Date 07/02/2023

Défi 04: Cyber-sécurisation « by design » de systèmes cyber-physiques

Groupe de travail défi 04

Sébastien Dupont, Guillaume Ginis - CETIC
Sereysethy Touch - UNamur
Doha Ouardi - UNamur
Jean-Michel Dricot - ULB
Benoît Duhoux - UCL

https://cyberwal.be
https://cyberexcellence.be

Agenda

Introduction

Research challenges

- ASGARD An Adaptive Self-guarded Honeypot
- Co-Simulation edge-cloud
- Cyber Range Scenarios
- Coordination-based Process Algebra for Security
- Vacsine - Adaptive continuous security orchestration for Cloud/Edge

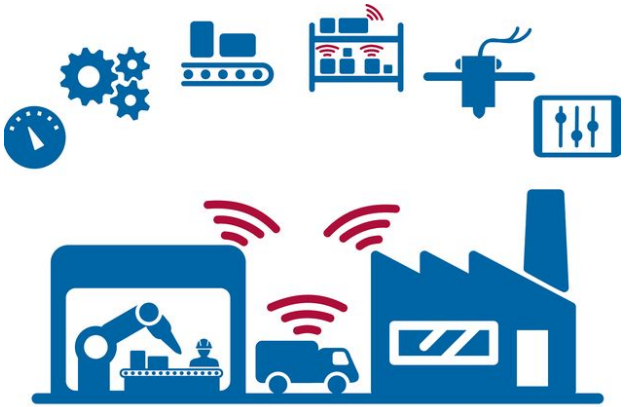
Case study

Next steps

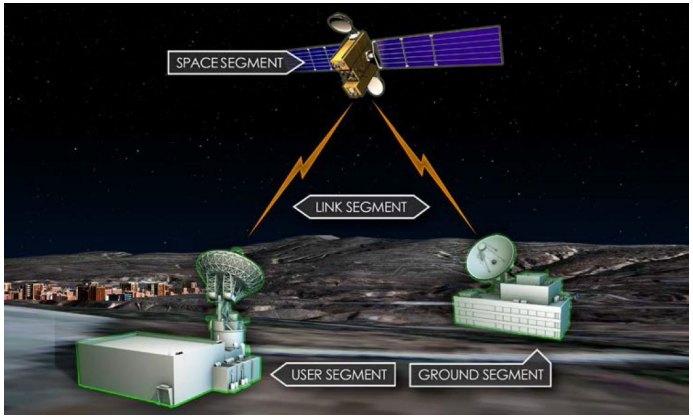
Défi 04 : Cyber-sécurisation « by design » de systèmes cyber-physiques

Résumé du défi

- Domaines: **Industrie 4.0** & **espace**
- **Cyber Physical System** = système intelligent incorporant des réseaux de composants logiciels et physiques qui interagissent entre eux (**edge**)
- besoin d'une plus grande **puissance de calcul déportée**
- accroissement des **communications** nécessaires entre ces composants ou avec une partie centrale
- Nécessite une haute **tolérance** aux pannes, facilité de **mise à jour**



ENISA - Cybersecurity is a key enabler for Industry 4.0 adoption

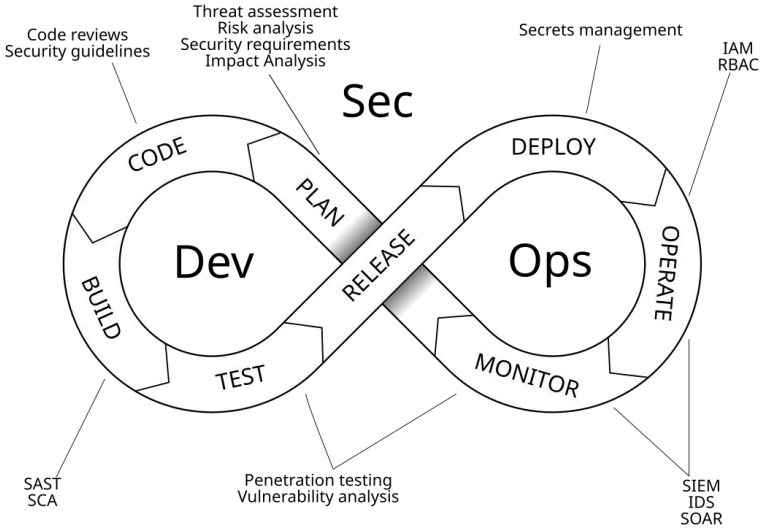


Bailey, B., et al. « Defending spacecraft in the cyber domain. » Aerospace Corp. TR OTR202000016, El Segundo, CA (2019).

Défi 04 : Cyber-sécurisation « by design » de systèmes cyber-physiques

Challenges de recherche:

- Etudier l'application de méthodes et outils en tenant compte des spécificités de ces domaines
- Démontrer le succès de l'approche DevSecOps
- Sécurité « By Design »
- Sécuriser en profondeur - modèle « zero trust »
- Minimiser et visibilité de la surface d'attaque
- Eviter la sécurité par l'obscurité
- Rester simple, assessment vs certification
- CNSSI 1200, CCSDS 35X.0-B, NIST CSF, ISA/IEC - 62443 ou FDAM



Impact:

- Détecter les vulnérabilités au plus tôt
  - minimiser leur impact pour **réduire le risque**
  - DevSecOps = qualité + sécurité + vitesse
- Convergence entre l'IT et l'OT
  - unifier le **contrôle et la surveillance** pour faciliter la gestion de la sécurité (**edge**)

Défi 04 : Cyber-sécurisation « by design » de systèmes cyber-physiques

Problèmes de recherche

- An Adaptive Self-guarded Honeypot (UNamur)
- IoT Security (ULB)
- Cyber Range Scenarios (UCL)
- Coordination-based Process Algebra for Security (UNamur)
- Vacsine - Adaptive continuous security orchestration for Cloud/Edge (CETIC)
- ...

