SFM '21 | SHAPING THE FUTURE OF MOBILITY

COMBOIOS DE PORTUGAL | CRP CENTRO RODOFERROVIÁRIO PORTUGUÊS | Infraestruturas de Portugal | UIC INTERNATIONAL UNION OF RAILWAYS

#EUYearofRail

Equipment and services in the transport of the future

Railway safety in an increasingly automated world

Luis Gargaté, Critical Software

Automation vs Safety

ATO

ERTMS / ETCS

Conventional ATP

How will the Transportation industry move to a greater level of automation, and what will be the role of the railway industry?

Systems and software engineering company

Pioneers in safety-critical embedded software development and testing

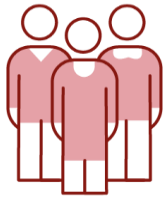
Founded in 1998 with NASA as the first client

Three Main Divisions: High-Integrity Systems, Smart Technology Solutions and Digital Engineering Services

Why: To help build a better and safer world

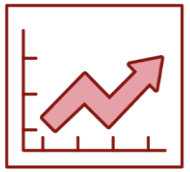
How: Through a strong **culture** and community of **experts**, **passionate** about taking on the world's most demanding **challenges**

What: We engineer dependable, transformative and trusted technologies



1000 +
employees

Global
vision

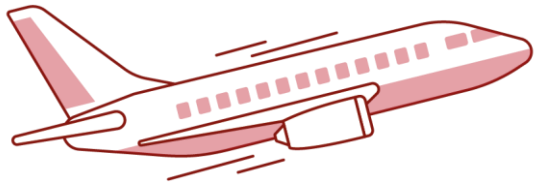


Growth
& reinvestement

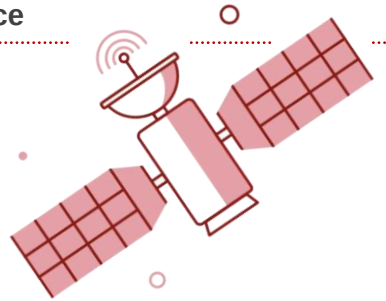
High-Integrity Systems

We provide systems, software and services for mission- and business-critical applications.

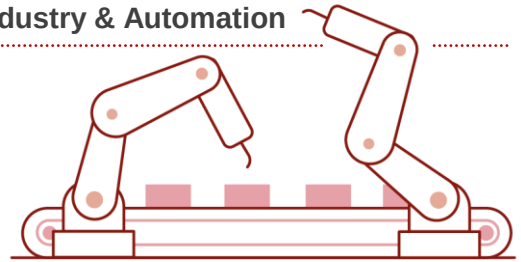
Aerospace



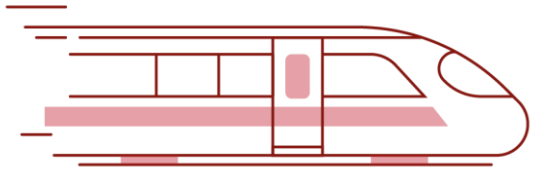
Space



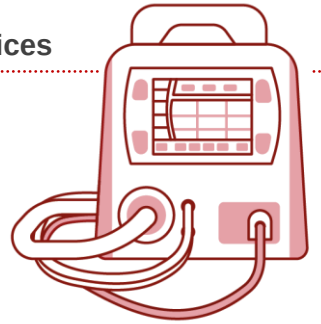
Industry & Automation



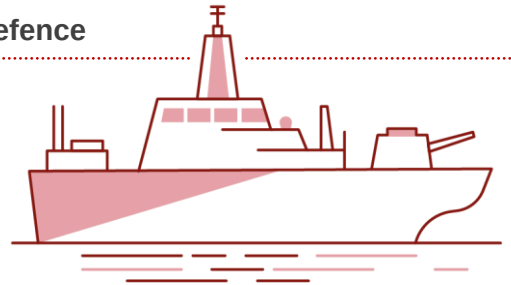
Railway



Medical Devices



Defence



Automotive

Aeronautics

- Pilot-supervised auto-pilot (climb, cruise, descent);
- System can degrade under certain conditons and Pilot needs to take over;
- ILS CAT III C – plane can land and stop on the runway autonomously (3 auto-pilot Systems engaged, pilot, airplane and runway need to be certified);
- Safe return emergency Autoland (Garmin / Cirrus Vision Jet);
- https://www.youtube.com/watch?v=PiGkzgfR_c0

Railway

GoA 1

GoA 2

GoA 3

GoA 4

Increased automation levels

More controled enviornment

Two main subjects to discuss…

Safety with…

Humans-in-the-loop in supervised systems

- Human factors
- User Interaction Design & Human error
- Higher automation and better automation

The road to…

Largely unsupervised (safe) systems

- Artificial Inteligence
- Machine learning
- Predictability and safety…?

