

Ez a dokumentum kizárólag tájékoztató jellegű, az intézmények semmiféle felelősséget nem vállalnak a tartalmáért

► **B**

A BIZOTTSÁG 482/2008/EK RENDELETE

(2008. május 30.)

a léginavigációs szolgáltatók által kialakítandó, szoftverbiztonságot garantáló rendszer létrehozásáról és a 2096/2005/EK rendelet módosításáról

(EGT-vonatkozású szöveg)

(HL L 141., 2008.5.31., 5. o.)

Módosította:

Hivatalos Lap

	Szám	Oldal	Dátum
► M1 A Bizottság 1035/2011/EU végrehajtási rendelete (2011. október 17.)	L 271	23	2011.10.18.

**A BIZOTTSÁG 482/2008/EK RENDELETE****(2008. május 30.)****a léginavigációs szolgáltatók által kialakítandó, szoftverbiztonságot garantáló rendszer létrehozásáról és a 2096/2005/EK rendelet módosításáról****(EGT-vonatkozású szöveg)**

AZ EURÓPAI KÖZÖSSÉGEK BIZOTTSÁGA,

tekintettel az Európai Közösséget létrehozó szerződésre,

tekintettel a léginavigációs szolgáltatóknak az egységes európai égbolt keretében történő ellátásáról szóló, 2004. március 10-i 550/2004/EK európai parlamenti és tanácsi rendeletre („léginavigációs szolgálati rendelet”)⁽¹⁾ és különösen annak 4. cikkére,

mivel:

- (1) Az 550/2004/EK rendelet szerint a Bizottság – figyelembe véve a már létező közösségi jogszabályokat – meghatározza és elfogadja az Eurocontrol biztonsági szabályozó követelmények (ESARR-ok) vonatkozó intézkedéseit. Az „ATM-rendszerek szoftvere” elnevezésű ESARR 6 biztonsági szabályozási követelménycsomagot fogalmaz meg a szoftverbiztonságot garantáló rendszer megvalósításához.
- (2) A léginavigációs szolgáltatók ellátására vonatkozó közös követelmények megállapításáról szóló, 2005. december 20-i 2096/2005/EK bizottsági rendelet⁽²⁾ (12) preambulumbekzdésének utolsó mondata rögzíti, hogy „az ESARR 1 ATM-mel kapcsolatos repülésbiztonsági felügyeletről szóló, illetve az ESARR 6 ATM-rendszerek szoftveréről szóló vonatkozó rendelkezéseit azonosítani kell, és külön közösségi jogszabállyal kell elfogadni.”
- (3) A 2096/2005/EK rendelet II. melléklete előírja a légiforgalmi szolgáltatók számára a repülésbiztonság-irányítási rendszernek, valamint a változásokból eredő kockázatok értékelésére és csökkentésére vonatkozó repülésbiztonsági követelményeknek a végrehajtását. A légiforgalmi szolgáltatóknak e repülésbiztonság-irányítási rendszer keretében, a változásokból eredő kockázatok értékelésének és csökkentésének részeként olyan, a szoftverbiztonságot garantáló rendszert kell meghatározniuk és megvalósítaniuk, amely kifejezetten a szoftverekkel kapcsolatos kérdések kezelésére szolgál.
- (4) A szoftvert magukban foglaló funkcionális rendszerek esetében a legfőbb szoftverbiztonsági célkitűzés, hogy az európai légiforgalmi szolgáltatás hálózati rendszereiben alkalmazott szoftverek („EATMN-szoftverek”) használatával járó kockázat a még megfelelő szintre csökkenjen.

⁽¹⁾ HL L 96., 2004.3.31., 10. o.

⁽²⁾ HL L 335., 2005.12.21., 13. o. Az 1315/2007 rendelettel (HL L 291., 2007.11.9., 16. o.) módosított rendelet.

