



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)

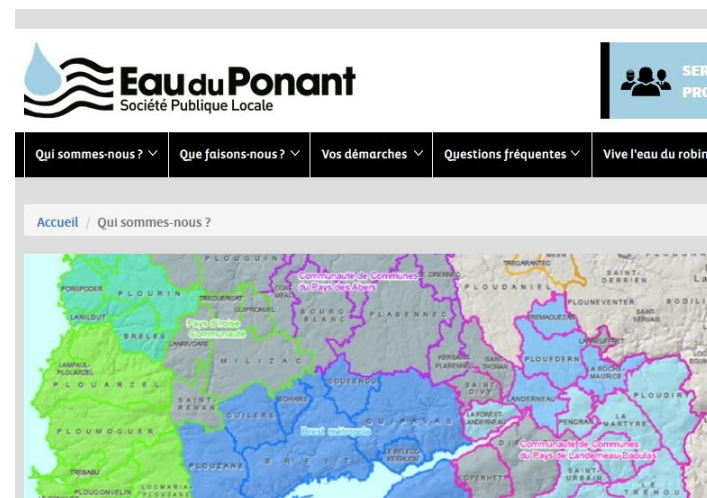
Alain Plantec

Joaquin Garcia-Alfaro

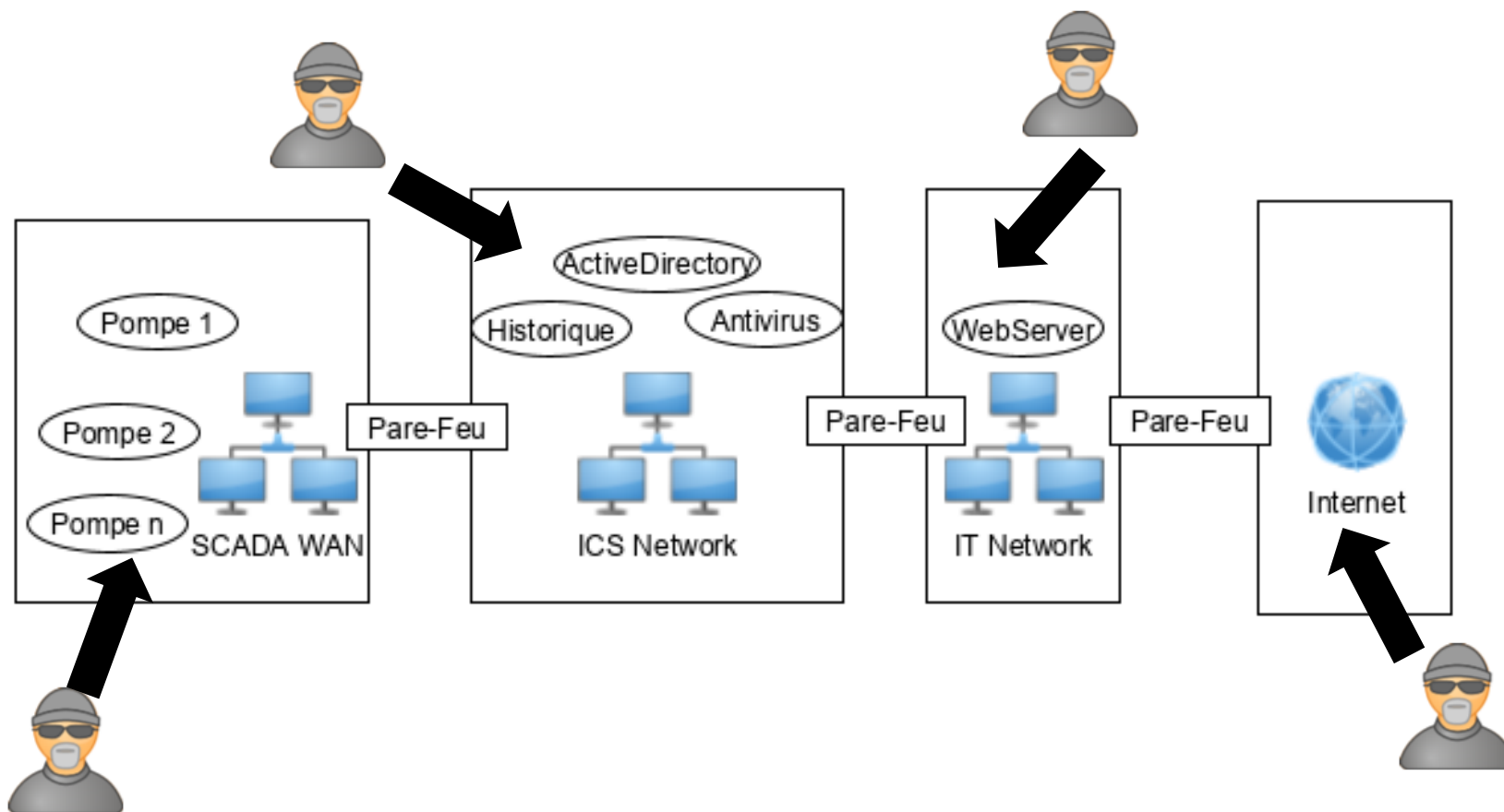
Sommaire

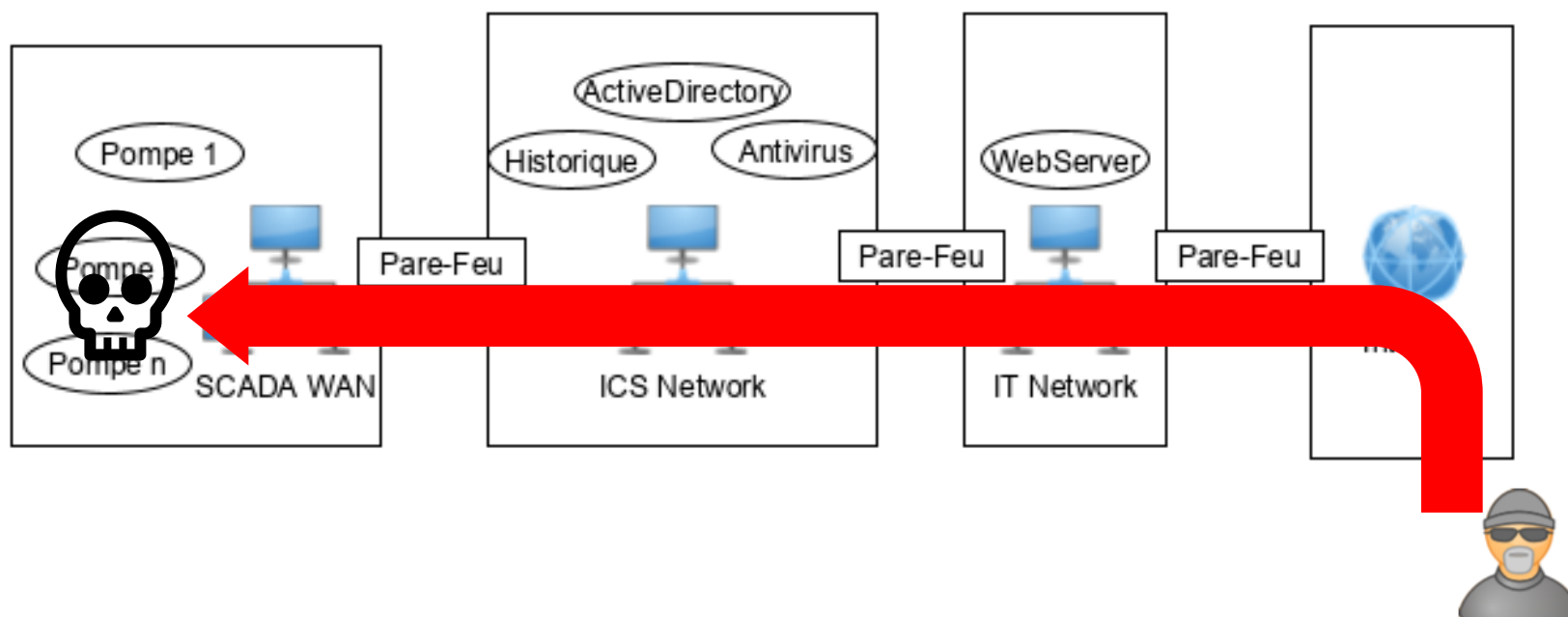
- Contexte
- Problématique
- Avancement
- Conclusion

Contexte Cyber Threat Intelligence



Contexte Cyber Threat Intelligence





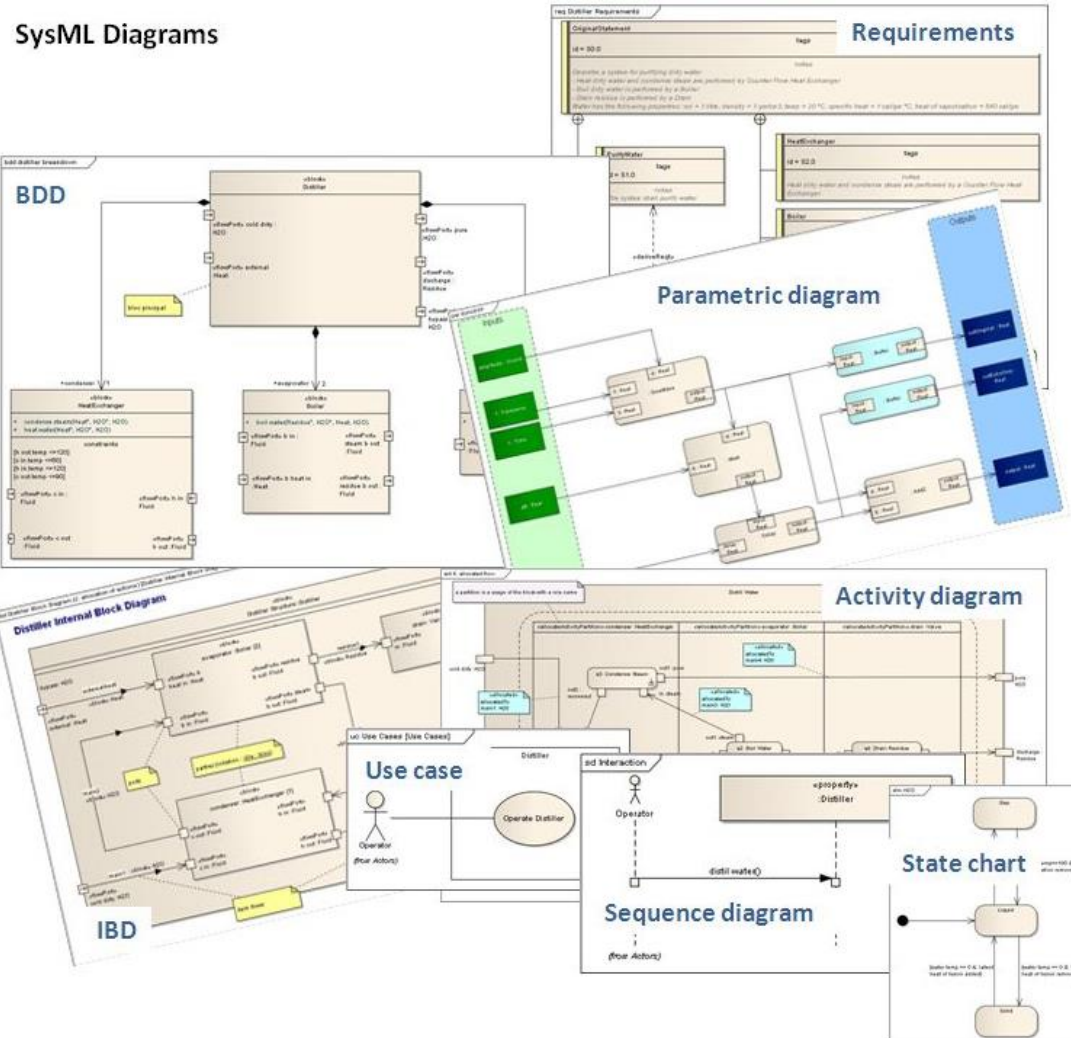
- Système de contrôle industriel
 - Interfaces cyber-physiques
 - Systèmes hétérogènes (specs & plateformes)
 - Fonctionnement dynamique

Comment attaquer le système ?