Supervised Systems

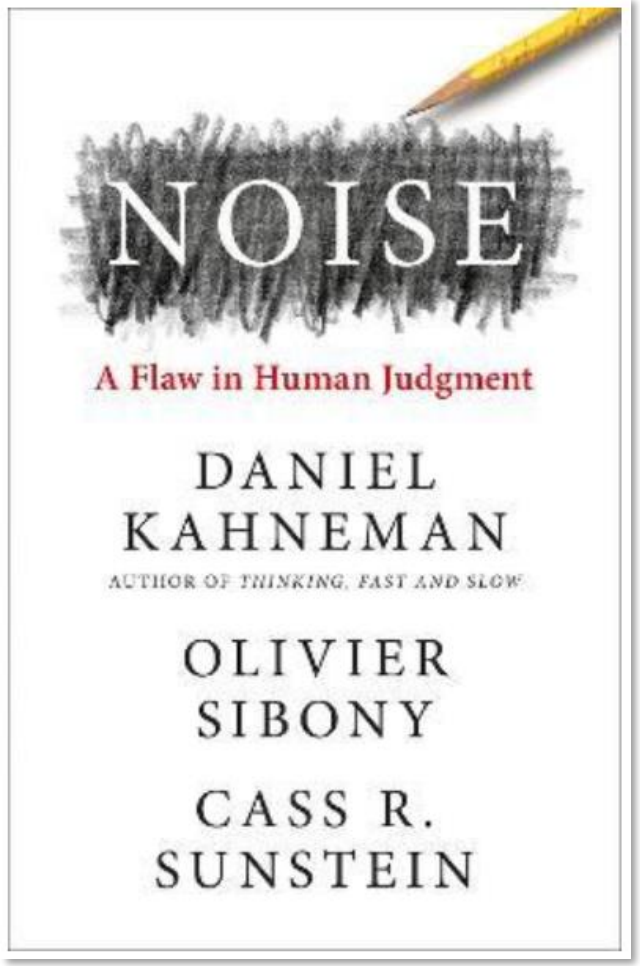
Time, measured in years…

Unsupervised Systems

Supervised Systems

- Humans are not very reliable (e.g. book on the right)
- Humans can be trained, but…
- … technology often progresses too fast;
- … cost pressure works against us;
- … factors like stress (too high or too low!), perception errors, sleep deprivation work against us;
- And this is why, generally, automated systems increase safety.

Human failure rate
$3{,}5 \times 10^{-3}$

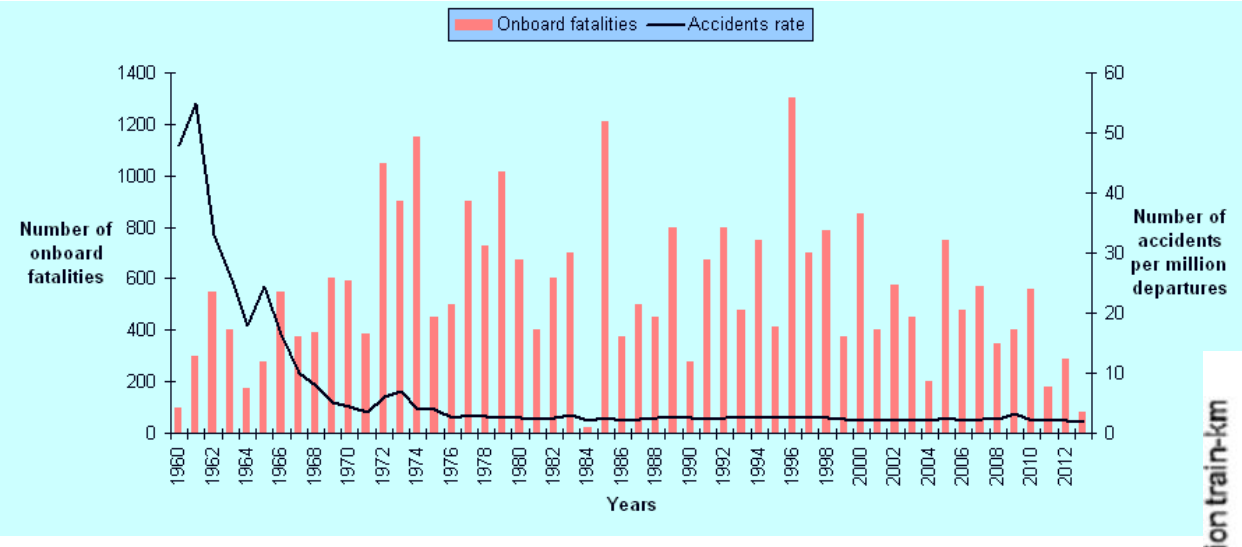


Is more automation always better?

