THALES

Méthodes formelles : De l'ENS Paris-Saclay à Thales Research & Technology

10 ans de l'Institut Farman

Parcours personnel

ENS Cachan

- 6 mois de stage, 3 ans de thèse
  - Laboratoire Spécification et Vérification
  - 5 Projets Farman

école normale supérieure paris–saclay

Thales Research & Technology

- 3 ans et 6 mois
  - Equipe Méthodes Formelles
  - Laboratoire Système Embarqués Critiques
  - n projets de recherche interne ($n > 0$)

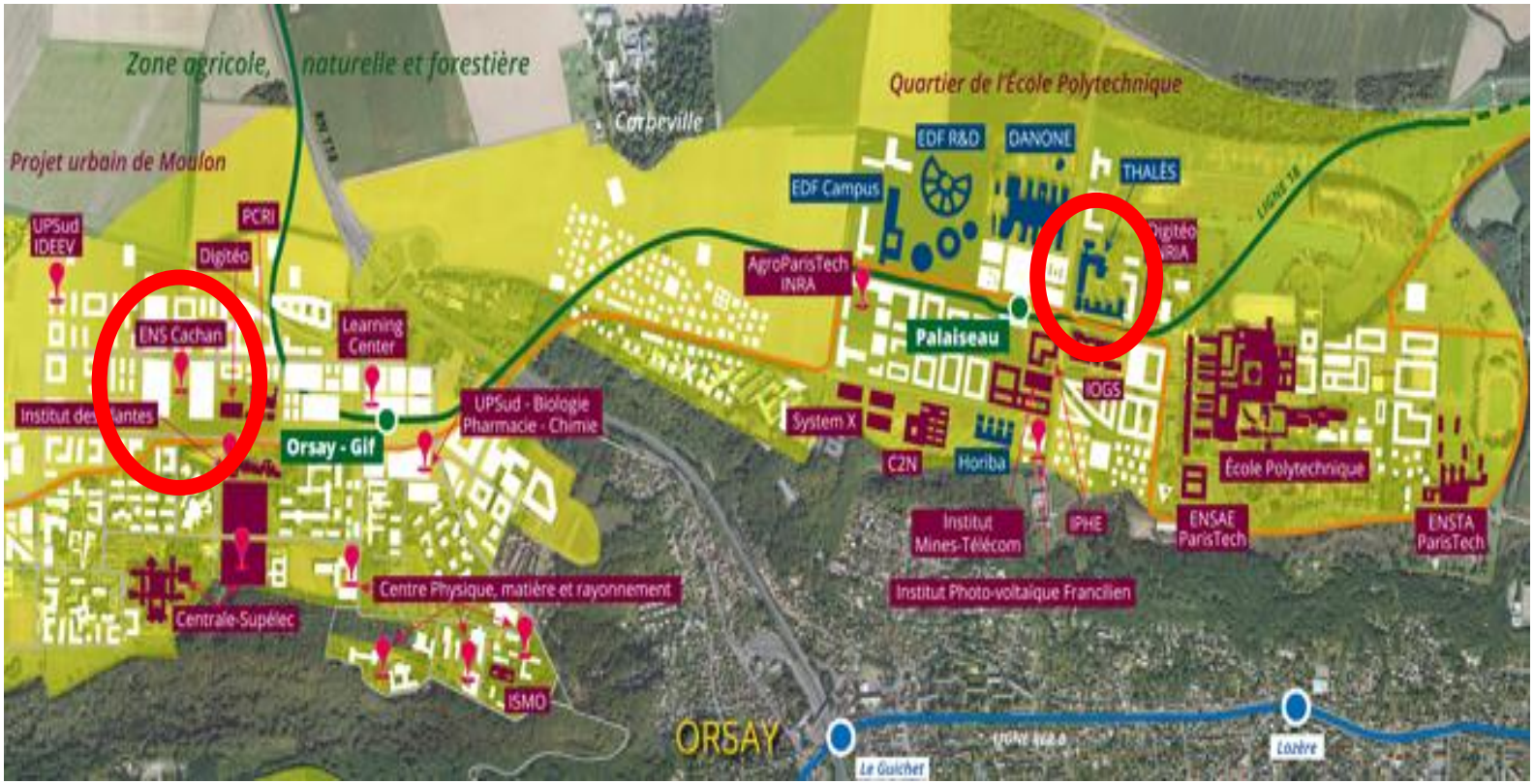
THALES

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2017 Tous Droits réservés.

