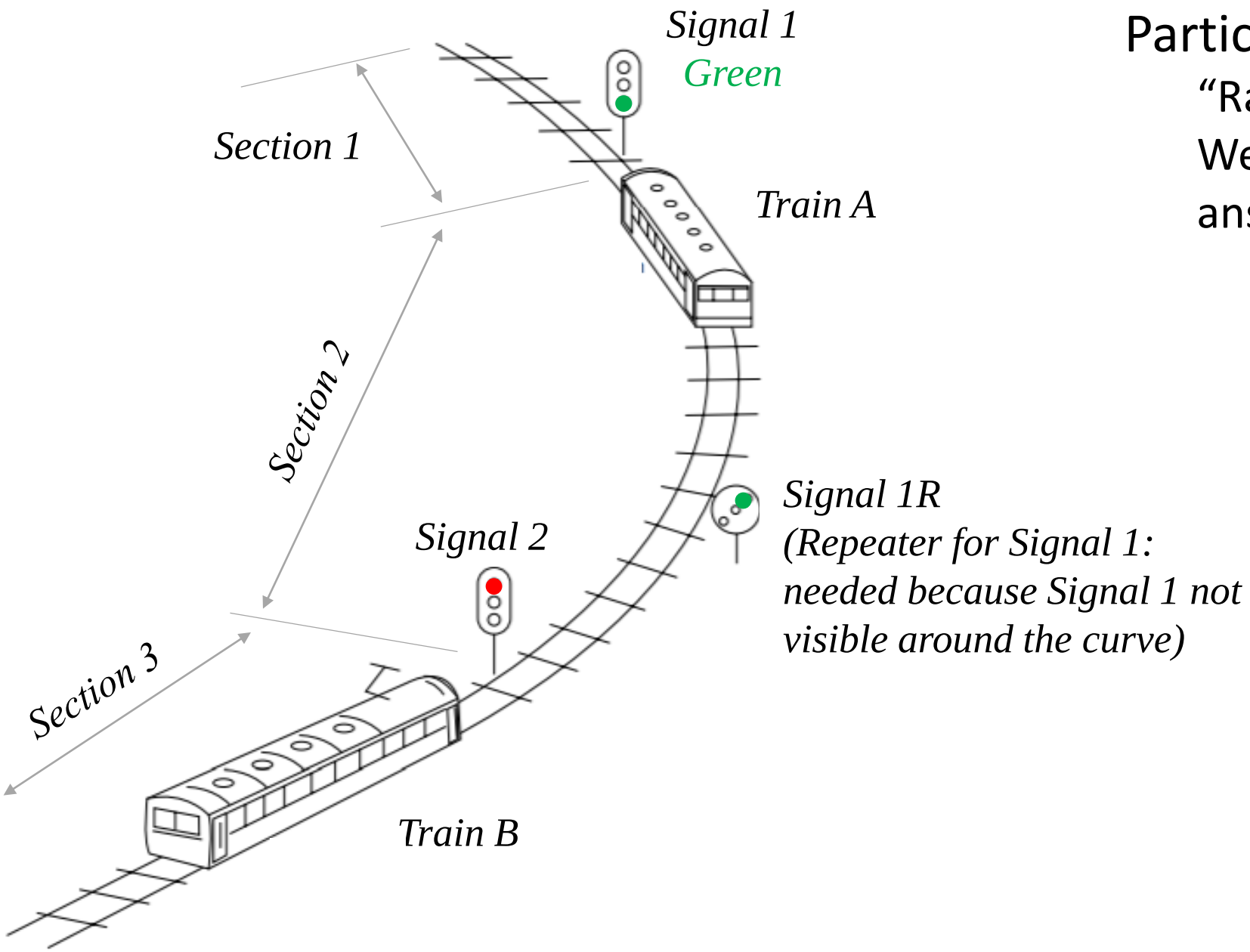
Massachusetts Institute of Technology

Short STPA Exercise
Train Signaling

John Thomas
Nikhil Bugalia

Overview

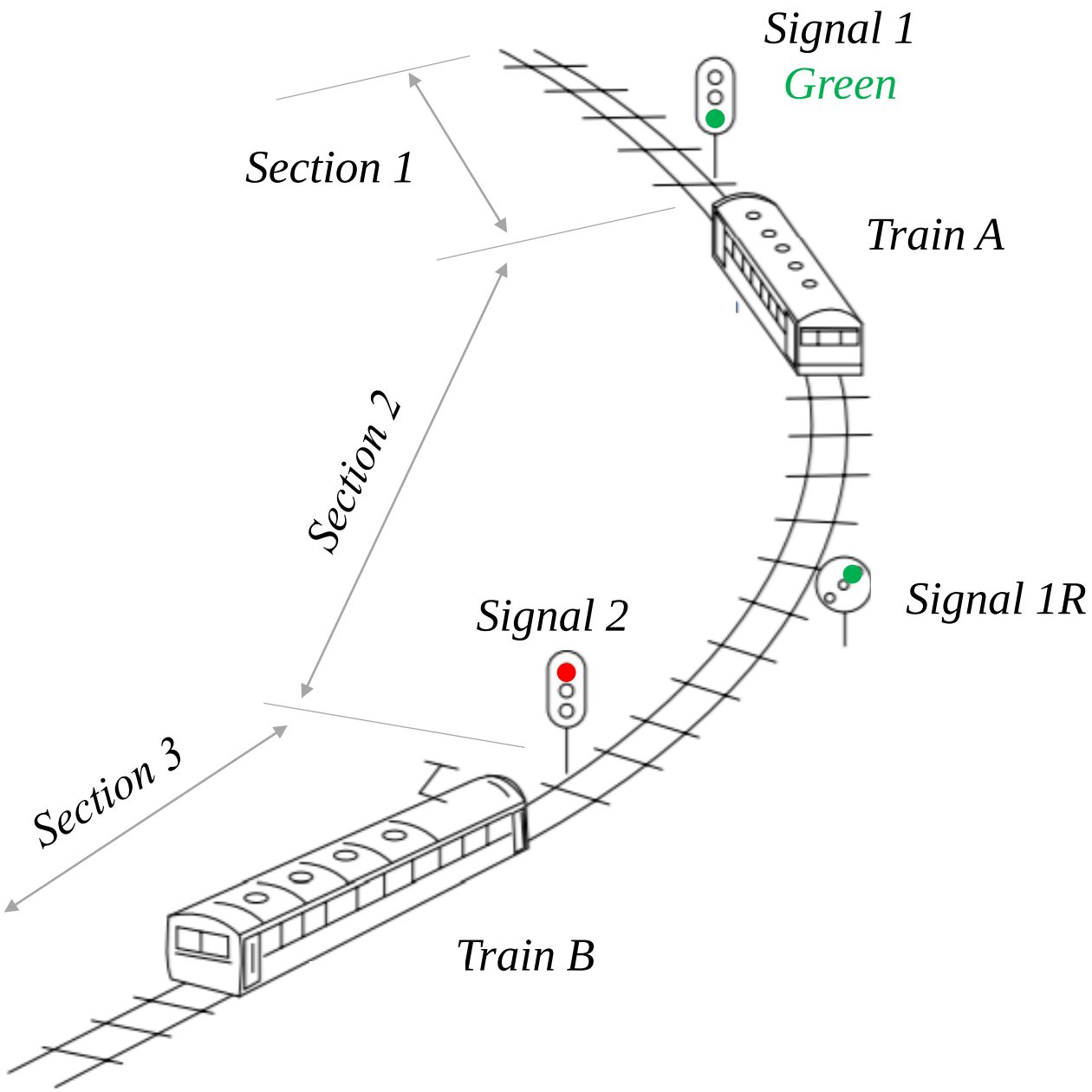


Participate in this exercise!

