

Workshop
27/08/2019

Tithnara Nicolas SUN

Philippe Dhaussy (Lab-STICC)
Lionel Van Aertryck (DGA-MI)

Ciprian Teodorov (Lab-STICC)

Table of contents

- Introduction
 - Contexte
 - Problématique
 - Approche
- Cyber Threat Application (CTA)
- Conclusion

- Cyber-sécurité des systèmes de controle industriel
- Système de controle industriel
 - Interfaces cyber-physiques
 - Fonctionnement dynamique
 - Nombreux langages de specification
 - Nombreuses plateforme d'exécution
- Modélisation d'attaque
 - Attack trees, DAGs, graphs
 - Soit très haut-niveau -> découplé du domaine technique
 - Soit très bas-niveau -> proche du domaine technique

- Comment capturer le système et son fonctionnement nominal tout en le composant avec des scénarios d'attaque ?
- Comment décorrélérer l'architecture du système de la modélisation d'attaque?
- Comment modéliser la surface d'attaque du système?
- Comment gérer l'hétérogénéité du système ?

- **1. Opportunisme** – Degré de sophistication variable pour se focaliser sur les points d'intérêts. (*"Zoom"*)
- **2. Séparation système/attaque** – Modélisation du système 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. Connaissance partielle** – Modélisation de point de vue lié à un acteur. (*"Vision, portée & capacités d'interaction restreintes"*)
- **5. Support d'exécution** – Modélisation exécutable.
- **6. Hétérogénéité sémantique** – Support de différents langages

- Methodology based on the integration of two correlated processes :
 - Target system modeling process – TSM - (captures the « situation »)
 - Executable attack modeling process – EAM
- The TSM process enables capturing the semantics of the system
- The EAM process focuses on the specification of attack scenarios
- The TSM and EAM link is established at the semantic level through the formal definition of **attack surface operations** (operations exposed from the TSM semantics).

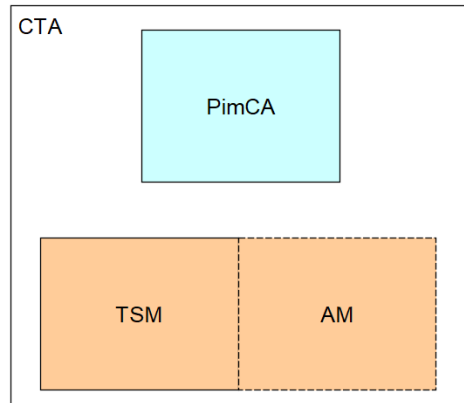
1. Target System Modeling Language [\[30/06/19\]](#)
2. Attack surface operations [\[1/09/19\]](#)
3. Attack modeling language [\[15/09/19\]](#)
4. OBP2 adapter, or hand-made simulator [\[30/09/19\]](#)
5. Case-study I - [\[30/10/19\]](#)

	Mai	Juin	Juillet	Aout	Septembre	Octobre
Target System Modeling (TSM) Language						
Attack Surface operations						
Attack Modeling Language (AML)						
OBP2 adapter						
Case-study I						

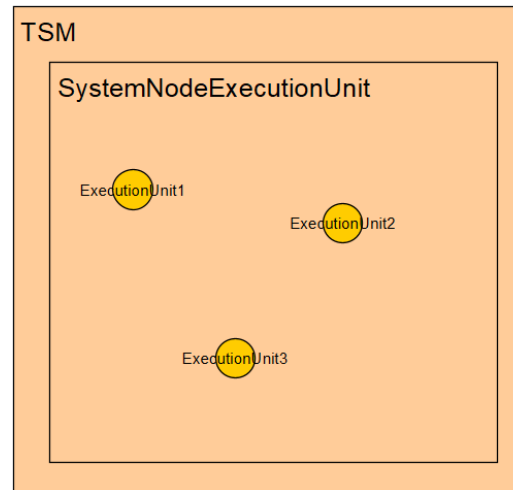
System modeling for cybersecurity purposes:

- Based on PimCA [2]
- Step-by-step attack scenario execution [2][5]
- Along with cases study

