Safety Management within the HumanDrive Project

11th July 2018

Transport Systems Catapult

HumanDrive Consortium

Richard Hillman

HUMAN DRIVE

Using machine learning to develop

natural, human like vehicle control

Using machine learning to develop natural, human like vehicle control

The **BIG** Ambition

Grand Drive

Autonomous Drive

- ‘Grand Drive’ will be an end-to-end journey of around 200 miles including Motorway, A-Road and Country Road driving
- Using Machine Learning and AI to provide human-like control
- Research into human driving behaviour using physical vehicles and simulator
- Transport Systems Catapult and Horiba MIRA responsible for the Safety Work Package
- Cyber Security covered by a separate Work Package

2017

July 2017
Project Start

2018

Autumn 2018
Static Environment Trials

2019

Summer 2019
Dynamic Trials

Winter 2019
Grand Drive

Dec 2019
Project Complete

HUMAN DRIVE

NISSAN HITACHI Inspire the Next Cranfield University MIRA aimsun. UNIVERSITY OF LEEDS ATKINS highways england CATAPULT Transport Systems SBD

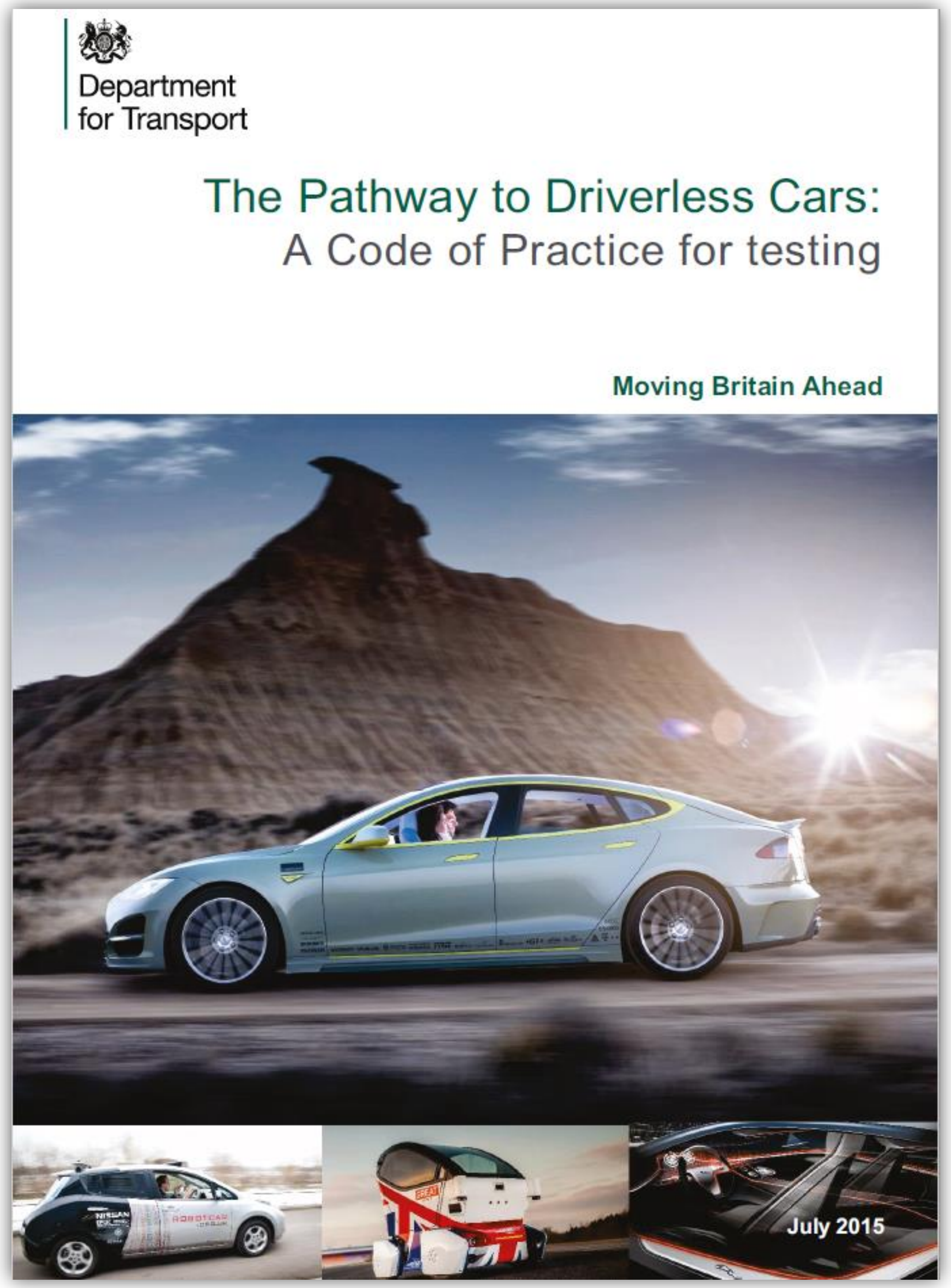
HumanDrive.co.uk @HumanDriveCav HumanDriveCav

We work with Innovate UK

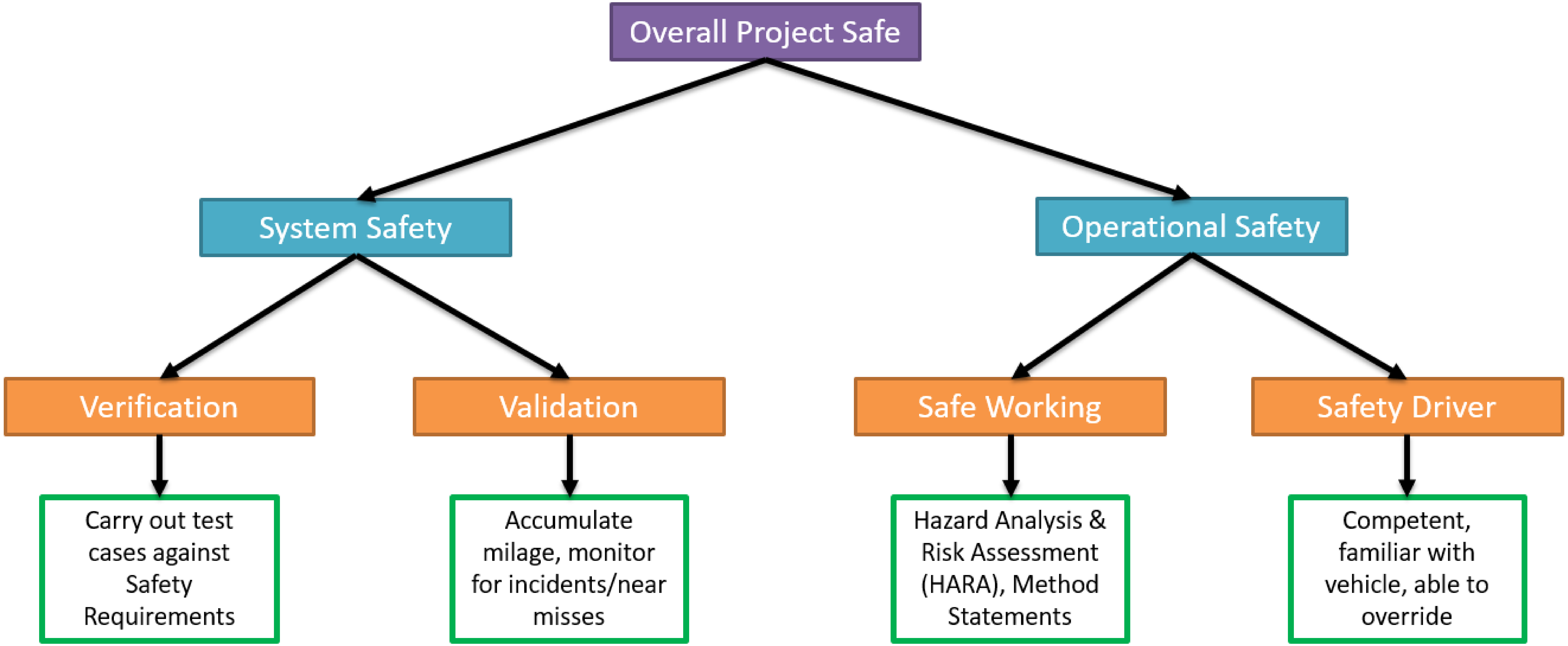
Safety Methodology

- Comply with UK Driverless Cars Code of Practice
- Comply with UK traffic laws
  - Highway Code
  - Road Vehicles (Construction and Use) Regulations 1986
  - Road Traffic Act 1988
- Notify relevant authorities along route

