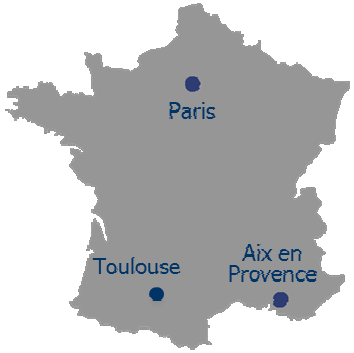
Systerel

Solutions temps réel sécurisées

Validation Formelle de Données



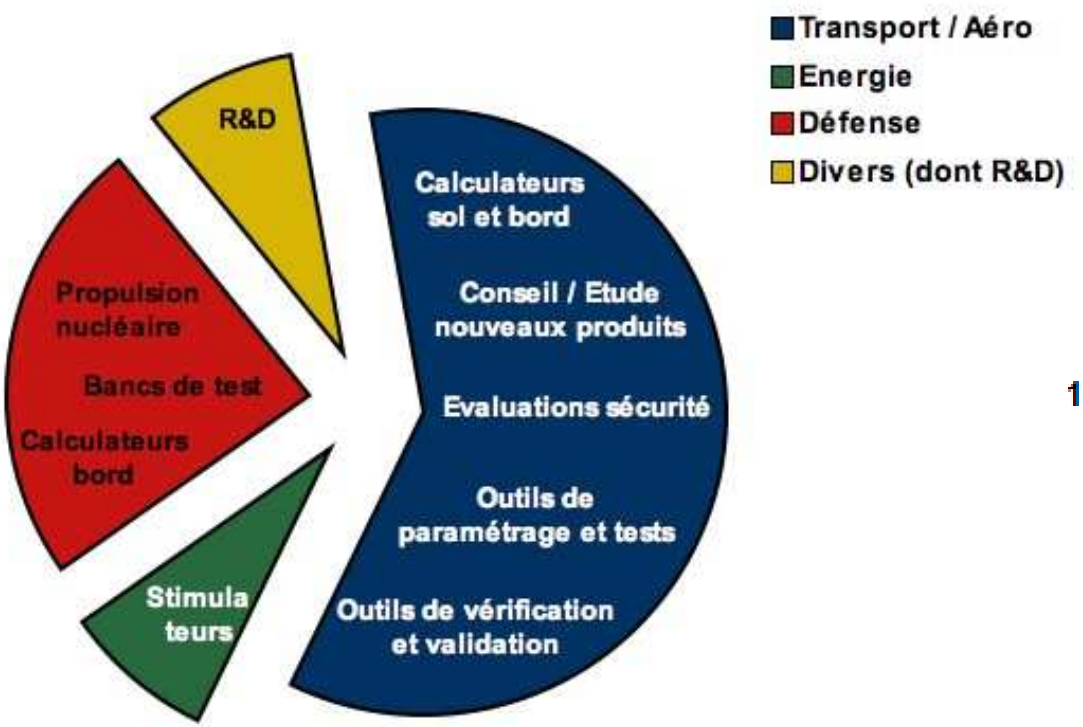
Agréé Crédit Impôt Recherche

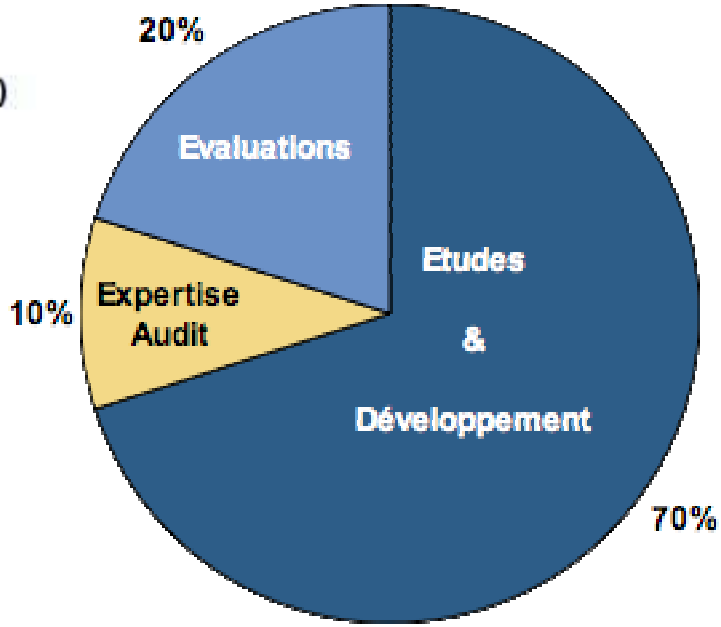
Agenda

- Systerel
- Quelques précisions…
  - Validation des données ?
- Approches classiques
- Validation formelle de données

