Méthodes formelles et langages pour le développement de logiciels fiables dans l'industrie

Institut Henri Poincaré, 28 avril 2014

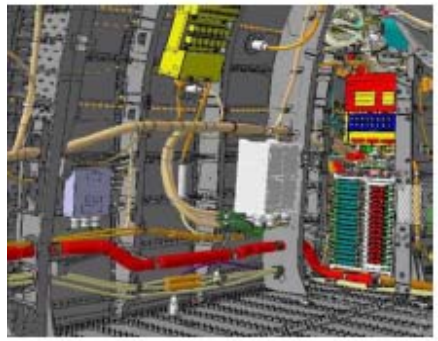
(Δ Analyse de Valeur)
Regard sur 25 ans de méthodes formelles dans l'aéronautique

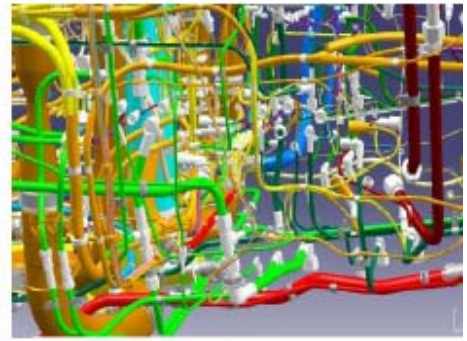
Emmanuel Ledinot
Direction de la Prospective

$\Delta=\lambda f.(f\ f)$

DASSAULT AVIATION

Contexte





- **Ingénierie des systèmes cyber-physiques et des systèmes de mission**
- **Spécification, développement, IVVQ de logiciels critiques**
- **Méthodes Formelles pour la Safety … et plus récemment la Security***

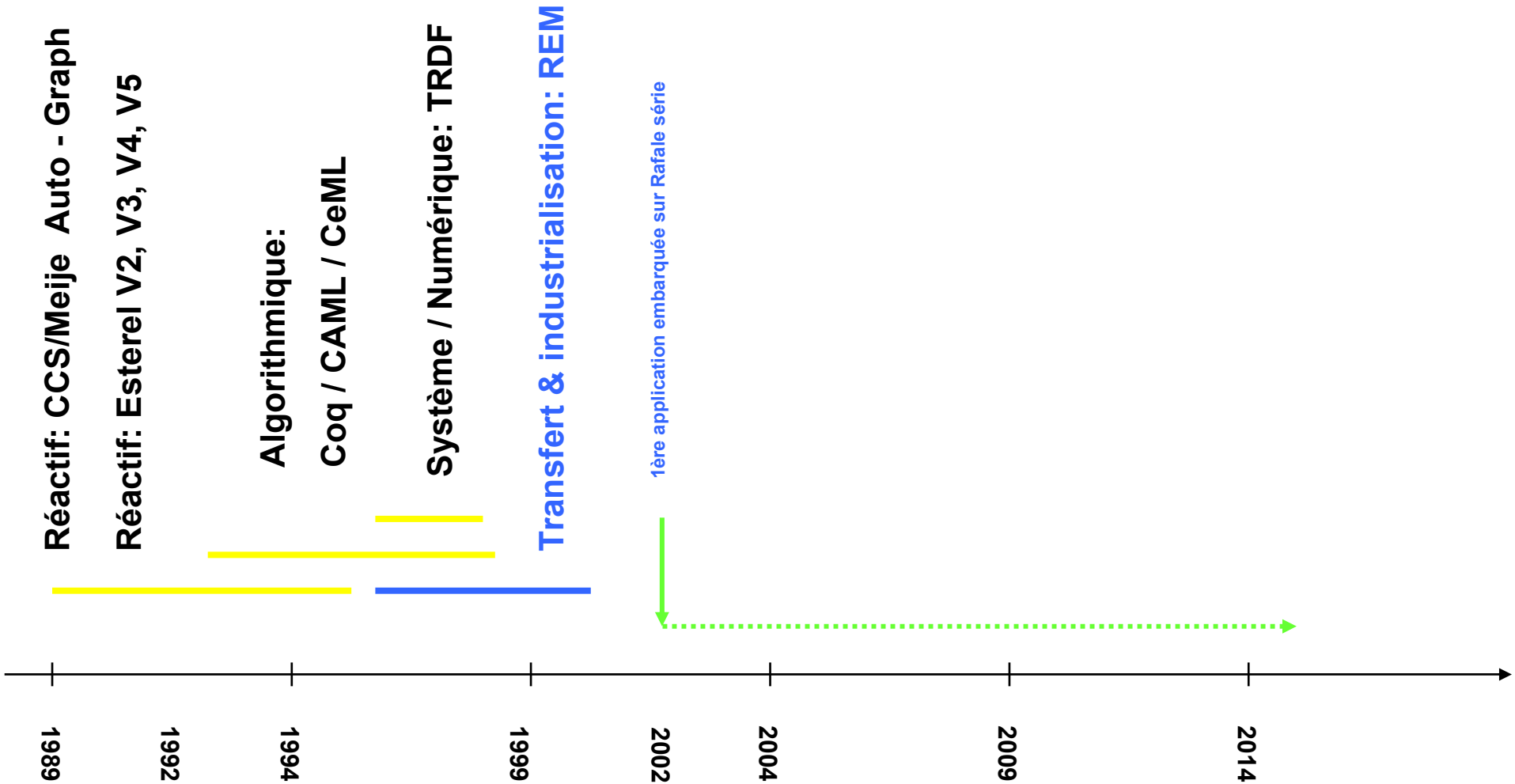
DASSAULT AVIATION

* aspect non traité dans l'exposé

Plan

- **Ancrage**
  - Revue des "success" et "failure" stories Dassault (1989-2014)
- **Constats**
  - Langages, Sémantique, Analyse, Qualification, Diffusion
- **Analyse**
  - (Δ Analyse de Valeur) = ?
- **Perspectives**
  - Proposition d'orientations recherche