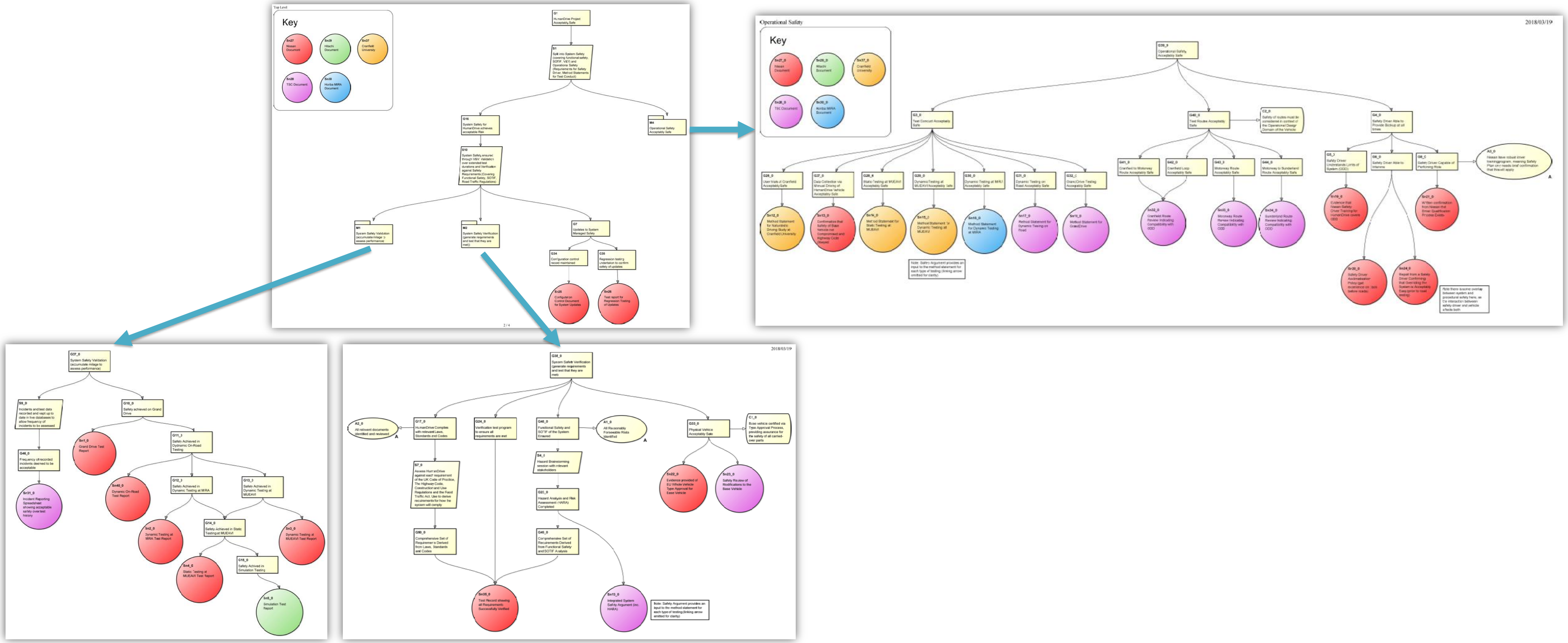
- **Produce Safety Case**, covering
  - Functional Safety - safety when system has fault
  - Safety of the Intended Function (SOTIF) - safe performance when operating as designed
  - Highways England GD04 Risk Assessment
  - Written *with regard* to ISO 26262, but not *strict adherence* to it



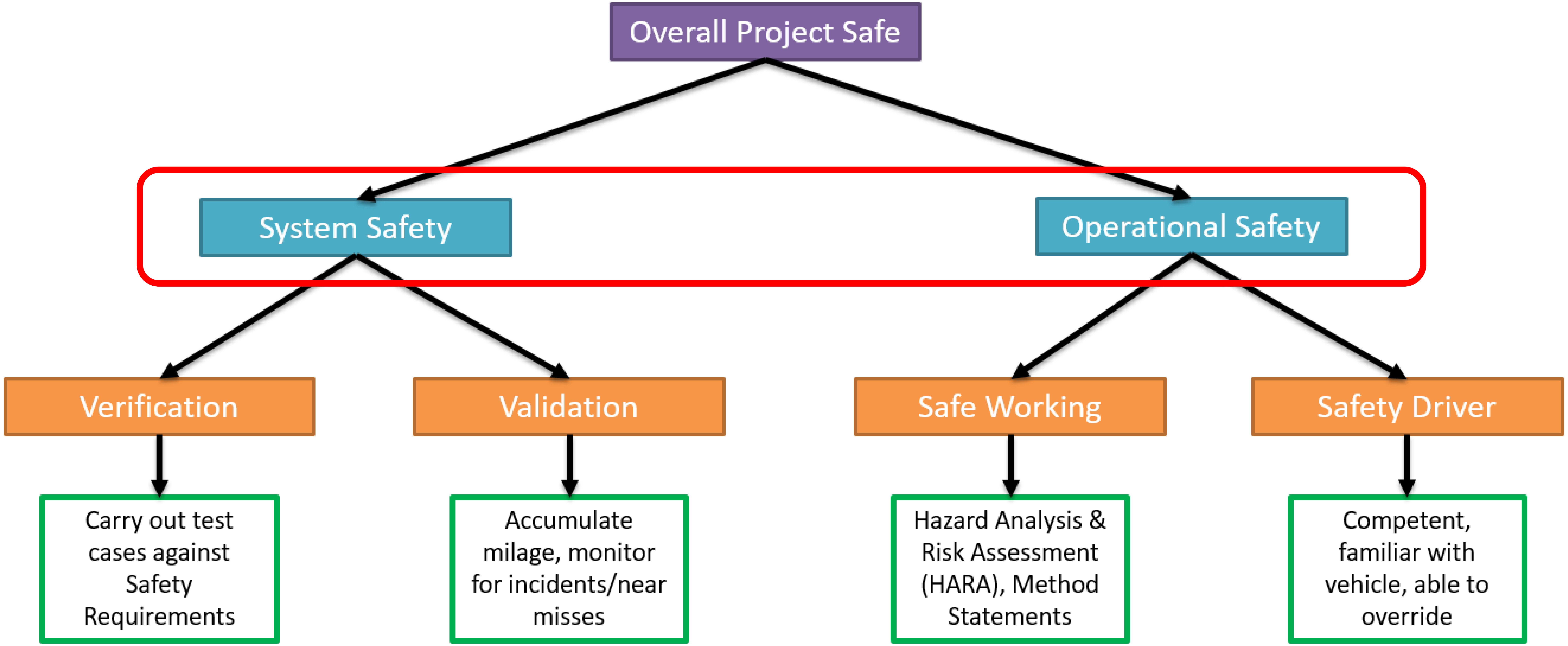
Safety Case 'Pillars'



Safety Case 'Pillars' (Full GSN Model)



Safety Case ‘Pillars’



System Safety Vs Operational Safety

Need to define the 'Operational Design Domain'/ System Boundary

- Geographical locations and road types/ features
- Weather Conditions/ lighting
- Traffic Scenarios/ Types

For example:

- Horse and Rider = In Scope → System Requirement(s)
- Horse and Rider = Not In Scope → Operational Requirement(s) e.g. safety driver take over, motorways only etc.
- Either way → More general requirements for safety driver to correct any errors

This was achieved by:

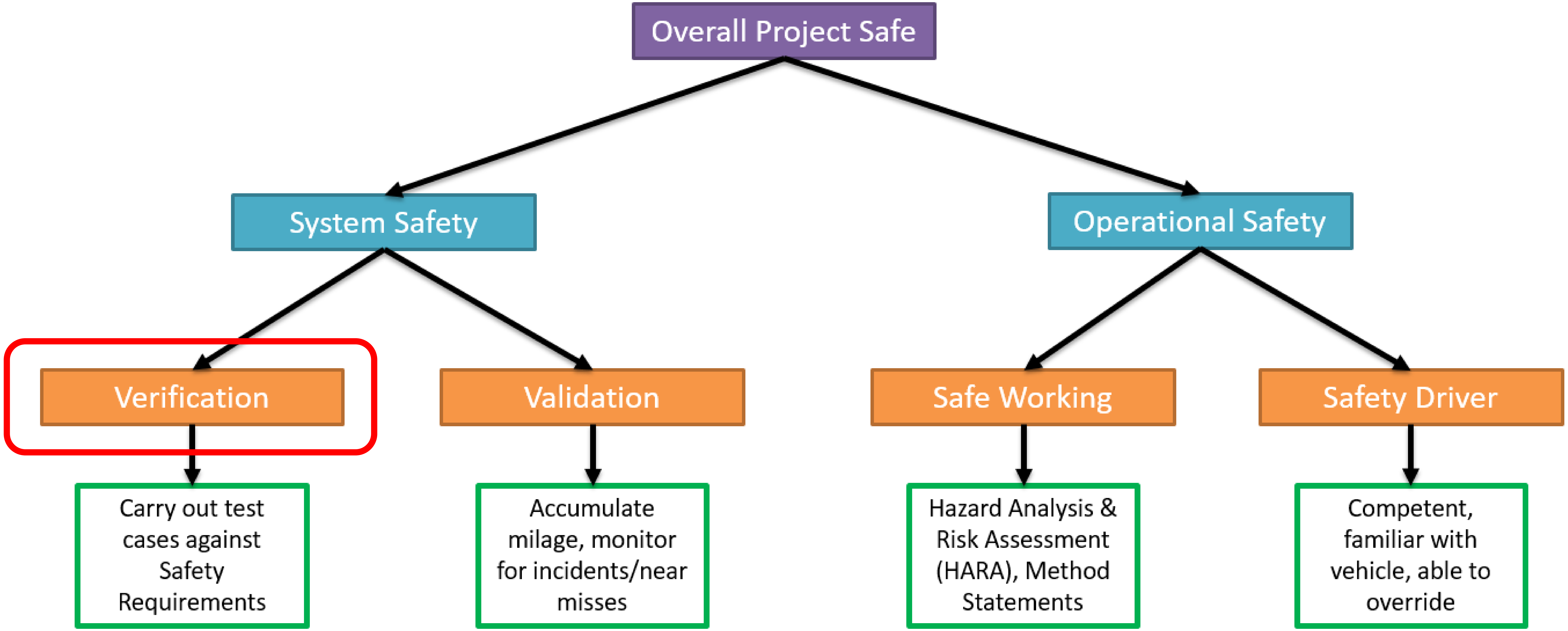
- Review of routes to be used
- Discussion with Nissan / Hitachi
- Review of Code of Practice, Highway Code, Construction & Use regs, Road Traffic Act…….