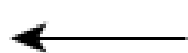
- Comment modéliser le système ?
- Comment modéliser les attaques ?

Contexte Modéliser le système

SysML



RAFT



Relations



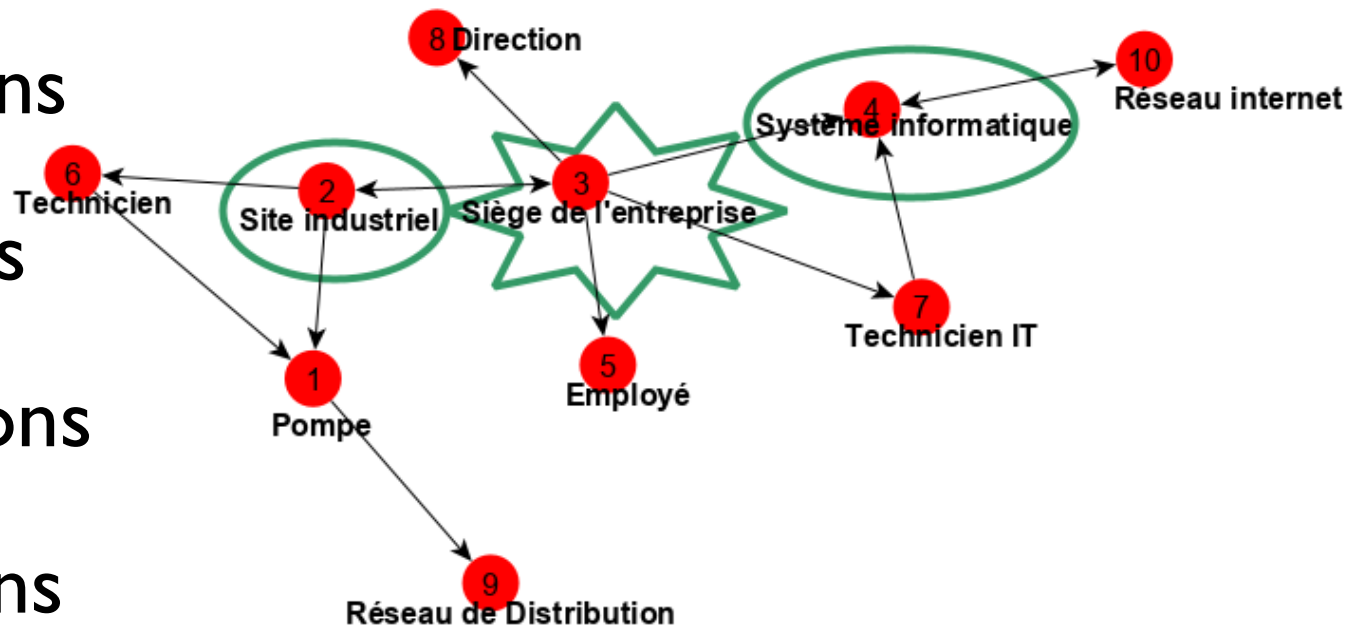
Acteurs



Fonctions

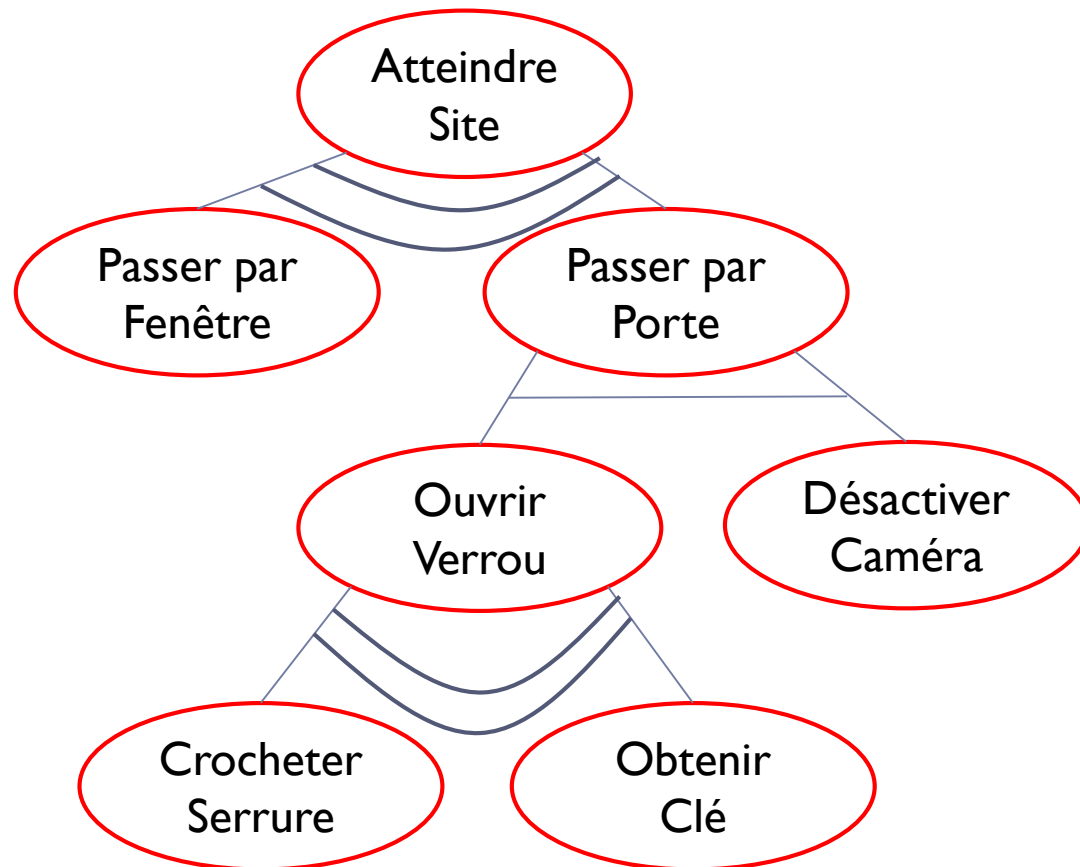
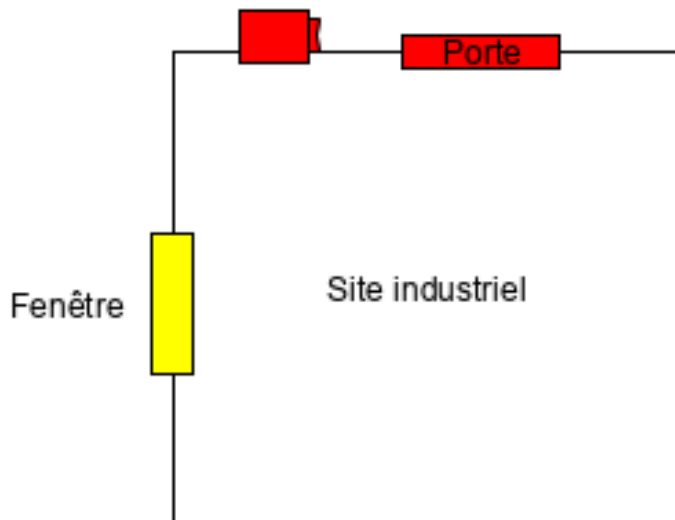


Tensions



[1]

Arbres d'Attaque



[2][3]

Modèle de Dolev-Yao

Modèle formel d'attaquant

Protocole de cryptographie

Cryptographie parfaite

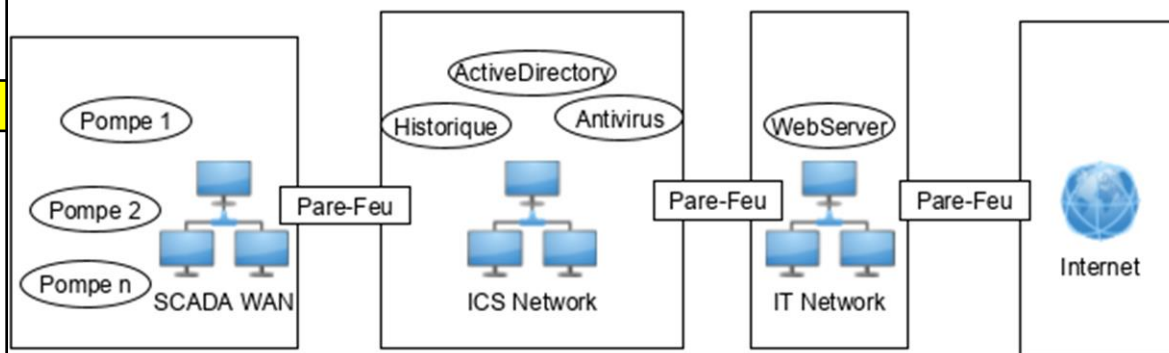
Attaquant omnipotent dans le réseau

Basé sur des règles

[4]

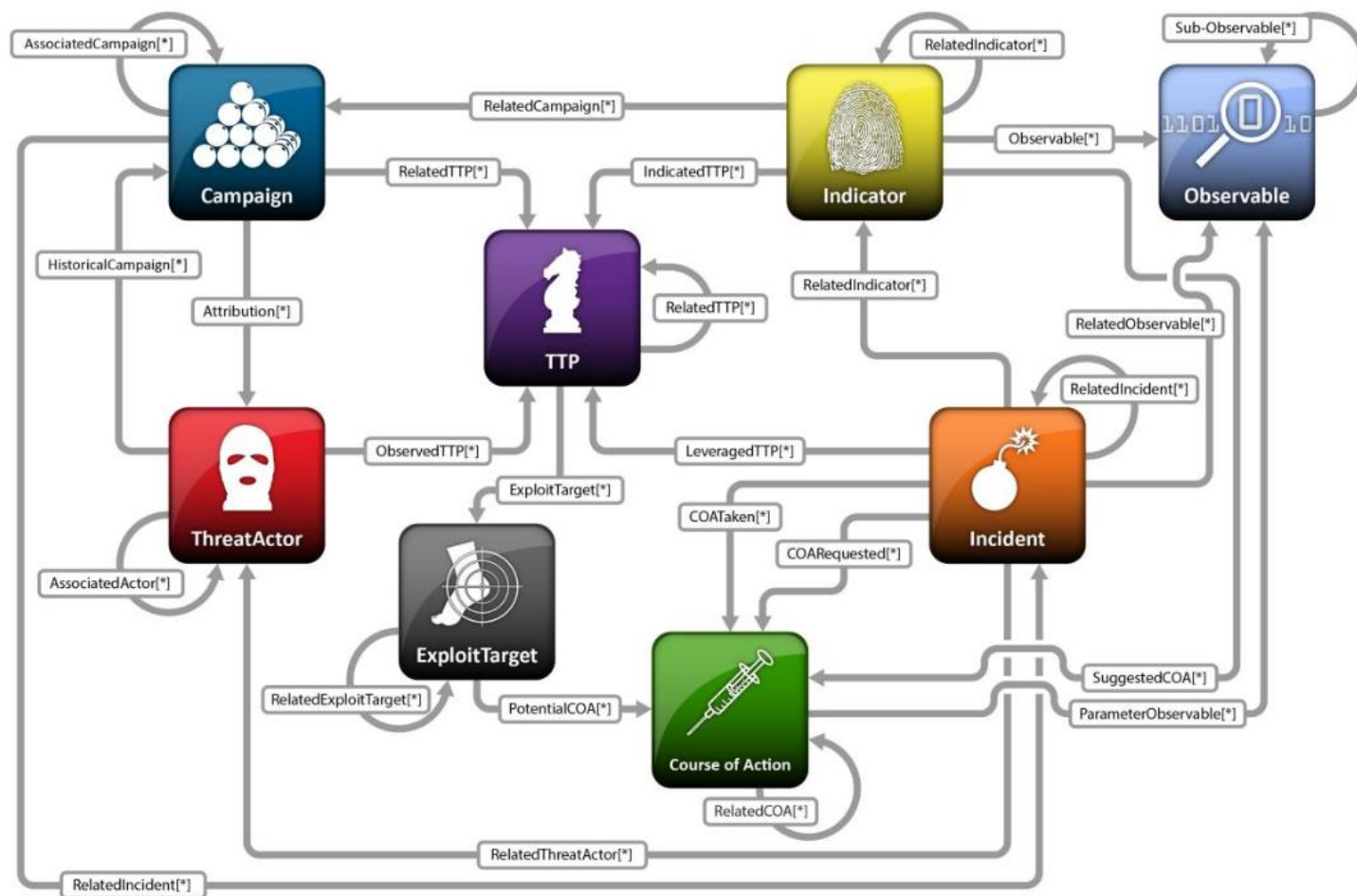
	Attack Name
1	ICS Insider
2	IT Insider
3	Common Ransomware
4	Targeted Ransomware
5	Zero-Day Ransomware
6	Ukrainian Attack
7	Sophisticated Ukrainian Attack
8	Market Manipulation
9	Sophisticated Market Manipulation
10	Cell-Phone WIFI
11	Hijacked Two-Factor
12	Industrial Internet of Things Pivot
13	Malicious Outsourcing
14	Compromised Vendor Website
15	Compromised Remote Site
16	Vendor Back Door
17	Stuxnet
18	Hardware Supply Chain
19	Nation-State Crypto Compromise
20	Sophisticated Credentialed ICS Insider