Only if safety is at the core of system design.

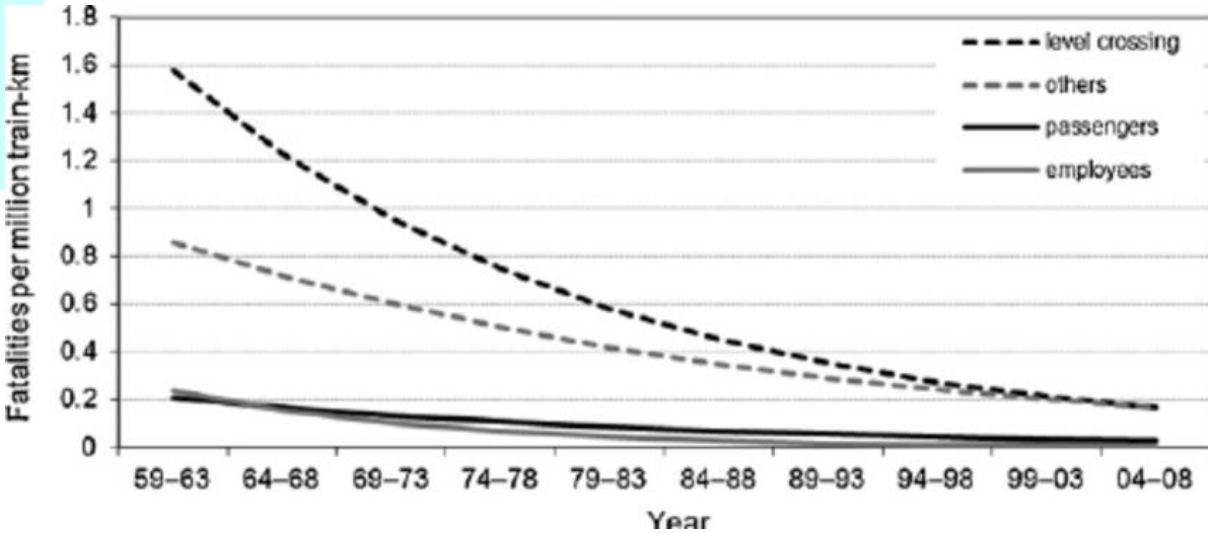
A 100% safe System does not exist.

(Parentesis – safety IS increasing)



Railway

Aeronautics



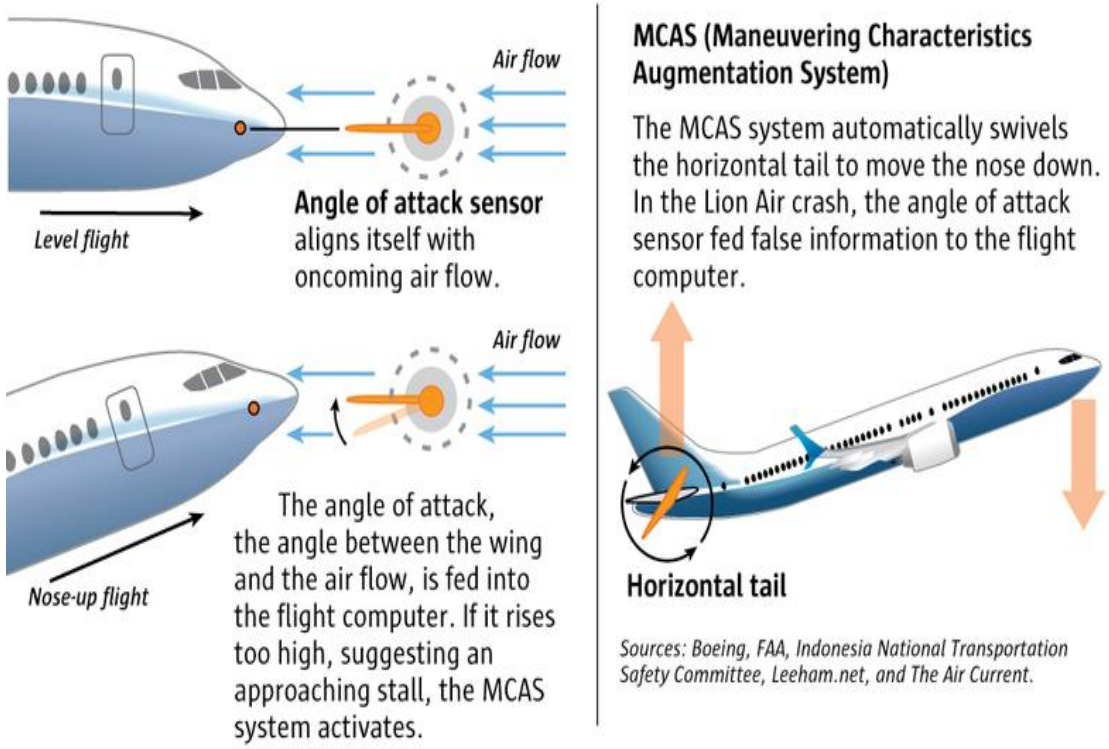
(both are safer than walking)

