



UNIVERSITÀ
DEGLI STUDI
DI PADOVA



SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP



Introduction to Cyber-Physical Systems and IoT Security

Alessandro Brighente



Contacts

- Mail: alessandro.brighente@unpd.it
- Website: <https://www.math.unipd.it/~abrighen/>


Education


- M.Sc in Telecommunication Engineering
- Ph.D. in Information Engineering
- Visiting researcher at Nokia Bell Labs and University of Washington
- Assistant professor, Department of Mathematics

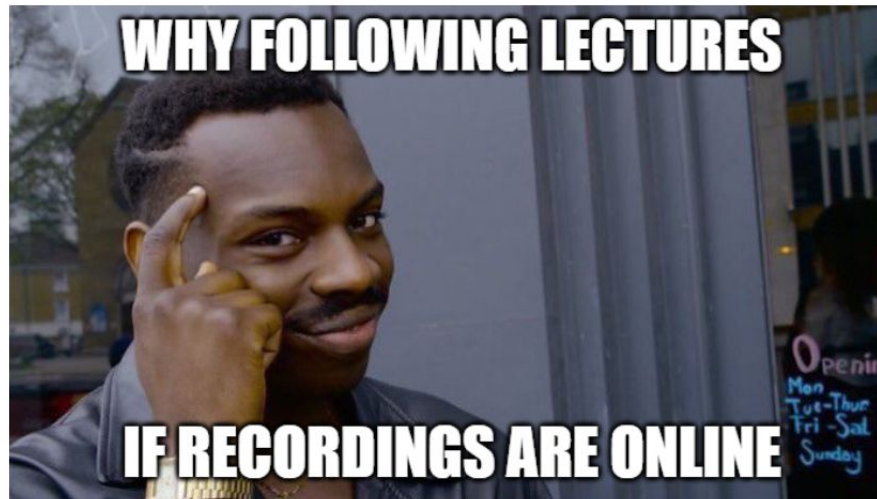
Research Interests:

Security and Privacy in

- Network Security
- Cyber-Physical Systems
- Distributed ledger technology

- **Language:** 
- **Credits:** 6 CFU
- **Schedule:** I semester.
- **Lectures mode:** you can attend the course at the University.
Lectures will be also recorded and available in the Moodle platform.

- **Language:** 
- **Credits:** 6 CFU
- **Schedule:** I semester.
- **Lectures mode:** you can attend the course at the University.
Lectures will be also recorded and available in the Moodle platform.



- During classes, we will explore attacks and countermeasures for CPS and IoT security
- We will provide you some code and simulators to test attacks and gain some insights on specific applications

Fundamentals

- What is a Cyber-Physical System
- Security Requirements in CPS

Automotive Security

- The CAN bus protocol
- Error handling in CAN bus and bus-off attack
- Network attacks on CAN bus
- Keyless cars security and attacks to distance bounding protocols

Autonomous Driving

- Introduction to controllers
- Levels of automation and modes of operation
- Attacks on controllers and countermeasures

Drones

- Drone components and basic functioning
- Protocols for drone location and fail-safe procedures
- Drone detection systems

Industrial Control Systems

- Industrial Control Network Protocols
- PLC and their functioning
- Attacks and countermeasures to industrial control systems

Internet of Things

- Network protocols for the internet of things
- Remote attestation
- Intrusion and anomaly detection

The overall exam grade is divided according to the following criteria:

- 40%: mid-term report on work implementing attacks and countermeasures on a topic chosen from the first part of the course
- 40%: final report on work implementing attacks and countermeasures on a topic of your choice from the second part of the course
- 20%: final theoretical exam (10 multiple choice questions)

At the end of the course, the student will be able to

- Analyze a control flow and understand its fundamental operations, with particular reference to the CAN protocol.
- Ability to implement control layer and network layer attacks.
- Ability to analyze CAN bus traffic and infer information on its operation.
- Implement simple controllers and test their safety.
- Analyze a ladder logic program for PLC and understand how it works. Implement attacks capable of altering its functioning and design secure programs.

At the end of the course, the student will be able to

- Understand the functioning of the main industrial protocols, implement integrity and availability attacks, and develop countermeasures.
- Understand how drone positioning protocols and fail safe procedures work. Implement GPS spoofing attacks to divert trajectories.
- Implement remote attestation protocols for IoT devices and analyze their performance.