Expérimentation dans la factory

- Déploiement d'un système à sécuriser dans une sandbox de la CYBER Factory
- Etude de cas :
  - systèmes autonomes connectés (Robots, edge) + gestion (Cloud)
  - Introduction de vulnérabilités

Acteurs industriels

Eric Viseur, Thales
System Engineer

Vincent Boucher, B12 Consulting
Managing partner

Tom Selleslagh, Stratos Solutions
Acquisition et traitement de données aériennes de haute précision

Gordan Ristic, NSI SA
Team Leader Network & Security

Sebastien Chaumat, Dekimo
Open source IT Architect

2. Problèmes de recherche

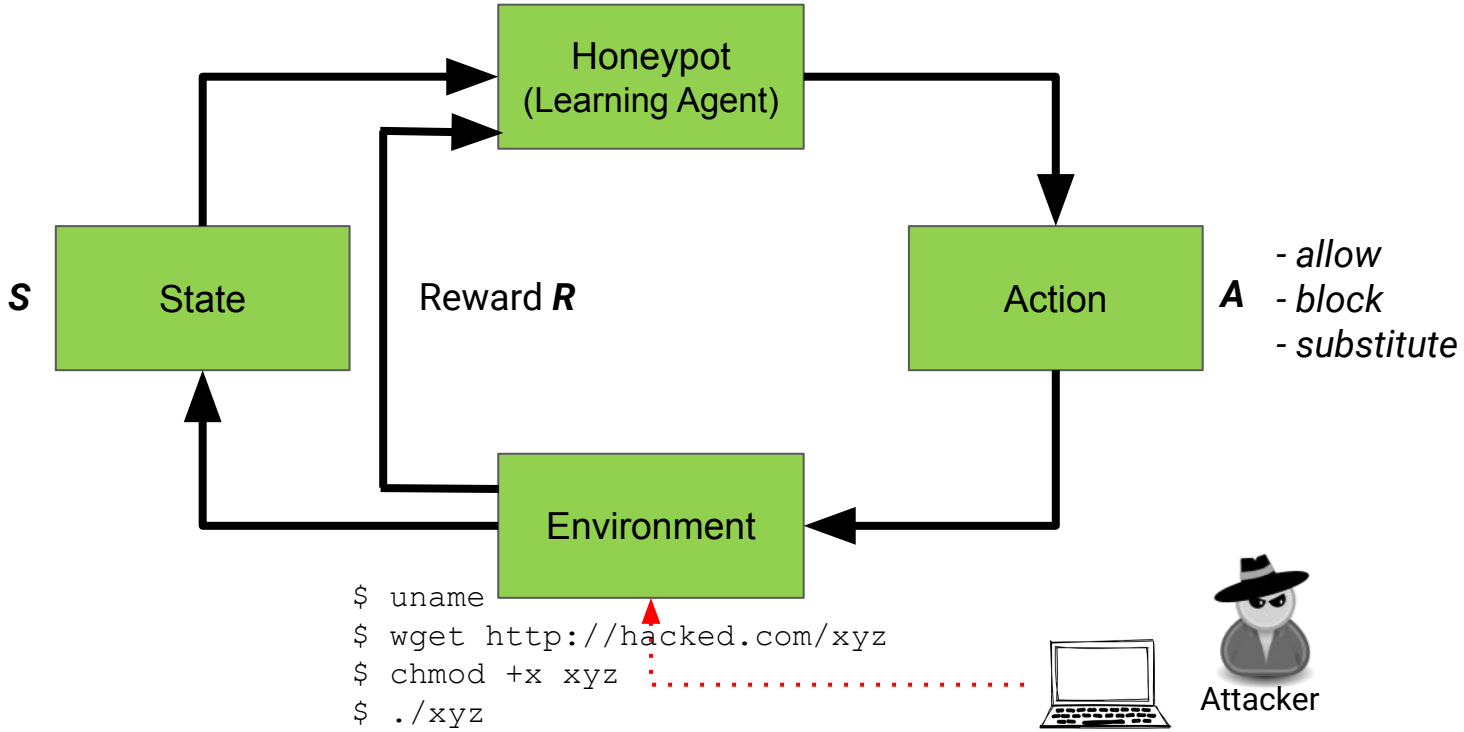
ASGARD - An Adaptive Self-guarded Honeypot

S. Touch, UNamur

Adaptive (smart) honeypot:

- Interact with the attackers to collect their tools
- Defend itself from being deeply compromised

Our approach: a honeypot as a RL agent



Cyber range scenarios

B. Duhoux, UCLouvain

Virtual training ground

for security experts

Cyber Range Scenarios

Set of hardware components, network topologies, software systems with a specific version that contain vulnerabilities

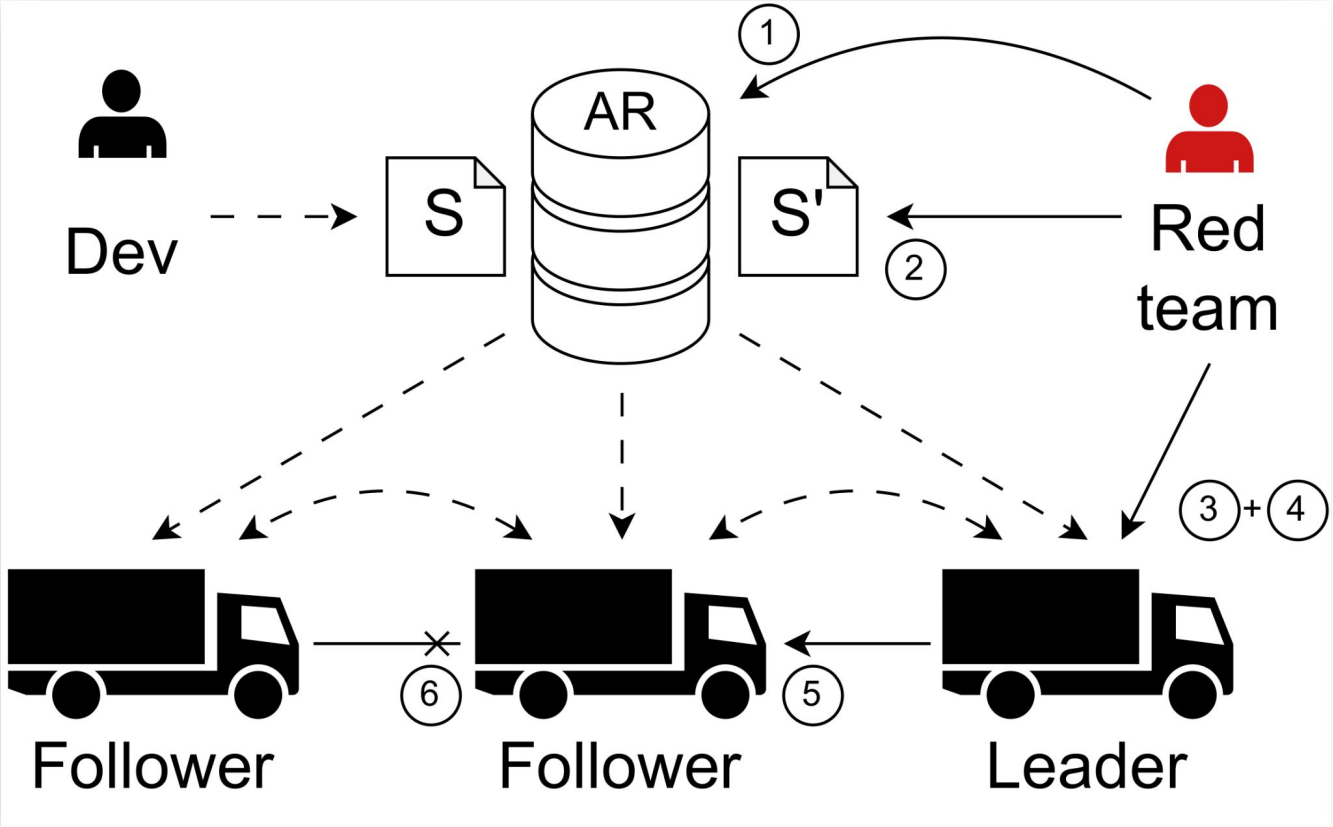
The manual creation of scenarios including contextual information has several disadvantages:

- Need experts,
- time-consuming,
- not really reusable.

⇒ So we need a semi-automatic solution to facilitate the work of CRS designers / engineers.

Sécurisation by design de systèmes cyber-physiques

Cyber range scenarios

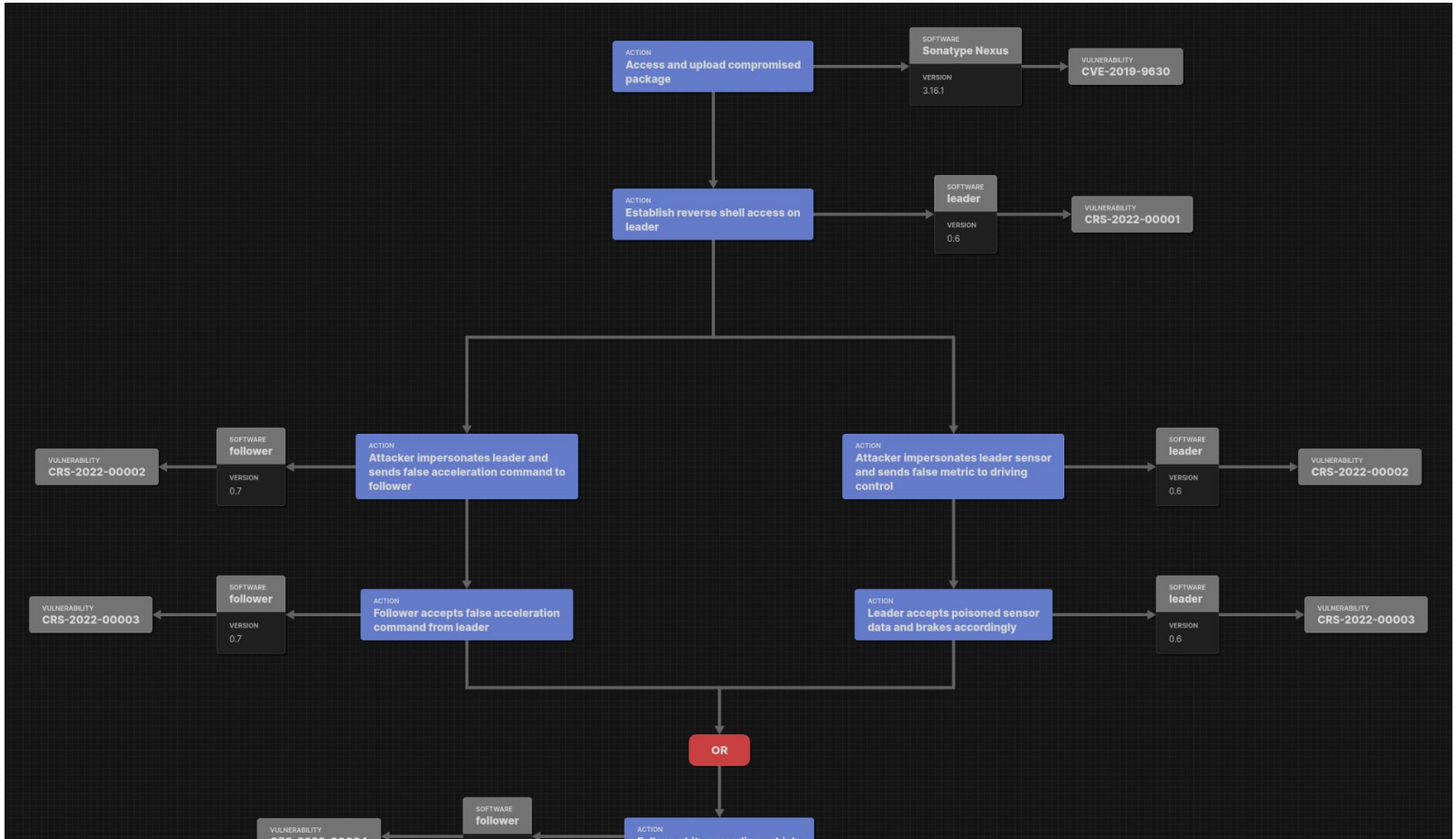


Sécurisation by design de systèmes cyber-physiques