"Raise your hand" if you're back

We'll use Slido to collect your answers in real-time

Overview

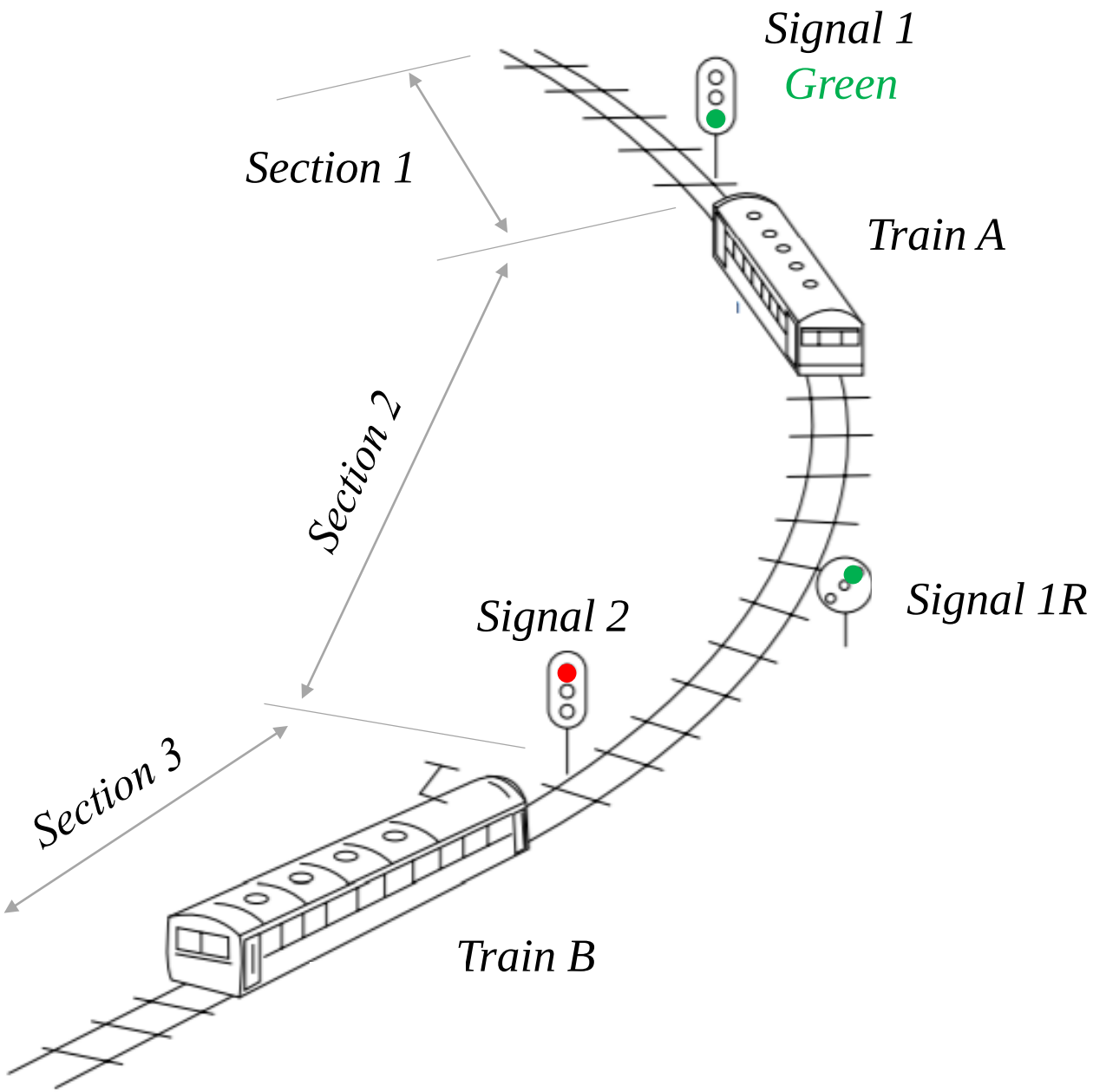


STPA Step 1: Purpose of the Analysis

Losses:
- L1: Loss of life
- Etc.

