Регулатива (ЕК) бр. 482/2008 на Комисијата

од 30 мај 2008 година

За воспоставување систем за контрола на безбедноста на софтверот што треба да се спроведе од давателите на услуги во воздушната пловидба и измена и дополнување на Анекс II кон Регулативата (ЕК) бр. 2096/2005

(Текст со важност за ЕЕО (Европска економска област))

КОМИСИЈАТА НА ЕВРОПСКИТЕ ЗАЕДНИЦИ,

имајќи го предвид Договорот за основање на Европската заедница,

имајќи ја предвид Регулативата (ЕК) бр. 550/2004 на Европскиот парламент и на Советот, од 10 март 2004 година, за обезбедување услуги на воздушна пловидба во единственото Европско небо (Регулативата за давање услуги)[1], а особено членот 4 од неа,

со оглед на тоа што:

(1) во согласност со Регулативата (ЕК) бр. 550/2004, Комисијата треба да ги идентификува и да ги усвои соодветните одредби од безбедносните регулаторни барања на Евроконтрол (ESARR), земајќи го предвид постоечкото законодавство на Заедницата. ESARR 6 насловен како „Софтвер во ATM системите“ обезбедува збир безбедносни регулаторни барања за спроведување на системот за контрола на безбедноста на софтверот.

(2) Регулативата (ЕК) бр. 2096/2005 на Комисијата, од 20 декември 2005 година, која ги утврдува условите за обезбедување услуги на воздушна пловидба[2], во последната реченица од цитатот 12 вели дека „соодветните одредби од ESARR 1 за контролата на безбедноста во ATM и ESARR 6 за софтверот во ATM системите, треба да се идентификуваат и да се усвојат преку одделни акти на Заедницата“.

(3) Анекс II кон Регулативата (ЕК) бр. 2096/2005 предвидува давателите на услуги во воздушниот сообраќај да спроведат систем за управување со безбедноста, како и безбедносни барања за процена на ризикот и посредување, имајќи ги предвид промените што настануваат. Во рамките на овој систем за управување со безбедноста и како дел од проценатa на ризикот и активностите за посредување, имајќи ги предвид промените, давателот на услуги во воздушниот сообраќај треба да дефинира и да спроведе систем за контрола на безбедноста во софтверот, за посебно да се справат со аспектите поврзани со софтверот.

---

[1] Сл. весник L 96, 31.3.2004, стр. 10.

[2] Сл. весник L 335, 21.12.2005, стр. 13. Регулатива последно изменета со Регулативата (ЕК) бр. 1315/2007 (Сл. Весник L 291. 9.11.2007г. , стр. 16).

(4) Примарната цел за безбедноста на софтверот која треба да биде исполнета за функционалните системи кои содржат софтвер е да се обезбеди ризиците поврзани со користењето на софтверот во системите на Европската мрежа за управување со воздушниот сообраќај (EATMN софтверот) да се намалат на ниво што може да се толерира.

(5) Оваа Регулатива не треба да ги опфаќа воените операции и обуки, како што е наведено во членот 1(2) од Регулативата (ЕК) бр. 549/2004 на Европскиот парламент и на Советот, од 10 март 2004 година, со која се дефинира рамката за создавање единствено Европско небо (Рамковната регулатива)[3].

(6) Затоа, Анекс II кон Регулативата (ЕК) бр. 2096/2005 треба соодветно да се измени и да се дополни.

(7) Мерките предвидени со оваа регулатива се во согласност со мислењето на Комисијата за единственото Европско небо,

ЈА ДОНЕСЕ СЛЕДНАВА РЕГУЛАТИВА:

Член 1

Предмет и опсег

1. Оваа Регулатива ги утврдува барањата за дефинирање и спроведување на системот за контрола на безбедноста на софтверот од страна на давателите на услуги на воздушна пловидба (ATS), субјектите кои обезбедуваат управување со воздушниот сообраќај (ATFM) и управување со воздушниот простор (ASM) за општиот воздушен сообраќај и давателите на услуги на комуникација, навигација и надзор (CNS).

