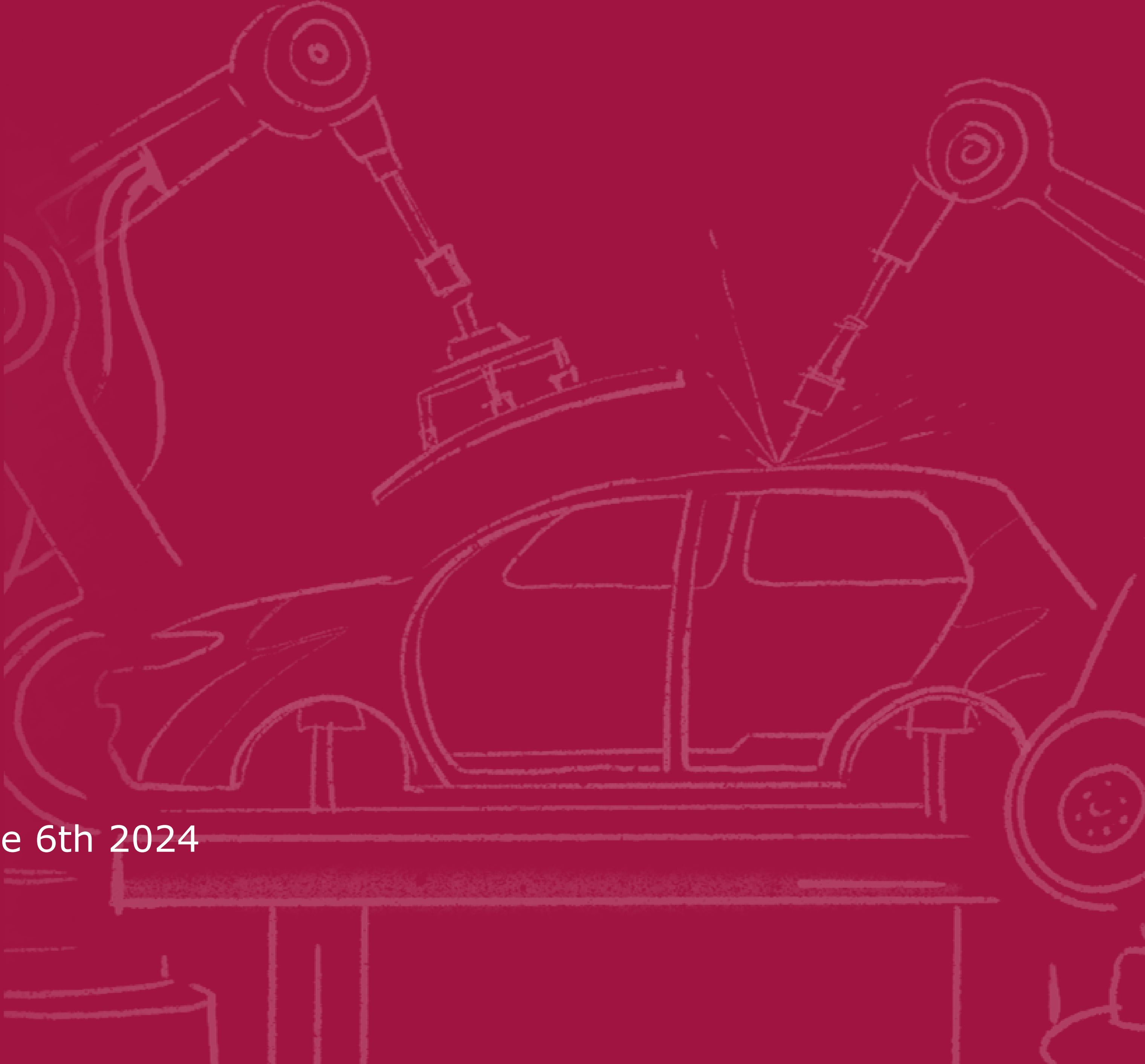
Applying STPA in car series production

Sebastian Kaiser, msg Plaut Austria, June 6th 2024



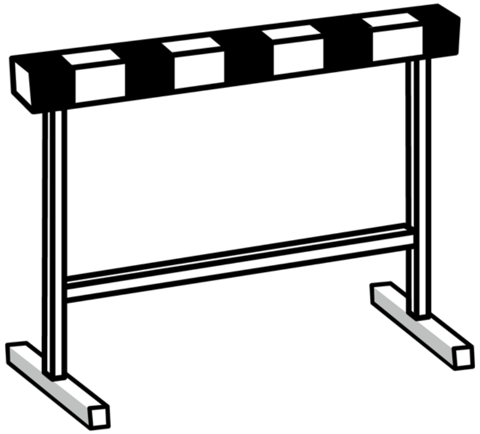
DISCLIMER!

- The following images are not the property of the creator of this presentation but are used with the consent of the image owner.
- The sources of the illustrations are therefore listed for the online version of this presentation.

