Modèle système dynamique pour l'analyse de la menace

Tithnara Nicolas SUN

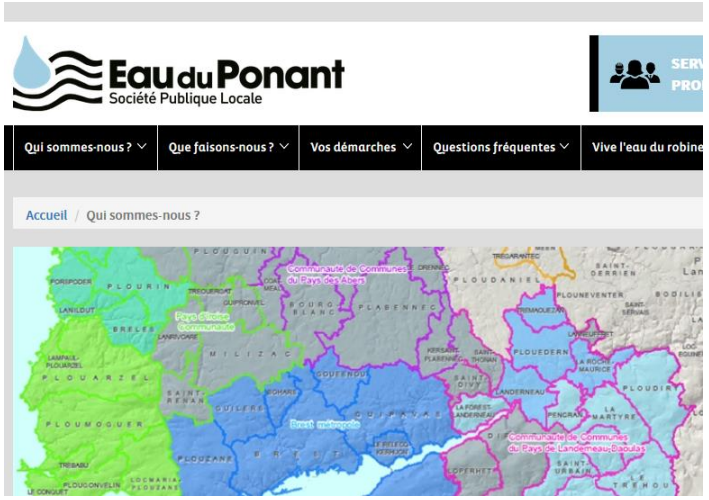
Philippe Dhaussy (Lab-STICC)
Lionel Van Aertryck (DGA-MI)
Ciprian Teodorov (Lab-STICC)
Alain Plantec
Joaquin Garcia-Alfaro

Sommaire

- Contexte
- Avancement
- Conclusion

Contexte
Cyber Threat Intelligence





Contexte
Cyber Threat Intelligence

- Système de contrôle industriel
  - Interfaces cyber-physiques
  - Systèmes hétérogènes (specs & plateformes)
  - Fonctionnement dynamique

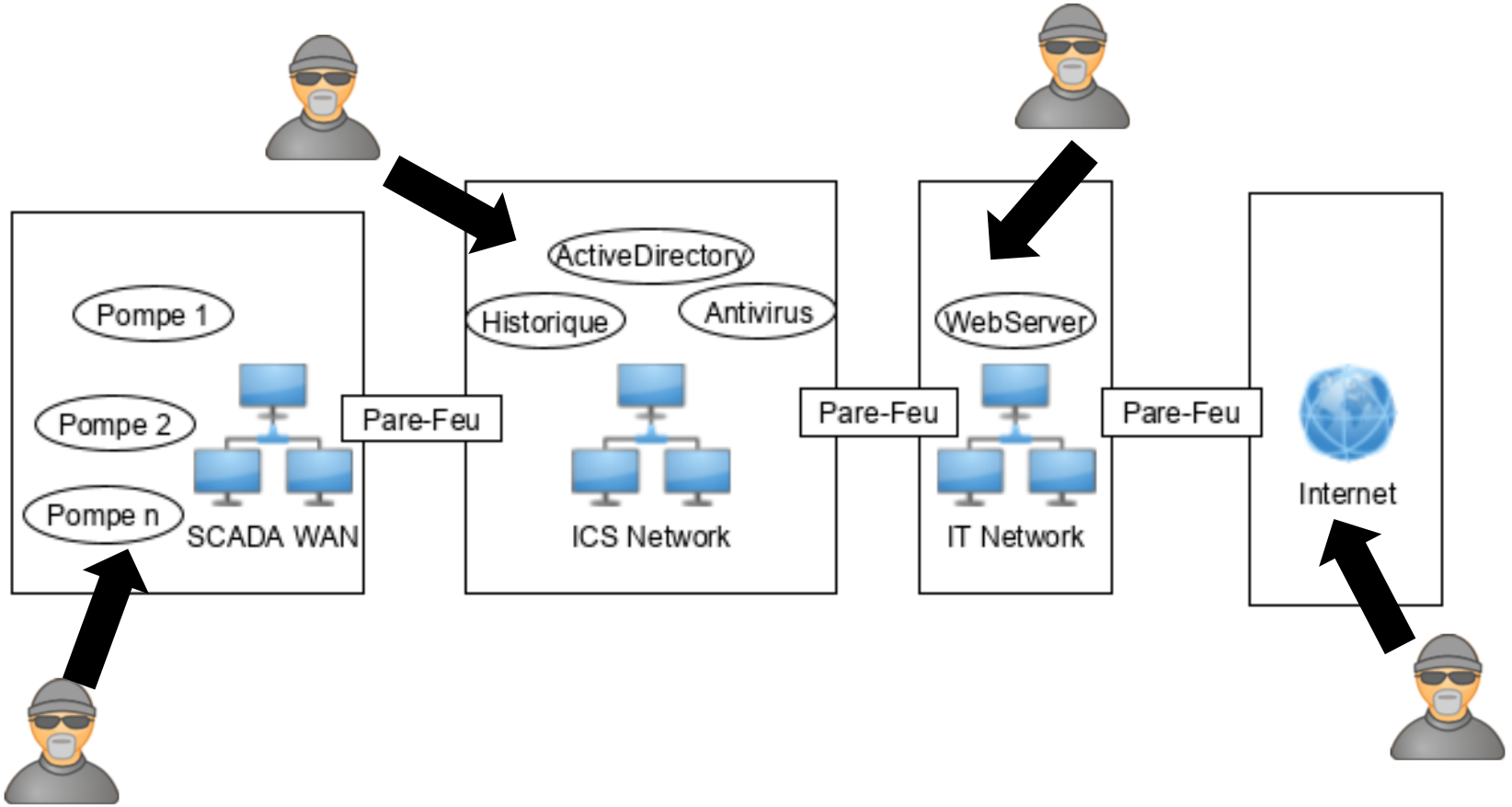
Surface d'attaque :

Ensemble des **points d'entrée** et des **points de communication** qu'un système possède avec l'extérieur.[1]

Zone de contention entre l'attaquant & la défense.

