EUROPEJSKA ORGANIZACJA BEZPIECZEŃSTWA ŻEGLUGI POWIETRZNEJ

WYMAGANIA EUROCONTROL W ZAKRESIE PRZEPISÓW BEZPIECZEŃSTWA (ESARR)

ESARR 6

OPROGRAMOWANIE W SYSTEMACH ZARZĄDZANIA RUCHEM LOTNICZYM

Edycja:	**1.0**
Data edycji oryginału:	**06.11.2003**

EUROPEJSKA ORGANIZACJA BEZPIECZEŃSTWA ŻEGLUGI POWIETRZNEJ

EUROCONTROL

Decyzja Stałej Komisji

DECYZJA Nr 100

Zatwierdzająca wymagania EUROCONTROL w zakresie przepisów bezpieczeństwa - ESARR 6 – zatytułowane „*Oprogramowanie w Systemach Zarządzania Ruchem Lotniczym*”

STAŁA KOMISJA BEZPIECZEŃSTWA ŻEGLUGI POWIETRZNEJ

Mając na uwadze Międzynarodową Konwencję EUROCONTROL w sprawie Współpracy w zakresie Bezpieczeństwa Żeglugi Powietrznej, poprawioną Protokołem podpisanym w Brukseli w dniu 12 lutego 1981 r., w szczególności jego Artykuły 1(c), 2.1(j), 6.1 i 7.1;

Mając na uwadze Protokół konsolidujący Międzynarodową Konwencję EUROCONTROL w sprawie Współpracy w zakresie Bezpieczeństwa Żeglugi Powietrznej, otwarty do podpisu w dniu 27 czerwca 1997 r., w szczególności Artykuł 2.1(i) skonsolidowanej Konwencji, uzupełnionej tym Protokołem;

Mając na uwadze Decyzje Nr 71 i 72 z dnia 9 grudnia 1997 r. w sprawie wczesnego wdrożenia niektórych klauzul zrewidowanej Konwencji, w szczególności paragraf 5 Decyzji Nr 72;

W odpowiedzi na propozycję Rady Tymczasowej,

PODEJMUJE NINIEJSZYM PONIŻSZĄ DECYZJĘ:

Komisja zatwierdza do włączenia i wdrożenia w krajowych systemach prawnych Państw Członkowskich EUROCONTROL Wymagania EUROCONTROL w zakresie przepisów bezpieczeństwa - ESARR 6 – zatytułowane „Oprogramowanie w Systemach Zarządzania Ruchem Lotniczym”, tak jak opracowane przez Komisję ds. Przepisów Bezpieczeństwa.

Powyższa decyzja wejdzie w życie w dniu jej podpisania.

Bruksela, 06.11.2003

/ ---------- /

J. TURECKY
Przewodniczący Komisji

WYKAZ ZMIAN

Niniejsze wydanie uwzględnia wszystkie zmiany tego dokumentu do dnia 6 listopada 2003 r.

SPIS TREŚCI

STRESZCZENIE

Niniejsze wymagania EUROCONTROL w zakresie przepisów bezpieczeństwa (ESARR) zostały przygotowane przez Komisję ds. Przepisów Bezpieczeństwa.

ESARR 6 dotyczy wdrażania systemów zapewnienia bezpieczeństwa oprogramowania w celu ograniczenia ryzyka związanego z wykorzystaniem oprogramowania w naziemnych systemach związanych z bezpieczeństwem zarządzania ruchem lotniczym do dopuszczalnego poziomu.

Celem niniejszego ESARR-u jest zapewnienie jednolitych wymagań dotyczących przepisów wykorzystania oprogramowania w systemach ATM. Nie wskazuje on żadnego konkretnego systemu zapewnienia bezpieczeństwa w oprogramowaniu, jako spełniającego obowiązkowe wymagania. Niniejszy ESARR nie stanowi także odwołania do określonych krajowych lub międzynarodowych standardów zapewnienia bezpieczeństwa w oprogramowaniu.

Postanowienia niniejszego dokumentu powinny zostać wprowadzone w przeciągu 3 lat od daty ich przyjęcia przez EUROCONTROL.