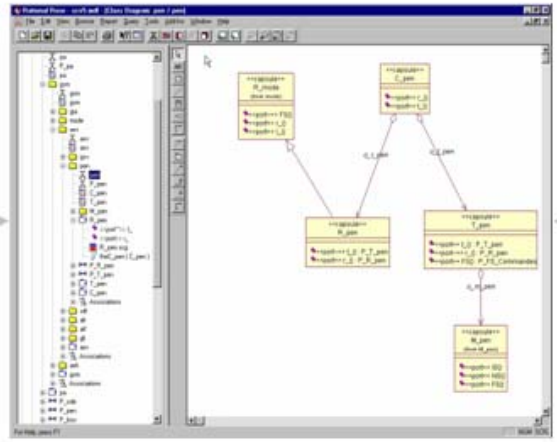
Retour d'expérience 1989-2014



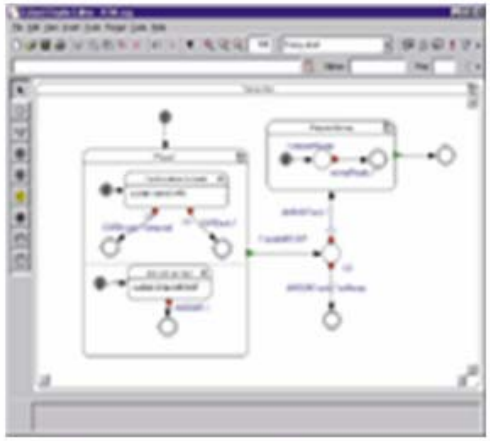
REM: Atelier intégrant IBM/**R**ational Rose, **E**sterel Studio et **M**atlab/Simulink

Rose / Esterel / Matlab

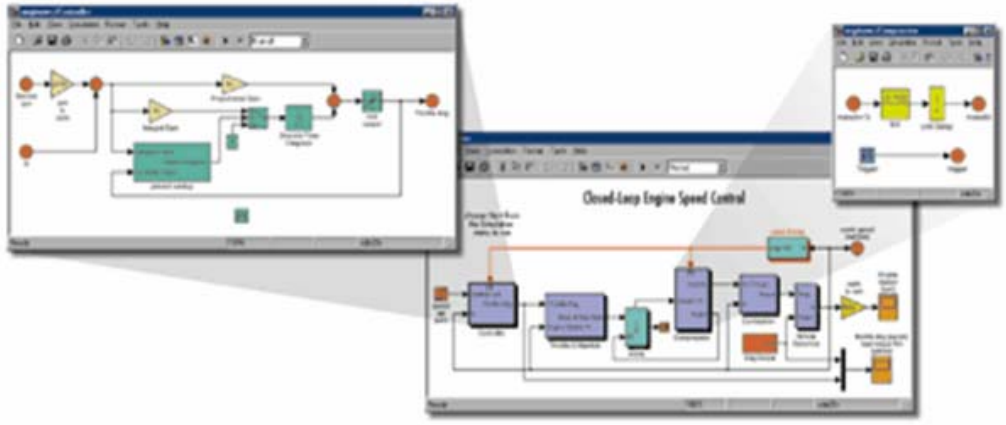
Rose : pour la définition de l'architecture



Esterel studio : pour les fonctions logiques

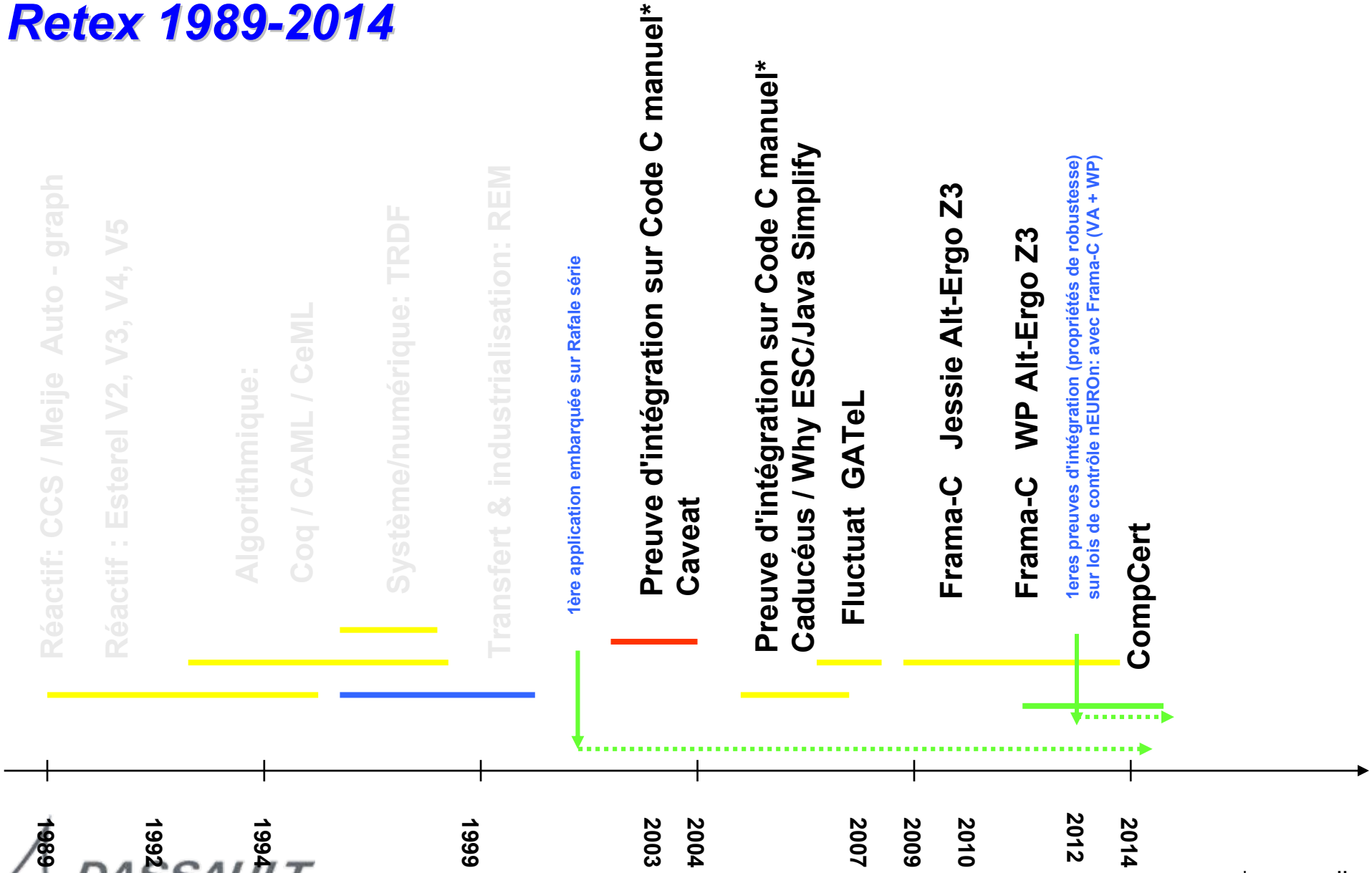


Matlab / Simulink : pour les fonctions d'automatique



DASSAULT

Retex 1989-2014



* avec aliasing

Constats (1/2)