Systerel

Ingénierie des systèmes sécuritaires





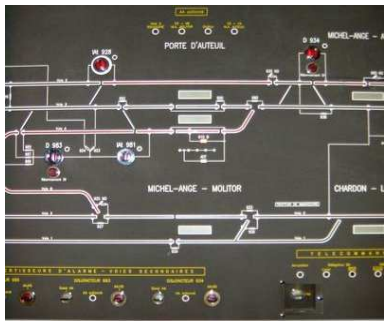
Expériences industrielles

- RATP
  - L14 : Maintenances des outils
  - L13 : premières versions d'OVADO
  - L1, L3 et L5 : version générique d'OVADO
- CNES
  - Etude validation de données pour un système de gestion de charge utile
- AREVA TA
  - Validation de données CBTC

Quelques précisions …

Systèmes génériques

- Pilote automatique de métro
  - Description des voies

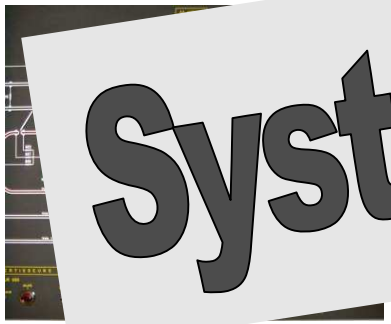


- Poste de manœuvre
  - Description des itinéraires

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

Systèmes génériques

- Pilote automatique de métro
  - Description des voies



Systèmes paramétrés

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

Des données

- Système
  - Mesures de l'environnement
- Dérivées
  - Modèles de l'environnement
- Logiciel
  - Dimensionnement
  - Pré-calculées
- Sous-système
  - Plan d'adressage
- Tests
  - Description de configuration de test
- …

