Systerel

Solutions temps réel sécurisées

Validation Formelle de Données

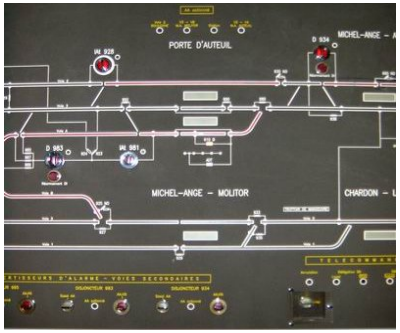
Agréé Crédit Impôt Recherche

Programme

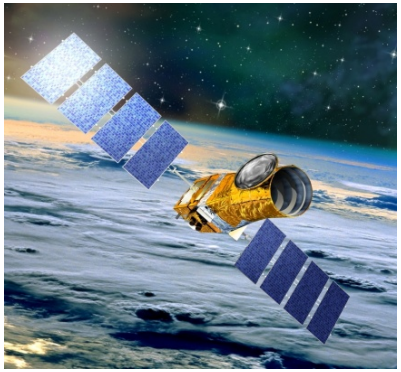
- Quel besoin ?
- Rétrospective des solutions
- Exemples de formalisation
- Conclusion

Systèmes embarqués critiques

- Pilote automatique de métro
  - Description des voies

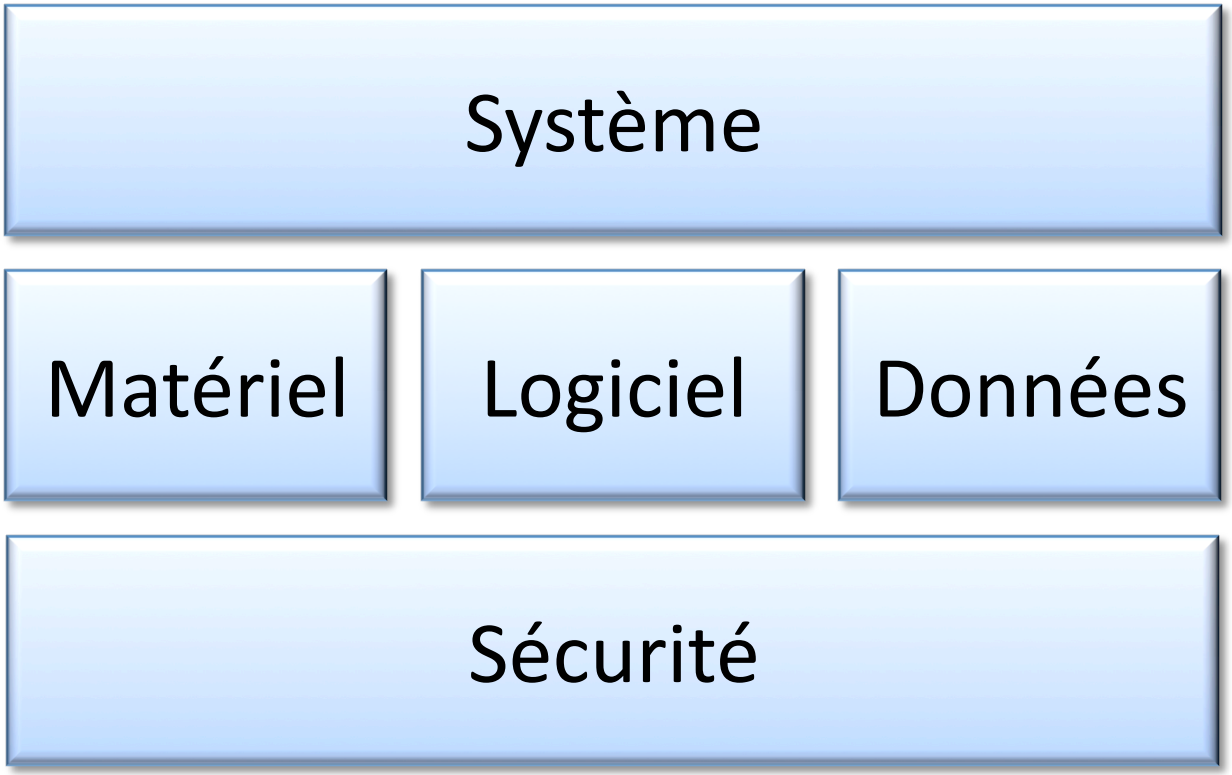


- Poste de manœuvre
  - Description des itinéraires



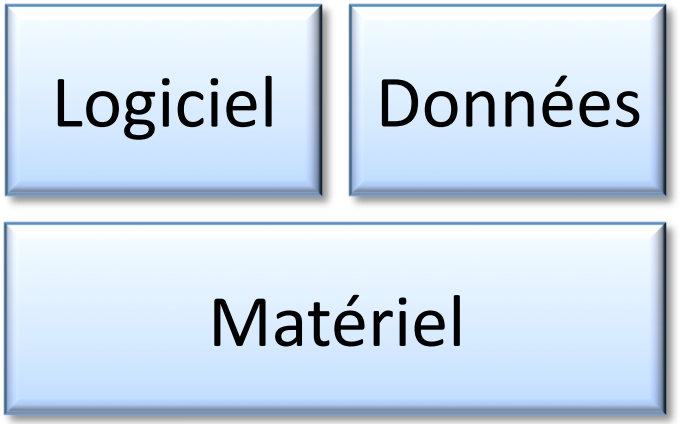
- Système de gestion de la charge utile
  - Gestion des modes, I/O Instrumentation, etc.

Organisation projet



Logiciels génériques

- Séparation des problèmes
- Validation à moindre coût
- Facilité de déploiement
- Recommandation de la norme CENELEC



