Institut Mines-Télécom

ANOMALY DETECTOR FOR CYBER-PHYSICAL INDUSTRIAL SYSTEMS

ANNA GUINET
TELECOM SUDPARIS
FRANCE

9th November 2018

TELECOM SudParis
Une école de l'IMT

iCIS
Radboud University

CONTENTS

1
PRESENTATION

Institut Mines-Télécom

Master's Degree
Telecom SudParis
Cybersecurity specialization

Cybersecurity engineer
Thales C&S
Integration & risk analysis

Senior Internship
University of Malaga
Trust metrics for the IoT

Research associate
(*Ingénieure de recherche*)
Telecom SudParis
CPS resilience

- Cryptography
- Network security (IP protocols)
- Darknets study (senior project)
- Risk analysis : EBIOS 2010

- Industrial control systems (ICS)
- SCADA systems & protocols
- Human threats in CPS : HCI, etc.

CONTENTS

Cyber-Physical System (CPS): Systems that integrate Computation, Communication and Control-Physical processes

_____

Lee and Seshia (2016). Introduction to embedded systems: A cyber-physical systems approach. MIT Press.

Moreover…

Systems with integrated computational and physical capabilities that **can interact with humans** through many new modalities

_____

Baheti and Gill (2011). Cyber-physical systems. The impact of control technology.

Cyber-physical systems have today the following features:

- **Large scale** – large number of physically distributed subsystems
- **Complex** – large number of variables, non-lineary & uncertainty
- **Human in the loop** – human beings & feedback control systems

Examples:

- **Industrial control systems**
- **Intelligent transportation systems**
- **Smart cities**
- **E-health**

Difference between ICT and ICS

	ICT	ICS
Aim	Information protection	Safety of services and people
Lifetime	<5 years	>10 years
Security properties priorities	↑ Confidentiality Integrity Availability	↑ Availability Integrity Confidentiality
Network	TCP/IP	SCADA (and TCP/IP)
Connectivity	Connected to Internet	Isolated (or strong restrictions)

Cyber-physical resilience

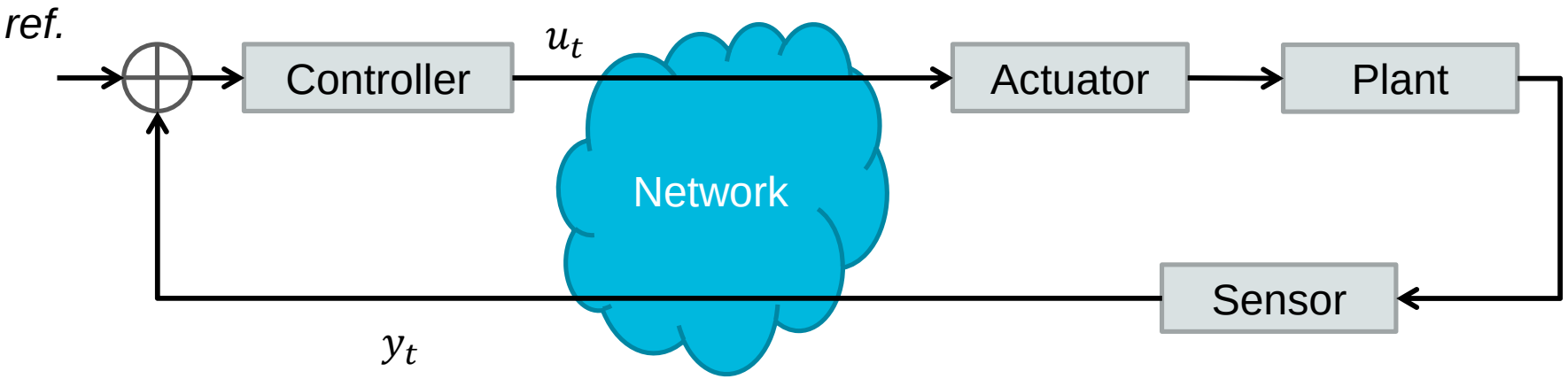
- Offer **critical functionalities** (e.g. safety functions) under the presence of failures and attacks

A resilient control systems should*:

- **Identify** threats
- **Minimize** their impact
- **Mitigate** them, or recover to a normal operation in a reasonable time

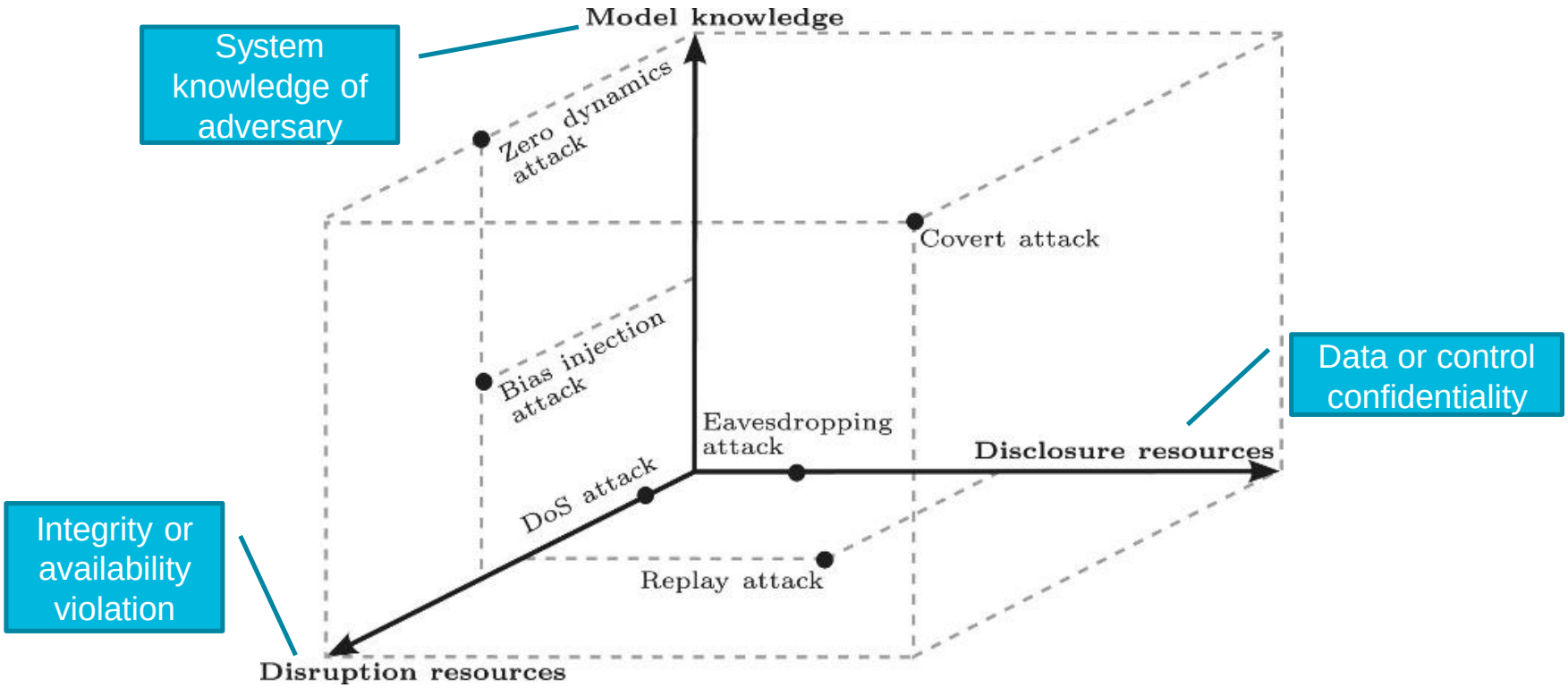
*Queiroz (2012). A holistic approach for measuring the survivability of SCADA systems. PhD, RMIT University.

