VERORDNUNG (EG) Nr. 482/2008 DER KOMMISSION

vom 30. Mai 2008

über die Einrichtung eines Systems zur Gewährleistung der Software-Sicherheit durch Flugsicherungsorganisationen und zur Änderung von Anhang II der Verordnung (EG) Nr. 2096/2005

(Text von Bedeutung für den EWR)

DIE KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN —

gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft,

gestützt auf die Verordnung (EG) Nr. 550/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 über die Erbringung von Flugsicherungsdiensten im einheitlichen europäischen Luftraum („Flugsicherungsdienste-Verordnung") [1], insbesondere auf Artikel 4,

in Erwägung nachstehender Gründe:

(1) Gemäß der Verordnung (EG) Nr. 550/2004 bestimmt und billigt die Kommission die relevanten Bestimmungen der Eurocontrol-Anforderungen im Bereich der Sicherheitsregelung (Eurocontrol Safety Regulatory Requirements, ESARR) und berücksichtigt dabei die bestehenden Gemeinschaftsvorschriften. Die ESARR 6 „Software in Flugverkehrsmanagementsystemen" enthalten ein Paket von Sicherheitsanforderungen für die Einführung eines Systems zur Gewährleistung der Software-Sicherheit.

(2) Im letzten Satz von Erwägungsgrund 12 der Verordnung (EG) Nr. 2096/2005 der Kommission vom 20. Dezember 2005 zur Festlegung gemeinsamer Anforderungen bezüglich der Erbringung von Flugsicherungsdiensten [2] heißt es, dass „die einschlägigen Bestimmungen der ESARR 1 zur Sicherheitsaufsicht im Flugverkehrsmanagement und der ESARR 6 zur Software in Flugverkehrsmanagementsystemen benannt und durch getrennte Rechtsakte der Gemeinschaft angenommen werden [sollten]."

(3) Gemäß Anhang II der Verordnung (EG) Nr. 2096/2005 müssen Erbringer von Flugverkehrsdiensten ein Sicherheitsmanagementsystem einrichten sowie eine Risikobewertung und -minderung im Hinblick auf Änderungen vornehmen. Im Rahmen ihres Sicherheitsmanagements und als Teil ihrer Risikobewertung und -minderung im Hinblick auf Änderungen sollten die Erbringer von Flugverkehrsdiensten ein System zur Gewährleistung der Software-Sicherheit definieren und einrichten, das der gezielten Behandlung von Software-Aspekten dient.

(4) Im Bereich der Software-Sicherheit funktionaler Systeme soll vorrangig das Ziel erreicht werden, die mit der Verwendung der in den europäischen Flugverkehrsmanagementnetzsystemen enthaltenen Software („EATMN-Software") verbundenen Risiken auf ein tolerierbares Niveau zu senken.

(5) Diese Verordnung sollte nicht für den militärischen Einsatz- und Ausbildungsbetrieb im Sinne von Artikel 1 Absatz 2 der Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Festlegung des Rahmens für die Schaffung eines einheitlichen europäischen Luftraums (Rahmenverordnung) [3] gelten.

(6) Anhang II der Verordnung (EG) Nr. 2096/2005 sollte dementsprechend geändert werden.

(7) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des Ausschusses für den einheitlichen Luftraum —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Gegenstand und Anwendungsbereich

(1) Mit dieser Verordnung werden Anforderungen festgelegt für die Definition und Einführung eines Systems zur Gewährleistung der Software-Sicherheit durch Flugsicherungsdienste (Air Traffic Services, ATS), durch Einrichtungen, die für die Flugverkehrsflussregelung (Air Traffic Flow Management, ATFM) und das Luftraummanagement (Air Space Management, ASM) für den allgemeinen Flugverkehr zuständig sind, sowie durch Kommunikations-, Navigations- und Überwachungsdienste (Communication, Navigation and Surveillance Services, CNS).