Cyber-Physical Systems (CPSs) are characterized by the deep complex intertwining among :

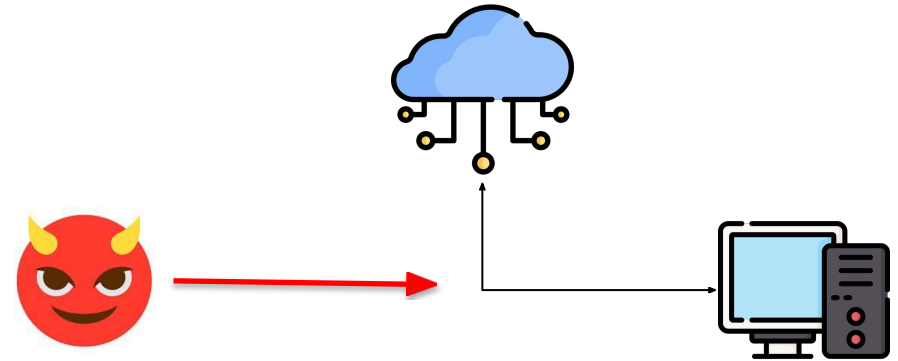
- The world of Physical Processes, or Operational Technology, or OT
- The world of Information Technology, or IT.

Some Example:

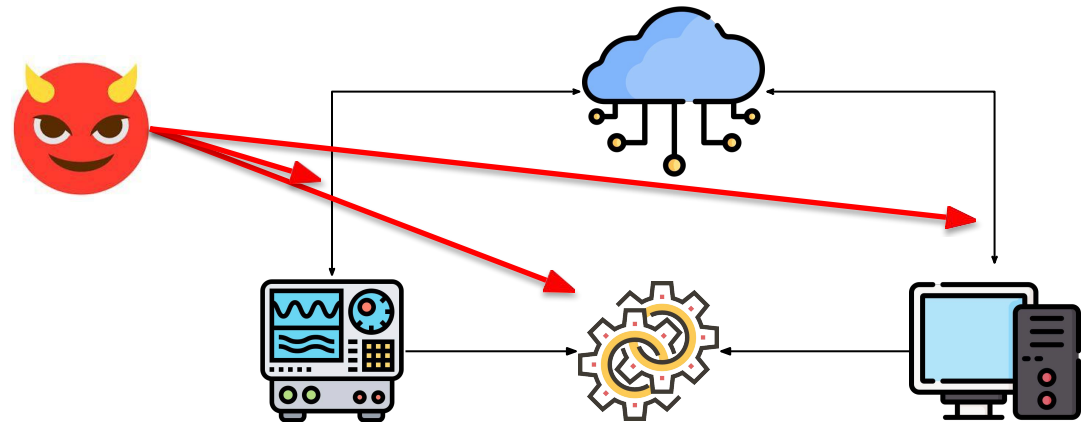
- *Smart Grid*
- *Smart Cars*
- *Industrial Control Systems*
- *e-Health Devices*



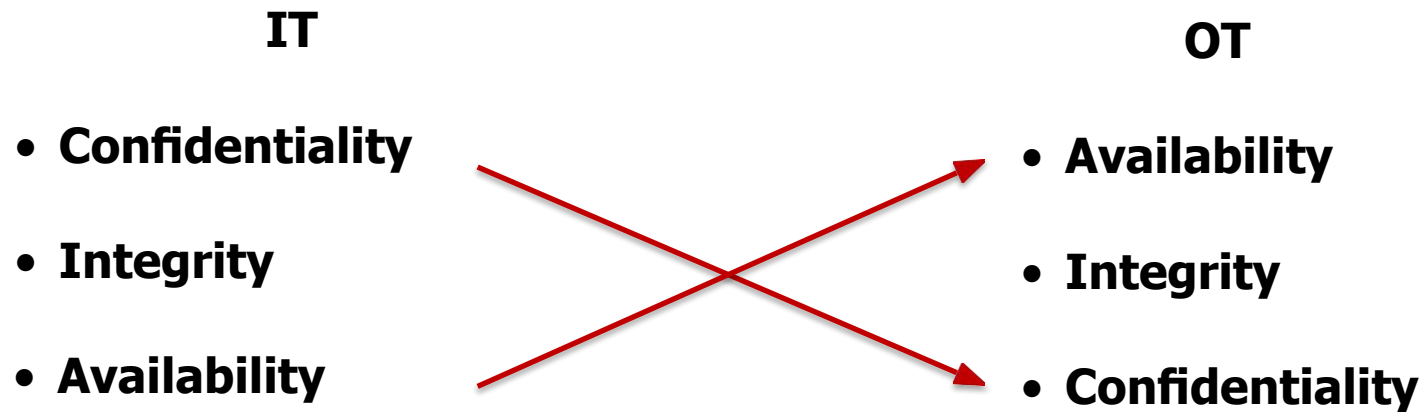
Traditional IT Systems



Cyber-Physical Systems



According to the literature on CyberSecurity, CIA paradigm is **reversed**:



What if we lose Availability of nuclear plants monitoring data?



