Software Development for Unmanned Aerial Systems

Instructor:

Jane Cleland-Huang, PhD

JaneClelandHuang@nd.edu

Department of Computer Science and Engineering

University of Notre Dame

A Preliminary Look at Safety Analysis

Hazard Analysis → **Mitigations** → **Safety Evidence**

Hazard Analysis

- What hazards could occur?
- What failures could cause the hazard to occur?

Mitigations

- How can we prevent these failures from occurring and specify them as safety requirements.

Safety Evidence

- How can we demonstrate that safety has been successfully achieved?

Hazard: UAVs collide in midair

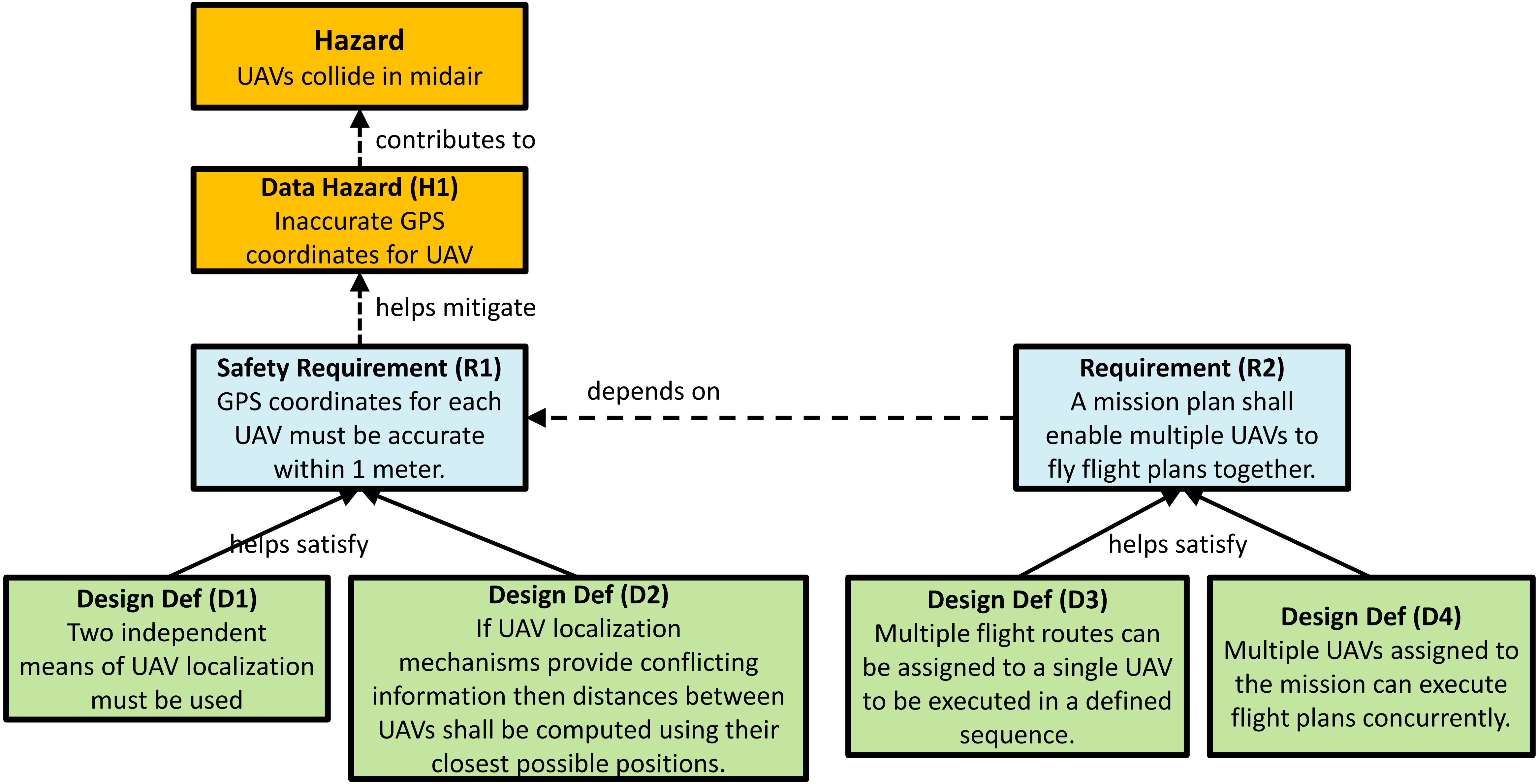
Why are we focusing on this problem?

