

Този документ е средство за документиране и не обвързва институциите

► **V**

**РЕГЛАМЕНТ (ЕО) № 482/2008 НА КОМИСИЯТА**

от 30 май 2008 година

относно изграждане на система за осигуряване безопасността на софтуера, която да бъде въведена от доставчиците на аеронавигационни услуги, и за изменение на приложение II към Регламент (ЕО) № 2096/2005

(текст от значение за ЕИП)

(ОВ L 141, 31.5.2008 г., стр. 5)

Изменен със:

Официален вестник

№ страница дата

► **M1**

Регламент за изпълнение (ЕС) № 1035/2011 на Комисията от 17 октомври 2011 година

L 271

23

18.10.2011 г.

**РЕГЛАМЕНТ (ЕО) № 482/2008 НА КОМИСИЯТА****от 30 май 2008 година****относно изграждане на система за осигуряване безопасността на софтуера, която да бъде въведена от доставчиците на аеронавигационни услуги, и за изменение на приложение II към Регламент (ЕО) № 2096/2005****(текст от значение за ЕИП)**

КОМИСИЯТА НА ЕВРОПЕЙСКИТЕ ОБЩНОСТИ,

като взе предвид Договора за създаване на Европейската общност,

като взе предвид Регламент (ЕО) № 550/2004 на Европейския парламент и на Съвета от 10 март 2004 г. за осигуряването на аеронавигационно обслужване в единното европейско небе („Регламент за осигуряване на обслужване“) <sup>(1)</sup>, и по-специално член 4 от него,

като има предвид, че:

- (1) Съгласно Регламент (ЕО) № 550/2004 от Комисията се изисква да определи и приеме съответните разпоредби на регулаторните изисквания за безопасност на Евроконтрол („ESARR“), като се съобрази с действащото законодателство на Общността. ESARR 6, наричан „Софтуер в системите УВД“, предвижда набор от регулаторни изисквания за безопасност за въвеждането на система за осигуряване безопасността на софтуера.
- (2) Регламент (ЕО) № 2096/2005 на Комисията от 20 декември 2005 г. за определяне на общи изисквания при доставянето на аеронавигационни услуги <sup>(2)</sup> посочва в последното изречение на съображение 12, че: „Съответните разпоредби от ESARR 1 за надзор на безопасността при УВД и от ESARR 6 за софтуера в системите за УВД следва да се определят и приемат с отделни актове на Общността.“
- (3) Приложение II към Регламент (ЕО) № 2096/2005 изисква доставчиците на обслужване на въздушното движение да въведат система за управление на безопасността, както и изисквания за безопасност за оценка и намаляване на риска във връзка с промени. В рамките на своята система за управление на безопасността и като част от дейностите по оценка и намаляване на риска във връзка с промените, доставчиците на обслужване на въздушното движение следва да формулират и въведат система за осигуряване безопасността на софтуера, предназначена специално за проблемите, свързани със софтуера.
- (4) Основната цел пред безопасността на софтуера при функционалните системи, които работят с такъв, е да се гарантира, че рисковете, свързани с ползването на софтуер от системите на европейската мрежа за управление на въздушното движение (софтуер за ЕМУВД), са сведени до допустимо ниво.

<sup>(1)</sup> ОВ L 96, 31.3.2004 г., стр. 10.

<sup>(2)</sup> ОВ L 335, 21.12.2005 г., стр. 13. Регламент, изменен с Регламент (ЕО) № 1315/2007 (ОВ L 291, 9.11.2007 г., стр. 16).

**▼B**

- (5) Настоящият регламент следва да не обхваща военните операции и учения, посочени в член 1, параграф 2 от Регламент (ЕО) № 549/2004 на Европейския парламент и на Съвета от 10 март 2004 г. за определяне на рамката за създаването на Единно европейско небе (рамков регламент) <sup>(1)</sup>.
- (6) Приложение II към Регламент (ЕО) № 2096/2005 следва да бъде съответно изменено.
- (7) Мерките, предвидени в настоящия регламент, са в съответствие със становището на Комитета за единно небе,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

*Член 1*

**Предмет и обхват**

1. Настоящият регламент определя изискванията към формулирането и въвеждането на система за осигуряване безопасността на софтуера от доставчиците на обслужване на въздушното движение (ОВД), субектите, осигуряващи управлението на потоците въздушно движение (УПВД) и управлението на въздушното пространство (УВП) за целите на общото въздушно движение, и доставчиците на обслужване по комуникация, навигация и обзор (КНО).