- [1] *Analyse et réduction de la surface d'attaque* / Mickael Dorigny / https://www.information-security.fr/ / 19 Décembre 2015

Contexte
Cyber Threat Intelligence



Comment produire une analyse de sécurité?

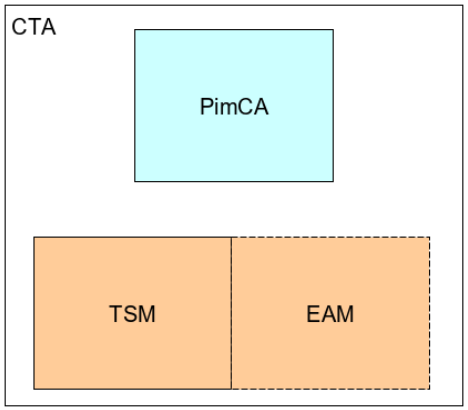
①Comment est fait le système ?

②Comment fonctionne le système ?

③Comment attaquer le système ?

Méthodologie basée sur la fédération de trois DSL: **Cyber Threat Application (CTA)**

- Pimca - (Modéliser la structure)
- Target system modeling – TSM - (Modéliser le comportement nominal)
- Executable attack modeling – EAM – (Dérouler des scénarios d'attaque)



Contexte
Approche envisagée

- Comment est fait le système ?

  Pimca①

- Comment fonctionne le système ?

  TSM②

- Comment attaquer le système ?

  EAM③

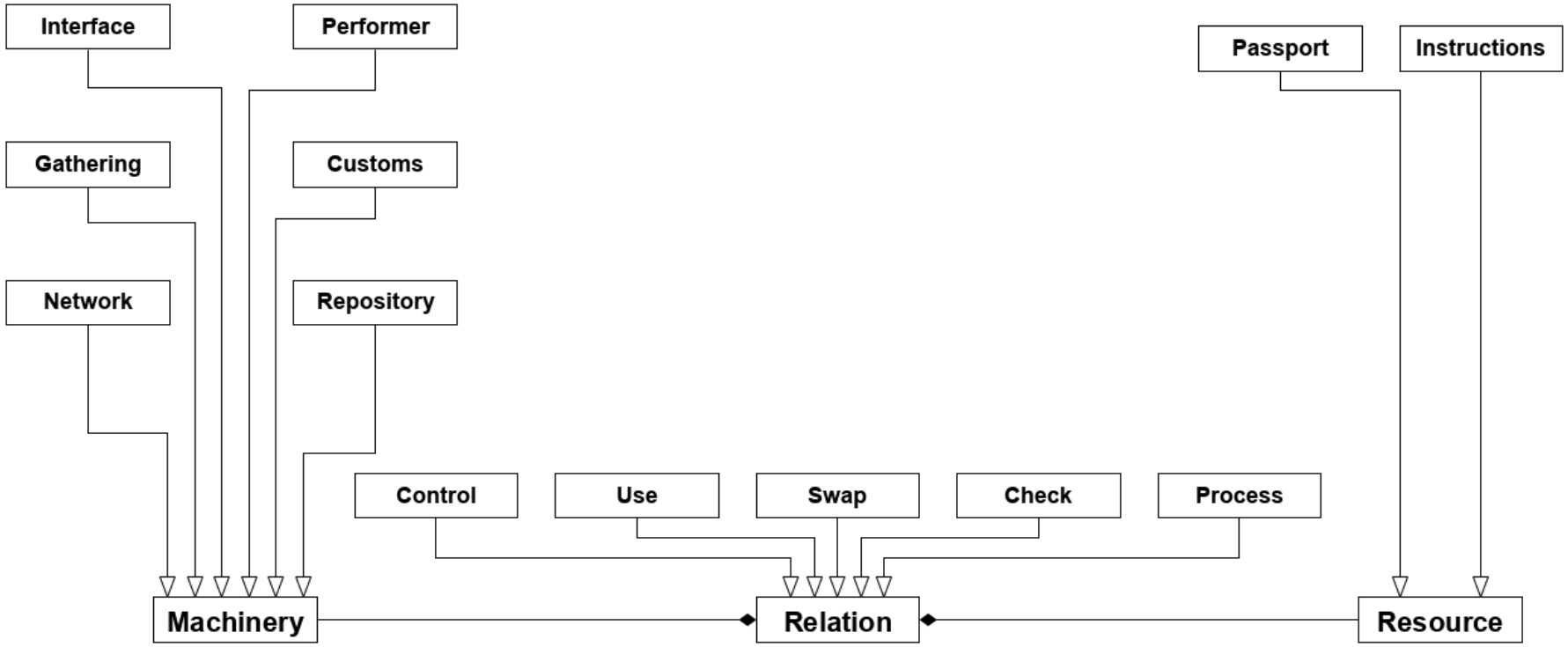
Avancement

A)Pimca

B)TSM-EAM

Contribution PimCA

- Architecture statique du système



Contribution Pimca

Machinerie:

- Elément **actif** pourvu d'un **comportement**
  - **Performer** := Entité humaine.
  - **Réseau** := Entité qui transmet les données/messages/matières d'une machinerie à l'autre.
  - **Douane** := Entité qui bloque les échanges à moins d'avoir accès au passeport correspondant.
  - **Interface** := Entité marque la séparation d'un espace à un autre.
  - **Regroupement** := Ensemble de machineries.
  - **Conteneur** := Entité qui contient des ressources.

Contribution Pimca

Ressource:

- Elément **passif**
- **Instructions** := Description d'un comportement de machinerie.
- **Passeport** := Ressource dont dépend une douane, nécessaire pour communiquer à travers la douane.

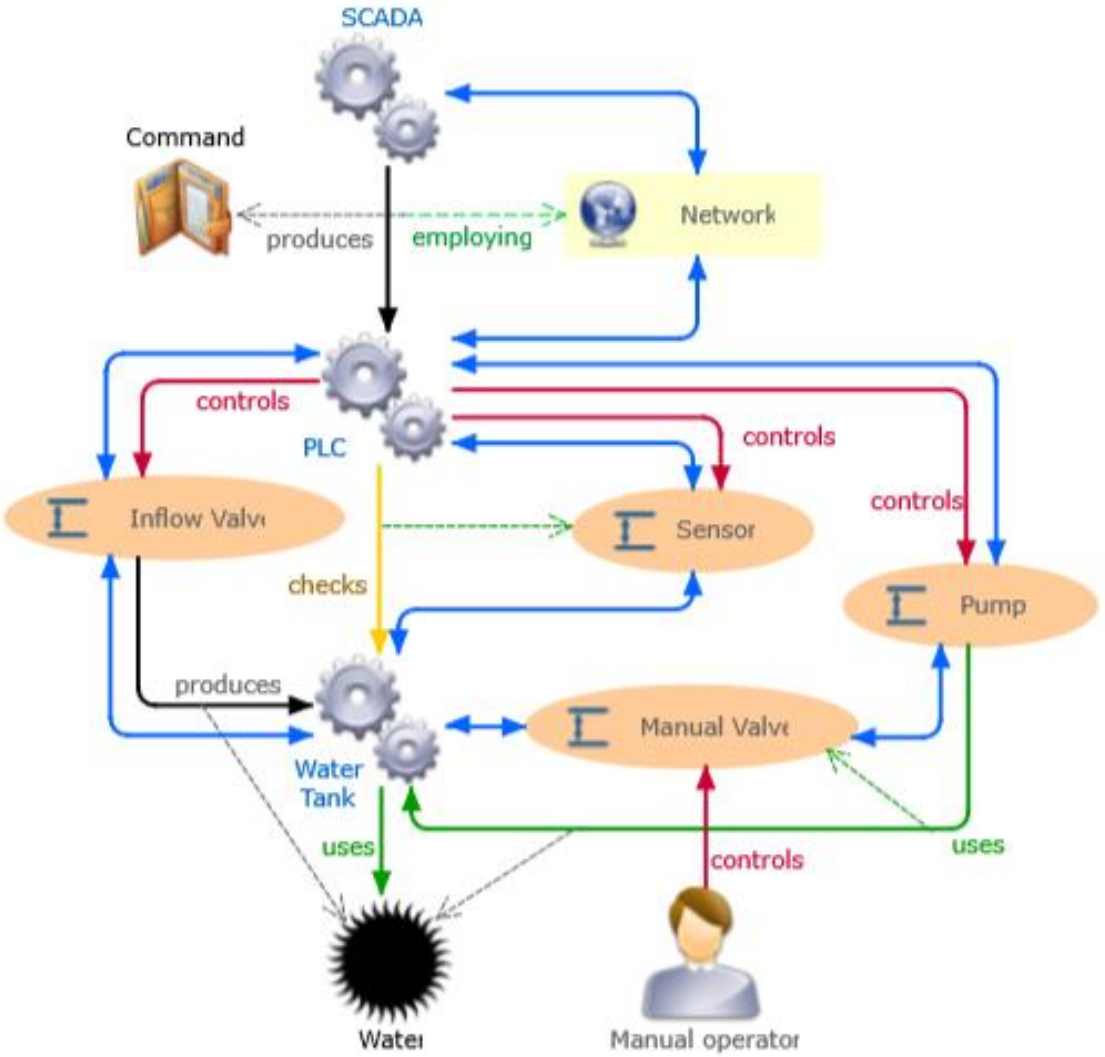
Contribution Pimca

Nom	Sens	Description
Echange	Bidirectionnel	Lien de communication générique entre deux entités, existence de variables partagées
Vérification	Unidirectionnel	Lien de droit en lecture, existence de variables observables chez la cible.
Contrôle	Unidirectionnel	Lien de droit en écriture, existence de variables observables et de comportements déclenchables chez la cible. Présuppose le lien de vérification.
Utilisation	Unidirectionnel	Lien de droit en écriture limité, existence de certain comportement déclenchable chez la cible.
Processus	Unidirectionnel	Lien de flux de matière/données.

