Secure Autonomous Systems

CSCI 6907/3907 88

Fall 2022

Prof. Sibin Mohan

https://bit.ly/secureauto-fall22

Definitions

- Autonomy
- Cyber-Physical Systems
- Real-Time Systems

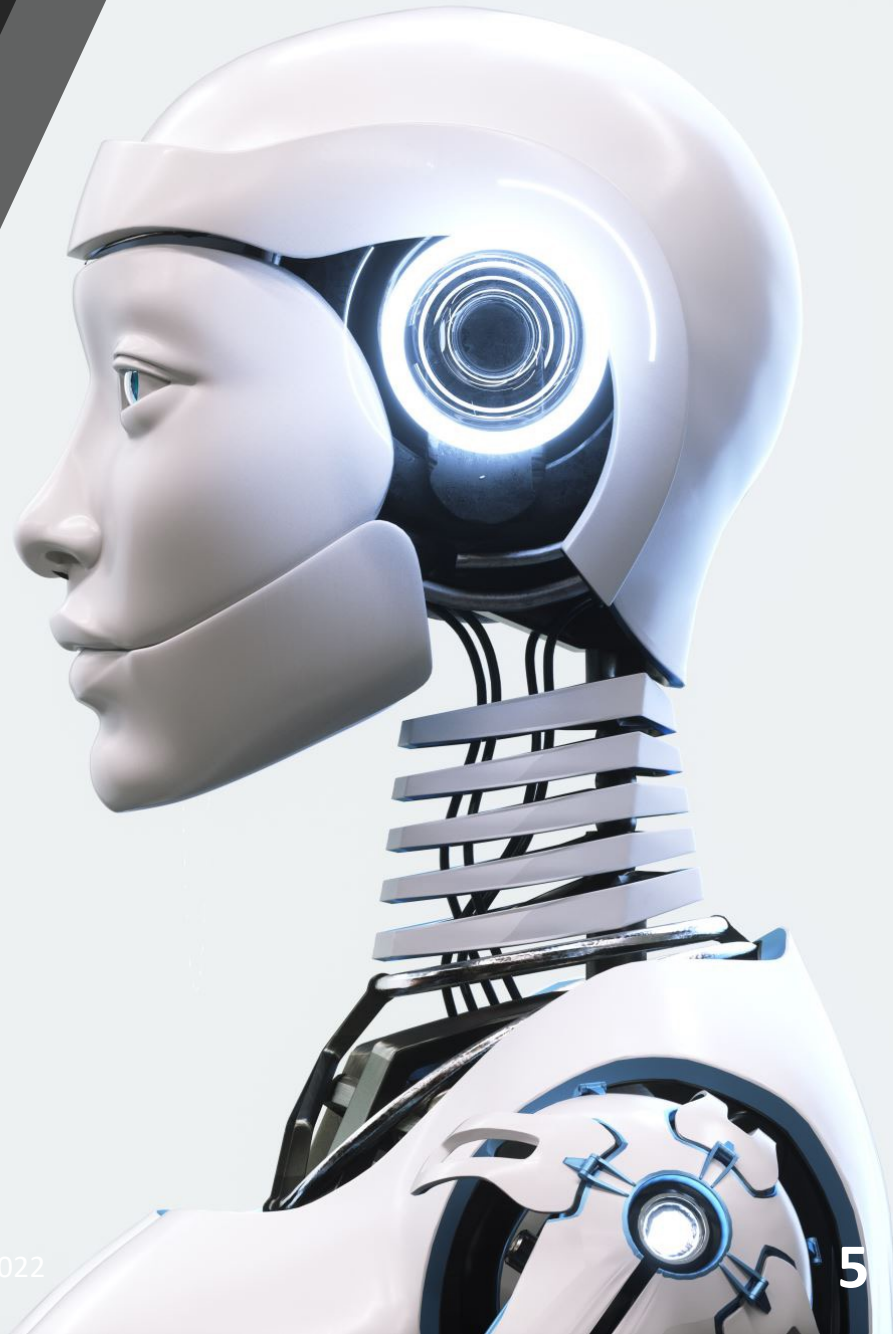
Autonomy

Aspects of Autonomy?

- Perception
- Compute
- Actuation
- Planning
- Sensing
- Motion

Autonomy | A Definition

Autonomy is the **ability to perform given tasks** based on the **system's perception without human intervention**



Detour | This Course

Secure Autonomous Systems (CPS)
CSCI 6907_88 / CSCI 3907_88
Instructor: **Prof. Sibin Mohan** [Sibin/Prof. Sibin/Prof. Mohan]
Days/Times: TUE/THUR **12:45 PM – 2:00 PM**
Location: **SMITH 115**
Contact: **Blackboard**
Office Hours: **TUE/THUR 2:00 – 3:00 PM** [**SEH 5830**]

TA

- **Mohammad Samad** [he goes by “Sam”]
- Email: **sam.ulhaque@gwu.edu**
- Office Hours: TBA

Note: contact via **Blackboard** first

Course Content

- *design* of autonomous, cyber-physical and real-time systems
- *sensing*, IMU, GPS, Radar, LIDAR, Camera, etc.
- *localization*, Simultaneous localization And Mapping (SLAM)
- Extended Kalman Filter (EKF)
- *attacks* and *defenses* related to these topics
- *privacy and ethical issues* in the design and deployment of autonomous systems

https://bit.ly/secureauto-fall22

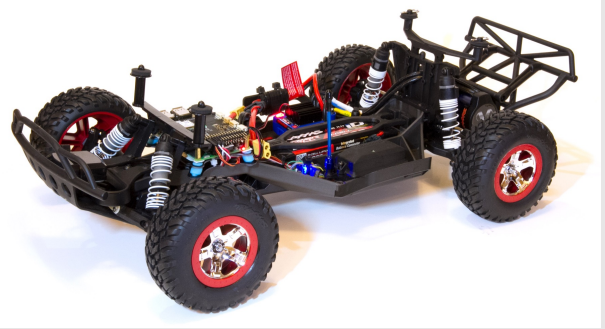
Course Content

- *design* of autonomous, cyber-physical and real-time systems
- *sensing*, IMU, GPS, Radar, LIDAR, Camera, etc.
- *localization*, Simultaneous localization And Mapping (SLAM)
- Extended Kalman Filter (EKF)
- *attacks* and *defenses* related to all of these topics
- *privacy and ethical issues* in the design and deployment of autonomous systems

Security

https://bit.ly/secureauto-fall22

Course Content | MPs



- Hands-on exercises [4]
- open-source simulation and control platforms
  - Gazebo
  - VEINS
- One of the MPs will have a leaderboard-style competition!
- Final MP will involve programming/attacking an actual **hardware rover**

https://bit.ly/secureauto-fall22

Course Content | Paper Reading+Presentation

- Exploring state-of-the-art research in the area
- Learn how to **read** and **critique** relevant papers
- Present papers in class
  - Each student presents **three papers** over the course of the term

https://bit.ly/secureauto-fall22

Grading Critera

In-class participation	**5%**
MP1 [V2X/VEINS]	**10%**
MP2 [UAV Security/Gazebo]	**10%**
MP3 [V2X Attack/Leaderboard/VEINS]	**20%**
MP4 [Hardware Rover]	**25%**
Paper Reading/Critique	**30%**

