# Les méthodes formelles dans le cycle de vie

Virginie Wiels
ONERA/DTIM
Virginie.Wiels@onera.fr

# Plan

- Introduction
- Différentes utilisations possibles
- Différentes techniques
  pour différentes propriétés à différents niveaux
- Synthèse

# Introduction

# Méthodes formelles?... Définition

Méthode formelle

- Notation formelle
- Analyse formelle

- Notation formelle
  - ✓ Sémantique définie mathématiquement
  - ✓ Donc non ambiguë

- Analyse formelle
  - ✓ Traitement automatisé de modèles exprimés dans la notation formelle

# Méthodes formelles?... Historique

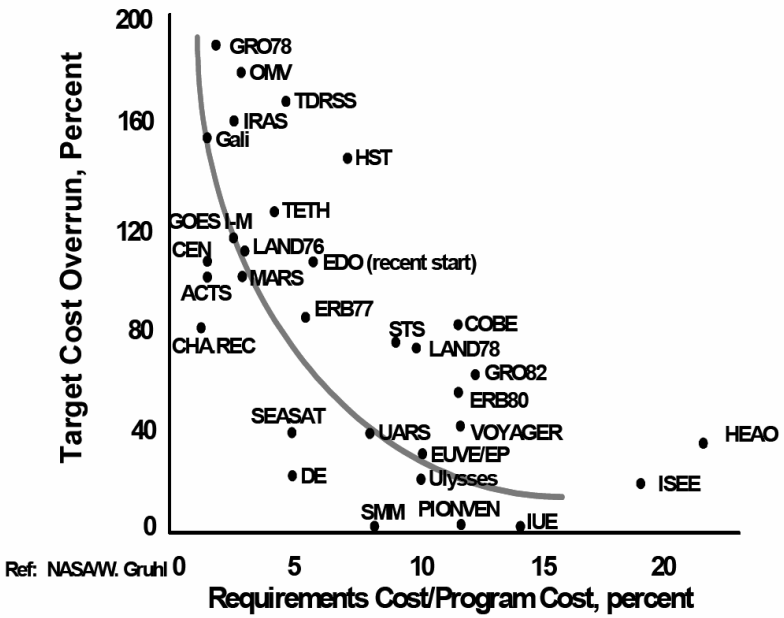
- Premiers travaux datent des années 60
  - ✓ Pour montrer la correction d'un programme
- Nombreux langages, techniques et outils
  - ✓ Industriels et recherche
  - ✓ + ou – complexes
  - ✓ Pour différents types de systèmes et de propriétés
- Choisir méthode adaptée / objectif

# Différentes utilisations possibles

# Modèle formel : une utilité en soi

- Développement classique : seul énoncé formel = produit (code pour du logiciel)
  - ✓ Tard dans le processus de développement

- Modèle formel en amont
  - ✓ Révéler les ambiguïtés
  - ✓ Détecter les erreurs au plus tôt
  - ✓ Consolidation des phases amont
  - ✓ Produit plus mûr plus tôt
  - ✓ Phases amont plus coûteuses
    - Mais développement globalement plus efficace