Challenging problem that must be addressed if we are going to have safe UAV flights.

FMECAs (Failure Mode Effect riticality Analysis)

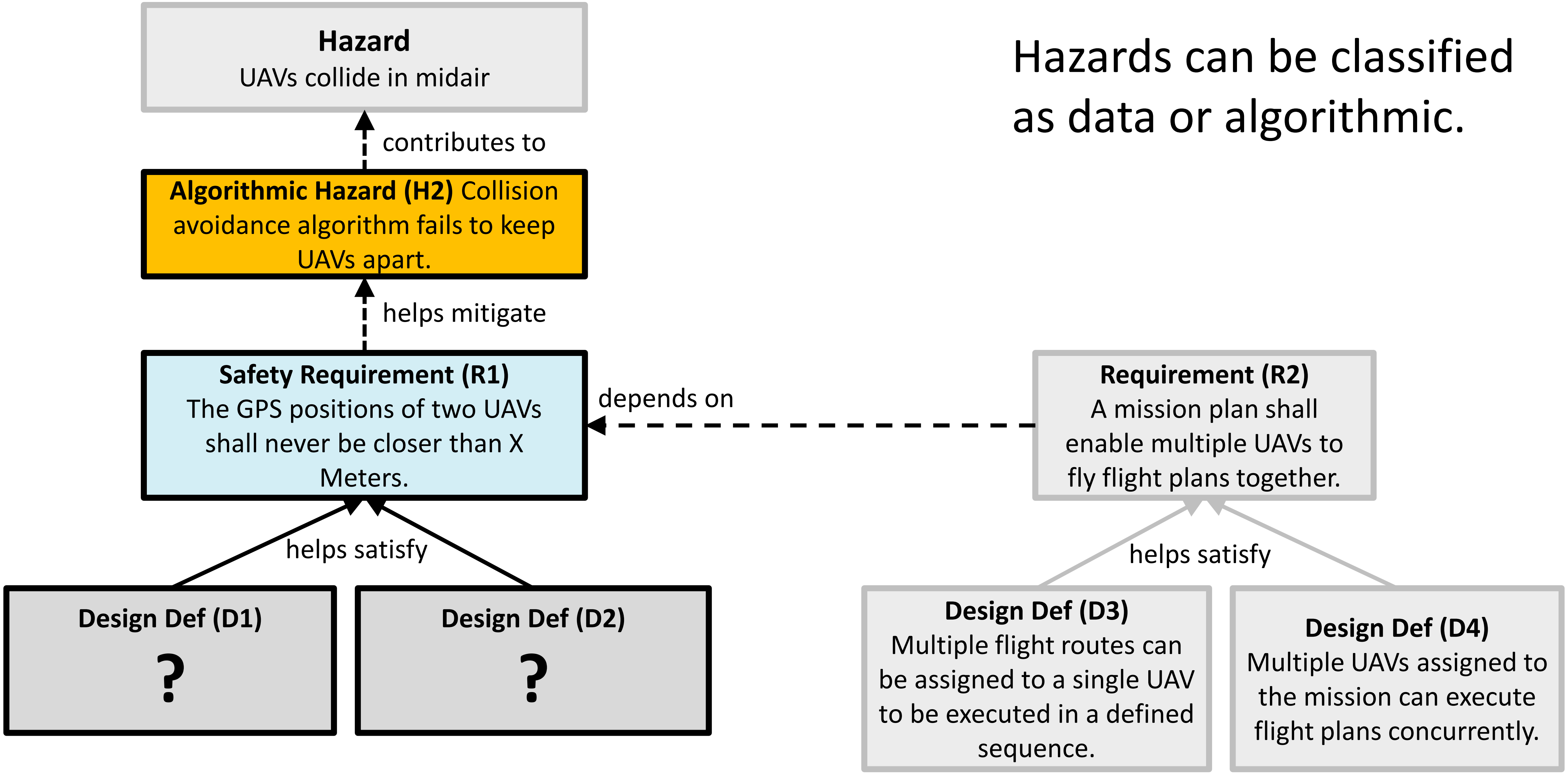
ID	Data Item	Data Fault Type	Description		Effect	Criticality
FM-D2	Battery level indicator	Faulty error detection	Low battery level is not detected.	EF-4	Drone runs out of power and lands in an uncontrolled way.	Critical
FM-D3	Battery level	Faulty data	Battery level indicator depicts incorrect power availability.	EF-5	Drone runs out of power and lands in an uncontrolled way.	Critical
FM-D4	Drone health	Missing data	Drone fails to communicate its location	EF-6	Mission control can not accurately track the drone, potentially causing accidents such as drone crashes.	Critical
FM-D5	Altitude level	Faulty error detection	Altitude reading is lower than the actual altitude of the drone.	EF-7	Drone flies too high potentially entering the flight path of an airplane.	Critical
FM-D1	Landed status	Faulty status	On ground status = true even though drone is still in the air.	EF-8	Propellers stop prematurely and drone crashes	Critical