Networked control system: Control system whose control loops are connected through a communication network



- Modeling of CPS using **feedback control theory**
- **Controller** commands the system using corrective feedback, based on the distance between a reference signal and the system output

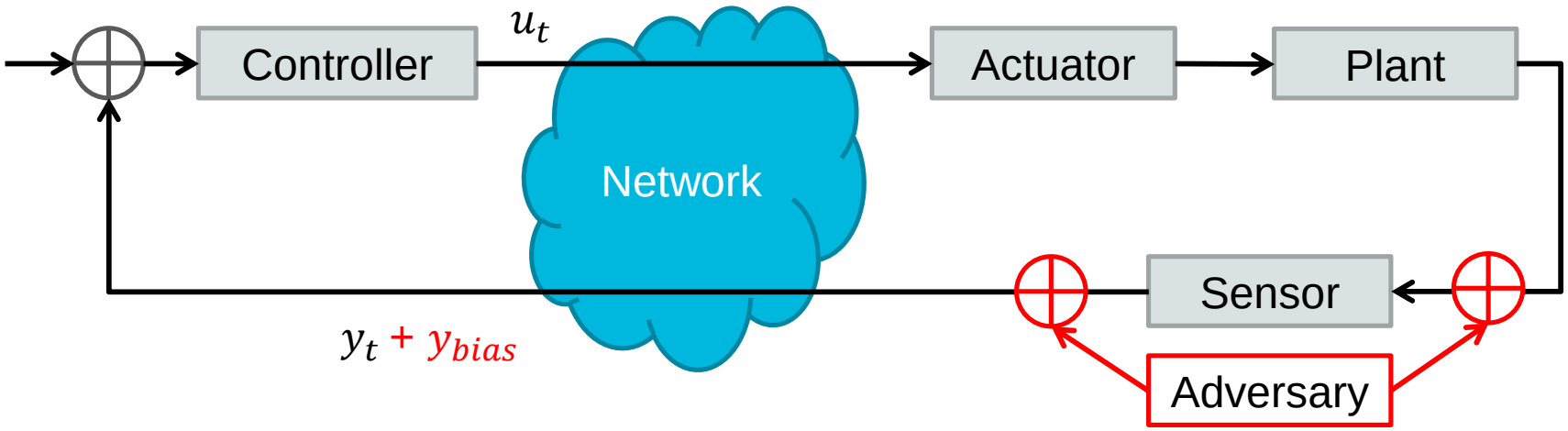
A **cyber-physical attack** exploits vulnerabilities, to harm the physical processes through the network



Teixeira, Shames, Sandberg, & Johansson (2015). A secure control framework for resource-limited adversaries. *Automatica*, *51*, 135-148.

False-data injection attack

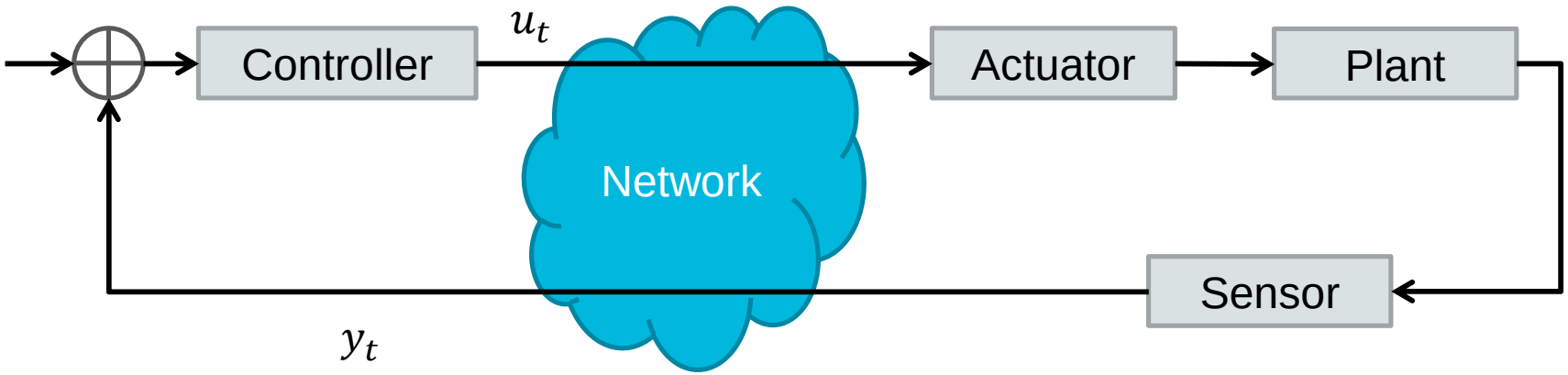
- **How**: Modification of sensors reading by physical interferences, by the communication channel or individual meters to generate wrong control decisions
- **Attack capabilities**: Limited knowledge of the physical system required
- **Countermeasure:** Comparison of sensor measurements and system dynamics



Hernan (2017). *Detection of attacks against cyber-physical industrial systems*, PhD, Institut National des Télécommunications.

Replay attack

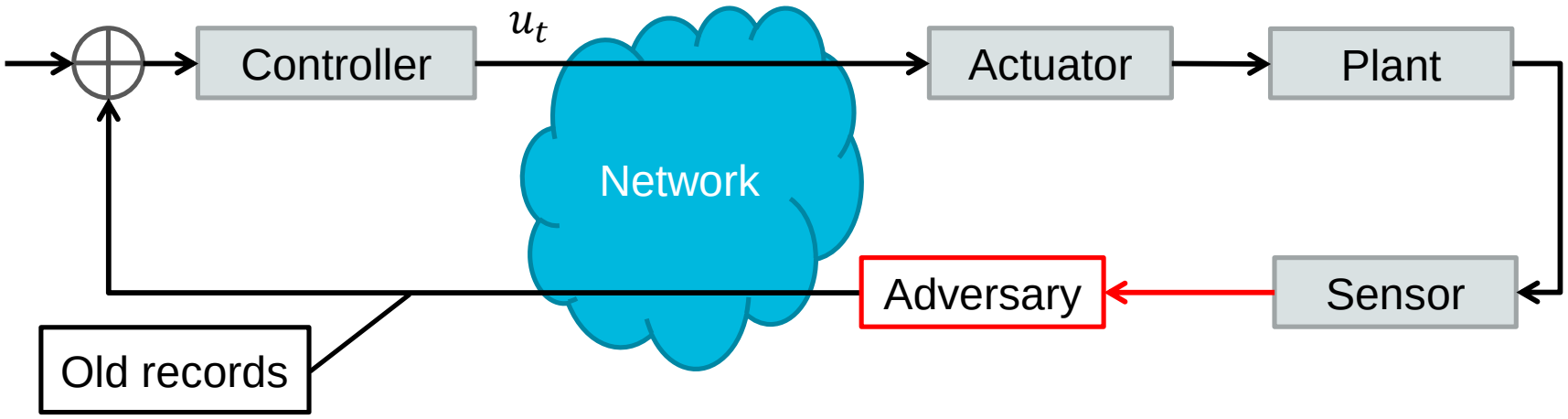
- **How**: Replay previous sensor measurements and modification of control inputs
- **Attack capabilities**: No knowledge of the physical system required
- **Countermeasure:** Add some protection on input control signals



Hernan (2017). *Detection of attacks against cyber-physical industrial systems*, PhD, Institut National des Télécommunications.

Replay attack

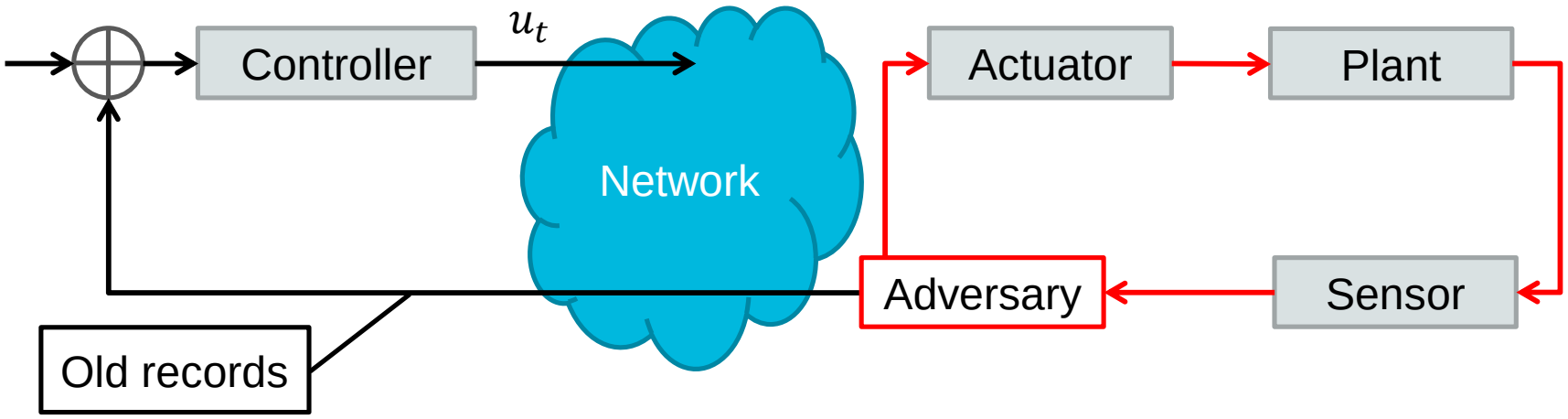
- **How**: Replay previous sensor measurements and modification of control inputs
- **Attack capabilities**: No knowledge of the physical system required
- **Countermeasure:** Add some protection on input control signals



Hernan (2017). *Detection of attacks against cyber-physical industrial systems*, PhD, Institut National des Télécommunications.