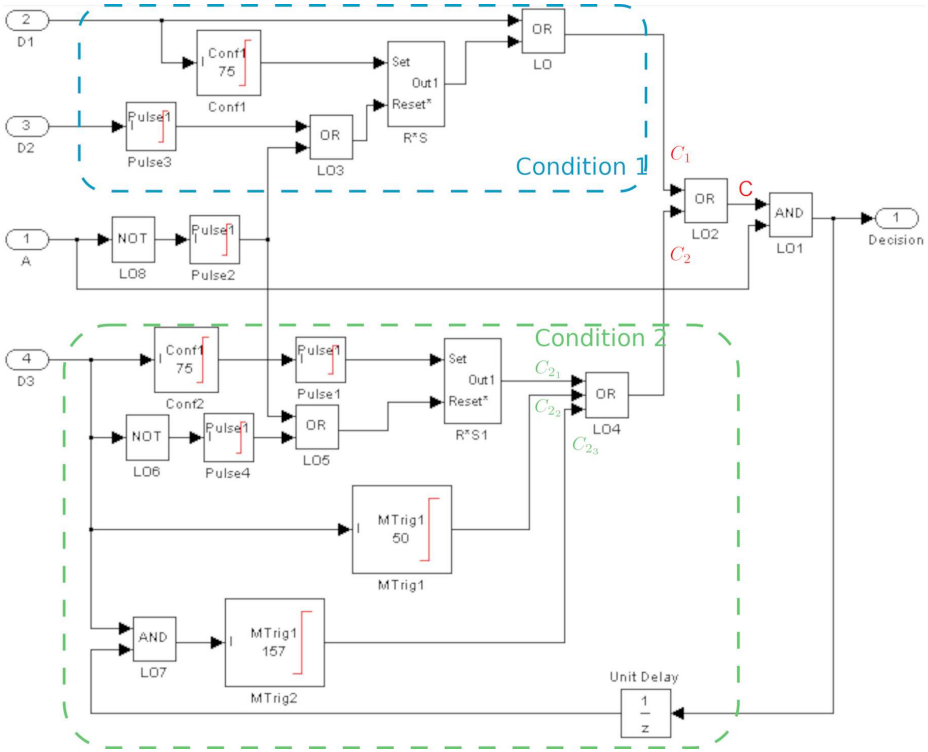



Projets NASA: corrélation effort phases amont / respect budget

ONERA
THE FRENCH AEROSPACE LAB

# Modélisation pour la simulation

- Prototypage, exploration de choix de conception
- Validation par test de modèles

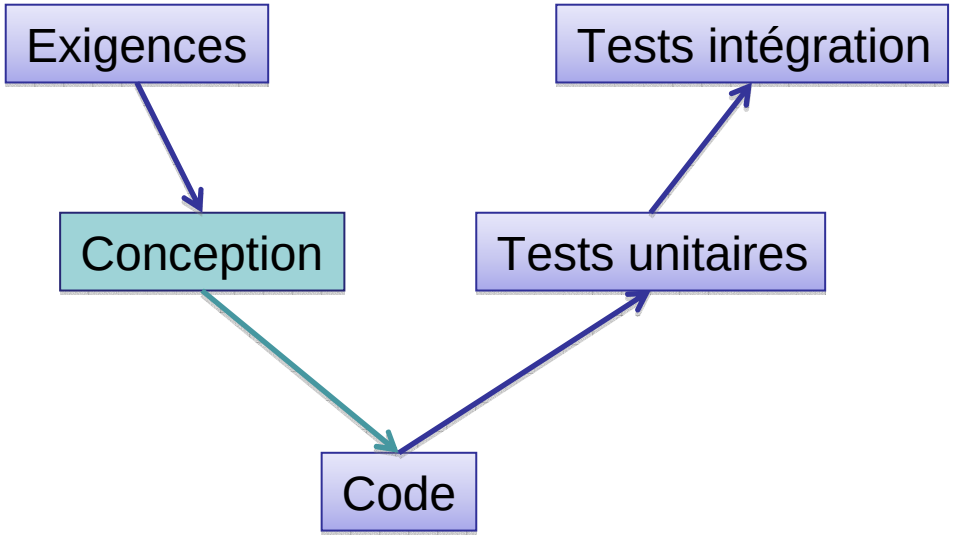



Exemple scade

ONERA
THE FRENCH AEROSPACE LAB

# Génération de code

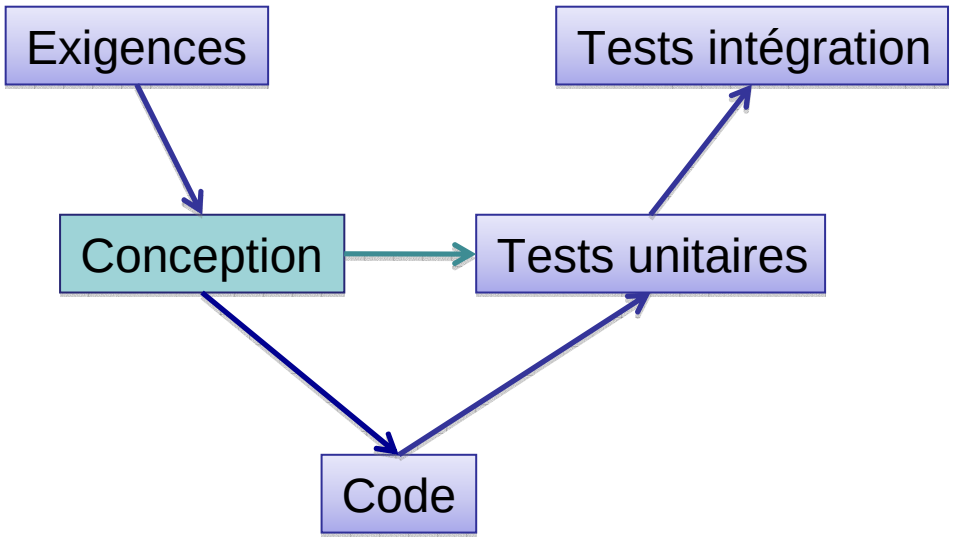
- Génération automatique de code à partir de modèles
  - ✓ Pas d'erreur de codage manuel
  - ✓ Gain en productivité
  - ✓ Vérification au plus tôt sur le modèle




