THE UNIVERSITY of ADELAIDE

CRICOS PROVIDER 00123M

Symposium on Recent Advances on Intelligent Engineering
Obuda University, 12 September

Cyber-Physical Systems: Analysis and Design

Peng Shi
School of Electrical and Mechanical Engineering

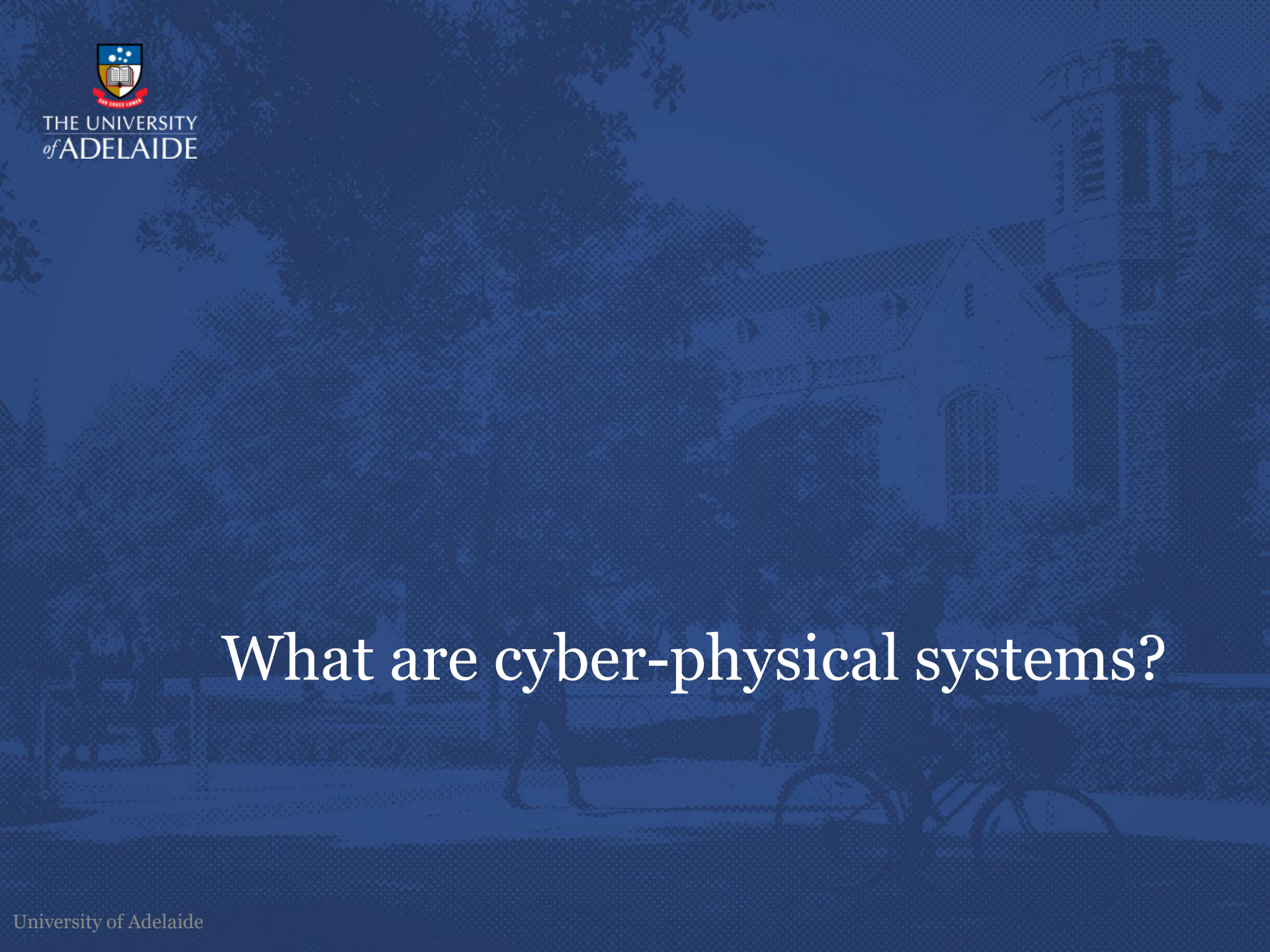
adelaide.edu.au

Cyber-Physical Systems: Analysis and Design

Peng Shi
School of Electrical and Mechanical Engineering
University of Adelaide, Australia

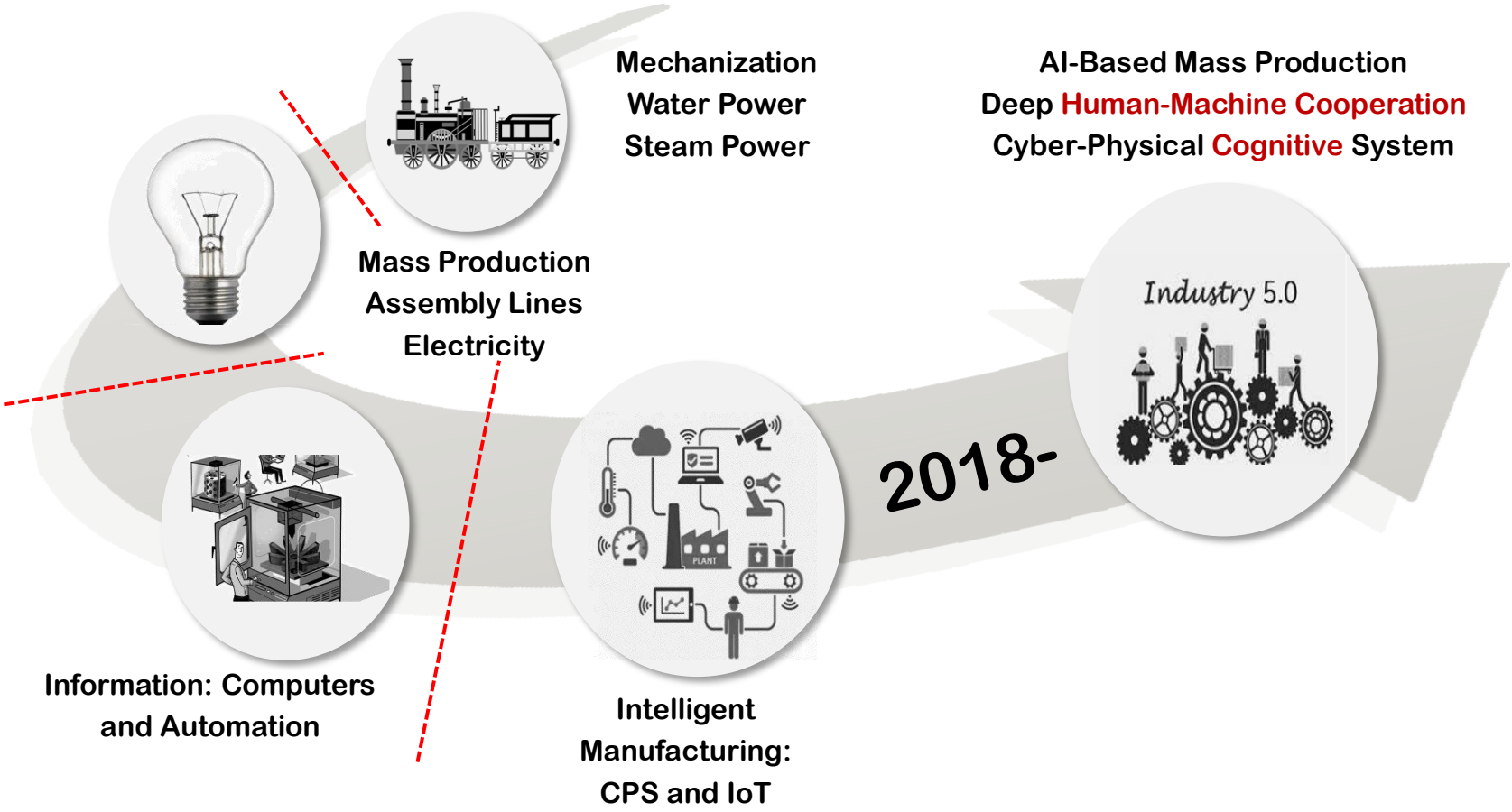
Outline

- What are cyber-physical systems?
- Cyber-physical system security
- Attack design
- Conclusion

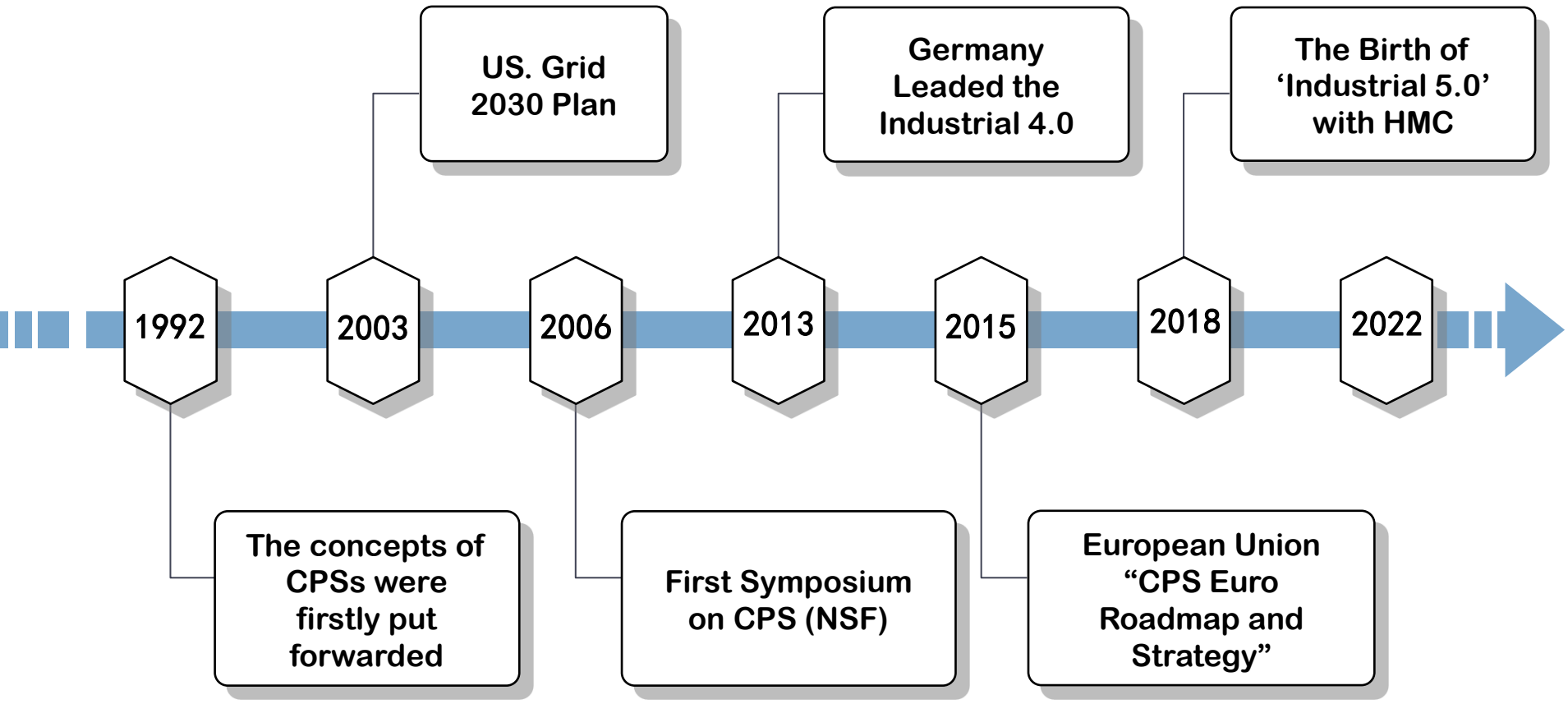


What are cyber-physical systems?

