Aide à la spécification et au développement formel de systèmes

Nicolas Stouls *(Nicolas.Stouls@imag.fr)*
Laboratoire LSR IMAG, Saint Martin d'Hères France

Cadre, motivations et Méthode :

Cadre :

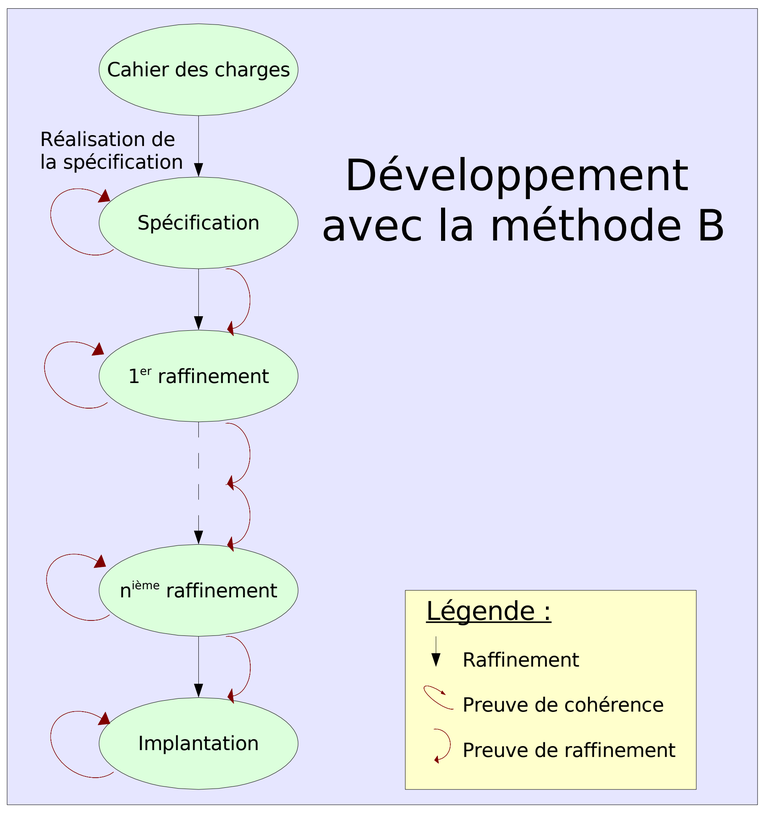
- Développements formels de **logiciels**
  Méthode B
- **Validation / sécurité** des systèmes
  Spécification et vérification de règles de sécurité
- **Systèmes embarqués**
  Cartes à puce, composants réseau, automobile, ...

Motivations :

- Erreurs moins coûteuses si trouvées dès la spécification
- Méthodes actuelles de vérification des spécifications :
  - Relecture *(Garanties **non quantifiables**)*
  - Test système *(**Après implantation** complète)*
  - Preuve *(Risque de sous spécification, **difficultés d'expression** des propriétés, partiellement automatique)*

Méthode :

- Retro-ingénierie des spécifications
  *Automate **symbolique** sémantiquement **équivalent** à la spécification initiale*
  Prise en compte du raffinement
  Choix du niveau de granularité de la vision pour un système modulaire
- Aide à la compréhension
  *Complémentarité des **points de vue** affichés*
- Aide à la vérification
  *Proposition d'un **langage** d'expression des **propriétés de sécurité** et d'une **méthode de vérification***



Projets et partenariats :

Projets :