ONERA
THE FRENCH AEROSPACE LAB

# Génération de tests

- Génération automatique de tests
  - ✓ Conformité du code par rapport au modèle
  - ✓ Couverture du modèle
  - ✓ Oracle automatisé



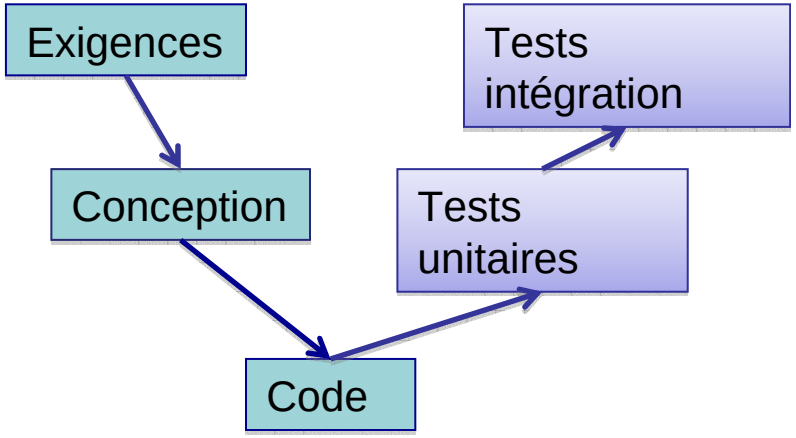

ONERA
THE FRENCH AEROSPACE LAB

# Vérification

- Classique = dynamique
  - ✓ Simulation / test
  - ✓ Non exhaustif
  - ✓ Test exerce le hardware

- Formel = statique
  - ✓ Pas d'exécution
  - ✓ Automatisé
  - ✓ Exhaustif/ propriété considérée

# Vérification




- Vérifications syntaxiques

- Vérification de propriétés génériques
  - Absence de run-time error
  - Calcul de wcet
  - Analyses dédiées

- Vérification de propriétés applicatives
  - ✓ Propriétés définies par l'utilisateur
  - ✓ Propriétés exprimées formellement

# Vérification

- Compromis généralité / automaticité
- Compromis généralité / efficacité

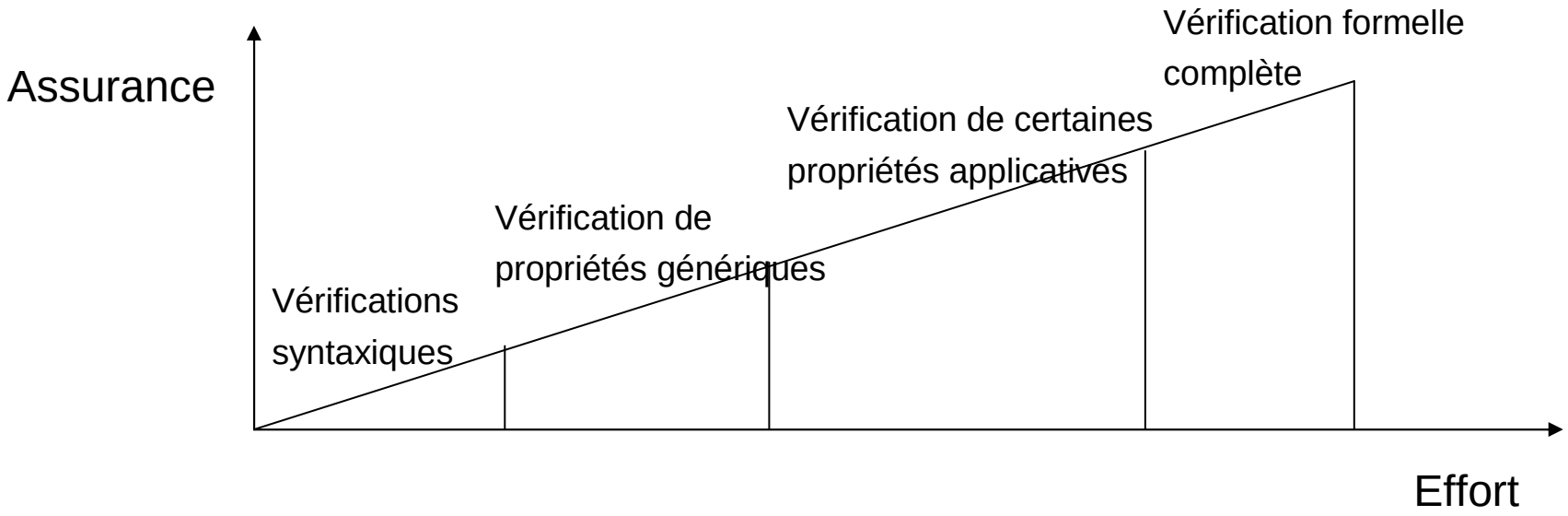
- Attention
  - ✓ Conformité modèle / réel
  - ✓ Hypothèses
  - ✓ Méthode formelle

