IFSTTAR

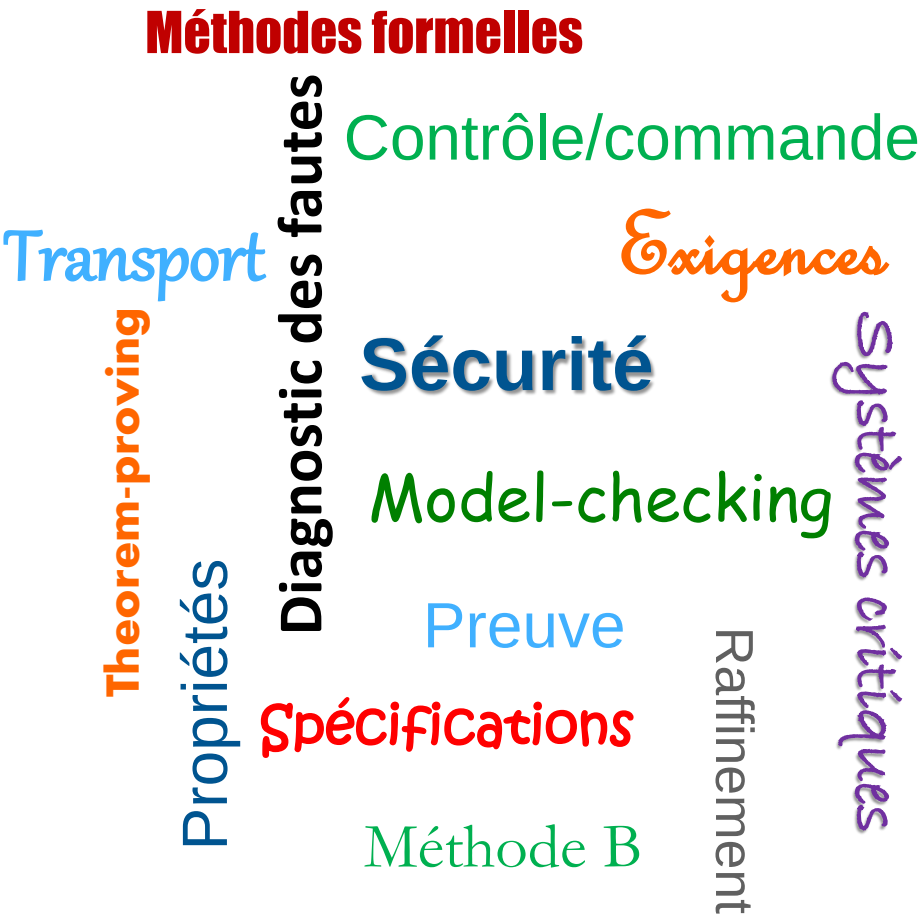
TransForm

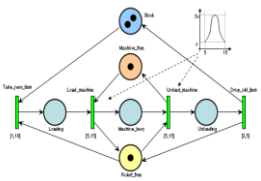
Appel à participation

Journée du 14 décembre 2017 à l'IFSTTAR Villeneuve d'Ascq

TransForm : méthodes Formelles pour les systèmes de Transport

Un groupe de travail impliquant des industriels et des académiques, autour de l'utilisation des méthodes formelles pour les applications transport





Contact: Mohamed GHAZEL, IFSTTAR-COSYS/ESTAS
David MENTRÉ, MERCE-CIS
mohamed.ghazel@ifsttar.fr d.mentre@fr.merce.mee.com

Programme

9h45-10h15 : Accueil des participants

10h15 - 10h30 : Introduction (Mohamed Ghazel, IFSTTAR & David Mentré, MERCE)

10h30 - 11h15 : Discussion ouverte autour des activités du groupe
* Objectifs du groupe
* Thématiques & domaines d'application
* Types de travaux / exposés, autres activités

11h15 - 12h : Retour sur 20 ans d'application des méthodes formelles dans le ferroviaire (Laurent Voisin - Systerel)

