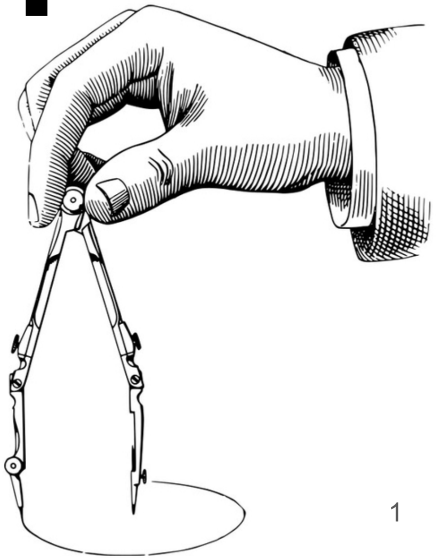
Charting The Cyber-Physical System Security Landscape



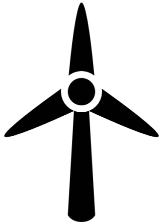
Miguel A. Arroyo

Ph.D. Candidacy Exam
Nov. 27th, 2018



Cyber-Physical Systems

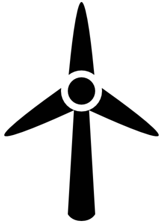
Systems that sense and actuate on the physical environment.





Cyber-Physical Systems

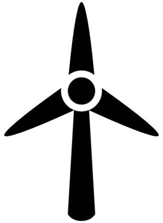
Systems that ***sense*** *and actuate on the physical environment.*



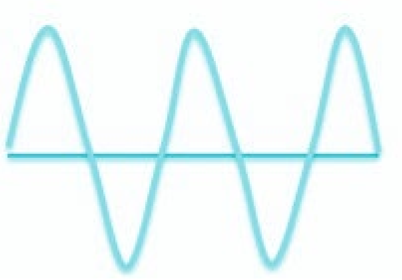


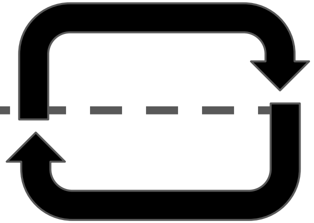
Cyber-Physical Systems

Systems that ***sense*** *and* ***actuate*** *on the physical environment.*



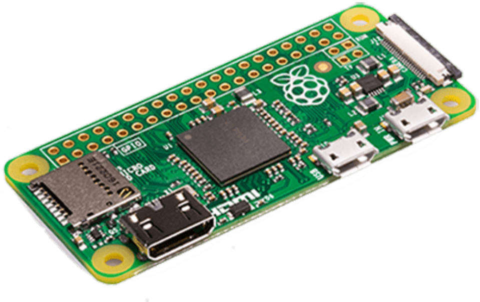
Analog





Digital

0100111101

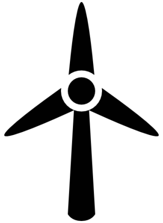




The Problem

“Our daily lives will depend more and more on these systems. Our lives, our money, our welfare. How can we design cyber-physical systems that we can bet our lives on?”

--Jeannette M. Wing

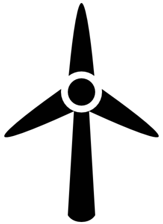




The Problem

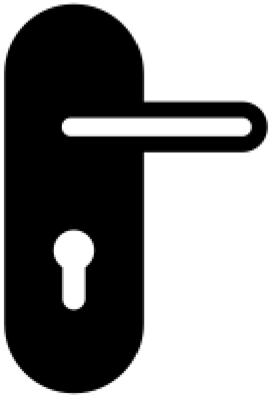
"Our daily lives will depend more and more on these systems. Our lives, our money, our welfare. ***How can we design cyber-physical systems that we can bet our lives on?****"*

--Jeannette M. Wing



Safety

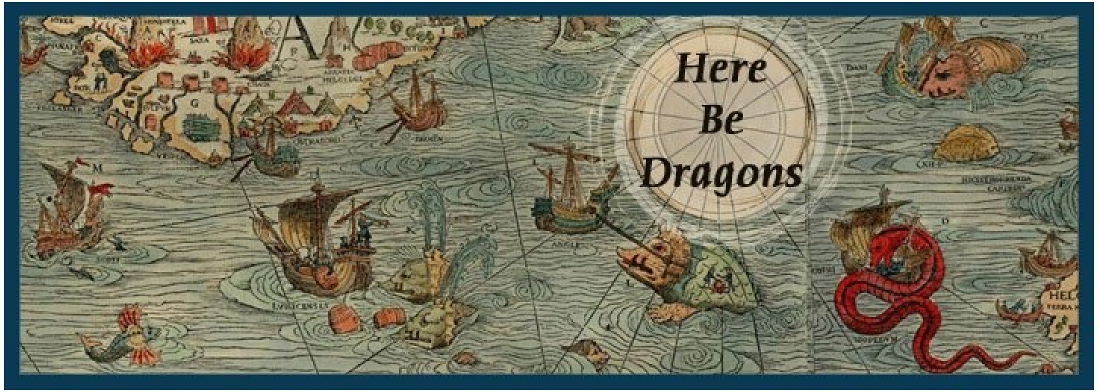
Security



Safety

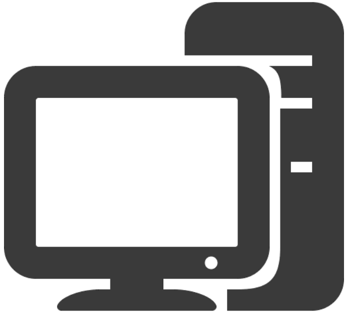
The Claim

CPS Security is Different

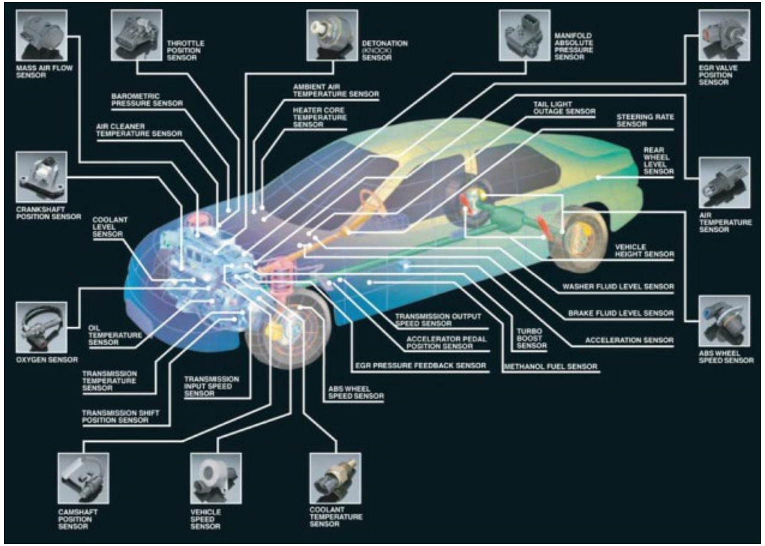


CPS Security is Different…

- It can overlap with traditional cyber-security.
    - Similar software and network vulnerabilities [1,4].

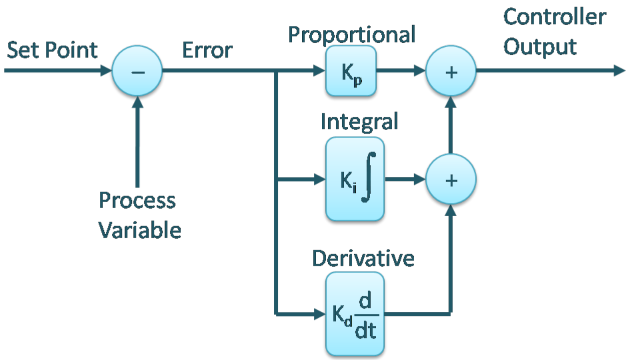


~



CPS Security is Different...

- It opens up unexplored surfaces.
  - Control algorithms [2,3]
  - Physical environment [5-10]



Research Question

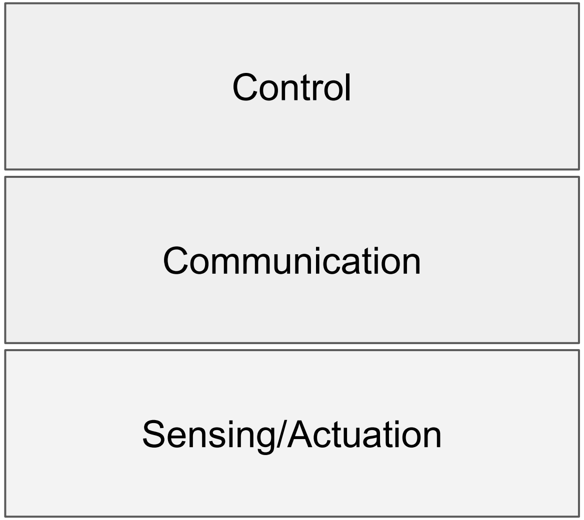
Research Question

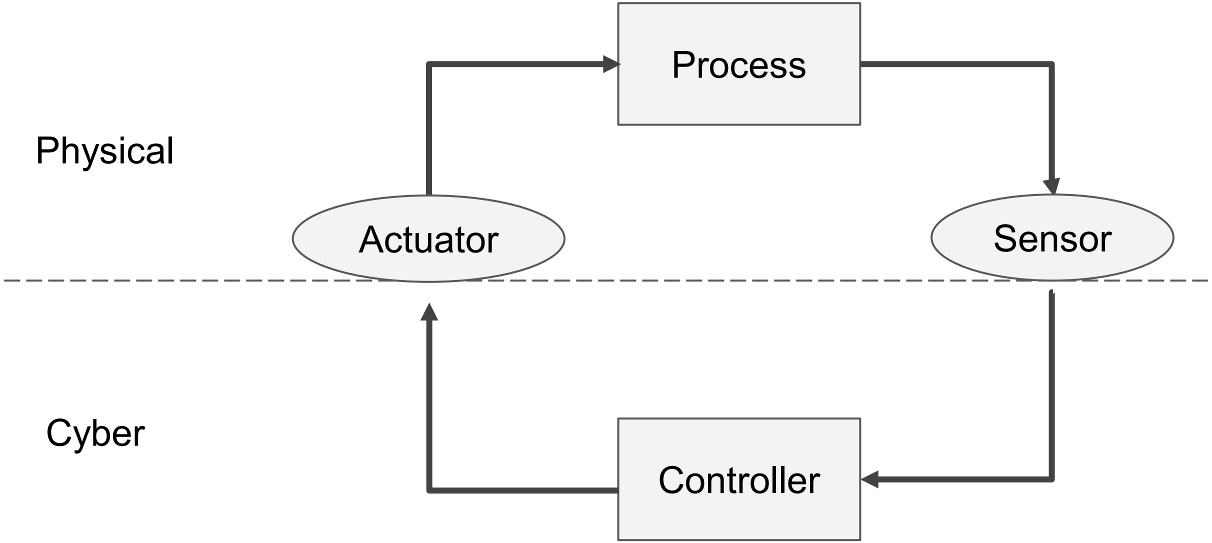
To what degree can existing security techniques help and what new opportunities exist?

