

# **UML, langage objet et certification**

**Boulangier Jean-Louis**

**Jean-louis.boulangier@utc.fr**

**Université de Technologie de Compiègne**

**Laboratoire HEUDIASYC**



# Catégories du logiciel

- **Les logiciels «grande consommation»**
  - sans conséquence (jeux, familiale, ...)
  - avec conséquence « financière »
  
- **Les logiciels «sur mesure»**
  
- **Les logiciels «critiques de fonctionnement»**

# Cadre ferroviaire

## ➤ Norme EN 50128:

- Norme européenne;
- Exclusivement applicable au logiciel et à l'interaction entre le logiciel et le matériel;
- 5 niveaux de criticité:
  - ✓ Pas critique: SIL0,
  - ✓ SIL1, SIL2,
  - ✓ Critique : SIL3, SIL4
- Applicable à:
  - ✓ L'application;
  - ✓ Le(s) système(s) d'exploitation ;
  - ✓ Les outils d'aides aux développements ;

# Type de développement

## ➤ Développement actuel:

- Développement classique ADA83 ;
- Développement formel avec la méthode B ;
- Développement formel avec SCADE (Lustre) ;
- Utilisation du C sur les parties non sécuritaire ou de bas niveau

## ➤ Évolution vers:

- Développement UML pour l'aspect spécification;
- Génération de code C++ à partir de spécification UML;
- Développement ADA 95 ;
- Développement en JAVA (partie non sécuritaire).

# A propos d'UML

- **Spécification : apparition de modélisation UML**
  - UML est une notation;
  - Problèmes de sémantique;
  - Problème de méthodologie;
  - Outillage ....
- **Conception : Génération de code orienté objet à partir de spécification UML**
  - Processus de génération de code;
  - Génération partielle
    - => codage complémentaire

# EN 50128

- **La programmation orienté objet est introduite:**
  - Objet;
  - Classe d'objet;
  - Héritage multiple;
  - Polymorphisme.

# Exigence de la norme EN 50128

## ➤ **Spécification :**

- ?

## ➤ **Conception :**

- Langage fortement typé HR de SIL1 à SIL4
- Programmation orienté objet R de SIL1 à SIL4
  
- Sous-ensemble du langage HR de SIL3 à SIL4
- Traducteur validé HR de SIL1 à SIL4
- Traducteur éprouvé à l'utilisation HR de SIL0 à SIL4

## ➤ **Vérification**

- Métrique
- Testabilité

# Norme de codage

## ➤ Il faut:

1. Guide du style de codage HR de SIL1 à SIL4
2. Pas d'objets dynamiques HR de SIL3 à SIL4
3. Pas d variables dynamiques HR de SIL3 à SIL4
4. Usage limité des pointeurs R de SIL1 à SIL4
5. Usage limité de la récursivité HR de SIL3 à SIL4
6. Pas de branchements inconditionnel HR de SIL1 à SIL4

## ➤ **2,3 et 4 sont acceptés si partie intégrante d'un compilateur ou d'un traducteur validé**

# Conclusions

## ➤ **UML:**

- Définition d'un référentiel de développement d'application certifiable;
- Définition d'un référentiel de certification;
- Définition des processus de traduction
  - ✓ Minimisation des aspects dynamiques,
  - ✓ Justification des constructions,
  - ✓ ...

## ➤ **Langage Objet:**

- Définition de norme (banc de test);
- Définition d'un sous-ensemble certifiable;

## ➤ **Processus:**

- Méthodologie
- Métriques
- Testabilité