

RÈGLEMENT (CE) N° 482/2008 DE LA COMMISSION

du 30 mai 2008

établissant un système d'assurance de la sécurité des logiciels à mettre en œuvre par les prestataires de services de navigation aérienne et modifiant l'annexe II du règlement (CE) n° 2096/2005

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION DES COMMUNAUTÉS EUROPÉENNES,

gestion du trafic aérien («logiciels EATMN») ont été réduits à un niveau tolérable.

vu le traité instituant la Communauté européenne,

vu le règlement (CE) n° 550/2004 du Parlement européen et du Conseil du 10 mars 2004 relatif à la fourniture de services de navigation aérienne dans le ciel unique européen («règlement sur la fourniture de services») ⁽¹⁾, et notamment son article 4,

(5) Le présent règlement ne doit pas s'appliquer aux opérations et à l'entraînement militaires visés à l'article 1^{er}, paragraphe 2, du règlement (CE) n° 549/2004 du Parlement européen et du Conseil du 10 mars 2004 fixant le cadre pour la réalisation du ciel unique européen («règlement-cadre») ⁽³⁾.

considérant ce qui suit:

(6) Il y a donc lieu de modifier l'annexe II du règlement (CE) n° 2096/2005 en conséquence.

(1) En vertu du règlement (CE) n° 550/2004, la Commission est tenue d'identifier et d'adopter les dispositions pertinentes des exigences réglementaires de sécurité d'Eurocontrol («ESARR»), compte tenu de la législation communautaire existante. L'ESARR 6, intitulée «Logiciels des systèmes ATM», constitue un ensemble d'exigences réglementaires de sécurité pour la mise en œuvre d'un système d'assurance de la sécurité des logiciels.

(7) Les mesures prévues au présent règlement sont conformes à l'avis du comité du ciel unique,

A ARRÊTÉ LE PRÉSENT RÈGLEMENT:

*Article premier***Objet et champ d'application**

(2) Le règlement (CE) n° 2096/2005 de la Commission du 20 décembre 2005 établissant les exigences communes pour la fourniture de services de navigation aérienne ⁽²⁾ dispose, à la dernière phrase de son considérant 12, que «les dispositions pertinentes de l'exigence ESARR 1 concernant la supervision de la sécurité dans le domaine GTA et de l'exigence ESARR 6 sur les logiciels des systèmes GTA doivent être identifiées et adoptées dans le cadre d'autres actes communautaires».

1. Le présent règlement établit les exigences applicables à la définition et à la mise en œuvre d'un système d'assurance de la sécurité des logiciels par les prestataires de services de la circulation aérienne (ATS), par les entités assurant la gestion des courants de trafic aérien (ATFM) et la gestion de l'espace aérien (ASM) pour la circulation aérienne générale, ainsi que par les prestataires de services de communication, de navigation et de surveillance (CNS).

(3) L'annexe II du règlement (CE) n° 2096/2005 impose aux prestataires de services de la circulation aérienne de mettre en œuvre un système de gestion de la sécurité, ainsi que des exigences de sécurité concernant l'évaluation et l'atténuation des risques pour tout changement. Au sein de son système de gestion de la sécurité et dans le cadre de ses activités d'évaluation et d'atténuation des risques pour tout changement, le prestataire de services de la circulation aérienne doit définir et mettre en œuvre un système d'assurance de la sécurité des logiciels portant spécifiquement sur les aspects logiciels.

Il identifie et adopte les dispositions obligatoires de l'exigence réglementaire de sécurité d'Eurocontrol — ESARR 6 — intitulée «Logiciels des systèmes ATM», publiée le 6 novembre 2003.

2. Le présent règlement s'applique aux nouveaux logiciels et à toute modification apportée aux logiciels des systèmes ATS, ASM, ATFM et CNS.

Il ne s'applique pas aux logiciels des composants embarqués, ni aux équipements spatiaux.

*Article 2***Définitions**

Aux fins du présent règlement, les définitions énoncées à l'article 2 du règlement (CE) n° 549/2004 s'appliquent.