A Data Hazard

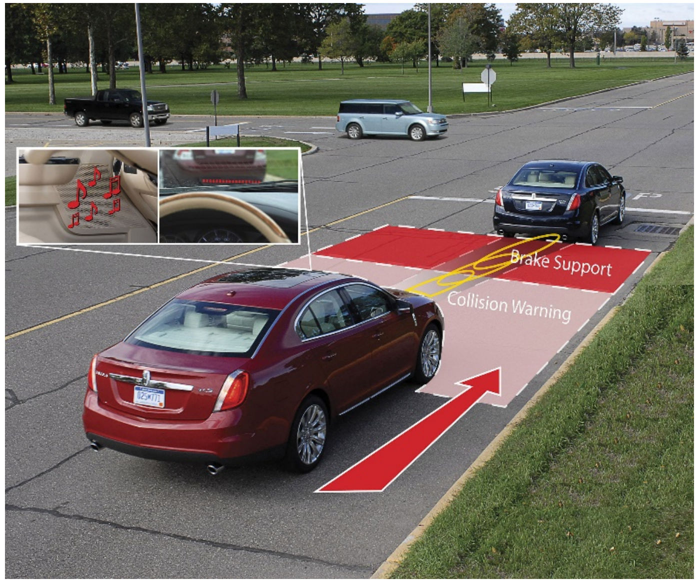


Another Hazard (Algorithmic?

Hazards can be classified as data or algorithmic.