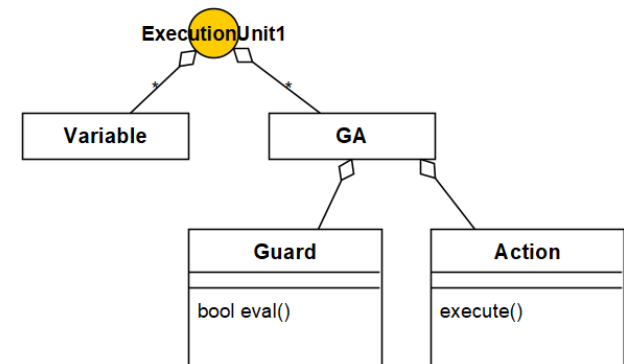
- OpenFlexo










- ExecutionUnit



- Guard/Action






Icône-Concept	Description
 Machinery	Machinerie : système manipulant des Ressources (regroupement particulier) : voiture, animal, PC, processus
 Performer	Exécutant (spécialise Machinerie) : ce qui transforme la Ressource, e.g. UC/Programme, cerveau, régulateur.
 Network	Réseau (spécialise Machinerie) : zone d'échange de matière, d'information, d'énergie, etc. : câblage, tuyauterie, IPC Engine.
 Customs	Douane (spécialise Machinerie) : fonctionnalité particulière mise en place par une Machinerie pour identifier & autoriser une autre Machinerie : cadenas, garde, login, crypto
 Interface	Interface (spécialise Machinerie) : permet de passer d'une Machinerie à une autre, du monde physique au monde virtuel et inversement : NIC, caméra, clavier, écran.
 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. exécutant, configuration, mémoire.
 Repository	Entrepôt : zone de stockage de Ressource : armoire, bâtiment, disquette, database, file system



Machinerie:

- Élément **actif** pourvu d'un **comportement** [6]
- **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 separation du monde physique au monde cyber ou inversement.
- **Regroupement** := Ensemble de machineries.
- **Conteneur** := Entité qui contient des ressources.

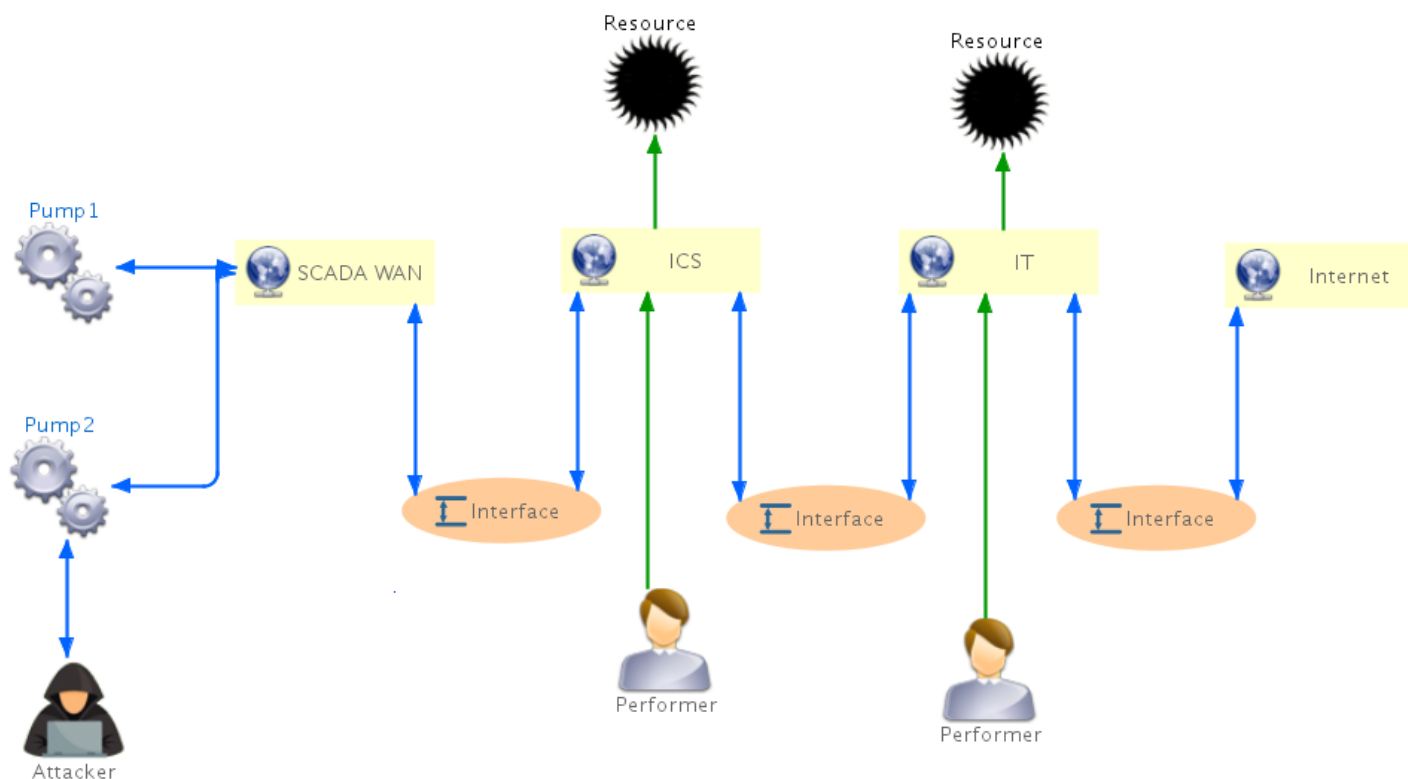
Icône-Concept	Description
 Resource	Ressource : ce qui est transformé, manipulé par une Machinerie : matière, électricité, document, log, data
 Instructions	Consigne (spécialise Ressource) : La direction, les paramètres que l'exécutant suit : Fichier de configuration, ordre, politique de sécurité
 Passeport	Passeport (spécialise Ressource) : élément à fournir à la Douane pour être identifié / autorisé : clef, carte d'identité, badge, login/password, clef de chiffrement

