Pimca, modélisation système pour la cybersécurité

Tithnara Nicolas SUN

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

Sommaire

- Contexte
- Langage Pimca
- Cas d'étude

Contexte
Cyber Threat Intelligence

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

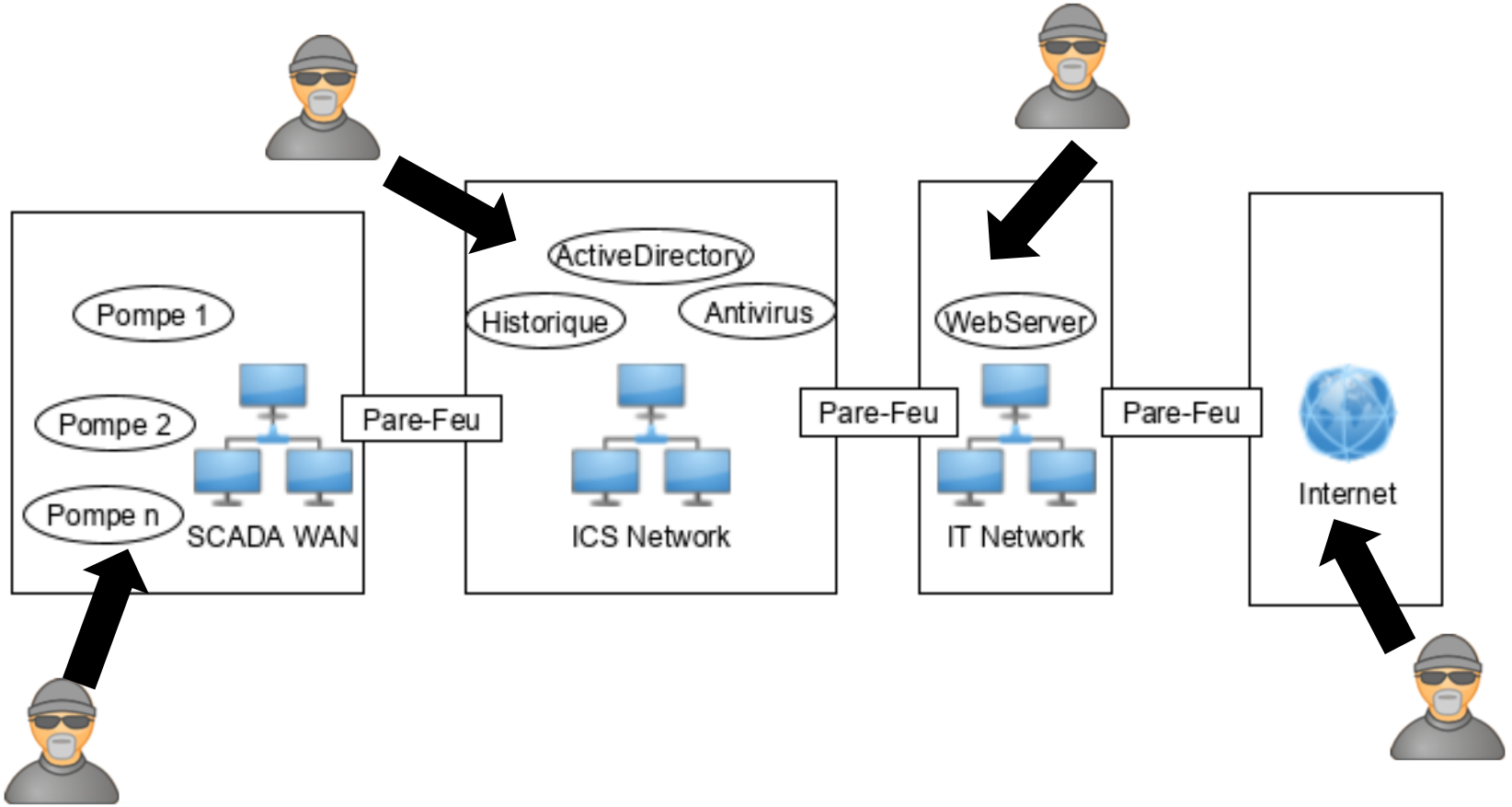
Surface d'attaque :

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?

- Comment est fait le système ?
- Comment fonctionne le système ?
- Comment attaquer le système ?