Exemples étalons



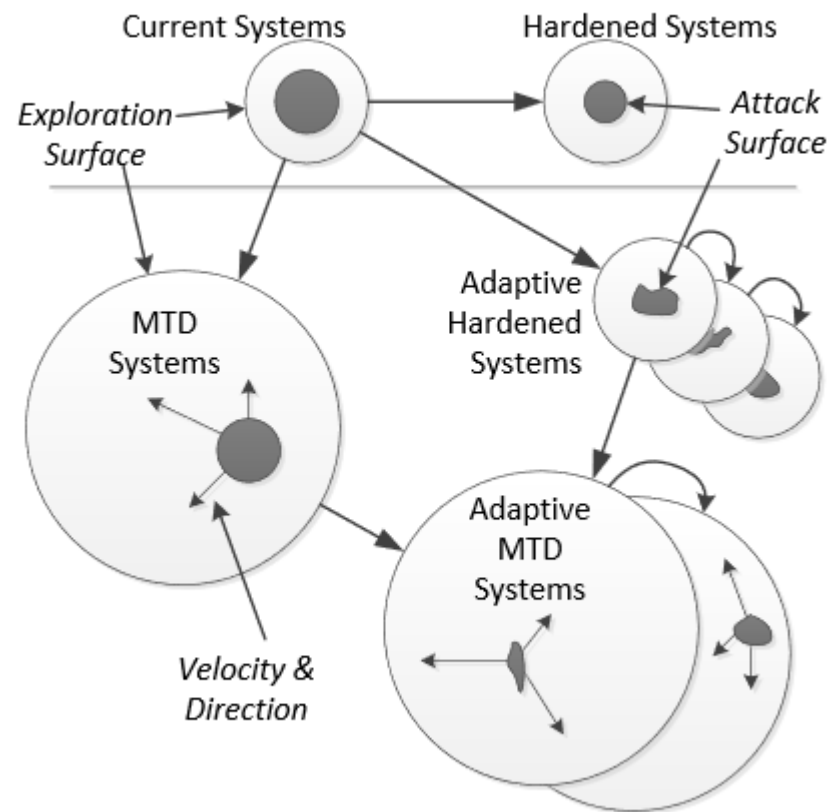
[5]

STIX



[6]

Moving Target Defense



[7]

Enjeux

- **① Raffinement localisé** – Degré de sophistication variable pour se focaliser sur les points d'intérêts. (*"Zoom"*)
- **② Séparation système/attaque** – Modélisation du système dynamique indépendamment de la modélisation d'attaque. (*"Comportement nominal du système"*)
- **③ Réification de la surface d'attaque** – Surface d'attaque explicite pour permettre la modélisation d'attaque. (*"Points d'interaction /d'entrée explicites"*)
- **④ Multi-vues** – Modélisation de point de vue lié à un acteur. (*"Vision, portée & capacités d'interaction restreintes"*)
- **⑤ Support d'exécution** – Modélisation exécutable.
- **⑥ "Opportunisme"** – Modélisation du comportement de l'attaquant.
- **⑦ Hétérogénéité sémantique** – Support de différents langages.

Problématique

- Capturer le système et son fonctionnement nominal.
- Capturer des scénarios d'attaques.
- Comment évaluer la surface d'attaque du système ?

Approche envisagée

- Méthodologie basée sur l'intégration 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)
- Le lien PimCA-TSM-EAM est établi au niveau sémantique à travers la définition formelle des **opérations sur la surface d'attaque**. (opérations exposées par la sémantique TSM)

Avancement

A) Terminologie

B) Contribution

C) Cas d'étude

Terminologie

Surface d'attaque :

Ensemble des **points d'entrée** et des **points de communication** qu'un système possède avec l'extérieur.[8]

Zone de contention entre l'attaquant & la défense.

Terminologie

Attaquant, Threat Actor, Adversaire :

Entité ayant pour objectif de **nuire** au système. [9][10]

Vulnérabilité, Faille :

Erreur ou **faiblesse** de conception, d'implémentation ou de fonctionnement. [9][10]

Terminologie

Menace, Threat :

Adversaire motivé et capable d'**exploiter** une **vulnérabilité**. [9][10]

Attaque, Incident :

Acte malveillant, moyen [séquence d'actions] d'exploiter une vulnérabilité. [9][10]

Terminologie

Cyber Threat Intelligence :

Connaissance sur les **adversaires**, leurs **motivations**, leurs **intentions** et leurs **méthodes**, **collectée**, **analysée** et **partagée** entre différents agents à différents niveaux pour protéger les biens critiques. [11]

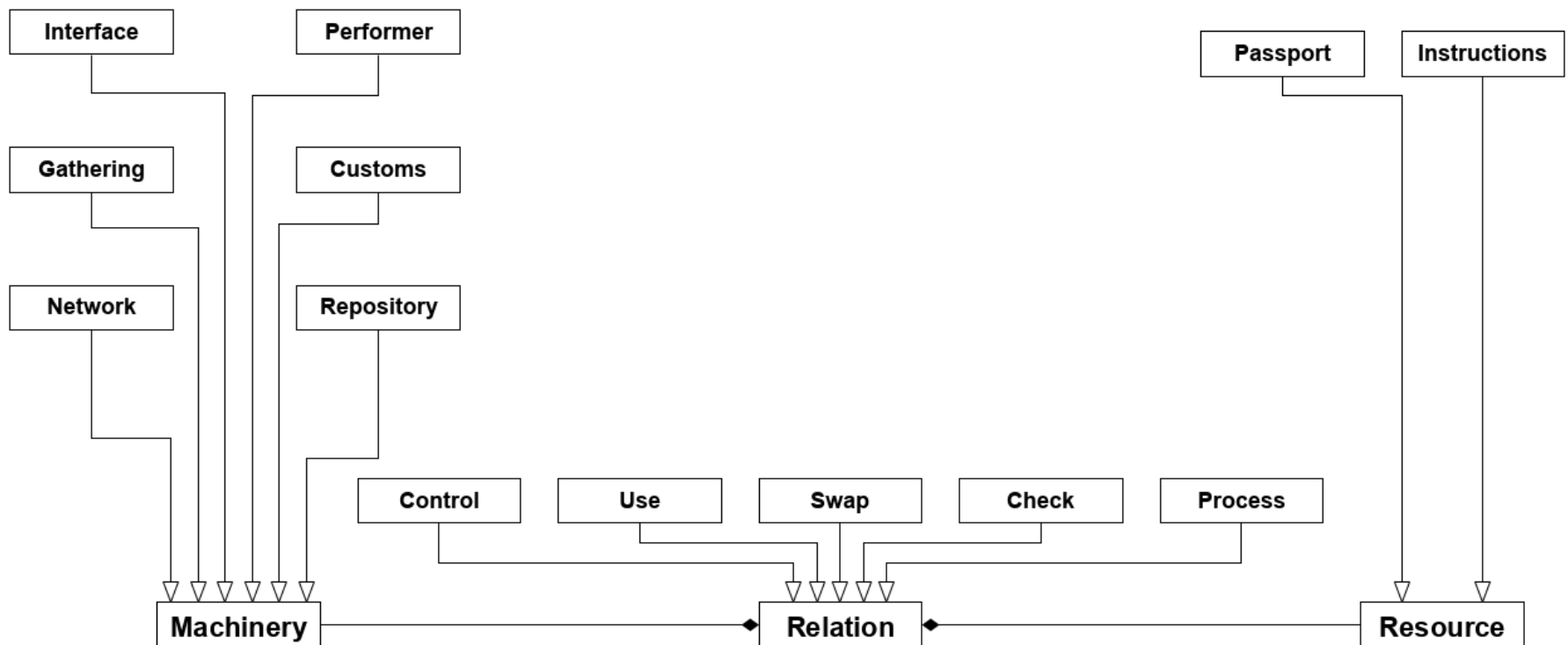
Avancement

A) Terminologie

B) Contribution

C) Cas d'étude

- Architecture statique du système





Machinerie:

- Élément **actif** pourvu d'un **comportement** ⑦
 - **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. ①
 - **Conteneur** := Entité qui contient des ressources. ①



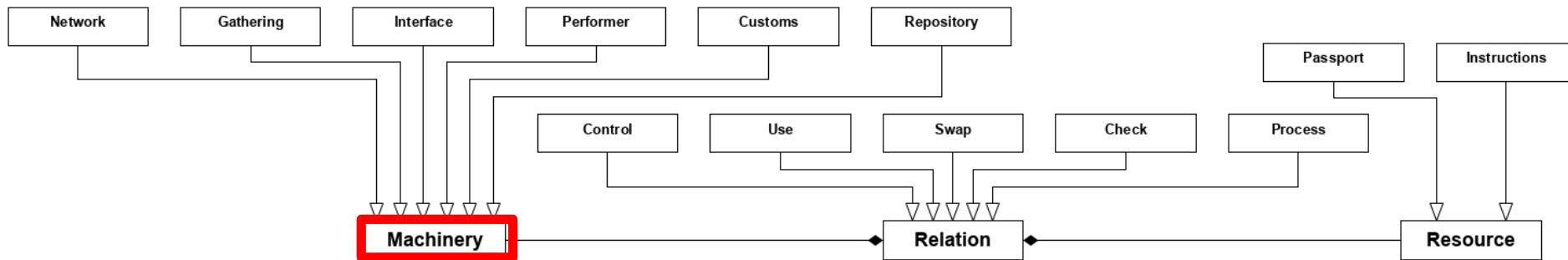
Ressource:

- Élément **passif**
- **Instructions** := Description d'un comportement de machinerie. **7**
- **Passeport** := Ressource dont dépend une douane, nécessaire pour communiquer à travers la douane.