MATERIAŁ WPROWADZAJĄCY

*Przepisy niniejszego rozdziału **nie** są obowiązkowe*

A. ZAKRES

i. ESARR 6 dotyczy wykorzystania oprogramowania w naziemnych systemach związanych z bezpieczeństwem zarządzania ruchem lotniczym (ATM), stosowanych dla zapewniania służb ATM w cywilnym ruchu lotniczym, włączając w to wszystkie działania operacyjne na oprogramowaniu, takie jak szybkie przejście czy zamiana urządzeń w czasie pracy.

ii. Zakres ESARR 6 jest ograniczony do naziemnych elementów ATM i do naziemnych usług wspomagających, włącznie z systemami łączności, nawigacji i dozorowania (*Communication, Navigation and Surveillance - CNS*) pozostającymi pod kontrolą organu zarządzania ruchem lotniczym. ESARR 6 nie może być stosowany do pokładowych ani satelitarnych elementów systemów ATM, o ile nie zostanie zmodyfikowany i odpowiednio oceniony.

iii. Niniejsze wymagania w zakresie przepisów bezpieczeństwa zostały opracowane przy założeniu dokonywania oceny ryzyka i jego ograniczenia do odpowiedniego poziomu, wobec wszystkich aspektów ATM, włącznie z tymi funkcjami ATM, które mają być realizowane przez oprogramowanie.

iv. ESARR 6 nie proponuje żadnych typów rozwiązań zapewniających zgodność oprogramowania z jego wymaganiami. Jest to rola standardów zapewniania oprogramowania. Niniejszy ESARR nie stanowi także odwołania do jakichkolwiek konkretnych krajowych lub międzynarodowych standardów zapewniania bezpieczeństwa w oprogramowaniu.

B. UZASADNIENIE

i. Na mocy Decyzji SRC numer 6/8/5 zaakceptowano włączenie opracowania wymagań w zakresie przepisów bezpieczeństwa EUROCONTROL dla systemów ATM, opartych na oprogramowaniu, do programu prac SRC. Uznano, że w zakresie Standardów i Zalecanych Praktyk (SARPS) ICAO nie istnieje w chwili obecnej żaden poprzedzający go przepis.

ii. ESARR 3 (Wykorzystywanie Systemów Zarządzania Bezpieczeństwem przez Organy Zarządzania Ruchem Lotniczym) wymaga, aby systemy zarządzania bezpieczeństwem obejmowały ocenę i ograniczanie ryzyka w systemie ATM i klasyfikowania wszystkich funkcji systemu ATM pod kątem ich znaczenia dla bezpieczeństwa. ESARR 3 wymaga również ograniczania ryzyka tam, gdzie ocena wskazuje, że jest to niezbędne ze względu na znaczenie samej zmiany.

iii. ESARR 4 (Ocena i Ograniczanie Ryzyka w Systemie Zarządzania Ruchem Lotniczym) rozszerza wymagania ESARR 3 w zakresie oceny i ograniczania ryzyka. Przewiduje także stosowanie procesów obejmujących pełne systemy ATM, w tym ludzi, procedury i wyposażenie (sprzęt i oprogramowanie) oraz ich wzajemne relacje, w trakcie wdrażania lub planowania zmian w systemie ATM.

iv. ESARR 6 stanowi kontynuację rozwoju przepisów w zakresie bezpieczeństwa i rozszerza ESARR 4 w aspektach dotyczących oprogramowania w systemach ATM. Rozważane są także uzupełniające wymagania bezpieczeństwa dla sprzętu.

v. Bezpieczeństwo stanowi zasadniczą cechę systemów ATM. Jest ono nadrzędne w stosunku do efektywności operacyjnej. Coraz bardziej rozbudowane systemy ATM, automatyka funkcji operacyjnych uprzednio wykonywanych ręcznie, a także powszechne stosowanie oprogramowania, wymagają bardziej formalnego podejścia do osiągania bezpieczeństwa przy użyciu tych systemów.

vi. Celem niniejszego ESARR-u jest dostarczenie organom wydającym przepisy oraz organom zarządzania ruchem lotniczym jednolitego zestawu wymagań w zakresie przepisów bezpieczeństwa dla wykorzystania oprogramowania w systemach ATM.

C. CELE BEZPIECZEŃSTWA

i. Głównym celem bezpieczeństwa systemów ATM w zakresie oprogramowania jest ograniczenia ryzyka związanego z wykorzystaniem oprogramowania ATM do dopuszczalnego poziomu.

PRZEPISY OBOWIĄZKOWE

1. OGÓLNE WYMAGANIA BEZPIECZEŃSTWA

1.1. W ramach Systemu Zarządzania Bezpieczeństwem i działań w zakresie oceny i ograniczania ryzyka, organ zarządzania ruchem lotniczym powinien zdefiniować i wdrożyć system zapewniania bezpieczeństwa oprogramowania, włączając w to wszystkie działania operacyjne na oprogramowaniu, takie jak szybkie przejście czy zamiana urządzeń w czasie pracy.