⁽¹⁾ JO L 96 du 31.3.2004, p. 10.

⁽²⁾ JO L 335 du 21.12.2005, p. 13. Règlement modifié par le règlement (CE) n° 1315/2007 (JO L 291 du 9.11.2007, p. 16).

⁽³⁾ JO L 96 du 31.3.2004, p. 1.

On entend également par:

- 1) «logiciels»: les programmes informatiques et les données de configuration correspondantes, y compris les logiciels pré-développés, à l'exclusion des éléments électroniques tels que les circuits intégrés spécifiques d'une application, les réseaux de portes programmables ou les dispositifs de contrôle de logique sur support physique;
- 2) «données de configuration»: des données permettant de configurer un système logiciel générique pour un cas particulier d'utilisation;
- 3) «logiciel pré-développé»: un logiciel non développé spécifiquement pour le contrat considéré;
- 4) «assurance de la sécurité»: toutes les actions planifiées et systématiques nécessaires pour donner l'assurance requise qu'un produit, un service, une organisation ou un système fonctionnel atteint un seuil de sécurité acceptable ou tolérable;
- 5) «organisation»: tout prestataire de services de la circulation aérienne (ATS), tout prestataire de services de communication, de navigation et de surveillance (CNS) ou toute entité assurant la gestion des courants de trafic aérien (ATFM) ou la gestion de l'espace aérien (ASM);
- 6) «système fonctionnel»: une combinaison de systèmes, de procédures et de ressources humaines organisée afin de remplir une fonction dans le contexte de la gestion du trafic aérien (ATM);
- 7) «risque»: la combinaison de la probabilité la plus élevée ou de la fréquence d'un événement aux conséquences dommageables provoqué par un danger et de la gravité de ces conséquences;
- 8) «danger»: toute condition, tout événement ou toute circonstance qui pourrait provoquer un accident;
- 9) «nouveau logiciel»: un logiciel qui a été commandé, ou pour lequel des contrats ont été signés, après l'entrée en vigueur du présent règlement;
- 10) «objectif de sécurité»: une déclaration qualitative ou quantitative définissant la fréquence ou la probabilité maximales auxquelles un danger pourrait se produire;
- 11) «exigences de sécurité»: des moyens de diminuer un risque tels que définis par la stratégie de diminution des risques permettant d'atteindre un objectif de sécurité particulier, y compris les exigences organisationnelles, opérationnelles, procédurales, fonctionnelles, de performance, les exigences d'interopérabilité ou les caractéristiques environnementales;
- 12) «basculement ou remplacement à chaud»: le remplacement d'un composant ou d'un logiciel du système du réseau européen de gestion du trafic aérien (EATMN) pendant que le système est opérationnel;
- 13) «exigence de sécurité d'un logiciel»: une description de ce qui doit être produit par un logiciel, compte tenu des entrées et des contraintes, dont le respect assure que le logiciel EATMN répond aux impératifs de sécurité et aux exigences opérationnelles;
- 14) «logiciel EATMN»: un logiciel utilisé dans les systèmes du réseau EATMN visés à l'article 1^{er};
- 15) «validité des exigences»: la confirmation, par examen et apport de preuves objectives, que les exigences particulières pour un usage spécifique sont celles prévues;
- 16) «effectué de manière indépendante»: pour les activités du processus de vérification du logiciel, lorsque l'activité de vérification est réalisée par une (ou des) personne(s) différente(s) du responsable du développement de l'élément à vérifier;
- 17) «défaillance d'un logiciel»: l'incapacité d'un programme à exécuter correctement une fonction requise;
- 18) «panne d'un logiciel»: l'incapacité d'un programme à exécuter une fonction requise;
- 19) «COTS»: une application disponible dans le commerce, vendue sur catalogues publics et non destinée à être personnalisée ou améliorée;
- 20) «composants logiciels»: des sous-ensembles pouvant être intégrés ou connectés à d'autres sous-ensembles logiciels réutilisables, afin de les combiner et de créer une application logicielle sur mesure;
- 21) «composants logiciels indépendants»: des composants logiciels qui ne sont pas rendus inopérants par le dysfonctionnement à l'origine du danger;
- 22) «temps de réponse d'un logiciel»: le temps mis par un logiciel pour réagir à des saisies particulières ou à des événements périodiques, ou la performance d'un logiciel en termes de transactions ou de messages traités par unité de temps;
- 23) «capacité d'un logiciel»: l'aptitude d'un logiciel à traiter un volume particulier de flux de données;
- 24) «précision»: la précision requise pour les résultats obtenus par un traitement logiciel;
- 25) «consommation des ressources»: la quantité de ressources au sein du système informatique pouvant être utilisées par l'application logicielle;

