Description de PimCa

Le langage PimCA a été défini par une équipe de DGA-MI et un outil de modélisation basé sur cette définition a été développé au laboratoire. Le langage PimCA permet de modéliser des systèmes à différents niveaux d’abstraction. La modélisation de la structure d’un système mais aussi les graphes d’attaques possibles sont exprimables dans ce langage.

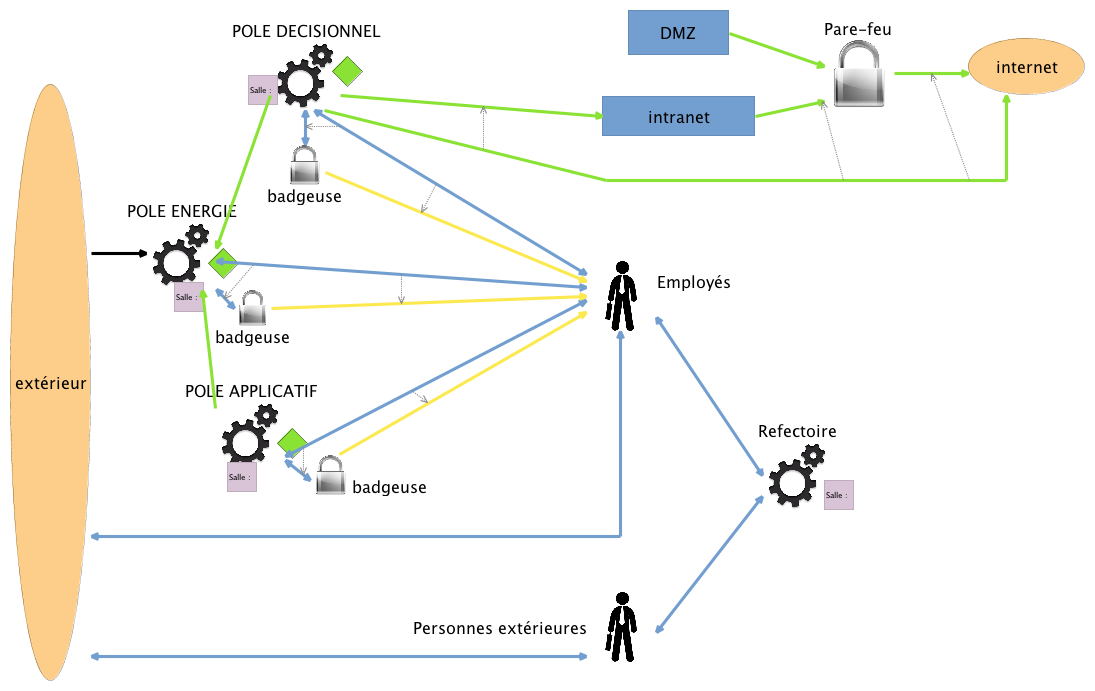


Figure 1: Un modèle réalisé avec l'outillage PimCA

Nous décrirons ici le langage PimCa dans son ensemble mais aussi un sous ensemble de PimCa appeler PimCa-Light.

# Pimca

L'outillage PimCA est basé sur le framework EMF(Eclipse Modeling Framework) avec un métamodèle au format Ecore représentant les concepts et les relations du langage. Il existe un éditeur graphique réalisé à l’aide du composant open source Sirius permettant d'éditer un diagramme de connaissance. Cet outillage a été développé au cours de l’année 2015. Ainsi les modèles de niveau système et les modèles des architectures numériques seront réalisés avec cet outillage dans la suite de nos expérimentations.

Le langage possède deux grandes composantes :

* Un modèle de connaissance,
* Un modèle de scénarii d’attaque

## Le modèle de connaissance

Le modèle de connaissance (Knowledge Model) représente un système faisant l’objet d’une analyse de sécurité. Le système est composé (entre autre) d’un ensemble de machineries (Machinery), interconnectées entre elles par trois types de flux : énergie (Energy), matière/données (Matter/Data), et contrôle (Control), cf figure 2.

