# A Structured Argument for Assuring Safety of the Intended Functionality (SOTIF)

John Birch, David Blackburn, John Botham, Ibrahim Habli, David Higham, Helen Monkhouse, Gareth Price, Norina Ratiu, Roger Rivett

Submitted as a short paper to
WAISE 2020: Third International Workshop on Artificial Intelligence Safety Engineering

# Acronyms

| | |
|---|---|
| ODD: | **O**perational **D**esign **D**omain |
| ADS: | **A**utomated **D**riving **S**ystem |
| DDT: | **D**ynamic **D**riving **T**ask |

# Agenda

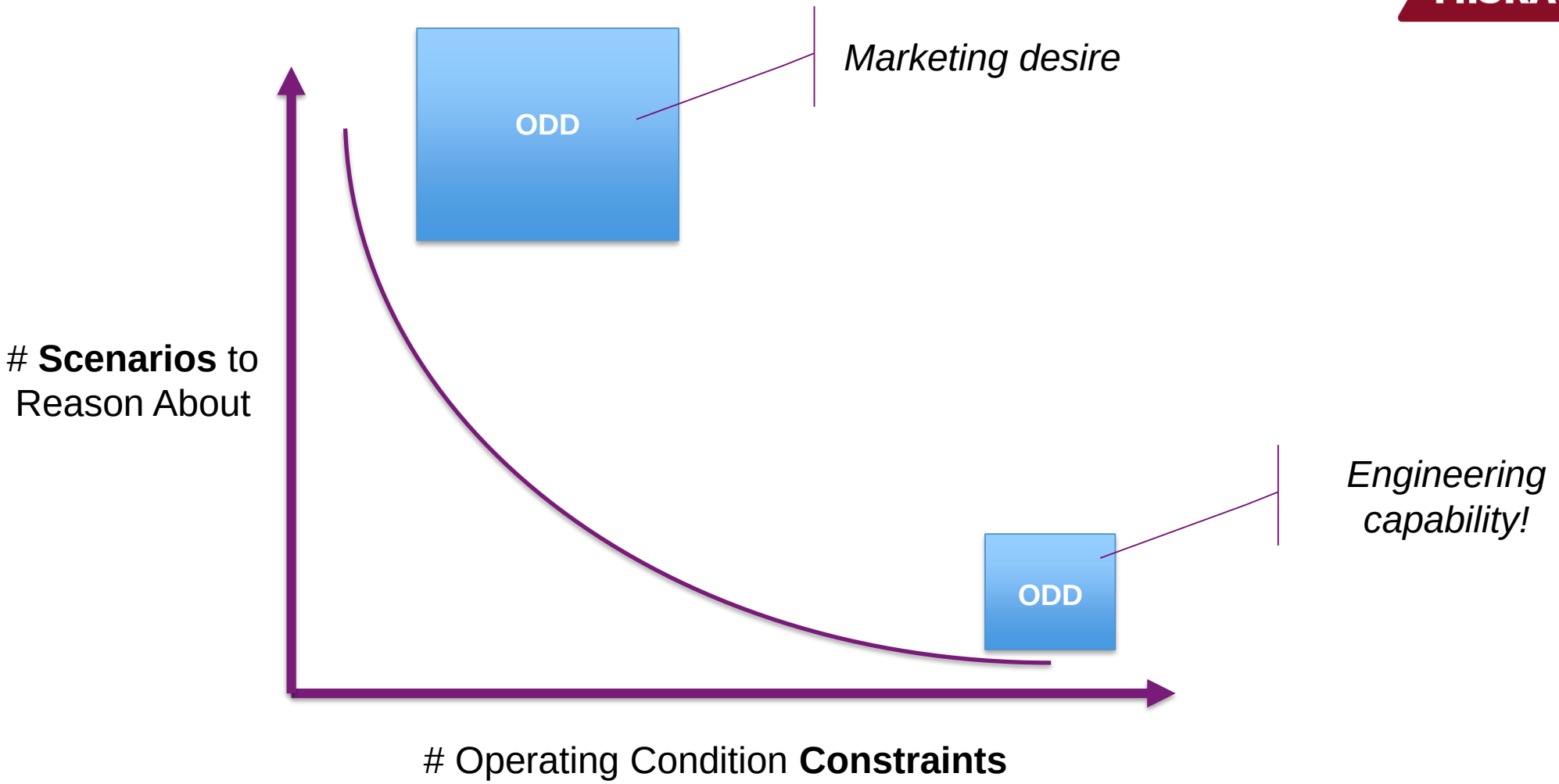
- What is an ODD?
- What role does it play in ADS Safety Assurance?
- Typical ADS Drive Cycle
- ODD-Activation States
- Example Safety Claims
- Safety Argument Pattern