What are CPS

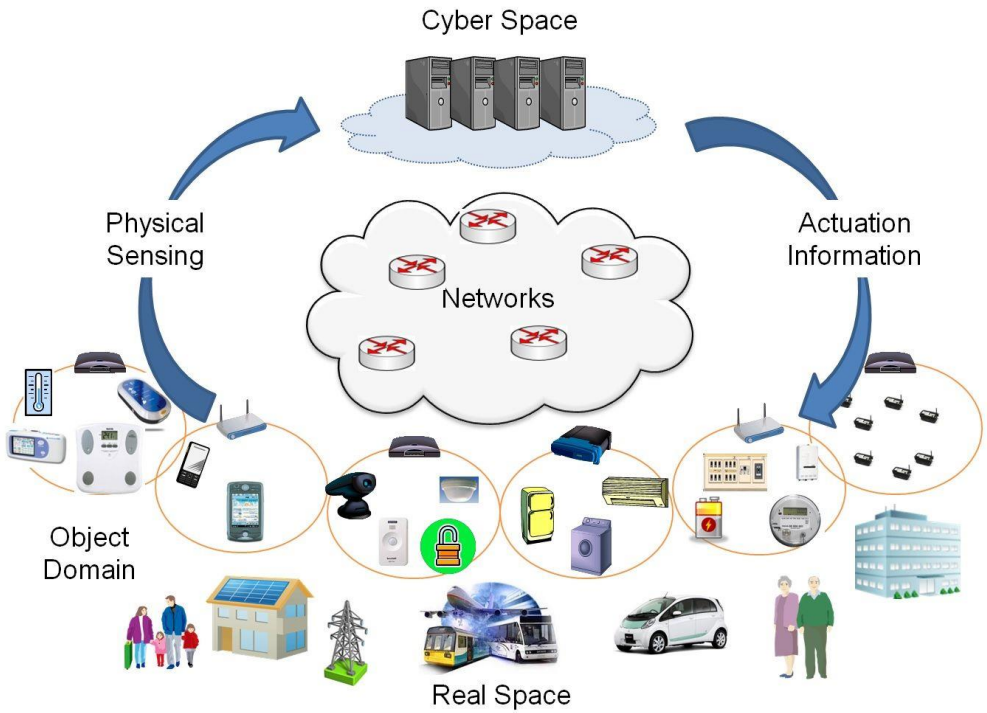

Mechanization
Water Power
Steam Power
Mass Production
Assembly Lines
Electricity
Information: Computers
and Automation
Intelligent
Manufacturing:
CPS and IoT
2018-
AI-Based Mass Production
Deep Human-Machine Cooperation
Cyber-Physical Cognitive System
Industry 5.0

What are CPS


1992
2003
2006
2013
2015
2018
2022
US. Grid 2030 Plan
Germany Leaded the Industrial 4.0
The Birth of 'Industrial 5.0' with HMC
The concepts of CPSs were firstly put forwarded
First Symposium on CPS (NSF)
European Union "CPS Euro Roadmap and Strategy"

What are CPS

- Cyber-physical system is a combination of physics with cyber components, potentially networked and tightly interconnected.

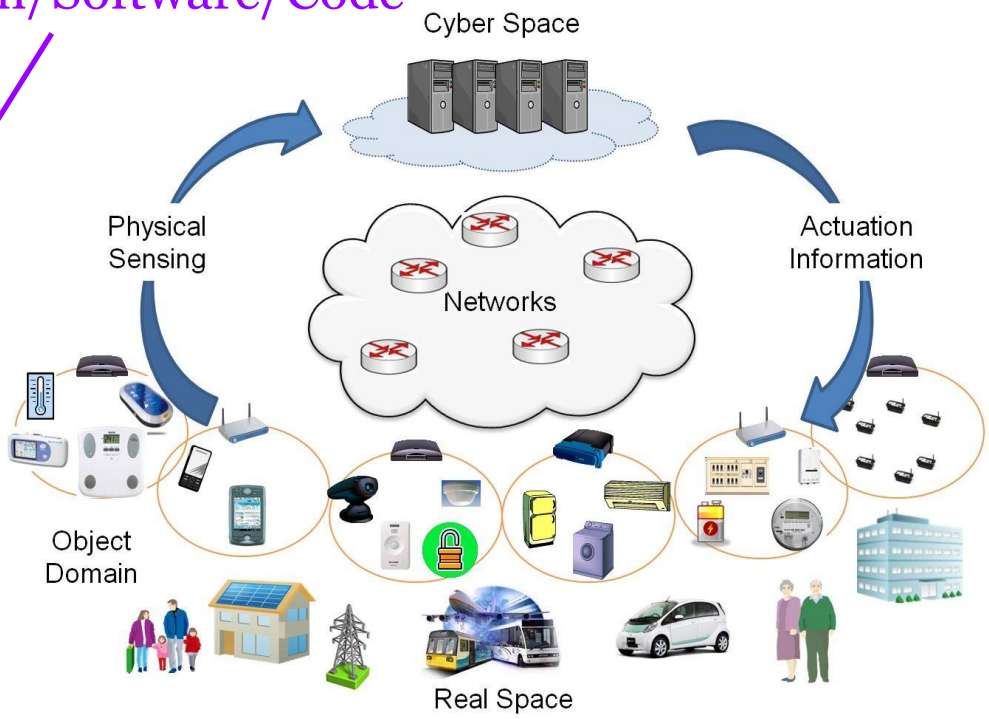


What are CPS

Computation/Software/Code

Plant/Process/System

- Cyber-physical system is a combination of physics with cyber components, potentially networked and tightly interconnected.



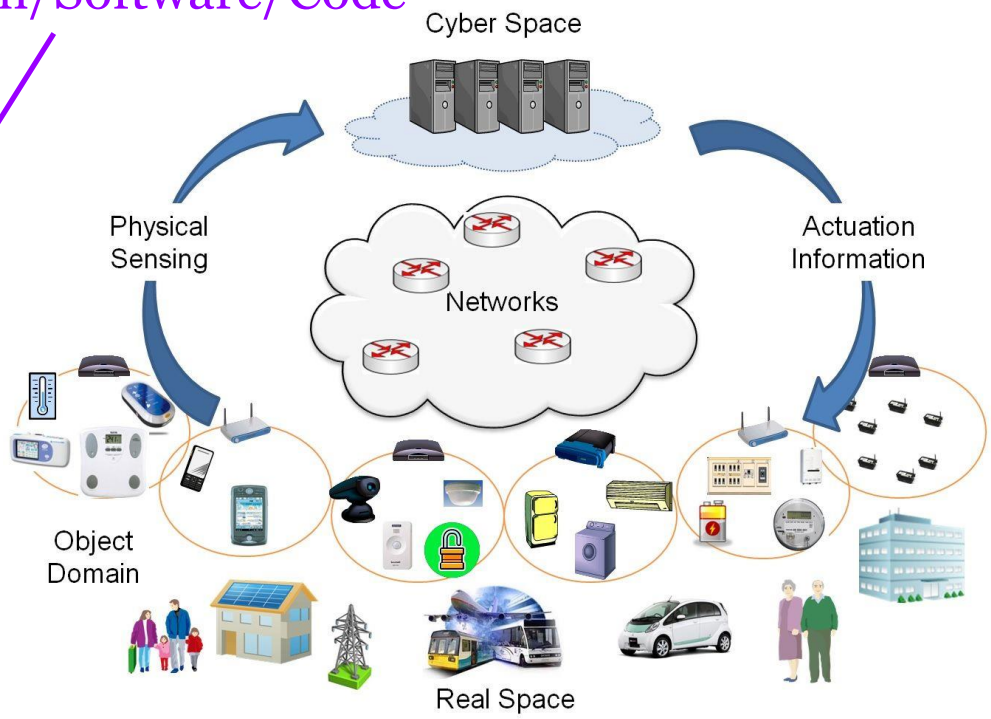
What are CPS

Do not design the physics and the cyber separately

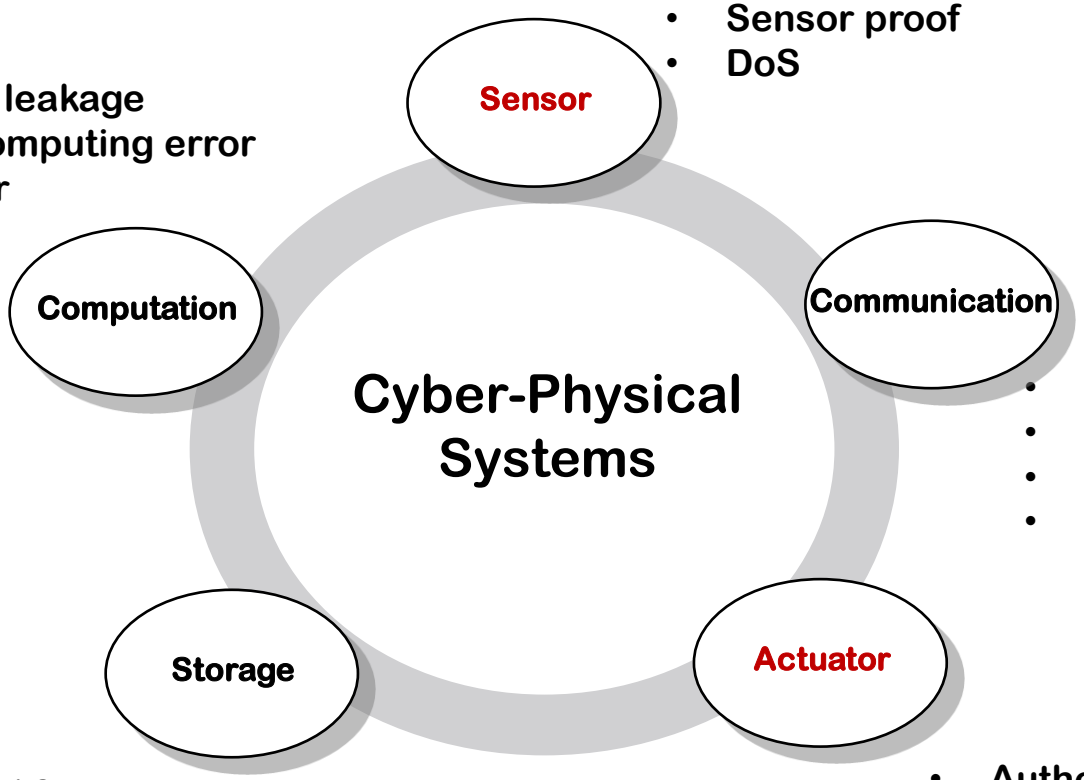
Computation/Software/Code

Plant/Process/System

- Cyber-physical system is a combination of physics with cyber components, potentially networked and tightly interconnected.



Components of CPS



- Sensor proof
- DoS

- Information leakage
- Enforced computing error
- Timing error

- Eavesdropping
- Packet modification
- Man-in-the-middle attack
- Resource blocking

- Storage modification
- Data remanence

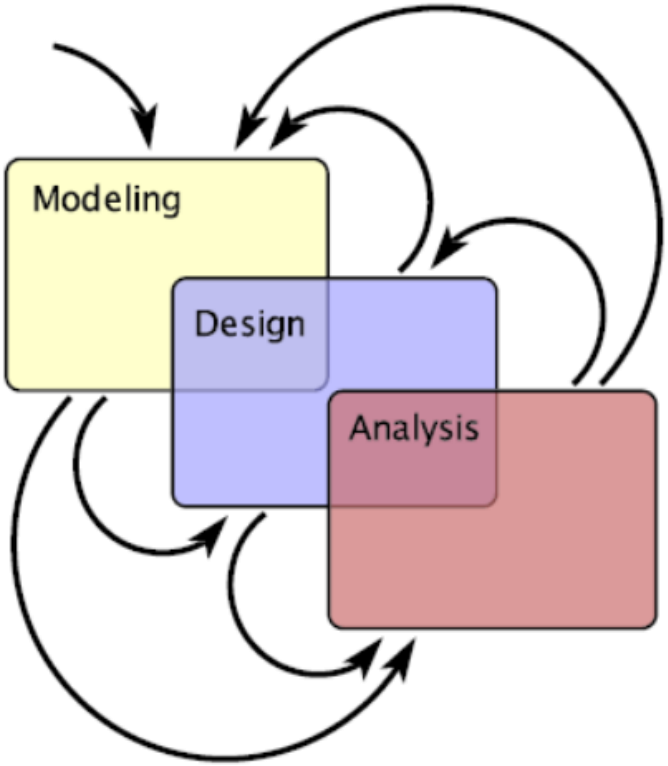
- Authentication failure
- Deadline miss

Cross-Discipline Insights of CPS

Computer Science and Engineering
- Control with shared processors
- Component privacy
- Verification and validation with timing

Control, Estimation and System Theory
- System resilient to large changes
- Design methods that scale well
- Framework for heterogeneous components

Communication and Information Theory
- Coordination among several controllers
- CPS security
- Control across communication channels