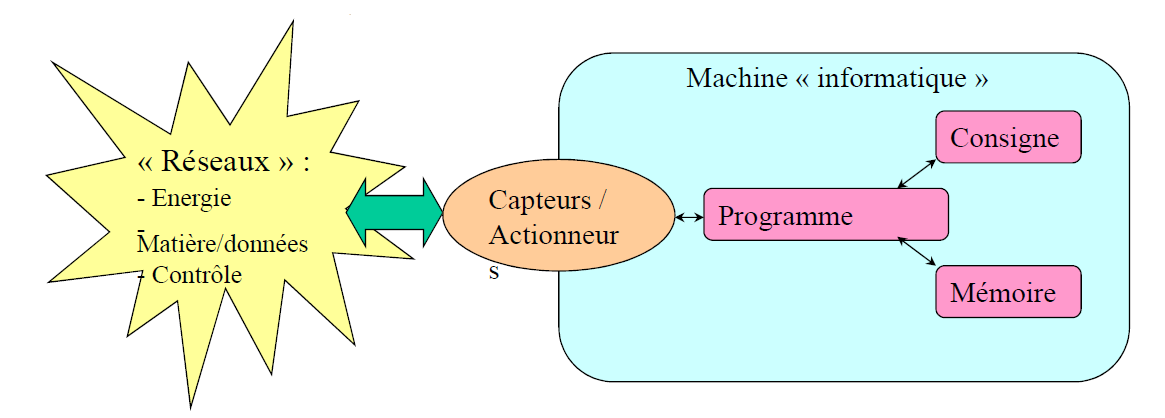


Figure 2 : Schéma des concepts principaux de Pimca

La machinerie est caractérisée par trois concepts clés : exécution – configuration – mémoire avec leur interface.

### Les concepts principaux

#### Les « machines » :

|  |  |
| --- | --- |
| **Icône-Concept** | **Description** |
| **machineMachinery** | **Machinerie** : système manipulant des Ressources (regroupement particulier) : voiture, animal, PC, processus |
| **C:\Users\creffst\AppData\Local\Microsoft\Windows\INetCache\Content.Word\executant.pngPerformer** | **Exécutant (spécialise Machinerie)** : ce qui transforme la Ressource, e.g. UC/Programme, cerveau, régulateur. |
| **reseauNetwork** | **Réseau** **(spécialise Machinerie)** : zone d’échange de matière, d’information, d’énergie, etc. : câblage, tuyauterie, IPC Engine. |
| **douaneCustoms** | **Douane (spécialise Machinerie)** : fonctionnalité particulière mise en place par une Machinerie pour identifier & autoriser une autre Machinerie : cadenas, garde, login, crypto |
| **interfaceInterface** | **Interface (spécialise Machinerie)** : permet de passer d’une Machinerie à une autre, du monde physique au monde virtuel et inversement : NIC, caméra, clavier, écran. |
| **regroupement Gathering** (non réifié) | **Regroupement** : ensemble logique d’objets de tout type, entrepôt sans Ressource. Un regroupement ne possède pas les infos propres à une machinerie, c.-à-d. executant, configuration, mémoire. |
| **C:\Users\creffst\AppData\Local\Microsoft\Windows\INetCache\Content.Word\entrepot.pngRepository** | **Entrepôt** : zone de stockage de Ressource : armoire, bâtiment, disquette, database, file system |

#### Les « ressources » :

|  |  |
| --- | --- |
| **Icône-Concept** | **Description** |
| **ressourceResource** | **Ressource** : ce qui est transformé, manipulé par une Machinerie : matière, électricité, document, log, data |
| **consigneInstructions** | **Consigne (spécialise Ressource)** : La direction, les paramètres que l’exécutant suit : Fichier de configuration, ordre, politique de sécurité |
| **C:\Users\creffst\AppData\Local\Microsoft\Windows\INetCache\Content.Word\passeport.pngPasseport** | **Passeport (spécialise Ressource) :** élément à fournir à la Douane pour être identifié / autorisé : clef, carte d’identité, badge, login/password, clef de chiffrement |

#### Les « relations » :

|  |  |
| --- | --- |
| **Icône-Concept** | **Description** |
| **Verification** | **Vérificateur** : Visualise le bon fonctionnement du processus |
| **Swap** | **Echange** : Communication d’égal à égal, utilisation / production interdépendante. |
| **Control** | **Contrôle** : Donne la direction, agit sur la consigne, administre |
| **Use** | **Utilisation**, Consommation, Client : Besoin pour fonctionner (ressource, énergie, exécutant, …) |
| **Produce** | **Développeur**, Producteur, Fournisseur : Réalise un objet, une ressource |
| **Maintain** | **Maintenance** : Agit partiellement sur la constitution d’objet, l’état, … |
| **adt** | **Au travers de** |

Un des intérêts de ce modèle de connaissances est la capacité de modéliser des systèmes à différents niveaux d’abstraction ou de raffinement. PimCa peut être utilisé par exemple pour décrire un système numérique dans son contexte mais aussi les différentes architectures associées.

