Cyber-Physical System
현황 및 주요 이슈

Kyung-Joon Park (박경준)
DGIST, Korea

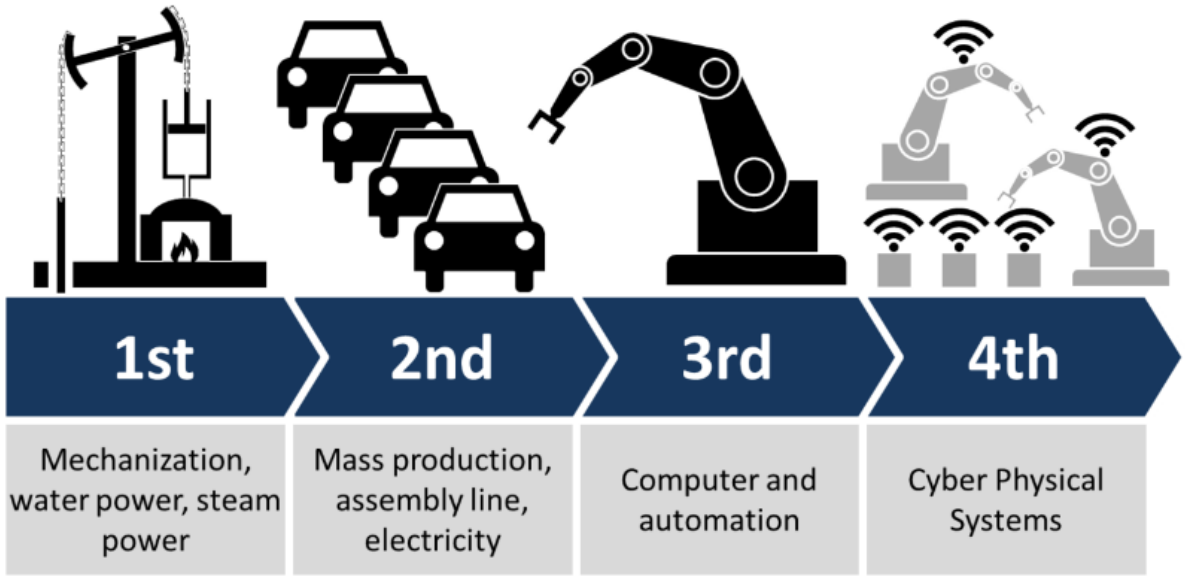
Nov. 30, 2018
KNOM Workshop 2018

DGIST 대구경북과학기술원
Daegu Gyeongbuk Institute of Science & Technology

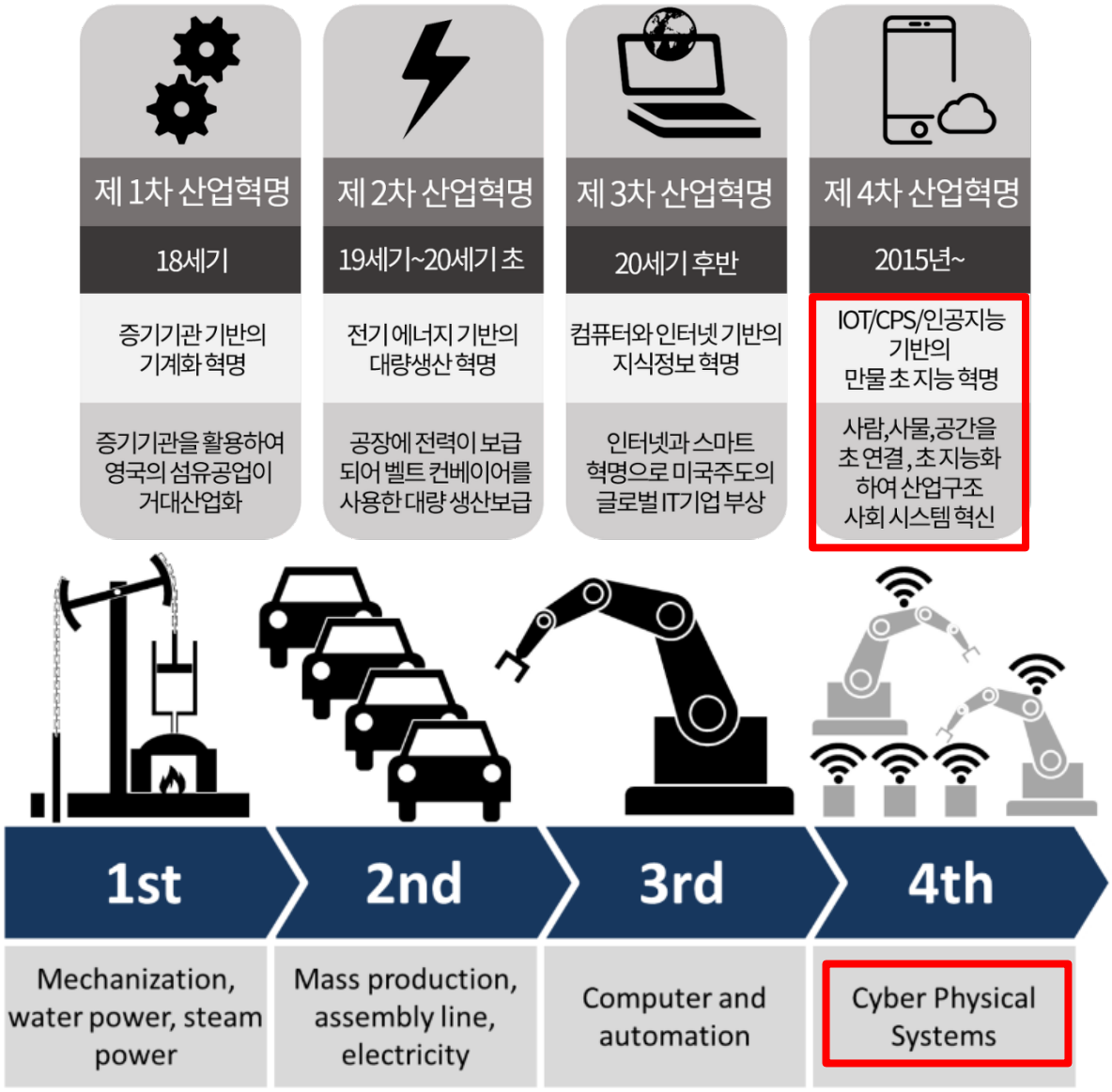
Contents

- Introduction on CPS
  - Era of convergence
  - CPS as networked control systems
- Cyber-physical security
  - Illustrative example: Stuxnet
- Resilient CPS testbed
  - Train control system as hierarchical control system
- Conclusions

Enabler of 4th industrial revolution



Enabler of 4th industrial revolution



Era of convergence

- Individual discipline of engineering is getting old
  - Mechanical engineering more than 200 years
  - Electrical engineering more than 100 years
  - Computer science & engineering more than 50 years

- Era of convergence is coming or has already come
  - Individual discipline is mature
  - Opportunities in the crossroads

Cyber-physical systems (CPS)?

Cyber-physical systems (CPS)?

- Tight coordination between computational and physical elements [NSF Program 10-515, 30M USD each year]

Cyber-physical systems (CPS)?

- Tight coordination between computational and physical elements [NSF Program 10-515, 30M USD each year]
- **Network** of interacting elements instead of standalone devices

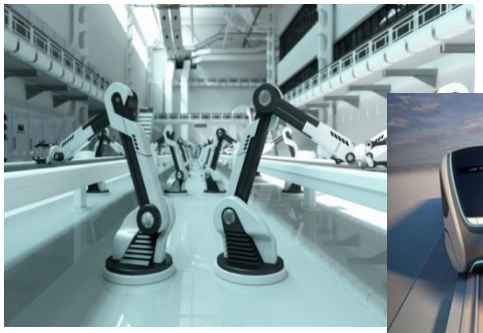
Cyber-physical systems (CPS)?

- Tight coordination between computational and physical elements [NSF Program 10-515, 30M USD each year]
- **Network** of interacting elements instead of standalone devices
- Difference from embedded systems?
  - Embedded system: focus on computational part
  - CPS: focus on link between computational and physical parts

Cyber-physical systems (CPS)?

- Tight coordination between computational and physical elements [NSF Program 10-515, 30M USD each year]
- **Network** of interacting elements instead of standalone devices
- Difference from embedded systems?
  - Embedded system: focus on computational part
  - CPS: focus on link between computational and physical parts
- Various applications; aerospace, automotive, healthcare, chemical processes, civil infrastructure, energy, manufacturing, transportation, entertainment
  - Virtually, every complex man-made system can be CPS

Illustration of CPS

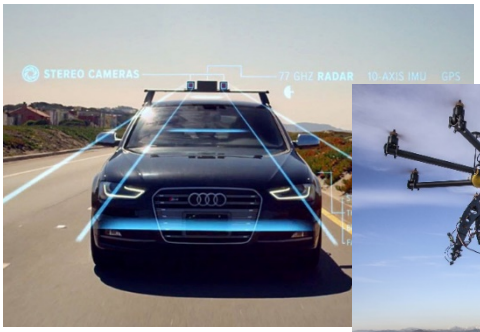


Smart factory

Automated train

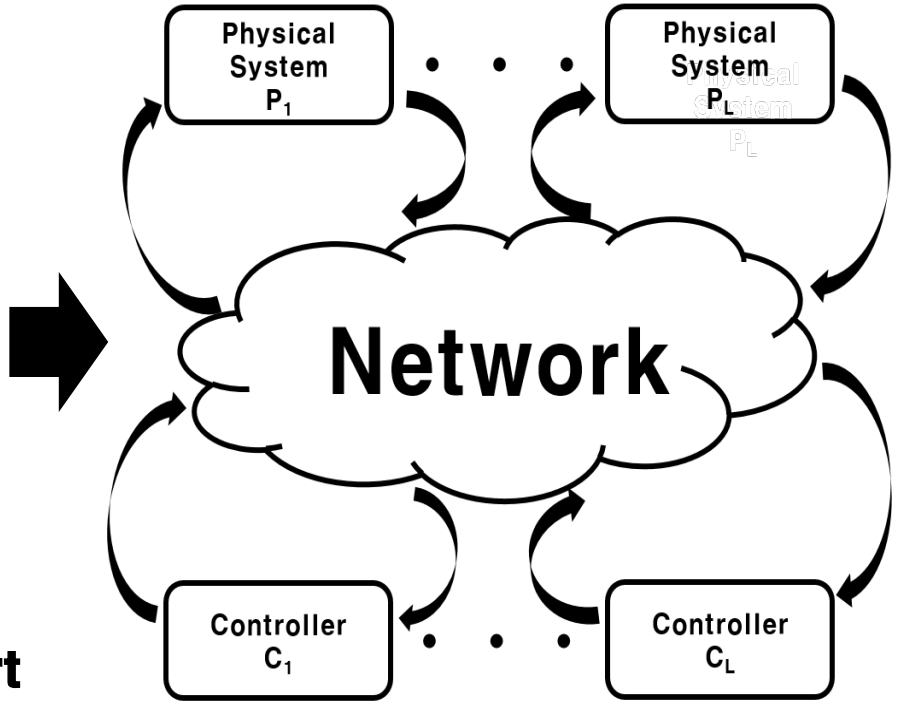
CPS applications

Smart building

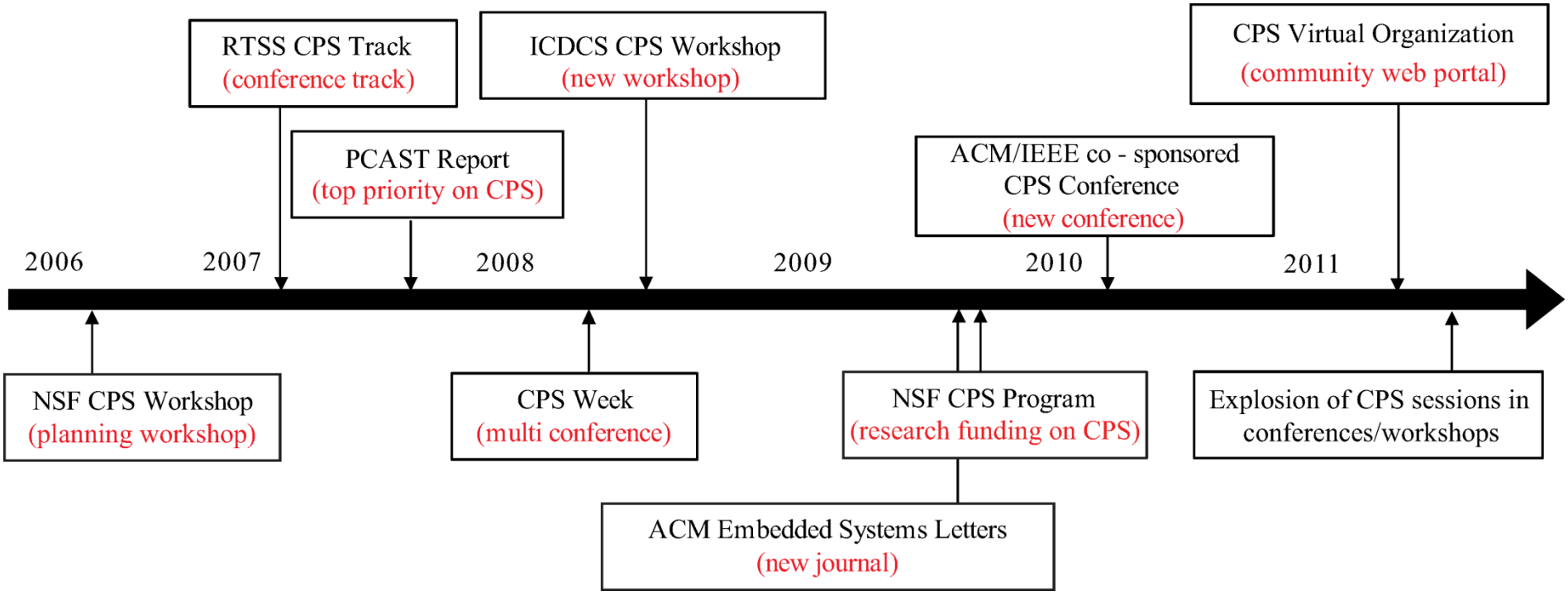


Self-driving cars

drones



Expanding interest in CPS



Where CPS differs from traditional embedded systems

- Traditional embedded systems

  Software on small computers. Technical problem is one of optimization with limited resources

- CPS

  Computing and networking integrated with physical processes. Technical problem is managing dynamics, time, and concurrency in networked computational and physical systems

Still, CPS is not clear ☹

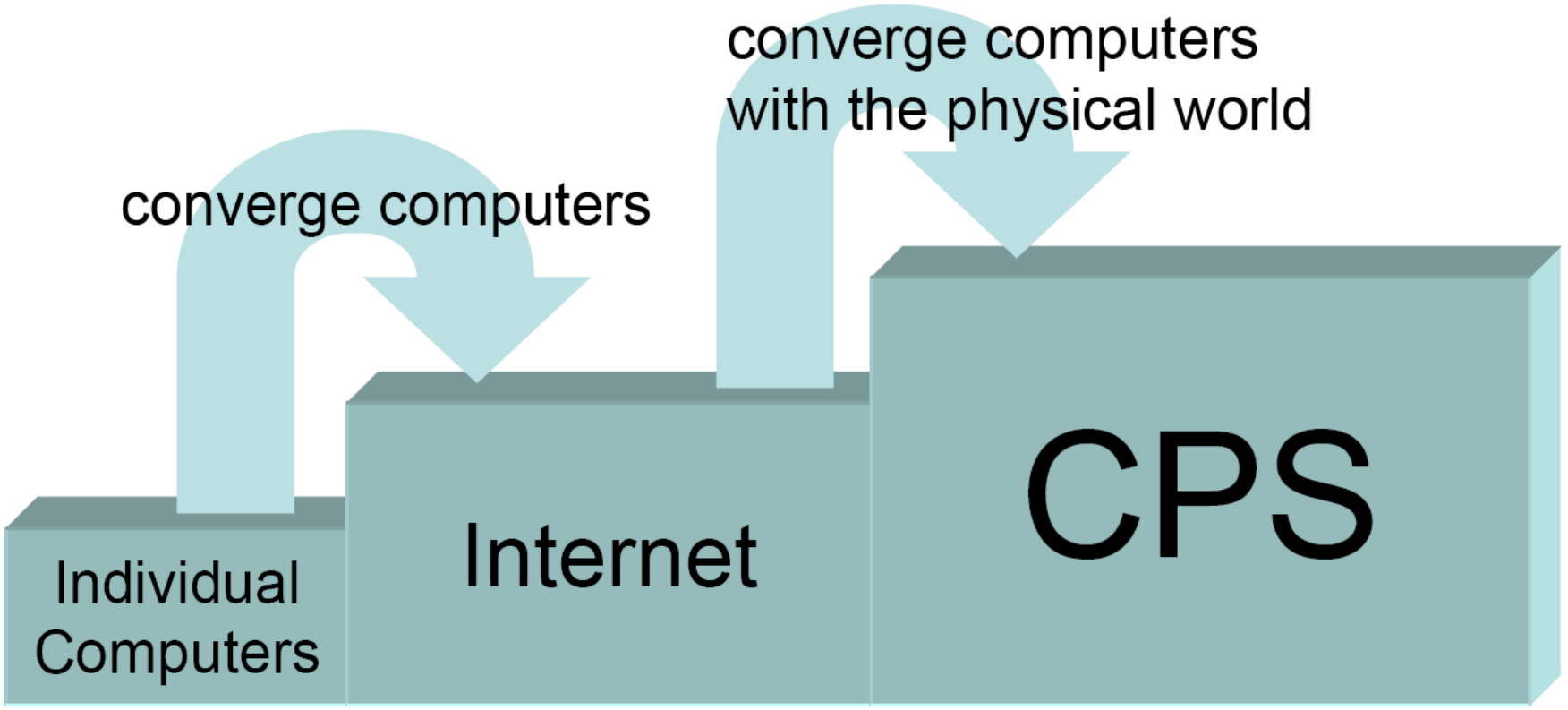
- Right, no clear definition exists
  - Everyone says his/her area is CPS ☺
- However, CPS is more than just another acronym
  - Meaningful studies are coming
  - IEEE/ACM Conference on CPS in CPS Week (and many more)

Major challenges

- Models for physical and for computation diverge
  - Physical: time continuum, ODEs, dynamics
  - Cyber (or computational): discrete logic

