Sécurité des systèmes cyber-physiques

Focus sur les systèmes contrôle-commande SCADA

Joaquin Garcia-Alfaro

Laboratoire CNRS SAMOVAR & Télécom SudParis
Université Paris-Saclay

Séminaire iRENAV, 21 octobre 2016

Plan

- **Contexte & focus SCADA**
- **Systèmes cyber-physiques**
- **Véracité du feedback**
- **Synthèse & perspectives**

Focus sur les systèmes SCADA

http://www.panoptesec.eu/

Dynamic Risk Approaches for Automated Cyber Defense

FP7-ICT-2013-10

Consortium

RHEA

TELECOM SudParis

INSTITUT Mines-Télécom

s@movar

Supélec

acea

UNIVERSITÄT ZU LÜBECK

SAPIENZA UNIVERSITÀ DI ROMA

ROTAS OPERA TENET AREPO SATOR epistematica

NOKIA

L'un des objectifs de recherche du projet

- Prévenir des attaques contre systèmes contrôle-commande SCADA

Focus sur les systèmes SCADA

http://www.panoptesec.eu/

CHAIRE
CYBER CNI
Sécurité des infrastructures critiques

Consortium

L'un des objectifs de recherche du projet

- Prévenir des attaques contre systèmes contrôle-commande SCADA

Problématique à traiter

- Malware qui arrive à passer du SI de gestion au SI industriel
- Mauvaises configurations, pas de chiffrement, équipements anciens, accès des parties tierces, applications non autorisées, ...

Objectifs

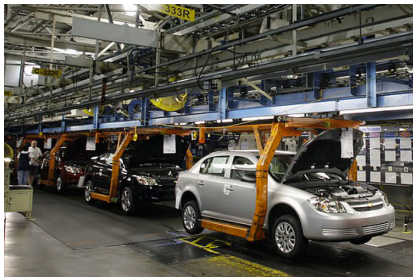
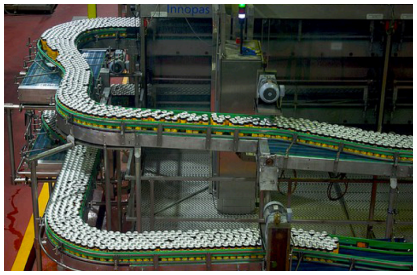
- **Développement des compétences et connaissances sur les systèmes de contrôle-commande**
- **Identifier leurs problématiques sécurité, sûreté, résistance, ...**

Méthodologie

- **Représentation d'un système dynamique et complexe avec modèles théoriques**
- **Banc de test pour mettre en place les modèles, expérimenter et vérifier les résultats**

Qu'est-ce qu'un SCADA ?

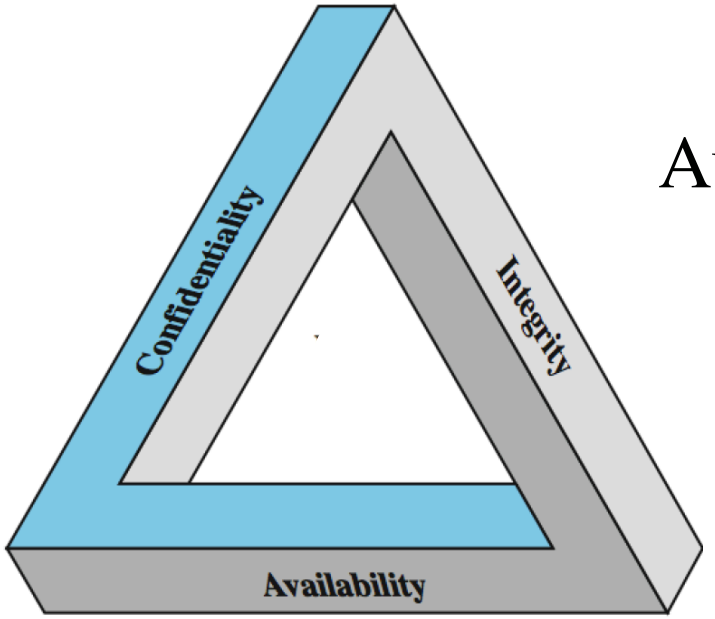
- **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition
  - Système de contrôle et d'acquisition de données
- Ex. systèmes (distribués) à contrôle centralisé ...


- ... et critiques, car certains sont des OIV (Opérateurs d'Importance Vitale)



Enjeux & défis



Aussi

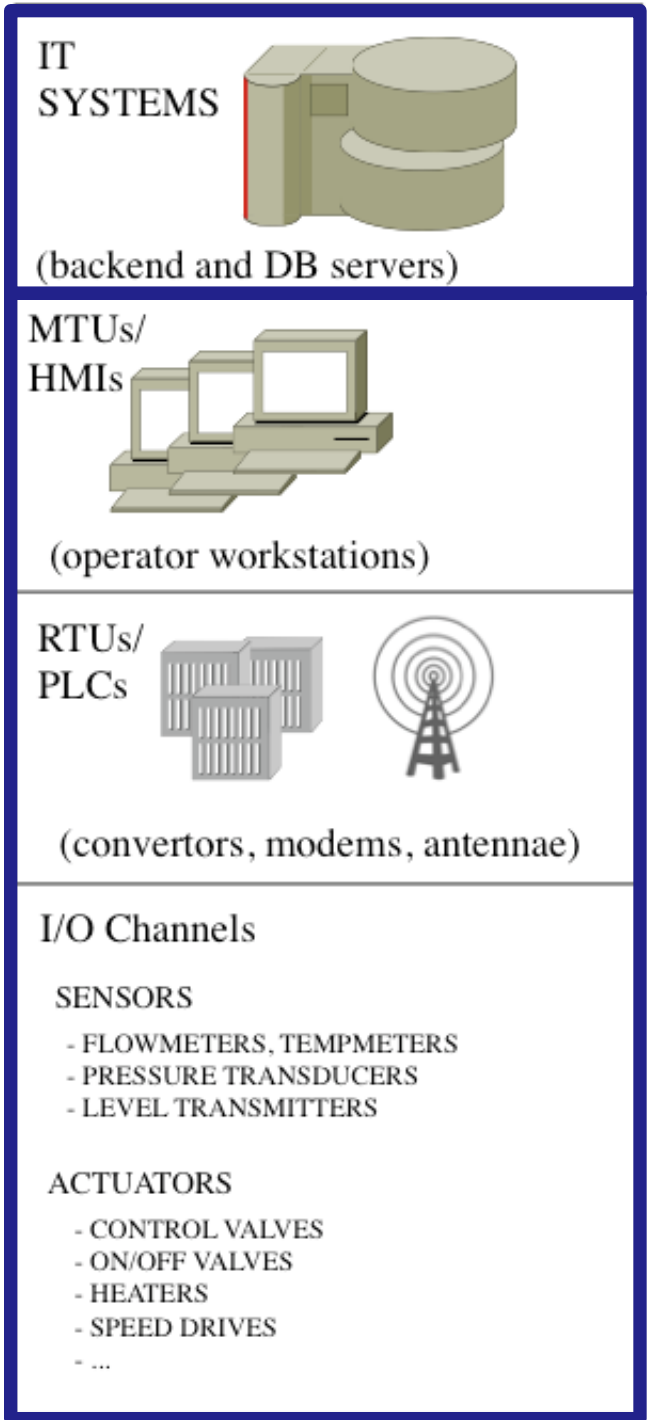
- Fiabilité,
- Sûreté,
- Temps réel, ...

Actifs à protéger* : Information

Priorité	Système IT	MTUs à I/O
#1	Confidentialité	Disponibilité
#2	Intégrité	Intégrité
#3	Disponibilité	Confidentialité

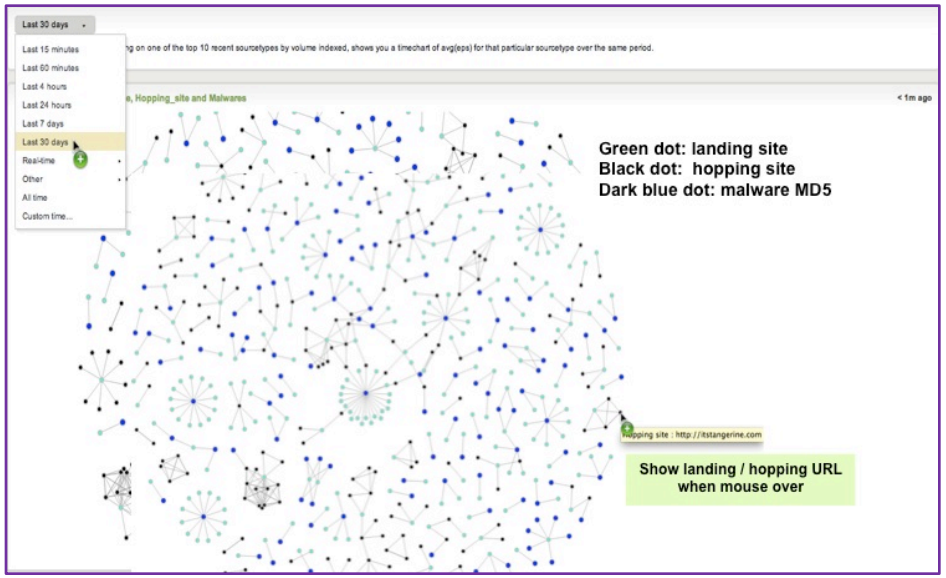
Processus

* HIRSCHMANN, Why is Cyber Security Still a Problem? *TOFINO Security Series*

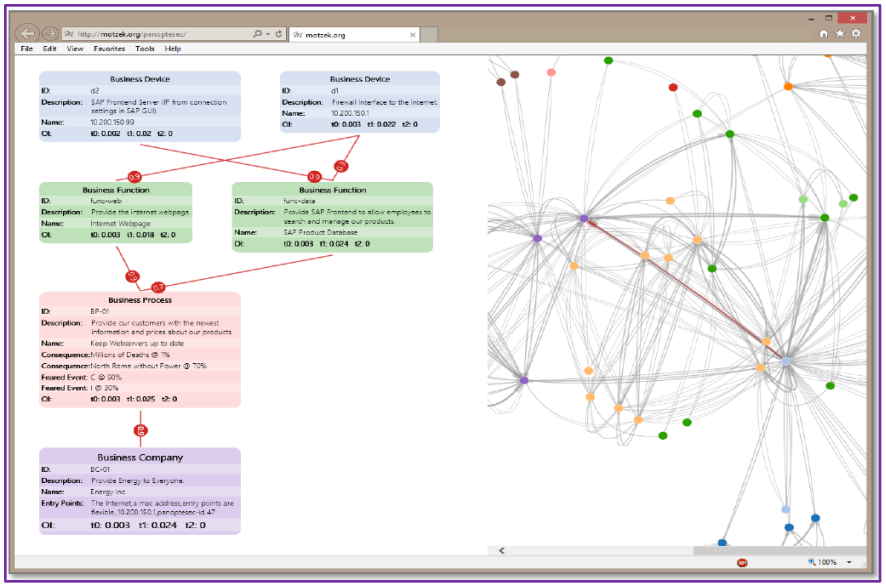


L'approche du projet PANOPTESEC

- Evaluation et gestion du risque
- Utilisation de *graphes d'attaque* & *graphes de mission*



Anticiper l'exploitation des vulnérabilités



Réduire l'impact des attaques

PANOPTESEC

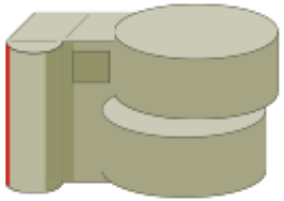
Eléments d'un SCADA

Intergiciels basés sur l'utilisation des :

- **RTUs (*Remote Terminal Units*)**
- **PLCs (*Programmable Logic Controllers*)**

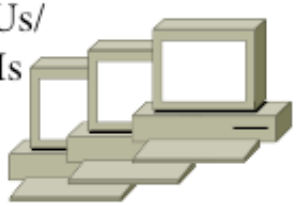
pour contrôler capteurs et actuateurs, souvent déployés loin (des centaines de *km*)

IT SYSTEMS



(backend and DB servers)

MTUs/ HMIs



(operator workstations)

RTUs/ PLCs

(convertors, modems, antennae)