▼B

- (5) Indokolt, hogy e rendelet hatálya ne terjedjen ki az egységes európai égbolt létrehozására vonatkozó keret megállapításáról szóló, 2004. március 10-i 549/2004/EK európai parlamenti és tanácsi rendelet⁽¹⁾ (keretrendelet) 1. cikkének (2) bekezdésében említett katonai műveletekre és kiképzésre.
- (6) Ezért a 2096/2005/EK rendelet II. mellékletét megfelelően módosítani kell.
- (7) Az e rendeletben előírt intézkedések összhangban vannak az egységes égbolttal foglalkozó bizottság véleményével,

ELFOGADTA EZT A RENDELETET:

1. cikk

Tárgy és hatály

(1) Ez a rendelet meghatározza a szoftverbiztonságot garantáló rendszerek a légiforgalmi (ATS) szolgáltatók, a légiforgalmi áramlásszervező (ATFM) és légtér-gazdálkodási (ASM) egységek, valamint a kommunikációs, navigációs és légtérelőirányító (CNS) szolgáltatók általi meghatározására és megvalósítására vonatkozó követelményeket.

Ez a rendelet meghatározza és elfogadja a 2003. november 6-án kiadott, az „ATM-rendszerek szoftverei” elnevezésű – ESARR 6 – Eurocontrol biztonsági szabályozási követelmények kötelező előírásait.

(2) Ez a rendelet az ATS-, ASM-, ATFM- és CNS-rendszerek új szoftvereire és e rendszerek minden szoftvermódosítására alkalmazandó.

Ez a rendelet nem vonatkozik sem a fedélzeti eszközök, sem a világűrbe telepített berendezések szoftvereire.

2. cikk

Fogalommeghatározások

E rendelet alkalmazásában az 549/2004/EK rendeletben 2. cikkében megállapított fogalommeghatározások alkalmazandók.

Ezenkívül még a következő fogalommeghatározások alkalmazandók:

1. „szoftver”: számítógépes programok és kapcsolódó konfigurációs adatok, beleértve a nem külön fejlesztésű szoftvereket, de kizárva az elektronikus összetevőket, különösen az alkalmazáspecifikus integrált áramköröket, a programozható kaputömböket vagy a szilárdtest jelfogókat;
2. „konfigurációs adatok”: olyan adatok, amelyek segítségével egy általános szoftverrendszert az adott feladatra konfigurálnak;

⁽¹⁾ HL L 96., 2004.3.31., 1. o.

▼ B

3. „nem külön fejlesztésű szoftver”: olyan szoftver, amelyet nem az adott szerződés céljára fejlesztettek ki;
4. „a biztonság garantálása”: azon tervszerű és módszeres intézkedések összessége, amelyek ahhoz szükségesek, hogy valamely termék, szolgáltatás, szervezet vagy funkcionális rendszer elfogadható vagy még megfelelően biztonságos szintje kellően szavatolható legyen;
5. „szervezet”: ATS- vagy CNS-szolgáltató, illetve ATFM- vagy ASM-szolgáltatást nyújtó egység;
6. „funkcionális rendszer”: az ATM kontextusában valamely funkció végrehajtását szolgáló rendszerek, eljárások és emberi erőforrások kombinációja;
7. „kockázat”: a veszélyből eredő káros hatás általános valószínűségének vagy bekövetkezési gyakoriságának és a hatás súlyosságának kombinációja;
8. „veszély”: bármely olyan körülmény vagy esemény, amely balesetet idézhet elő;
9. „új szoftver”: olyan szoftver, amelyet e rendelet hatálybalépése után rendeltek meg, vagy amelyről e rendelet hatálybalépése után írtak alá szerződést;
10. „biztonsági célkitűzés”: a veszély bekövetkezéének várható legnagyobb gyakoriságát vagy valószínűségét meghatározó minőségi vagy mennyiségi nyilatkozat;
11. „biztonsági követelmény”: a kockázatkezelési stratégia alapján meghatározott kockázatcsökkentési eszköz, amely megvalósítja az adott biztonsági célkitűzést, beleértve a szervezeti, eljárásbeli, funkcionális, teljesítménybeli és interoperabilitási követelményeket, illetőleg a környezeti jellemzőket is;
12. „rendszerátállítás vagy forrócsere”: az európai légiforgalmi szolgáltatási hálózat (EATMN) rendszerösszetevőinek vagy szoftverének működés közben történő cseréje;
13. „szoftverbiztonsági követelmény”: annak leírása, amit a szoftvernek tennie kell – tekintettel a bemenő adatokra és a megszorításokra –, aminek teljesülése szavatolja, hogy az EATMN-szoftver biztonságosan és az üzemeltetési célnak megfelelően működik;
14. „EATMN-szoftver”: az 1. cikk (2) és (3) bekezdésében említett EATMN rendszerekben használt szoftver;
15. „a követelmények érvényessége”: annak vizsgálatával és objektív bizonyítékok szolgáltatásával való megerősítése, hogy az adott felhasználásra vonatkozó követelmények megfelelnek-e az előírt követelményeknek;
16. „független megvalósítású”: a szoftver-ellenőrzési eljárás akkor ilyen, ha az ellenőrzési eljárás feladatait más látja el, mint az ellenőrzés tárgyának fejlesztője;