12h - 13h30 : Pause déjeuner autour d'un buffet

13h30 - 14h10 : Les Méthodes formelles au service de la voiture autonome (Vassil Todorov - Peugeot Citroën Automobiles)

14h10 - 14h50 : SPARK - Retours d'expérience et intérêt en transport (Yannick Moy - Adacore)

14h50 - 15h10 : Pause café

15h10 - 15h50 : Méthodes formelles appliquées aux spécifications textuelles - V&V sur les changements de modes de la normes ERTMS (Matthieu Perin - IFSTTAR)

15h50 - 16h30 : Le langage AltaRica et la problématique du MBSA (Michel Batteux - SystemX)

16h30 - 16h45 : Notes de fin (Mohamed Ghazel - IFSTTAR & David Mentré - MERCE)

Contact: Mohamed GHAZEL, IFSTTAR-COSYS/ESTAS
David MENTRÉ, MERCE-CIS
mohamed.ghazel@ifsttar.fr d.mentre@fr.merce.mee.com

Résumés :

1- Retour sur 20 ans d'application des méthodes formelles dans le ferroviaire (Laurent Voisin - Systerel)

Je présenterai un retour d'expérience sur l'application des méthodes formelles dans le domaine industriel des logiciels de signalisation au cours des vingt dernières années. Je présenterai tout d'abord un bref survol de quelques unes des techniques disponibles et de leur domaine d'application. J'insisterai ensuite sur l'importance primordiale de l'outillage pour une utilisation en milieu industriel. Finalement, je présenterai la mise en oeuvre pratique de ces techniques formelles lors d'un projet industriel substantiel de développement d'un logiciel sûr et décrirait les leçons tirés de ce genre d'application dans la décennie passée.

2- Méthodes formelles au service de la voiture autonome (Vassil Todorov - Peugeot Citroën Automobiles)

La part croissante des fonctions d'assistance à la conduite, leur criticité, ainsi que la perspective d'une certification de ces fonctions, rendent nécessaire leur vérification et leur validation avec un niveau d'exigence que le test seul ne peut assurer. Depuis quelques années déjà d'autres domaines comme l'aéronautique ou le ferroviaire sont soumis à des contextes équivalents. Pour répondre à certaines contraintes ils ont localement mis en place des méthodes formelles.
Le groupe Peugeot Citroën Automobiles expérimente différentes techniques formelles afin de déterminer celles qui seraient pertinentes, pour quel type de développement, ainsi que l'impact de leur déploiement sur le processus. Cette présentation fait un tour d'horizon des techniques formelles expérimentées sur du code embarqué réellement utilisé en production, donne une synthèse des résultats obtenus et propose quelques perspectives pour l'avenir.

3- SPARK - Retours d'expérience et intérêt en transport (Yannick Moy - Adacore)

L'approche SPARK est utilisée depuis 30 ans pour produire des logiciels avec de très hautes garanties de fiabilité, sûreté et sécurité, dans les domaines avioniques, militaire, ferroviaire, réseau. Le produit SPARK a connu un renouveau depuis 2014 avec un changement de langage et de technologie. Les spécifications sont désormais intégrées au langage de programmation, et les prouveurs SMT fournissent le moteur de preuve automatique. L'utilisation industrielle de SPARK répond à des besoins divers d'assurance qualité, parfois vis-à-vis de fournisseurs, parfois parce que le coût d'une erreur est prohibitif.

Contact: Mohamed GHAZEL, IFSTTAR-COSYS/ESTAS
David MENTRÉ, MERCE-CIS
mohamed.ghazel@ifsttar.fr d.mentre@fr.merce.mee.com

Suivant les besoins, l'objectif qualité n'est pas le même, ce à quoi SPARK répond en ayant défini des niveaux d'assurance logicielle allant de règles de codage sémantique jusqu'à la vérification fonctionnelle. Je montrerai ces niveaux d'assurance, en les illustrant par des projets industriels qui les ont appliqué, et en faisant le pont avec les objectifs typiques des standards de certification logicielle comme EN 50128 pour le ferroviaire ou ISO 26262 pour l'automobile.

