alvorlighetsgrad,

8. «fare» ethvert forhold og enhver hendelse eller omstendighet som kan føre til en ulykke,

9. «ny programvare» programvare som er bestilt eller som det er underskrevet en bindende kontrakt om etter denne forordnings ikrafttredelse,

10. «sikkerhetsmål» en kvalitets- eller kvantitetserklæring som definerer den høyeste hyppighet eller sannsynlighet som en fare kan forventes å inntreffe med,

11. «sikkerhetskrav» et middel for å redusere risikoen fastsatt i tilknytning til sikkerhetsreduksjonsstrategien som gjør det mulig å oppnå et bestemt sikkerhetsmål, herunder krav med hensyn til organisering, drift, framgangsmåter, funksjon, ytelse, samtrafikkevne eller miljøegenskaper,

12. «systemovergang eller bytte under drift» å skifte ut systemkomponenter eller programvare i det europeiske nett for lufttrafikkstyring (EATMN) mens systemet er i drift,

13. «sikkerhetskrav til programvare» en beskrivelse av hva programvaren skal produsere på grunnlag av hva som innmates og begrensningene som foreligger, og der oppfyllelse av kravene sikrer at EATMN-programvaren fungerer sikkert og oppfyller driftsbehovene,

14. «EATMN-programvare» programvare som brukes i EATMN-systemene nevnt i artikkel 1,

15. «validering av krav» en bekreftelse etter undersøkelse og framlegging av objektive bevis på at de særlige kravene til et bestemt bruksformål er oppfylt,

16. «oppnådd på en uavhengig måte» innenfor rammen av verifisering av programvare, at verifikasjonsprosessen utføres av en eller flere andre personer enn den som har utviklet programvaren som er gjenstand for verifisering,

17. «programvarefunksjonssvikt» at et program ikke kan utføre en påkrevd funksjon på en riktig måte,

18. «programvaresvikt» at et program ikke kan utføre en påkrevd funksjon,

19. «COTS» et kommersielt tilgjengelig brukerprogram som selges av forhandlere gjennom offentlig tilgjengelige kataloger, og som normalt ikke skal tilpasses eller forbedres,

20. «programvarekomponenter» moduler som kan bygges inn i eller koples til andre programvaremoduler som kan brukes på nytt, for å kombinere og skape en kundetilpasset brukerprogramvare,

21. «uavhengige programvarekomponenter» programvarekomponenter som ikke settes ut av drift som følge av den funksjonssvikt som forårsaket faren,

22. «programvarens reaksjonstid» den tid som programvaren trenger for å reagere på en viss innmating eller på periodiske hendelser, og/eller programvarens ytelse målt i antall behandlede transaksjoner eller meldinger per tidsenhet,

23. «programvarekapasitet» programvarens evne til å håndtere en gitt datastrøm,

24. «nøyaktighet» den presisjon som kreves for de beregnede resultatene,

25. «programvarens ressursbruk» den mengde ressurser i datasystemet som kan utnyttes av brukerprogramvaren,

26. «programvarestabilitet» programvarens oppførsel ved uventet innmating, maskinvarefeil og strømbrudd, enten i selve datasystemet eller i tilknyttet utstyr,

27. «evne til å tåle overbelastning» systemets oppførsel ved, og særlig dets evne til å tåle, innmating som skjer raskere enn ventet under normal drift av systemet,

28. «riktig og fullstendig verifikasjon av EATMN-programvare» alle sikkerhetskrav til programvare som på en riktig måte angir hva som kreves av programvarekomponenten i samsvar med risikovurderings- og risikoreduksjonsprosessen, og at oppfyllelsen av disse sikkerhetskravene er vist i henhold til det nivå som kreves ifølge sikkerhetsnivået for programvaren,

29. «livssyklusdata for programvare» data som produseres i løpet av programvarens livssyklus for å planlegge, styre, forklare, definere, registrere eller dokumentere virksomhet. Disse dataene muliggjør programvarens livssyklusprosesser, godkjenning av systemet eller utstyret samt endringer av programvareproduktet etter godkjenning,

30. «programvarens livssyklus»

    a) en ordnet samling av prosesser som en organisasjon anser som tilstrekkelig og egnet til å produsere et programvareprodukt,

    b) den tidsperiode som begynner med beslutningen om å produsere eller endre et programvareprodukt, og som avsluttes når produktet tas ut av drift,

31. «sikkerhetskrav til systemet» et sikkerhetskrav som gjelder for et funksjonssystem.

Artikkel 3

Alminnelige sikkerhetskrav

1. Når en organisasjon skal gjennomføre en risikovurderings- og risikoreduksjonsprosess i samsvar med gjeldende fellesskapsregelverk eller nasjonal lovgivning, skal den definere og gjennomføre et system for sikkerhetsbekreftelse av programvare som særlig skal håndtere forhold knyttet til EATMN-programvare, herunder alle driftsmessige programvareendringer foretatt elektronisk, og særlig systemovergang eller bytte under drift.