Ressource:

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

Name	Nom	Sens	Description
Swap	Echange	Bidirectionnel	Lien de communication générique entre deux entités, existence de variables partagées
Check	Vérification	Unidirectionnel	Lien de droit en lecture, existence de variables observables chez la cible.
Control	Contrôle	Unidirectionnel	Lien de droit en écriture, existence de variables observables et de comportements déclenchables chez la cible. Présuppose le lien de vérification.
Use	Utilisation	Unidirectionnel	Lien de droit en écriture limité, existence de certain comportement déclenchable chez la cible.
Produce	Production	Unidirectionnel	Lien de flux de matière/données. Implique un process de fonctionnement nominal.
Maintain	Maintenance	Unidirectionnel	???

The Top 20 Cyber Attacks Against Industrial Control Systems, <https://static.waterfall-security.com/Top-20-ICS-Attacks.pdf>










The Top 20 Cyber Attacks Against Industrial Control Systems, <https://static.waterfall-security.com/Top-20-ICS-Attacks.pdf>

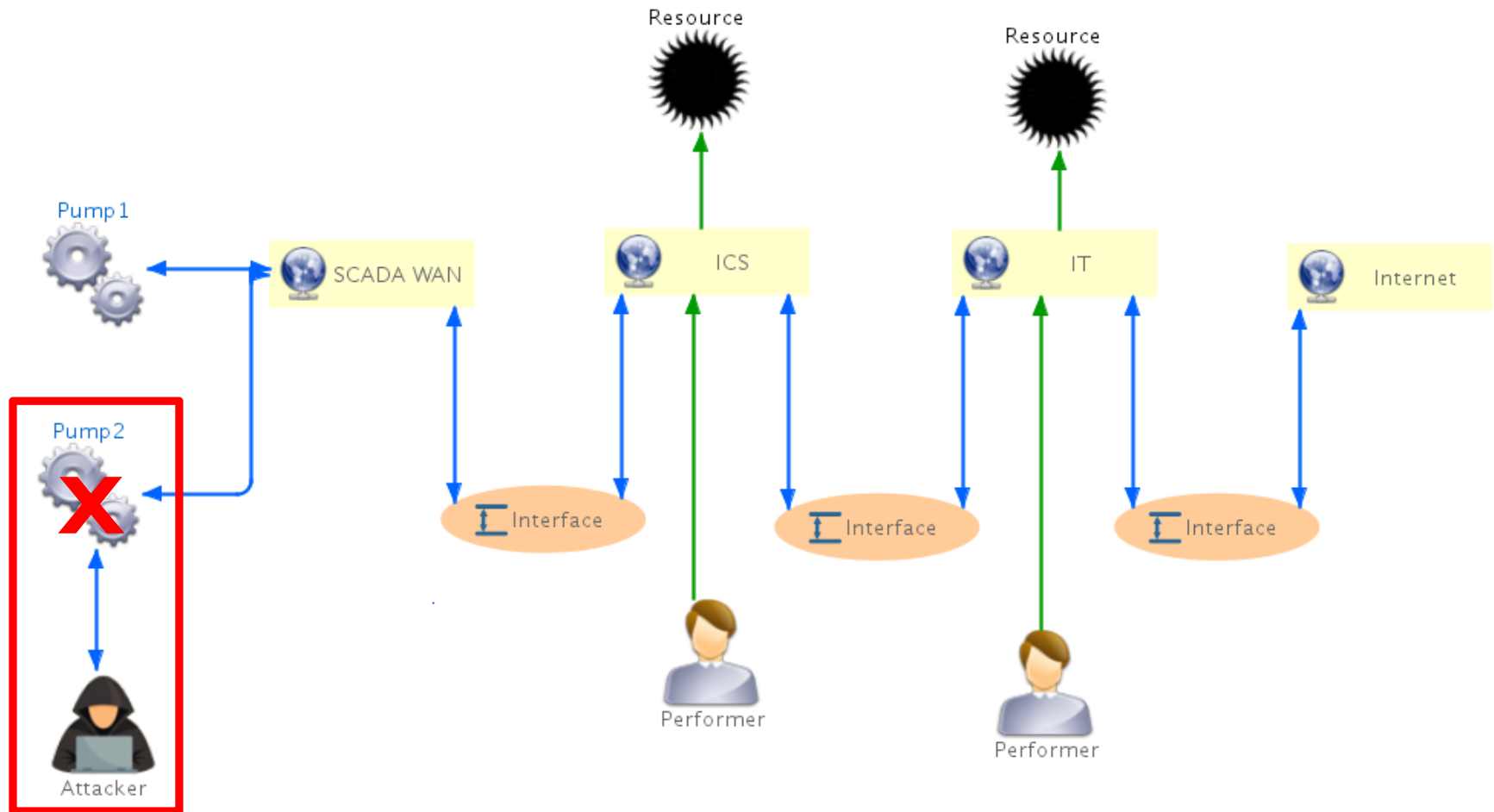
	Attack Name	Steps		
1	ICS Insider			
2	IT Insider			
3	Common Ransomware			
4	Targeted Ransomware			
5	Zero-Day Ransomware			
6	Ukrainian Attack			
7	Sophisticated Ukrainian Attack			
8	Market Manipulation			
9	Sophisticated Market Manipulation			
10	Cell-Phone WIFI			
11	Hijacked Two-Factor			
12	Industrial 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			