## Le modèle de scénarii d’attaque

Ce modèle de scénarios d’attaque regroupe l’ensemble des possibles et représente un support d’analyse pour la sélection du chemin d’attaque le plus sûr. Ce modèle est basé sur le séquencement des activités définissant un scenario, ou plusieurs, qui peut être séquentiel ou parallèle. Ces scénarii sont basés sur les éléments structuraux du modèle de connaissance associés aux activités qui sont : observer le système, raisonner sur le système et agir sur le système. Différentes actions pour agir sur le système étant possibles. Sans détailler plus avant ces différentes actions, nous pouvons noter que dans un premier temps nous nous attacherons aux actions d’observation et de raisonnement, dans le sens où nous chercherons à évaluer les observations effectuées.

# PimCa-Light

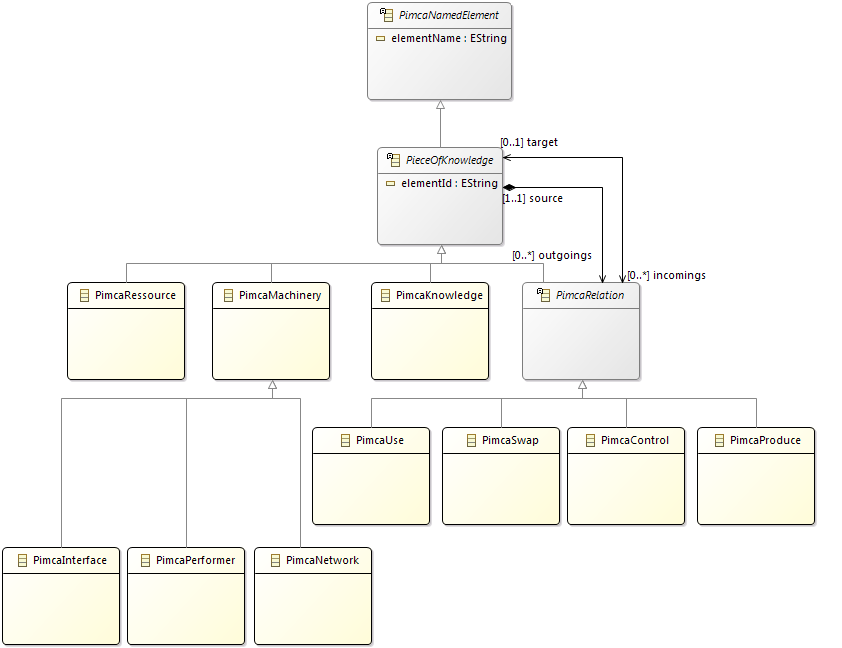
PimCa-Light est une simplification du langage PimCa. Cette simplification doit permettre de décrire notre système étudié grâce à l'outillage, c’est pourquoi seules les notions utiles à notre cas d’étude ont été gardées.

Figure 3:Metamodèle de PimCa-Light

Le méta model présenté dans la figure 3 permet d’instancié un model PimCa représentant le system étudié dans le cas d’usage.

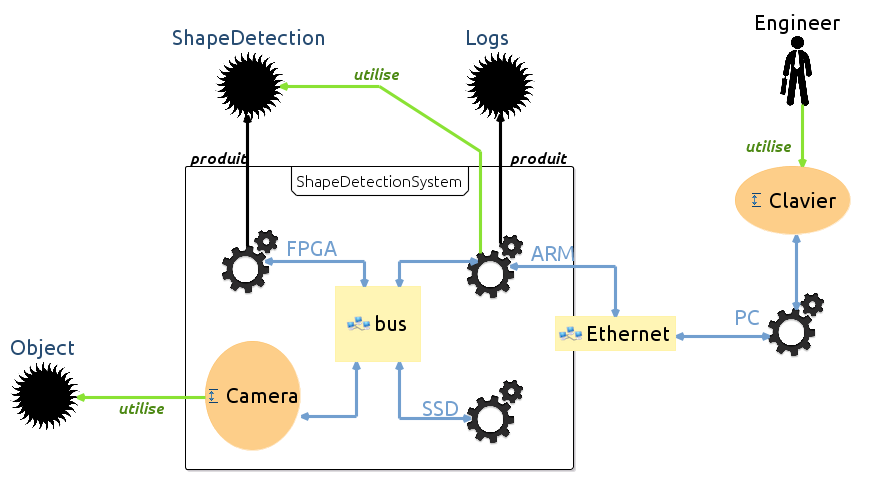


Figure 4: Modèle PimCa d'un system de reconnaissance de forme

Le système présenté dans la figure 4 est un système cyber physique(CPS) qui se compose d'un FPGA pour la récupération et le pré-traitement du flux vidéo, lui-même relié à un processeur au travers de son banc de registres. Il est possible d'accéder au processeur par communication réseau via une liaison Ethernet.