Quelques motivations pour l'usage des méthodes formelles

Slide 1

Christian Attiogbé
Faculté des sciences – Université de Nantes
Christian.Attiogbe@univ-nantes.fr

Motivations générales

Slide 2

- Développer des systèmes sûrs, fiables, robustes
- Inévitable dans les domaines dits critiques
  (sécurité, coût financier, vie humaine, etc)
- Gros projets industriels
  (contrôle de processus, systèmes embarqués, etc)
- Domaine médical, etc

Mais il y a un prix à payer.

Construire un système/des composants : une activité technique/scientifique.

Motivations générales

Slide 3

- Bonne analyse/compréhension des cahiers de charges
- Maîtriser la complexité des systèmes
- Qualité des systèmes (fiabilité)
- Expliquer les limites (rigoureusement)
- Evaluation (rigoureusement)
- Maintenance (évolution, comprendre les fautes, corriger, ...)
- ...

Nécessité de disposer d'outils adéquats : rigueur

Outils d'ingénierie

Motivations : nouveaux systèmes d'exploitation

De plus en plus complexes

Embarqués (dans des appareils divers, d'usage courant)

Par exemple dans les cartes à puces : technologie Smart Cards

Slide 4

⇒ Améliorer le cycle de développement en systématisant certaines tâches

- code (généré et) prouvé correct
- jeu de tests

→ recours aux méthodes formelles

Motivations : certification

Industrialisation de produits (composants, logiciels, systèmes)
Domaine des Technologies de l'Information (sécurité, etc)

- Common Criteria, (norme internationale IS0/IEC 15408)
  (Common Criteria for Information Technology Security Evaluation)
- ITSEC (E4, ...) - norme Européenne correspondante

Information technology – Security techniques – Evaluation criteria for IT security

Slide 5 Exemple ISO/IEC 15408

ITSEC : Critère Européen pour evaluations security,
C'est l'équivalent européen du Critère commun mondial, IS0/IEC 15408, pour les évaluations de sécurité.

Garanties...

Motivations : produits certifiés

Un produit certifié est celui qui a l'agrément d'un organisme de certification (compétent et reconnu) pour sa conformité aux exigences des Critères Communs (CC) et des Méthodologies Communes dans le domaine des technologies de l'information.

Slide 6 Un certificat de CC est toujours accompagné d'un rapport qui contient les informations importantes sur l'évaluation aussi bien que sur l'utilis tion sûre du produit.

Motivations : analyse fine des besoins

$$g(x) = \begin{cases} 1 & si\ x \in \{0,1,2,3,4\} \\ \\ -1 & si\ x \in \{8,9,10,11\} \end{cases}$$

comment définir g ?

Slide 7

$$f(x) = \begin{cases} bleu & si\ x \in \{0,1,3,5\} \\ \\ rouge & si\ x \in \{a,b,d,f\} \end{cases}$$

comment définir f ?

Rapport - Commission d'enquête Ariane 501

Echec du vol Ariane 501

Président de la Commission : Professeur J.-L. LIONS

`www.cnes.fr/espace_pro/communiques/cp96/rapport_501/rapport_501_3.html`

Le vol inaugural d' **Ariane 5** *qui a eu lieu le* **4 juin 1996** *s'est soldé par un échec.*

Slide 8 *Environ 40 secondes seulement après le démarrage de la séquence de vol, le lanceur, qui se trouvait alors à une altitude de quelques 3700 mètres, a dévié de sa trajectoire, s'est brisé et a explosé.*

Des ingénieurs des équipes du projet Ariane 5 du CNES et de l'industrie ont immédiatement commencé à **rechercher les causes de cet échec**.

Ariane : Commission d'enquête indépendante

Slide 9

Prof. Jacques-Louis Lions (Président)
Académie des Sciences (France)
Dr. Lennart Lübeck (Vice-Président) SSC (Suède)
M. Jean-Luc Fauquembergue DGA (France)
M. Gilles Kahn INRIA (France)
Prof. Wolfgang Kubbat Université technique de Darmstadt (Allemagne)
Dr. Ing. Stefan Levedag Daimler Benz Aerospace (Allemagne)
Dr. Ing. Leonardo Mazzini Alenia Spazio (Italie)
M. Didier Merle Thomson CSF (France)
Dr. Colin O'Halloran DERA (U.K.)

Ariane : Mandat de la commission d'enquête

Slide 10

- déterminer les causes de l'échec du lancement,
- analyser l'adéquation des essais de qualification et des essais de recette face aux problèmes rencontrés,
- recommander les actions correctives pour éliminer les causes de l'anomalie et d'autres faiblesses éventuelles des systèmes incriminés.

Ariane : Cause de l'accident

C'est la perte totale des informations de guidage et d'attitude 37 secondes après le démarrage de la séquence d'allumage du moteur principal (30 secondes après le décollage) qui est à l'origine de l'échec d'Ariane 501.

Slide 11

Cette perte d'informations est due à des erreurs de spécification et de conception du logiciel du système de référence inertielle.

Les revues et essais approfondis effectués dans le cadre du programme de développement d'Ariane 5 **ne comportaient pas les analyses ou essais adéquats du système de référence inertielle ou du système complet de contrôle de vol** *qui auraient pu mettre en évidence la défaillance potentielle.*