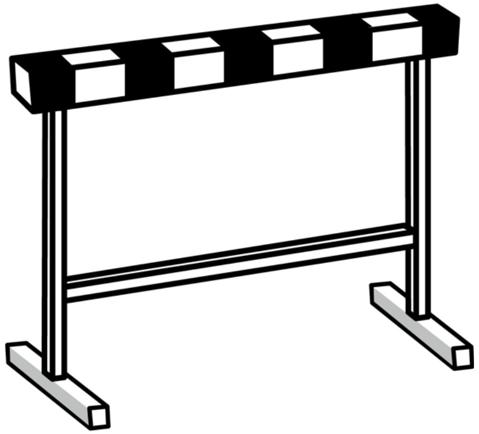
Sources of icons and figures

- Hurdle image: https://www.pngwing.com/en/free-png-vdzgupww
- Plaster icon: Designed by Freepick
- Steering wheel: Designed by Freepik
- Exposure icon: Designed by Freepick
- Priority icon: Designed by Freepick
- Speedometer: Designed by Freepick
- Jumper: Designed by Freepick
- Car: Iconpacks.net

The challenges of STPA in European Automotive industry

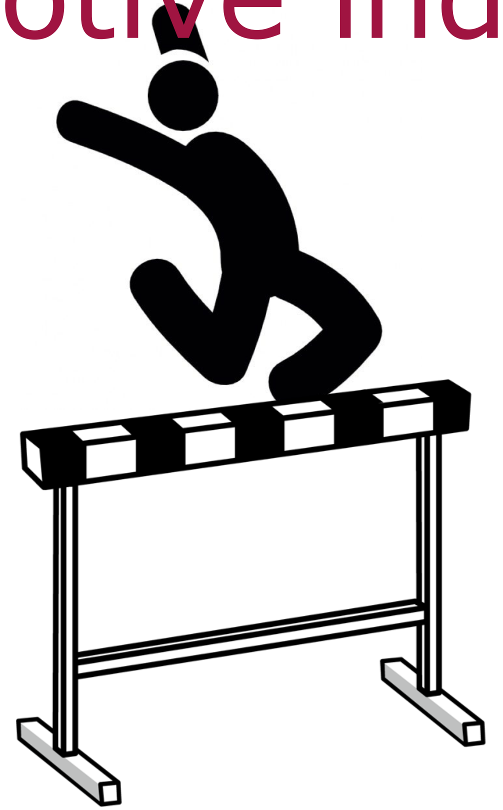


ISO 26262 obligatory for road approval

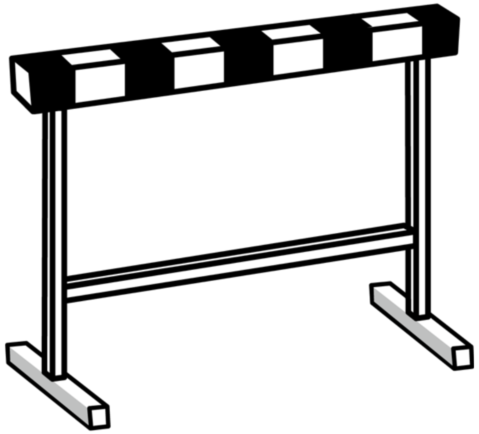


Overwhelmed by STPA outputs

The challenges of STPA in European Automotive industry

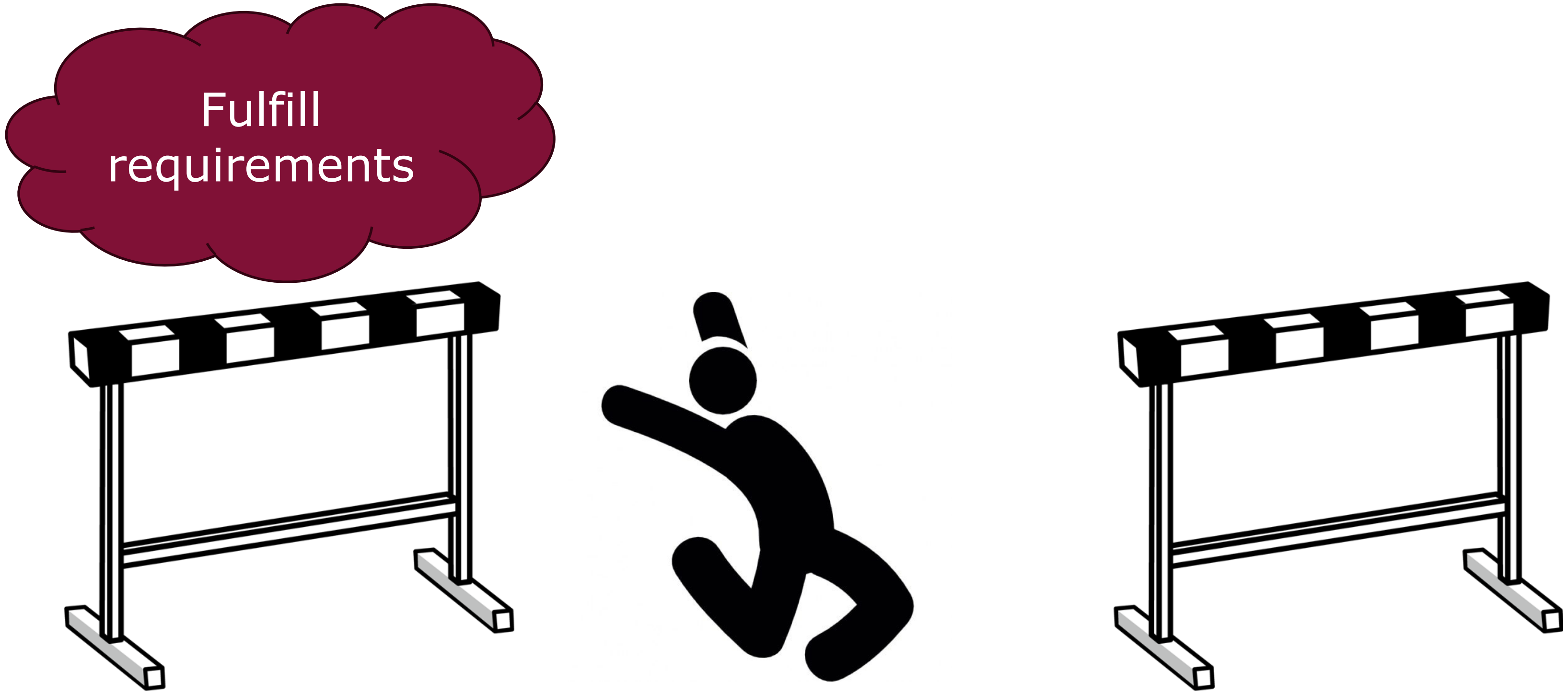


ISO 26262 obligatory for road approval