Thales Research & Technology

TRT

- Centre de recherche « Corporate » du grope
- Sur le plateau de Saclay



Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2017 Tous Droits réservés.

Thales

L'intelligence collective pour un monde plus sûr

Partout où des décisions critiques doivent être prises, Thales est présent.
Sur les marchés que le Groupe sert (aéronautique, espace, transport terrestre, sécurité, défense),
ses équipements et systèmes aident ses clients à choisir la meilleure option et à agir en conséquence.

L'expertise de ses **64 000 collaborateurs** et sa présence opérationnelle dans **56 pays** en font ainsi **un acteur clé de la sécurité des citoyens, des infrastructures et des États.**

Salariés
64 000

Une présence mondiale
56 pays

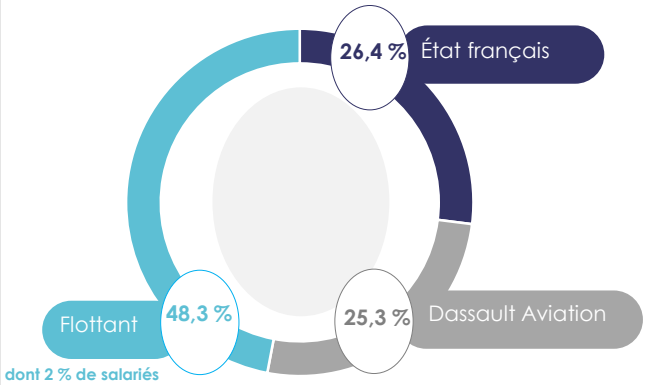
R & D Autofinancée* 2016
731 millions d'euros

* N'inclut donc pas la R & D réalisée sur financements externes.

Une structure équilibrée du chiffre d'affaires

Chiffre d'affaires 2016
15 milliards d'euros

Répartition du capital
(au 31 décembre 2014)

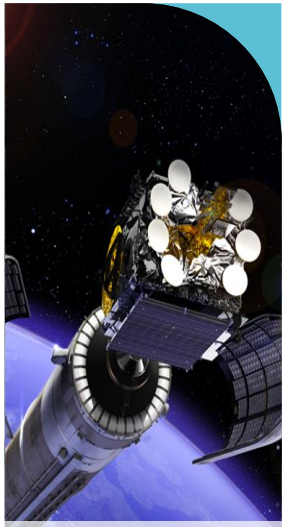


Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2017 Tous Droits réservés.