▼ B

17. „szoftver téves működése”: a programnak valamely megkövetelt funkció helyes elvégzésére való képtelensége;
18. „szoftverhiba”: a programnak valamely megkövetelt funkció elvégzésére való képtelensége;
19. „COTS”: kereskedelmi forgalomban kapható, nyilvános katalógusokból kereskedőktől beszerezhető alkalmazások, amelyeket nem szántak testreszabásra vagy továbbfejlesztésre;
20. „szoftverösszetevő”: testre szabott szoftveralkalmazás létrehozása céljából beillesztés vagy összekapcsolás útján más, újrahasználható szoftverelemekkel kombinálható alkotóelem;
21. „független szoftverösszetevők”: olyan szoftverösszetevők, amelyek nem válnak működésképtelenné veszélyt okozó meghibásodási állapot hatására;
22. „a szoftver válaszideje”: az időkeret, amelyen belül a szoftvernek válaszolnia kell egy adott bevitelre vagy rendszeresen bekövetkező eseményre és/vagy a szoftvernek az egységidő alatt kezelt műveletek vagy üzenetek számában kifejezett teljesítménye;
23. „a szoftver kapacitása”: a szoftver képessége egy adott adatmennyiség kezelésére;
24. „pontosság”: a kiszámított értékek megkívánt pontossága;
25. „a szoftver erőforrás-felhasználása”: a számítástechnikai rendszeren belüli azon erőforrás-mennyiség, amelyet az alkalmazás felhasználhat;
26. „a szoftver zavartűrése”: a szoftver viselkedése váratlan bevitel, hardverhiba és a számítástechnikai rendszerben vagy a kapcsolódó eszközökben fellépő tápellátás kimaradása esetén;
27. „túlterhelhetőség”: a rendszer viselkedése – és különösen tűrőképessége – a rendszer megszokott működése során a vártnál nagyobb ütemben jelentkező bevételek esetén;
28. „pontos és teljes EATMN-szoftverellenőrzés”: mindazon szoftverbiztonsági követelmény, amely pontosan előírja, hogy a kockázatelemző és -csökkentő eljárás mit vár el az adott szoftverösszetevőtől, és ennek megvalósítása bizonyítottan a szoftverbiztonságot garantáló rendszer által megkövetelt szinten történik;
29. „a szoftver életciklusadatai”: a szoftver életciklusa során a szoftver tevékenységeinek tervezése, irányítása, magyarázata, meghatározása, nyilvántartása és bizonyítása céljából összegyűjtött adatok; ezek az adatok lehetővé teszik a szoftver életciklusa folyamatának, a rendszernek vagy a berendezésnek a jóváhagyását, valamint a szoftvertermék jóváhagyás utáni módosítását.