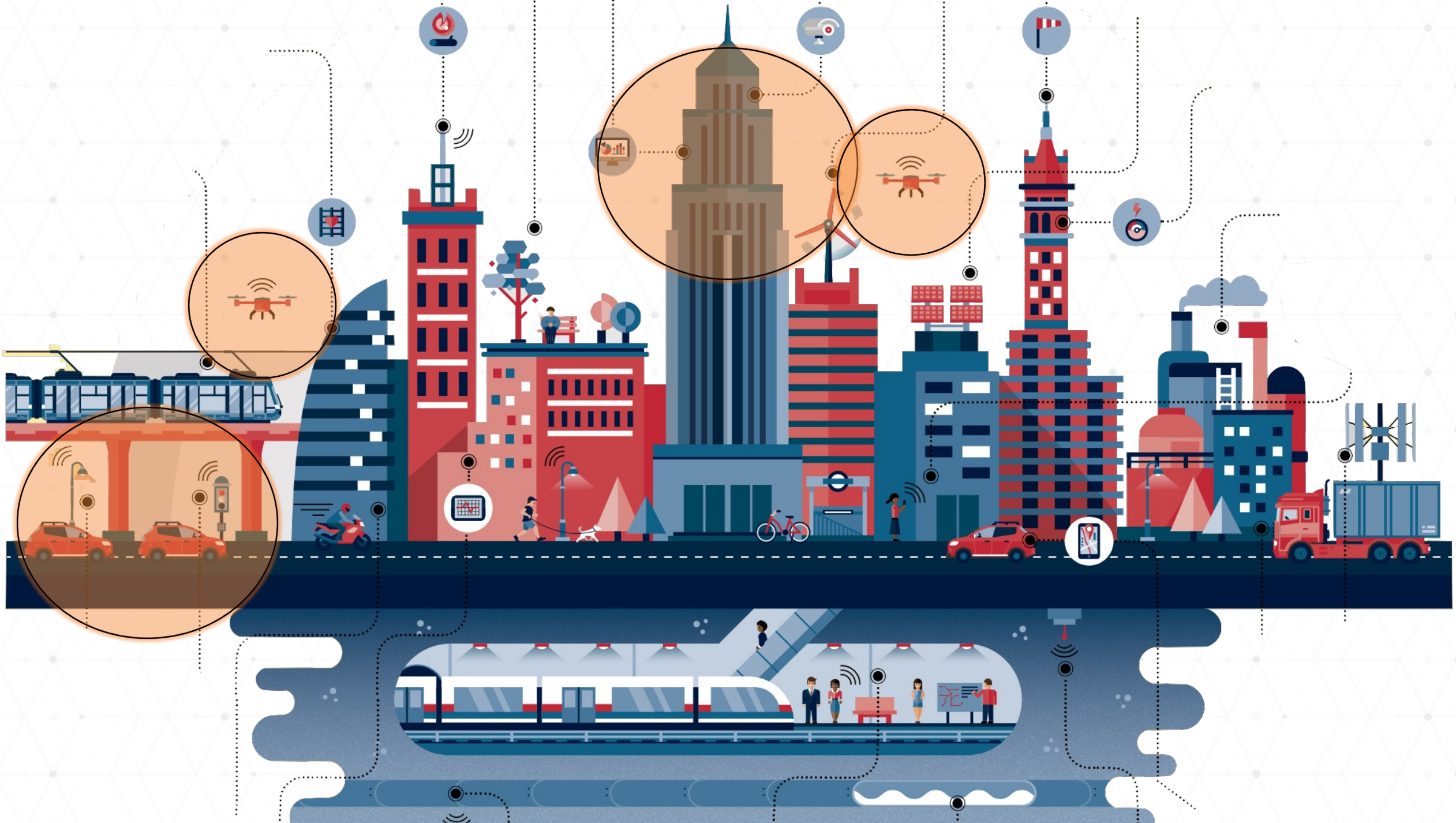
Grades

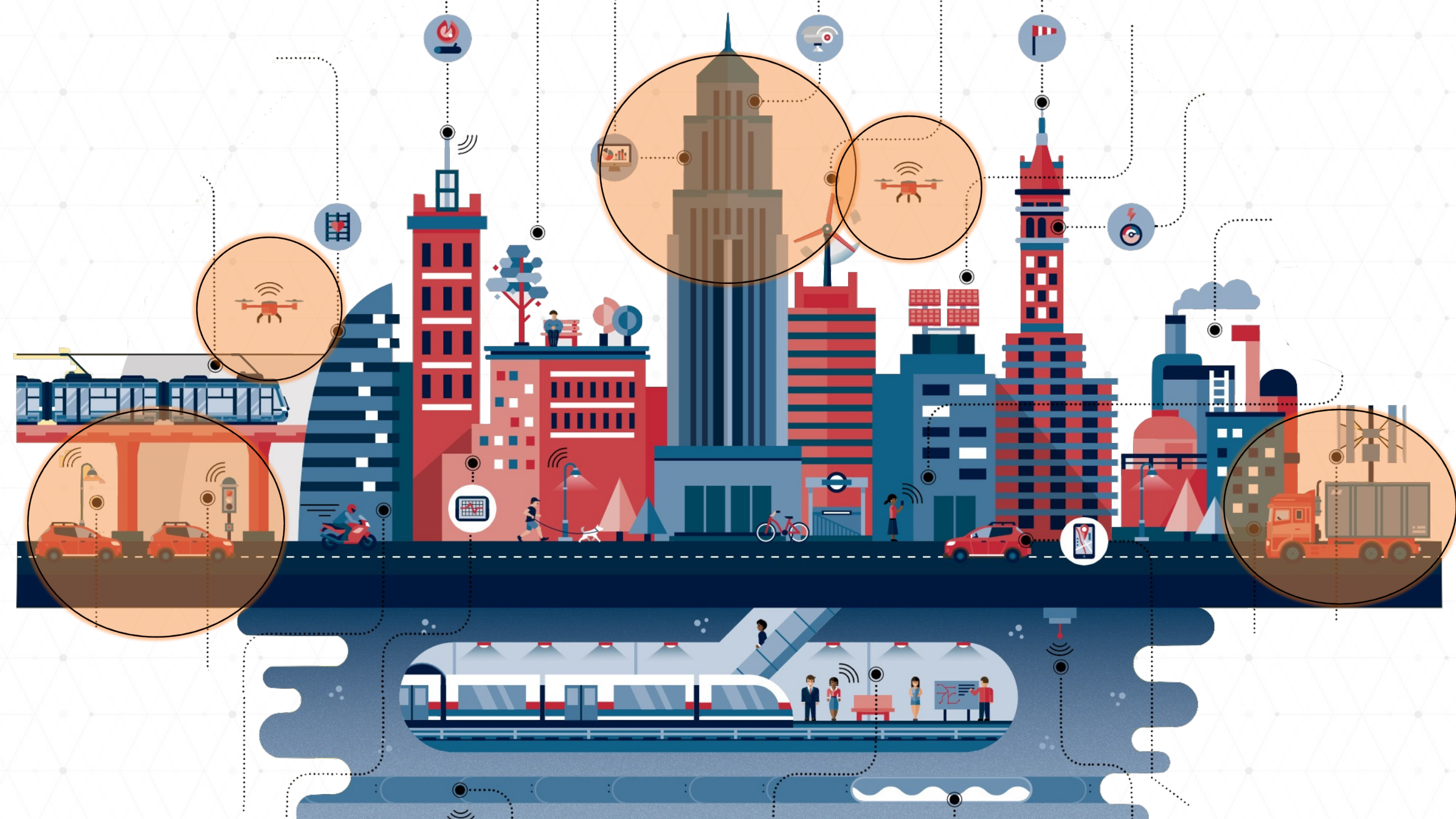
Conversion from numerical to letter grades

6907	3907
95 – 100 = A	90 – 100 = A
90 – 94 = A-	86 – 90 = A-
87 – 89 = B+	82 – 84 = B+
83 – 86 = B	78 – 81 = B
80 – 82 = B-	75 – 77 = B-
77 – 79 = C+	72 – 74 = C+
73 – 76 = C	68 – 71 = C
70 – 72 = C-	65 – 67 = C-
67 – 69 = D+	62 – 64 = D+
60 – 66 = D	55 – 61 = D
50 – 59 = D-	45 – 54 = D-
< 50 = F	< 45 = F