Les marchés de Thales

MARCHÉS DUAUX
Militaires & Civils

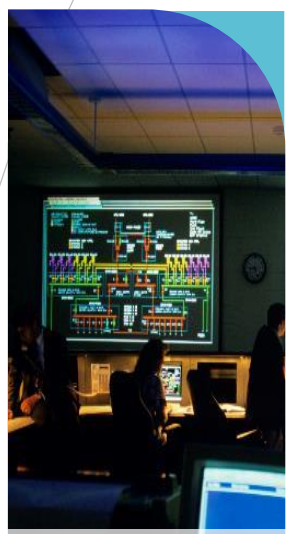
AÉRONAUTIQUE



ESPACE

TRANSPORT TERRESTRE

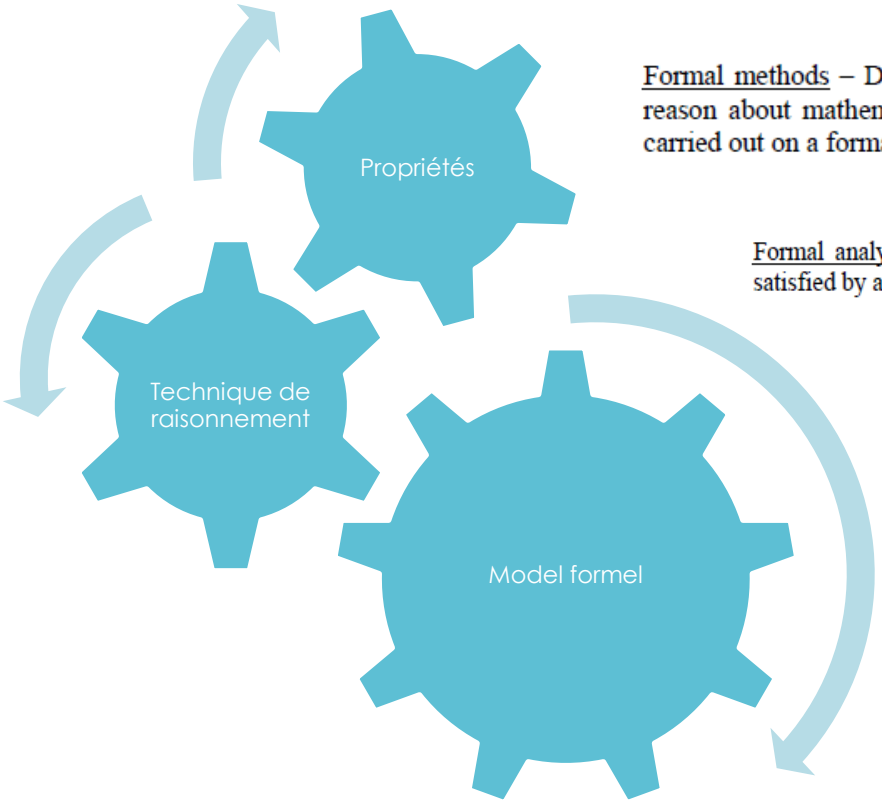
DÉFENSE



SÉCURITÉ

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2017 Tous Droits réservés.

Méthodes formelles ?



Définition de la DO-333

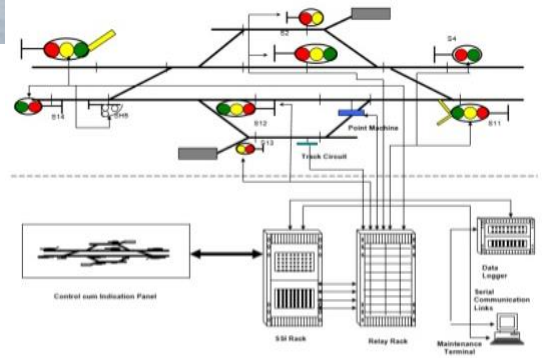
- Norme avionique pour le logiciel

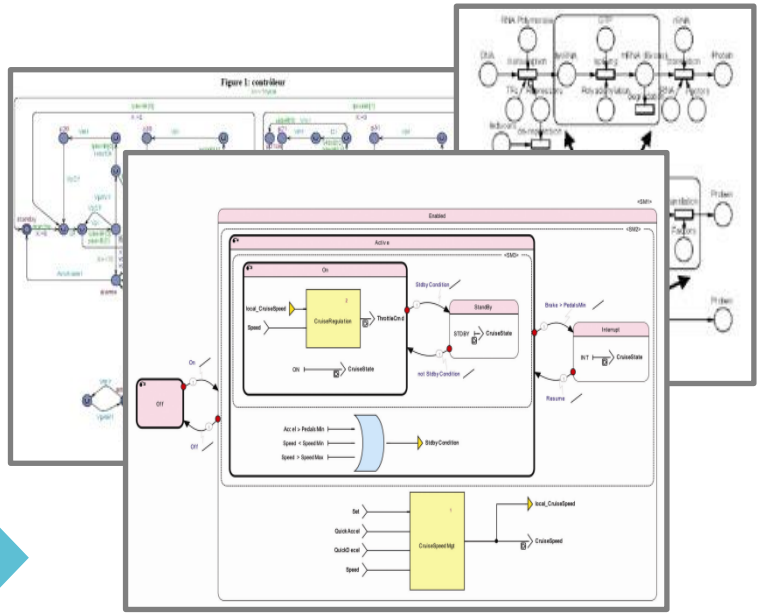
Formal methods – Descriptive notations and analytical methods used to construct, develop and reason about mathematical models of system behavior. A formal method is a formal analysis carried out on a formal model.

