

# UE INF222

## Modèles et Vérification

### Complément au cours d'introduction concernant l'activité de vérification

Sylvie Vignes

Télécom ParisTech - groupe S3



## Rappel

### ○ La Validation

- a pour objectif de s'assurer que le système ou le sous-système développé a la **capacité à fournir les services** attendus par le client et les utilisateurs finaux.

**Validation\* : construit-on le bon produit ?**

### ○ La Vérification

- ensemble des activités permettant d'assurer la **conformité technique de réalisation** du système ou du sous-système logiciel en développement

**Vérification\* : construit-on correctement le produit ?**

\* Référence ISO 8402

Quality Management & Quality Assurance



INF222 - 2

## Exemples de « modélisation et vérification »

- Par ces exemples, il s'agit de
  - donner un aperçu de **différentes "classes de systèmes"**
  - décrire textuellement le modèle initial abstrait
  - d'illustrer la variété de préoccupations qu'un concepteur doit **vérifier**
- Ex1 : un programme de tri
- Ex2 : un système transactionnel
- Ex3 : un protocole de transmission
- Ex4 : un système réactif



INF222 - 3

## Ex1 : un programme de tri

- Un **modèle abstrait** décrit
  - «le quoi» :
    - *Le programme prend en entrée un fichier séquentiel et sort un fichier trié*
  - Ce qui qualifie le modèle et qu'il faut vérifier:  
= les **propriétés** du modèle
    - *Tous les éléments en entrée doivent se retrouver en sortie*
    - *Les éléments doivent être classés entre eux selon un critère*
- Remarque : beaucoup de programmes réalisent ce modèle abstrait avec une efficacité variable («le comment»)



INF222 - 4

## Ex2 : Un système bancaire

- Préalable: réutiliser des systèmes existants
  - La base de données, (SGBD)
  - L'interface Homme\_Machine
- Le **modèle abstrait** concerne le métier de la banque (comptes, clients, ...), le traitement de données (contraintes de cohérence)
- La **vérification** concerne
  - la cohérence de chaque transaction,
    - le rollback si une transaction est interrompue
  - La sécurité d'accès liée aux rôles des utilisateurs
  - ...



INF222 - 5

## Ex3 : Un protocole de transmission

- La spécification du protocole décrit le séquençement de différents messages entre 2 (ou plusieurs) sites...
- Le **modèle abstrait** doit
  - dégager la « mission » du protocole
  - ignorer l'aspect réparti,
  - ignorer les détails trop concrets

« le quoi » : transmettre totalement ou partiellement les éléments d'un fichier

Les propriétés :  
ordre et continuité des données ne doivent pas être modifiées, etc
- La description doit permettre de **vérifier** que le séquençement est correct, sous certaines hypothèses



INF222 - 6

## Ex4 : Accès par une porte avec digicode

- Le **modèle abstrait** décrit
  - le fonctionnement du contrôle
  - en réponse à des sollicitations en entrée
    - La porte s'ouvre (signal de sortie OPEN) si la personne introduit le code (signal d'entrée CODE) et si ce code correspond au code configuré.
    - en cas d'erreur du code, le signal RETRY est émis.
    - ...
- La **vérification** concerne
  - Les règles de fonctionnement
  - Les règles de sécurité
  - ...
    - la présence d'une personne devant la porte est notifiée par le signal DETECT.
    - En cas de détection d'incendie, l'entrée du code est annulée



INF222 - 7

## Conclusion

- D'après ces exemples, les préoccupations de vérification
  - sont fonctionnelles ou non fonctionnelles
  - concernent:
    - L'algorithmique séquentielle ou parallèle
    - Les propriétés « critiques »
      - des Systèmes d'Information
      - des systèmes réactifs synchrones
      - des systèmes embarqués
      - ...
- Plusieurs **Profil UML** dédiés à des « classes de systèmes » permettant de faire le lien avec les notations formelles de méthodes de vérification



INF222 - 8