



## COORDINATEUR : AIRBUS

## PARTENAIRES : ÉNS, CNRS

### Abstract :

We develop a semantic static analyzer based on abstract interpretation to check for run-time errors, data-races and deadlocks in real-time concurrent embedded avionics C software. AstréeA is automatic, efficient, and sound, with no false negative and few false alarms.

### OBJECTIFS DU PROJET

#### Vérification des logiciels embarqués critiques

Le test est coûteux et ne trouve pas toutes les erreurs

⇒ montée en puissance des méthodes formelles

L'analyse statique sémantique est automatique, efficace, sûre, sur le code source

⇒ idéale dans un contexte industriel

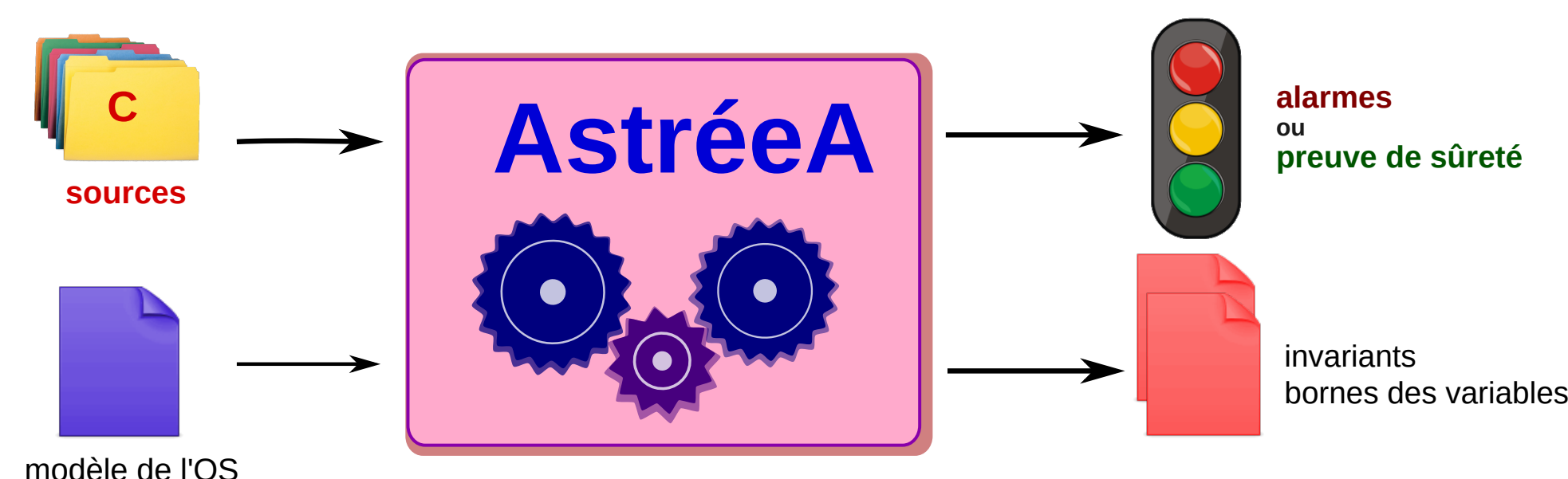
État de l'art : Astrée

analyse des RTE sur les logiciels C synchrones

**AstréeA : extension aux logiciels concurrents**

Difficulté : couvrir tous les ordonnancements

AstréeA signale toutes les erreurs arithmétiques, d'accès mémoire, data-races, deadlocks, violations d'API et d'assertions sur les logiciels C embarqués multi-threads temps-réels en mémoire partagée



