dgac

STAC

Journée Technique 2011

Sécurité des logiciels ATM versus certification des logiciels embarqués

Pantxoa AMORENA DGA-TA

Frédéric LE TENNIER STAC

DGA

Présent pour l'avenir

Ressources, territoires et habitats
Énergie et climat
Développement durable
Prévention des risques
Infrastructures, transports et mer

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Écologie, du Développement durable, des Transports et du Logement

Plan de la présentation

Logiciels embarqués :
à bord des aéronefs

Logiciels ATM :
systèmes de contrôle aérien

- Comparatif sur les aspects :
  - Historique des normes et règlements
  - Historique comparé des technologies et des normes/règlements
  - Principes d'évaluation de la sécurité des logiciels
  - Caractéristiques des logiciels
  - Criticité des logiciels
  - Principes de surveillance par les autorités

Historique des normes et règlements

DO-178
ED-12
(1982)

DO-178A
ED-12A
(1985)

DO-178B
ED-12B
(1992)

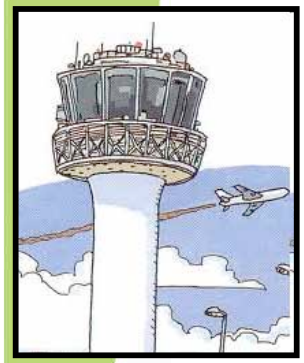
DO-178C
ED-12C
(2011…)

FAR 25
(1965)

JAR 25
(1990)

CS 25
(2003)

1970 1980 1990 2000 2010



ESARR 4
(2001)

CE Ciel Unique
(2004)

ESARR 6
(2003)

CE 482/2008
(2008)

DO-278B
ED-109
(2002)

ED-153
(2009)

Historique technologies vs normes & règlementation

DO-178A ED-12A (1985)

DO-178B ED-12B (1992)

DO-178C ED-12C (2011…)

A320 1988

A330, A340 1993-1994

A380 2007

1970 1980 1990 2000 2010

CAUTRA 1 1961-65 CAUTRA 2 1966-72	CAUTRA 3 1973-1985	CAUTRA 4 1985-...

DO-278B ED-109 (2002)

CE 482/2008 (2008)

Principes d'évaluation

- Principes identiques : **assurance logicielle**
  - Pas d'évaluation quantitative de « taux de défaillance »
  - Approche qualitative, confiance dans les processus de développement
  - Niveau de rigueur, de confiance (« **Assurance Level** ») : DAL, AL, SWAL…
- Mais systèmes sensiblement différents : problématiques différentes (cf. planche suivante)

Caractéristiques techniques

Caractéristiques	Embarqué	ATM
Logiciels COTS	En nombre limité, produits aéro avec kit de certification	Très nombreux, y compris « grand public »
Logiciels « Legacy »	Existent, mais pas la règle parce que démonstration difficile	Essentiel des logiciels, pas de preuves selon normes AL
Taille des logiciels	Souvent entre 10.000 à 100.000 lignes. Voire 300.000 lignes pour gestion moteur à 1 million pour le flight management	400.000 lignes pour cœur du traitement PdV, 200.000 pour le cœur traitement radar (hors poursuite), plus de 800.000 pour la visu radar
Nombre de logiciels	Une centaine, regroupés dans un aéronef	Plusieurs centaines, répartis sur toute la France (métro, DOM/TOM)
Paramétrables	Possible, mais généralement sur un nombre limité de paramètres pour l'exploitant	Hautement paramétrables, par fournisseur, exploitant
Cycle de vie à gérer pour l'Assurance Logicielle	Réalisation (« certificat de type » d'avion) Par « modifications », par « type aéronef »	Réalisation, mais aussi « exploitation/utilisation » Evolutions plus nombreuses, plus rapides, en « continu »
Gestion des transitions	Peuvent se faire avion « au sol »	Système H24

Criticités

- Embarqué : des logiciels très critiques
  - Défaillance peut entrainer la perte de l'aéronef
- ATM : des logiciels critiques, mais
  - Par nature, les fonctions ATM sont moins critiques (N'entrainent pas directement la perte de l'aéronef)
  - L'humain est presque toujours « dans la boucle »

Maintenance

Flight mngt

Radio mngt

Ctrl moteur

Cmd de vol

DAL D DAL C DAL B DAL A

SWAL 4 SWAL 3 SWAL 2 SWAL 1

Plans de vol

Radio

Visu. & traitt Radar

Surveillance par les autorités (France)

	Embarqué	ATM
Autorité	EASA	Autorités Nationales de Surveillance (ANS)
Entité surveillée	Constructeur	Prestataire de Service de Navigation Aérienne (PSNA)
Type de décision	Certification de type de l'aéronef	Acceptation de mise en service d'un changement
Mode de surveillance lors des phases du cycle de vie du logiciel		
Planification	Revue des documents de planification	Revue des documents de planification
Réalisation	Audit (inspection sur place, etc.)	Revue des documents (provisoires) de l'étude de sécurité, au fur et à mesure
Fin de réalisation	Revue finale : bilan de l'audit, de l'engagement de l'industriel	Revue des documents de « l'étude de sécurité » finale, dont l'engagement du PSNA
Exploitation, utilisation		Audits du PSNA (niveau « SMS »), dans le cadre de la surveillance continue

Le futur

Embarqué

De nouveaux enjeux, avec des logiciels de plus en plus complexes, plus d'informatique, plus d'afficheurs, etc.

Evolution de la DO-178 (DO-178C):
- OOT, Model-based…
- IMA: Integrated Modular Avionics
- ADN: Avionic Data Networks

ATM

Mise en commun, interopérabilité des systèmes entre Prestataires de Service de Navigation Aérienne : FAB (Functional Airspace Blocks), développements en coopération

Implication de l'EASA : nouveau corpus règlementaire, surveillance des systèmes pan-européens…

SESAR : nouveaux concepts opérationnels, nouvelle répartition sol/bord pour les fonctions ATM, systèmes encore plus complexes…

Merci de votre attention

Frédéric Le Tennier
STAC/SINA/NA
frederic.le-tennier@aviation-civile.gouv.fr

Pantxoa Amorena
DGA-TA
pantxoa.amorena@dga.defense.gouv.fr