CPS Fundamentals

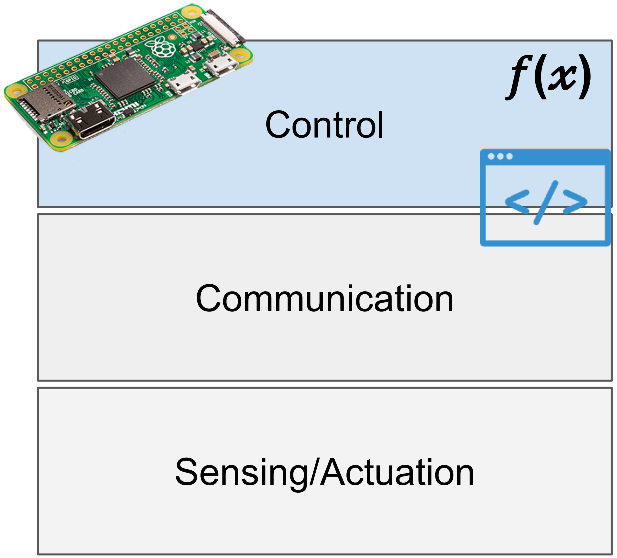
A 30,000ft view

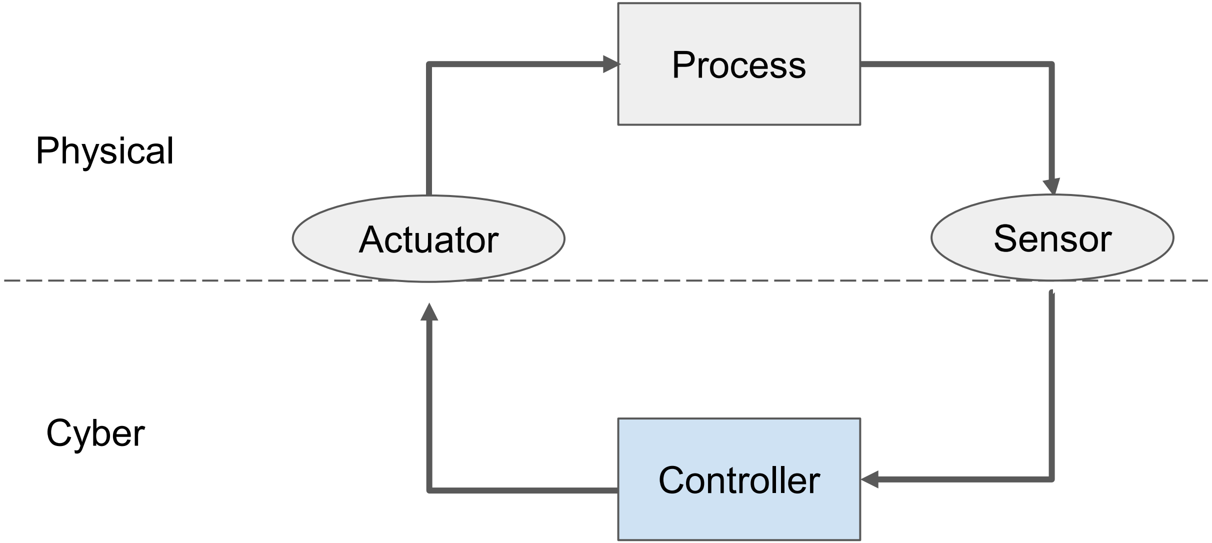
CPS Components





CPS Components

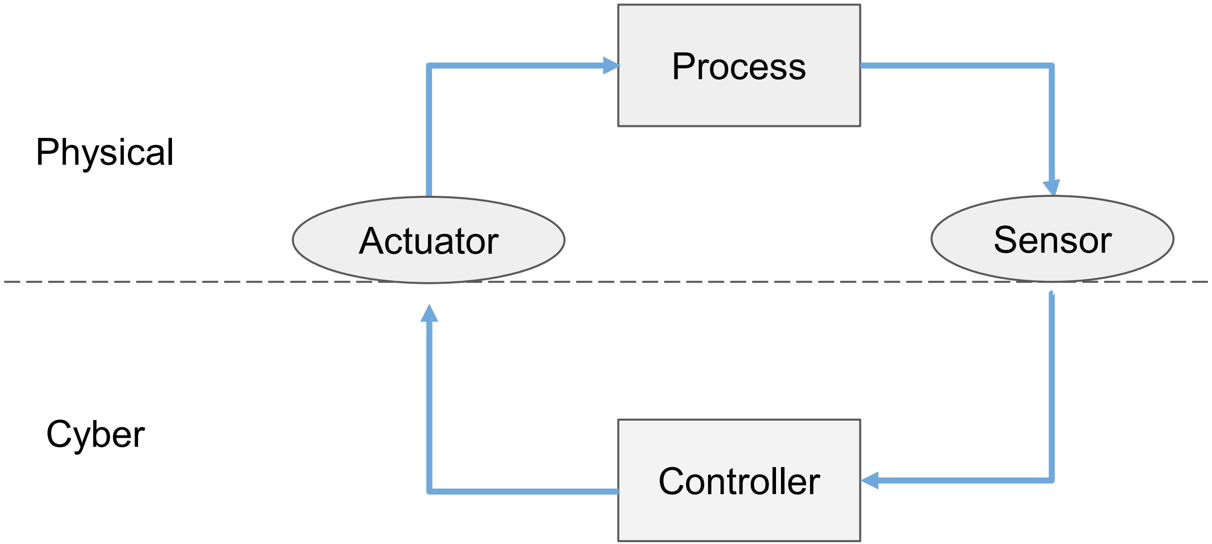




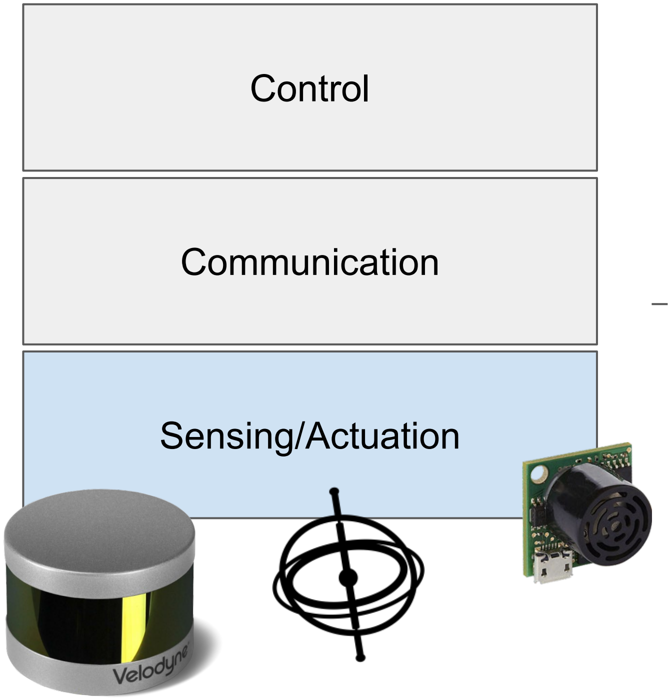
CPS Components

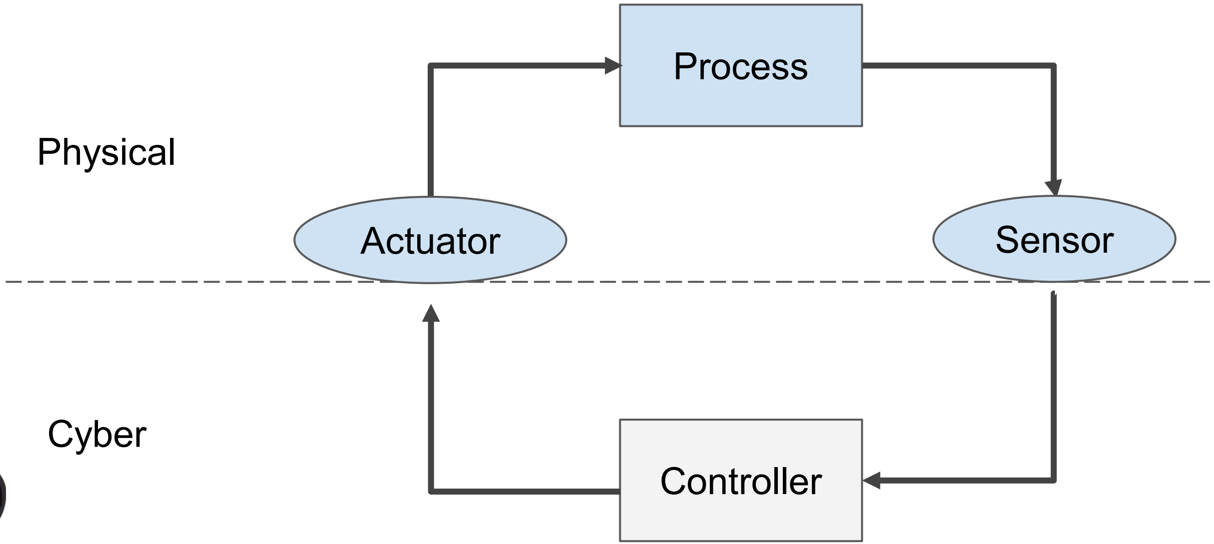
Control

Communication

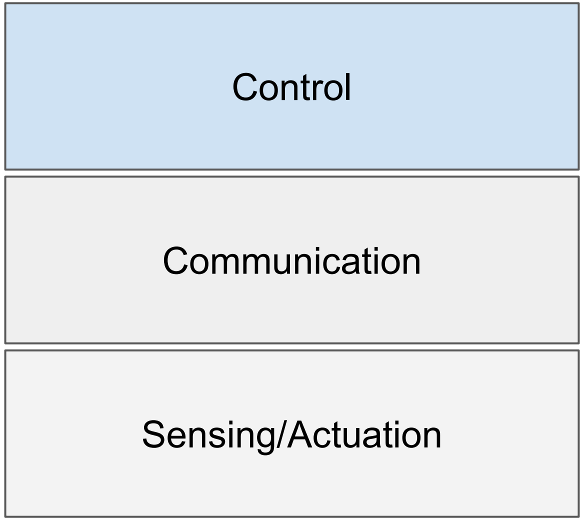


CPS Components





Threat Vectors

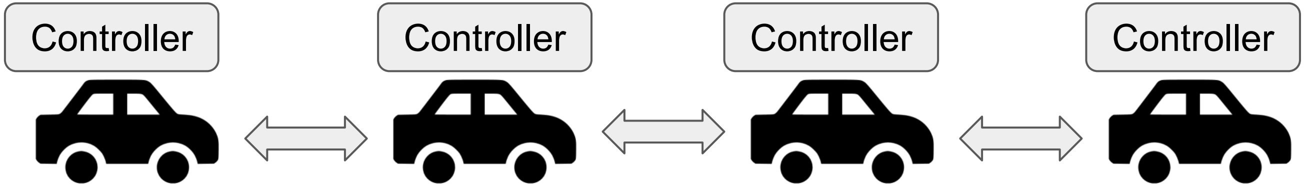

Control
Communication
Sensing/Actuation

Threat Vectors: **Control**

- **Algorithmic**
  - Violation of assumptions in control algorithms due to adversarial behavior.

Threat Vectors: **Control**

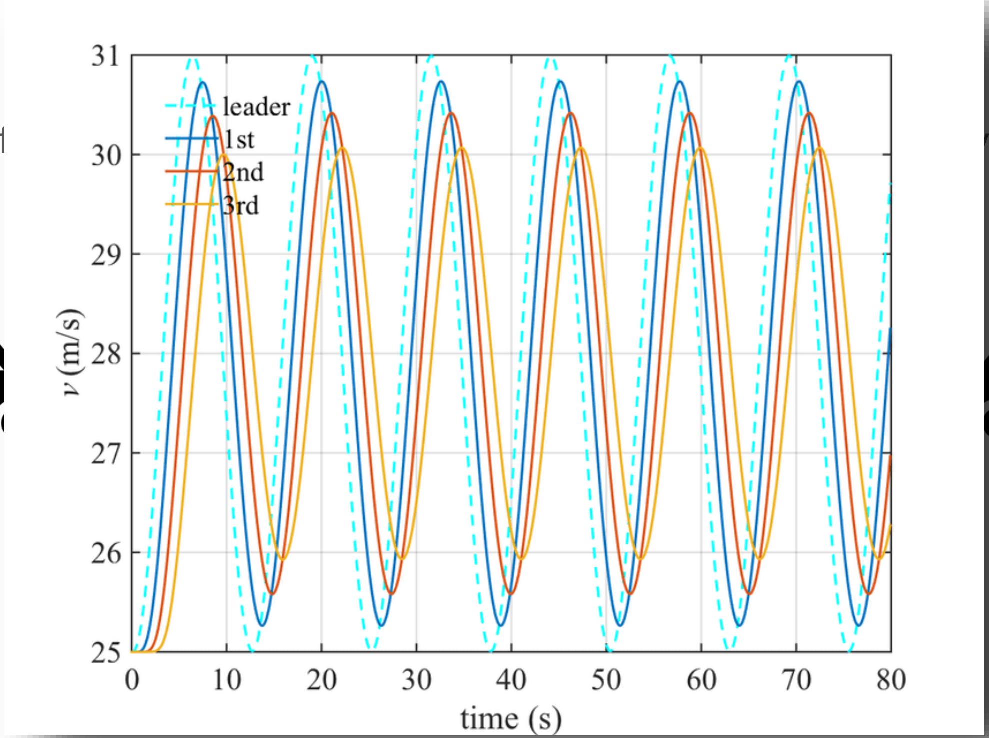
- **Algorithmic**
  - Violation of assumptions in control algorithms due to adversarial behavior.



Dadras et al. [3]
Vehicular Platooning in an Adversarial Environment

Threat Vectors: **Control**

- **Algorithmic**
  - Violation of ... ior.



Dadras et al. [3]
Vehicular Platooning in an Adversarial Environment

Threat Vectors: **Control**

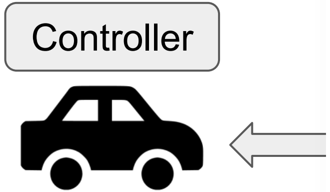
- **Algorithmic**
  - Violation of assumptions in control algorithms due to adversarial behavior.

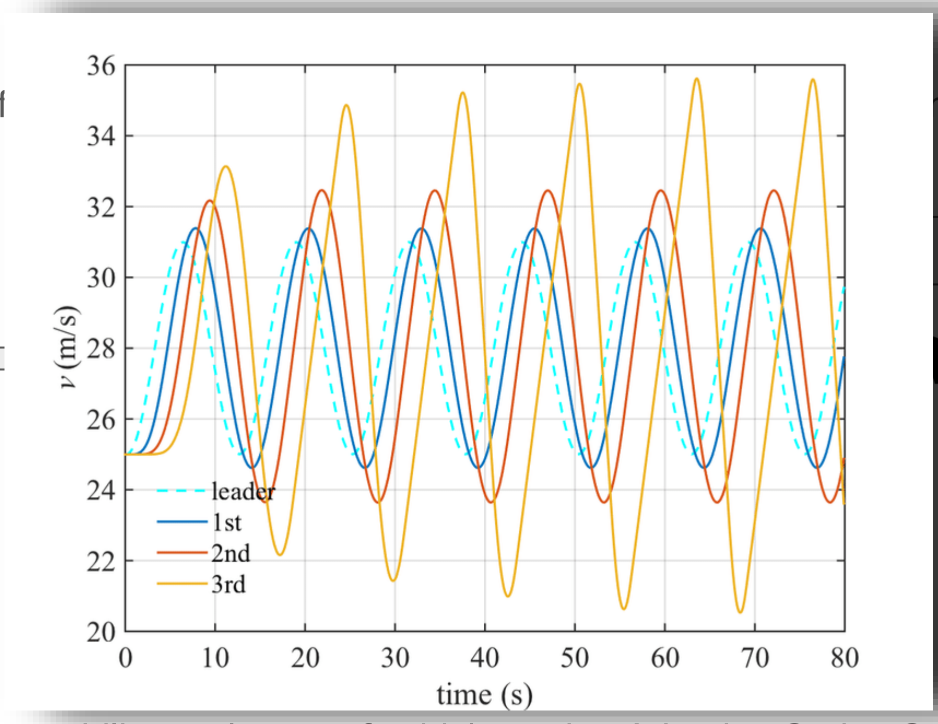
Destabilize a platoon of vehicles using Adaptive Cruise Control.

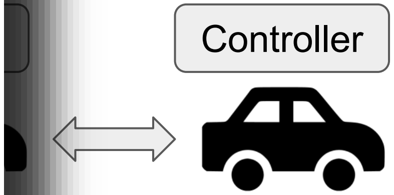
Dadras et al. [3]
Vehicular Platooning in an Adversarial Environment

Threat Vectors: **Control**

- **Algorithmic**
  - Violation of
  avior.







Destabilize a platoon of vehicles using Adaptive Cruise Control.

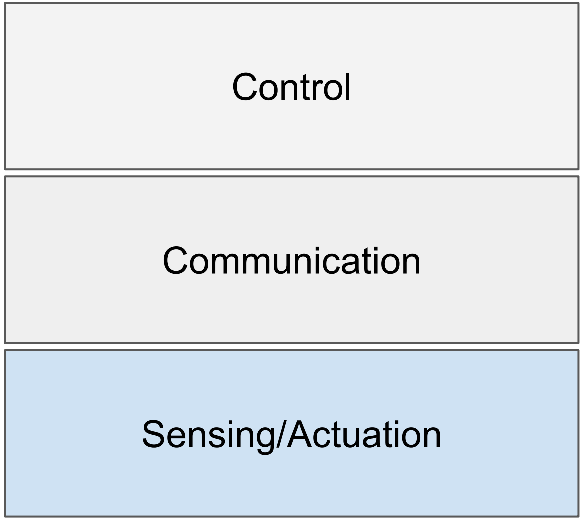
Dadras et al. [3]
Vehicular Platooning in an Adversarial Environment

Threat Vectors: **Control**

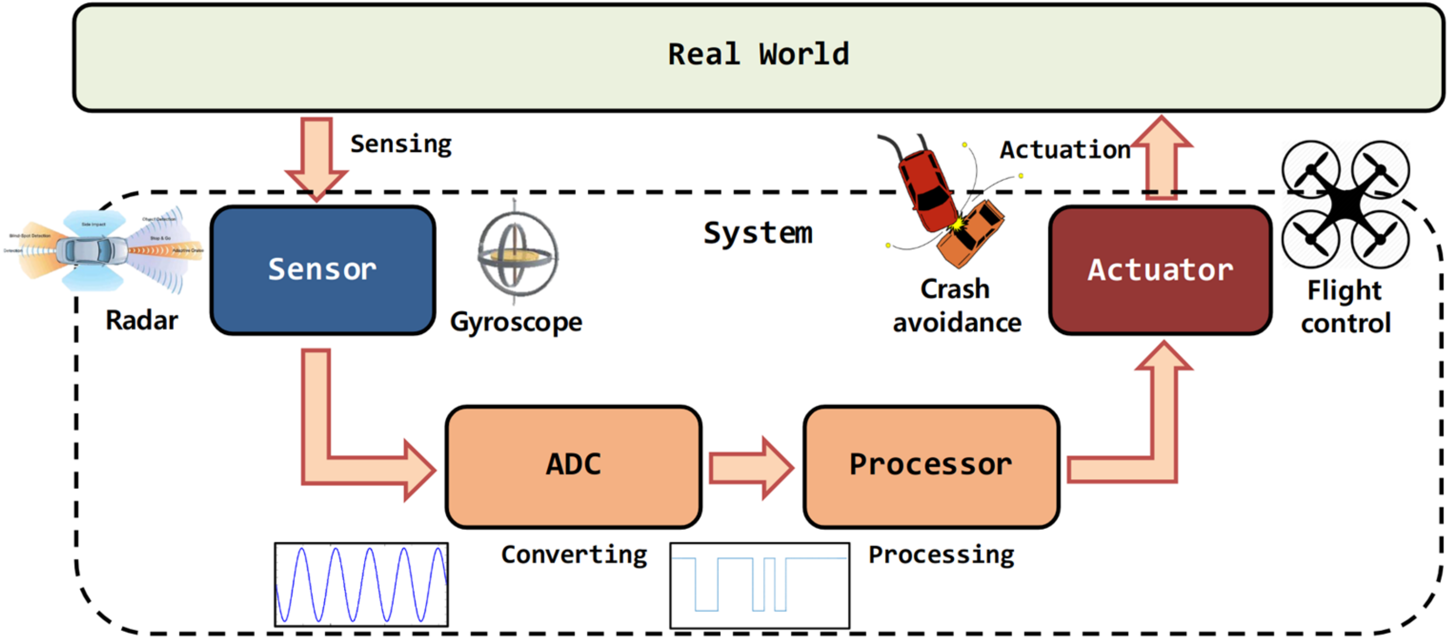
- **Algorithmic**
  - Violation of assumptions in control algorithms due to adversarial behavior.

Take Away

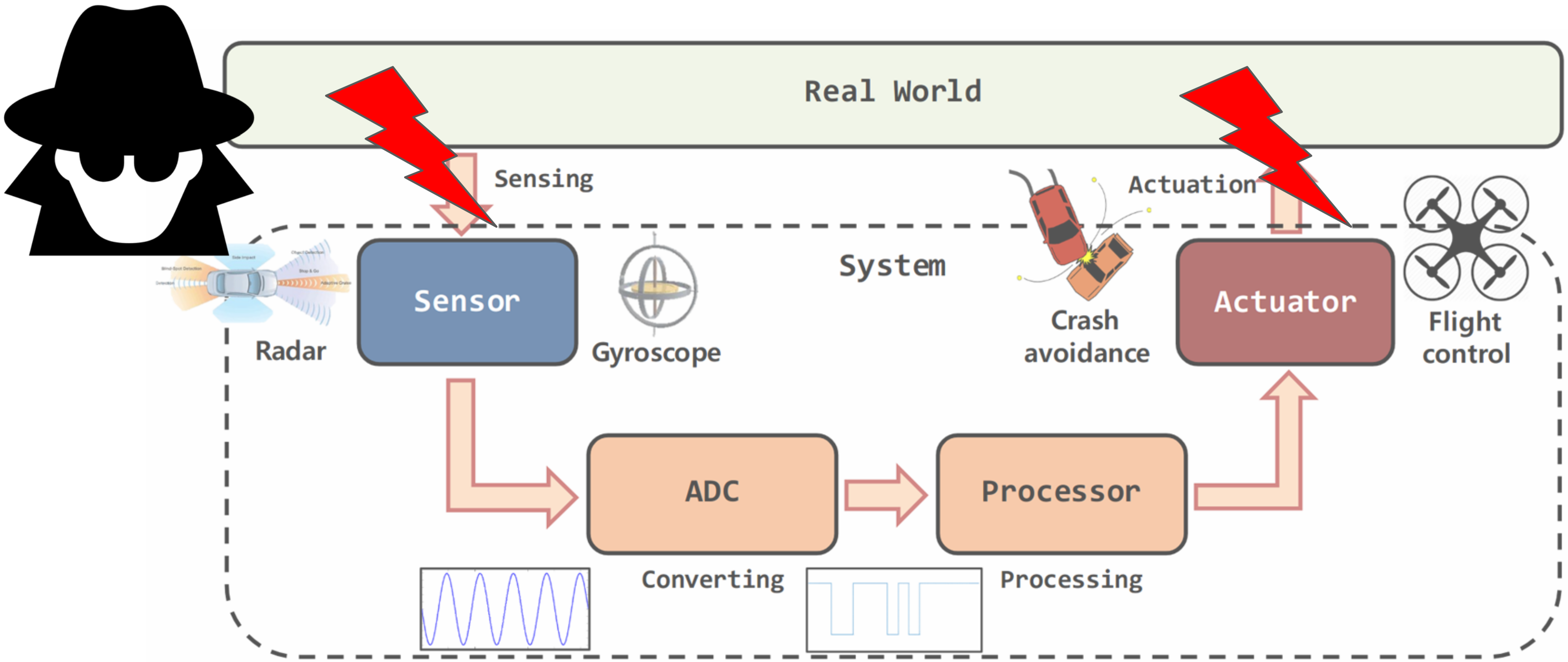
Even perfectly secure hardware & software may be compromised if control algorithms cannot properly handle malicious inputs.