I/O Channels

SENSORS

- FLOWMETERS, TEMPMETERS
- PRESSURE TRANSDUCERS
- LEVEL TRANSMITTERS

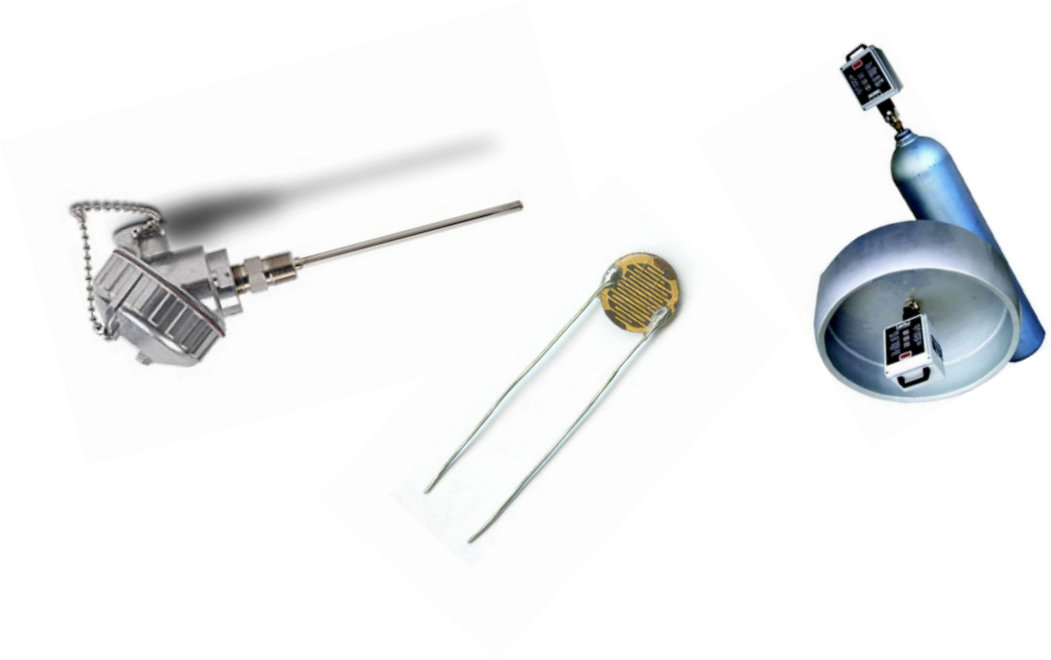
ACTUATORS

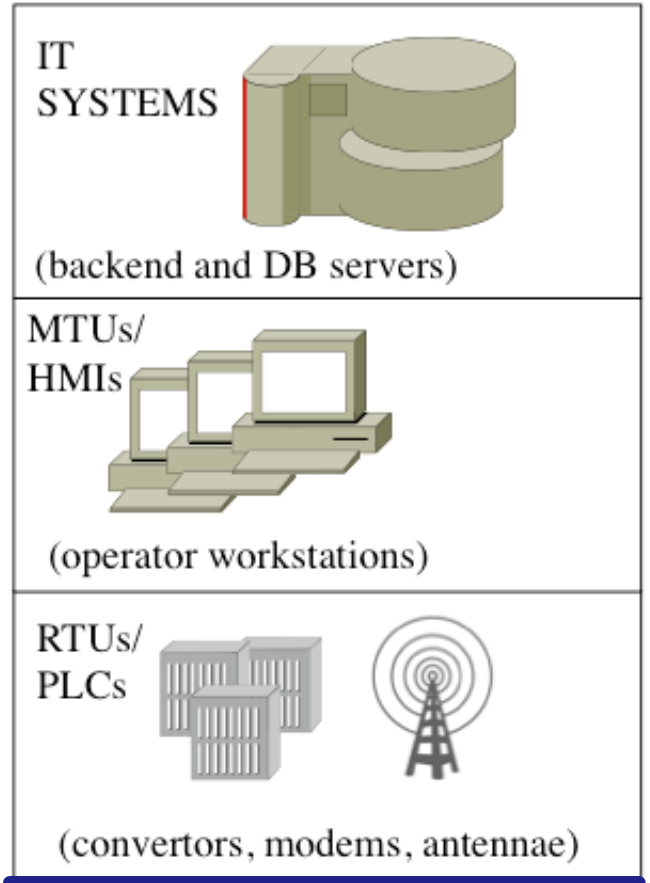
- CONTROL VALVES
- ON/OFF VALVES
- HEATERS
- SPEED DRIVES
- ...

Eléments d'un SCADA

Sécurité intrinsèque données E/S ?

- **Actuateurs** : effectuent les actions physiques (ex. déplacement, émission de lumière, etc.) et rendent compte à la partie commande
- **Capteurs** : mesurent l'état d'un événement physique (ex. tension électrique, température, humidité, etc.)





Plan

- Contexte & focus SCADA
- **Systèmes cyber-physiques**
- Véracité du feedback
- Synthèse & perspectives

Questions fondamentales …

- Que sont les *systèmes cyber-physiques* (CPSs) ?
- Sont-ils nouveaux ?
- Comment leur sécurité diffère de la SSI traditionnelle ?

Que sont les CPSs ?

- Des systèmes qui surveillent des entités physiques, en prenant des mesures pour contrôler (et/ou corriger) leurs comportements

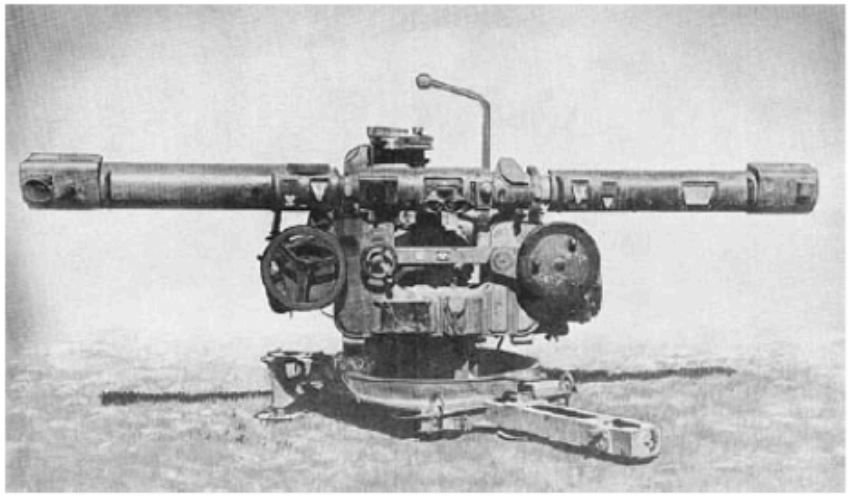
... mais aussi :

Définition alternative

« Systèmes avec des éléments de calcul complémentaires aux éléments physiques, **qui peuvent interagir avec des humains** parmi nouvelles technologies »

Sont-ils nouveaux ?

Réponse courte : **Non, ils ne sont pas nouveaux ***



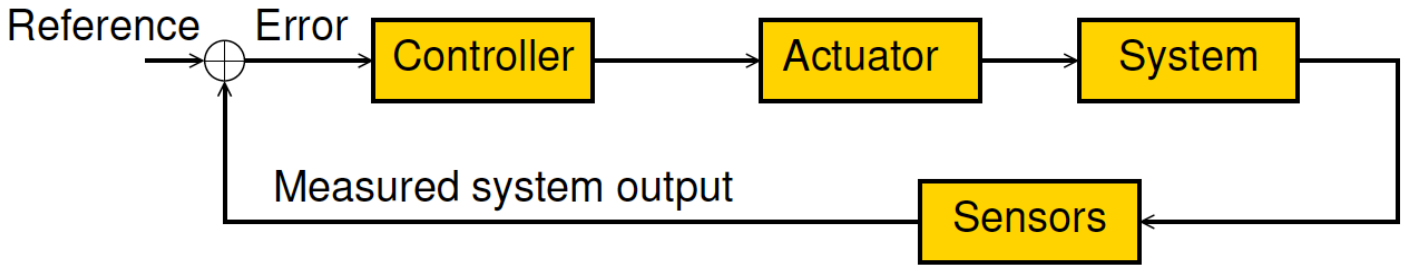
Kommandogerät 40 (Canon antiaérien - Seconde Guerre mondiale)

- Intégration d'éléments mécaniques, électroniques et de communication
- Rétroaction humaine (au moins cinq personnes pour le faire fonctionner)

** Cyber–Physical Systems: A Perspective at the Centennial. Kim and Kumar. Proceedings of the IEEE, Vol. 100, pages 1287-1308, May 2012.*

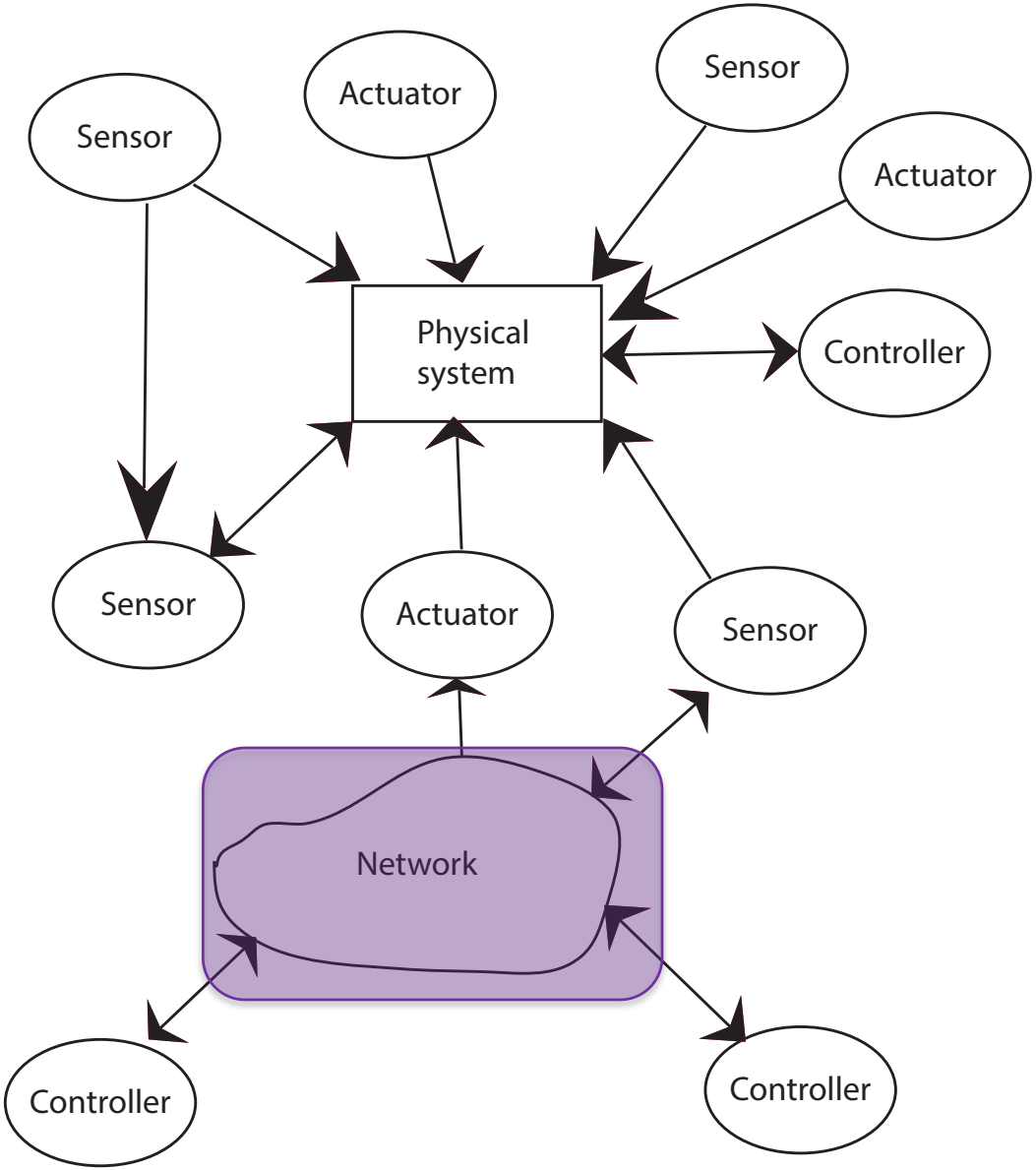
Ingrédients clés : contrôle et retroaction

- **Contrôle :** conduire un système (dynamique et complexe) aux états souhaités
- **Rétroaction (feedback) :** action en retour d'un effet sur sa propre cause, par rapport à un *signal de référence*, ainsi que les entrées et sorties du système



- Exemples : suivi des trajectoires (robotique), régulation de la température, congestion trafic TCP/IP, équilibrer le mouvement oscillatoire d'un pendule, etc.

Ingrédients clés : E/S & réseau

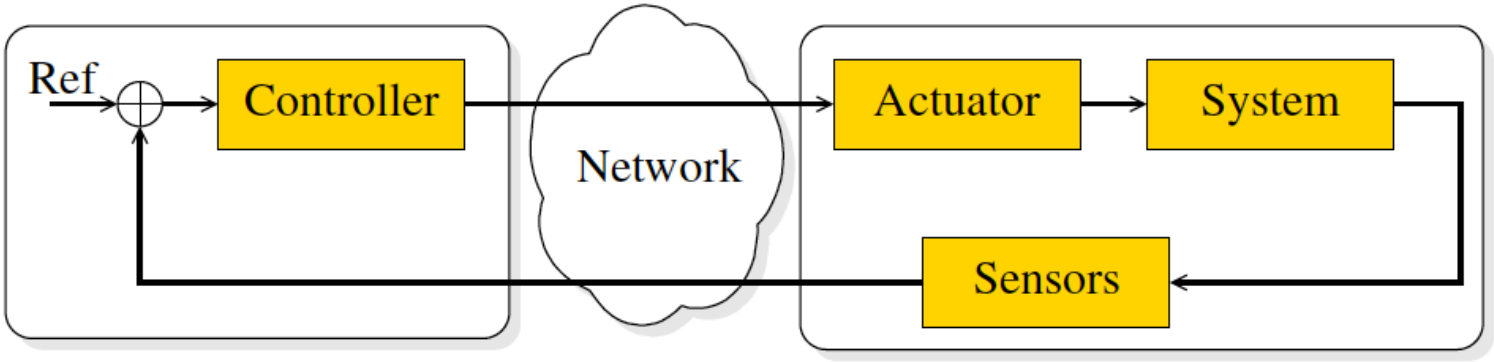


Systèmes contrôlés en réseau

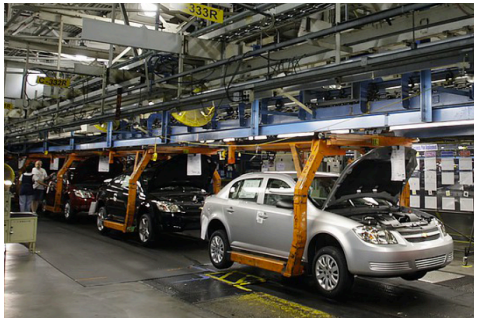
- D'un point de vue méthodologique, on peut modéliser un CPS sous la forme d'un système contrôlé en réseau (SCR ou NCS, *Networked-Control System*)

