



*R*éseau
d' *I*ngénierie
de la *S*ûreté de fonctionnement

Atelier Thématique

Justification de sûreté de fonctionnement
(*dependability case*) : approches industrielles,
méthodes de construction et structures

Mardi 18 mars 2002 - LAAS-CNRS, Toulouse

Constat et objectifs

- Les approches suivies pour justifier la sûreté de fonctionnement d'un système en vue d'une licence d'exploitation ou d'une certification sont diverses, souvent empiriques, coûteuses et peu efficaces.
- Buts de l'atelier
 - ✓ comparer les diverses pratiques, référentiels et approches utilisées :
 - démonstration de conformité avec des standards, avec des guides de sûreté, des niveaux de risques acceptables;
 - démonstration de propriétés, de réalisation de critères de conception
 - démonstration d'objectifs de sûreté à atteindre (claims).
 - ✓ dégager des pistes pour rendre la démonstration de sûreté et la collecte des éléments de preuve (« evidence ») plus efficace.
- Divers points de vue à examiner : constructeur, exploitant, régulateur, certificateur,...

Programme

9h15 - 9h20	<i>Introduction et présentation de l'atelier</i>	M. Kaâniche (LAAS-CNRS)
9h20 - 10h00	<i>Sûreté de fonctionnement : point de vue du régulateur sur les concepts, modèles et méthodes de démonstration</i>	P-J. Courtois (AVN)
10h00 - 10h40	<i>Le Do-178B : logique, historique, contenu et application</i>	G. Ladier (Airbus France)
10h40 - 11h10	<i>Pause</i>	
11h10 - 11h50	<i>Justification de sûreté de fonctionnement des logiciels spatiaux : évolution vers la certification</i>	J-P. Blanquart, J-F. Muller (Astrium)
11h50 - 12h30	<i>GALILEO : Software classification methodology and standardisation</i>	V. Magnier (ESA)
12h30 - 13h45	<i>Buffet</i>	
13h45 - 14h25	<i>Processus d'étude de sécurité pour la certification du système de protection HGV de signalisation ferroviaire</i>	V. LaLumia (Technicatome)
14h25 - 15h05	<i>Intégration des justificatifs de sécurité (safety case) dans une démarche globale de mise en service</i>	Y. Garnier (SNCF)
15h05 - 15h30	<i>Composants COTS et sûreté de fonctionnement</i>	J. Arlat (LAAS-CNRS)
15h30 - 16h	<i>Pause</i>	
16h - 17h	<i>Synthèse et conclusions</i>	