

# Safety in a Changing World

## The Case for Human-Centred Dynamic Safety Cases

IEEE Let's Meet - Bruges

Laure Buysse

# Who am I?



- Dual Specialisation in EO and ICT (Engineering Technology)
- TETRA (Technology Transfer) Safety Assurance in Industry 4.0:
  - Cooperative Robot
  - Autonomous Mobile Robot (AMR / AGV)
- FWO PhD Fellowship Strategic Basic Research
- Research:
  - Safety of Autonomous Systems ; Robotics
    - Safety cases ; Hazard analysis techniques
  - Safety of Artificial Intelligence
  - Digital Twins

A 3D rendering of a warehouse conveyor belt system. The scene shows a central conveyor belt with several cardboard boxes moving along it. The boxes are brown with white labels and some have recycling symbols. Red laser lines form a grid on the floor, indicating a navigation or tracking system. The lighting is bright, and the overall aesthetic is clean and futuristic.

# Autonomous Systems



A photograph of an Amazon Hercules robot in a warehouse. The robot is a tall, yellow, cylindrical structure with multiple shelves, mounted on a blue base with wheels. It is positioned in a large, industrial space with high ceilings and metal beams. In the background, there are other similar robots and a yellow pillar with the number '2B 13' on it. The text 'Hercules Robot' and 'Amazon' is overlaid on the image in white, bold font.

# Hercules Robot

## Amazon



**Autonomous Taxi**

**Waymo**



A wide-angle photograph of a modern automotive assembly line. The scene is filled with industrial machinery, including overhead conveyor systems and robotic workstations. In the foreground, a silver car chassis is being processed by a robotic arm. The background shows multiple lanes of the assembly line stretching into the distance, with various components and parts visible. The lighting is bright and industrial, highlighting the metallic surfaces and the organized layout of the factory floor.

# Semi-Autonomous Assembly Line

**General Motors**

# A Revolution for Industry

## Autonomous systems

- Systems, machines, robots...
- Operating independent based on previous and current inputs

Boost in Productivity

Improved Safety

Less Mundane Task for Humans

Extend human capabilities

Cost Efficient

Multi-Functional

But ...

## Industrial robot crushes man to death in South Korean distribution centre

Tesla Autopilot feature was involved in 13 fatal crashes, US regulator says  
Machine apparently identified man inspecting it as one of the boxes it was stacking

BBC

Safety (assurance) is still a major roadblock in designing, developing and deploying these systems.

staff injuries'

30 September 2020

## Amazon Drone Crashes Kill Jeff Bezos' Delivery Dreams

Billions of dollars and a decade later, and Amazon's delivery by drone program still isn't off the ground.

badly delayed  
officials say

Share  Save 

...e, the robotaxi firm, denies the city's claims its vehicle  
...ed ambulance which resulted in injured person's

