Titre de la thèse : FIDES Tolérance aux fautes et reconfiguration fiable dans une architecture automobile HPC/ZCU

L'ISAE-SUPAERO cherche des candidats pour une thèse CIFRE. Une thèse CIFRE est un partenariat de recherche qui permet à un doctorant de réaliser son projet de thèse en partageant son temps entre une entreprise et un laboratoire universitaire, avec le soutien financier de l'État, favorisant ainsi un échange fructueux entre le monde académique et le secteur industriel.

Directeur de thèse :	R. Vingerhoeds (ISAE-SUPAERO - DISC)
Co-Directeur de thèse :	M. Lauer (ISAE-SUPAERO - DISC)
Co-Encadrant :	J.B. Chaudron (ISAE-SUPAERO - DISC)
Co-Directeur du monde socio-économique :	Ph. Cuenot (Continental
Montage financements :	Bourse CIFRE (dossier en cours de montage) avec Continental

Mots-clefs :

Systèmes embarqués, tolérance aux fautes, reconfiguration

Contexte :

Les architectures Electrique/Electronique (E/E) mises en place dans les systèmes automobiles évoluent, en centralisant la majeure partie des fonctionnalités sur un calculateur central Haute performance HPC complexe – un System on Chip incluant plusieurs cœurs temps-réel et des cœurs de performance –, connecté à des calculateurs zonaux ZCU distribués géographiquement dans le véhicule. Au niveau logiciel, le HPC va multiplexer plusieurs logiciels (Autosar, adaptive autosar, Linux), et, suivant les cœurs d'exécution, pourra embarquer un hyperviseur, permettant d'assurer la sûreté du niveau QM jusqu'au niveau ASIL D. Les ZCU, connectés en étoile au HPC, embarqueront un système Autosar classique et seront responsable de l'interface avec les capteurs et actuateurs du véhicule proches.

Une telle architecture, dans un contexte de sûreté de fonctionnement requis par la norme ISO 26262, se doit de garantir des propriétés de tolérance aux fautes. En effet, le calculateur central d'un système réparti en étoile est un point unique de défaillance, et les chemins de communication entre les différents calculateurs doivent être garantis pour éviter une défaillance globale en cas de problème de communication.

Le calculateur central contient plusieurs unités de calcul qui peuvent être utilisées pour assurer une redondance qui permet d'implémenter des techniques de tolérance aux fautes classiques, et de fournir des mécanismes de reconfiguration vers un mode dégradé de fonctionnement en cas de détection d'une anomalie. Par ailleurs, les calculateurs zonaux ZCU peuvent aussi être mis à contribution lors de la reconfiguration dynamique du système.

Sujets de la thèse :

Dans ce contexte, le travail effectué dans cette thèse se focalisera sur les **trois socles** suivants :

1) D'un point de vue architectural, il s'agira d'analyser la solution existante et de proposer des améliorations de l'architecture matérielle en identifiant les points bloquants pour garantir la tolérance aux fautes du système et offrir des mécanismes de reconfiguration. Les redondances nécessaires au niveau réseau et unités de calcul seront identifiées en fonction des possibles modes de défaillance des composants de l'architecture.
2) Le deuxième socle portera sur l'architecture logicielle permettant la définition de plusieurs modes opérationnels. En fonction du niveau d'autonomie visé, il devient nécessaire de dépasser le mode *fail-safe* classiquement utilisé pour aller vers la gestion de modes dégradés plus fins. On peut envisager ces différents modes opérationnels comme un ensemble de configurations interconnectées qui permettent d'assurer la safety du véhicule depuis le mode nominal jusqu'aux différents modes dégradés.
3) Le troisième socle est la surveillance du système. Au-delà du monitoring local qui identifie un dysfonctionnement d'un composant, le monitoring devra vérifier que la plateforme exécutive reste dans état global cohérent. En cas de déviation de la spécification, il faut lancer une reconfiguration garantissant la safety, qui permettra de basculer vers une autre configuration globale sûre, ceci malgré la distribution du calcul entre les différentes entités du système et les contraintes temps-réel des applications. Les deux derniers socles sont intimement liés : chaque mode opérationnel correspond à une configuration du système de surveillance/monitoring qui décide de lancer une reconfiguration sûre vers une autre configuration globale définie dans le deuxième socle avant que la safety du système soit mise en défaut.

Perspectives pour le doctorant :

Le doctorant, au-delà des formations (scientifiques, linguistiques ou relatives à l'insertion dans le monde du travail…) proposées par l'école doctorale et des séminaires proposés par les laboratoires, bénéficiera de formations complémentaires proposées dans les établissements sous forme de stages courts (coordination d'une équipe, …). Enfin, il aura la possibilité de suivre les enseignements de master dans les établissements partenaires (processus en ingénierie système, modélisation système, théorie de la décision, théorie du vote).

Nous envisageons par ailleurs un séjour de quelques mois à l'étranger dans des universités avec lesquelles les équipes entretiennent de fortes collaborations : TU Delft, MIT, TUM ...

Sur le plan de son intégration dans des communautés scientifiques, le doctorant sera encouragé à participer et à présenter ses travaux dans des conférences internationales scientifiques et/ou dans des revues scientifiques internationales, ainsi que lors du séminaire doctoral et de la Conférence de l'AFIS (région parisienne)

Le doctorant aura d'excellentes perspectives au vu de la connaissance qu'il aura au niveau des systèmes embarqués, la tolérance aux fautes, et la reconfiguration. Le jeune docteur pourra aisément poursuivre sa carrière dans ces domaines (autant dans l'industrie que dans un établissement de recherche).

Ce projet de recherche constitue pour le doctorant donc une étape importante afin de déployer ces compétences pluridisciplinaires et de concrétiser ses savoirs au travers d'une thèse.

L'équipe ISAE-SUPAERO :

Le Département d'Ingénierie des Systèmes Complexes (DISC, 41 personnels permanents, 26 enseignants-chercheurs, dont 17 HDR) regroupe les activités de recherche menées dans les domaines de l'ingénierie des systèmes complexes dans le but de développer des méthodes, techniques et outils permettant de maîtriser (c'est-

à-dire comprendre, analyser, évaluer, contrôler et concevoir) le comportement fonctionnel, opérationnel et les performances de ces systèmes. Afin d'aborder cet objectif scientifique le DISC développe à travers sa composante Mathématique une expertise transverse en méthodes d'analyse, d'optimisation et de modélisation stochastiques servant de support formel non seulement au développement de modèles rigoureux mis en œuvre dans les domaines automatique et informatique mais également dans l'ensemble des domaines scientifiques ayant trait aux sciences pour l'ingénieur.

L'équipe DISC couvre les domaines des Mathématiques et de l'Informatique, ayant 4 groupes de recherche : Mathématiques Appliquées (MA), Apprentissage Décision Optimisation (ADO), Conception Analyse des Systèmes Critiques (CASC) et Systèmes Connectés (SysCo). Une équipe technique transverse fournit un support de haut niveau dans le domaine du développement et de la maintenance de plateformes expérimentales réalisées dans le cadre des activités de recherche ou d'enseignement.

Le doctorant sera accueilli et encadré au sein du DISC par Rob Vingerhoeds, Professeur, Michael Lauer, Professeur Associé, et Jean-Baptiste, Chercheur. Cette thèse se déroulera sur dans les équipes CASC et SysCo.