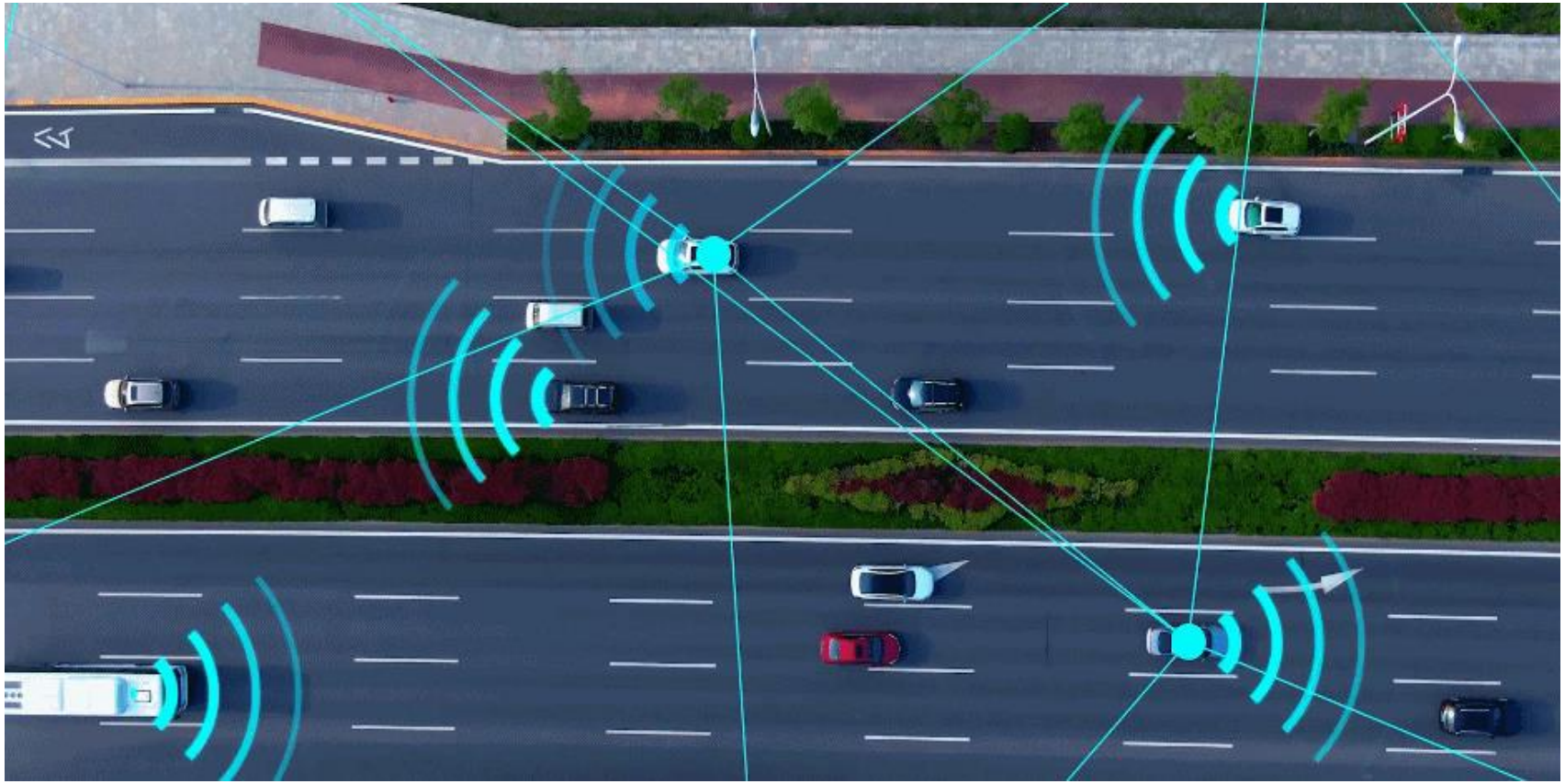


Typical examples of CPS

Robotic systems

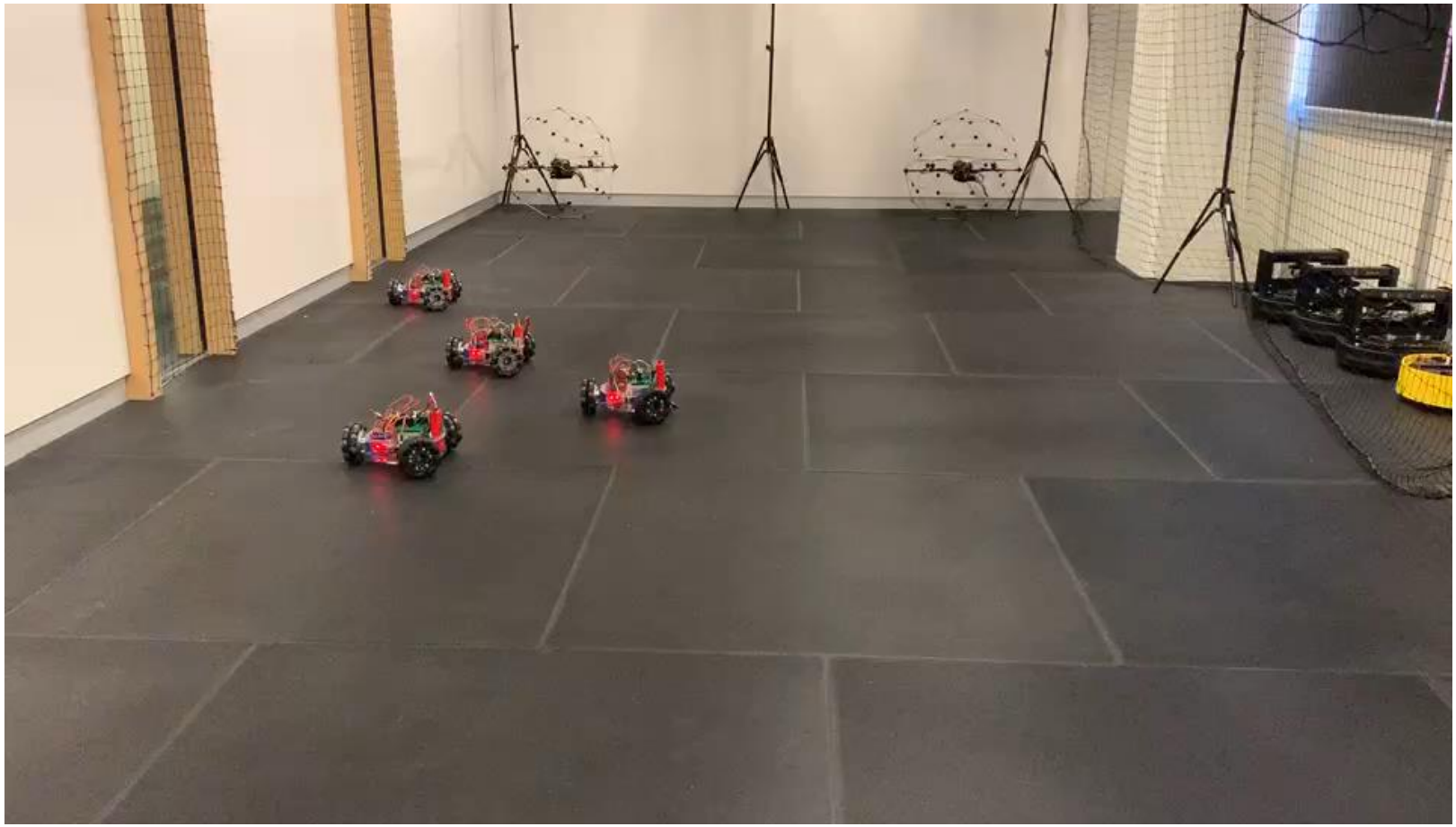
Typical examples of CPS

Intelligent transportation systems



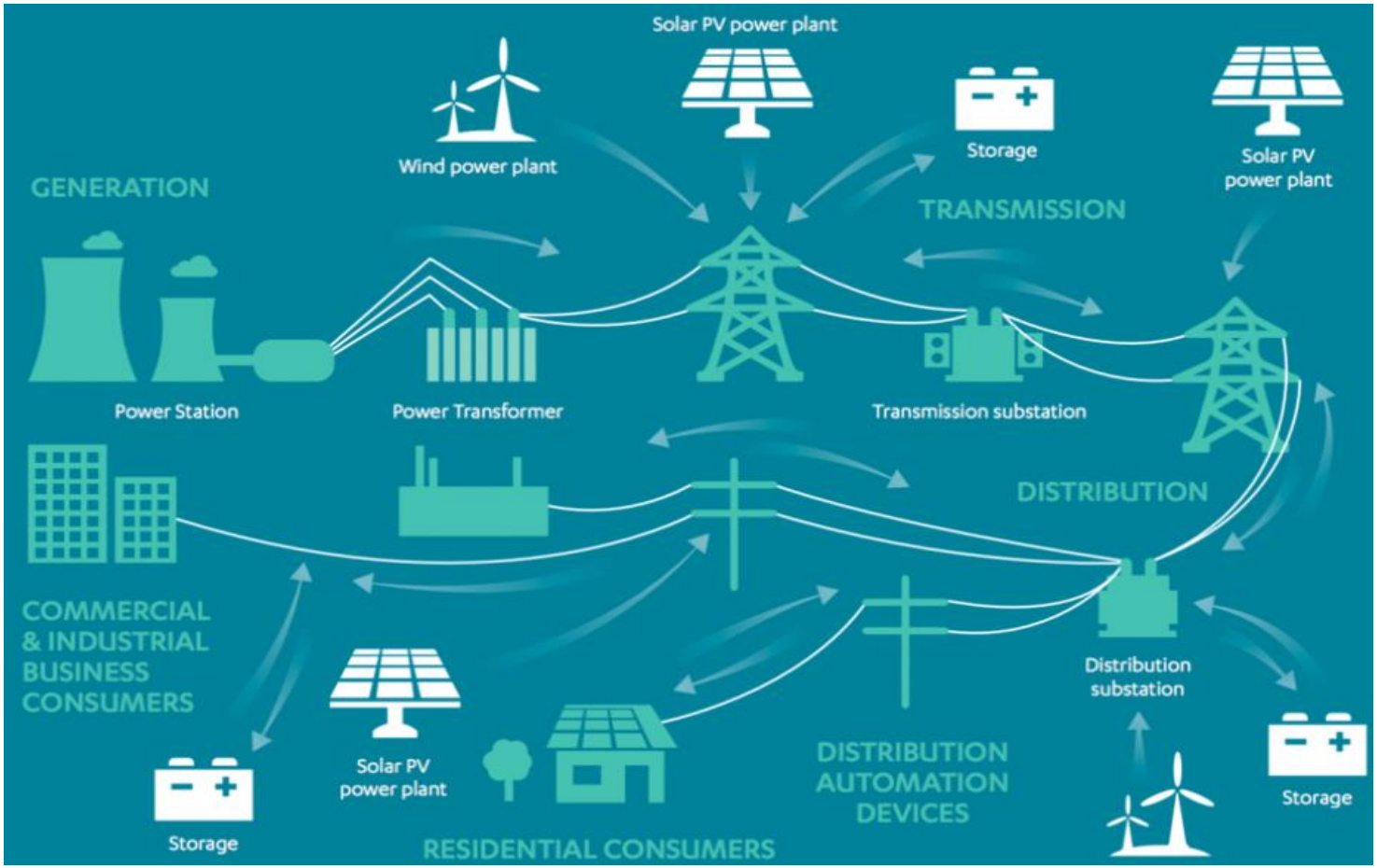
Typical examples of CPS

Multiple vehicular systems



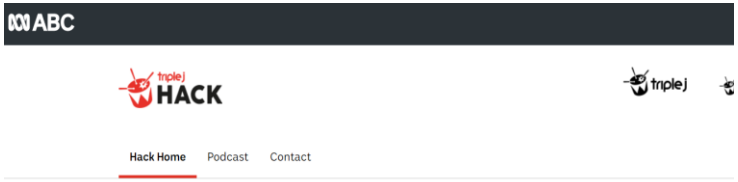
Typical examples of CPS

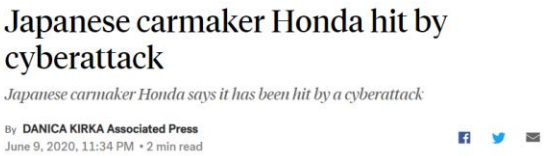
Smart Grids



Cyber-physical system security

CPS: Security Incidents





https://www.bbc.com/news/technology-55439190
https://www.foxbusiness.com/technology/solarwinds-hackers-viewed-microsofts-source-code
https://abcnews.go.com/Business/wireStory/japanese-carmaker-honda-hit-cyber-attack-71152068
https://www.abc.net.au/triplej/programs/hack/the-worlds-first-digital-weapon-stuxnet/7926298
https://www.euronews.com/2021/08/02/italian-website-for-vaccination-appointments-targeted-by-hackers

CPS security

A Joint Cybersecurity Advisory published by the Cybersecurity & Infrastructure Security Agency about destructive malware targeting organizations in Ukraine is seen Feb. 28.

Russia Ukraine: 'Most serious cyberattack of the Ukraine war' cripples tens of thousands modems (9news.com.au)

CPS security

- Cyber security was earlier studied in computer science, defined as preventing attackers from achieving objectives through unauthorized access to computers and networks.