Cyber range scenarios

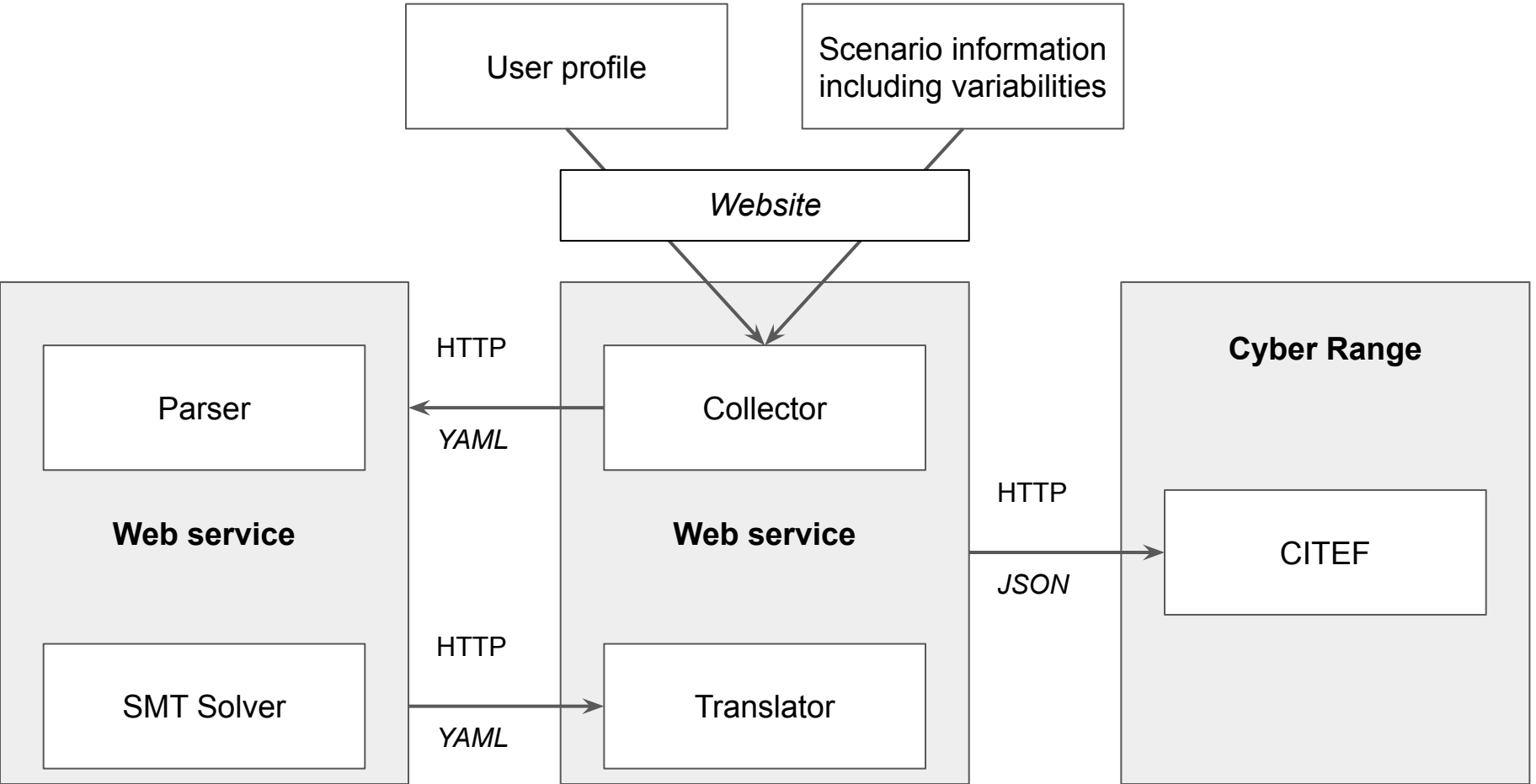
UCLouvain

digital wallonia cyberwal



Sécurisation by design de systèmes cyber-physiques

Cyber range scenarios



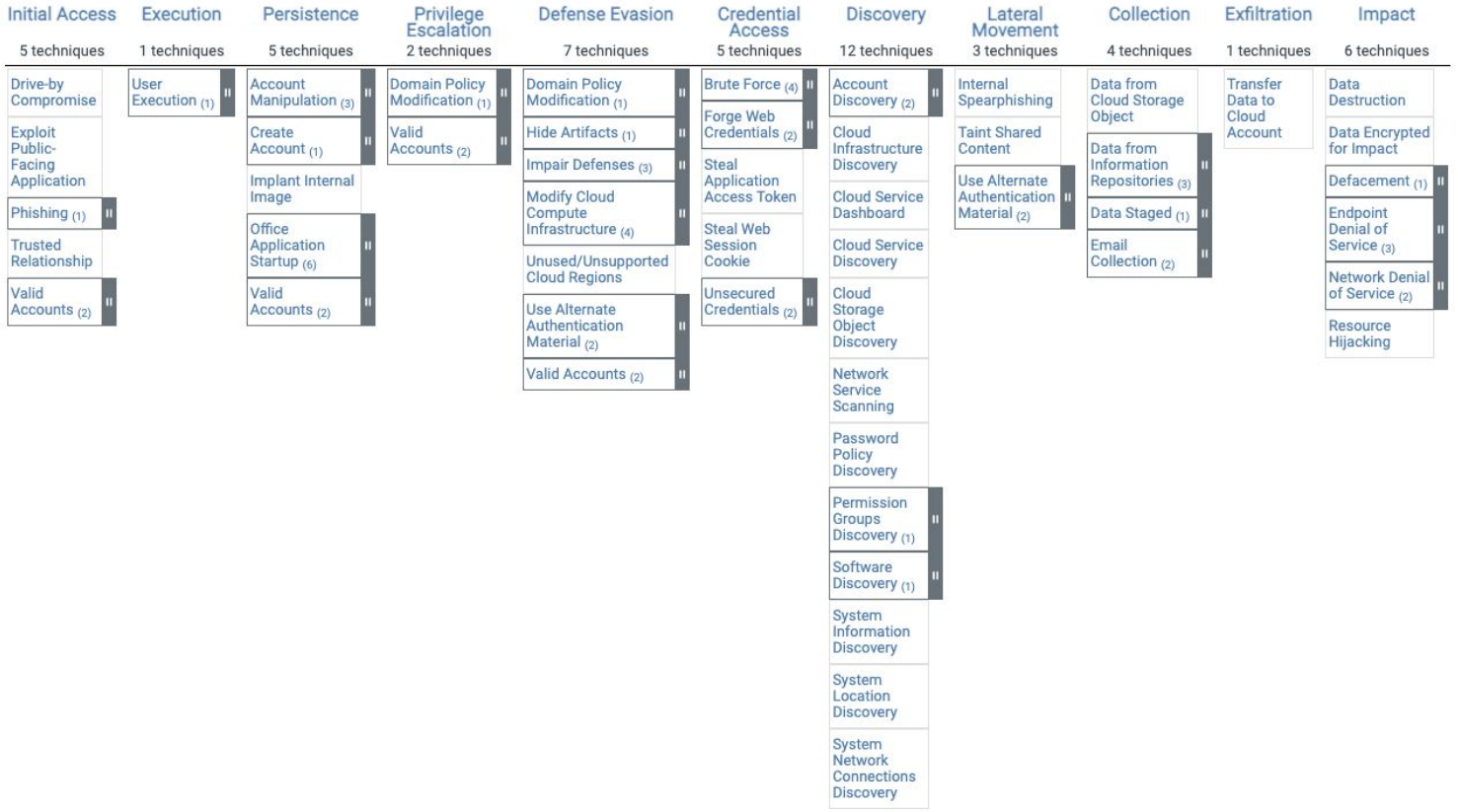
Sécurisation by design de systèmes cyber-physiques