Contribution Pimca

Cas d'étude :

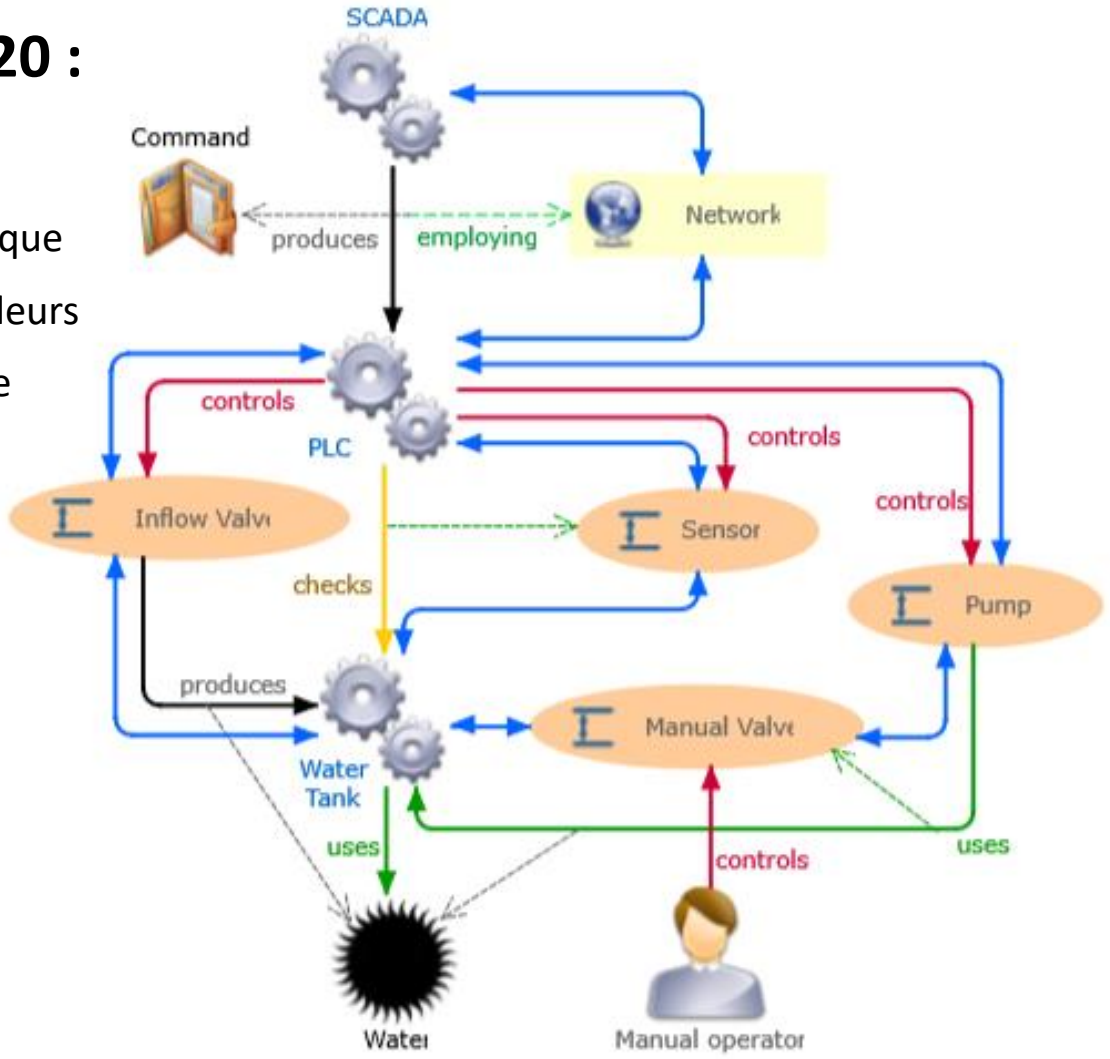
Station de pompe d'eau



Contribution Pimca

Article soumis à ICISSP 2020 :

1. Modéliser le système
   - Pour souligner la surface d'attaque
   - Pour communiquer entre décideurs
   - Pour permettre des analyses de sécurité
2. Modéliser 2 use cases
   - Pompe
   - Réseau d'entreprise
3. Comparer à la littérature