End of Detour

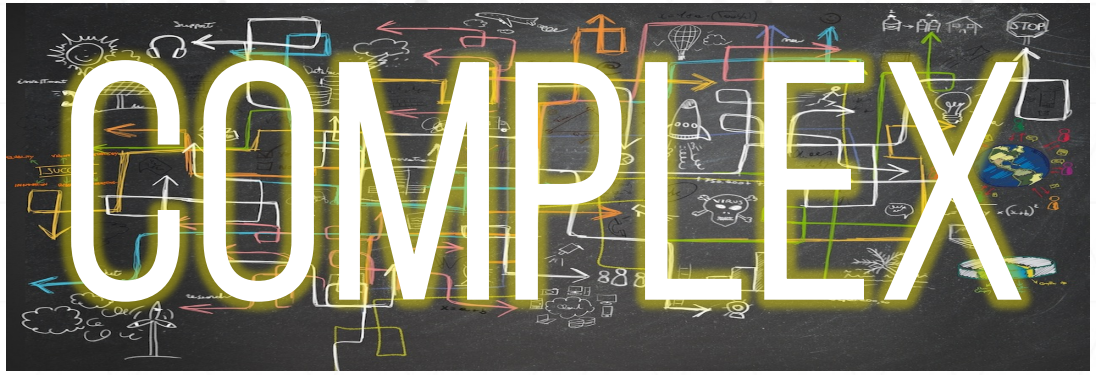
- Back to definitions/concepts
  - Cyber-Physical Systems
  - Real-Time Systems
  - Security/Safety/Resiliency



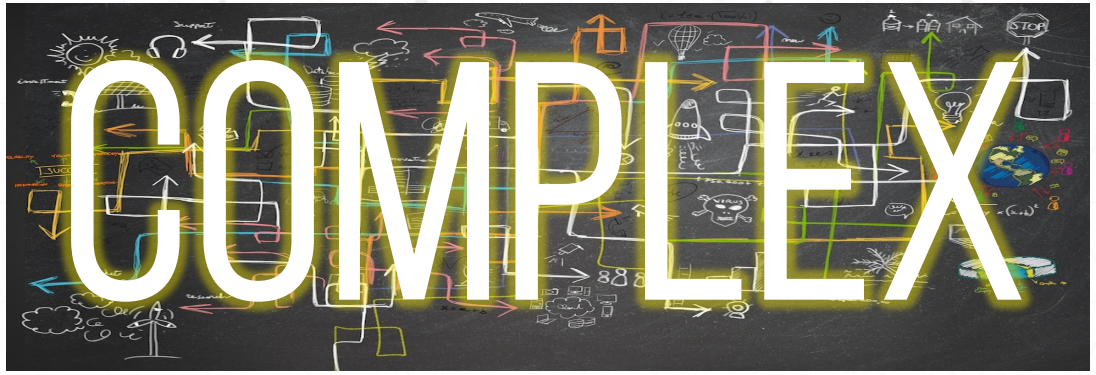


LARGE

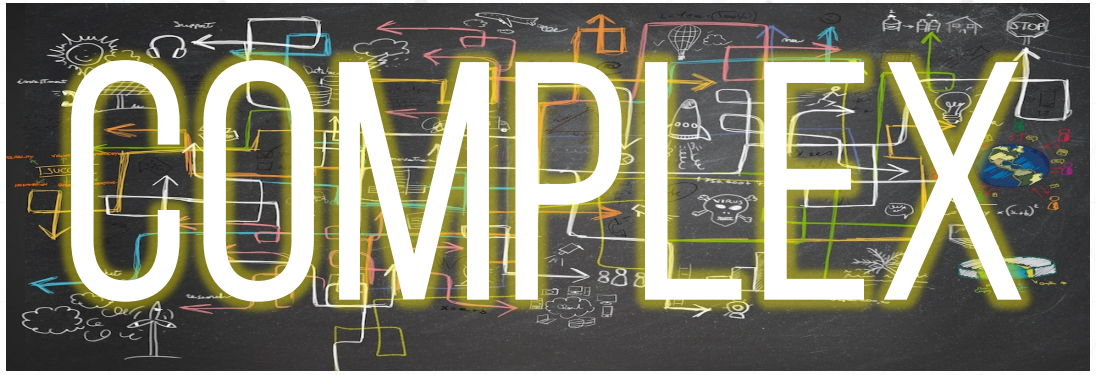
LARGE



LARGE



LARGE



SYSTEMS

LARGE

COMPLEX

MODELING, ANALYSIS, SECURITY ARE **HARD PROBLEMS**

INTERCONNECTED

SYSTEMS

CYBER-PHYSICAL SYSTEMS

CYBER-PHYSICAL SYSTEMS

CYBER

```
                TS      TEMPR60         # FOR GENERALIZED RETURN TO OTHER BANKS.
P40A/P          TC      BANKCALL        # SUBROUTINE TO CHECK PGNCS CONTROL
                CADR    G+N,AUTO# AND AUTO STABILIZATION MODES
                CCS     A               # +0 INDICATES IN PGNCS, IN AUTO
                TCF     TURNITON        # + INDICATES NOT IN PGNCS AND/OR AUTO
                CAF     APSFLBIT        # ARE WE ON THE DESCENT STAGE?
                MASK    FLGWRD10
                CCS     A
                TCF     GOBACK          # RETURN
                CAF     BIT5            # YES, CHECK FOR AUTO-THROTTLE MODE
                EXTEND
                RAND    CHAN30
                EXTEND
                BZF     GOBACK          # IN AUTO-THROTTLE MODE -- RETURN
TURNITON        CAF     P40A/PMD        # DISPLAYS V50N25 R1=203 PLEASE PERFORM
                TC      BANKCALL        # CHECKLIST 203 TURN ON PGNCS ETC.
                CADR    GOPERF1
                TCF     GOTOP00H        # V34E TERMINATE
                TCF     P40A/P          # RECYCLE
GOBACK          CA      TEMPR60
                TC      BANKJUMP        # GOODBYE.  COME AGAIN SOON.
```

software, control algorithms, code

networking, communication

ECUs, microcontrollers, PLCs

CYBER-PHYSICAL SYSTEMS

CYBER

PHYSICAL

```
                TS      TEMPR60         # FOR GENERALIZED RETURN TO OTHER BANKS.
P40A/P          TC      BANKCALL        # SUBROUTINE TO CHECK PGNCS CONTROL
                CADR    G+N,AUTO# AND AUTO STABILIZATION MODES
                CCS     A               # +0 INDICATES IN PGNCS, IN AUTO
                TCF     TURNITON        # + INDICATES NOT IN PGNCS AND/OR AUTO
                CAF     APSFLBIT        # ARE WE ON THE DESCENT STAGE?
                MASK    FLGWRD10
                CCS     A
                TCF     GOBACK          # RETURN
                CAF     BIT5            # YES, CHECK FOR AUTO-THROTTLE MODE
                EXTEND
                RAND    CHAN30
                EXTEND
                BZF     GOBACK          # IN AUTO-THROTTLE MODE -- RETURN
TURNITON        CAF     P40A/PMD        # DISPLAYS V50N25 R1=203 PLEASE PERFORM
                TC      BANKCALL        # CHECKLIST 203 TURN ON PGNCS ETC.
                CADR    GOPERF1
                TCF     GOTOP00H        # V34E TERMINATE
                TCF     P40A/P          # RECYCLE
GOBACK          CA      TEMPR60
                TC      BANKJUMP        # GOODBYE.  COME AGAIN SOON
```

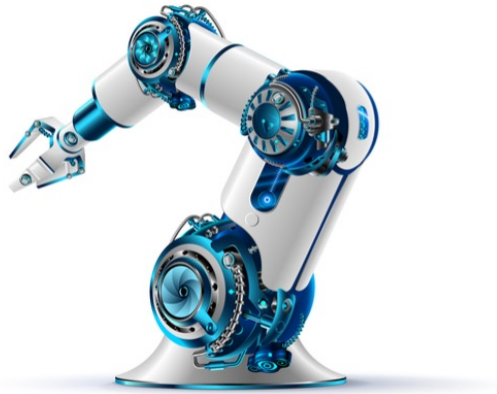
software, control algorithms, code

networking, communication

ECUs, microcontrollers, PLCs

sensors

actuators, motors



”plants”