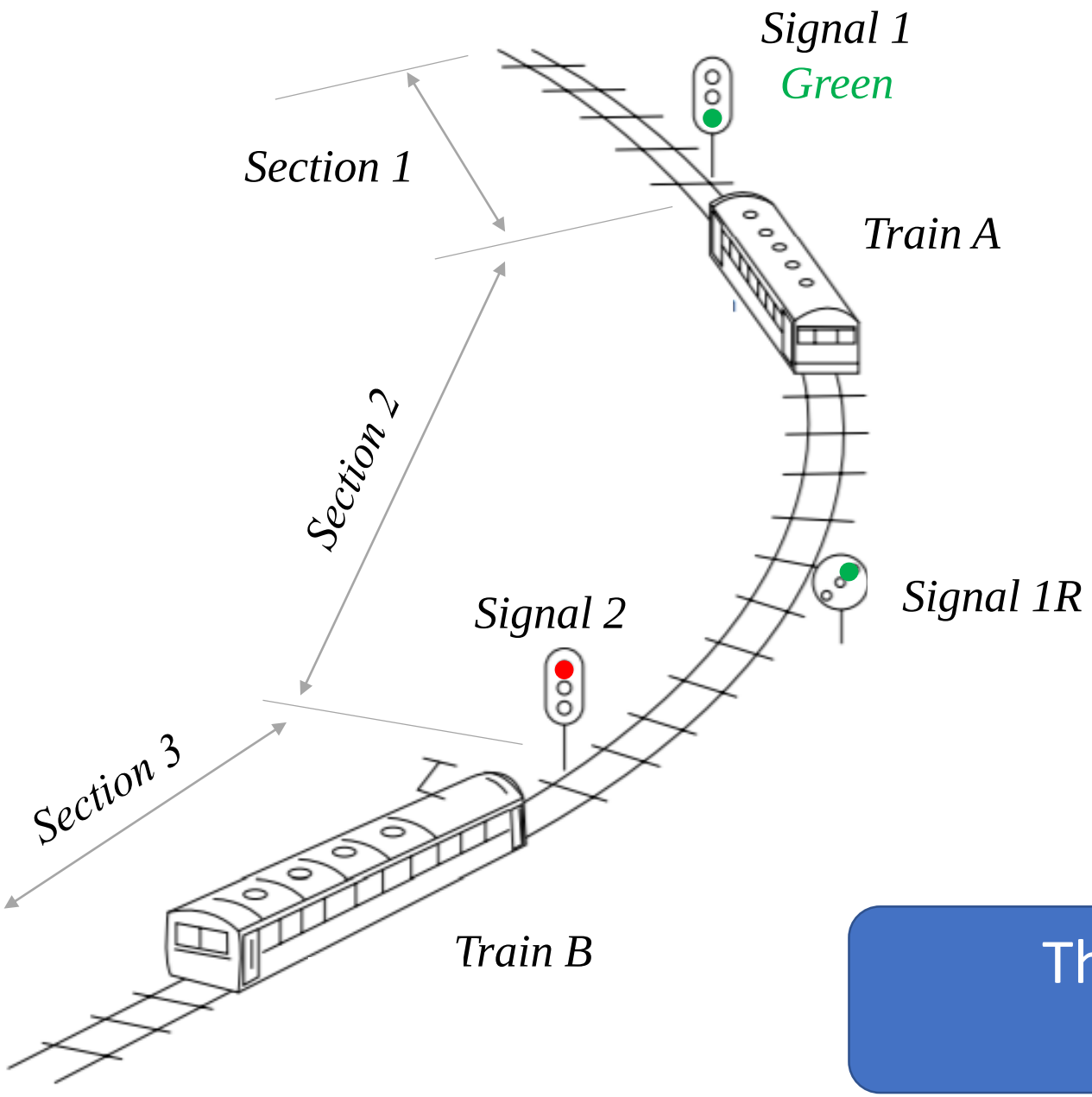
System-level Hazards:
- H1: Train violates minimum separation from other trains
- Etc.

Safety Constraints
- ?

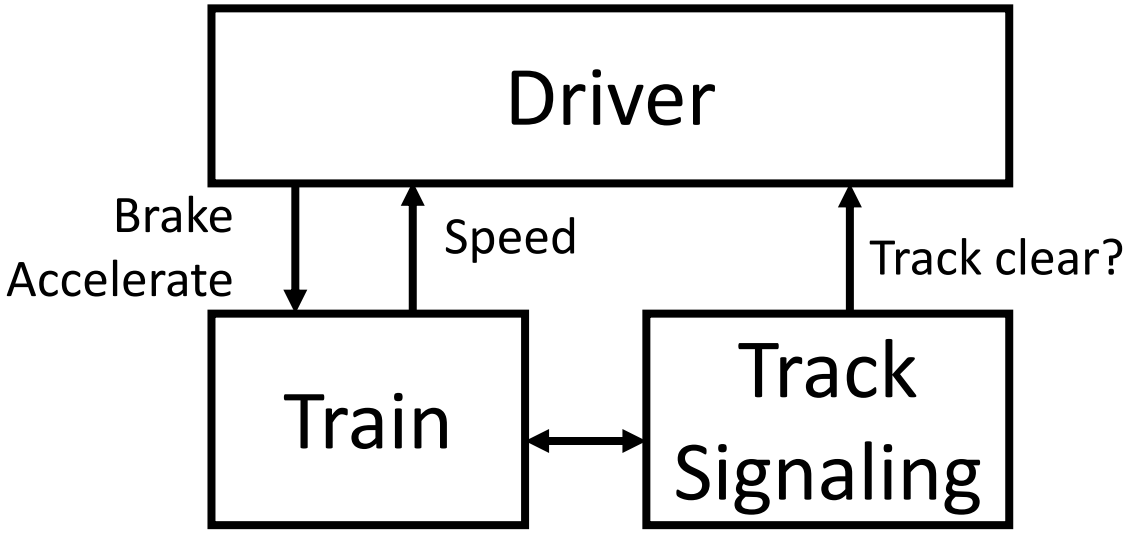


STPA Step 2:
Sketch the Control Structure

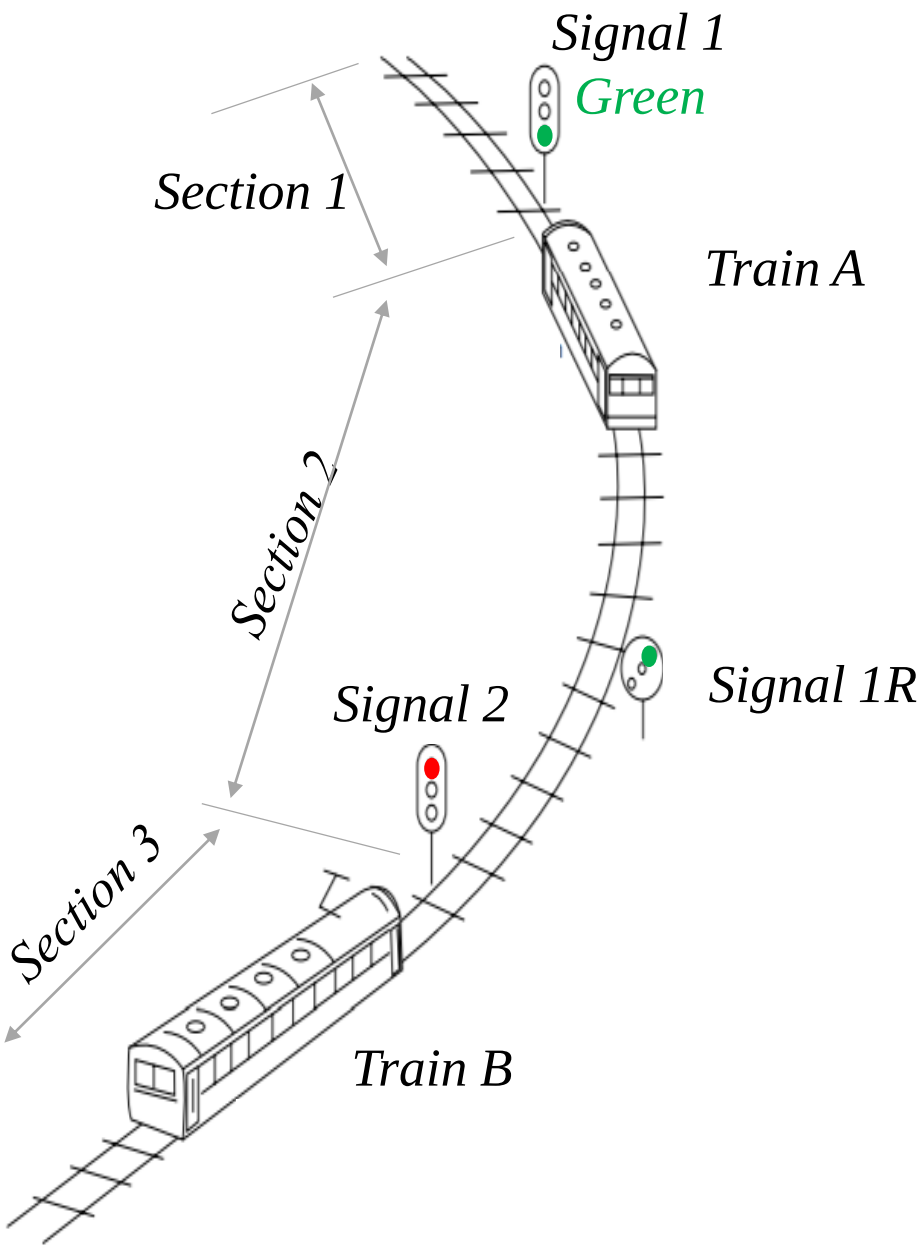
- Name the controlled processes
- Name the controllers
- Name the control actions
- Name the feedback