Overwhelmed by STPA outputs

The challenges of STPA in European Automotive industry

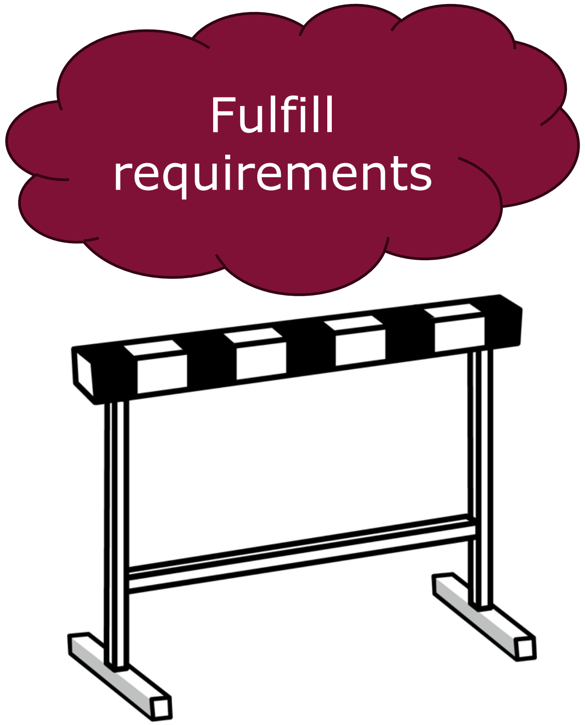


Fulfill requirements

ISO 26262 obligatory for road approval

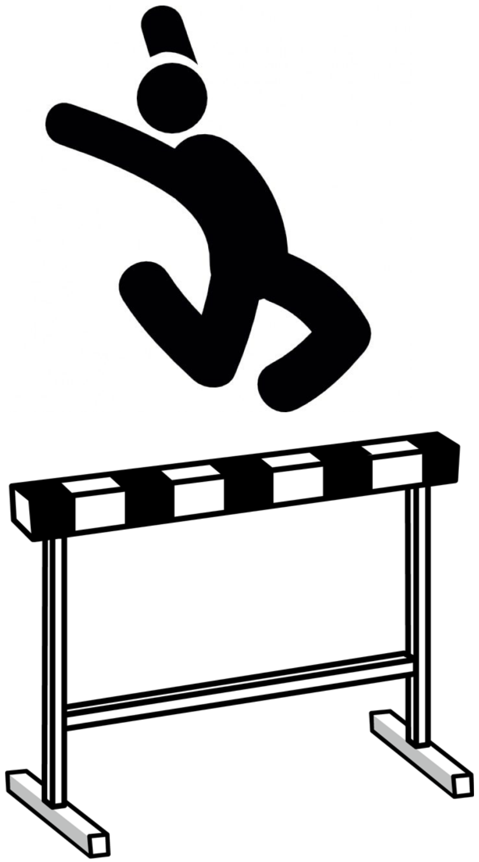
Overwhelmed by STPA outputs

The challenges of STPA in European Automotive industry



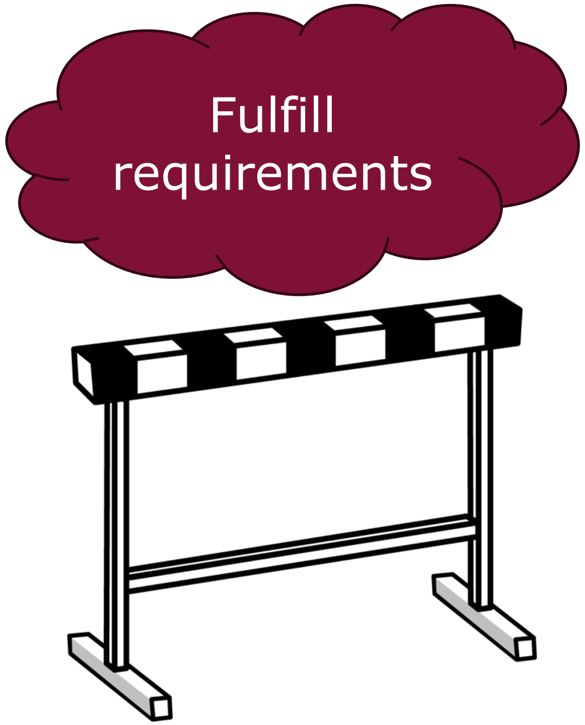
Fulfill requirements

ISO 26262 obligatory for road approval



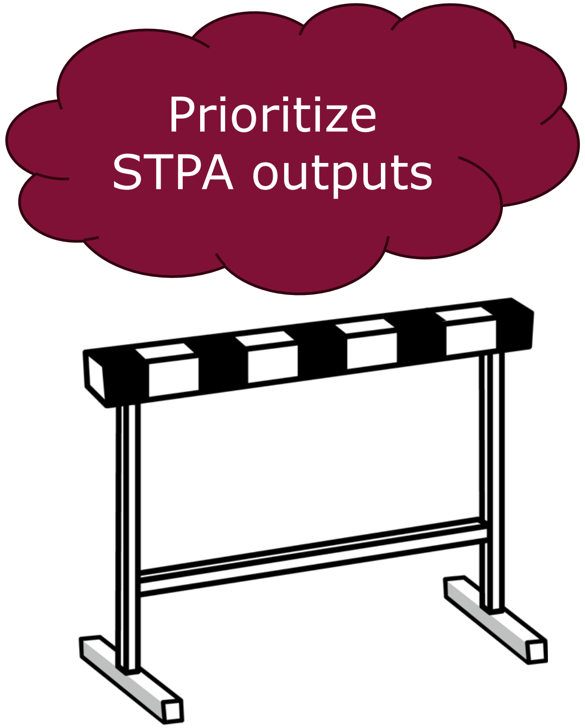
Overwhelmed by STPA outputs

The challenges of STPA in European Automotive industry



Fulfill requirements

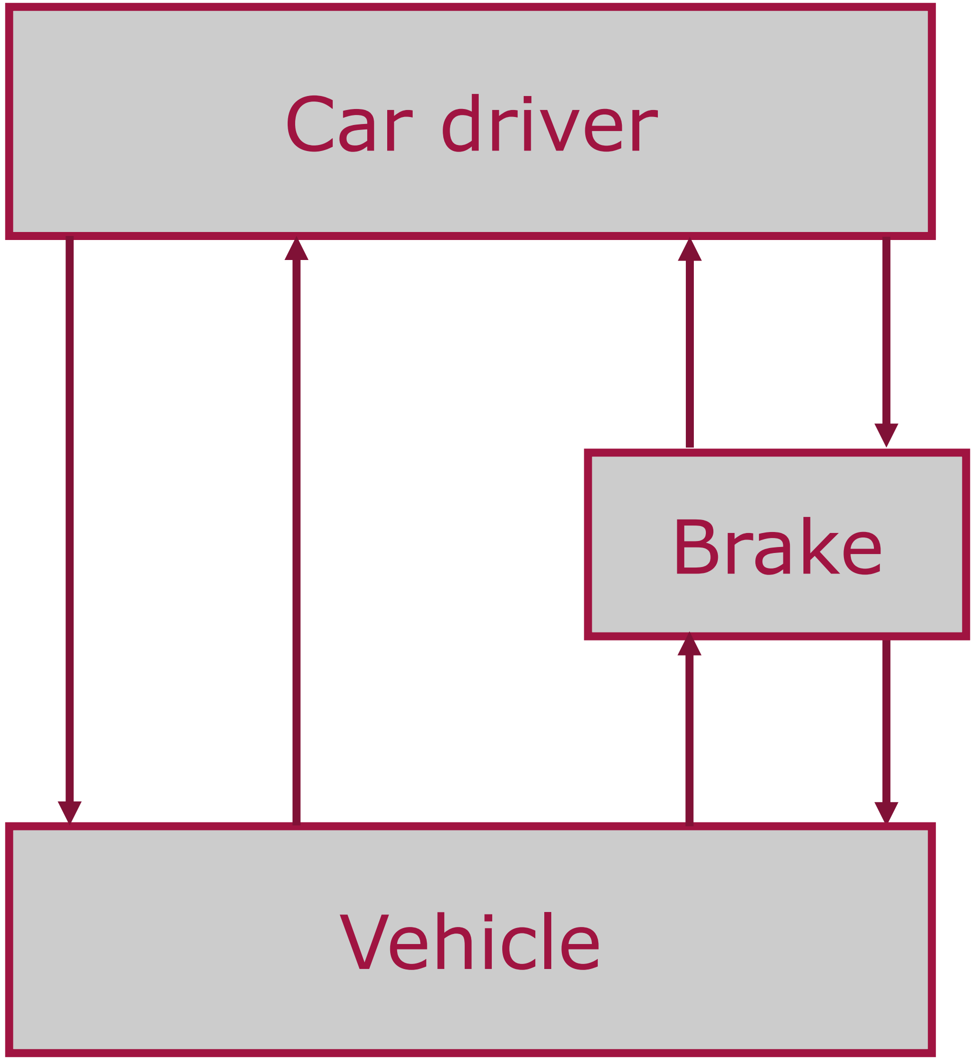
ISO 26262 obligatory for road approval



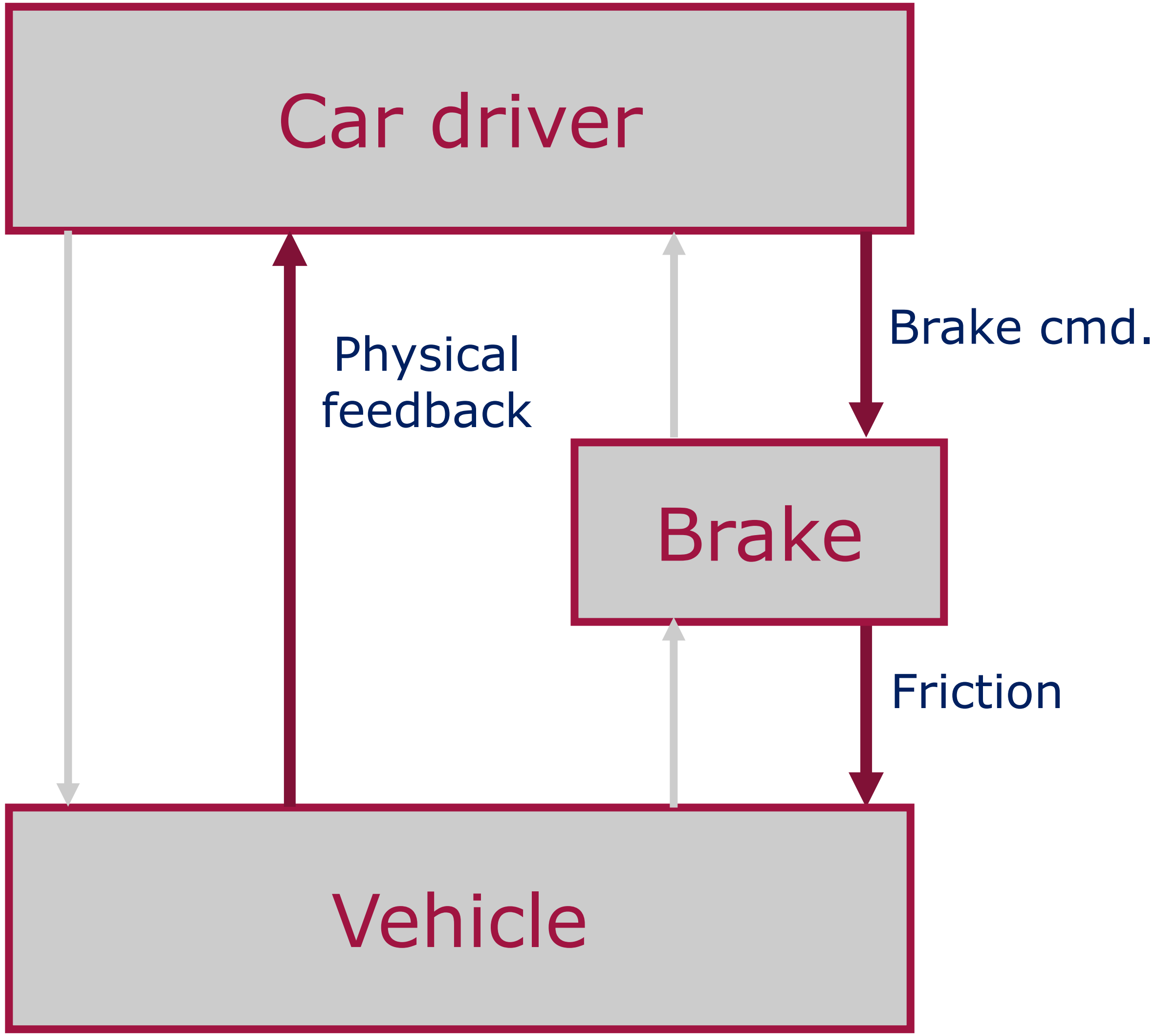
Prioritize STPA outputs