# What is an ODD?

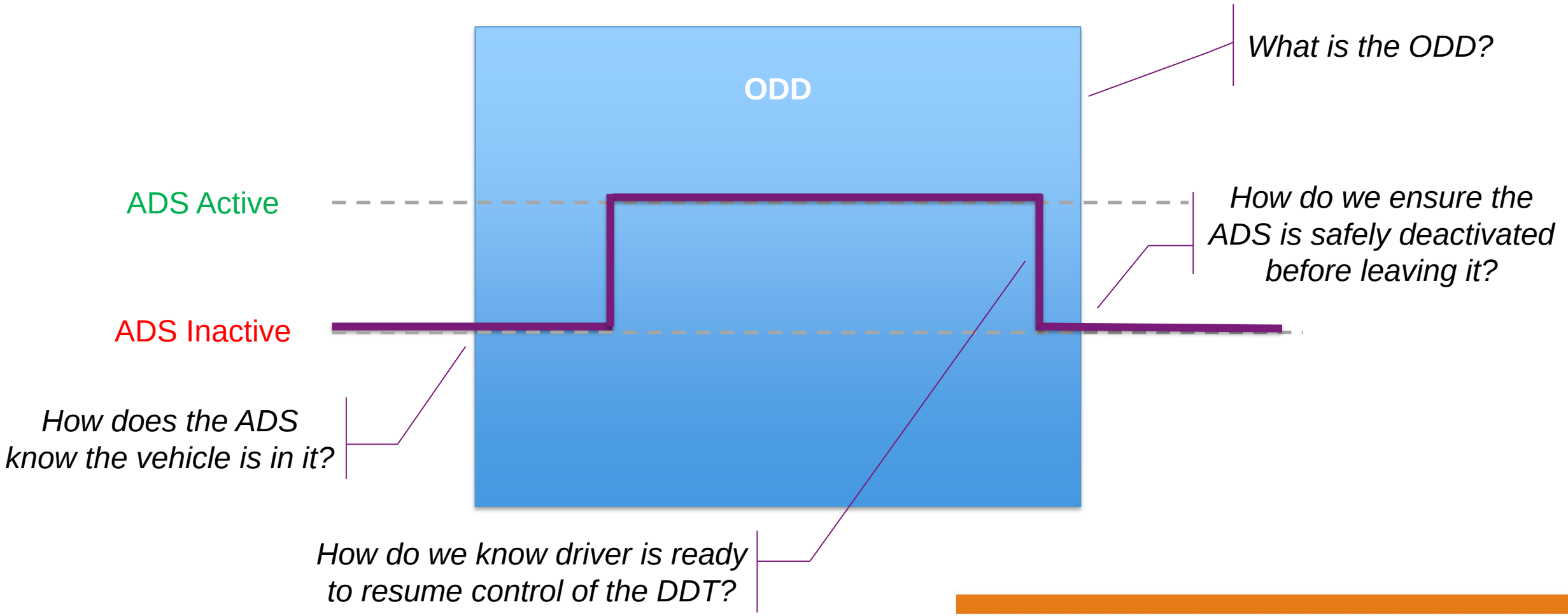
SAE J3016 2018:

*“Operating conditions under which a given driving automation system or feature thereof is specifically designed to function…”*