CBTC : ~ 50 000

CBTC : ~ 200 000

Télécommandes satellite
~ 10 000

1500 adresse IP

Contraintes

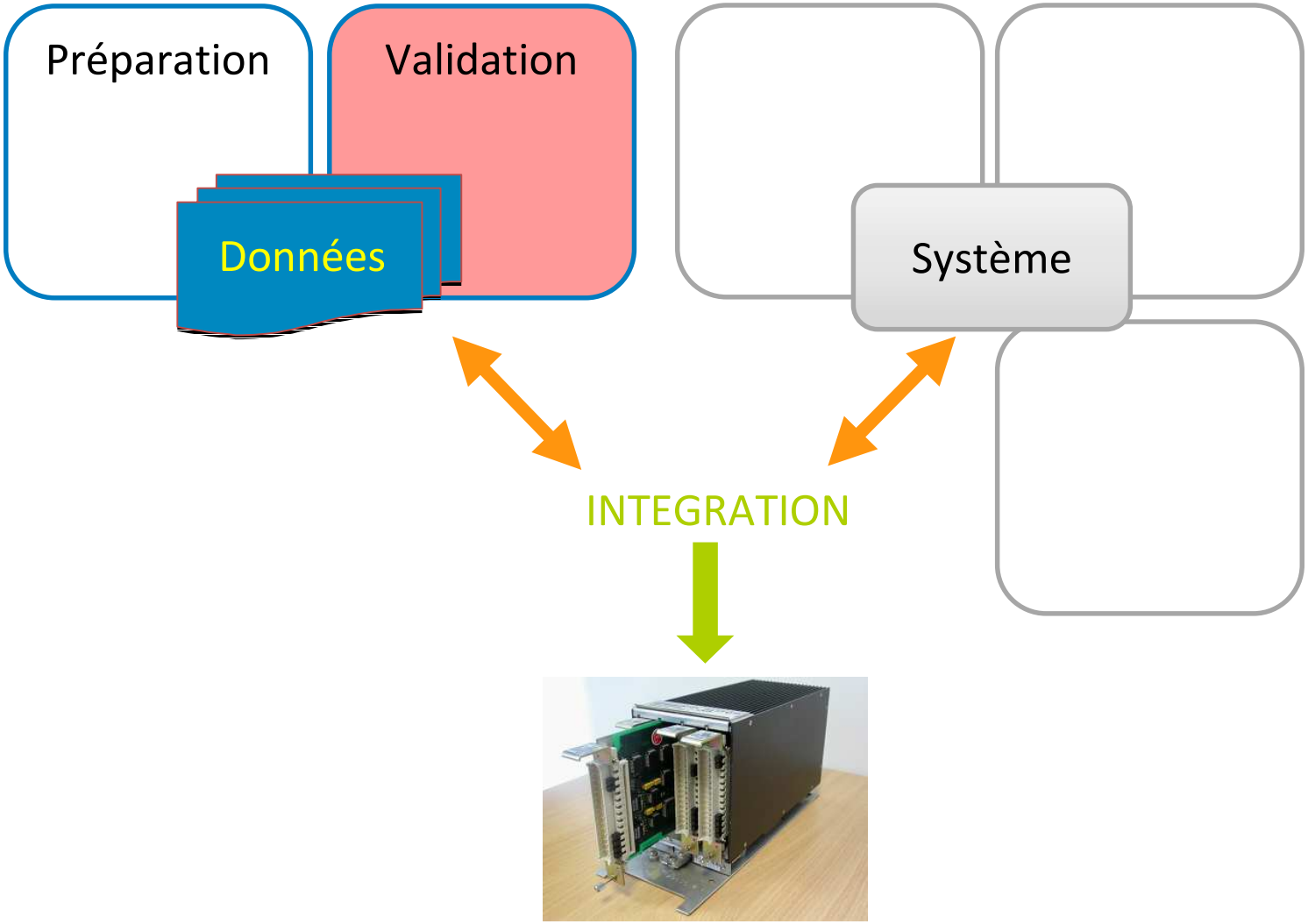
- Généralité
  - Liens entre les données
  - Invariantes (indépendantes du fonctionnement du système)

- Exemples
  - Intervalles de définition
  - Dimensionnement de collections
  - Versions des équipements
  - Adresse unique
  - Matrice de connexion I/O
  - Dimensionnement de zone
  - …

Validation de données

Vérifier que les données respectent les contraintes

Contrôles débarqués



Approches classiques…

Approches classiques

- Validation par effet de bord
- Validation manuelle
- Programme de validation

Validation par effet de bord

- Validation des données lors de la validation du système instancié

- Perte de la généricité du système
- Détection difficile des anomalies liées aux paramétrages
- Interdit par les normes

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 hard codées / Pas de moyen d'analyse « interactif »
  - Manque de maitrise de la validation : qu'est-ce que le programme vérifie?