Contexte
Approche envisagée

- Comment est fait le système ?
- Comment fonctionne le système ?
- Comment attaquer le système ?

Pimca pour la modélisation de surface d'attaque dans le système

Comment produire une analyse de sécurité?

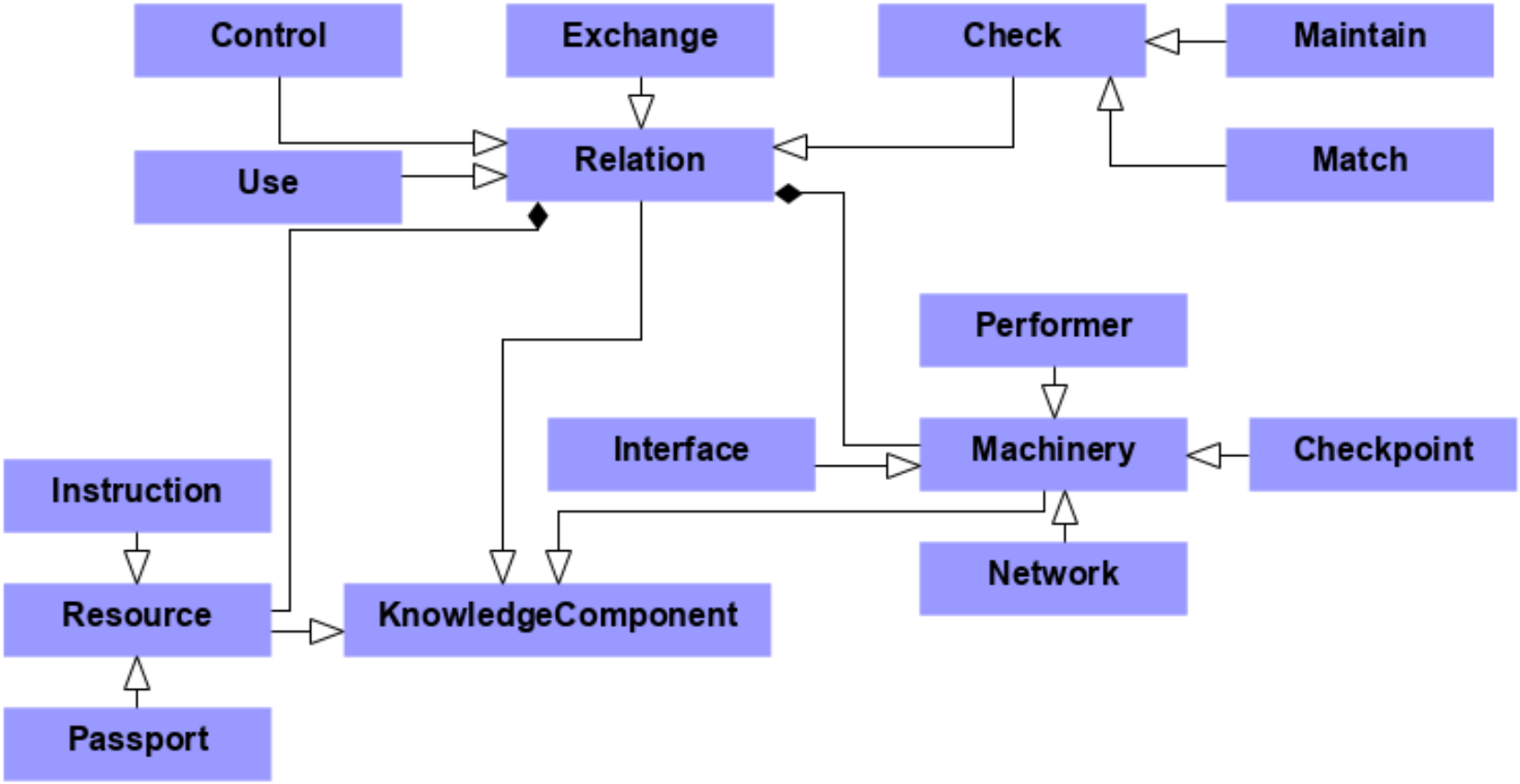
- Dolev-Yao [2]
- Moving Target Defense [3]
- STRIDE [4], Dagger [5]

