Institut Mines-Télécom

TELECOM SudParis

INSTITUT Mines-Télécom

s@movar UMR 5157

CHAIR OF CYBERCNI Critical National Infrastructures

DÉTECTION DES ATTAQUES CONTRE LES SYSTÈMES CYBER-PHYSIQUES INDUSTRIELS

J. GARCIA-ALFARO

CV

http://j.mp/jgalfaro

2002 - 2006 : Ing. en informatique (Barcelone) & double doctorat en informatique (Barcelone & Rennes)

« Sécurité des Systèmes d'Information (SSI) »

2007 - 2009 : Postdoc, *CaixaBank Award*, CarletonU (Ottawa)

« Sécurité des réseaux sans fils (EM/RF-, O- & A-comms) »

2009 - 2012 : Chercheur à IMT Atlantique, Futur & Ruptures (Rennes)

« Sécurité réseaux spontanés & systèmes RFID »

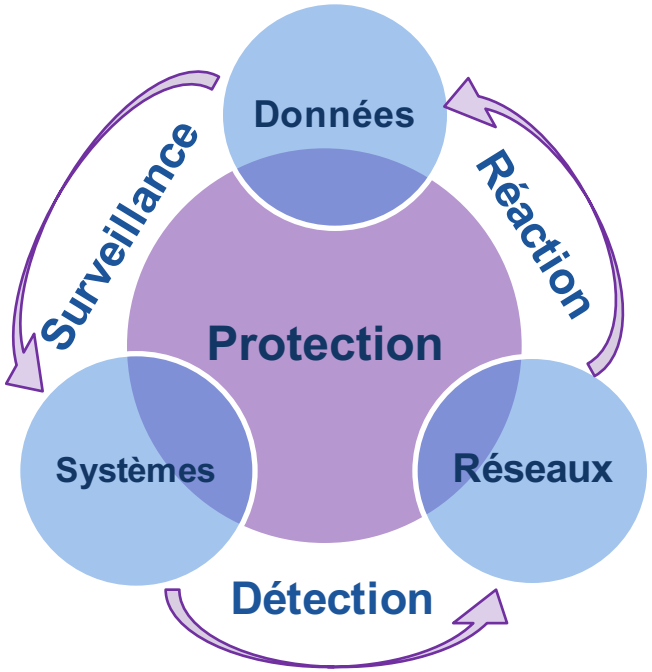
Depuis 2013 : Télécom SudParis, sécurité des infrastructures critiques

HDR (2013), senior IEEE/ACM (2014), Qualif. Prof., sec. 27 (2015), Prof. IMT (2016)

RECHERCHE

- **Equipe R3S, UMR 5157/CNRS SAMOVAR**
  - Réseaux, Systèmes, Services, *Sécurité*

- **« Sécurité des infrastructures critiques »**
  - Problèmes de protection posés par les systèmes cyber-physiques