Do we have to care?



UNIVERSITÀ
DEGLI STUDI
DI PADOVA



SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP



DIPARTIMENTO
MATEMATICA
HIT HUMAN INSPIRED TECHNOLOGY
Research Centre

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS MORE

Forbes

ANDY GREENBERG SECURITY 07.21.2015 06:00 AM

Hackers Remotely Kill a Jeep on the Highway—With Me in It

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

EDITORS' PICK | Apr 29, 2021, 10:48am EDT | 18,895 views

Watch A Tesla Have Its Doors Hacked Open By A Drone

ZDNet AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL

BMW and Hyundai hacked by Vietnamese hackers, report claims

Hacks linked to Ocean Lotus (APT32), a group believed to operate with orders from the Vietnamese government.

[Click me for the video!](#)

Do we have to care?



UNIVERSITÀ
DEGLI STUDI
DI PADOVA



SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP



DIPARTIMENTO
MATEMATICA
HIT HUMAN INSPIRED TECHNOLOGY
Research Centre



CNN

US

Attacks on US power grid have been subject of extremist chatter for years. DHS bulletin warns of attacks on critical infrastructure amid other targets

Cyberattack Forces a Shutdown of a Top U.S. Pipeline

The operator, Colonial Pipeline, said it had halted for its 5,500 miles of pipeline after being hit by ransomware attack.

