CLEARSY

Safety Solutions Designer

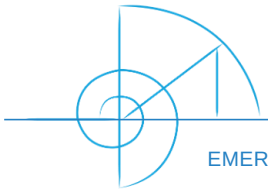
NOV
2025

AIX
LYON
PARIS
STRASBOURG

WWW.CLEARSY.COM

Méthodes formelles dans l'industrie

Sûreté ferroviaire



EMERIC.TOURNIAIRE@CLEARSY.COM

DÉVELOPPER UN SYSTÈME FERROVIAIRE

Qu’est-ce qu’un train ?

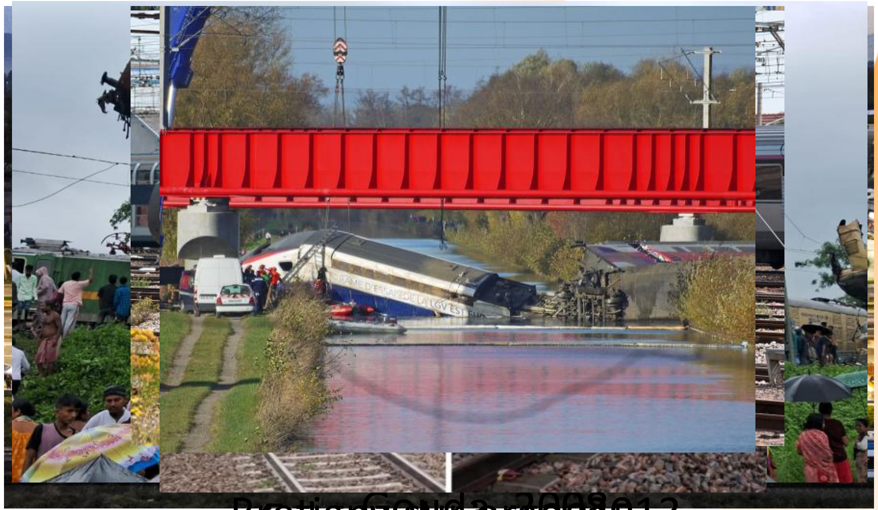
- Convoi lourd (400t)
- Rapide (120–300km/h)
- Guidé par rails

$$d_{Freinage} > d_{Visibilité}$$

⇒ Garantir impérativement l’absence d’obstacle

Causes d’accident

- ▶ Déraillement sur rail
  - ▷ rail cassé
  - ▷ survitesse
- ▶ Déraillement sur aiguillage
- ▶ Collision
  - ▷ Nez-à-nez
  - ▷ Rattrapage
  - ▷ Prise en écharpe
- ▶ Obstacles