Control
Communication
Sensing/Actuation

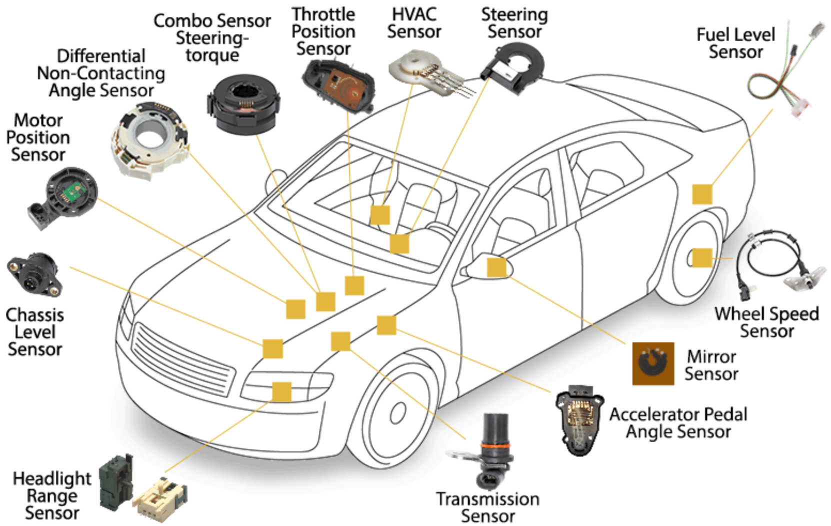
Threat Vectors: **Sensing & Actuation**

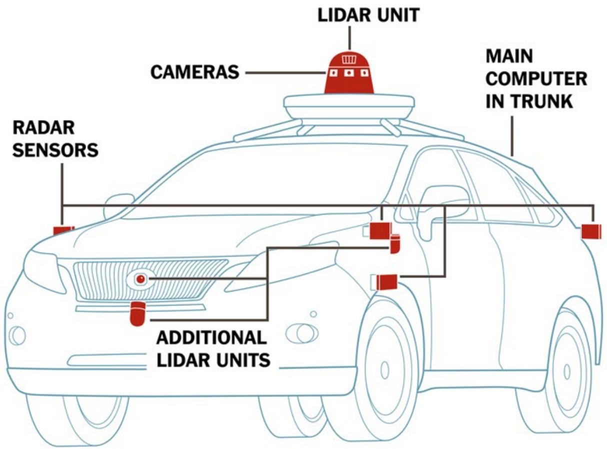


Threat Vectors: **Sensing & Actuation**

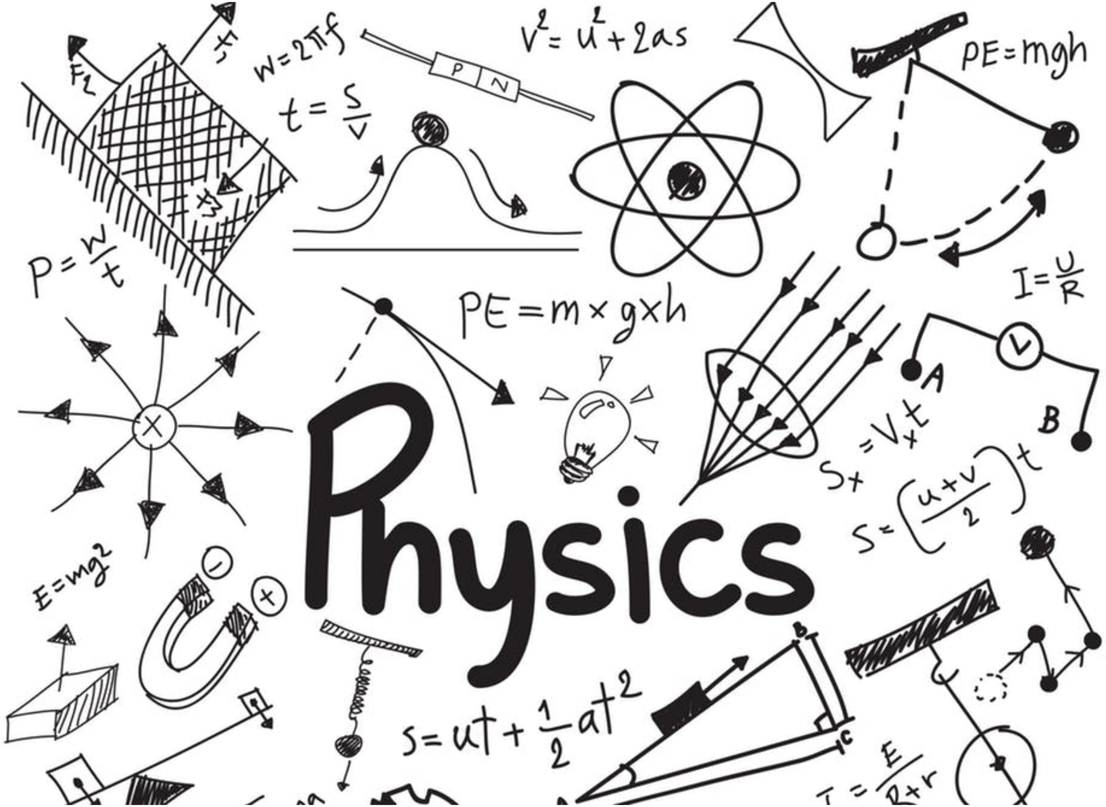


Threat Vectors: **Sensing & Actuation**

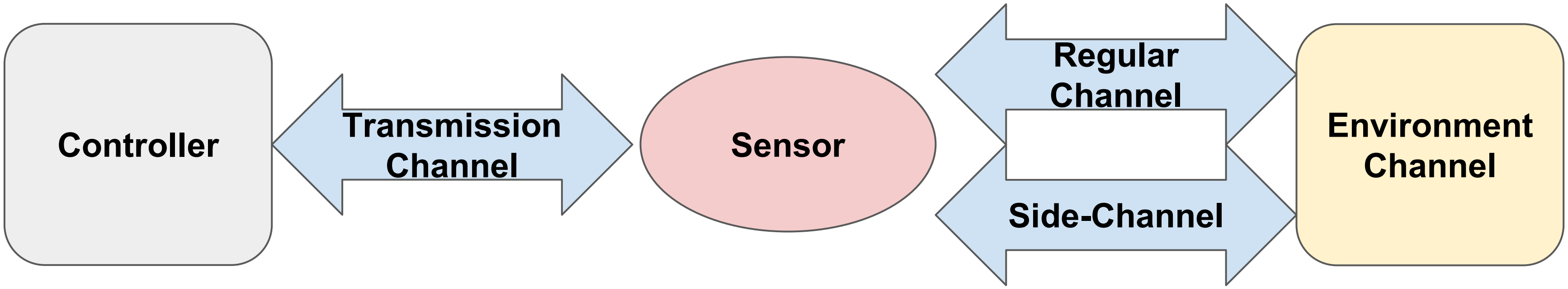




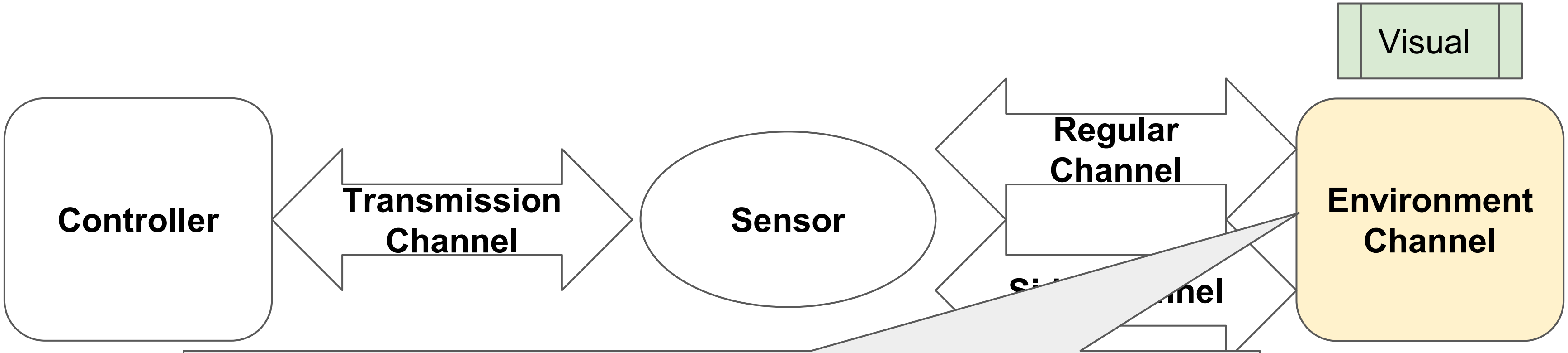
Threat Vectors: **Sensing & Actuation**



Threat Vectors: **Sensing & Actuation**



Threat Vectors: **Sensing & Actuation**

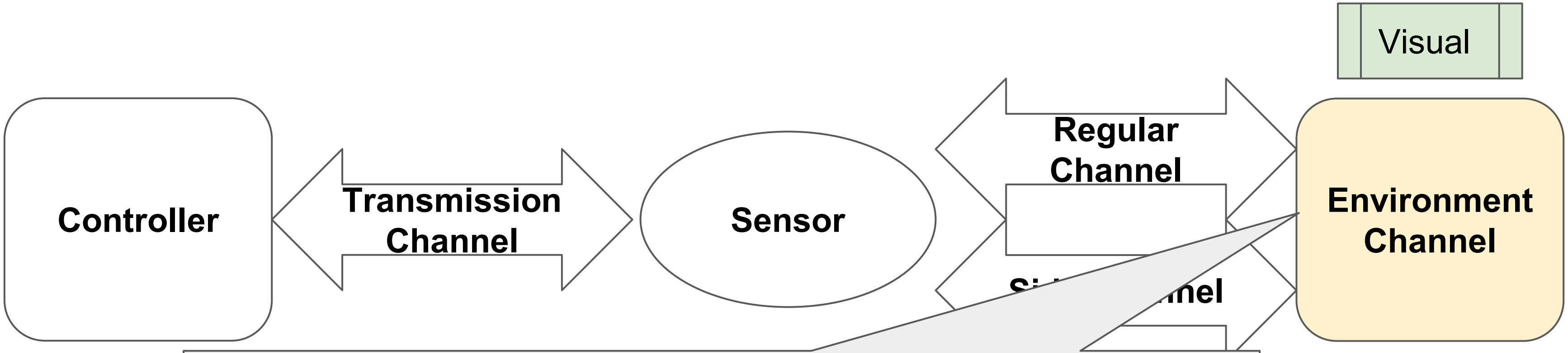


Environment Channel: Surrounding where sensing occurs.

Davidson et al. [9] - Project visual pattern to exploit optical flow sensors.

Eykholt et al. [10] - Minimally modify visual environment to force DNN misclassification.

Threat Vectors: **Sensing & Actuation**



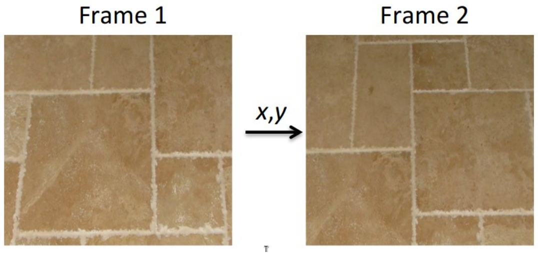
Environment Channel: Surrounding where sensing occurs.

Davidson et al. [9] - Project visual pattern to exploit optical flow sensors.

Eykholt et al. [10] - Minimally modify visual environment to force DNN misclassification.

Threat Vectors: **Sensing & Actuation**

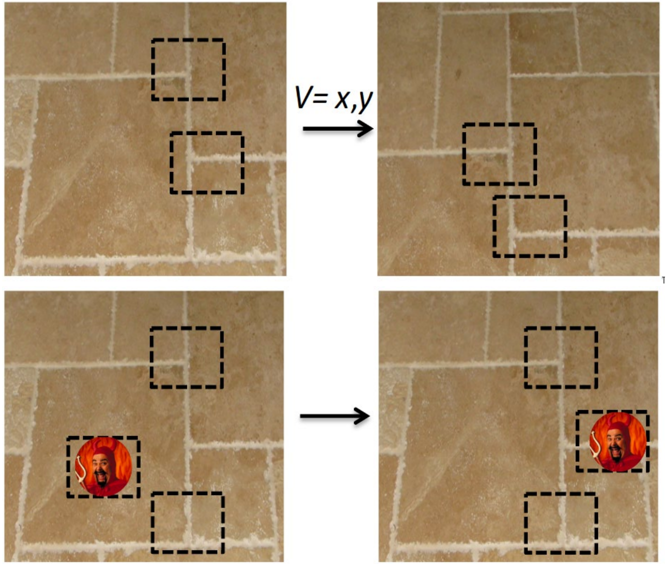
- **Visual Spoofing**
  - Modification of the visual environment.



Davidson et al. [9]
Controlling UAVs with Sensor Input Spoofing Attacks

Threat Vectors: **Sensing & Actuation**

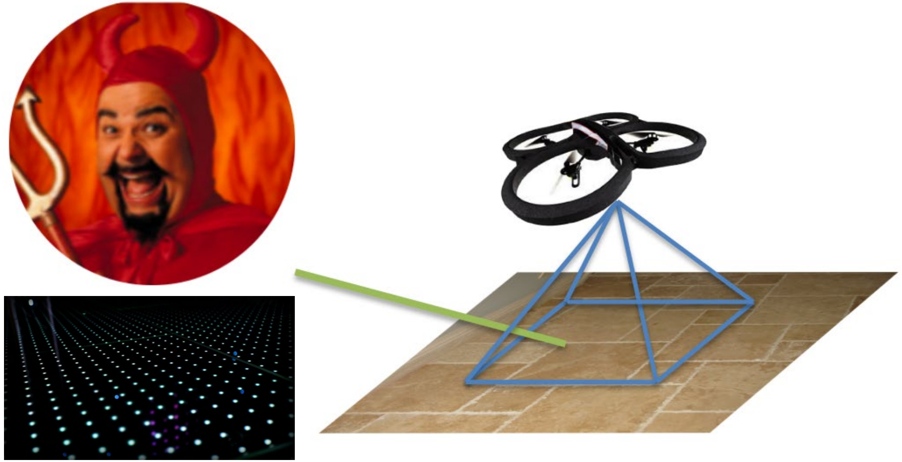
- **Visual Spoofing**
  - Modification of the visual environment.



Davidson et al. [9]
Controlling UAVs with Sensor Input Spoofing Attacks

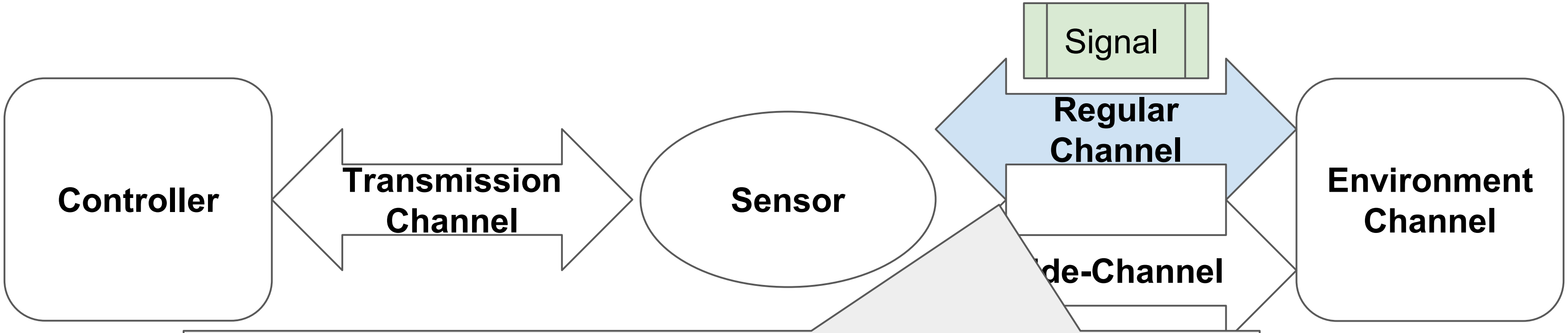
Threat Vectors: **Sensing & Actuation**

- **Visual Spoofing**
  - Modification of the visual environment.



Davidson et al. [9]
Controlling UAVs with Sensor Input Spoofing Attacks

Threat Vectors: **Sensing & Actuation**

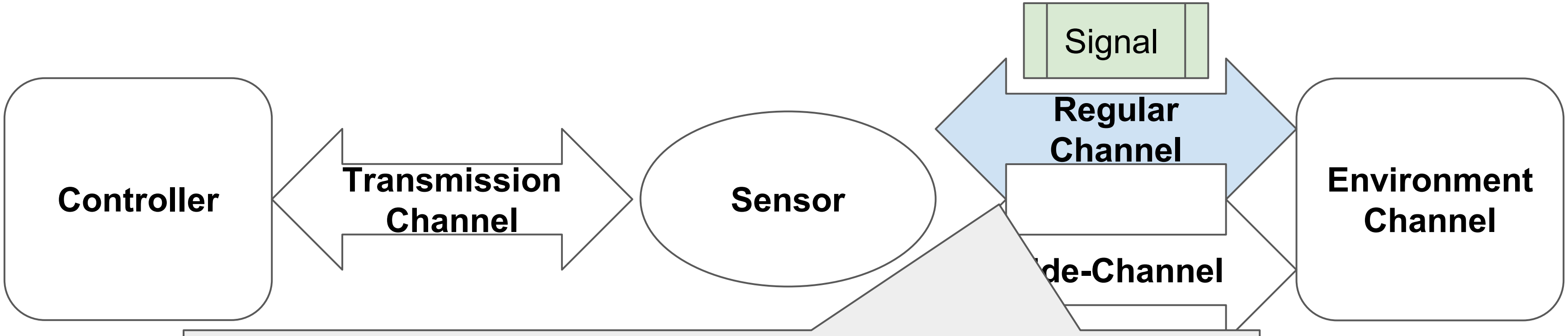


Regular Channel: Physical quantity being directly sensed.

Shoukry et al. [5] - Manipulate magnetic vehicle braking sensor.

Park et al. [8] - Saturate readings of infusion pump IR sensor.