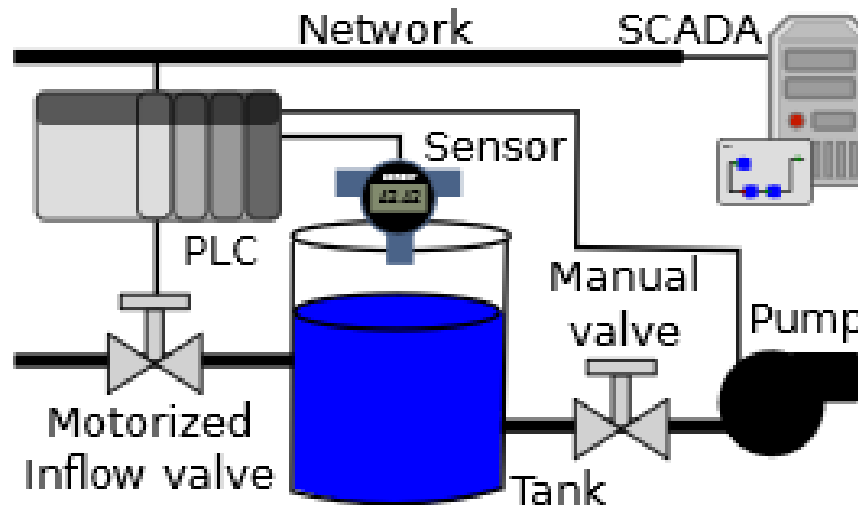
- Première approche (à raffiner/faire évoluer)
- Chaque type implique des guards/actions différentes