Origine des données

- Physique
  - Mesures de l'environnement

CBTC : ~ 50 000

- Dérivées
  - Modèles de l'environnement

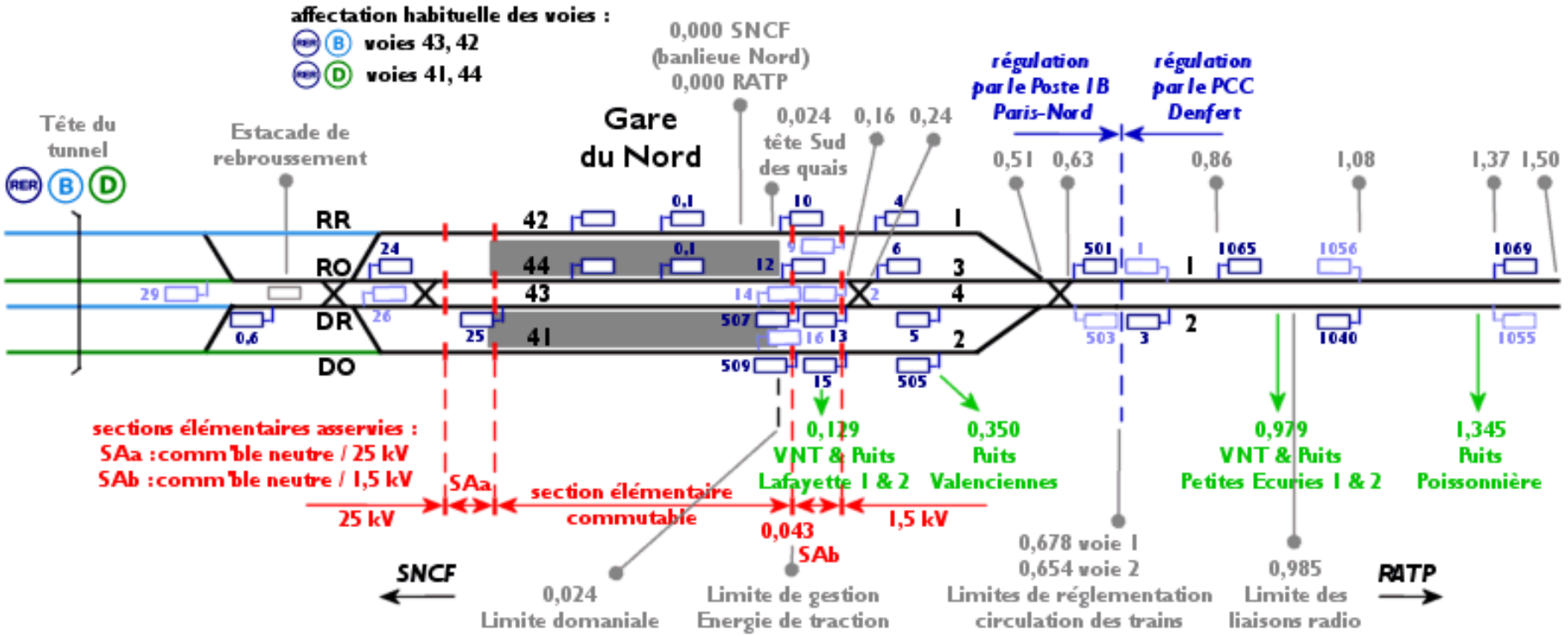
CBTC : ~ 200 000

- Technique
  - Plan d'adressage réseau

CBTC : ~ 1500 adresses IP

- Logiciel
  - Précalculs

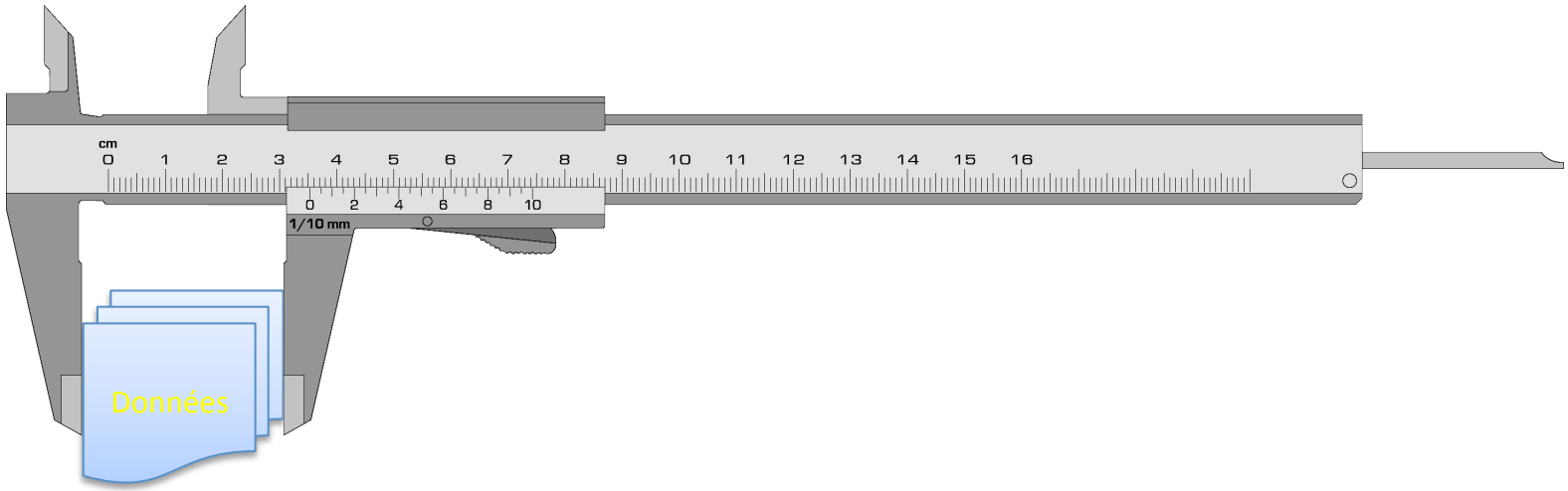
Exemple


affectation habituelle des voies :
B voies 43, 42
D voies 41, 44
0,000 SNCF
(banlieue Nord)
0,000 RATP
Tête du tunnel
Estacade de rebroussement
Gare du Nord
0,024 tête Sud des quais
0,16
0,24
régulation par le Poste IB Paris-Nord
régulation par le PCC Denfert
0,51
0,63
0,86
1,08
1,37
1,50
RR
RO
DR
DO
42
44
43
41
sections élémentaires asservies :
SAa :comm'ble neutre / 25 kV
SAb :comm'ble neutre / 1,5 kV
SAa
25 kV
section élémentaire commutable
1,5 kV
0,043
SAb
0,129
VNT & Puits
Lafayette 1 & 2
0,350
Puits
Valenciennes
0,979
VNT & Puits
Petites Ecuries 1 & 2
1,345
Puits
Poissonnière
0,678 voie 1
0,654 voie 2
Limites de réglementation circulation des trains
0,985
Limite des liaisons radio
SNCF
RATP
0,024
Limite domaniale
Limite de gestion
Energie de traction