- There is a huge cultural gap
  - Electrical Engineering vs. Computer Science

CPS as next theme after Internet



Courtesy of Q. Wang

IoT vs. CPS

- IoT
  - Connect, and sense & control in primitive manner

IoT vs. CPS

- IoT
  - Connect, and sense & control in primitive manner

IoT vs. CPS

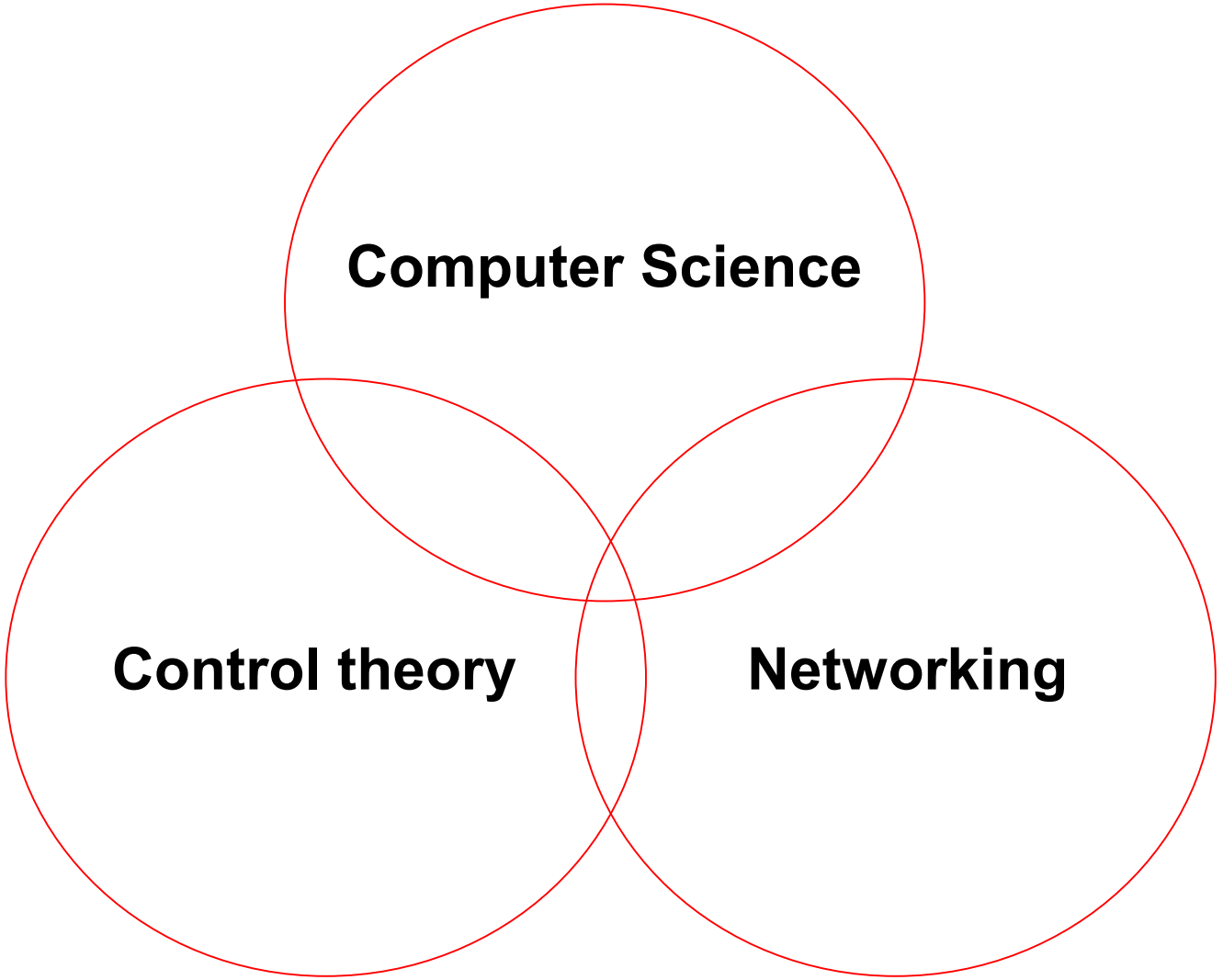
- CPS
  - Connect devices and physical systems
  - Sense and Control physical world in real time

- CPS ≈ real-time IoT
  - Real-time is NOT just fast, BUT deadline-aware

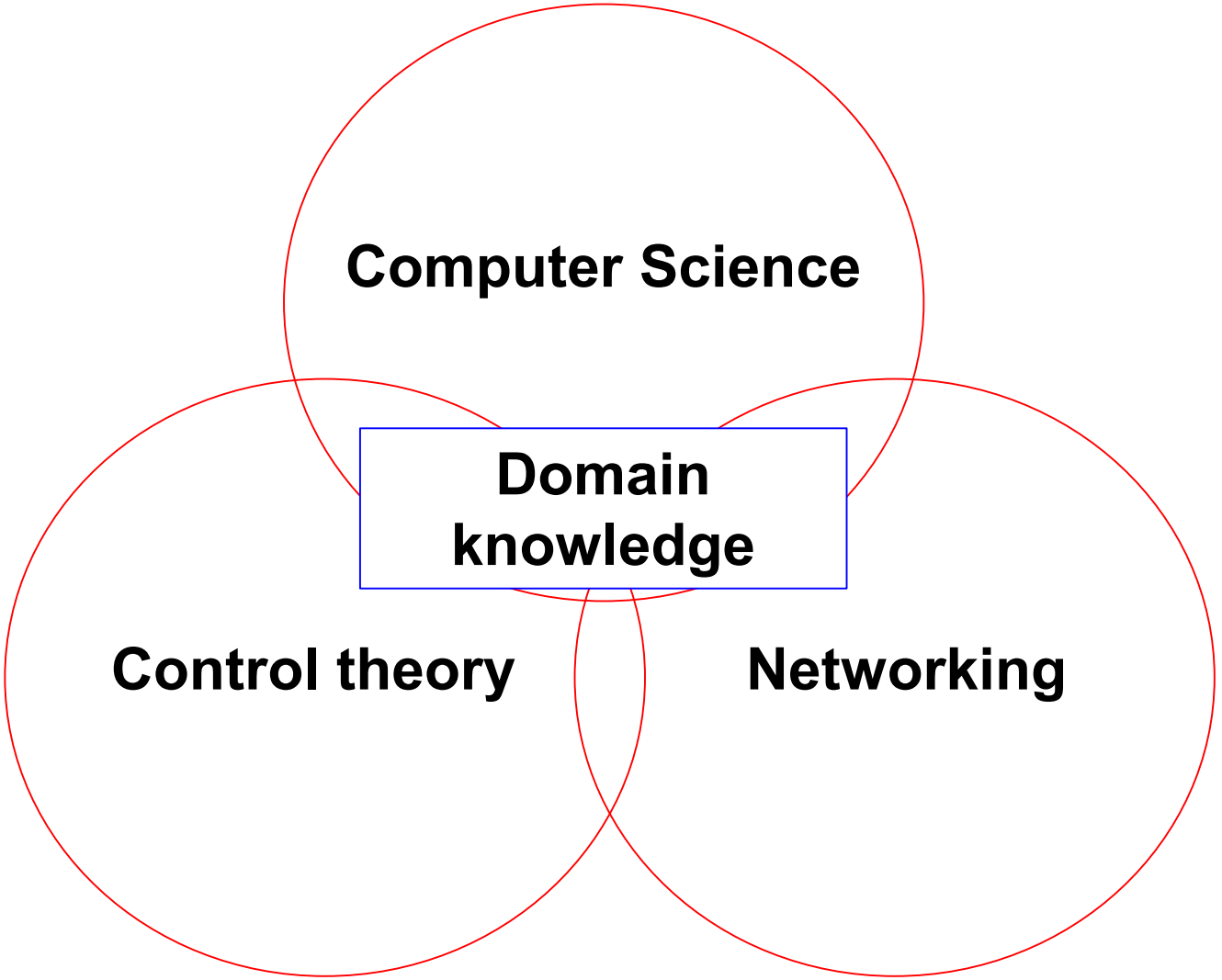
Major Components of CPS

- Three major components in CPS
  - Physical systems: Real-world systems in continuous time
  - Cyber systems: Computing systems in discrete logic
  - Networks: communication medium

Convergence research

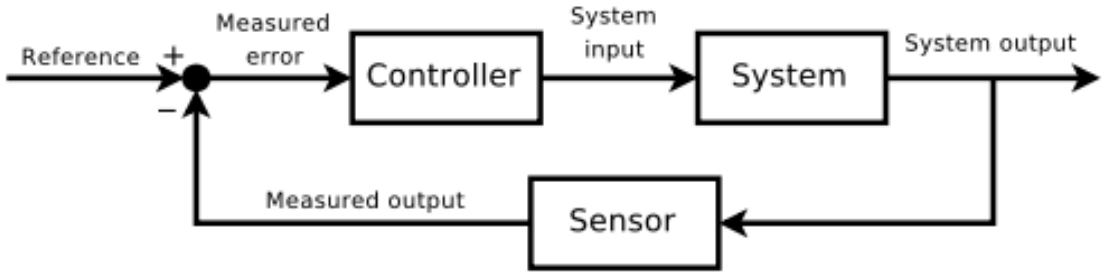


Convergence research



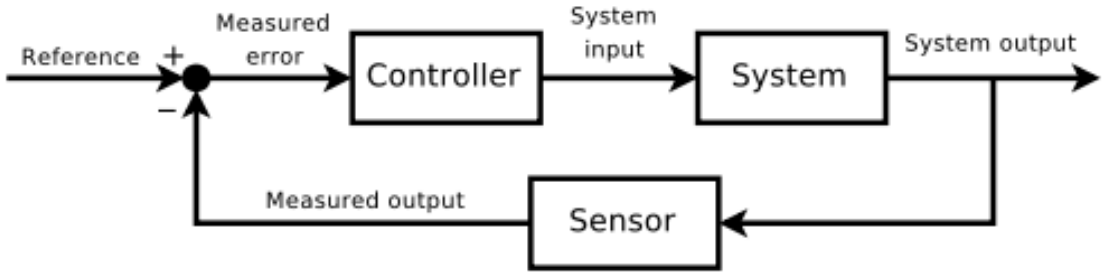
Control theory

- Interdisciplinary branch of engineering and mathematics
  - Deals with behavior of dynamical systems with inputs, and how their behavior is modified by feedback



Control theory

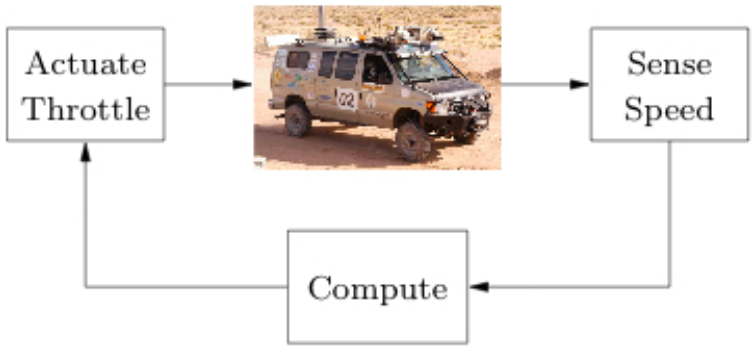
- Interdisciplinary branch of engineering and mathematics
  - Deals with behavior of dynamical systems with inputs, and how their behavior is modified by feedback



- Goes back to steam engine
  - Centrifugal governor

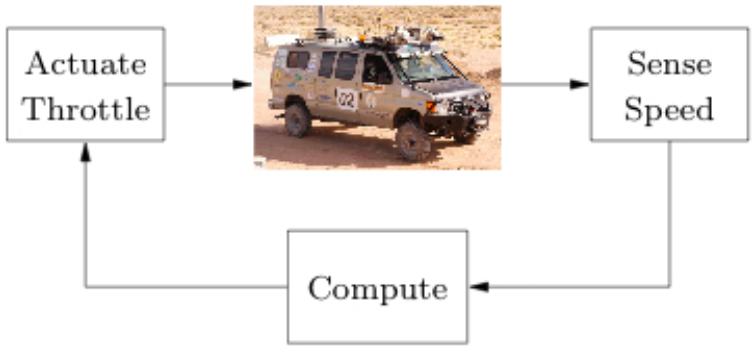
Control example

- Cruise control
  - Open loop vs. closed loop

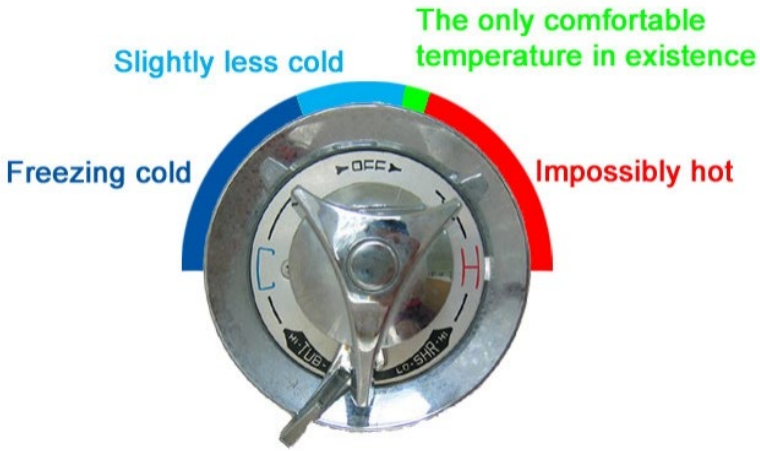


Control example

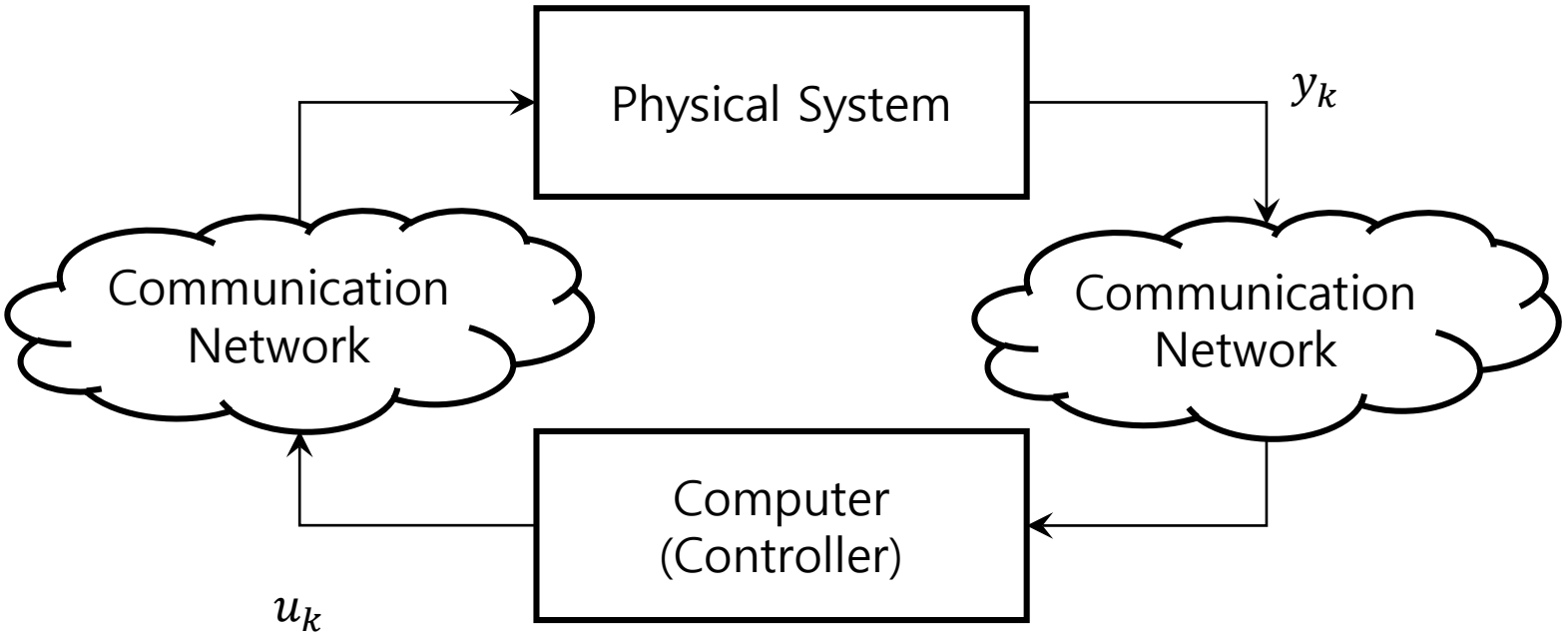
- Cruise control
  - Open loop vs. closed loop



- Shower temperature control

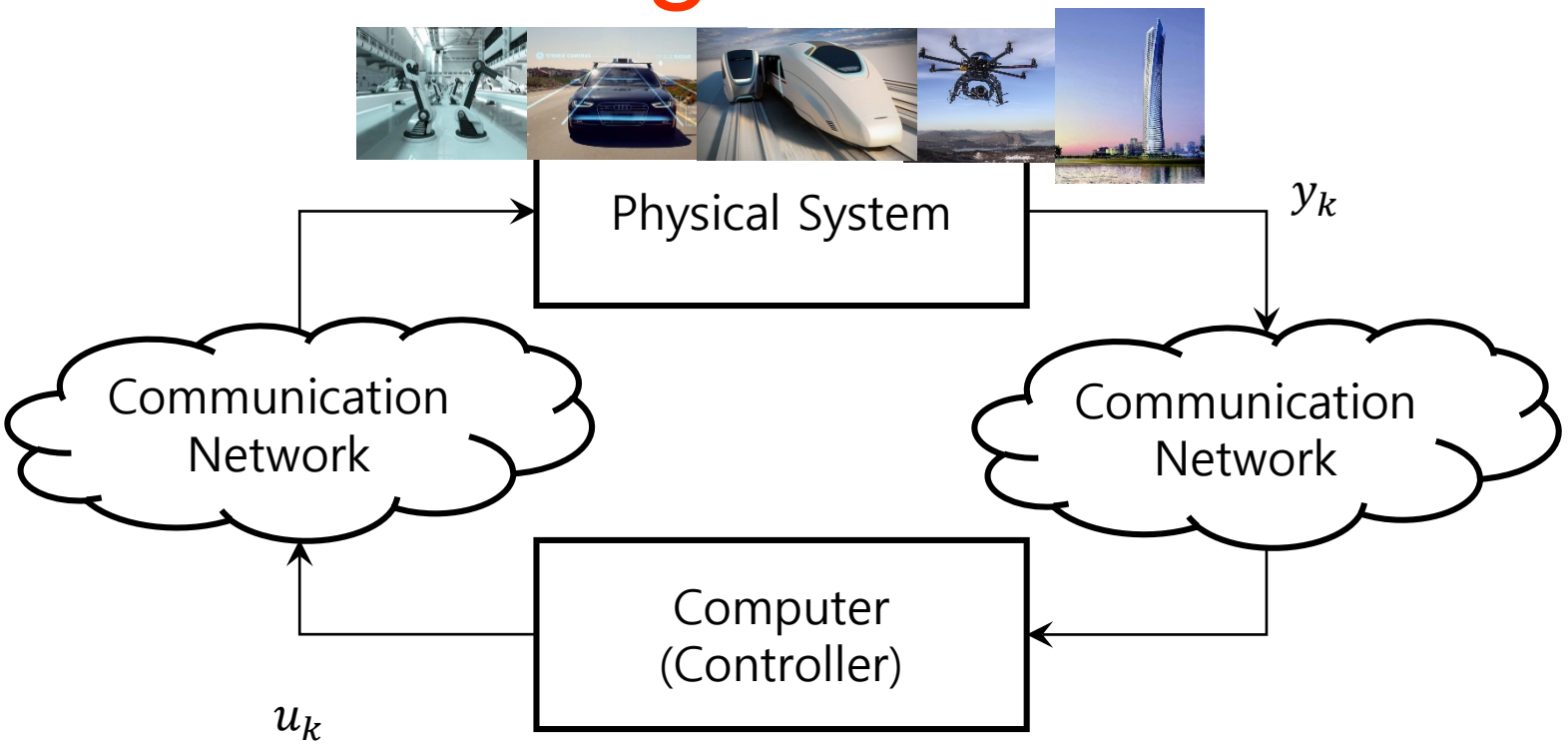


Block diagram of CPS



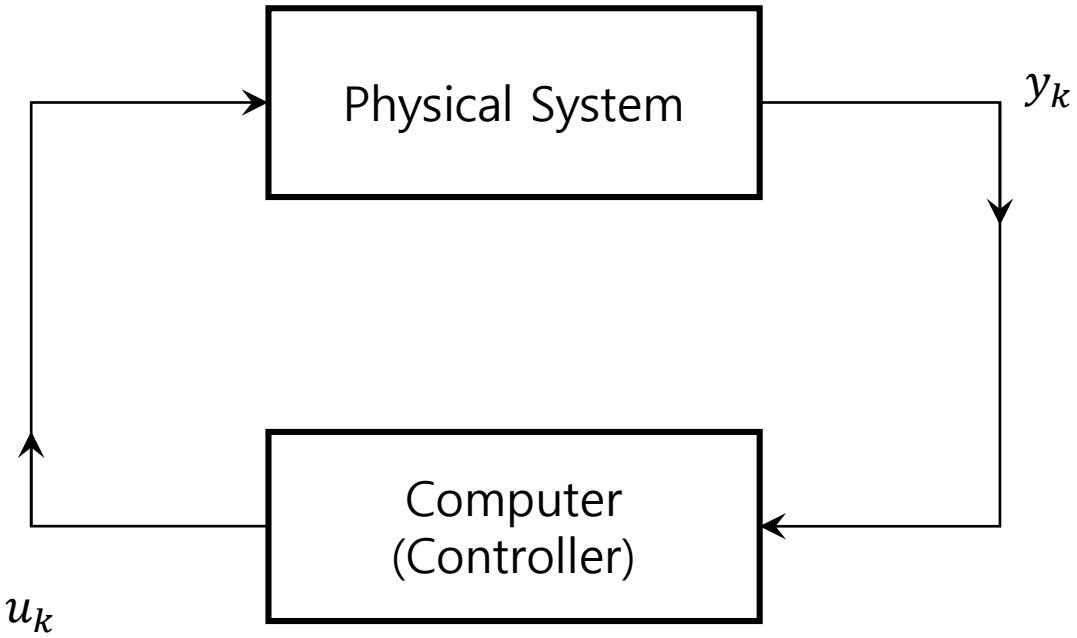
- Nothing new, just networked control system (NCS)
- Agree. But, no unifying theory yet