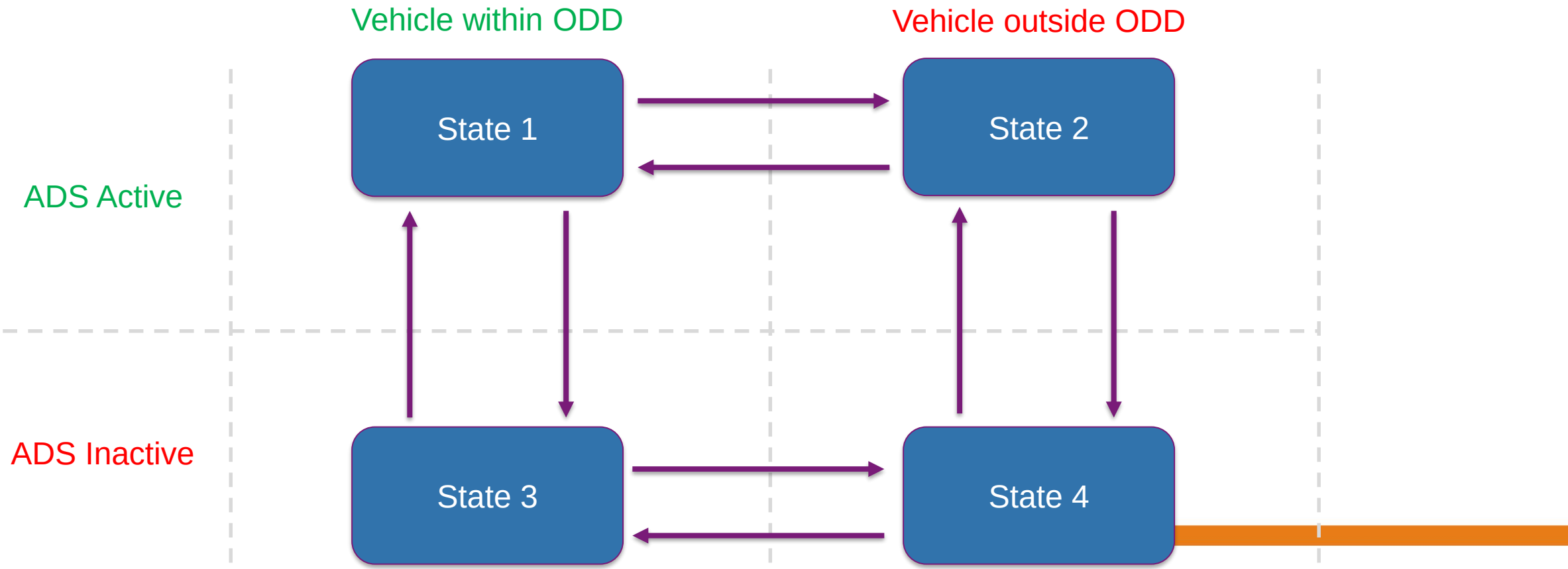
# What role does it play in ADS Safety Assurance?