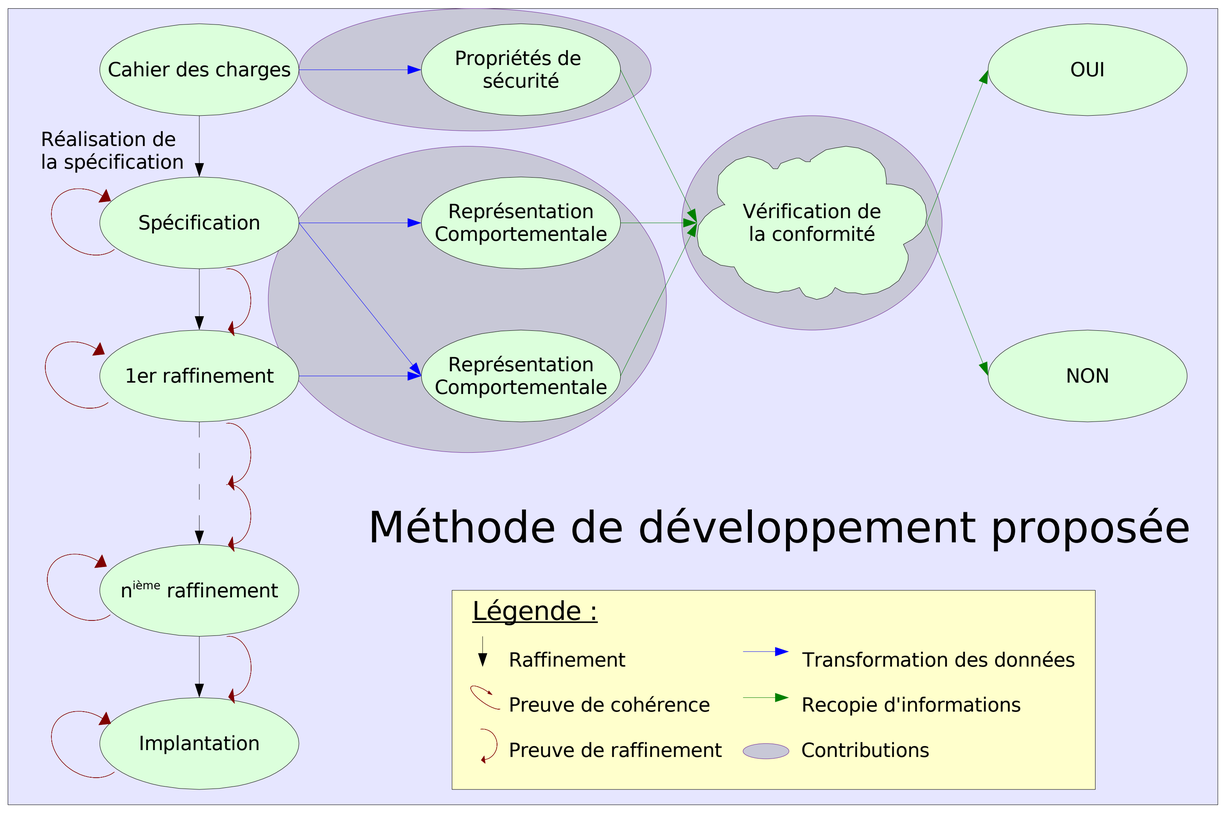
- RNTL BOM *(2001-2003)*
  B optimisant la mémoire, pour génération de code pour cartes à puce.
- RNTL EDEN *(2002-2005)*
  Validation formelle de logiciels pour certification de plus haut niveau selon les critères communs.
- ACI sécurité GECCOO *(2003-2006)*
  Génération de code certifié pour des applications orientées objets.
- Projet IMAG MODESTE *(2004-2006)*
  Modélisation pour la sécurité : Tests et raffinement en vue d'un processus de certification.
- ACI sécurité POTESTAT *(2004-2007)*
  Politiques de sécurité : Test et analyse par le test de réseaux ouverts.
- RNTL POSE *(2006-2007)*
  Tests de conformité de politiques de sécurité de systèmes enfouis.

Partenaires industriels :

- Axalto *(Louveciennes)*
- Leirios *(Lyon)*
- Gemplus *(Gémenos)*
- Silicomp-AQL *(Rennes)*
- ST Microelectronics *(Crolles)*
- ClearSy *(Anciennement Stéria, Aix en Provence)*
- Trusted Logic *(Versailles)*

Partenaires publiques :

- CEA/LIST *(Fontenay-aux-Roses)*
- CEA/LETI *(Grenoble)*
- IMAG/LSR *(Grenoble)*
- IMAG/VERIMAG *(Grenoble)*
- INRIA *(Sophia Antipolis)*
- INRIA Futurs *(Saclay)*
- IRISA *(Rennes)*
- LIFC *(Besançon)*
- LORIA *(Nancy)*
- LRI *(Orsay)*



Etudes de cas réalisées :

- DEMONEY : *Applet JavaCard de porte-monnaie électronique utilisant les différents composants de sécurité fournis par JavaCard (© Trusted Logic).*
  Particularités :
  - *Prise en compte de la **modularité***
  - *Prise en compte du **raffinement***

- Site internet de B4free : *Modélisation des autorisations de téléchargement de l'outil B4free (© ClearSy).*
  Particularités :
  - *Proposition d'une **méthode** permettant d'expliciter certaines propriétés sur l'automate.*
  - *Prise en compte du **raffinement***