Той определя и приема задължителните разпоредби от Регулаторните изисквания за безопасност на Евроконтрол — ESARR 6, наричани „Софтуер в системите УВД“, издадени на 6 ноември 2003 г.

2. Настоящият регламент се прилага по отношение на новия софтуер, както и за всяка промяна в софтуера на системите за ОВД, УВП, УПВД и КНО.

Той не се прилага за софтуера на бордови елементи и за космическо оборудване.

*Член 2*

**Определения**

За целите на настоящия регламент се прилагат определенията, посочени в член 2 от Регламент (ЕО) № 549/2004.

Прилагат се и следните определения:

1. „софтуер“ означава компютърни програми и съответните конфигурационни данни, включително готови софтуерни продукти, но без електронни устройства, като например специфични за дадено приложение интегрални схеми, програмируеми матрици с логически елементи или полупроводникови цифрови контролери;
2. „конфигурационни данни“ означава данните, които се използват за конфигурирането на софтуерна система с общо предназначение към конкретна употреба от заложените в нея;

<sup>(1)</sup> ОВ L 96, 31.3.2004 г., стр. 1.

**▼ B**

3. „готов софтуерен продукт“ означава софтуер, който не е разработен за целите на конкретния договор;
4. „осигуряване на безопасност“ означава всички планирани и систематични действия, необходими за получаване на необходимата гаранция, че за даден продукт, услуга, организация или функционална система е постигната приемлива или допустима безопасност;
5. „организация“ означава доставчик на ОВД, доставчик на обслужване по КНО или субект, осигуряващ УПВД или УВП;
6. „функционална система“ означава комбинация от системи, процедури и човешки ресурси, организирани за извършване на определена функция в контекста на УВД;
7. „риск“ означава комбинацията от общата вероятност или честотата на възникване на вреден ефект, породен от опасност, и степента на сериозност на този ефект;
8. „опасност“ означава всяко състояние, събитие или обстоятелство, което може да предизвика произшествие;
9. „нов софтуер“ означава софтуер, който е поръчан или за който са подписани обвързващи договори след влизане в сила на настоящия регламент;
10. „цел на безопасността“ означава качествено или количествено твърдение, което определя максималната честота или вероятност, при която се очаква възникване на дадена опасност;
11. „изискване за безопасност“ означава средство за намаляване на риска, дефинирано от стратегията за намаляване на риска, с което се постига определена цел на безопасността, включително организационни, оперативни, процедурни, функционални изисквания, а също и изисквания, свързани с работните показатели или оперативната съвместимост, както и екологични характеристики;
12. „прехвърляне от стара на нова система или замяна по време на работа“ означава подход за замяна на системните компоненти или софтуера за Европейската мрежа за управление на въздушното движение (ЕМУВД), докато системата функционира;
13. „изискване за безопасност на софтуера“ означава описание на очакваното действие на софтуера предвид входящите данни и ограниченията и, ако е постигнато, гарантиране безопасната работа на софтуера за ЕМУВД, според оперативната необходимост;
14. „софтуер за ЕМУВД“ означава софтуера, използван от системите на ЕМУВД, посочени в член 1;
15. „валидност на изискванията“ означава потвърждаване чрез проверка и осигуряване на обективни доказателства, че конкретните изисквания към целевата употреба са изпълнени;
16. „постигнат в условия на независимост“ в контекста на дейностите в процеса на проверка на софтуера означава, че те са извършени от лице или лица, различно/и от тези, които са разработили продукта, който е обект на проверката;