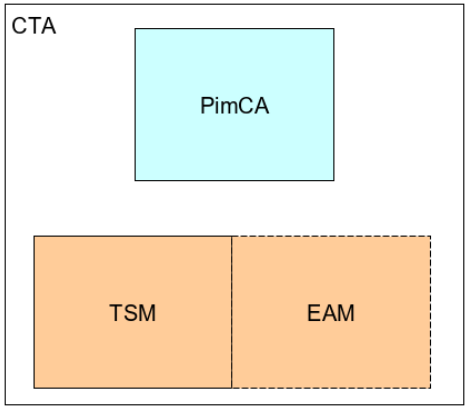
Avancement

A)Pimca

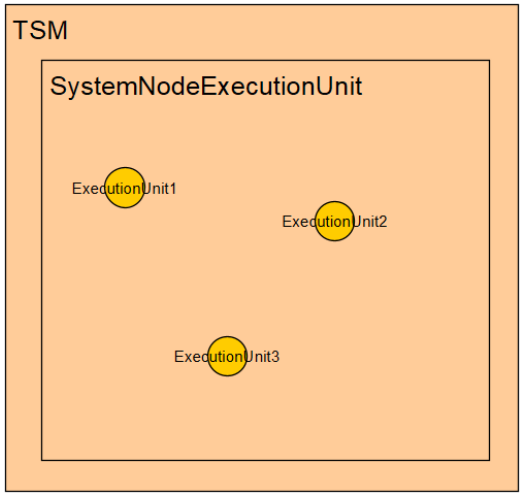
B)TSM-EAM

Contribution TSM-EAM

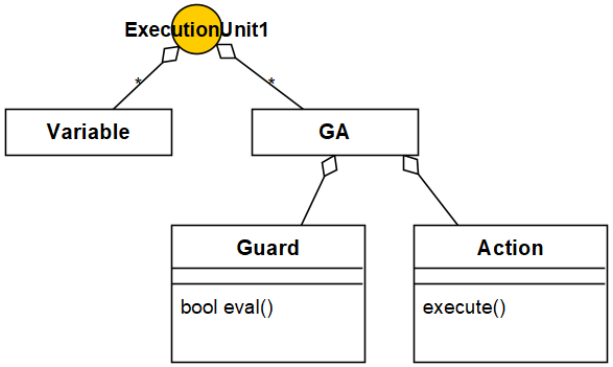
- Dynamique TSM-EAM②③



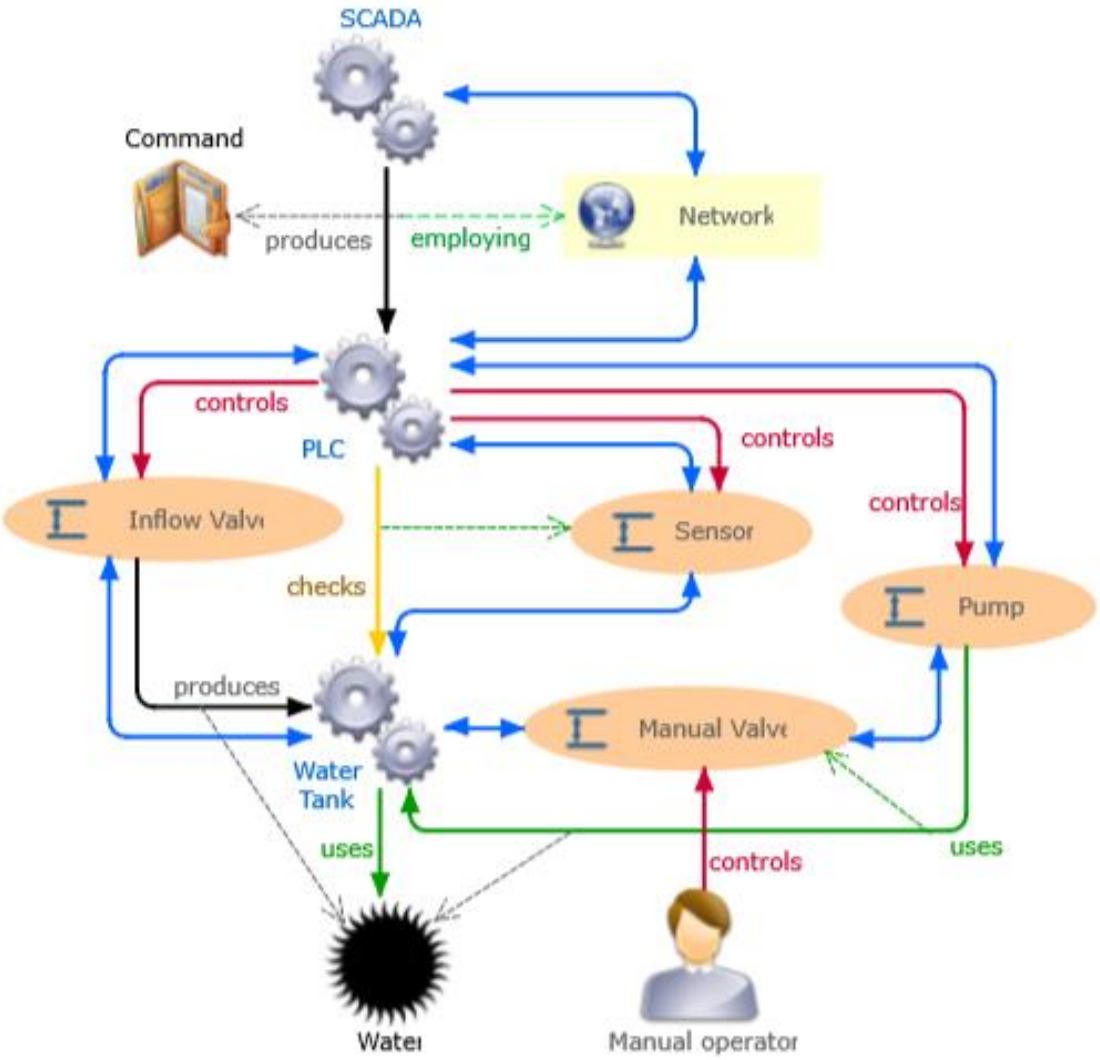
- ExecutionUnit



- Guard/Action



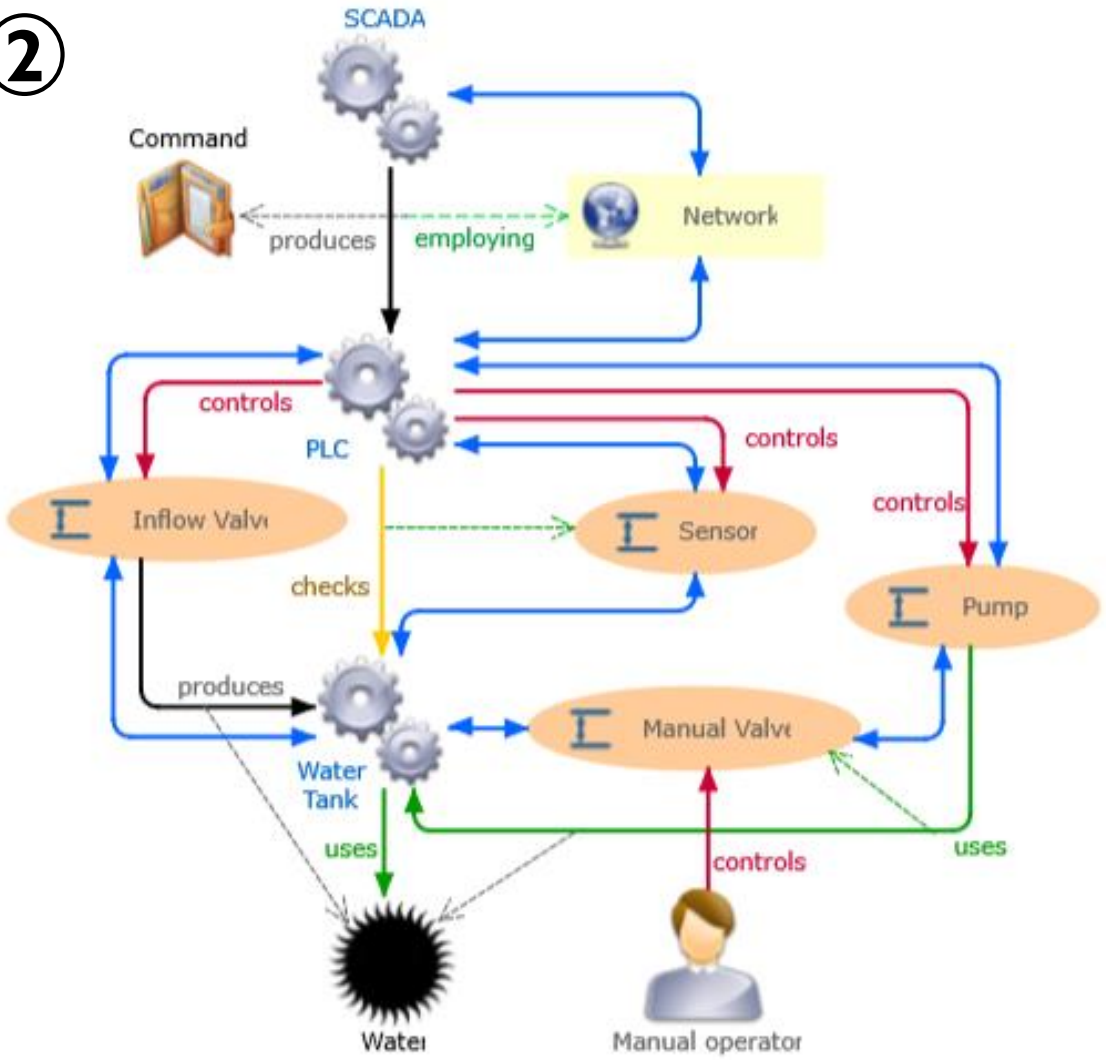
Contribution TSM-EAM



Contribution TSM-EAM

1.La valve d'entrée fait rentrer l'eau dans le réservoir.
2.Le capteur vérifie le niveau d'eau dans le réservoir.
3.Le capteur communique sa mesure au PLC.
4.Quand le niveau d'eau atteint un seuil (Instructions), le PLC ordonne à la valve de se fermer et à la pompe de se mettre en marche.
5. Quand le niveau d'eau atteint un seuil (Instructions), le PLC ordonne à la valve de s'ouvrir et à la pompe de s'éteindre.
6.La valve manuelle peut être ouverte ou fermée par un agent humain.
7.Une centrale SCADA communique avec le PLC.