- Notation :
  sémantique bien définie
- Analyses :
  correction de la technique

ONERA
THE FRENCH AEROSPACE LAB

# Conclusion

- Eventail de techniques
  - ✓ Choisir la bonne technique pour un objectif donné
- Utilisables à différents niveaux
- Nécessitant un investissement plus ou moins important




ONERA
THE FRENCH AEROSPACE LAB

# Différentes techniques

# Différents types de techniques

- Preuve
- Model checking
- Interprétation abstraite

Mais aussi…

- Résolution de contraintes
- Network calculus, analyses d'ordonnançabilité
- Techniques probabilistes

# Pour différents types de propriétés

- Fonctionnel
- Temps réel
- Sûreté de fonctionnement

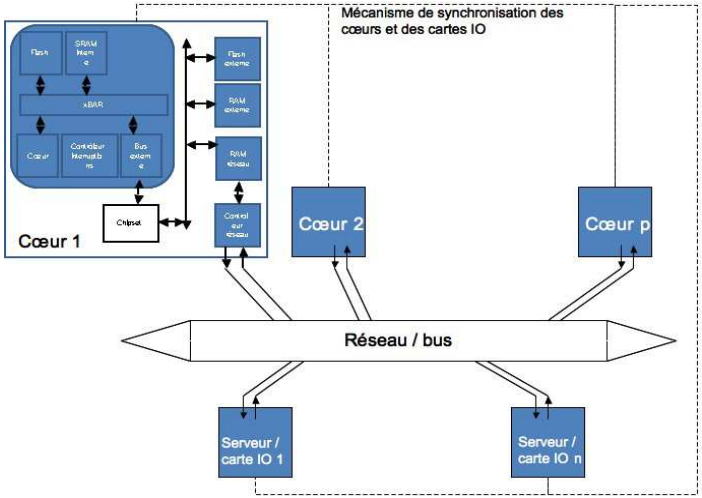
Le système produit les bons résultats

dans les temps

En tenant compte des défaillances

## A différents niveaux

- Plateforme (processeur, réseau)
- Logiciel
- Système




ONERA
THE FRENCH AEROSPACE LAB

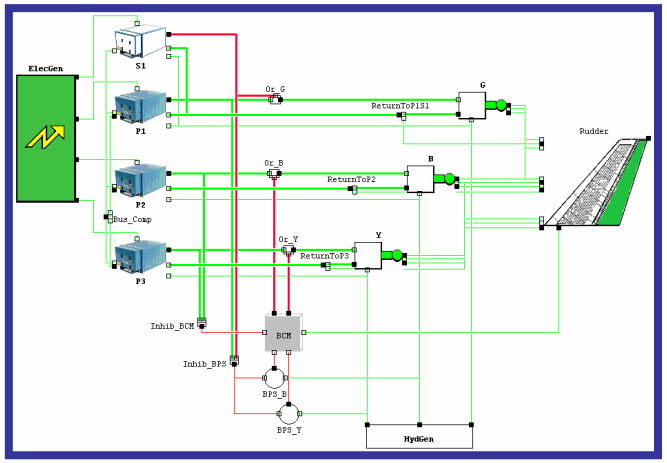
Vehicle

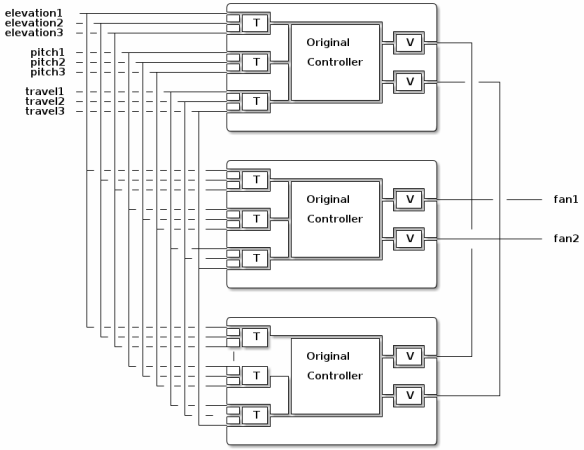
Systems

Software

Platform

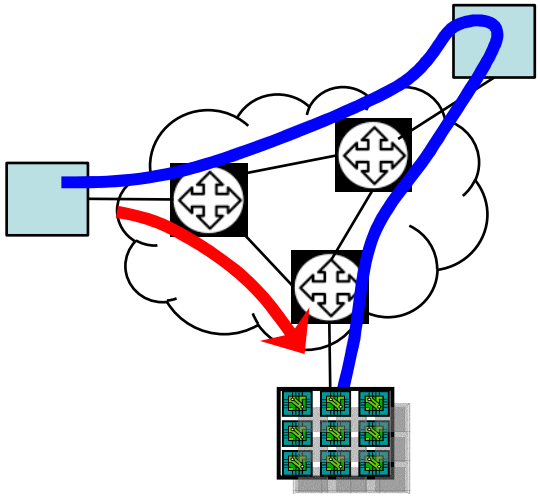
Analyses formelles
de sûreté de fonctionnement