Formal analysis – The use of mathematical reasoning to guarantee that properties are always satisfied by a formal model.

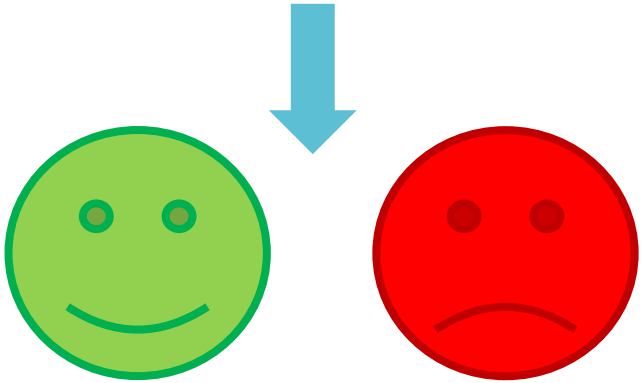
Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2017 Tous Droits réservés.

Méthodes formelles





$$\forall i, j \in \textbf{\textit{Trains}} \;\&\&\; \textbf{\textit{Num Train}}(i).\textbf{\textit{Cross}} \;\&\&\; \textbf{\textit{Train}}(j).\textbf{\textit{Cross}} \Rightarrow i == j$$



Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2017 Tous Droits réservés.

Recherche à TRT

Recherche « appliquée »

- Entre TRT et une ou plusieurs entités Thales
- Projet d'un an pour montrer l'applicabilité technique et/ou industrielle
- Dossier à soumettre en fin d'année