Replay attack

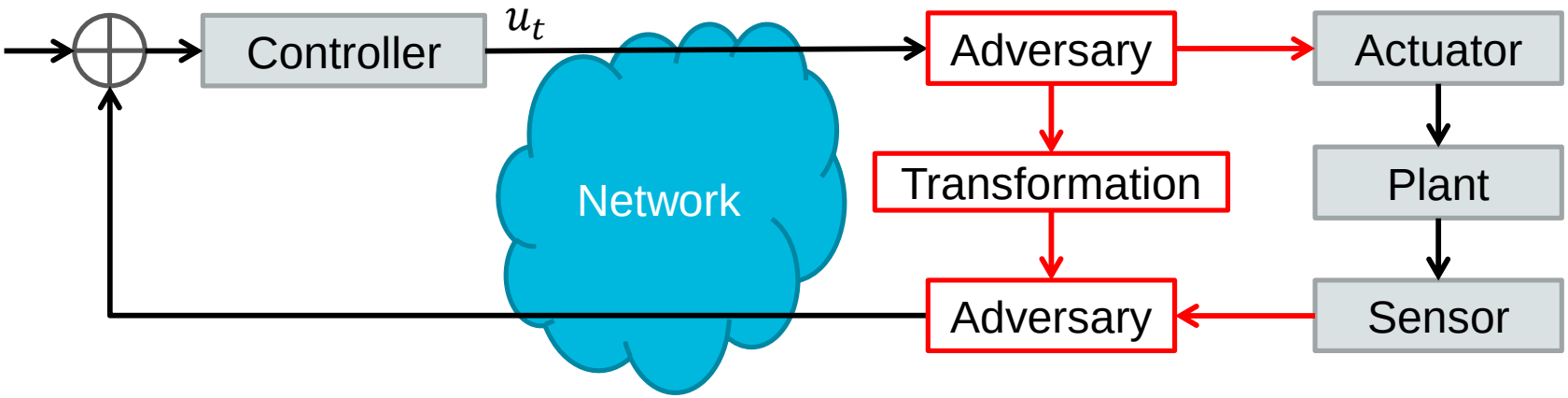
- **How**: Replay previous sensor measurements and modification of control inputs
- **Attack capabilities**: No knowledge of the physical system required
- **Countermeasure:** Add some protection on input control signals



Hernan (2017). *Detection of attacks against cyber-physical industrial systems*, PhD, Institut National des Télécommunications.

Covert attack

- **How**: Modification of control inputs and sensor measurements
- **Attack capabilities**: Knowledge of the physical system required
- **Countermeasure:** Undetectable from the regular system operation



Hernan (2017). *Detection of attacks against cyber-physical industrial systems*, PhD, Institut National des Télécommunications.

DoS attack

- **How**: Disrupt the communication on a channel to isolate the monitor process

Zero dynamic attack

- **How:** Disrupt the unobservable part of the system
- **Countermeasure:** Verify if all the states are observable

Command injection attack

- **How:** Exploit protocols and devices vulnerabilities to inject false commands
- **Countermeasure:** Signature-based IDS

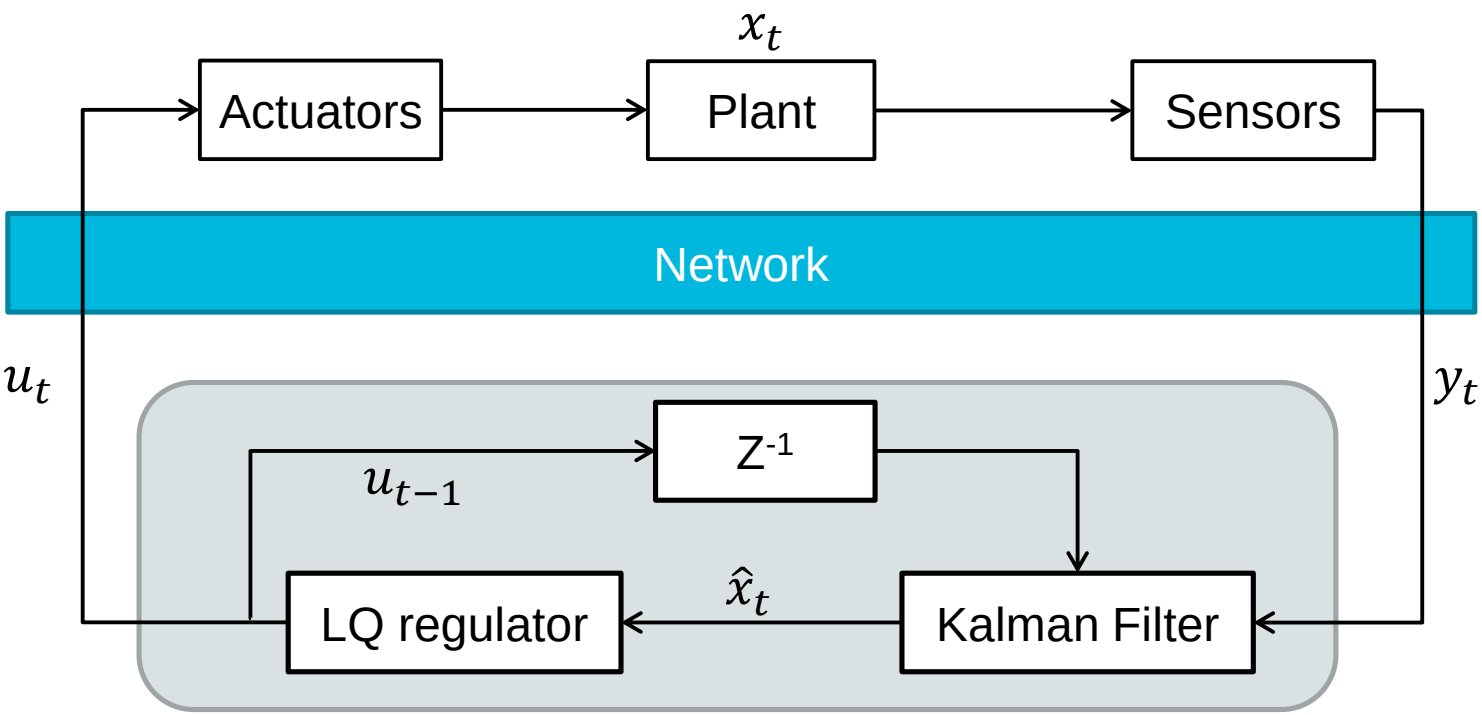
Rubio-Hernan (2017). *Detection of attacks against cyber-physical industrial systems*, PhD, Institut National des Télécommunications.

CONTENTS

Periodic and intermittent event-triggered control watermark detector

- **System specifications**:
  - Discrete linear time-invariant **LTI system**
  - Linear Quadratic Gaussian **LQG controller**
- **Strategy:**
  - **Challenge-response** authentication scheme
  - **Non-stationary watermark-based** (noise) to verify the integrity of the control loop
- **Countermeasure** against adversaries that have partial or full knowledge of the system dynamics
- **Penalty:** performance loss

Mo, Weerakkody, & Sinopoli. (2015). Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs. *IEEE Control Systems*, *35*(1), 93-109.
Rubio-Hernan, De Cicco & Garcia-Alfaro (2016). Event-triggered watermarking control to handle cyber-physical integrity attacks. In *Nordic Conference on Secure IT Systems* (pp. 3-19). Springer, Cham.