Regs, Codes and Standards Compliance Review

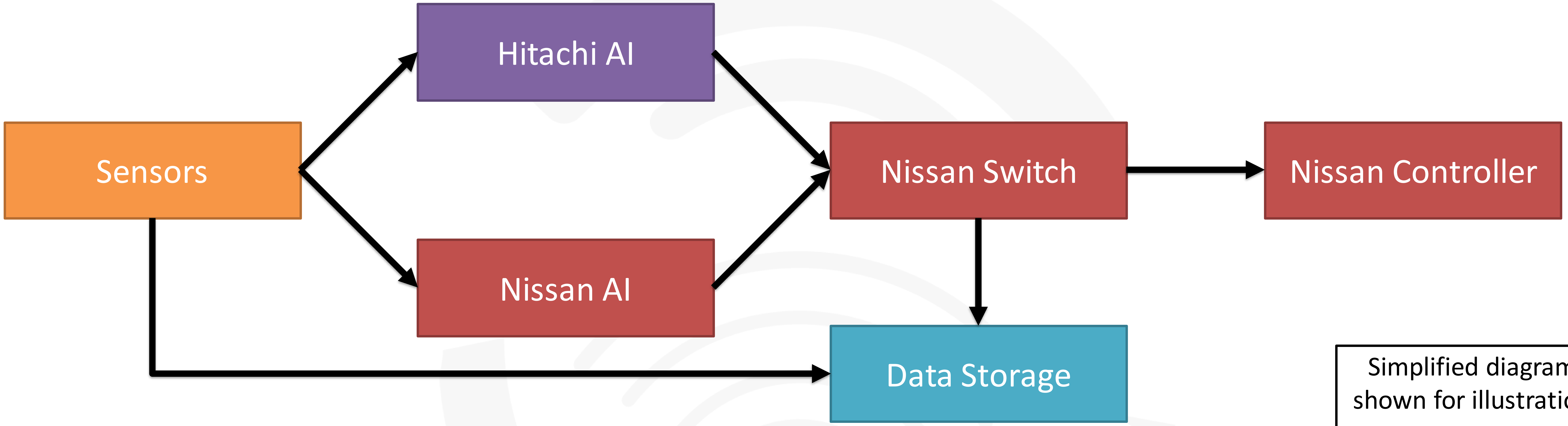
Each ‘objective’ can be addressed with **System Safety** and/ or **Operational Safety** Requirements

HC Rule	Objective	Rele vanc	WP1	WP3	WP4	WP6	WP8	System Safety Requirement(s)	Operational Safety Requirement(s)	Notes
Intro	This section should be read by all drivers, motorcyclists, cyclists and horse riders. The rules in The Highway Code do not give you the right of way in any circumstance, but they advise you when you should give way to others. Always give way if it can help to avoid an incident.			x	x			The autonomous system shall attempt to avoid a collision when possible, regardless of right-of-way	The safety driver shall intervene when they perceive an unacceptable risk (optimal intervention may be to apply brakes or throttle, to correct steering, or to take full manual control)	
103	Signals warn and inform other road users, including pedestrians (see ‘Signals to other road users’), of your intended actions. You should always •give clear signals in plenty of time, having checked it is not misleading to signal at that time •use them to advise other road users before changing course or direction, stopping or moving off •cancel them after use •make sure your signals will not confuse others. If, for instance, you want to stop after a side road, do not signal until you are passing the road. If you signal earlier it may give the impression that you intend to turn into the road. Your brake lights will warn traffic behind you that you are slowing down •use an arm signal to emphasise or reinforce your signal if necessary. Remember that signalling does not give you priority			x	x			Indicator signals to other road users shall be given autonomously for every manouvre for which much signals are appropriate Indicator signals must be provided at least 2 seconds (TBC) before the manourvre commences Indicator signals must be cancelled not more than 2 seconds after the manoeuvre for which they are given is completed Indicator signals shall be inhibited at any point in time where there is a likely alternative manoeuvre that the signal would also signify (e.g. don't indicate left for a future turn or to stop if there is another left turn that will be passed prior to the intended manoeuvre)	The safety driver shall correct any erroneous signals/ lack of signals given by the autonomous system	
104	You should also •watch out for signals given by other road users and proceed only when you are satisfied that it is safe •be aware that an indicator on another vehicle may not have been cancelled			x	x			The autonomous system shall attempt to avoid a collision when possible, regardless of right-of-way The autonomous system shall retain a sufficient error margin to ensure a collision is avoided even if other road users act in an unpredictable way (e.g. if they accelerate suddenly or move contrary to their indicator signals)	The safety driver shall intervene when they perceive an unacceptable risk (optimal intervention may be to apply brakes or throttle, to correct steering, or to take full manual control) The safety driver shall correct any erroneous signals/ lack of signals given by the autonomous system	
105	You MUST obey signals given by police officers, traffic officers, traffic wardens (see ‘Signals by authorised persons’) and signs used by school crossing patrols.			x				Production solution: The vehicle must be able to respond to humans directing traffic by being able to reconise the signal being given and respond accordingly	The Safety Driver shall intervene to comply with signals given by humans directing traffic (police, traffic officers etc.)	
	Police stopping procedures. If the police want to stop your vehicle they will, where			x				Production solution: The autonomous system shall be able to respond	The Safety Driver shall take manual control to respond to an	

Safety Case ‘Pillars’



Functional Architecture Diagram



Simplified diagram shown for illustration purposes

Key points:

- Redundancy between processing systems if one suffers functional failure
- No redundancy in sensors/ actuators – hand over to driver
- Limited ability to detect non-functional errors (incorrect values, e.g. poorly chosen path) - **Safety Driver Responsible** for ensuring vehicle follows safe path

Analysis of the Functional Architecture

HAZID (Hazard Identification) documented how faults propagate through this architecture

- Assumes one fault at a time (other than where faults can remain latent)
  - no output/ uninterpretable output
  - a clearly wrong output and
  - an incorrect but plausible output
- Considers each sub-subsystem within the architecture in turn

System Description					Failure Effect / Safety impact			Potential Outcome											
Owner	Sub-System	Sub-sub-system	Failure Mode	Possible Failure Causes	Local	HumanDrive System	Operational situation with harm Safety impact	Loss of AD Control	Unintended Braking	Unintended Accel	Unintended Steering	Lack of Braking	Lack of Accel	Lack of Steering	Driver take Control	Detection Method	Existing Controls Risk Elimination or Mitigation Measures	Additional Controls Risk Elimination or Mitigation Measures	Safety Goal

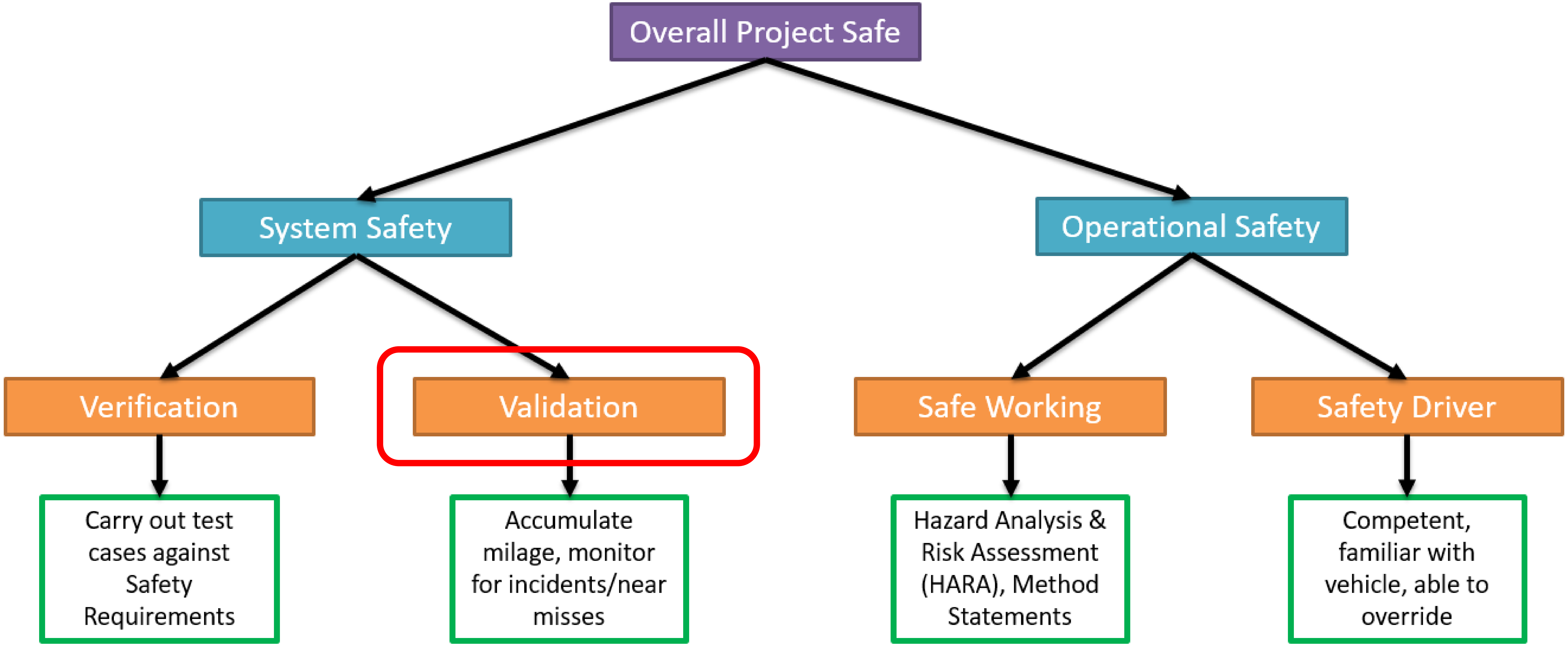
Output of this was:

- **Safety Goals** derived directly from this functional analysis
- List of possible **vehicle level errors** to use in Hazard Analysis and Risk Assessment (HARA)…….