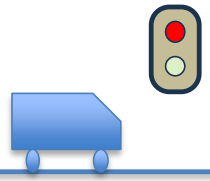
Gouda 2008
Inde 2024-06
France, 2024

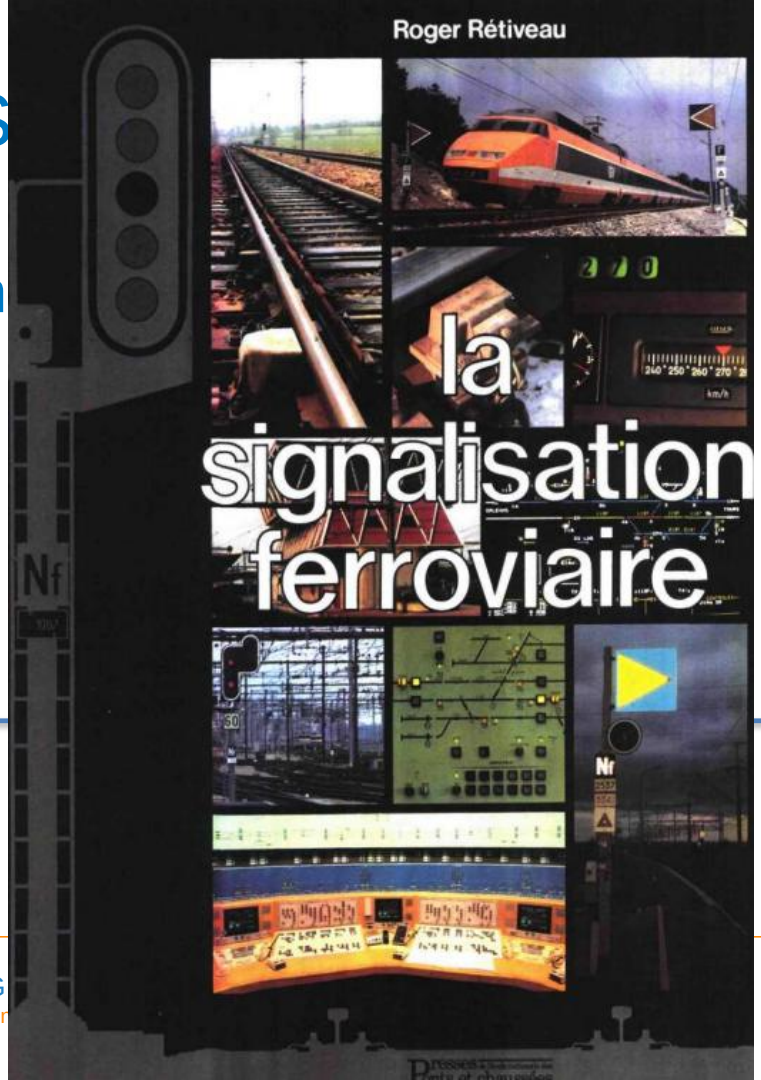
Critical systems

- Bugs = ☠
- Formal methods
  - Highly recommanded by norms
  - and by CLEARSY
- Railway industry