Simplified Control Structure



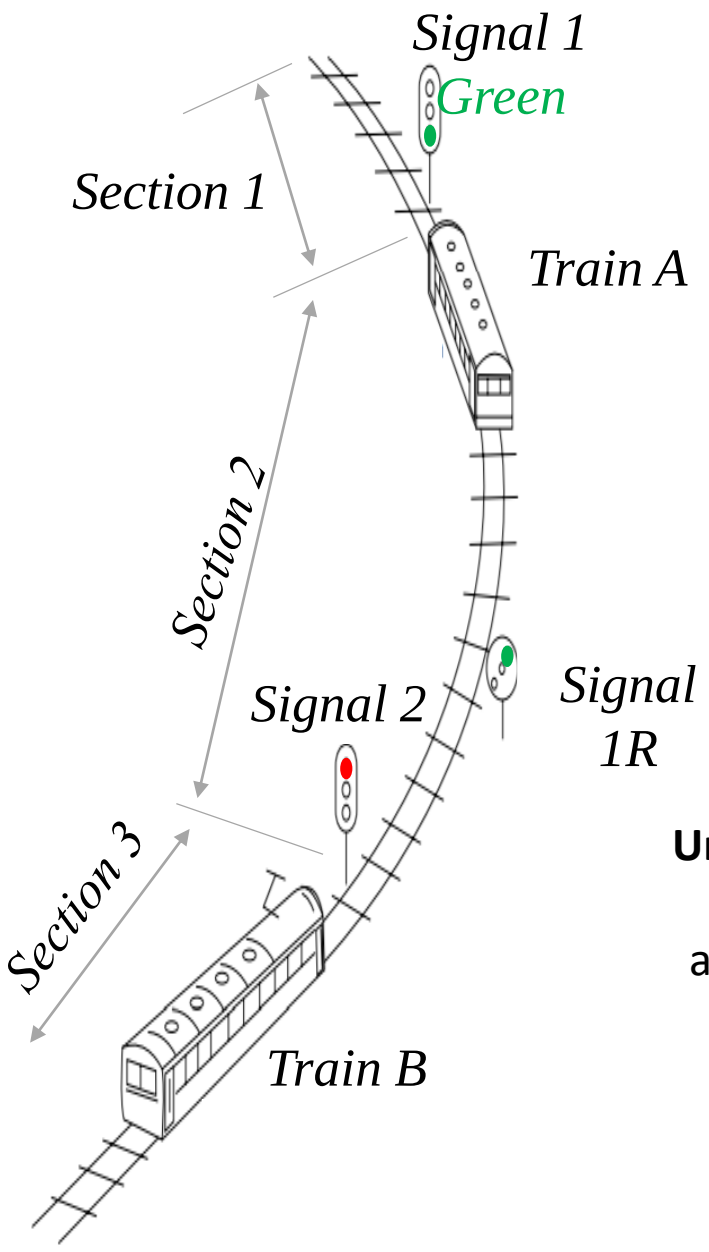
This is an oversimplified model !
But… is it still useful?

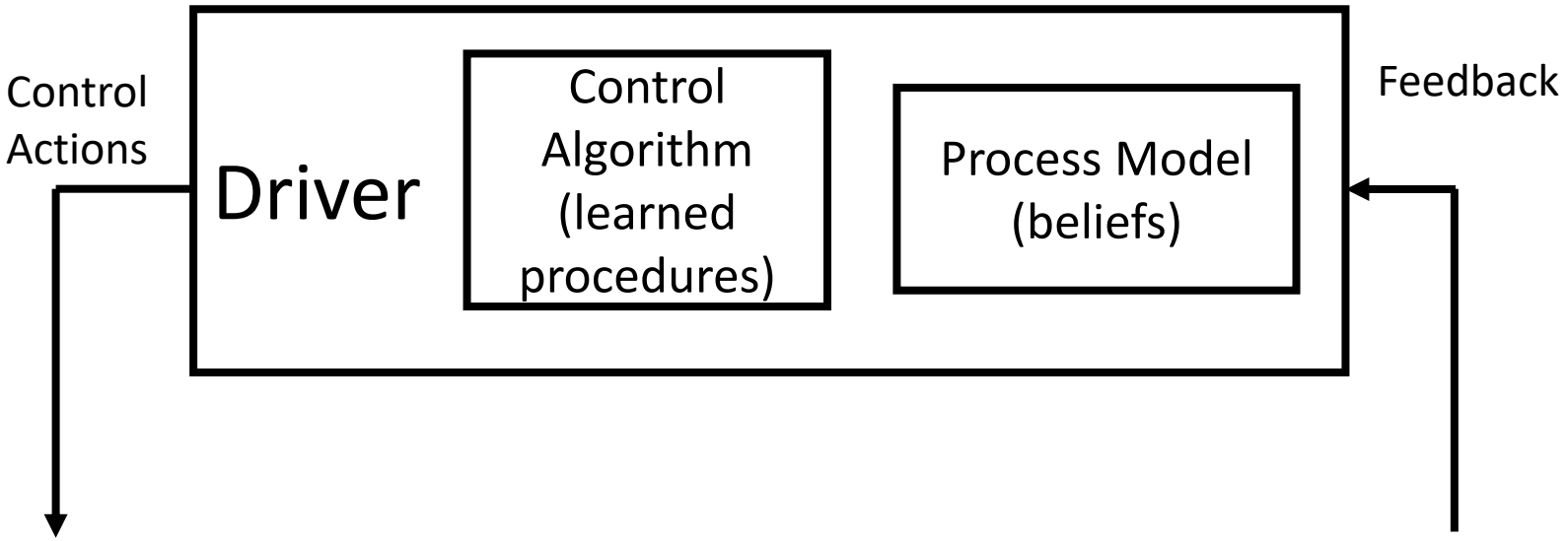


STPA Step 3:
Identify Unsafe Control Actions

	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped Too Soon / Applied too long
Brake Command	Driver does not provide Brake Cmd when _____	Driver provides Brake Cmd when _____	[...]	[...]
Accelerate Command	Driver does not provide Accelerate Cmd when _____	Driver provides Accelerate Cmd when _____	[...]	[...]