- **Langages**
  - **Choix structurants à long terme**
    - **Esterel .vs. StateCharts, SCADE .vs. Simulink/RTW**
    - **Fonctionnel (Coq + OCaml + CeML) .vs. Impératif (C + Caveat -> Why -> Jessie -> WP)**
    - **Modelica .vs. Simulink**

Constats (1/2)

- Langages
  - Choix structurants à long terme
    - Esterel .vs. StateCharts, SCADE .vs. Simulink/RTW
    - Fonctionnel (Coq + OCaml + CeML) .vs. Impératif (C + Caveat -> Why -> Jessie -> WP)
    - Modelica .vs. Simulink

- **Sémantique**
  - **Causalité pour les langages synchrones**
    - **Diagnostic des cycles, préemption forte/faible, arbitrages intégration flots de données / syncharts**
  - **Causalité pour les systèmes hybrides**
  - **Calcul des Constructions Inductives, isomorphisme de Curry-Howard**
    - **programmation par preuve, paradigme intéressant du développement correct par construction**
    - **Réalise l'esprit de la DO-178:**

      - le calcul doit réaliser toutes les exigences

      - et rien de plus

      Identité entre structure du programme et structure de sa justification de conformité à la spécification: → garantie d'absence de code non traçable et non activable *fonctionnellement*

Idéal en théorie Inutilisable en pratique (industrielle)

Constats (2/2)

- **Analyse**
  - **Apparition des BDD et du calcul symbolique sur les systèmes à états finis (~90s): véritable rupture**
  - **Frama-C: "Cadriciel" ouvert multi-paradigmes d'analyse statique (~07) : a été décisif pour parvenir aux premières preuves d'intégration**

Constats (2/2)

- Analyse
  - Apparition des BDD et du calcul symbolique sur les systèmes à états finis (~90s): véritable rupture
  - Frama-C: "Cadriciel" ouvert multi-paradigmes d'analyse statique (~07) : a été décisif pour parvenir aux premières preuves d'intégration

- **Entreprenariat**
  - **Dimensionnant: Verilog, Ilog, Simulog, Esterel Tech., Polyspace, Prover, TrustInSoft, …**
  - **Prise de risque Esterel Studio .vs. Statemate en 1995: importance de l'implication de Thales**

Constats (2/2)

- Analyse
  - Apparition des BDD et du calcul symbolique sur les systèmes à états finis (~90s): véritable rupture
  - Frama-C: "Cadriciel" ouvert multi-paradigmes d'analyse statique (~07) : a été décisif pour parvenir aux premières preuves d'intégration
- Entreprenariat
  - Dimensionnant: Verilog, Ilog, Simulog, Esterel Tech., Polyspace, Prover, TrustInSoft, …
  - Prise de risque Esterel Studio .vs. Statemate en 1995: importance de l'implication de Thales
- **Base de pré-qualification d'outils par le produit**
  - **CompCert: premier cas validé utilisable en opérationnel. Apporte:**
    - **Garantie 0-bug du compilateur C**
    - **Transfert de propriétés prouvées par analyse statique du source C vers l'assembleur**
    - **Dissemblance 100% par rapport aux compilateurs C commerciaux (.vs. partage de parties de gcc)**
  - **Généralisation à des bases de confiance (noyaux prouvés corrects) d'outils de développement & vérification**

DASSAULT AVIATION

Petites phrases ici et là

- **"Les méthodes formelles perceront le jour où elles traiteront le *non* critique"**
- **"On veut des outils push-button, ça doit être du push button"**

- **"On prouve les propriétés les plus critiques. On vérifie qu'on peut toujours calculer l'espace d'états accessibles, si on ne peut plus, on revoit le design. On aimerait bien utiliser davantage la preuve, mais on n'a pas le temps.**

- **"Ce qu'on retient surtout, c'est qu'à notre grande surprise, l'utilisation des méthodes formelles nous a fait réduire la taille par 10"**

DASSAULT AVIATION

(Δ Analyse de Valeur)

- **La vérification formelle est insuffisamment efficiente pour**
  - **être applicable à tout type de criticité de logiciel**
  - **être utilisée par les développeurs eux-mêmes*, e.g les concepteurs de lois de contrôle**
  - **être applicable aux propriétés fonctionnelles "boucle fermée" (physique temps continu)**

* sauf peut être le model checking, plus accessible

** en vérification unitaire, substitution à iso ou moindre coût mise en œuvre par Airbus

(Δ Analyse de Valeur)

- La vérification formelle est insuffisamment efficiente pour
  - être applicable à tout type de criticité de logiciel
  - être utilisée par les développeurs eux-mêmes*, e.g les concepteurs de lois de contrôle
  - être applicable aux propriétés fonctionnelles "boucle fermée" (physique temps continu)

- **Différentiateur exhaustivité: modéré**
  - **l'assurance développement par le processus (DO-178) et la vérification dynamique (tests) permettent d'atteindre les objectifs réglementaires de sûreté**
  - **la contrainte économique exclut un surcoût pour un complément de couverture de vérification avéré non nécessaire**
  - **en vérification d'intégration la preuve est nécessairement un complément** aux tests, donc un surcoût**

* sauf peut être le model checking, plus accessible

** en vérification unitaire, substitution à iso ou moindre coût mise en œuvre par Airbus

DASSAULT AVIATION

(Δ Analyse de Valeur)

