
semcon
PRODUCT
DEVELOPMENT
BASED ON
HUMAN
BEHAVIOUR.

Safer Transitions of Responsibility for Highly Automated Driving: Designing HMI for Transitions with Functional Safety in Mind.

Matthew Sassman and Richard Wiik

Semcon Sweden AB

Presented by Matthew Sassman

Agenda

1. Aim/Purpose of the paper
2. Highly Automated Driving
3. ISO 26262: Road Vehicles - Functional Safety
4. Transitions of Responsibility: Protocols and Failures
5. Ensuring Safe Transitions
6. Negotiating Different Priorities

Aim/Purpose of the Paper

- Explain some relevant concepts of Functional Safety to HMI Designers
- Get Functional Safety Experts and HMI Designers on the same page
- HMI Designers will gain the most from this paper
  - highlight parts of ISO 26262 that impact on their jobs the most.
  - when/where/how HMI Designers play a role in ensuring compliance with ISO 26262

Highly Automated Driving

- SAE Level 4 Automation (or ‘Highly Automated’) vehicles take full responsibility within defined operational design domains (ODDs)
- When vehicles enter/exit operational design domains, there can be changes of who is responsible for the dynamic driving task
- Developing ISO 26262 compliant Level 4 Automation system will be a challenge
  - Interaction Sequence diagrams of transitions/protocols

… but first, let’s talk a little bit about ISO 26262.

ISO 26262: Background

The International Organization of Standards released the first version of “ISO 26262: Road Vehicles - Functional Safety” in 2011

Introduced Automotive Safety Integrity Levels (ASILs)

- how ASILs are compiled and handled
- categorize the risk level for a hazardous event (i.e. headlight failure)
- a metric of the cost of failure

ISO 26262: ASILs

Severity Score	Exposure Score	Controllability Score		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

ASIL is a composite score of three characterics:

- **Severity** (**S**) is how bad resulting injuries may be
- **Exposure** (**E**) is how often the event is likely to happen
- **Controllability** (**C**) is how easy or difficult it would be for the average driver to maintain control in the situation.

ISO 26262: ASILs

Severity Score	Exposure Score	Controllability Score		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

More formal definitions:

Severity (**S**) is a measure of potential injury in the case of failure, and ranges from S1, light and moderate injuries, up to S3, life-threatening injuries (survival uncertain) and fatal injuries.

Exposure (**E**) is a measure of the relative expected frequency of exposure for each operational situation where a specific hazard may occur, and ranges from E1, very low probability of exposure to the situation, to E4, high probability of exposure

Controllability (**C**) is a measure of how easy or difficult it would be for the driver, or other persons involved, to control the situation, and ranges from C1, simply controllable by 99% of drivers, to C3, uncontrollable or difficult to control.

ISO 26262: ASILs

Severity Score	Exposure Score	Controllability Score		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

ASILs can be given to entire systems, and these will be inherited by the elements that make up that system.