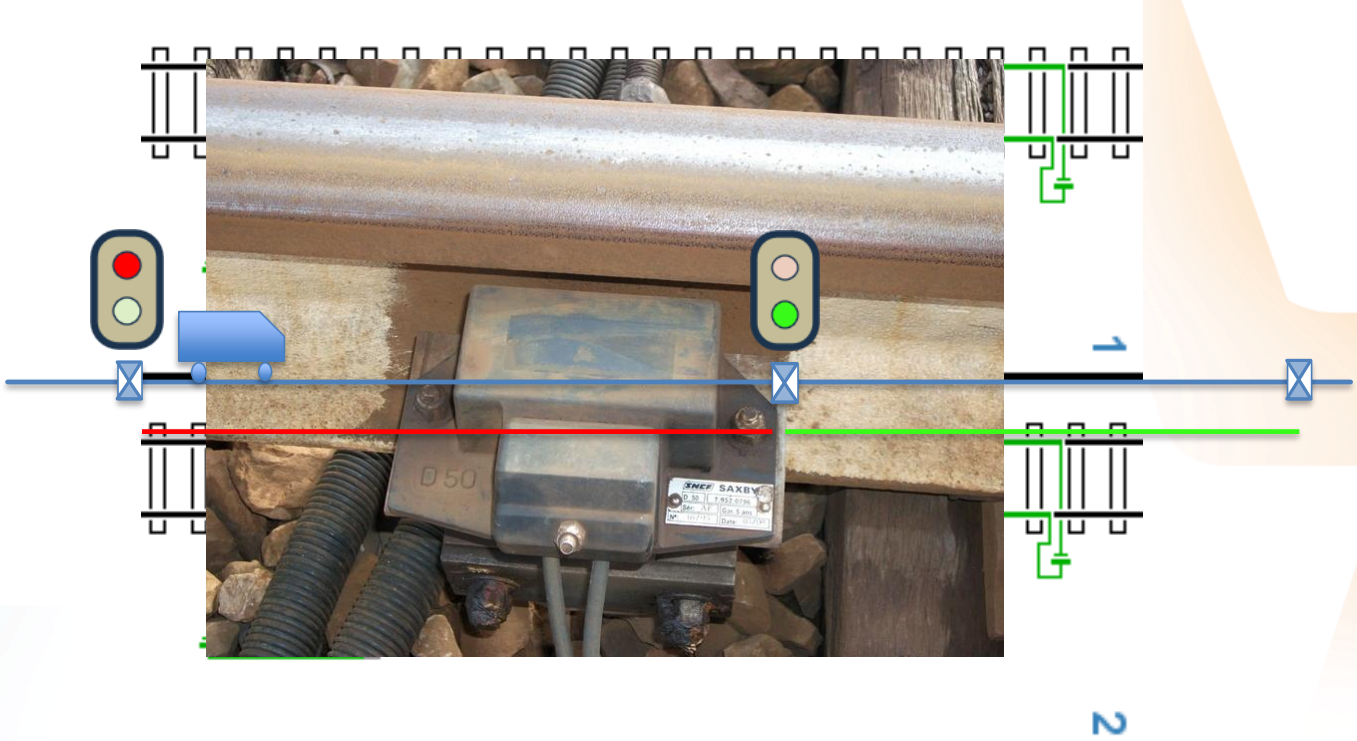
S

Signal = indication

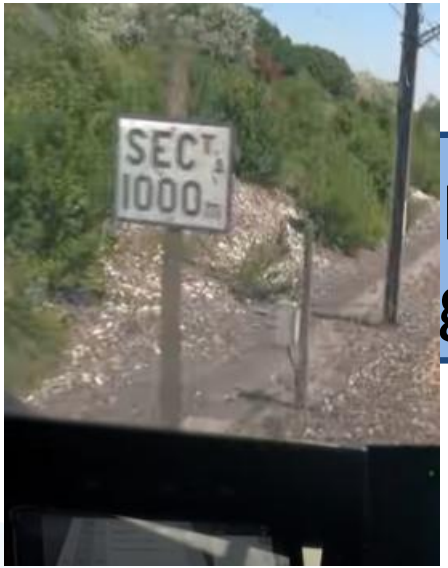




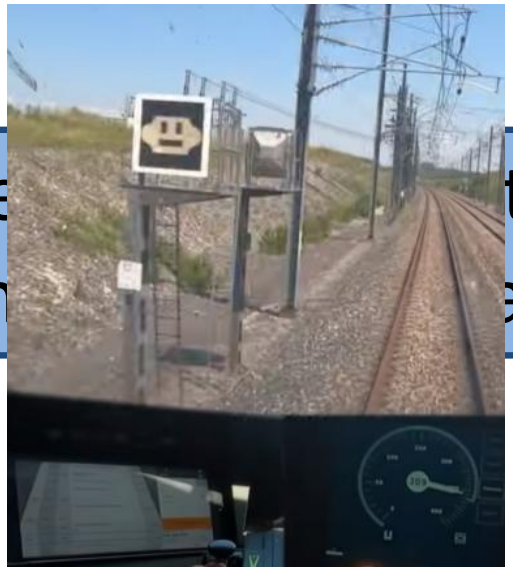
Détection des trains et espacement



Avec la Vitesse ?