4- Méthodes formelles appliquées aux spécifications textuelles - V&V sur les changements de modes de la norme ERTMS/ETCS (Matthieu Perin - IFSTTAR)

La complexité et la taille des spécifications données sous formes textuelles sont souvent source de problèmes lors de la mise en oeuvre. Ainsi il convient de supprimer au plus tôt les erreurs, au pire de détecter des comportement potentiellement fautif qu'il faut tester spécifiquement. Le travail présenté montre comment à partir d'un modèle NuSMV représentant la spécification des changements de modes ERTMS/ETCS (subset 26, baseline 3) on peut détecter des comportement normalement interdits, pour ensuite proposer des tests visant à garantir que l'implémentation répond aux exigences de comportement souhaitées.

5- Le langage AltaRica et la problématique du MBSA (Michel Batteux - SystemX)

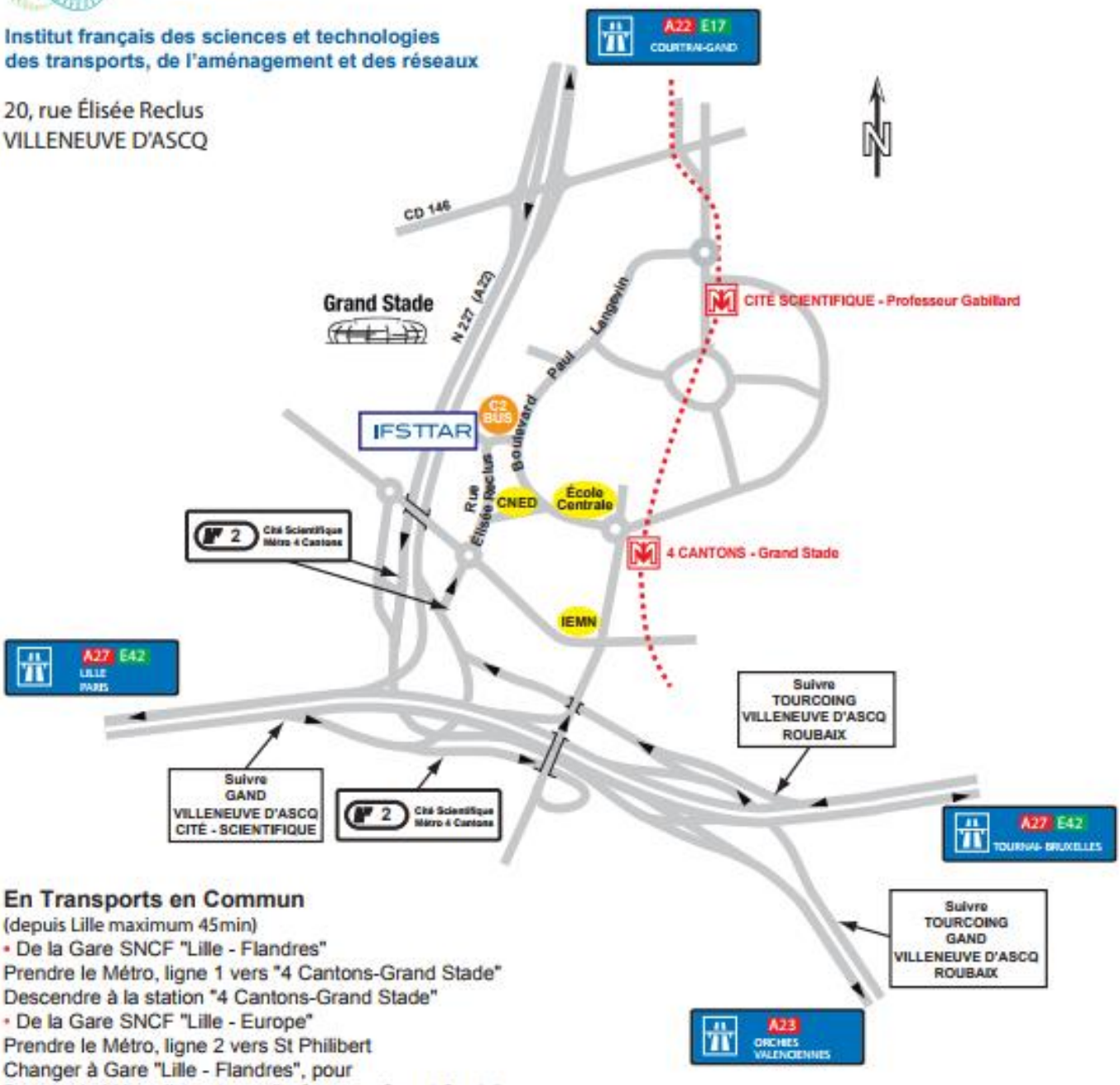
Les méthodes et outils classiques pour les études probabilistes de sûreté de fonctionnement sont bien maîtrisés mais sont éloignés des spécifications du système concerné. La sûreté de fonctionnement dite basée sur les modèles, nommée MBSA pour "Model-Based Safety Assessment", vise à réduire cet écart entre les spécifications du système et les méthodes et outils classiques. Le langage AltaRica est une telle solution MBSA, qui permet de modéliser le système à plus haut niveau, proche des modèles d'architecture système. Nous verrons dans l'exposé comment, au travers du langage AltaRica, il est possible de mener des études probabilistes de sûreté de fonctionnement ; puis nous aborderons des problématiques sous-jacentes liées aux activités de modélisation telles que, par exemple, comment maintenir des modèles, comment synchroniser les modèles de sûreté de fonctionnement et les modèles d'architecture système.