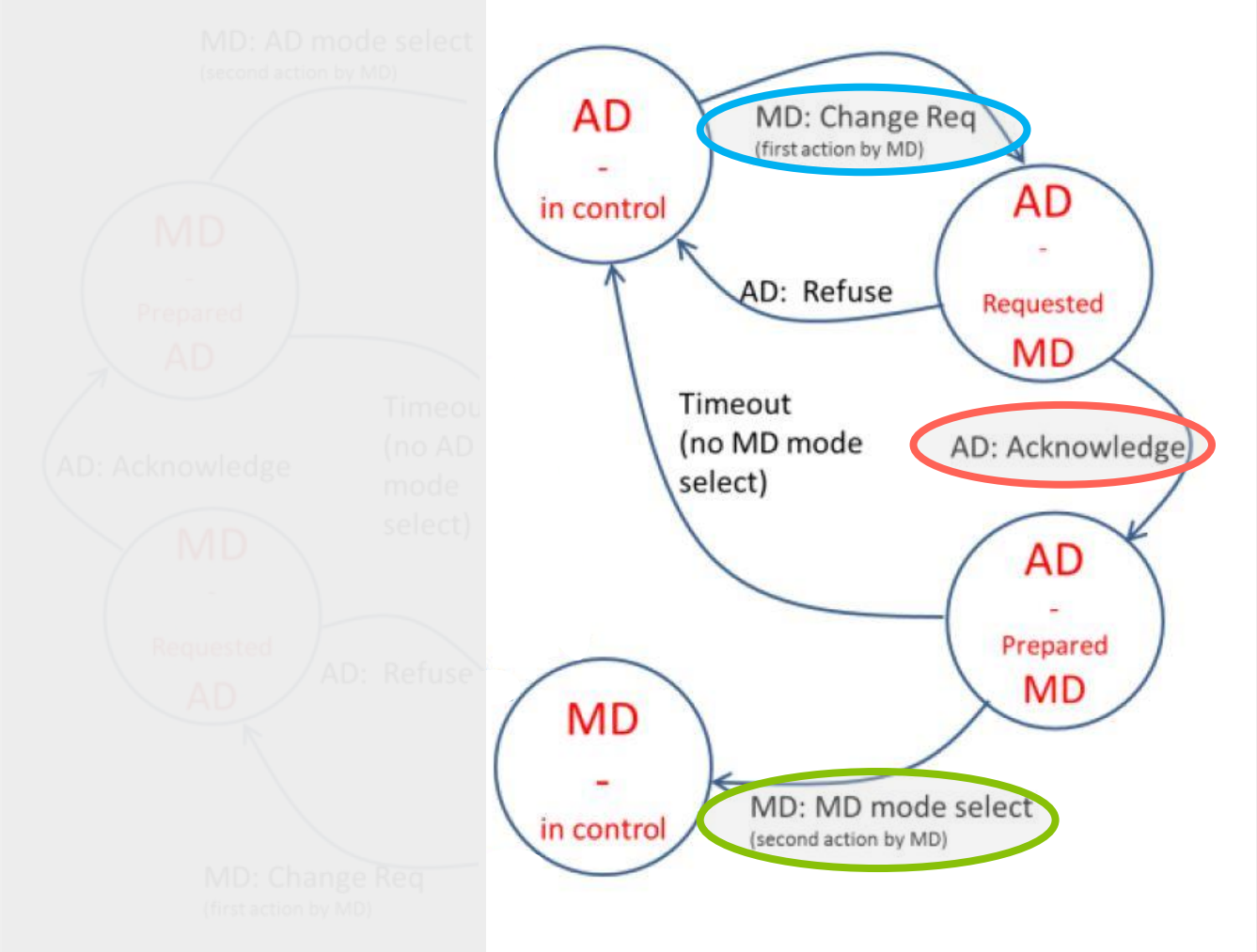
Decomposition is braking down the ASIL over several elements as a way to lower the ’cost of failure’ for each of these elements.

Elements, in these cases, could be individual components, steps in a protocol, etc…