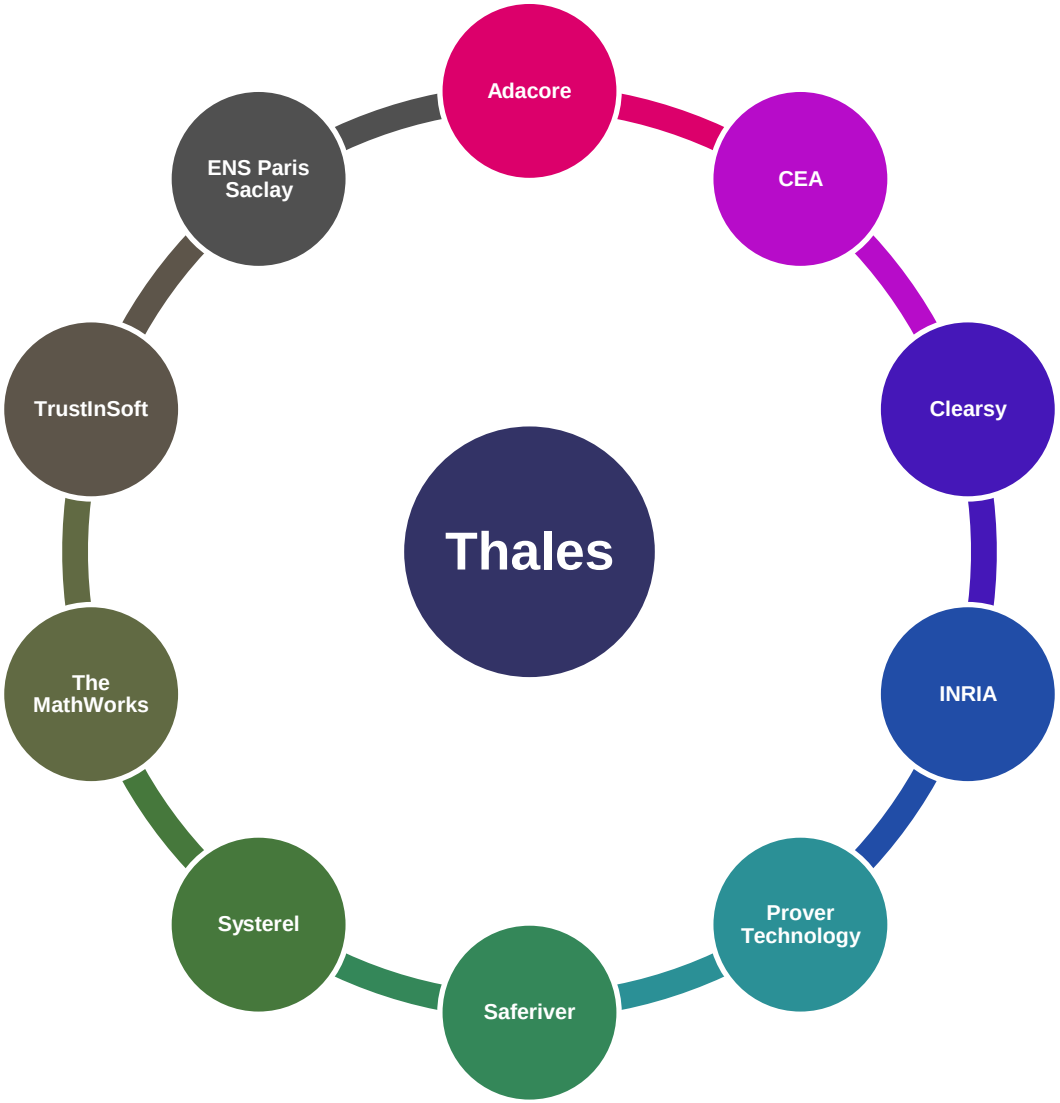
- A peu près un projet Farman

Recherche « amont »

- Projets de recherche : ANR, H2020, FUI, etc.
- Vision long terme

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2017 Tous Droits réservés.

Thales & l'écosystème « formel »



Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2017 Tous Droits réservés.

Est-ce que l'on s'en sert vraiment ?

Utilisation dans Thales

- Analyse de code C/Ada
  - Communications
  - Sécurité
  - Entre autres
- Model checking
  - Ferroviaire
  - Entre autres
- Theorem proving
  - Ferroviaire
  - Entre autres
- Entre autres utilisations également
  - CESTI Thales

Success stories hors Thales

- Intel : Theorem Proving
- Microsoft : Model checking
- Siemens/Alstom : B (Theorem proving)
- Airbus : Analyse de code, analyse de WCET

Autres utilisations

- Amazon, Apple, Dassault, Facebook, Gemalto, RockwellCollins, SNCF, RATP, etc.

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2017 Tous Droits réservés.