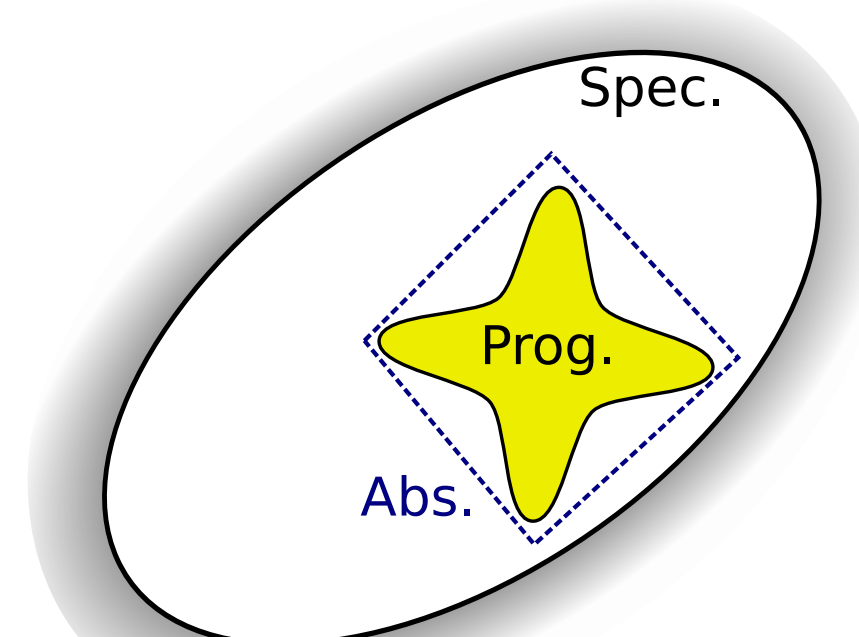
### MÉTHODOLOGIE

#### Interprétation abstraite :

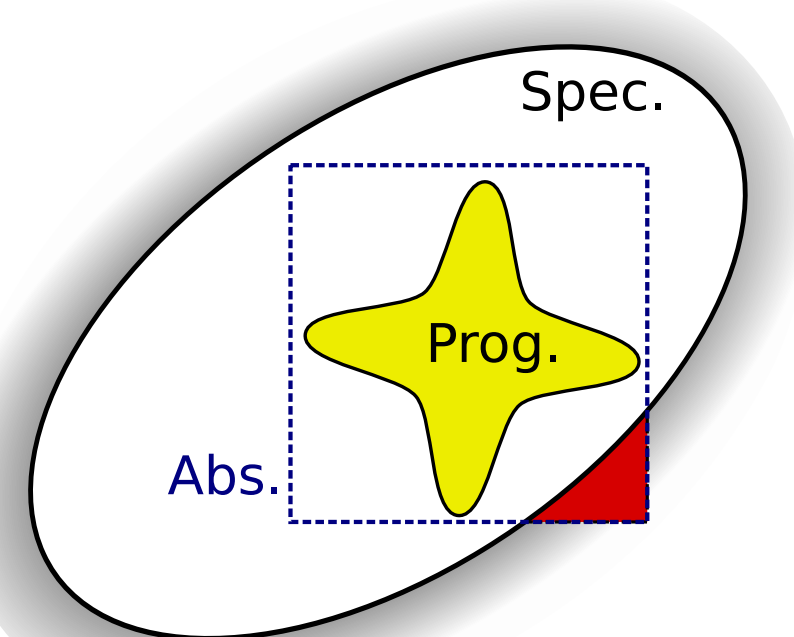
théorie de l'approximation sûre des sémantiques

#### Spécificités d'AstréeA :

- analyse modulaire thread à thread ⇒ efficacité
- spécialisation des abstractions ⇒ précision
- abstraction des interférences entre threads
- ordonnancement temps-réel, verrous, priorités
- sûreté vis-à-vis des mémoires faiblement cohérentes



correction prouvée



fausse alarme

analyse sûre :  $(Abs. \subseteq Spec.) \Rightarrow (Prog. \subseteq Spec.)$

### RÉSULTATS

- développement de nouvelles abstractions
- amélioration de la précision de l'analyse
- nouveaux modèles d'OS : POSIX, OSEK
- analyses en contexte académique et industriel
- transfert industriel vers AbsInt**

[www.absint.com](http://www.absint.com)



Cas d'étude principal : application ARINC 653, 2.1 Mloc de C, 15 processus

contexte académique : réduction par 6 des alarmes

|    | OS    | taille | stub | temps | mem.  | select.       |
|----|-------|--------|------|-------|-------|---------------|
| #1 | ARINC | 2.1M   | 5.2K | 24h   | 27GB  | <b>99,94%</b> |
| #2 | ARINC | 1.9M   | 2.4K | 154h  | 18GB  | 99,56%        |
| #3 | ARINC | 2.2M   | 2.3K | 160h  | 23GB  | 99,52%        |
| #4 | POSIX | 31.8K  | 2.2K | 1h    | 0,6GB | 97,28%        |
| #5 | POSIX | 33.1K  | 1.2K | 35h   | 2.5GB | 97,18%        |

contexte industriel : nouveaux cas d'études

### PERSPECTIVES

- déploiement industriel : avionique, automobile
- spécialisation pour améliorer la précision
- assurance sur le binaire avec CompCert

La sûreté est requise pour la certification DO-178C !

