ASTRÉE est paramétrable et dispose de directives d'analyses pour s'adapter aux besoins spécifiques des utilisateurs. Il peut être également facilement étendu pour inclure de nouvelles abstractions permettant d'atteindre l'objectif de précision, sans aucune fausse alarme, sur des familles précises de programmes.

Un exemple de famille de programmes pour lequel **ASTRÉE** est très précis est celui des codes de contrôle commande temps réel engendrés automatiquement à partir d'une spécification synchrone de haut niveau (comme SCADE tm).

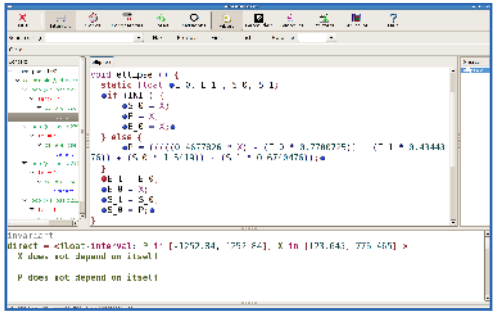
ASTRÉE a été utilisé pour vérifier l'absence d'erreurs à l'exécution dans le logiciel de commande de vol électrique primaire de l'A340 et de l'A380.

Mots-clés : interprétation abstraite, analyse statique, erreur à l'exécution, méthodes formelles, code critique, contrôle commande, temps réel synchrone, sûreté, avionique

Équipe ABSTRACTION
Centre de recherche INRIA Paris - Rocquencourt
Département d'informatique
École normale supérieure
45 rue d'Ulm
75230 Paris cedex 05

Patrick Cousot
Patrick.Cousot@ens.fr
Tel.: +33 1 44 32 20 64

http://www.astree.ens.fr/



INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

ASTRÉE

Analyse statique de code C critique temps réel synchrone embarqué

ASTRÉE

Analyse statique de code C critique temps réel synchrone embarqué

L'analyseur statique **ASTRÉE** prouve l'absence d'erreurs à l'exécution dans les codes critiques temps réel synchrone embarqués écrits en C.

Les erreurs trouvées par **ASTRÉE** sont :

- Tout usage de C défini dans la norme internationale de C (ISO/IEC 9899:1999) ayant un comportement indéfini (comme une division par zéro ou un débordement d'index de tableau) ;
- Toute violation de la norme internationale de C (ISO/IEC 9899:1999) relative aux comportements spécifiques d'une implémentation sur une machine donnée (comme la taille des entiers et les débordements arithmétiques) ;
- Tout usage potentiellement erroné ou incorrect de C contraire à des règles optionnelles de bon usage définies par l'utilisateur (comme l'exclusion de l'arithmétique modulaire pour les entiers signés même si c'est l'option implantée par le matériel) ;
- Toute violation d'assertions optionnelles insérées par l'utilisateur dans le code source.

ASTRÉE est basé sur l'interprétation abstraite de la sémantique des programmes analysés et calcule donc une sur-approximation de l'ensemble des comportements possibles du code à l'exécution. **ASTRÉE** est donc correct et ne peut jamais omettre de signaler une erreur à l'exécution.

Par contre, **ASTRÉE** est incomplet à cause de la sur-approximation qui peut introduire des comportements et donc des erreurs fictives impossibles dans toutes les exécutions réelles. On parle alors de fausses alarmes. L'objectif est donc de calculer des approximations suffisamment précises pour éviter toute fausse alarme (les vraies alarmes devant conduire à une correction du code).