Block diagram of CPS

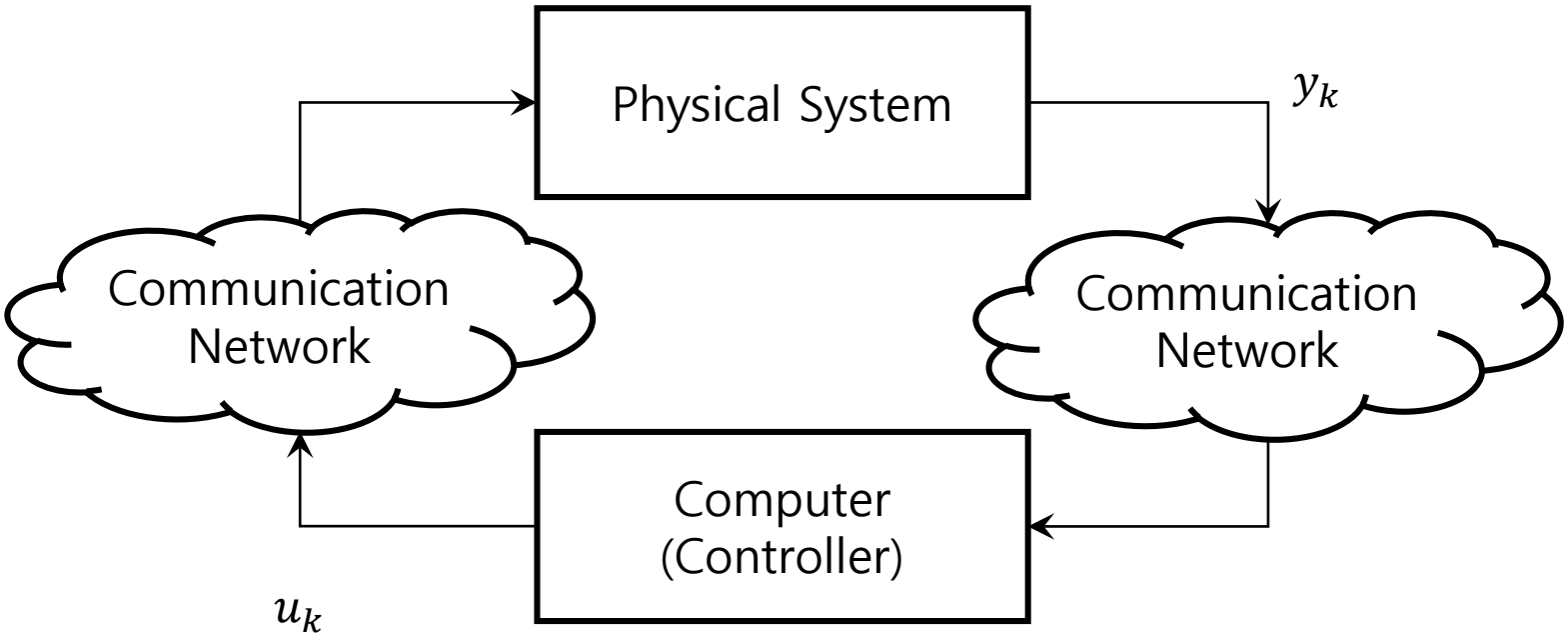


- Nothing new, just networked control system (NCS)
- Agree. But, no unifying theory yet

Typical feedback control system

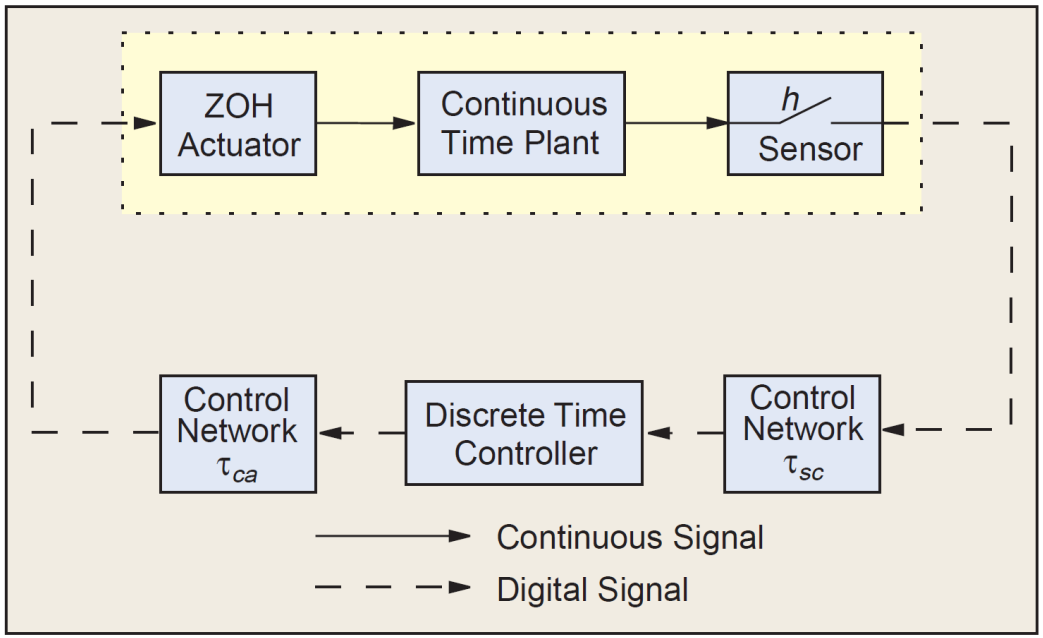


Networked control system (NCS)



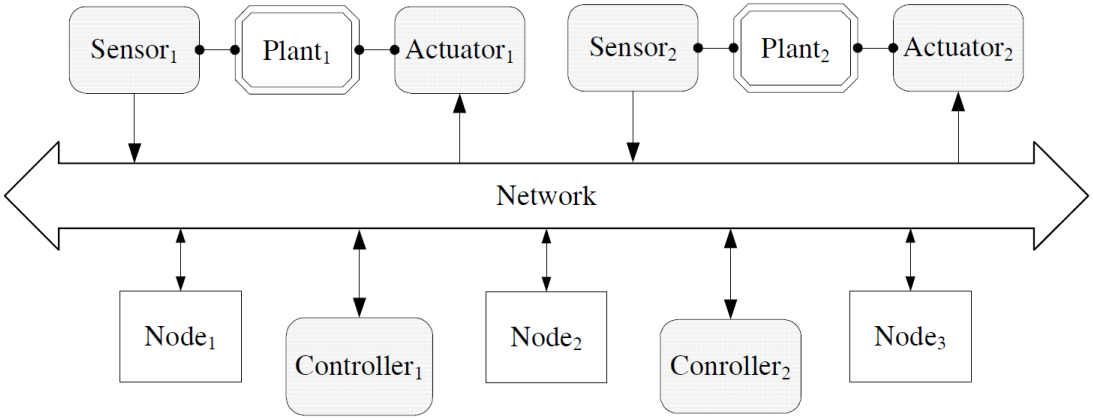
Traditional vs. CPS

- Networked control system
  - Control over networks with delay and packet loss
  - Focus on control or stability of physical systems
  - Control and networking, no (or little) about cyber



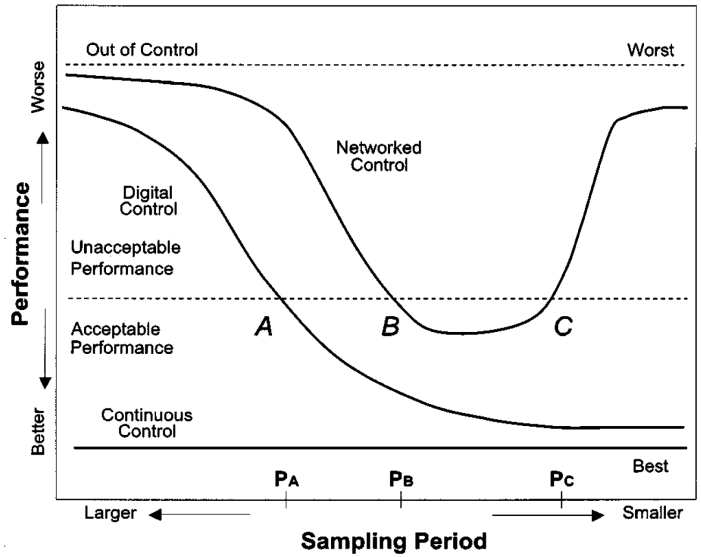
Traditional vs. CPS

- Control and real-time scheduling co-design
  - Control under real-time scheduling constraints
  - Control and cyber, no (or little) about networking



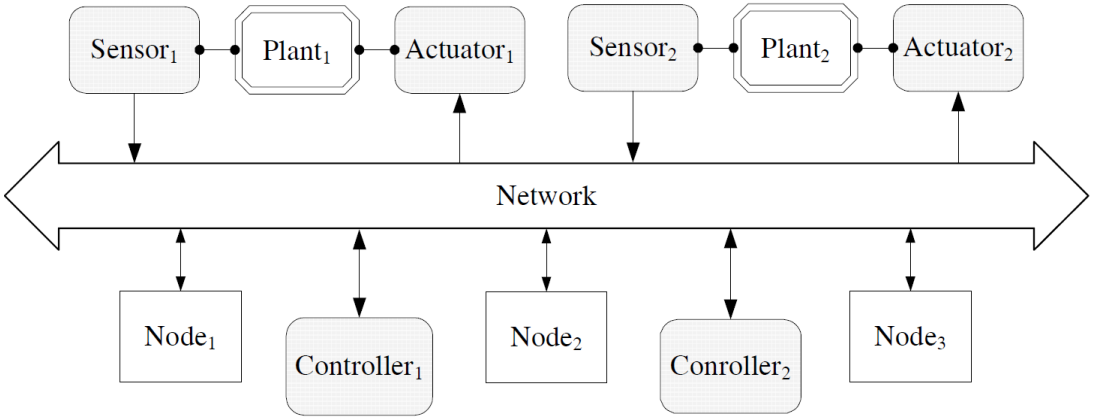
$$\text{maximize } U(\mathbf{p})$$

$$\text{subject to } e2eRspTime_i(\mathbf{p}) \leq p_i, i = 1, \cdots, N$$



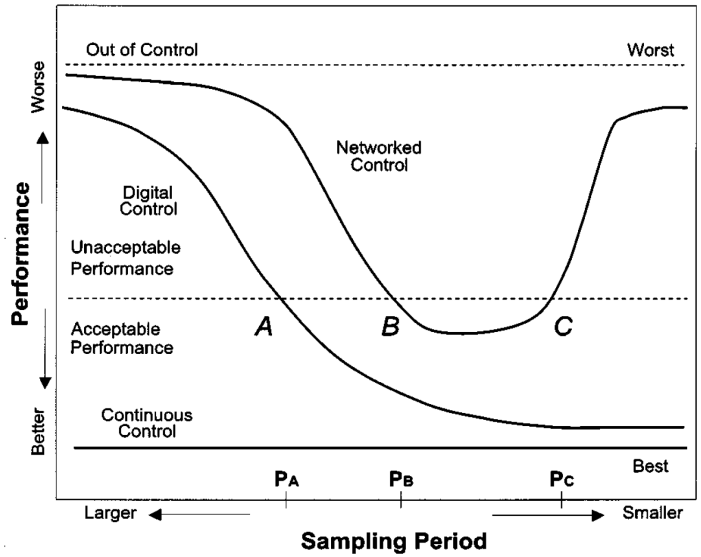
Traditional vs. CPS

- Control and real-time scheduling co-design
  - Control under real-time scheduling constraints
  - Control and cyber, no (or little) about networking



$$\text{maximize } U(\mathbf{p})$$

$$\text{subject to } e2eRspTime_i(\mathbf{p}) \leq p_i, i = 1, \cdots, N$$



- **No unifying theory for physical, cyber, and networking**

Focus on fundamentals, not applications!

- Virtually, every man-made systems are CPS
- So what? We are already studying them in each existing research domain
- **No fundamental theory** on interaction between cyber and physical
  - Understand physical, apply it to cyber and vice versa

Cyber-physical security

SECURITYWEEK NETWORK: Information Security News | Infosec Island | Suits and Spooks

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | Security White Pape

Malware & Threats | Cybercrime | Mobile & Wireless | Risk & Compliance | Security Architecture | Manage

Home > Security Architecture

Cyberphysical Security: The Next Frontier

By Nate Kube on March 23, 2015

Tweet 추천 29 RSS

A debate recently arose within our technical teams, which I feel reflects an industry topic that merits discussion. The term "cybersecurity" has taken on prominence, particularly with the general public, and also with commercial customers. It appears in news headlines, books and more recently, as a corporate initiative rallying cry. Yet for our security specialists, who spend their days deep within industrial systems, the standalone term "cyber" has distinct connotations.

In this column, I'd like to introduce the various perspectives on cybersecurity as a moniker, share some illuminating data, and present a vernacular to move our field forward. First, a technical set of viewpoints on the layman's use of cybersecurity:

Cybersecurity is positioned as a subset of information security (InfoSec): "Cybersecurity is the process of applying security measures to ensure confidentiality, integrity, and availability of data." This hierarchy and definition, argues one of our R&D specialists, limits the role of protection to that of information (data) only.

INFO-CON
디지털
포렌식의 세계
이해하기 쉬우면서도 디지털 포렌식의 세분화된 내용까지 깊이 있게!!

보안뉴스

전체기사 | 사건·사고 | 공공·정책 | 비즈니스 | 국 제 | 테 크 | 오피니언

→ 전체기사

Home > 뉴스 > 전체기사

사이버 공격? 물리적 공격? 이젠 사이버 물리 공격!

입력날짜 : 2015-01-15 16:35 스크랩 프린트하기 목록

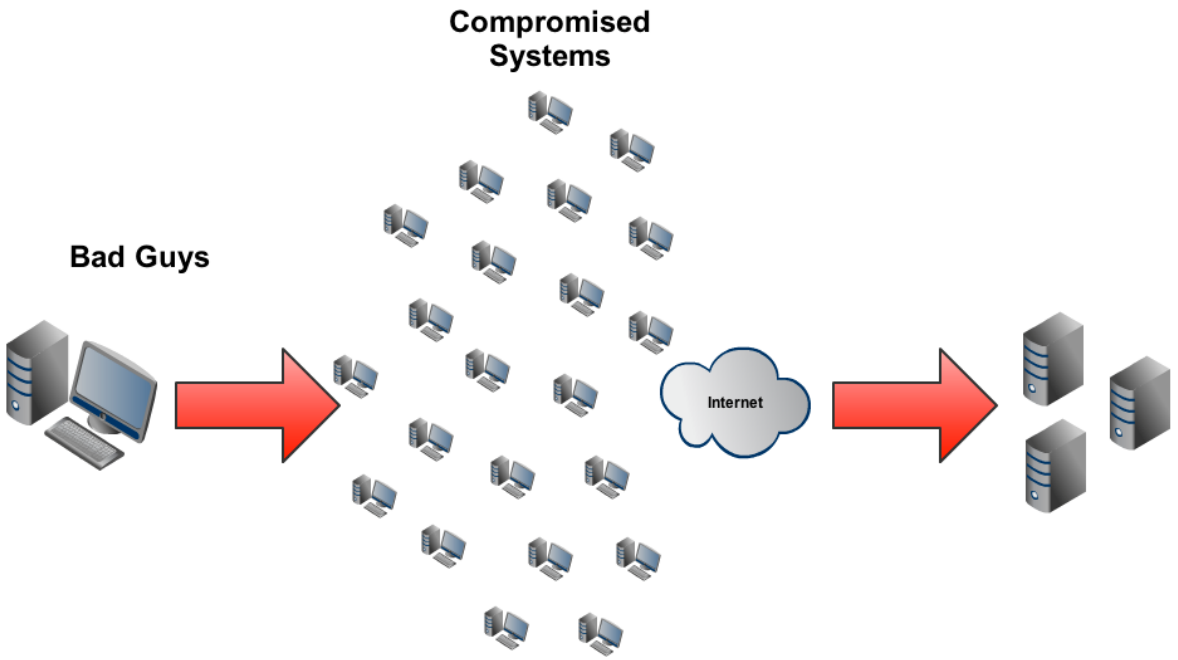
좋아요 54 트윗 2

해커들, 공장이나 발전소 등 주요 시설물 타격위해 공정 과정 공부
기존의 보안 및 방어법으로는 스턱스넷 등 사이버 물리 공격 못 막아

[보안뉴스 문가용] 이란 핵 공장을 겨냥한 스턱스넷의 경우나 한수원 사태 때문에 불거진 발전소 및 공장에 대한 사이버 공격에 대해 해외에서도 한창 연구 분석 중에 있다. 그런데 문제는 '해킹'이 아니다. "해킹만 걱정할 거 같으면 사실 발 뻗고 자도 됩니다. 흔히 상상하는 것처럼 해커가 원격에서 공장이나 발전소를 날려버릴 수는 없기 때문입니다." 랭그너 커뮤니케이션(Langner Communications)의 창립자인 랄프 랭그너(Ralph Langner)가 주장한다. 랄프는 몇 안 되는 스턱스넷 전문가이기도 하다.