Contraintes

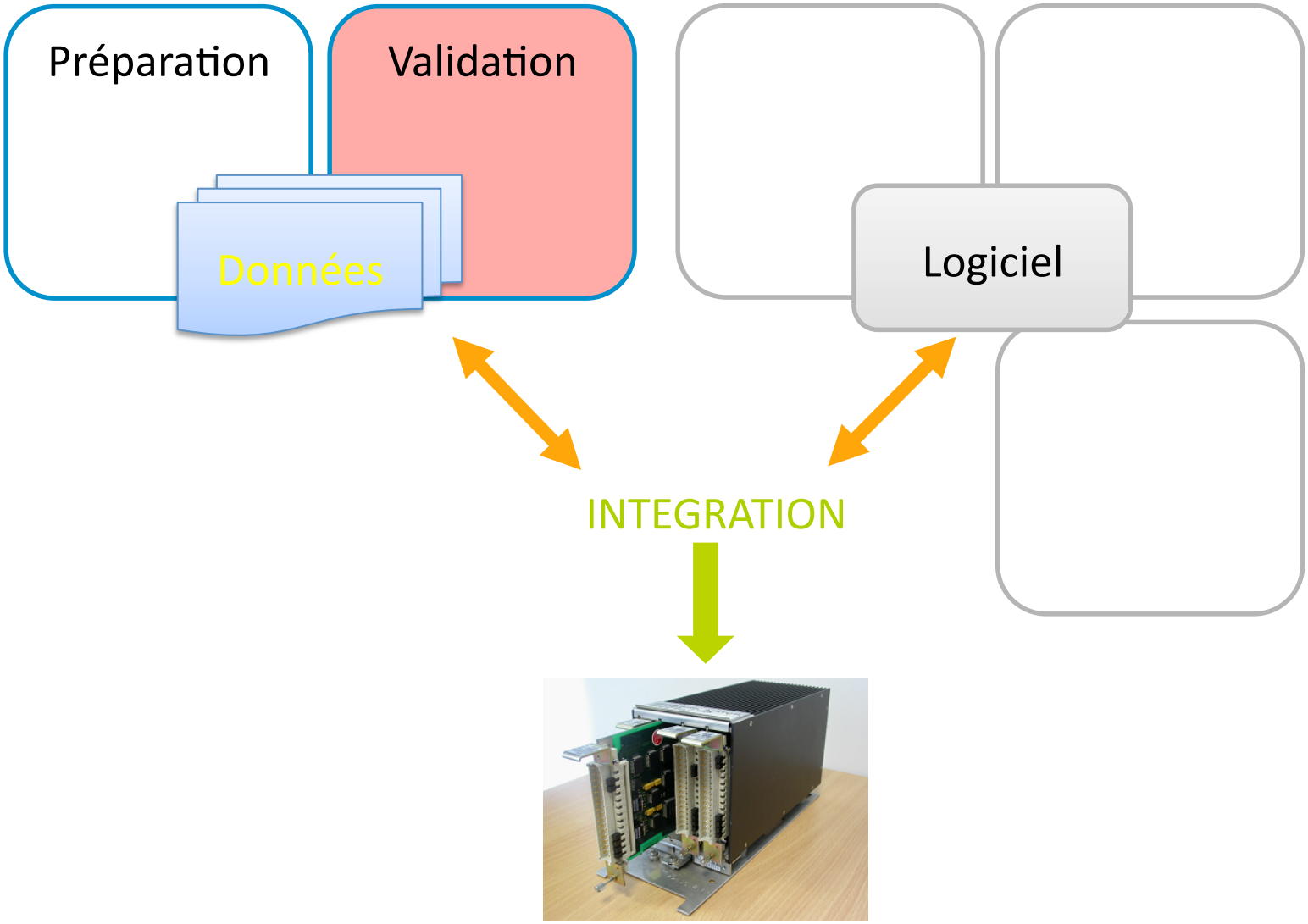
- Cohérence
- Hypothèses du système
- Exactitude des données dérivées
- Pré-conditions du logiciel