Threat Vectors: **Sensing & Actuation**



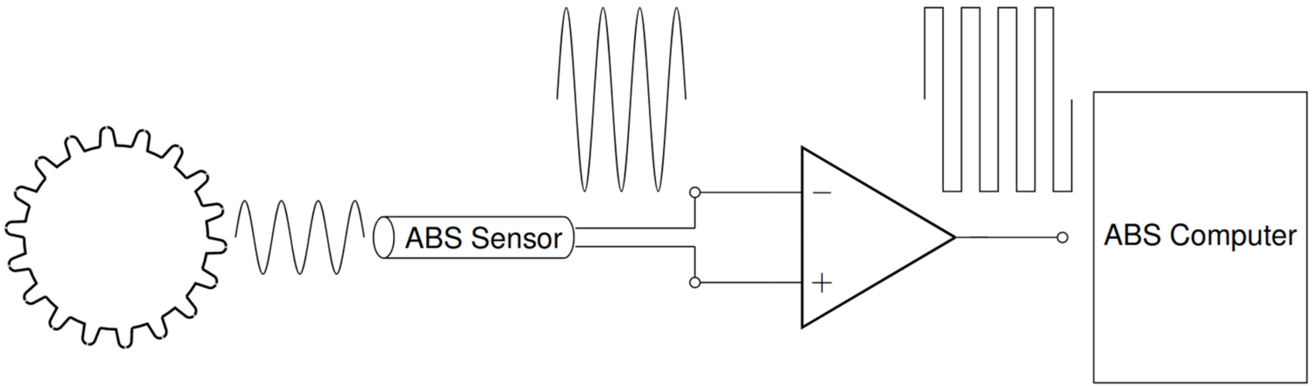
Regular Channel: Physical quantity being directly sensed.

Shoukry et al. [5] - Manipulate magnetic vehicle braking sensor.

Park et al. [8] - Saturate readings of infusion pump IR sensor.

Threat Vectors: **Sensing & Actuation**

- **Signal Spoofing**
  - Modification of the analog signal being sensed.



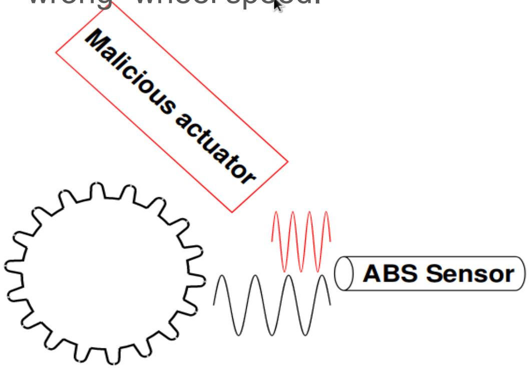
Shoukry et al. [5]
Non-Invasive Spoofing Attacks for Anti-Lock Braking Systems

Threat Vectors: **Sensing & Actuation**

- **Signal Spoofing**
  - Modification of the analog signal being sensed.

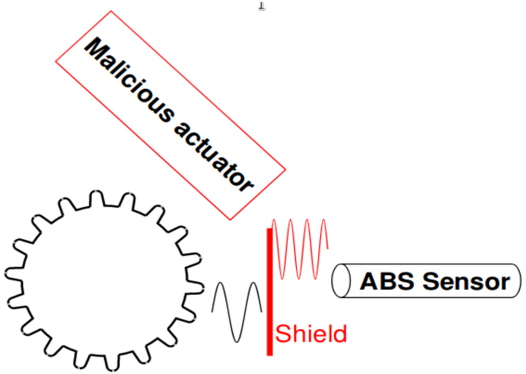
Disruptive attack:
Magnetic field is superimposed
to the
original magnetic field.

Result: sensor will measure
“wrong” wheel speed.



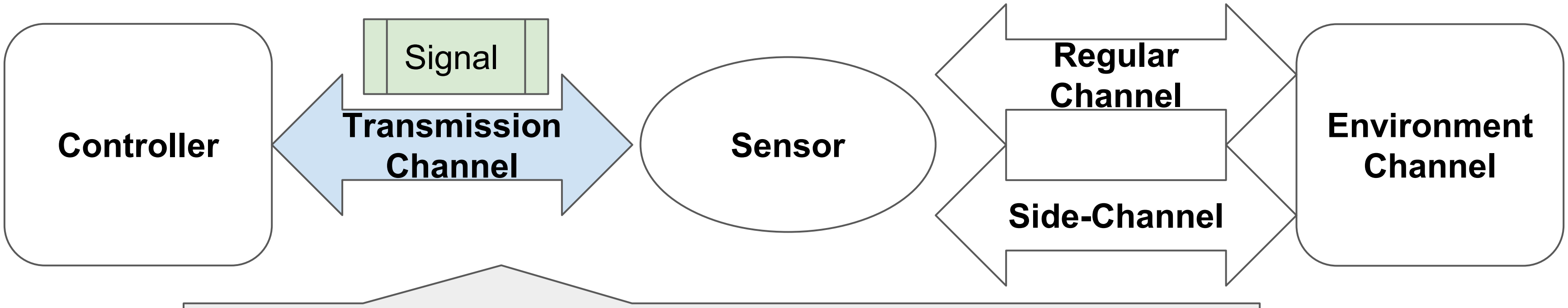
Spoofing attack:
Attacker shields the sensor from
the environment while generating
synthetic signal.

Result: precisely control the
“measured” wheel speed.



Shoukry et al. [5]
Non-Invasive Spoofing Attacks for Anti-Lock Braking Systems

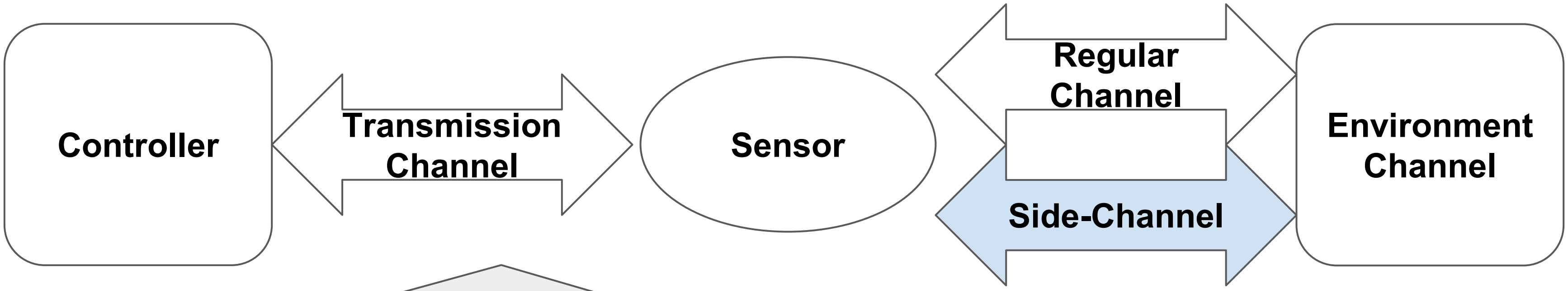
Threat Vectors: **Sensing & Actuation**



Transmission Channel: Interconnect between sensor and digitalization components.

Kune et al. [6] - Inject EMI to transmission wire in cardiac devices.

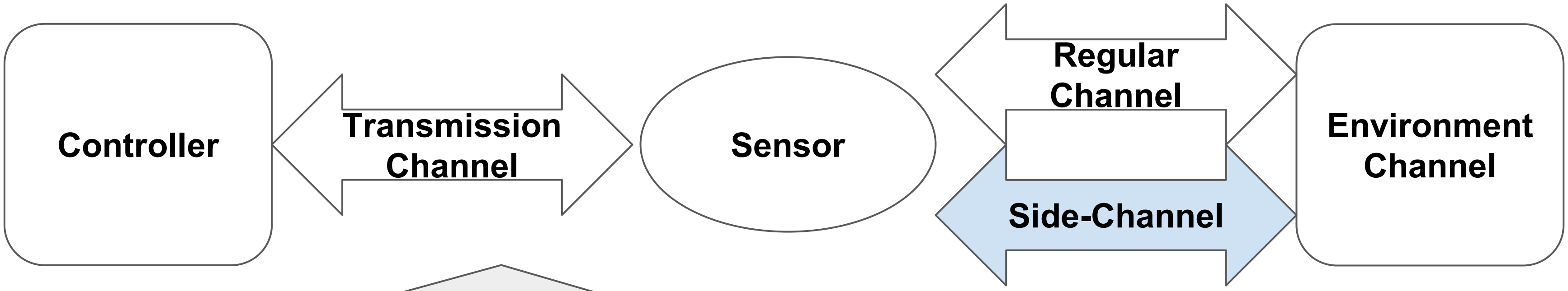
Threat Vectors: **Sensing & Actuation**



Side-Channel: Physical quantity NOT being directly sensed.

Son et al. [7] - Force resonance behavior on MEMS gyroscope.

Threat Vectors: **Sensing & Actuation**

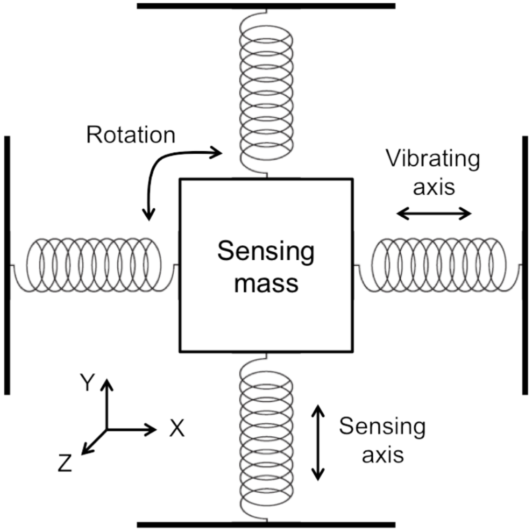


Side-Channel: Physical quantity NOT being directly sensed.

Son et al. [7] - Force resonance behavior on MEMS gyroscope.

Threat Vectors: **Sensing & Actuation**

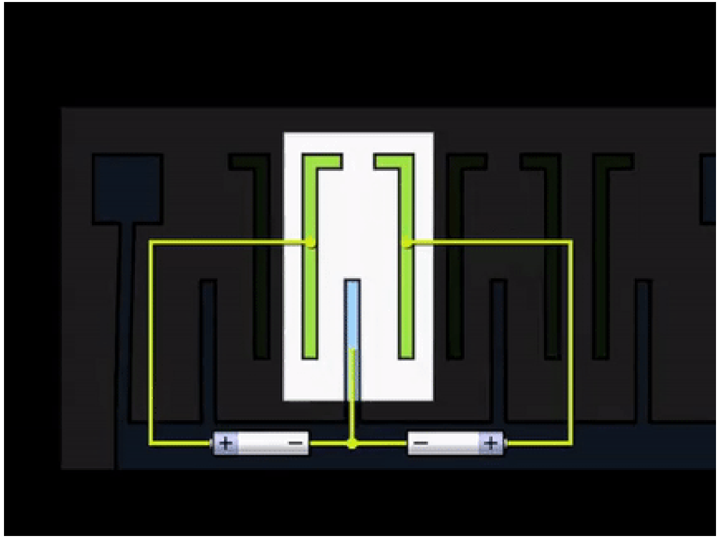
- **Signal Spoofing**
  - Modification of the analog signal being sensed.



Son et al. [7]
Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors

Threat Vectors: **Sensing & Actuation**

- **Signal Spoofing**
  - Modification of the analog signal being sensed.



Son et al. [7]
Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors

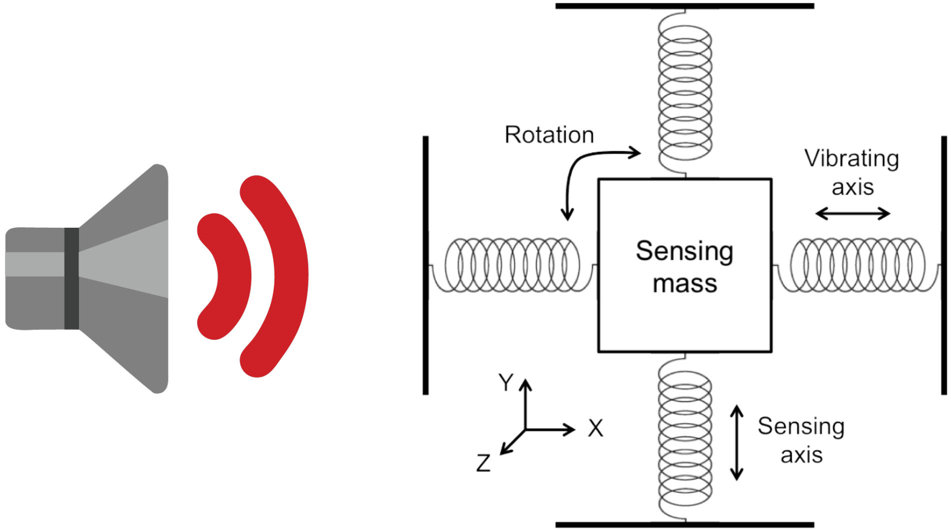
Threat Vectors: **Sensing & Actuation**

- **Signal Spoofing**

Son et al. [7]
Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors

Threat Vectors: **Sensing & Actuation**

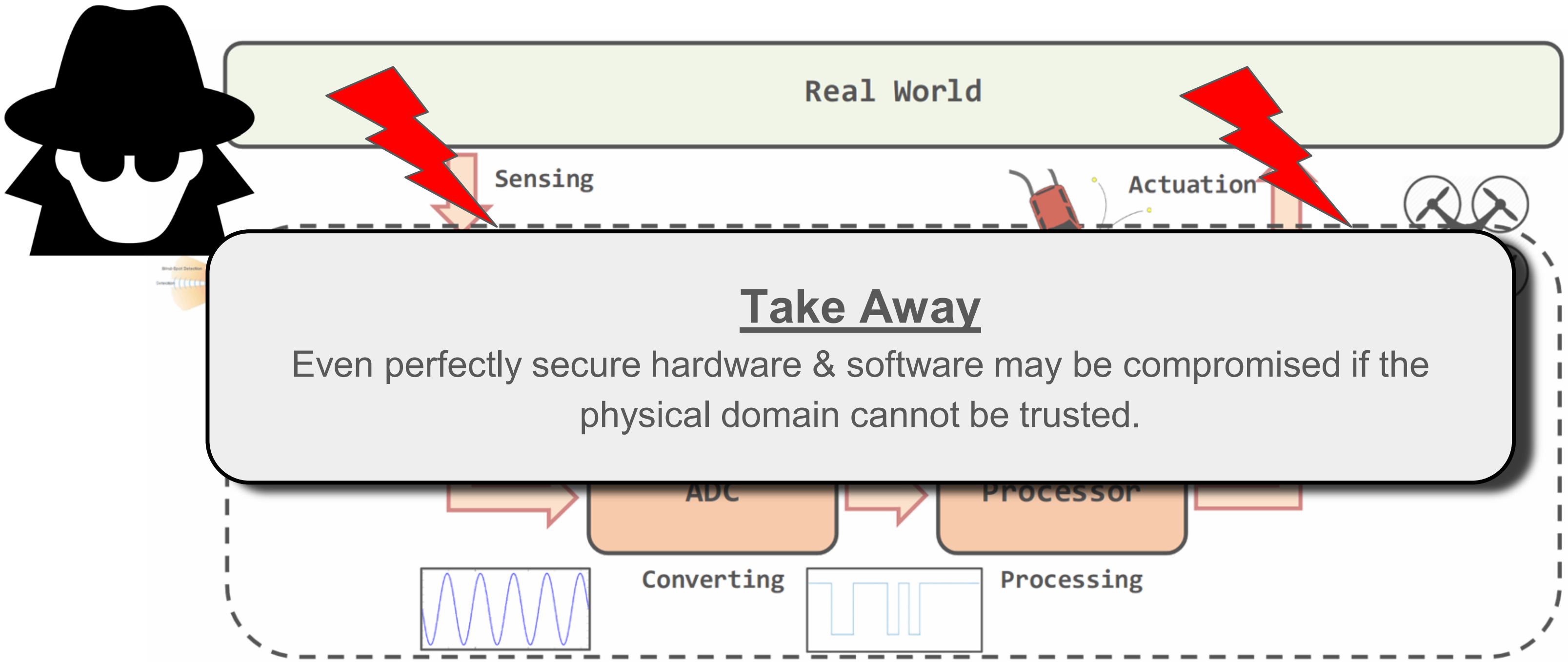
- **Signal Spoofing**
  - Modification of the analog signal being sensed.



Use sound to cause MEMS sensors to resonate and destabilize drone.

Son et al. [7]
Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors

Threat Vectors: **Sensing & Actuation**



Take Away

Even perfectly secure hardware & software may be compromised if the physical domain cannot be trusted.