Cyber range scenarios

UCLouvain

digital wallonia cyberwal

MITRE ATT&CK™



2.4 Coordination-based Process Algebra for Security

D. Ouardi, UNamur

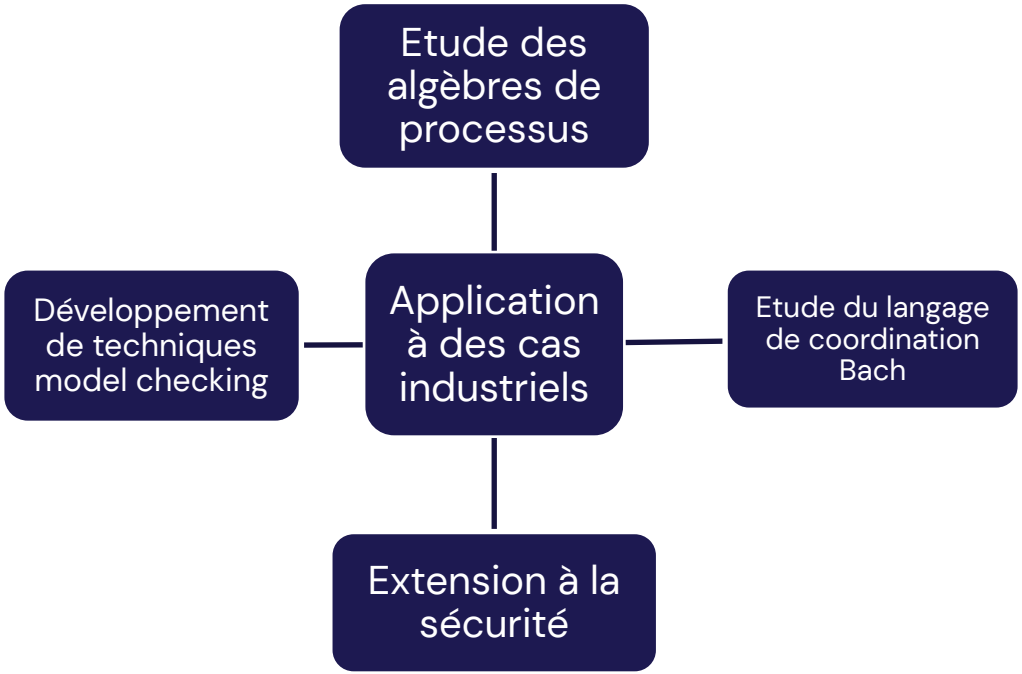
Sécurisation by design de systèmes cyber-physiques

2.4 Project CPA4Sec:Coordination-based Process Algebra for Security

Contexte et problématique industrielle associés au sujet de recherche

Développer des protocoles de sécurité corrects est notoirement difficile

⇒ utilisation de méthodes formelles



VACSINE - Adaptive continuous security orchestration for Cloud/Edge

S. Dupont, G. Ginis, CETIC

Sécurisation by design de systèmes cyber-physiques

Vacsine - Adaptive continuous security orchestration for Cloud/Edge

Vacsine Objectives

https://github.com/cetic/vacsine

Continuous security assessment

risk assessment to measure security response efficiency

Orchestration

Automated response testing and evaluation

Privacy

federated learning at the edge

Observability

intrusion/anomaly detection

Image ref: NIST Cyber Security Framework

IoT Security

J.M. Dricot, ULB

Sécurisation by design de systèmes cyber-physiques

IoT Security - Activités de recherche

ULB

digital wallonia cyberwal

- Sécurité des IoT
  - Protocoles et architectures
  - Device security (hardware roots of trust)
  - Design conjoint cloud-hardware

- Axes principaux actuels
  - Internet des objets
  - Smart grids Mécanismes de type edge-fog-cloud
  - Spatial (hardware sécurisé pour les nanosatellites)

- Deux thèses qui se terminent (mais sans suite)
  - [Adverserial machine learning]
  - [Smart contracts dans la blockchain]

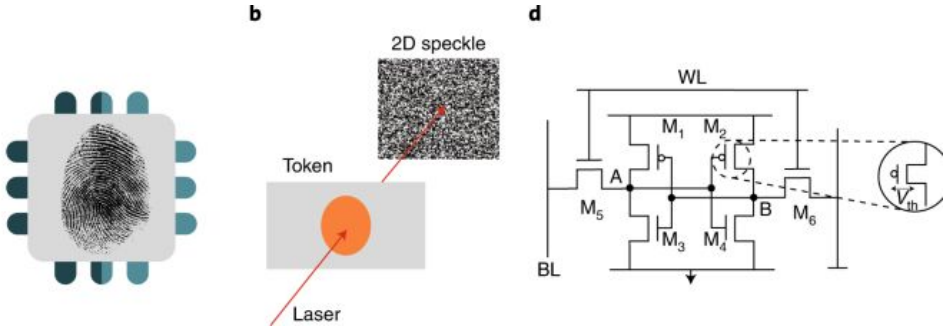
Recherche financée par la Région Wallonne