Overwhelmed by STPA outputs

Control Structure – Automotive example



Control Structure – Automotive example



Solving the issue with STPA!

System-level hazard

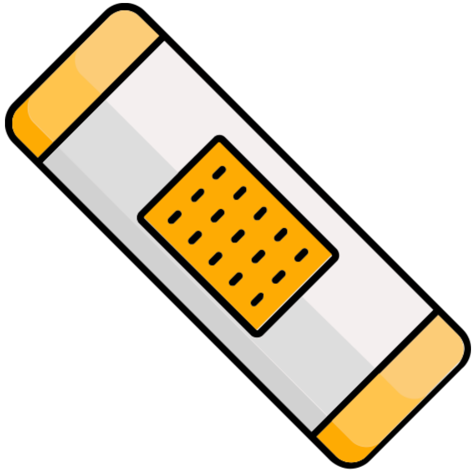
H-1: The vehicle violates the minimum separation from other persons or objects while driving [L-x]

System state to be prevented

System-level Constraint

SC-1: The vehicle must satisfy the minimum separation from other persons or objects while driving [H-1]

Parameter S: required by ISO 26262!



Severity

LOW
S0
S1
S2
S3
HIGH

How bad is it?

Solving the issue with STPA!

Sub-Hazards

H-1.1: The vehicle violates the minimum separation from other persons or objects **while driving at a very low speed (< 5 mph)**