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. Peut être actif ou inactif.

②

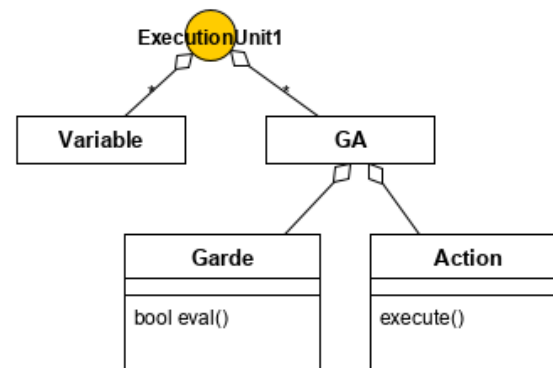
• Machinerie dotée de comportement ⑦



• Choix d'implémentation : Garde/Action

Ensemble de variables

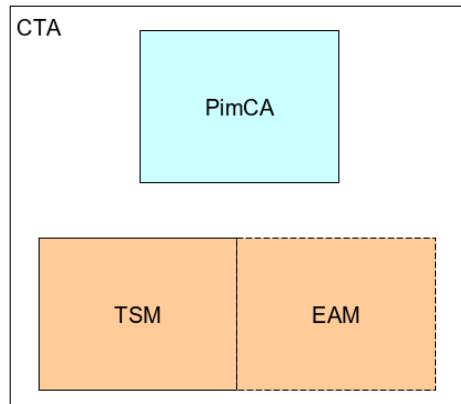
Ensemble de Garde/Action



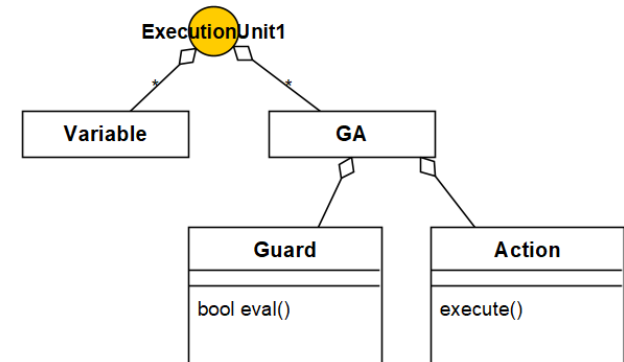
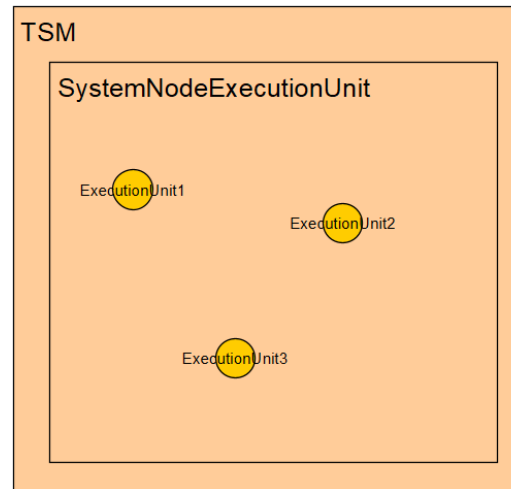
- OpenFlexo



- Guard/Action



- ExecutionUnit



Contribution Executable Attack Modeling

	Attack Name	Steps			
1	ICS Insider				
2	IT Insider				
3	Common Ransomware				
4	Targeted Ransomware				
5	Zero-Day Ransomware				
6	Ukrainian Attack				
7	Sophisticated Ukrainian Attack				
8	Market Manipulation				
9	Sophisticated Market Manipulation				
10	Cell-Phone WIFI				
11	Hijacked Two-Factor				
12	Industrial Internet of Things Pivot				
13	Malicious Outsourcing				
14	Compromised Vendor Website				
15	Compromised Remote Site				
16	Vendor Back Door				
17	Stuxnet				
18	Hardware Supply Chain				
19	Nation-State Crypto Compromise				
20	Sophisticated Credentialed ICS Insider				

③

- Social engineering attack
- Malware injection
- Observation/Understanding/Design/Research
- Privilege elevation
- Pivoting
- Malware execution
- Trace erasure

[5]

Modélisation de systèmes pour la cyber-sécurité:

- Basée sur PimCA ②
- Exécution de scénario pas-à-pas ⑤
- Validée par des cas d'études

Avancement

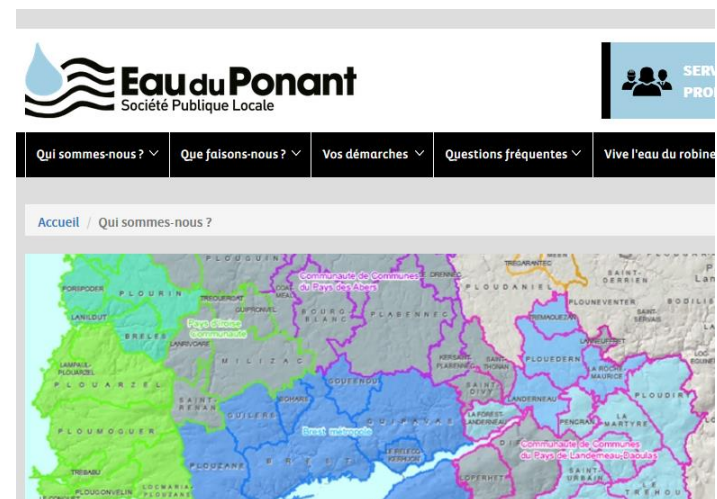
Avancement

A) Terminologie

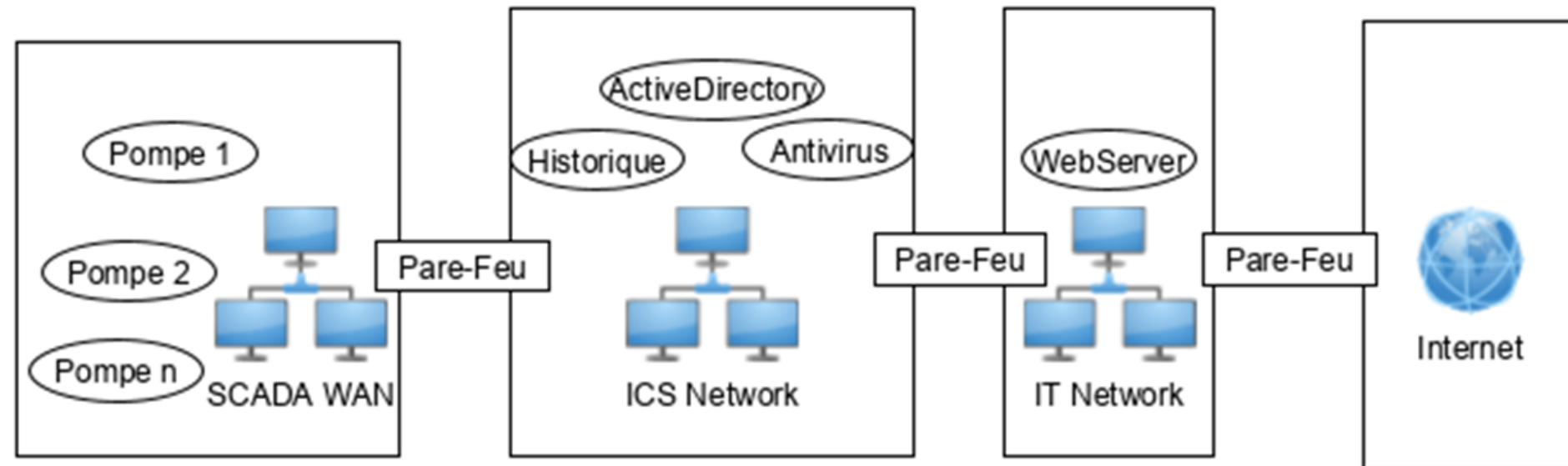
B) Contribution

C) Cas d'étude

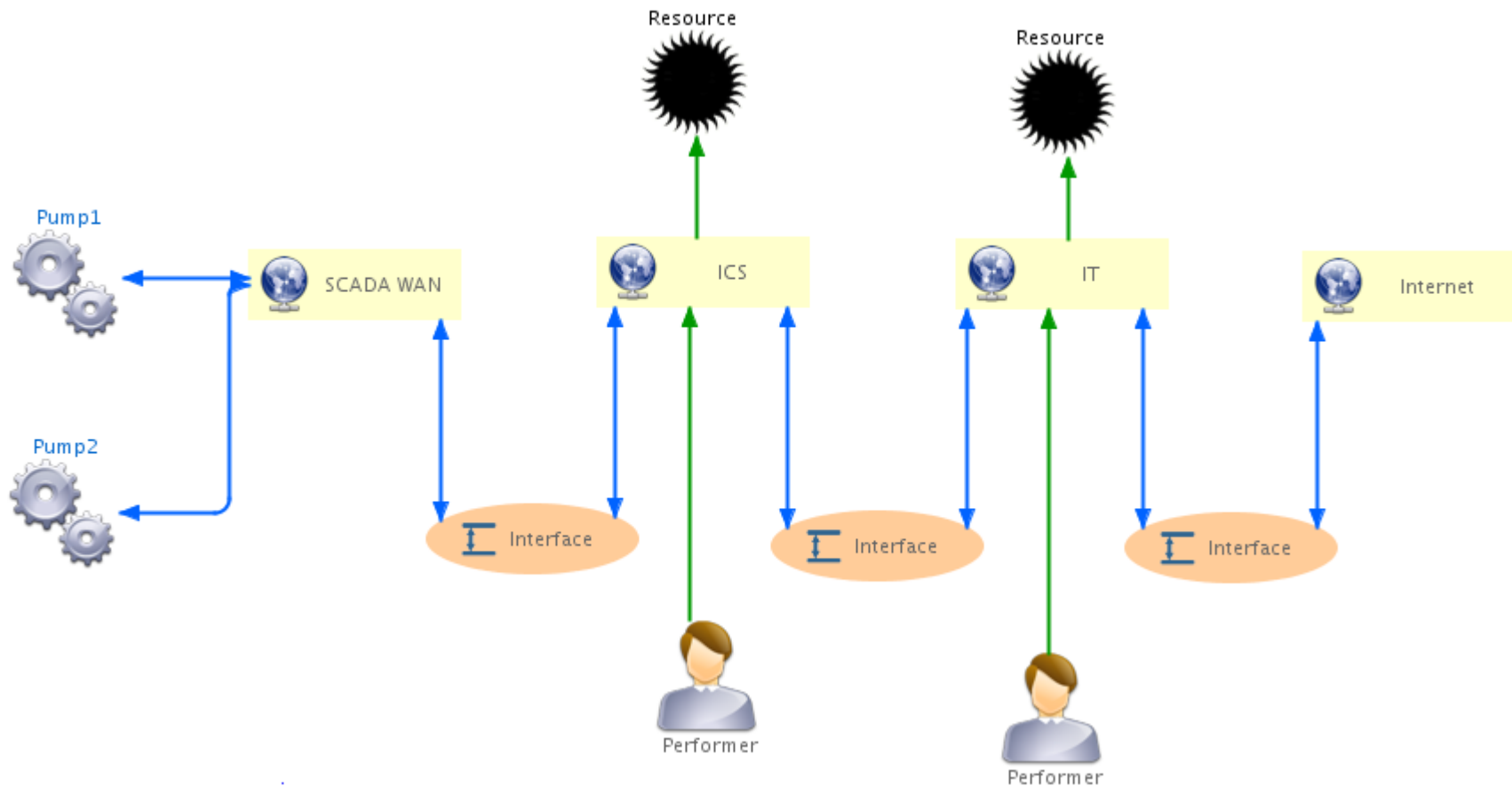
Cas d'étude



Cas d'étude










Cas d'étude



Cas d'étude

Steps	Market Manipulation
1	Exploiting Internet-exposed vulnerable service
2	IT network foothold
3	Remote Access Tool downloaded into the system
4	IT Domain Privilege elevation
5	Pivoting to ICS
6	RAT propagation
7	ICS Observation/Understanding
8	Targeted mis-operation on a single physical piece
9	Trace erasure
10	Sell single physical piece at high price

