Aurora

An Overview of the

Safety Case Framework

September, 2021

Overview

Agenda

- What is a safety case and why?
- Our top level claim and principles
- Safety Case Tailoring
- Safety Case walkthrough

Our Approach

A Safety Case Based Approach

- No singular piece of evidence captures the totality of safety
- There are complex interactions and relationships between the various pieces of evidence

- An argument without evidence is baseless
- Evidence without an argument is trivial

A safety case is a structured argument, supported by evidence, intended to justify that a system is acceptably safe for a specific application in a specific operating environment.

What it is and is not

A Completed Safety Case

Is:

- A structured argument that includes the safety elements of federal and state guidance
- A clear and defensible argument on why a system is safe to operate
- A useful tool to evaluate holistic efforts to promote safety, including by providing insights into the safety culture and development processes
- A way to address operational safety
- Able to adapt relevant industry standards

Is Not:

- A regulatory framework
- A single standard that addresses or defines SDV safety
- A new test procedure with new metrics
- A checklist

Rationale for a Safety Case Based Approach

No Silver Bullet

No single test, industry standard, or best practice can address the totality of safety for the AV

In our safety case, we harmonize and adapt various existing industry standards and best practices

High Complexity

The complex relationships and safety implications between the different sub-components, components, and system levels are difficult to convey and understand

We use a structured argument and a hybrid of Goal Structured Notation and narrative prose to convey these relationships

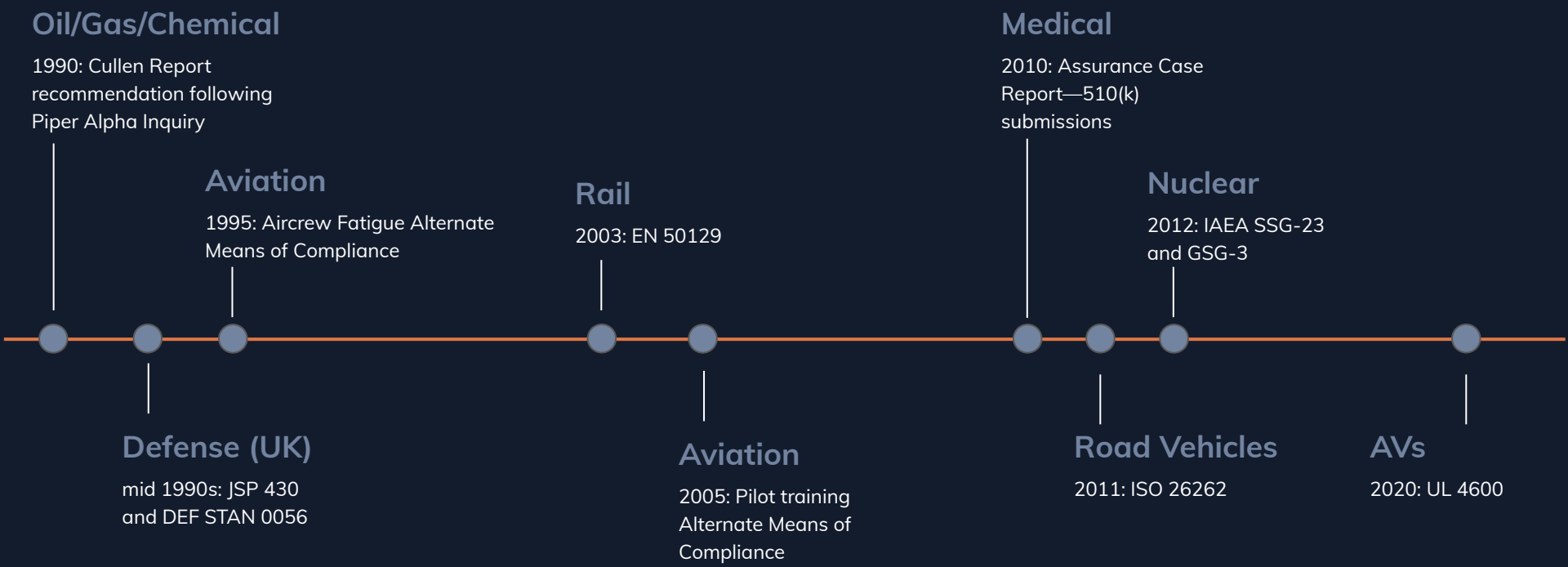
Enterprise not product level

Safety should be addressed at an enterprise level, not a product, component, or subsystem level

We scope our Safety Case Framework at the Self-Driving Enterprise level

Overview

Safety Cases in Other Industries



Aurora's self-driving vehicles are acceptably safe to operate on public roads

TOP LEVEL CLAIM

G1
Proficient

The self-driving vehicle is acceptably safe during nominal operation

+

G2
Fail-Safe

The self-driving vehicle is acceptably safe in presence of faults and failures

+

G3
Continuously Improving

All identified potential safety issues posing an unreasonable risk to safety are evaluated, and resolved with appropriate corrective and preventative actions