Human factors and UxD in safety

UxD & Automation as contributing factors to accidents – two examples

Boeing 737 MAX 8

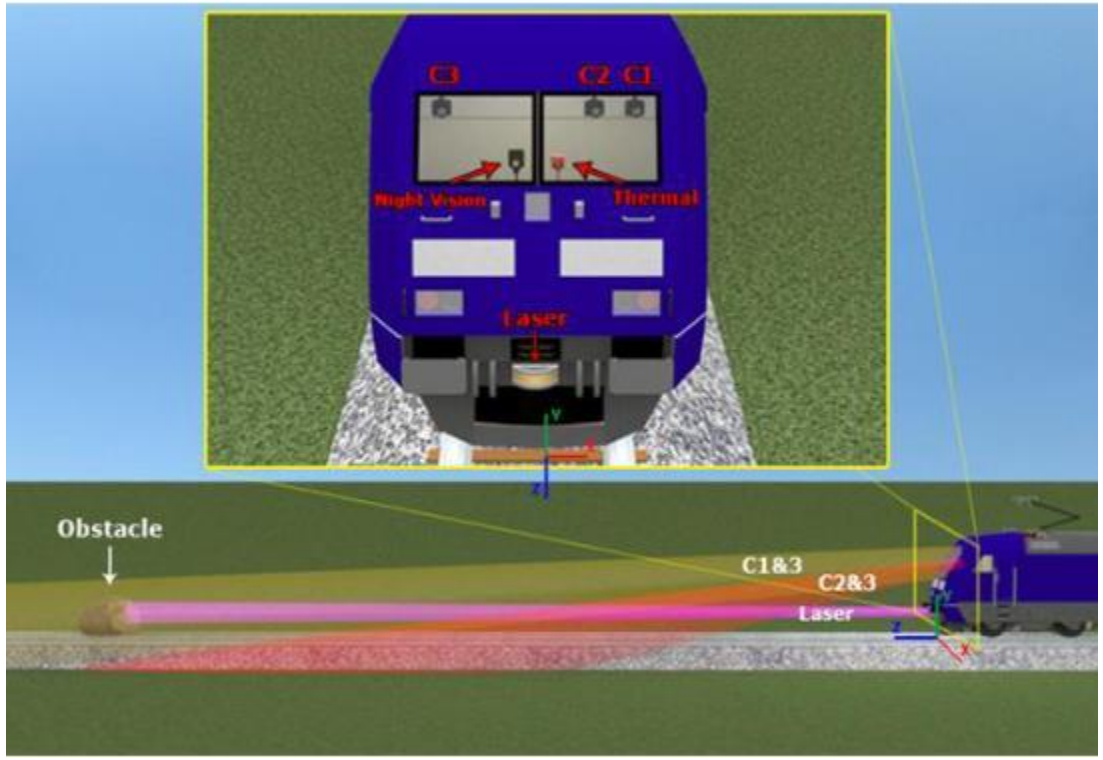
Lion Air Flight 610 & Ethiopian Airlines Flight 302 / 2019



Airbus 330-203

Air France 447 over the Atlantic / 2005

Enhancing safety – a railway domain example



Shift2Rail project example
Ref. Ares(2019)777843 - 10/02/2019

A system for obstacle detection and avoidance

- Several types of sensors (infra-red, night vision, lidar, …);
- Sensor fusion and software;

Questions:

1) How can you test the system thoroughly given environmental conditions? (snow, fog, smoke, glare, …)
2) Limitations of a system like this?
3) Or in short: how to get to an appropriate SIL level (2 to 4)?