SCR (Systèmes Contrôlés en Réseau)

L'architecture globale (incluant le réseau) doit également satisfaire la contrainte temps-réel

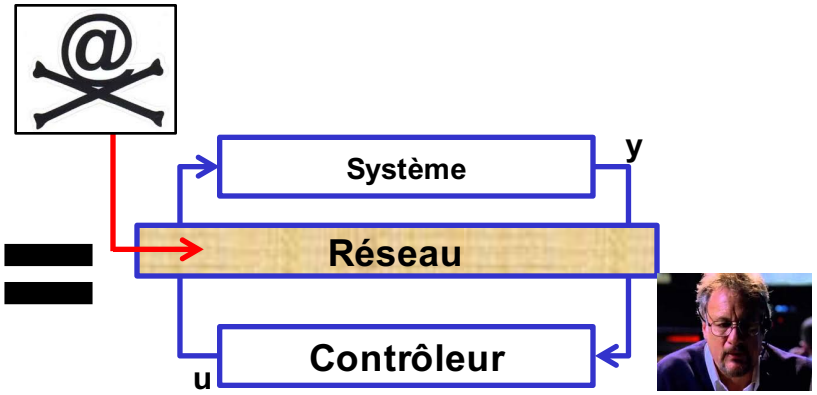


SCR & SCADA



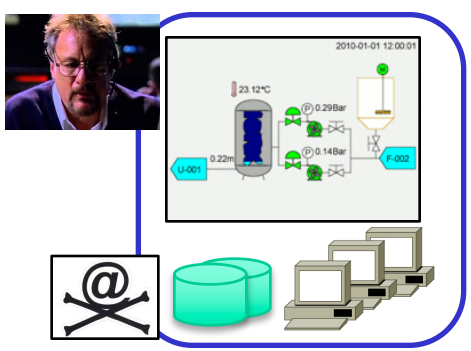
Système contrôlé

Technologies de l'information et de la communication



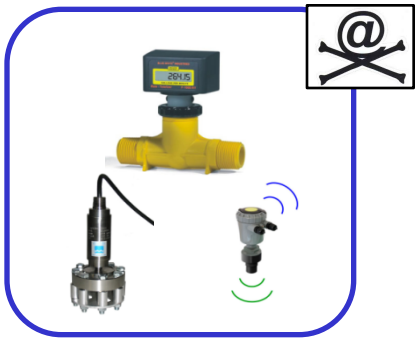
Système Cyber-Physique (CPS)
Système Contrôlé en Réseau (SCR)

SCADA (supervisory control and data acquisition, ou système de contrôle et d'acquisition de données)



Système de gestion

Automates programmables



Capteurs et actionneurs

Problématiques traitées dans la littérature des SCR

- Stabiliser un système qui a des pertes de paquets réseau
- Limiter le débit de données (ex. du contrôleur aux capteurs)
- Efficience énergétique dans les SCR sans fils
- Sécurité
  - Depuis l'**incident *stuxnet***, la communauté recherche SCR & théorie du contrôle semblent avoir **un intérêt croissant sur la sécurité des CPS**

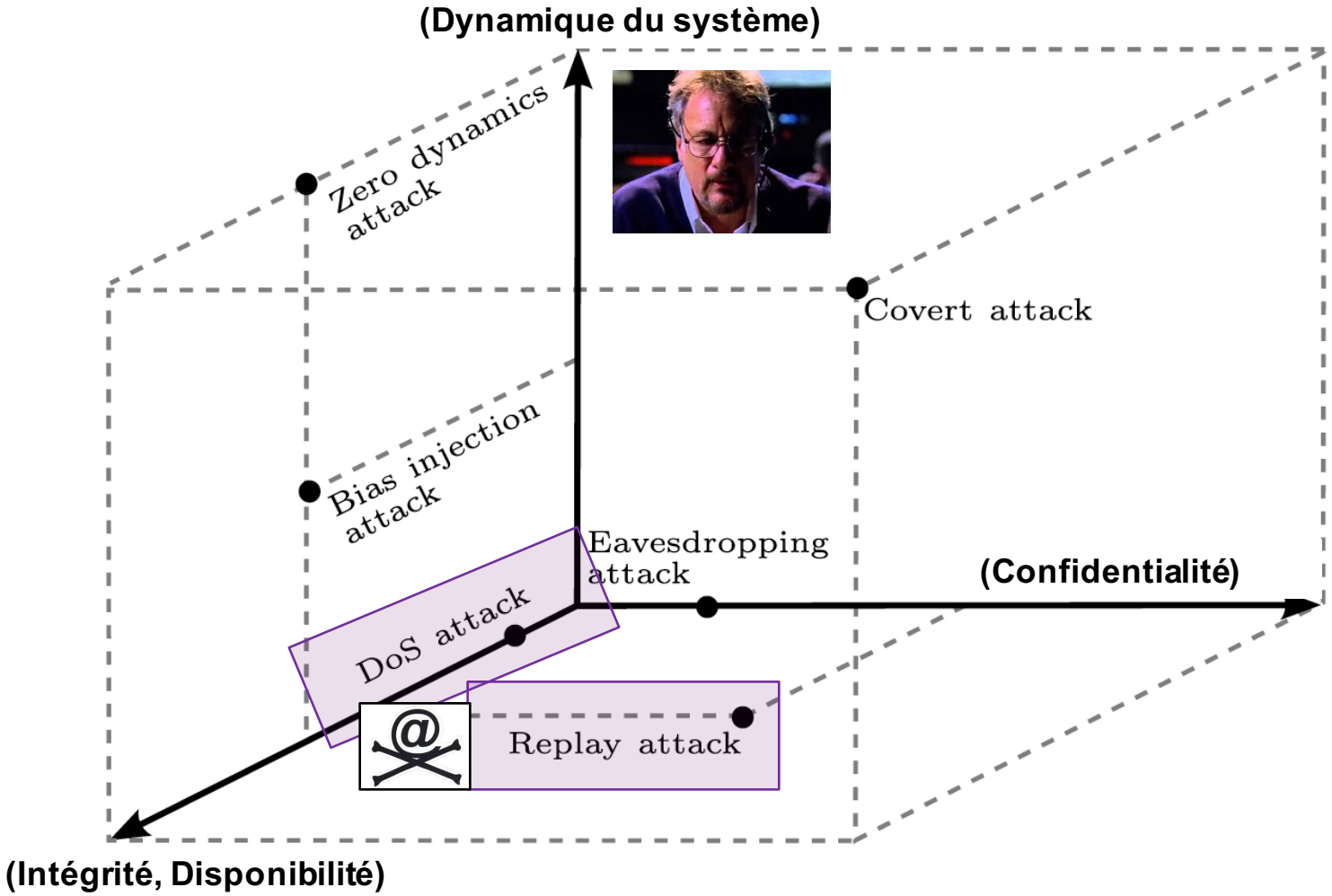
Problématiques de sécurité

- Couche cyber
  - Communications non chiffrées
  - Configuration manuelle des contrôleurs (à distance ou en personne)
  - Noms d'utilisateurs & mots de passe par défaut
  - …

- Surfaces d'attaque
  - Physique & contrôle (couche **physique**)
  - Communication & réseau (couche **cyber**)
  - Surveillance & gestion (couche **humaine**)
  - …

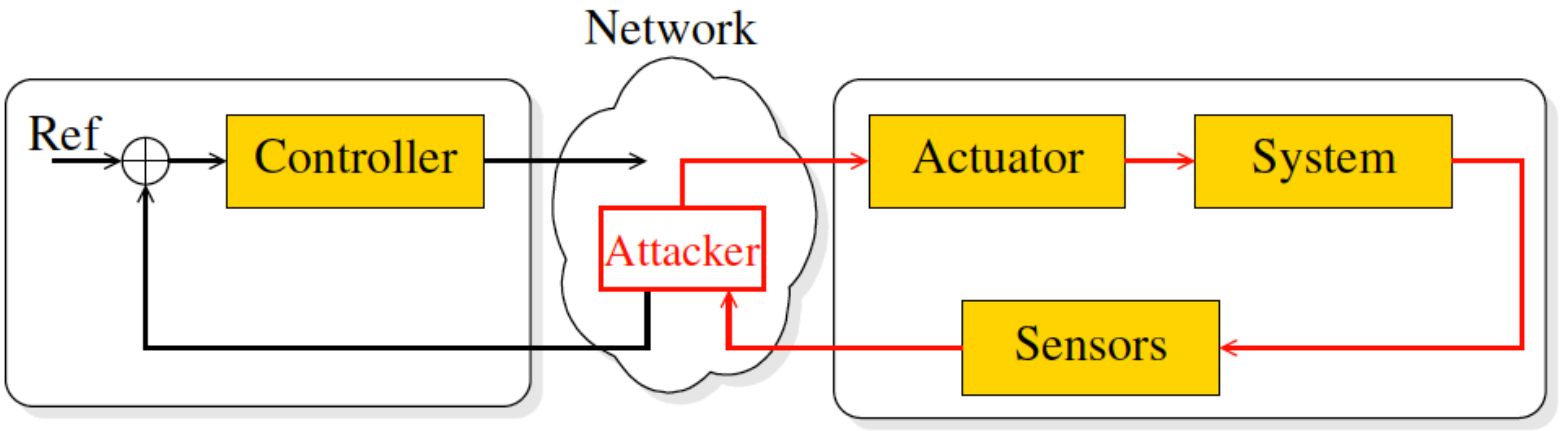
- Types d'attaque
  - Données (Contrôle & **Mesures** / Actuateurs & Capteurs)
  - Estimations & **Commandes** (Contrôleur & HMIs)
  - ...

Attaques d'exemple*



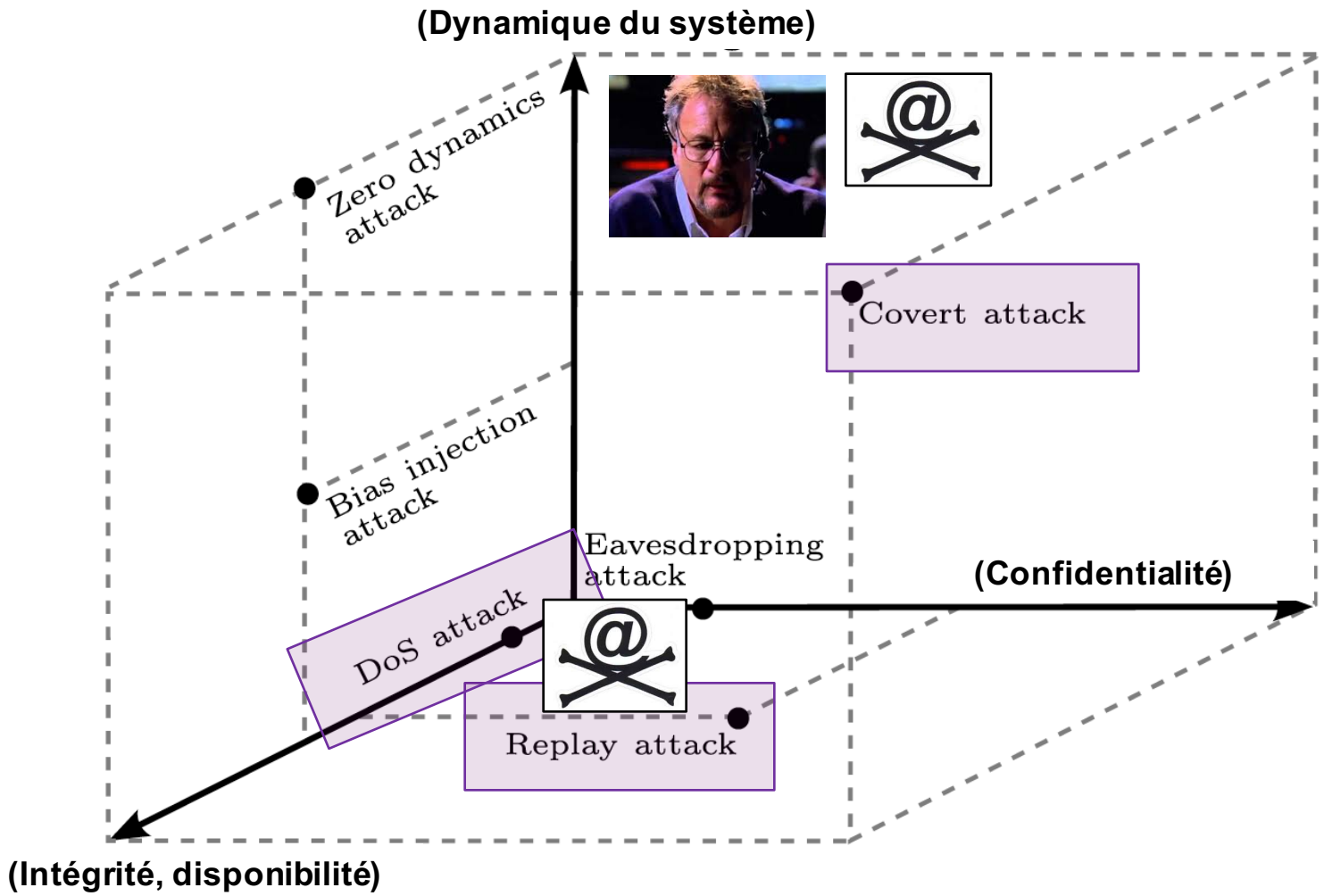
** A secure control framework for resource-limited adversaries. Texeira et al., Automatica, 51(1):135-148, 2015.*