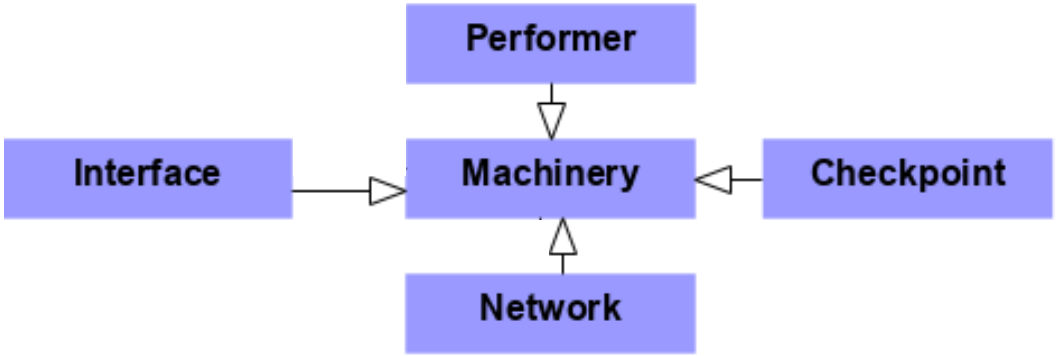
Pimca

- Souligner la surface d'attaque
- Offrir un aspect graphique
- Modéliser à un haut niveau d'abstraction
- Offrir des relations riches

Pimca
Langage

- Diagramme de classes

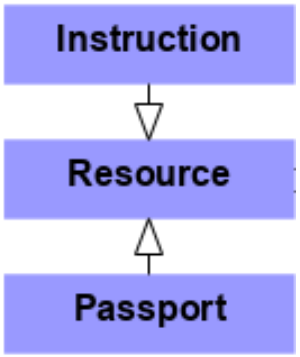




Machinerie:

- 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.

Pimca
Langage



Ressource:

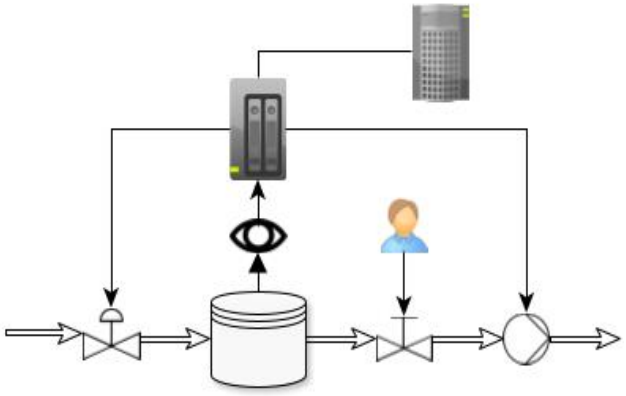
- Elément **passif**
- **Instructions** := Description d'un comportement de machinerie.
- **Passeport** := Ressource dont dépend une douane, nécessaire pour communiquer à travers la douane.