CYBER-PHYSICAL SYSTEMS

CYBER

software, control algorithms, code

networking, communication

ECUs, microcontrollers, PLCs

PHYSICAL

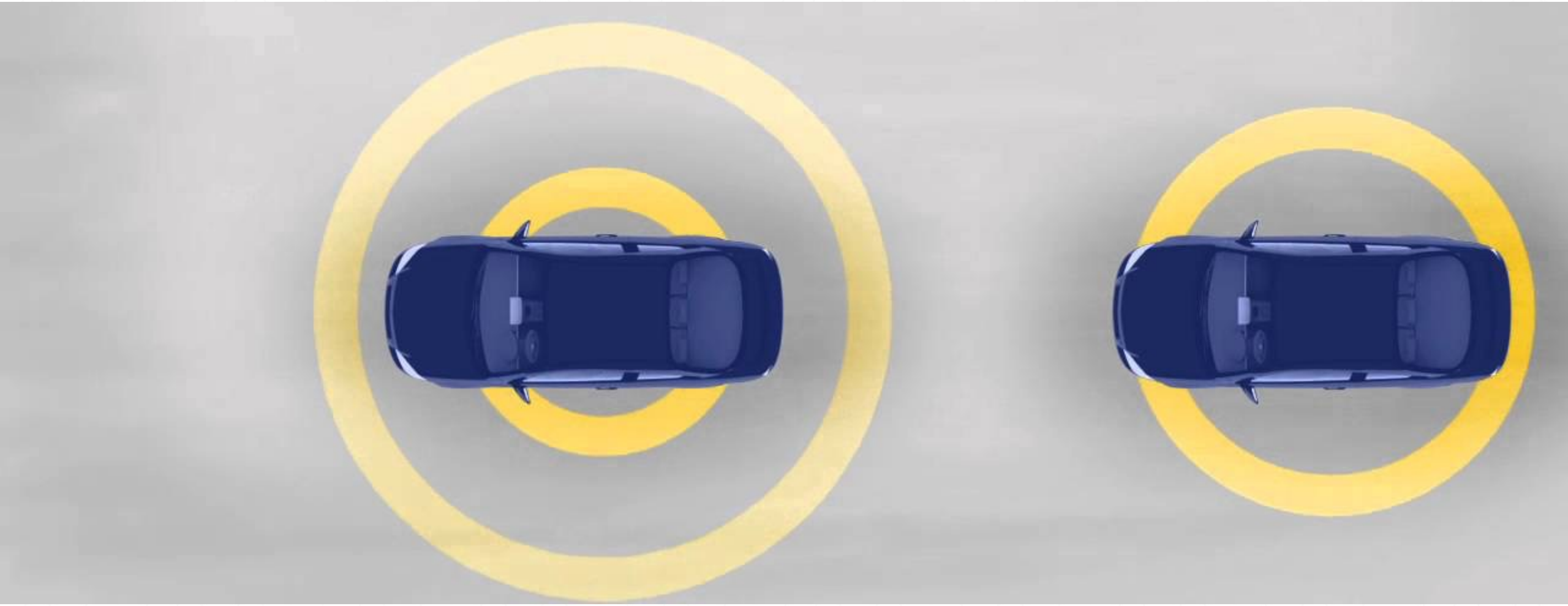
sensors

actuators, motors

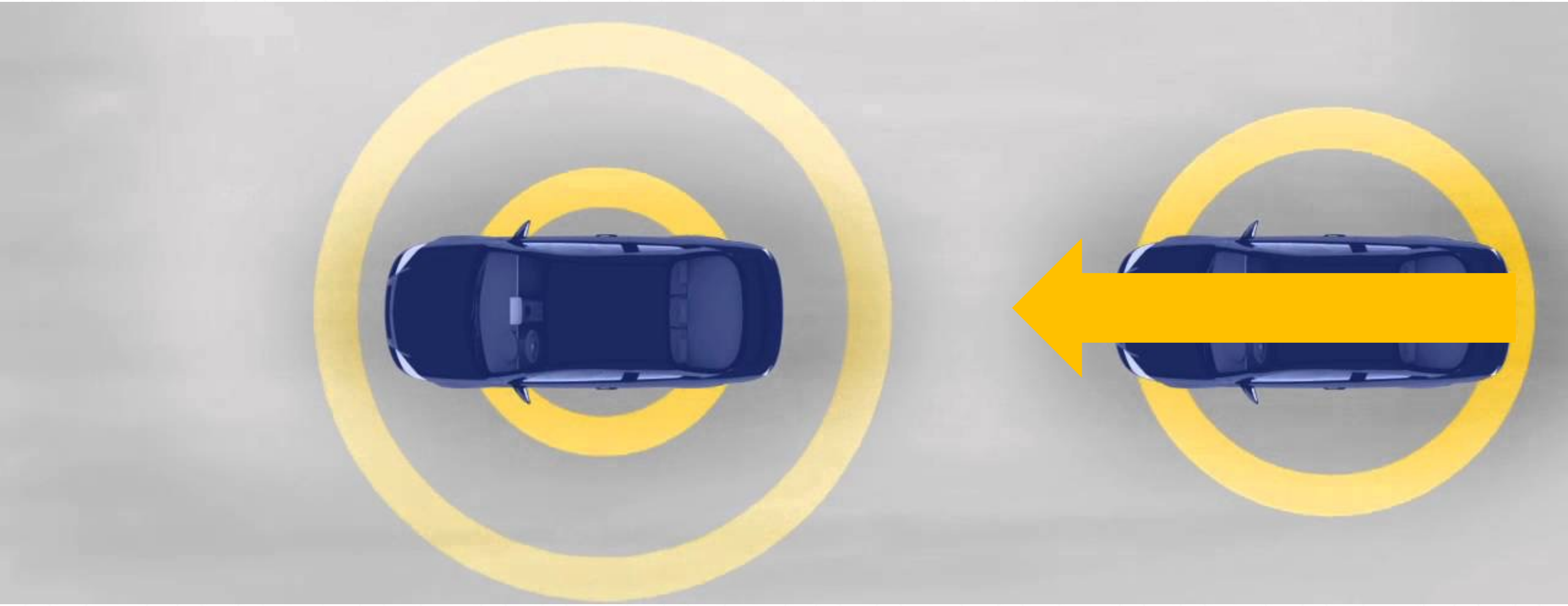
”plants”