Ги идентификува и ги усвојува задолжителните одредби според регулаторните барања за безбедност на Евроконтрол – ESARR 6 – со наслов „Софтвер во ATM системите“ издадено на 6 ноември 2003 година.

2. Оваа Регулатива ќе се применува на новиот софтвер и сите промени во софтверот на системите за ATS, ASM, ATFM и CNS.

Нема да се однесува на софтверот за компонентите за леталата и за вселенската опрема.

Член 2

Дефиниции

За целите на оваа Регулатива ќе се применуваат дефинициите во член 2 од Регулативата (ЕК) бр. 549/2004.

Исто така, ќе се применуваат следните дефиниции:

[3] Сл. весник L 96, 31.3.2004, стр. 1

1. „софтвер“ значи компјутерски програми и соодветни податоци за конфигурација, вклучително неразвоен софтвер, но со исклучок на електронски предмети, имено, интегрирани кола за одредени апликации, влезни низи што може да се програмираат или цврсти логички контролори;

2. „податоци за конфигурација“ значи податоци што конфигурираат генерички софтверски систем за одредена намена;

3. „неразвоен софтвер“ значи софтвер што не се развива за тековниот договор;

4. „контрола на безбедноста“ значи сите планирани и систематски активности што се неопходни за да се обезбеди соодветна сигурност дека производот, услугата, организацијата или функционалниот систем ќе постигнат прифатливо ниво или задоволително ниво на толеранција во однос на безбедноста;

5. „организација“ значи или ATS давател, CNS давател или субјект кој обезбедува ATFM или ASM;

6. „функционален систем“ значи комбинација на системи, постапки и човечки ресурси организирани да вршат функција во контекст на ATM;

7. „ризик“ значи комбинација на целокупната веројатност или фреквенција на штетните влијанија предизвикани од ризикот и сериозноста на таквото влијание;

8. „опасност“ значи секоја состојба, настан или околност која може да предизвика несреќа;

9. „нов софтвер“ значи софтвер што е нарачан или за кој се потпишани обврзувачки договори, по стапување во сила на оваа Регулатива;

10. „безбедносна цел“ значи квалитативна или квантитативна изјава со која се дефинира максималната фреквенција или веројатност според која може да се очекува појава на одредена опасност;

11. „безбедносно барање“ значи средство за посредување на ризик, дефинирано според стратегијата за посредување со ризик, со кое се постигнува одредена безбедносна цел, вклучително организациско, оперативно, процедурално, функционално, изведбено или интероперабилно барање или одредена карактеристика во врска со животната средина;

12. „премостување или замена за време на функционирање“ значи пристап на замена на компонентите на системот на Европската мрежа за управување со воздушниот сообраќај (EATMN) или софтверот додека системот е во функција;

13. „барање за безбедноста на софтверот“ значи опис на тоа што треба да се генерира со софтверот според влезните информации и дадените ограничувања, кои, ако се исполнат, се обезбедува дека EATMN софтверот ќе работи безбедно и според оперативните потреби;

14. „EATMN софтвер“ значи софтвер што се користи во EATMN системите, наведени во членот 1;

15. „валидност на барањата“ значи потврда со испитување и давање докази дека се исполнети одредените барања за намената;

16. „постигнато независно“ значи, во однос на активностите за верификација на софтверот, дека активностите во процесот на верификација ги изведува лице (лица) различни од програмерот на делот што се верификува;

17. „нефункционирање на софтверот“ значи неможност на програмата точно да ја извршува функцијата;

18. „пад на софтверот“ значи неможност на програмата да ја извршува функцијата;

19. „COTS“ значи комерцијално достапна апликација што се продава преку јавни каталози и не е наменета да се специјализира или да се надградува;

20. „софтверски компоненти“ значи елементи што може да се додаваат или меѓусебно да се поврзуваат со други елементи на софтверот за да комбинираат и да создадат специјализирана софтверска апликација;