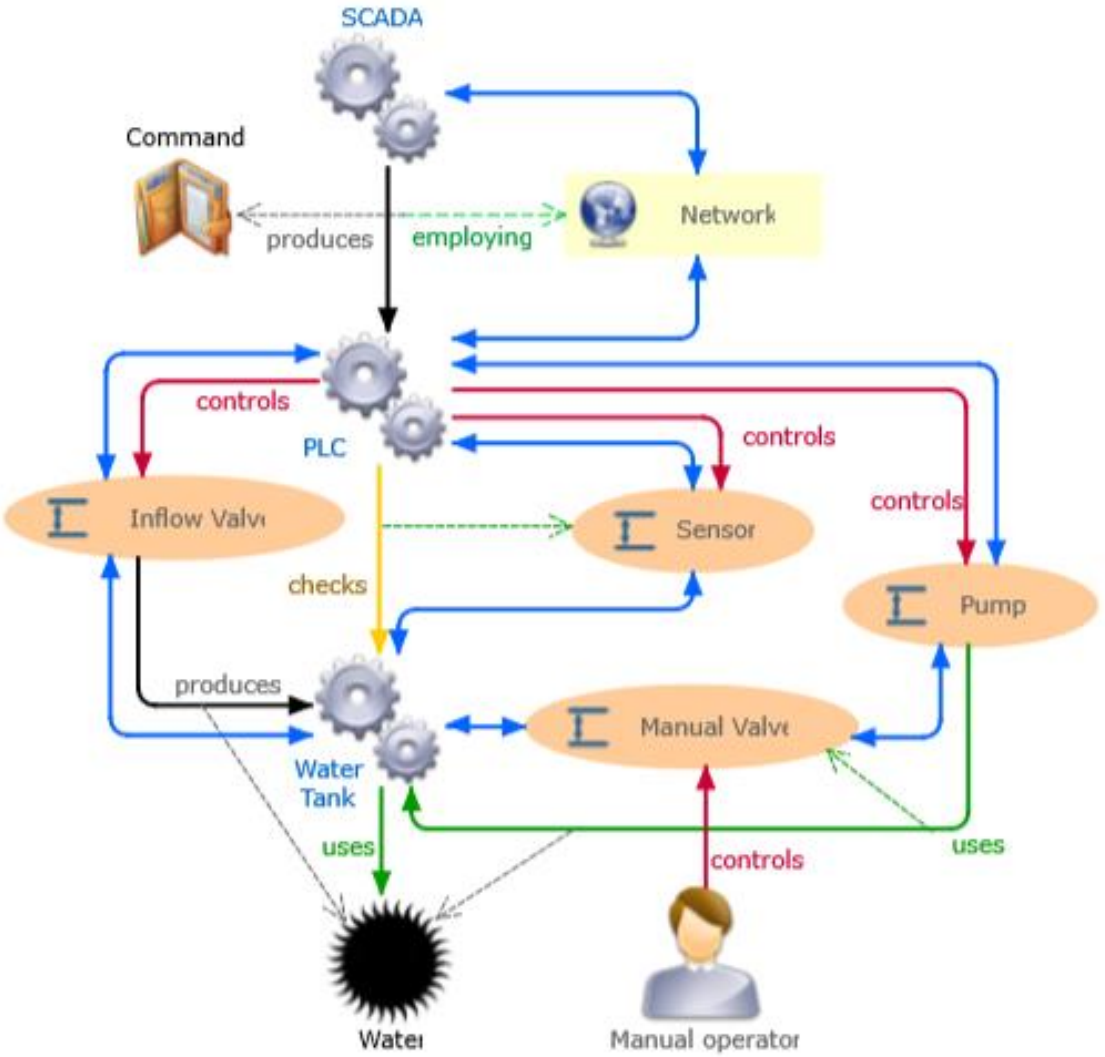
Pimca
Langage

Nom	Sens	Description
Echange	Bidirectionnel	Lien de communication générique entre deux entités, existence de variables partagées
Vérification	Unidirectionnel	Lien de surveillance/maintenance, notification de l'observateur sur certains comportements de l'observé,
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.

Cas d'étude :