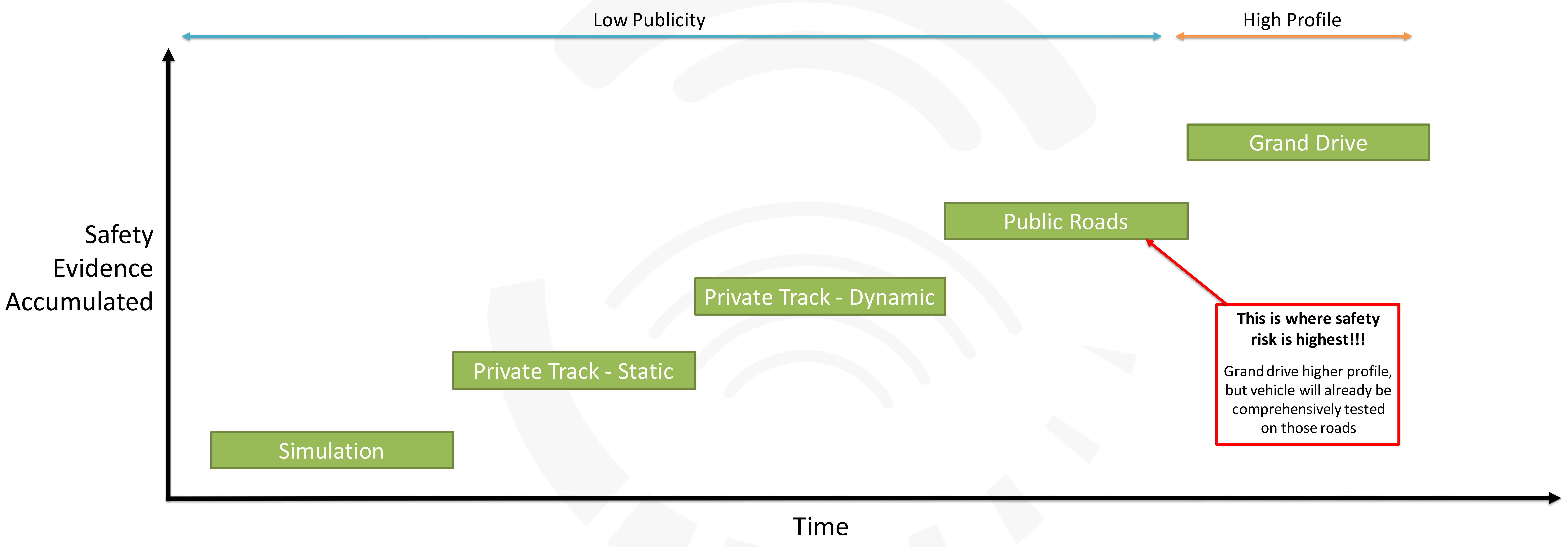
Verify Safety of Physical Vehicle

- **Type-Approved base vehicle (Nissan Leaf)** – not proportionate to repeat tests
  - Crash testing
  - Pedestrian Protection
  - ABS, ESC
  - Electromagnetic Compatibility (EMC)
- **Visual inspection to confirm modifications are safe**
  - No hardware mounted where it could cause injury (accident or normal use)
  - No hardware that could be contacted by airbag
  - No hardware that could contact a pedestrian
  - All hardware securely attached
  - Field of view not compromised
- **Review with Fire Service**
- **Would need more thorough review if not based on production vehicle**

Safety Case 'Pillars'

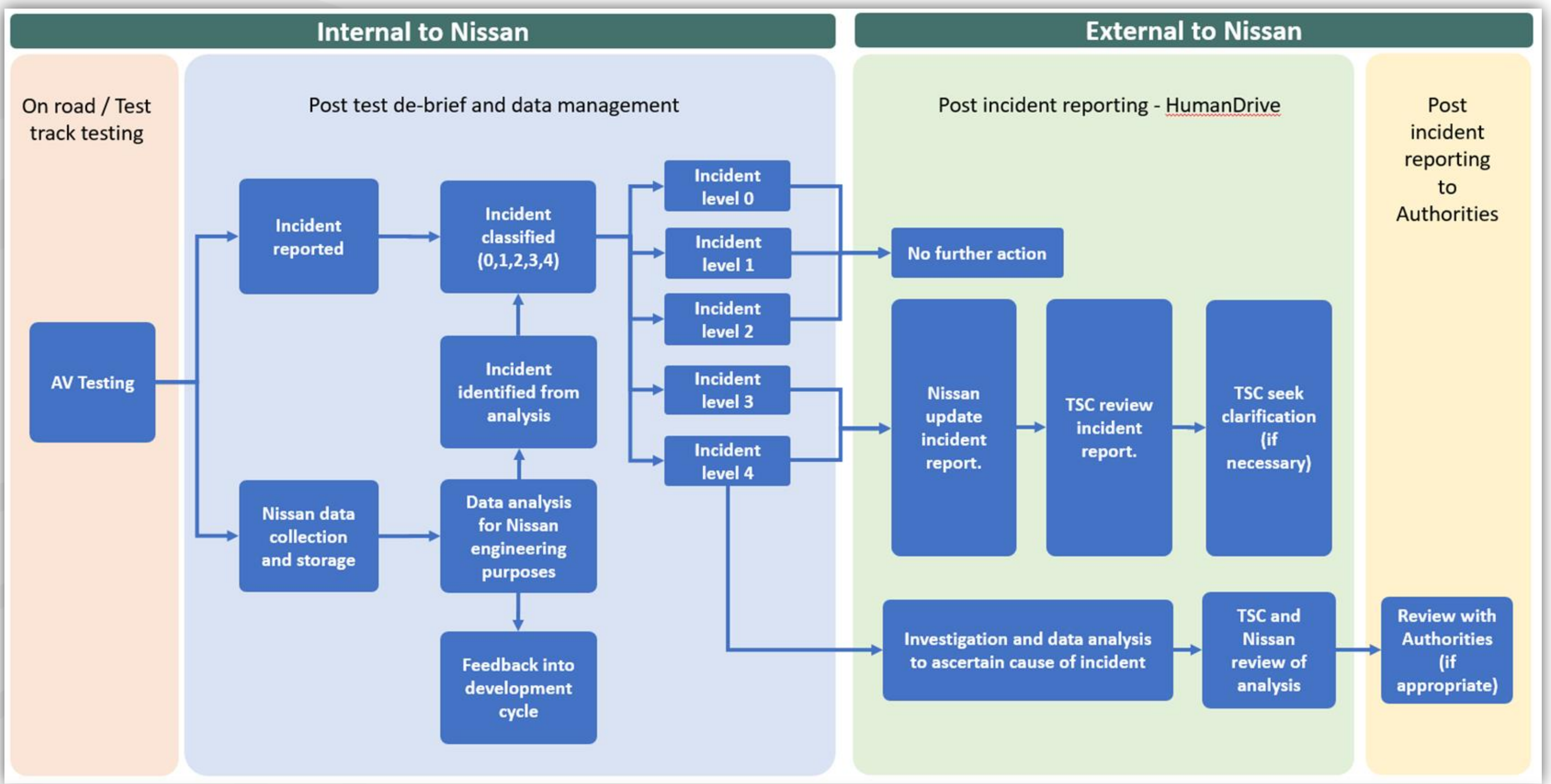


Building Safety Evidence



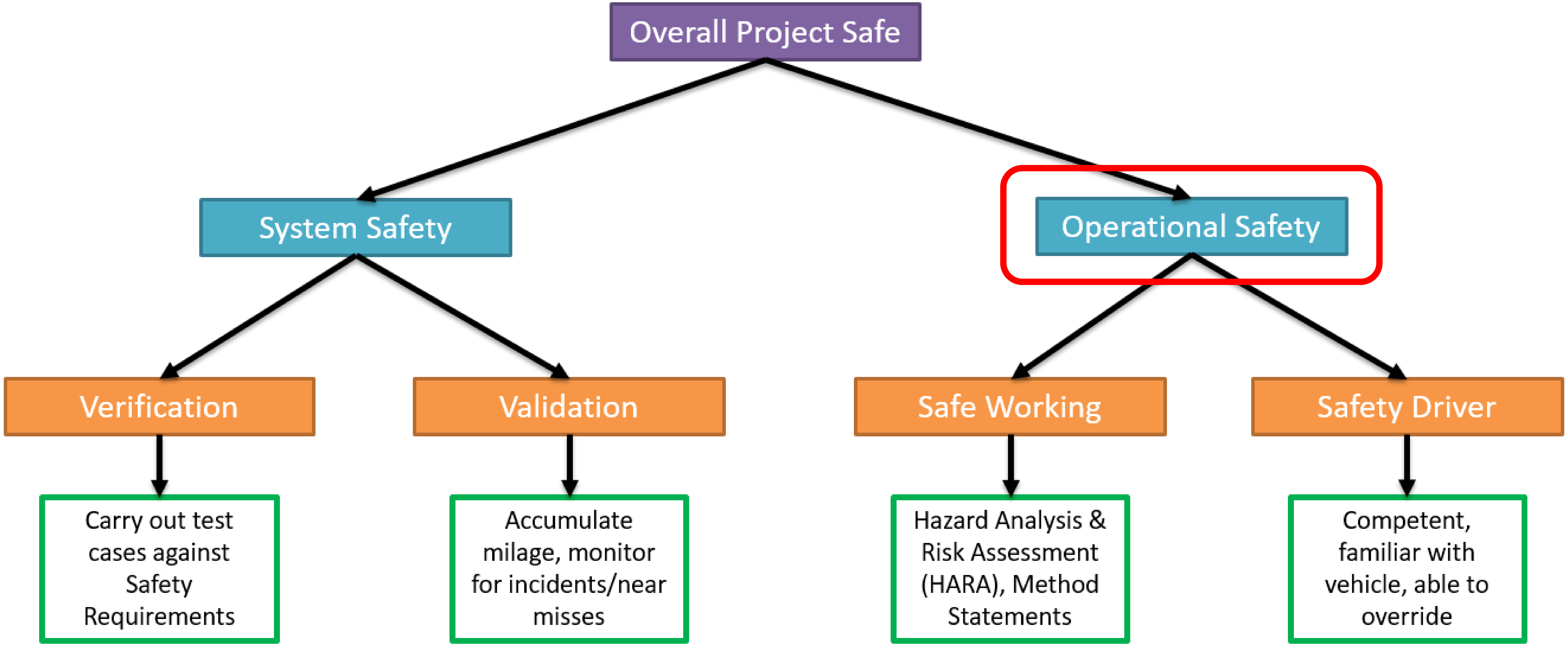
Incident Reporting

- Formal process for incident reporting agreed and documented
- All incidents feed back into development cycle
- Accidents and near misses to be reviewed with TSC
- Assists appropriate response to incident itself
- Allows an overall impression of safety performance to be built up over time