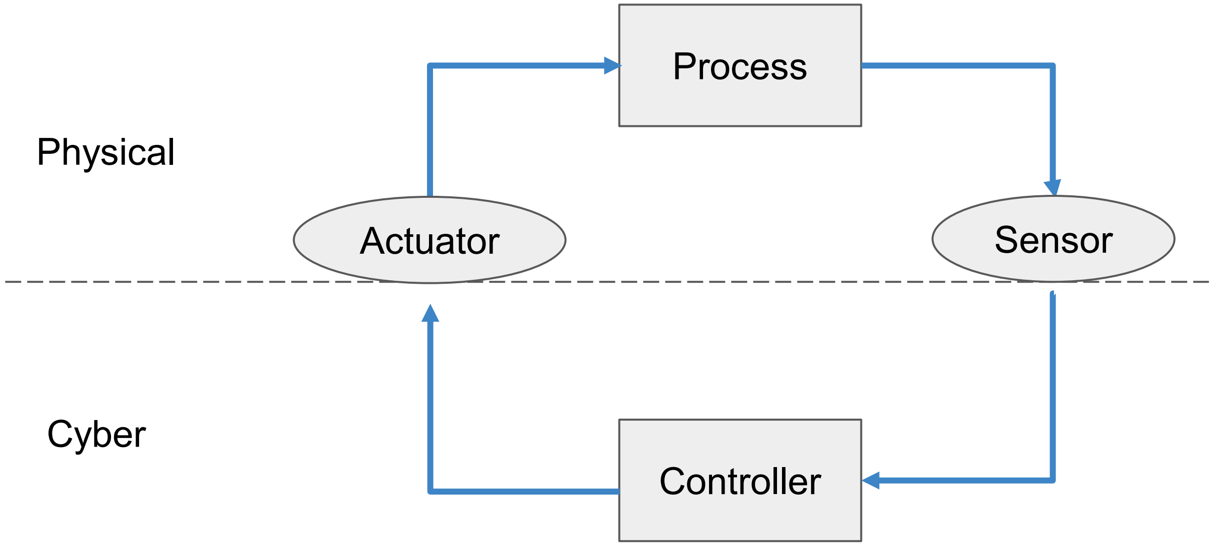
CPS Fundamentals

Revisited

A 30,000ft view

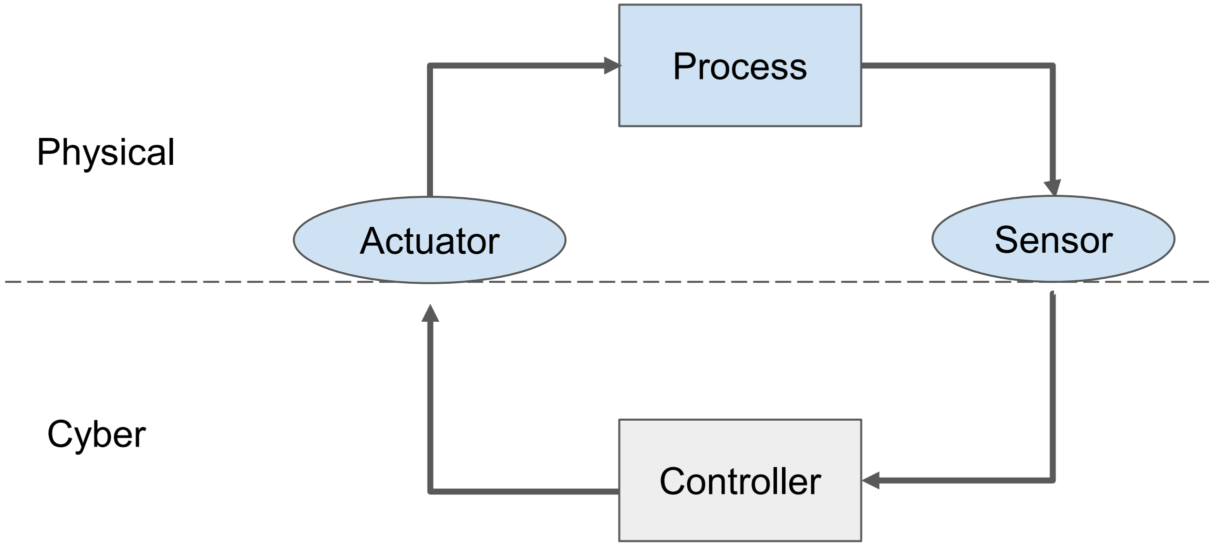
CPS Properties

- **Feedback**



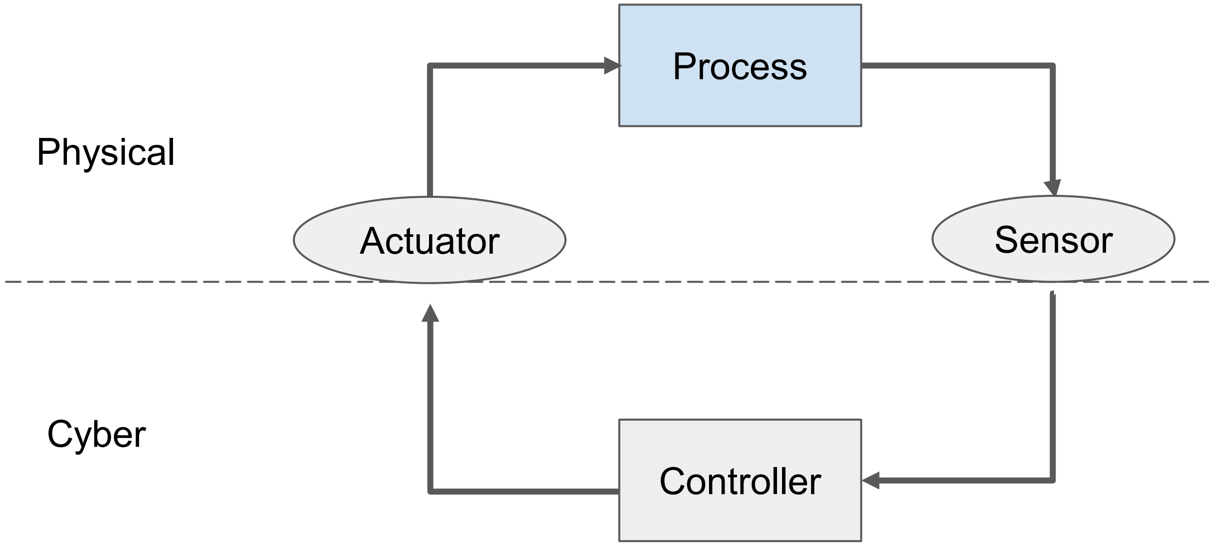
CPS Properties

- Feedback
- **Dynamic**



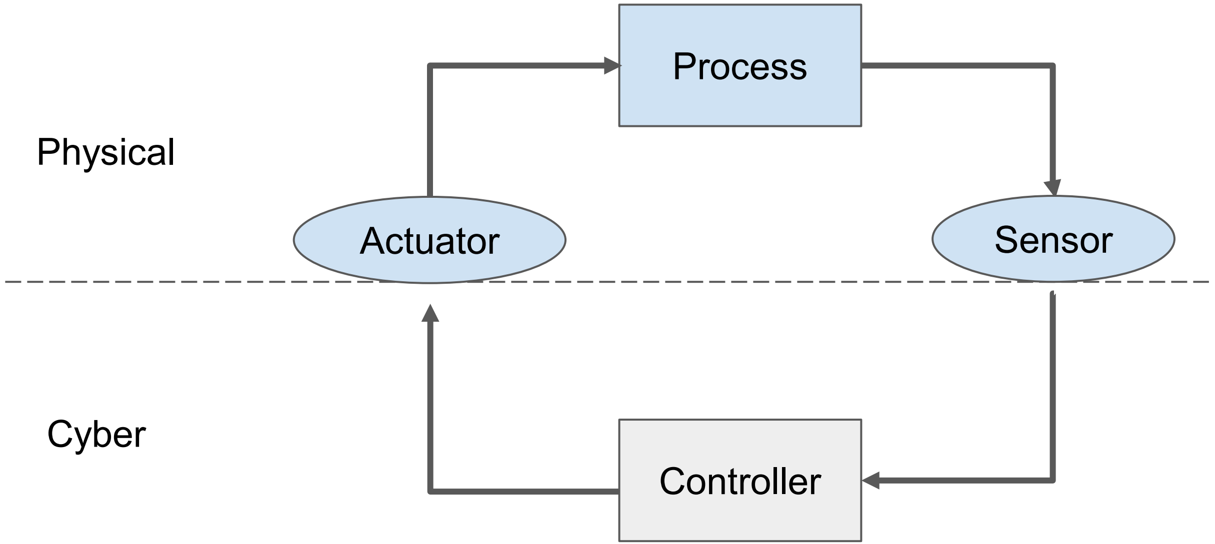
CPS Properties

- Feedback
- Dynamic
- **Observable**



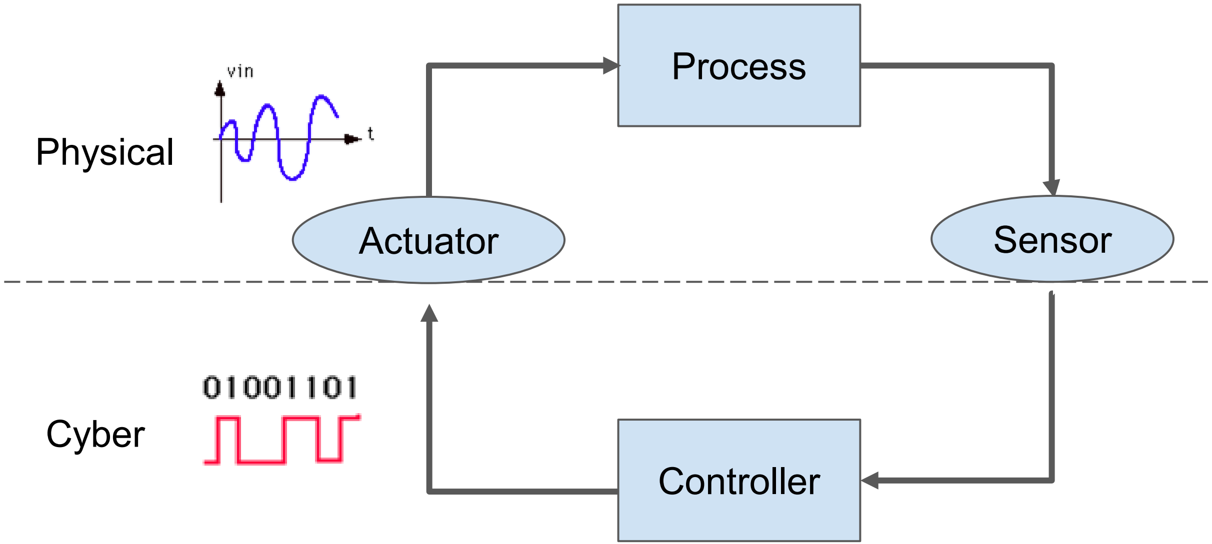
CPS Properties

- Feedback
- Dynamic
- Observable
- **Physically Bounded**



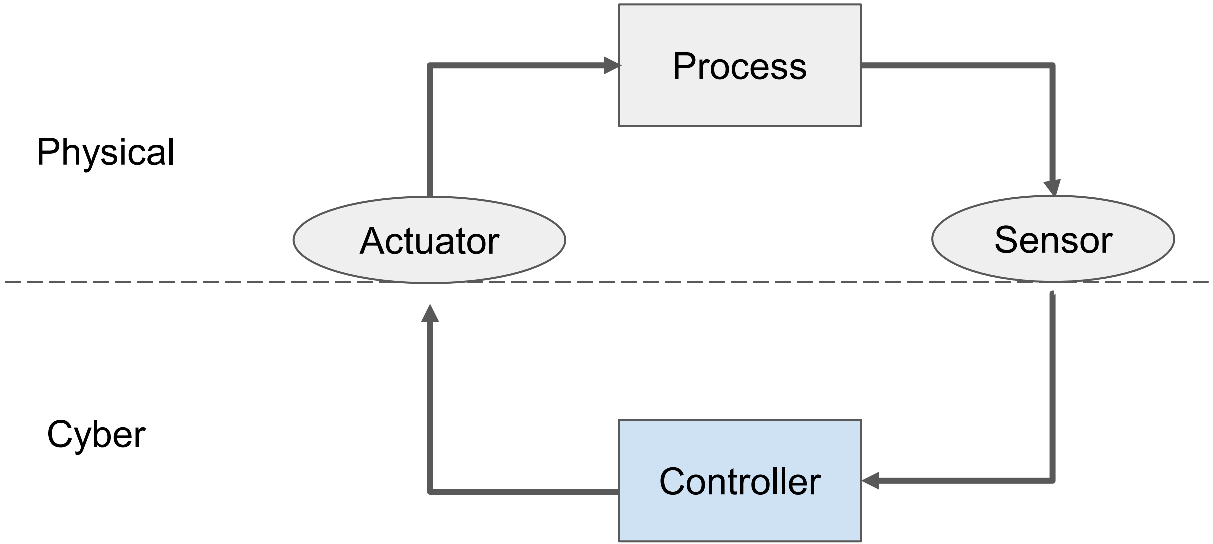
CPS Properties

- Feedback
- Dynamic
- Observable
- Physically Bounded
- **Error Tolerant**



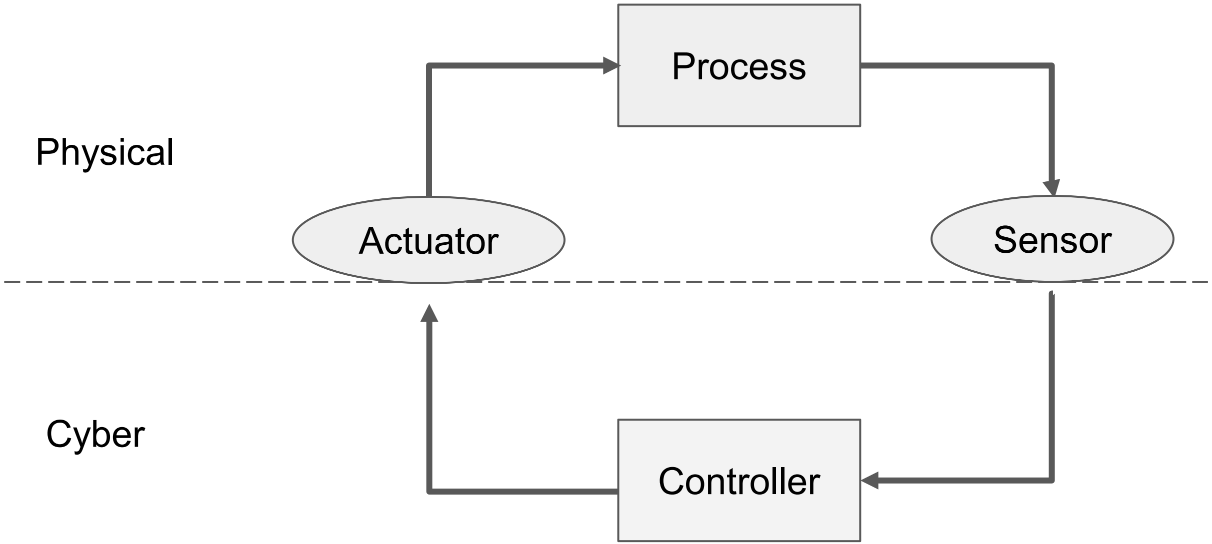
CPS Properties

- Feedback
- Dynamic
- Observable
- Physically Bounded
- Error Tolerant
- **Event-driven**



CPS Properties

- Feedback
- Dynamic
- Observable
- Physically Bounded
- Error Tolerant
- Event-driven

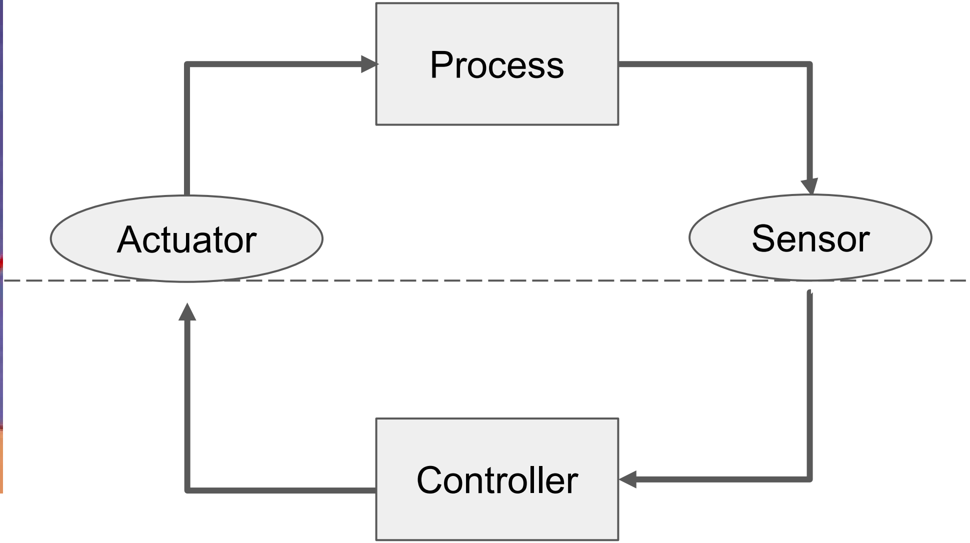


CPS Properties

- Feedback
- Dynamic
- Observable
- Physically Bounded
- Error Tolerant
- Event-driven

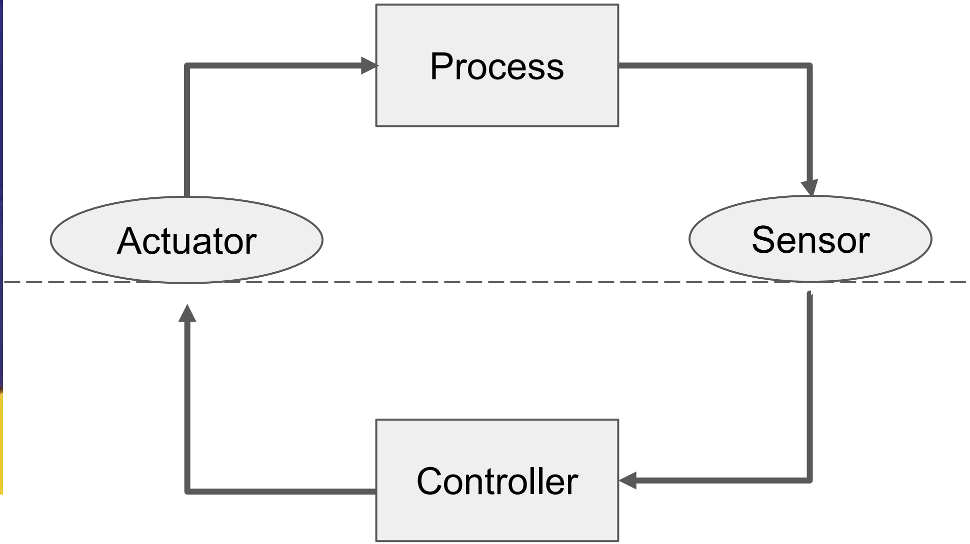
CPS Properties

- Feedback
- Dynamic
- Observable
- Physically Bounded
- Error Tolerant
- Event-driven