**▼B**

17. „нарушение в работата на софтуера“ означава невъзможността на дадена програма да изпълни правилно необходимата функция;
18. „отказ на софтуера“ означава невъзможността на дадена програма да изпълни необходимата функция;
19. „COTS (commercial-off-the-shelf)“ означава предлагано в търговската мрежа приложение, разпространявано от дистрибутори чрез публични каталози, за което не се предвижда съобразяване с индивидуалните нужди на потребителя или подобряване на характеристиките;
20. „софтуерни компоненти“ означава градивен блок, който може да бъде включен или свързан заедно с други софтуерни компоненти за многократно използване с цел комбиниране и създаване на софтуерно приложение, съобразено с потребностите на потребителя;
21. „автономни софтуерни компоненти“ означава софтуерни компоненти, които не спират да функционират при същото състояние на отказ, което води до поява на опасност;
22. „количествени времеви параметри на софтуера“ означава времето, което е необходимо, за да може софтуерът да реагира на определени входящи данни или периодични събития и/или работата на софтуера по отношение на обработваните за единица време операции или съобщения;
23. „капацитет на софтуера“ означава възможността на софтуера да обработва определено количество входящи данни;
24. „точност“ означава изискваната точност на изчислените резултати;
25. „използваем системен софтуерен ресурс“ означава количеството компютърен системен ресурс, който може да се използва от приложния софтуер;
26. „стабилност на софтуера“ означава поведението на софтуера при постъпване на неочаквани входящи данни, откази на хардуера и прекъсвания в захранването в самата компютърна система или в свързани периферни устройства;
27. „устойчивост на претоварване“ означава поведението на системата, и по-специално нейната устойчивост, при подаване на данни с по-висока скорост от очакваната при нормално функциониране на системата;
28. „прецизна и цялостна проверка на софтуера за ЕМУВД“ означава, че всички изисквания по отношение на безопасността на софтуерната система, които показват по прецизен начин какво се очаква от софтуерния компонент в процеса на оценка и намаляване на риска, и тяхното прилагане е в съответствие с изискванията за нивото на гаранциите на софтуера;
29. „данни за жизнения цикъл на софтуера“ означава данните, които да създават по време на жизнения цикъл на софтуера с цел да се планира, насочи, обясни, определи, запише или осигури доказателство за извършени операции; тези данни подпомагат процесите по време на жизнения цикъл на софтуера, одобрението на системата или оборудването, както и измененията на софтуерния продукт след получаването на одобрение;

**▼B**

30. „жизнен цикъл на софтуера“ означава:
- а) сбор от последователни процеси, определени от дадена организация за достатъчни и адекватни за изработване на софтуерен продукт;
  - б) период от време, започващ с решение за изработване или изменение на софтуерен продукт и завършващ с изтегляне на продукта от експлоатация;
31. „изискване за безопасност на системата“ означава изискване за безопасност по отношение на дадена функционална система.

*Член 3***Общи изисквания за безопасност**

1. Когато от една организация се изисква да приложи процес на оценка и намаляване на риска в съответствие с действащото законодателство на общностно или национално равнище, тя формулира и прилага система за осигуряване безопасността на софтуера, специално предназначена да решава въпроси, свързани със софтуера за ЕМУВД, включително всички оперативни промени, извършвани в реално време, и по-специално прехвърляне от стара на нова система или замяна по време на работа.
2. Организацията гарантира като минимум, че нейната система за осигуряване безопасността на софтуера предоставя доказателства и аргументи, които доказват следното:
  - а) изискванията за безопасност на софтуера показват по ясен начин какво се очаква от софтуера, за да бъдат изпълнени целите и изискванията за безопасност, формулирани в процеса на оценка и намаляване на риска;
  - б) обръща се внимание на възможността за проследяване по отношение на всички изисквания за безопасност на софтуера;
  - в) инсталирането на софтуера не е свързано с функции, които се отразяват неблагоприятно на безопасността;
  - г) софтуерът за ЕМУВД изпълнява изискванията при степен на увереност, съответстваща на критичното значение на софтуера;
  - д) дават се гаранции, които потвърждават общите изисквания за безопасност, посочени в букви от а) до г), и аргументи, показващи, че необходимите гаранции винаги се осигуряват на базата на:
    - i) известна изпълнима версия на софтуера;
    - ii) известен диапазон от конфигурационни данни;
    - iii) известен набор от софтуерни продукти и описания, включително спецификации, които са били използвани при разработването на въпросната версия.
3. Организацията предоставя на националния орган за надзор необходимите гаранции за изпълнение на изискванията, посочени в параграф 2.