Traditional cyber attack

- Cyber-only attack: DDoS
  - Do not care much about how cyber affects physical



Cyber-physical attack? Stuxnet

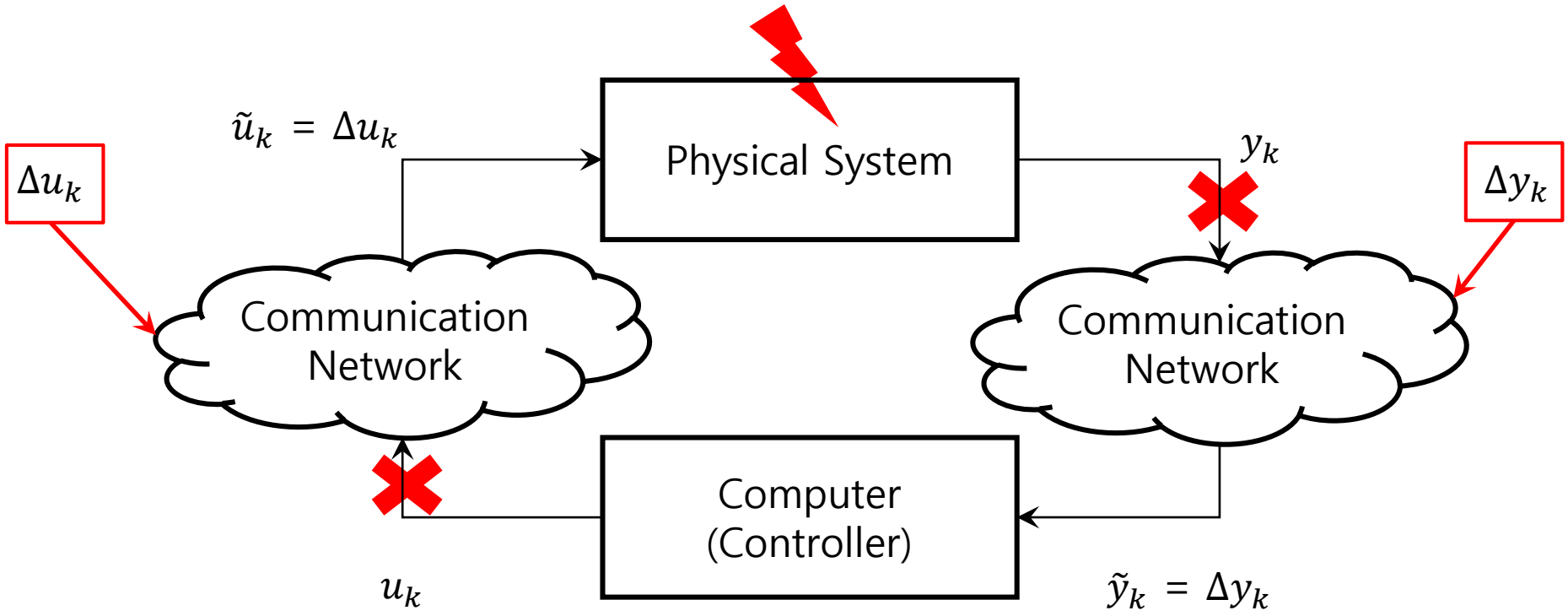
- Cyber-physical attack: Stuxnet
  - Exploits how cyber affects physical
  - Monitors frequency of attached motors, and attacks systems that spin between 807 Hz and 1,210 Hz
  - Periodically modifies frequency to 1,410 Hz and to 2 Hz and to 1,064 Hz, affects operation of connected motors

How Stuxnet works?

- Abruptly change motor frequency while fooling sensors

How Stuxnet works?

- Abruptly change motor frequency while fooling sensors



How Stuxnet fool the sensors?

How Stuxnet fool the sensors?

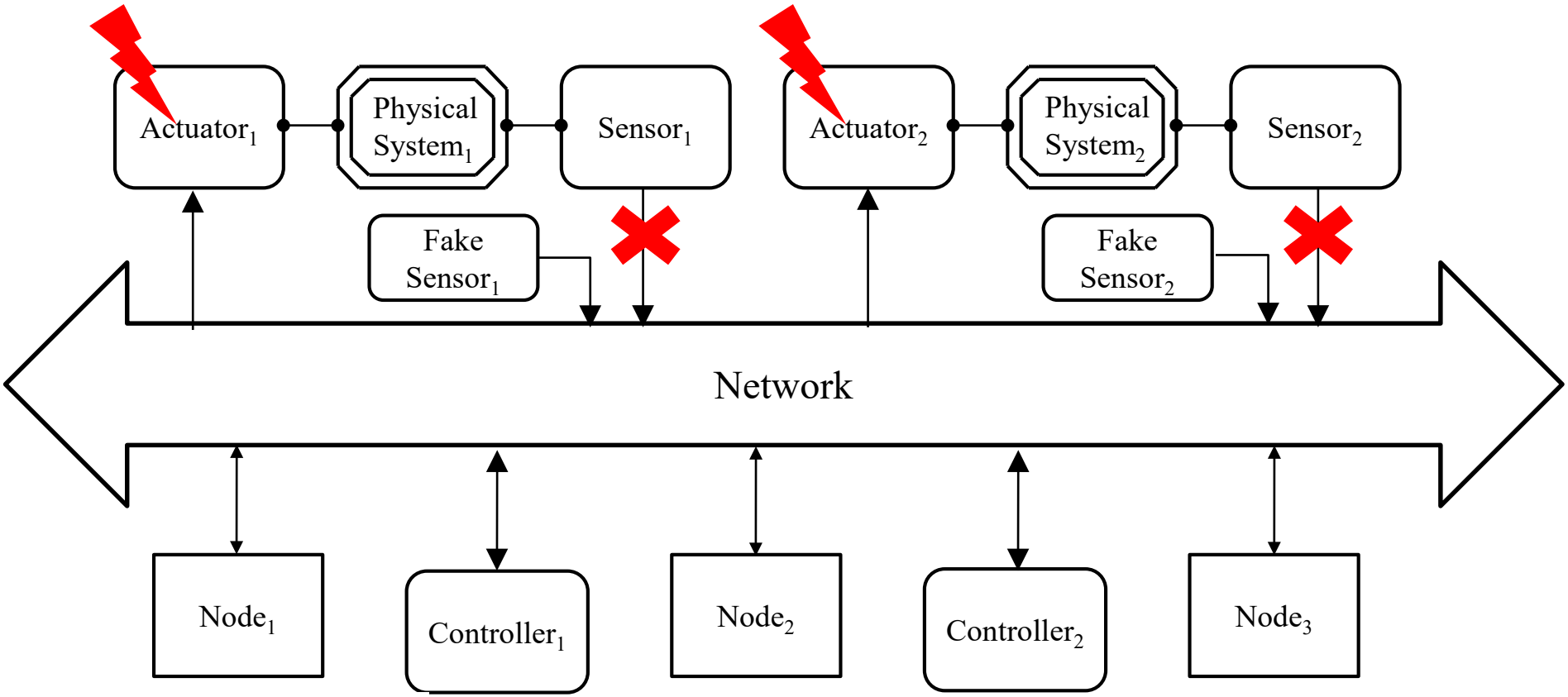
How Stuxnet fool the sensors?

How Stuxnet fool the sensors?

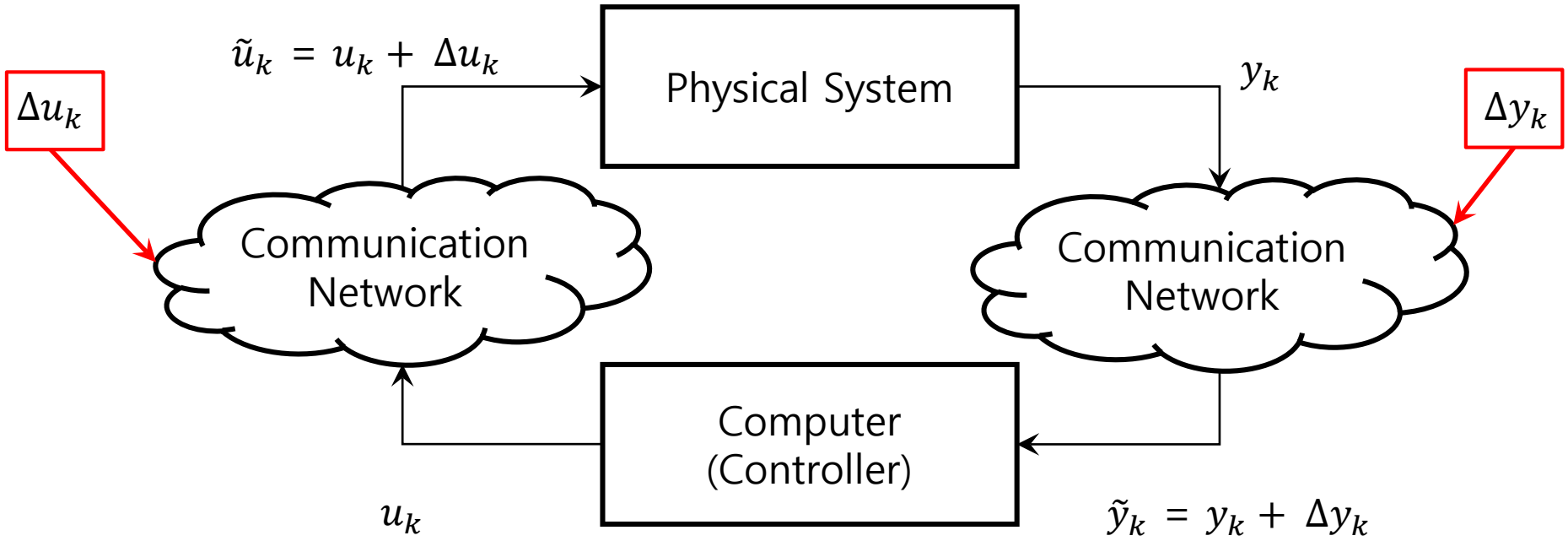
Replay attack!

How Stuxnet works?

- Abruptly change motor frequency while fooling sensors

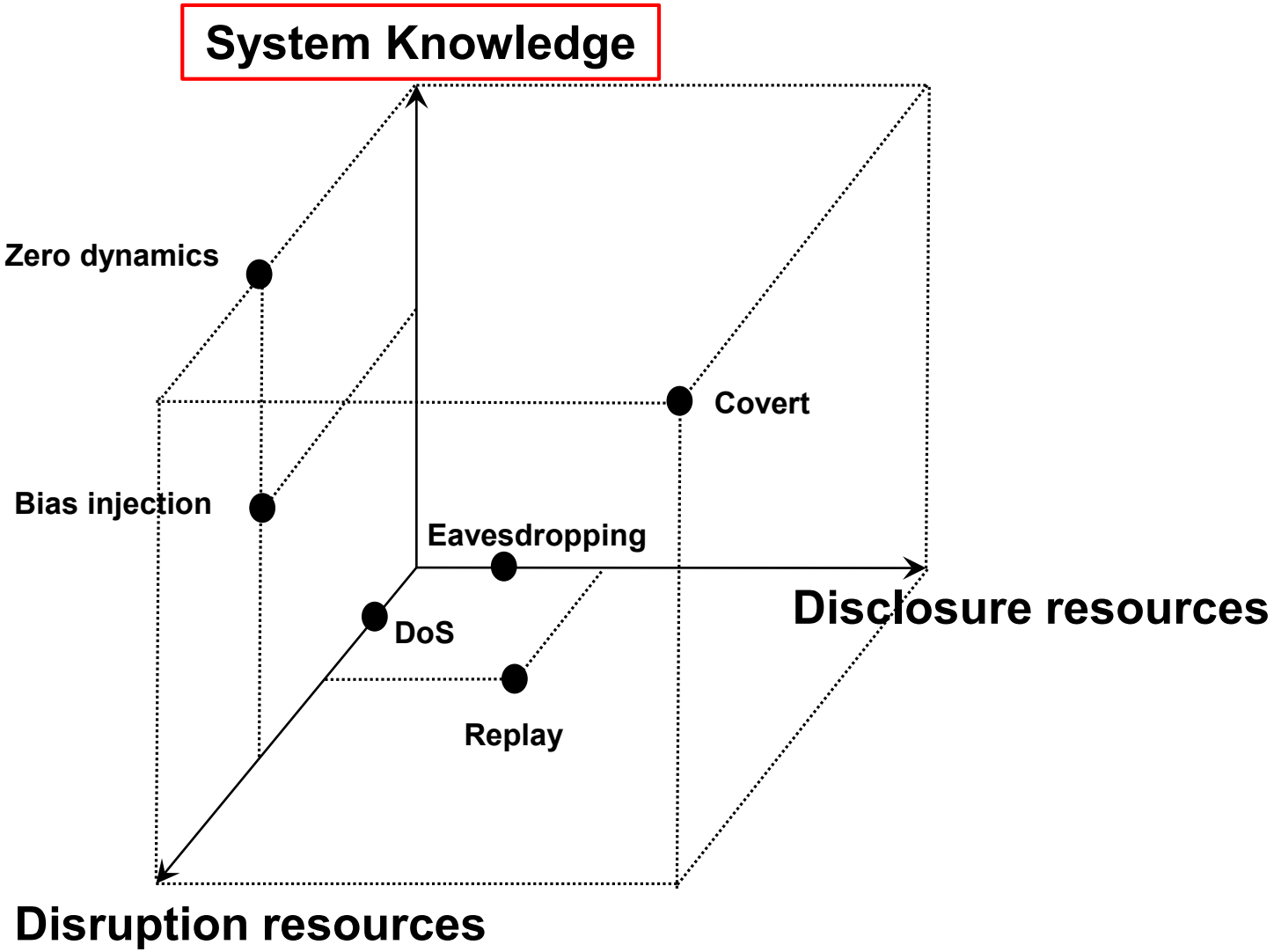


CPS under attack

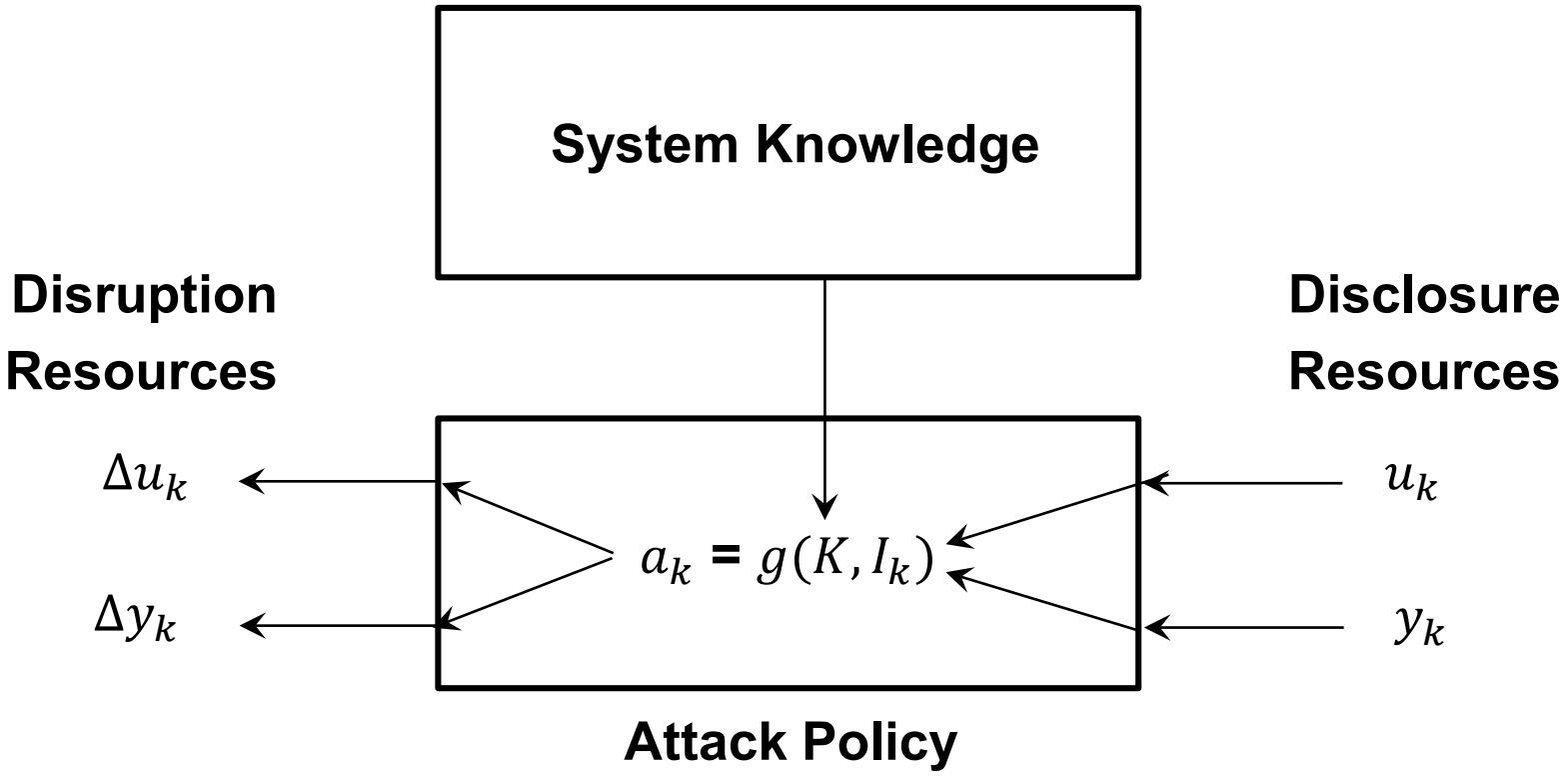


Credit: Texeira et al, IEEE CSM Jan. 2015

Cyber-physical attack space



CPS adversary model



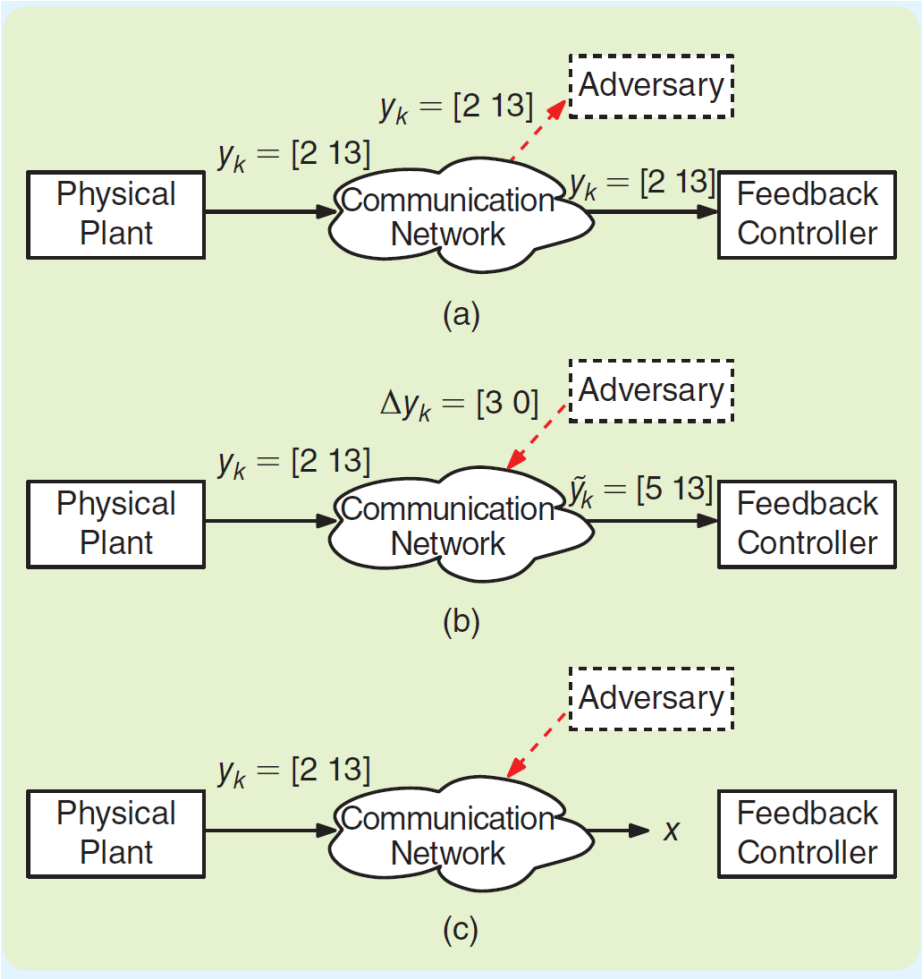
Credit: Texeira et al, IEEE CSM Jan. 2015