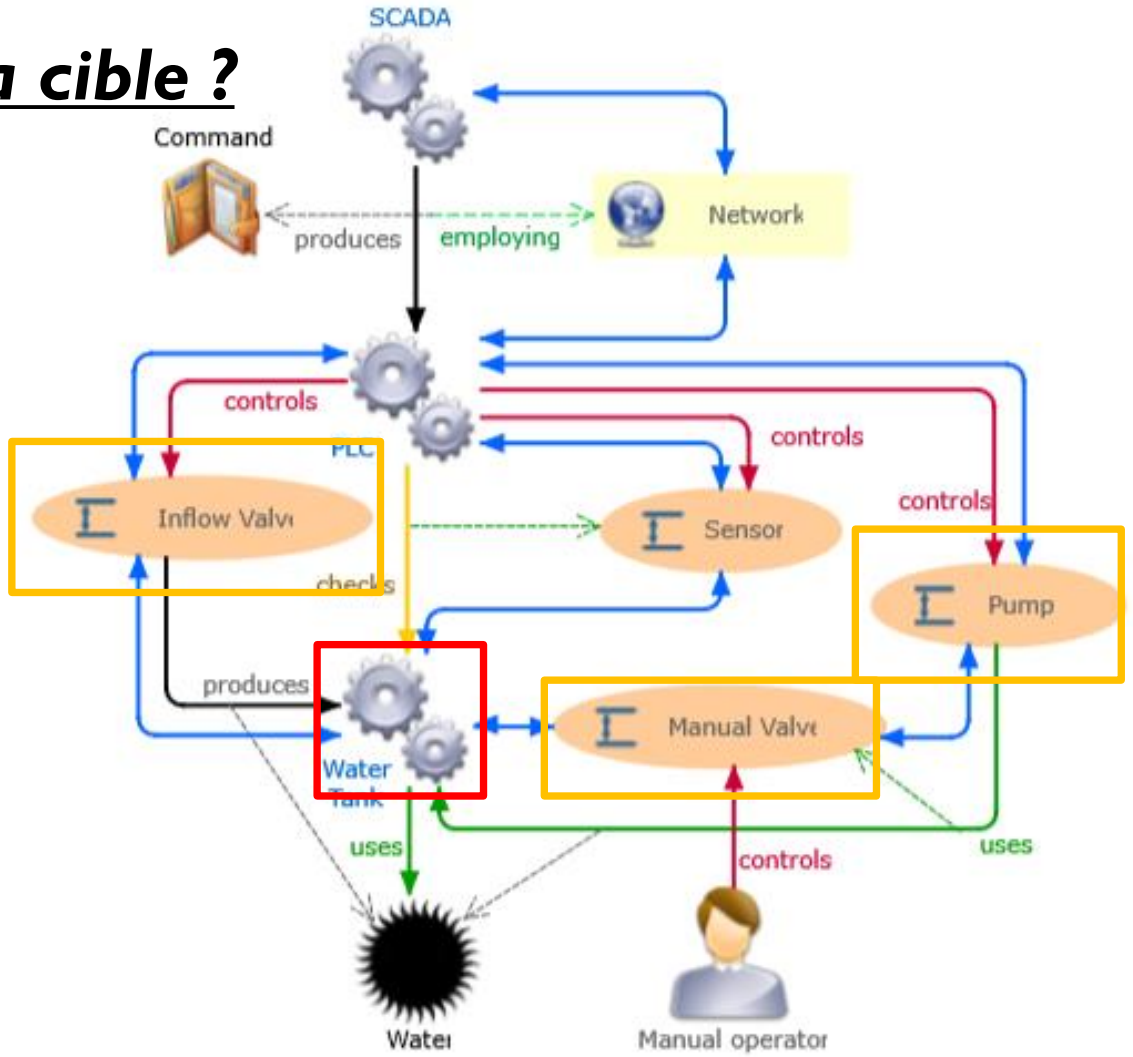
Station de pompe d'eau





Comment atteindre la cible ?

Cible: Réservoir d'eau
Déduction d'objectifs intermédiaires
=> Vanne d'entrée, vanne de sortie et pompe

