Conception des systèmes critiques : un savoir-faire pour vos marchés de demain.
Référentiel, méthodes et bonnes pratiques

Mardi 1er Octobre 2013
de 9h00 à 16h30
au Pôle PEGASE (Aix en Provence)

Les équipements intégrant des composants matériels et logiciels sont devenus incontournables dans de nombreux secteurs industriels : aéronautique, ferroviaire, énergie, médical… .
Les applications qui exploitent ces équipements sont complexes et souvent critiques, leurs défaillances pouvant entrainer de lourdes pertes en termes humains et économiques.
Concevoir un système critique avec les meilleures pratiques en vigueur est un élément différenciant et souvent obligatoire pour développer ses marchés en forte croissance.

Ce séminaire CAP'TRONIC – Pôle PEGASE propose un panorama des méthodes et outils pour améliorer la fiabilité des systèmes embarqués et assurer un niveau de sureté de fonctionnement maximal.

Lors de cette journée, les thèmes suivants seront abordés par des experts du domaine :
- Grandes familles de normes applicables aux systèmes critiques
- Outils de conception (méthodes formelles, analyseur de code…)
- Prise en compte du facteur humain dans ces types d'applications

Cette journée sera ponctuée de témoignages d'entreprises.

PROGRAMME

8:45 **Accueil**

9:00 **Sûreté de Fonctionnement des systèmes critiques : État des lieux et évolutions récentes** – ***Michel Dufresne, SERMA***
Intervention permettant de présenter une vision de l'embarqué critique dans l'industrie : les domaines, les enjeux, les grandes familles de normes et les implications en terme de méthodes, outils, briques pour l'industrie.

9:20 **La norme DO 178** – ***Julien Munerot, ERASM***
L'accroissement rapide de l'utilisation de logiciels dans les systèmes critiques embarqués du domaine aéronautique s'est traduit dès le début des années 1980 par un besoin de recommandations techniques et méthodologiques destinées aux acteurs de la communauté aéronautique.
Le document DO-178 fournit et décline ces recommandations pour chacun des processus requis en vue de la certification du logiciel (Planification/Développement/Vérification/Gestion de configuration/Assurance Qualité Logiciel) et ce, en fonction du niveau de sécurité du logiciel à développer.
Au cours de cette présentation, nous aborderons notamment les enjeux du processus de vérification, pour lesquels la DO-178 est la plus exigeante en termes de volume d'activité.

9:40 DO-254 : normes et standards autour du développement hardware - *Pascal Aristote, SILKAN*

Afin d'assurer un niveau de sureté de fonctionnement suffisant, le respect de standards et normes encadrant le développement de composant numérique et de carte, est aujourd'hui incontournable.
Le constat est simple :
- Ces standards de développement hardware sont souvent une traduction des bonnes pratiques appliquées à vos métiers dans l'entreprise.
- Même imposée, toute l'entreprise bénéficie de l'application de telle méthode ou procédure. La qualité des produits est meilleure et la relation client-fournisseur facilitée.

Des exemples seront présentés vous permettant de juger de l'effort nécessaire pour adresser ces marchés comme l'aéronautique, le nucléaire ou le spatial.

10:15 Systèmes, logiciels et données : conception d'un système critique et mise en œuvre industrielle de différentes méthodes formelles - *Mathieu Clabaut, SYSTEREL*

Que ce soit pour réaliser des logiciels, valider des données ou concevoir des systèmes, les équipes de SYSTEREL mettent en œuvre des méthodes formelles depuis plus de 15 ans. Nous présenterons un panorama de notre retour d'expérience sur la mise en œuvre industrielle de différentes méthodes formelles.

10:45 Pause

11:00 Développement et intégration de systèmes critiques - *Christophe Barnier, ERASM*

Le développement de systèmes critiques pose la problématique de définir « ce qui est critique » et des conditions de maintien de ce niveau de sécurité lors de l'interaction entre différents systèmes.
Cette présentation a pour but de présenter :

- Le choix du niveau de DAL (interaction entre fonctions réalisées et conséquences de leurs défaillances)
- L'approche Exigences vs Fonctions
- La continuité du niveau de sécurité entre composant
- La caractérisation des limites de sécurité

11:30 Pourquoi et comment qualifier un outil pour la conception et la vérification de systèmes complexes - *Pascal Aristote, SILKAN*

De nos jours, le développement d'un système complexe est impensable sans l'utilisation d'outils de conception ou de vérification.
Souvent, la définition de méthode et de procédure d'utilisation d'un outil vient de l'expérience interne de l'entreprise ou de son personnel. Ces méthodes empiriques ne sont plus suffisantes au regard des exigences de développement d'un système critique.
La qualification devient donc un moyen de s'assurer du bon fonctionnement de l'outil dans l'environnement qui lui est appliqué et pour la tâche qui lui incombe.