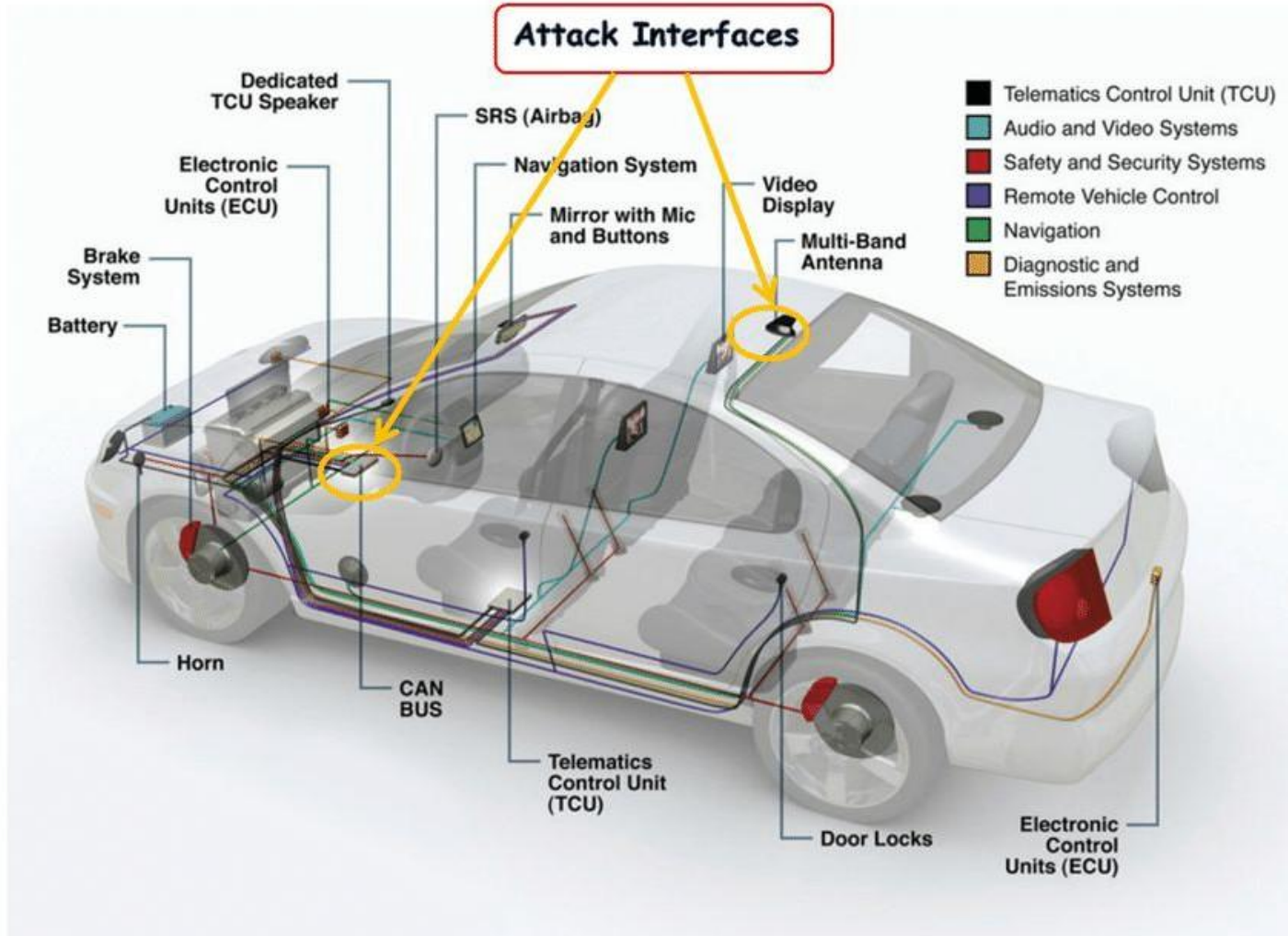
Subscribe to newsletters

Forbes

FORBES > INNOVATION > SUSTAINABILITY

U.S. Water Supply System Being Targeted By Cybercriminals

CAN bus

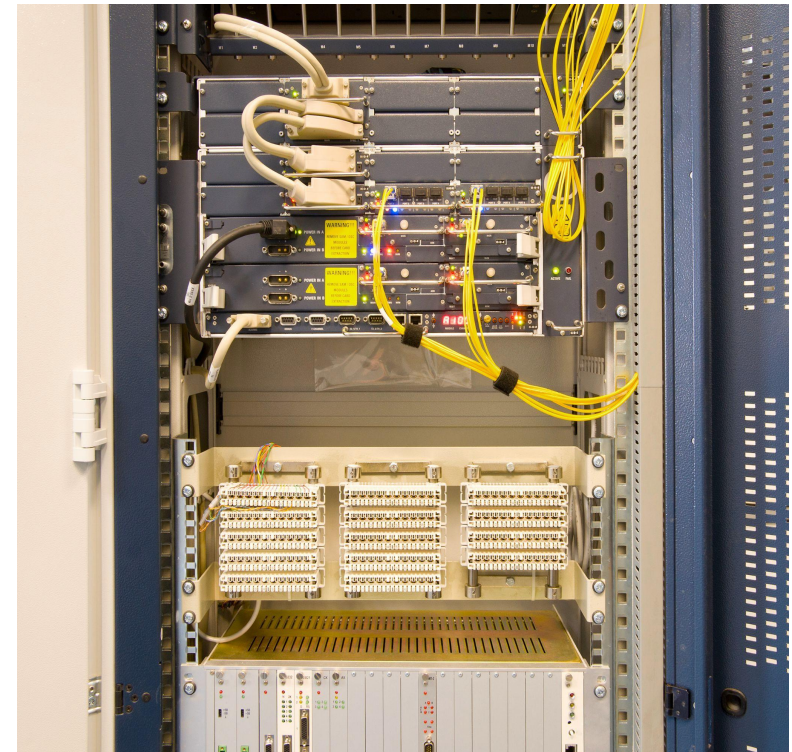


Benefits of organizing vehicles in platoons:

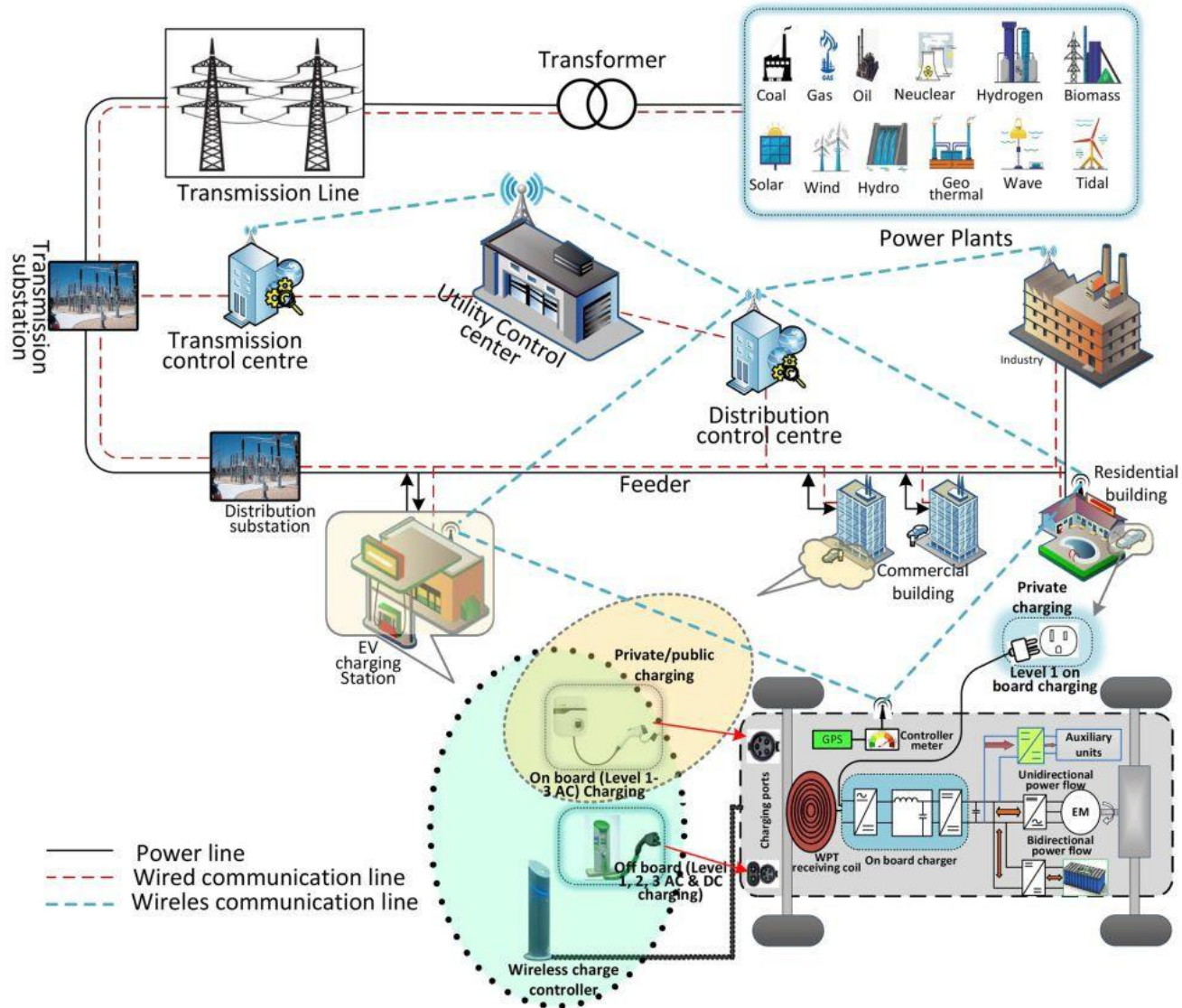
- Fuel Efficiency
- Road Capacity
- Road Safety
- “Greener”



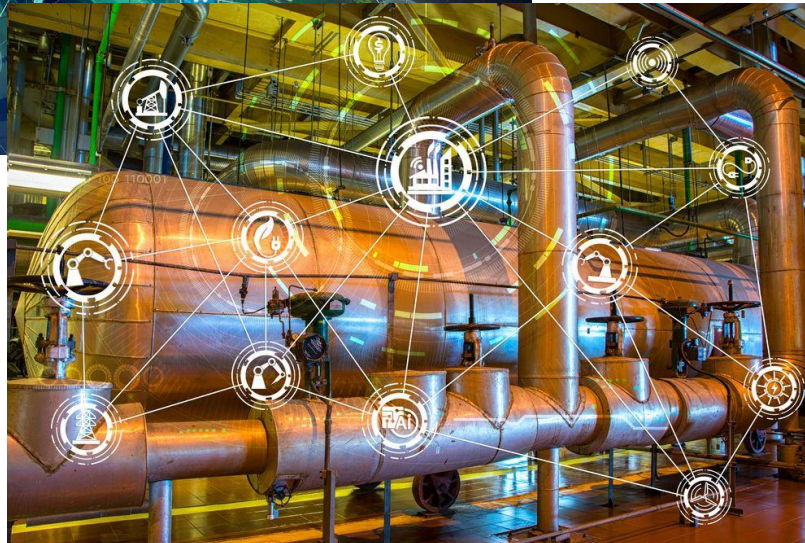
- Industrial systems have dedicated networks and components
- Operational technology + information technology
- Dedicated computing systems



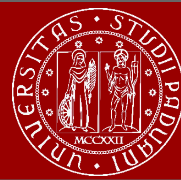
Vehicle-to-Grid (V2G)



- IoT devices are employed in safety-critical systems



Structure of a Drone



- Multiple modules to acquire and process data
- Communication module as enabler

