AnaStaSec

Analyse statique de propriétés de sécurité

- Coordinateur :
  - Jérôme Feret
- Site web :
  - http://www.di.ens.fr/~feret/anastasec
- Équipe :
  - Airbus Operations SAS
  - AMOSSYS
  - CEA List
  - INRIA Paris-Rocquencourt (Antique, Prosecco)
  - INRIA Rennes - Bretagne Atlantique (Celtique)
  - TrustInSoft

Enjeux

Formellement, la sécurité est une équivalence entre des ensembles de traces.

État de l'art :

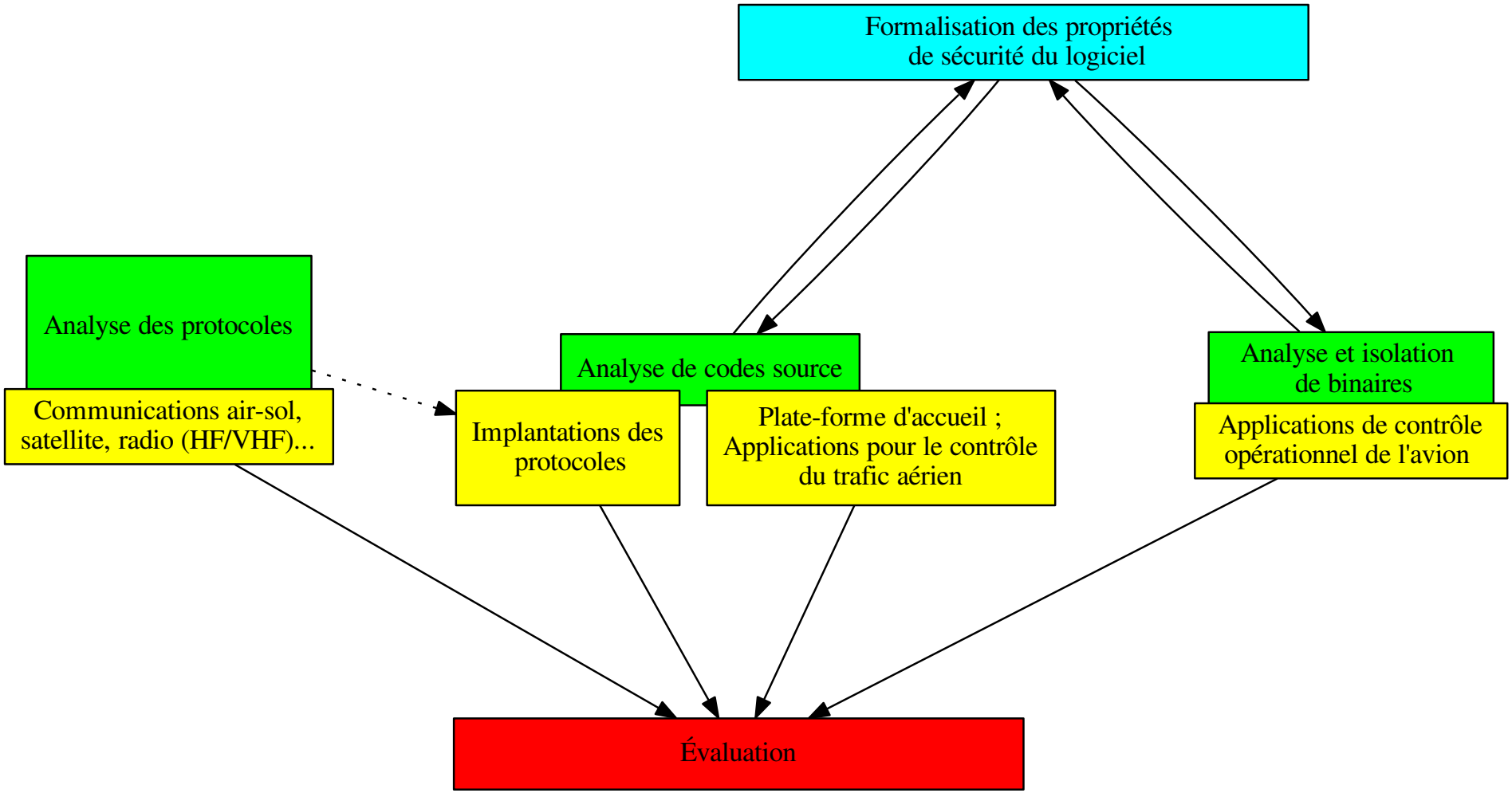
- Beaucoup de travaux sur l'analyse de protocoles de communication ;
- Quelques travaux sur leur implantation ;
- Pas/peu de travaux sur du logiciel embarqué industriel.

Seule une analyse automatique est économiquement viable.

Cas d'étude : prouver la sécurité d'un système avionique comprenant

1. la plate-forme d'accueil (système d'exploitation, applications de surveillance)
2. des applications de confiance (contrôle du trafic aérien)
3. des applications tierce-partie (contrôle opérationel de l'avion)
4. des protocoles de communication.

Plan d'action



Retombées attendues

- Retombées scientifiques :
  - passage à l'échelle des méthodes formelles pour la sécurité ;
  - conception de nouveaux domaines abstraits dédiés ;
  - interactions entre analyse causale et interprétation abstraire.

- Retombées sociétales :
  - conception d'un processus d'évaluation pour la sécurité des systèmes critiques ;
  - renforcement des standards auprès des autorités ;
  - amélioration de la qualité des logiciels embarqués.