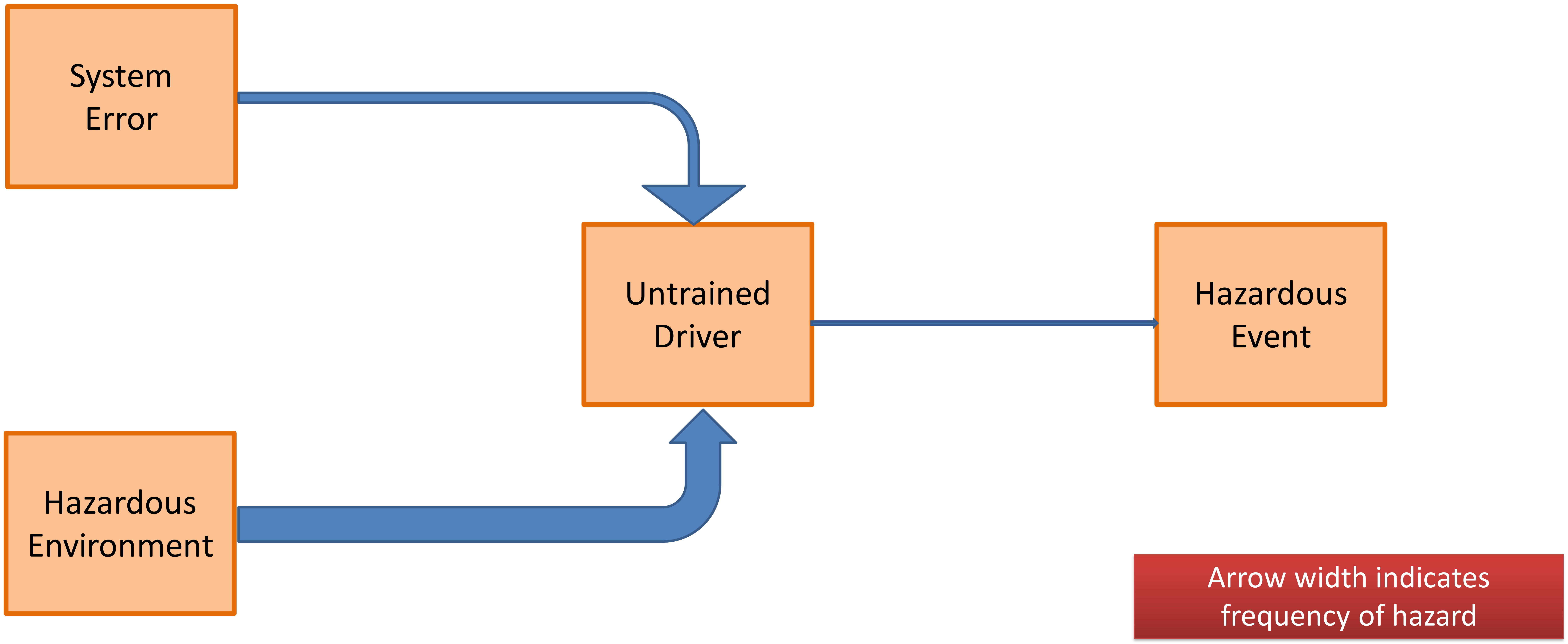


ID No.	Date	Time	Vehicle ID	Incident Description 1 or 2 sentences describing nature and severity	Location e.g. City Street/ Highway/ Coutry Road/ Motorway	Conditions e.g. Sunny/ raining/ cloudy/ night/ wet surface/ fog etc.	Incident Duration	Test Type e.g. static obstacles, private roads, dynamic obstacles, private/ public road, Grand Drive	Incident Definition Use code on 'Incident Definitions' tab
Example	09/12/2017	14:15	NS16 TSC	Vehicle drifted over centre markings as oncoming traffic approached. Safety driver corrected path to ensure safe passing distance	Country Road	Sunny, wet surface	1-2 seconds	Dynamic testing on public road	2

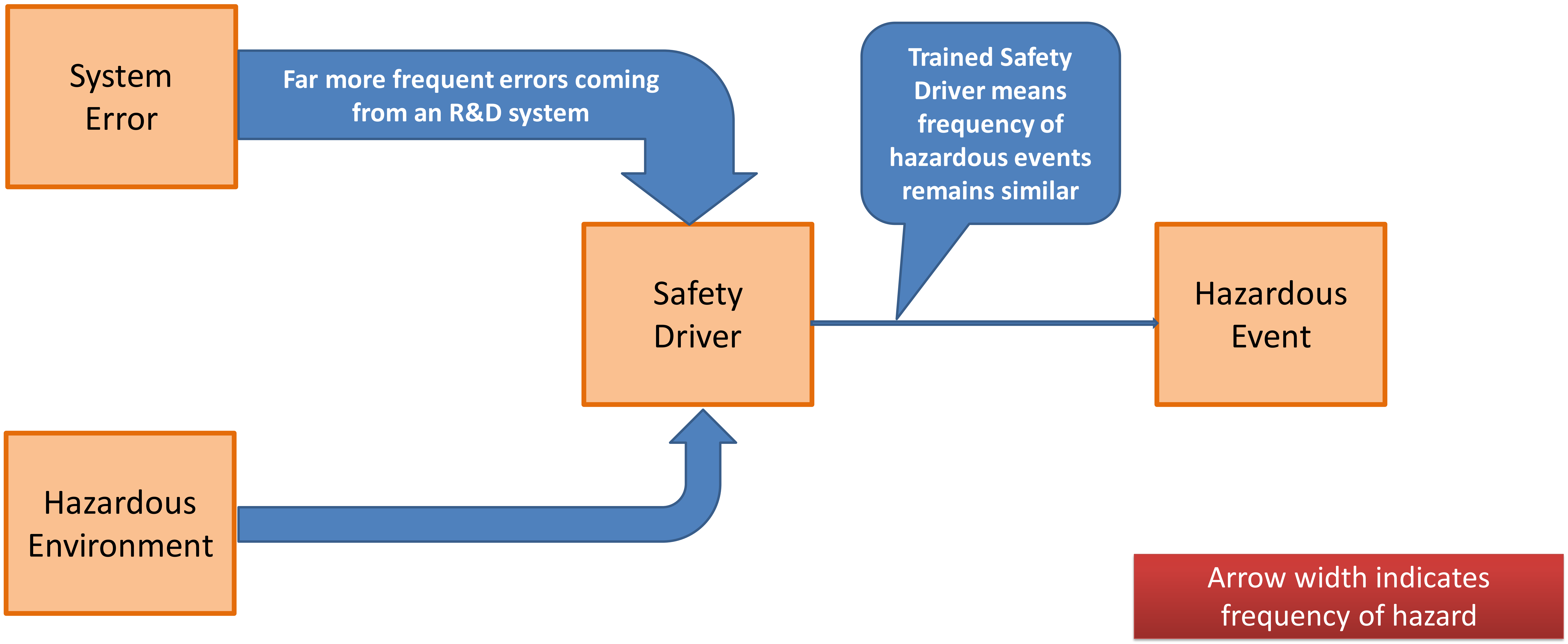
Safety Case 'Pillars'