- 26) «robustesse d'un logiciel»: le comportement d'un logiciel en cas de saisies de données imprévues, de défaillances matérielles ou d'interruption de l'alimentation électrique, dans le système informatique lui-même ou dans les dispositifs connectés;
- 27) «tolérance à la surcharge»: le comportement du système, et notamment sa tolérance, lorsque la quantité de données en entrée est supérieure à celle prévue pendant le fonctionnement normal du système;
- 28) «vérification correcte et complète d'un logiciel EATMN»: le cas où toutes les exigences de sécurité d'un logiciel énoncent correctement les exigences applicables au composant logiciel en vertu du processus d'évaluation et d'atténuation des risques, et où leur mise en œuvre est démontrée au niveau requis par le niveau d'assurance logicielle;
- 29) «données du cycle de vie d'un logiciel»: les données produites pendant le cycle de vie d'un logiciel pour planifier, diriger, expliquer, définir, enregistrer ou prouver des activités; ces données rendent possible l'approbation du processus de cycle de vie du logiciel, du système ou des équipements ainsi que des modifications apportées au produit logiciel après son approbation;
- 30) «cycle de vie d'un logiciel»:
- a) l'ensemble organisé de processus qu'une organisation juge suffisant et adéquat pour produire un produit logiciel;
 - b) le délai compris entre la décision de produire ou de modifier un produit logiciel et le moment où ce produit est retiré du service;
- 31) «exigence de sécurité applicable au système»: l'exigence de sécurité applicable à un système fonctionnel.
- a) les exigences de sécurité des logiciels énoncent correctement les critères auxquels doivent répondre les logiciels pour être conformes aux objectifs et aux exigences de sécurité, tels qu'ils sont définis dans le processus d'évaluation et d'atténuation des risques;
 - b) la traçabilité de toutes les exigences de sécurité des logiciels est assurée;
 - c) la mise en œuvre des logiciels ne comporte aucune fonction nuisant à la sécurité;
 - d) les logiciels EATMN satisfont aux exigences qui leur sont applicables avec un niveau de confiance cohérent avec la criticité des logiciels;
 - e) des assurances sont fournies, confirmant le respect des exigences générales de sécurité énoncées aux points a) à d), et les arguments qui démontrent l'assurance requise reposent, en tout temps, sur:
 - i) une version exécutable connue des logiciels;
 - ii) un ensemble connu de données de configuration;
 - iii) un ensemble connu de produits logiciels et de descriptions de logiciel, notamment les spécifications, utilisés dans la production de la version considérée.
3. L'organisation met à la disposition de l'autorité de surveillance nationale les assurances requises démontrant le respect des exigences prévues au paragraphe 2.

Article 3

Exigences de sécurité générales

1. Lorsqu'une organisation doit mettre en œuvre un processus d'évaluation et d'atténuation des risques en vertu du droit communautaire ou national applicable, elle définit et met en œuvre un système d'assurance de la sécurité des logiciels portant spécifiquement sur les aspects liés aux logiciels EATMN, y compris l'ensemble des modifications opérationnelles apportées en ligne, et notamment les basculements opérationnels ou les remplacements à chaud.