STPA Step 4: Build Scenarios



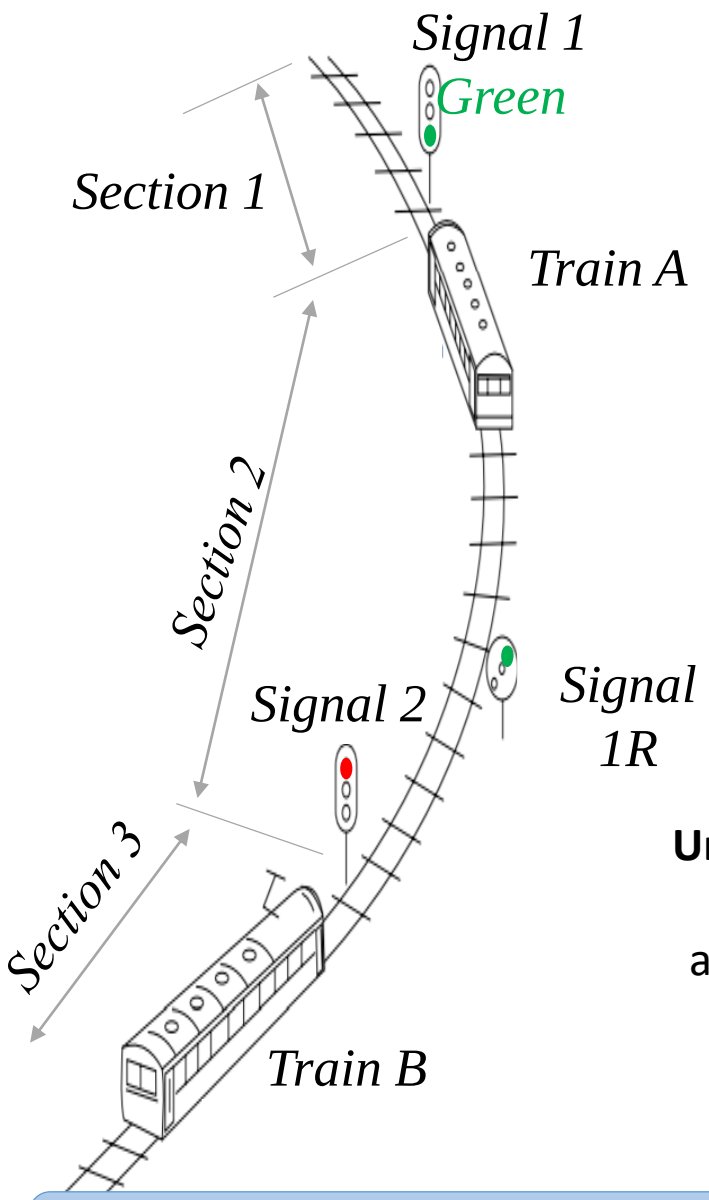


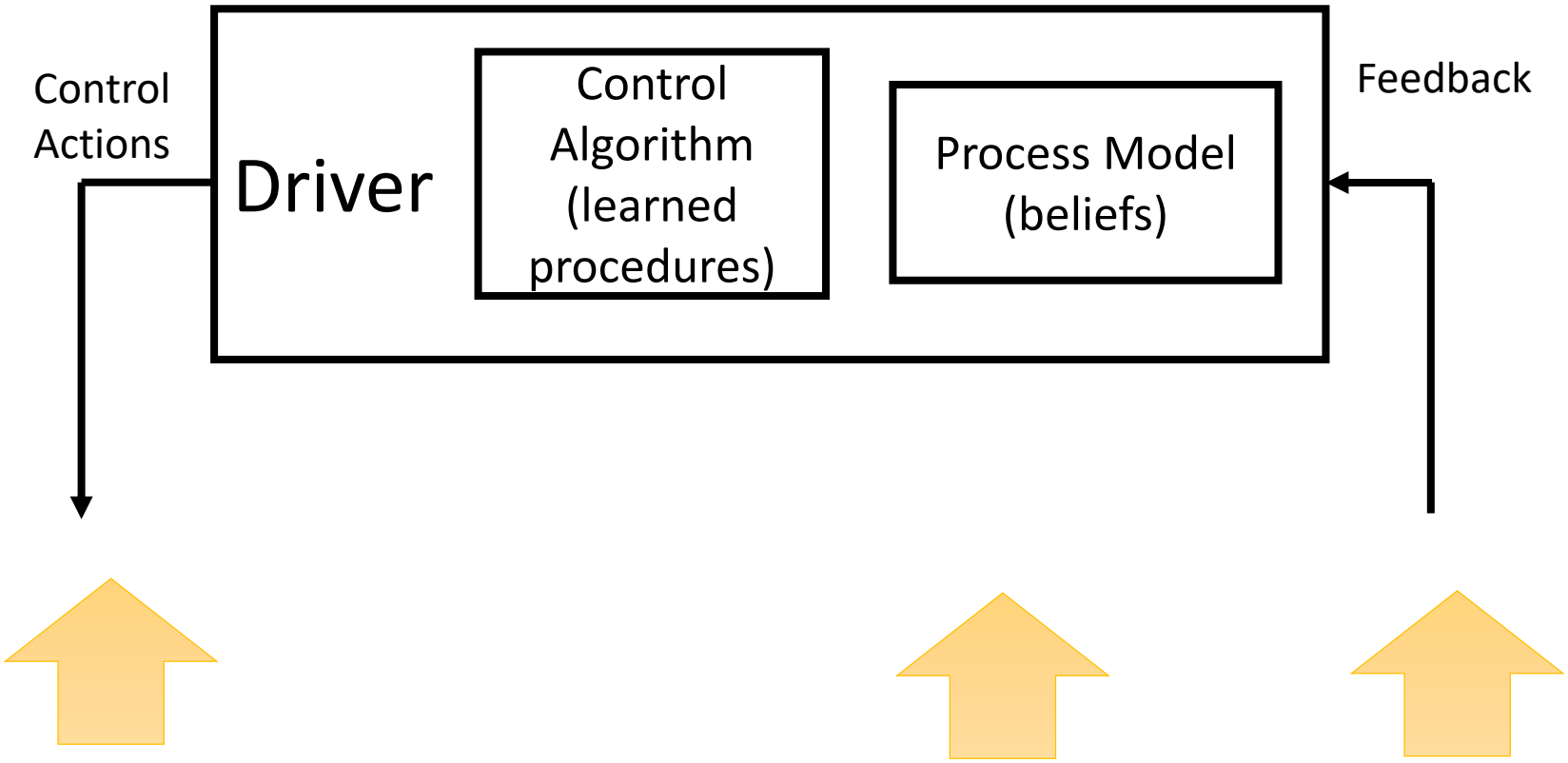
Unsafe Control Action: Driver provides accelerate cmd when track ahead is occupied

Process Model Flaw: Driver believes _____

Feedback: Driver receives feedback _____

STPA Step 4: Build Scenarios





Unsafe Control Action: Driver provides accelerate cmd when track ahead is occupied

Process Model Flaw: Driver believes track ahead is clear

Feedback: Driver receives feedback: signal is **green**

(Signal 1, 1R, or 2?)