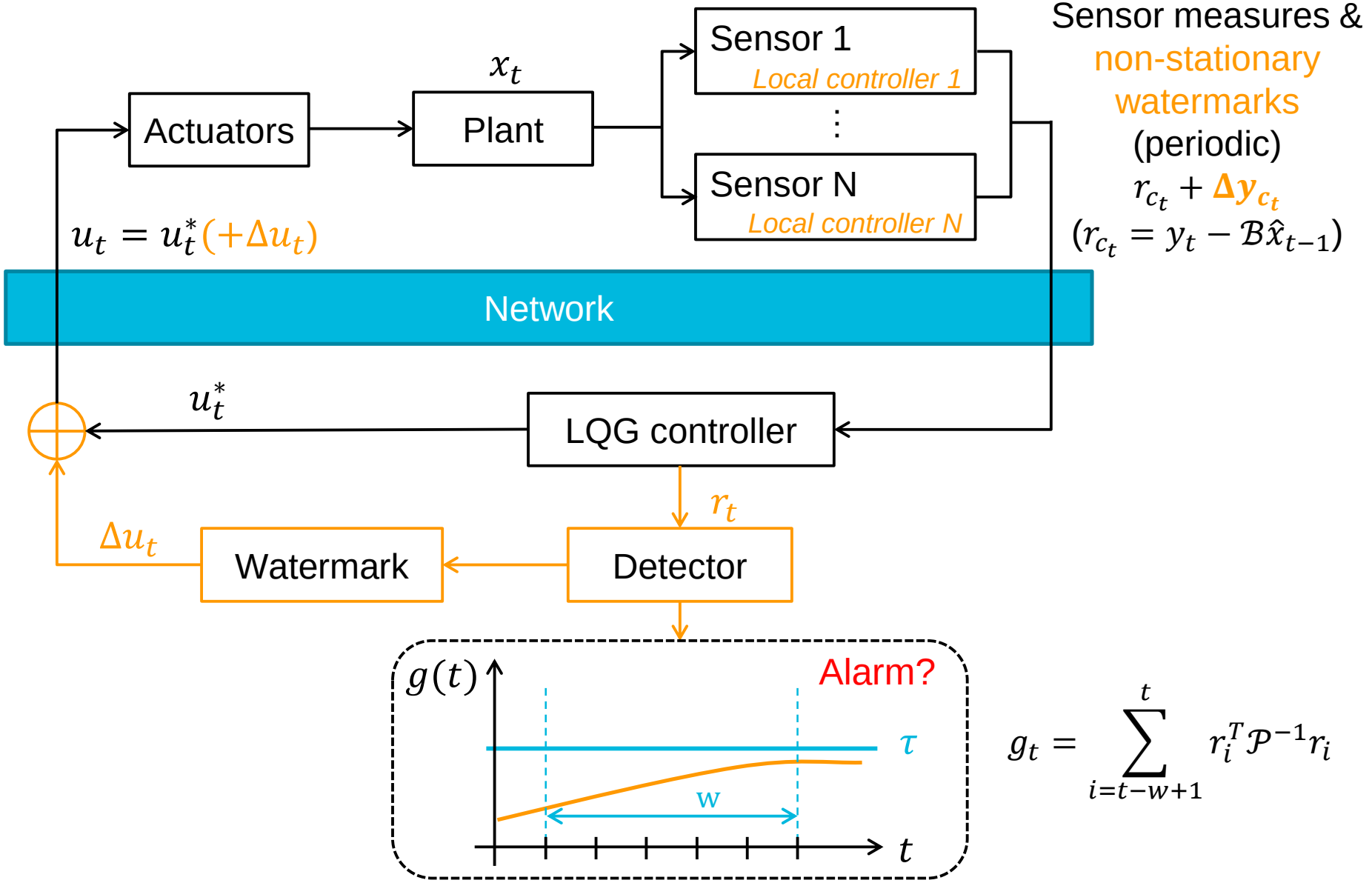
LQG controller

$$x_{t+1} = Ax_t + Bu_t + w_t$$

with $A \in \mathbb{R}^{p \times p}$ state matrix
$B \in \mathbb{R}^{p \times m}$ input matrix
$w_t \sim N(0, Q)$ noise