21. „независни софтверски компоненти“ значи оние софтверски компоненти што не се неоперативни од состојбата што ја предизвикува опасноста;

22. „софтверски активности со временски интервал“ значи времето што е дадено за софтверот да одговори на зададените влезни информации или периодични настани и/или функционирање на софтверот во однос на трансакциите или пораките што се манипулираат во единица време;

23. „софтверски капацитет“ значи можноста на софтверот да ракува со одредена количина проток на податоци;

24. „точност“ значи бараната прецизност на обработените резултати;

25. „користење на софтверските ресурси“ значи количината на ресурсите во рамките на компјутерскиот систем што може да се користи од апликативниот софтвер;

26. „големина на софтверот“ значи однесувањето на софтверот во случај на несакани влезни информации, хардверски грешки и прекини во напојувањето, или во компјутерскиот систем или во поврзаните уреди;

27. „толеранција на оптоварување“ значи однесувањето на системот во случајна, а особено толеранција на влезни информации што се јавуваат повеќе од очекуваното за време на нормалното функционирање на системот;

28. „точна и целосна верификација на EATMN софтверот“ значи сите безбедносни барања за софтверот кои точно укажуваат на тоа што се бара од софтверската компонента според проценатa на ризикот и процесот на посредување, и нивното спроведување се демонстрира на нивото што се бара од нивото за контрола на софтверот;

29. „податоци за животниот циклус на софтверот“ се податоците што се генерираат за време на животниот циклус на софтверот, за планирање, насочување, појаснување, дефинирање, забележување или обезбедување докази за активностите; овие податоци ги овозможуваат процесите за животниот циклус на софтверот, одобрувањето на системот или опремата и измените во софтверскиот производ по одобрувањето;

30. „животен циклус на софтверот“ значи:

(а) збир процеси определени со организација кои ќе бидат соодветни за генерирање на софтверскиот производ;

(б) временскиот период што започнува со одлуката за генерирање или измена на софтверски производ и завршува кога производот ќе се повлече од употреба;

31. „барање за безбедност на системот“ значи барање безбедност за функционалноста на системот.

Член 3

Основни безбедносни барања

1. Во случај кога е потребна организација за спроведување на процена на ризик и процес на посредување во согласност со применливото законодавство на Заедницата или националното законодавство, ќе дефинира и ќе спроведе систем за контрола на безбедноста на софтвер за аспектите поврзани со EATMN софтверот, вклучително сите он-лајн софтверски оперативни промени, а особено премостувањето и замената за време на функционирањето на системот.

2. Организацијата минимално ќе обезбеди системот за контрола на безбедноста на софтверот да генерира докази и аргументи што ќе го покажат следното:

(а) барањата за безбедност на софтверот точно да наведат што се бара од софтверот, со цел да се исполнат целите за безбедност и безбедносните барања, како што е укажано со проценатa на ризик и процесите за посредување;

(б) следењето се опфаќа во однос на сите безбедносни барања во врска со софтверот;

(в) спроведувањето на софтверот не содржи функции кои негативно влијаат на безбедноста;

(г) EATMN софтверот ги задоволува барањата со нивото на сигурност, кое соодветствува со критичноста на софтверот;

(д) сигурноста се обезбедува со потврдување дека се исполнети општите безбедносни барања наведени во точките (а) до (г) и аргументите што покажуваат дека бараната контрола во секое време се изведува од:

(i) позната извршна верзија на софтверот;

(ii) познат опсег на податоци за конфигурација;

(iii) познат збир од софтверски производи и описи, вклучително и спецификации, кои се искористени во генерирањето на таа верзија.

3. Организацијата ќе ја обезбеди потребната сигурност, за националното надзорно тело, покажувајќи дека барањата предвидени во ставот 2 се исполнети.