- **Requête outils "Presse-Bouton"**
  - **Composante 1 : ignorance des limites intrinsèques de décidabilité et de complexité**
  - **Composante 2 : refus d'utiliser des outils FM insuffisamment matures**

DASSAULT AVIATION

(Δ Analyse de Valeur)

- Requête outils "Presse-Bouton"
  - Composante 1 : ignorance des limites intrinsèques de décidabilité et complexité
  - Composante 2 : refus d'utiliser des outils FM insuffisamment matures

- **Valeur insuffisamment mise en valeur**
  - **Vérifier formellement contraint à faire petit, simple, structuré, régulier, compris**
  - **Contrainte à valeur économique potentielle**
    - **Bien qu'il soit difficile de démontrer qu'on a gagné l'argent qu'on aurait dépensé en plus en faisant plus complexe**
    - **dépendance (complexité ⇔ coût) : fortement non linéaire**

DASSAULT AVIATION

(Δ Analyse de Valeur)

- **Vérifier formellement contraint à dégager la structure d'invariants**
  - **Du problème à résoudre par le comportement à réaliser**
  - **Du comportement réalisé pour satisfaire les propriétés du problème posé**

DASSAULT AVIATION

* hors model checking états finis, surtout en preuve d'intégration comportant des propriétés numériques complexes

(Δ Analyse de Valeur)

- Vérifier formellement contraint à dégager la structure d'invariants
  - Du problème à résoudre par le comportement à réaliser
  - Du comportement réalisé pour satisfaire les propriétés du problème posé

- **Dégager la structure d'invariants conduit à**
  - **Maximiser l'uniformité**
  - **Minimiser le nombre de "situations" à vérifier (cas, modes, exceptions, …)**
  - **Expliciter les principes de fonctionnement, favorable à**
    - **la formation des utilisateurs du comportement réalisé**
    - **la maintenance (corrective et évolutive) des développements, notamment par des tierces parties**
    - **l'intérêt que trouvent les développeurs et les vérificateurs à leur travail**

Méthodes Formelles comme rasoir d'Ockham ?

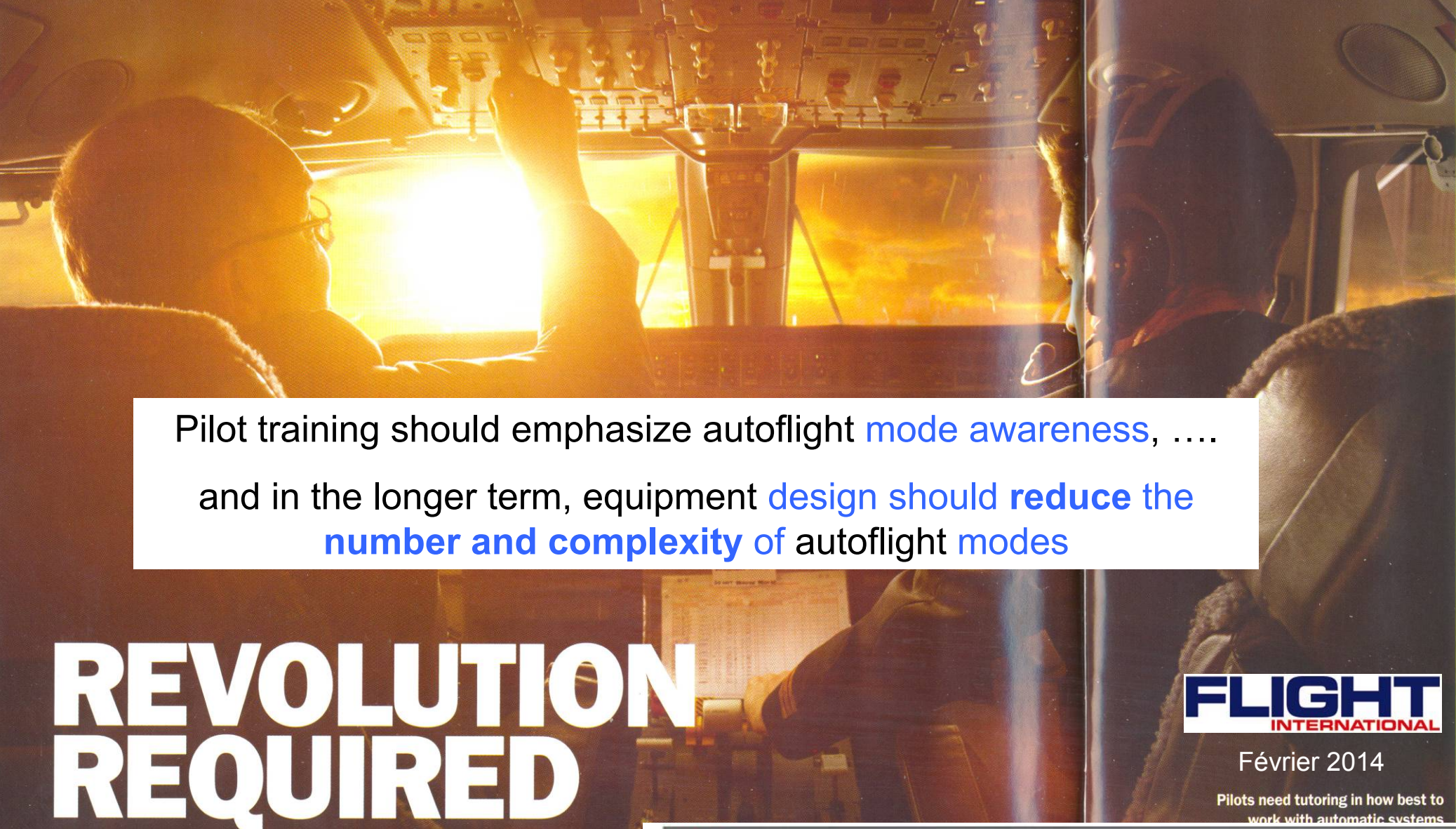
- **Rasoir d'Ockham: "Point de Pluralité sans Nécessité"**
  - **Valeur: simple de faire compliqué, compliqué de faire simple**

Méthodes Formelles comme rasoir d'Ockham ?