+

G4
Resilient

The self-driving vehicle is acceptably safe in case of reasonably foreseeable misuse and unavoidable events

+

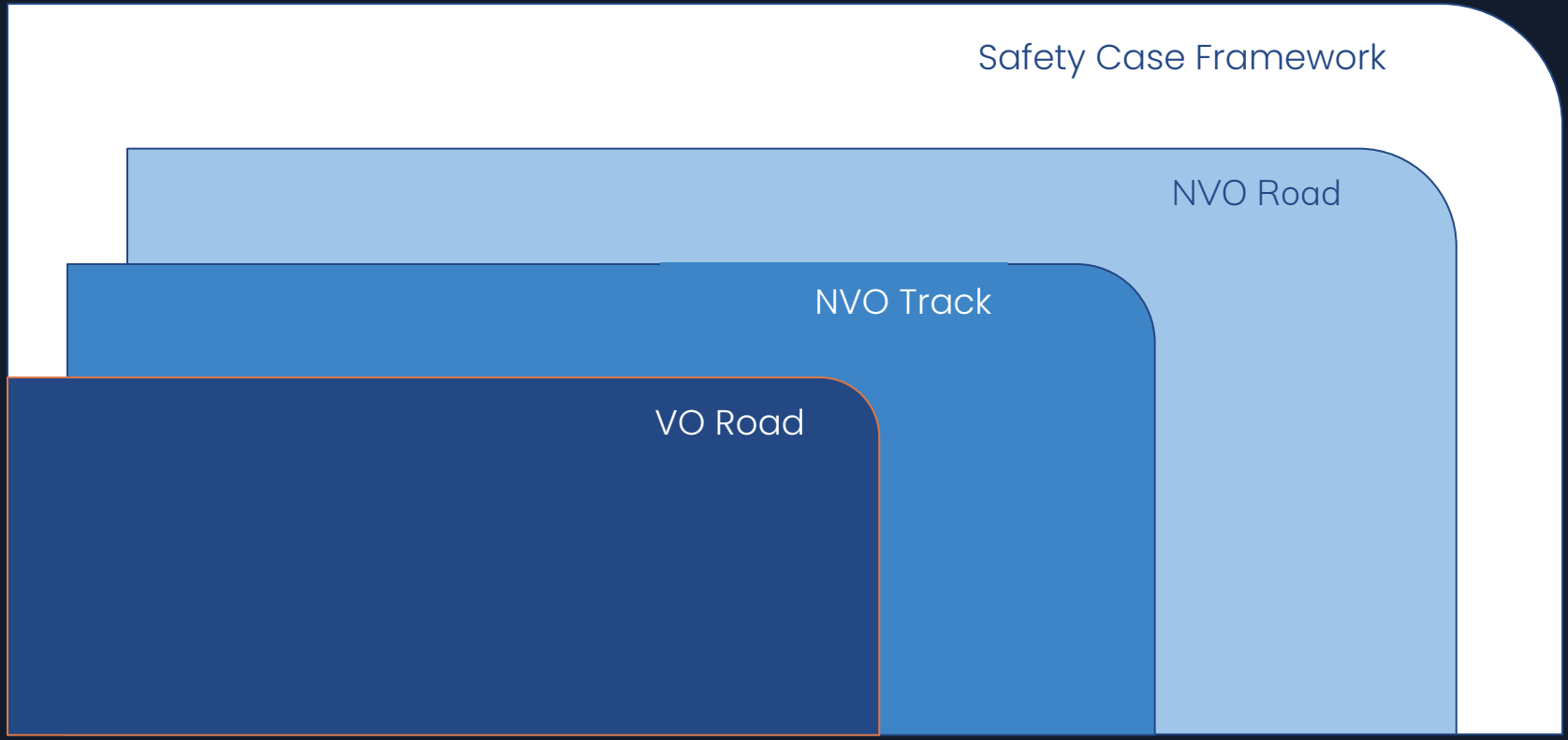
G5
Trustworthy

The self-driving enterprise is trustworthy

+

Start with the end

Safety Case Tailoring



*not to scale

An Example

Walking Through the Structured Argument

https://safetycaseframework.aurora.tech/gsn

What it is and is not

A Completed Safety Case

Is:

- A structured argument that includes the safety elements of federal and state guidance
- A clear and defensible argument
- A useful tool to evaluate holistic efforts to promote safety, including by providing insights into the safety culture and development processes
- Addresses operational safety
- Adapts relevant industry standards

Is Not:

- A regulatory framework
- A single standard that addresses or defines SDV safety
- A new test procedure with new metrics
- A checklist