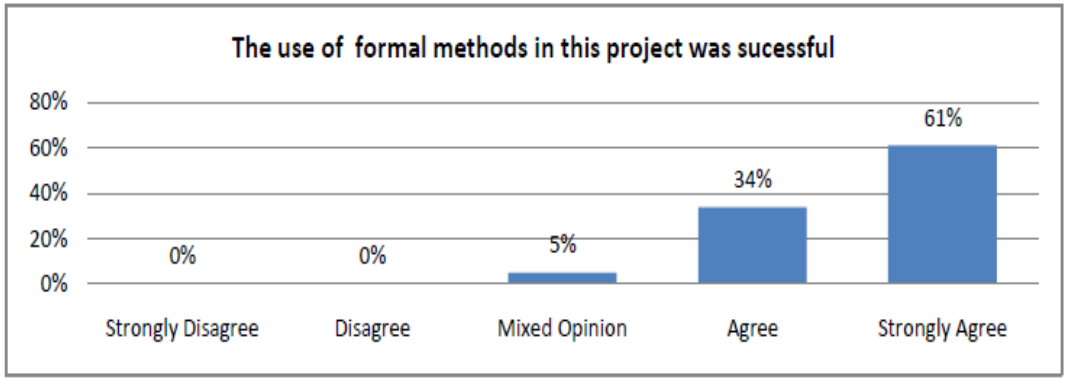
Utilisation industrielle : retours

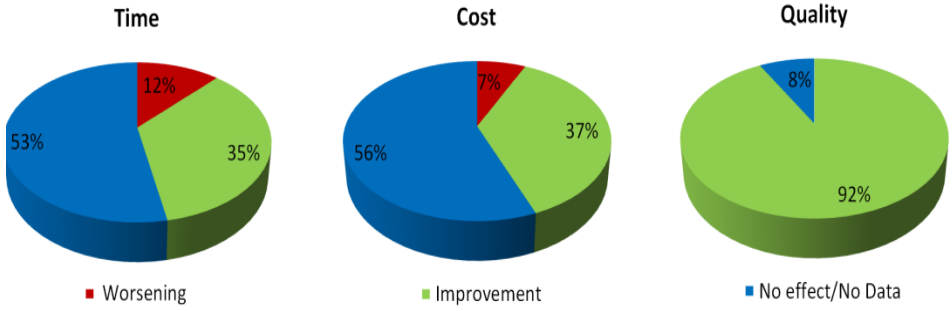
- J. Woodcock , P. Gorm Larsen, et al., *Formal methods: Practice and experience,* ACM Comput. Surv., 2009

Retours de 62 projets industriels

- Du monde entier
- Dans toutes les branches de l'industrie des systèmes critiques