SENSING AND ACTUATION IS EVERYWHERE

SENSING/ACTUATION IN THE REAL WORLD

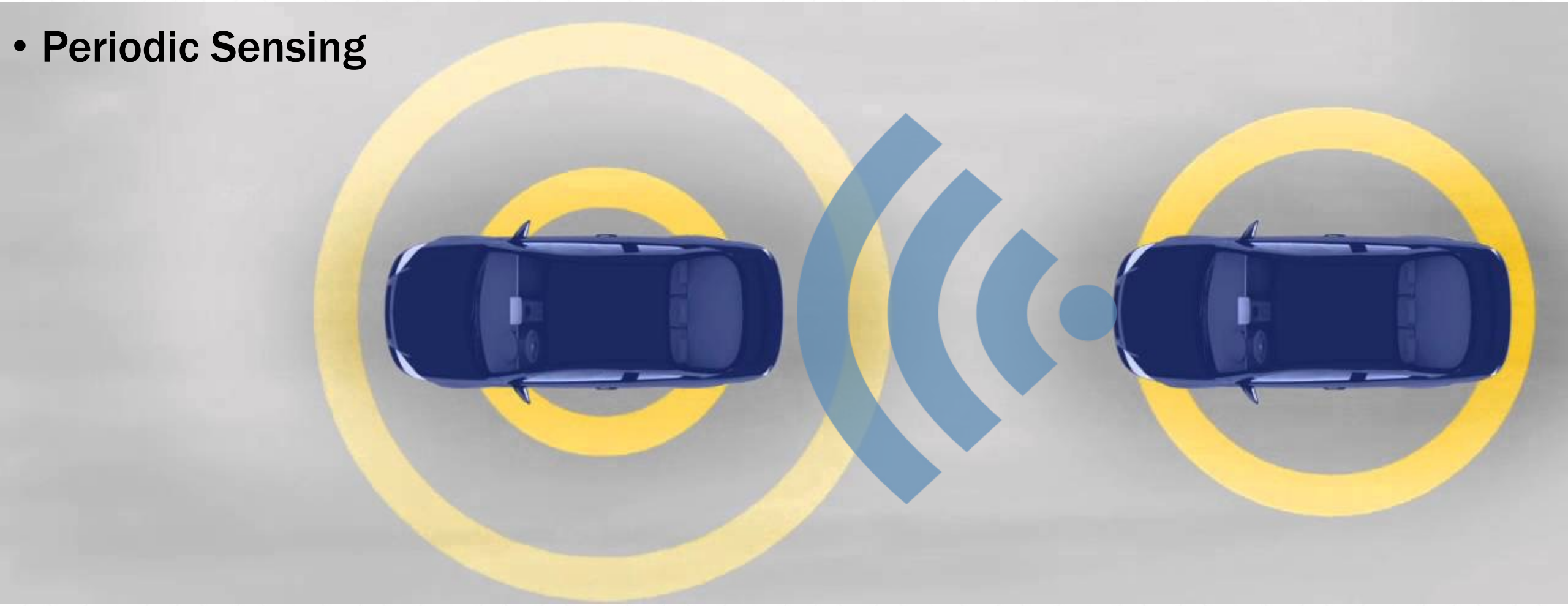


SENSING/ACTUATION IN THE REAL WORLD



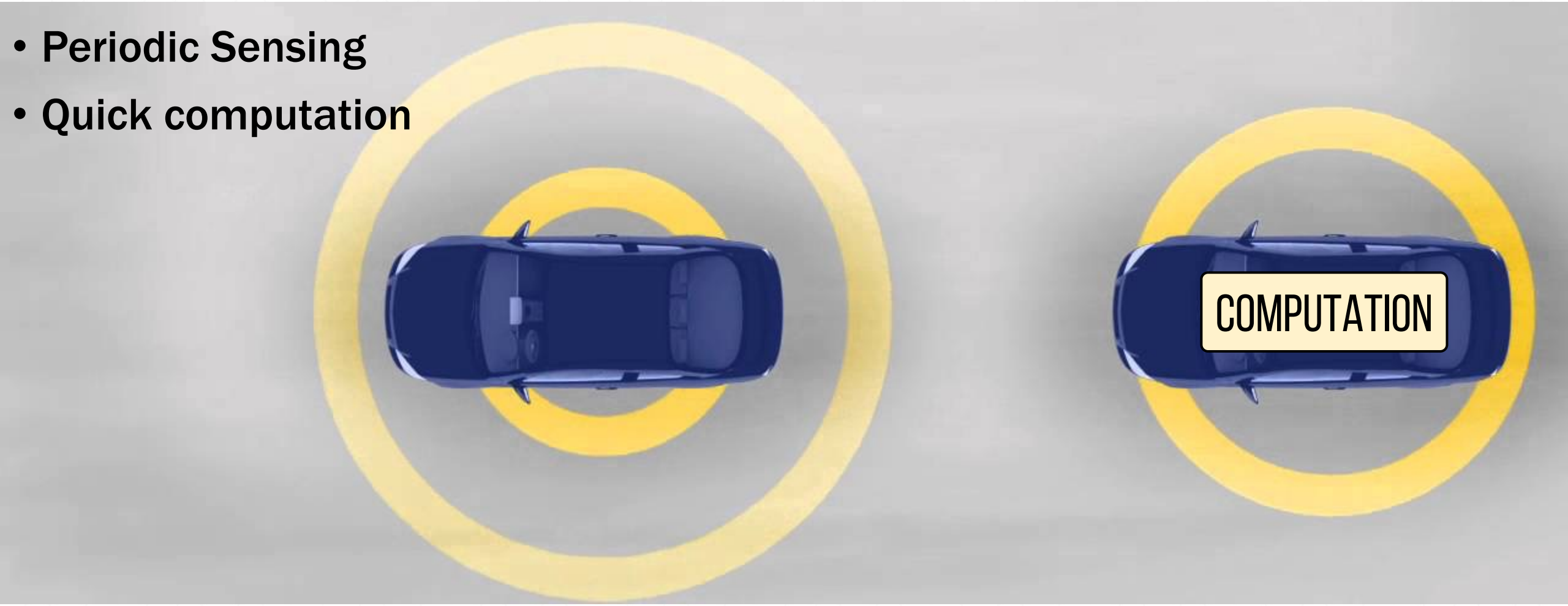
SENSING/ACTUATION IN THE REAL WORLD

- Periodic Sensing



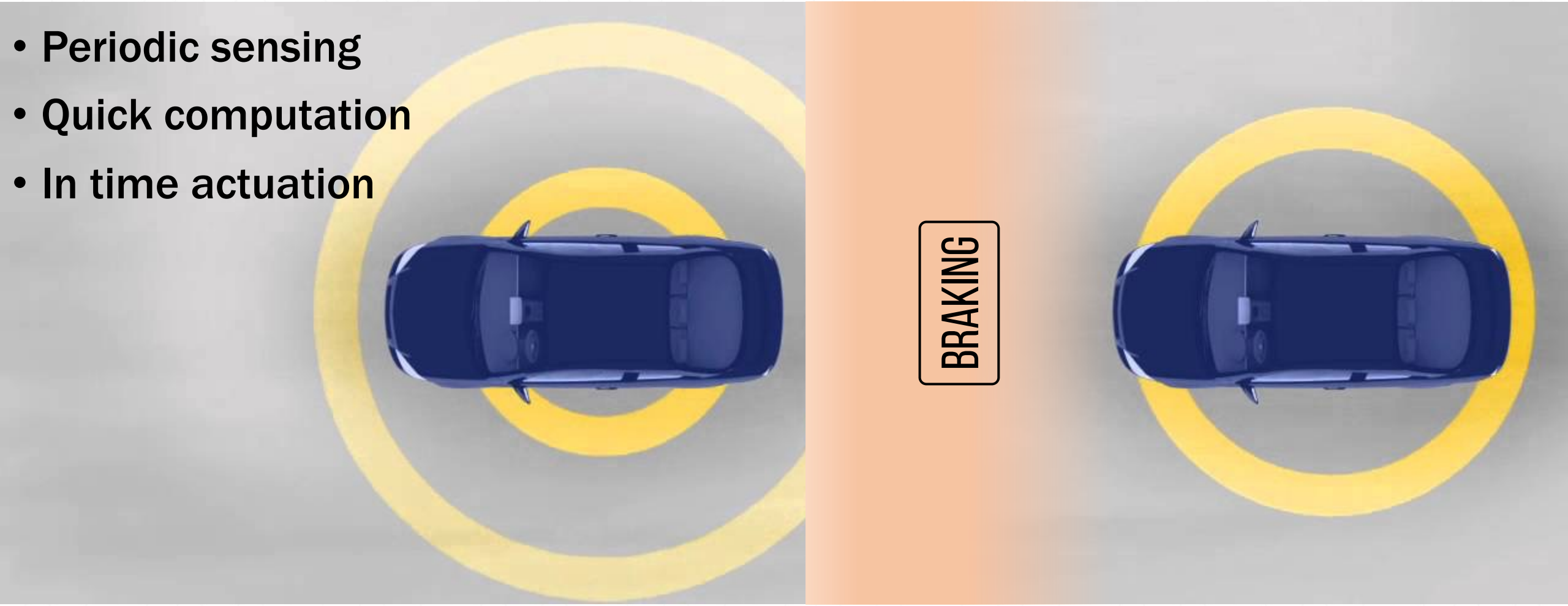
SENSING/ACTUATION IN THE REAL WORLD

- Periodic Sensing
- Quick computation



SENSING/ACTUATION IN THE REAL WORLD

- Periodic sensing
- Quick computation
- In time actuation



PERIODIC SENSING

QUICK COMPUTATION

IN TIME ACTUATION


PERIODIC SENSING
QUICK COMPUTATION
IN TIME ACTUATION
TIME

REAL-TIME SYSTEMS

REAL-TIME SYSTEMS

"A system that requires both, **logical** as well as **temporal** correctness."