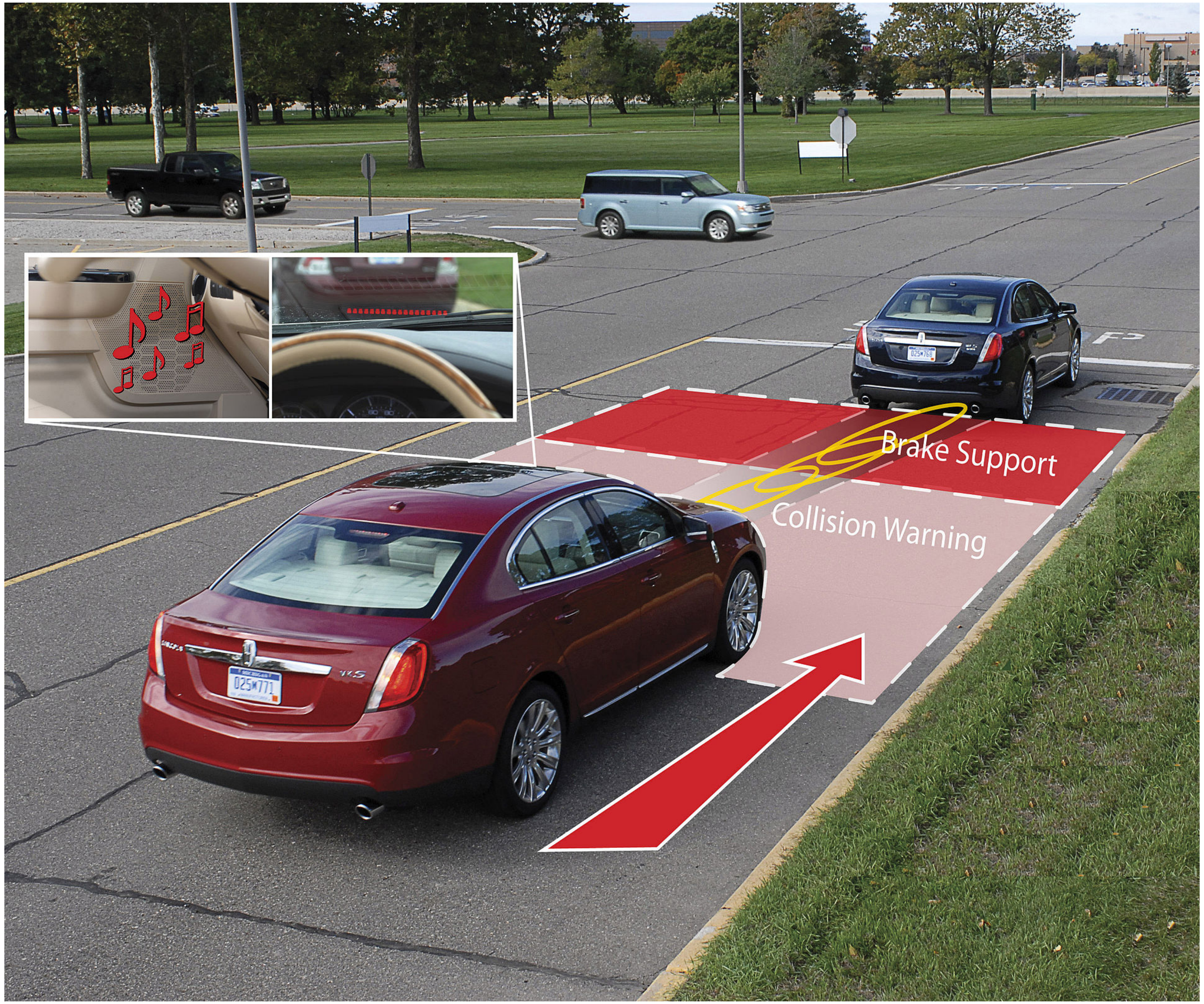


Some thoughts on Collision Avoidance



What can we learn about collision avoidance from three other domains?

Cars



How do you imagine collision avoidance systems work in cars?

https://www.lifewire.com/automobile-collision-avoidance-systems-534805

Airplanes

Solution of last resort.

What do you know about collision avoidance in airplanes?

https://www.flyingmag.com/how-it-works-tcas-ii

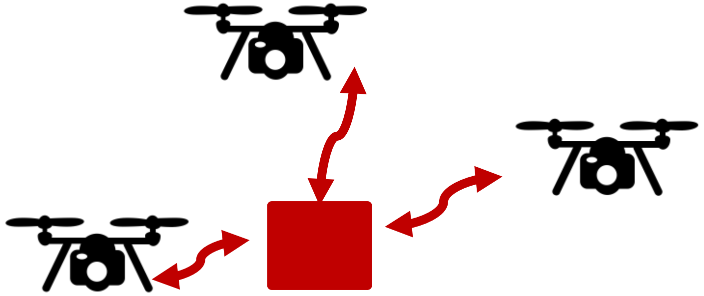
People

How do humans avoid each other when moving in a confined space?