Steps	Compromised Remote Site
1	Breaking into physical site of unstaffed SCADA WAN node
2	Plugging and hiding laptop into switch
3	Remote controlling of the laptop via WIFI
4	Pivoting into the SCADA WAN
5	Shutdown

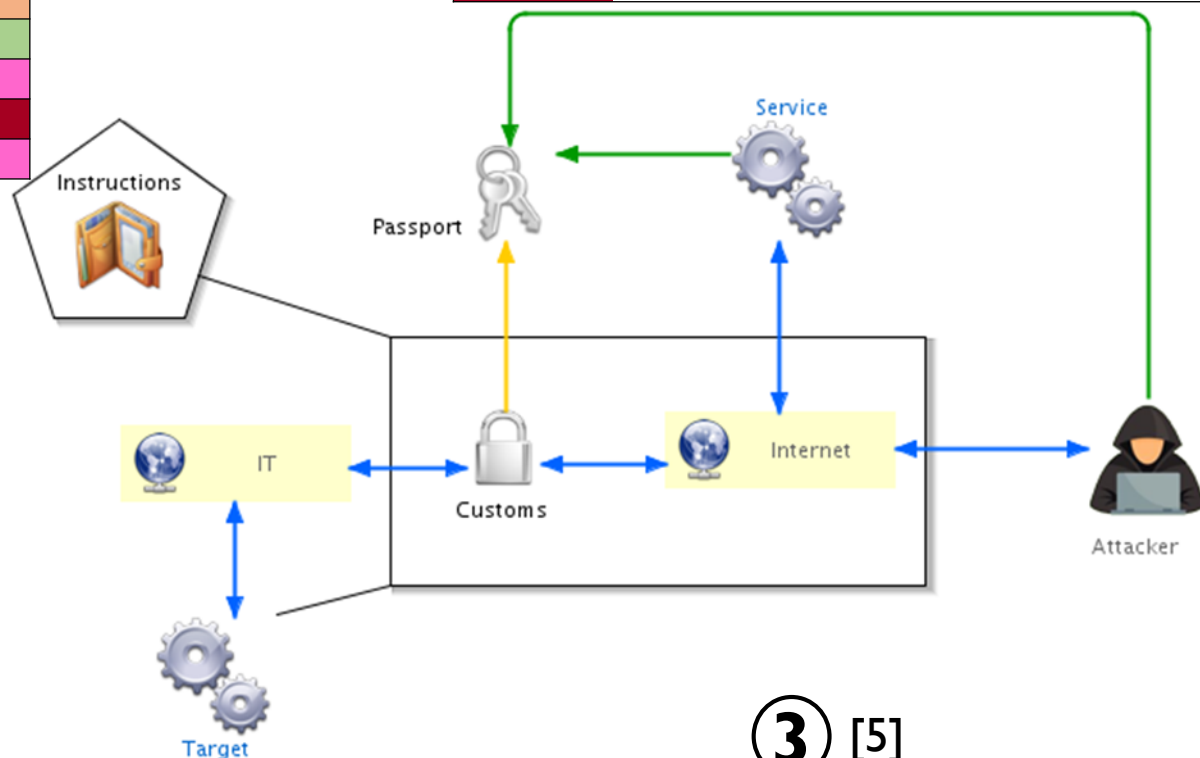
	Social engineering attack
	Malware injection
	Observation/Understanding/Design/Research
	Privilege elevation
	Pivoting
	Malware execution
	Trace erasure

③ [5]

Cas d'étude Market Manipulation

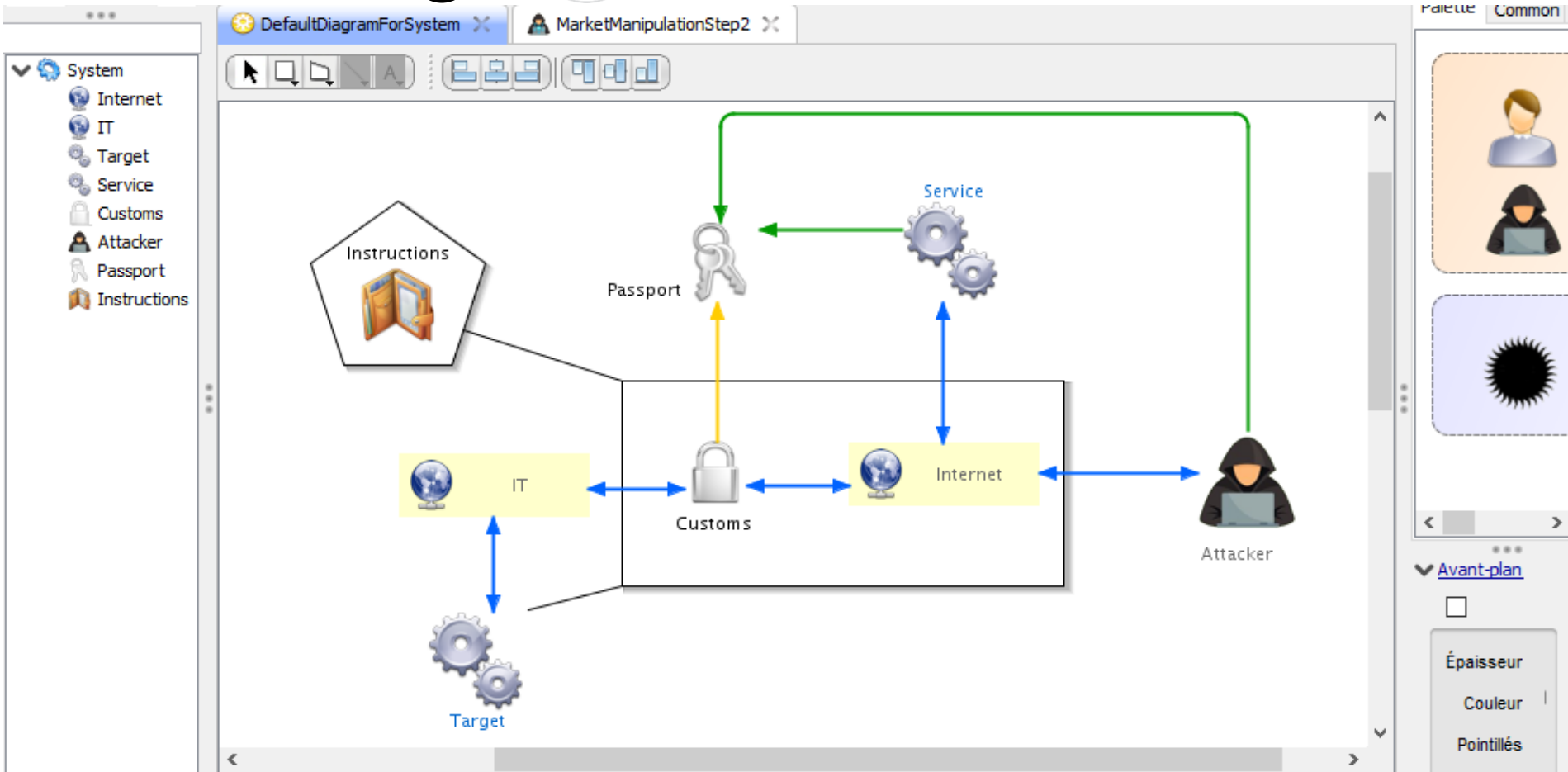
Steps	Market Manipulation
1	Exploiting Internet-exposed vulnerable service
2	IT network foothold
3	Remote Access Tool downloaded into the system
4	IT Domain Privilege elevation
5	Pivoting to ICS
6	RAT propagation
7	ICS Observation/Understanding
8	Targeted mis-operation on a single physical piece
9	Trace erasure
10	Sell single physical piece at high price

	Social engineering attack
	Malware injection
	Observation/Understanding/Design/Research
	Privilege elevation
	Pivoting
	Malware execution
	Trace erasure



③ [5]

Implémentation ⑤




Cas d'étude Market Manipulation

Implémentation ⑤



Internet x Attacker x

 **Attacker**

Variables

Variable	Type
internet	Internet
exploredInternet	Boolean
knownService	Boolean
attackedService	Boolean
password	Boolean
reachedIT	Boolean
exploredIT	Boolean
targetDown	Boolean

Variable:

Cardinalité:

Description:

Garde/actions

Action	Garde
exploreInternet()	(!(exploredInternet))
attackService()	(knownService & !(attackedService))
getPassword()	(attackedService & !(password))
passCustoms()	(password & exploredInternet)
exploreIT()	(reachedIT & !(exploredIT))
attackTarget()	(exploredIT & !(targetDown))
success()	targetDown
init()	(counter = 0)

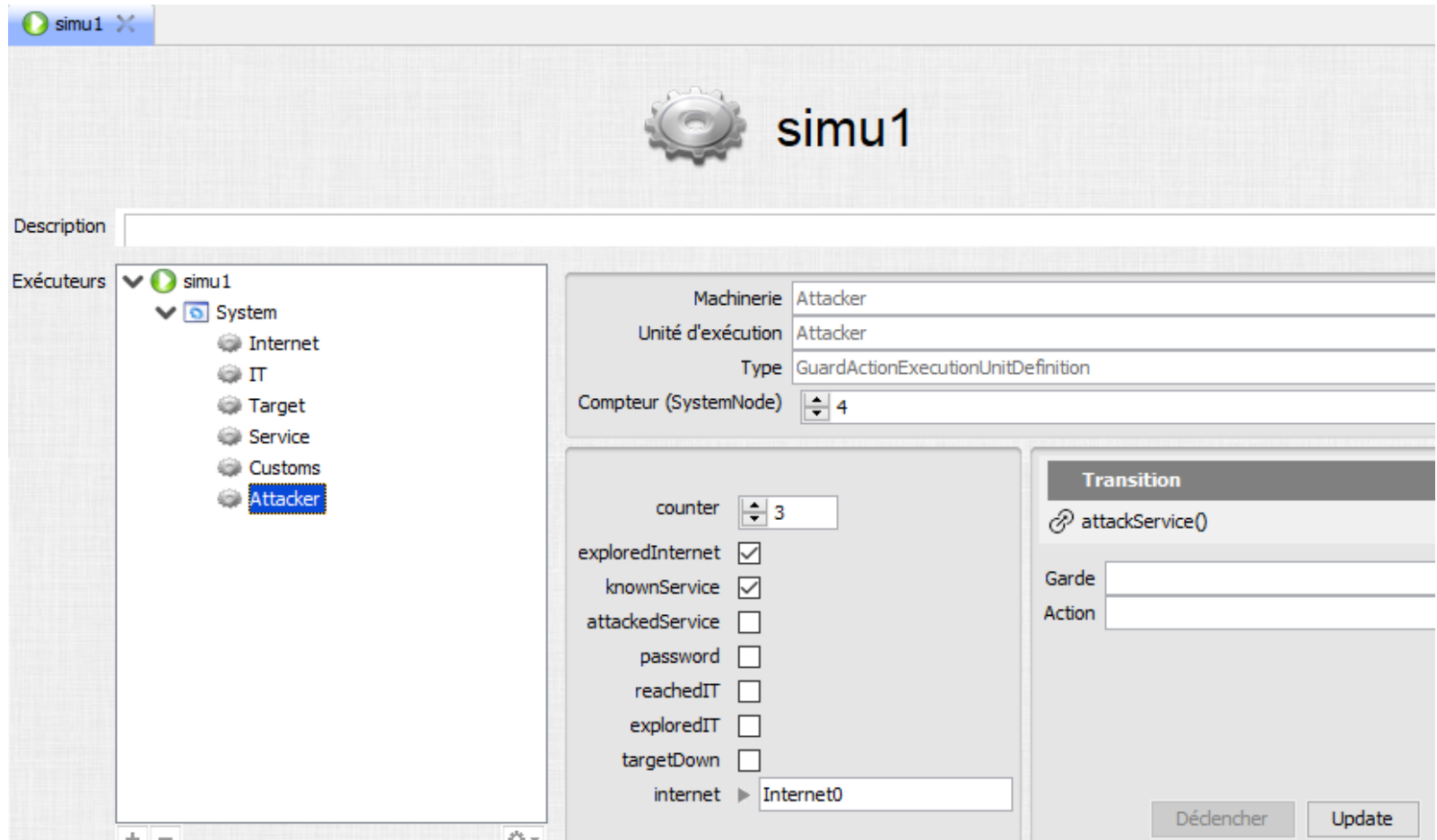
action:

guard:

Description:

exploreInternet()
↔ this.internet.explorationQuery = true

Implémentation ⑤



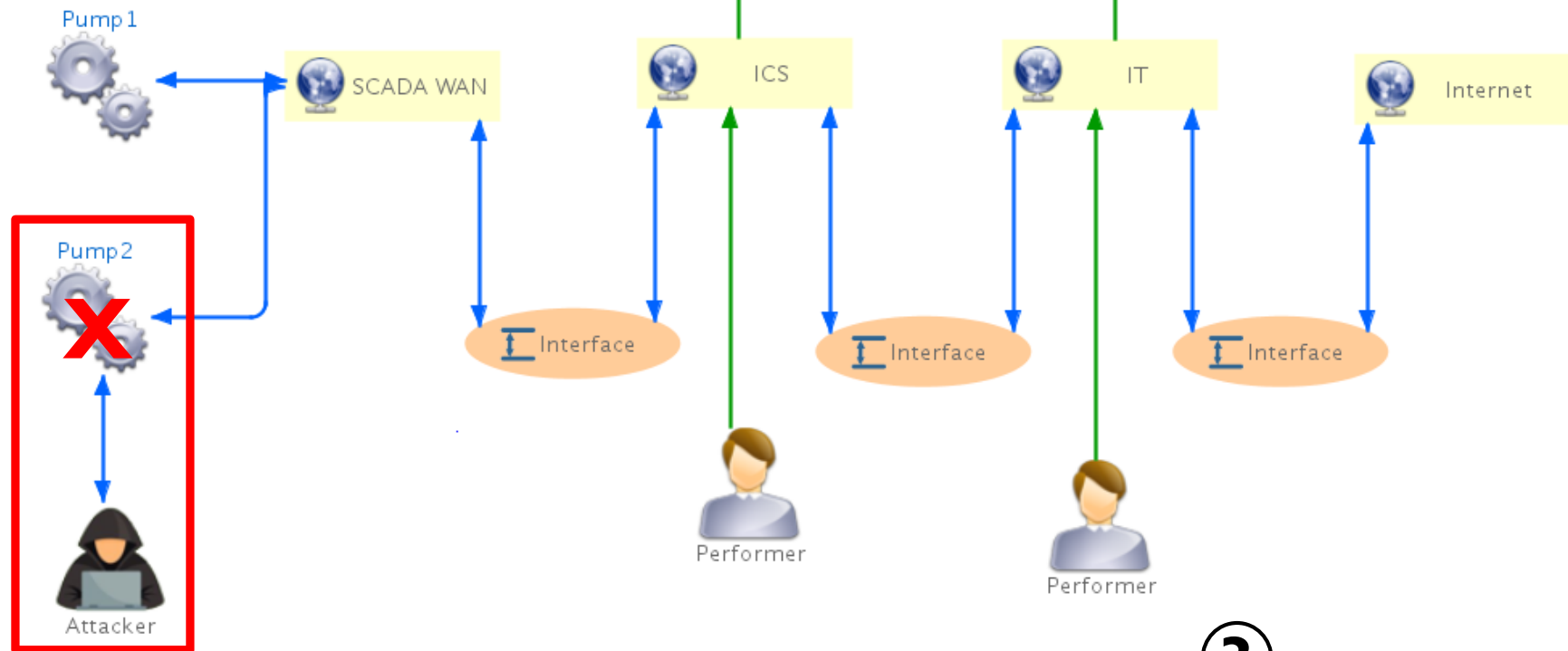
Bilan:

- ③ Réification de la surface d'attaque 😐
- ⑤ Support d'exécution 😊

Cas d'étude

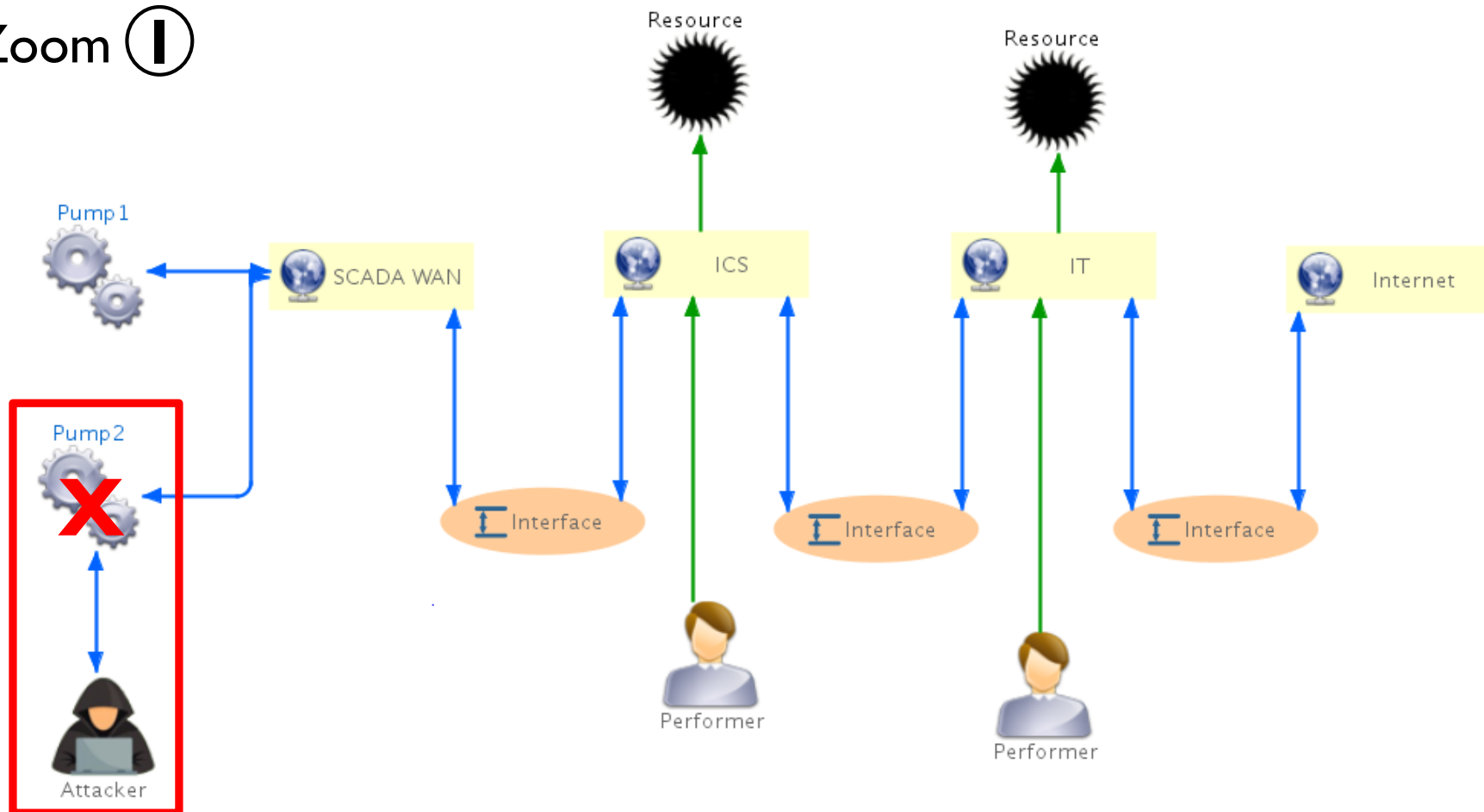
Compromised Remote Site

Steps	Compromised Remote Site
1	Breaking into physical site of unstaffed SCADA WAN node
2	Plugging and hiding laptop into switch
3	Remote controlling the laptop via WIFI
4	Pivoting into the SCADA WAN
5	Shutdown