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

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

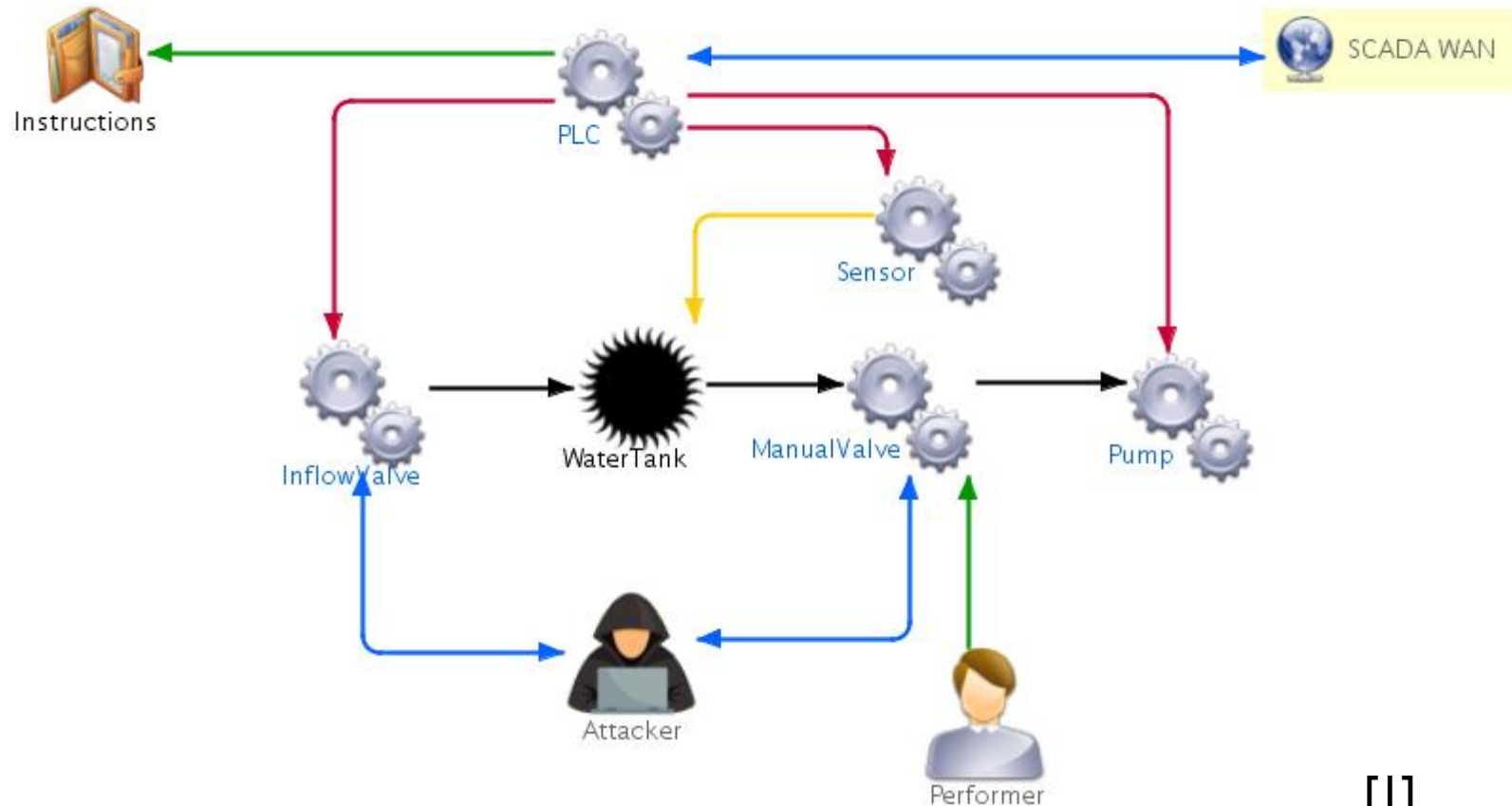
	Social engineering attack
	Malware injection
	Observation/Understanding/Design /Research
	Privilege elevation
	Pivoting
	Malware execution
	Trace erasure