Validation de données



Vérifier que les données respectent les contraintes

Contrôles débarqués



Approches

- Validation manuelle
- Programme de validation
- Validation formelle

Validation manuelle

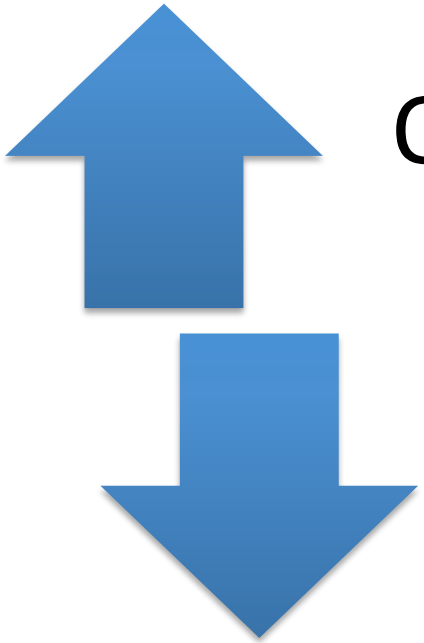
```
const UInt32 lOutDataRxQueuingPortsNumber = 2;
const UInt32 lInDataTxQueuingPortsNumber = 3;
const UInt32 lIoDevicesNumber = 3;

const UInt8 cInDataTxConnectionTable[3][3] =
{
    {OFF,   OFF,   ON},
    {OFF,   ON,   OFF},
    {ON,   OFF,   OFF}
};

const UInt8 cOutDataRxConnectionTable[2][3] =
...
```

Impossible avec beaucoup de données

Programme de validation

- Maintenance difficile
  - Reprise à chaque évolution des contraintes
- Incompréhension
  - L'informaticien ne comprend pas les contraintes
- Propriétés dans le programme
  - Analyse des erreurs codée en dur / Pas de moyen d'analyse « interactif »
  - Manque de maitrise de la validation : qu'est-ce que le programme vérifie?

Validation formelle de données



Quoi

Comment

Un nouveau rôle

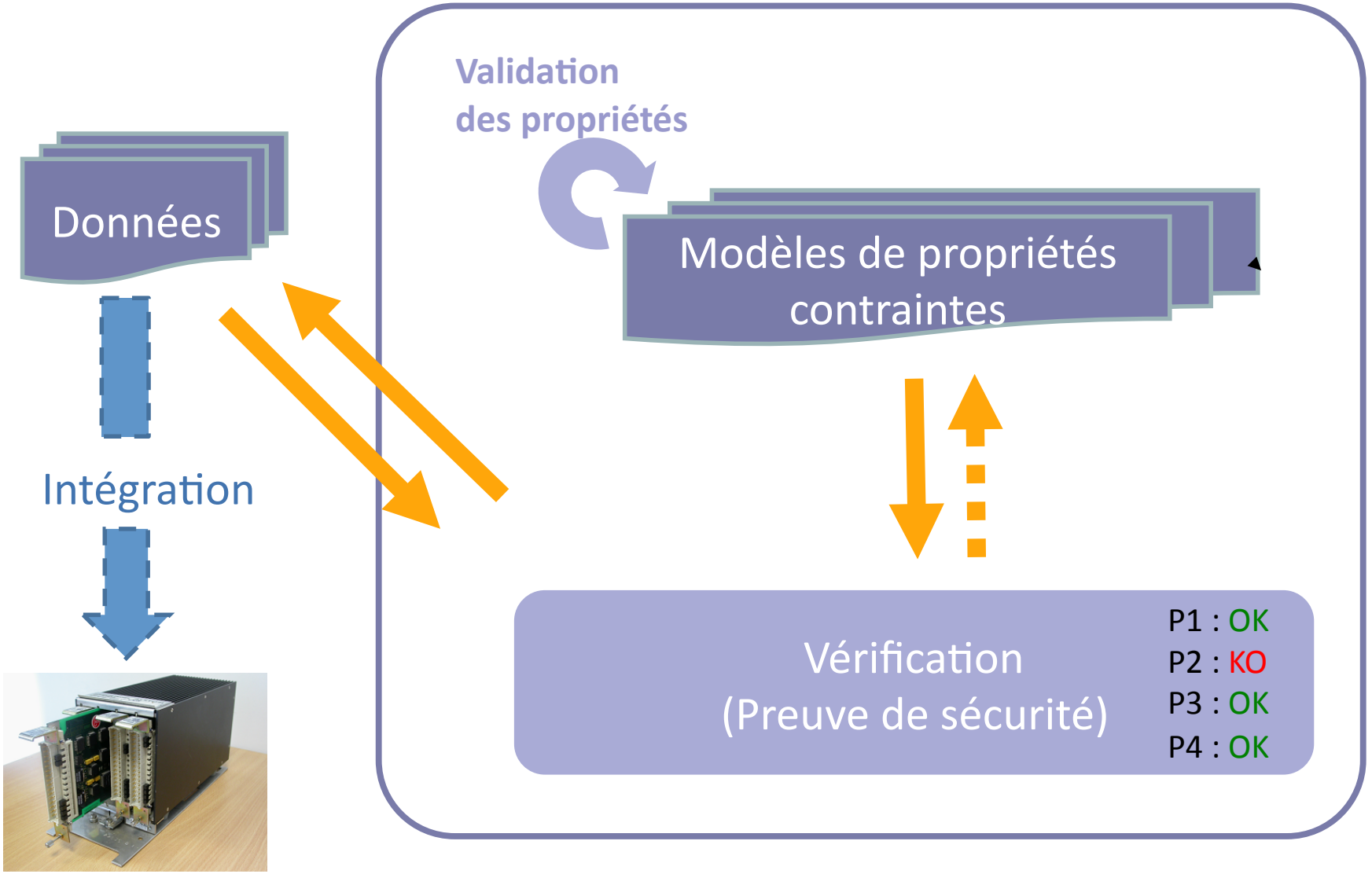
- L'expert métier
  - Identifie les propriétés en langage naturel
  - Aide à la validation des propriétés formalisées