→ **Less kinetic energy**

H-1.3: The vehicle violates the minimum separation from other persons or objects **while driving at high speed (> 30 mph)**

→ **Higher kinetic energy**

Solving the issue with STPA!

Sub-Hazards

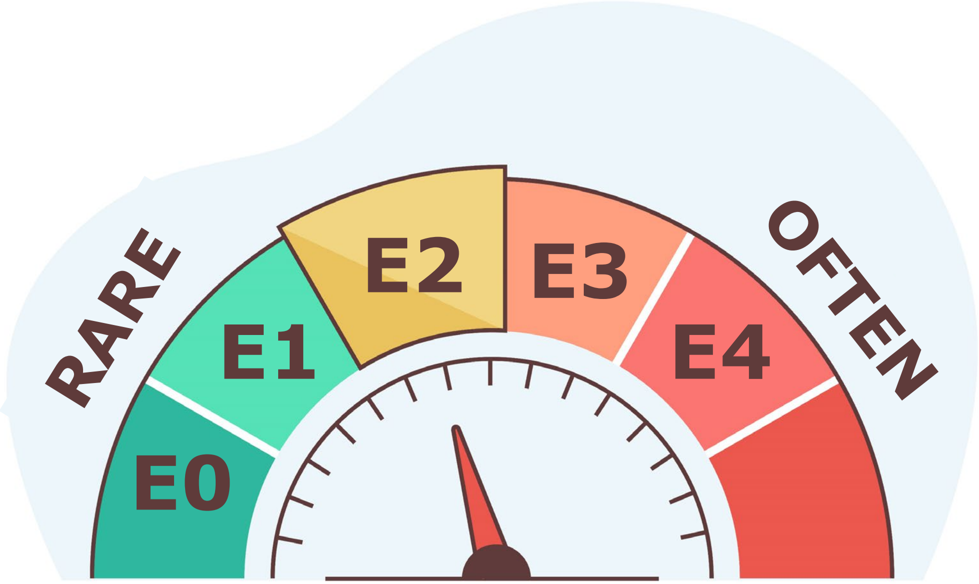
H-1.1: The vehicle violates the minimum separation from other persons or objects **while driving at a very low speed (< 5 mph)**

Less kinetic energy → **S2** (e.g. rear-end collision with low speed)

H-1.3: The vehicle violates the minimum separation from other persons or objects **while driving at high speed (> 30 mph)**

Higher kinetic energy → **S3** (e.g. front collision with high speed)

Parameter E: required by ISO 26262!