Durch die Verordnung werden die Vorschriften der EUROCONTROL-Anforderungen im Bereich der Sicherheitsregelung — ESARR 6 über Software in Flugverkehrsmanagementsystemen vom 6. November 2003 bestimmt und gebilligt.

(2) Die Verordnung gilt für neue Software und jede Software-Änderung in ATS-, ASM-, ATFM- und CNS-Systemen.

Sie gilt nicht für die Software bordgestützter Komponenten und weltraumgestützter Ausrüstungen.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung gelten die Begriffsbestimmungen von Artikel 2 der Verordnung (EG) Nr. 549/2004.

[1] ABl. L 96 vom 31.3.2004, S. 10.
[2] ABl. L 335 vom 21.12.2005, S. 13. Verordnung geändert durch die Verordnung (EG) Nr. 1315/2007 (ABl. L 291 vom 9.11.2007, S. 16).
[3] ABl. L 96 vom 31.3.2004, S. 1.

Ferner gelten folgende Begriffsbestimmungen:

1. „Software“ sind Computerprogramme und dazugehörige Konfigurationsdaten, einschließlich Standardsoftware, jedoch mit Ausnahme elektronischer Bausteine wie anwendungsspezifische integrierte Schaltungen, speicherprogrammierbare Steuerungen und festen Logikkontrolleinheiten;

2. „Konfigurationsdaten“ sind Daten, durch die ein generisches Softwaresystem für einen bestimmten Verwendungszweck konfiguriert wird;

3. „Standardsoftware“ ist Software, die nicht speziell für einen Vertrag entwickelt wurde;

4. „Gewährleistung der Sicherheit“ sind alle geplanten und systematischen Aktionen, die notwendig sind, um ein angemessenes Vertrauen zu erzeugen, dass ein Produkt, ein Dienst, eine Organisation oder ein funktionales System einem akzeptablen oder tolerierbaren Niveau an Sicherheit genügt;

5. „Organisation“ ist eine Flugsicherungsorganisation oder eine Stelle, die CNS-, ATFM- oder ASM-Aufgaben erfüllt;

6. „funktionales System“ ist eine Kombination von Systemen, Verfahren und Personal mit dem Ziel, eine Funktion im Bereich des Flugverkehrsmanagements zu erfüllen;

7. „Risiko“ ist die Kombination der Gesamtwahrscheinlichkeit oder Häufigkeit des Vorkommens einer schädlichen Auswirkung, die von einer Gefahr verursacht wird, und der Schwere dieser Auswirkung;

8. „Gefahr“ ist jede Bedingung, jeder Vorfall oder Umstand, die oder der einen Unfall verursachen könnte;

9. „neue Software“ ist eine Software, die bestellt wurde oder für die nach dem Inkrafttreten dieser Verordnung entsprechende verbindliche Verträge geschlossen wurden;

10. „Sicherheitsziel“ ist eine qualitative oder quantitative Aussage, die die maximale Häufigkeit oder Wahrscheinlichkeit eines erwarteten Gefahreneintritts angibt;

11. „Sicherheitsanforderung“ ist eine aus der Risikominderungsstrategie abgeleitete Maßnahme zur Risikominderung, die ein bestimmtes Sicherheitsziel erreicht und organisatorische, operative, prozedurale, funktionale, Leistungs- und Interoperabilitätsanforderungen sowie Umweltcharakteristika beinhaltet;

12. „Umschaltung oder Hot Swap“ ist eine Technik, bei der Komponenten oder Software von Flugverkehrsmanagementnetz(EATMN)-systemen während des Betriebs ausgetauscht werden;

13. „Software-Sicherheitsanforderung“ ist eine Beschreibung der von der Software aufgrund bestimmter Eingaben und Bedingungen zu erbringenden Leistungen, durch die gewährleistet wird, dass die EATMN-Software sicher und entsprechend den Betriebsanforderungen funktioniert;