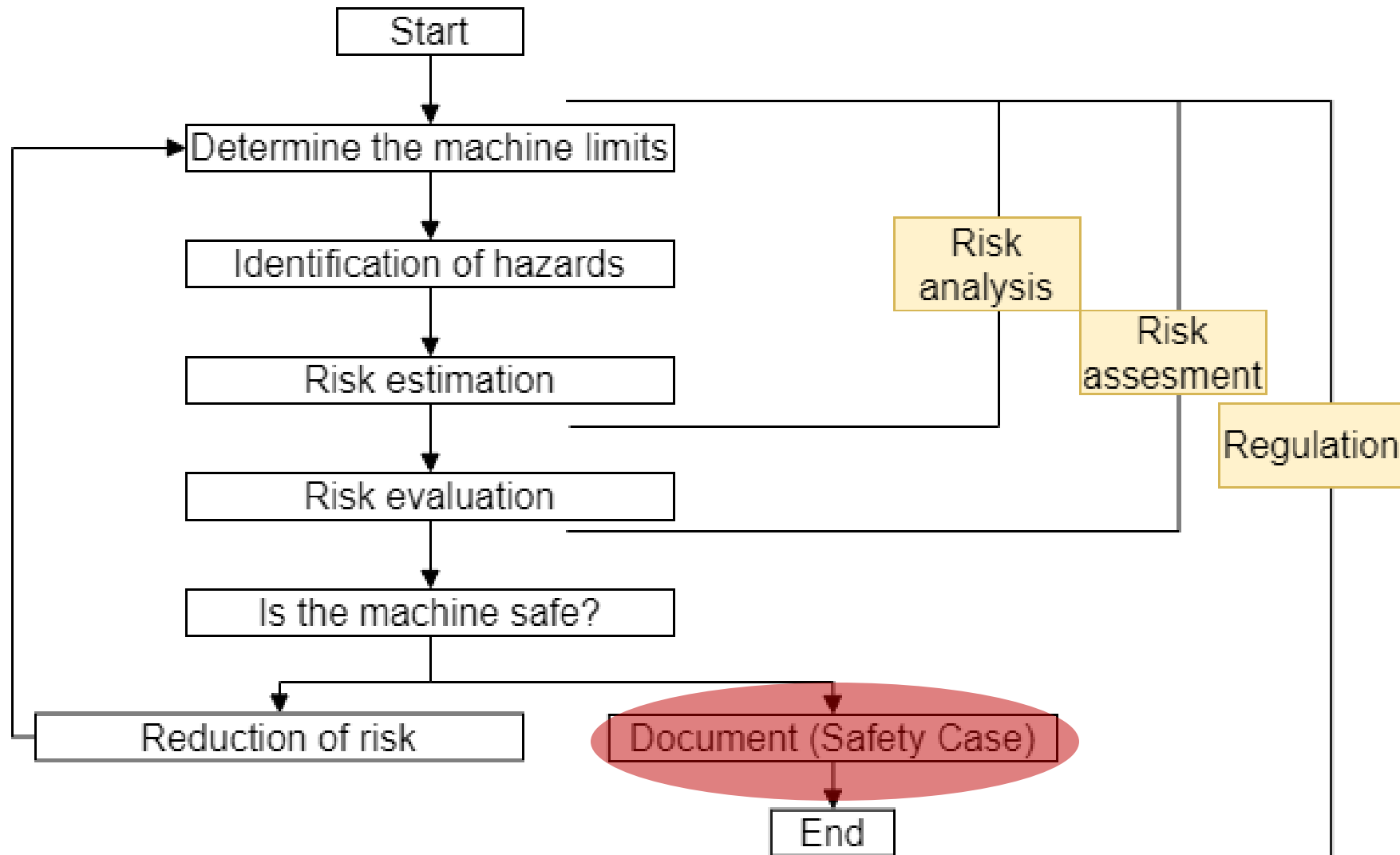




A 3D rendering of a warehouse conveyor belt system. Several cardboard boxes are positioned on the belt, moving away from the viewer. The boxes feature various labels, including barcodes and a prominent 'FRAGILE' warning. A red laser grid is overlaid on the scene, creating a perspective view of the floor and the boxes. The lighting is bright, highlighting the textures of the cardboard and the metallic components of the conveyor.

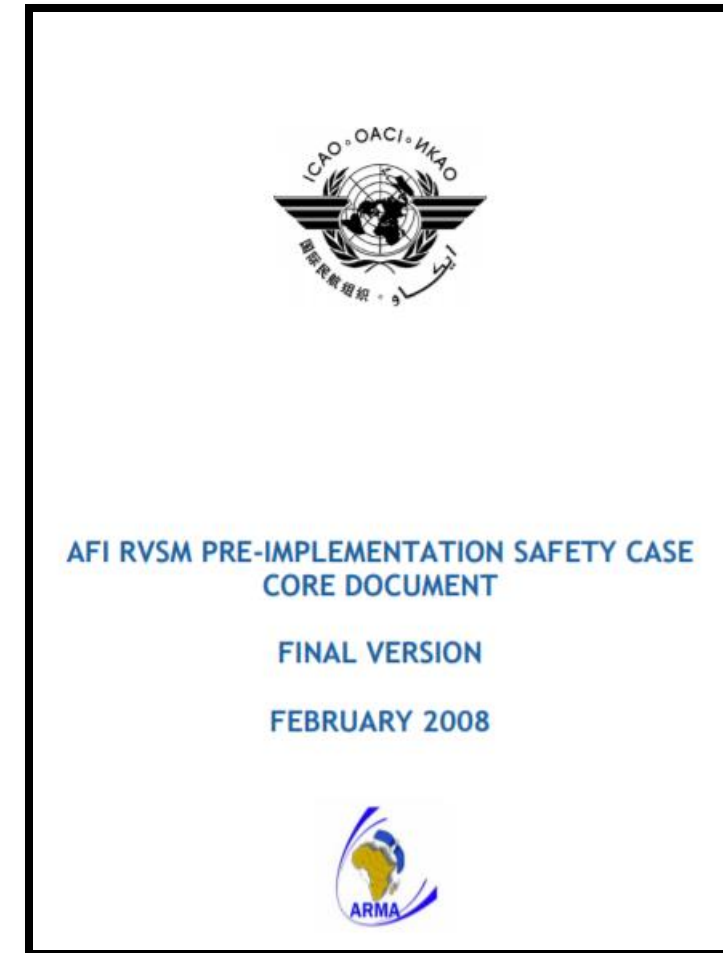
# Safety Assurance

# How to



# What is a (static) safety case?

- Contents:
  - Claims about property/system
  - Arguments logically linking evidence and assumptions to the claim(s)
  - Evidence and assumptions supporting the arguments
  - Justification of the choice of top-level claim and the method of reasoning
- Structure not universal (! Sector specific standards !)
- Requires a safety analysis



# Safety Cases – They seem perfect ...

- Difference between the actual, the depicted and the explained

The gap can lead to “**a culture of ‘paper safety’ at the expense of real safety**”.\*

- Our initial state of belief in safety is based on predictions and assumptions. We should always be aware of uncertainty and the fact that we are designing under imperfect knowledge.