12:00 Evolution de la certification aéronautique en regard de la complexité de l'électronique - *Frédéric FAUBLADIER, EUROCOPTER*

L'objectif de la présentation sera de montrer que la certification Aéronautique de l'électronique complexe dépasse aujourd'hui les aspects DO254 et nécessite dorénavant une implication des métiers systèmes, Hardware, Software et sureté de fonctionnement. Cette présentation est illustrée au travers de 4 exemples : La

gestion des COTS complexes, des Single event upset, problème ouvert et la gestion de la design assurance au niveau équipement.

Une conclusion sur les écueils actuels face à cette évolution sera présentée.

12:30 Buffet

13:45 Analyseur de code : prouver l'absence d'erreur dans les codes embarqués - *Jérôme Feret, Ecole Normale Supérieure, chercheur équipe ABSTRACTION*

ASTREE est un analyseur statique de code permettant de prouver l'absence d'erreurs au Run Time (RTE). Ce programme a été utilisé pour prouver complètement et automatiquement l'absence d'erreur au Run Time :
- du logiciel de contrôle de vol de l'Airbus A340 et A380 « fly-by-wire system »
- du logiciel du véhicule « Jules Vernes Automated Transfer Vehicle »

Dans cette présentation, après un court rappel sur l'histoire d'ASTREE, il sera donné une vue globale de la structure de l'analyseur ainsi qu'une description de certaines abstraction utilisées.

14:15 Témoignage de donneur d'ordre (sous réserve)

14:45 Plus de 10 ans de diffusion de la méthode B - *Etienne Prun, CLEARSY*

La méthode B tire sa légitimité du développement d'outils approuvés et utilisés à grande échelle, dans le monde industriel et universitaire, tels que l'Atelier B. CLEARSY est détenteur de cet atelier logiciel, de sa diffusion, des évolutions, de la maintenance de sa plateforme de développement. L'Atelier B constitue une référence pour le développement de logiciels prouvés.
Après un bref historique, nous présenterons quelques projets types d'application, tant pour la réalisation et la preuve de logiciels, que la preuve de systèmes. Nous finirons par les développements en cours sur l'Atelier B, ainsi que les pistes d'améliorations envisagées.

15:30 Les facteurs humains dans la criticité des systèmes : L'Humain comme élément positif de la sécurité

Laurent CHAUDRON, Dr. HDR - Directeur Centre ONERA de Salon-de-Provence
Ivan PASTORELLI, MCF HDR, GREDEG UMR-CNRS 7321 - Co-directeur scientifique du CEFH

Cette intervention permettra de comprendre les enjeux de la prise en compte du facteur humain dans la conception d'un système complexe et de connaître les effets de seuil dans la fiabilité des systèmes d'organisation.
Les effets de seuils des phénomènes sont encore peu documentés et largement inexpliqués en ce qui concerne la fiabilité des systèmes socio techniques.
Ils couvrent plusieurs aspects, notamment :
- des dégradations de fiabilité soudaines et plus que proportionnels dus à la diffusion de modes organisationnels particuliers.
- Une courbe des coûts de sécurité qui suit une fonction cube pour les activités dont la fiabilité avoisine les 10-6.
- L'interaction entre des technologies de maturités différentes qui induit, via des effets de désapprentissage, des accidents résiduels.

16:30 Café et Fin séminaire

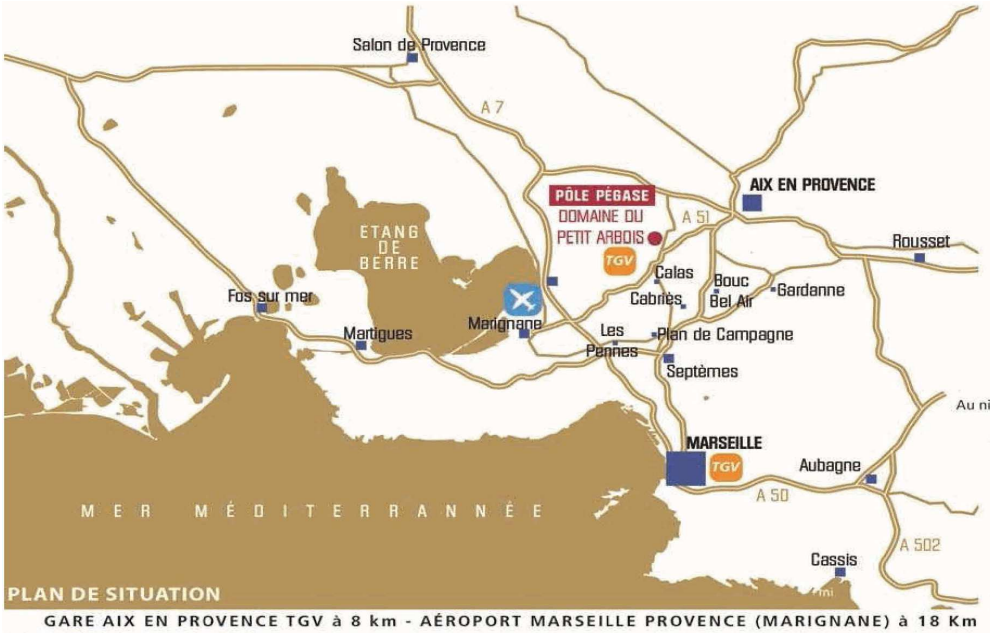
Contacts :
Gaëlle MARMET, POLE PEGASE : gaelle.marmet@pole-pegase.com
Jean-Luc BAUDOUIN, CAP'TRONIC : baudouin@captronic.fr
Alain BRITON, CAP'TRONIC : briton@captronic.fr