Exposure

How often does it happen?

Solving the issue with STPA!

Sub-Hazards

H-1.1: The vehicle violates the minimum separation from other persons or objects**while driving at a very low speed (< 5 mph)**

H-1.3: The vehicle violates the minimum separation from other persons or objects**while driving at high speed (> 30 mph)**

Solving the issue with STPA!

Sub-Hazards

H-1.1: The vehicle violates the minimum separation from other persons or objects

while driving at a very low speed (< 5 mph)

H-1.3: The vehicle violates the minimum separation from other persons or objects

while driving at high speed (> 30 mph)

Solving the issue with STPA!

Sub-Hazards

H-1.1: The vehicle violates the minimum separation from other persons or objects**while driving at a very low speed (< 5 mph)**

→ **Happens less often**

H-1.3: The vehicle violates the minimum separation from other persons or objects**while driving at high speed (> 30 mph)**

→ **Happens more often**

Solving the issue with STPA!

Sub-Hazards

H-1.1: The vehicle violates the minimum separation from other persons or objects **while driving at a very low speed (< 5 mph)**

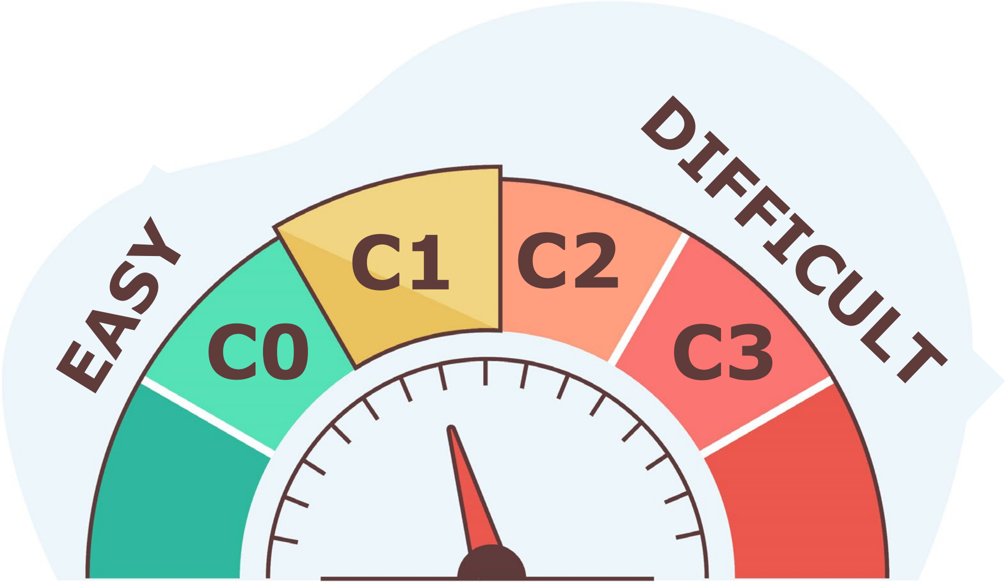
Happens less often → **E2** (e.g. Parking lot)

H-1.3: The vehicle violates the minimum separation from other persons or objects **while driving at high speed (> 30 mph)**

Happens more often → **E4** (e.g. regular drive in a city)

Parameter C: required by ISO 26262!