# Safety Cases – They seem perfect ...

- The content of a safety case contains many different elements, such as
  - System design
  - System configuration
  - Intended environment
  - Identified hazard
  - Risk mitigation principles

All of these can, and often do, **change**, especially when dealing with autonomous systems. Moreover, **modular system** show great variation by default and all **different domains and environments** need to be included.

A 3D rendering of a warehouse conveyor belt system. The scene shows a central conveyor belt with several cardboard boxes moving along it. The boxes are brown and have white labels with barcodes. The floor is a dark blue-grey color with a red grid pattern overlaid on it. Red laser lines form a grid on the floor, and some boxes have red laser lines projected onto them. The perspective is from a low angle, looking down the length of the conveyor belt. The lighting is soft and even.

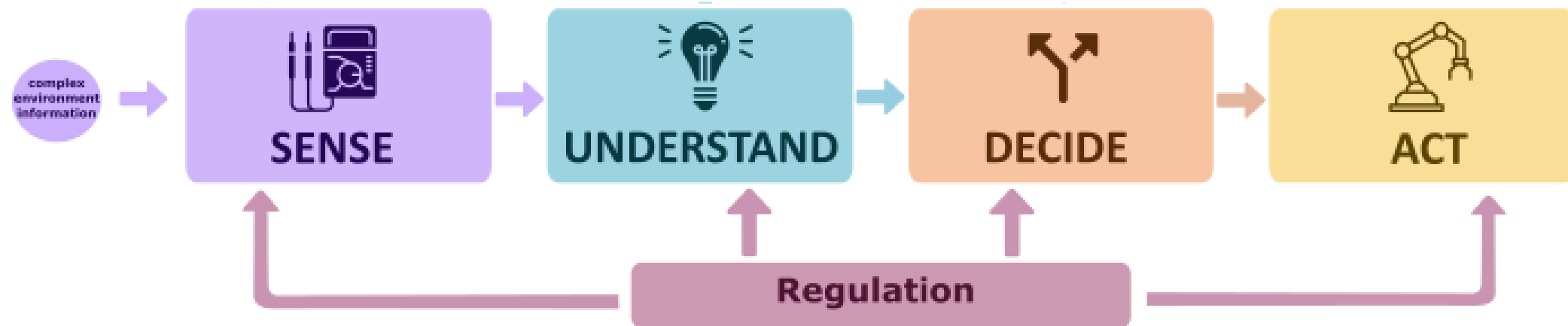
# Dynamic Safety Cases

# Dynamic Safety Cases

*To continuously assess confidence in the validity of the safety case through-life and proactively update the arguments and reasoning of the safety case*