Scenario #1: This explains why Driver B might accelerate into Train A if Train A&B already in Section 2.

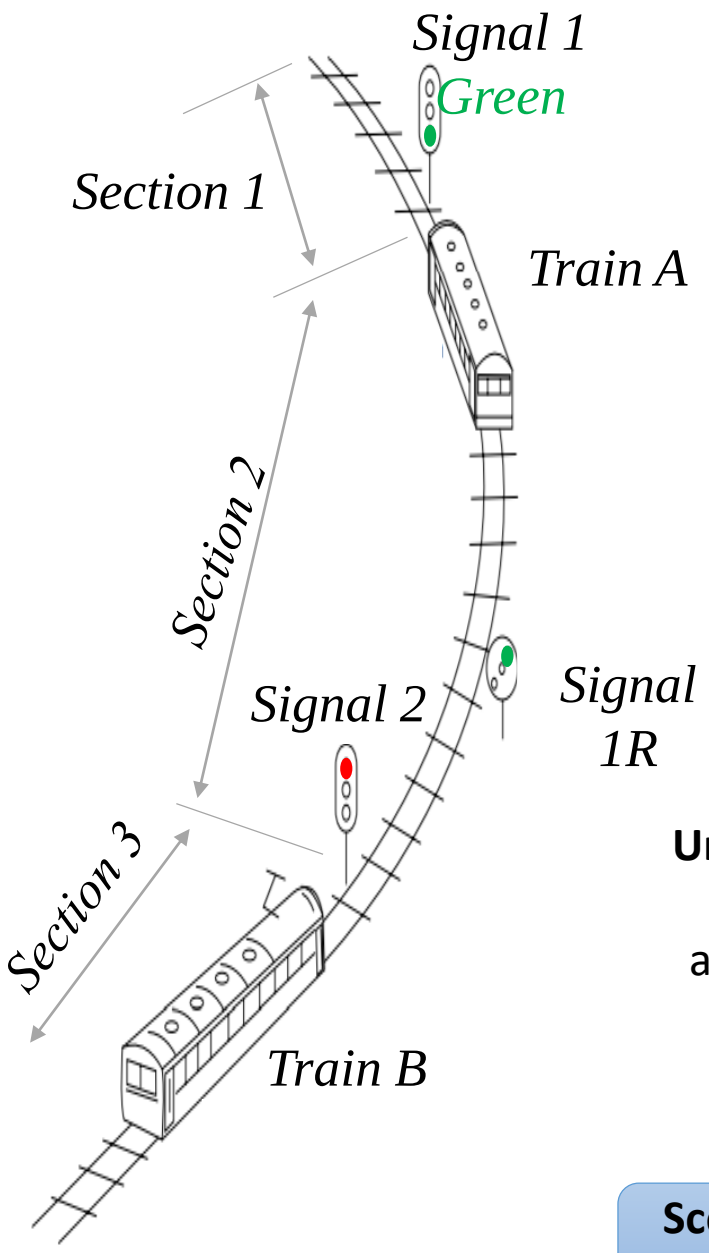
Controlled Process

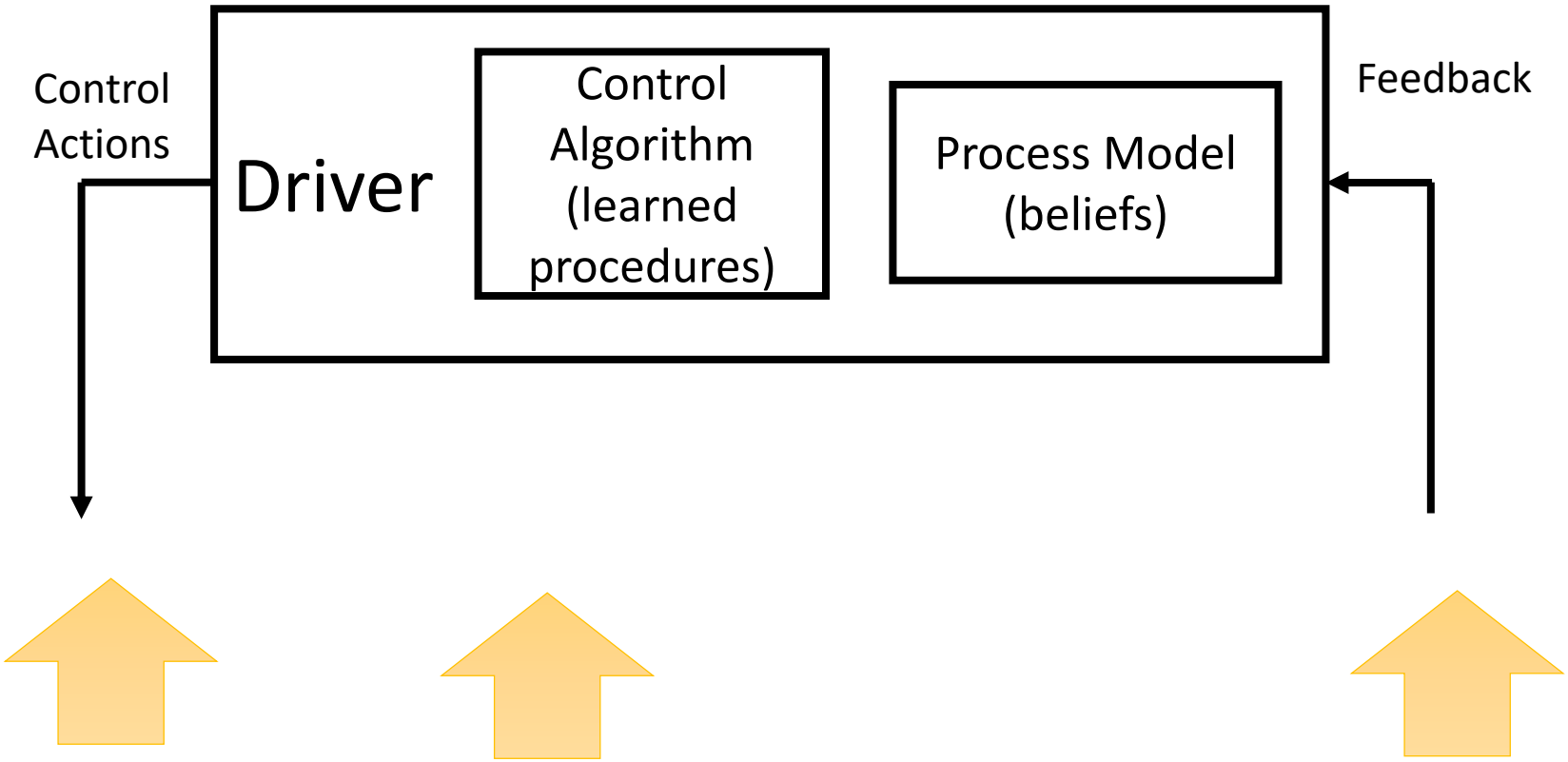
Signal 1R is green because Section 1 is clear (even if Section 2 ahead is occupied!)