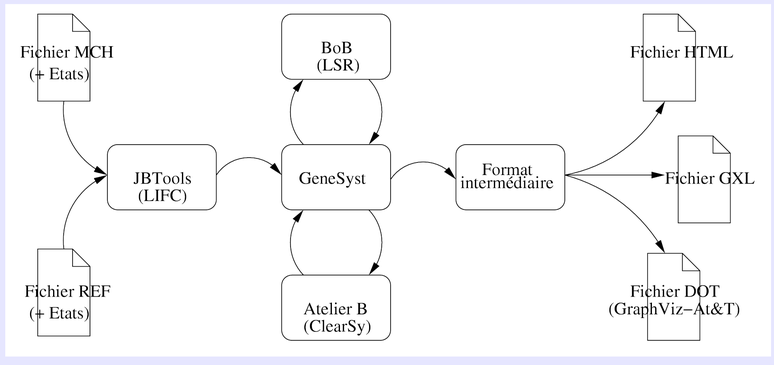
- Moniteur réseau : *Développement d'un observateur réseau détectant les violations d'une politique de sécurité.*
  Particularités :
  - *Raffinements suivant les couches ISO du protocole TCP/IP*
  - ***Conservation des propriétés** de sécurité par raffinement*
  - ***Difficultés** de prise en compte du **raffinement***

Publications :

[1] N. Stouls et V. Darmaillacq. *Développement formel d'un moniteur détectant les violations de politiques de sécurité de réseaux*, AFADL 2006.
[2] D. Bert, M-L. Potet et N.Stouls. GeneSyst: *A Tool to Reason about Behavioral Aspects of B Event Specifications. Application to Security Properties*, LNCS n°3455 p.299-318, Springer-Verlag, ZB 2005.
[3] N. Stouls et M-L. Potet. *Explicitation du contrôle de développement B événementiel*, AFADL-2004
[4] F. Badeau, D. Bert, S. Boulmé, C. Métayer, M-L. Potet, N. Stouls et L. Voisin. *Adaptabilité et validation de la traduction de B vers C - Points de vue du projet BOM,* série TSI, numéro 7/2004, Hermès-Lavoisier.
[5] F. Badeau, D. Bert, S. Boulmé, C. Métayer, M-L. Potet, N. Stouls et L. Voisin. *Traduction de B vers des langages de programmation*, AFADL 2003.

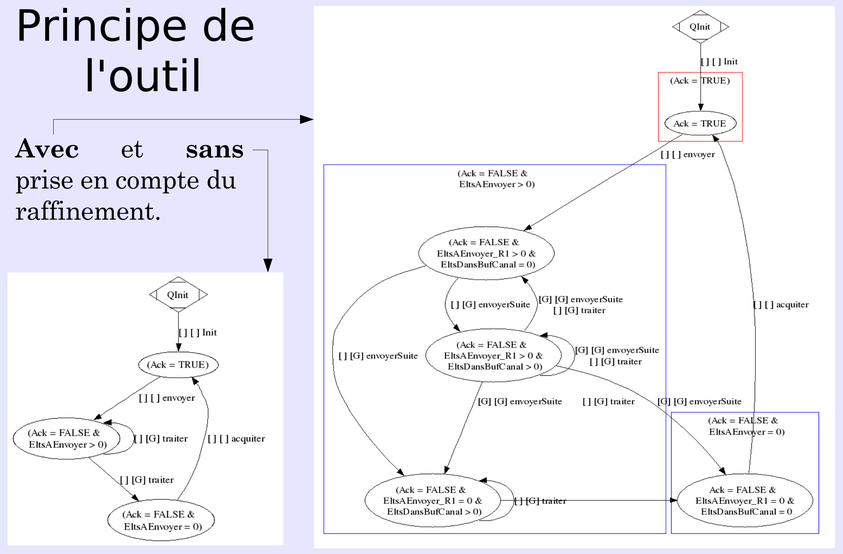
Outil réalisé : *GénéSyst*

- Génération d'un automate comportemental d'une spécification
- Calcul de l'automate **par la preuve**
- Prise en compte du premier niveau de **raffinement**



Principe de l'outil

Avec et **sans** prise en compte du raffinement.



Propositions effectuées :

- Logique d'**expression des propriétés de sécurité** comportementales
- Méthode de **vérification syntaxique** des propriétés sur l'automate

Retombées socio-économiques :

- Aide à la **certification** des systèmes *(Critères communs)*
  ⇨ **Gain quantifiable de confiance** dans la sécurité

(ferroviaire, aéronautique, automobile, carte à puce, téléphone portable, etc)

Bilan :

- Outil
- Utilisation de l'outil sur différentes étude de cas
  - ***Utilité** pour la détection d'incohérences*
  - ***Précision** de l'automate*
  - ***Difficultés** pour la prise en compte du raffinement*
- Utilisation de la logique d'expression des propriétés et de la méthode de vérification
  - ***Expressivité** suffisante*
  - ***Efficacité** de la méthode*

Perspectives :

- Génération de l'automate :
  - Améliorer la prise en compte de la **modularité**
  - Améliorer la **précision** et le **temps d'exécution** de l'outil
- Expression des propriétés :
  - ***Etendre** le langage de description*
  - ***Outiller***