PROTECTION INDUSTRIE 4.0

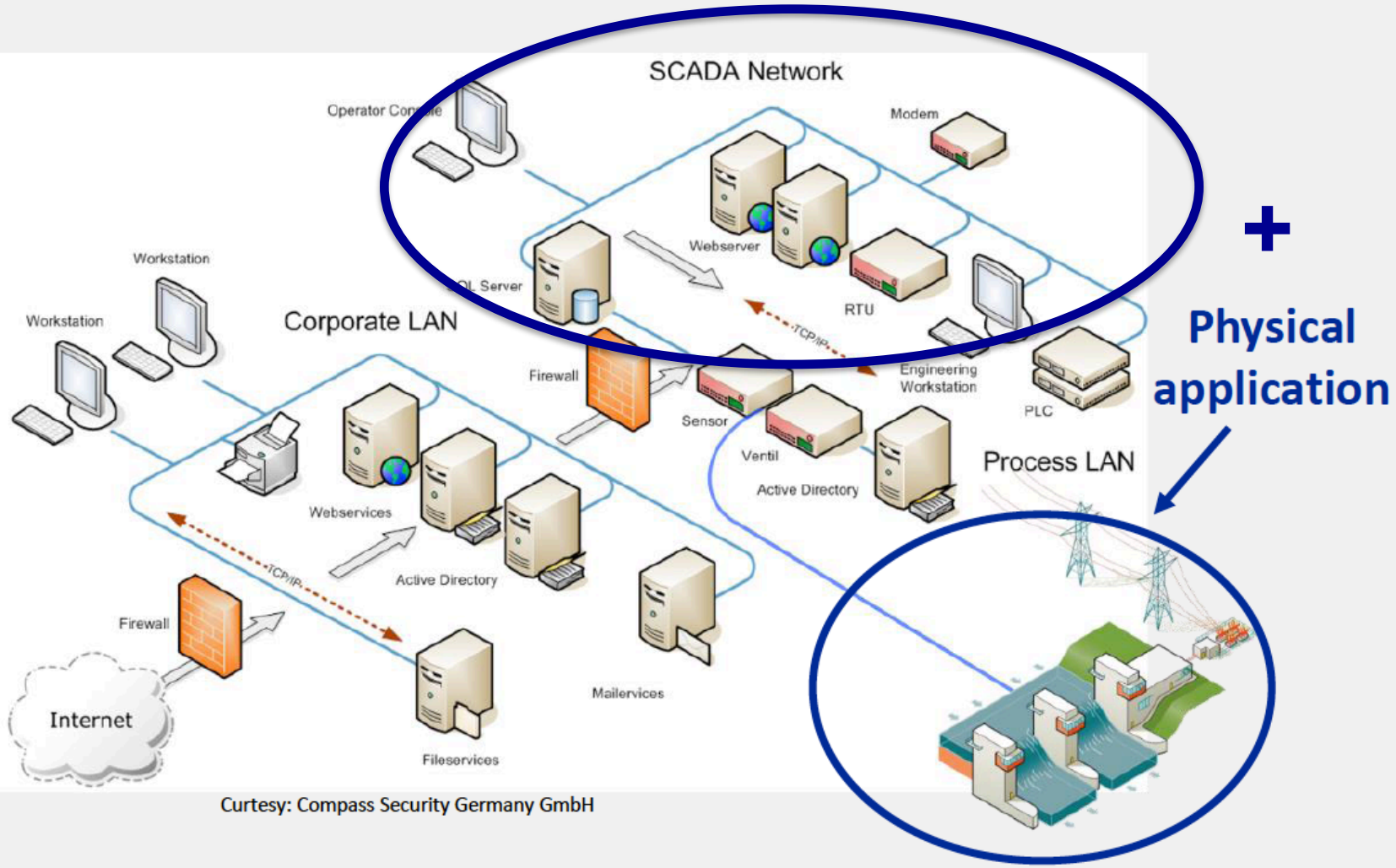
SYSTÈMES CYBER-PHYSIQUES INDUSTRIELS

« Systèmes avec des éléments de calcul & comm complémentaires aux éléments physiques, qui peuvent ***interagir avec des êtres humains*** »

Sécurité ?