- **Rasoir d'Ockham: "Point de Pluralité sans Nécessité"**
  - **Valeur: simple de faire compliqué, compliqué de faire simple**

- **Pertinence pour l'aéronautique**
  - **Source: Flight International Février 2014**
    Synthèse d'un rapport d'étude FAA 2013 sur la formation des pilotes et les situation d'incompréhension des états systèmes
  - **Parmi les recommandations, incitation à revoir le concept d'emploi des automatismes et la complexité des logiques systèmes**

DASSAULT AVIATION



Pilot training should emphasize autoflight mode awareness, ….

and in the longer term, equipment design should **reduce** the **number and complexity** of autoflight modes

REVOLUTION REQUIRED

FLIGHT INTERNATIONAL

Février 2014

Pilots need tutoring in how best to work with automatic systems

Pilots are still essential for safe flying, but increased cockpit automation has uncovered fundamental training needs, a new

tion Administration decided som must be done, but it also realised that quired changes in pilot training philo might be so profound that they woul to build a case based on irrefutable d the industry would flinch from the lenge. So the FAA, working with in

ANALYSIS

WORKING GROUP RECOMMENDATIONS

■ Develop and implement standards and guidance for maintaining and improving knowledge and skills for manual flight operations, and provide pilots with opportunities to refine this knowledge and practice the skills. Training and checking should directly address this topic, and "operators' policies for flight

autoflight mode awareness, and in the longer term, equipment design should reduce the number and complexity of autoflight modes.

■ Information automation (for example integrated navigation displays, electronic flightbags) and its purpose should be more carefully defined, and pilots should be

should be designed to support pilots in their flight guidance tasks, rather than make the pilot an observer.

■ Highly integrated automated systems design should take account of failures that could result from systems integration, and the validation process improved.

the pilots.

■ Develop flightcrew strategies to help them address malfunctions for which there is no specific procedure.

■ Update SOPs appropriately as operational experience suggests.

■ Flightpath management: teach crew to concentrate on the flight-

Méthodes Formelles comme rasoir d'Ockham?

- Rasoir d'Ockham: "Point de Pluralité sans Nécessité"
  - Maximiser l'uniformité, Minimiser l'irrégularité (cas, modes, exceptions,…)
  - Valeur: simple de faire compliqué, compliqué de faire simple

- Pertinence pour l'aéronautique
  - Source: Flight International Février 2014,
  - Parmi les recommandations, incitation à revoir concepts d'emploi et complexité des logiques systèmes

- **Perspective de moyen outillé de contention de la complexité?**
  - **par la formalisation logique et pas seulement comportementale**
  - **par la contrainte de rendre compte exhaustivement de la combinatoire implicite**
  - **Exigence d'exhaustivité comme contrainte de régularisation logique en conception autant, sinon plus, que comme accroissement de couverture en vérification**

DASSAULT AVIATION

Une Orientation Générale Partagée

- **Extrait des Entretiens de Toulouse 2014**
  - **Avec l'aimable autorisation d'Hervé Delseny d'Airbus**
  - **Partie d'une planche de présentation des avantages constatés des méthodes formelles par rapport au test**
  - **Comprendre en premier**
  - **Exhaustivité de la vérification de conformité (correctness) en second**

AIRBUS THALES AAE Collège de Polytechnique

Formal Method : Advantages vs Brakers

Formal Methods improve the understanding of specifications

More accuracy and less ambiguity

Proof of conformity to the specification

Proof is exhaustive

DASSAULT AVIATION

Plan

- **Ancrage**
  - Revue des "success" et "failure" stories Dassault (1989-2014)
- **Constats**
  - Langages, Sémantique, Analyse, Qualification, Diffusion
- **Analyse**
  - (Δ Analyse de Valeur) = ?
- **Perspectives**
  - Proposition d'orientations de recherche

DASSAULT AVIATION

Proposition d'orientations de recherche

- **Mener une recherche Méthodes Formelles Orientée Usage**
  - **Exemple: Boogie de Microsoft Research Redmond pour (C#, Spec#)**
  - **Approche "correcteur orthographique" sur source annoté par la spécification**
  - **Interactions contextualisées sur les entités manipulées par le développeur**
  - **Disparition des outils formels vu de l'utilisateur, analyse en tâche de fond**
  - **Compatible de toutes les criticités de logiciel et de tous les profils de compétence**
  - **Assure la composante 2 de la requête "push button"**

Proposition d'orientations de recherche

- Mener une recherche Méthodes Formelles Orientée Usage
  - Exemple: Boogie de Microsoft Research Redmond pour (C#, Spec#)
  - Approche "correcteur orthographique"
  - Interactions contextualisées sur les entités manipulées par le développeur
  - Disparition des outils formels vu de l'utilisateur, analyse en tâche de fond
  - Compatible de toutes les criticités de logiciel et de tous les profils de compétence
  - Assure la composante 2 de la requête "push button"

- **Développer des bases de confiance prouvées correctes pour les outils formels**
  - **Prudence des autorités aéronautiques face à la complexité des outils formels (cf. TQL4 du DO-330)**
  - **Promotion des pré-qualifications plus orientées produit que processus**
  - **A l'instar de l'architecture de Coq et de l'exemple CompCert**