14. „EATMN-Software“ ist die in den europäischen EATMN-Systemen gemäß Artikel 1 verwendete Software;

15. „Anforderungsvalidierung“ ist die durch Prüfung und objektive Nachweise erbrachte Bestätigung, dass die mit einem bestimmten Verwendungszweck verknüpften Anforderungen erfüllt sind;

16. „unabhängig erbracht“ bedeutet im Rahmen der Software-Verifizierung, dass die Verifizierung von einer anderen Person als dem Entwickler des Gegenstands der Verifizierung durchgeführt wird;

17. „Software-Störung“ ist das Unvermögen eines Programms, eine geforderte Funktion korrekt auszuführen;

18. „Software-Ausfall“ ist das Unvermögen eines Programms, eine geforderte Funktion auszuführen;

19. „COTS-Anwendungen“ (Commercial Off-The-Shelf) sind kommerziell verfügbare Anwendungen, die über öffentliche Kataloge vertrieben werden und nicht zur kundenspezifischen Anpassung oder Aufrüstung konzipiert sind;

20. „Software-Komponenten“ sind Bausteine, die installiert oder zum Aufbau kundenspezifischer Anwendungen mit anderen, wieder verwendbaren Software-Bausteinen zusammengefügt werden können;

21. „unabhängige Software-Komponenten“ sind Software-Komponenten, die durch die Störung, durch die die Gefahr verursacht wird, nicht außer Betrieb gesetzt werden;

22. „Software-Reaktionszeit“ ist die Zeit, in der die Software auf bestimmte Eingaben oder regelmäßige Ereignisse reagieren muss, und/oder die Leistungsfähigkeit der Software, gemessen in verarbeiteten Transaktionen oder Meldungen je Zeiteinheit;

23. „Software-Kapazität“ ist die Fähigkeit der Software, einen bestimmten Datenfluss zu verarbeiten;

24. „Genauigkeit“ ist die geforderte Exaktheit der berechneten Ergebnisse;

25. „Ressourcennutzung“ ist die Menge an Ressourcen innerhalb des Computersystems, die von der Anwendungssoftware genutzt werden kann;

26. „Software-Stabilität“ ist das Verhalten der Software bei unvorhergesehenen Eingaben, Hardware-Fehlern und Unterbrechungen der Stromversorgung, entweder im Computersystem selbst oder in angeschlossenen Geräten;

27. „Überlasttoleranz“ ist das Verhalten des Systems und insbesondere seine Toleranz gegenüber Eingaberaten, die die bei normalem Systembetrieb zu erwartende Datenmenge übersteigen;

28. „korrekte und vollständige Verifizierung der EATMN-Software“ bedeutet, dass alle Software-Sicherheitsanforderungen die an die Software-Komponente im Rahmen der Risikobewertung und -minderung gestellten Ansprüche korrekt darstellen und dass die Erfüllung dieser Sicherheitsanforderungen nach Maßgabe der geforderten Software-Sicherheitsanforderungsstufe nachgewiesen wird;

29. „Lebenszyklusdaten“ sind die während des Software-Lebenszyklus produzierten Daten, die der Planung, Steuerung, Erklärung, Definition, Aufzeichnung oder dem Nachweis von Vorgängen dienen; diese Daten ermöglichen die Freigabe der Software-Lebenszyklusprozesse, des Systems oder der Ausrüstung sowie anschließender Software-Änderungen;

30. „Software-Lebenszyklus“ ist

    a) eine Anordnung von Prozessen, die von einer Organisation für ausreichend und angemessen im Hinblick auf die Herstellung eines Software-Produkts erachtet wird;

    b) die Zeitspanne, die mit der Entscheidung über die Herstellung oder Änderung eines Software-Produkts beginnt und mit der Außerdienststellung des Produkts endet;

31. „Systemsicherheitsanforderung“ ist eine für ein funktionales System geltende Sicherheitsanforderung.