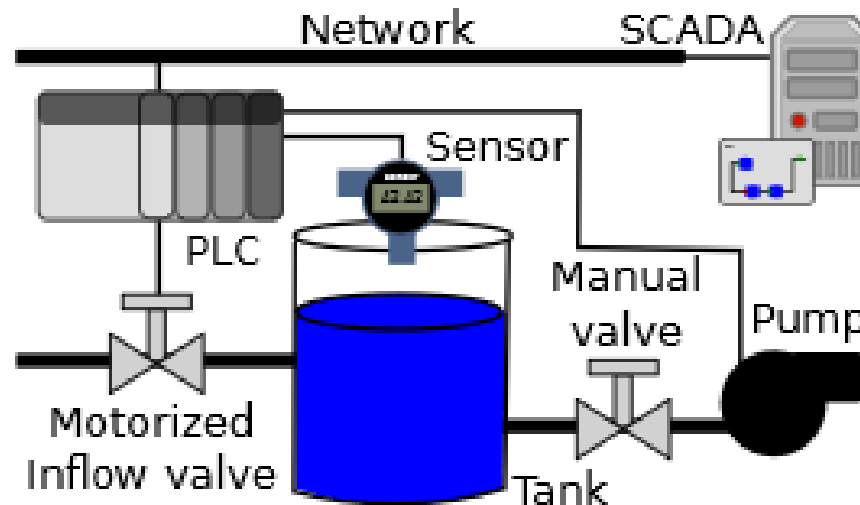


3

Zoom ①



Zoom ①

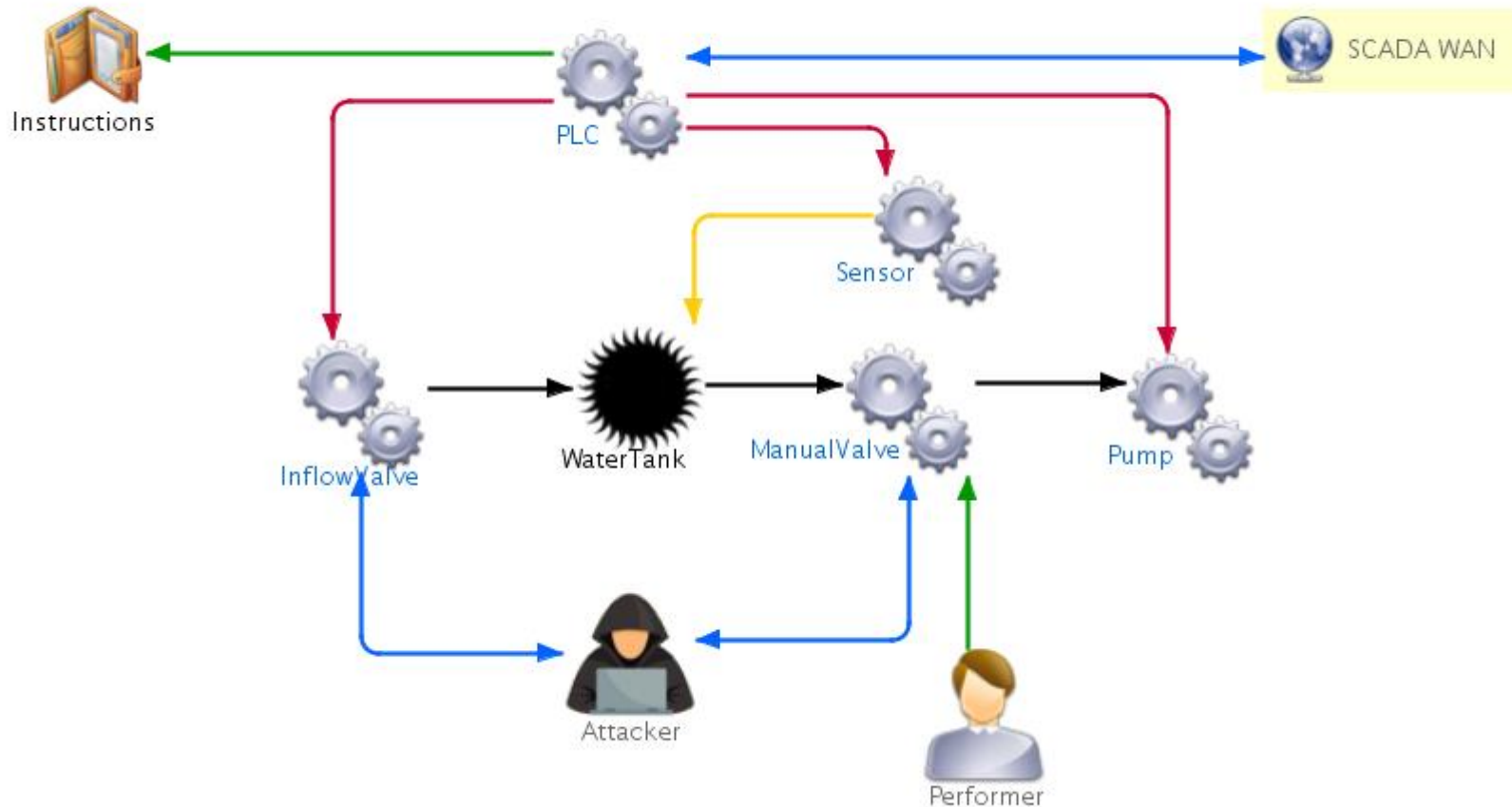


CPDY: Extending the Dolev-Yao Attacker with Physical-Layer Interactions, Marco Rocchetto & Nils Ole Tippenhauer, 2016

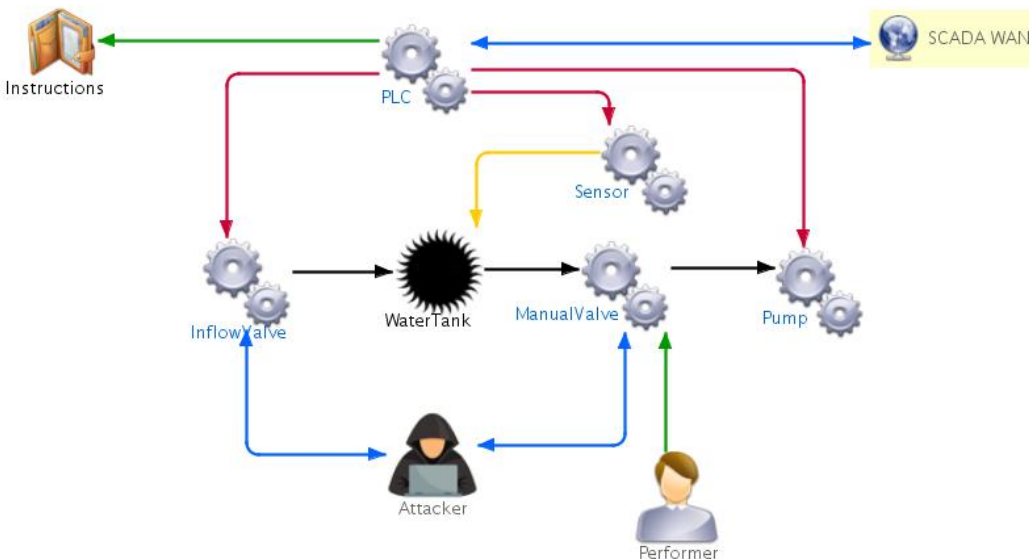
<https://arxiv.org/pdf/1607.02562.pdf>

[12]

Zoom ①



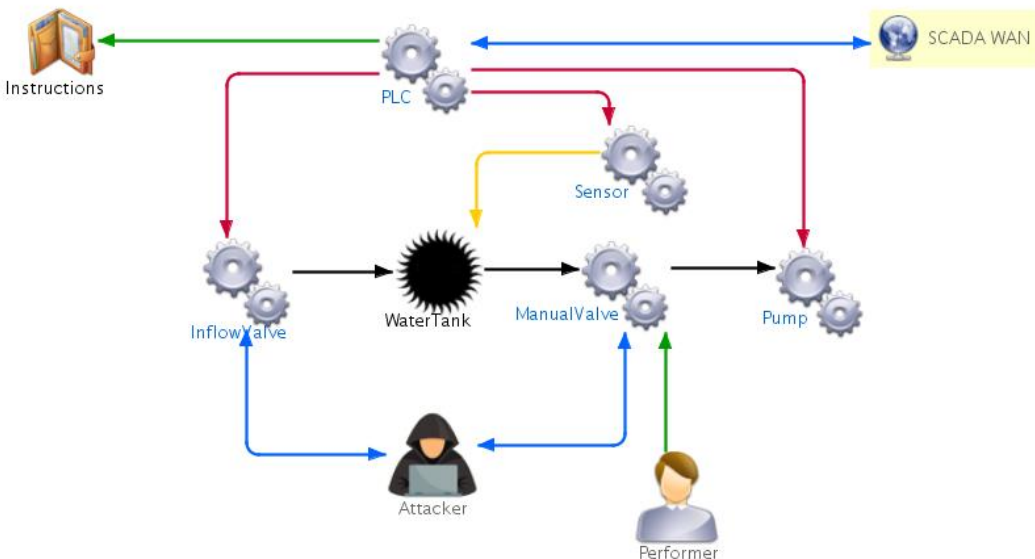
2



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.

[12]

2

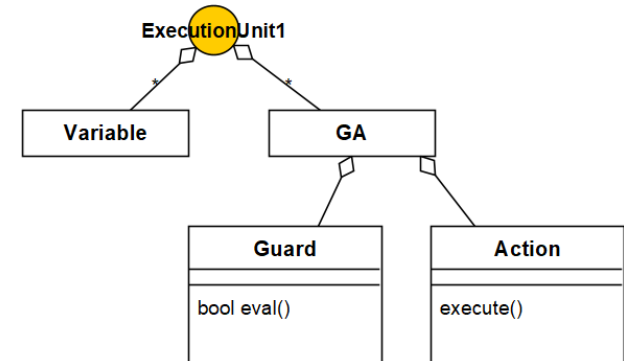
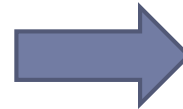
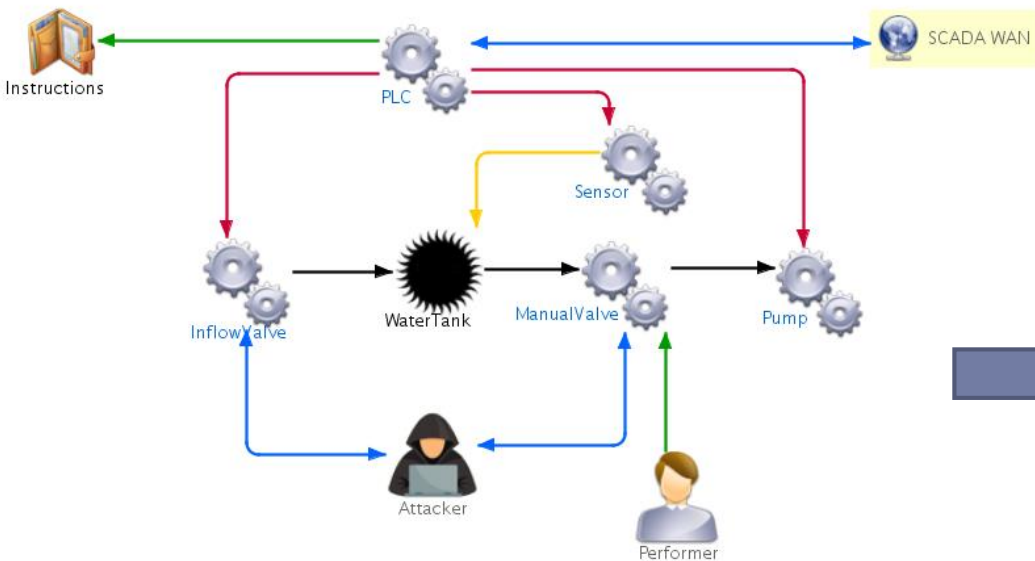


Exemple de scénario d'attaque:

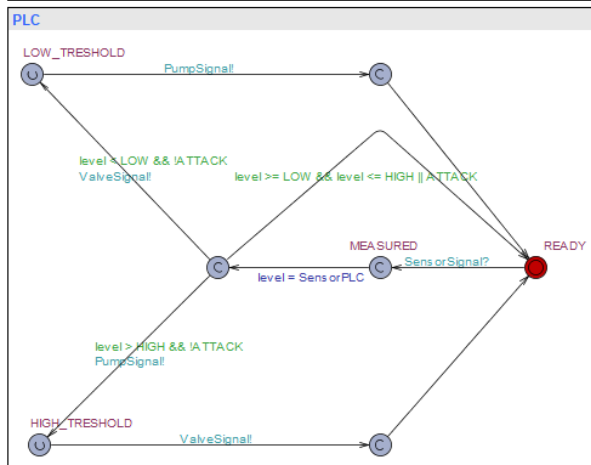
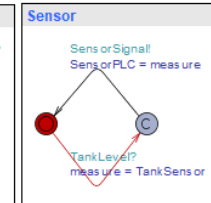
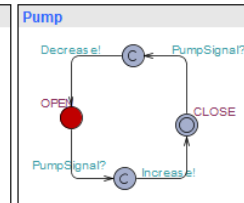
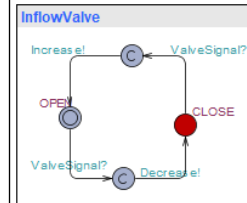
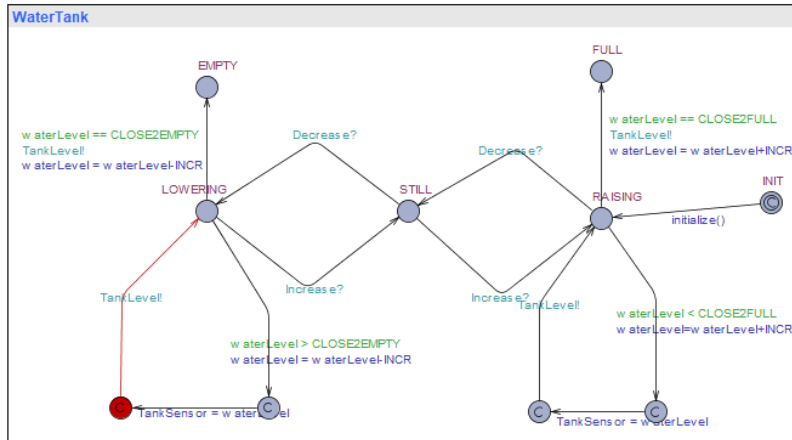
1. L'attaquant ferme manuellement la valve de sortie.
2. L'attaquant force la valve d'entrée ouverte.
3. L'attaquant cause un débordement du réservoir.