REAL-TIME SYSTEMS

"A system that requires both, **logical** as well as **temporal** correctness."

- **Temporal correctness defined as a constraint: deadline**

REAL-TIME SYSTEMS

"A system that requires both, **logical** as well as **temporal** correctness."

- **Temporal correctness defined as a constraint: deadline**
- **Deadlines determine usefulness of results**
  - **Deadline passes → usefulness drops**

REAL-TIME SYSTEMS

"A system that requires both, **logical** as well as **temporal** correctness."

- **Temporal correctness defined as a constraint: deadline**
- **Deadlines determine usefulness of results**
  - **Deadline passes → usefulness drops**
- **Use well-defined scheduling algorithms [e.g. RM, EDF]**

REAL-TIME SYSTEMS

"A system that requires both, **logical** as well as **temporal** correctness."

- **Temporal correctness defined as a constraint: deadline**
- **Deadlines determine usefulness of results**
  - **Deadline passes → usefulness drops**
- **Use well-defined scheduling algorithms [e.g., RM, EDF]**

ONE OF THE **FOUNDATIONAL** AREAS FOR CYBER-PHYSICAL SYSTEMS

REAL-TIME SYSTEMS

Consider an airbag deployment system

REAL-TIME SYSTEMS

Consider an airbag deployment system

REAL-TIME SYSTEMS

Consider an airbag deployment system

REAL-TIME SYSTEMS

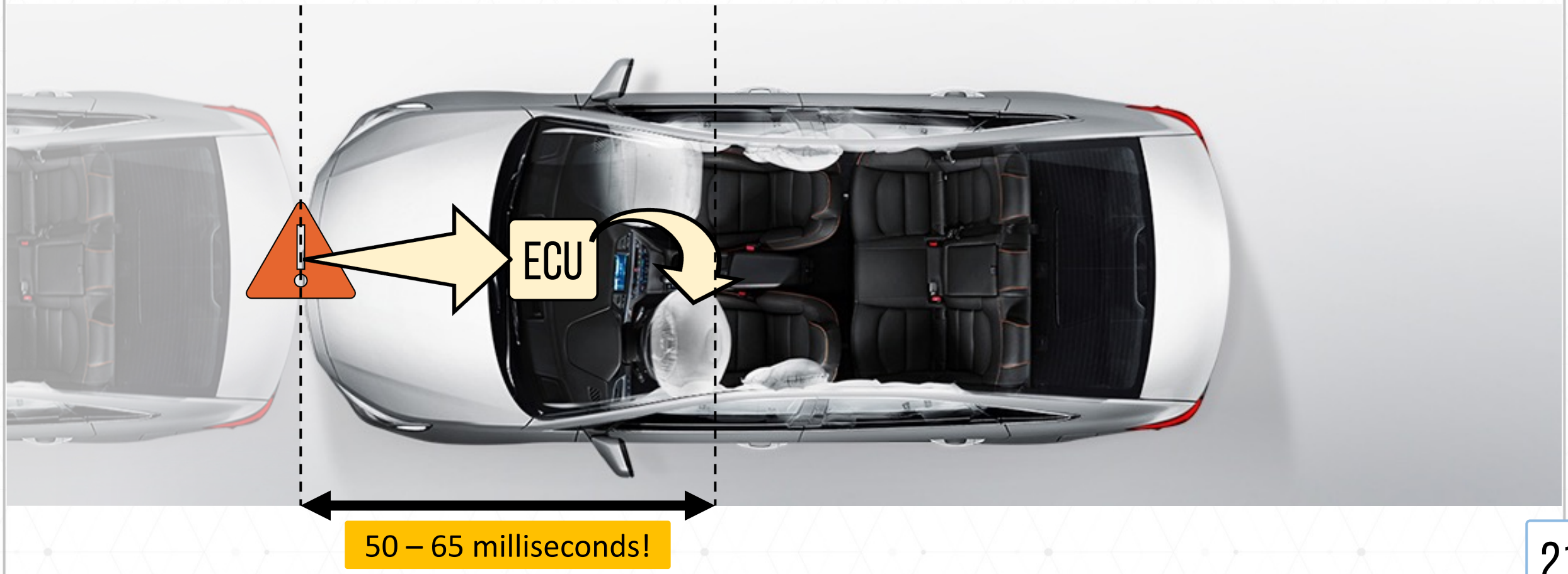
Consider an airbag deployment system

REAL-TIME SYSTEMS

Consider an airbag deployment system

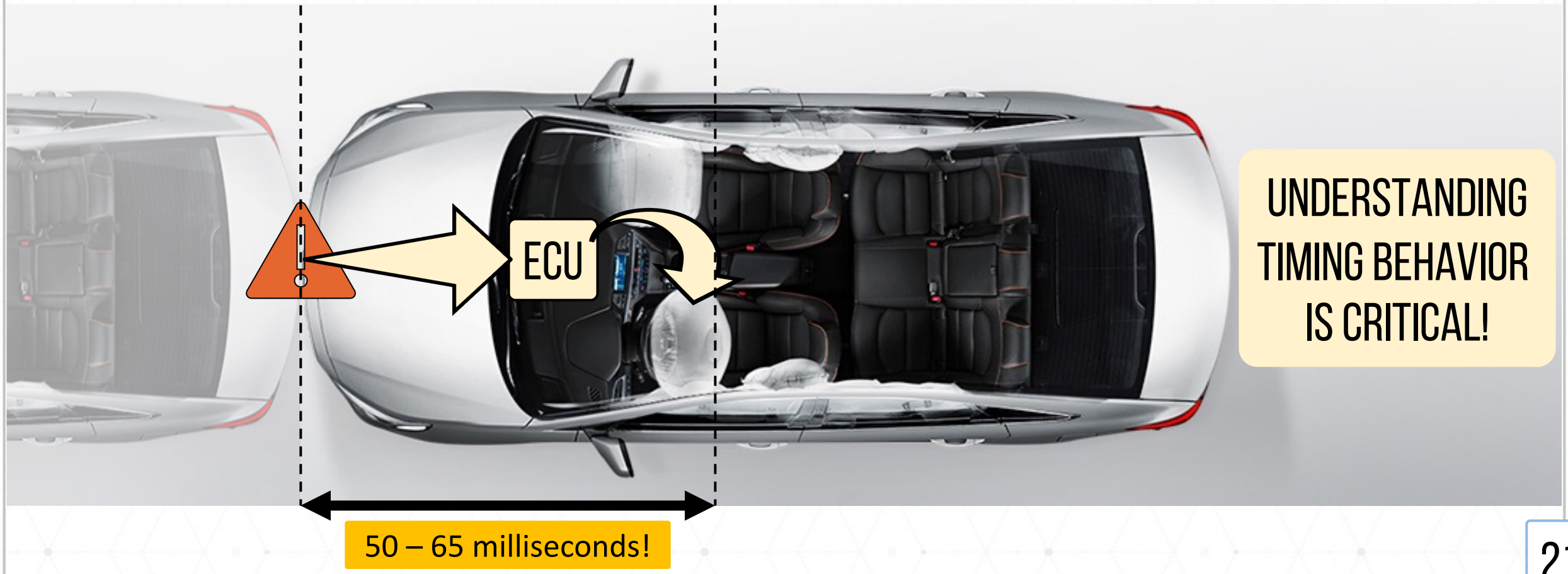
REAL-TIME SYSTEMS

Consider an airbag deployment system



REAL-TIME SYSTEMS

Consider an airbag deployment system



UNDERSTANDING TIMING BEHAVIOR IS CRITICAL!

REAL-TIME SYSTEMS

Consider an airbag deployment system

UNDERSTANDING TIMING BEHAVIOR IS CRITICAL!

DEADLINES = SAFETY OF PHYSICAL SYSTEM

REAL-TIME SYSTEMS

Consider an airbag deployment system

WHY NOT RUN CODE REALLY FAST?