Controllability

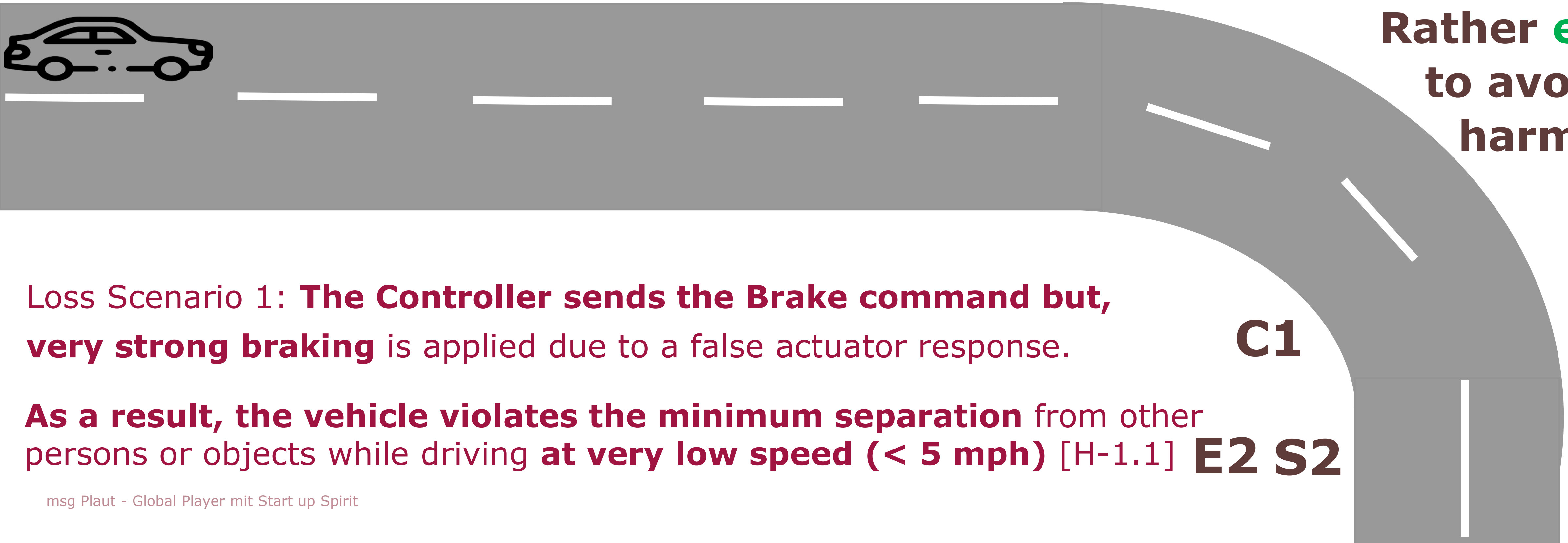


Can you avoid harm?

Assessing the controllability!

Undesired strong
breaking
is applied

Scenario 1



Rather easy to avoid harm

C1

Loss Scenario 1: **The Controller sends the Brake command but, very strong braking** is applied due to a false actuator response.

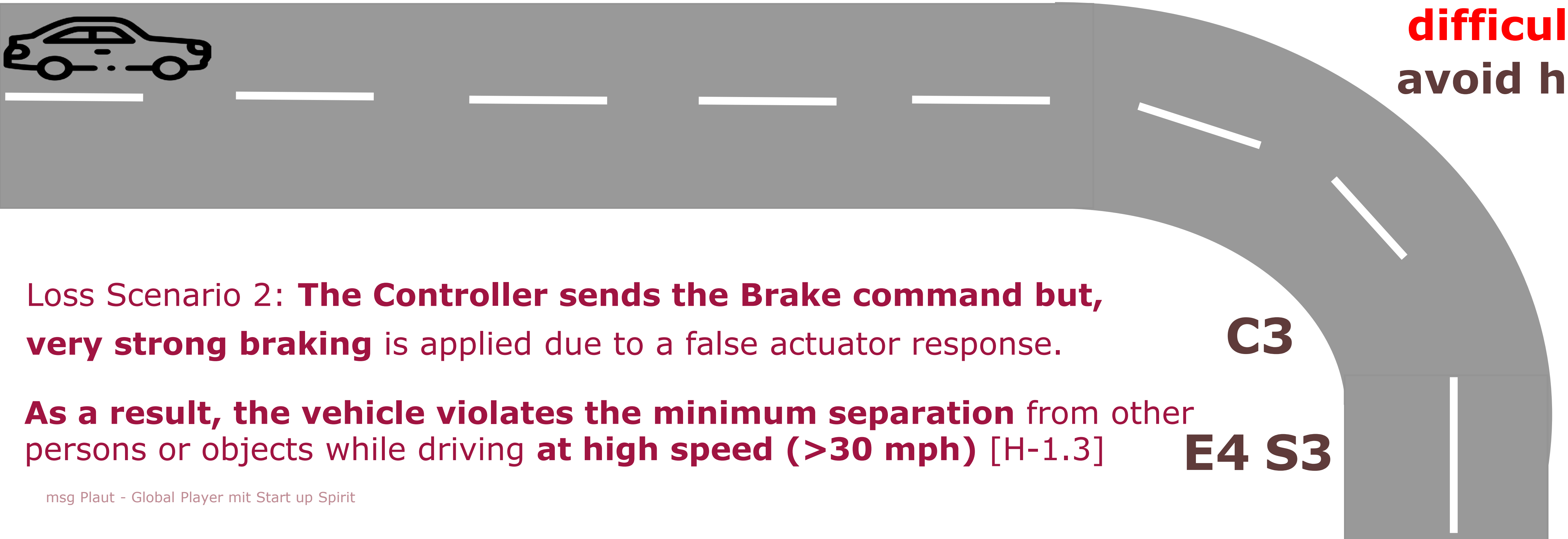
As a result, the vehicle violates the minimum separation from other persons or objects while driving **at very low speed (< 5 mph)** [H-1.1]

E2 S2

Assessing the controllability!

Undesired strong
breaking
is applied

Scenario 2



Rather difficult to avoid harm

Loss Scenario 2: **The Controller sends the Brake command but, very strong braking** is applied due to a false actuator response.

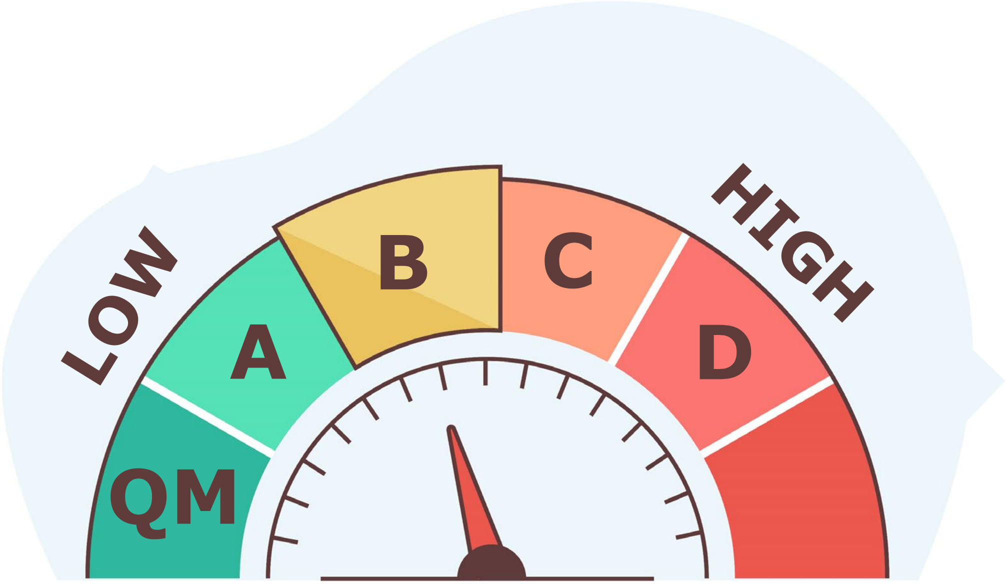
As a result, the vehicle violates the minimum separation from other persons or objects while driving **at high speed (>30 mph)** [H-1.3]