Success!

You all just used STPA to identify Scenario #1

STPA Step 4: Build Scenarios





Unsafe Control Action: Driver provides accelerate cmd when track ahead is occupied

Control Algorithm (L Procedure) Flaw: There is a procedure to proceed through red lights after 1 minute at 20km/hr

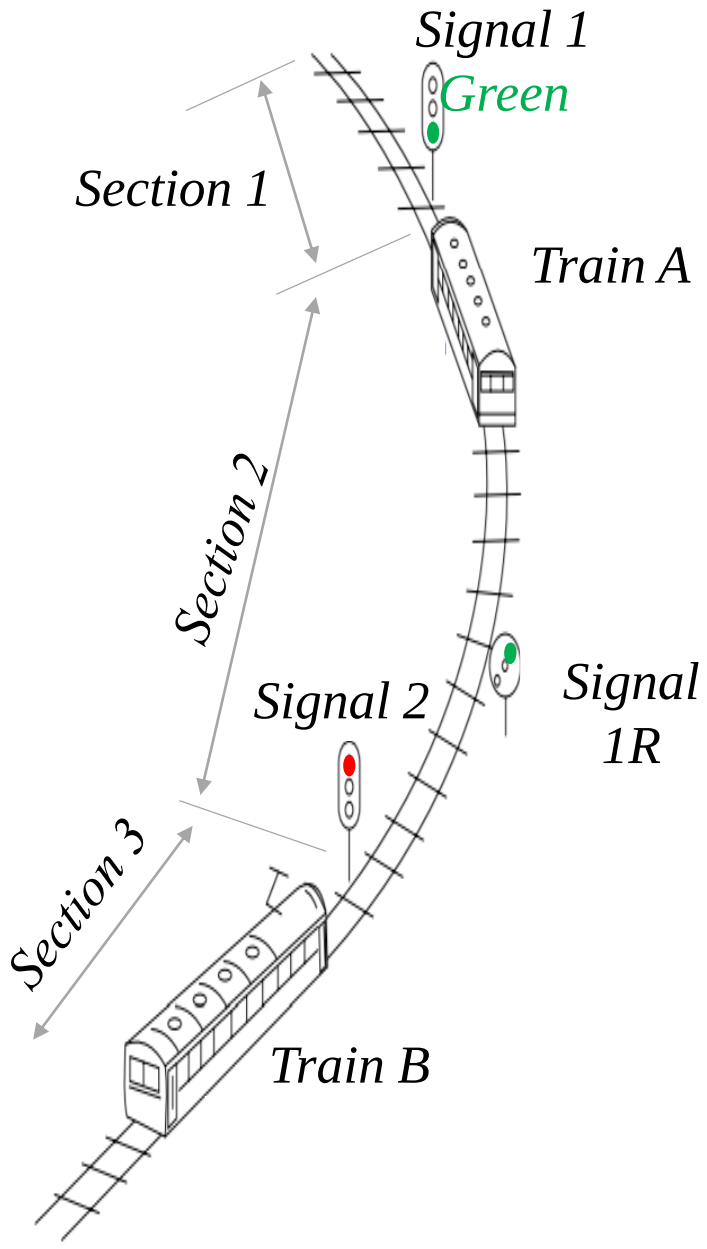
Feedback: Driver receives feedback: signal is **red**

Scenario #2: This would explain why a driver would pass Red Signal 2, resulting in Train A&B occupying Section 2. That would set the stage for previous Scenario #1!

Success!

You all just used STPA to identify Scenario #2

Identify Controls/Mitigations



Unsafe Control Action: Driver provides accelerate cmd when track ahead is occupied

Control Algorithm (L Procedure) Flaw: There is a procedure to proceed through red lights after 1 minute at 20km/hr

Process Model Flaw: Driver believes track ahead is clear

Feedback: Driver receives feedback: signal is green

Driver receives feedback: signal is red

Controls, Design Features, Procedures, Training Cases, Mitigations?

- **?**
- **?**
- **?**
- **?**

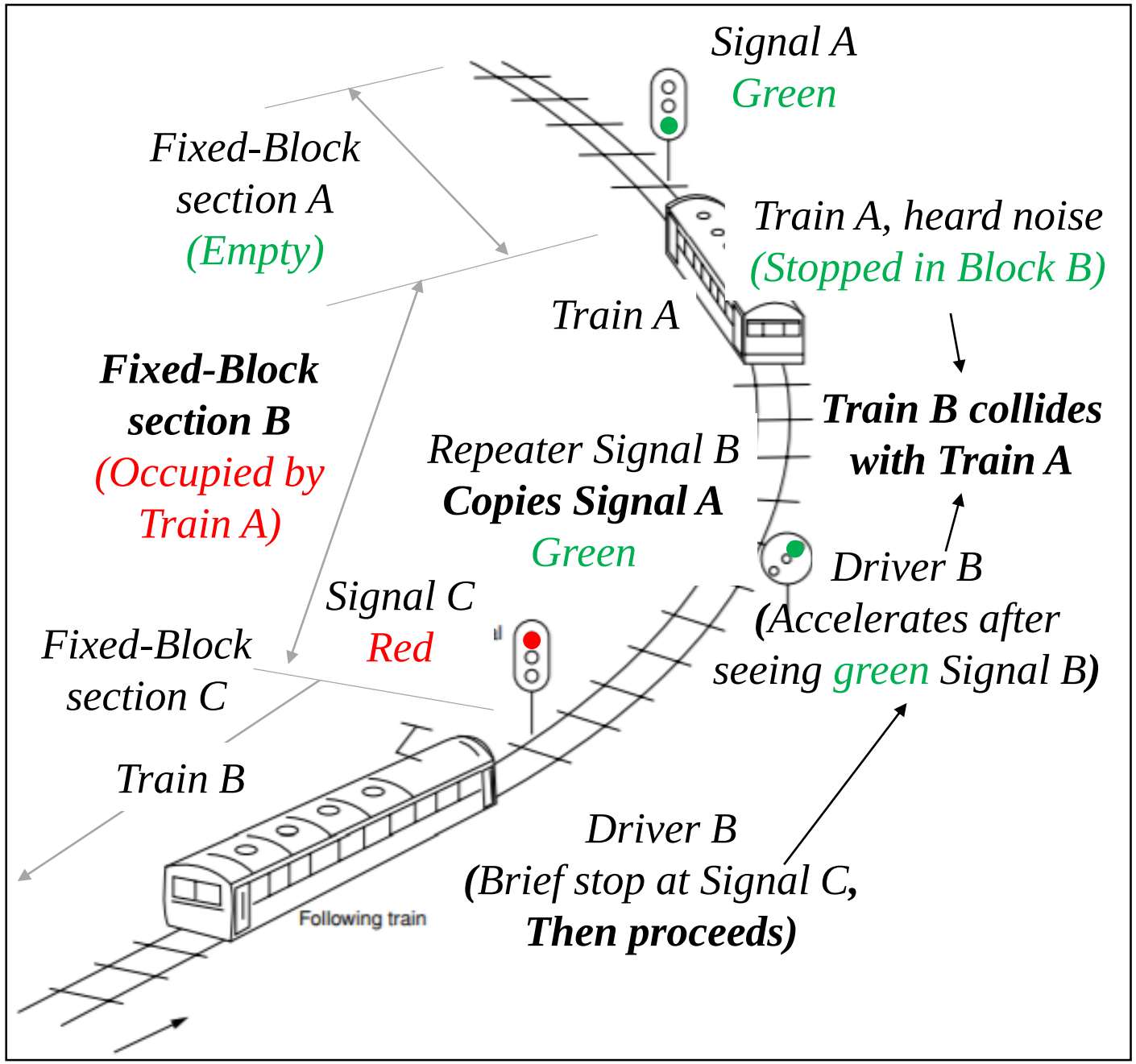
STPA Homework
A Railway accident in Japan
(Among the safest railway system of world)