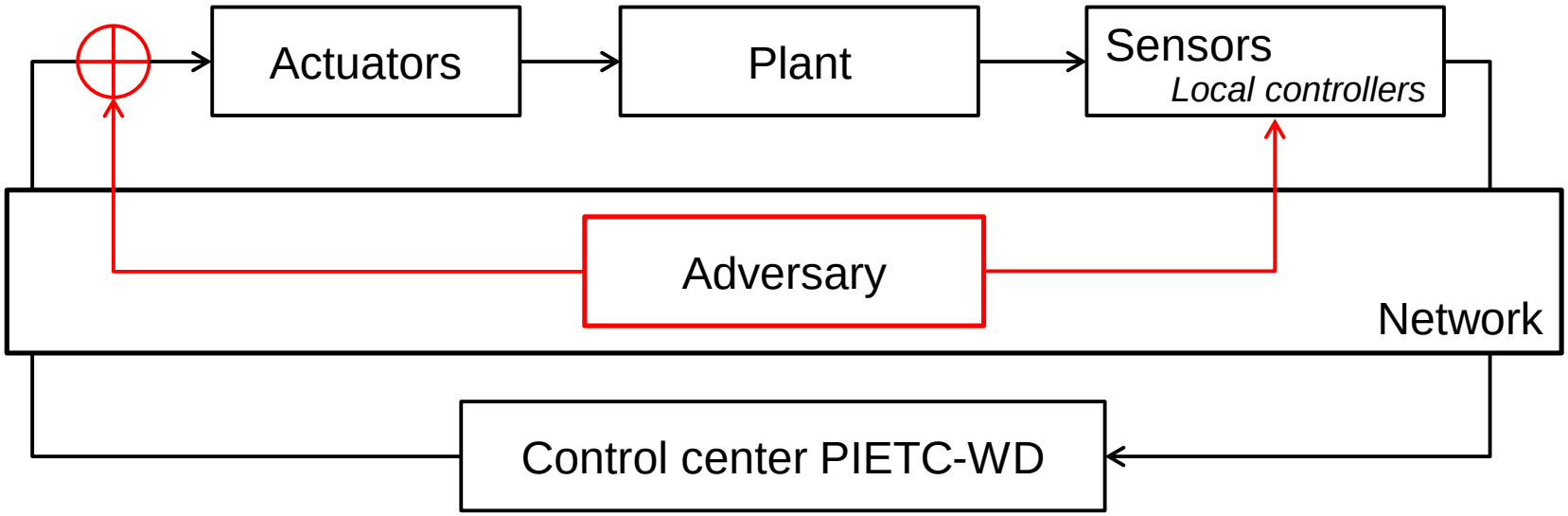
$$y_t = Cx_t + v_t$$

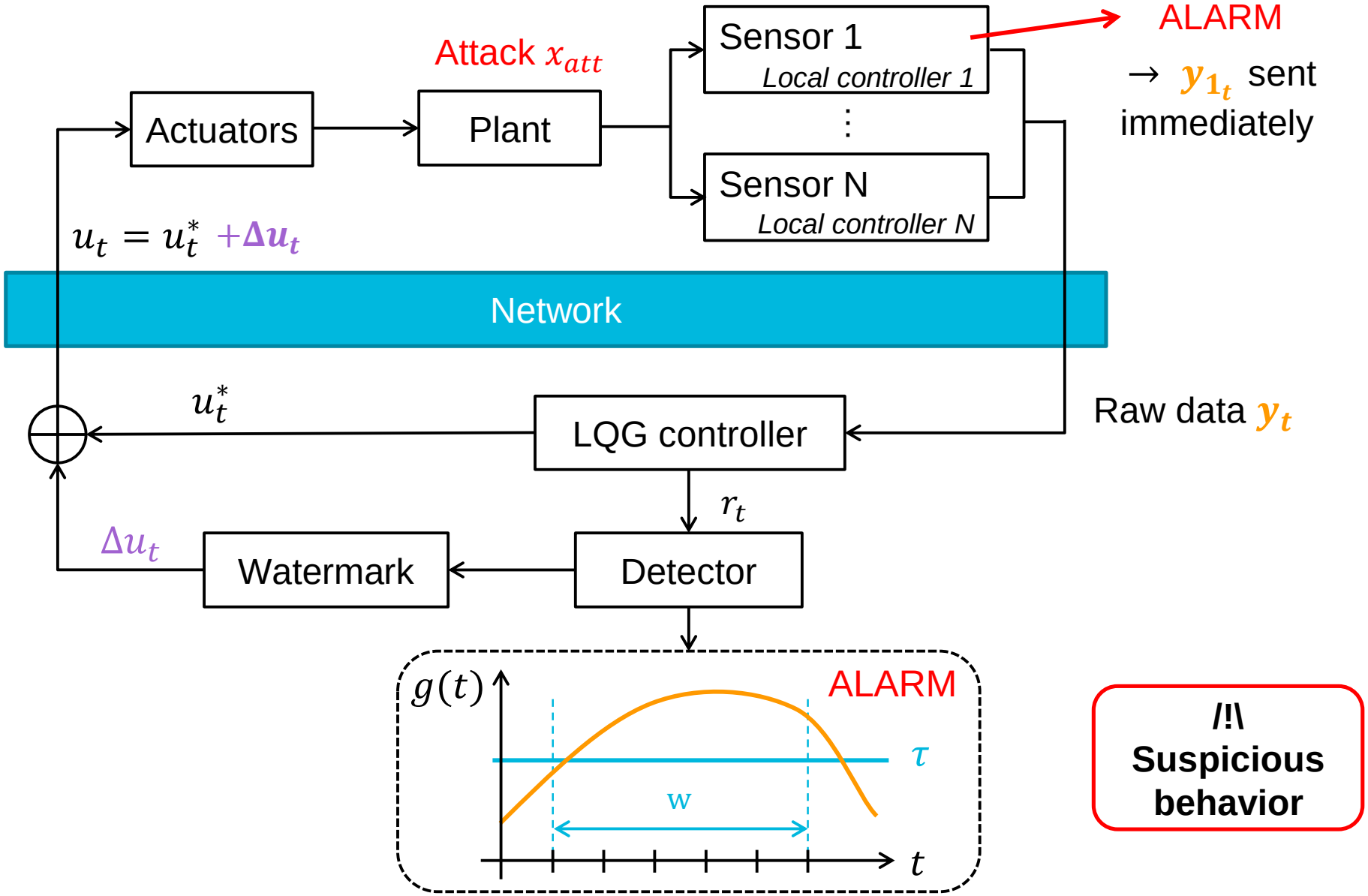
with $C \in \mathbb{R}^{n \times p}$ output matrix
$v_t \sim N(0, R)$ noise

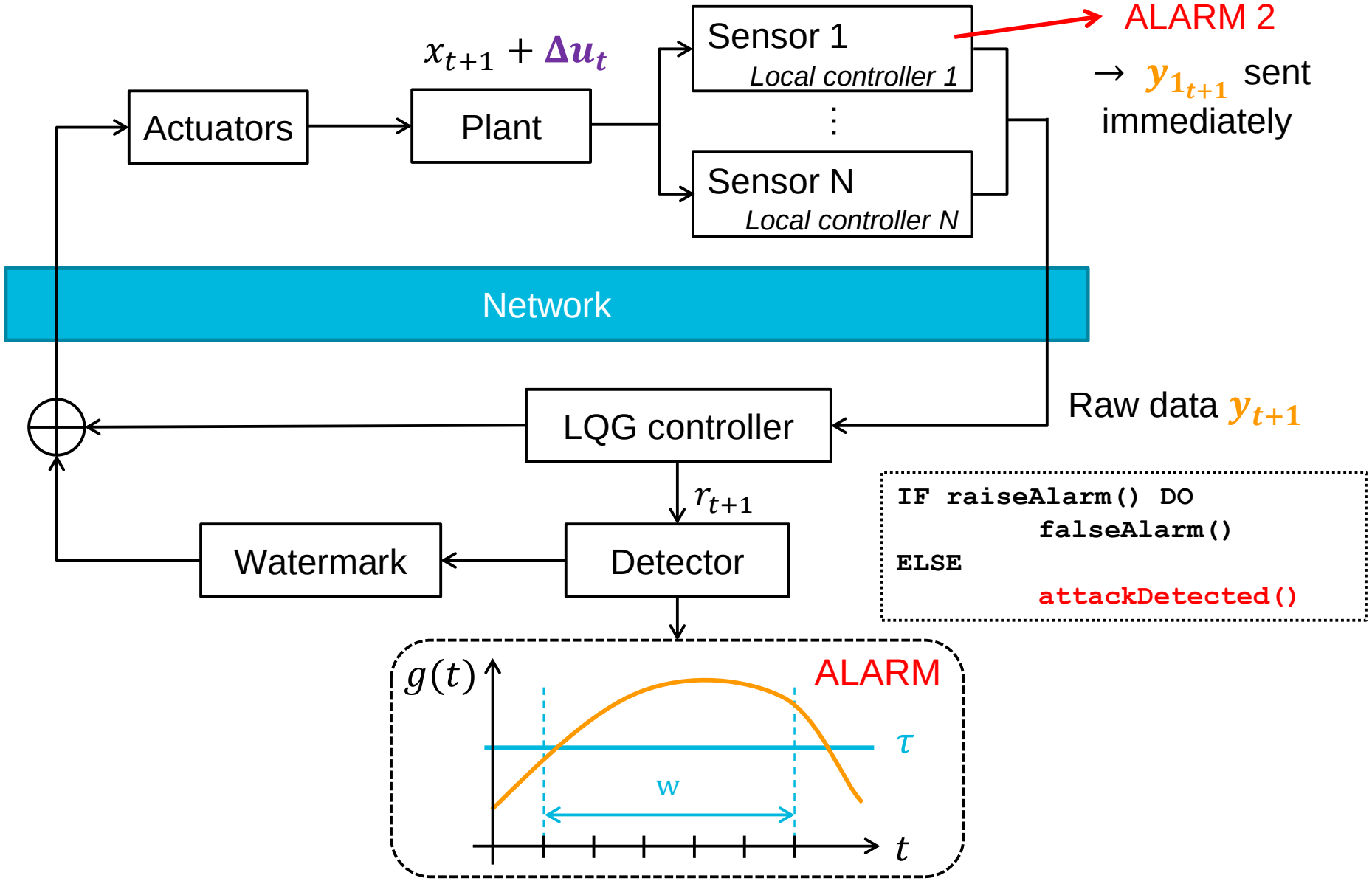

Sensor measures & non-stationary watermarks (periodic)
$r_{c_t} + \Delta y_{c_t}$
$(r_{c_t} = y_t - \mathcal{B}\hat{x}_{t-1})$
Sensor 1
Local controller 1
Sensor N
Local controller N
x_t
Actuators
Plant
$u_t = u_t^*(+\Delta u_t)$
Network
u_t^*
LQG controller
r_t
Δu_t
Watermark
Detector
$g(t)$
Alarm?
τ
w
t
$g_t = \sum_{i=t-w+1}^{t} r_i^T \mathcal{P}^{-1} r_i$

Cyber-physical adversary

- **Aim:** Use identification methods to gain knowledge about the system parameters, from the network, to influence the physical behavior.