# Typical ADS Drive Cycle

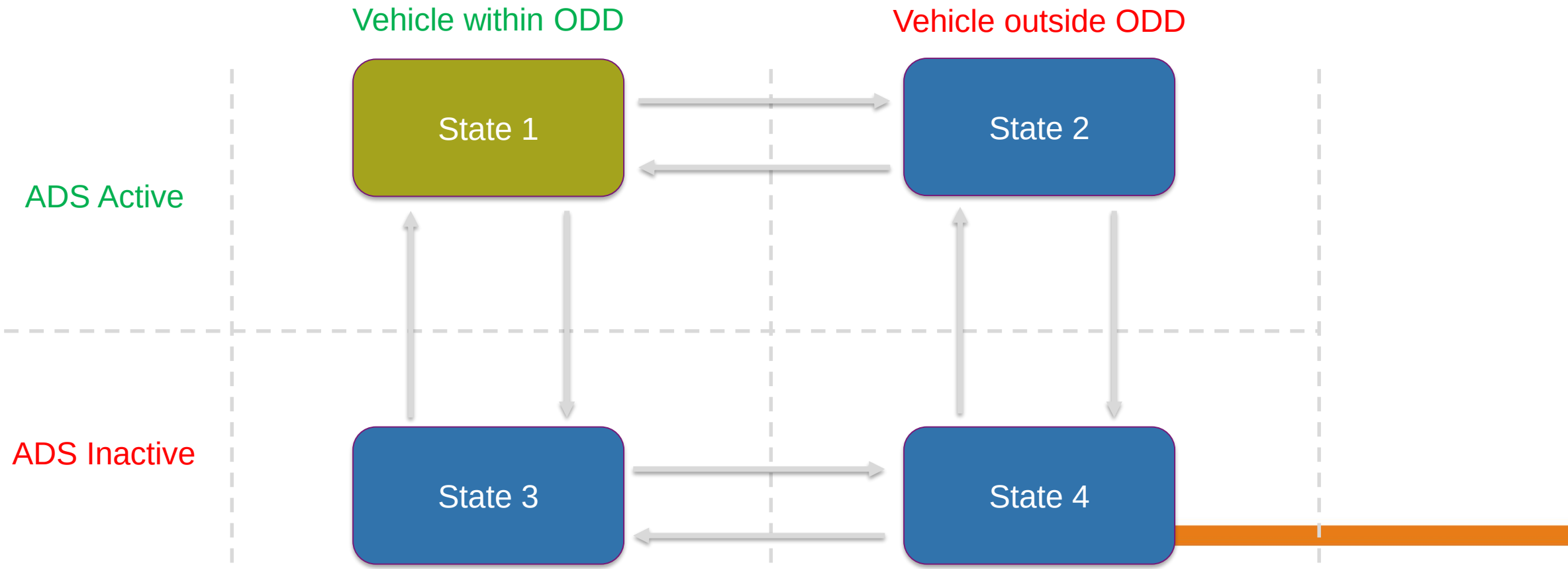


# ODD-Activation States



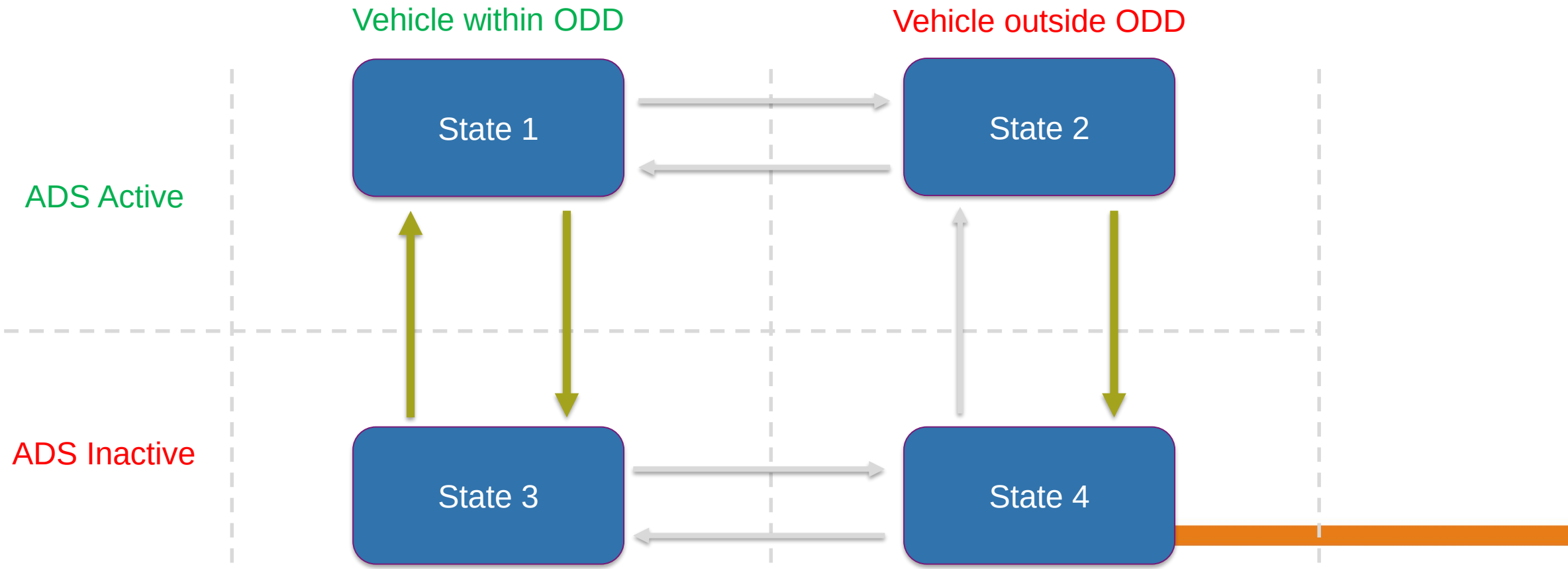
# Example Safety Claims

- *All scenarios are known*