Sécurisation by design de systèmes cyber-physiques

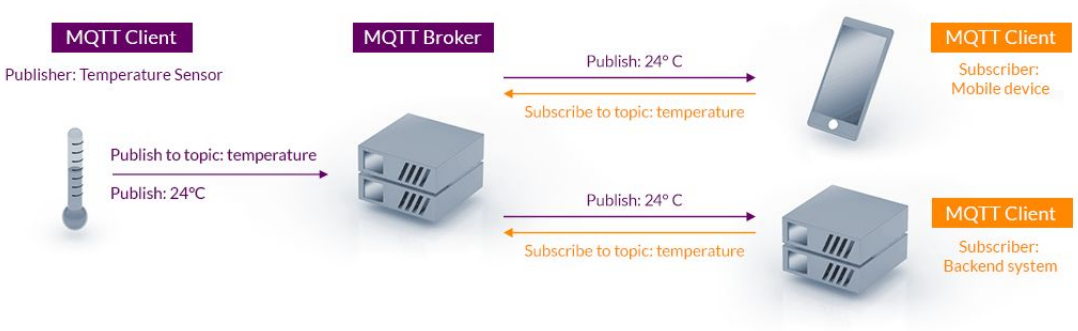
IoT Security - Activités de recherche

ULB

- Roots of trust



- Privacy by design

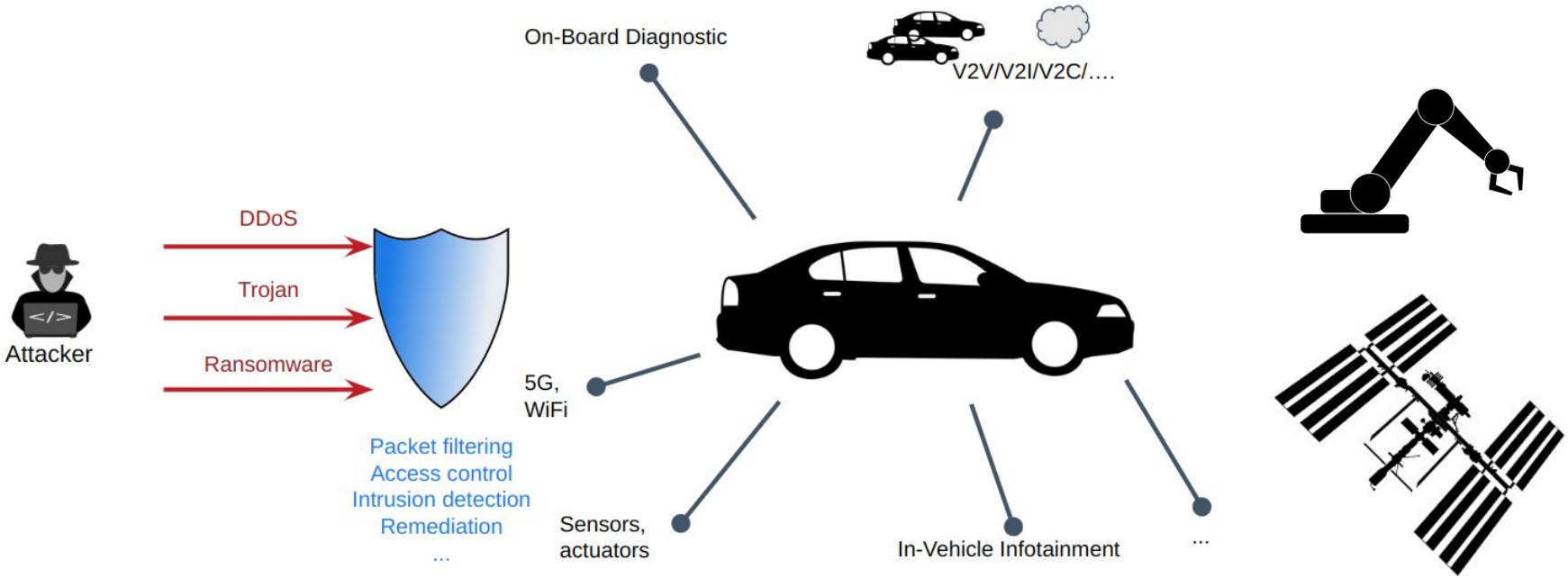


Recherche financée par la Région Wallonne

3. Etude de cas

Sécurisation by design de systèmes cyber-physiques

3. Etude de cas - sécurité CPS - Connected vehicles

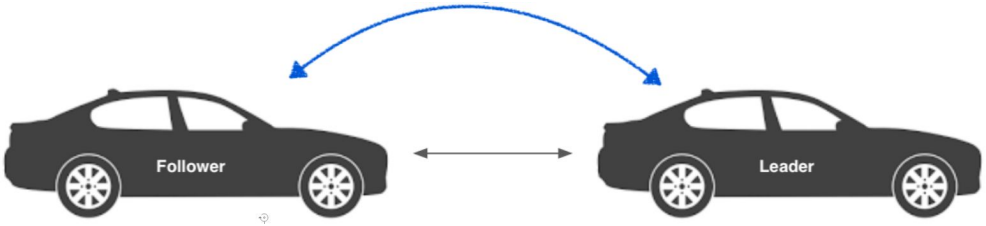


Sécurisation by design de systèmes cyber-physiques

3. Etude de cas - sécurité CPS - Connected vehicles

One **leader** vehicle is followed by N other vehicles (« **followers** »).

The vehicles can exchange information on a **V2V** (vehicle to vehicle) interface and on a **V2I** (vehicle to infrastructure) interface



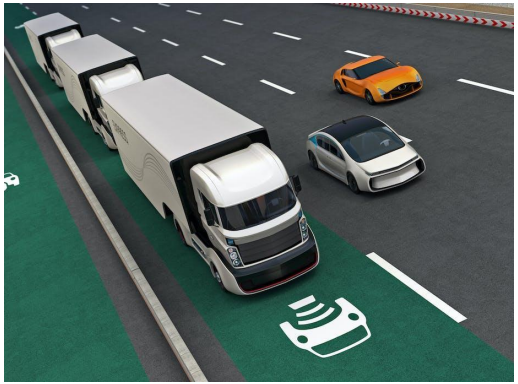
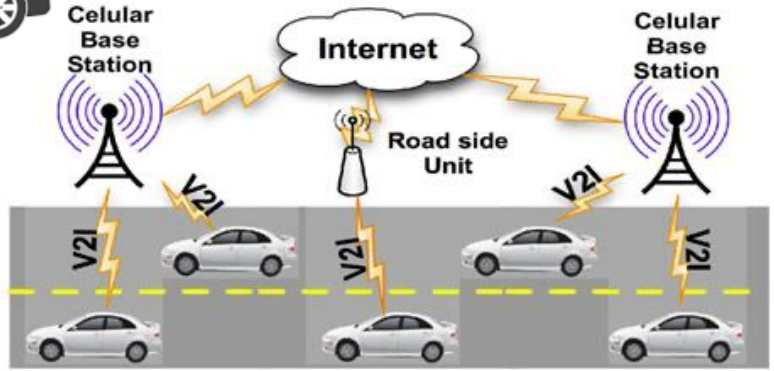