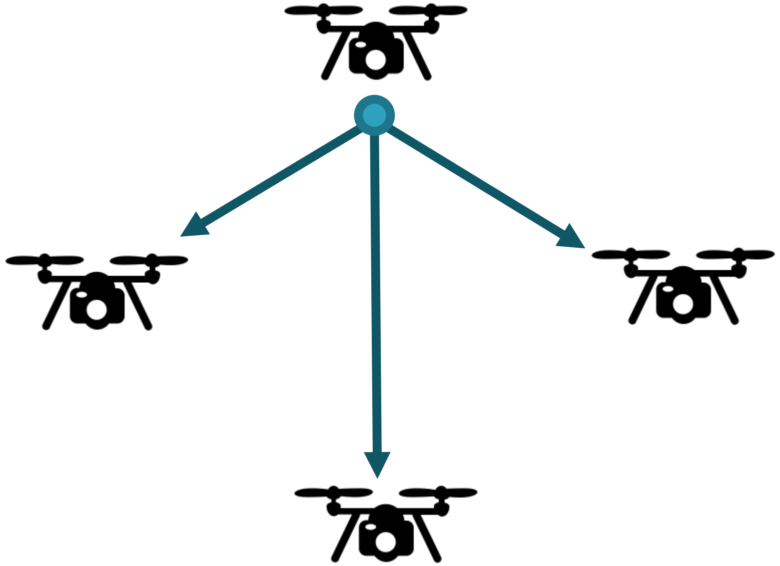
Let’s try it and see..