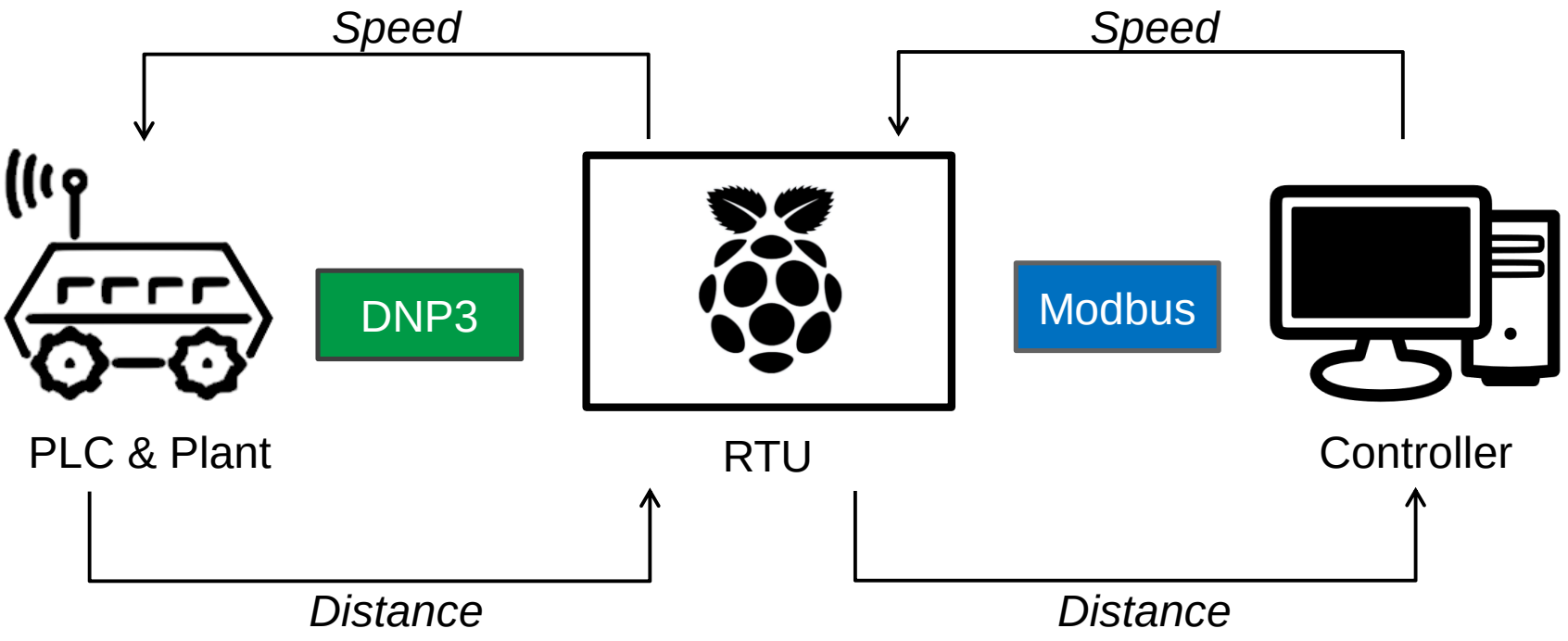


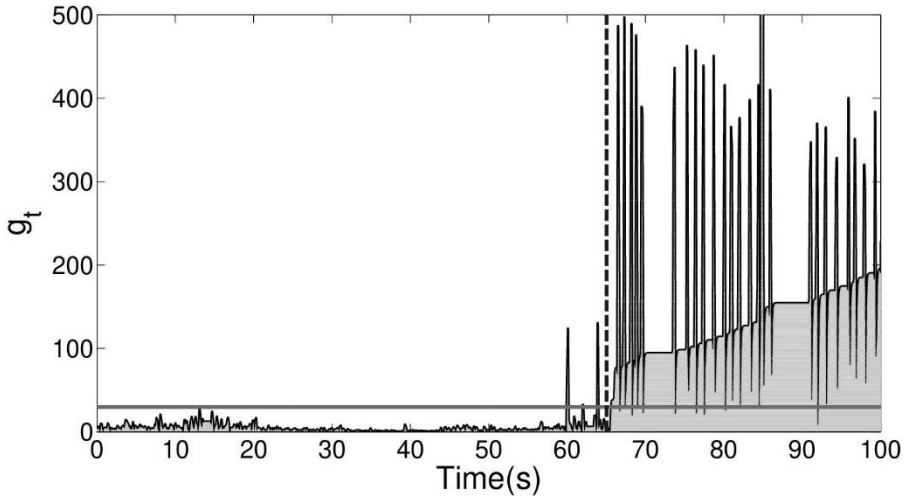

Attack x_{att}
Sensor 1
Local controller 1
Sensor N
Local controller N
ALARM
→ y_{1_t} sent immediately
Actuators
Plant
$u_t = u_t^* + \Delta u_t$
Network
u_t^*
LQG controller
Raw data y_t
r_t
Δu_t
Watermark
Detector
$g(t)$
ALARM
τ
w
t
/!\
Suspicious behavior


$x_{t+1} + \Delta u_t$
Actuators
Plant
Sensor 1
Local controller 1
Sensor N
Local controller N
ALARM 2
→ $y_{1_{t+1}}$ sent immediately
Network
LQG controller
Raw data y_{t+1}
r_{t+1}
Watermark
Detector
IF raiseAlarm() DO
falseAlarm()
ELSE
attackDetected()
$g(t)$
ALARM
τ
w
t

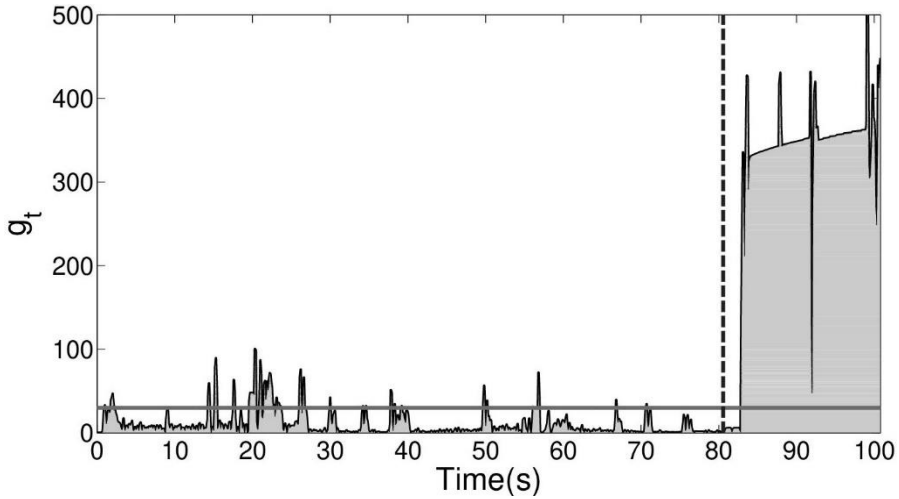
SCADA Testbed

- LEGO Mindstorm EV3 & Raspberry Pi
- **Closed-loop** system with wired and wireless communications

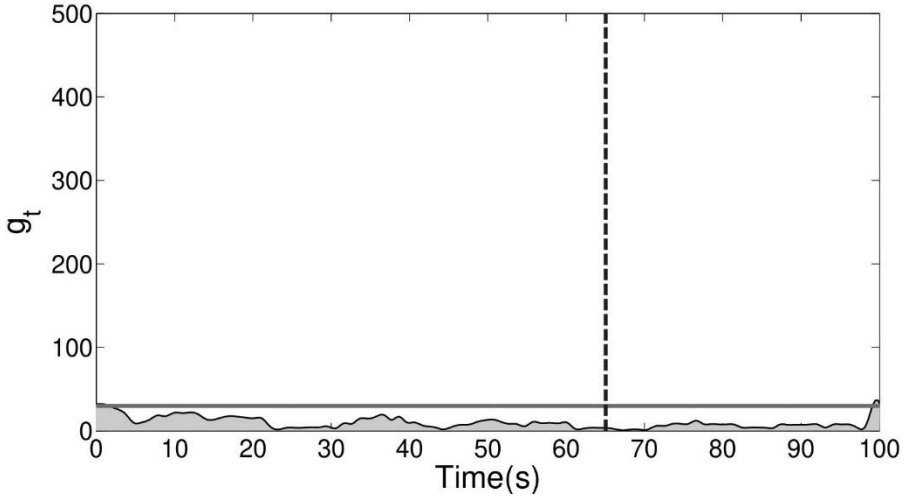




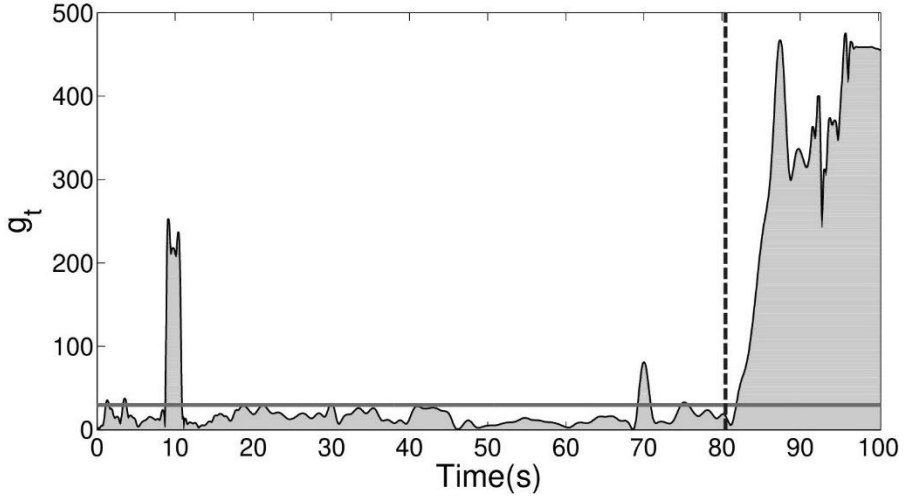
Sensor detectors without intermittent policy