Production System

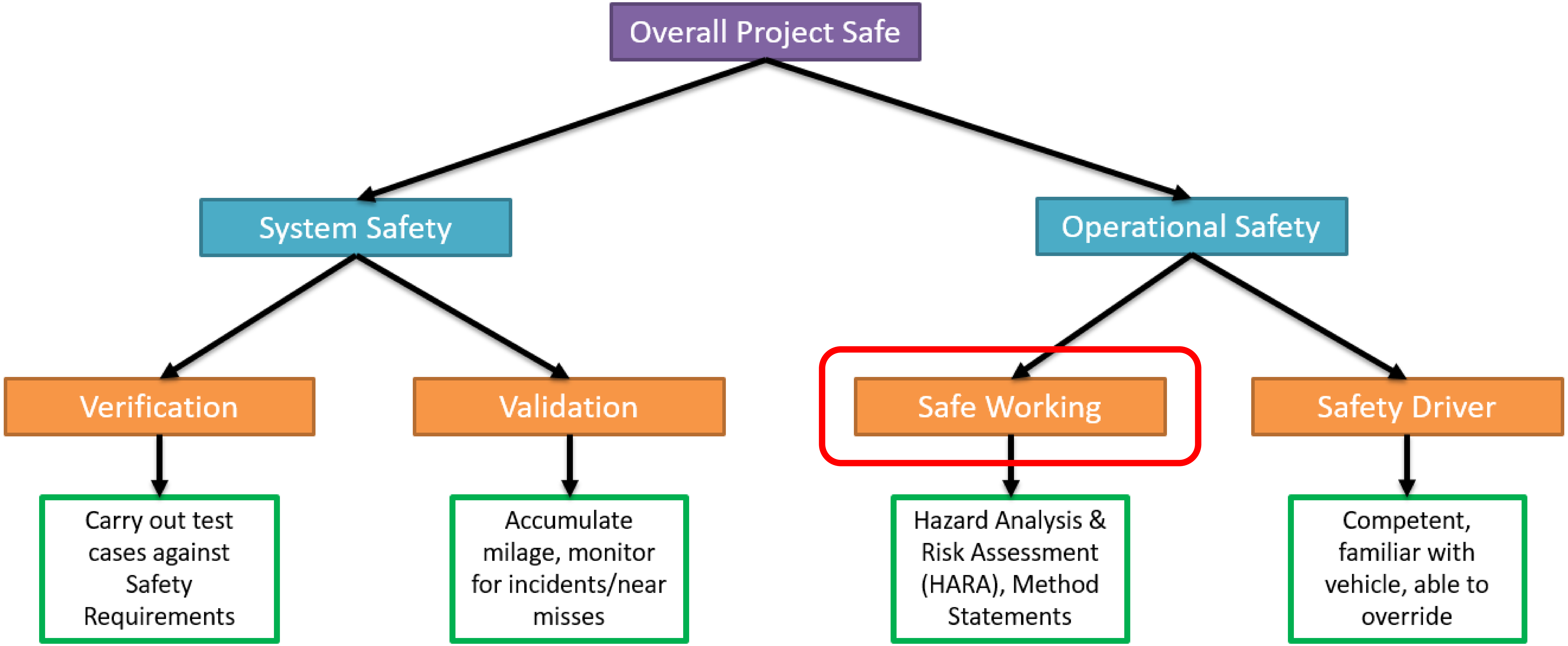


R&D System



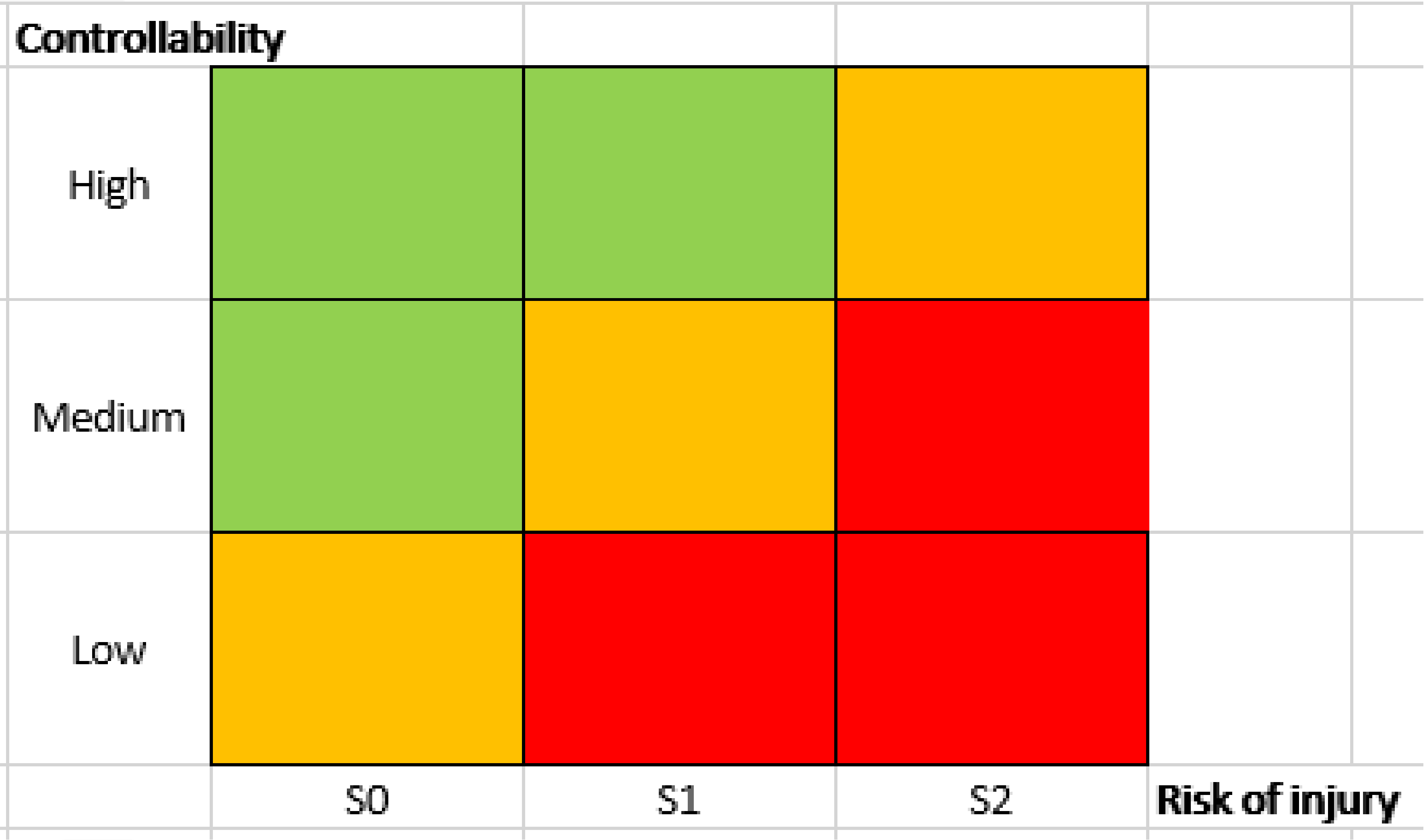
System Error
Far more frequent errors coming from an R&D system
Trained Safety Driver means frequency of hazardous events remains similar
Safety Driver
Hazardous Event
Hazardous Environment
Arrow width indicates frequency of hazard

Safety Case ‘Pillars’



Scoring System for HARA

- **‘Risk of Injury’** is a multiple of scores for:
  - Road Type (Motorway, Dual Carriageway, Single Carriageway)
  - Traffic Flow (Free Flow, Unstable Flow, Breakdown Flow)
  - Road Set-Up (Straight, Normal Curve, Tight Curve, Roundabout etc.)
  - Scenario (Unintended Steering, Lack of Braking, Unintended Acceleration etc.)



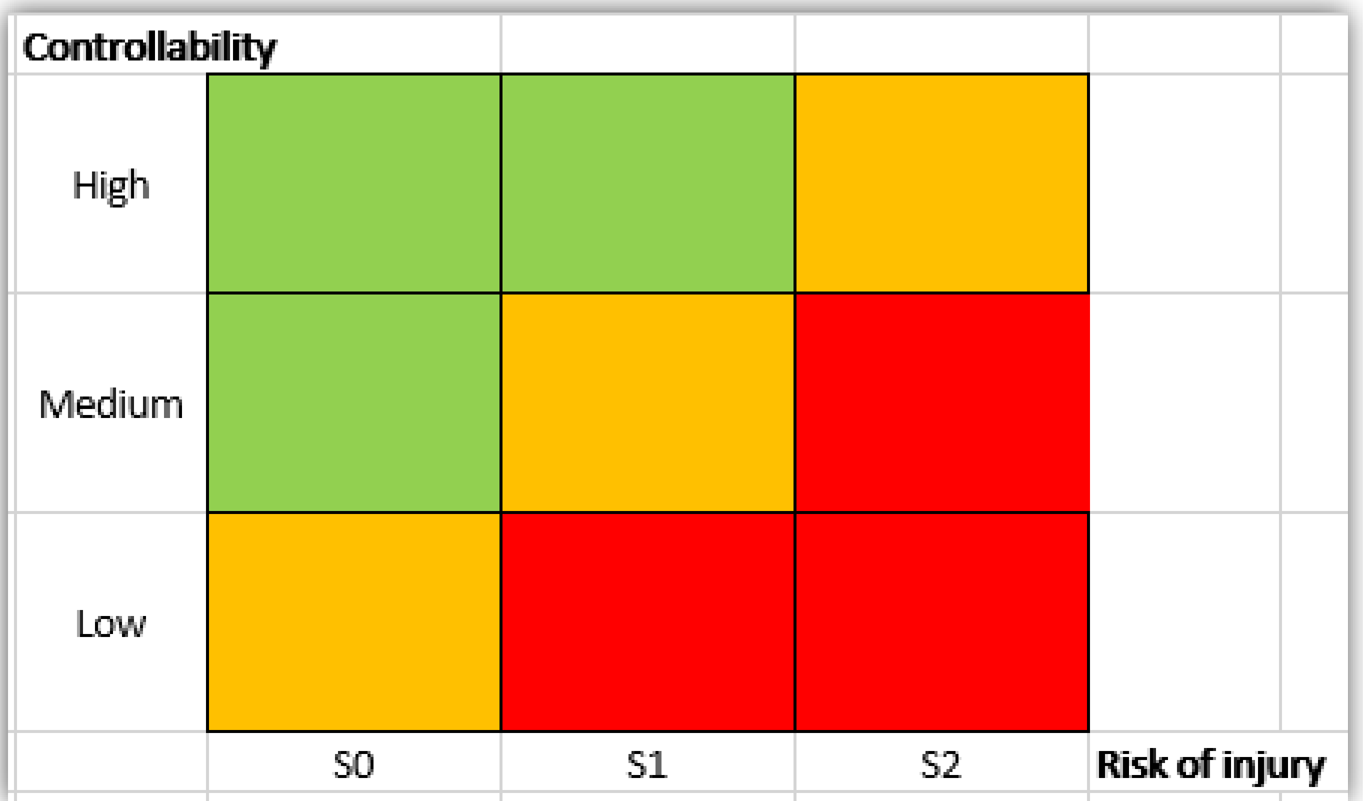
- **‘Controllability’** reflects Safety Driver intervention
  - How is error detected?
    - Prior warning
    - Alert provided as failure occurs
    - Driver only detects when which drifts off path/ fails to brake
  - What reaction time is available?
    - Depends on speed, lane width, traffic density etc.