Inscriptions : Janique PERNOUD : pernoud@captronic.fr

Plan POLE PEGASE ci-dessous

CAP'TRONIC

POLE PEGASE



PLAN DE SITUATION

GARE AIX EN PROVENCE TGV à 8 km - AÉROPORT MARSEILLE PROVENCE (MARIGNANE) à 18 Km

Arrivée par le Nord
Direction : Aix-en-Provence
Sortie : Aix Ouest - Les Milles
Sortie : Les Milles
Continuer : jusqu'à la sortie n°5 : Europôle de l'Arbois, secteur du Petit Arbois D543
Suivre : Direction Europôle de l'Arbois, secteur du Petit Arbois.

Arrivée par le Sud
Direction : Aix-en-Provence par l'A51
Sortie : Plan de Campagne
Direction : Calas par la D543
Traverser : Calas jusqu'au rond point de la Gremeuse
Direction : Eguilles
Secteur du Petit Arbois par la D543
Suivre : Direction Europôle de l'Arbois, secteur du Petit Arbois.

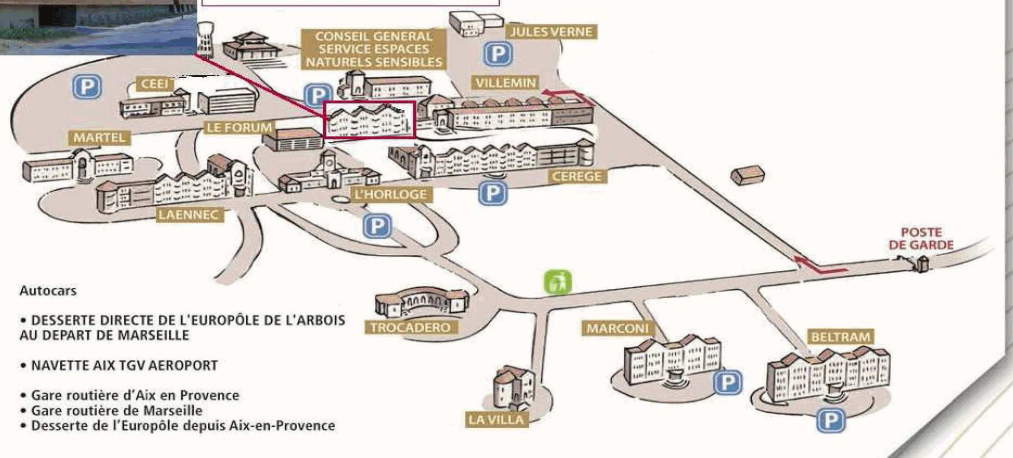
Arrivée par l'Est
Direction Aix-en-Provence
Au niveau d'Aix suivre : Marseille / Les Milles par l'A51
Sortie : Les Milles
Continuer : jusqu'à la sortie n°5 : Europôle de l'Arbois, secteur du Petit Arbois D543
Suivre : Direction Europôle de l'Arbois, secteur du Petit Arbois.

Arrivée par l'Ouest
depuis Montpellier
Suivre : Direction Lyon A7
Sortie : Vitrolles Griffon
depuis Marignane
Suivre : Aix-en-Provence Puis
Direction : Les Milles - Calas par la D9
Sortie : Calas - Secteur du Petit Arbois
Suivre : Europôle de l'Arbois, secteur du Petit Arbois.

Les bureaux du Pôle Pégase se situent au bâtiment reconnaissable à ses feuilles de platane.
1ère entrée lorsque que le bâtiment se situe à votre gauche) au 1er étage.

PLAN DU DOMAINE DU PETIT ARBOIS

GPS : 43°29'29"N/5°19'52"E



Autocars

- DESSERTE DIRECTE DE L'EUROPÔLE DE L'ARBOIS AU DEPART DE MARSEILLE
- NAVETTE AIX TGV AEROPORT
- Gare routière d'Aix en Provence
- Gare routière de Marseille
- Desserte de l'Europôle depuis Aix-en-Provence