Attaque (cyber-physique) par rejeu



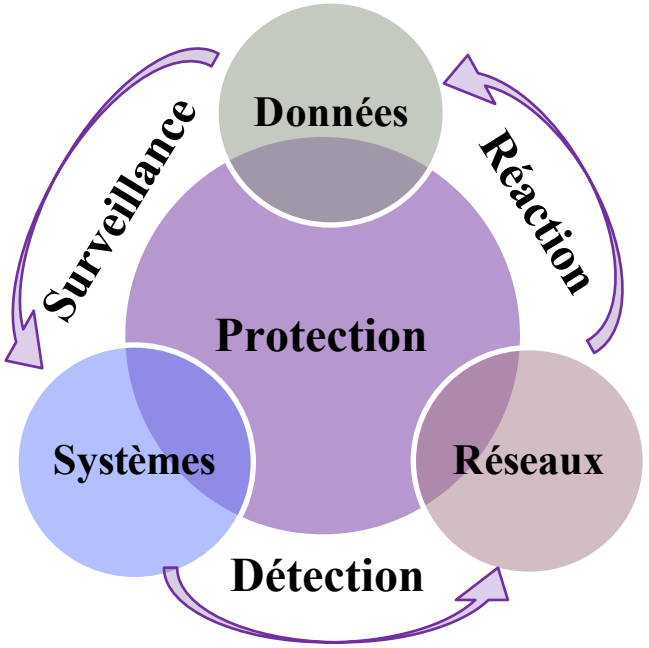
- Step 1: Sensors output is recorded
- Step 2: Recorded sensors output is replayed and sent to the controller
- Step 3: A control signal is sent to disrupt system functionalities

Attaques d'exemple*



** A secure control framework for resource-limited adversaries. Texeira et al., Automatica, 51(1):135-148, 2015.*

Prévention des attaques

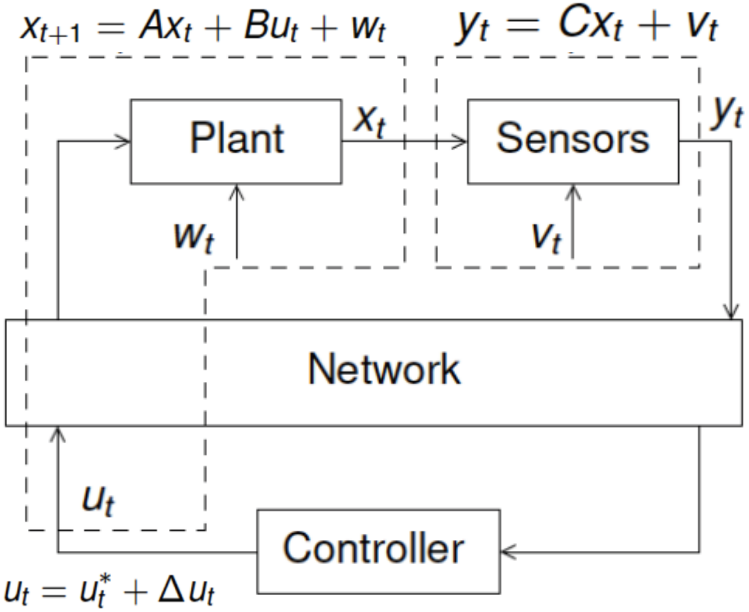


- Un système de contrôle bien conçu doit résister à des perturbations externes (défaillances et attaques)
- Plusieurs techniques ont été proposées dans la littérature de la théorie du contrôle pour prévenir les attaques cyber-physiques*
- La plupart des techniques visent à caractériser la malveillance et détecter des mesures anormales
  - Une fois détectée, activer la réaction pour mettre le système en mode dégradé

** A survey on the security of cyber-physical systems. Wu, Sun, and Chen. Control Theory and Technology, 14(1):2–10, February 2016.*

Surveillance & détection couche physique*

- **But :** protection des environnements vulnérables
  - Difficulté : surveiller/protéger systèmes industriels, sans perturber fonctionnement temps réel



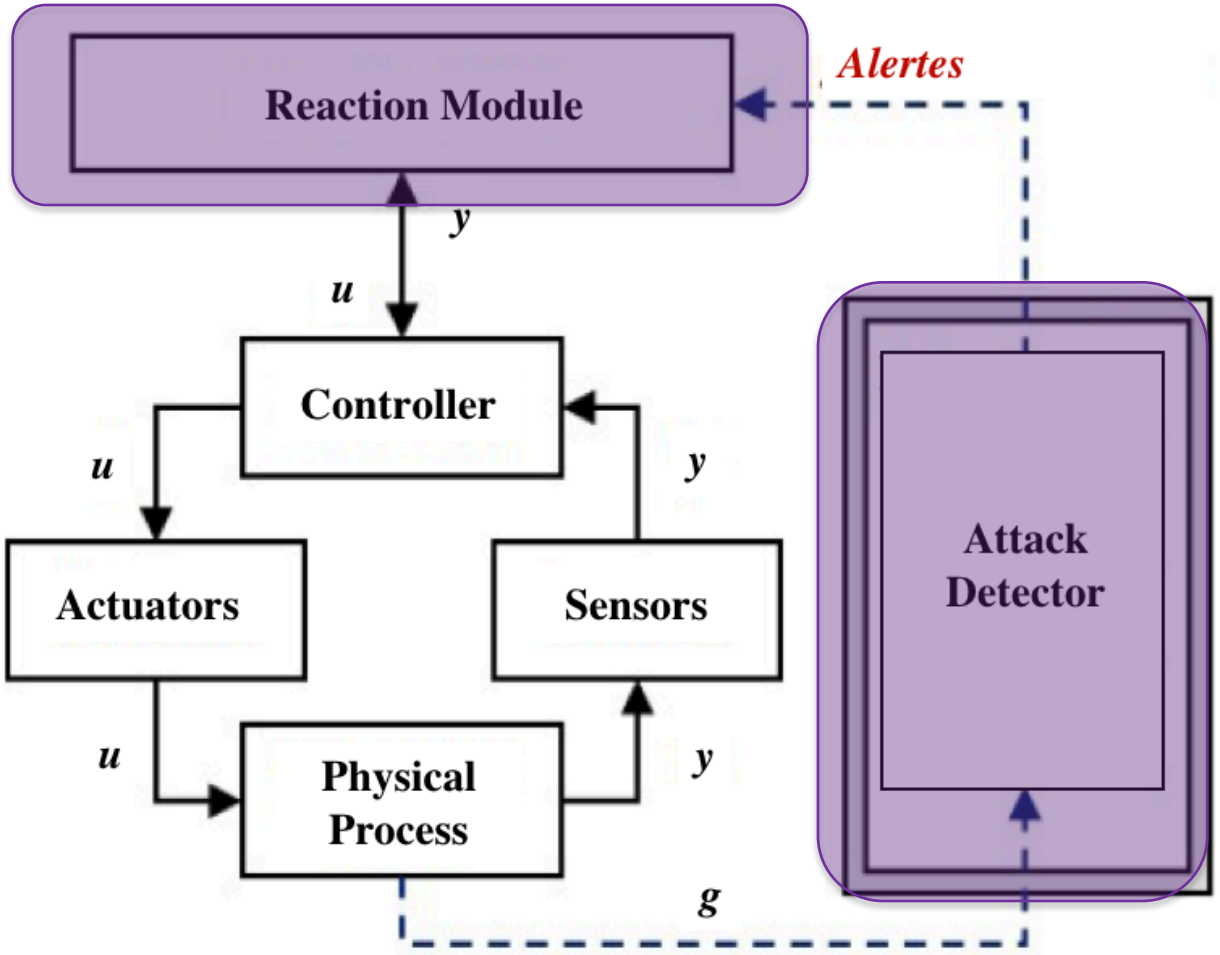
- **Approche défi-réponse** (modification imperceptible des comportements normaux)
  - Théorie du contrôle & modèles LTI (*linéaires invariants dans le temps*)
- Défi : u_t ; Réponse : y_t
- Analyse statistique entre défi et réponse :

$$g_t = \sum_{i=t-w+1}^{t} (y_i - C\hat{x}_{i|i-1})^T \mathcal{P}^{-1} (y_i - C\hat{x}_{i|i-1})$$

- **Si g_t dépasse un certain seuil ⇝ alerte**

* Rubio-Hernan, De Cicco, Garcia-Alfaro, « Revisiting a Watermark-based Detection Scheme to Handle Cyber-Physical Attacks », *11th Intl. ARES Conference*, ***Best Paper Runner-up Award***, Aug 2016.

Mitigation des attaques après la détection



Revisiting a Watermark-based Detection Scheme to Handle Cyber-Physical Attacks*

Joint work with

Jose Rubio-Hernan and Luca de Cicco

**** 11th International Conference on Availability, Reliability and Security (ARES 2016), August 2016. (Best Paper Runner-Up Award)***

Watermark Approach by Mo et al.

Idea [Mo et al., 2009, 2015]

Adding a watermark signal to the control signal which serves as an authentication signal

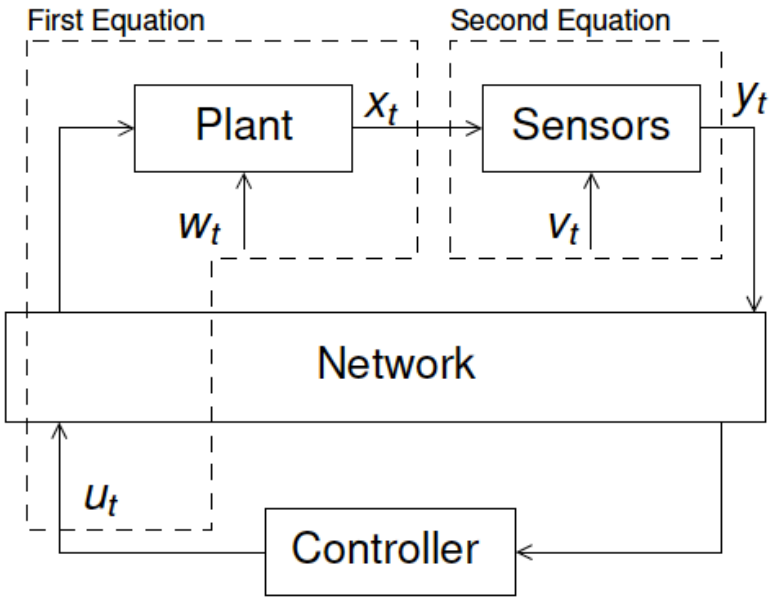
- Conceptually similar to a challenge-response authentication scheme
- In this case the watermark is the challenge the response is the sensor output
- Main advantages:
  - Only the controller has to be changed
  - It does not require encryption

** Physical Authentication of Control Systems. Mo, Weerakkody and Sinopoli. IEEE Control Systems, Vol. 35, pages 93–109, 2015.*

The Mo et al. Approach (1/2)

System is modeled as follows:

$$x_{t+1} = Ax_t + Bu_t + w_t$$
$$y_t = Cx_t + v_t$$



- x_t is the state vector in $\mathbb{R}^n$
- $u_t \in \mathbb{R}^p$ is the control action
- y_t system output vector in $\mathbb{R}^m$

The Mo et al. Approach (2/2)

- The control signal input of the plant is:

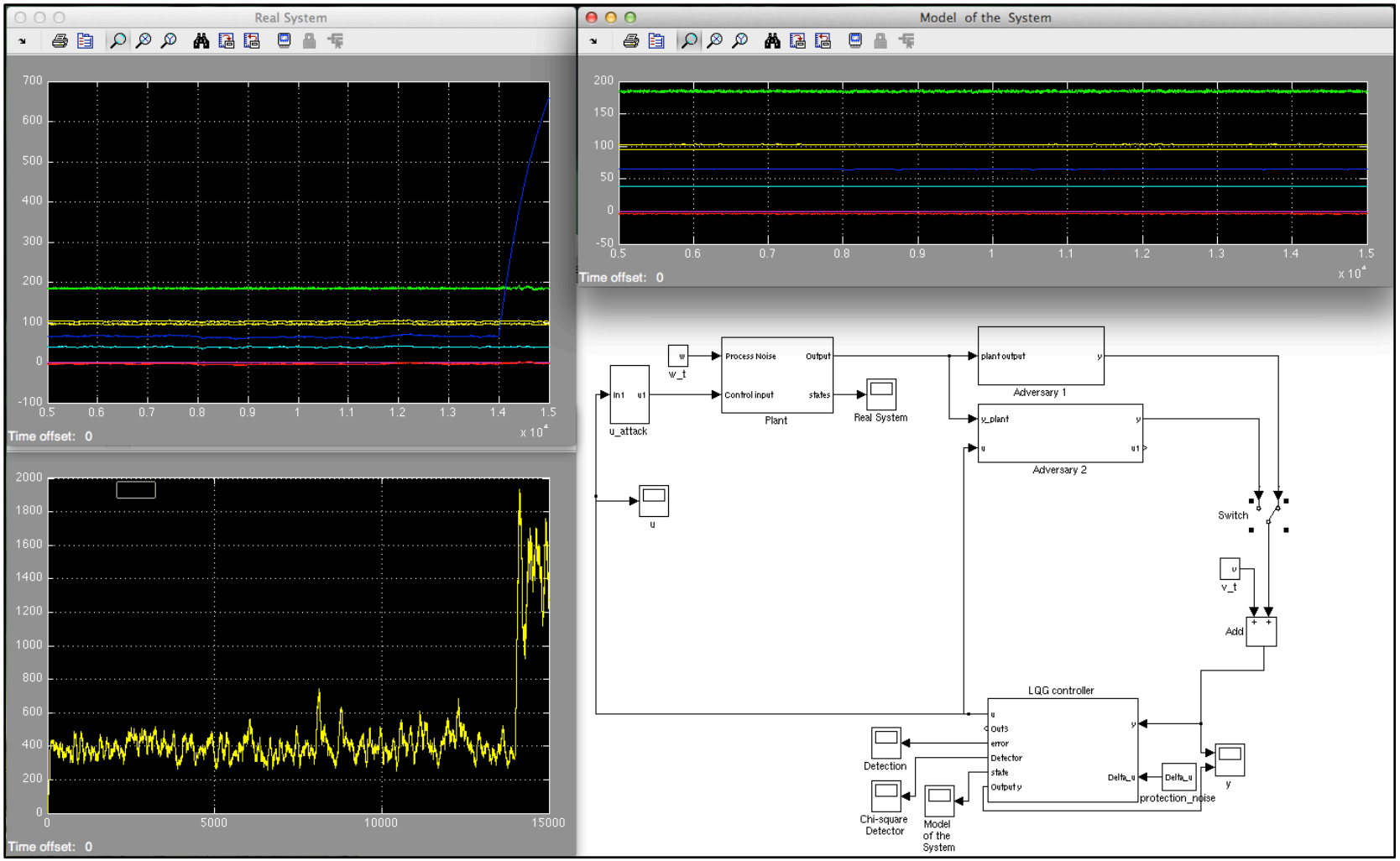
$$u_t = u_t^* + \Delta u_t$$

- $\Delta u \in \mathbb{R}^p$ are p Gaussian stationary processes independent from the noises
- A detector is used at the controller that computes alarms based on Kalman filter residues

$$g_t = \sum_{i=t-w+1}^{t} (y_i - C\hat{x}_{i|i-1})^T \mathcal{P}^{-1} (y_i - C\hat{x}_{i|i-1}) \quad (1)$$