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

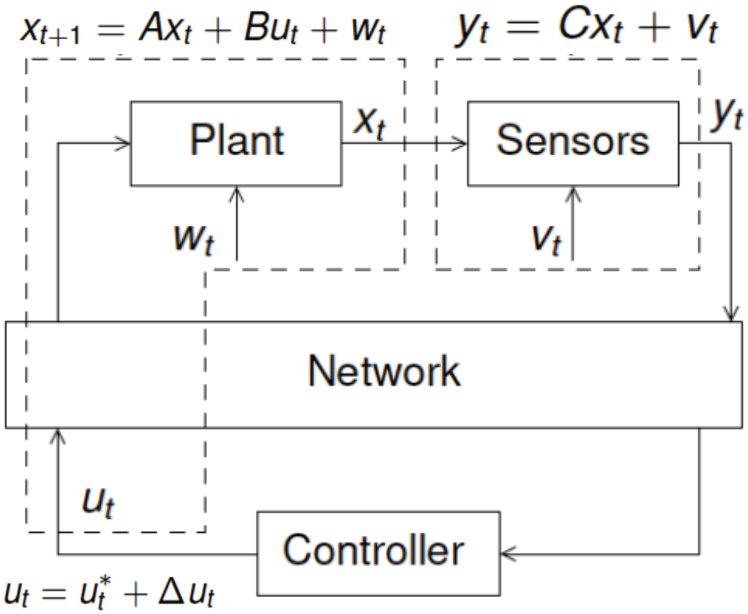
EN BREF ...



Source: *Hacking Chemical Plants for Competition*, Krotofil and Larsen, DefCon23, 2015.

SURVEILLANCE ET DÉTECTION [*]

Exemple : Protection parmi des approches **défi-réponse**



- **Pseudo-signature canaux contrôle** (modification imperceptible des messages envoyés par le contrôler)
  - Modèles LTI (*linéaires invariants dans le temps*)
- Défi : u_t ; Réponse : y_t
- Analyse statistique entre défi et réponse :

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

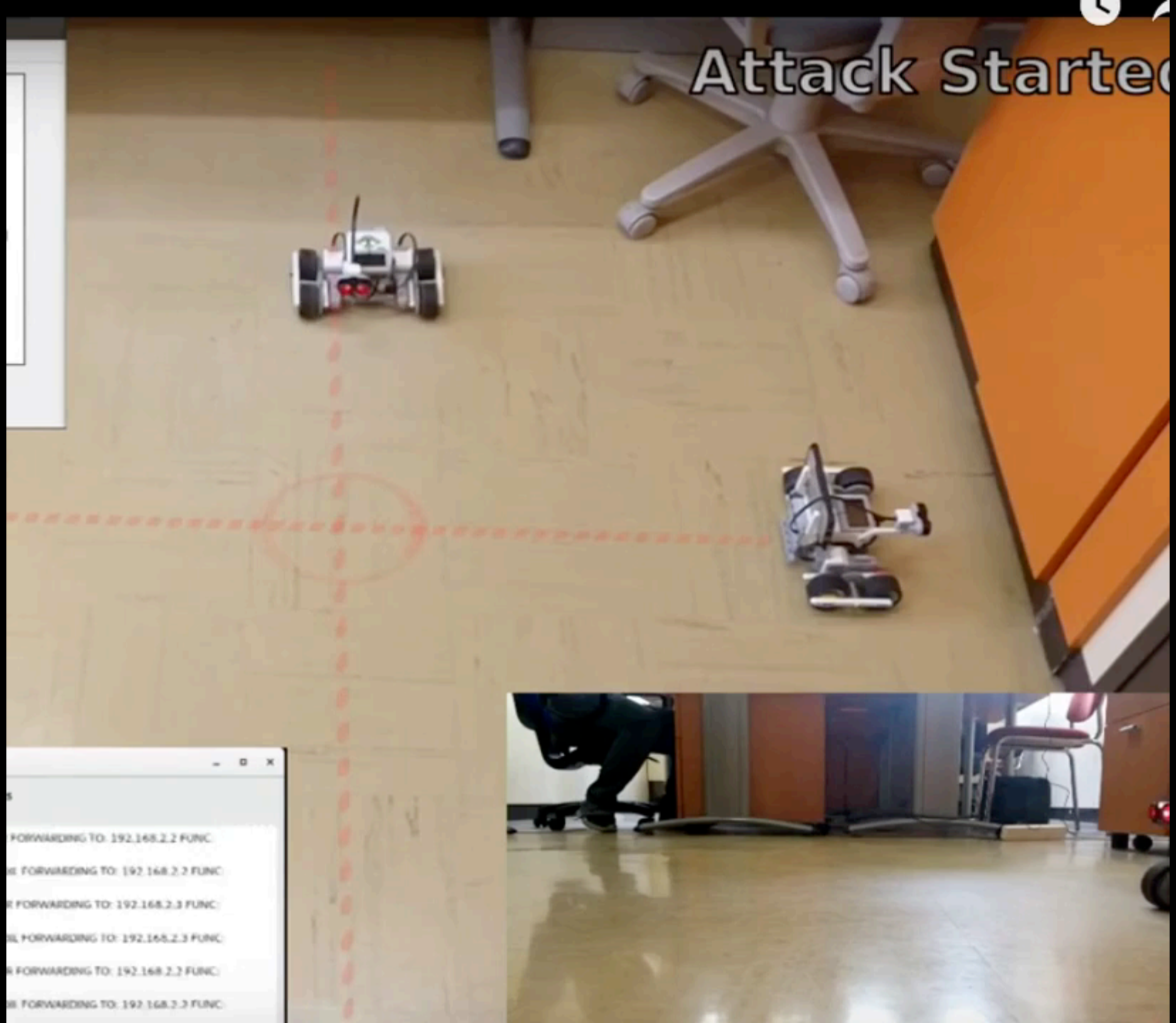
- **Si g_t dépasse un certain seuil ⇝ alerte**