Towards a Collision Avoidance Algorithm

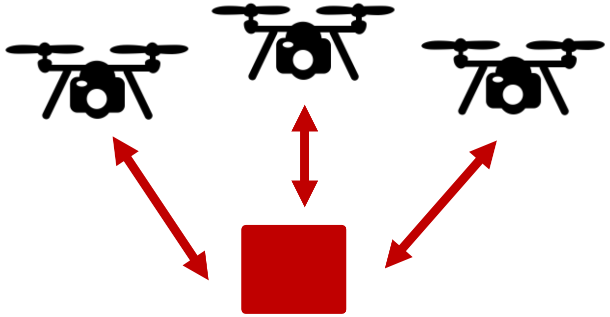
Centralized planned



Broadcast or detect positions of other UAVs in ROI



Centralized Responsive



Obstacle Detection and Avoidance

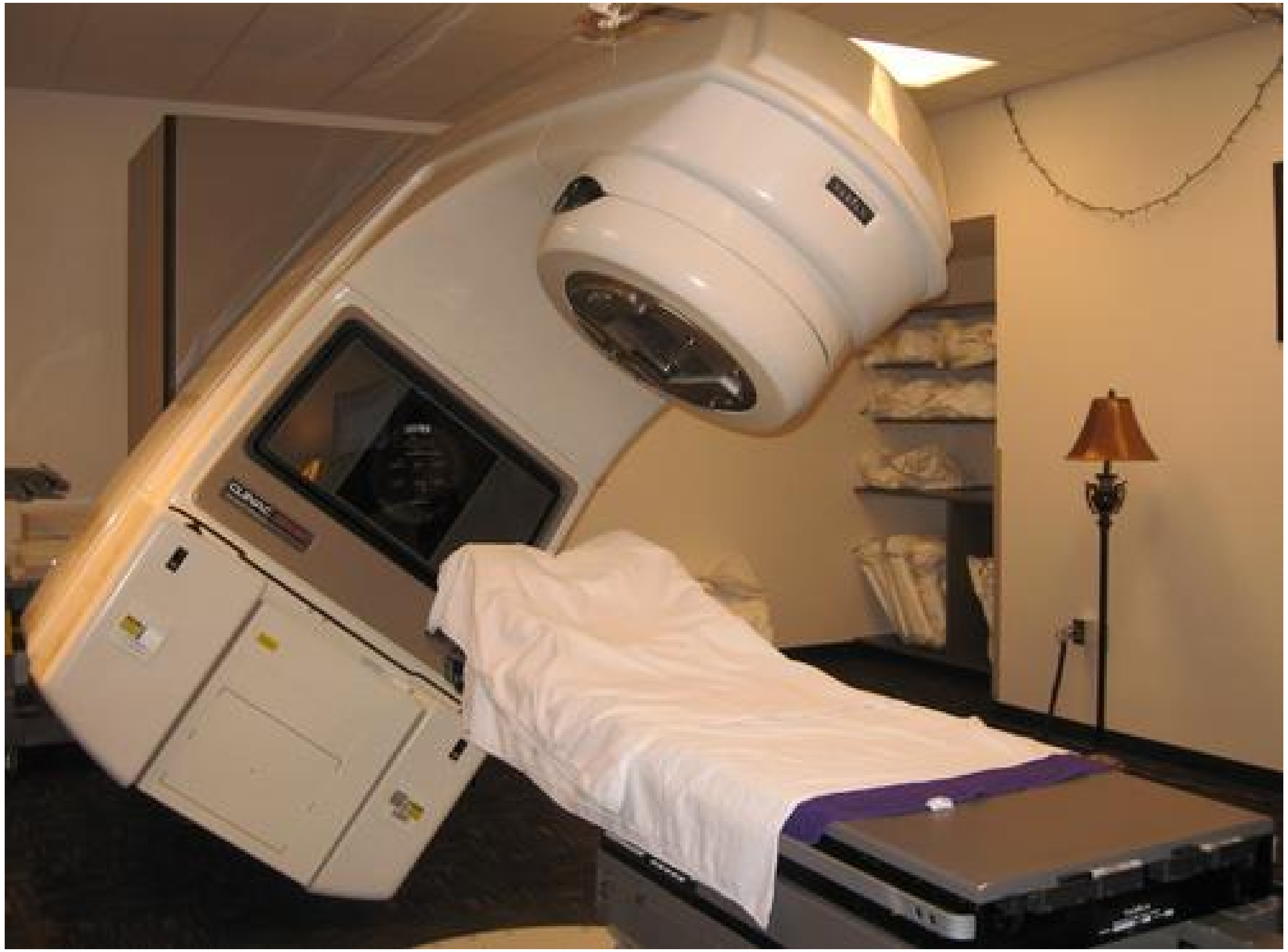
Environmental Assumptions

It is essential to understand your assumptions!

Wheels are turning if, and only if, the plane is on the runway.

Led to an accident when a plane failed to brake because the runway was wet and hydroplaning occurred.

Environmental Assumptions



A modern radiotherapy machine (NOT the Therac!)

The operator will not enter data faster than X words per minute.

Environmental Assumptions come in many shapes & sizes

Physical environment:
Expected to hold invariantly regardless of the system,
e.g., A train is moving iff its physical speed is non-null

Operational environment:
Describes the operational environment surrounding the system,
e.g., The lens cap will be removed before flight

Adjacent system:
Describes the behavior of adjacent systems that interact with the system being developed, e.g., The Sensor will provide the current temperature to the Thermostat with an accuracy of 0:1F

User interface:
Describes the users and their behavior,
e.g., The operator will not enter data faster than X words per minute

Regulatory:
Describes how regulations aect the system or related components,
e.g., The device meets industrial standards for electrical safety

Development process:
Describes policies or procedures impacting the development process and/or operation of the system,
e.g., The developer knows that transient signals should be ignored when the spacecraft lander's legs unfold

One Algorithm (not an as-is solution!)

https://www.youtube.com/watch?v=Hc6kng5A8lQ

http://gamma.cs.unc.edu/CA/ClearPath.pdf

Activity #2:
What assumptions are made in this model?

Hint: think about UAV capabilities, their environment, physics etc.