- *All known scenarios are safe*



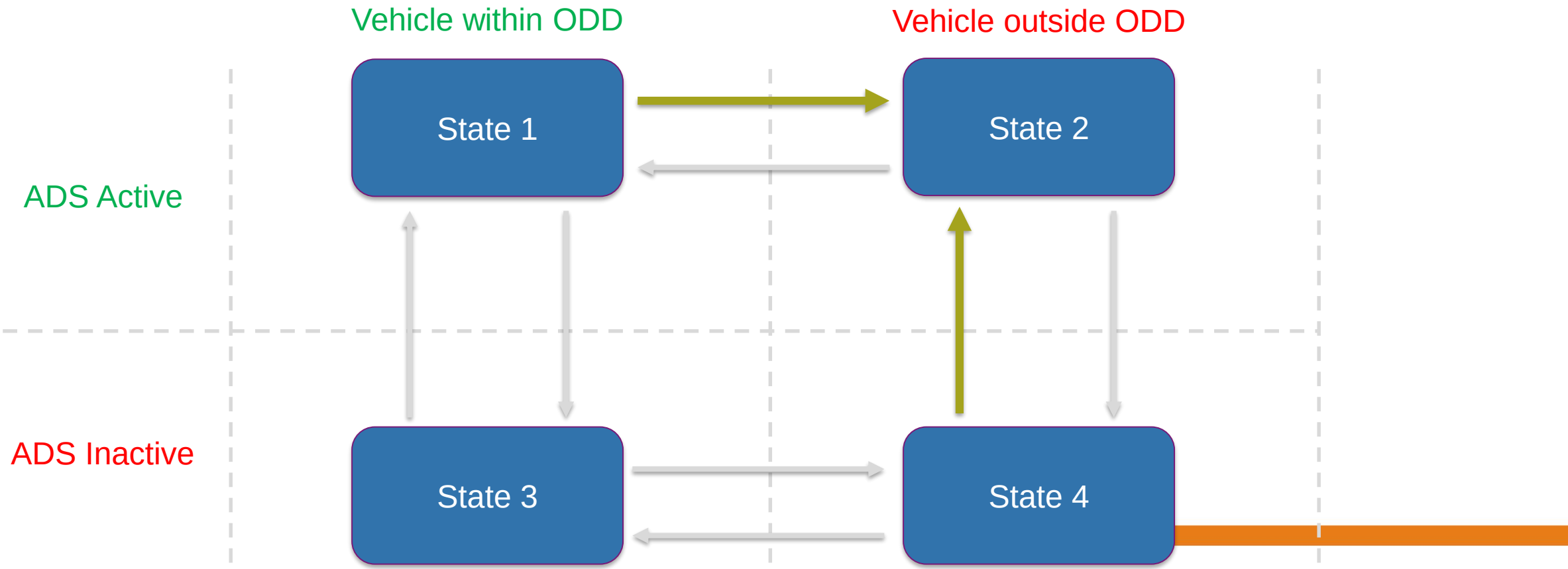
# Example Safety Claims

- *Handover of DDT is intuitive and predictable*
- *Driver is ready for handover of DDT before it occurs*