CIA in CPS

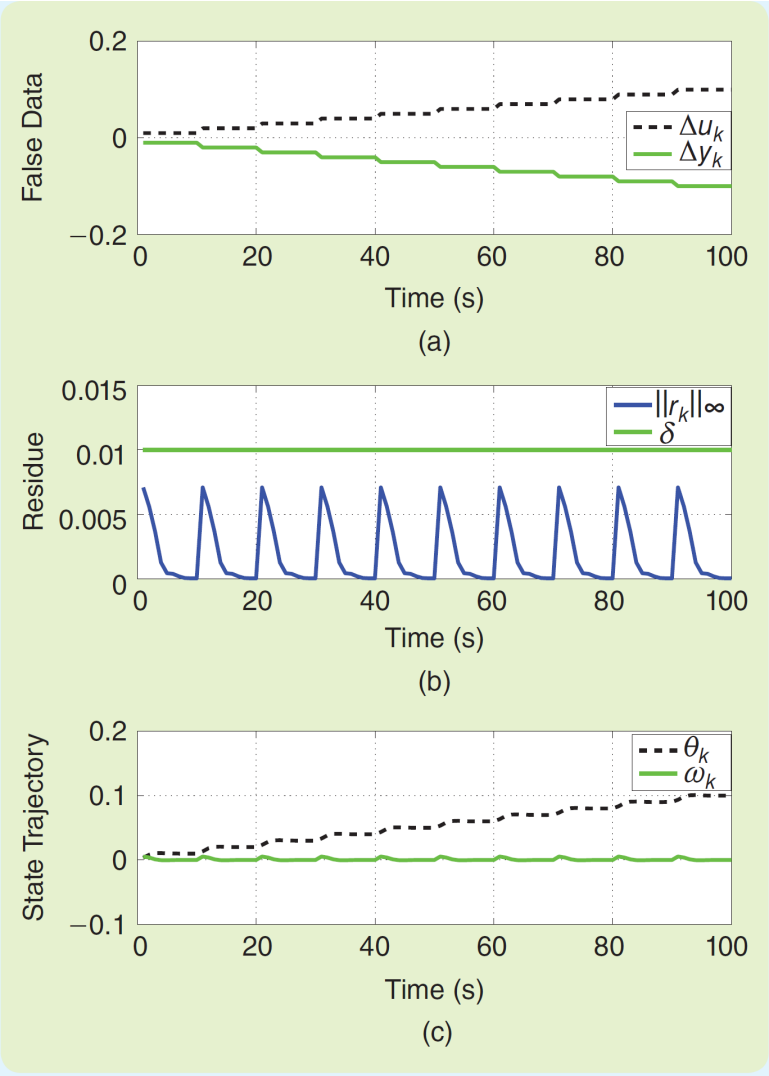
Confidentiality

Integrity

Availability

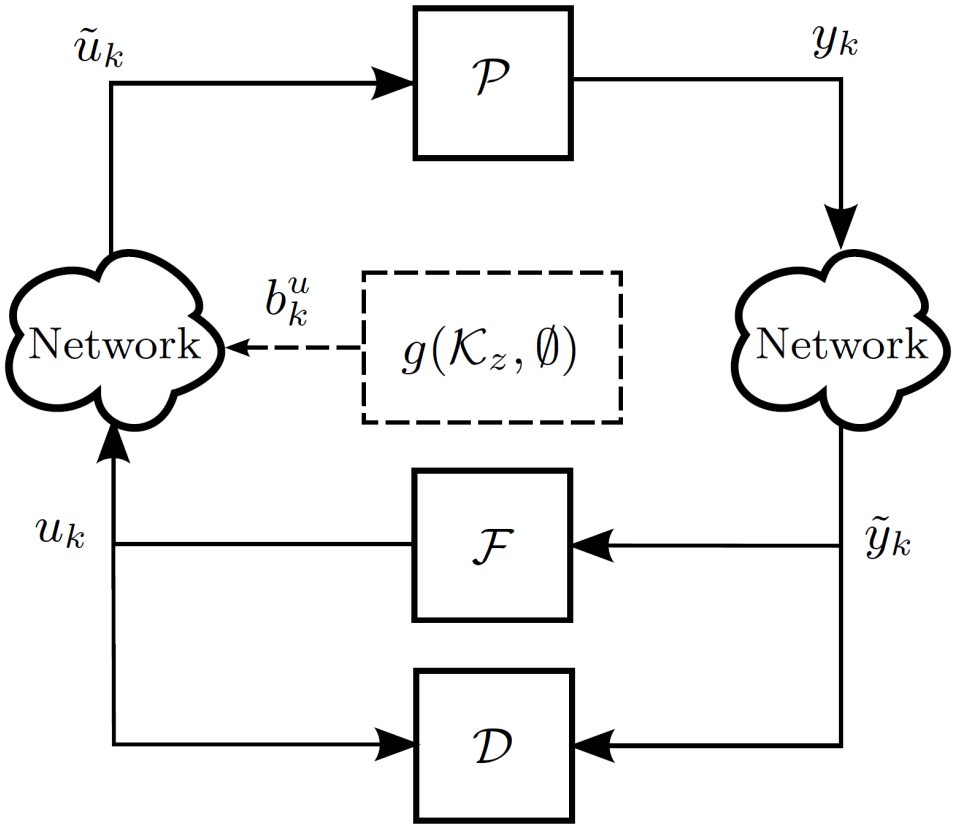


Zero-dynamics attack



Credit: Texeira et al, IEEE CSM Jan. 2015

Zero dynamics attack



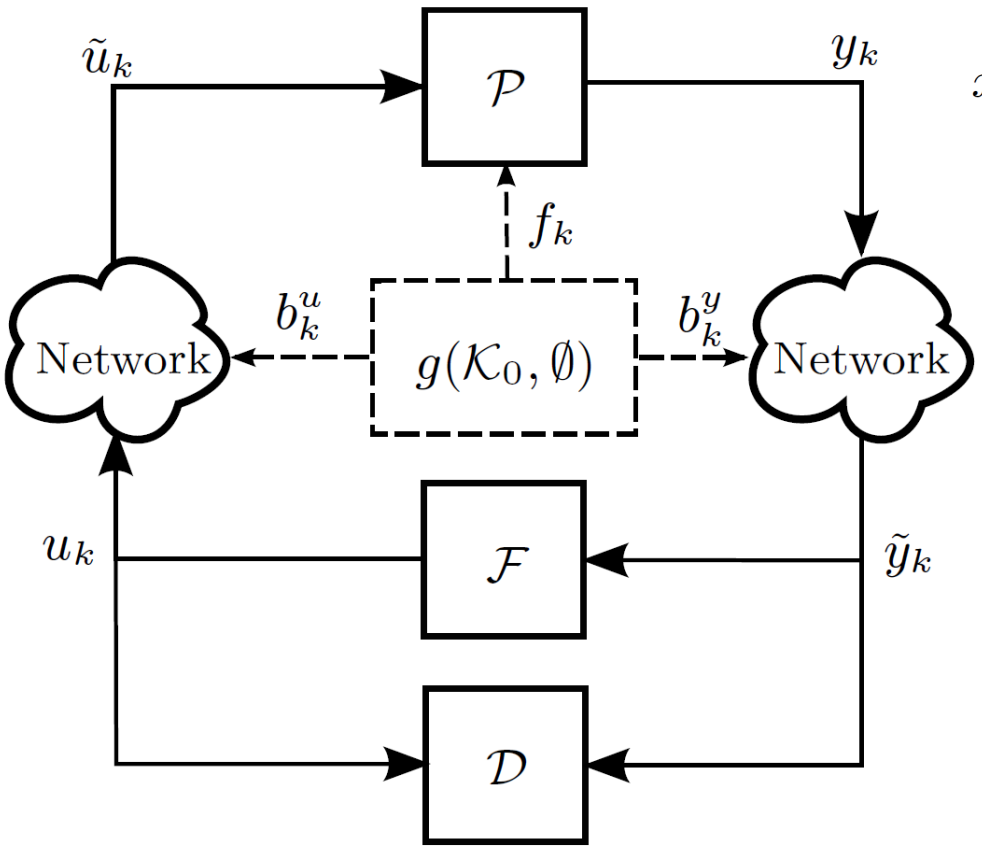
$$x_{k+1}^a = Ax_k^a + Ba_k$$
$$\tilde{y}_k^a = Cx_k^a$$

$$a_k = g\nu^k$$

$$\begin{bmatrix} \nu I - A & -B \\ C & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ g \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Credit: Texeira et al, IEEE CSM Jan. 2015

Bias injection attack



$$x_\infty^a = [I \quad 0]\,(I - \mathbf{A}_c)^{-1}\,\mathbf{B}_c a_\infty =: G_{xa} a_\infty$$

$$\max_{a_\infty} \|G_{xa} a_\infty\|_2^2$$

$$\text{s.t.} \qquad \|G_{ra} a_\infty\|_2^2 \leq \delta_\alpha^2$$

Credit: Texeira et al, IEEE CSM Jan. 2015

Models

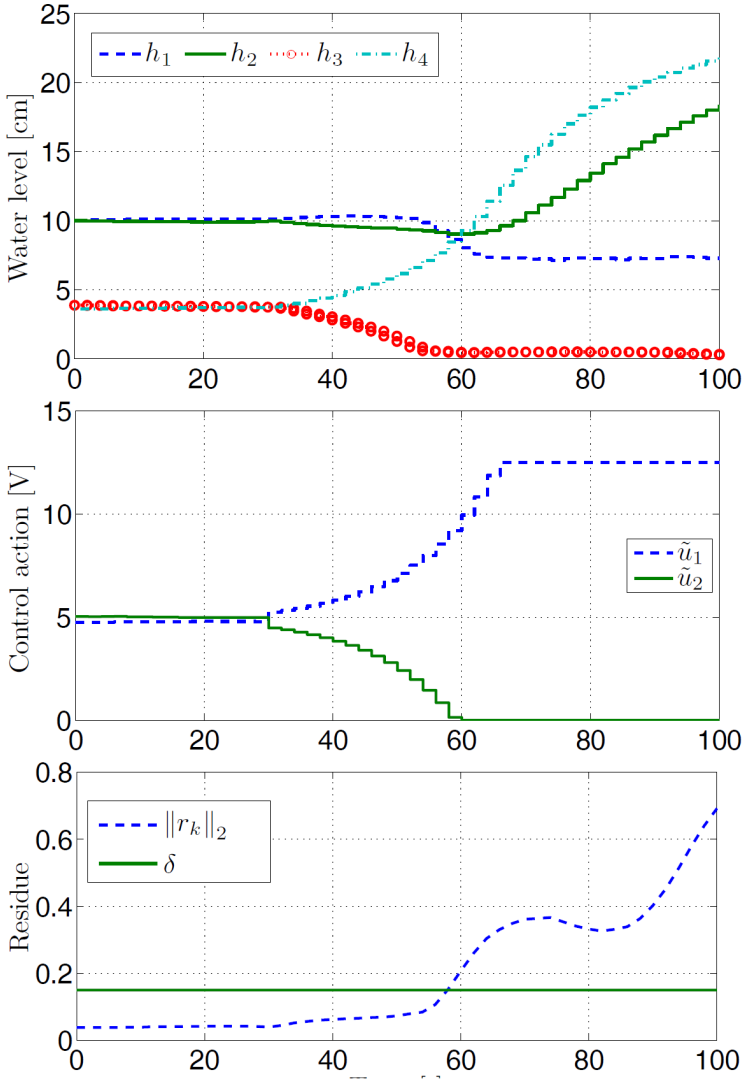
$$\mathcal{P}: \begin{cases} x_{k+1} = Ax_k + B\tilde{u}_k + Gw_k + Ff_k \\ y_k = Cx_k + v_k \end{cases}$$

$$\mathcal{F}: \begin{cases} z_{k+1} = A_c z_k + B_c \tilde{y}_k \\ u_k = C_c z_k + D_c \tilde{y}_k \end{cases}$$

$$\mathcal{D}: \begin{cases} \hat{x}_{k|k} = A\hat{x}_{k-1|k-1} + Bu_{k-1} + K(\tilde{y}_k - \hat{y}_{k|k-1}) \\ r_k = V(\tilde{y}_k - \hat{y}_{k|k}) \end{cases}$$

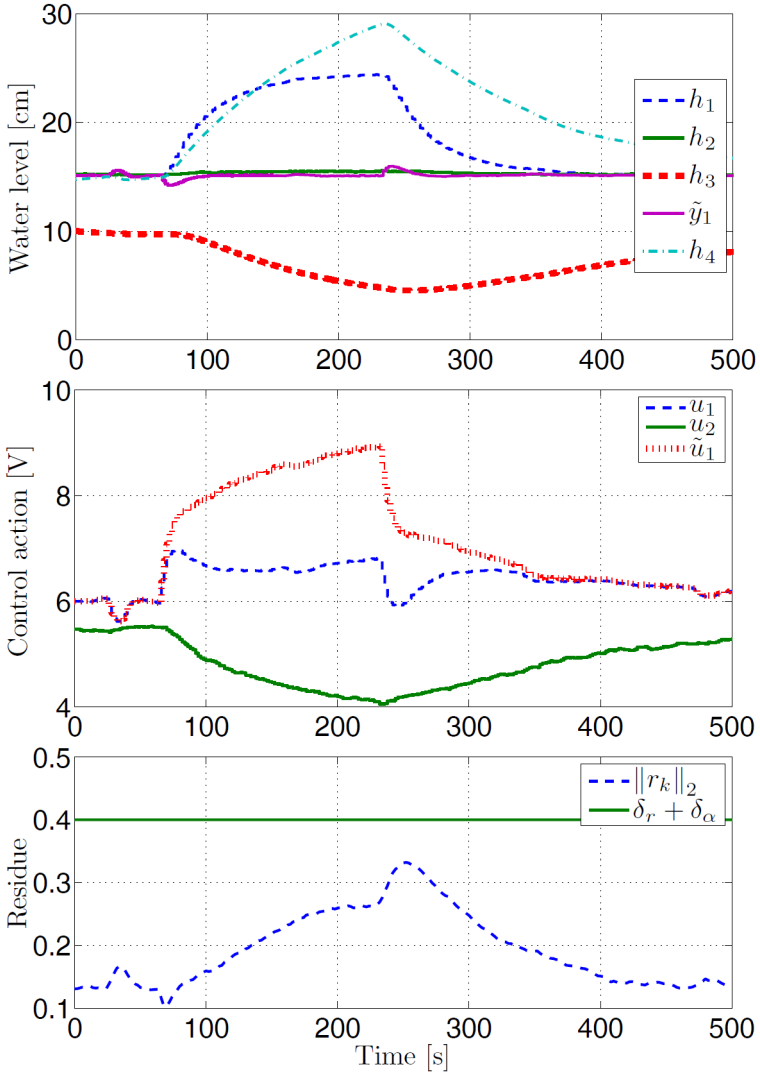
Credit: Texeira et al, IEEE CSM Jan. 2015

Quadruple-tank: Zero dynamics attack



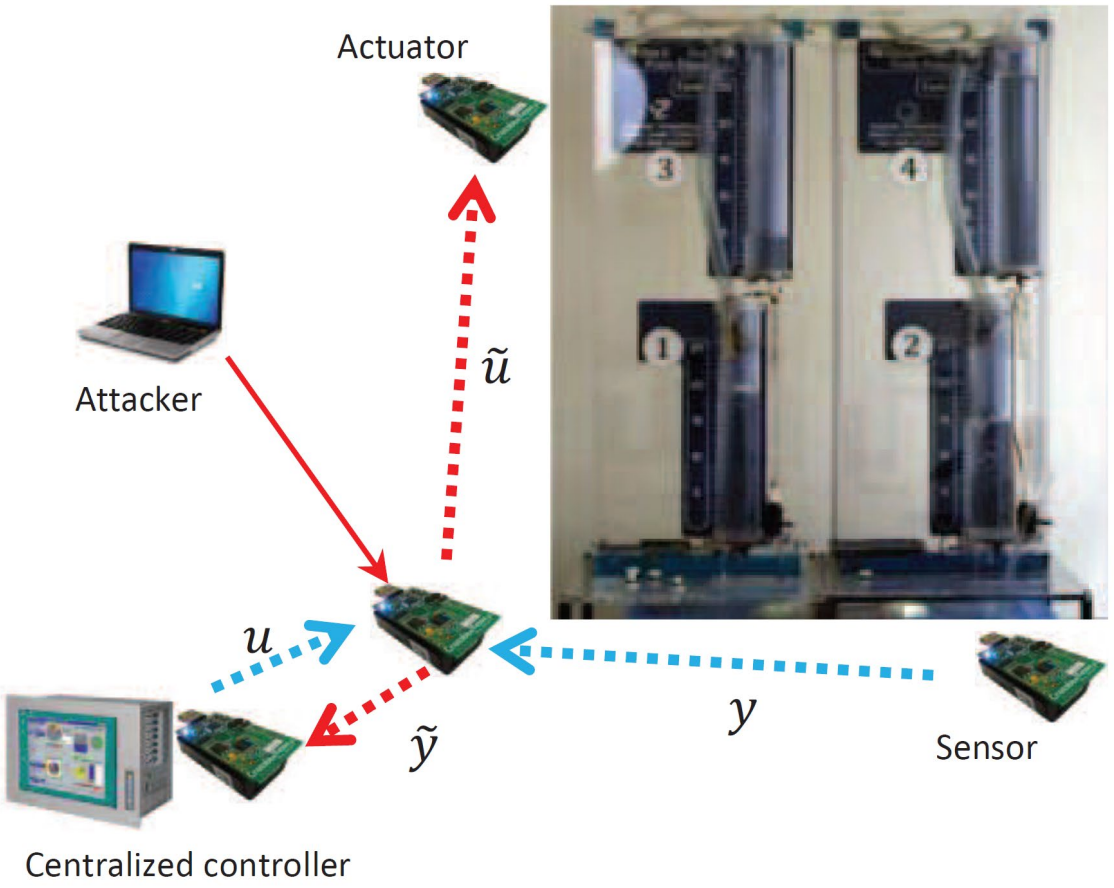
Credit: Texeira et al, IEEE CSM Jan. 2015

Quadruple-tank: bias attack



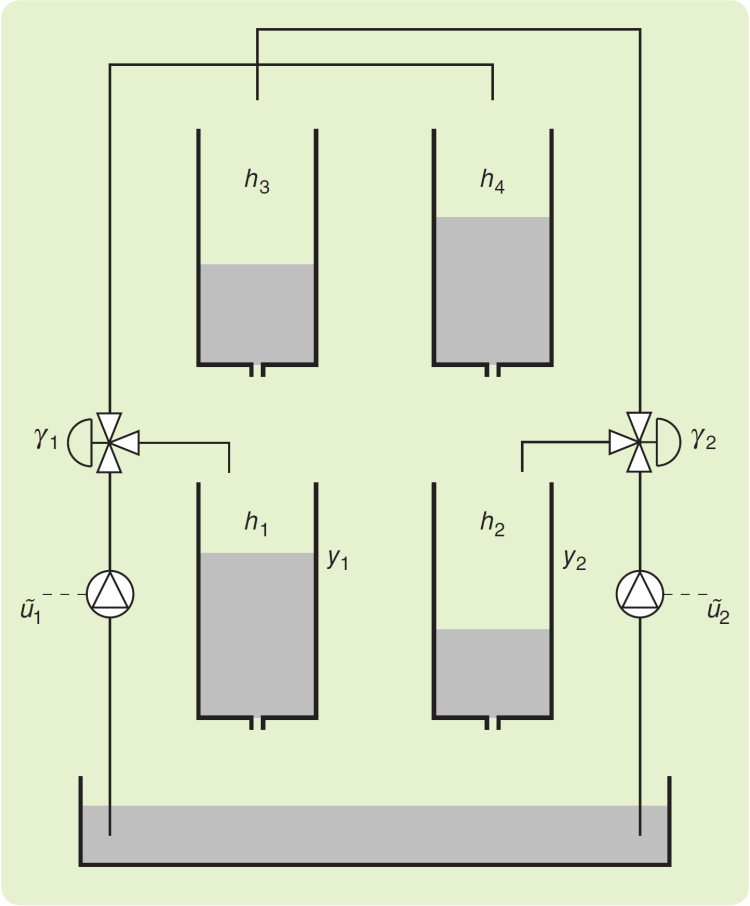
Credit: Texeira et al, IEEE CSM Jan. 2015