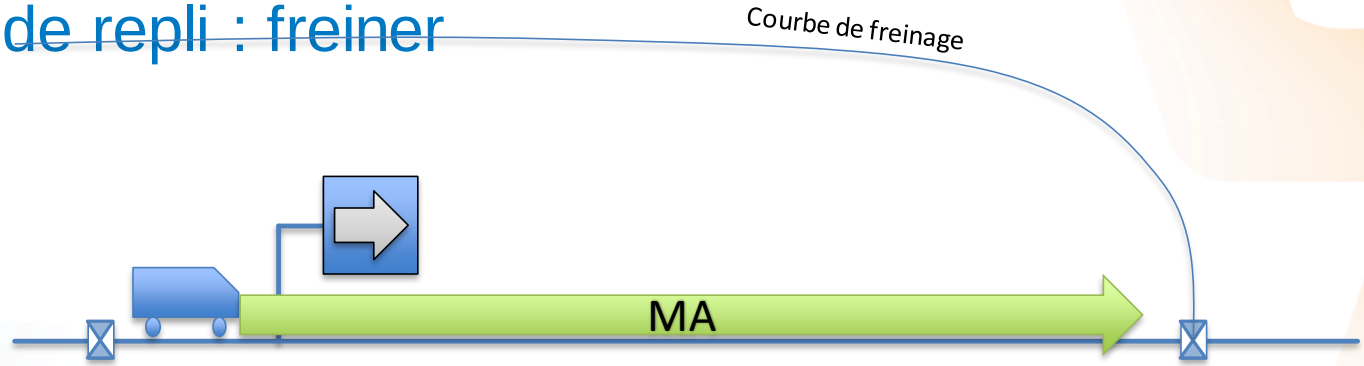
pe
gn



te
ale

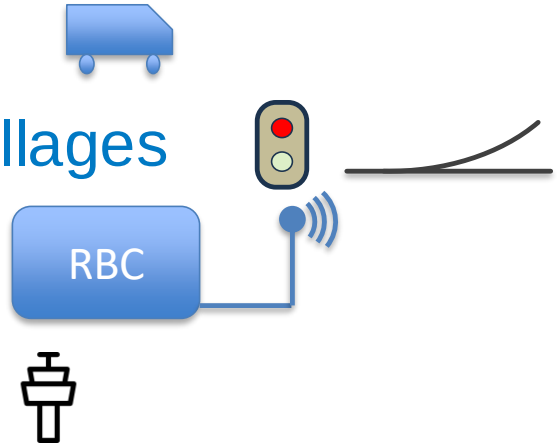
Autorisations de mouvement

- Envoyées par balises, radio, ou GSM-R
- Supervision par courbes de freinage
- État de repli : freiner



Plein de sous-systèmes

- Trains
- Signalisation, aiguillages
- Bloc radio/GSM
- Conducteur
- Agent de contrôle