C3

E4 S3

ASIL derived from S, E, C combination

Risk assessment



How much effort?

Prioritize the outputs of STPA!

Sub-Hazard

H-1.1

Loss Scenario

Scenario 1

$$\underbrace{\textbf{S2}\quad\textbf{E2}\qquad\qquad\textbf{C1}}_{\textbf{[QM]}}$$

Constraint

SC-1.1: The vehicle **must satisfy the minimu distance** from other objects and persons while driving **at a very low speed**.

Sub-Hazard

H-1.3

Loss Scenario

Scenario 2

$$\underbrace{\textbf{S3}\quad\textbf{E4}\qquad\qquad\textbf{C3}}_{\textbf{[ASIL D]}}$$

Constraint

SC-1.3: The vehicle **must satisfy the minimu distance** from other objects and persons while driving **at high speed**.

Prioritize the outputs of STPA!

Sub-Hazard **Loss Scenario**

H-1.1 Scenario 1

S2 E2 C1

Constraint

SC-1.1: The vehicle **must satisfy the minimu** **distance** from other objects and persons while driving **at a very low speed**.

[QM]

Sub-Hazard **Loss Scenario**

H-1.3 Scenario 2

S3 E4 C3

Constraint

SC-1.3: The vehicle **must satisfy the minimu** **distance** from other objects and persons while driving **at high speed**.

[ASIL D]

Prioritize the outputs of STPA!

Sub-Hazard **Loss Scenario** **Constraint**

H-1.1 Scenario 1

S2 E2 C1

SC-1.1: The vehicle **must satisfy the minimu** **distance** from other objects and persons while driving **at a very low speed.** **[QM]**

Sub-Hazard **Loss Scenario** **Constraint**

H-1.3 Scenario 2

S3 E4 C3

SC-1.3: The vehicle **must satisfy the minimu** **distance** from other objects and persons while driving **at high speed** **[ASIL D]**

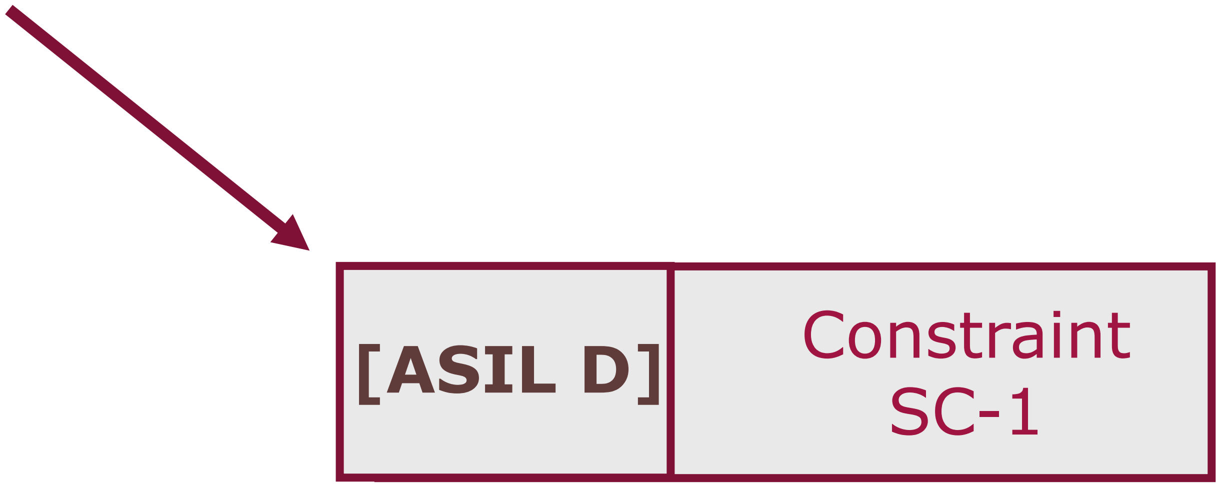
Prioritize the outputs of STPA!

Constraint

SC-1.1: The vehicle **must satisfy the minimum distance** from other objects and persons while driving **at a very low speed** **[QM]**

Constraint

SC-1.3: The vehicle **must satisfy the minimu** **distance** from other objects and persons while driving **at high speed.** **[ASIL D]**



[ASIL D]

Constraint
SC-1

The advantages of our procedure!

- Fulfill standards in order to get road approval!
- Overall better results by STPA application!
- Prioritization in line with Automotive procedures!

Thank you for you attention!

Sebastian Kaiser

Business Consultant Automotive
sebastian.kaiser@msg-plaut.com

msg Plaut Austria GmbH
Modecenterstraße 17, Unit 4 / 6.OG
1110 Wien

office.at@msg-plaut.com
msg-plaut.com