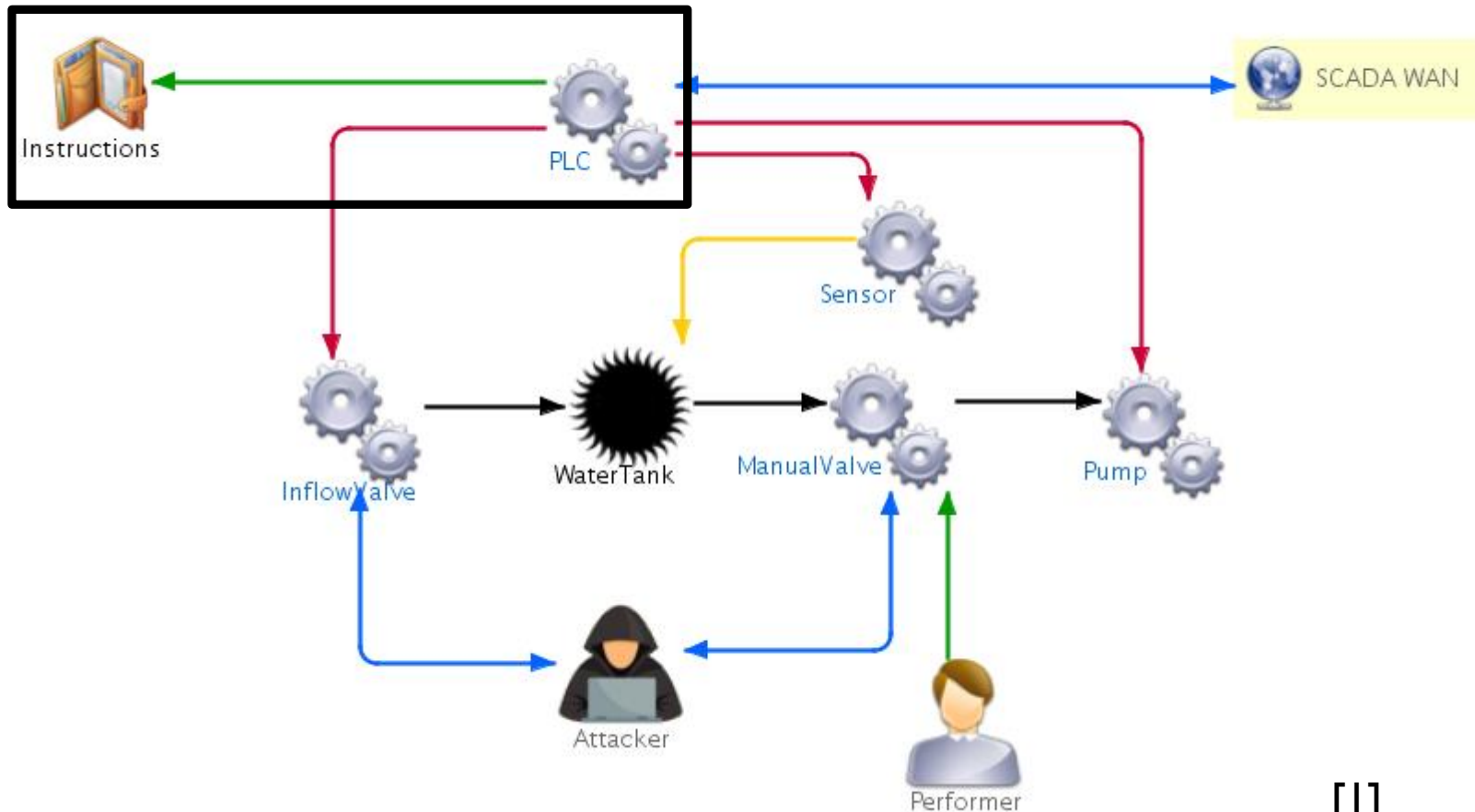




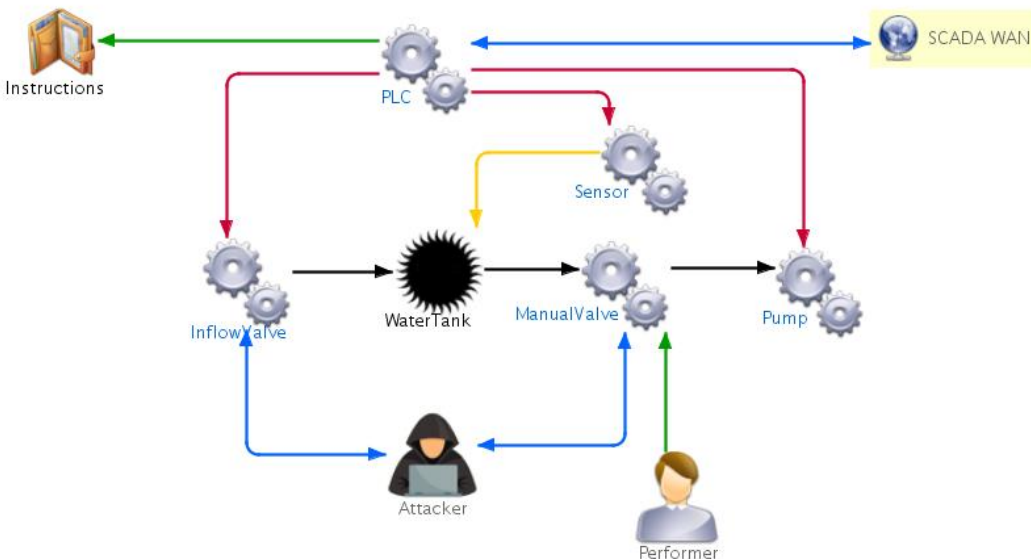
CPDY: Extending the Dolev-Yao Attacker with Physical-Layer Interactions, Marco Rocchetto & Nils Ole Tippenhauer