Член 4

Барања што се применуваат за системот за контрола на безбедноста на софтверот

Организацијата минимално ќе обезбеди системот за контрола на безбедноста на софтверот:

1. да биде документиран, како дел од целокупната процена на ризикот и документацијата за посредување;

2. да распредели нивоа на сигурност на софтверот за целиот оперативен EATMN софтвер, во согласност со барањата предвидени во Анекс I;

3. вклучително и обезбедување на:

(а) валидност на барањата за безбедност на софтверот, во согласност со барањата предвидени во Анекс II, дел А;

(б) верификација на софтверот во согласност со барањата предвидени во Анекс II, дел Б;

(в) управување со конфигурацијата на софтверот, во согласност со барањата утврдени во Анекс II, дел В;

(г) можност за следење на барањата за безбедноста на софтверот, во согласност со барањата предвидени во Анекс II, дел Г;

4. Определување на степенот до кој ќе се дефинира контролата; овој степен мора да се дефинира за секое ниво на контрола и да се зголемува како што се зголемува критичноста на софтверот, а за таа цел:

(а) варијациите во степенот на сериозност на контролите по нивоа мора да ги вклучува следните критериуми:

(i) потребно да се реализира независно;

(ii) потребно да се реализира;

(iii) не е потребно;

(б) контролата што е соодветна на секое ниво на контрола на софтверот мора да обезбеди сигурност дека EATMN софтверот може безбедно да функционира во рамките на толеранцијата;

5. Користи повратни информации на EATMN софтверското искуство за потврдување дека системот за контрола на софтверот и нивоата се соодветно назначени. За таа цел, ефектите од нефункционирањето на софтверот или падот на истиот, кои се пријавуваат според соодветните барања за пријавување и процена на безбедносните ситуации, ќе се проценат во споредба со ефектите идентификувани за системот во однос на категоријата на сериозност, дефинирана во делот 3.2.4 од Анекс II кон Регулативата (ЕК) бр. 2096/2005.

Член 5

Барања што се применуваат за промените во софтверот и за специјалниот софтвер

1. За сите промени во софтверот или специфичните типови софтвер, како што е COTS, неразвојниот софвтер или претходно користениот софтвер за кој не може да се применат некои од барањата наведени во членот 3(2)(г) или (д) или членот 4(2), (3), (4) или (5), организацијата ќе обезбеди системот за контрола на софтверот да обезбеди, користејќи други средства одобрени од националното надзорно тело, исто ниво на сигурност како нивото за контрола на безбедноста што е дефинирано.

Тие средства мора да овозможат доволно ниво на сигурност, така што софтверот ќе ги исполни безбедносните цели и барања, како што е идентификувано со проценатa на безбедносниот ризик и процесот на посредување.

2. При проценатa на средствата наведени во ставот 1, националното надзорно тело може да користи призната организација или надлежно тело.

Член 6

Измена и дополнување на Регулативата (ЕК) бр. 2096/2005

Во Анекс II кон Регулативата (ЕК) бр. 2096/2005, се додава следниот дел:

„3.2.5 дел 5

Систем за контрола на безбедноста на софтверот

Во рамките на функционирањето на системот за управување со безбедноста, давателот на услуги во воздушниот сообраќај ќе спроведе систем за контрола на безбедноста на софтверот, во согласност со Регулативата (ЕК) бр. 482/2008 на Комисијата, од 30 мај 2008 година, со која се дефинира системот за контрола на безбедноста на софтверот што треба да го воспостават давателите на услуги на воздушна пловидба и измена и дополнување на Анекс II кон Регулативата (ЕК) бр. 2096/2005 (*).

(*) Сл. весник L 141, 31.5.2008, стр. 5

Член 7

Влегување во сила

Оваа Регулатива влегува во сила на дваесеттиот ден од нејзиното објавување во Службениот весник на Европската унија.

Ќе се применува од 1 јануари 2009 година за новиот софтвер на EATMN системите, наведени во членот 1(2), во првиот потстав.