[*] Rubio, De Cicco, Garcia. « Cyber-Physical Attacks & Watermark-based Detection », *11th Intl. ARES Conference*, ***Best Paper Award***, Aug 2016 ; & **Trans. Emerging Tel. Tech.,** DOI: 10.1002/ett, 2017

APPROCHE

- **Formalisation, expérimentation et évaluation**
  - Banc de test pour mettre en place les modèles, expérimenter avec eux, et vérifier les résultats
- **Plateforme Chaire CNI & THDsec**

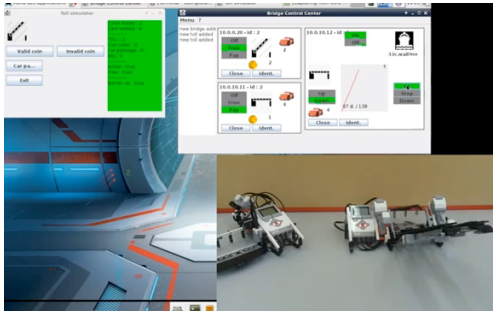
http://j.mp/TSPScada


Attack Started
FORWARDING TO: 192.168.2.2 FUNC
FORWARDING TO: 192.168.2.3 FUNC
FORWARDING TO: 192.168.2.3 FUNC
FORWARDING TO: 192.168.2.3 FUNC
FORWARDING TO: 192.168.2.2 FUNC
FORWARDING TO: 192.168.2.3 FUNC

APPROCHE

- **Formalisation, expérimentation et évaluation**
  - Banc de test pour mettre en place les modèles, expérimenter avec eux, et vérifier les résultats

- **Plateforme Chaire CNI & THDsec**



http://j.mp/TSPScada

CYBER-SÉCURITÉ

LA PLATEFORME POUR
la sécurité des infrastructures connectées

TELECOM SudParis

http://j.mp/THDsec

SYNTHÈSE

Plein de défis & enjeux

- Contrôle réseau & analyse de grands ensembles de données

Évaluation des risques

- SSI traditionnelle encore applicable ...
- ... mais ne peut pas résoudre le problème
- Différences fondamentales entre SI & SO en terme de sécurité

Notre approche

- Formalisation à base de modèles (attaques & contremesures)
- Banc de test pour expérimenter et vérifier les résultats

Perspectives

- cyber-résilience & redondance ⇝ tolérance aux attaques cyber-physiques

REFERENCES

- 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.