Image source: https://theconversation.com/coming-soon-to-a-highway-near-you-truck-platooning-87748

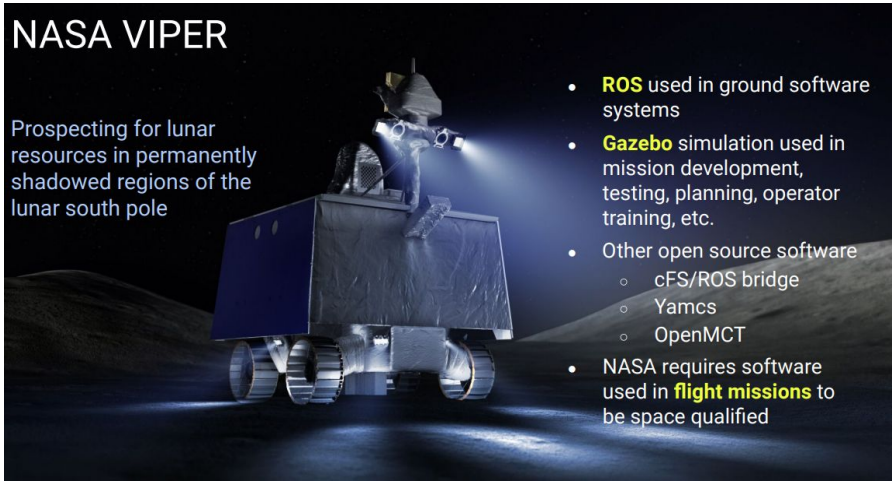


Sécurisation by design de systèmes cyber-physiques

3. Etude de cas - sécurité CPS - Connected vehicles

ROS Robot Operating System https://www.ros.org/

ROS-Industrial is an open-source project that extends the advanced capabilities of ROS to manufacturing automation and robotics.
https://rosindustrial.org



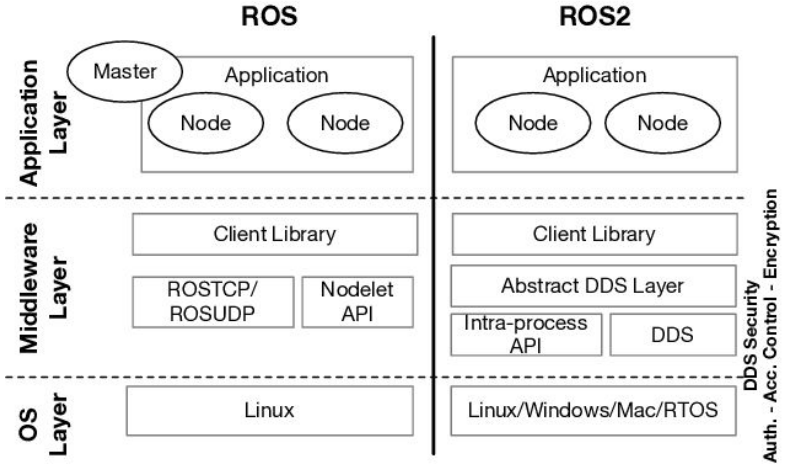
An open-source **space robotics framework** for developing fligh-quality robotics and autonomous space systems

https://space.ros.org/

Sécurisation by design de systèmes cyber-physiques

3. Etude de cas - sécurité CPS - Connected vehicles

ROS



Mazzeo, Giovanni & Staffa, Mariacarla. (2020). TROS: Protecting Humanoids ROS from Privileged Attackers. International Journal of Social Robotics. 12. 10.1007/s12369-019-00581-4.

ROS Protocol v1 :

- Publish/Subscribe mechanism with topics
- Use a master to manage communication
- **No encryption**
- **No authentication**
- Basically **No security**

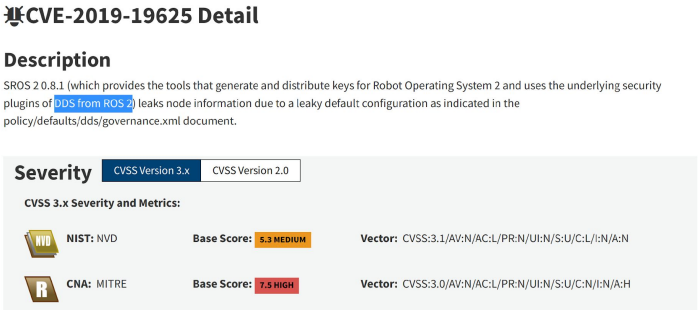
ROS2 introduces:

- security - AuthN, AuthZ, communication encryption
- real time
- distributed processing
- resilience & robustness
- ...

Sécurisation by design de systèmes cyber-physiques

3. Etude de cas - sécurité CPS - Connected vehicles

Vulnerabilities discovered on ROS2 and SROS2 (secured ROS2 variant).



CVE-2019-19625 Detail

Description

SROS 2 0.8.1 (which provides the tools that generate and distribute keys for Robot Operating System 2 and uses the underlying security plugins of DDS from ROS 2) leaks node information due to a leaky default configuration as indicated in the policy/defaults/dds/governance.xml document.