- In normal operation (no attack) g_t is small
- If a replay attack is carried out the g_t increase

Simulating the Approach in Matlab/Simulink



Uncovered Issues

- Via simulation, we can show that a cyber-physical adversary is able to escape the detector

Cyber-physical Adversary

An attacker that is able to eavesdrop the messages containing the output of the controller with the intention of improving its knowledge about the system model

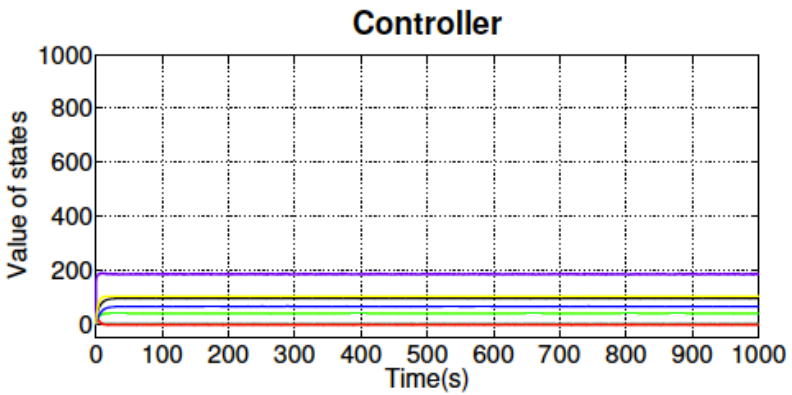
- Such attacker can leverage system identification tools to gather the system model and extract the watermark Δu_t from $u_t = u_t^* + \Delta u_t$
- The extracted watermark can be used to authenticate messages to disrupt system dynamics

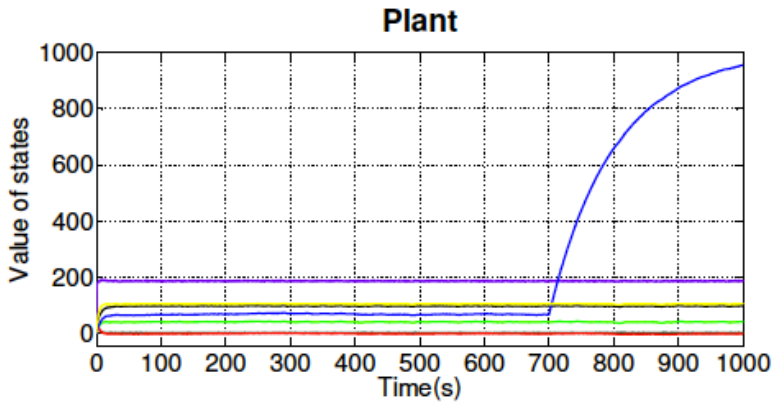
An Implementation of our Proposed Attack

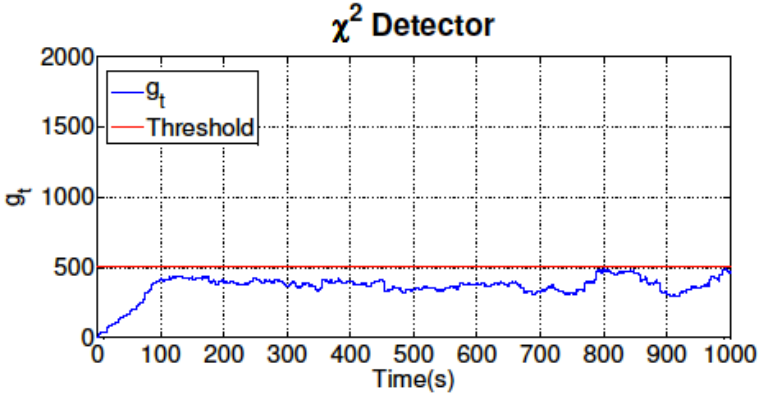
- The attacker eavesdrops u_t and y_t
- A Least Mean Square (LMS) filter is used to get an input-output model $\mathcal{W}$ from u_t to y_t
- By doing so the watermark Δu_t is obtained
- An arbitrary u'_t can be sent to the system
- We can extract y_t^* from y_t and record it
- We fake the controller by authenticating y_t^* with the acquired watermark

Validating the Attack in Matlab/Simulink

A cyber-physical attack is started at time $t = 700s$







- The attacker disrupt system dynamics (the controller does not perceive it)
- The attack is **not detected**

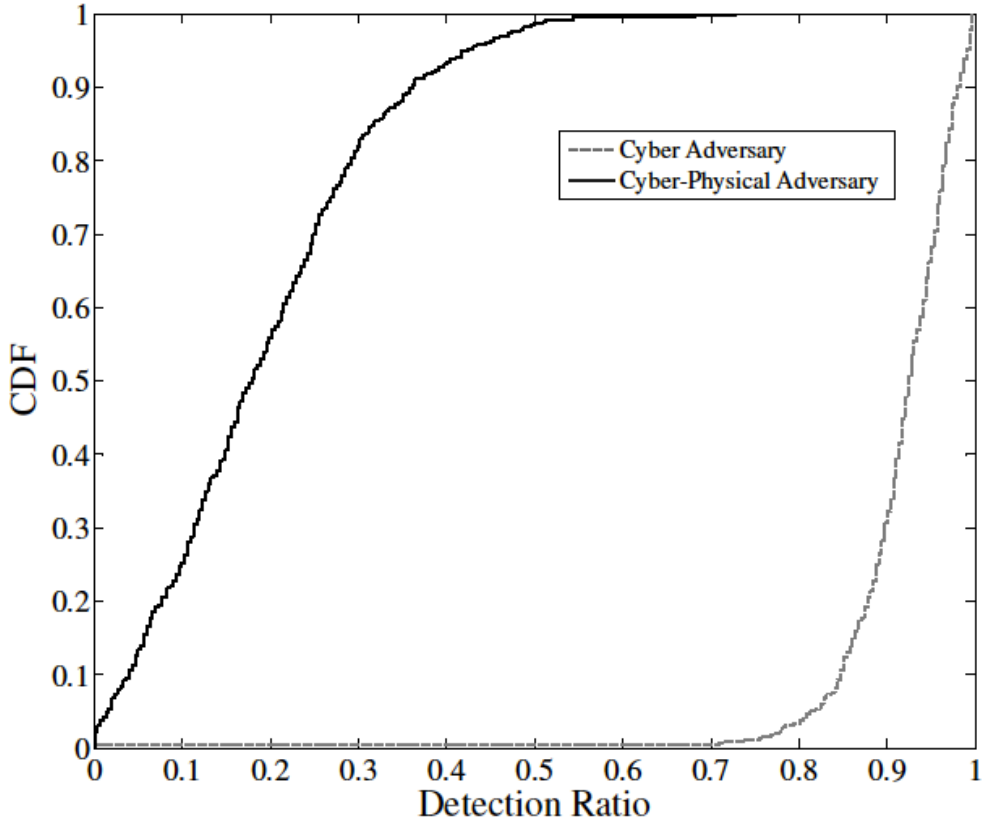
Detection Ratio

To quantify the detector performance we use the **Detection Ratio (DR)** index:

$$DR = \frac{\sum_{t=T_0}^{T_0+T_a} \mathbf{1}_{g_t \geq \gamma}}{T_a} \in [0, 1] \tag{2}$$

- In words: amount of time an attack is detected ($g_t \geq \gamma$) divided by the attack duration T_a
- $DR = 0$ if the attack is never detected, $DR = 1$ if it is always detected

Comparing Cyber and Cyber-Physical Adversary DR



500 simulations

Cyber adversary:
DR average = 0.9

Cyber-physical adversary:
DR average = 0.2

The Watermark-Detector protection scheme by Mo et. al is not sufficiently robust against cyber-physical adversaries

Revisiting the Mo et al. Approach

Towards a multi-watermark cheme

Switch among N watermarks to increase the Detection Ratio

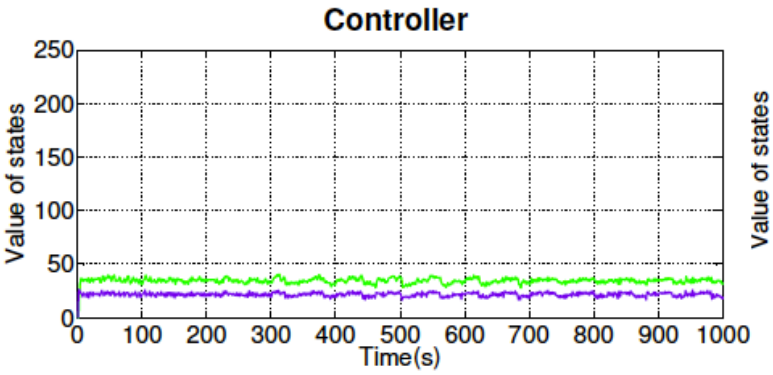
$$\Delta u_t = \Delta u_t^{(s(t,T))} \tag{3}$$

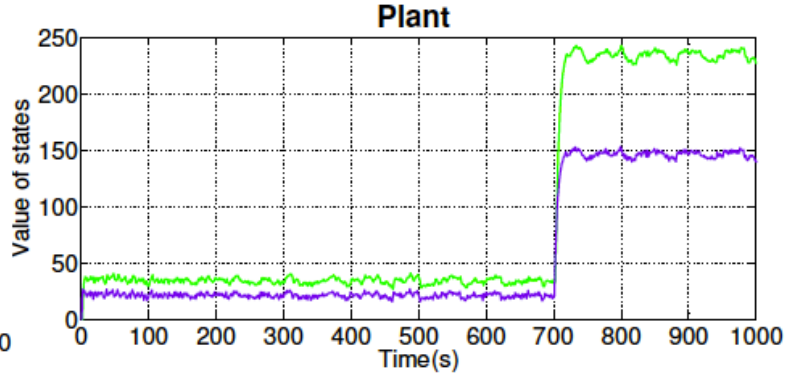
where $\Delta u_t^{(i)}$ with $i \in \mathcal{I} = 0, \ldots, N-1$ is the i-th of the N watermarks, T is the periodicity and T is the switching period

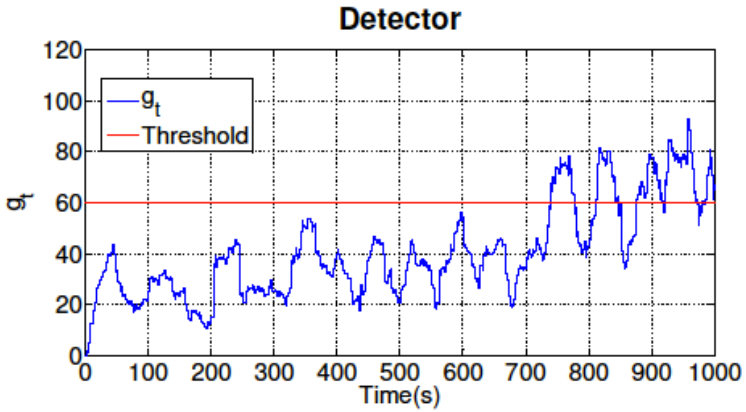
We moved from a static watermark mechanism to an **adaptive** watermark mechanism