Validation Formelle de données

le **quoi**

le **comment**

Un nouveau rôle

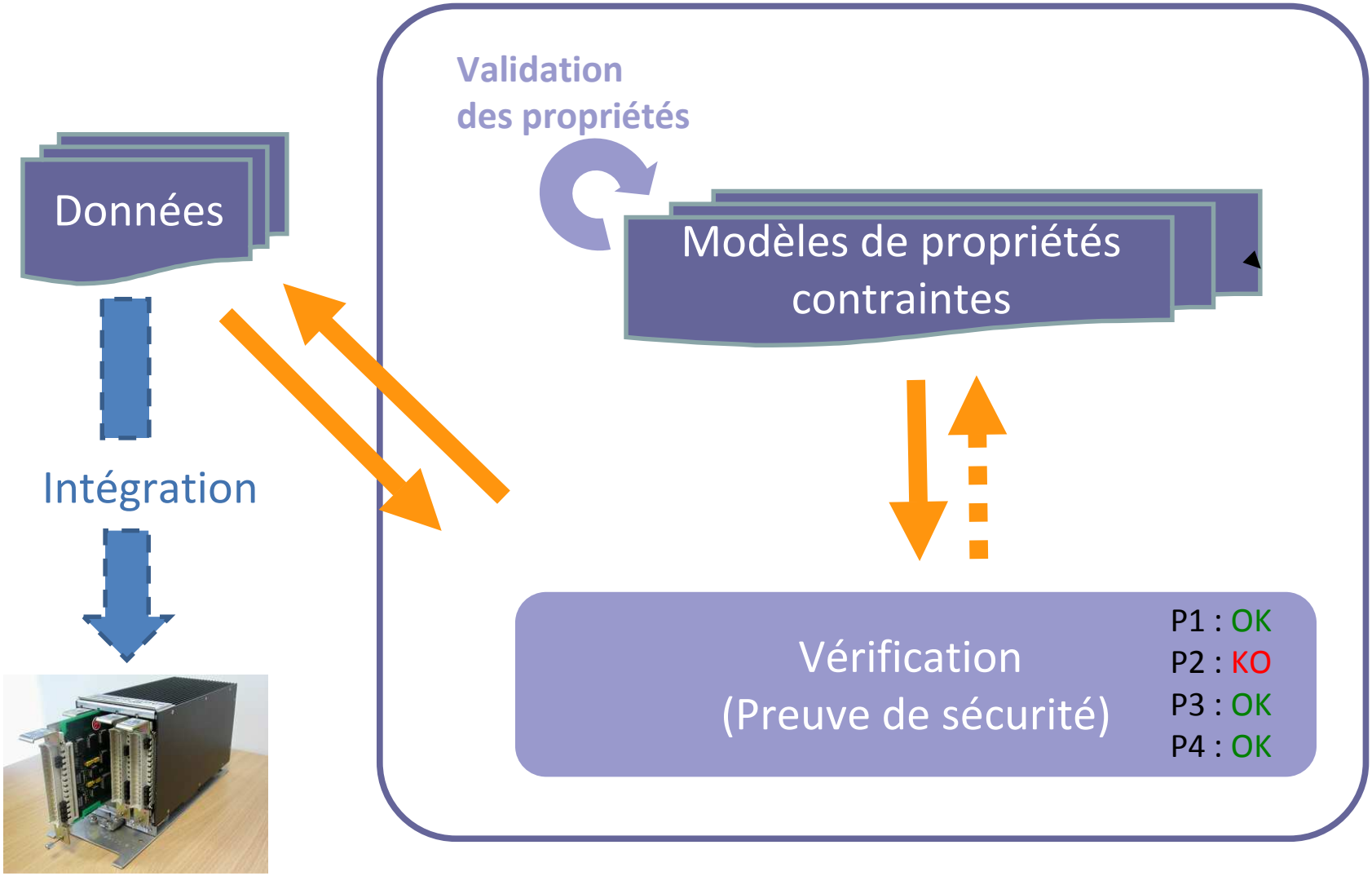
- L'expert métier
  - Identifie les propriétés en langage naturel
  - Aide à la validation des propriétés formalisées