- CPS security includes both security, which sometimes is used as a system property that corresponds to defend against attacks, and resiliency, a system property that corresponds to survival and recovery after the occurrence of an attack[1]

[1] S. M. Dibaji, M. Pirani, D. B. Flamholz *et al.*, "A systems and control perspective of CPS security," *Annual reviews in control,* vol. 47, pp. 394-411, 2019.

CPS security

- Cyber security was earlier studied in computer science, defined as preventing attackers from achieving objectives through unauthorized access to computers and networks.

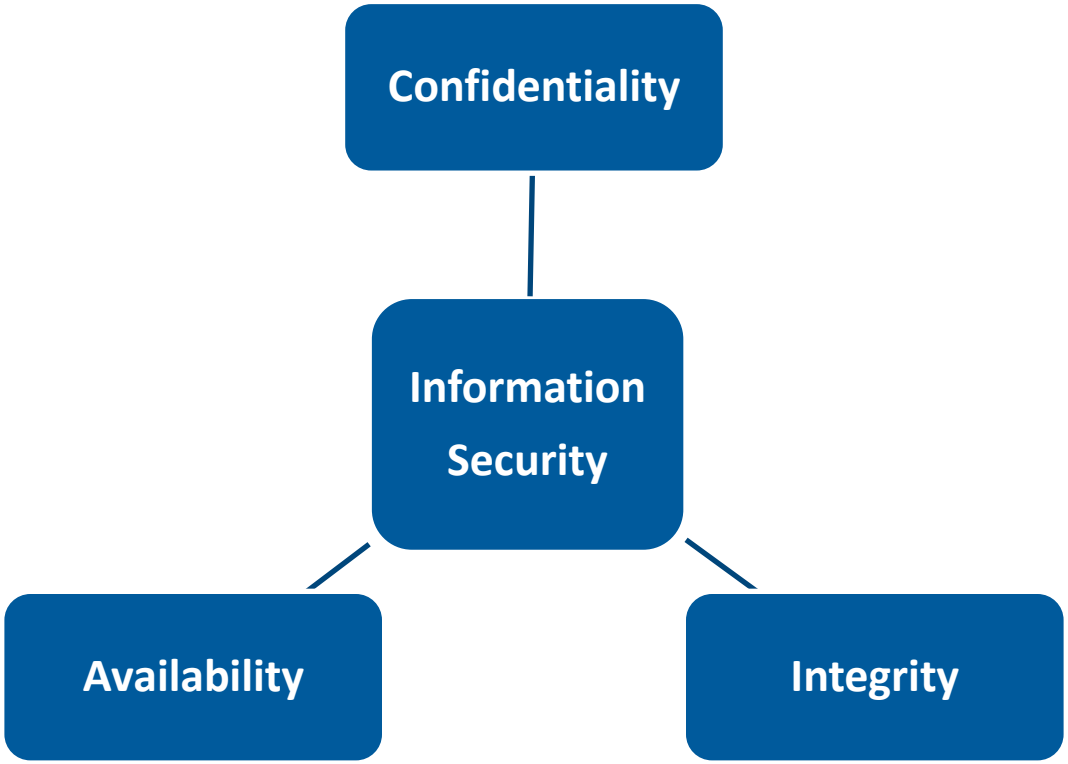
- The intrinsically open attribute of the cyber layer leads to information eavesdropping, privacy intrusion, and service interruption, even causing the negative impacts of physical processes mirrored from cyberspace to the nature world
- Owing to the deep integration of cyber and physical realms, normal operation can be disrupted leading to serious security incidents
- From the perspective of control engineering, security is crucial for CPSs

[1] S. M. Dibaji, M. Pirani, D. B. Flamholz *et al.*, "A systems and control perspective of CPS security," *Annual reviews in control,* vol. 47, pp. 394-411, 2019.

CPS security

Security objectives

CIA Triad



What is the CIA Triad? Confidentiality, Integrity and Availability | Cybrary

CPS security

Security objectives **CIA Triad**

- Confidentiality
  - Rules limiting who has access to information
- Integrity
  - Rules governing how and when information is modified
- Availability
  - Assurance that people who are authorized to access information are able to do so

CPS security

Security objectives **CIA Triad**

- Confidentiality → **Disclosure attack**
  - Rules limiting who has access to information
- Integrity → **Deception attack**
  - Rules governing how and when information is modified
- Availability → **Disruption attack**
  - Assurance that people who are authorized to access information are able to do so

CPS security

Types of cyber-attacks

- **Disclosure attack**
  - The aim is to find access to informative signals or obtain conclusive information about them

CPS security

Types of cyber-attacks

- **Disclosure attack**
  - The aim is to find access to informative signals or obtain conclusive information about them
- Deception attack
  - Data and resources that cannot be modified without authorization
    - Characterized by Bernoulli random variable

CPS security

Types of cyber-attacks

- **Disclosure attack**
  - The aim is to find access to informative signals or obtain conclusive information about them
- Deception attack
  - Data and resources that cannot be modified without authorization
- Disruption attack
  - Communication channels that are accessible to authorized parties at appropriate times
    - Characterized by Bernoulli variables, pulse-width-modulated jamming signals, the maximum number of consecutive jamming actions and attack frequency and duration

CPS security

Types of cyber-attacks

- **Disclosure attack**
  - The aim is to find access to informative signals or obtain conclusive information about them
- Deception attack
  - Data and resources that cannot be modified without authorization
- Disruption attack
  - Communication channels that are accessible to authorized parties at appropriate times
- **Hybrid cyber-attacks**

Dynamic hybrid-triggered-based fuzzy control for nonlinear networks under multiple cyber-attacks," *IEEE Transactions on Fuzzy Systems, DOI: 10.1109/TFUZZ.2021.3134745, 2021*

CPS security

Differences Between Faults and Attacks

Attacks

- Man-in-the-Middle impacts, namely, malicious human impacts
- Minimize mathematical assumptions/dependencies
- Potentially bypass the anomaly detection
- Aided by AI techniques, attacks can be more complex and intelligent
- Mirror the basic attribute of CPS: Human-machine interaction

Faults

- Physical disturbance events not act in a coordinated manner
- Mathematical assumptions/dependencies (magnitudes/statistics)
- Effectively monitored by anomaly detection and identification
- Not induced by human impacts

CPS security

Differences Between Security and Safety

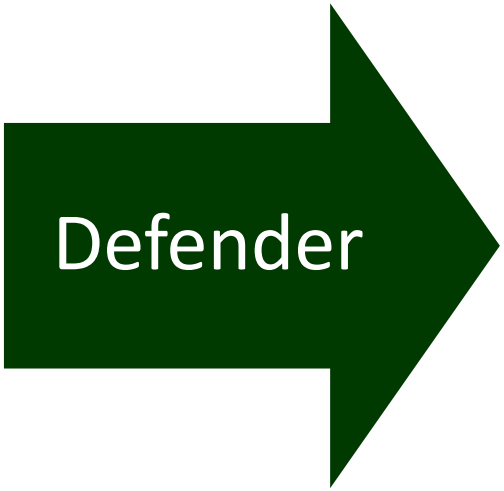
Security

- **Goal:** Protecting the systems from humans
- **Risk Source:** Potential 'human-in-the-loop' attacks by virtue of accessing the system locally or remotely to threat the normal operation and configuration
- **Assessment:** The sources of threats are normally unknown and hard to predict in view of the adversary abilities. Difficult to assess its impacts
- **Influence:** The system itself and its operation environment

Safety

- **Goal:** Protecting humans from the systems
- **Risk Source:** Accident risk of systems caused impacts on the system environments leading to nature destroying
- **Assessment:** The features of hazards are more scrutable. Such analysis can be deployed by set-based methodologies. Its feedback is reliable when the hazards are relatively stable
- **Influence:** The system's operation environment.

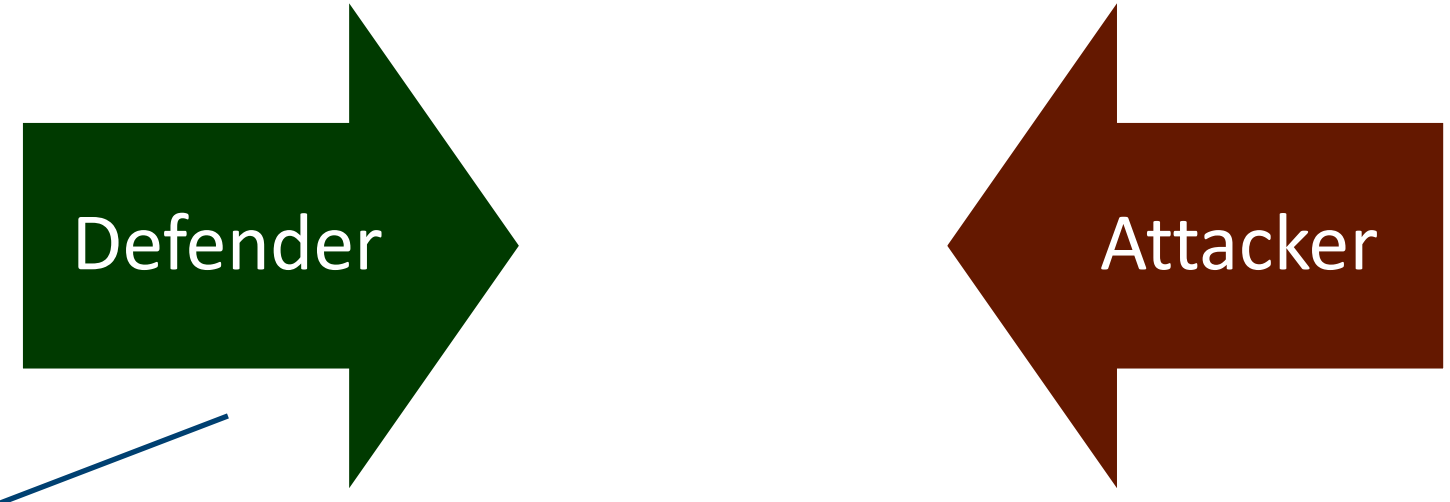
CPS security



Make effective countermeasures against cyber-attacks, ensuring that CPS run safely and securely

Design stealthy attacks to degrade the system performance without being detected

CPS security



Given the available sensor measurement of **a system** subject to the attack, develop a desirable security control scheme such that

- the actual system state can be estimated accurately and reliably
- the manipulated system can be recovered from attacked operation back to normal

- ❑ Attack detection
- ❑ Secure estimation
- ❑ Secure control

Fuzzy-model-based lateral control for networked autonomous vehicle systems under hybrid cyber-attacks, ***IEEE Transactions on Cybernetics***, 2022

Dissipativity-based sliding-mode control of cyber-physical systems under denial-of-service attacks. ***IEEE Transactions on Cybernetics***, 2020

Resilient adaptive event-triggered fuzzy tracking control and filtering for nonlinear networked systems under denial of service attacks, ***IEEE Transactions on Fuzzy Systems***. 2021.

Attack and estimator design for multi-sensor systems with undetectable adversary, ***Automatica*** 2019

Dynamic hybrid-triggered-based fuzzy control for nonlinear networks under multiple cyber-attacks, ***IEEE Transactions on Fuzzy Systems***, 2021

Sparse false injection attacks reconstruction via descriptor sliding mode observers, ***IEEE Transactions on Automatic Control***, 2020

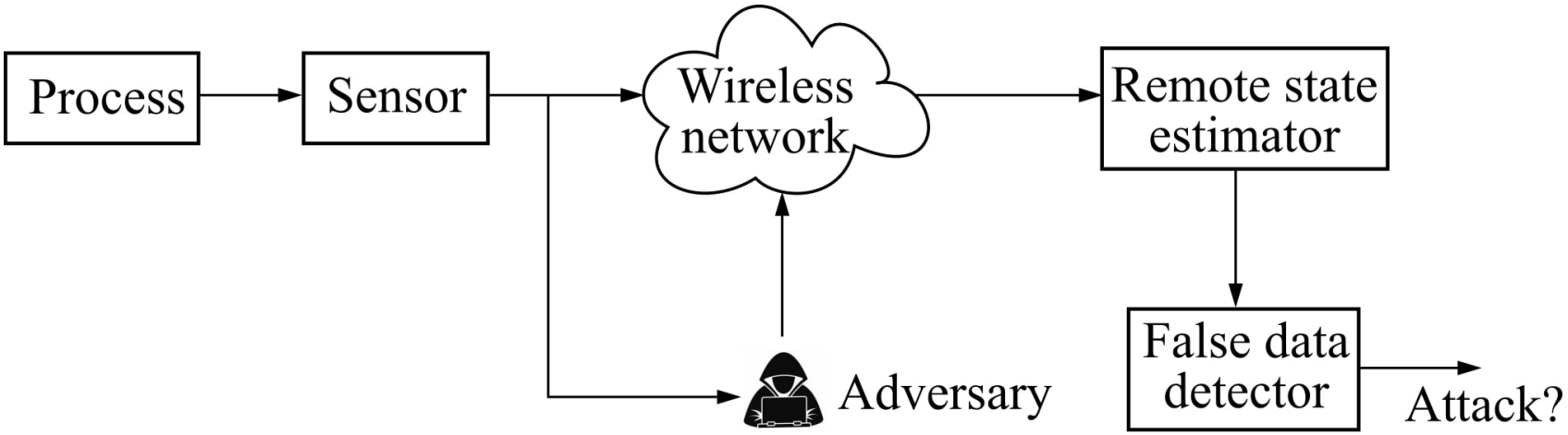
Memory-based continuous event-triggered control for networked T–S fuzzy systems against cyberattacks, ***IEEE Transactions on Fuzzy Systems***, 2020