Quadruple-tank process



Credit: Texeira et al, IEEE CSM Jan. 2015

Quadruple-tank model



$$\frac{dh_1}{dt} = -\frac{a_1}{A_1}\sqrt{2gh_1} + \frac{a_3}{A_1}\sqrt{2gh_3} + \frac{\gamma_1 k_1}{A_1}u_1,$$

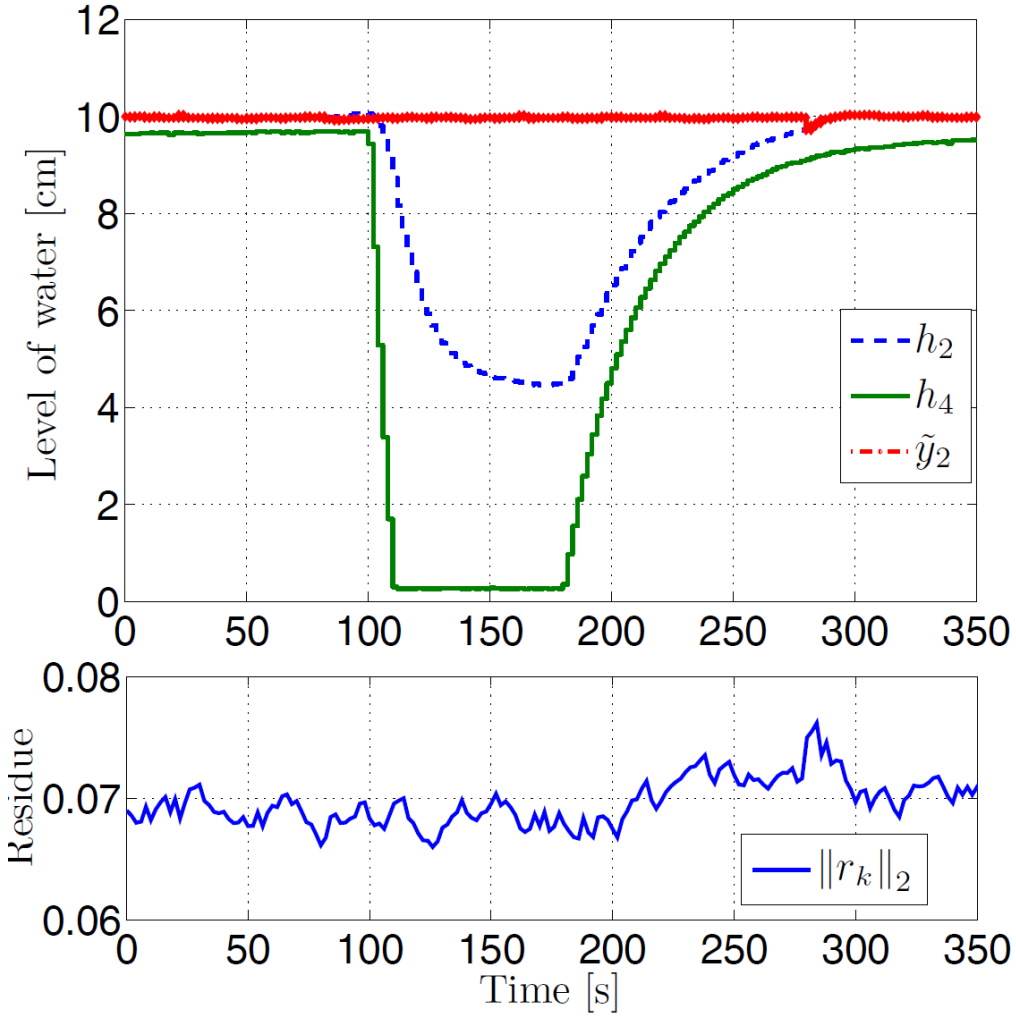
$$\frac{dh_2}{dt} = -\frac{a_2}{A_2}\sqrt{2gh_2} + \frac{a_4}{A_2}\sqrt{2gh_4} + \frac{\gamma_2 k_2}{A_2}u_2,$$

$$\frac{dh_3}{dt} = -\frac{a_3}{A_3}\sqrt{2gh_3} + \frac{(1-\gamma_2)k_2}{A_3}u_2,$$

$$\frac{dh_4}{dt} = -\frac{a_4}{A_4}\sqrt{2gh_4} + \frac{(1-\gamma_1)k_1}{A_4}u_1,$$

Credit: Texeira et al, IEEE CSM Jan. 2015

Quadruple-tank: Replay attack



Credit: Texeira et al, IEEE CSM Jan. 2015

Models

$$\mathcal{P}: \begin{cases} x_{k+1} = Ax_k + B\tilde{u}_k + Gw_k + Ff_k \\ y_k = Cx_k + v_k \end{cases}$$

$$\mathcal{F}: \begin{cases} z_{k+1} = A_c z_k + B_c \tilde{y}_k \\ u_k = C_c z_k + D_c \tilde{y}_k \end{cases}$$

Models

$$\mathcal{P}: \begin{cases} x_{k+1} = Ax_k + B\tilde{u}_k + Gw_k + Ff_k \\ y_k = Cx_k + v_k \end{cases}$$

Physical system model

$$\mathcal{F}: \begin{cases} z_{k+1} = A_c z_k + B_c \tilde{y}_k \\ u_k = C_c z_k + D_c \tilde{y}_k \end{cases}$$

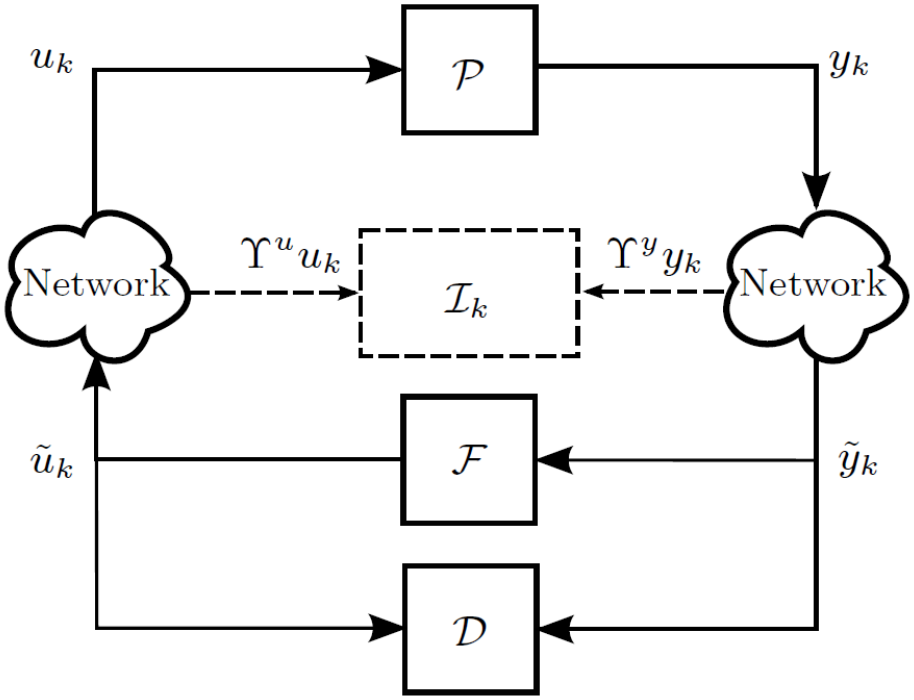
Models

$$\mathcal{P}: \begin{cases} x_{k+1} = Ax_k + B\tilde{u}_k + Gw_k + Ff_k \\ y_k = Cx_k + v_k \end{cases}$$

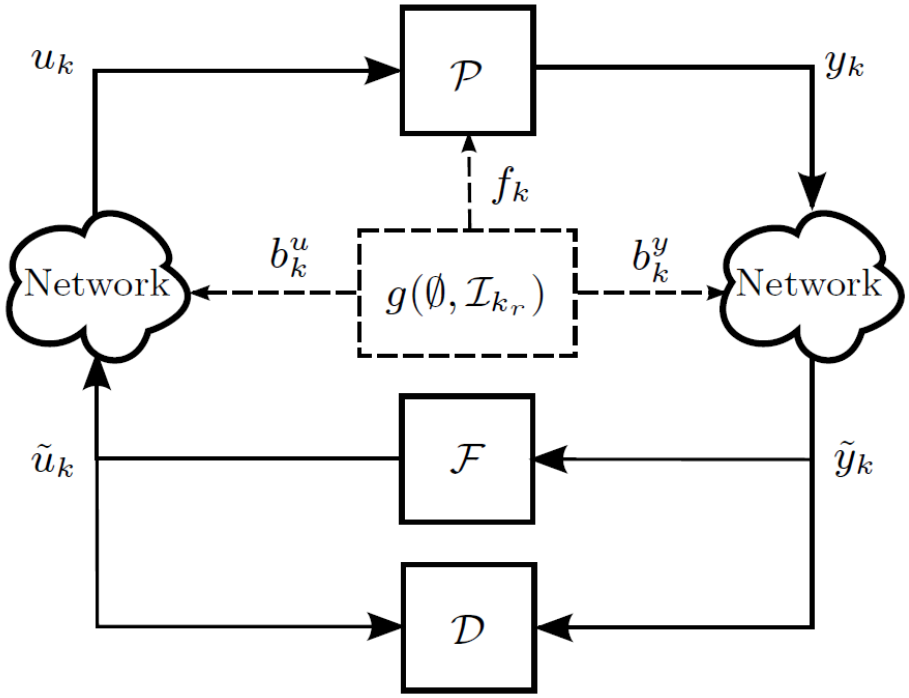
$$\mathcal{F}: \begin{cases} z_{k+1} = A_c z_k + B_c \tilde{y}_k \\ u_k = C_c z_k + D_c \tilde{y}_k \end{cases}$$

Feedback controller model

Replay attack

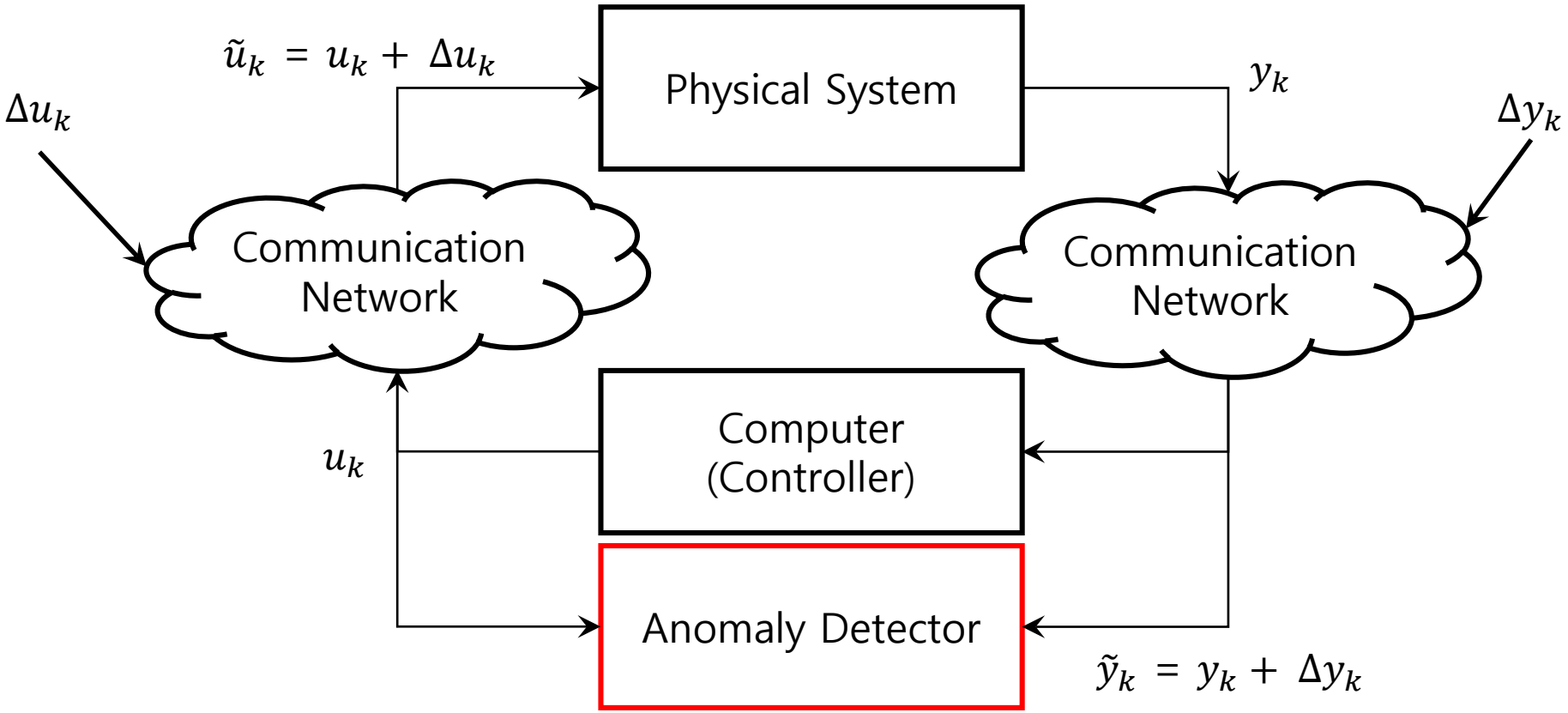


Phase I of replay attack



Phase II of replay attack

Anomaly detector for CPS attack



Anomaly detector

$$\mathcal{D}: \begin{cases} \hat{x}_{k|k} = A\hat{x}_{k-1|k-1} + Bu_{k-1} + K(\tilde{y}_k - \hat{y}_{k|k-1}) \\ r_k = V(\tilde{y}_k - \hat{y}_{k|k}) \end{cases}$$

1. under nominal behavior of the system (i.e., $f_k = 0$, $u_k = \tilde{u}_k$, $y_k = \tilde{y}_k$), the expected value of the residue converges asymptotically to a neighborhood of zero, i.e., $\lim_{k\to\infty} \|\mathbb{E}\{r_k\}\| \leq \delta_r$, with $\delta_r \in \mathbb{R}^+$;

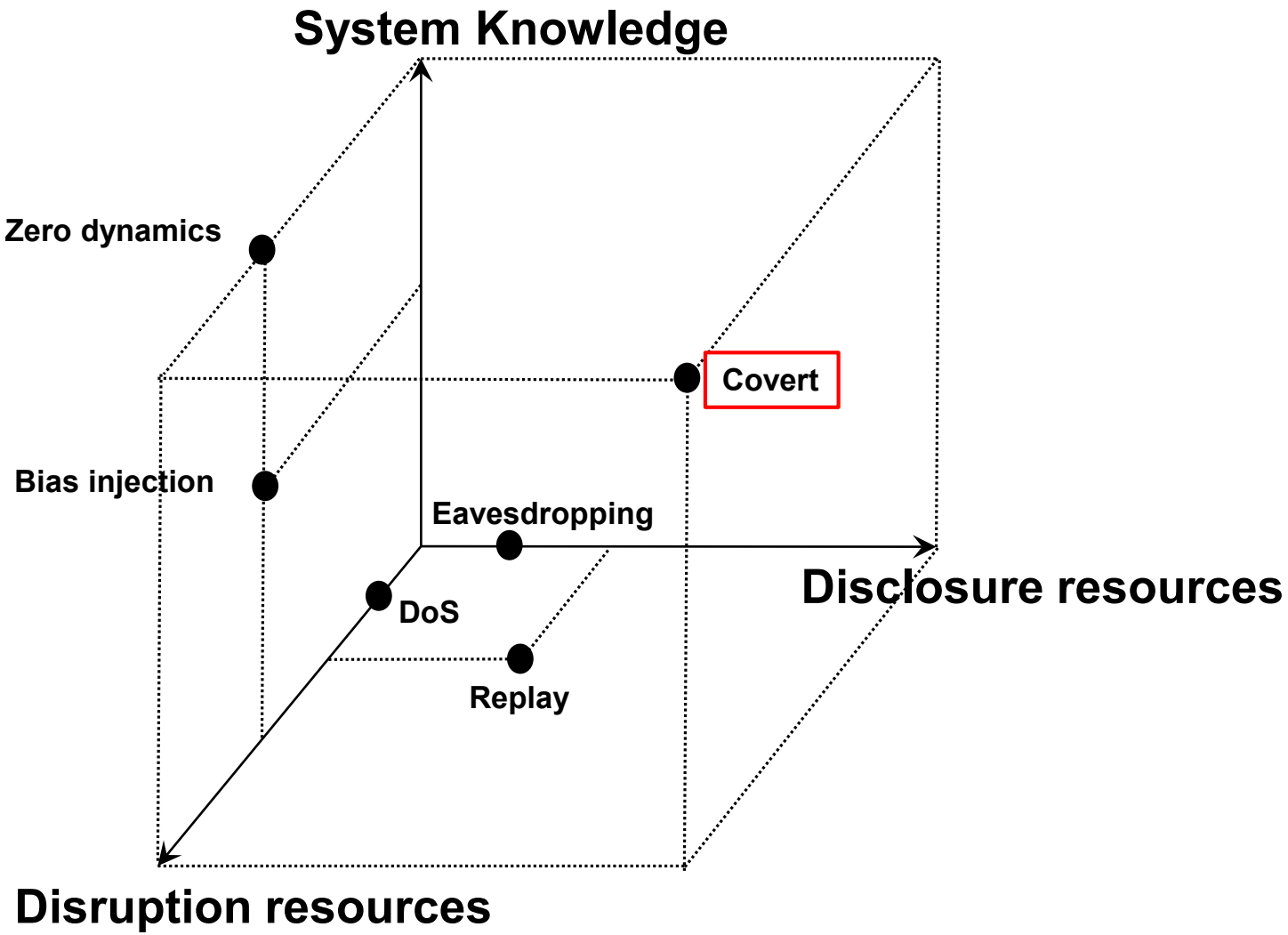
2. the residue is sensitive to the anomalies ($f_k \not\equiv 0$).

An alarm is triggered if the residue meets

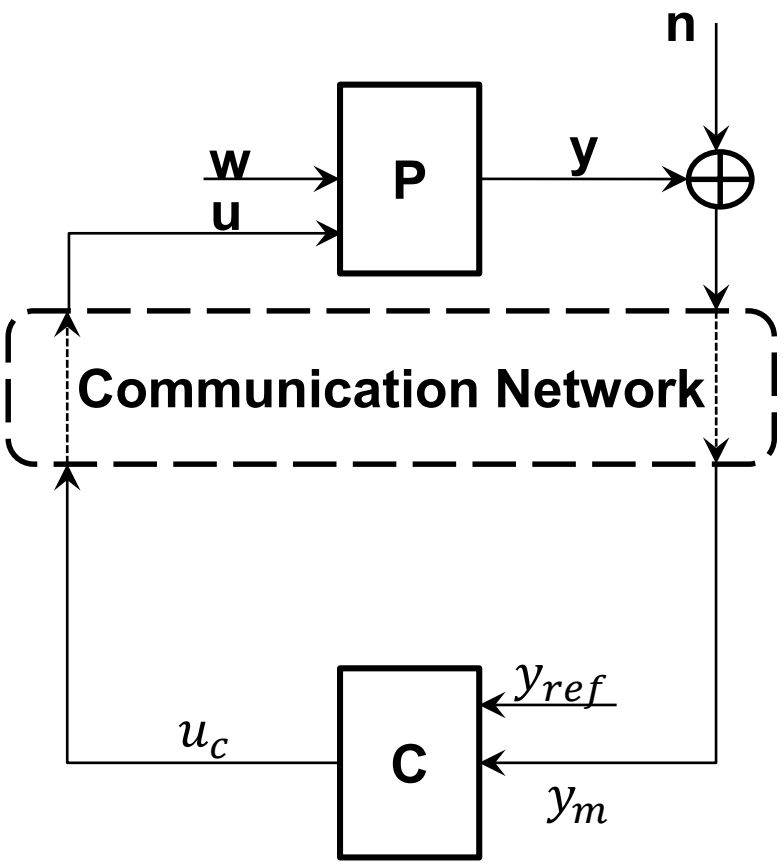
$$\|r_k\| \geq \delta_r + \delta_\alpha,$$

where $\delta_\alpha \in \mathbb{R}^+$ is chosen so that the false alarm rate does not exceed a given $\alpha \in [0, 1]$.