[12]

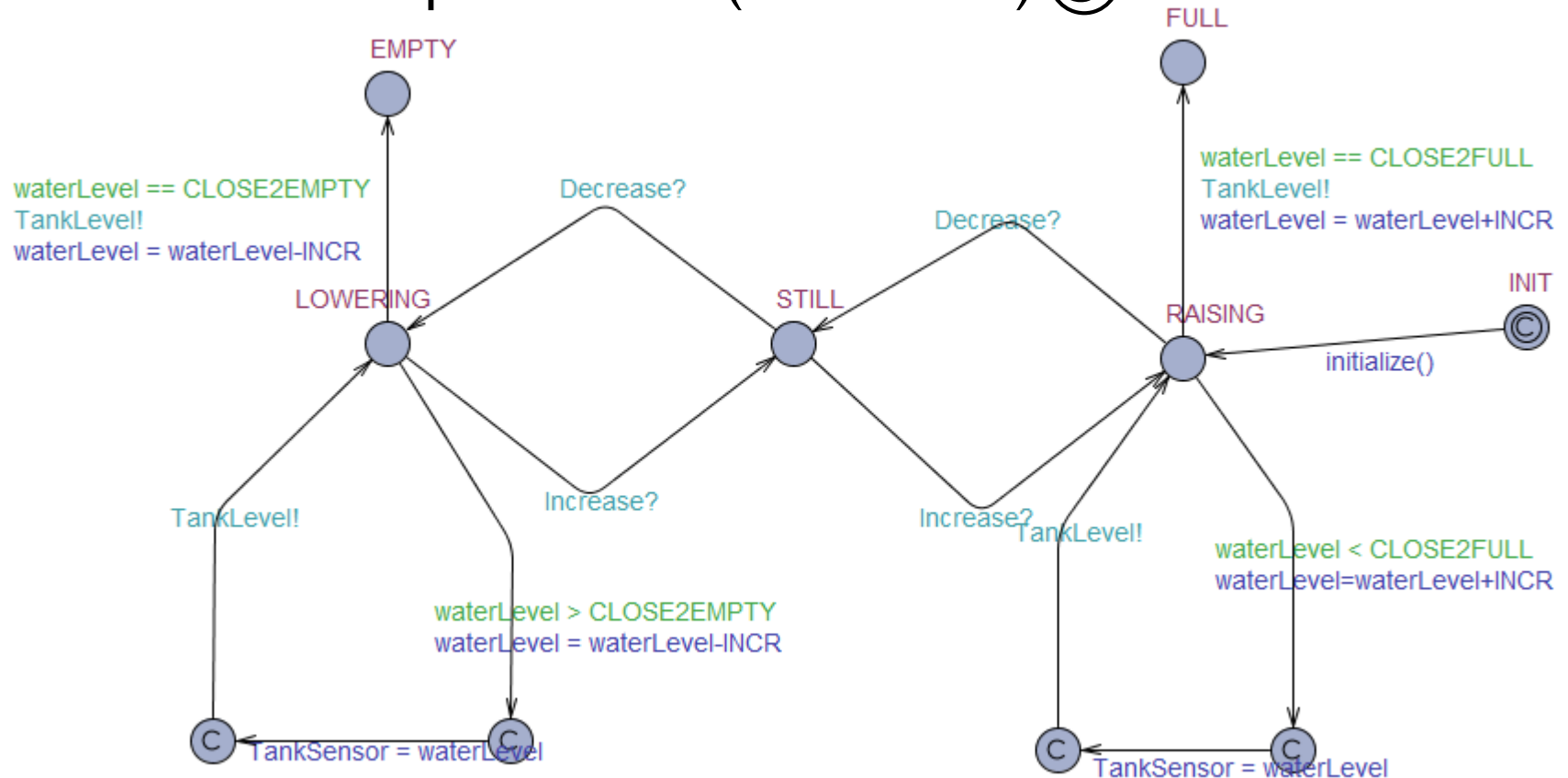
Exécution : étude préliminaire ⑤



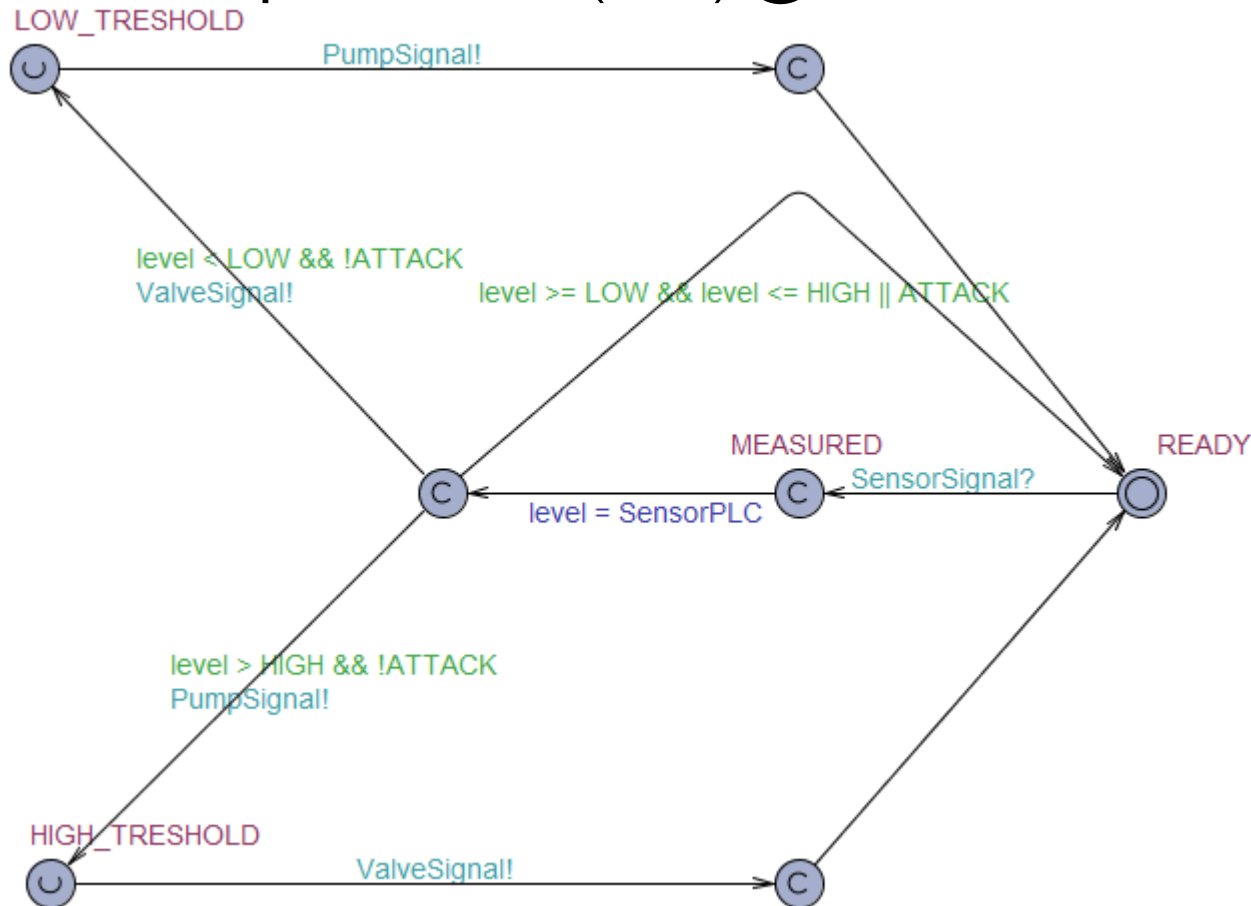
Exécution : étude préliminaire ⑤







Exécution : étude préliminaire (Water Tank) ⑤



Exécution : étude préliminaire (PLC) ⑤



Bilan:

- ① Raffinement localisé 
- ② Séparation système/attaque 
- ③ Réification de la surface d'attaque 
- ⑤ Support d'exécution 

Conclusion

Approche

- PimCA
- Target System Modeling
- Executable Attack Modeling
- **Cyber Threat Application**

Structure

Comportement nominal








Scénarios d'attaque

Éléments stabilisés...

- Méta-modèle TSM
- Outillage OpenFlexo
- Traitement de cas d'étude
- Exécution
- Raffinement localisé

...et à préciser

- PimCA
- EAM

- ① Raffinement localisé 
- ② Séparation système/attaque 
- ③ Réification de la surface d'attaque 
- ④ Connaissance partielle 
- ⑤ Support d'exécution 
- ⑥ Opportunisme 
- ⑦ Hétérogénéité sémantique 

Rentrée des doctorants MathSTIC (2018 & 2019)

4 Soutenances de thèse (Théotime Bollengier, Fadi Obeid, Cyrielle Feron, Luka Le Roux)

Séminaire poster de l'équipe MOCS

Journée des doctorants de 1^{ère} année du Lab-Sticc

Journée Méthodes Formelles pour la Sécurité

MOOC Défis et enjeux de la cybersécurité

Formation LaTeX par la pratique par Vincent LE GARREC

Formation Gestion du trac dans le cadre de la prise de parole en public

Encadrement de TD Base de données (x2)

Encadrement de Projet Informatique Python (x2)

- PimCA à MODELSWARD 2020
(Soumission Octobre 2019)
- Validation de l'ensemble du premier cas d'étude
- Réification de la surface d'attaque③

- Rédaction d'un second article sur l'approche globale
- Traitement d'autres cas d'étude
- Enjeux restants ④⑥⑦
- Rédaction du manuscrit

Merci de votre attention

Bibliographie

- [1] *Redefining the Center of Gravity in Joint Force Quarterly (JFQ) issue 59* / Dale C. Eikmeier / Washington D.C. USA / 2010
- [2] *Attack Modeling for Information Security and Survivability* / Andrew P. Moore, Robert J. Ellison, Richard C. Linger/ Software Engineering Institute, Carnegie Mellon University, USA / Mars 2001
- [3] *Is my attack tree correct?* / Maxime Audinot, Sophie Pinchinat, & Barbara Kordy / IRISA Rennes, University Rennes 1, INSA Rennes, France / Août 2017
- [4] *On the Security of Public Key Protocols* / Danny Dolev & Andrew C. Yao / IEEE Transactions on Information Theory / Mars 1983
- [5] *The Top 20 Cyberattacks on Industrial Control Systems* / Andrew Ginter / VP Industrial Security Waterfall Security Solutions / 2017
- [6] *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX)* / Sean Barnum / The MITRE Corporation / 20 Février 2014

Bibliographie

- [7] *Towards a Theory of Moving Target Defense* / Rui Zhuang, Scott A. DeLoach, Xinming Ou / Kansas State University, Manhattan, USA / 2014
- [8] *Analyse et réduction de la surface d'attaque* / Mickael Dorigny / <https://www.information-security.fr/> / 19 Décembre 2015
- [9] *Towards Threat, Attack, and Vulnerability Taxonomies* / Dennis Hollingworth / Network Associates laboratories USA / 2003
- [10] *Trust in Cyberspace* / Fred B. Schneider / Committee on Information Systems Trustworthiness, Washington, D.C. USA / 1999
- [11] *Definitive Guide to Cyber Threat Intelligence* / Jon Friedman, Mark Bouchard, CISSP / CyberEdge Group Annapolis, USA / 2015
- [12] *CPDY: Extending the Dolev-Yao Attacker with Physical-Layer Interactions* / Marco Rocchetto & Nils Ole Tippenhauer / Université du Luxembourg, Université de Singapour / <https://arxiv.org/pdf/1607.02562.pdf> / 2016