2. Organisasjonen skal minst sikre at dens system for sikkerhetsbekreftelse av programvare ved hjelp av dokumentasjon og argumenter viser følgende:

a) sikkerhetskravene til programvaren angir på en riktig måte hva som kreves av programvaren for at sikkerhetsmålene og –kravene fastlagt under risikovurderings- og risikoreduksjonsprosessen skal være oppfylt,

b) alle sikkerhetskrav til programvare omfatter sporbarhet,

c) innføringen av programvaren inneholder ingen funksjoner som innvirker negativt på sikkerheten,

d) EATMN-programvaren oppfyller sine krav med en grad av pålitelighet som tilsvarer programvarens kritikalitet,

e) forsikringer gis som bekrefter at de alminnelige sikkerhetskravene fastsatt i bokstav a)-d) er oppfylt, og argumentene til støtte for den påkrevde sikkerhet til enhver tid bygger på

    i) en kjent gjennomførbar versjon av programvaren,

    ii) en kjent samling konfigurasjonsdata,

    iii) en kjent samling av programvareprodukter og -beskrivelser, herunder spesifikasjoner, som er brukt ved produksjonen av den aktuelle versjonen.

3. Organisasjonen skal sørge for at den nasjonale tilsynsmyndighet får tilgang til de forsikringer som kreves for å vise at kravene fastsatt i nr. 2 er oppfylt.

Artikkel 4

Krav til systemet for sikkerhetsbekreftelse av programvare

Organisasjonen skal minst sikre at systemet for sikkerhetsbekreftelse av programvare

1. er dokumentert, særlig som en del av dokumentasjonen av den overordnede risikovurdering og -reduksjon,

2. tildeler programvaresikkerhetsnivåer til all operativ EATMN-programvare i samsvar med kravene fastsatt i vedlegg I,

3. kan godtgjøre at

    a) sikkerhetskravene til programvaren er validert i samsvar med kravene fastsatt i vedlegg II del A,

    b) programvaren er verifisert i samsvar med kravene fastsatt i vedlegg II del B,

c) programvarens konfigurasjonsstyring er i samsvar med kravene fastsatt i vedlegg II del C,

d) sikkerhetskravene til programvaren er sporbare i samsvar med kravene fastsatt i vedlegg II del D,

4. fastsetter hvor strenge krav forsikringene oppfyller; strenghetsgraden skal fastsettes for hvert programvaresikkerhetsnivå, og den skal øke når programvarens kritikalitet øker; for det formål skal

a) variasjonen i strenghetsgrad for hvert programvaresikkerhetsnivå omfatte følgende kriterier:

i) skal oppnås på en uavhengig måte

ii) skal oppnås

iii) behøver ikke oppnås

b) forsikringene for hvert programvaresikkerhetsnivå gi tilstrekkelig tillit til at EATMN-programvare kan benyttes med en akseptabel sikkerhetsrisiko,

5. anvender tilbakemelding fra erfaringer med EATMN-programvare for å bekrefte at systemet for sikkerhetsbekreftelse av programvare og tildelingen av sikkerhetsnivåer er hensiktsmessige. For det formål skal virkningene av programvarefunksjonssvikt eller programvaresvikt som blir meldt i samsvar med relevante krav om melding og vurdering av sikkerhetshendelser, vurderes i forhold til de virkningene som er angitt for det berørte system i klassifiseringen av alvorlighetsgrad gjengitt i avsnitt 3.2.4 i vedlegg II til forordning (EF) nr. 2096/2005.

Artikkel 5

Krav som gjelder endringer av programvare og særskilt programvare

1. For endringer av programvare eller særskilte programvaretyper som COTS, standardprogramvare eller programvare som er brukt tidligere, og som noen av kravene i artikkel 3 nr. 2 bokstav d) eller e) eller i artikkel 4 nr. 2, 3, 4 eller 5 ikke kan anvendes på, skal organisasjonen sørge for at systemet for sikkerhetsbekreftelse av programvare på en annen måte, som velges og godkjennes i samråd med den nasjonale tilsynsmyndighet, gir samme grad av pålitelighet som gjeldende programvaresikkerhetsnivå, når et slikt er fastsatt.

Disse midlene skal skape tilstrekkelig tillit til at programvaren oppfyller sikkerhetsmålene og sikkerhetskravene i samsvar med sikkerhetsvurderings- og risikoreduksjonsprosessen.

2. Ved vurderingen av midlene nevnt i nr. 1 kan den nasjonale tilsynsmyndighet benytte en godkjent organisasjon eller et meldt organ.

Artikkel 6

Endring av forordning (EF) nr. 2096/2005

I vedlegg II til forordning (EF) nr. 2096/2005 skal nytt nr. 3.2.5 avsnitt 5 lyde:

«3.2.5 Avsnitt 5

System for sikkerhetsbekreftelse av programvare

Innenfor rammen av sikkerhetsstyringssystemet skal ytere av lufttrafikktjenester innføre et system for sikkerhetsbekreftelse av programvare i samsvar med kommisjonsforordning (EF) nr. 482/2008 av 30. mai 2008 om opprettelse av et system for sikkerhetsbekreftelse av programvare, som skal gjennomføres av ytere av flysikringstjenester, og om endring av vedlegg II til forordning (EF) nr. 2096/2005(*).