Three Watermarks, period T=20s

A Cyber-physical adversary which starts the attack at time $t = 700s$



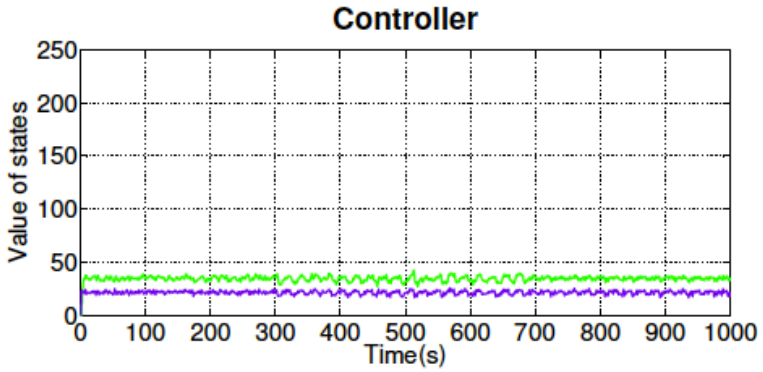


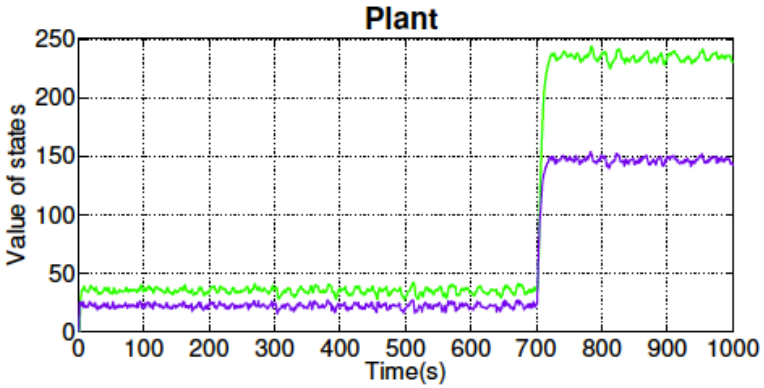


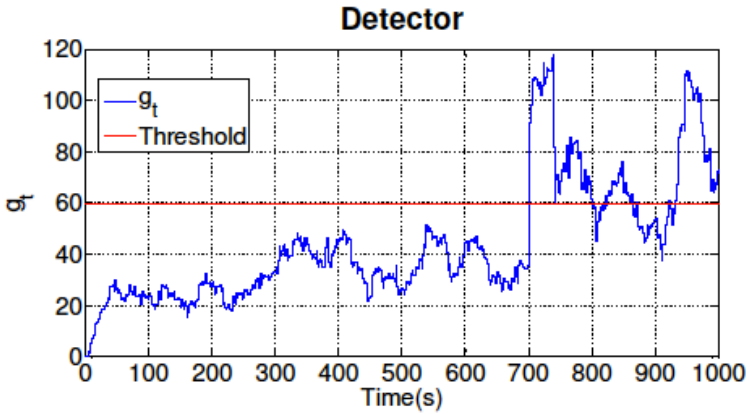
- The attacker disrupt system dynamics (the controller does not perceive it)
- The attack is detected after a while
- Slightly larger oscillations in state dynamics due to the new watermark

Three Watermarks, period T=7s

A Cyber-physical adversary which starts the attack at time $t = 700s$

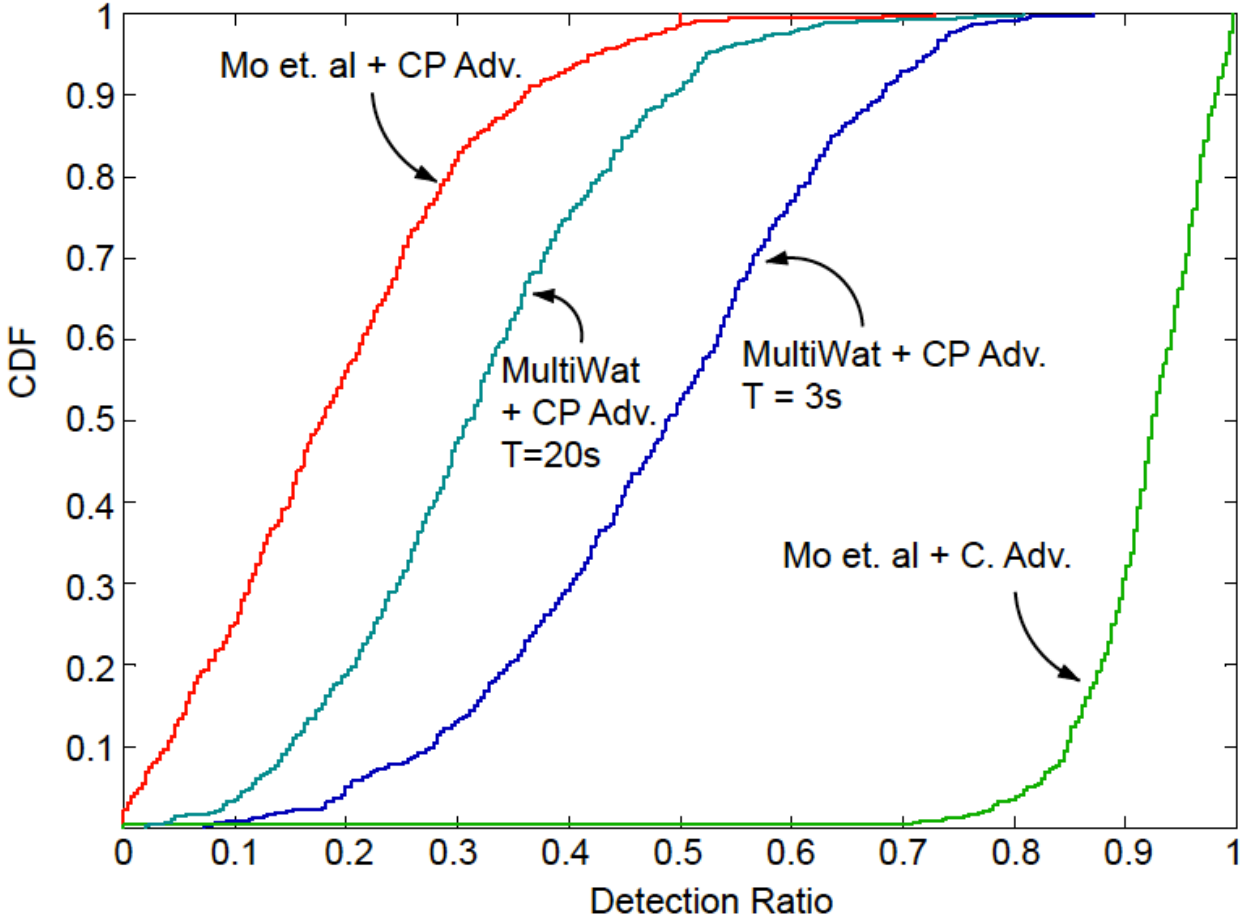




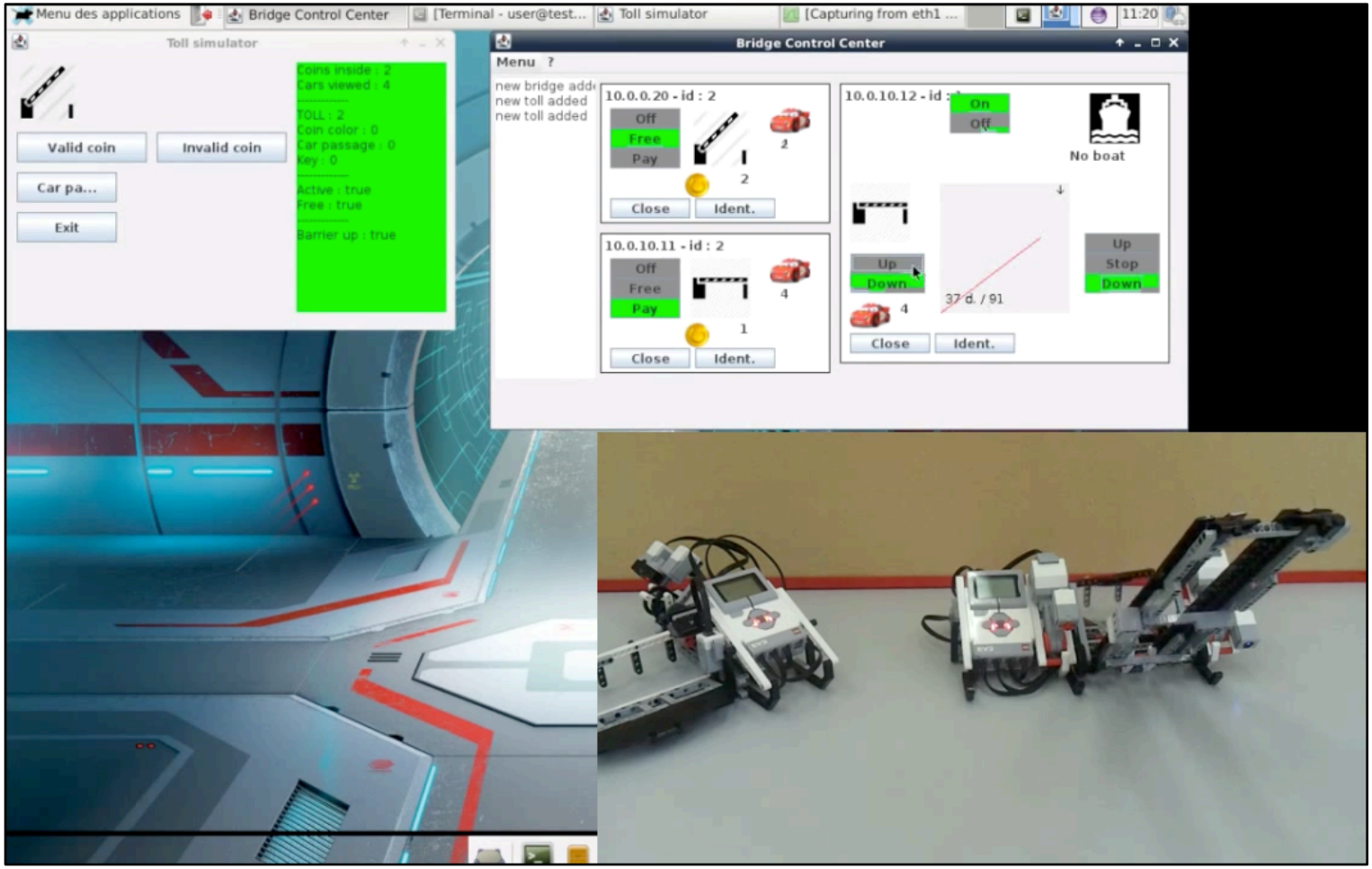


- The attacker disrupt system dynamics (the controller does not perceive it)
- The attack is detected very quickly (DR higher wrt the previous case)
- High frequency oscillations in state dynamics due to the new watermark

Detection Ration vs. Switching Frequency (CDF)



Lego Testbed

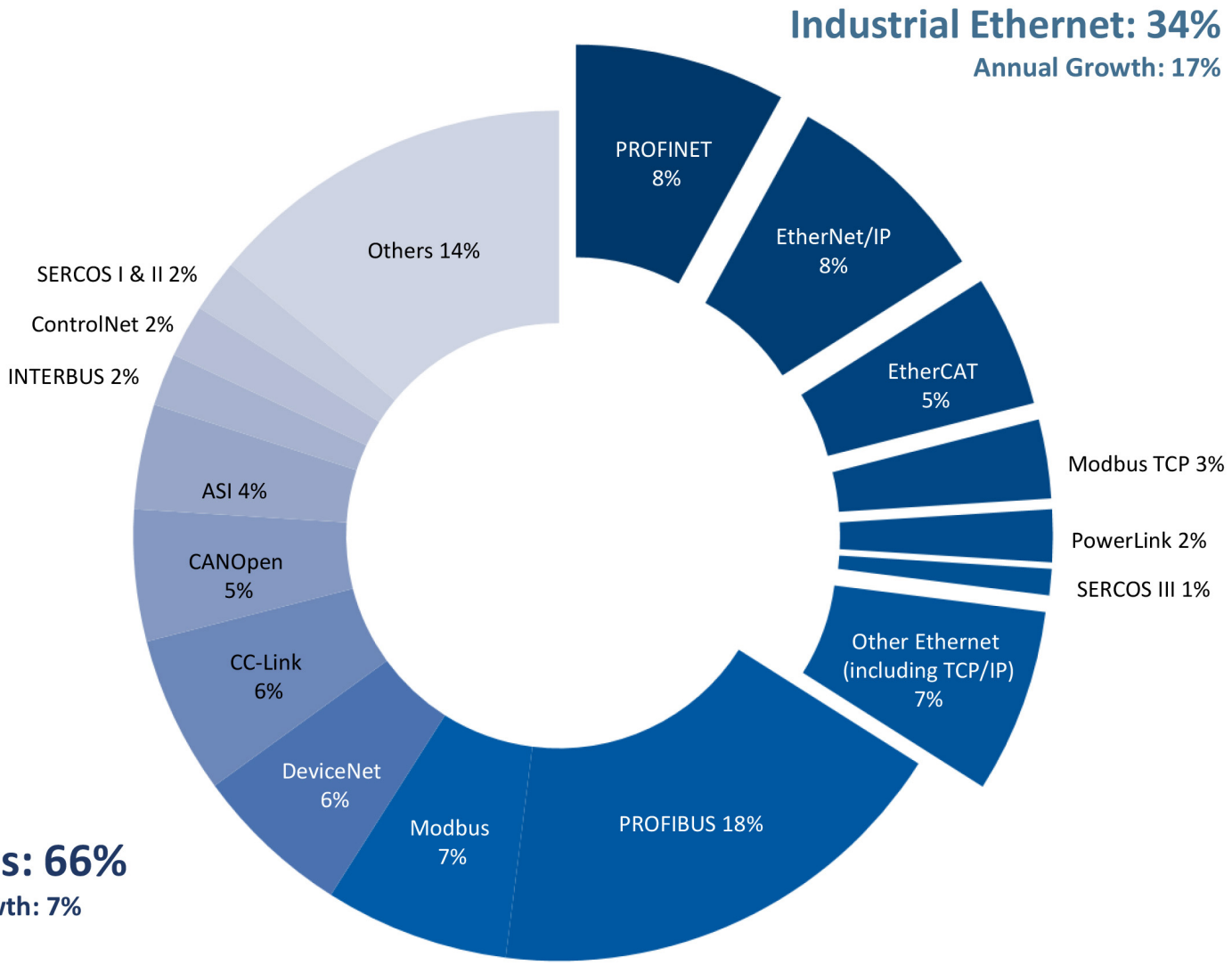


http://j.mp/TSPScada (or google+“legoscada”)