50 – 65 milliseconds!

UNDERSTANDING TIMING BEHAVIOR IS CRITICAL!

CPS Challenges

Limited Resources
- Computational power, energy, cost

Timing Requirement
- Safety, reliability, deadlines

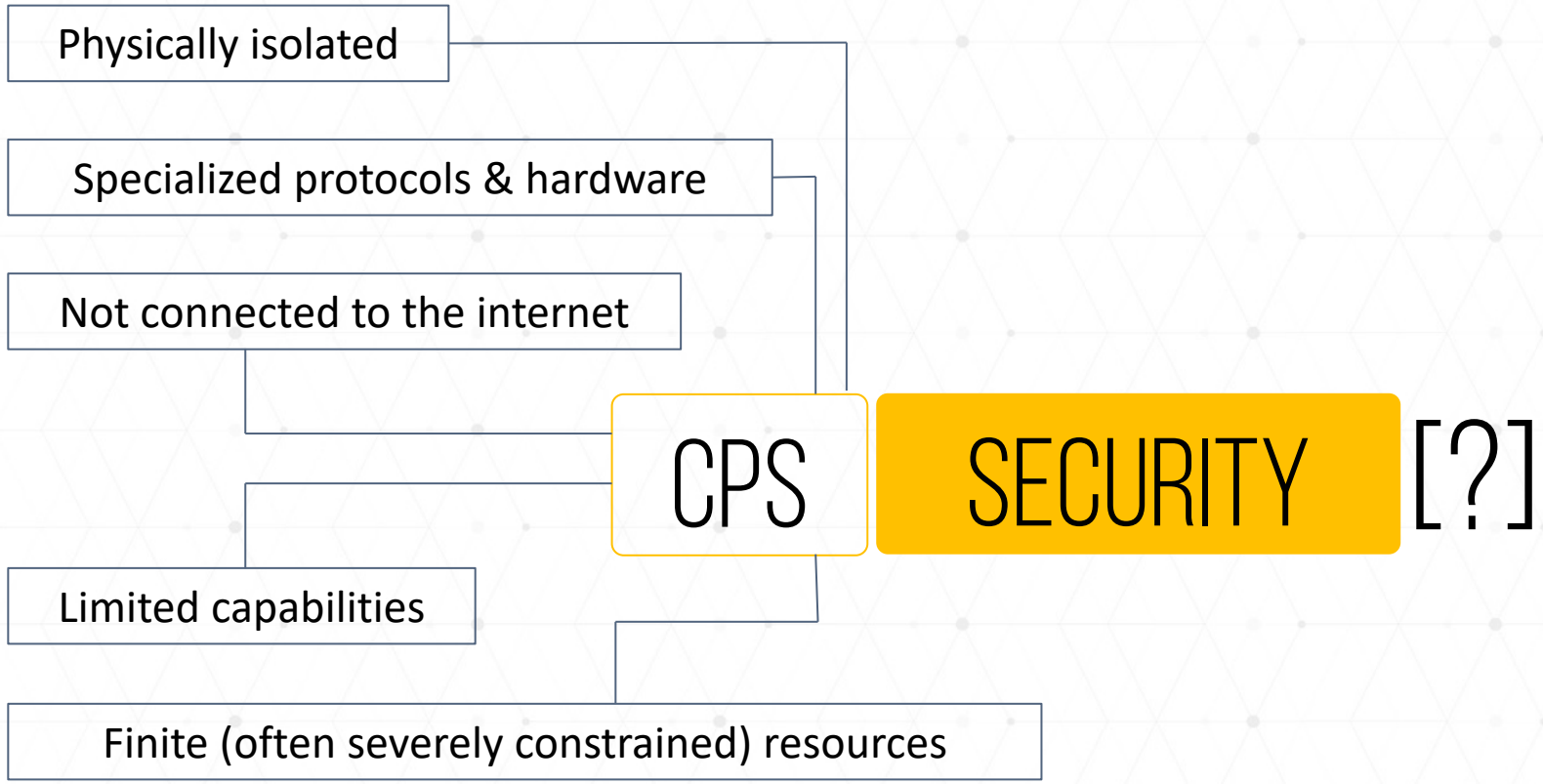
CPS Challenges

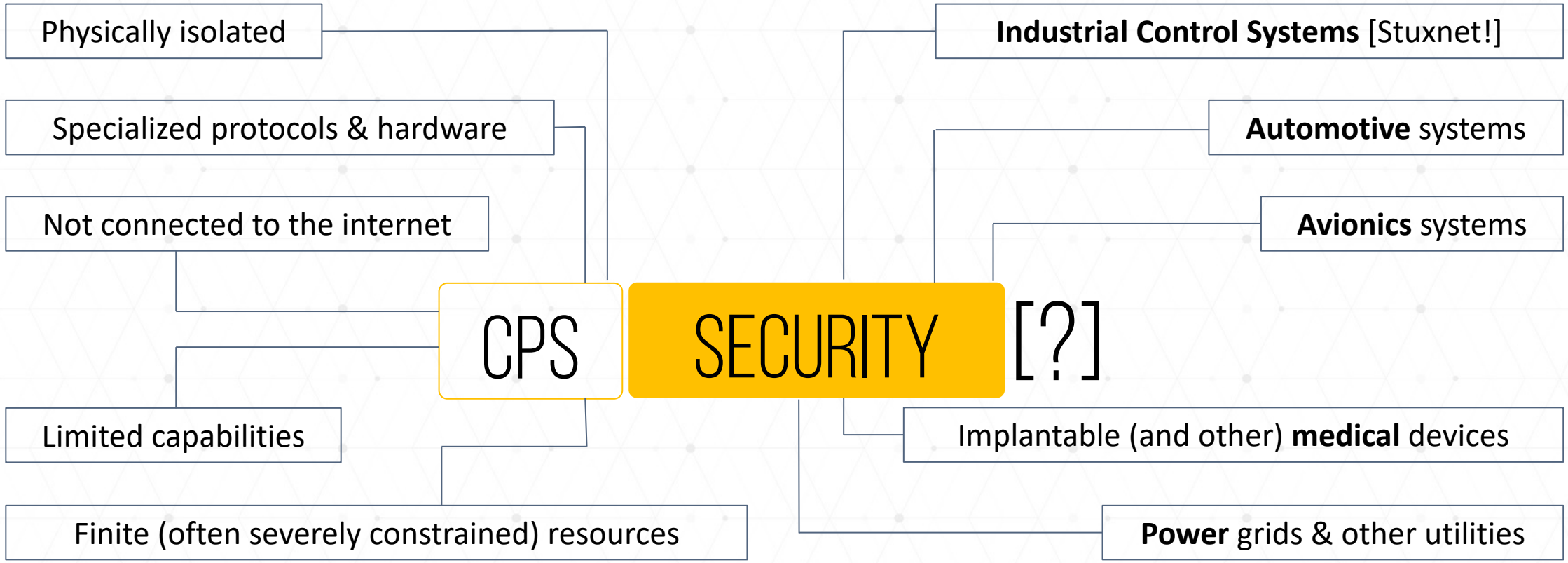
Limited Resources
- Computational power, energy, cost

Timing Requirement
- Safety, reliability, deadlines

Security/System Upgradability
- Schedulability, Verifiability

CPS SECURITY


Physically isolated
Specialized protocols & hardware
Not connected to the internet
Limited capabilities
Finite (often severely constrained) resources
CPS
SECURITY
[?]


Physically isolated
Specialized protocols & hardware
Not connected to the internet
Limited capabilities
Finite (often severely constrained) resources
CPS
SECURITY
[?]
Industrial Control Systems [Stuxnet!]
Automotive systems
Avionics systems
Implantable (and other) medical devices
Power grids & other utilities

Autonomous Cars | UAVs | Medical/surgical robots | IoT

Delivery robots | Smart Manufacturing Systems

Physically isolated

Specialized protocols & hardware

Not connected to the internet

Limited capabilities

Finite (often severely constrained) resources

CPS

SECURITY

Industrial Control Systems [Stuxnet!]