(*) EUT L 141 av 31.5.2008, s. 5.»

Artikkel 7

Ikrafttredelse

Denne forordning trer i kraft den 20. dag etter at den er kunngjort i *Den europeiske unions tidende*.

Den får anvendelse fra 1. januar 2009 på ny programvare for EATMN-systemene nevnt i artikkel 1 nr. 2 første ledd.

Den får anvendelse fra 1. juli 2010 på alle endringer av programvaren for EATMN-systemene nevnt i artikkel 1 nr. 2 første ledd som er i drift på nevnte dato.

Denne forordning er bindende i alle deler og kommer direkte til anvendelse i alle medlemsstater.

Utferdiget i Brussel, 30. mai 2008.

For Kommisjonen

Antonio TAJANI

Medlem av Kommisjonen

VEDLEGG I

Krav som gjelder programvaresikkerhetsnivået nevnt i artikkel 4 nr. 2

1. Ved bestemmelse av programvaresikkerhetsnivået knyttes graden av strenghet for programvaresikkerheten til EATMN-programvarens kritikalitet ved anvendelse av skjemaet for klassifisering av alvorlighetsgrad i nr. 3.2.4 avsnitt 4 i vedlegg II til forordning (EF) nr. 2096/2005 kombinert med sannsynligheten for en viss skadelig virkning. Det skal fastsettes minst fire programvaresikkerhetsnivåer, og nivå 1 skal være det mest kritiske.

2. Et tildelt programvaresikkerhetsnivå skal stå i forhold til den alvorligste virkning som programvarefunksjonssvikt eller programvaresvikt kan forårsake, som nevnt i nr. 3.2.4 avsnitt 4 i vedlegg II til forordning (EF) nr. 2096/2005. Det skal særlig tas hensyn til risikoene knyttet til programvarefunksjonssvikt eller programvaresvikt og arkitektoniske mottiltak og/eller mottiltak knyttet til framgangsmåte.

3. EATMN-programvarekomponenter som det ikke kan påvises er uavhengige av hverandre, skal tildeles det programvaresikkerhetsnivået som gjelder for den mest kritiske av de avhengige komponentene.

VEDLEGG II

Del A: Krav som gjelder validering av sikkerhetskravene til programvare i henhold til artikkel 4 nr. 3 bokstav a)

1. I sikkerhetskravene til programvare skal EATMN-programvarens funksjon ved nominelt og nedsatt funksjonsnivå angis, dvs. reaksjonstid, kapasitet, nøyaktighet, programvarens ressursbruk på målmaskinvaren, stabilitet under unormale driftsforhold og evne til å tåle overbelastning, når dette er relevant.

2. Sikkerhetskravene til programvaren skal være fullstendige og riktige, og være i samsvar med sikkerhetskravene til systemet.

Del B: Krav som gjelder verifisering av programvare i henhold til artikkel 4 nr. 3 bokstav b)

1. EATMN-programvarens funksjon, dvs. reaksjonstid, kapasitet, nøyaktighet, programvarens ressursbruk på målmaskinvaren, stabilitet under unormale driftsforhold og evne til å tåle overbelastning, skal oppfylle kravene til programvaren.

2. EATMN-programvaren skal verifiseres på en hensiktsmessig måte ved analyse og/eller prøving og/eller tilsvarende metoder, etter avtale med den nasjonale tilsynsmyndighet.

3. Verifiseringen av EATMN-programvaren skal gjennomføres på en riktig og fullstendig måte.

Del C: Krav som gjelder konfigurasjonsstyring av programvare i henhold til artikkel 4 nr. 3 bokstav c)

1. Det skal finnes framgangsmåter for identifisering av konfigurasjon, sporbarhet og tilstandsregistrering slik at det kan påvises at programvarens livssyklusdata er under konfigurasjonskontroll i EATMN-programvarens samlede livssyklus.

2. Det skal finnes framgangsmåter for melding og sporing av problemer samt korrigerende tiltak slik at det kan påvises at sikkerhetsproblemer knyttet til programvaren er redusert.

3. Det skal finnes framgangsmåter for gjenfinning og frigivelse av data slik at programvaresyklusdata kan gjenopprettes og leveres i EATMN-programvarens samlede livssyklus.

Del D: Krav som gjelder sporbarheten for sikkerhetskravene til programvare i henhold til artikkel 4 nr. 3 bokstav d)

1. Hvert sikkerhetskrav til programvare skal spores tilbake til det designnivå det skal tilfredsstille.

2. Hvert sikkerhetskrav til programvare på hvert designnivå det skal tilfredsstille, skal føres tilbake til et sikkerhetskrav til systemet.