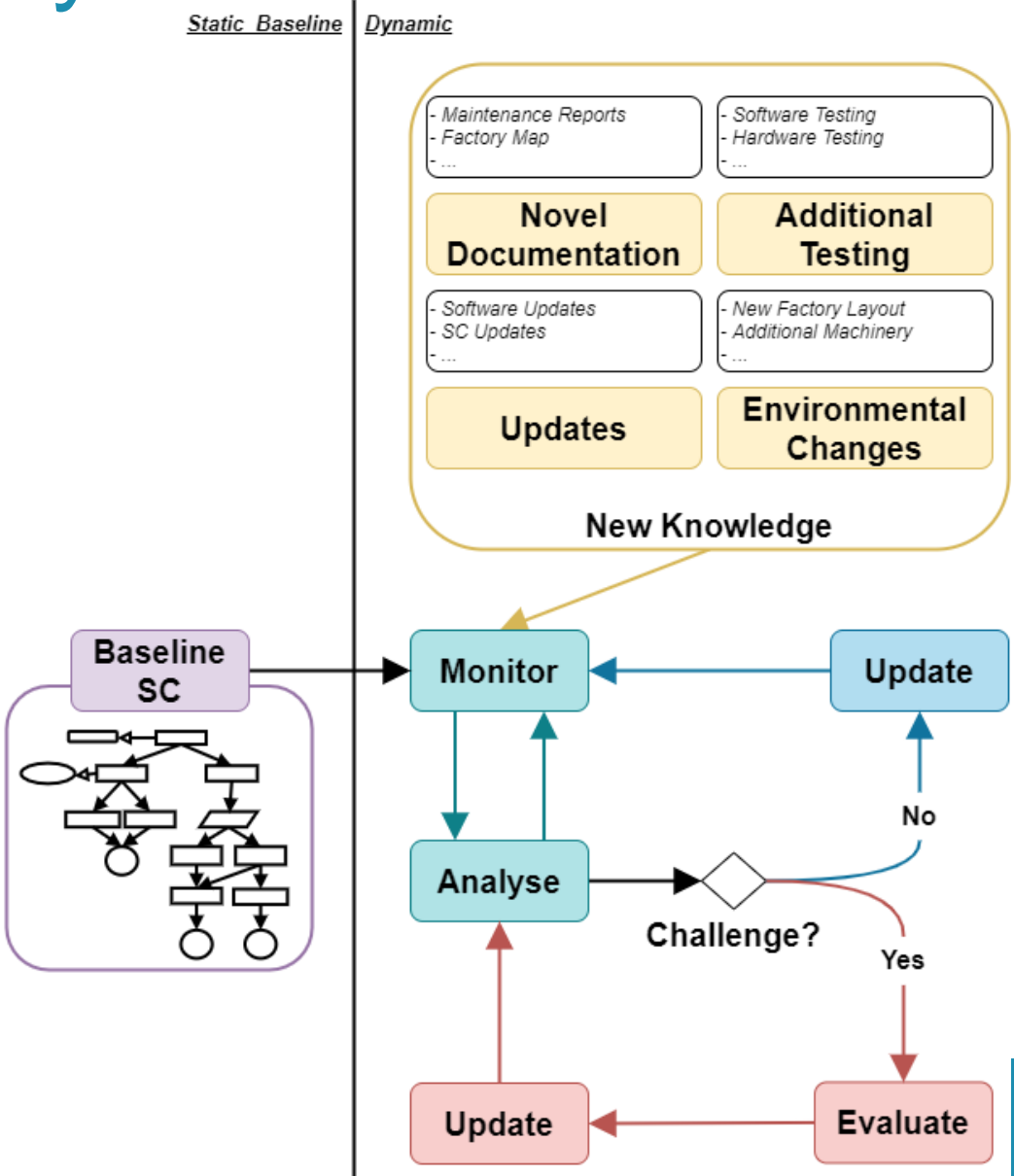
- The fundamental idea behind a DSC is to **reduce the gap between safety at run-time and the safety case as drawn up during design** and development. Especially for autonomous systems, where
  - Exhaustive testing is impossible
  - The design is made under imperfect knowledge
  - the system is prone to emergent behaviour.
- The strength of the extended DSC framework lies in
  - (1) filling in unknowns at run-time wherever possible and
  - (2) keeping track of the assurance deficits or unknowns that cannot be resolved during system design