1.2. Organ zarządzania ruchem lotniczym powinien zagwarantować w ramach systemu zapewnienia bezpieczeństwa oprogramowania, co najmniej że:

a) wymagania dla oprogramowania są określone prawidłowo w zakresie spełniania celów i wymagań bezpieczeństwa, zgodnie z wynikami oceny i ograniczania ryzyka,

b) wszystkie wymagania dla oprogramowania są możliwe do prześledzenia;

c) wdrożenie oprogramowania nie zawiera funkcji, które niekorzystnie wpływają na bezpieczeństwo,

d) oprogramowanie ATM spełnia wymagania z poziomem ufności odpowiadającym stopniowi krytyczności oprogramowania.

e) gwarancje spełnienia powyższych ogólnych wymagań bezpieczeństwa oraz ich dowody wynikają zawsze z następujących źródeł:

i. znanej wersji wykonawczej oprogramowania,

ii. znanego zakresu danych konfiguracyjnych,

iii. znanego zestawu programów i ich opisów (włącznie ze specyfikacjami), użytych w produkcji aktualnej wersji oprogramowania.

1.3. Organ zarządzania ruchem lotniczym powinien zapewnić upoważnione władze państwowe, że spełnione zostały wymagania zawarte w punkcie 1.2.

2. WYMAGANIA DOTYCZĄCE SYSTEMU ZAPEWNIENIA BEZPIECZEŃSTWA OPROGRAMOWANIA

Organ zarządzania ruchem lotniczym powinien zagwarantować co najmniej, że system zapewniania bezpieczeństwa oprogramowania:

2.1. Jest udokumentowany i stanowi część ogólnej dokumentacji dotyczącej oceny i ograniczania ryzyka w systemie ATM.

2.2. Przydziela poziomy gwarantowania oprogramowania (poziomy SWAL – „*Software Assurance Levels*") całemu oprogramowaniu operacyjnemu ATM.

2.3. Zawiera gwarancje:

a) weryfikacji wymagań dla oprogramowania,

b) weryfikacji oprogramowania,

c) zarządzania konfiguracją oprogramowania,

d) śledzenia wymagań dla oprogramowania.

2.4. Określa dokładność, z jaką mają być ustanawiane powyższe gwarancje. Dokładność powinna być określana dla każdego z poziomów gwarantowania oprogramowania i wzrastać wraz ze wzrostem poziomu krytyczności oprogramowania. W tym celu:

a) dokładności zapewniania bezpieczeństwa, w zależności od poziomu gwarantowania oprogramowania, powinny być zróżnicowane pod względem:

i. kryteriów wymaganych do niezależnego osiągnięcia,

ii. kryteriów wymaganych do osiągnięcia,

iii. kryteriów nie wymaganych,

b) zapewnienia odpowiadające każdemu z poziomów gwarantowania oprogramowania powinny dawać dostateczną pewność, że oprogramowanie ATM może być używane z dopuszczalnym bezpieczeństwem.

2.5. Dostarcza zwrotnych informacji wynikających z doświadczeń uzyskiwanych podczas użytkowania oprogramowania ATM w celu potwierdzenia, że system zapewniania bezpieczeństwa oprogramowania i ustanowione poziomy gwarantowania oprogramowania są właściwe. W tym celu skutki każdej usterki oprogramowania oraz nieprawidłowości pojawiające się w trakcie pracy operacyjnej powinny być zgłaszane zgodnie z ESARR 2 i oceniane na zasadach opisanych w ESARR 4.

2.6. Zapewnia ten sam poziom poufności, jak poziom gwarantowania oprogramowania - zarówno dla oprogramowania projektowanego na zamówienie, jak i dla oprogramowania gotowego (COTS), poprzez zastosowanie dowolnych metod, uzgodnionych z upoważnionymi władzami państwowymi.

3. WYMAGANIA STOSOWANE DLA POZIOMÓW GWARANTOWANIA OPROGRAMOWANIA

Organ zarządzania ruchem lotniczym, w ramach systemu zapewnienia bezpieczeństwa oprogramowania, powinien zagwarantować co najmniej, że:

3.1. Poziomy gwarantowania oprogramowania odpowiadają dokładnościom wymaganym przez stopień krytyczności oprogramowania ATM, z zastosowaniem schematu klasyfikacji klas zagrożeń zawartych w ESARR 4, połączonego z prawdopodobieństwem zaistnienia określonych zdarzeń. Powinny zostać określone przynajmniej cztery poziomy gwarantowania oprogramowania, przy czym poziom 1 jest najbardziej krytyczny.

3.2. Przydzielony poziom gwarantowania oprogramowania powinien być współmierny do najpoważniejszego skutku, jaki może wywołać usterka oprogramowania lub kombinacja kilku usterek oprogramowania, zgodnie z ESARR 4. Uwzględniane powinno być również ryzyko towarzyszące usterkom oprogramowania łącznie ze zidentyfikowaną ochroną poprzez architekturę systemową lub procedury.