Proposition d'orientations de recherche

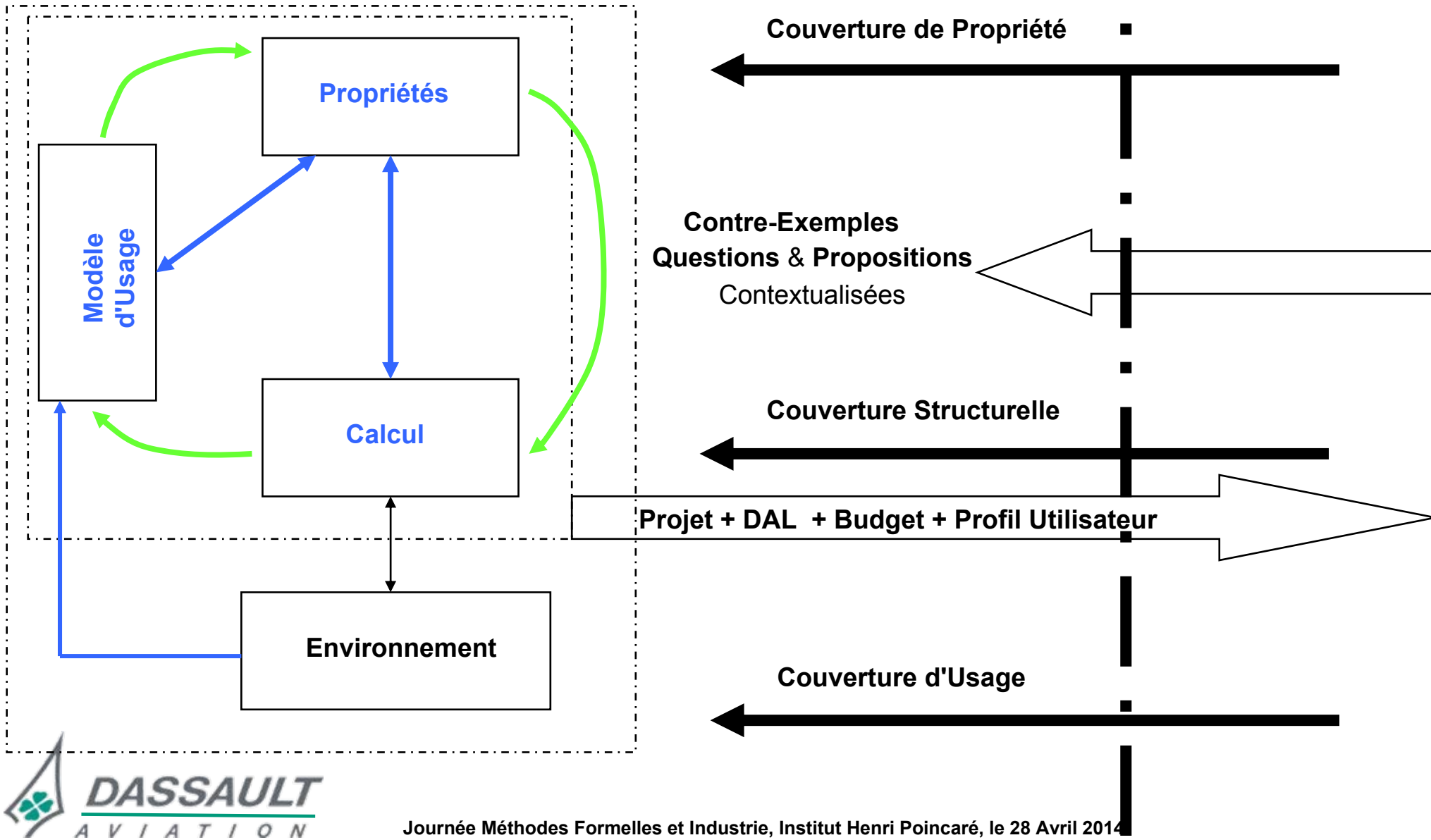
- Mener une recherche Méthodes Formelles Orientée Usage
  - Exemple: Boogie de Microsoft Research Redmond pour (C#, Spec#)
  - Approche "correcteur orthographique"
  - Interactions contextualisées sur les entités manipulées par le développeur
  - Disparition des outils formels vu de l'utilisateur, analyse en tâche de fond
  - Compatible de toutes les criticités de logiciel et de tous les profils de compétence
  - Assure la composante 2 de la requête "push button"

- Développer des base de confiance prouvées correctes pour les outils formels
  - Prudence des autorités aéronautiques face à la complexité des outils formels (cf. TQL4 du DO-330)
  - Promotion d'une base de pré-qualification plus orientée produit
  - A l'instar de Coq et CompCert

- **Développer des techniques pour les vérifications "boucle fermée par la physique"**
  - **Propriétés non exprimables sur les seules variables du logiciel**
  - **Analyse des équations algébro-différentielles de la physique contrôlée par le logiciel**

DASSAULT AVIATION

Recherche Orientée Usage



DASSAULT AVIATION

Vérification Multimodale

- **Multimodalité**
  - **Vérification par analyse statique et dynamique**
  - **Exploration déterministe et aléatoire, dirigée* par la *spécification* et *le modèle d'usage***
  - **Coopération de tous les domaines de valeur au service de la couverture de vérification, sous contrainte de budget ingénieurs + temps de calcul**

DASSAULT AVIATION

* Requis par la DO-178: requirement-based verification

Vérification Multimodale

- Multimodalité
  - Vérification par analyse statique et dynamique
  - Exploration déterministe et aléatoire, dirigée* par la *spécification* et *le modèle d'usage*
  - Coopération de tous les domaines de valeur au service de la couverture de vérification, sous contrainte de budget ingénieurs + temps de calcul

- **Stratégie d'exploration de la relation de conformité, fonction**
  - **du DAL et des contraintes réglementaires de couverture associées**
  - **du modèle d'usage (langage ou distribution des traces d'entrée)**
  - **du budget heures ingénieurs (composante 1) et temps de calcul (PC, cluster HPC)**
  - **de la difficulté à faire croitre la couverture: itérations trajectoire → faisceau → tube → preuve**

DASSAULT AVIATION

* Requis par la DO-178: requirement-based verification

Vérification Multimodale

- Multimodalité
  - Vérification par analyse statique et dynamique
  - Exploration déterministe et aléatoire, dirigée* par la *spécification* et *le modèle d'usage*
  - Coopération de toutes les techniques au service de la couverture de vérification, sous contrainte de budget ingénieurs + temps de calcul