2. L'organisation veille, au minimum, à ce que son système d'assurance de la sécurité des logiciels produise des preuves et des arguments qui démontrent que:

Article 4

Exigences applicables au système d'assurance de la sécurité des logiciels

L'organisation veille, au minimum, à ce que le système d'assurance de la sécurité des logiciels:

- 1) soit documenté, en particulier dans le cadre de la documentation globale relative à l'évaluation et à l'atténuation des risques;
- 2) attribue des niveaux d'assurance logicielle à tous les logiciels EATMN opérationnels conformément aux exigences énoncées à l'annexe I;
- 3) offre des assurances quant à:
 - a) la validité des exigences de sécurité des logiciels, conformément aux exigences énoncées à l'annexe II, partie A;
 - b) la vérification des logiciels, conformément aux exigences énoncées à l'annexe II, partie B;

- c) la gestion de la configuration des logiciels, conformément aux exigences énoncées à l'annexe II, partie C;
- d) la traçabilité des exigences de sécurité des logiciels, conformément aux exigences énoncées à l'annexe II, partie D.
- 4) précise la rigueur d'établissement des assurances; la rigueur doit être précisée pour chaque niveau d'assurance logicielle et doit augmenter avec la criticité du logiciel; à cette fin:
- a) les degrés de rigueur pour l'établissement des assurances, par niveau d'assurance logicielle, doivent être les suivants:
- i) à effectuer de manière indépendante;
- ii) à effectuer;
- iii) non obligatoire;
- b) les assurances correspondant à chaque niveau d'assurance logicielle doivent indiquer avec suffisamment de confiance que le logiciel EATMN peut être exploité dans des conditions tolérables de sécurité;
- 5) exploite les retours d'expérience des utilisateurs de logiciels EATMN pour confirmer le caractère adéquat du système d'assurance de la sécurité des logiciels et des niveaux d'assurance attribués. Dans cette optique, les incidences de toute défaillance ou panne logicielle, signalées conformément aux exigences concernant la notification et l'analyse des événements liés à la sécurité, sont évaluées par rapport aux incidences identifiées pour le système concerné conformément au mécanisme de classification du degré de gravité établi au point 3.2.4 de l'annexe II du règlement (CE) n° 2096/2005.

Article 5

Exigences applicables aux modifications de logiciels ou à des types particuliers de logiciels

1. Pour toute modification de logiciel ou pour des types particuliers de logiciels comme les COTS, les logiciels pré-développés ou les logiciels réutilisés pour lesquels certaines des exigences énoncées à l'article 3, paragraphe 2, points d) ou e), ou à l'article 4, points 2) à 5), ne peuvent être appliquées, l'organisation veille à ce que le système d'assurance de la sécurité des logiciels offre, par tout autre moyen choisi en accord avec l'autorité de surveillance nationale, le même niveau de

confiance que le niveau d'assurance logicielle pertinent éventuellement défini.

Ces moyens doivent indiquer avec suffisamment de confiance que le logiciel respecte les objectifs et les exigences de sécurité identifiés par le processus d'évaluation et d'atténuation des risques pour la sécurité.

2. Pour évaluer les moyens visés au paragraphe 1, l'autorité de surveillance nationale peut faire appel à un organisme agréé ou à un organisme notifié.

Article 6

Modification du règlement (CE) n° 2096/2005

À l'annexe II du règlement (CE) n° 2096/2005, la section suivante est ajoutée:

«3.2.5 section 5

Système d'assurance de la sécurité des logiciels

Dans le cadre de l'application du système de management de la sécurité, le prestataire de services de la circulation aérienne met en œuvre un système d'assurance de la sécurité des logiciels conformément au règlement (CE) n° 482/2008 de la Commission du 30 mai 2008 établissant un système d'assurance de la sécurité des logiciels à mettre en œuvre par les prestataires de services de navigation aérienne et modifiant l'annexe II du règlement (CE) n° 2096/2005 (*).

(*) JO L 141 du 31.5.2008, p. 5.»

Article 7

Entrée en vigueur

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Il s'applique à partir du 1^{er} janvier 2009 aux nouveaux logiciels des systèmes du réseau EATMN visés à l'article 1^{er}, paragraphe 2, premier alinéa.