Automotive systems

Avionics systems

Implantable (and other) **medical** devices

Power grids & other utilities

Autonomous Cars | UAVs | Medical/surgical robots | IoT

Delivery robots | Smart Manufacturing Systems

Physically isolated

Specialized protocols & hardware

Not connected to the internet

Limited capabilities

Finite (often severely constrained) resources

Industrial Control Systems [Stuxnet!]

Automotive systems

Avionics systems

Implantable (and other) **medical** devices

Power grids & other utilities

CPS SECURITY RESILIENCY

RESILIENCY?

RESILIENCY?

SOFTWARE ERRORS CAN RESULT IN PHYSICAL FAILURES

RESILIENCY?

SOFTWARE ERRORS CAN RESULT IN PHYSICAL FAILURES

SECURITY AND RESILIENCY

SECURITY AND RESILIENCY

ATTACKER INTENT

SECURITY AND RESILIENCY

ATTACKER INTENT ..... Cause systems to crash

SECURITY AND RESILIENCY

ATTACKER INTENT ..... Cause systems to crash

NOT CONCERNED WITH DATA BEING STOLEN

SECURITY AND RESILIENCY

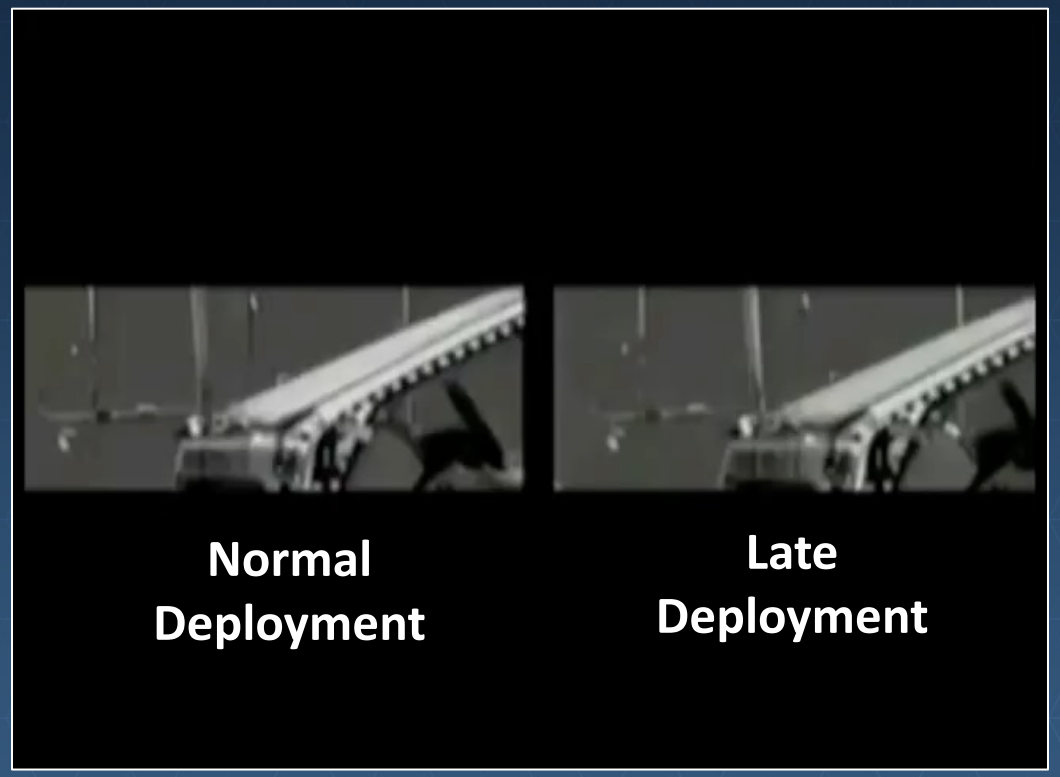
ATTACKER INTENT

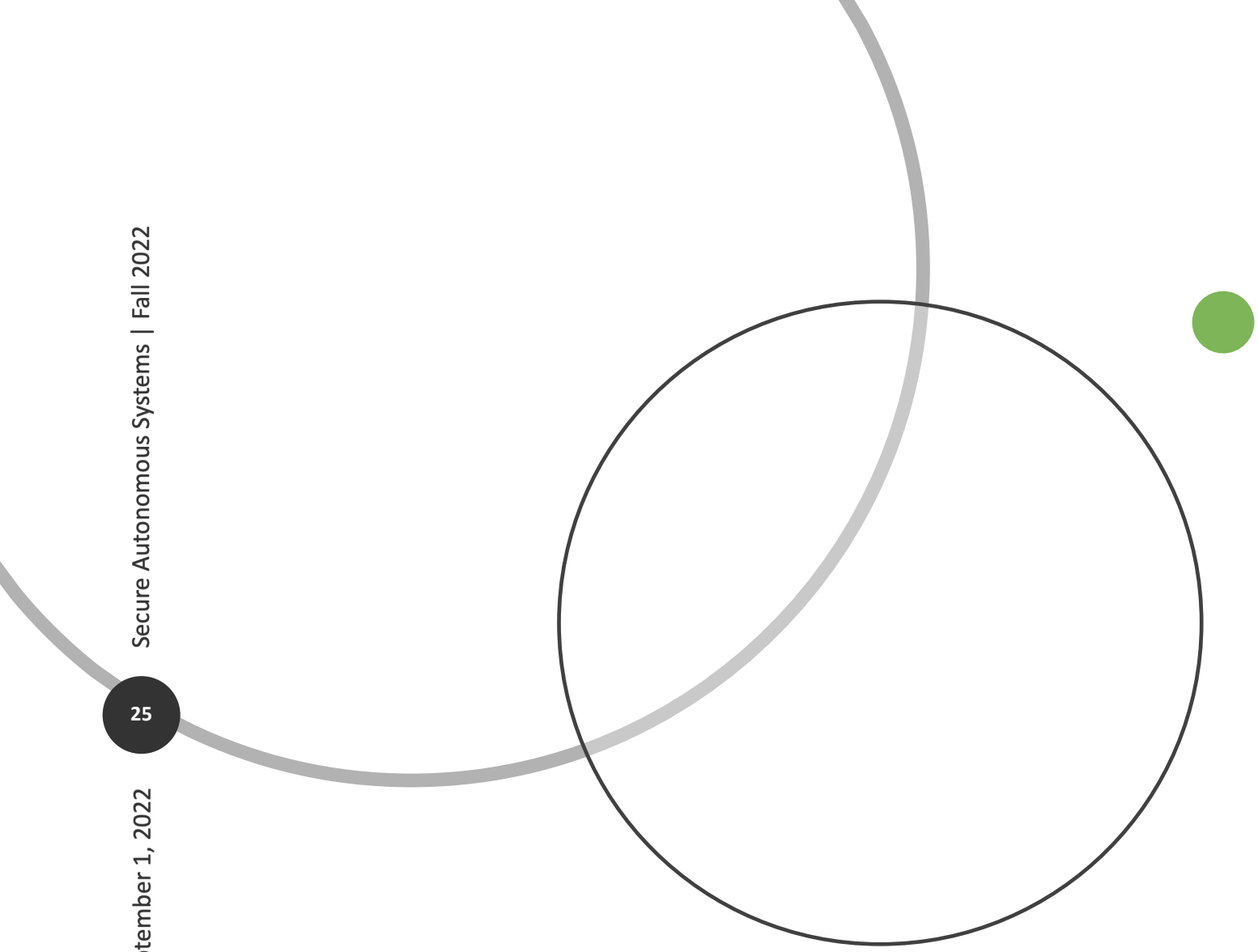
Cause systems to crash

What if airbag deployment is delayed?

SECURITY AND RESILIENCY

ATTACKER INTENT ..... Cause systems to crash





Next Lecture

- **Design** of Autonomous Systems
- **Sensing**
  - IMU, GPS, Radar, LIDAR, Camera, etc.