# Dynamic Safety Case

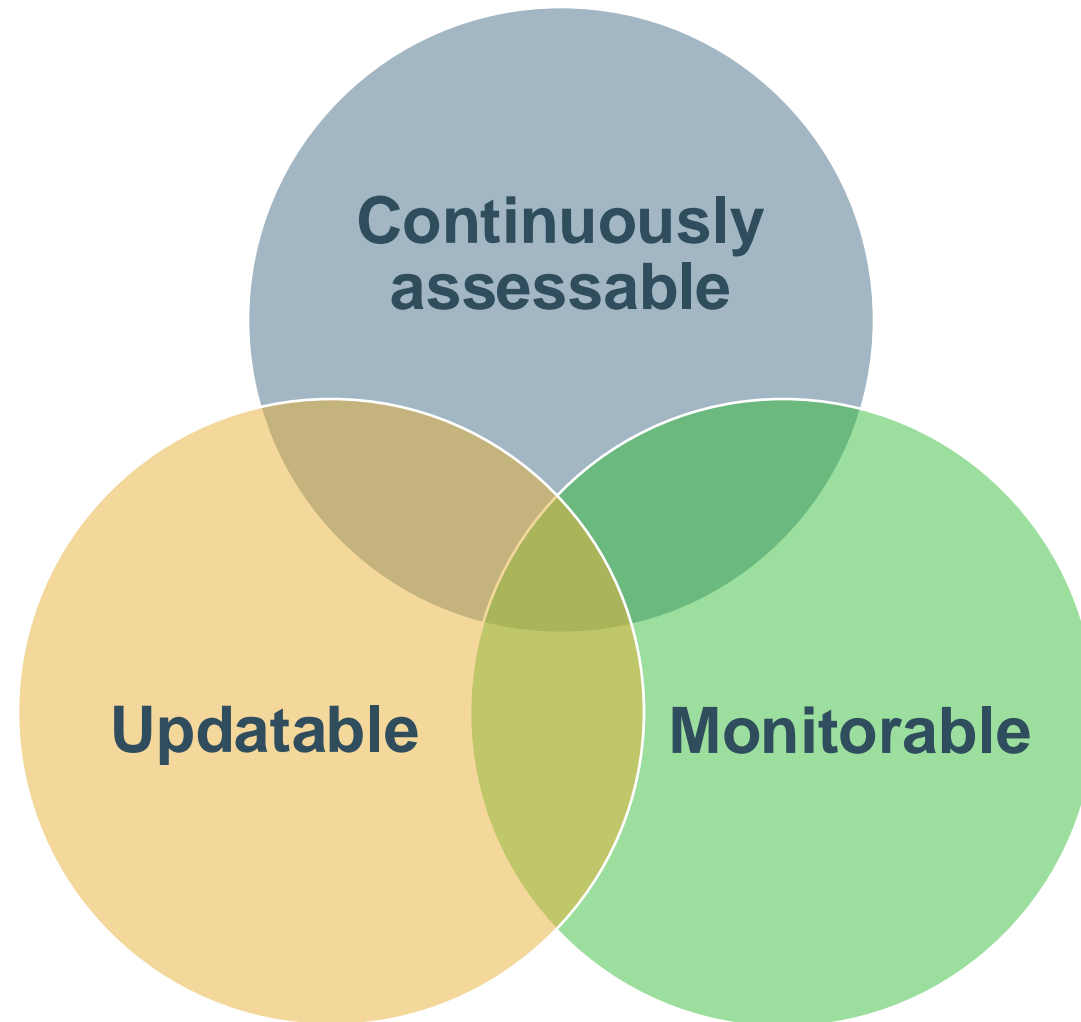




# Dynamic Safety Cases - Process



# Dynamic Safety Cases - Characteristics

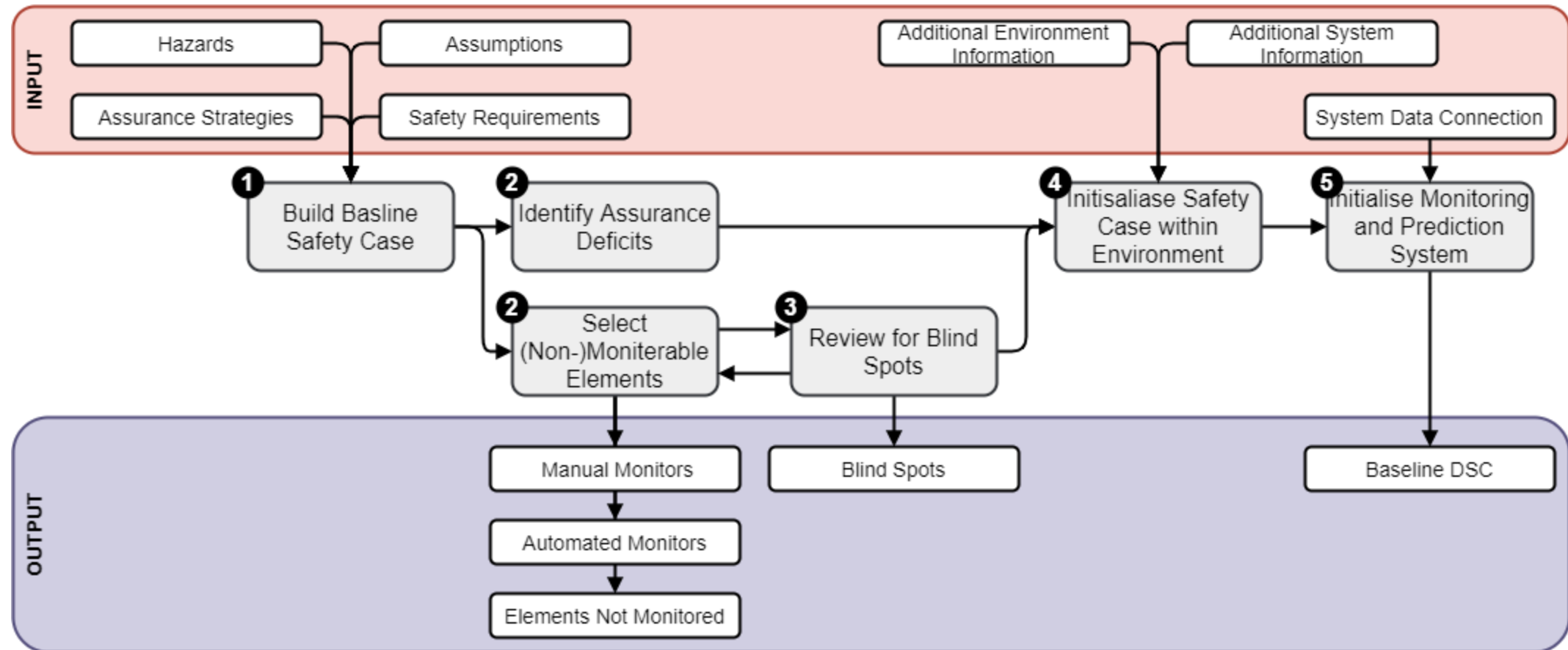


# Dynamic Safety Cases – Differentiating Between Systems

Different systems operating in various environments with changing levels of uncertainty and complexity inevitably require a different degree of care at run-time