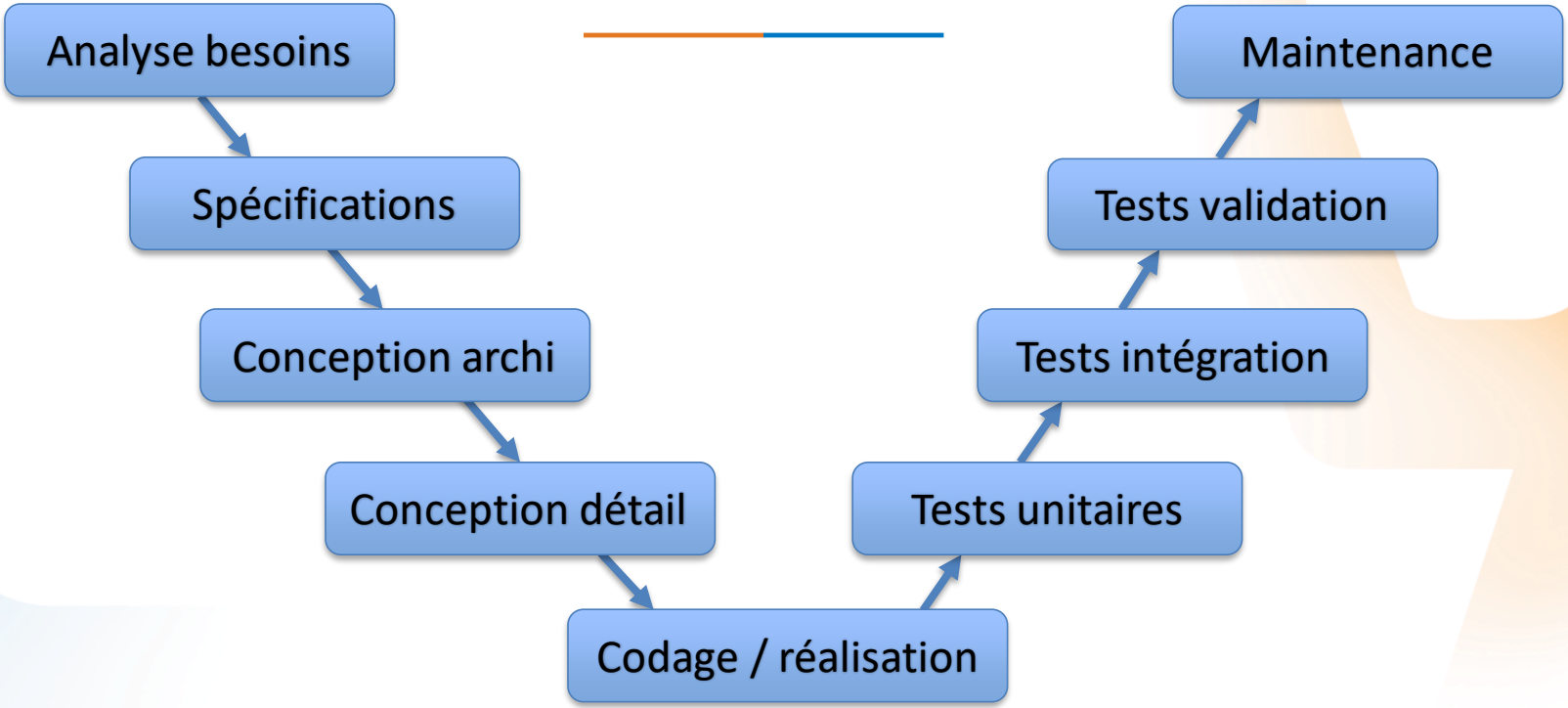
Conclusion partielle

- Certains de ces systèmes sont pilotés par logiciel
- Programmation **critique** (bug = ☠)
- Heureusement il y a une norme !
  - EN 50716
  - Impose un cadre (documentation, vérifications, codage, maintenance)
  - Accidents : probabilité ~ 1 / 1000 siècles
  - ou « Globalement Au Moins Équivalent »

Exemple (simplifié)

- L'exploitant conçoit le système et fait un appel d'offres
- Le fournisseur fabrique un sous-système (e.g. le RBC)
- Le fournisseur se fait auditer par un certificateur
- Le certificat est transmis à l'EPSF (État)
- Mise en service (~10 ans après)

Cycle en V


Analyse besoins
Spécifications
Conception archi
Conception détail
Codage / réalisation
Tests unitaires
Tests intégration
Tests validation
Maintenance

État de repli

- En cas de doute, repli
  - Train
  - Détecteur de train
  - Porte automatique d'un métro
  - Voiture automatique
  - Avion