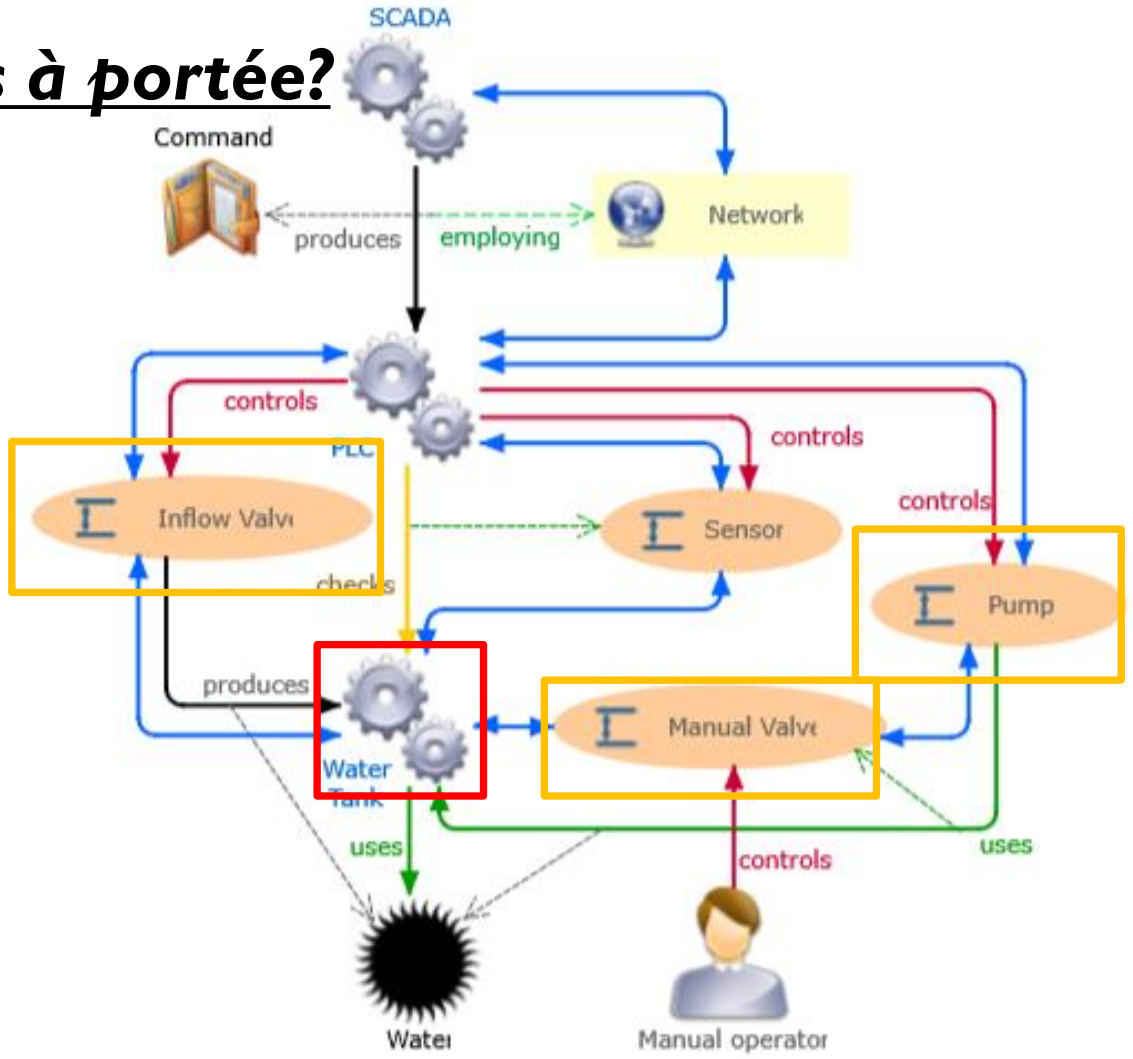


Quelles sont les cibles à portée?