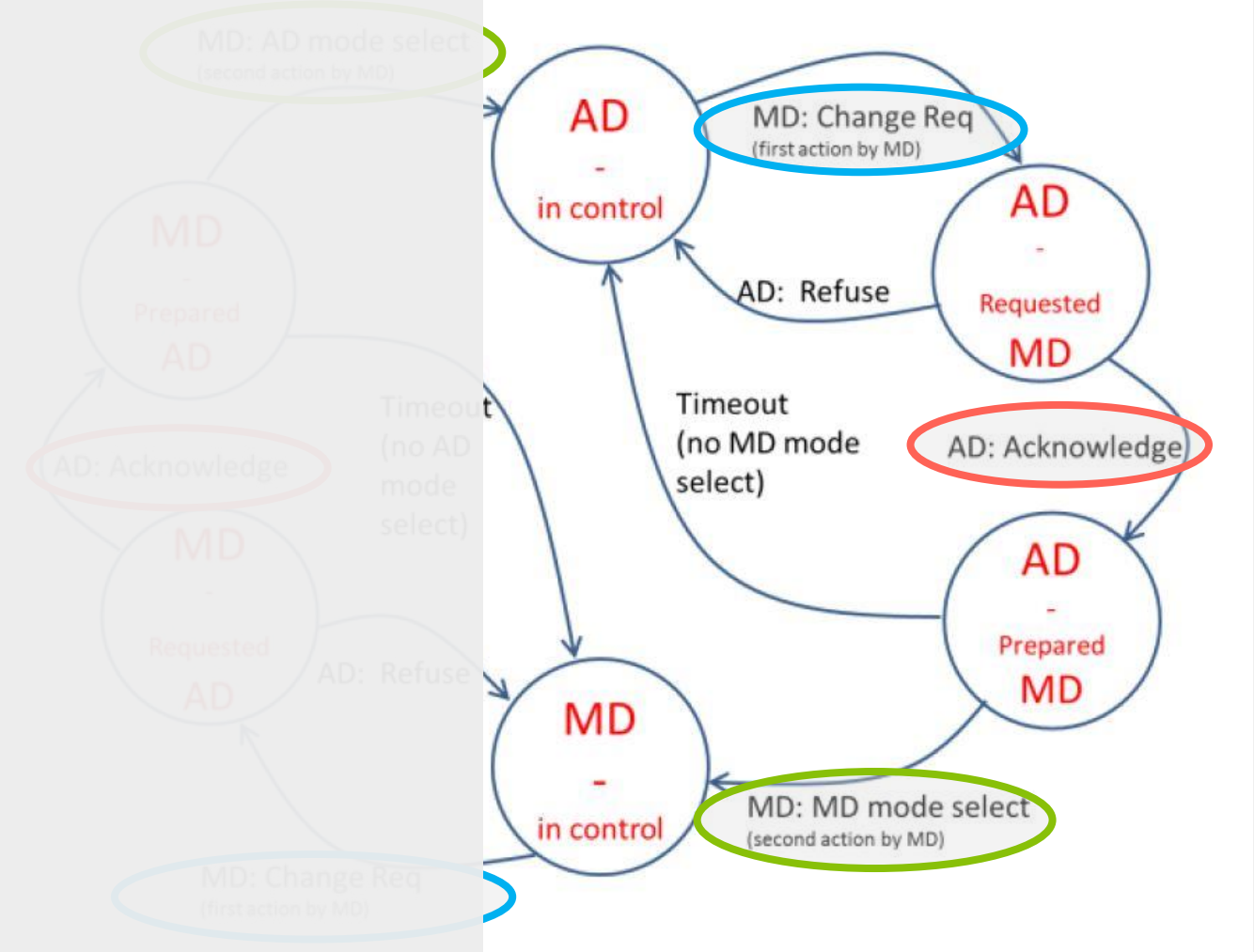
Controllability and HMI Design

- A **good HMI solution** can potentially affect **Controllability**
- By creating an interaction that is **easy to understand**, the situation will be **more controllable**, and the overall ASIL will be lower.
- However, sometimes it is **harder to simplify complex interactions**, necessitating **breaking the task down** into smaller steps to improve controllability.

