Un aspect de l'ingénierie et du logiciel : la fiabilité du logiciel.

Nicolas Magaud

8 mars 2008, Strasbourg

Pourquoi vérifier les programmes ?

Qualités attendues pour un logiciel :

- il ne suffit pas qu'un logiciel soit performant et ergonomique,
- il faut surtout qu'il se comporte comme on l'a prévu !

Pourquoi vérifier les programmes ?

Qualités attendues pour un logiciel :

- il ne suffit pas qu'un logiciel soit performant et ergonomique,
- il faut surtout qu'il se comporte comme on l'a prévu !

Un bug peut coûter cher :

- des vies humaines (transports, médecine, centrales nucléaires)
- de l'argent (vols spatiaux, transactions bancaires, . . .)

Quelques exemples remarquables (1)...

Ariane Vol 501, 1996

- 10 années de travail,
- $500 millions de satellites à lancer...
- ...pour seulement 39 secondes de vol !

Quelques exemples remarquables (1)...

Ariane Vol 501, 1996

- 10 années de travail,
- \$500 millions de satellites à lancer...
- ...pour seulement 39 secondes de vol !

Quelques exemples remarquables (1)...

Ariane Vol 501, 1996

- 10 années de travail,
- \$500 millions de satellites à lancer...
- ...pour seulement 39 secondes de vol !

Analyse après l'accident...

Cause : une représentation inadéquate des nombres

- réutilisation d'un programme de Ariane 4,
- conversion d'un nombre de 64 bits en 16 bits,
- Ariane 5 se déplace plus vite...
- l'erreur n'est pas gérée...

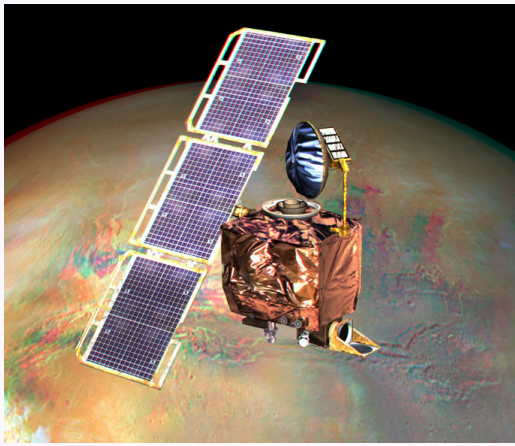
Conséquences :

- retard pour la suite du programme Ariane 5
- image ternie auprès des futurs clients, mauvaise publicité

Quelques exemples remarquables (2) . . .

Mars Climate Orbiter (1999)

Coût: 125 millions de dollars.



Cause :

- Un problème d'unité dans l'expression d'une force de poussée.
- Une équipe travaille avec le système métrique (Jet Propulsion Laboratory),
- Une autre équipe travaille avec le système anglo-saxon (Lockheed Martin Astronautics).

D'autres exemples...

Radiothérapie et surexpositions à des radiations

- Therac-25 (1985-1987)
  3 morts dues à un bug dans le logiciel Therac-25.
- Accident de radiothérapie de l'hôpital d'Epinal en 2004-2005
  Mauvaise ergonomie d'un logiciel de calibrage.

Autres domaines

- SNCF, instabilité du système de réservations
- Problème d'interception d'un missile Patriot
  On February 25, 1991, a Patriot missile defense system operating at Dhahran, Saudi Arabia, during Operation Desert Storm failed to track and intercept an incoming Scud.

Ingénierie du logiciel et fiabilité...

- Un programme est un objet mathématique comme un autre.

Tests

- on cherche a démontrer qu'un programme n'est pas correct dans certains cas.
- comment être exhaustif ? a-t-on tout testé ?

Preuves formelles

- on cherche a démontrer qu'un programme vérifie certaines propriétés.
- comment être sur de ses démonstrations ? les faire vérifier par une machine !