Safety implies not only having a consistent and strong system design but also being able to prove that the system performs according to requirements.

Largely unsupervised systems – dealing with a very large number of scenarios

A "open" environment becomes unpredictable… → Hazard log can increase exponentially;

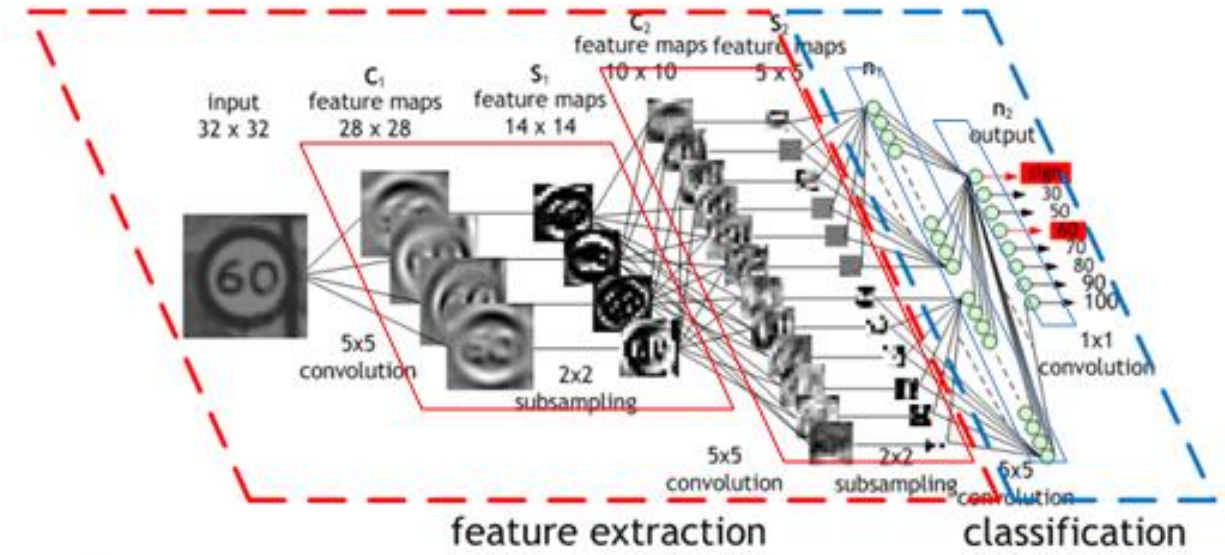
Can a camera system detect a white obstacle in snow conditions?
What about fog? What about fog and snow?
How much snow?
…
(list goes on) → Number of test case scenarios tends to infinity

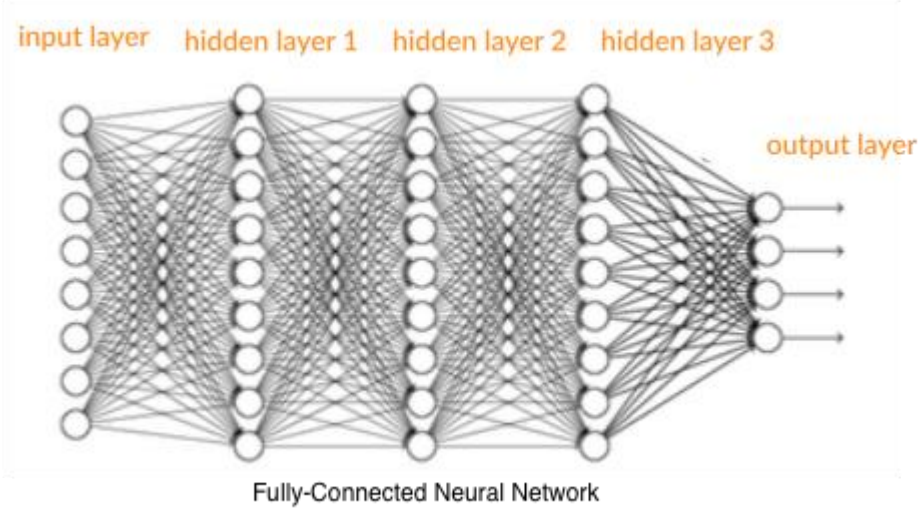
→ The algorithms themselves are unpredictable because they are strongly non-linear (e.g. neural networks / AI / learning algorithms)