Contact: Mohamed GHAZEL, IFSTTAR-COSYS/ESTAS
David MENTRÉ, MERCE-CIS
mohamed.ghazel@ifsttar.fr d.mentre@fr.merce.mee.com

IFSTTAR

Institut français des sciences et technologies
des transports, de l'aménagement et des réseaux

20, rue Élisée Reclus
VILLENEUVE D'ASCQ



En Transports en Commun

(depuis Lille maximum 45min)

- De la Gare SNCF "Lille - Flandres"

Prendre le Métro, ligne 1 vers "4 Cantons-Grand Stade"
Descendre à la station "4 Cantons-Grand Stade"

- De la Gare SNCF "Lille - Europe"

Prendre le Métro, ligne 2 vers St Philibert
Changer à Gare "Lille - Flandres", pour
Prendre le Métro, ligne 1 vers "4 Cantons-Grand Stade"
Descendre à la station "4 Cantons-Grand Stade"
À la station "4 Cantons-Grand Stade" sortir sur la gauche,
direction "Grand Stade 12 min"
Passer devant, l'École Centrale, le CNED
Puis tourner à gauche au panneau
"Météo-France, IFSTTAR"
(Distance 600 m)

En voiture

- En venant de Lille ou Paris (A1-E17)

Suivre la direction "Villeneuve d'ascq - 4 Cantons"
et prendre la sortie 2 "Cité Scientifique - Métro 4 Cantons"

- En venant de Valenciennes (A23) ou Bruxelles (A27-E42)

Suivre la direction "Lille",
puis suivre la direction "Villeneuve d'Ascq - Métro 4 Cantons"
et prendre la sortie 2 "Cité Scientifique - Métro 4 Cantons"

- En venant de Tourcoing - Gand (A22-N227)

Suivre "Valenciennes - Bruxelles"
Sortie 2 "Cité Scientifique - Métro 4 Cantons"
Dans tous les cas suivre Zone C, parking C2 BUS

Contact: Mohamed GHAZEL, IFSTTAR-COSYS/ESTAS
David MENTRÉ, MERCE-CIS
mohamed.ghazel@ifsttar.fr d.mentre@fr.merce.mee.com