3.3. Składnikom oprogramowania ATM, których nie można od siebie oddzielić, powinien zostać przydzielony poziom gwarantowania oprogramowania odpowiadający najbardziej krytycznemu z tych składników.

4. WYMAGANIA DOTYCZĄCE ZAPEWNIANIA WERYFIKACJI WYMAGAŃ DLA OPROGRAMOWANIA

Organ zarządzania ruchem lotniczym powinien zagwarantować, w ramach systemu zapewnienia bezpieczeństwa oprogramowania co najmniej, że wymagania dla oprogramowania:

4.1. Określają zachowanie funkcjonalne (w trybie nominalnym i zdegradowanym) oprogramowania ATM, wydajność czasową, wydajność ogólną, dokładność, wykorzystanie zasobów docelowej platformy sprzętowej, odporność na nietypowe warunki operacyjne oraz tolerancję na przeciążenie.

4.2. Są kompletne i poprawne oraz wypełniają wymagania bezpieczeństwa systemowego.

5. WYMAGANIA STOSOWANE DLA ZAPEWNIENIA WERYFIKACJI OPROGRAMOWANIA

Organ zarządzania ruchem lotniczym, w ramach systemu zapewnienia bezpieczeństwa oprogramowania, powinien zagwarantować co najmniej, że:

5.1. Zachowanie funkcjonalne oprogramowania ATM, wydajność czasowa, wydajność ogólna, dokładność, wykorzystanie zasobów docelowej platformy sprzętowej, odporność na typowe warunki operacyjne oraz tolerancja na przeciążenie spełniają postawione wymagania dla oprogramowania.

5.2. Oprogramowanie ATM jest odpowiednio sprawdzane poprzez analizę lub testowanie lub poprzez równoważne metody, na podstawie uzgodnień z upoważnioną władzą państwową.

5.3. Weryfikacja oprogramowania jest poprawna i kompletna.

6. WYMAGANIA DOTYCZĄCE ZAPEWNIENIA ZARZĄDZANIA KONFIGURACJĄ OPROGRAMOWANIA

Organ zarządzania ruchem lotniczym, w ramach systemu zapewnienia bezpieczeństwa oprogramowania, powinien zagwarantować co najmniej, że:

6.1. W konfigurowaniu oprogramowania ATM stosowana jest rejestracja i śledzenie zmian, udowadniające, że dane o cyklu użytkowania oprogramowania pozostają pod kontrolą przez cały ten okres.

6.2. Raporty o problemach związanych z tym oprogramowaniem, zagrażające bezpieczeństwu, a także ich śledzenie oraz działania naprawcze są prowadzone w sposób udowadniający ich ograniczanie.

6.3. Wdrożone zostały procedury pozyskiwania informacji, umożliwiające odtwarzanie i przedstawianie danych cyklu życia oprogramowania przez cały okres jego istnienia.

7. WYMAGANIA DOTYCZĄCE ZAPEWNIENIA ŚLEDZENIA WYMAGAŃ OPROGRAMOWANIA

Organ zarządzania ruchem lotniczym, w ramach systemu zapewnienia bezpieczeństwa oprogramowania, powinien zagwarantować co najmniej, że:

7.1. Każde z wymagań dla oprogramowania jest prześledzone do tego samego poziomu projektowego, na którym wykazane zostaje jego spełnienie.

7.2. Każde z wymagań dla oprogramowania, na każdym poziomie projektowym, na którym wykazane zostaje jego spełnienie, jest prześledzone, aż do wymagania systemowego.

8. ZASTOSOWANIE

8.1. Niniejsze przepisy bezpieczeństwa stosuje się do cywilnych i wojskowych organów zarządzania ruchem lotniczym, ponoszących odpowiedzialność za zarządzanie bezpieczeństwem w naziemnych systemach ATM i w innych naziemnych systemach wspierających (włącznie z CNS), które pozostają pod ich zarządem.

8.2. Systemy zapewniania bezpieczeństwa oprogramowania, funkcjonujące już w odniesieniu do systemów ATM, pozostających pod bezpośrednim zarządem wojskowym, mogą zostać zaakceptowane pod warunkiem, że są zgodne z postanowieniami obowiązkowymi ESARR 6.

8.3. Przepisy obowiązkowe niniejszych wymagań ESARR powinny zostać wprowadzone co najmniej jako wymagania regulacyjne upoważnionej władzy państwowej, odpowiedzialnej za wydawanie przepisów.

9. TERMIN WPROWADZENIA

9.1. Wymagania ESARR 6 należy wprowadzić w okresie 3 lat od zaakceptowania ich przez EUROCONTROL.

10. WYJĄTKI

Brak

11. DEFINICJE

11.1.1. Definicje terminów używanych w dokumentach ESARR są podane w Słowniku określeń i definicji na potrzeby ESARR.