Hybrid-triggered interval type-2 fuzzy control for networked systems under attacks, ***Information Sciences,*** 2021

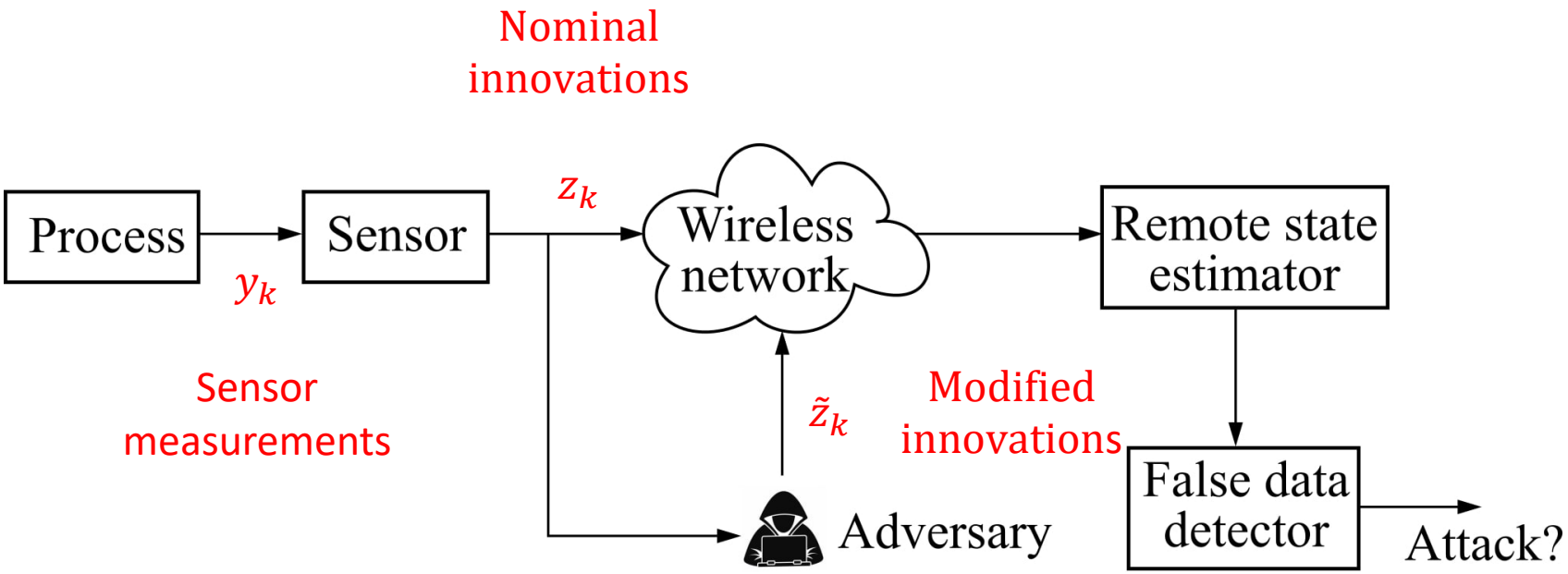
Event-triggered control for networked systems under denial of service attacks and applications, ***IEEE Transactions on Circuits and Systems I: Regular Papers***, 2021