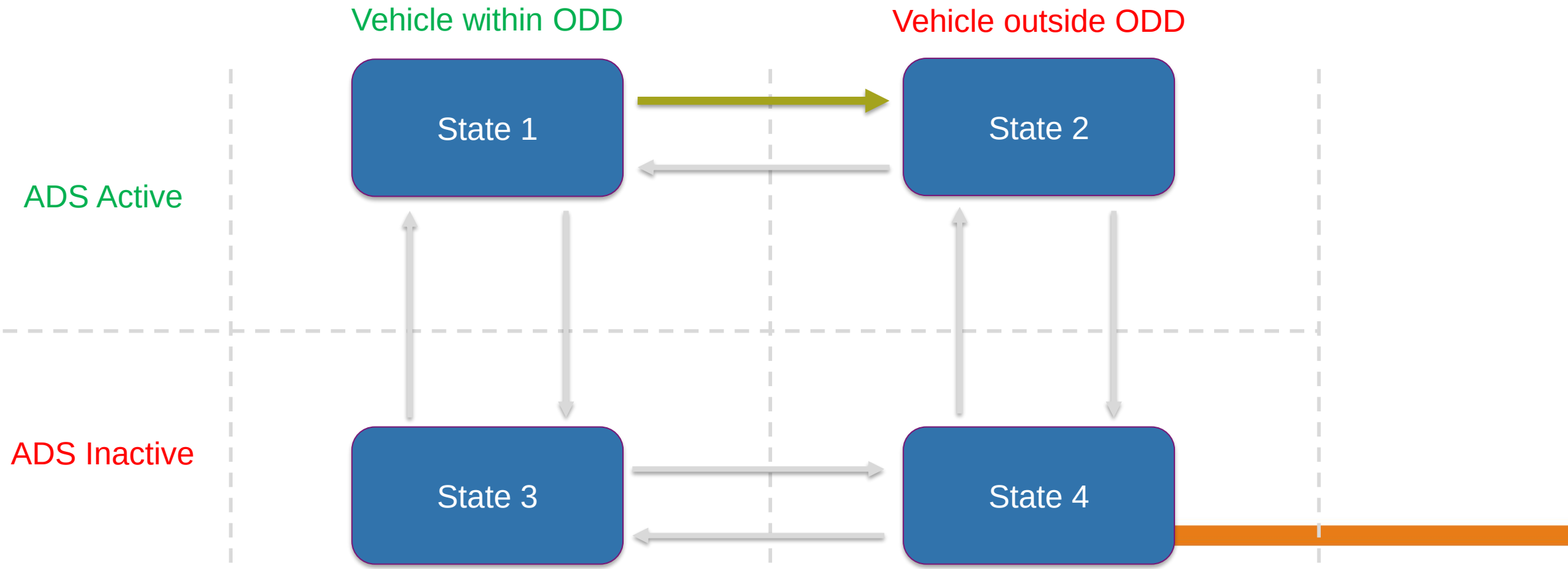
# Example Safety Claims

- *ADS will never cause this transition*



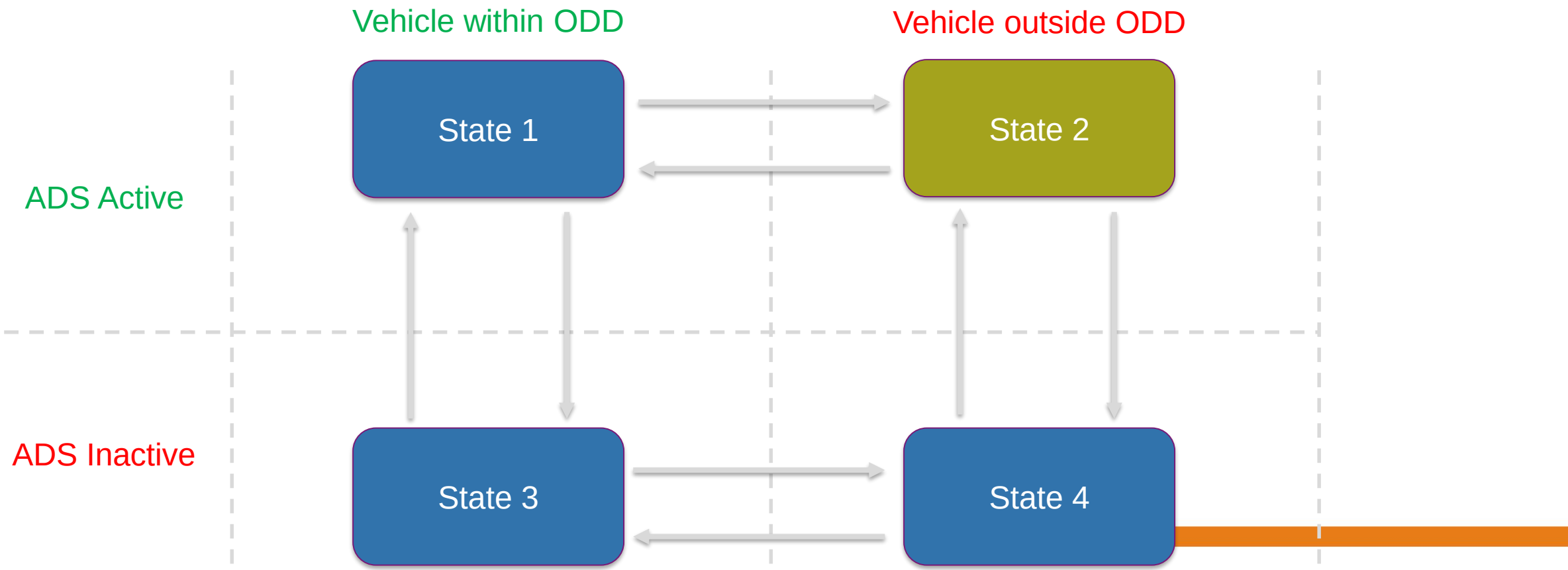
# Example Safety Claims

- *ADS will detect this transition (e.g. due to sudden weather change) and take appropriately safe action*
- *This transition will not occur frequently due to overly narrow ODD*