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

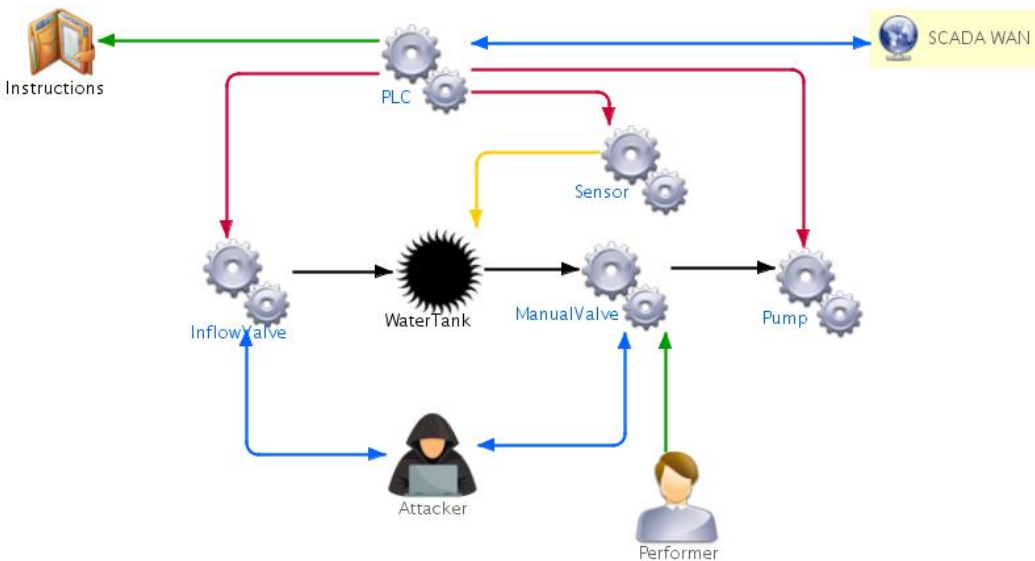




[1]



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][5]