«pas de panne simple amenant
à une catastrophe »




Model checking
de propriétés fonctionnelles
« Le pilote et le copilote n'ont jamais
la priorité en même temps »

Preuve de propriétés fonctionnelles
sur des programmes
« Dans des conditions d'exécution C,
Le résultat de la fonction est X »



Réseau : network calculus pour le calcul
des temps de traversée pire cas
Processeur : interprétation abstraite pour le
calcul du wcet

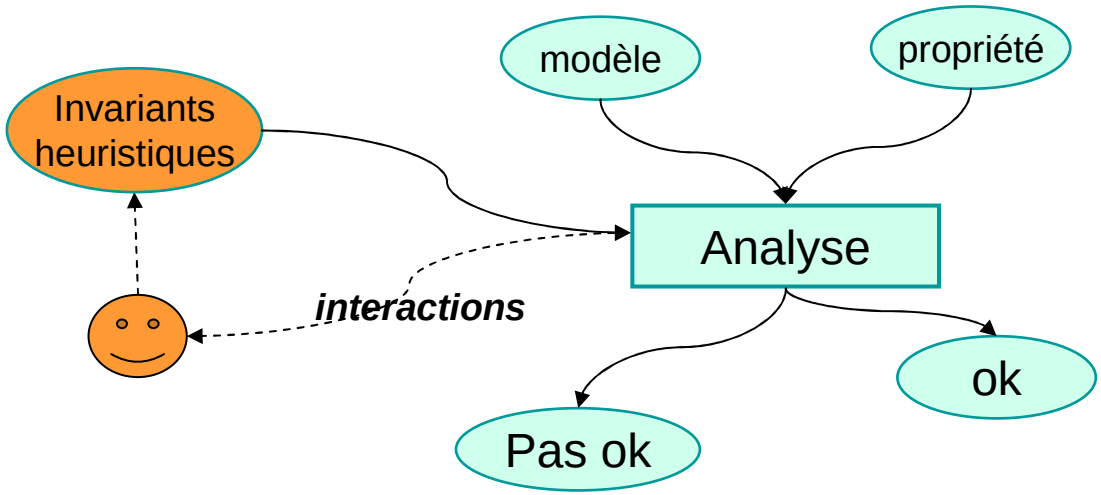
ONERA
THE FRENCH AEROSPACE LAB

# Synthèse

ONERA
THE FRENCH AEROSPACE LAB

# Synthèse

- Automatisation/exhaustivité
- Eventail de techniques
- Spécialiser/adapter pour efficacité
  - ✓ Phase expérimentale
  - ✓ Phase opérationnelle




ONERA
THE FRENCH AEROSPACE LAB

# Synthèse

- Utilisations industrielles
  - ✓ au programme aujourd'hui!
- Certification
  - ✓ Sécurité : méthodes formelles obligatoires pour les plus hauts niveaux de certification des critères communs
  - ✓ Utilisation des méthodes formelles recommandées dans le domaine ferroviaire
  - ✓ Aéronautique : DO-333 supplément technique du DO-178C sur les  méthodes formelles