**▼B***Член 4***Изисквания, приложими към системата за осигуряване безопасността на софтуера**

Организацията гарантира като минимум, че системата за осигуряване безопасността на софтуера:

1. е документирана, по-конкретно като част от пълната документация по оценка и намаляване на риска;
2. разпределя нива на гаранции за софтуера за всеки оперативен софтуер за ЕМУВД в съответствие с изискванията, посочени в приложение I;
3. включва гаранции за:
  - а) валидност на изискванията за безопасност на софтуера в съответствие с изискванията, посочени в приложение II, част А;
  - б) проверка на софтуера в съответствие с изискванията, посочени в приложение II, част Б;
  - в) управление на конфигурацията на софтуера в съответствие с изискванията, посочени в приложение II, част В;
  - г) проследяване на изискванията за безопасност на софтуера в съответствие с изискванията, посочени в приложение II, част Г;
4. определя степента на възискателност при установяване нивата на гаранциите; степента на възискателност следва да се определя за всяко ниво на гаранция на софтуера и нараства с увеличаване критичността на софтуера; за тази цел:
  - а) варирането в степента на възискателност за дадено ниво на гаранциите на софтуера следва да включва следните критерии:
    - i) изискване за постигане в условия на независимост;
    - ii) изискване за постигане;
    - iii) няма изискване за постигане;
  - б) гаранциите, съответстващи на всяко ниво на безопасност на софтуера, следва да дават достатъчна увереност за функционирането на софтуера за ЕМУВД при допустимо ниво на безопасност;
5. използва обратна връзка на базата на опита със софтуера за ЕМУВД, за да потвърди, че системата за осигуряване безопасността на софтуера и задаването на нивата на безопасност са адекватни. За тази цел ефектите от нарушение в работата на софтуера или от отказ на софтуера, докладвани според съответните изисквания за докладването и за оценката на събития, свързани с безопасността, се оценяват чрез съпоставка с идентифицираните за въпросната система ефекти от схемата за класификация на степен на сериозност, определена в раздел 3.2.4 от приложение II към **►M1** Регламент за изпълнение (ЕС) № 1035/2011 на Комисията <sup>(1)</sup> ◀.

(<sup>1</sup>) ОВ L 271, 18.10.2011 г., стр. 23.

**▼B***Член 5***Изисквания, приложими за промени на софтуера и за конкретен софтуер**

1. За всяка промяна на софтуера или за конкретни видове софтуер, като COTS, готови софтуерни продукти или вече използван софтуер, за които някои от изискванията от член 3, параграф 2, буква г) или д) или член 4, параграф 2, 3, 4, или 5 не са приложими, организацията гарантира, че системата за осигуряване безопасността на софтуера осигурява по други избрани и съгласувани с националния орган за надзор начини същата степен на увереност като тази при съответстващото ниво на гаранции, когато такова е дефинирано.

Тези начини следва да дават достатъчна степен на увереност, че софтуерът отговаря на целите и изискванията за безопасност, определени в процеса на оценка и намаляване на риска.

2. При оценяването на начините, посочени в параграф 1, националният орган за надзор може да използва призната организация или нотифициран орган.

**▼M1****▼B***Член 7***Влизане в сила**

Настоящият регламент влиза в сила на двадесетия ден след публикуването му в *Официален вестник на Европейския съюз*.

Той се прилага от 1 януари 2009 г. за новия софтуер за системите ЕМУВД, посочени в член 1, параграф 2, първа алинея.