SCADA Protocols (non exhaustive list)

- **Siemens quad 4 meter**
- **CONITEL 2000**
- **CONITEL 2100**
- **CONITEL 3000**
- **CONITEL 300**
- **HARRIS 5000**
- **HARRIS 5600**
- **HARRIS 6000**
- **UCA 2.0 or MMS**
- **PG & E 2179**
- **MODBUS**
- **DNP3**
- **IEC 61850**
- **…**

Fieldbus vs. Industrial Ethernet



Source: HMS Industrial Networks

SCADA Protocols (non exhaustive list)

- Siemens quad 4 meter
- CONITEL 2000
- CONITEL 2100
- CONITEL 3000
- CONITEL 300
- HARRIS 5000
- HARRIS 5600
- HARRIS 6000
- UCA 2.0 or MMS
- PG & E 2179
- **MODBUS**
- **DNP3**
- IEC 61850
- …

Few existing general protocols

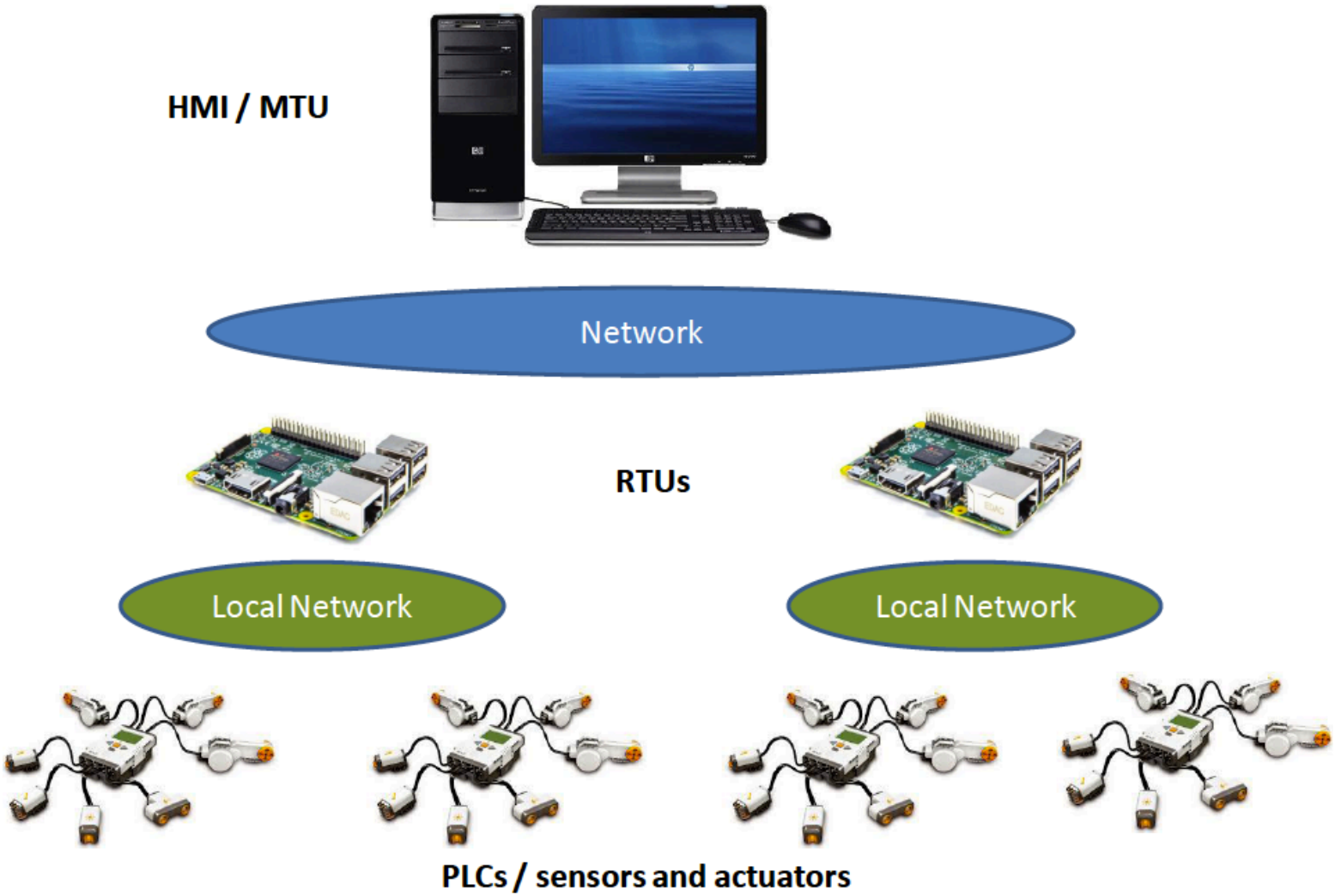
- MODBUS - Primitive with no security and not very extensible
- DNP3 - Advanced SCADA protocol
  - DNP1 and 2 are proprietary protocols

MODBUS

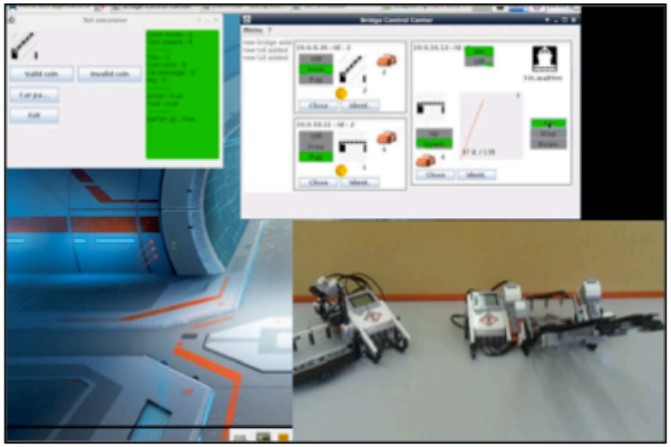
- Standardized communication protocol used by many SCADA systems around the globe
- Used to communicate with Remote Terminal Units (RTUs)
- Values stored in memory registers, organized as:

  - Input Registers: analog inputs of different types (e.g. voltage, amperage)
  - Input Status: digital input used to represent dichotomous values (e.g. electrical breakers, switches)
  - Coil Status: digital output used to switch voltage in a relay (e.g. switch power ON/OFF to field device)
  - Holding Registers: store additional data the can be used by other devices; less commonly used