②



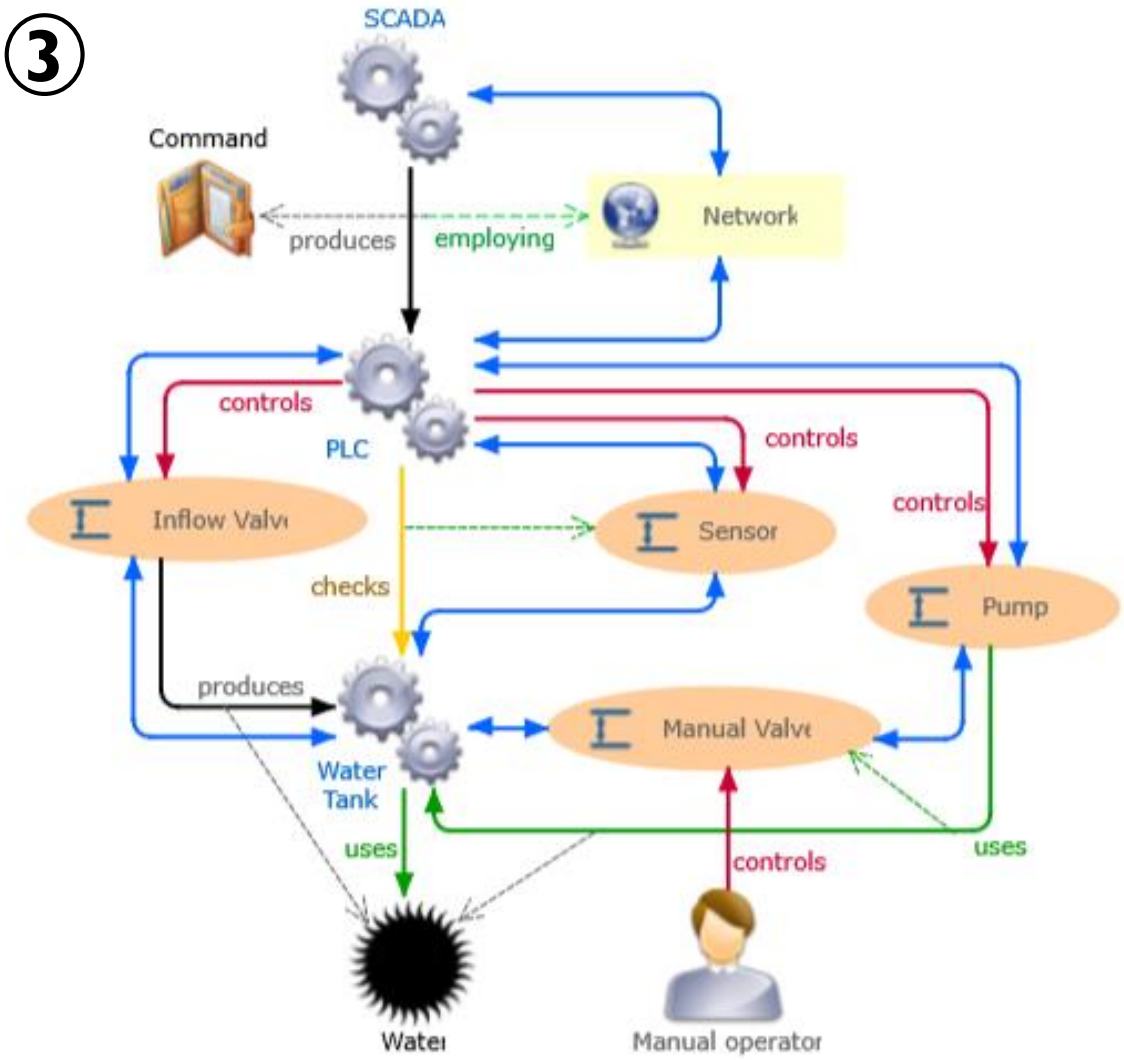
Contribution TSM-EAM

Exemple de scénario d'attaque:

1. L'attaquant ferme manuellement la valve de sortie.

2. L'attaquant force la valve d'entrée ouverte.

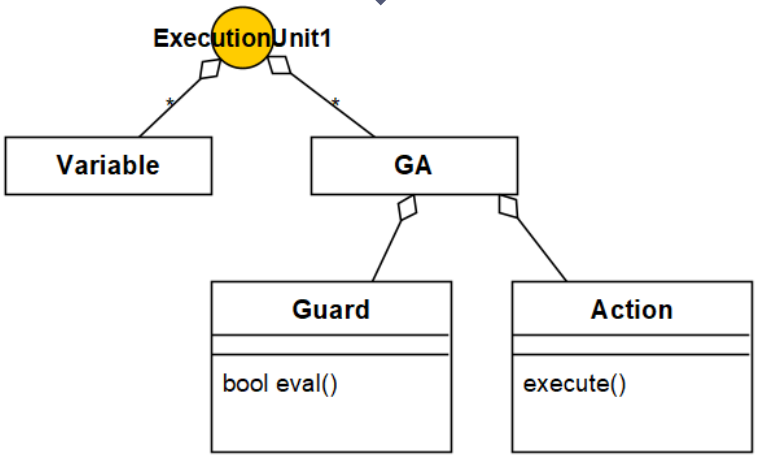
3. L'attaquant cause un débordement du réservoir.