Il s'applique à partir du 1^{er} juillet 2010 à toutes les modifications apportées aux logiciels des systèmes du réseau EATMN visés à l'article 1^{er}, paragraphe 2, premier alinéa, qui sont opérationnels à cette date.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 30 mai 2008.

Par la Commission

Antonio TAJANI

Membre de la Commission

ANNEXE I

Exigences applicables au niveau d'assurance logicielle visé à l'article 4, point 2)

1. Le niveau d'assurance logicielle met en rapport la rigueur des assurances logicielles et la criticité d'un logiciel EATMN, en utilisant le mécanisme de classification du degré de gravité établi à l'annexe II, point 3.2.4, section 4, du règlement (CE) n° 2096/2005, et la probabilité d'une incidence négative donnée. Un minimum de quatre niveaux d'assurance logicielle doit être fixé, le niveau 1 désignant le niveau le plus critique.
 2. Le niveau d'assurance logicielle attribué est déterminé au regard de l'incidence la plus grave qu'une défaillance ou une panne peut entraîner, conformément à l'annexe II, point 3.2.4, section 4, du règlement (CE) n° 2096/2005. Ce niveau doit en particulier tenir compte des risques associés aux défaillances ou aux pannes de logiciel, et des défenses architecturales ou procédurales recensées.
 3. Le niveau d'assurance logicielle du plus critique des composants dépendants doit être attribué aux composants logiciels EATMN dont l'indépendance ne peut être prouvée.
-

ANNEXE II

Partie A: exigences applicables aux assurances de validité des exigences de sécurité des logiciels visées à l'article 4, point 3 a)

1. Les exigences de sécurité des logiciels précisent le comportement fonctionnel, en modes nominal et dégradé, des logiciels EATMN ainsi que, selon les besoins, leurs temps de réponse, leur capacité, leur précision, leur consommation des ressources sur le matériel cible, leur robustesse en conditions anormales d'exploitation et leur tolérance à la surcharge.
2. Les exigences de sécurité des logiciels sont complètes et correctes, et conformes aux exigences de sécurité applicables au système.

Partie B: exigences applicables aux assurances de vérification des logiciels visées à l'article 4, point 3 b)

1. Le comportement fonctionnel des logiciels EATMN, leurs temps de réponse, leur capacité, leur précision, leur consommation des ressources sur le matériel cible, leur robustesse en conditions anormales d'exploitation et leur tolérance à la surcharge sont conformes aux exigences logicielles.
2. Les logiciels EATMN sont vérifiés de manière adéquate, par des analyses, des essais ou des moyens équivalents, comme convenu avec l'autorité de supervision nationale.
3. La vérification des logiciels EATMN est correcte et complète.

Partie C: exigences applicables aux assurances de gestion de la configuration des logiciels visées à l'article 4, point 3 c)

1. Il existe des procédures d'identification de la configuration, de traçabilité et d'enregistrement du statut de la configuration, qui permettent de prouver que les données du cycle de vie des logiciels sont soumises à un contrôle de configuration tout au long du cycle de vie des logiciels EATMN.
2. Il existe, pour les problèmes, des procédures de notification, de suivi, et de détermination des actions correctives nécessaires permettant de prouver que les problèmes de sécurité liés aux logiciels ont été atténués.
3. Il existe des procédures de restauration et de mise à disposition permettant de régénérer et de restituer les données du cycle de vie des logiciels tout au long du cycle de vie des logiciels EATMN.

Partie D: exigences applicables aux assurances de traçabilité des exigences de sécurité des logiciels visées à l'article 4, point 3 d)

1. La traçabilité de chaque exigence de sécurité des logiciels est rattachée au niveau de conception qu'elle doit satisfaire.
 2. La traçabilité de chaque exigence de sécurité des logiciels est rattachée, pour chaque niveau de conception qu'elle doit satisfaire, à une exigence de sécurité applicable au système.
-