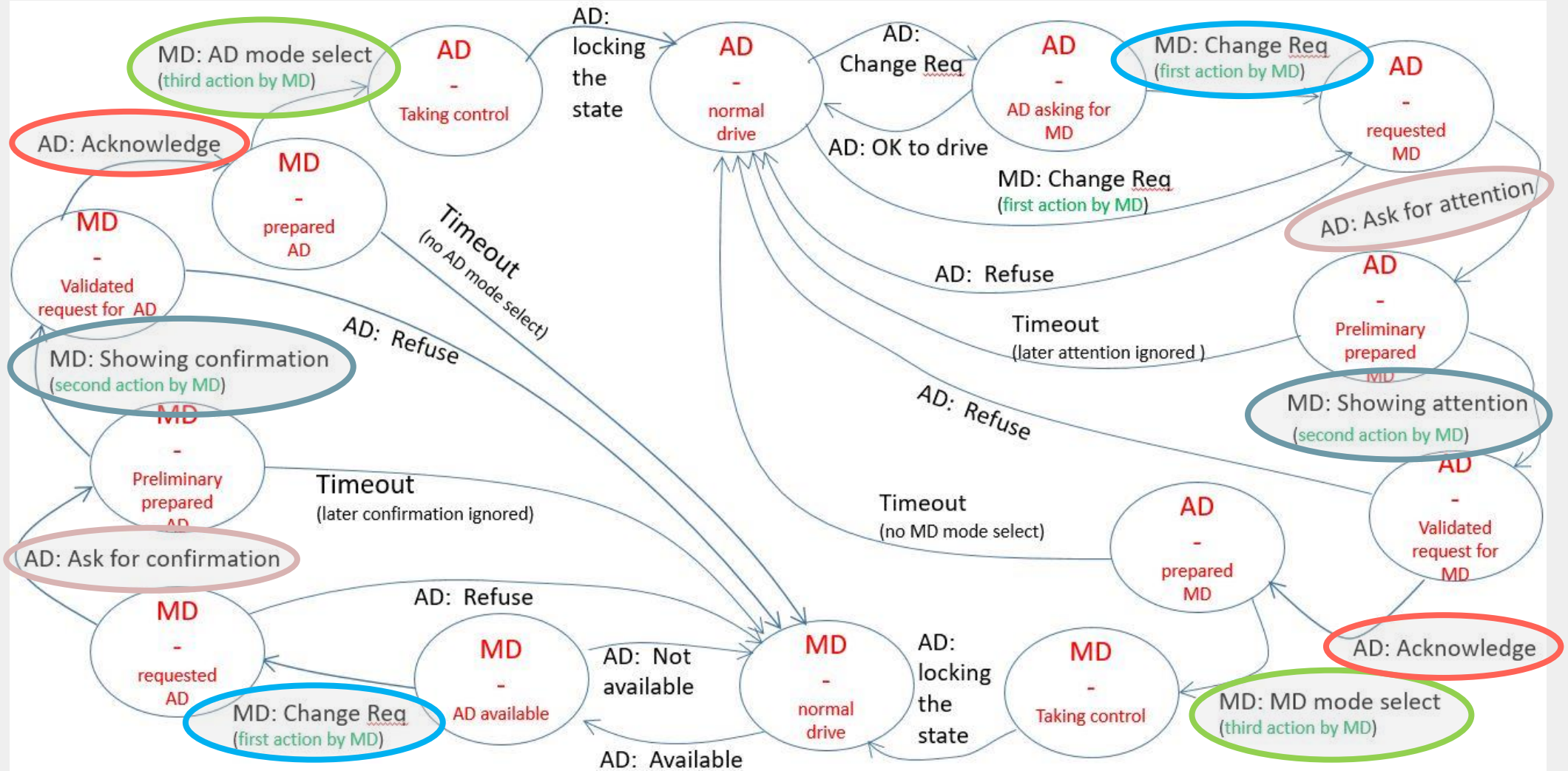
Minimal Transition Protocol



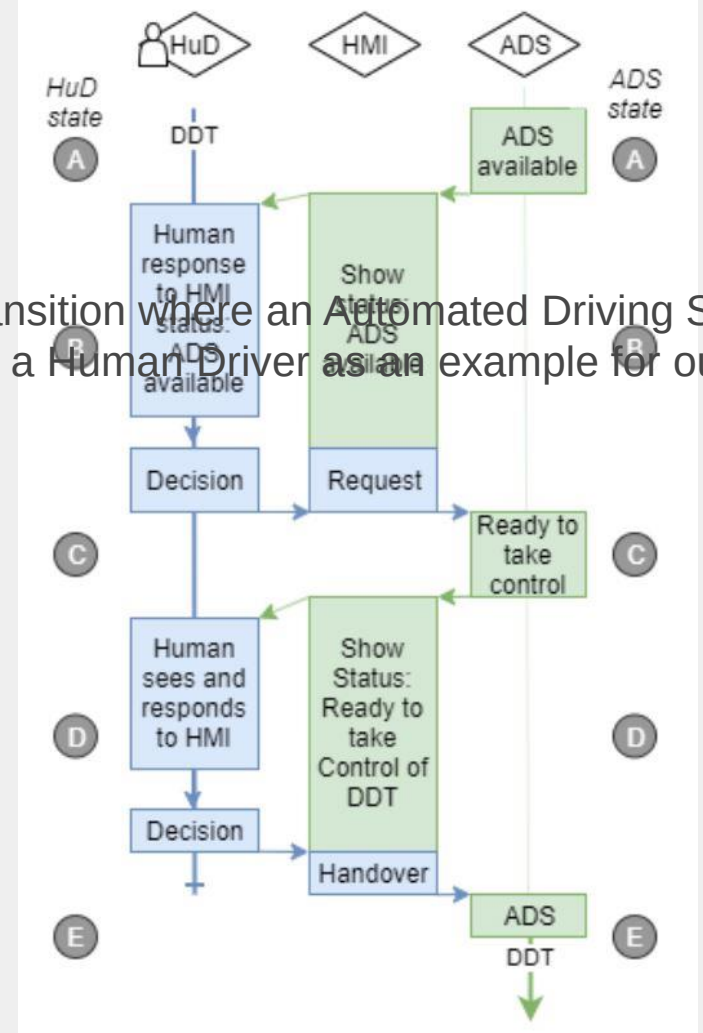
Minimal Transition Protocol



Multistep Transition Protocol