Artikel 3

Allgemeine Sicherheitsanforderungen

(1) Müssen Organisationen nach geltendem Gemeinschaftsrecht oder nationalem Recht ein Risikobewertungs- und -minderungsverfahren einrichten, so definieren und implementieren sie ein System zur Gewährleistung der Software-Sicherheit, das der gezielten Behandlung von Aspekten der EATMN-Software dient, einschließlich online durchgeführter Software-Änderungen, beispielsweise durch Umschaltung oder Hot Swap.

(2) Die Organisation sorgt dafür, dass sich mit ihrem System zur Gewährleistung der Software-Sicherheit anhand von Nachweisen und Argumenten mindestens Folgendes belegen lässt:

a) Die Software-Sicherheitsanforderungen stellen die von der Software zu erfüllenden Bedingungen, um den im Rahmen der Risikobewertung und -minderung beschriebenen Sicherheitszielen und -anforderungen zu entsprechen, korrekt dar.

b) Die Rückverfolgbarkeit sämtlicher Software-Sicherheitsanforderungen ist gewährleistet.

c) Die Einführung der Systems beinhaltet keine Funktion, die die Sicherheit beeinträchtigt.

d) Die EATMN-Software erfüllt die an sie gestellten Anforderungen mit einem Grad an Zuverlässigkeit, der der Kritikalität der Software entspricht.

e) Es bestehen Garantien, die die Erfüllung der allgemeinen in Buchstaben a bis d aufgeführten Sicherheitsanforderungen bestätigen und die Argumente für den Nachweis der geforderten Garantien lassen sich jederzeit durch Folgendes belegen:

    i) eine bekannte ausführbare Version der Software,

    ii) eine bekannte Menge an Konfigurationsdaten und

    iii) eine bekannte Palette an Software-Produkten und -Beschreibungen, einschließlich Spezifikationen, die bei der Herstellung der betreffenden Version verwendet wurden.

(3) Die Organisation stellt der nationalen Aufsichtsbehörde die notwendigen Garantien zur Verfügung, die die Erfüllung der Anforderungen gemäß Absatz 2 belegen.

Artikel 4

Anforderungen an das System zur Gewährleistung der Software-Sicherheit

Die Organisation sorgt dafür, dass das System zur Gewährleistung der Software-Sicherheit mindestens folgende Kriterien erfüllt:

1. Das System ist dokumentiert, insbesondere im Rahmen der Gesamtdokumentation zur Risikobewertung und -minderung.

2. Jeder operationellen EATMN-Software wird nach Maßgabe der Anforderungen in Anhang I eine Sicherheitsanforderungsstufe zugewiesen.

3. Das System umfasst Garantien für Folgendes:

    a) Validierung der Software-Sicherheitsanforderungen gemäß den Anforderungen in Anhang II Teil A,

    b) Software-Verifizierung gemäß den Anforderungen in Anhang II Teil B,

c) Software-Konfigurationsmanagement gemäß den Anforderungen in Anhang II Teil C,

d) Rückverfolgbarkeit der Software-Sicherheitsanforderungen gemäß den Anforderungen in Anhang II Teil D.

4. In dem System wird das mit den Garantien verknüpfte Anspruchsniveau festgelegt. Die Ansprüche werden für jede Software-Sicherheitsanforderungsstufe bestimmt und steigen mit zunehmender Software-Kritikalität. Zu diesem Zweck

a) müssen die mit den Software-Sicherheitsanforderungsstufen verbundenen Garantien nach folgenden Kriterien gestaffelt sein:

i) unabhängig zu erbringen,

ii) zu erbringen,

iii) nicht vorgeschrieben;

b) müssen die mit den einzelnen Software-Sicherheitsanforderungsstufen verbundenen Garantien hinreichende Gewähr bieten, dass die EATMN-Software mit einem akzeptablen Maß an Sicherheit betrieben werden kann.