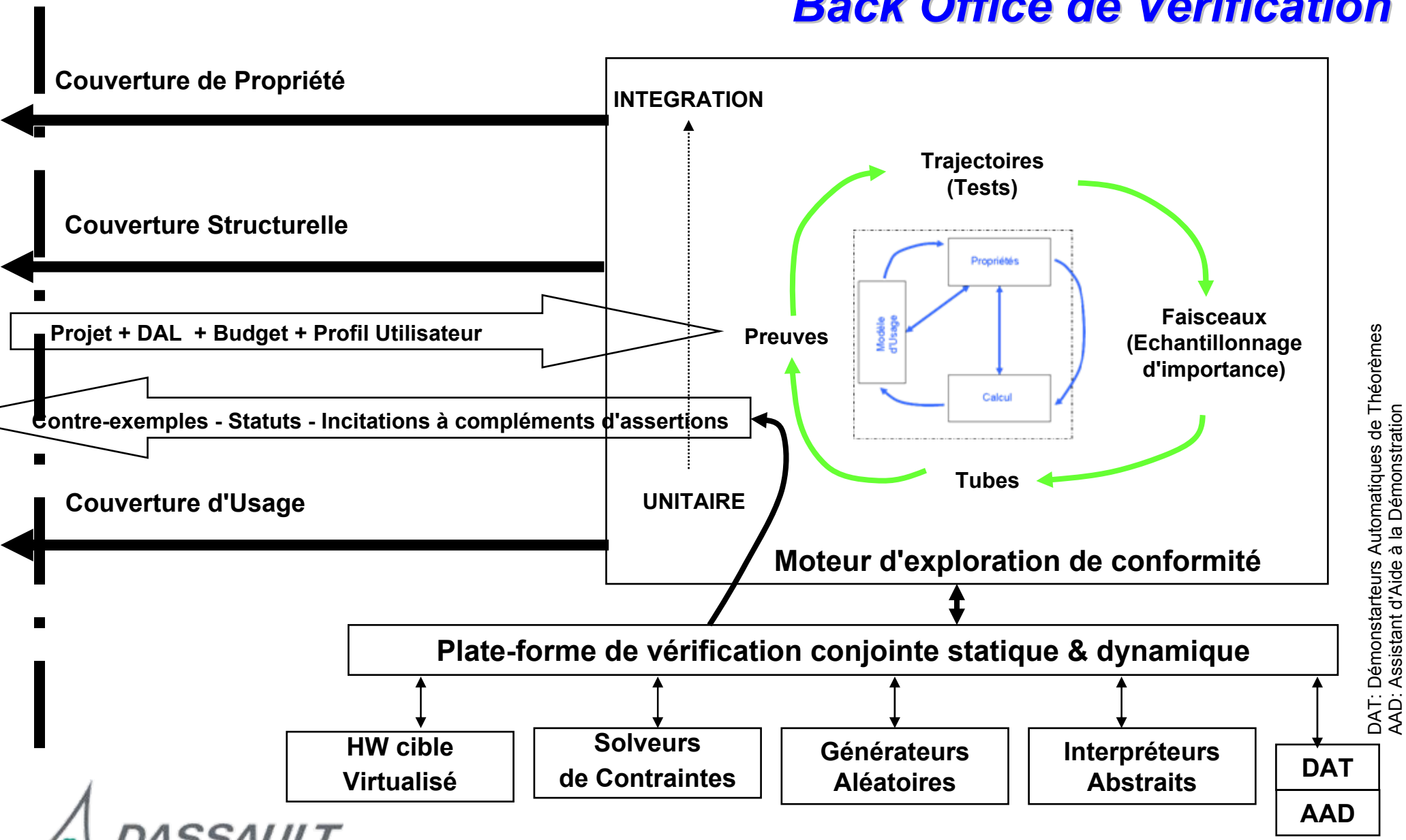
- Stratégie d'exploration de la relation de conformité, fonction
  - du DAL et des contraintes réglementaires de couverture associées
  - du modèle d'usage (langage ou distribution de traces d'entrée)
  - du budget heures ingénieurs (composante 1) et temps de calcul (PC, cluster HPC)
  - de la difficulté à faire croitre la couverture: itérations trajectoire → faisceau → tube → preuve

- **Principe**
  - **Ecriture unique ((Propriétés, Usage), Code ou Modèle), exploitation multiple en vérification**
  - **Génération automatique cas de test / cas de preuve**
  - **Supprimer la problématique du coût additionnel - piloter le choix du moyen de vérification par le rapport efficacité / coût et les contraintes (économiques, DAL)**

DASSAULT AVIATION

* Requis par la DO-178: requirement-based verification

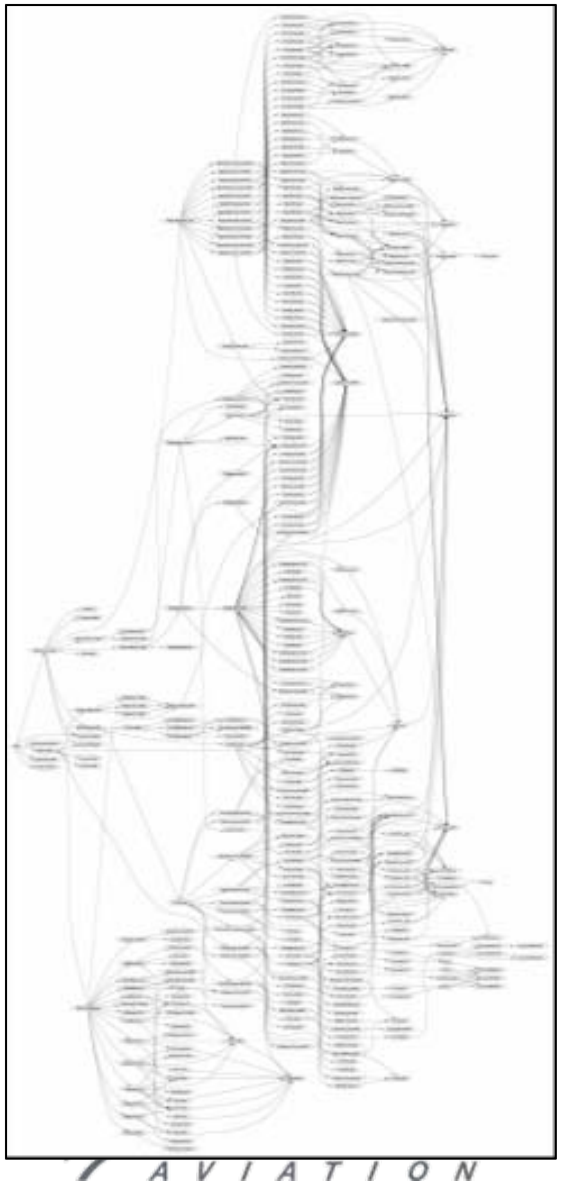
Back Office de Vérification



DAT: Démonstarteurs Automatiques de Théorèmes
AAD: Assistant d'Aide à la Démonstration

DASSAULT AVIATION

Vers une vérification multimodale avec Frama-C



Frama-C

File Project Analyses Help

Exit | Source files | Reparse | Load session | Save session | Back | Forward | Analyses | Stop

Source file

A
f_Ta
fa_Ta
fb_Ta
ffic_Ta

WP

Model: Store

Prover: Alt-Ergo

RTE Split Trace

Invariants References

Depth: 0 Scripts...