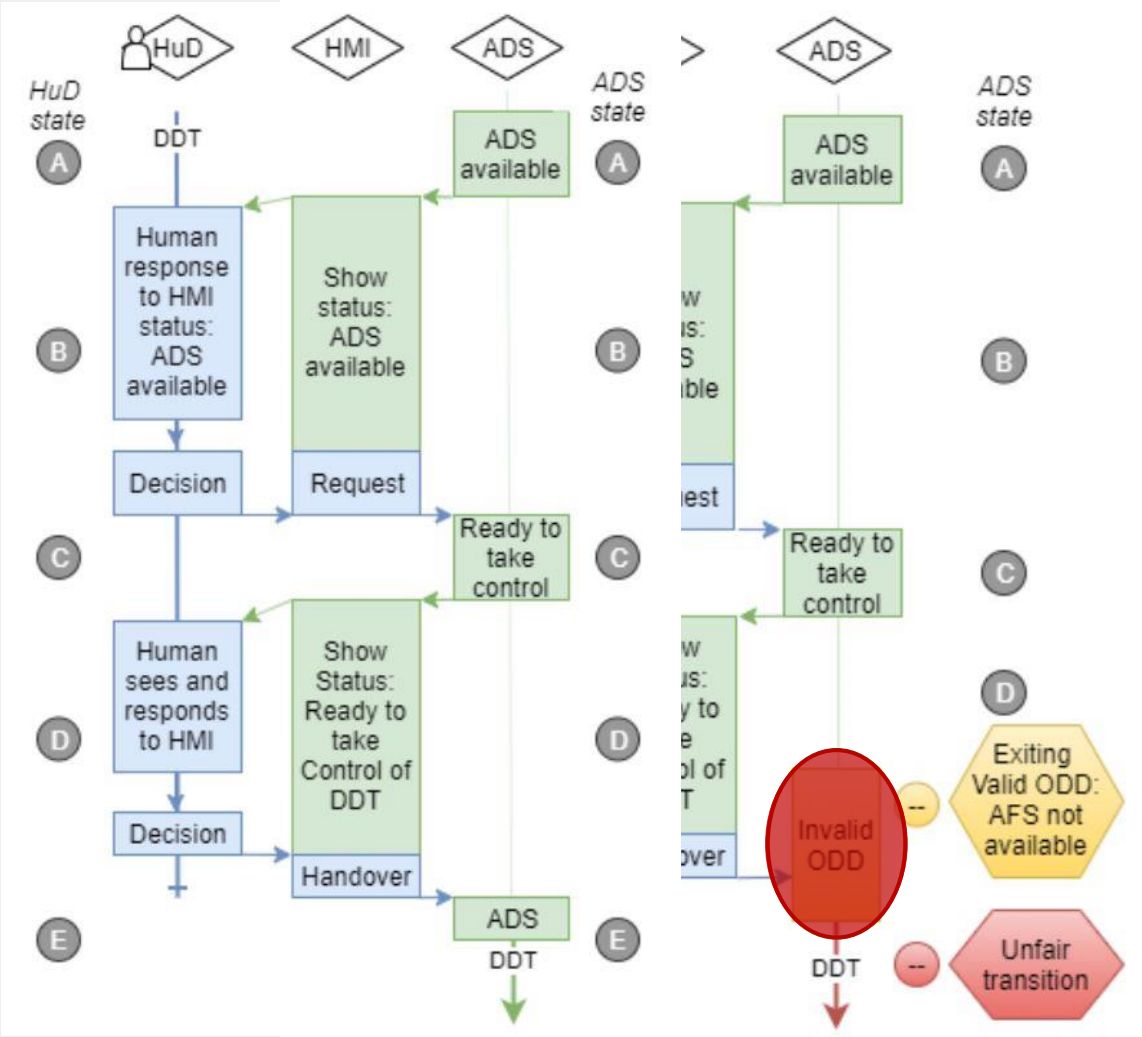


Failures and Transitions to avoid

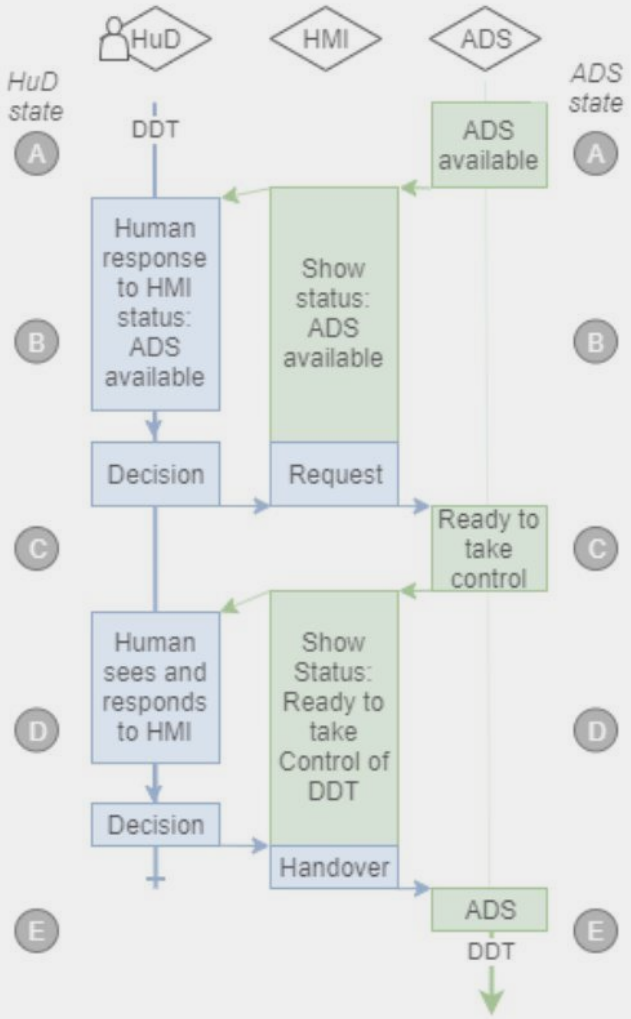


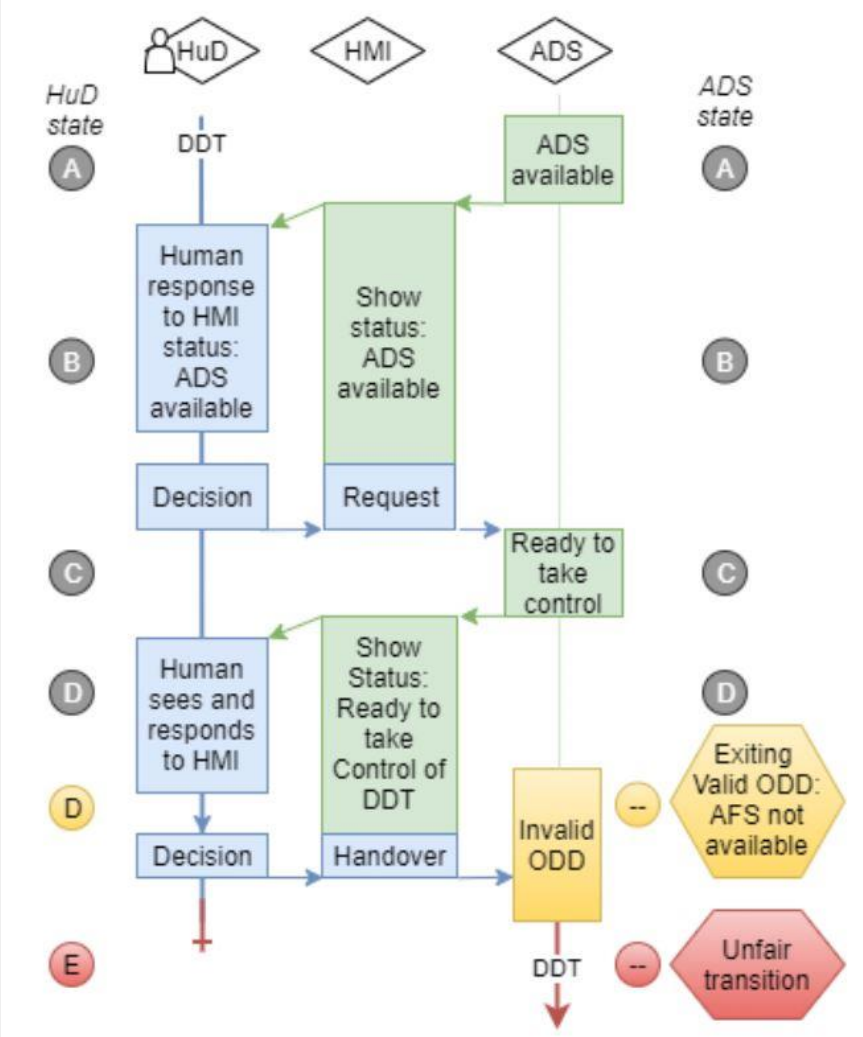
We will use the transition where an Automated Driving System takes over responsibility from a Human Driver as an example for outlining transitions to avoid.