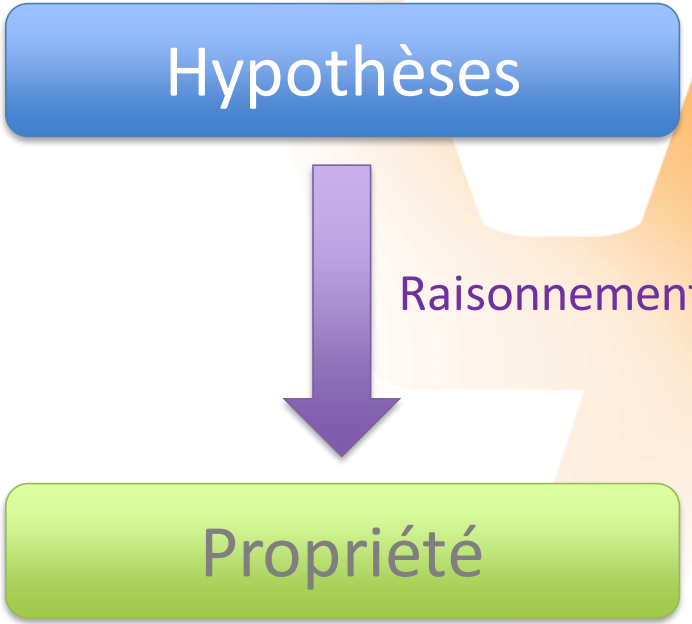
CLEARSY ET LA MÉTHODE B

CLEARSY en une slide

- ~160 personnes (140 ingénieur.e.s)
- Aix, Lyon, Paris, Strasbourg
- Spécialisée en sûreté de fonctionnement ferroviaire
  - Travaille pour SNCF, RATP, NY MTA, Siemens, Alstom…
- Utilise la méthode B

Méthodes formelles, principe

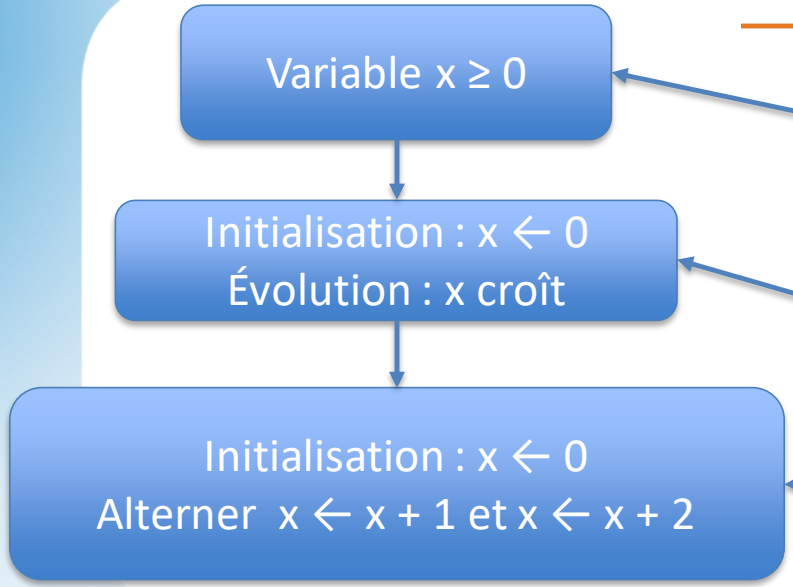
- Preuve d'une propriété
- Raisonnement rigoureux
- Couvre tous les cas possibles



Développement formel en B

- Spécification formelle
  - Langage mathématique (variables abstraites, quantificateurs, situations non déterministes)
- Implémentation
  - Langage impératif (variables concrètes, comportement déterministe)