Sensor detectors with intermittent policy



Central detector without intermittent policy



Central detector with intermittent policy

CONTENTS

- **PIETC-WD**
  - Decentralized detection mechanism with non-stationary watermark
  - Detection of integrity cyber-physical attacks
  - Impacts:
    - Performance
    - Detection time

- **Future Work: Resilient CPSs**
  - More thorough analysis of PIETC-WD
  - Mitigation of cyber-physical attacks
    - Programmable networking

References

- Lee and Seshia (2016). Introduction to embedded systems: A cyber-physical systems approach. MIT Press.
- Baheti and Gill (2011). Cyber-physical systems. The impact of control technology.
- Queiroz (2012). A holistic approach for measuring the survivability of SCADA systems. PhD, RMIT University.
- Teixeira, Shames, Sandberg, & Johansson (2015). A secure control framework for resource-limited adversaries. *Automatica*, *51*, 135-148.
- Rubio-Hernan (2017). *Detection of attacks against cyber-physical industrial systems*, PhD, INT.
- Rubio-Hernan, De Cicco & Garcia-Alfaro (2016). Event-triggered watermarking control to handle cyber-physical integrity attacks. In *Nordic Conference on Secure IT Systems* (pp. 3-19). Springer, Cham.
- Mo, Weerakkody, & Sinopoli. (2015). Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs. *IEEE Control Systems*, *35*(1), 93-109.

ANNEXES

Institut Mines-Télécom

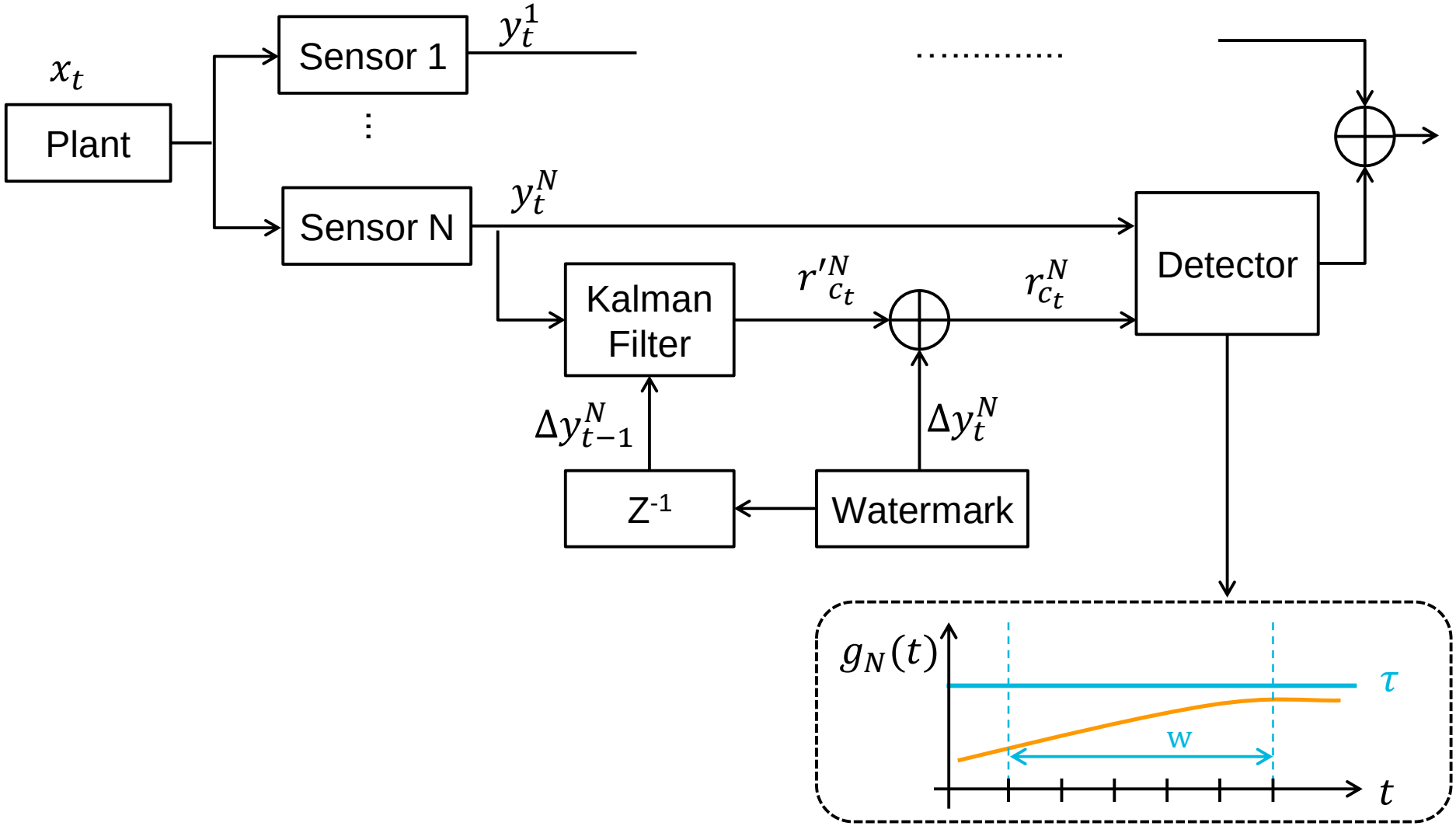
1 / Bridge and toll testbed

2 / Industrial chain testbed

3 / Railway control testbed

4 / Autonomous industrial agents testbed

Local controllers architecture



Performance loss

- **LQG controller performance loss**: quadratic cost J

$$J = \lim_{n\to\infty} E\left[\frac{1}{n}\sum_{i=0}^{n-1}\left(x_i^T \Gamma x_i + u_i^T \Omega u_i\right)\right] \quad \text{with}$$

$u_t \in \mathbb{R}^m$ control input
$x_t \in \mathbb{R}^p$ state vector
$\Gamma \in \mathbb{R}^{p\times p}$ positive definite cost matrix
$\Omega \in \mathbb{R}^{m\times m}$ positive definite cost matrix

