Méthode Formelle, Développement logiciel et Système sûr critique

Un système critique peut comporter une erreur venant de n'importe quel niveau de son développement (voir exécution) et ce pour diverses raisons.
Compilation réussie =/= 0 problèmes. Les méthodes formelles sont nécessaires pour assurer que les très nombreuses parties d'un tel système ne posent aucun risque.
Il existe plusieurs normes pour les systèmes sûr :

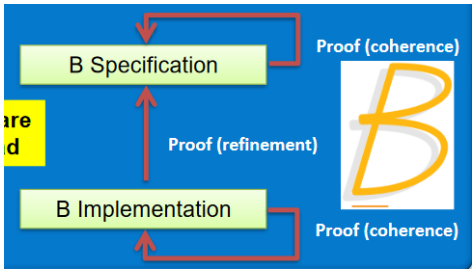
IEC61508/EN50128	Préservation de la vie humaine	Les méthodes formelles « Highly recommended » par les normes industrielles pour le développement de systèmes de sécurité de **niveau 4**
Common Criteria	Préservation de la confidentialité des données	Evaluation Assurance Level (**7 niveaux**)
DO-178 C	Est-ce que l'avion se crash ou pas	Development Assurance Level (**5 niveaux** de criticité)

On ne sait pas calculer la fiabilité d'un programme -> usage des maths pour se rassurer.

Méthodes formelles => techniques de raisonnement utilisant les mathématiques pour créer des spécifications et les vérifier, éventuellement pour les raffiner, voir pour les dériver ou les lier à un logiciel concret.

METHODE B (méthode formelle)

- Théorie des ensembles ($A \subseteq B$)
- Logique des prédicat 1er ordres ($P \Rightarrow Q$, existentiel, universel)
- Partie Statique : propriété
- Partie dynamique : comportement



Les preuves formelles de la méthode B dans la phase de dev permettent de supprimer la phase de test et de réduire les phases d'intégration des composants logiciels, de validation et d'intégration du logiciel dans le système.
Preuves => générées automatiquement.
Programme juste si 100% prouvées
Code logiciel généré à partir du modèle.

B système : analyse formelle de système => Modélisation du raisonnement utilisé pour la conception sûre
Niveaux : B système > analyse formelle > B logiciel

Voir graph p40

Vérification mathématique des données =>

- Formalisation des données (consistantes, corrections)
- Validation d'un ensemble de données partiellement construit
- Mise en évidence des contre-exemples de manière simple

Propriétés + Propriétés partagées + données ---> traducteur ---> model B ---> outils d'analyses ---> conformance et/ou contre-exemples

Il faut check l'hardware aussi car des pannes peuvent en provenir.