- L'informaticien
  - Réalise et adapte l'outil

Un nouveau rôle

- L'expert métier
  - Identifie les propriétés en langage naturel
  - Aide à la validation des propriétés formalisées
- Modélisateur / Vérificateur
  - Modélise les propriétés avec des mathématiques
  - Lance les outils
  - Réalise les analyses des propriétés en erreur
- L'informaticien
  - Réalise et adapte l'outil

Validation formelle



Séparation propriétés outils

- Les outils ont leur propre cycle de vie
  - Stabilité des outils
  - Mutualisation des efforts de développement

- Indépendance des propriétés
  - Facilite l'ajout/suppression
  - Groupes de propriétés suivant les versions du système

Double expression

- **Exigence exprimée en langage naturel**
  - Identification par les experts métiers

Distance faible facilitant la vérification

- **Propriété exprimée formellement**
  - Utilisation du langage des mathématiques

$$\Rightarrow \neg \wedge = \neq \leq \cap \subset \in$$

Briques de base

- Constantes (scalaires, tableaux)
  - Format imposé
- Définitions (théorie des ensembles)
  - Remontée en abstraction
  - Concepts métier
  - Corpus réutilisable
- Propriétés
  - Ce qu'on veut vérifier

Exemples simples de formalisation

- Structure
  - $c\_LongueurTrain \in 0 \mathinner{..} c\_nbMaxTrains \rightarrow INT$
- Contrôle de gamme
  - $c\_nbTrains \in 1 \mathinner{..} c\_nbMaxTrains$
  - $ran((1 \mathinner{..} c\_nbTrains) \lhd c\_LongueurTrain) \subseteq 20 \mathinner{..} 300$
- Valeurs invalides
  - $ran((1 \mathinner{..} c\_nbTrains) \lhd c\_LongueurTrain) = \{-1\}$

Exemples de formalisation

- Cohérence entres données redondantes
  - $d\_adresseEquipement = d\_equipementAdresse^{-1}$
- Pré-conditions du logiciel
  - $c\_tabTrie \in d\_sorted$
- Propriété système
  - $\forall s, a \cdot$
    $s \mapsto a \in d\_aiguilleProtegeeParSignal$
    $\Rightarrow$
    $min(d\_distance(s \mapsto a)) \geq 20$

Parallèle avec B

Développement B	Validation formelle
Analyse	Synthèse
Dynamique	Statique
Preuve	Calcul / Model checking

Pratique industrielle

- Le format des données est imposé
  - ➢ Adaptation outil d'extraction
- Utilisation de définitions intermédiaires:
  - ➢ Deux profils d'intervenants
- 8 années de retour d'expérience
- Très souple d'emploi, passe bien à l'échelle
- Fonctionne bien en pratique