5. Zur Bestätigung, dass das System zur Gewährleistung der Software-Sicherheit und die zugewiesenen Sicherheitsanforderungsstufen angemessen sind, wird auf frühere Erfahrungen mit EATMN-Software zurückgegriffen. Zu diesem Zweck werden die Auswirkungen von Software-Störungen oder -Ausfällen, die aufgrund der einschlägigen Bestimmungen zur Meldung und Bewertung von Sicherheitsvorfällen gemeldet werden, im Verhältnis zu den für das betreffende System ermittelten Auswirkungen bewertet, deren Schwere anhand des Klassifikationssystems in Anhang II Nummer 3.2.4 der Verordnung (EG) Nr. 2096/2005 eingestuft wird.

Artikel 5

Anforderungen an Änderungen von Software und Spezial-Software

(1) Bei Änderungen von Software oder von Spezial-Software wie COTS-Anwendungen, Standardsoftware oder bereits früher genutzter Software, auf die einige der Anforderungen von Artikel 3 Absatz 2 Buchstabe d oder e oder von Artikel 4 Nummer 2, 3, 4 oder 5 nicht angewandt werden können, sorgt die Organisation dafür, dass das System zur Gewährleistung der Software-Sicherheit mit anderen Mitteln, die im Einvernehmen mit der nationalen Aufsichtsbehörde ausgewählt werden, denselben Grad an Zuverlässigkeit bietet wie die für eine vergleichbare Software festgelegte Sicherheitsanforderungsstufe.

Diese Mittel bieten eine hinreichende Gewähr, dass die Software mit den Sicherheitszielen und -anforderungen im Einklang steht, die im Rahmen der Risikobewertung und -minderung ermittelt wurden.

(2) Die nationale Aufsichtsbehörde kann eine anerkannte Organisation oder eine benannte Stelle mit der Bewertung der in Absatz 1 genannten Mittel beauftragen.

Artikel 6

Änderung der Verordnung (EG) Nr. 2096/2005

In Anhang II der Verordnung (EG) Nr. 2096/2005 wird folgender Abschnitt angefügt:

„3.2.5. Abschnitt 5

System zur Gewährleistung der Software-Sicherheit

Im Rahmen des Sicherheitsmanagements richten die Flugsicherungsorganisationen ein System zur Gewährleistung der Software-Sicherheit gemäß der Verordnung (EG) Nr. 482/2008 vom 30. Mai 2008 über die Einrichtung eines Systems zur Gewährleistung der Software-Sicherheit durch Flugsicherungsorganisationen und zur Änderung von Anhang II der Verordnung (EG) Nr. 2096/2005 (*) ein.

(*) ABl. L 141 vom 31.5.2008, S. 5."

Artikel 7

Inkrafttreten

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Sie gilt ab dem 1. Januar 2009 für neue Software in den in Artikel 1 Absatz 2 Unterabsatz 1 genannten EATMN-Systemen.

Sie gilt ab dem 1. Juli 2010 für alle Software-Änderungen in den in Artikel 1 Absatz 2 Unterabsatz 1 genannten EATMN-Systemen, die zu diesem Zeitpunkt in Betrieb sind.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 30. Mai 2008

Für die Kommission
Antonio TAJANI
Mitglied der Kommission

ANHANG I

Anforderungen an die Software-Sicherheitsanforderungsstufen gemäß Artikel 4 Absatz 2

1. Bei der Bestimmung der Software-Sicherheitsanforderungsstufen werden die mit den Garantien verknüpften Anspruchsniveaus und die Kritikalität der EATMN-Software in Beziehung zueinander gesetzt, wobei das System für die Klassifizierung des Schweregrads in Anhang II Nummer 3.2.4 Abschnitt 4 der Verordnung (EG) Nr. 2096/2005 und die Wahrscheinlichkeit einer bestimmten schädlichen Auswirkung zugrunde gelegt werden. Zu bestimmen sind mindestens vier Software-Sicherheitsanforderungsstufen, wobei die Software-Sicherheitsanforderungsstufe 1 am anspruchsvollsten ist.