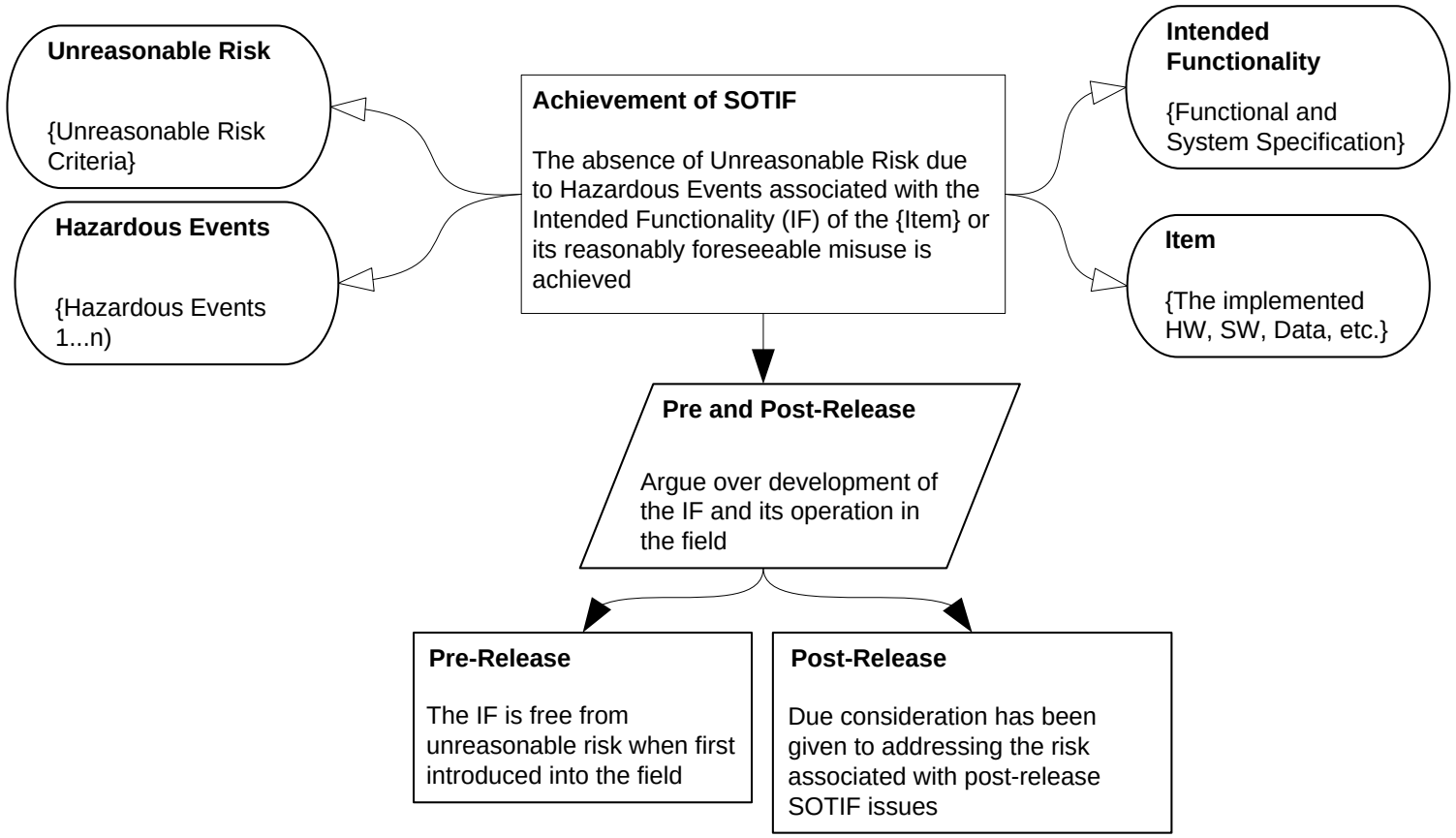


# Example Safety Claims

- *A justifiable strategy exists for managing risk associated with being in this state*