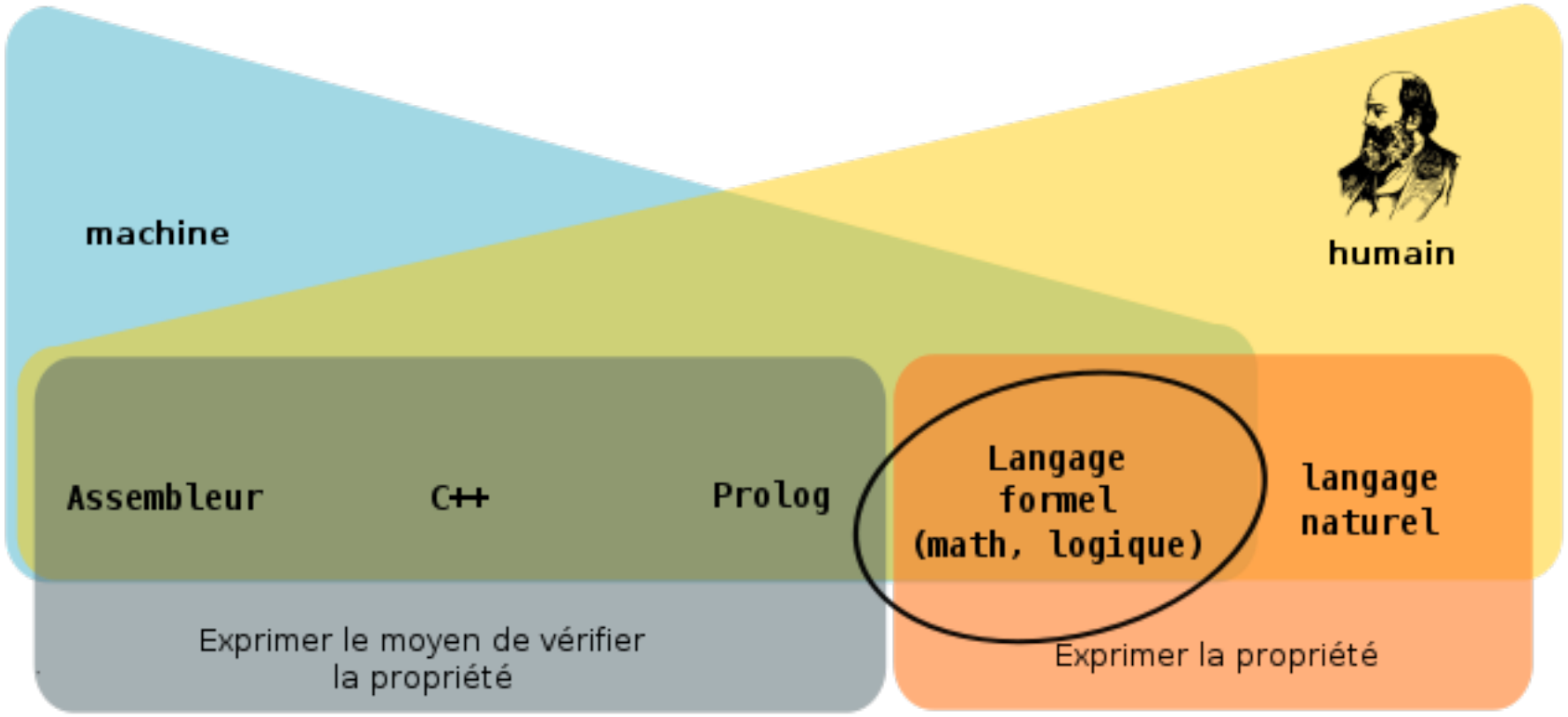
Les types d'outils

- Outils de preuve formelle
  - Ajout de règles (nécessite des experts de la preuve)
  - Peu adapté à une quantité importante
- Outils dédiés
  - Spécifiques à l'évaluation de propriétés
- Outil qualifié
  - OVADO outil de la RATP

Perspectives

- Utilisation industrielle au-delà du ferroviaire
- Représentativité des définitions intermédiaires
- Bonne définition des formules
- Contrôles de cohérence sur les propriétés
  - Analyse dimensionnelle
  - Cohérence des référentiels de mesure

A chacun son langage



Informaticien Modélisateur Expert métier

Question?

Laurent.Voisin@systerel.fr