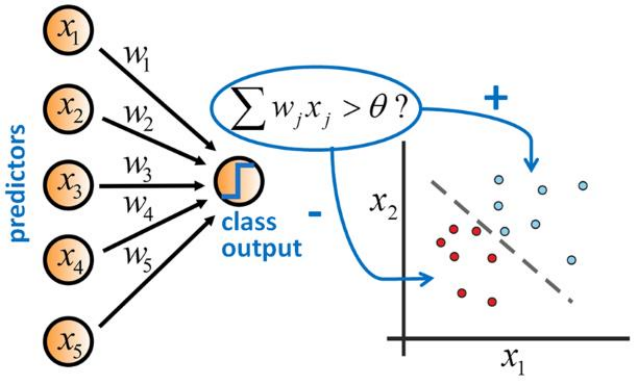
That is: although the algorithms work and we can show they work under certain conditions, it is almost impossible to show that they work under ALL conditions.

→ *The only option is to show that a system is safe because statistically it has less accidents in real-world conditions.*

Supervised training of a neural network for image recognition







Training set Images are shown to the network

Weights are adjusted

"Trained" network is a system with tuned weights on each neuron, that hopefully classifies well a very large number of new cases.

The leading role of railway systems

Bottom line:

1. *It is either possible to isolate a system enough such that predictable algorithms can be used… or*
2. *Complex systems using neural networks or other AI algorithms need to be employed. These are not deterministic, and safety cannot be easily assured.*

Isolation is the main reason why Light Railway systems are at the forefront of unsupervised automatic operation.

But how will we get to unsupervised systems in main lines (and in open environments like roads)?

We will need to deploy these non-linear "unpredictable" algorithms in the wild and statistically prove they are safer than humans.

Some conclusions and takeaways

Automation has an important role in safety and automation that will continue to increase.

But achieving unsupervised system operation in most environments is still very much in the future…

Achieving these systems will imply in many cases (maybe, except, in the railway domain) accepting that these systems will fail and accepting they will not be completely predictable and 100% safe.
We will need to accept that they will be only statistically better that humans.

Will we be able to accept this to move forward?

How will we solve issues like liability when such a system fails and lives are lost?

SFM 21 | SHAPING THE FUTURE OF MOBILITY

Critical software

Thank you!

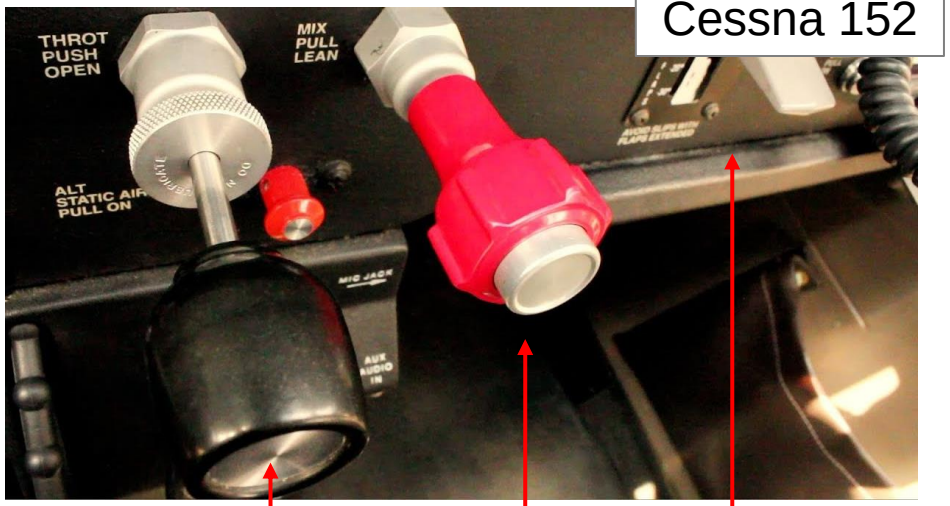
Luis Gargate

Business Development Director

lrgargate@criticalsoftware.com

An example in (old) avionics system design

Cessna 152



Engine power control | Mixture control | Flap control

Can you spot the design differences and any influence on safety?

Cessna 150

Engine power control | Mixture control | Flap control