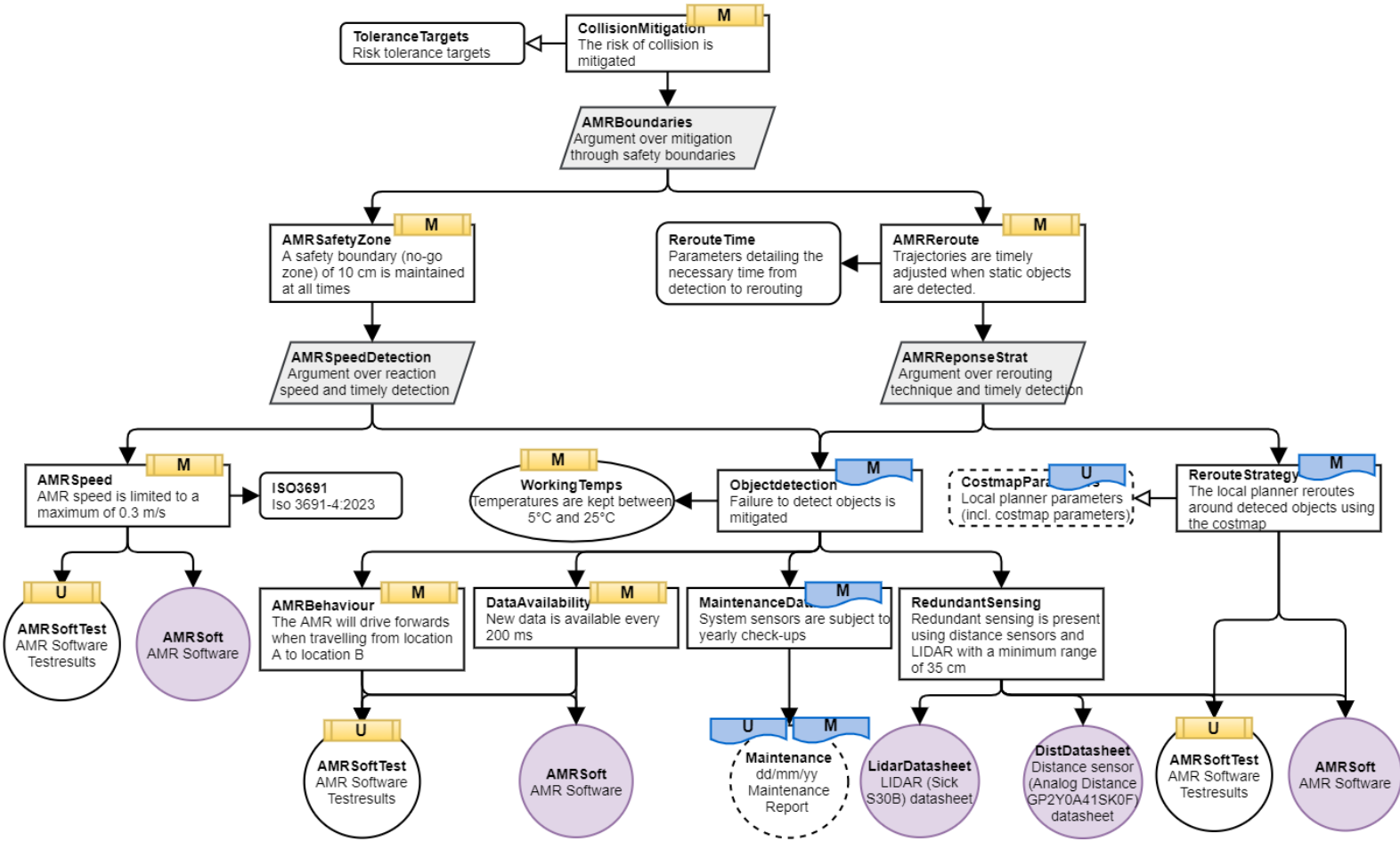
Monitorable				Assessable			
Setup	Coverage	Representativeness	Frequency	Depth	Procedure	Trigger	
1	Ad-Hoc	Partial	Updateable				Fault detection
			Content	Procedure	Trigger	Case to case con- sideration	
			1	Single elements	Case to case con- sideration	Change in system, environment or knowledge	
2	Systematic	Partial (combining formal and informal)	2	Single elements ; Patterns ; Single elements ;	(Limited) Guid- ance	Change in system, environment or knowledge ; Fault	nsive guid- Fault detection ; Change of knowl- edge
			3	New / Altered argumentation ; Pattern completion ; Single elements	Extensive ance	Change in system, environment or knowledge; Fault ; Systematic	Fault detection ; Change in knowl- edge ; Systematic checks