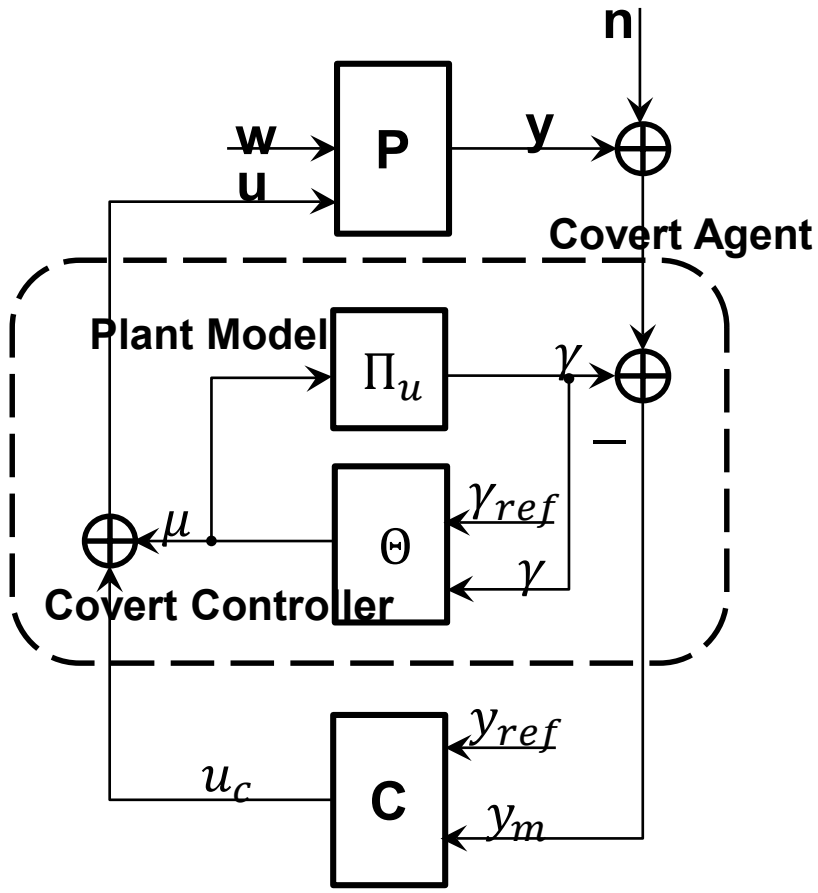
What if covert attack?



Covert attack



Nominal Controller



Nominal Controller

Covert attack analysis

$$y_m = SP_u C_{\text{ref}} y_{\text{ref}} + SP_w w + Sn,$$

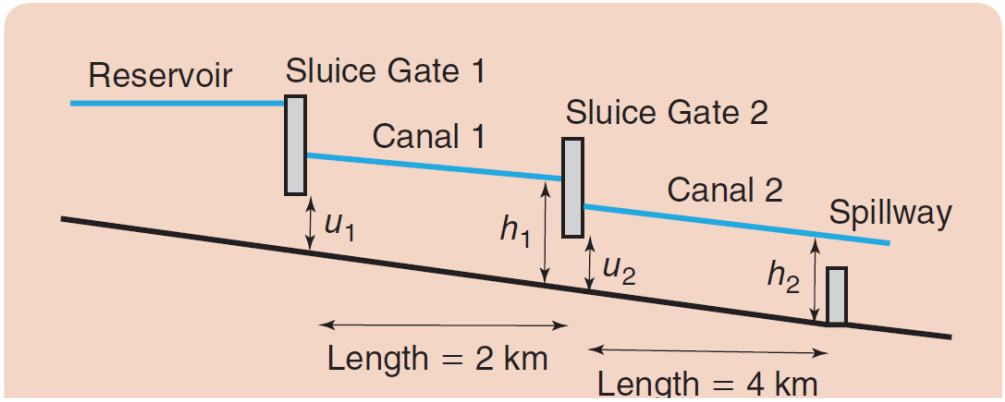
$$y_m = SP_u C_{\text{ref}} y_{\text{ref}} + SP_w w + Sn + S(P_u - \Pi_u)\mu.$$

$$w_{\text{covert}} = S(P_u - \Pi_u)(I - \Theta_\gamma \Pi_u)^{-1} \Theta_{\text{ref}} \gamma_{\text{ref}}.$$

With perfect knowledge of physical system

$P_u - \Pi_u = 0$ → covert action is undetectable!

Covert attack: Example



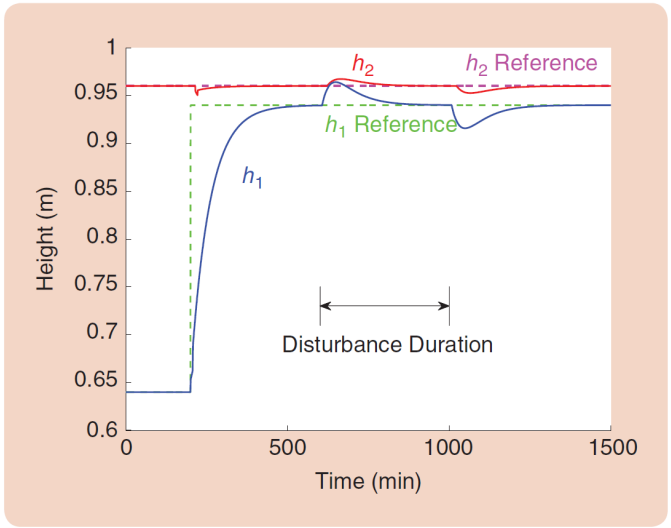


FIGURE 4 A nominal canal control system response. A reference step change of 0.1 m in h_1 is applied at 200 min. The h_2 reference is held constant throughout. From 600 min to 1000 min, an unmeasured flow disturbance (equivalent to raising the sluice gate u_1 by

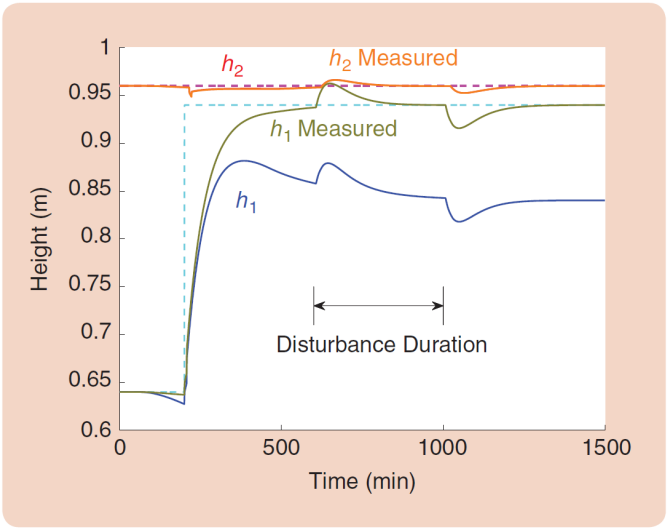
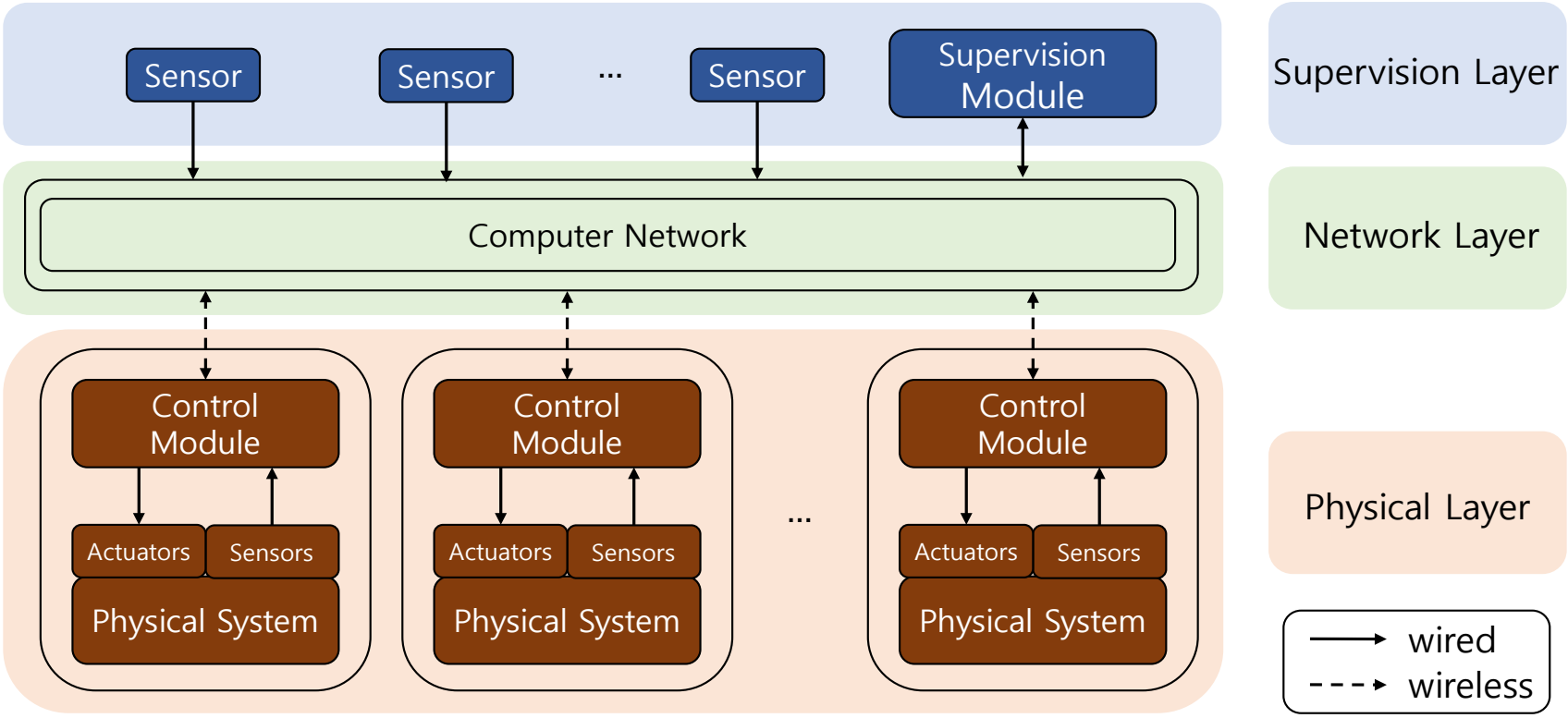


FIGURE 5 A misappropriated canal control system response. The reference and disturbances signals are identical to those in Figure 4. At 50 min, the covert agent's offset reference ξ_{ref} applies a ramp signal of 400 min duration setting the covert h_1 offset to −0.1 m.

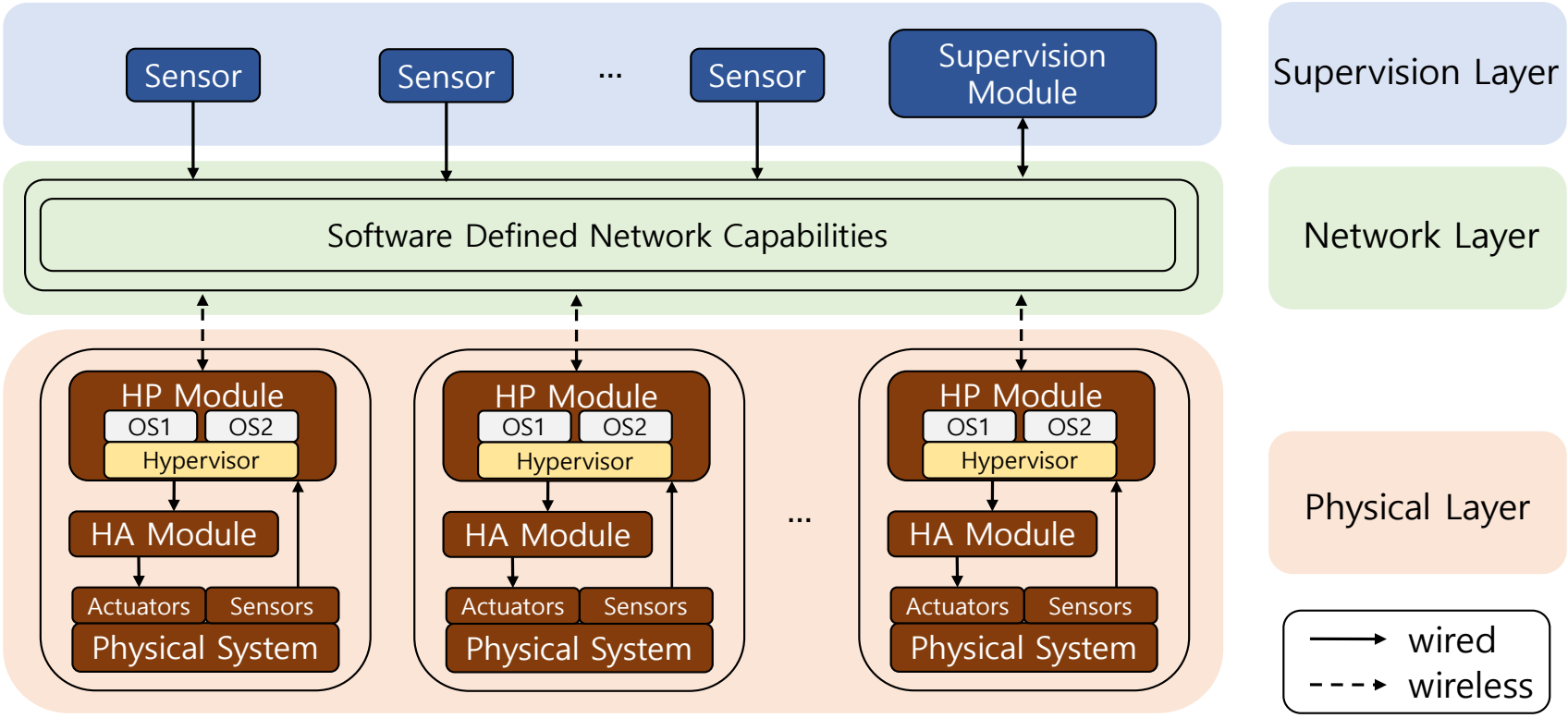
Attack-resilient CPS

- **Resilience**
  - Maintain normal operation in presence of attacks or faults
  - Maintain core function if normal operation is not possible
  - Fail gracefully when inevitable