- L'informaticien
  - Réalise et adapte l'outil

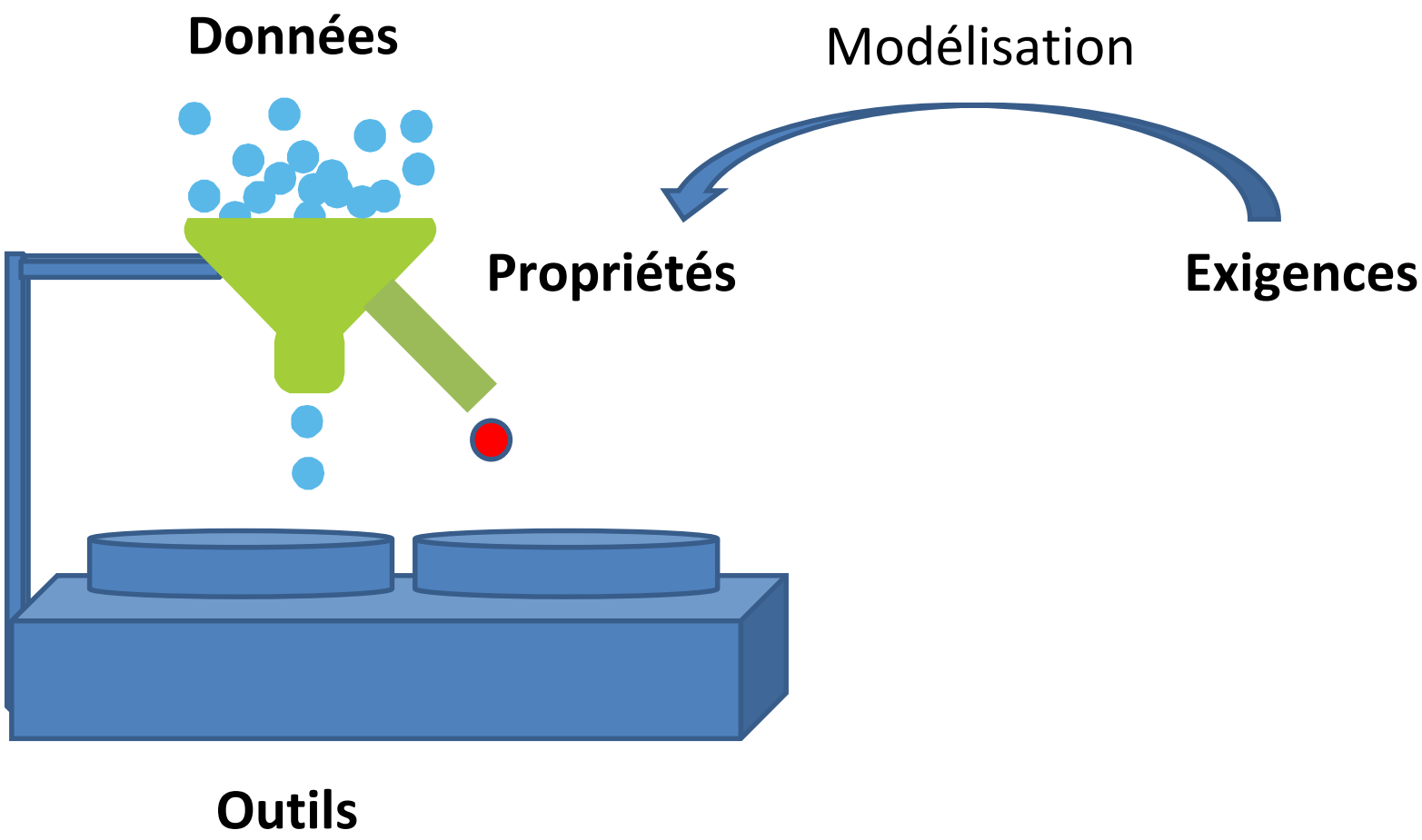
Un nouveau rôle

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

Validation formelle



Un filtre à données

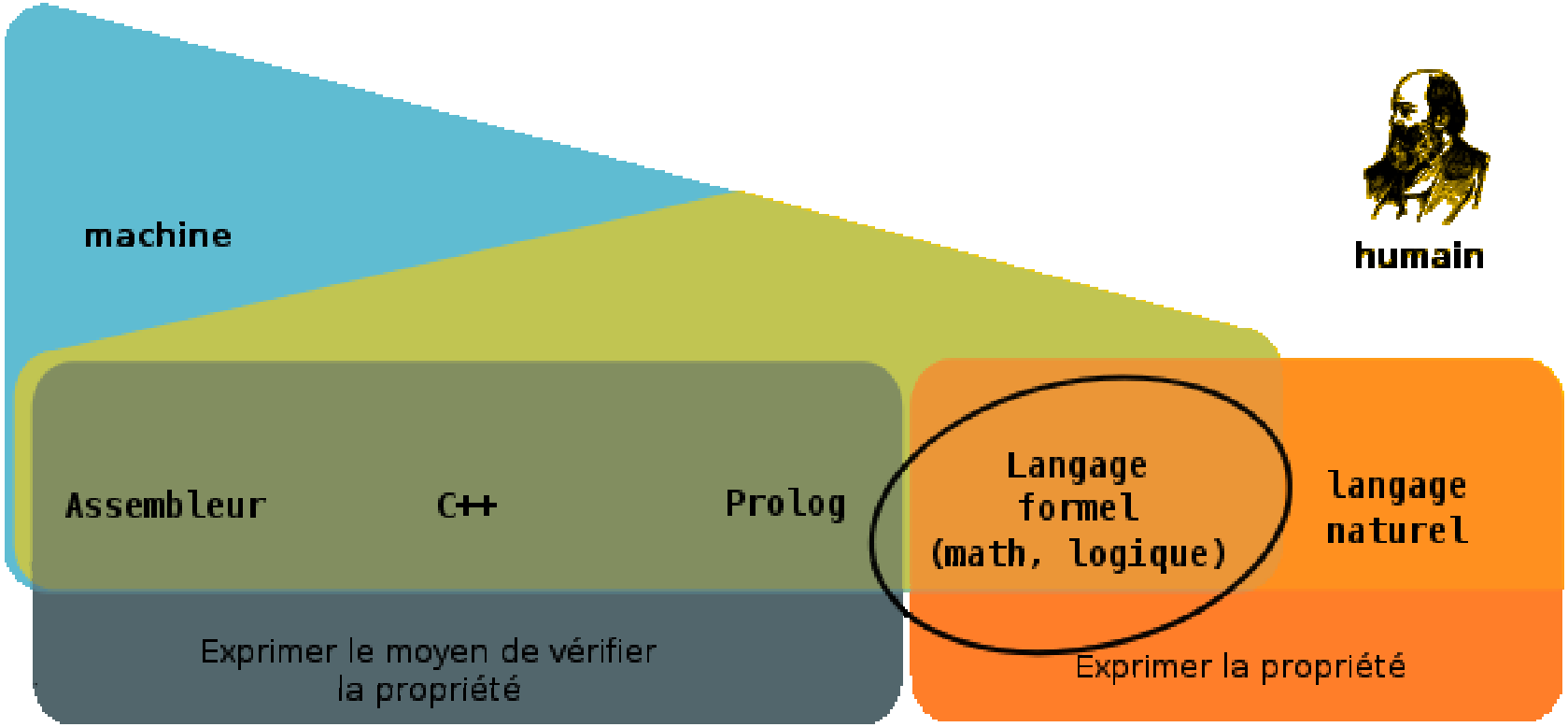


Séparation propriétés outils

- Les outils ont leur propre cycle de vie
  - Stabilité des outils

- Indépendance des propriétés
  - Facilite l'ajout/suppression
  - Groupe de propriétés suivant les versions

A chacun son langage



Informaticien Modélisateur Expert métier

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

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

Exemple d'expression de propriétés

Lors du séquencement d'une opération I/O, les ports et appareils décrits doivent être connectés

$$\forall (p,a) \;.\; p \mapsto a \in dom(Sequences)$$
$$\Rightarrow \quad (p \mapsto a) \in dom(Connectes)$$
$$\wedge \quad Connectes(p \mapsto a) = ON$$

```
private static boolean test_connected(int portId, int devId,
          List<Operation> seqs, boolean[][] connectStatus) {
     for (int i = 0; i < seqs.size(); i++) {
          final Operation op = seqs.get(i);
          final int sPortId = op.getPort();
          final int sDevId = op.getDevice();
          if (connectStatus[sDevId][sPortId] == false) {
               System.out.println("Port and devices not connected...");
               return false;
          }
     }
     return true;
}
```

Avantages

- Limiter les contraintes au niveau spécification
  - les experts métier sont dégagés des problématiques de vérification
- Permettre les vérifications
  - la relecture consiste à vérifier la bonne modélisation
  - les experts métier comprennent les propriétés
- Apport de la modélisation
  - Indépendance vis à vis du format des données
  - le modélisateur aide à la mise au point des propriétés

Les types d'outils

- Outils de preuve formelle
  - Ajout de règle (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

Tout reste à faire …

Maitrise du paramétrage

Maitrise des contraintes portant sur les données

Question?

christophe.metayer@systerel.fr