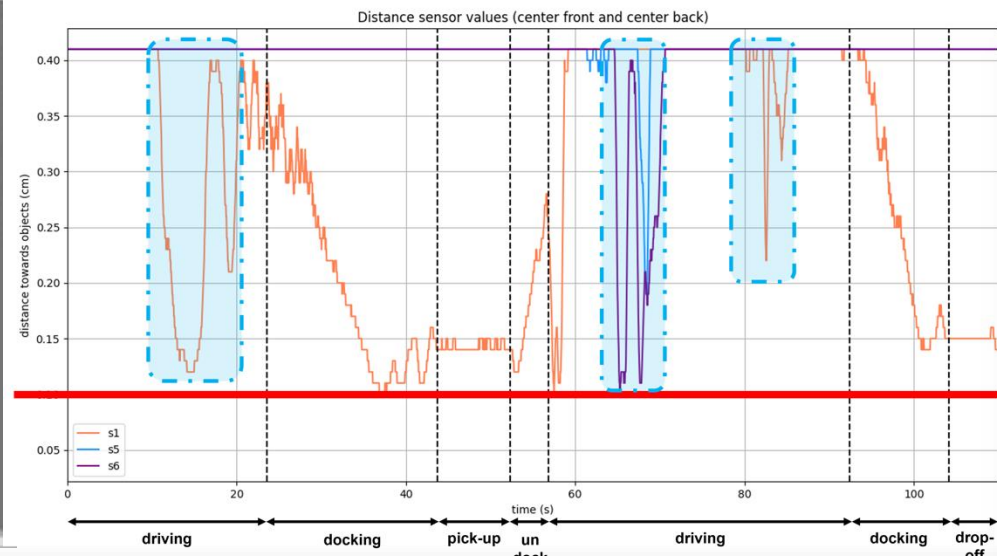
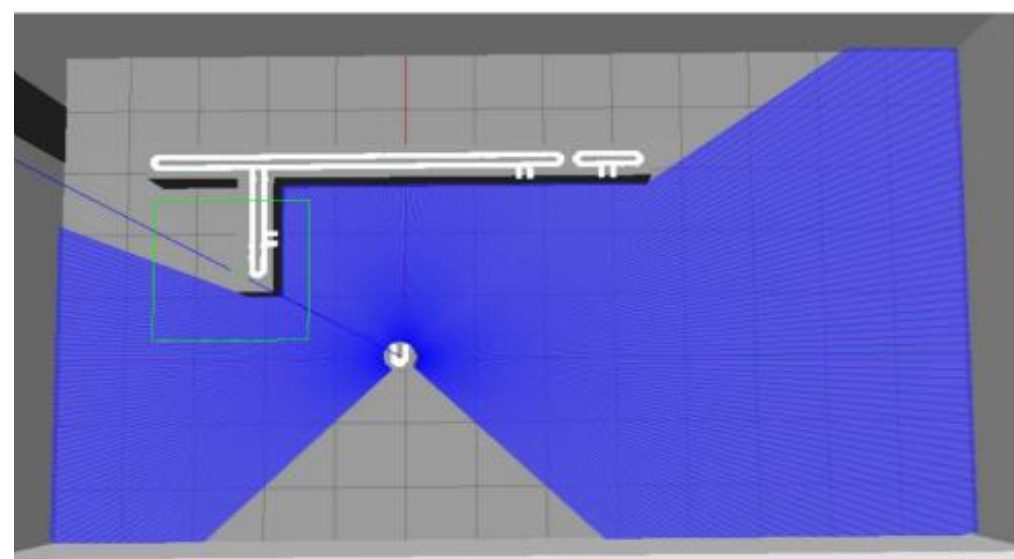
# Dynamic Safety Cases – Practical Workflow