Q4 – WP8 - HARA Workflow

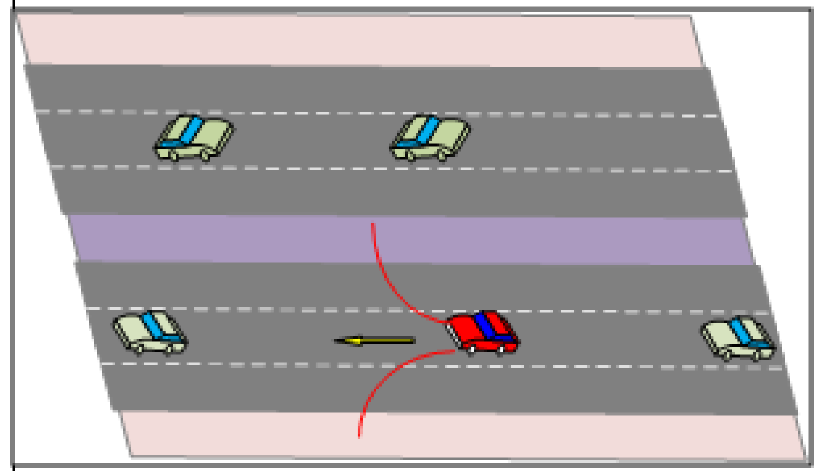
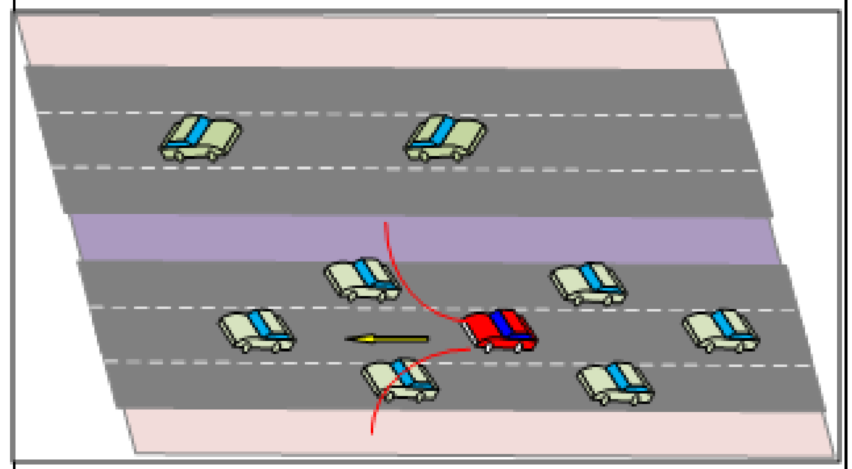
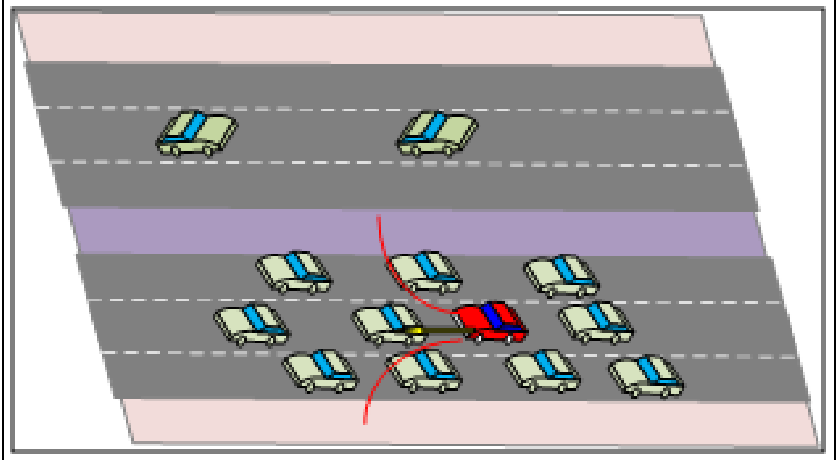
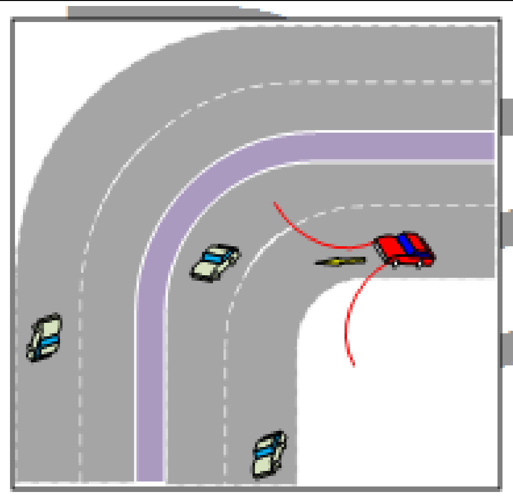
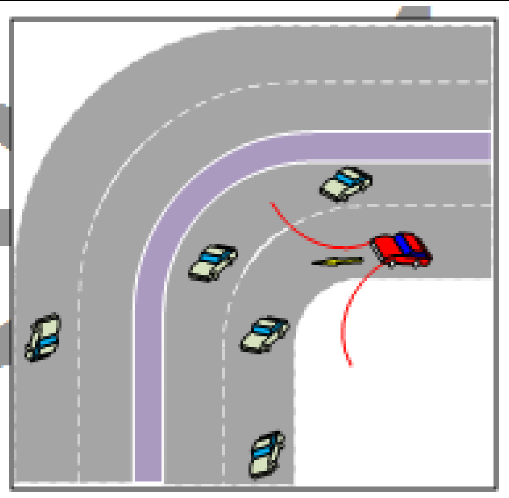
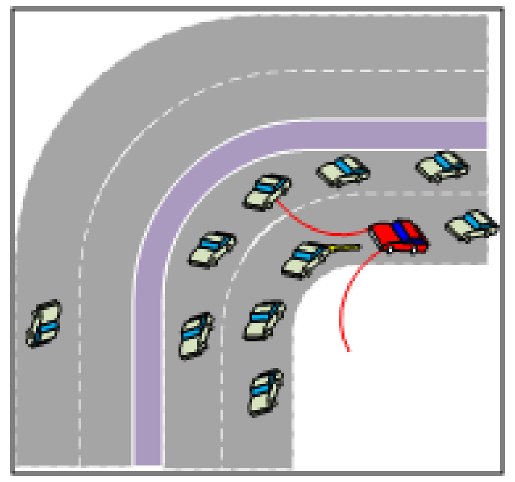
For each combination of factors (e.g. Dual Carriageway, Free Flow, Straight Road, Unintended Steering)

1. Multiply the weightings to get raw score (e.g. 0.3 x 0.1 x 0.1 x 0.8 = 0.0024)
2. Convert raw score into Risk of Injury Rating (S0 in example)
3. Assess controllability with normal driver in production L4 vehicle (e.g. Medium)
4. Use the table to classify scenario as Red, Amber or Green (example would be green)
5. Modify this baseline to reflect trained Safety Driver in HumanDrive vehicle
   a) Should the 'Risk of Injury' score be updated?
   b) Will the controllability increase?
6. Prioritise scenarios
   a) Green = OK
   b) Amber = Test to confirm controllability, allowable as long as risks 'ALARP'
   c) Red = Test to confirm controllability. If scenario remains red, remove from scope

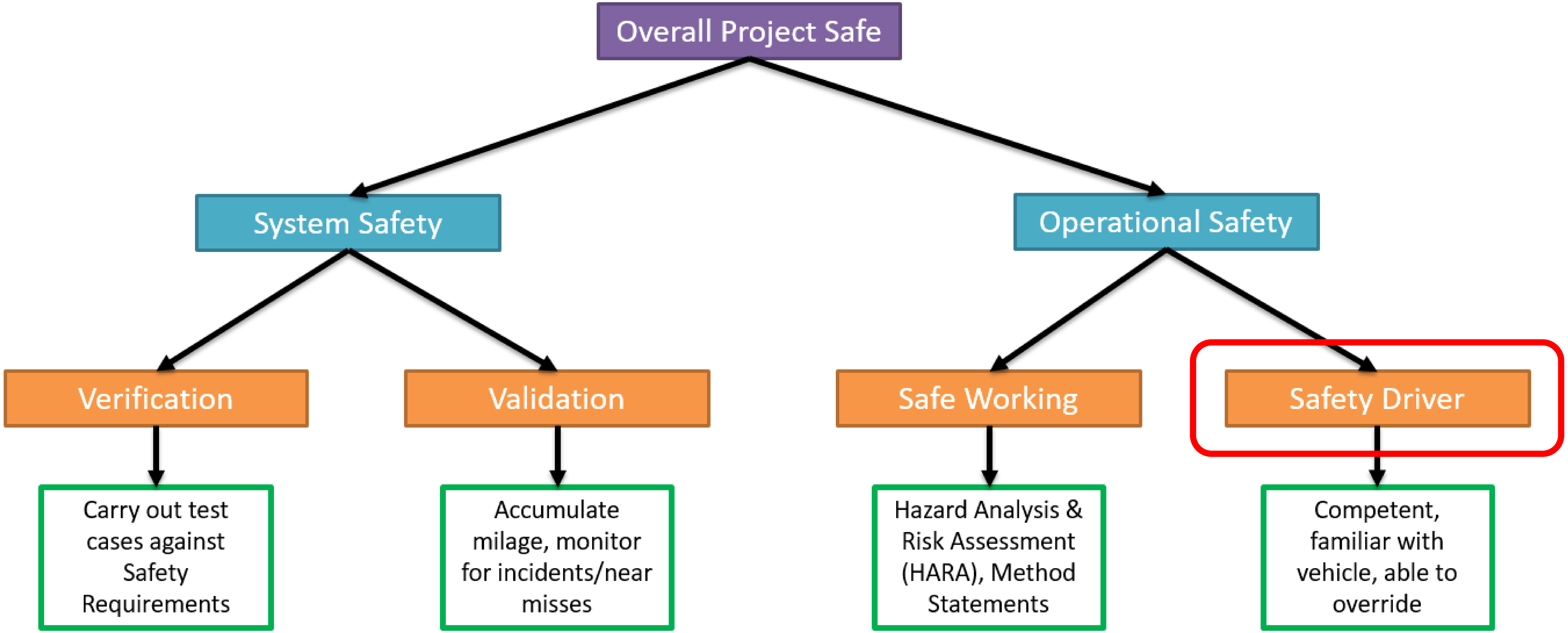
S0	0 to 0.005
S1	0.006 to 0.0447
S2	0.0448 to 0.16



Hazard Analysis and Risk Assessment

		Scenario to be tested (with A2 driver)	Free Flow	HARA line#	Acceptance would validate HARA line #	Can be validated by HARA line #	Unstable Flow	HARA line#	Acceptance would validate HARA line #	Can be validated by HARA line #	Forced or Breakdown Flow	HARA line#	Acceptance would validate HARA line #	Can be validated by HARA line #
Motorway	Straight	Note: Possibly no testing required if similar test for "Dual carriageway - straight" is marked as "acceptable" and stay within line width (total 3)												
		- Unintended or not permitted transition to HD mode	Not required - marked as "acceptable" without further test				Not required - marked as "acceptable" without further test				Not required - marked as "acceptable" without further test			
		- Unintended transition to MD mode	Not required - marked as "acceptable" without further test				Not required - marked as "acceptable" without further test				Not required - marked as "acceptable" without further test			
		- Unintended brake actuation	Not required - marked as "acceptable" without further test				Possibly no testing required				Possibly no testing required			
		- Unintended acceleration	Not required - marked as "acceptable" without further test				Not required - marked as "acceptable" without further test				Not required - marked as "acceptable" without further test			
		- Unintended steering actuation	Not required - marked as "acceptable" without further test				Not required - marked as "acceptable" without further test				Not required - marked as "acceptable" without further test			
		- Lack of brake actuation	Not required - marked as "acceptable" without further test				Possibly no testing required				Not required - marked as "acceptable" without further test			
		- Lack of acceleration	Not required - marked as "acceptable" without further test				Not required - marked as "acceptable" without further test				Not required - marked as "acceptable" without further test			
		- Lack of steering actuation	Not required - marked as "acceptable" without further test				Not required - marked as "acceptable" without further test				Not required - marked as "acceptable" without further test			
Motorway	Normal curve	Note: Possibly no testing required if similar test for "Dual carriageway - Normal curve" is marked as "acceptable" and stay within line width (total 3)												
		- Unintended or not permitted transition to HD mode	Not required - marked as "acceptable" without further test				Not required - marked as "acceptable" without further test				Not required - marked as "acceptable" without further test			