2. Die zugewiesenen Software-Sicherheitsanforderungsstufen entsprechen der jeweils schwersten Auswirkung, die durch Software-Störungen oder -Ausfälle verursacht werden kann, wobei Anhang II Nummer 3.2.4 Abschnitt 4 der Verordnung (EG) Nr. 2096/2005 zugrunde gelegt wird. Berücksichtigt werden insbesondere die aus Software-Störungen und -Ausfällen erwachsenden Risiken sowie die dazu bestehenden architektur- und/oder verfahrensbezogenen Schutzmaßnahmen.

3. Den EATMN-Software-Komponenten, deren Unabhängigkeit voneinander nicht nachgewiesen werden kann, wird die Software-Sicherheitsanforderungsstufe der abhängigen Komponente mit dem höchsten Sicherheitsanspruch zugewiesen.

ANHANG II

Teil A: Anforderungen an die Validierung der Software-Sicherheitsanforderungen gemäß Artikel 4 Absatz 3 Buchstabe a

1. In den Software-Sicherheitsanforderungen ist das funktionale Verhalten der EATMN-Software bei normalem und bei gestörtem Betrieb zu spezifizieren, d. h. je nach Bedarf Reaktionszeit, Kapazität, Genauigkeit, Ressourcennutzung in der Ziel-Hardware, Stabilität bei anormalen Betriebsbedingungen und Überlasttoleranz.

2. Die Software-Sicherheitsanforderungen müssen vollständig und korrekt sein und mit den Systemsicherheitsanforderungen im Einklang stehen.

Teil B: Anforderungen an die Software-Verifizierung gemäß Artikel 4 Absatz 3 Buchstabe b

1. Das funktionale Verhalten der EATMN-Software sowie deren Reaktionszeit, Kapazität, Genauigkeit, Ressourcennutzung in der Ziel-Hardware, Stabilität bei anormalen Betriebsbedingungen und Überlasttoleranz haben den Software-Sicherheitsanforderungen zu entsprechen.

2. Die EATMN-Software ist entsprechend den mit der nationalen Aufsichtsbehörde getroffenen Vereinbarungen durch Analyse und/oder Erprobung und/oder andere gleichwertige Mittel angemessen zu verifizieren.

3. Die Verifizierung der EATMN-Software ist ordnungsgemäß und vollständig durchzuführen.

Teil C: Anforderungen an das Software-Konfigurationsmanagement gemäß Artikel 4 Absatz 3 Buchstabe c

1. Es müssen Verfahren zur Konfigurationsidentifizierung, -rückverfolgung und -buchführung bestehen, die belegen, dass während des gesamten Lebenszyklus der EATMN-Software die entsprechenden Lebenszyklusdaten einer Konfigurationsüberwachung unterstehen.

2. Es müssen Verfahren für die Meldung und Rückverfolgung von Problemen sowie für entsprechende Abhilfemaßnahmen bestehen, die belegen, dass mit der Software zusammenhängende Sicherheitsprobleme gemindert werden.

3. Es müssen Verfahren zur Wiederherstellung und Freigabe von Daten bestehen, so dass während des gesamten Lebenszyklus der EATMN-Software die entsprechenden Lebenszyklusdaten reproduziert und bereitgestellt werden können.

Teil D: Anforderungen an die Rückverfolgbarkeit der Software-Sicherheitsanforderungen gemäß Artikel 4 Absatz 3 Buchstabe d

1. Jede Software-Sicherheitsanforderung muss sich auf die Entwurfsebene, auf der ihre Erfüllung nachgewiesen wird, zurückverfolgen lassen.

2. Jede Software-Sicherheitsanforderung muss sich auf jeder Entwurfsebene, auf der ihre Erfüllung nachgewiesen wird, auf eine Systemsicherheitsanforderung zurückverfolgen lassen.