# Dynamic Safety Cases – Practical Workflow



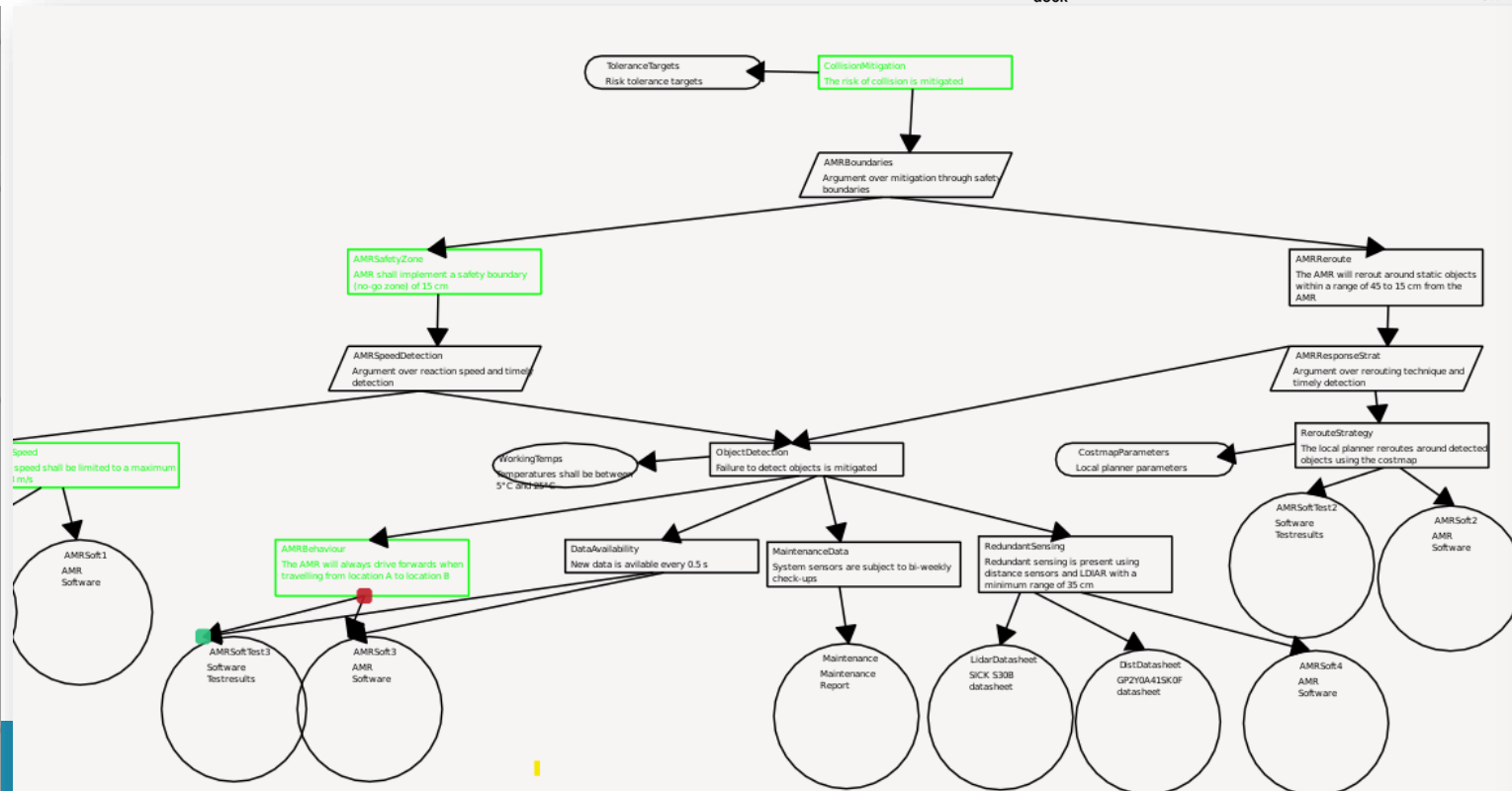


\_main\_.py x

File Help

Visualise Safety Case

ID	Logic Formula
CollisionMitigation	{vel > 0.0, bumper: false}
AMRSafetyZone	{vel > 0.0} -> {s1 > 0.15, s2 > 0.15,
AMRSpeed	{vel < 0.3}
AMRBehaviour	{vel_x_lin > -0.01}



▼ Additional Monitors

ID	Logic Formula	Requirement

A 3D rendering of a warehouse conveyor belt system. The scene is viewed from a high angle, looking down the length of the conveyor. Several cardboard boxes are positioned on the belt, moving away from the viewer. The boxes are brown with white labels and some have recycling symbols. The conveyor belt is dark blue with red laser lines forming a grid pattern on the floor. A semi-transparent dark grey bar is overlaid across the center of the image, containing the word "Conclusion" in white text.

# Conclusion

# Conclusion

- Safety first and safety last
- Safety cases as a useful practice to:
  - Reduce risk
  - Amplify confidence
  - Document conformance
  - Bundle all safety related information
- Dynamic safety case as an extension of the safety management system to deal with operational uncertainty inherent to autonomous systems.

# Questions?