Preparing the Testbeds

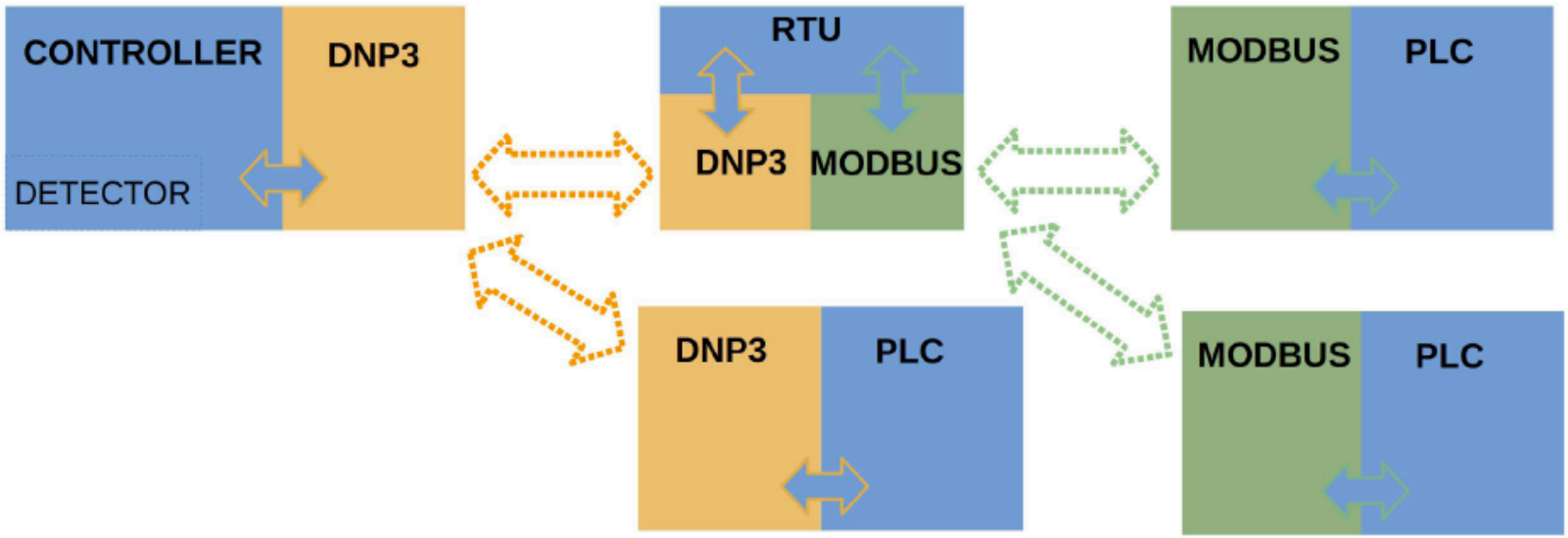


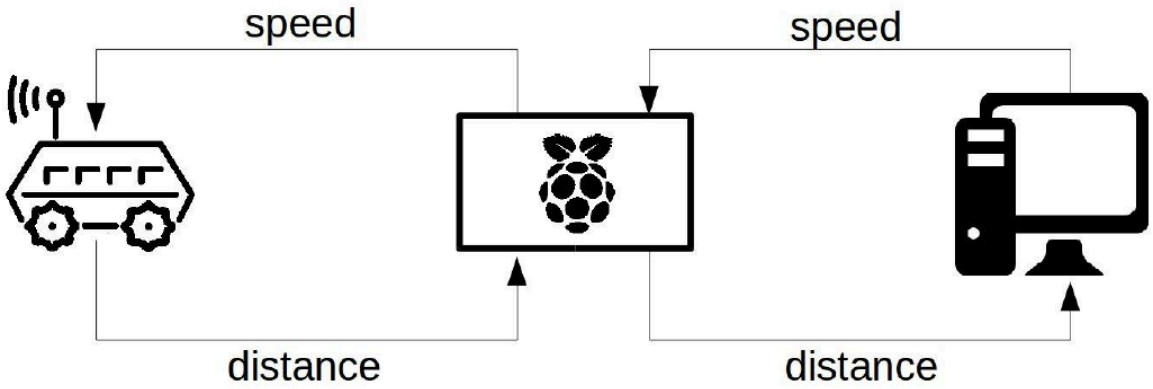
Sample Testbeds



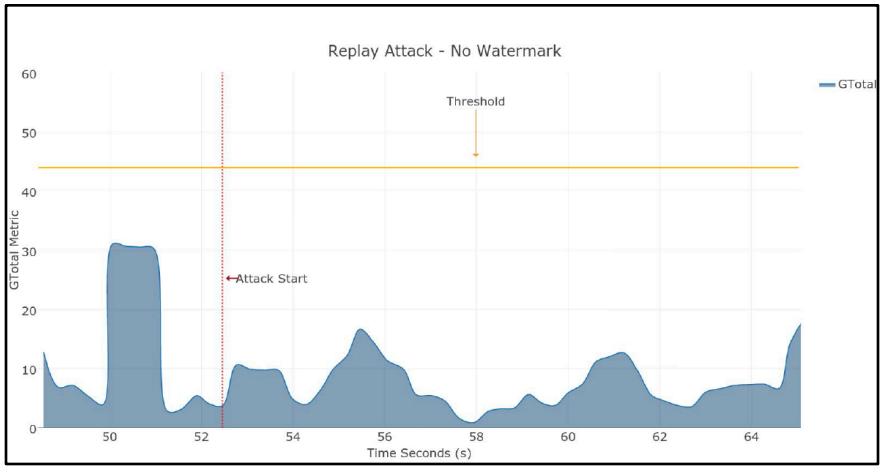
http://j.mp/TSPScada

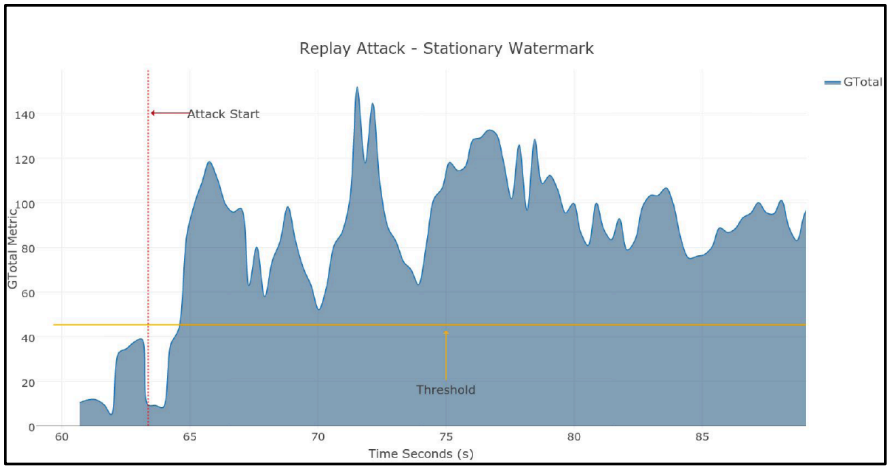
Testbed Validation

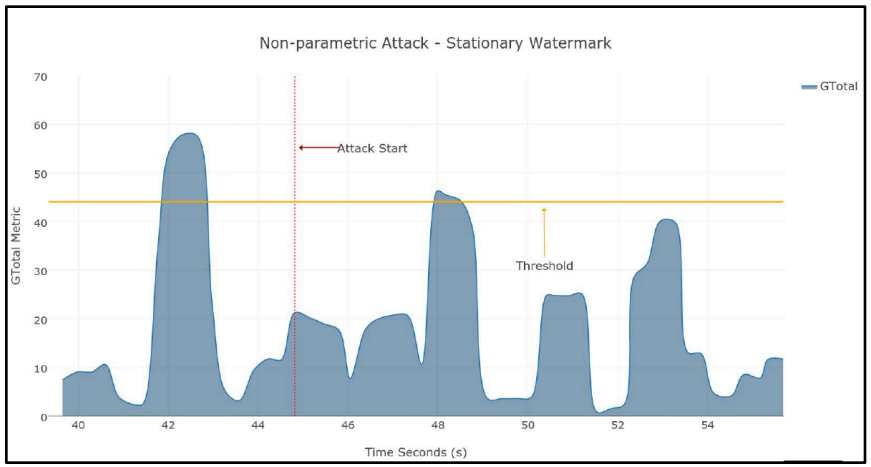


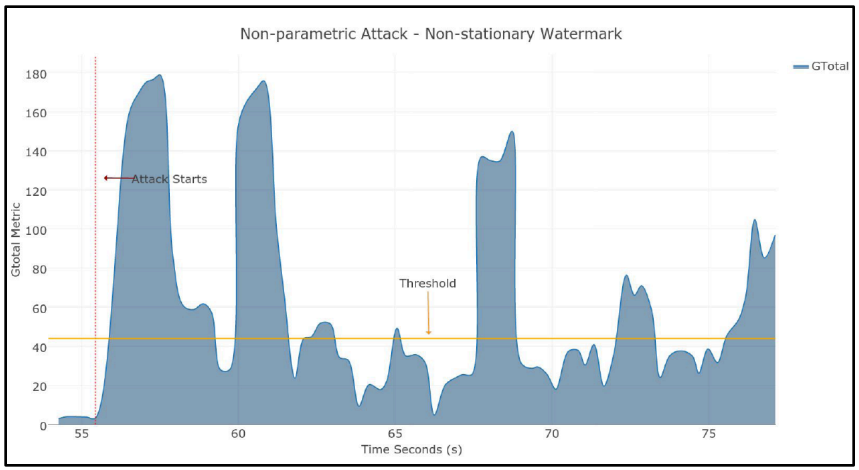


Testbed Results

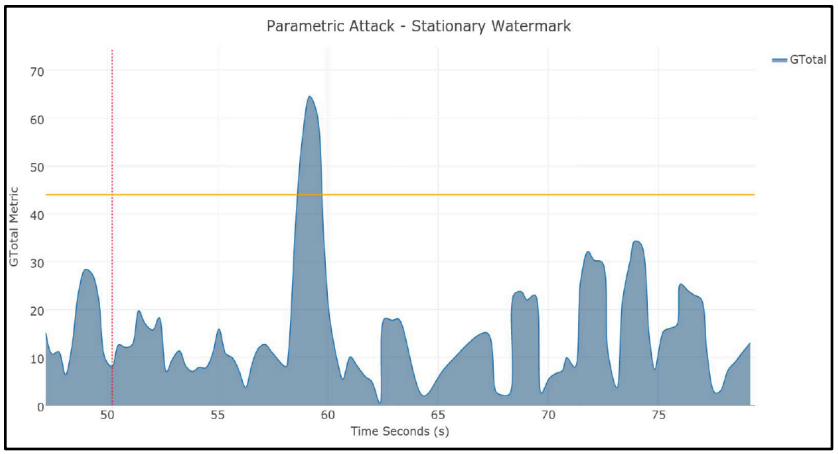


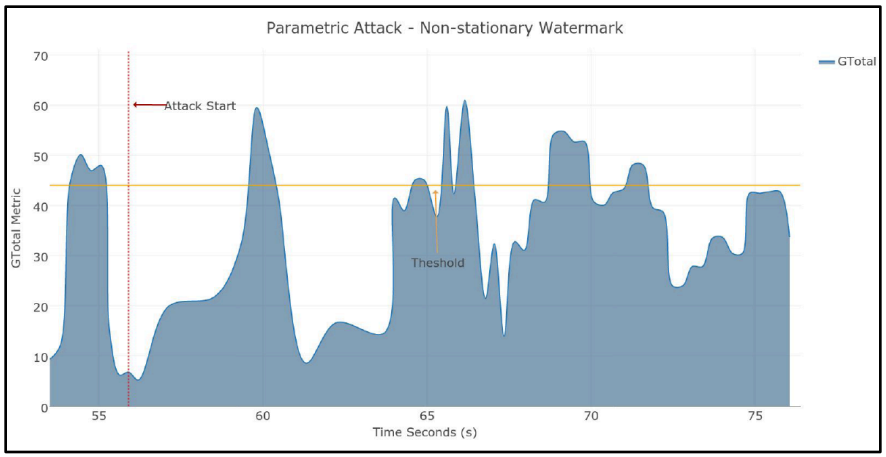






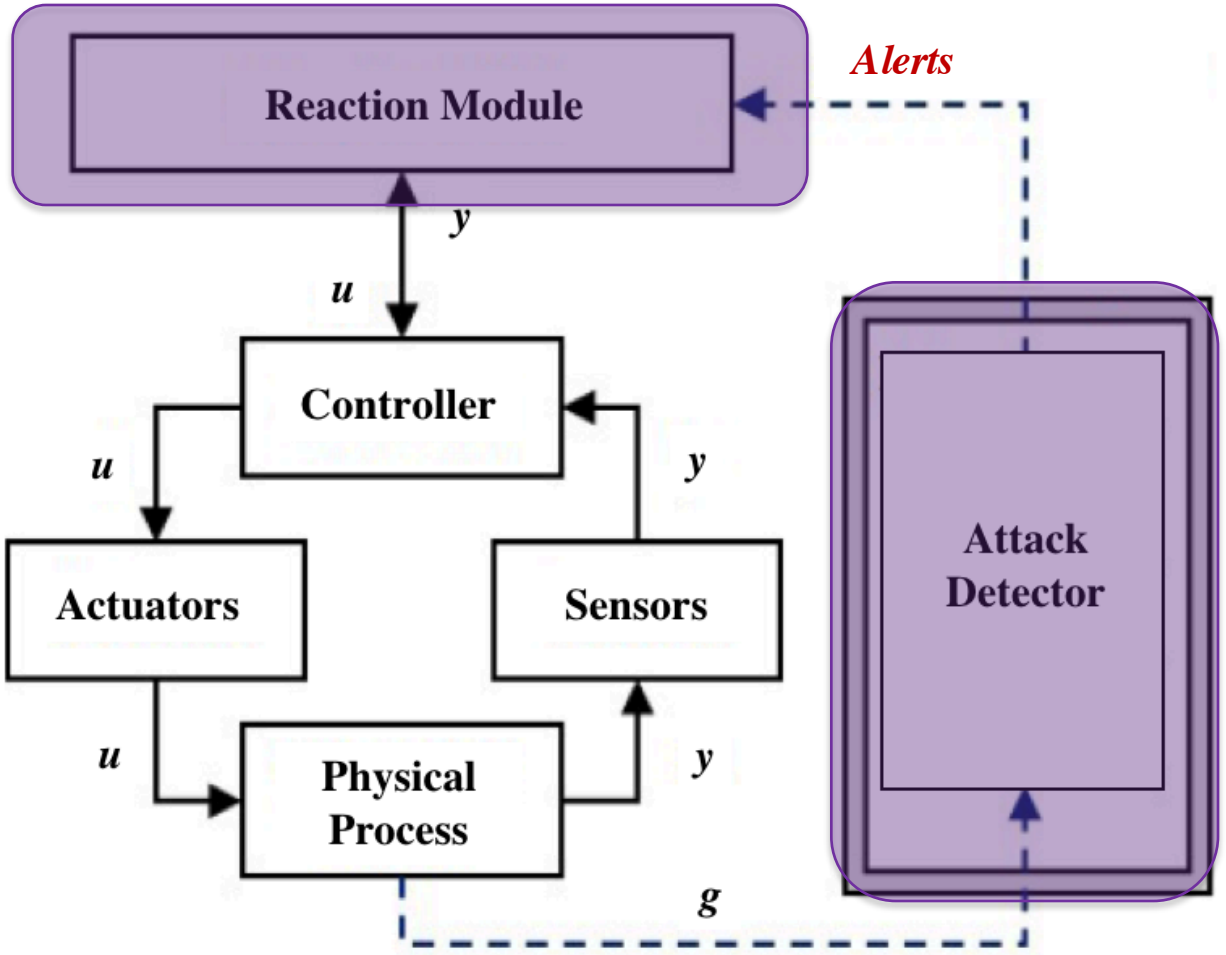
Testbed Results



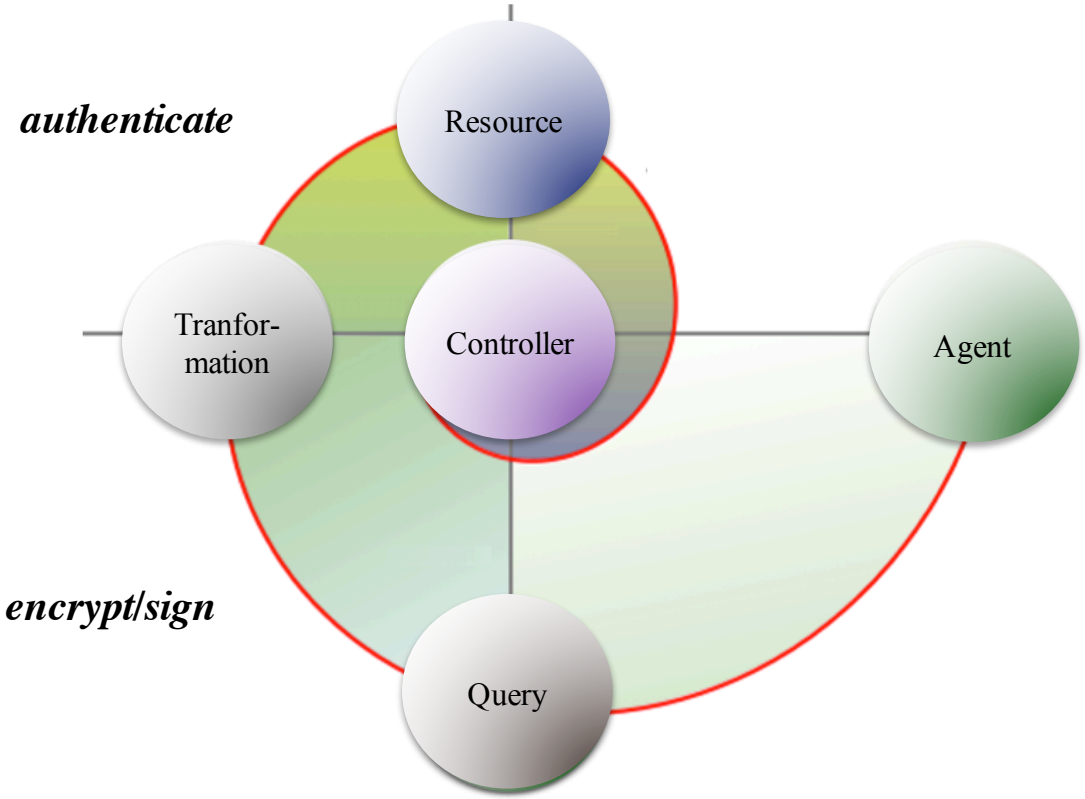


	Replay Attack	FIR Adaptive Attack (Non-parametric Attack)	Parametric Attack
True Positives	35.94%	14.80%	11.37%
False Negatives	64.06%	85.20%	88.63%
False Positives	0.98%	1.66%	1.35%

Reaction After Detection (1/2)



Reaction After Detection (2/2)



Plan

- Contexte
- Systèmes cyber-physiques
- Véracité du feedback
- **Synthèse & perspectives**

Synthèse

- Sujet multidisciplinaire, avec plein de défis & enjeux
  - Systèmes contrôlés en réseau & analyse de grands ensembles de données
- Évaluation des risques
  - SSI traditionnelle peut encore être applicable ...
  - ... mais ne peut pas résoudre complètement le problème
    - Différences fondamentales entre SI & CPS en terme de sécurité
- Notre approche :
  - Formalisation, expérimentation et évaluation à base de modèles (attaques, contremesures, politiques, ...)
  - Banc de test pour mettre en place les modèles, expérimenter avec eux, et vérifier les résultats
  - Modélisation, défi-réponse, avec théorie du contrôle & systèmes LTI

Merci. Questions ?

Références

- Hirschmann. Why is Cyber Security Still a Problem? *TOFINO Security Series, 2010*
- Kim & Kumar. Cyber–Physical Systems: A Perspective at the Centennial. *Proceedings of the IEEE*, Vol. 100, pages 1287-1308, May 2012.
- Krotofil & Larsen. Hacking Chemical Plants for Competition and Extortion, *DefCon23, 2015*
- Texeira et al. A secure control framework for resource-limited adversaries. *Automatica*, 51(1):135-148, 2015.
- Wu, Sun & Chen. A survey on the security of cyber-physical systems. *Control Theory and Technology*, 14(1):2–10, February 2016.
- Rubio, De Cicco, & Garcia-Alfaro. Revisiting a Watermark-based Detection Scheme to Handle Cyber-Physical Attacks. *ARES 2016*, August 2016.
- Mo, Weerakkody & Sinopoli. Physical Authentication of Control Systems. *IEEE Control Systems*, Vol. 35, pages 93–109, 2015.