Exemple simpliste

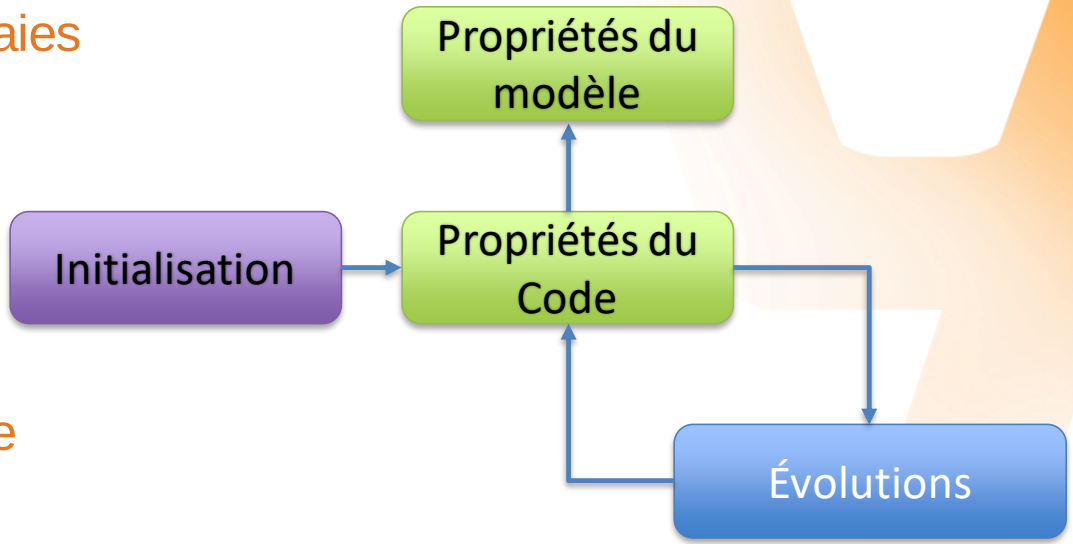



```
INVARIANT
    xx : INTEGER
    & xx >= 0


do_something =
BEGIN
    IF yy = 0
    THEN
        xx := xx + 1
    ELSE
        xx := xx + 2
    END;
    yy := 1 - yy
END
```

Obligations de preuves

- Initialisation
  - Les propriétés sont vraies au début
- Hérédité
  - Les propriétés restent vraies
- Rafinement
  - Les propriétés du code sont conformes



Obligations de preuves

- Générées automatiquement
- Le plus simple possible

=>

```
not(yy$1 = 0) &
"Refinement is correct"

xx$1+1<=xx$1+2
```

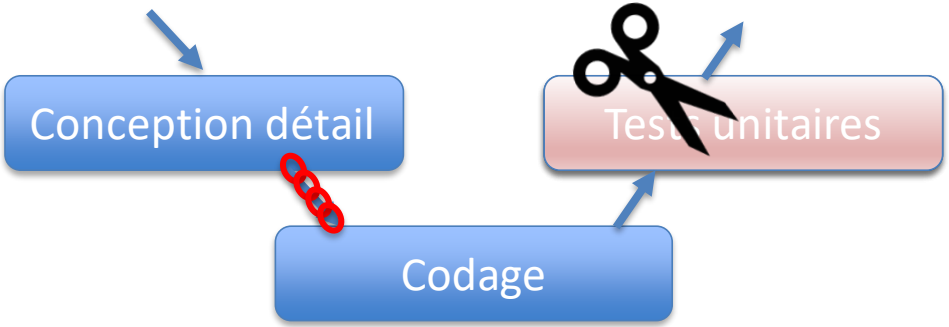
- Objectif
- Liste d'hypothèses
- Preuve rejouable donc vérifiable

Activité de développement formel

- On livre :
  - Le modèle et le code
  - Les preuves
  - Tout est 100% prouvé.
- Le client :
  - Vérifie que le modèle correspond à ses spécifications
  - Rejoue automatiquement les preuves
  - Transforme le code pour l'exécuter sur une machine sécuritaire

Bilan

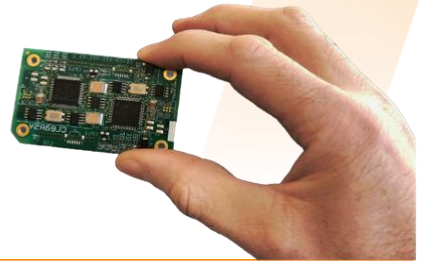
- Développement coûteux
  - Réservé au domaine sécuritaire
- Garantie de conformité
- Permet de supprimer les tests unitaires



UNE MACHINE SÉCURITAIRE : LA CLEARSY SAFETY PLATFORM

CLEARSY Safety Platform

- Code (prouvé)
- Compilé deux fois (redondance)
- 2 processeurs, 2 programmes, 4 exécutions
- En cas de problème, repli



Merci de votre attention

Avez-vous des questions ?