(Kagoshima line accident, Japan, 22 February 2002)

Nikhil Bugalia, PhD

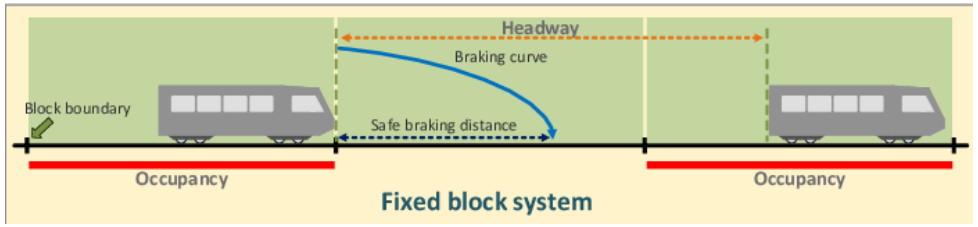
nikhilbugalia@gmail.com

Overview of the accident



- Driver A applies brakes to Train A, after hearing a noise as if something stuck the train (probably an animal crossing the track)

- Signal C, is showing Red, as the Fixed-Block section B is occupied by Train A.

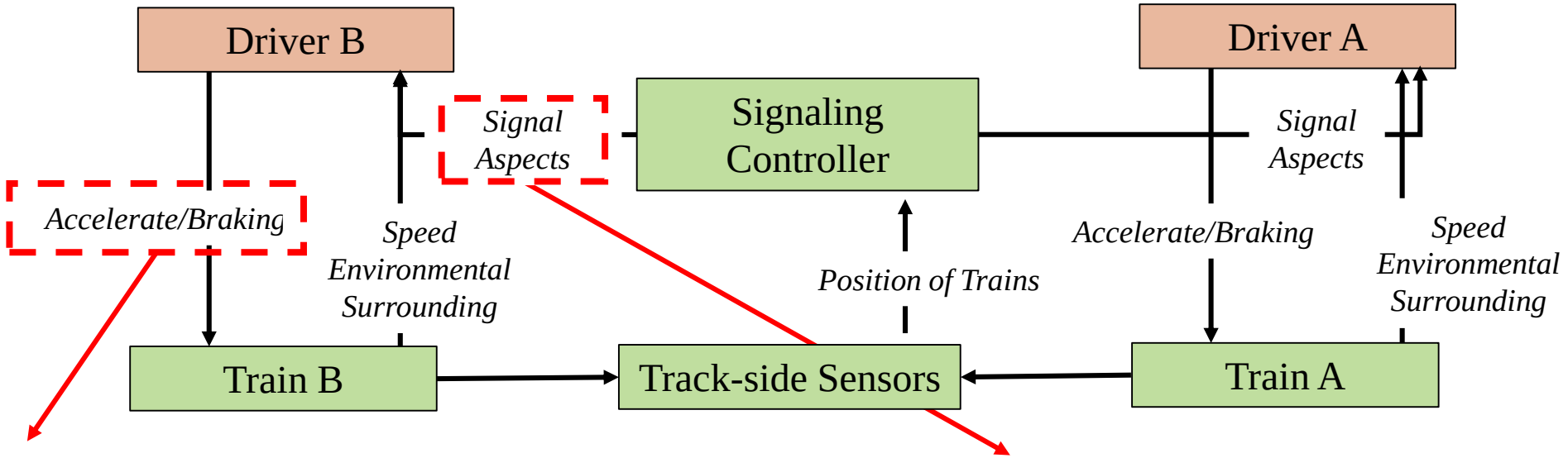


Signal shows red, if the track-block ahead is occupied

- Driver B, stops at Signal C, then moves at a slow speed after stopping for 1 minute

- Driver B, observes repeater signal B, which is showing a green-signal. Repeater signal, mimics the aspect of the signal ahead, and is installed at curves. Since there is no train in Section A, this aspect is "Green"

- Driver B, accelerates after seeing repeater Signal B, and rams into the stationary train A.



- **UCA 1 – Train Driver accelerates when Signal Aspect shows "stop"**

- Why would it make sense for the Driver to accelerate when signal aspect shows "stop"?

  ~~a) Driver makes a mistake (Signals Passed at Danger)~~

  b) Driver was asked to do so by his supervisors

- The railway company had a rule, to stop the train for 1 minute, and then proceed at a slow speed. Why?
- The long-waiting time of each train in a fixed-block system may introduce huge delays to other trains, when track reaching its capacity. Hence, such a rule was made to reduce the delay. Introducing such a rule was cheaper than changing the signaling system.

- **UCA 2 – Signaling Controller provides "Green Signal" when a train is present on the track ahead (<TBD mtrs.).**

- Why would it make sense for the signaling controller to provide "green signal" when a train is present on the track

  ~~a) The train ahead is not detected~~

  b) When the signal is designed to do so

- The repeater signal is designed to mimic the aspects of the next main signal. Its aspect is not based on the conditions at the track immediately ahead. (often used on curves, to assist drivers for seeing the next main).