Attack design

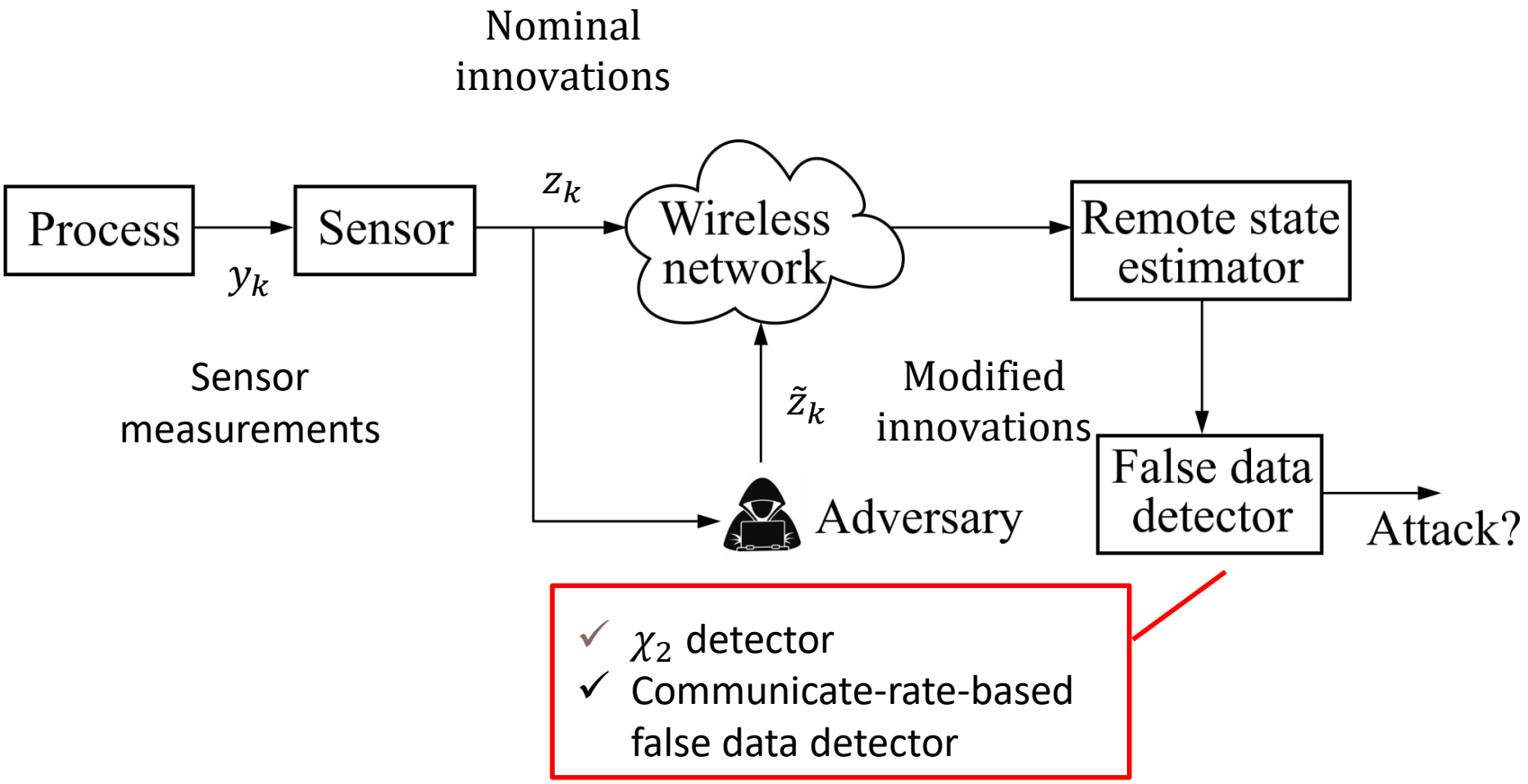
Attack design



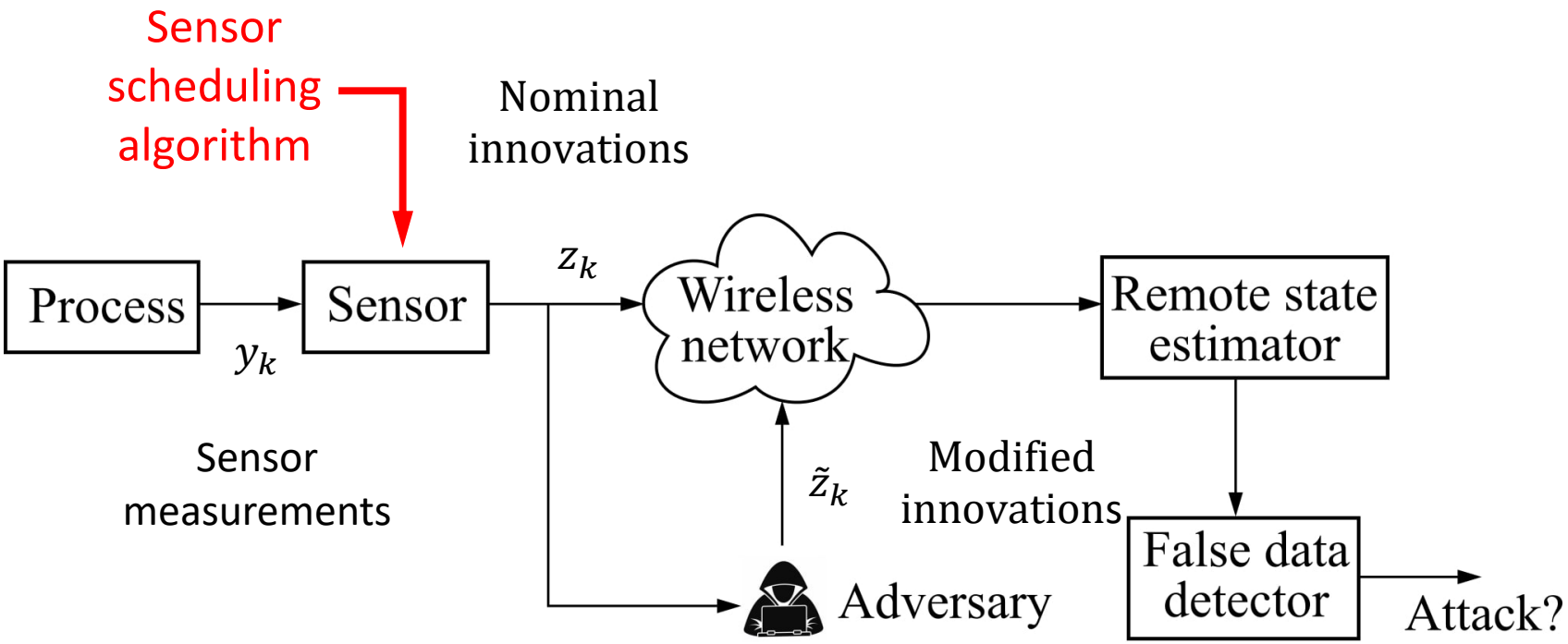
Attack design



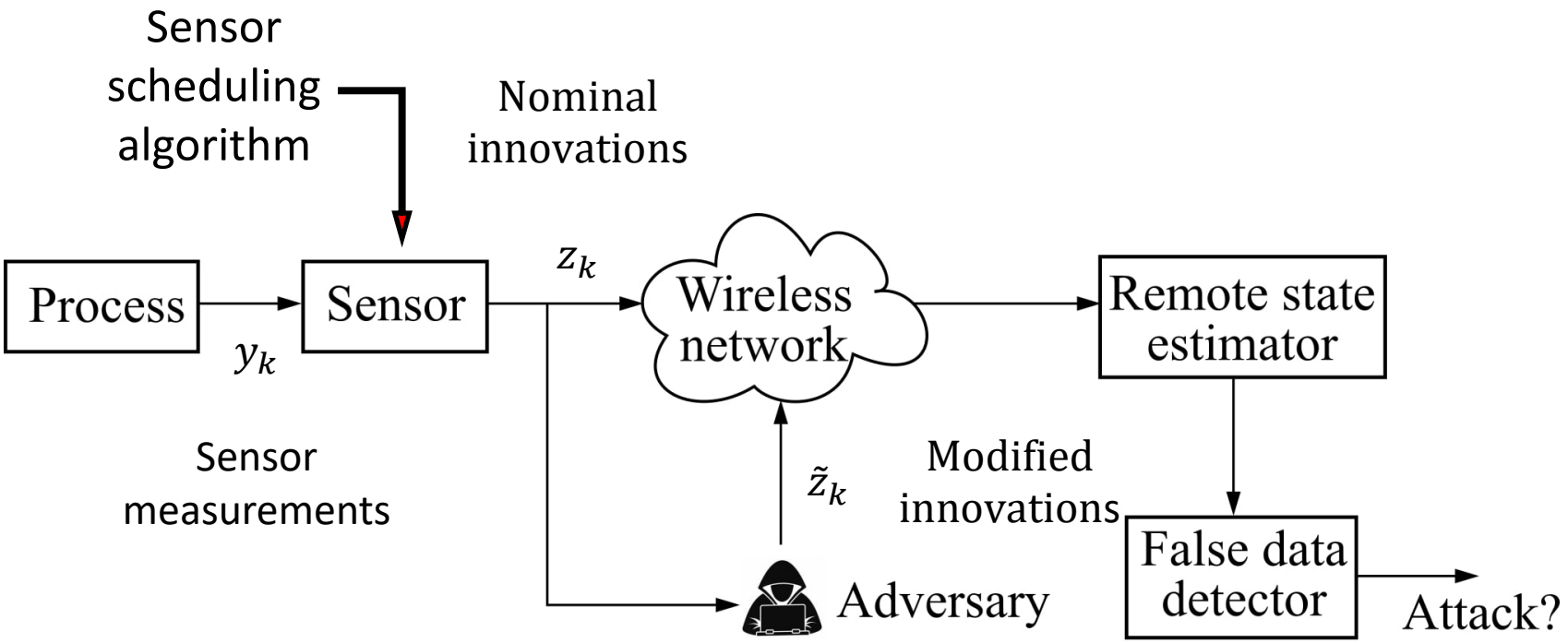
Attack design



Attack design

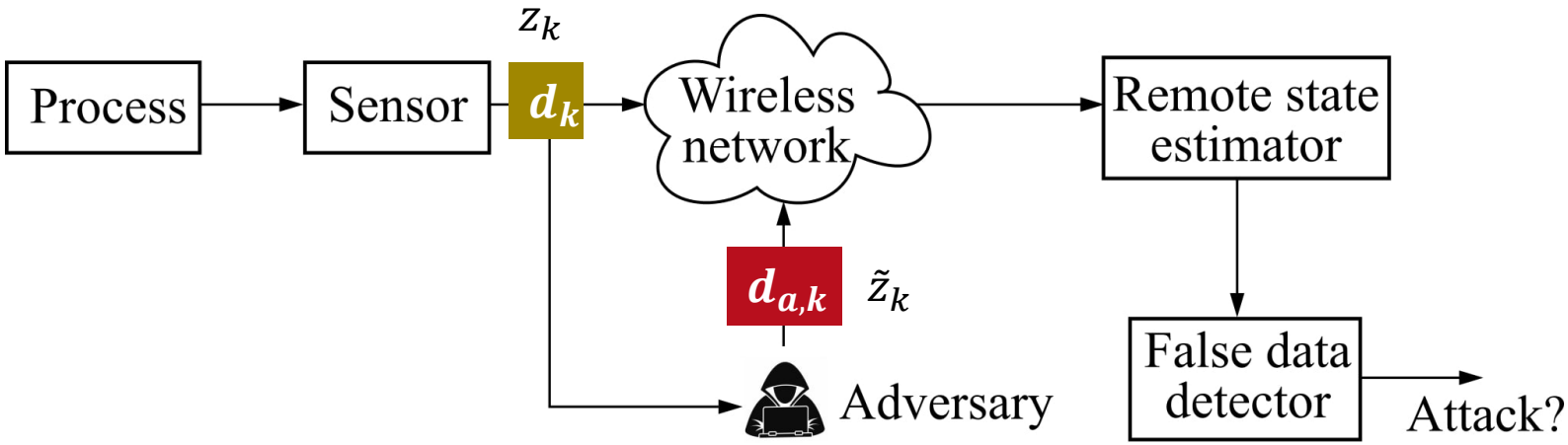


Attack design



- ✓ Intercept the transmitted packets
- ✓ Block the communication channel
- ✓ Inject false data

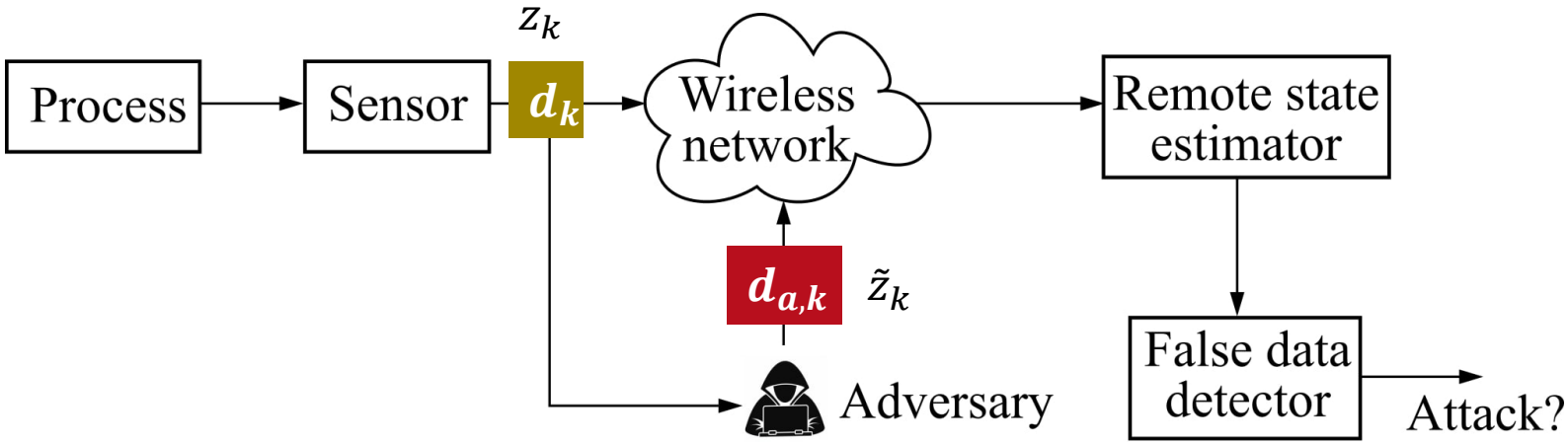
Attack design



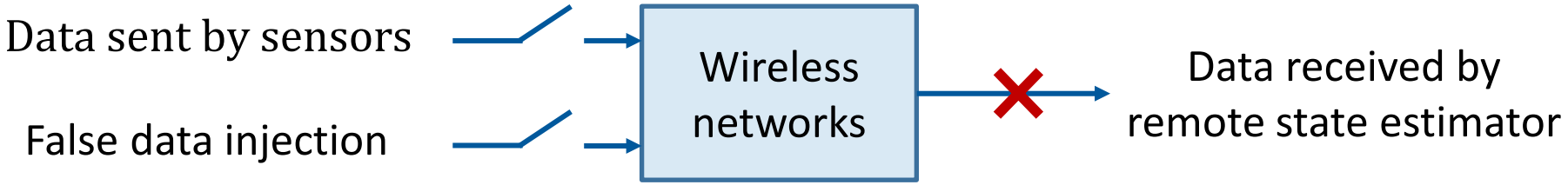
- d_k: Decisive sensor indicator
- $d_{a,k}$: Attack decision

- Case I: $d_k = 0, d_{a,k} = 0$. No attacks
- Case II: $d_k = 1, d_{a,k} = 0$. Disruption attacks
- Case III: $d_k = 0, d_{a,k} = 1$. Deception attacks
- Case IV: $d_k = 1, d_{a,k} = 1$. Hybrid attacks

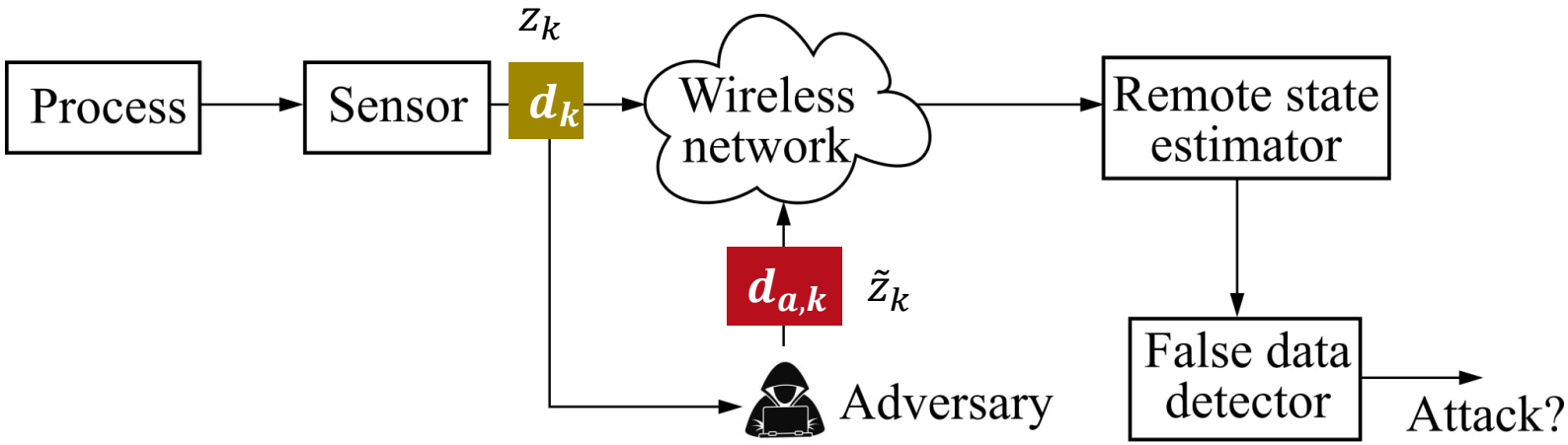
Attack design



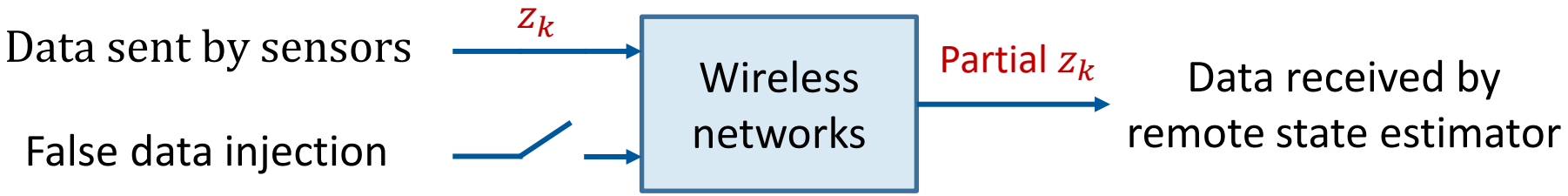
Case I: $d_k = 0, d_{a,k} = 0$. No attacks.



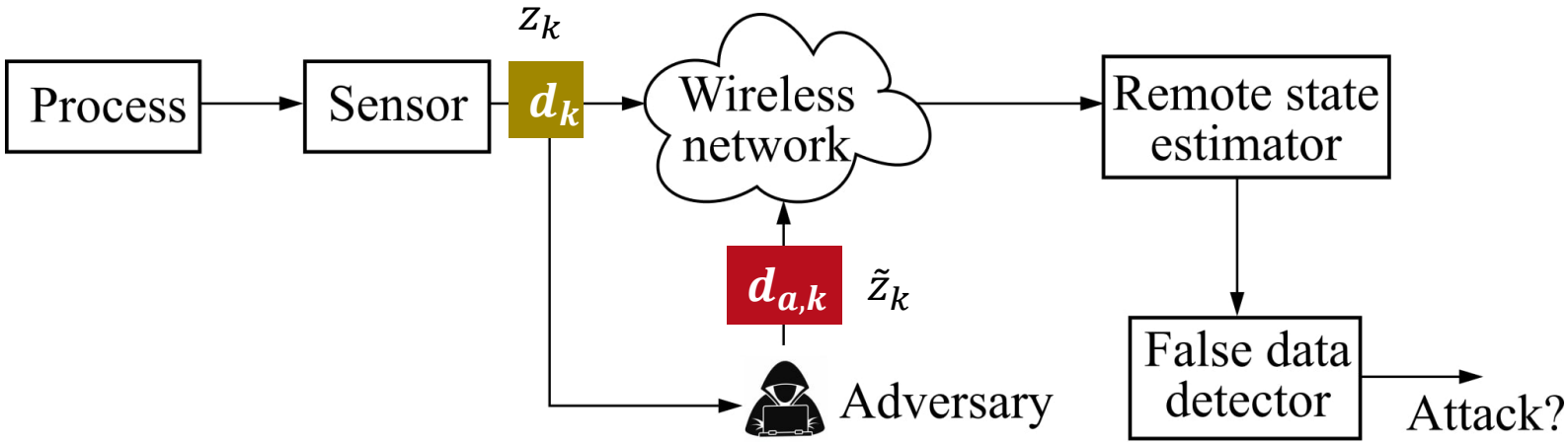
Attack design



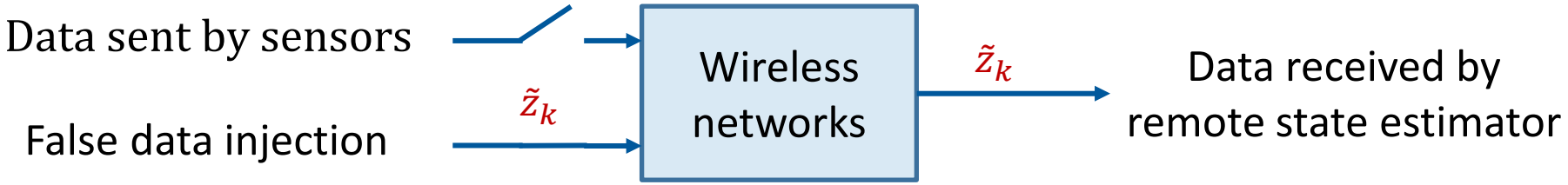
Case II: $d_k = 1, d_{a,k} = 0$. Disruption attacks