Capacités : Ingénierie sociale, accès réseau

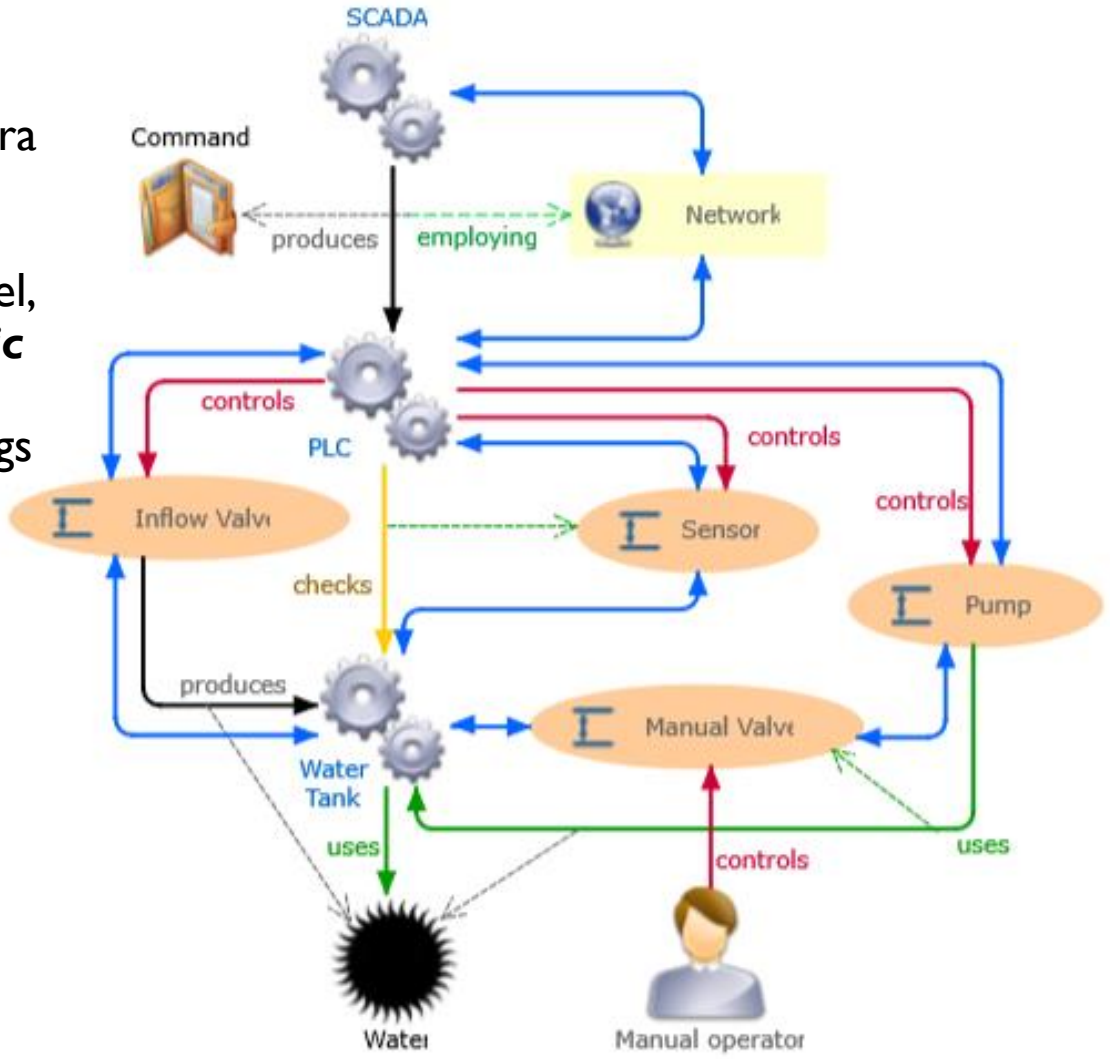
Déduction de points d'entrée

=> Opérateur manuel via le social, Instructions via le réseau



Pimca
Cas d'étude

Sun Tithnara N., Drouot Bastien, Golra Fahad R., Champeau Joël, Guérin Sylvain, Le Roux Luka, Mazo Raúl, Teodorov Ciprian, Van Aertryck Lionel, L'Hostis Bernard. ***A Domain-specific Modeling Framework for Attack Surface Modeling***. In the Proceedings of ICISSP 2020, SCITEPRESS, Valetta, Malta, 2020.



Modélisation dynamique

- Analyse formelle avec OBP2

- Scénarios d'attaque

Forcer vanne d'entrée		•					•	•	•		•	•
Fermer vanne manuelle			•						•	•		•
Bloquer pompe				•				•		•	•	
Brouiller réseau					•		•			•	•	•
Couper capteur						•						
Objectif 1	X	X	X	X	X	O	X	O	O	X	O	O
Objectif 2	-	-	-	-	-	O	-	X	X	-	O	O

TABLE 1 – Model-checking de la station de pompage (O : succès, X : échec)

Sun Tithnara N., Le Roux Luka, Teodorov Ciprian, Dhaussy Philippe. ***Exploration de Scénarios de Systèmes Cyber-Physiques pour l'Analyse de la Menace***. In the Proceedings of AFADL2020, Springer, 2020.

References

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

[2] Dolev, D. and Yao, A. C. (1981). *On the security of public key protocols*. In 22nd Annual Symposium on Foundations of Computer Science, SFCS '81, pages 350–357.IEEE Computer Society.

[3] Xu, J., Guo, P., Zhao, M., Erbacher, R. F., Zhu, M., and Liu,P. (2014). *Comparing different moving target defense techniques*. In First ACM Workshop on Moving Target Defense, pages 97–107. ACM.

[4] Khan, R., McLaughlin, K., Laverty, D., and Sezer, S.(2017). *STRIDE-based threat modeling for cyber-physical systems*. In 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), pages 1–6.

[5] E. Peterson. *Dagger : Modeling and visualization for mission impact situation awareness*. In MILCOM 2016-2016 IEEE Military Communications Conference, pages 25–30. IEEE, 2016.