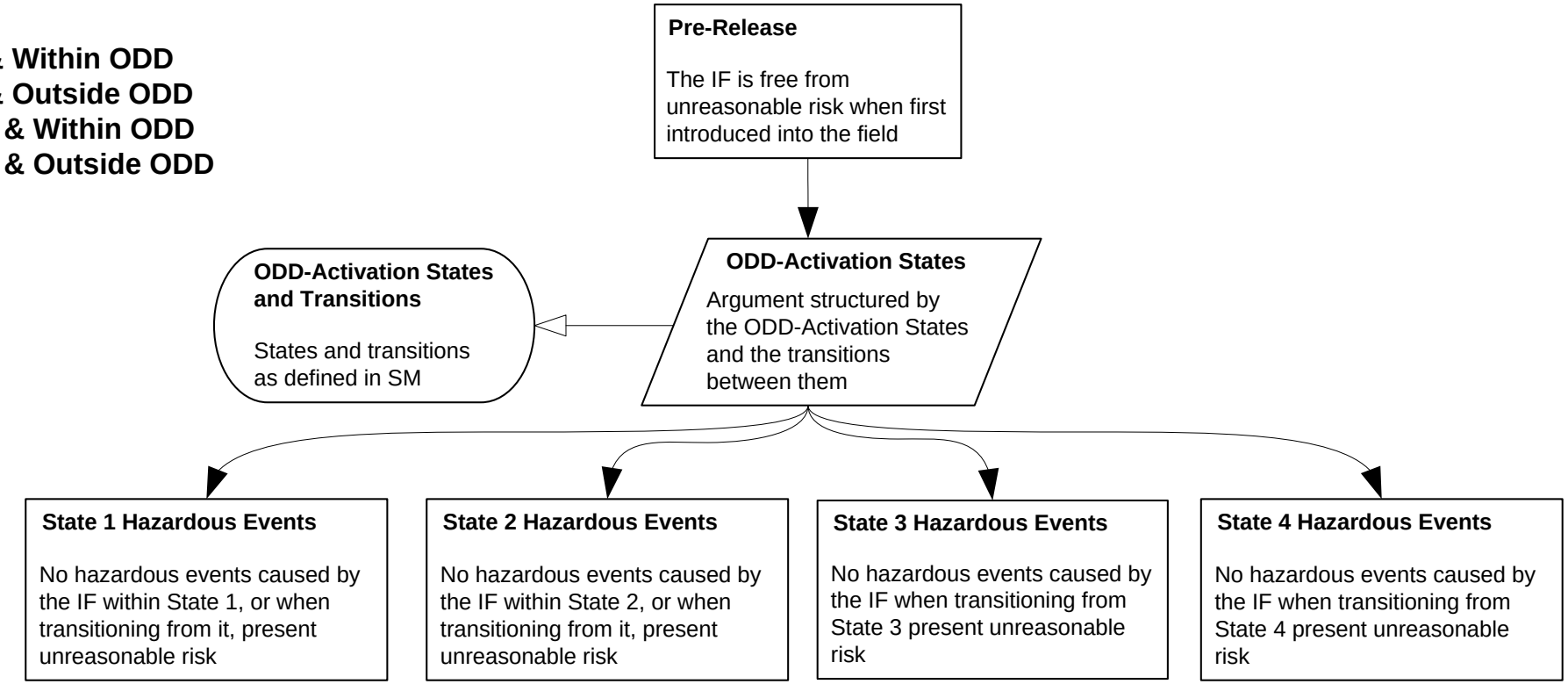


# Safety Argument Pattern



# Safety Argument Pattern

**State1: Active & Within ODD**
**State2: Active & Outside ODD**
**State3: Inactive & Within ODD**
**State4: Inactive & Outside ODD**



## Summary

- ODD plays an important role in safety assurance but should be handled with caution!
- Four “ODD-Activation States” are proposed
- Safety claims can be systematically identified by considering these states and transitions