Ќе се применува од 1 јули 2010 година за сите промени во софтверот на EATMN системите, наведени во членот 1(2), во првиот потстав, кои се во функција на тој датум.

Оваа Регулатива е целосно обврзувачка и директно применлива во сите земји-членки.

Брисел, 30 мај 2008 година.

За Комисијата

Антонио Тајани

Член на Комисијата

АНЕКС I

Барања што се применуваат за нивото на сигурност на софтверот, наведени во членот 4(2)

1. Нивото за сигурност на софтверот е поврзано со сериозноста на контролите на софтверот во однос на критичноста на EATMN софтверот, со користење на категоризацијата по сериозност, наведена во делот 4, точка 3.2.4 од Анекс II кон Регулативата (ЕК) бр. 2096/2005 комбинирано со веројатноста за појава на негативен ефект. Ќе се идентификуваат минимално четири нивоа на сигурност на софтверот, со ниво 1 како најкритично ниво.

2. Сите распределени нивоа ќе соодветствуваат со најсериозниот ефект што може да биде предизвикан со нефункционирање или пад на софтверот, како што е наведено во делот 4 од точка 3.2.4 од Анекс II кон Регулативата (ЕК) бр. 2096/2005. Ова, особено ќе ги земе предвид ризиците поврзани со дефектите во софтверот или падот на софтверот и архитектонските и/или процедуралните одбрани што се идентификувани.

3. Софтверските компоненти на EATMN што не можат да се прикажат како независни една од друга, ќе добијат ниво на сигурност на софтверот за најкритичните од зависните компоненти.

АНЕКС II

Дел А: Барања што се применуваат за валидноста на безбедносните барања за софтверот, наведени во членот 4(3) (а)

1. Барањата за безбедност на софтверот ќе го покажат функционалното однесување во номиналниот и намалениот режим на EATMN софтверот, операциите со временски интервали, капацитетот, точноста, користење на софтверските ресурси на хардверот, робустноста на невообичаени оперативни услови и толеранција на оптоварување, во зависност од тоа што е соодветно.

2. Барањата за безбедност на софтверот ќе бидат целосни и точни и ќе бидат соодветни на безбедносните барања за системот.

Дел Б: Барања што се применуваат за верификацијата на софтверот, наведени во членот 4(3) (б)

1. Функционалното однесување на EATMN софтверот, операциите со временски интервали, капацитетот, точноста, користењето на софтверските ресурси на хардверот, робустноста на невообичаени оперативни услови и толеранција на оптоварување, ќе бидат во согласност со барањата за софтверот.

2. EATMN софтверот соодветно ќе биде верификуван со анализа и/или тестирање и/или соодветни средства, како што е дефинирано од националното надзорно тело.

3. Верификацијата на EATMN софтверот ќе биде точна и целосна.

Дел В: Барања што се применуваат за обезбедување на управувањето со конфигурацијата на софтверот, наведени во членот 4(3) (в)

1. Идентификацијата на конфигурацијата, следењето и пресметката на статусот ќе бидат такви што податоците за животниот циклус на софтверот ќе бидат прикажани под контрола на конфигурацијата во текот на целиот животен циклус на EATMN софтверот.

2. Известувањето за појава на проблеми, следење и активности за корекција ќе бидат такви што безбедносните проблеми поврзани со софтверот ќе може да се прикажат дека се премостени.

3. Постапките за враќање и пуштање ќе бидат такви што податоците за животниот циклус на софтверот ќе може да се генерираат и да се доставуваат во текот на целиот животен циклус на EATMN софтверот.

Дел Г: Барања што се применуваат за можноста за следење на безбедносните барања за софтверот, наведени во членот 4(3) (г)

1. Секое безбедносно барање за софтверот ќе се следи на истото ниво на дизајн на кое се покажува задоволителен степен.

2. Секое безбедносно барање за софтверот, на секое ниво на дизајнот каде што ќе се покаже степен на задоволителност, ќе се следи на безбедносно барање за системот.