Safety Case 'Pillars'



Safety Driver Requirements

HARA results in requirements to prove that Safety Driver can intervene in critical scenarios

- Demonstrated by injecting faults on test track
- If not possible to show it is safe, remove from Operational Design Domain (i.e. take manual control at that point)

More generally, it must be shown that the Safety Driver is:

- Skilled at controlling vehicles
- Familiar with road traffic laws in the country
- Familiar with the Operational Design Domain of the specific test vehicle
- Familiar with physically taking control of the specific test vehicle

Also must verify that vehicle is able to accept overrides

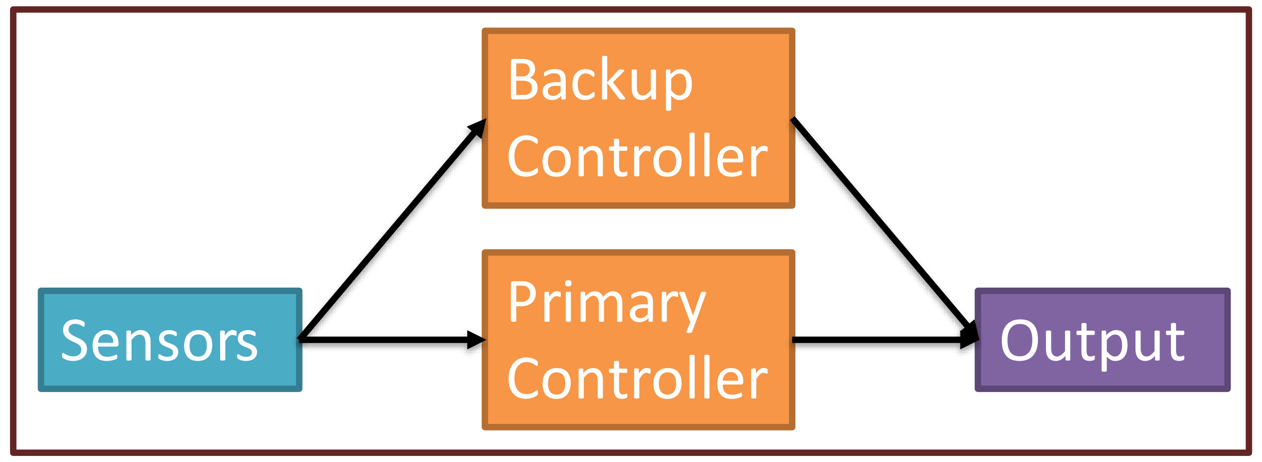
(i.e. driver doesn't have to fight against vehicle)

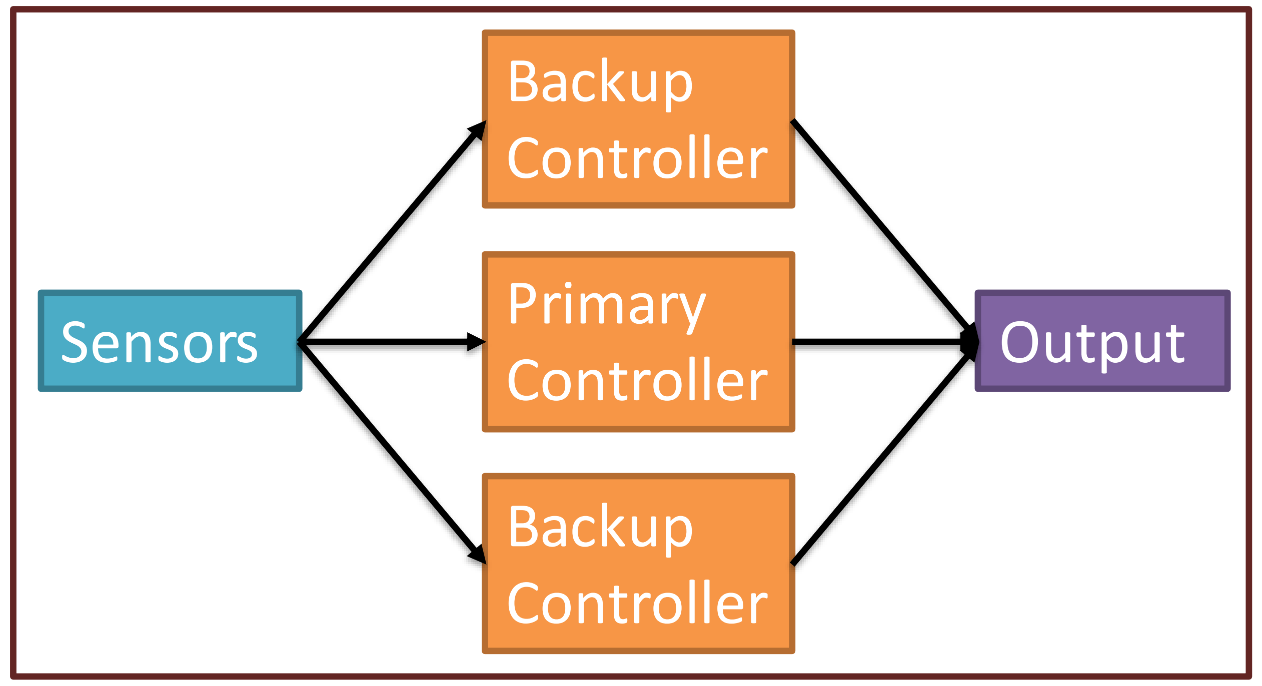
Challenge of Removing Safety Driver (1)

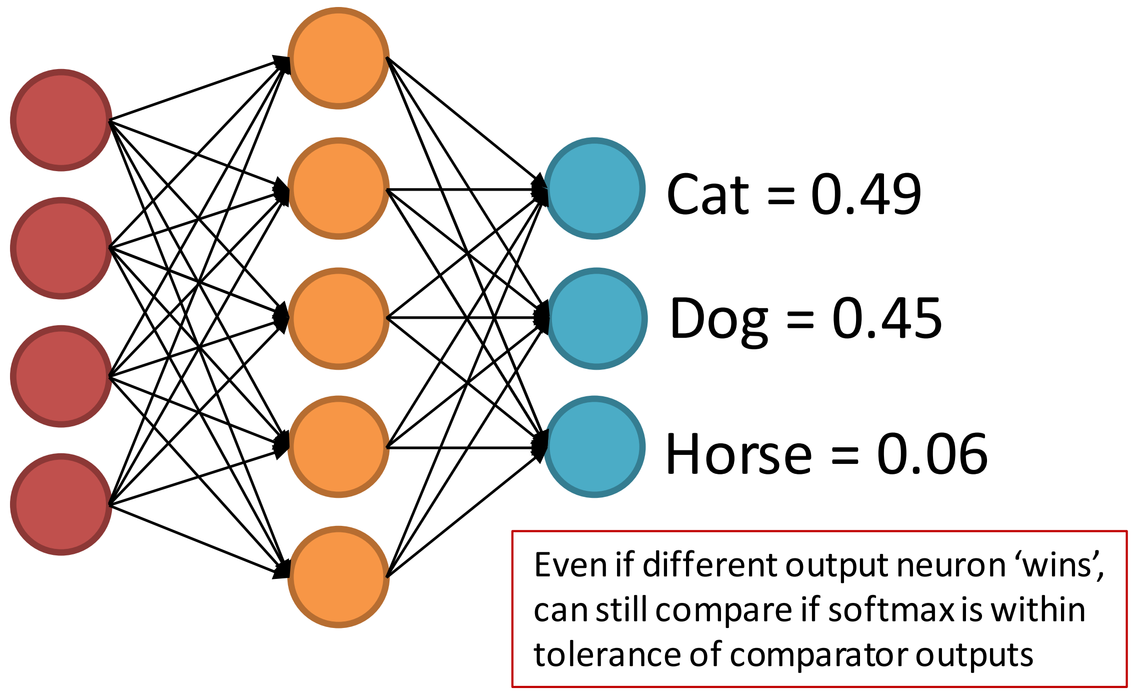
- Can L4/ L5 driving be achieved without checking the suitability of the path?
  - HumanDrive architecture provides redundancy for failure/ detected fault
  - Many errors expected to be due to limitations of system (perception, judgement), not faults

- Is 3-Way Check needed?
  - If 2-Way used, which is correct?

- 3 different subsystems would produce 3 different outputs
  (3 way check can't compare perception/ judgement if 3 subsystems are duplications)
  - Is it possible to have a 'safety curtain' where discrepancy is allowed only up to a threshold?
  - What about divergent outcomes? (e.g. avoid to left or right, no or no-go at junction in marginal decision)
    - Perhaps a tolerance band can be allowed for the output of 'Softmax' neurons in Artificial Neural Network







Challenge of Removing Safety Driver (2)

- Would also need redundancy in sensors and actuators
- Sensor redundancy makes classification complex (train system separately for failure of each sensor?)

- Should backup system(s) use traditional algorithms rather than Neural Networks?
  - Traditional algorithms have established safety standards (e.g. ISO26262 – robust development and verification methodology)
  - But is it possible to model how to negotiate complex situations (e.g. when to pull out at junction)?

- Validation of Neural Networks represents a new challenge for industry
  - Need standards for AI training robustness – arguably more important than coding of network!
  - How much physical milage will be needed?
  - Should key test cases be required (as per EuroNCAP active safety testing)
  - Simulation essential to gain sufficient milage/ coverage – how can regulators validate tools?

Conclusion

Safety Case should include:

- Evidence that risks associated with system and its operation have been identified, mitigated where necessary, and any mitigations verified
- Evidence of sustained safe performance before moving on to more challenging environments
- Evidence that the safety driver is capable of intervening
- Evidence that traffic laws and the Code of Practice are being adhered to

HumanDrive Consortium

http://humandrive.co.uk

Richard.Hillman@ts.catapult.org.uk

Using machine learning to develop natural, human like vehicle control

HUMAN DRIVE