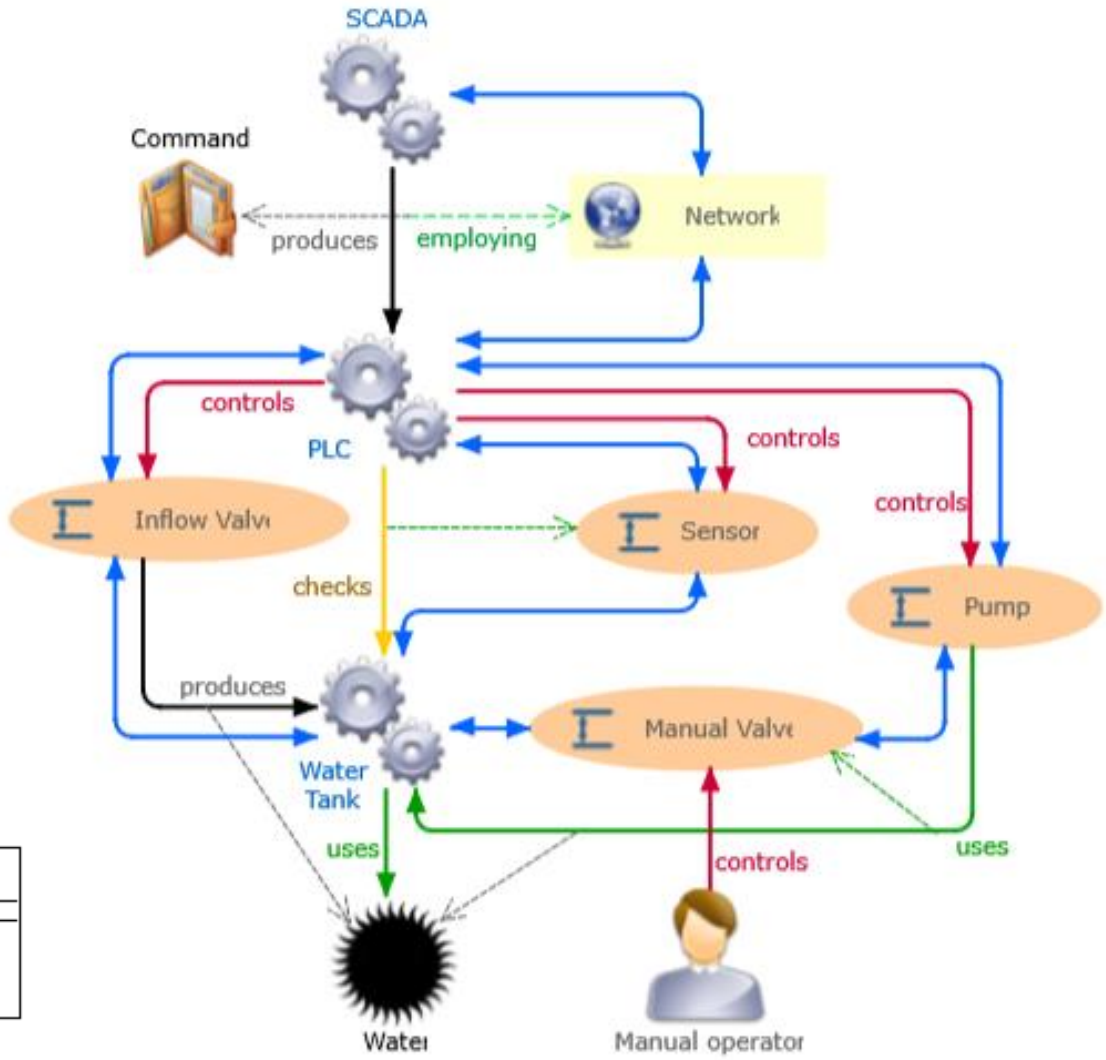


Contribution TSM-EAM

UPPAAL

② ③





Contribution TSM-EAM

Bilan :

- **Implémenté en Garde/Action ② ③**
- **Fédéré avec Pimca ①**
- **Dynamique du cas d'étude capture par des automates communiquant**

Contribution TSM-EAM

A venir :

- **Transcrire les automates en Guard/Action ou outiller des automates ?**
  - **Comment modéliser la synchronisation ?** Booléen bloquants ?
- **Justifier la séparation TSM-EAM ou les joindre en un ?**
- **Etablir le lien entre Pimca et la modélisation TSM-EAM**
- **Ecrire un second article sur TSM-EAM**

Contribution TSM-EAM

A venir :

Plan du 2e article

- **Intro idem**
- **Cyber Threat Application Framework**
  - **Running Example**
  - **TSM**
  - **EAM**
- **Case study: Water Pumping Station**
  - **Concrete Evaluation**
- **Related works**
- **Conclusion**

Conclusion

Conclusion
Bilan

Approche

- PimCA — *Structure*
- Target System Modeling — *Comportement nominal*
- Executable Attack Modeling — *Scénarios d'attaque*
- ➢ **Cyber Threat Application**

Eléments stabilisés…

- Pimca
- Outillage OpenFlexo
- Exécution
- 1er Article

…et à préciser

- EAM
- TSM
- 2e Article

Conclusion
Perspectives

- Validation de la dynamique du cas d'étude
- Stabilisation de EAM & TSM
- Rédaction du second article sur l'approche globale
- Rédaction du manuscrit

Merci de votre attention