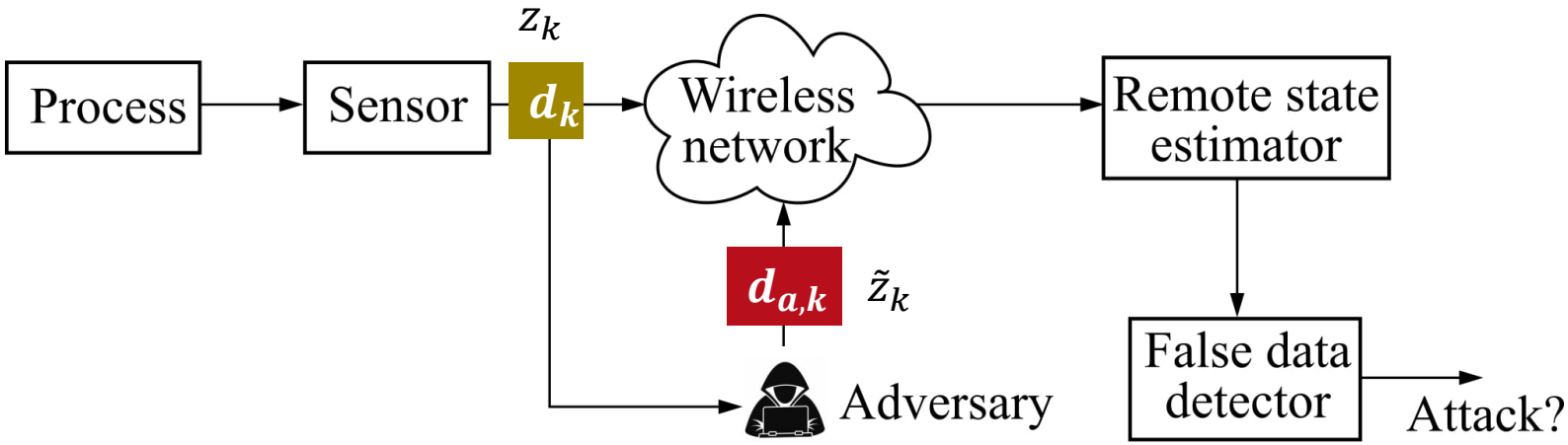
Attack design



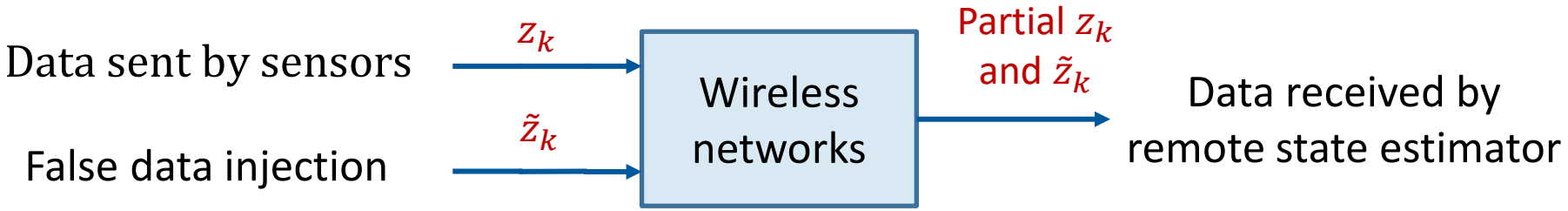
Case III: $d_k = 0$, $d_{a,k} = 1$. Deception attacks



Attack design



Case IV: $d_k = 1$, $d_{a,k} = 1$. Hybrid attacks



Attack design

Probability distribution of innovation

Nominal innovation $z_k \sim \mathcal{N}(0, \Sigma_k)$ (1)

Compromised innovation $\tilde{z}_k \sim \mathcal{N}(0, \Sigma_k)$ (2)

Transmission rate

Attack design

Probability distribution of innovation

Nominal innovation $z_k \sim \mathcal{N}(0, \Sigma_k)$ (1)

Compromised innovation $\tilde{z}_k \sim \mathcal{N}(0, \Sigma_k)$ (2)

Transmission rate

Total number of transmission under normal operation

$$\underline{\lambda}_k \leq \lambda_k = \sum_{i=1}^{k} d_i \leq \overline{\lambda}_k \quad (3)$$

Total number of transmission under attacks

$$\underline{\lambda}_k \leq \tilde{\lambda}_k \leq \overline{\lambda}_k \quad (4)$$

Attack design

Attack model

$\tilde{z}_k$

Compromised innovation $\tilde{z}_k \sim \mathcal{N}(0, \Sigma_k)$ (2)

Total number of transmission under attacks

$$\underline{\lambda}_k \leq \tilde{\lambda}_k \leq \overline{\lambda}_k \quad (4)$$

Stochastic event-based stealthy hybrid attacks on remote state estimation with packet dropouts, *IEEE Transactions on Automatic Control*

Design of stealthy attacks on remote estimation with historical data, *IEEE Transactions on Control of Network Systems*

Attack design

Attack model[1][2]

$\tilde{z}_k$

Compromised innovation $\tilde{z}_k \sim \mathcal{N}(0, \Sigma_k)$ (2)

Total number of transmission under attacks

$$\underline{\lambda}_k \leq \tilde{\lambda}_k \leq \bar{\lambda}_k \quad (4)$$

Attack evaluation

$$\tilde{P}_k = \mathbb{E}[(x_k - \tilde{x}_k)(x_k - \tilde{x}_k)^T] \quad (5)$$

[1] Z. Lian, P. Shi, C. P. Lim, and R. K. Agarwal, "Stochastic event-based stealthy hybrid attacks on remote state estimation with packet dropouts," *IEEE Transactions on Automatic Control, under revision, 2022.*
[2] Z. Lian, P. Shi, and C. C. Lim, "Design of stealthy attacks on remote estimation with historical data," *IEEE Transactions on Control of Network Systems, under review, 2022.*

Attack design

Attack model[1][2]

$\tilde{z}_k$

Compromised innovation $\tilde{z}_k \sim \mathcal{N}(0, \Sigma_k)$ (2)

Total number of transmission under attacks

$$\underline{\lambda}_k \leq \tilde{\lambda}_k \leq \bar{\lambda}_k \quad (4)$$

Attack evaluation

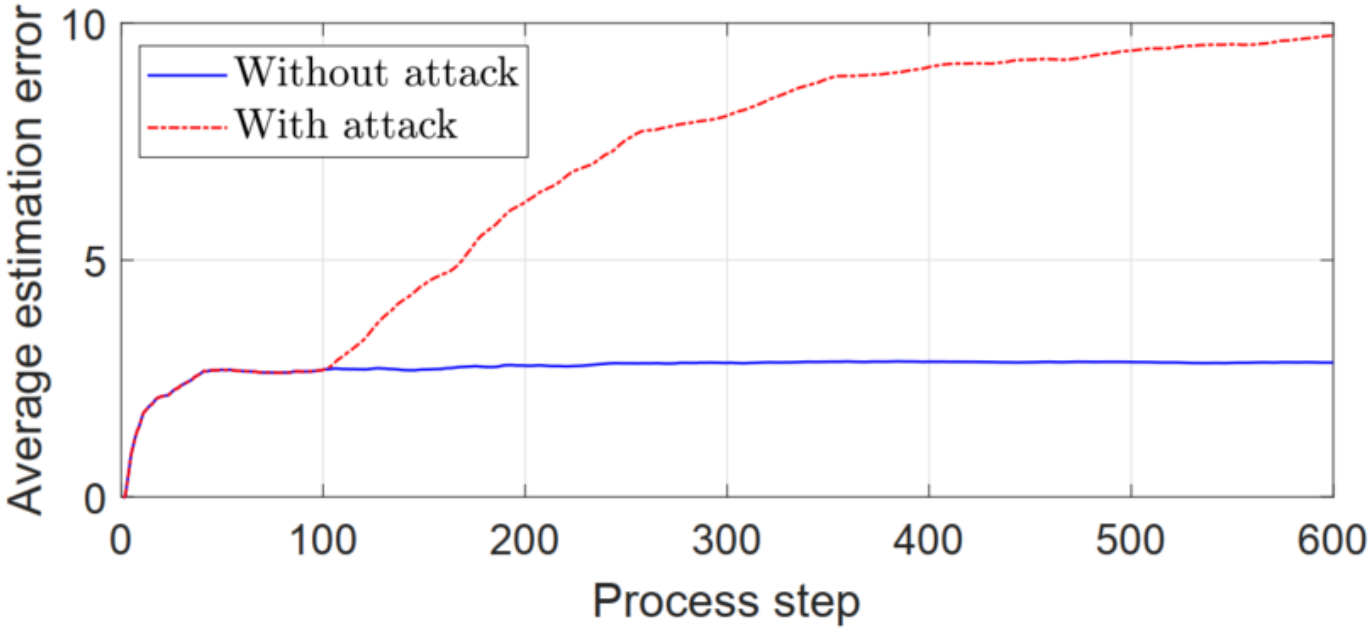
$$\tilde{P}_k = \mathbb{E}[(x_k - \tilde{x}_k)(x_k - \tilde{x}_k)^T] \quad (5)$$

Problem of interest

max $\tilde{P}_k$
subject to (2), and (4)