▼B

30. „a szoftver életciklusa”:
- a) valamely szervezet által meghatározott eljárások rendszerezett halmaza, amely elégséges és alkalmas arra, hogy egy szoftverterméket hozzanak létre;
 - b) azon időtartam, amely akkor kezdődik, amikor eldöntik, hogy létre kell hozni vagy módosítani kell egy szoftvert, és amely akkor ér véget, amikor a szoftvert kivonják a használatból;
31. „rendszerbiztonsági követelmény”: egy funkcionális rendszerrel szembeni biztonsági követelmény.

*3. cikk***Általános biztonsági követelmények**

- (1) Valahányszor egy szervezet a hatályos közösségi vagy nemzeti joggal összhangban kockázatelemző és -csökkentő eljárást köteles bevezetni, szoftverbiztonságot garantáló rendszert kell meghatároznia és megvalósítania a kifejezetten az EATMN-szoftverekkel kapcsolatos kérdések kezelésére, beleértve a szoftverek összes működés közbeni változtatását is, különösen a rendszerátállást vagy a forrócserét.
- (2) A szervezetnek biztosítania kell, hogy szoftverbiztonsági rendszere bizonyítékokkal és érvekkel igazolja legalább a következőket:
- a) a szoftverbiztonsági követelmények pontosan meghatározzák, hogy a kockázatelemző és -csökkentő eljárásban megállapított biztonsági célkitűzések és követelmények eléréséhez milyen elvárásokat kell teljesítenie a szoftvernek;
 - b) minden szoftverbiztonsági követelmény tekintetében meg van oldva a nyomon követhetőség;
 - c) a szoftver megvalósítása nem tartalmaz olyan funkciót, amely a biztonságot hátrányosan befolyásolja;
 - d) az EATMN-szoftver olyan megbízhatósági szinten teljesíti a vele szemben támasztott követelményeket, amely arányban áll a szoftver által betöltött szerep kritikusságával;
 - e) biztosítékokat adnak, amelyek megerősítik, hogy az a)–d) pontban említett általános biztonsági követelmények teljesülnek, és a megkívánt biztosítékokat igazoló érvek mindig az alábbiakból származnak:
 - i. a szoftver ismert, lefuttatható változata;
 - ii. ismert konfigurációs adathalmaz;
 - iii. ismert szoftvertermékek és -leírások, beleértve az adott verzió kifejlesztéséhez használt specifikációkat is.
- (3) A szervezetnek a nemzeti felügyeleti hatóság rendelkezésére bocsátják a megkívánt biztosítékokat, annak alátámasztására, hogy a (2) bekezdésben rögzített követelmények teljesülnek.

▼B

4. cikk

A szoftverbiztonságot garantáló rendszerre vonatkozó követelmények

A szervezet biztosítja, hogy a szoftverbiztonságot garantáló rendszer legalább:

1. dokumentálva van, különösen az átfogó kockázatelemző és -csökkentő rendszer dokumentációján belül;
2. az I. mellékletben meghatározott követelményeknek megfelelően minden használatban lévő EATMN-szoftverre szoftverbiztonsági szinteket jelöl ki;
3. biztosítékokat ad arra nézve, hogy:
 - a) a szoftverbiztonsági követelmények érvényessége megfelel a II. melléklet A. részében előírt követelményeknek;
 - b) a szoftverellenőrzés megfelel a II. melléklet B. részében előírt követelményeknek;
 - c) a szoftverkonfiguráció kezelése megfelel a II. melléklet C. részében előírt követelményeknek;
 - d) a szoftverbiztonsági követelmények nyomonkövethetősége megfelel a II. melléklet D. részében előírt követelményeknek;
4. meghatározza a biztosítékoktól elvárt alaposság mértékét. Az alaposság mértékét minden szoftverbiztonsági szintre meg kell határozni, úgy hogy a szoftver kritikusságával együtt növekedjen; ebből a célból:
 - a) a biztosítékok alaposságának szoftverbiztonsági szintenként változó mértékének magában kell foglalniuk az alábbi kritériumokat:
 - i. függetlenül teljesítendő;
 - ii. teljesítendő;
 - iii. teljesítése nem kötelező;
 - b) az egyes szoftverbiztonsági szinteknek megfelelő biztosítékoknak elégséges megbízhatósági szinten kell szavatolniuk, hogy az EATMN-szoftverek még megfelelő biztonsággal üzemeltethetők;
5. felhasználja az EATMN-szoftver visszacsatolásait annak megerősítésére, hogy a szoftverbiztonságot garantáló rendszer és a biztonsági szintek megfelelőek. Ebből a célból a szoftvernek a biztonsági események bejelentésére és elemzésére vonatkozó követelmények szerint bejelentett téves működését vagy hibáját az érintett rendszerre gyakorolt hatásokkal összehasonlítva kell elemezni a ►**MI** 1035/2011/EU bizottsági végrehajtási rendelet ⁽¹⁾ ◀ II. mellékletének 3.2.4. pontjában meghatározott súlyosságosztályozási rendszer alapján.

⁽¹⁾ HL L 271., 2011.10.18. 23. o.

▼B

5. cikk

A szoftverek változtatásaira és a specifikus szoftverekre vonatkozó követelmények

(1) A szoftverek bármilyen változtatása esetén, vagy specifikus olyan szoftvertípusok esetén, mint a COTS-szoftverek, a nem külön fejlesztésű szoftverek, illetve olyan szoftverek, amelyekre a 3. cikk (2) bekezdésének d) és e), vagy a 4. cikk (2), (3), (4) és (5) bekezdésében szereplő követelmények némelyike nem alkalmazható, a szervezetnek biztosítani kell, hogy a szoftverbiztonságot garantáló rendszer – a nemzeti felügyeleti hatósággal közösen kiválasztott és egyeztetett egyéb eszközök révén – ugyanolyan megbízhatósági szintet szavatoljon, mint amelyet a vonatkozó szoftverbiztonsági szint megkövetel, ha ez utóbbi meg van határozva.

Ezen eszközöknek elégséges megbízhatósági szinten kell biztosítaniuk, hogy a szoftver teljesíti a kockázatelemző és -csökkentő eljárásban meghatározott biztonsági célkitűzéseket és követelményeket.

(2) A nemzeti felügyeleti hatóság az (1) bekezdésben említett módszerek értékelésével elismert vagy bejelentett szervezetet bízhat meg.

▼M1**▼B**

7. cikk

Hatálybalépés

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ezt a rendeletet 2009. január 1-jétől kell alkalmazni az 1. cikk (2) bekezdésében említett EATMN-rendszerek új szoftvereire.

Ezt a rendeletet 2010. július 1-jétől az 1. cikk (2) bekezdésében említett és ebben az időpontban működésben lévő EATMN-rendszerek bármely változtatott szoftverére alkalmazni kell.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

▼B*I. MELLÉKLET***A 4. cikk (2) bekezdésében említett szoftverbiztonsági szintekre vonatkozó követelmények**