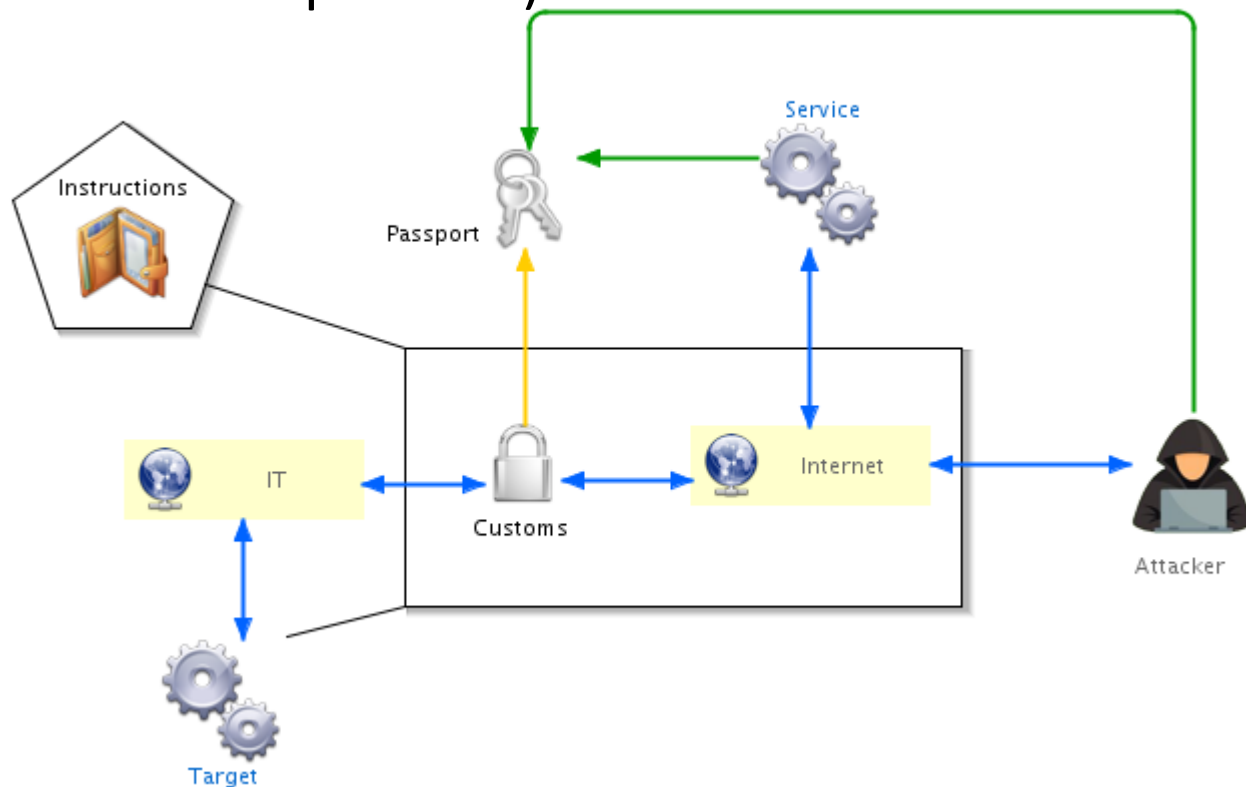


Exemple de scénario d'attaque:

- 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.[2][5]

- Modélisation de système via Pimca
 - Machineries
 - Ressources
 - Liens
- Modélisation d'attaque
 - Top 20 d'attaques
 - 7 patterns différents d'étapes élémentaires
 - Scénario d'attaque compose d'étapes élémentaires

- OpenFlexo, execution pas à pas sur un exemple simple
(Utilisation de booléens uniquement)



Conclusion Rappel

1. Target System Modeling Language [\[30/06/19\]](#) 😊
2. Attack surface operations [\[1/09/19\]](#) 😊
3. Attack modeling language [\[15/09/19\]](#) 😊
4. OBP2 adapter, or hand-made simulator [\[30/09/19\]](#) 😊
5. Case-study I - [\[30/10/19\]](#)

	Mai	Juin	Juillet	Aout	Septembre	Octobre
Target System Modeling (TSM) Language						
Attack Surface operations						
Attack Modeling Language (AML)						
OBP2 adapter						
Case-study I						

Conclusion

- To do (short-term)
 - **Comité de suivi individuel (CSI)** de 2e année (05/09/2019)
 - **Scénario** de ***Compromised Remote Network*** exécutable sur OpenFlexo (avec d'autres variables que des booléens)
 - **Ecriture d'article** (cf Overleaf)

Conclusion

- To do (mid-term)
 - **Autres cas d'études**
 - **3. Réification de la surface d'attaque** – Surface d'attaque explicite pour permettre la modélisation d'attaque. ("Points d'interaction/d'entrée explicites")
 - **4. Connaissance partielle** – Modélisation de point de vue lié à un acteur. ("Vision, portée & capacités d'interaction restreintes")

- Executable attack modeling on industrial control systems
- Some characteristics :
 - Cyber-physical interfaces
 - Dynamical systems
 - Semantic heterogeneity
 - Large number of specification and implementation languages
 - Large number of execution platforms
- Attack modeling
 - Attack trees, DAGs, graphs
 - Embedded attack strategies (embedded malicious code)
 - Either very abstract -> decoupled from the technical domain
 - Or very concrete -> coupled with the technical domain but low-level
 - Difficult to perform « execution-based » analysis

Introduction

Research questions

- How to capture an abstract operational semantics of the targeted system and compose it with executable attack modeling ?
- How to steer the focus towards architecture independent attack modeling ?
- How to capture the attack surface of the system-under attack (SUA) ?
- How to handle the semantic heterogeneity in the targeted system.

Introduction

Research questions

- **Opportunism** – The modeling language should allow an opportunism-based iterative refinement approach. The user should be able to detail only the points of interest, **and provide very abstract (generic) implementation for the other parts.**
- **Cyber-separation** – Ideally, the functional system model should be decoupled from the attack/defense actor modeling aspects. Which will enable focused reasoning both on the system aspects, and attack/defense models
- **Attack surface reification** – The attack surface should be exposed explicitly to ease the specification of attack/defense strategies
- **Incomplete knowledge** – The attack/defense actors act on the system having a limited knowledge. As opposed to specification languages which strive to provide an omniscient view on the system, attack discovery and modeling formalism should enable restricting the access to the « system model » to the attack surface.
- **Execution support** -- The formalism should provide the mechanisms for representing the system dynamics, even in the presence of partial behavior specification.
- **Multi-level abstraction** : mix abstraction levels
- **Semantic heterogeneity** : mix different languages

- Methodology based on the integration of two correlated processes :
 - Target system modeling process – TSM - (captures the « situation »)
 - Executable attack modeling process – EAM
- The TSM process enables capturing the semantics of the SUA
- The EAM process focuses on the specification of attack scenarios
- The TSM and EAM link is established at the semantic level through the formal definition of **attack surface operations** (operations exposed from the TSM semantics).