Unfair Transition

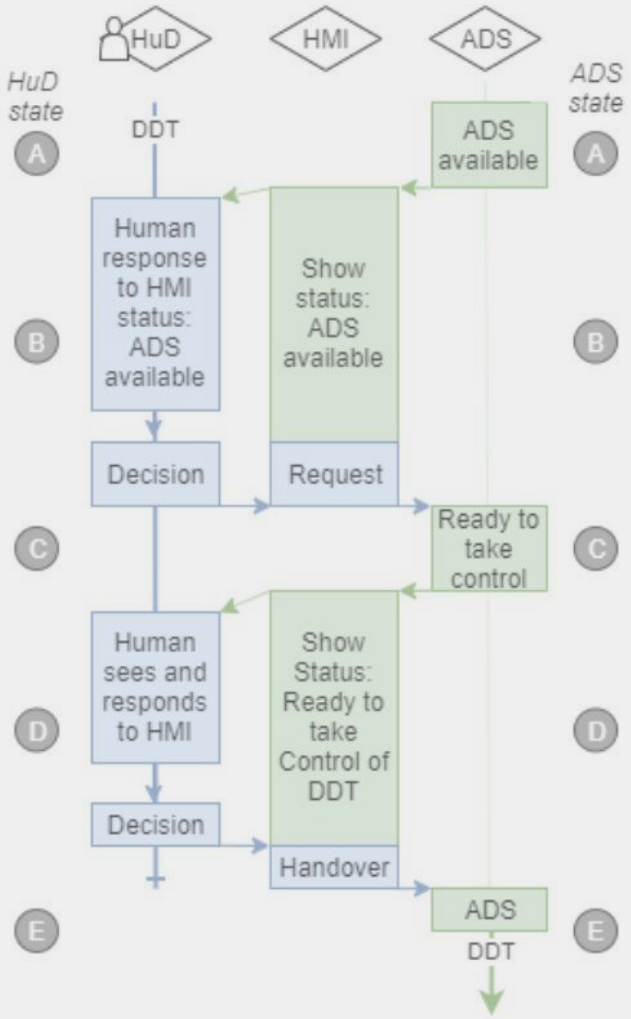


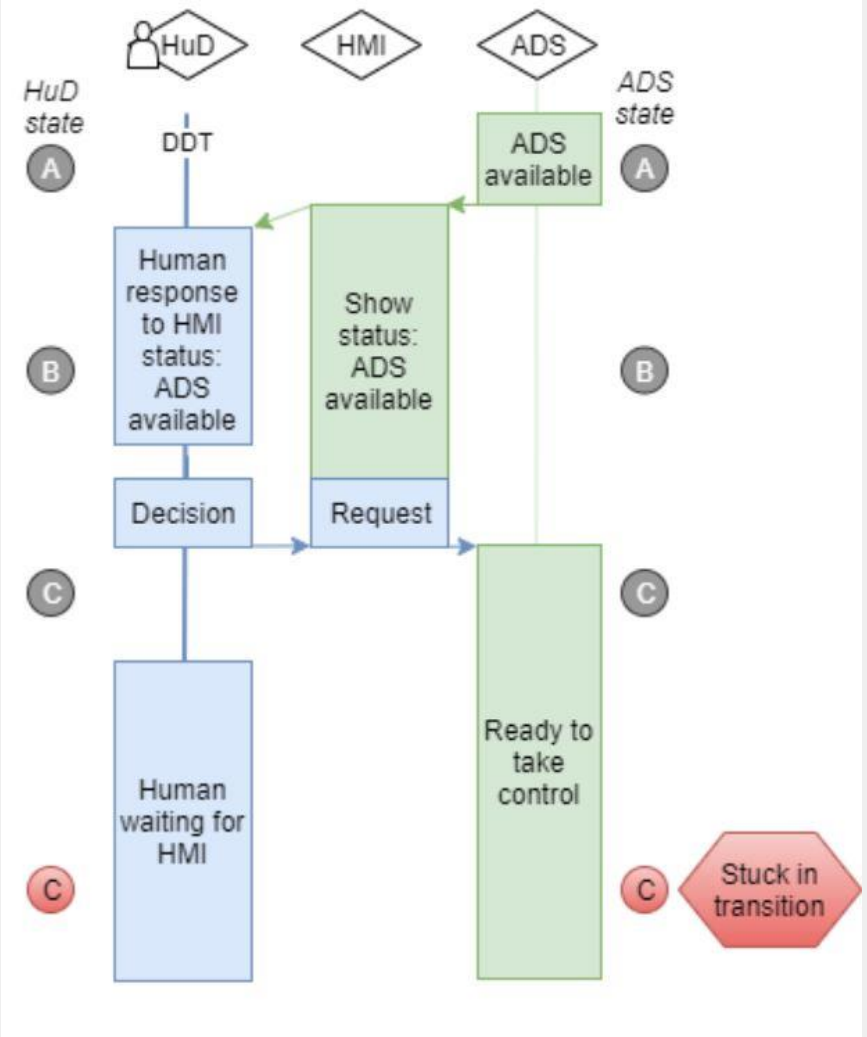
Stuck in Transition





Mode Confusion





How HMI Design might help Ensure Safe Transitions

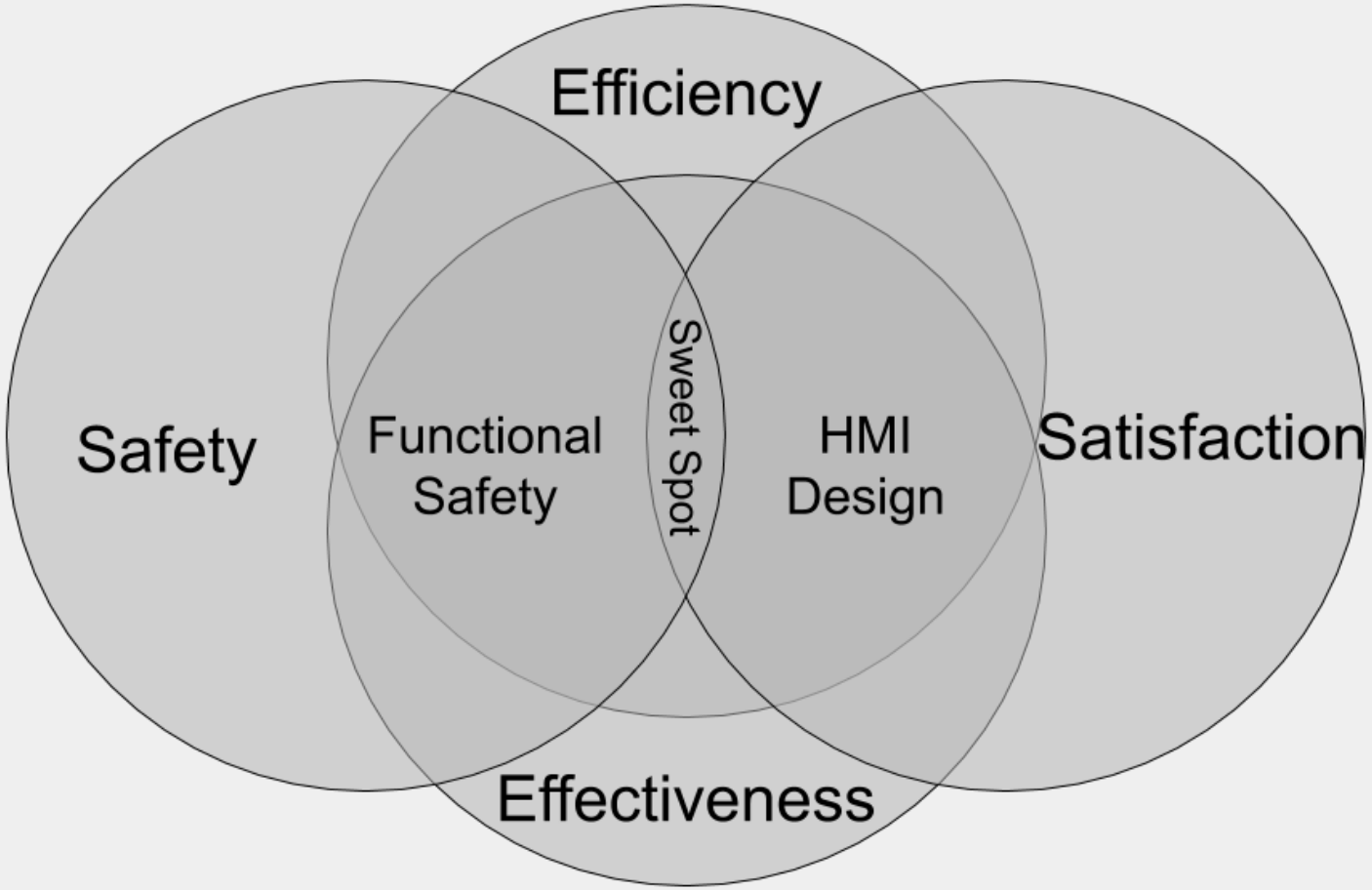
1) Both the driver and the ADS must consent to, accept, and communicate their acceptance of, the transfer to avoid unfair transitions

2) The recipient (driver or ADS) must be capable of safe operation in the current DDT to avoid unfair transitions.

3) The non-responsible party (driver or ADS) must not affect vehicle motion outside the constraints set by the DDT-responsible party (ADS or driver) to minimize the chance of Mode Confusion.

4) The transition sequence must not inhibit or limit the capability of the responsible party (driver or ADS), thus avoiding a stuck in transition situation where neither party has control.

Negotiating Different Priorities



Both Functional Safety and HMI Design are concerned with Efficiency and Effectiveness.

However, Functional Safety Experts will be more concerned with Safety than Satisfaction, while HMI Designers generally prioritise Satisfaction and User Experience.

Conclusions: Moving forward

In Summation, we've covered the following things:

1) Began explaining some Functional Safety basics to HMI Designers by identifying and introducing some the most relevant concepts from ISO 26262

2) Covered the complexity of transitions in Highly Automated Driving, and highlighted the points where HMI can make key differences in success

3) Discussed when, where, and how HMI Designers could help in ensuring compliance with ISO 26262 when it comes to implementing transition protocols in Highly Automated Driving

4) Illustrated how Functional Safety Experts and HMI Designers might look differently at similar problems in order to help bridge the gap between the disciplines and get everyone on the same page

Thank you for your time and attention today.

Matthew Sassman

Matthew.Sassman@semcon.com