Severity CVSS Version 3.x | CVSS Version 2.0

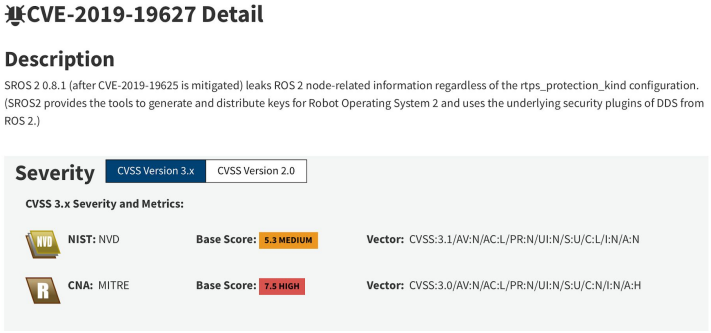
CVSS 3.x Severity and Metrics:

NIST: NVD — Base Score: 5.3 MEDIUM — Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CNA: MITRE — Base Score: 7.5 HIGH — Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

QUICK INFO

CVE Dictionary Entry:
CVE-2019-19625
NVD Published Date:
12/06/2019
NVD Last Modified:
12/13/2019
Source:
MITRE



CVE-2019-19627 Detail

Description

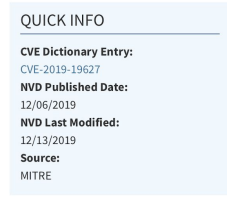
SROS 2 0.8.1 (after CVE-2019-19625 is mitigated) leaks ROS 2 node-related information regardless of the rtps_protection_kind configuration. (SROS2 provides the tools to generate and distribute keys for Robot Operating System 2 and uses the underlying security plugins of DDS from ROS 2.)

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD — Base Score: 5.3 MEDIUM — Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CNA: MITRE — Base Score: 7.5 HIGH — Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



QUICK INFO

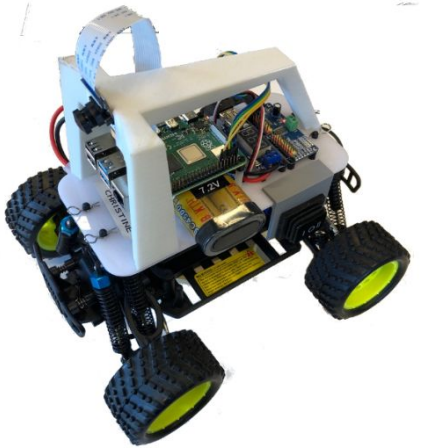
CVE Dictionary Entry:
CVE-2019-19627
NVD Published Date:
12/06/2019
NVD Last Modified:
12/13/2019
Source:
MITRE

References:

- Benhamouda, Fabrice & Lepoint, Tancrède & Loss, Julian & Orrù, Michele & Raykova, Mariana. (2022). **On the (in)Security of ROS.** Journal of Cryptology. 35. 10.1007/s00145-022-09436-0. (source)
- Deng, Gelei et al. "**On the (In)Security of Secure ROS2**." Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (2022) (source)
- Profanter, Stefan & Tekat, Ayhun & Dorofeev, Kirill & Rickert, Markus & Knoll, Alois. (2019). **OPC UA versus ROS, DDS, and MQTT: Performance Evaluation of Industry 4.0 Protocols**. 10.1109/ICIT.2019.8755050.

Sécurisation by design de systèmes cyber-physiques

3. Etude de cas - sécurité CPS - Connected vehicles

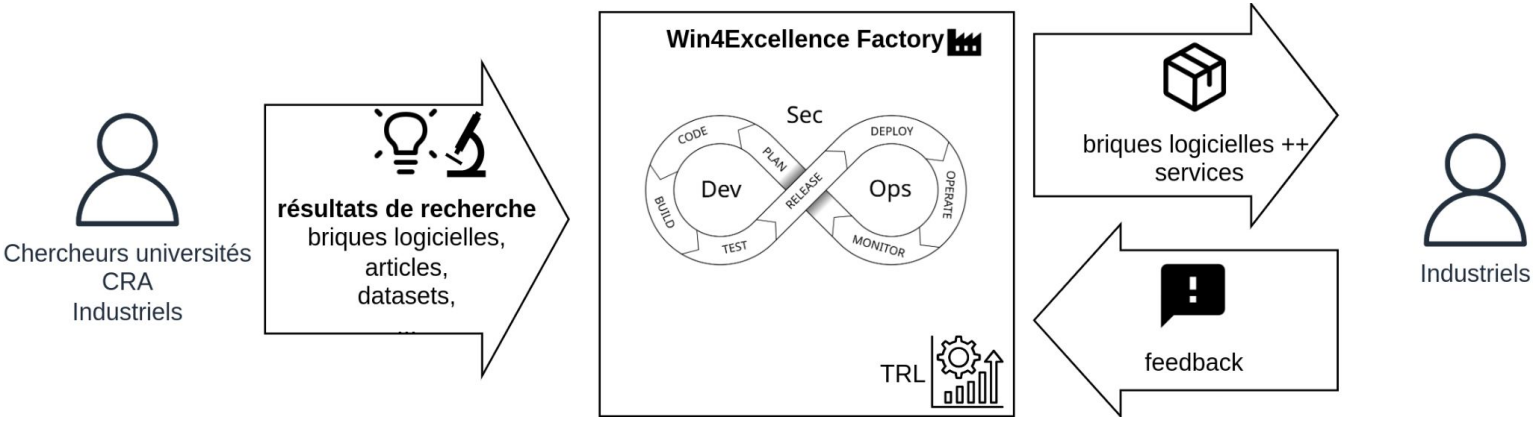


- Donkey Car chassis
- 2D Lidar
- Ultrasonic sensor
- Wide Lens camera
- RaspBerry Pi / Jetson Nano

Sécurisation by design de systèmes cyber-physiques

3. Etude de cas - sécurité CPS - Connected vehicles - CYBER FACTORY

La Win4Excellence Factory est une usine logicielle (ou *Software Factory en anglais). Cette plateforme matérielle et logicielle est utilisée sur les projets Win4Excellence pour favoriser la collaboration entre les acteurs de la recherche et de l'industrie wallons, et contribuer à la diffusion des résultats de recherche de ces projets.*



DevSecOps - increase quality, speed and security

4. Perspectives

Sécurisation by design de systèmes cyber-physiques

4. Perspectives

- **Interested ? Join us ! sebastien.dupont@cetic.be**

- Monthly status meetings
- Meeting with industry actors 05/2023

- Integration in the Cyber Factory
- Dissemination

Demo WalHub 25/04

STARS
STrategic Alliances boosting Railway Smes

Workshop STARS ??/05

Merci de votre attention