1. A szoftverbiztonsági szint a szoftverrel kapcsolatos biztosítékok alaposágának az EATMN-szoftverek által betöltött szerep kritikusságához mért – a ►**MI** 1035/2011/EU végrehajtási rendelet ◀ rendelet II. mellékletének 3.2.4. pontjának 4. szakaszában meghatározott súlyosságosztályozási rendszerrel meghatározott – viszonyát kombinálja egy adott hátrányos hatás bekövetkezésének valószínűségével. Legalább négy szoftverbiztonsági szintet kell meghatározni, ahol az 1. a legkritikusabb szintet jelöli.
2. A kijelölt szoftverbiztonsági szinteknek arányban kell állniuk azon, a ►**MI** 1035/2011/EU végrehajtási rendelet ◀ II. melléklete 3.2.4. pontjának 4. szakaszában említett legsúlyosabb hatással, amelyet a szoftver téves működése vagy hibája okozhat. Ennek különösen a szoftver téves működésével vagy hibájával kapcsolatos kockázatokat, valamint a strukturális és/vagy eljárási óvintézkedéseket kell figyelembe vennie.
3. Azon EATMN-szoftverösszetevőkre, amelyekről nem lehet bebizonyítani, hogy függetlenek egymástól, a függő összetevők közül a legkritikusabb összetevőre jellemző szoftverbiztonsági szintet kell kijelölni.



II. MELLÉKLET

A. rész: A 4. cikk (3) bekezdésének a) pontjában említett szoftverbiztonsági követelmények érvényességére vonatkozó követelmények

1. A szoftverbiztonsági követelmények esettől függően meghatározzák az EATMN-szoftverek funkcionalitását a névleges és csökkentett teljesítményű üzemmódban, azok válaszidejét, kapacitását, pontosságát, a célhardveren mért erőforrás-felhasználását, a rendellenes üzemeltetési körülményekkel szembeni zavartűrő képességét és a túlterhelhetőségét.
2. A szoftverbiztonsági követelményeknek teljeseknek és pontosaknak kell lenniük, valamint meg kell felelniük a rendszerbiztonsági követelményeknek.

B. rész: A 4. cikk (3) bekezdésének b) pontjában említett szoftver-ellenőrzési biztosítékokra alkalmazandó követelmények

1. Az EATMN-szoftverek funkcionalitásának, a válaszidőnek, a kapacitásnak, a pontosságnak, a célhardveren mért erőforrás-felhasználásnak, a rendellenes üzemeltetési körülményekkel szembeni zavartűrésnek és a túlterhelhetőségnek meg kell felelnie a szoftverre vonatkozó követelményeknek.
2. Az EATMN-szoftvert a nemzeti felügyeleti hatósággal egyeztetett módon elemzéssel és/vagy teszteléssel és/vagy ezzel egyenértékű módszerekkel megfelelően ellenőrizni kell.
3. Az EATMN-szoftver ellenőrzésének pontosnak és teljesnek kell lennie.

C. rész: A 4. cikk (3) bekezdésének c) pontjában említett szoftverkonfiguráció kezelésének biztosítására vonatkozó követelmények

1. A szoftverkonfiguráció azonosításának, nyomon követhetőségnek és állapota rögzítésének olyan módon kell történnie, hogy igazolható legyen, hogy az EATMN-szoftver életciklusa során a szoftverkonfiguráció végig ellenőrzés alatt áll.
2. A problémák jelentésének, nyomon követésének és a hibajavító intézkedéseknek olyanoknak kell lenniük, hogy igazolható legyen, hogy a szoftverrel kapcsolatos, biztonságot érintő problémákat megoldották.
3. Olyan helyreállítási és visszakeresési eljárásokat kell megállapítani, amelyekkel a EATMN-szoftver életciklusa során végig biztosítani lehet a szoftver életciklusadatainak újbóli előállítását és megjelenítését.

D. rész: A 4. cikk (3) bekezdésének d) pontjában említett szoftverbiztonsági követelmények nyomon követhetőségének biztosítására vonatkozó követelmények

1. Minden szoftverbiztonsági követelményt a fejlesztés azon szintjéig kell visszavezetni, amelynek való felelése bizonyítást nyert.
2. Minden szoftverbiztonsági követelményt, a fejlesztés minden olyan szintjén, amelynek való megfelelése bizonyítást nyert, vissza kell vezetni valamely rendszerbiztonsági követelményig.