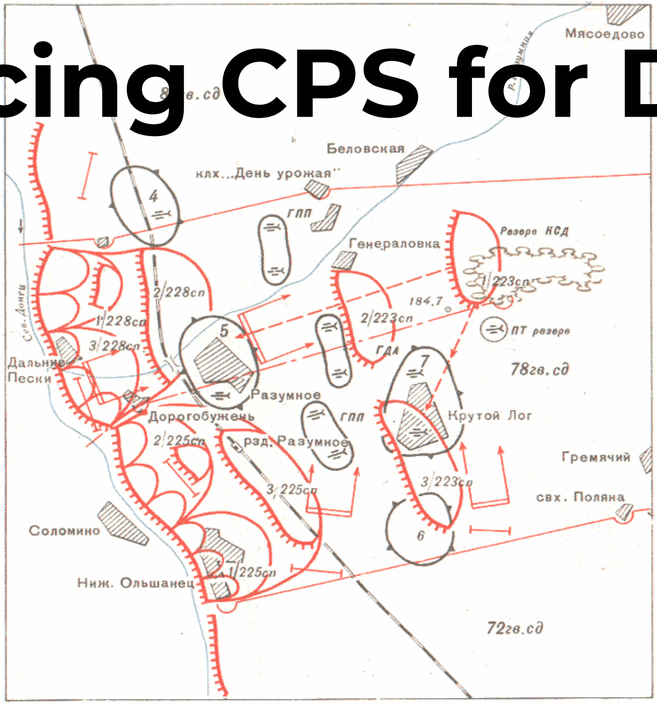


CPS Properties

- Feedback
- Dynamic
- Observable
- Physically Bounded
- Error Tolerant
- Event-driven



Embracing CPS for Defense



Defenses

Prevention

Defenses

Prevention

Detection

Defenses

Prevention

Detection

Mitigation

Prevention

Authentication

Prevention: Authentication

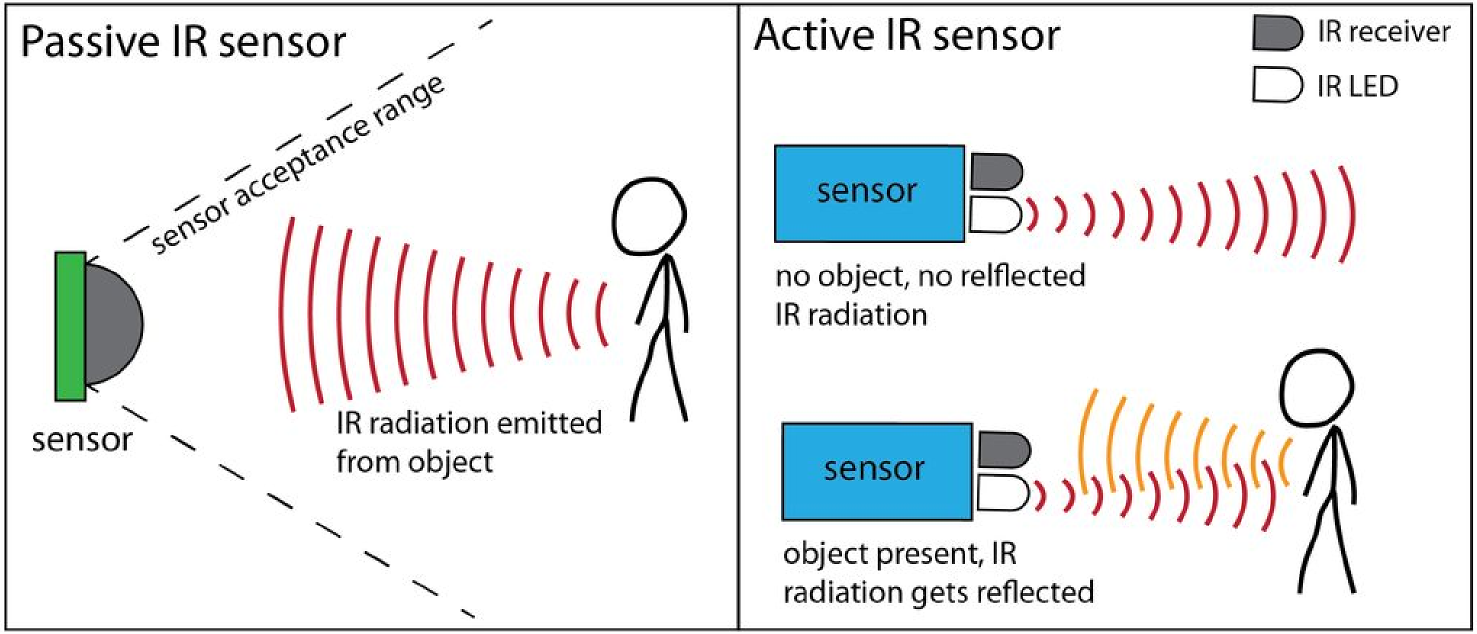
How to ensure that sensors are genuinely reporting valid information?

Prevention: Authentication

Shoukry et al. [11]

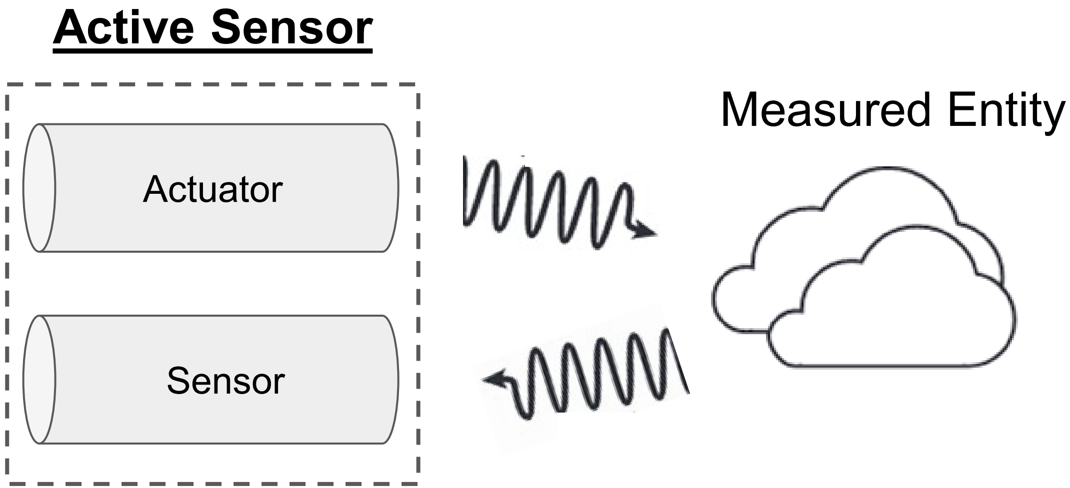
PyCRA: Physical Challenge-Response Authentication For Active Sensors Under Spoofing Attacks

Prevention: Authentication



Shoukry et al. [11]
PyCRA

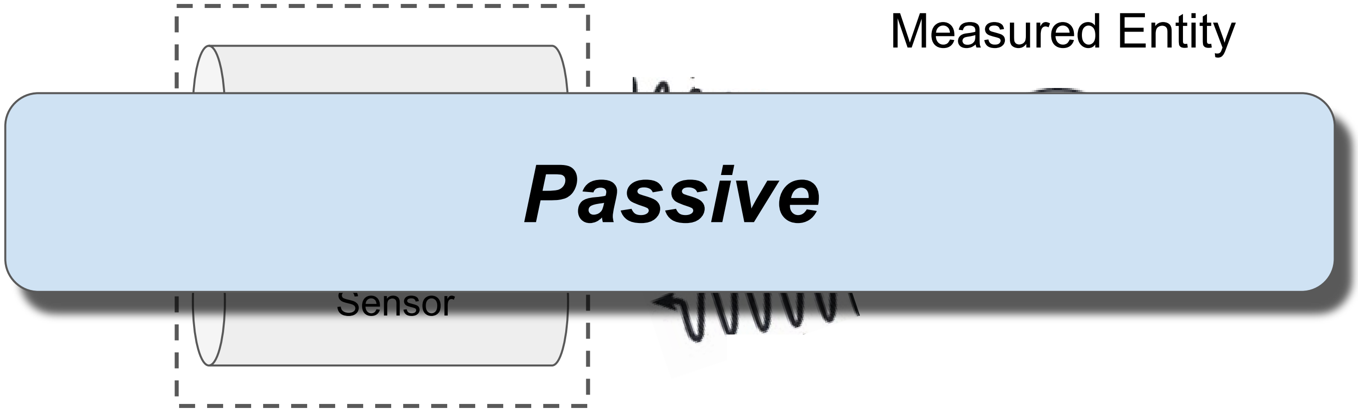
Prevention: Authentication



Shoukry et al. [11]
PyCRA

Prevention: Authentication

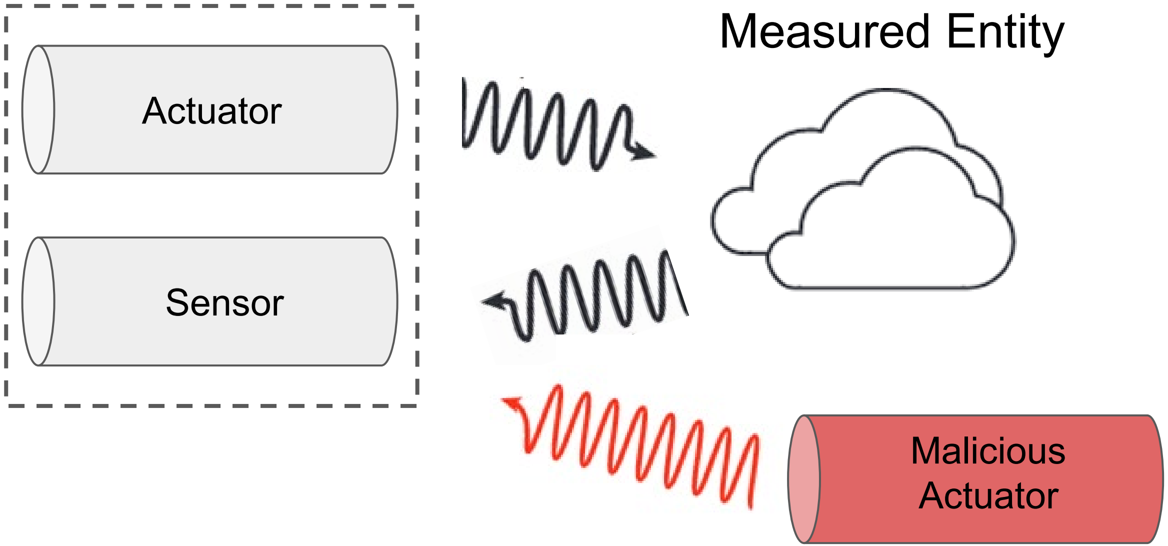
<u>**Active Sensor**</u>



Shoukry et al. [11]
PyCRA

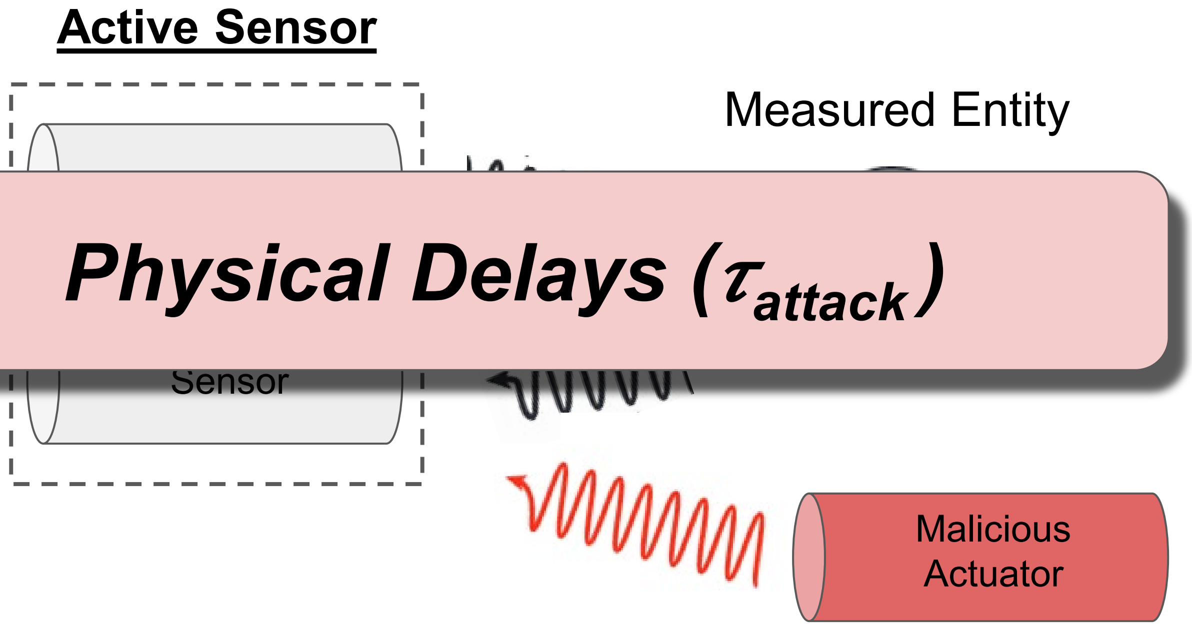
Prevention: Authentication

Active Sensor



Shoukry et al. [11]
PyCRA

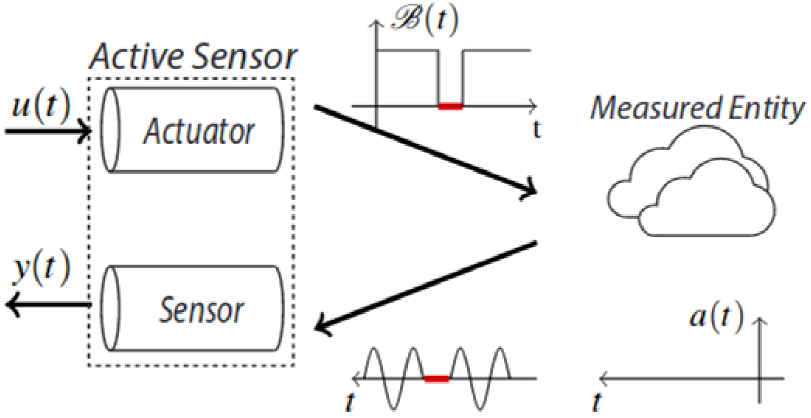
Prevention: Authentication



Physical Delays (τ_{attack})

Shoukry et al. [11]
PyCRA

Prevention: Authentication

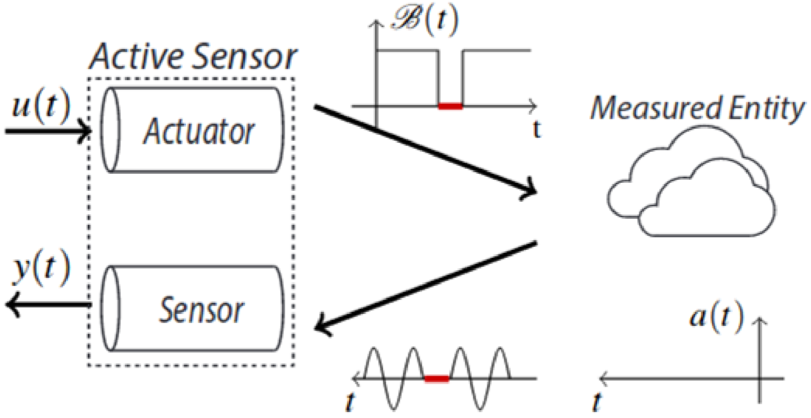


(b)

Operation with PyCRA

Shoukry et al. [11]
PyCRA

Prevention: Authentication

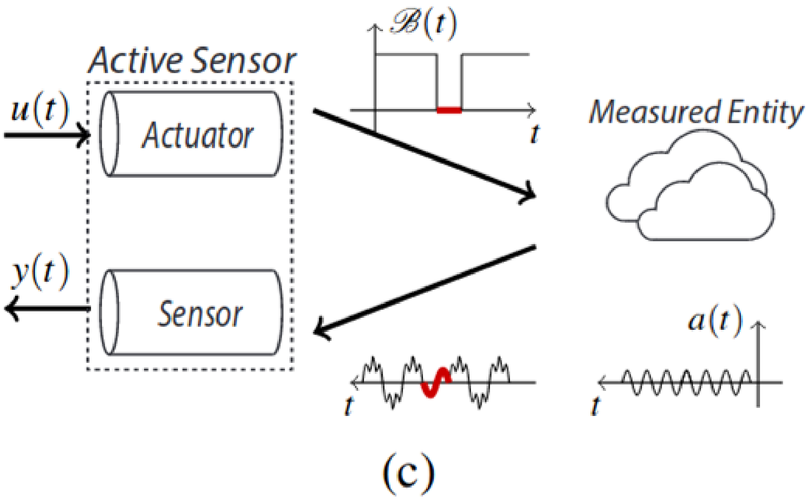


(b)

B (t) = u(t)A (t), u(t) ∊ {0,1}

Shoukry et al. [11]
PyCRA

Prevention: Authentication



Under Attack with PyCRA

Shoukry et al. [11]
PyCRA

Prevention: Authentication

<u>Take Away</u>

Fundamental properties of sensor physics can be useful for defense.

Shoukry et al. [11]
PyCRA

Prevention

- Formal Methods
  - Mitra et al. [12] - Verifying Cyber-Physical Interactions in Safety-Critical Systems
  - Bohrer et al. [13] - VeriPhy: Verified Controller Executables from Verified Cyber-Physical System Models
- Memory Safety
  - Clements et al. [14] - Protecting Bare-Metal Embedded Systems with Privilege Overlays
- Resilient Control
  - Ivanov et al. [15] - Attack-resilient Sensor Fusion for Safety Critical Cyber-Physical Systems
- System Architecture
  - Liu et al. [16] - Secure Autonomous Cyber-Physical Systems Through Verifiable Information Control Flow

Detection

Intrusion Detection

Detection

How to detect if a system is behaving maliciously?