Timeout: 10 Process: 4

Slicing

Activate: None

Enable 1 Verbosi

Libraries 2 Level

Impact

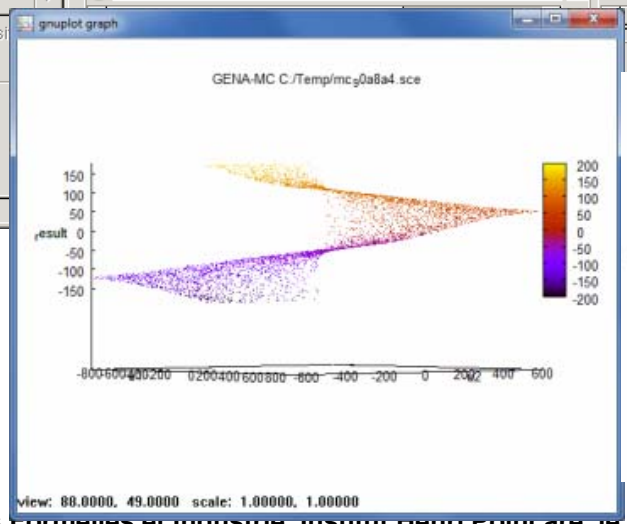
Metrics

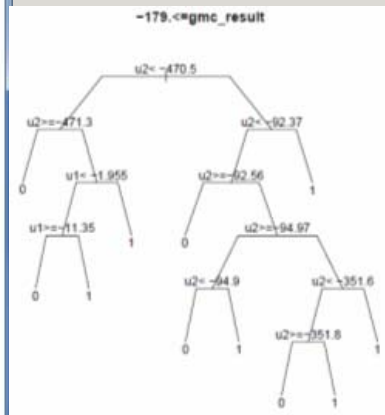
Occurrence

```
index2 = (unsigned int)0;
theSum = (unsigned int)0;
a_HUB = (unsigned int)0;
b_HUB = (unsigned int)0;
n1 = f_Ta((double *)TaHUB);
index1 = (unsigned int)0;
/*@ loop invariant 0 <= theSum && theSum <= mysum
    loop invariant 0 <= index1 && index1 <= n1;
    loop allocates \nothing;
    loop assigns theSum, index1, *TaHUB, a_HUB, b_HUB
    loop variant n1-index1;
*/
while (index1 < n1) {
  a_HUB = fa_Ta(*(TaHUB + index1));
  b_HUB = fb_Ta(*(TaHUB + index1));
  /*@ assert ROBUSTNESS_PROPERTY: 0 <= theSum;
  *(TaHUB + index1) = (double)ffic_Ta((double *)TaH
  theSum = (unsigned int)0;
  index2 = a_HUB;
  /*@ loop invariant a_HUB <= index2 && index2 <= b_
      loop invariant theSum == mysum{Here}(a_HUB, ind
      loop allocates \nothing;
      loop assigns theSum, index2;
```

Sensor_Accu.c

```
40                  loop variant n1-index1;
41      */
42      for(index1=0 ; index1<n1 ; index1++)
43      {
44          a_HUB = fa_Ta(*(TaHUB + index1));
45          b_HUB = fb_Ta(*(TaHUB + index1));
46          //@ assert ROBUSTNESS_PROPERTY: 0
47          *(TaHUB + index1) = ffic_Ta(TaHUB,the
48          theSum = 0;
49          /*@ loop invariant a_HUB<=index2<=b
50                  loop invariant theSum == my
51                  loop assigns theSum,index2;
52                  loop variant b_HUB-index2;
53          */
54          for(index2=a_HUB ; index2<b_HUB ; inc
55          {
56              theSum += index2;
57          }
58      }
59      return theSum;
60  }
```





En guise de conclusion

- **Une réelle progression de l'outillage et de l'utilisation opérationnelle**
  - **Malgré de nombreux tâtonnements**
  - **Malgré un impact limité pour le contrôle commande (continu)**

DASSAULT AVIATION

En guise de conclusion

- **Une réelle progression de l'outillage et de l'utilisation opérationnelle**
  - **Malgré de nombreux tâtonnements**
  - **Malgré un impact limité pour le contrôle commande (continu)**

- **Minimisation de la pluralité, valeur sous valorisée**

- **Exhaustivité, différentiateur sur valorisé en contexte de succès de l'assurance développement par le processus**

DASSAULT AVIATION

En guise de conclusion

- Une réelle progression de l'outillage et de l'utilisation opérationnelle
  - Malgré de nombreux tâtonnements
  - Malgré un impact limité pour le contrôle commande (continu)
- Minimisation de la pluralité, valeur sous valorisée
- Exhaustivité, différentiateur sur valorisé en contexte de succès de l'assurance développement par le processus
- **Mener une recherche intégrative orientée usage**
- **Piloter la couverture de vérification (usage et structure) par le compromis efficacité / coût uniformément pour toutes les modalités d'exploration**

DASSAULT AVIATION

En guise de conclusion

- Une réelle progression de l'outillage et de l'utilisation opérationnelle
  - Malgré de nombreux tâtonnements
  - Malgré un impact limité pour le contrôle commande (continu)
- Minimisation de la pluralité, valeur sous valorisée
- Exhaustivité, différentiateur sur valorisé en contexte d'évolution des processus sous pression essentiellement économique
- Mener une recherche intégrative orientée usage
- Piloter la couverture de vérification (usage et structure) par le compromis efficacité / coût uniformément pour toutes les modalités d'exploration
- **Encore beaucoup de temps avant de pouvoir fermer la boucle**

DASSAULT AVIATION