Résultats



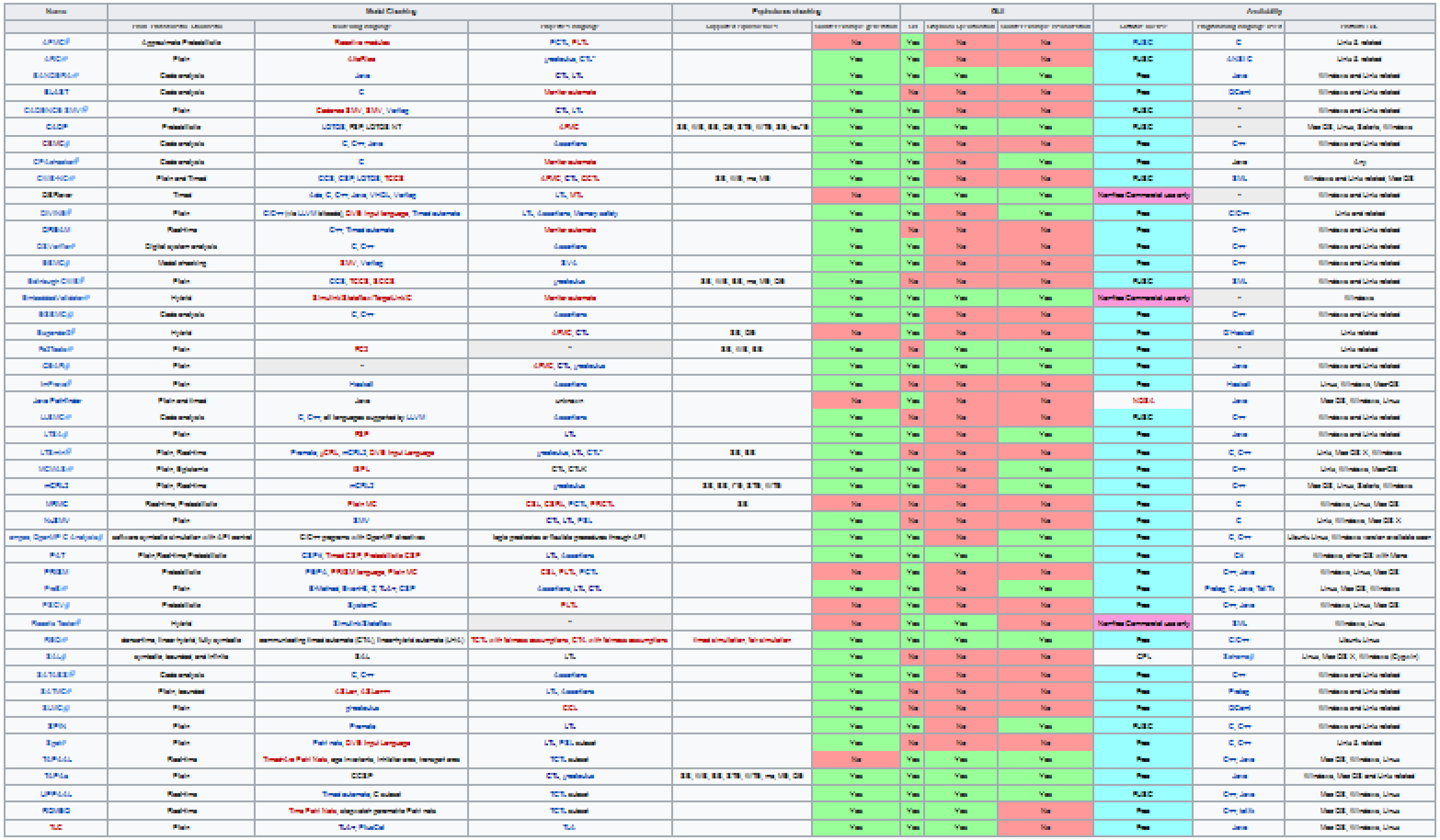


Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2017 Tous Droits réservés.

Quels sont les principaux obstacles ?

Multitude d'outils/de techniques

- Quoi essayer pour un novice ?



Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2017 Tous Droits réservés.

Quels sont les principaux obstacles ?

Multitude d'outils/de techniques

- Quoi essayer pour un novice ?

Manque de méthodologie

- Comment se servir des outils ?
- Comment débugguer ?
  - Son modèle
  - Son environnement
  - Ses propriétés

Difficulté d'évaluation du ROI

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2017 Tous Droits réservés.

Le futur des méthodes formelles dans l'industrie

Poussée des normes

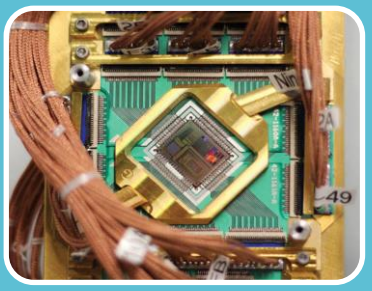
- Avionique: DO 333 (Suggestion)
- Ferroviaire: 50128 (Recommendation)
- Security: CC (Obligatoire pour EAL7)
- Automobile: 26262 (Recommendation)
- Défense: 00-55/00-56 (Recommendation)

Poussée des clients

- Des produits plus sûrs
- Moins de bug/Moins de maintenance

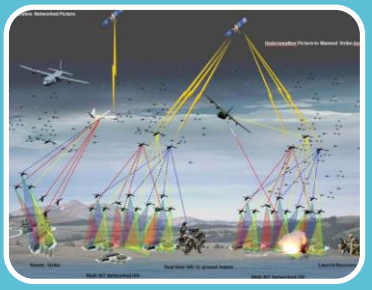
Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2017 Tous Droits réservés.

Challenge à plus long terme



Calcul quantique

- Quels gains pour la vérification ?
- Comment certifier leur comportement ?



Essaim de drônes

- Vérification des propriétés souhaitées ?
- Absence de propriétés non désirables ?

Intelligence artificielle

- Absence de bug ?
- Comment certifier son comportement ?

Ce document ne peut être reproduit, modifié, adapté, publié, traduit, d'une quelconque façon, en tout ou partie, ni divulgué à un tiers sans l'accord préalable et écrit de Thales - ©Thales 2017 Tous Droits réservés.