Detection: IDS

Cheng et al. [21]

Orpheus: Enforcing Cyber-Physical Execution Semantics to Defend Against Data-Oriented Attacks

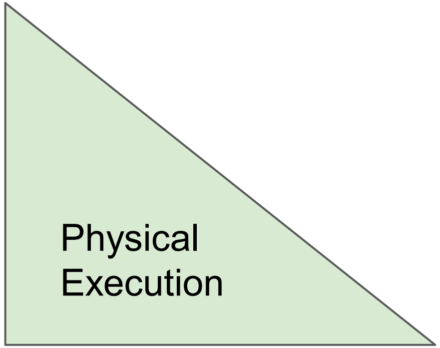
Detection: IDS

How to detect if **software** is behaving maliciously?

Cheng et al. [21]
Orpheus

Detection: IDS

How to detect if **software** is behaving maliciously?



Cheng et al. [21]
Orpheus

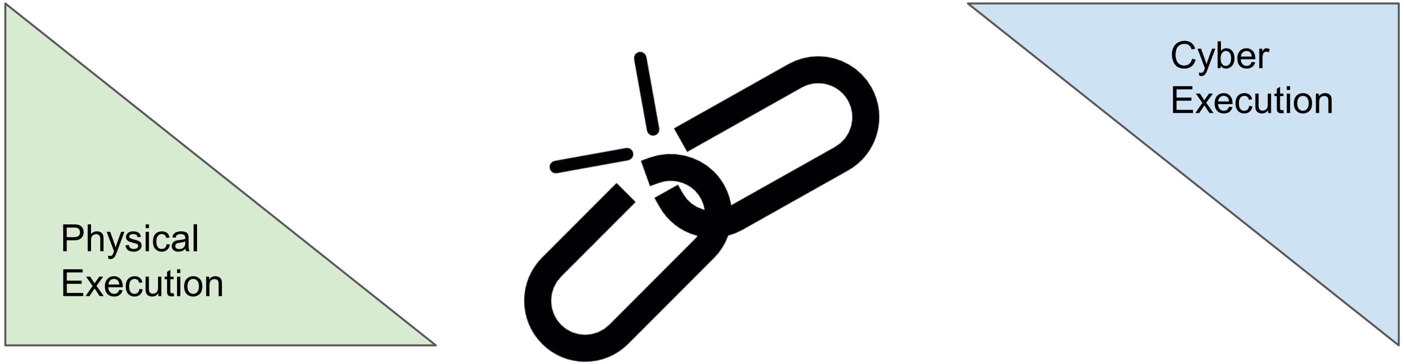
Detection: IDS

How to detect if **software** is behaving maliciously?

Cheng et al. [21]
Orpheus

Detection: IDS

How to detect if **software** is behaving maliciously?



Cheng et al. [21]
Orpheus

Detection: IDS

```
while(…){
  eventRead();
  if(Push_Event())
    push-syringe();
  else if(Pull_Event())
    pull-syringe();
  …
}
```

(a)

```
push-syringe(){
  steps = … ;
  for(i=0;i<steps;i++)
  {
    write(i2c,…);
    …
  }
}
```

(b)

<u>Attacks on control branch</u>

Execute a *valid-yet-unexpected* control flow path (eg. dispensing drugs at an unscheduled time).

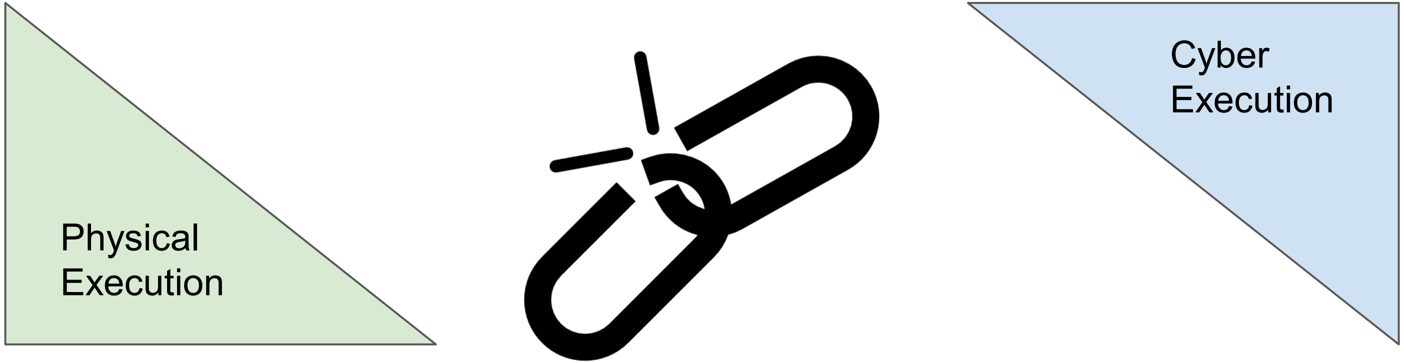
<u>Attacks on control intensity</u>

Manipulate the amount of control operations (eg. dispensing too much of a drug).

Cheng et al. [21]
Orpheus

Detection: IDS

How to detect if **software** is behaving maliciously?



Cheng et al. [21]
Orpheus

Detection: IDS

How to detect if **software** is behaving maliciously?

Cyber-Physical
Execution

Cheng et al. [21]
Orpheus

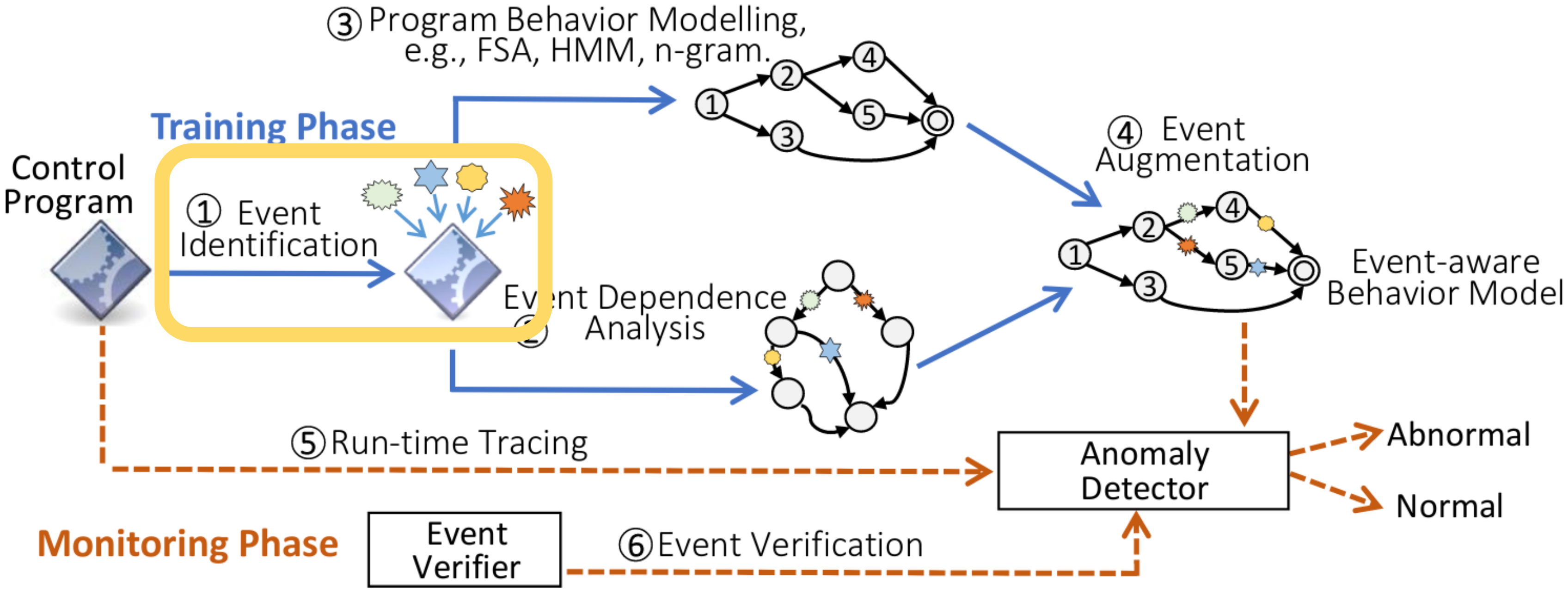
Detection: IDS

How to detect if software is behaving maliciously?

Augment **physical event constraints** on top of a program behavior model.

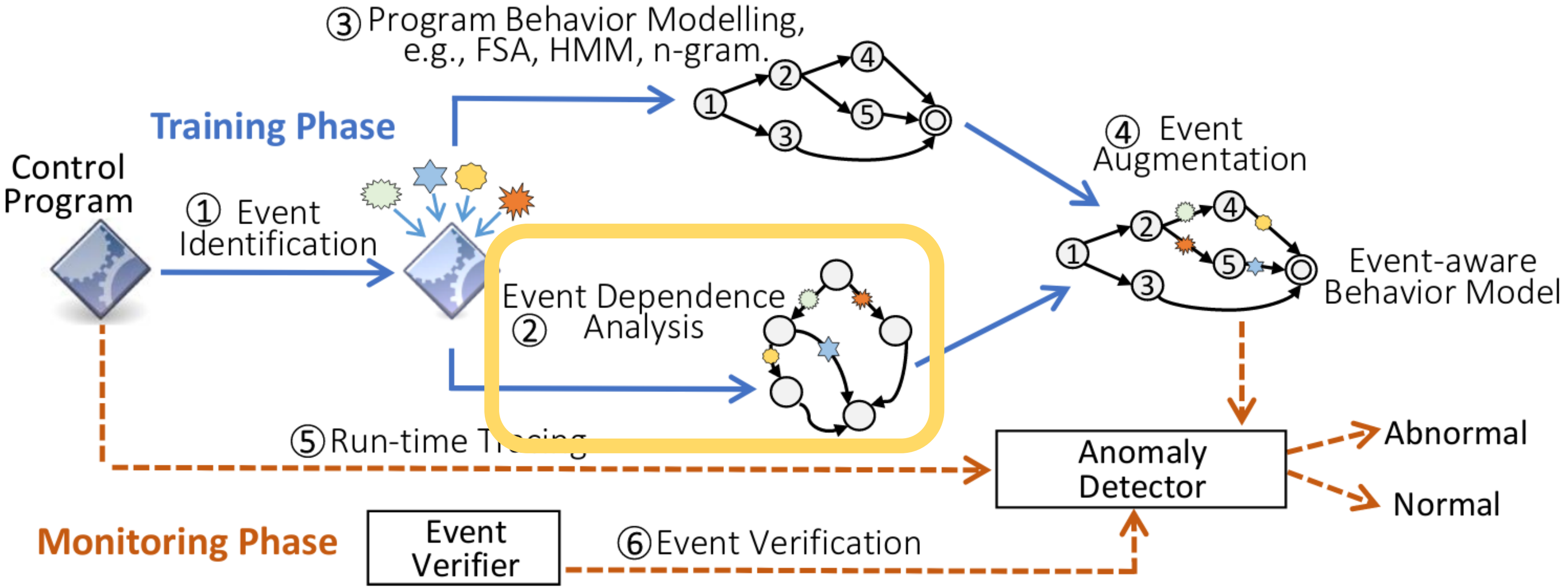
Cheng et al. [21]
Orpheus

Detection: IDS



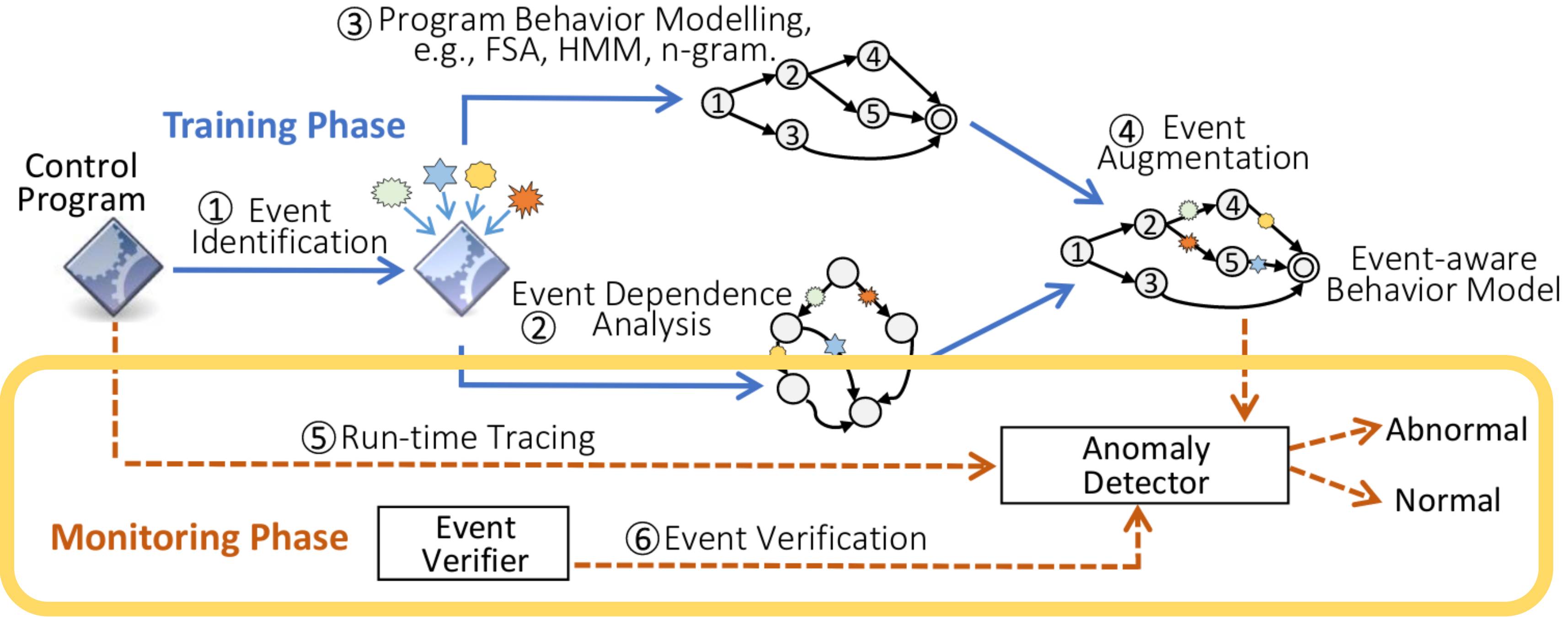
Cheng et al. [21]
Orpheus

Detection: IDS



Cheng et al. [21]
Orpheus

Detection: IDS



Cheng et al. [21]
Orpheus

Detection: IDS

<u>Take Away</u>

Fusion of program & physical event contexts can strengthen software.

Cheng et al. [21]
Orpheus

Detection

- Attestation
  - Valente and Cardenas [17] - Using Visual Challenges to Verify the Integrity of Security Cameras
  - Chen et al. [18] - Learning From Mutants: Using Code Mutation to Learn and Monitor Invariants of a Cyber-Physical System
- Vulnerability Discovery
  - Corteggiani et al. [22] - Inception: System-wide Security Testing of Real-world Embedded Systems Software
  - Pustogarov et al. [23] - Using Program Analysis to Synthesize Sensor Spoofing Attacks

Mitigation

Reconfiguration

Mitigation: Reconfiguration

How to make systems that can survive attacks?

Mitigation: Reconfiguration

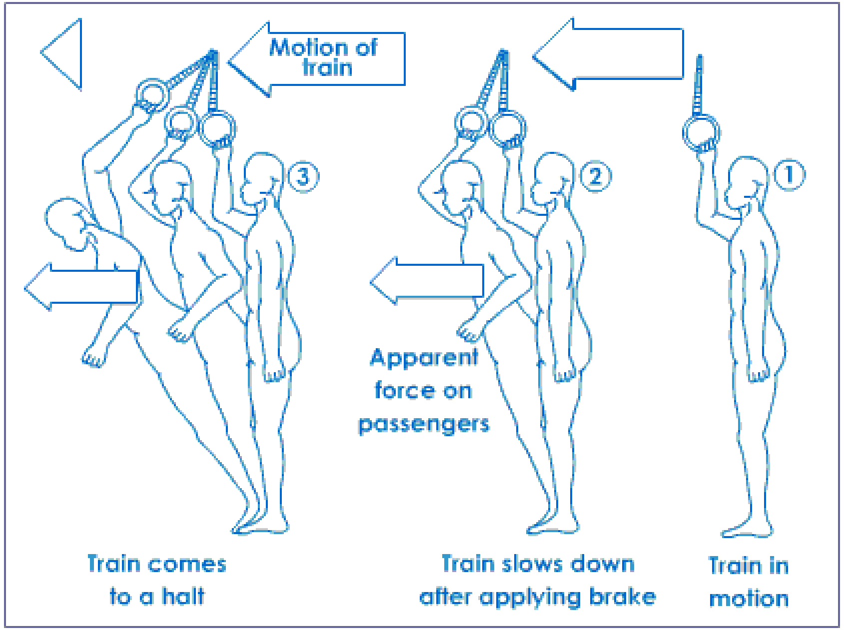
Abdi et al. [24]

Guaranteed Physical Security with Restart-Based Design for Cyber-Physical Systems