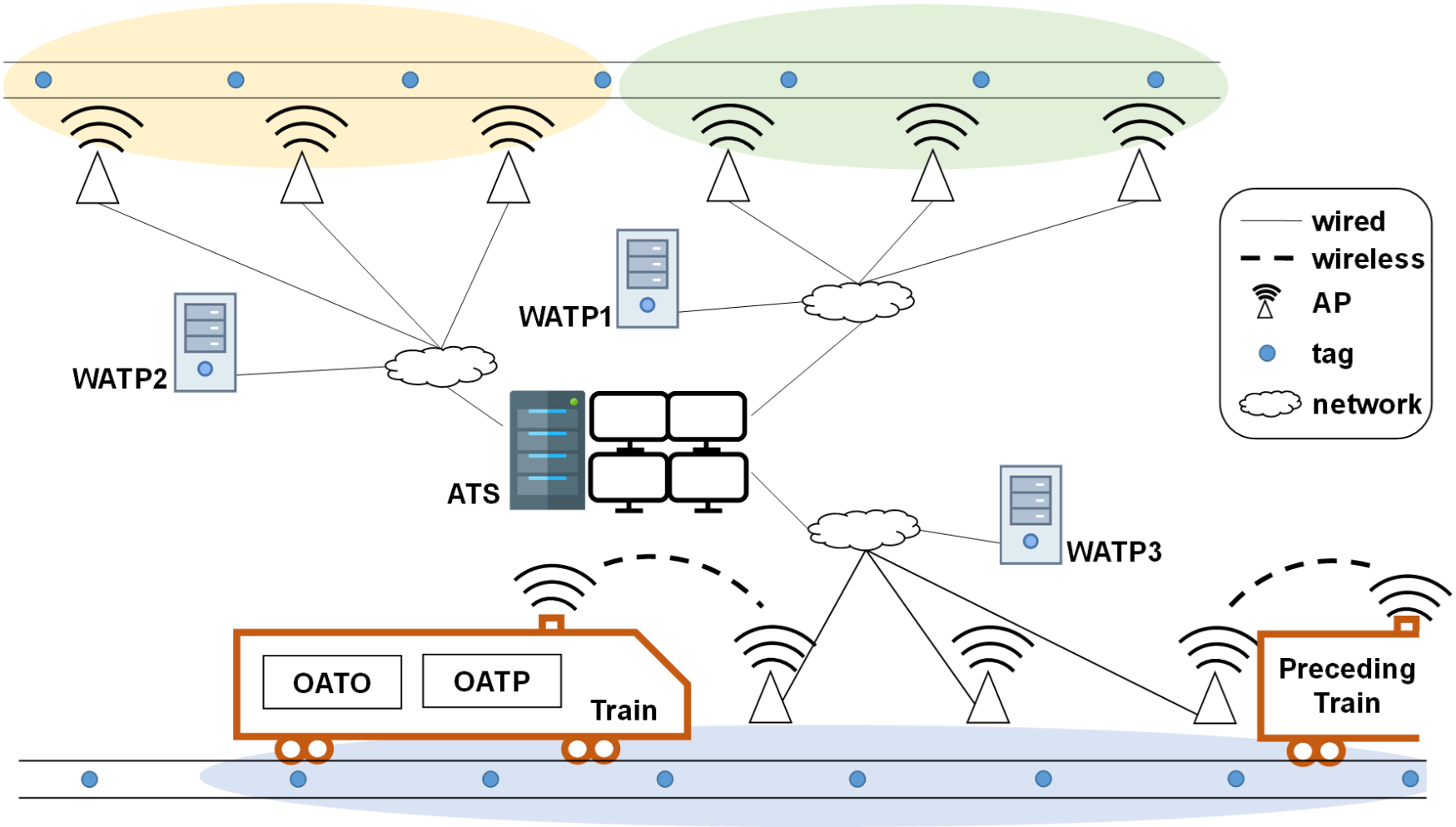
Hierarchical control systems



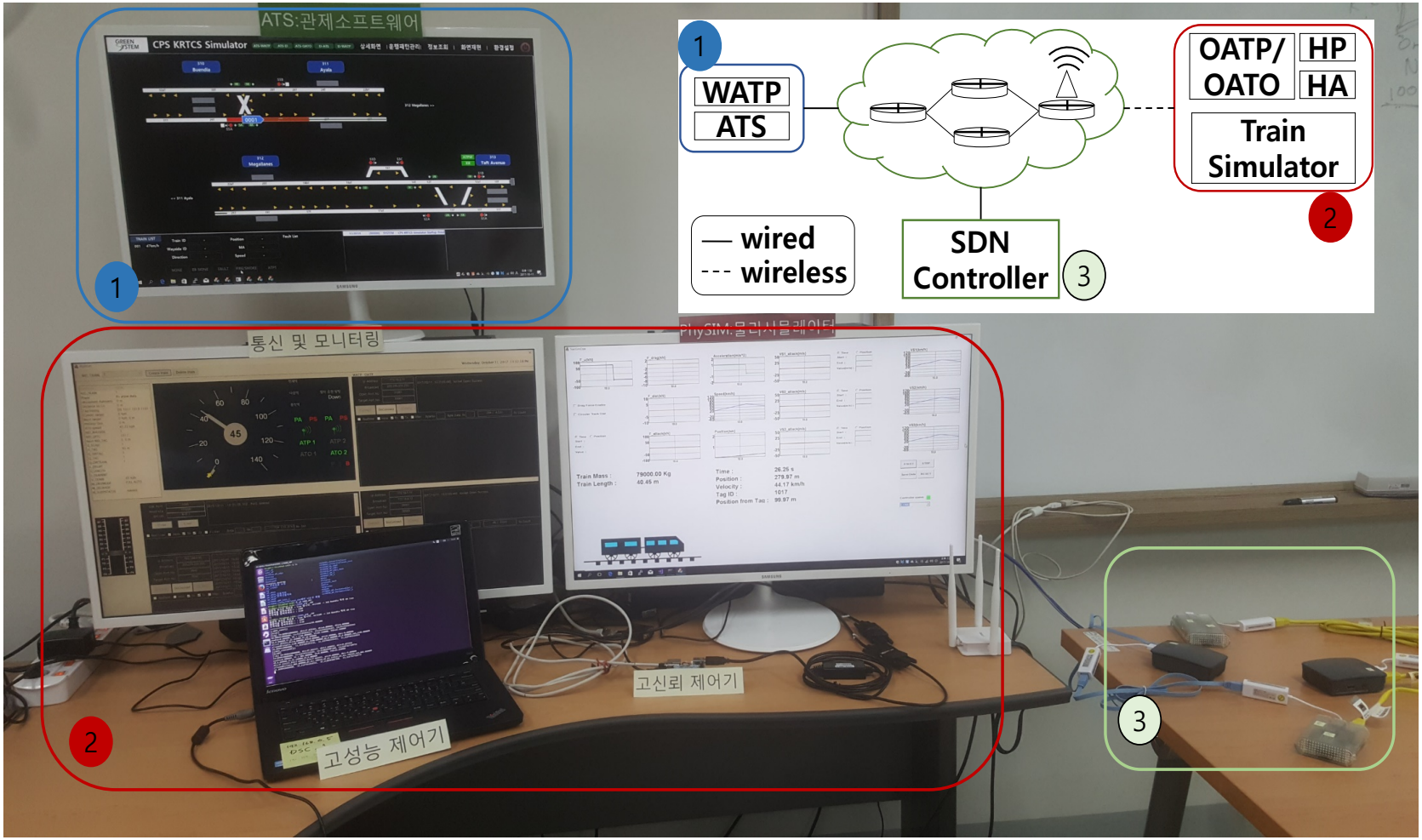
Resilient architecture



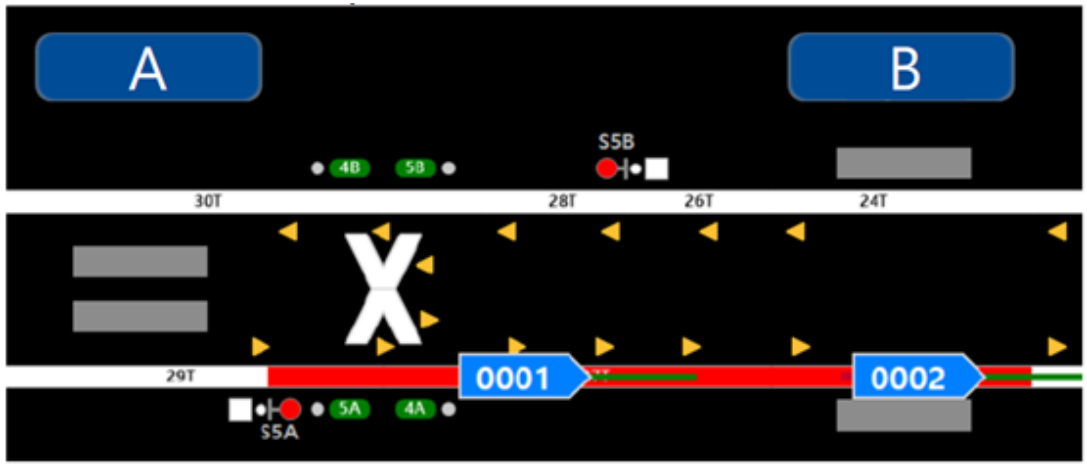
Communication based train control



CBTC testbed

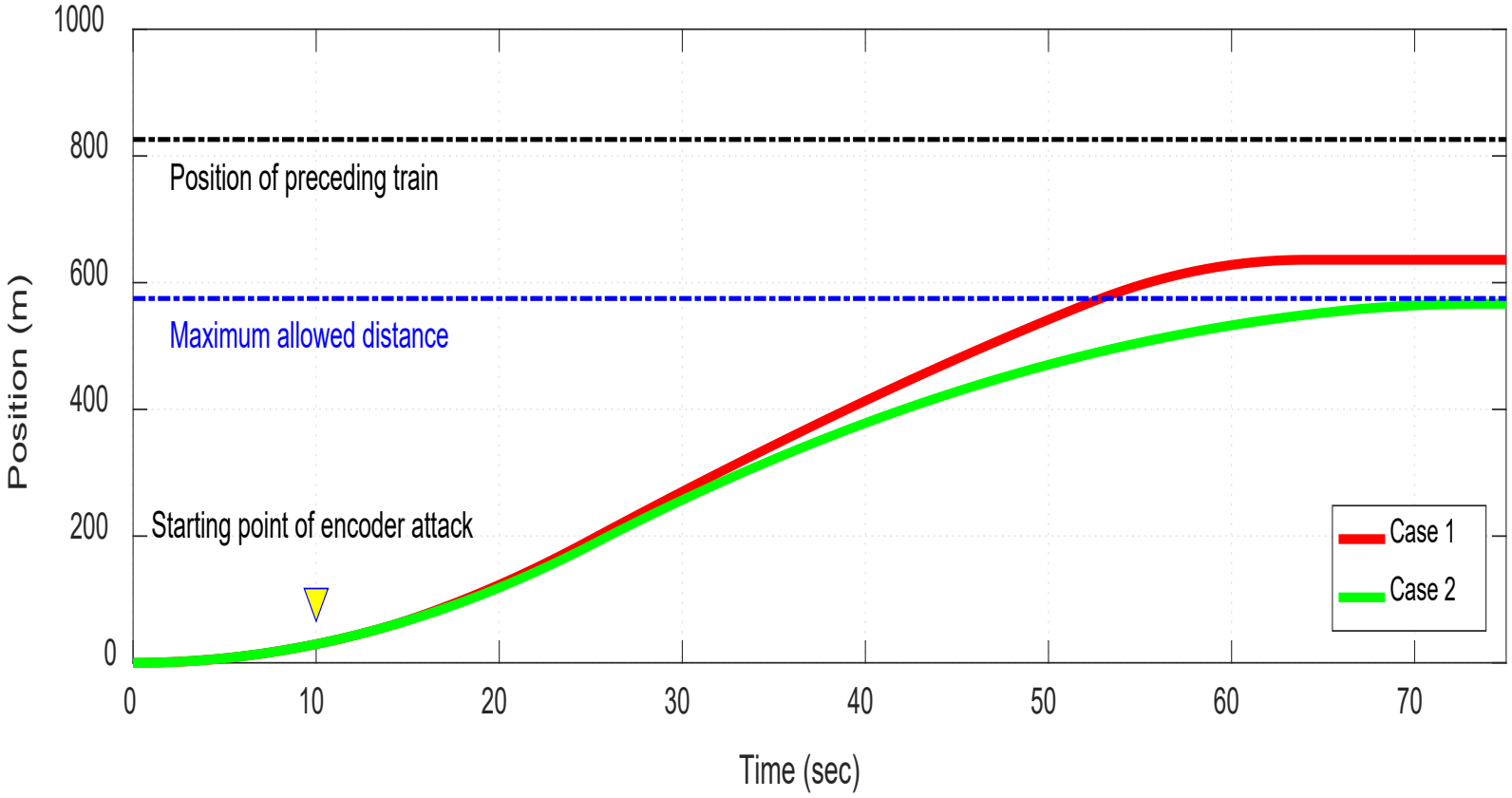


Demonstration scenarios

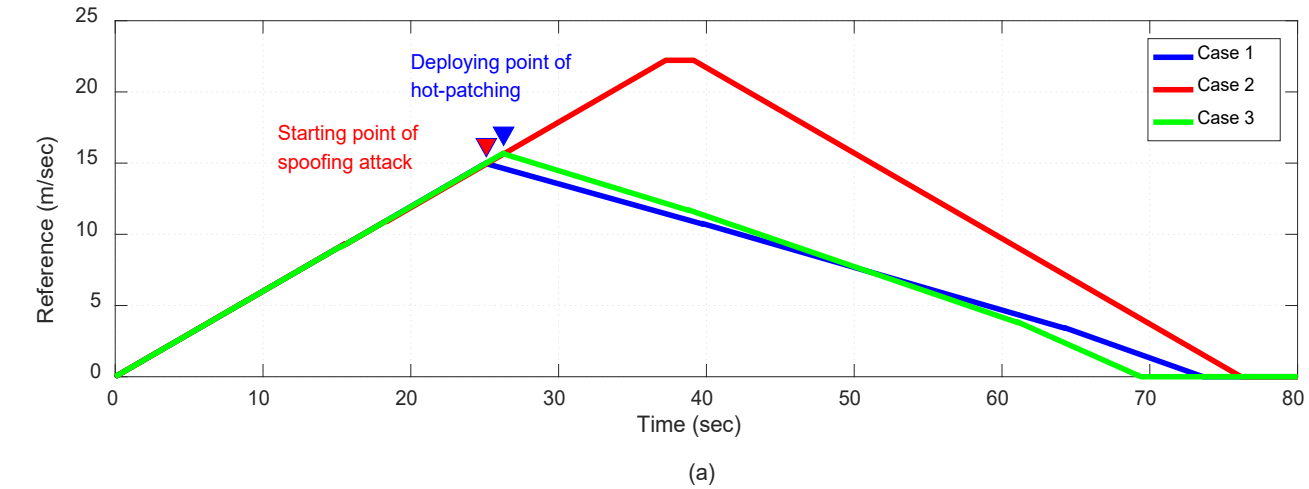


Demonstration Scenarios	Attack target	Consequence if attack is successful	Resilient algorithm
Scenario 1	Encoders of a train	• Train 1 stops by Emergency Braking system • Metro schedule disrupted causing passenger inconvenience	• Resilient state estimation • Sensor attack detection
Scenario 2	Communication message for maximum allowed travel distance	• Train 1 collides with Train 2 • Metro schedule disrupted causing passenger inconvenience • Passengers may be injured	• Hot-patching • Rerouting network traffic using SDN capability
Scenario 3	OATO HW/SW	• Train 1 stops by Emergency Braking system • Metro schedule disrupted causing passenger inconvenience	• Live migration • Graceful degradation of HA
Scenario 4	Network link	• Train 1 stops by Emergency Braking system • Metro schedule disrupted causing passenger inconvenience	• Rerouting network traffic using SDN capability

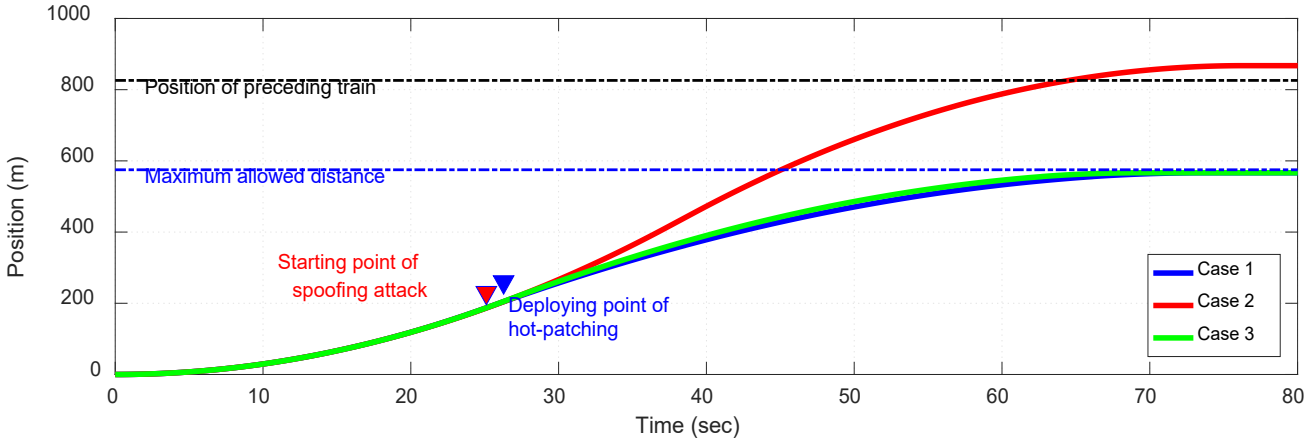
Resilience against encoder attack



Resilience against spoofing attack



(a)



(b)

Conclusions

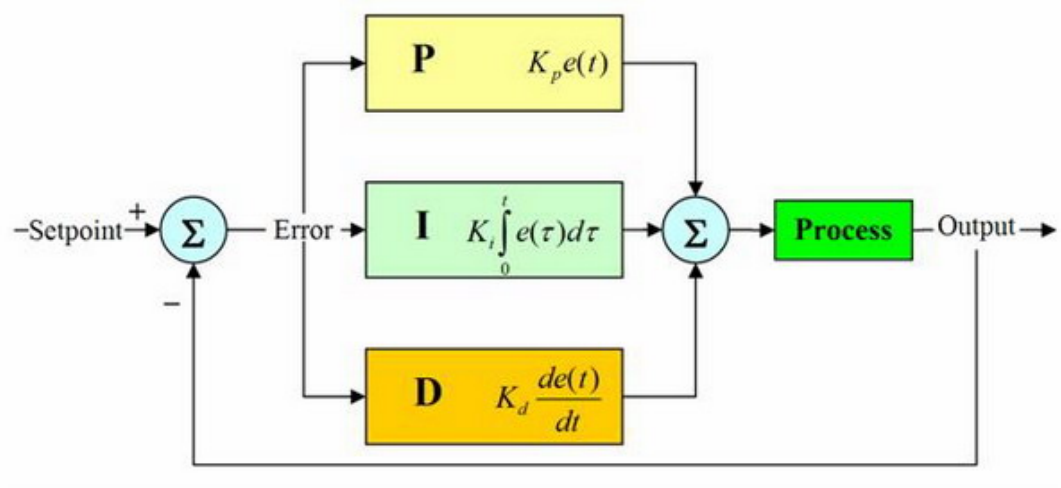
- CPS is an enabler for 4th industrial revolution
- CPS is playground for convergence
- Cyber-physical security opens a new dimension
- Resilience is critical for CPS

Thank you for your attention!
Questions?

Backup slides

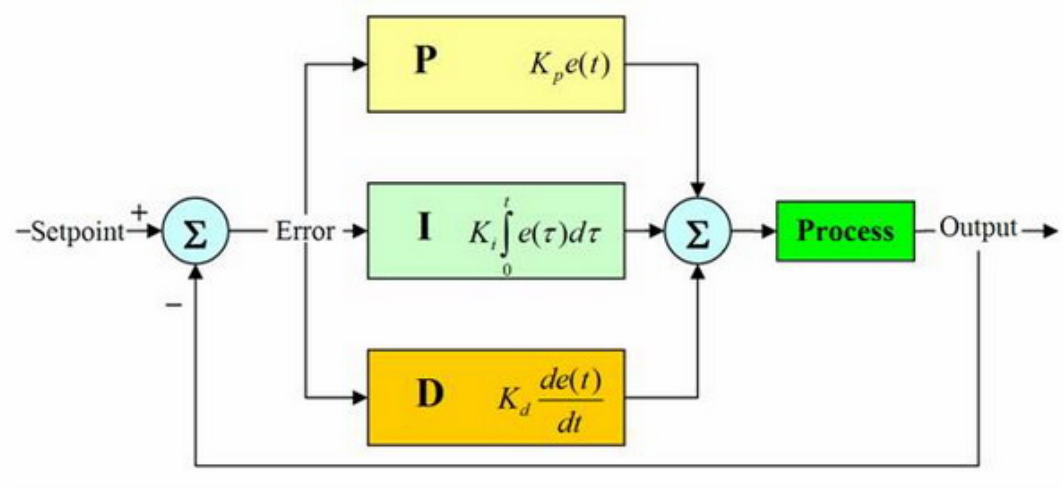
Celebrated PID control

- Proportional, integral, derivative

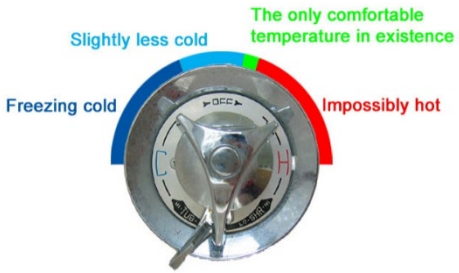


Celebrated PID control

- Proportional, integral, derivative



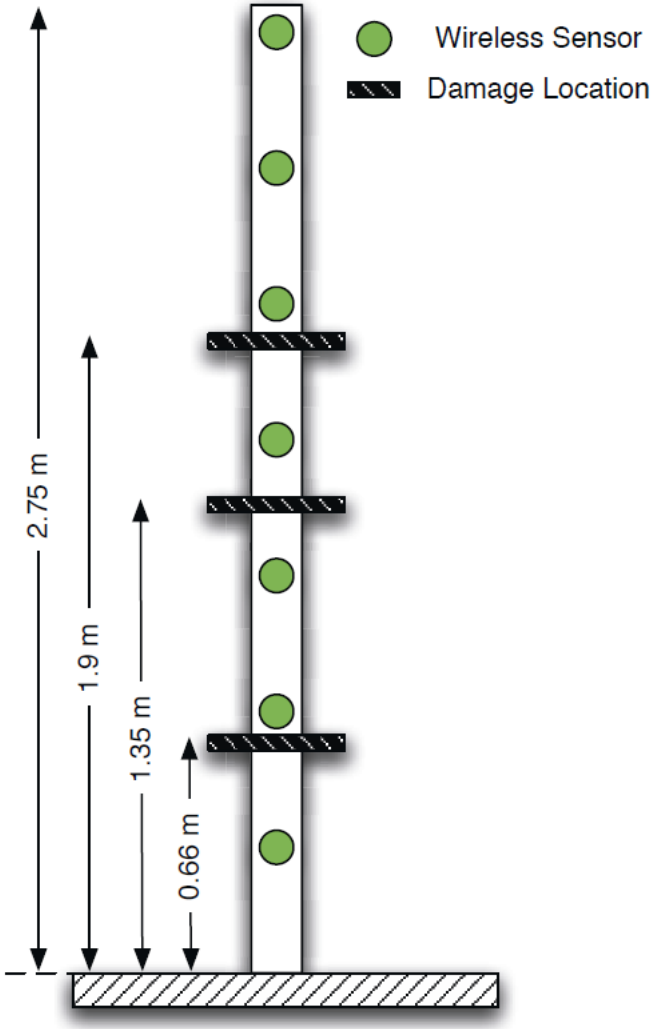
- Example: Shower temperature control



Constraints caused by NCS

- Time delay
- Packet loss
- Time-varying transmission/sampling interval
- Competition of multiple nodes accessing network
- Data quantization

Structural health monitoring



Physical & cyber vs. cyber-physical

- Physical in traditional civil engineering + centralized cyber approach
  - Large amount of data transmission to base station
- Cyber-physical approach
  - Local data processing in each sensor
- Performance
  - CPS approach **reduces latency and energy consumption by more than 60%**

Traditional cyber attack

- Cyber-only attack: DDoS
  - Do not care much about how cyber affects physical