Той се прилага от 1 юли 2010 г. по отношение на всички промени в софтуера за системите ЕМУВД, посочени в член 1, параграф 2, първа алинея, които функционират към тази дата.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави-членки.





*ПРИЛОЖЕНИЕ I*

**Изисквания, приложими за нивото на осигуряване безопасност на софтуера, посочено в член 4, параграф 2**

1. Нивото на гаранции на софтуера съотнася степента на сериозност на гаранциите на софтуера с критичността на софтуера за ЕМУВД, като използва схемата за класификация на степен на сериозност, установена в точка 3.2.4, раздел 4 от приложение II към ►**MI** Регламент за изпълнение (ЕС) № 1035/2011 ◀, съчетана с вероятността за възникване на определен неблагоприятен ефект. Определят се поне четири нива на гаранции на безопасност на софтуера, като ниво 1 е с най-висока степен на критичност.
2. Определеното ниво на гаранции на софтуера следва да съответства на най-неблагоприятния ефект, който може да бъде причинен от нарушения в работата на софтуера или откази на софтуера, както е посочено в точка 3.2.4, раздел 4 от приложение II към ►**MI** Регламент за изпълнение (ЕС) № 1035/2011 ◀. По-конкретно следва да се отчитат рисковете, свързани с нарушения в работата на софтуера или откази на софтуера, и установените структурни и/или процедурни защити.
3. За софтуерните компоненти на ЕМУВД, чиято независимост не може да бъде доказана, се определя ниво на гаранции на софтуера, равно на това на зависимите компоненти от най-критично значение.

*ПРИЛОЖЕНИЕ II***Част А: Изисквания, приложими за потвърждаване на нивото на безопасност на софтуера, посочено в член 4, параграф 3, буква а)**

1. Изискванията за безопасност на софтуера определят функционалното поведение на софтуера за ЕМУВД в нормален режим на работа и в режим със занижени параметри, както и количествените времеви параметри, капацитета, точността, използваемия софтуерен ресурс върху избрания хардуер, стабилността при извънредни условия на работа и устойчивостта на претоварване, съобразно случая.
2. Изискванията за безопасност на софтуера са пълни и точни и съответстват на изискванията за безопасност на системата.

**Част Б: Изисквания, приложими за проверката на софтуера, посочена в член 4, параграф 3, буква б)**

1. Функционалното поведение на софтуера за ЕМУВД, количествените времеви параметри, капацитетът, точността, използваемият софтуерен ресурс върху избрания хардуер, стабилността при извънредни условия на работа и устойчивостта на претоварване са в съответствие с изискванията към софтуера.
2. Софтуерът за ЕМУВД се подлага на адекватна проверка чрез анализ и/или тестове, и/или други съответни средства, според договореното с националния орган за надзор.
3. Проверката на софтуера за ЕМУВД е точна и пълна.

**Част В: Изисквания, приложими за управлението на конфигурацията на софтуера, посочена в член 4, параграф 3, буква в)**

1. Определянето на конфигурацията, проследяването и отчитането на статуса са такива, че да може да се покаже, че системните данни през жизнения цикъл на софтуера подлежат на контрол на конфигурацията през цялото време на жизнения цикъл на софтуера за ЕМУВД.
2. Докладването на проблеми, проследяването и корективните действия са такива, че да може да бъде доказано намаляването на проблеми по безопасността, свързани със софтуера.
3. Процедурите за извличане на необходимите данни и за пускане на нова версия са такива, че да позволяват регенериране и наличност на системните данни от жизнения цикъл на софтуера през целия жизнен цикъл на софтуера за ЕМУВД.

**Част Г: Изисквания, приложими за осигуряването на проследяемост на изискванията за безопасност на софтуера, посочени в член 4, параграф 3, буква г)**

1. Всяко изискване за безопасност на софтуера следва да може да бъде проследено до същото ниво от проектирането на софтуера, на което се демонстрира изпълнението му.
2. Всяко изискване за безопасност на софтуера на всяко ниво от проектирането на софтуера, на което се демонстрира изпълнението му, следва да може да бъде проследено до изискване за безопасността на системата.