Mitigation: Reconfiguration

Abdi et al. [24]
Restart-Based Design

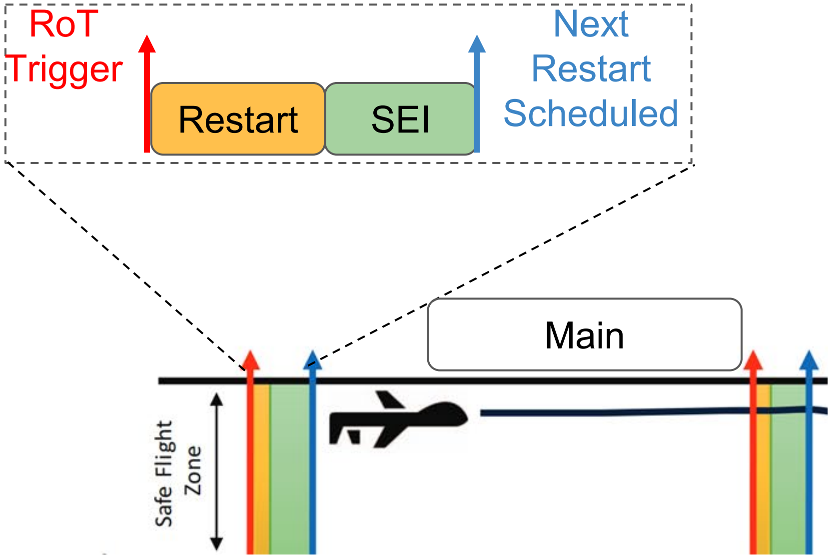
Mitigation: Reconfiguration



Inertia

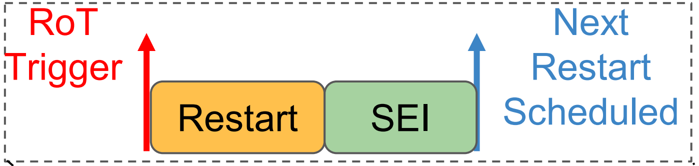
Abdi et al. [24]
Restart-Based Design

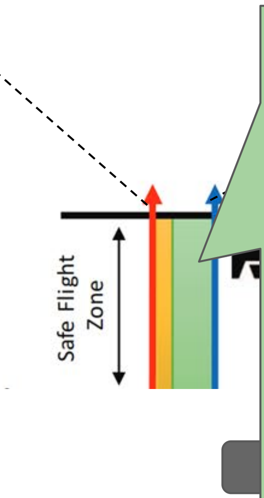
Mitigation: Reconfiguration



Abdi et al. [24]
Restart-Based Design

Mitigation: Reconfiguration



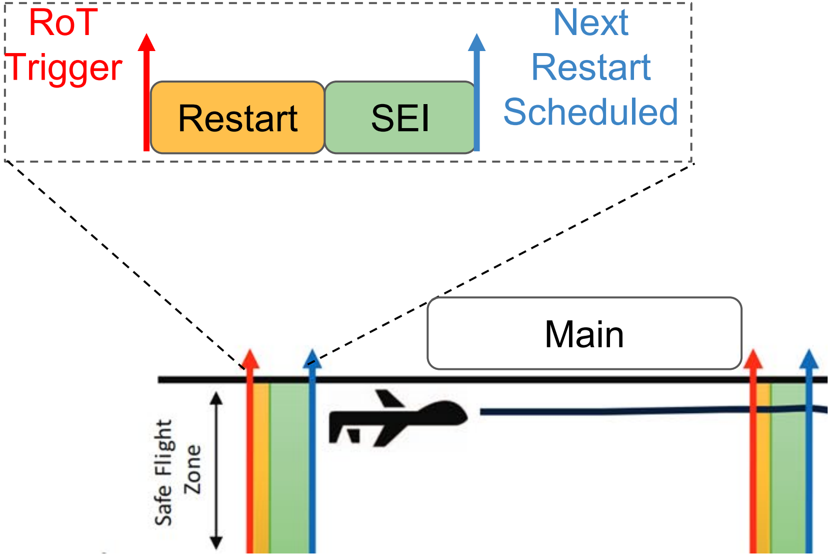


Secure Execution Interval

- `FindRestartTime`
  - Calculates restart times s.t the physical plant *cannot* reach an unsafe state until the restart takes place and, at the beginning of the next SEI, the state is still *recoverable* by the Safety Controller.
- `SafetyController`
  - Stabilizes the system if needed.

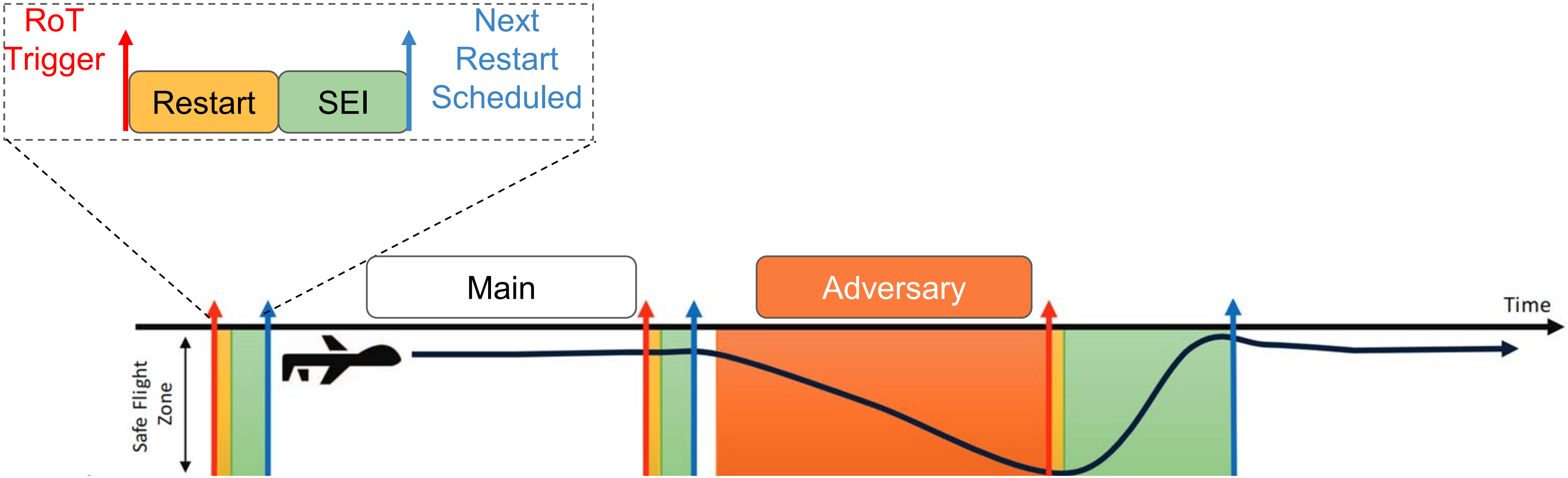
Abdi et al. [24]
Restart-Based Design

Mitigation: Reconfiguration



Abdi et al. [24]
Restart-Based Design

Mitigation: Reconfiguration



Abdi et al. [24]
Restart-Based Design

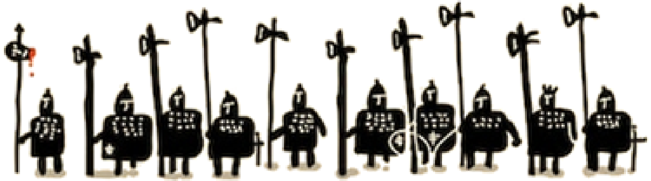
Mitigation: Reconfiguration

<u>Take Away</u>

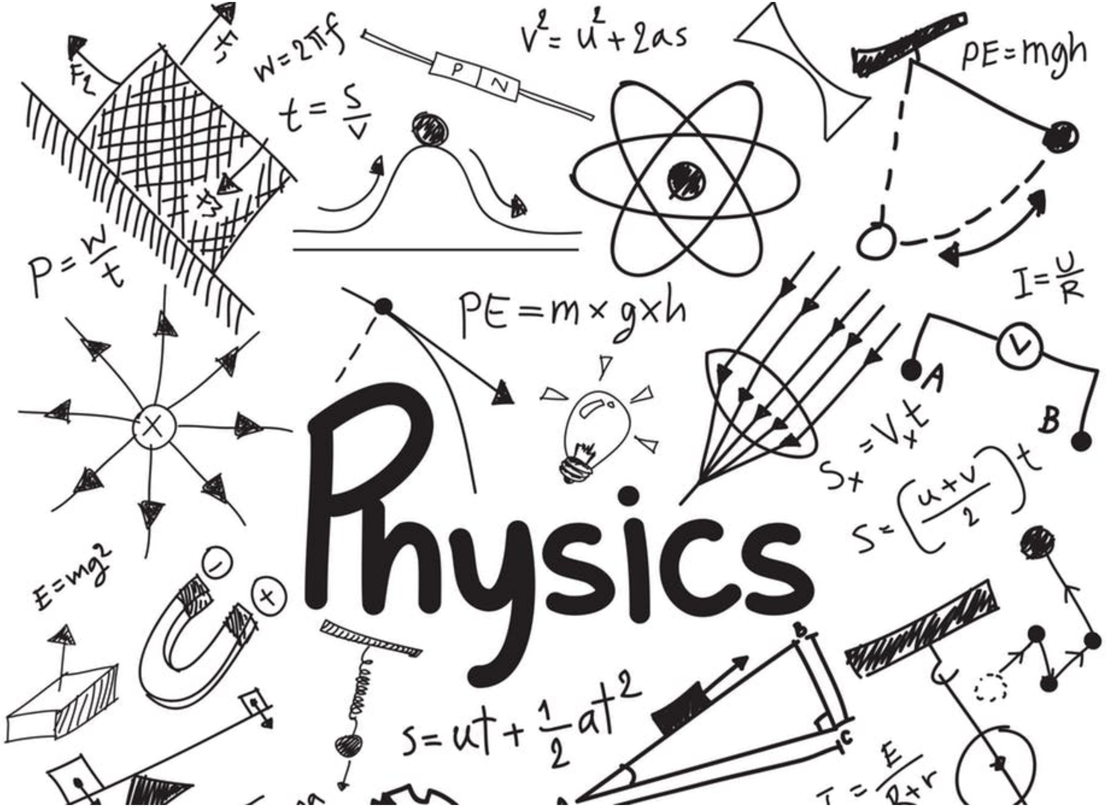
Inertia can help build attack-tolerant systems.

Abdi et al. [24]
Restart-Based Design

Defenses
Common Theme

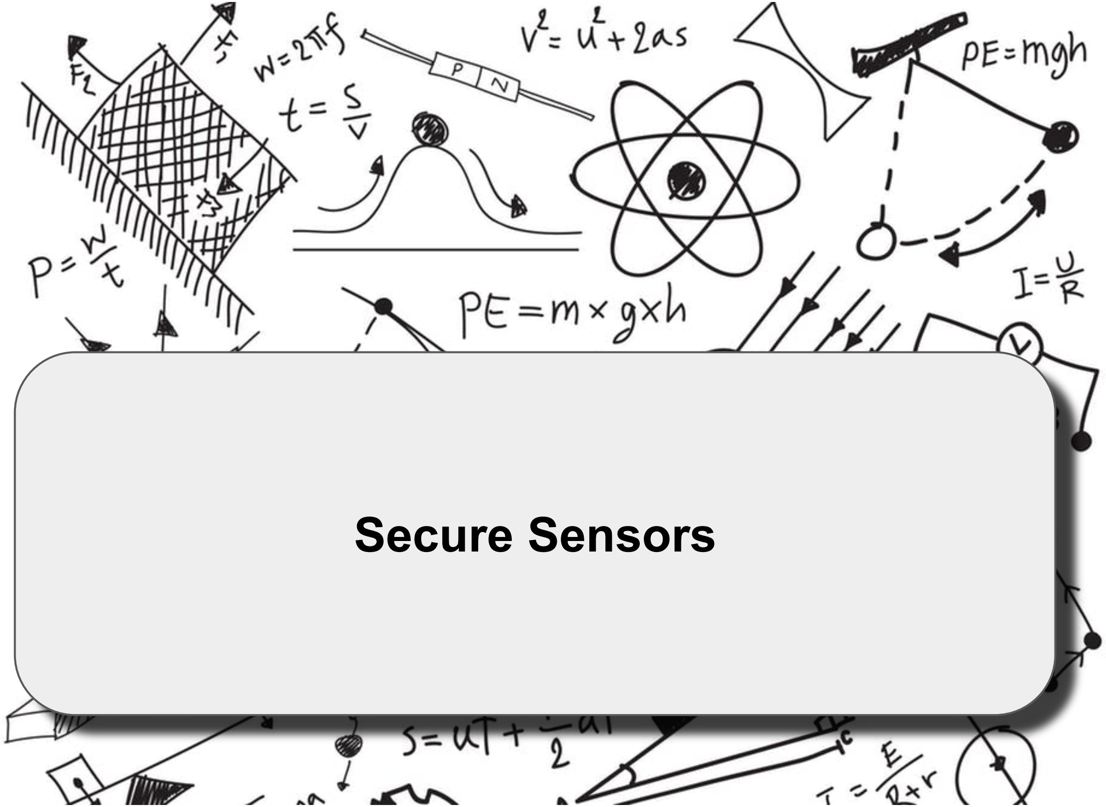


Defenses



Physics
W=2πf
P N
V²= u²+2as
PE=mgh
F1
F2
F3
t = S/V
P = W/t
PE=m×g×h
I=U/R
A
B
Sx = Vx t
S = (u+v/2) t
E=mg²
s=ut+1/2at²
I = E/R+r

Defenses



Secure Sensors

Defenses

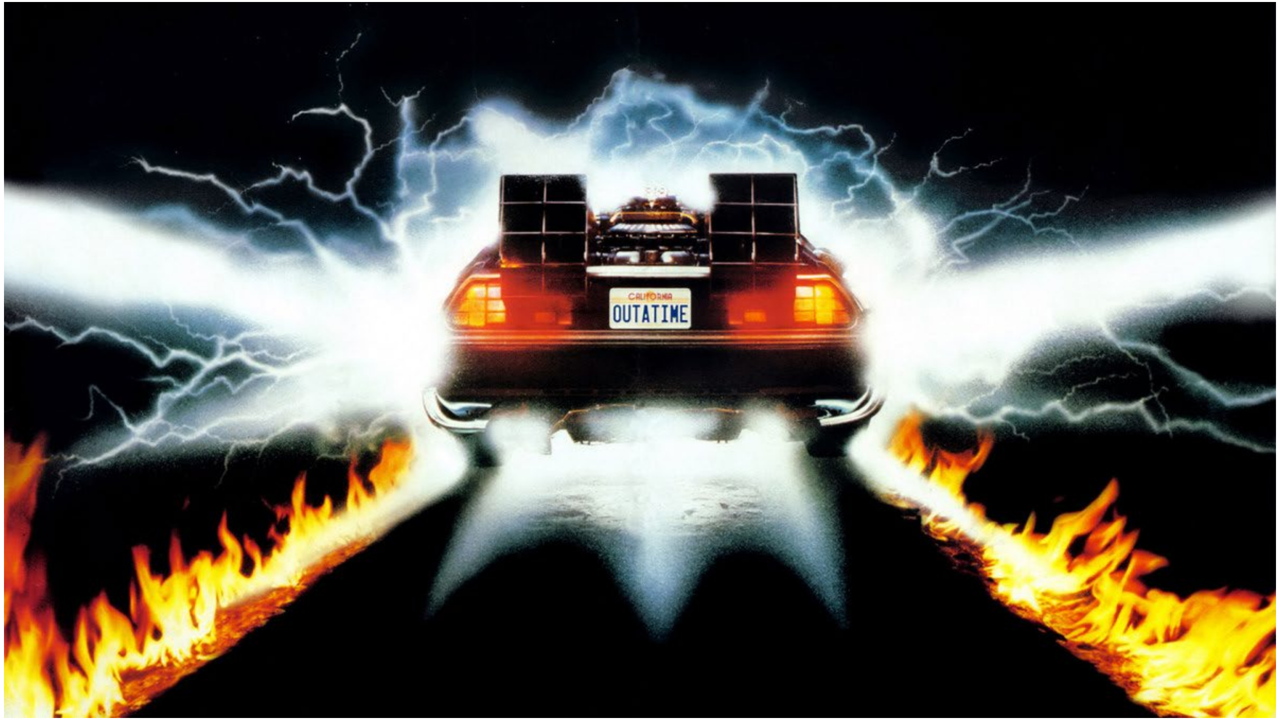
Secure Sensors

Secure Software

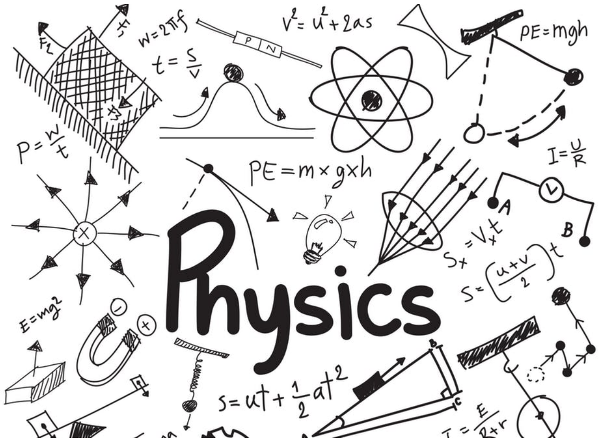
Defenses

Secure Sensors
Secure Software
Make systems more attack-tolerant

Future Work



Future Work

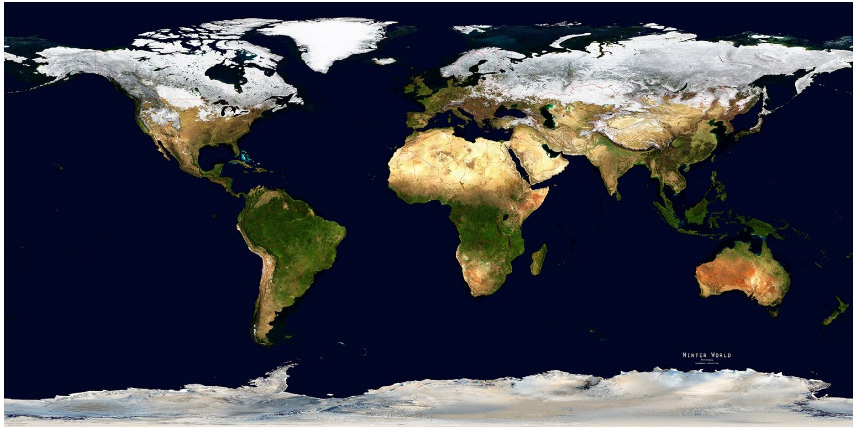


- Tailored Defenses for CPS.
- Distributed CPS

In Summary

CPS Security is Different

Today



Tomorrow

In Summary

CPS Security is Different

Questions?