Attack design

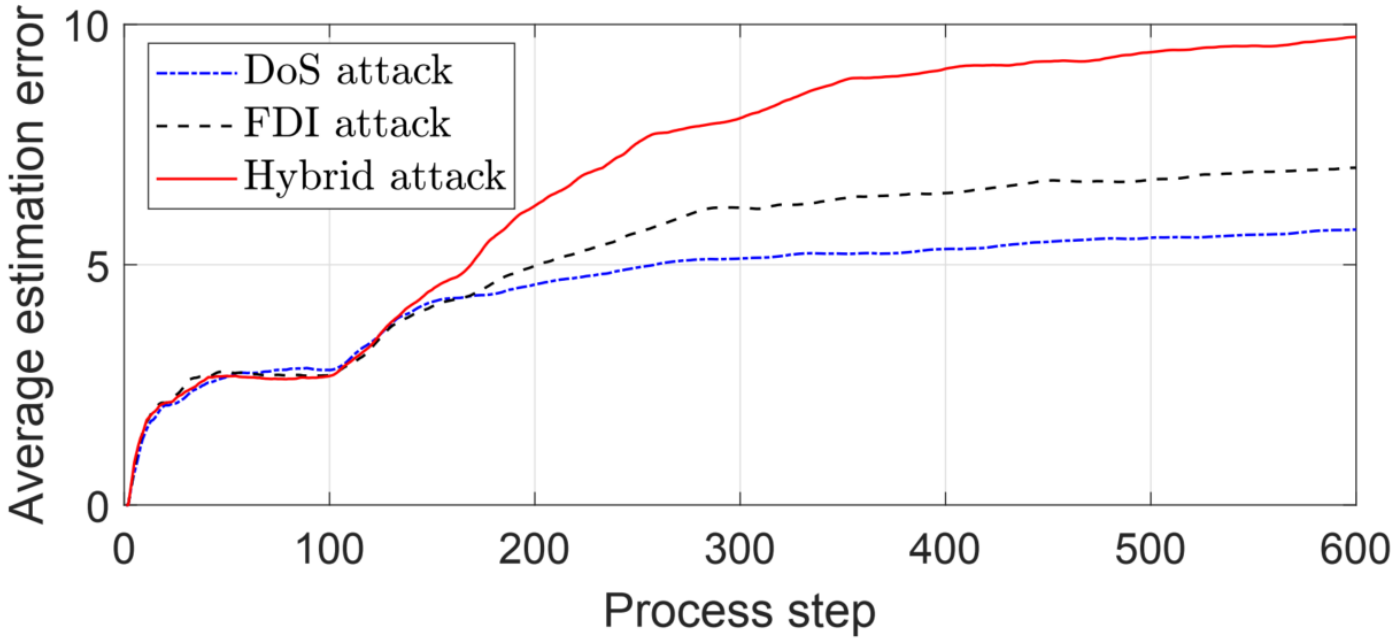
Simulation results



Average estimation error

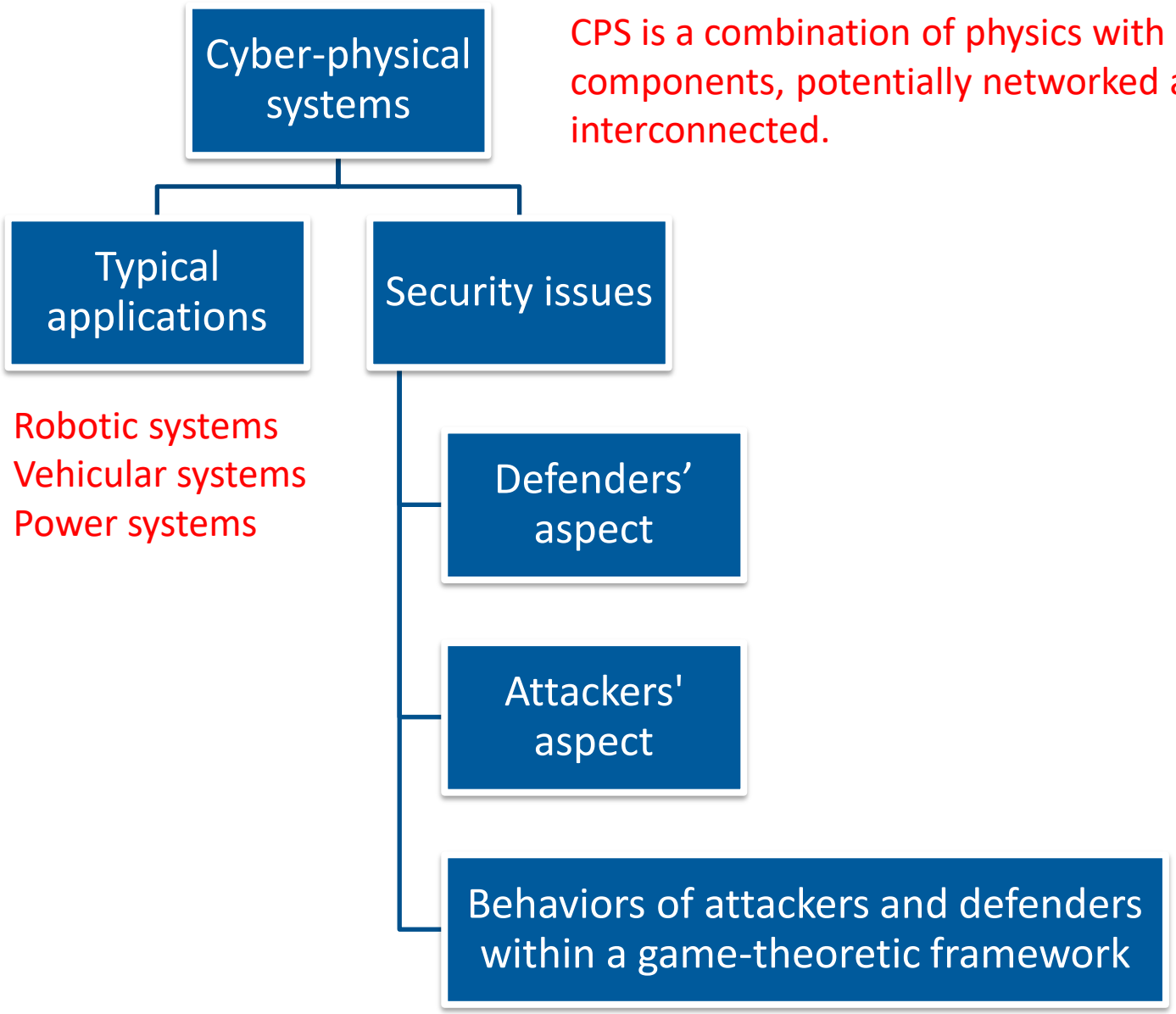
Attack design

Simulation results



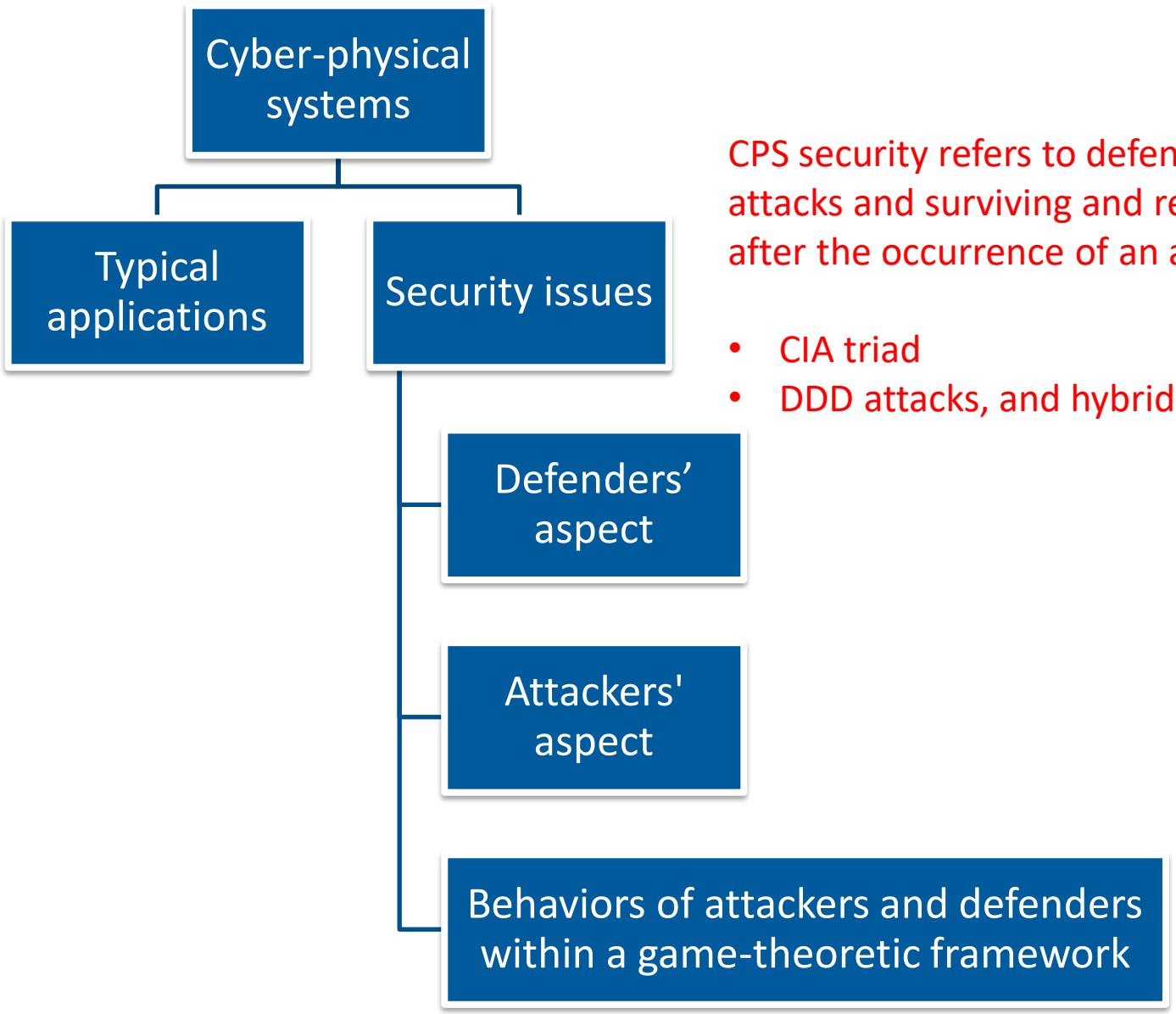
Average estimation error under different attack policies

Conclusion



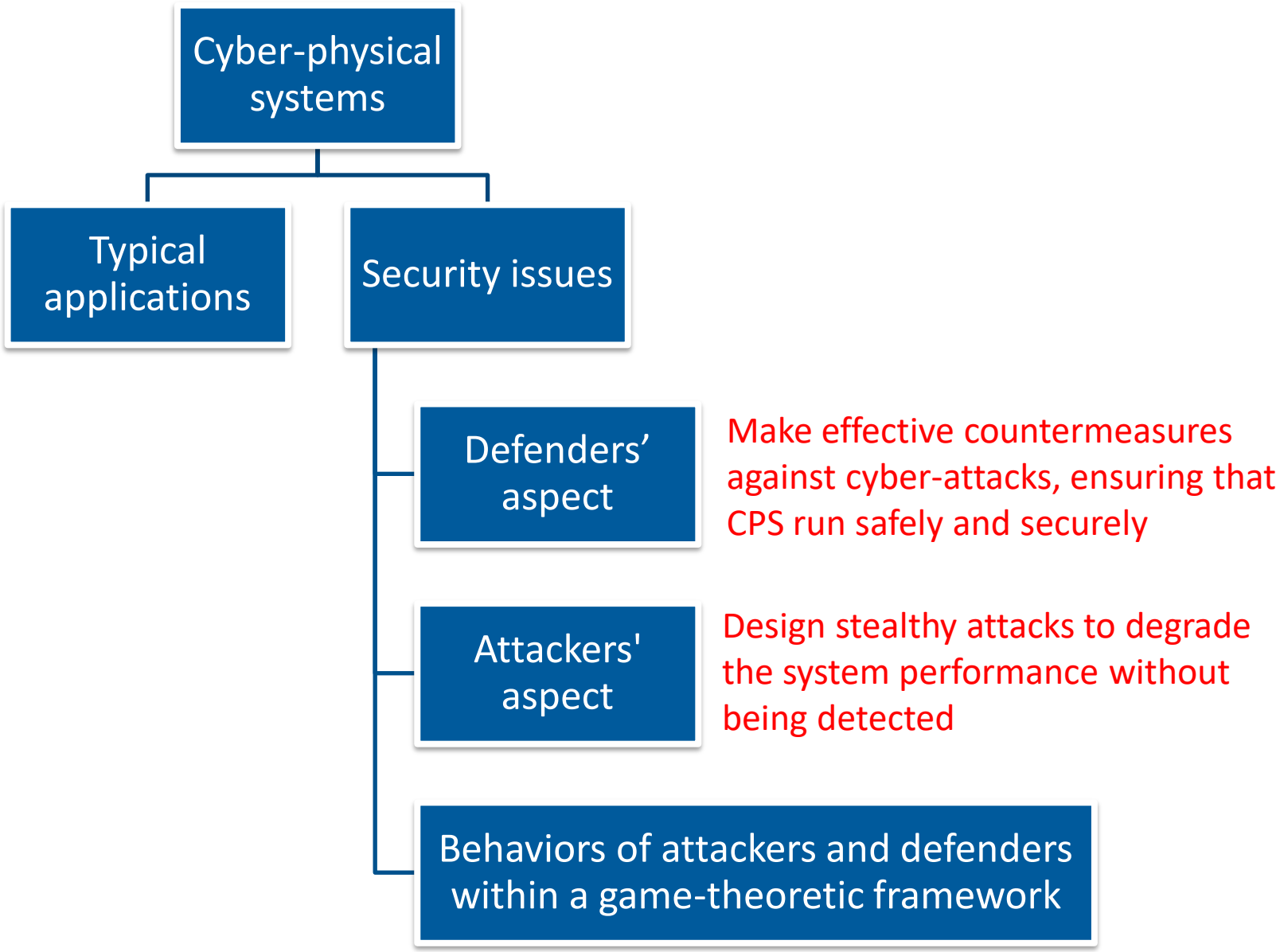
CPS is a combination of physics with cyber components, potentially networked and tightly interconnected.

- Robotic systems
- Vehicular systems
- Power systems



CPS security refers to defending against attacks and surviving and recovering after the occurrence of an attack.

- CIA triad
- DDD attacks, and hybrid attacks


Cyber-physical systems
Typical applications
Security issues
Defenders' aspect
Make effective countermeasures against cyber-attacks, ensuring that CPS run safely and securely
Attackers' aspect
Design stealthy attacks to degrade the system performance without being detected
Behaviors of attackers and defenders within a game-theoretic framework

Thank you for listening
Questions/Comments?

Plans --Professorship Program

Research collaborations in any forms

- Funding applications
- Junior staff/postgraduates training/supervisions
- Publications
- Journal special issues
- Conferences/symposiums/workshops/invited sessions
- Exchange programs
- .....
- .....

THE UNIVERSITY
of ADELAIDE