- **Non-stationary performance loss**: quadratic cost ΔJ_s

$$J = J^* + \Delta J_s$$

$$\beta = E\left[\Delta s^{(i)}\right] + Var\left[\Delta s^{(i)}\right]$$

SCADA Components

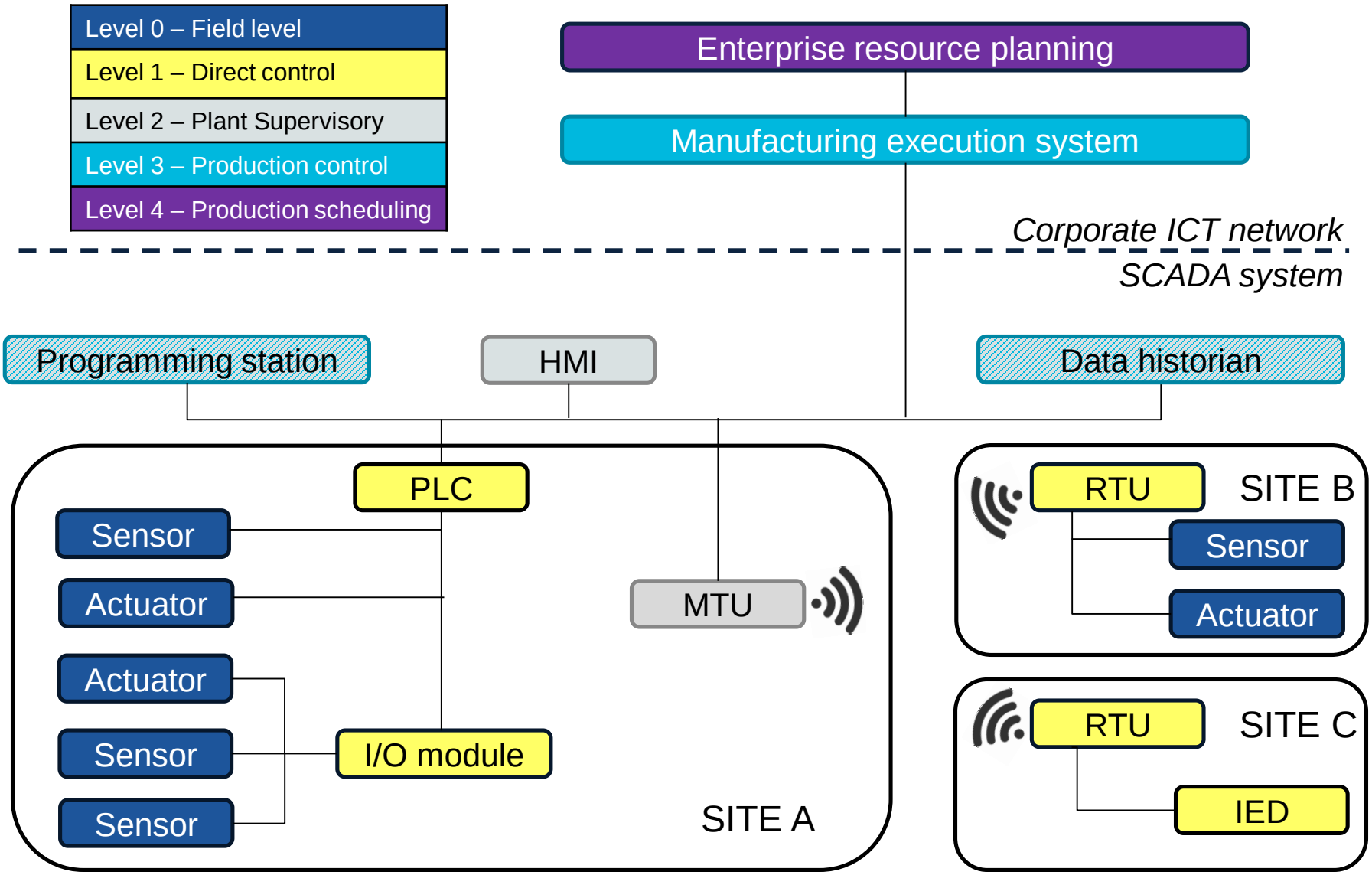
Supervisory Control And Data Acquisition (SCADA): A technology to monitor industrial environments

- **Programmable Logic Controller (PLC):** Microprocessors-based devices to control and acquire inputs/outputs
- **Intelligent Electronic Device (IED):** Small microprocessors with limited capabilities in power systems
- **Remote Terminal Unit (RTU)**: Stand-alone data acquisition and control units on a remote site via telemetry
- **Master Terminal Unit (MTU)**: Control center of the system to collect, store and control data from RTUs and PLCs
- **Human-Machine Interface (HMI):** Displays real-time operation information about the processes to the operators to coordinate and control the system

ISA 95

Definition of the different levels of SCADA Systems

- **Level 0 – Field level**: Physical plant
- **Level 1 – Direct control**: Measurement and manipulation of the plant
- **Level 2 – Plant Supervisory**: Control and supervision systems of the plant
- **Level 3 – Production control**: Work flow to produce the desired end products and optimization of the system
- **Level 4 – Production scheduling**: Establishment of the basic plant schedule (production, delivery, inventory, etc.)


Level 0 – Field level
Level 1 – Direct control
Level 2 – Plant Supervisory
Level 3 – Production control
Level 4 – Production scheduling
Enterprise resource planning
Manufacturing execution system
Corporate ICT network
SCADA system
Programming station
HMI
Data historian
PLC
Sensor
Actuator
Actuator
Sensor
Sensor
I/O module
MTU
SITE A
RTU
SITE B
Sensor
Actuator
RTU
SITE C
IED

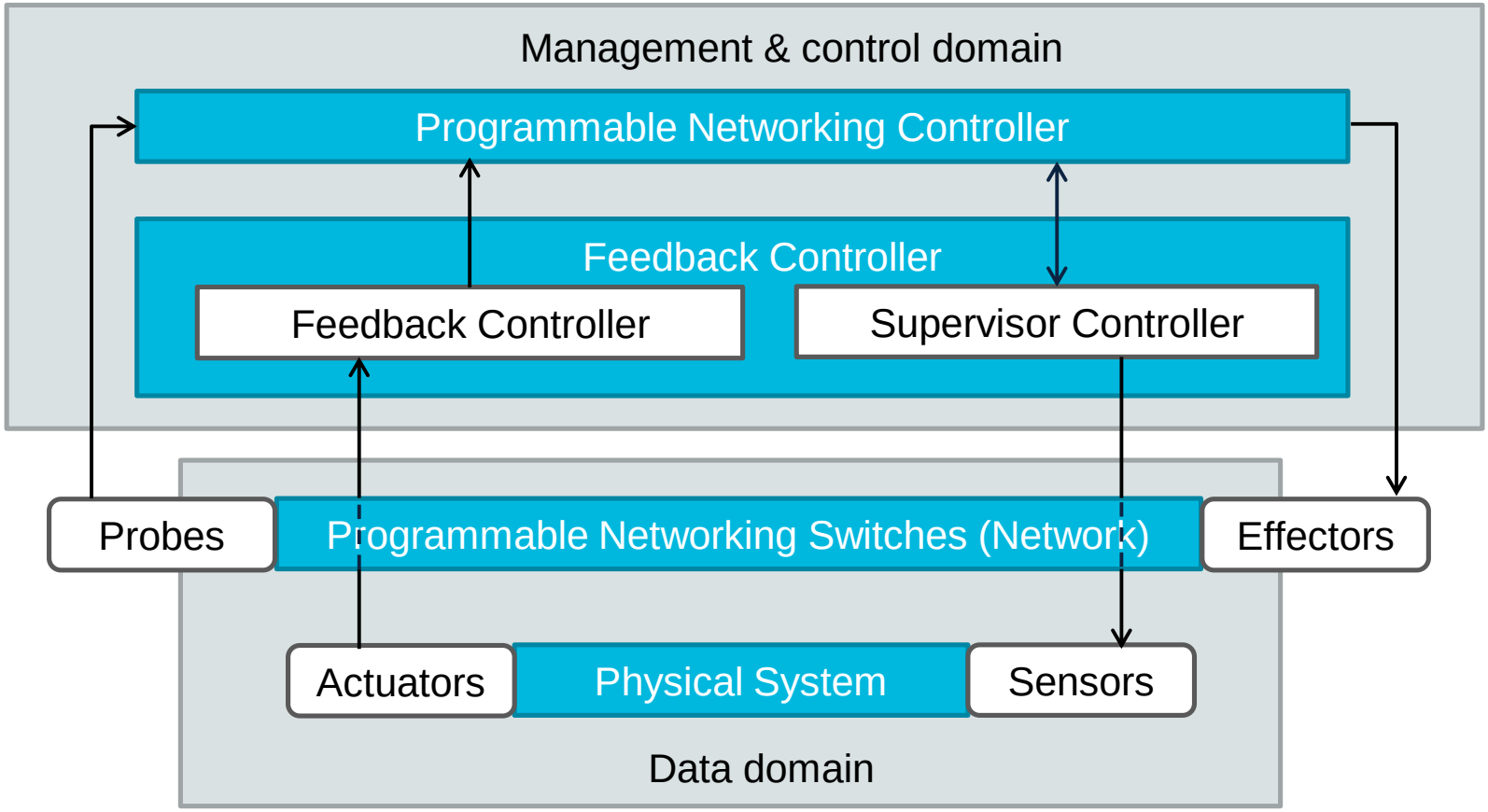
SCADA protocols

- Modbus
- PROFINET
- PROFIBUS
- DNP3
- IEC-60870-5-104
- EtherNet/IP
- Ethernet Powerlink
- AGA-12, etc.

/!\ Designed for safety and not security /!

OSI Level	Industrial protocols		
7	Modbus/TCP DNP3-SA PROFINET IO IEC-60870-5-104 EtherNet/IP	PowerLink	
6			
5			
4	TCP/UDP		
3	IP		
2	Ethernet	Ethernet PowerLink	Modbus ASCII/RTU PROFIBUS DNP3 AGA-12 IEC-60870-5-101
1	Physical		

Cyber-physical systems & Software-defined network



Rubio-Hernan, Sahay, De Cicco & Garcia-Alfaro (2018). Cyber-physical architecture assisted by programmable networking. *Internet Technology Letters*, e44.