TRAFIKVERKET

Konferens: HFN – drygt 25 år av verksamhet

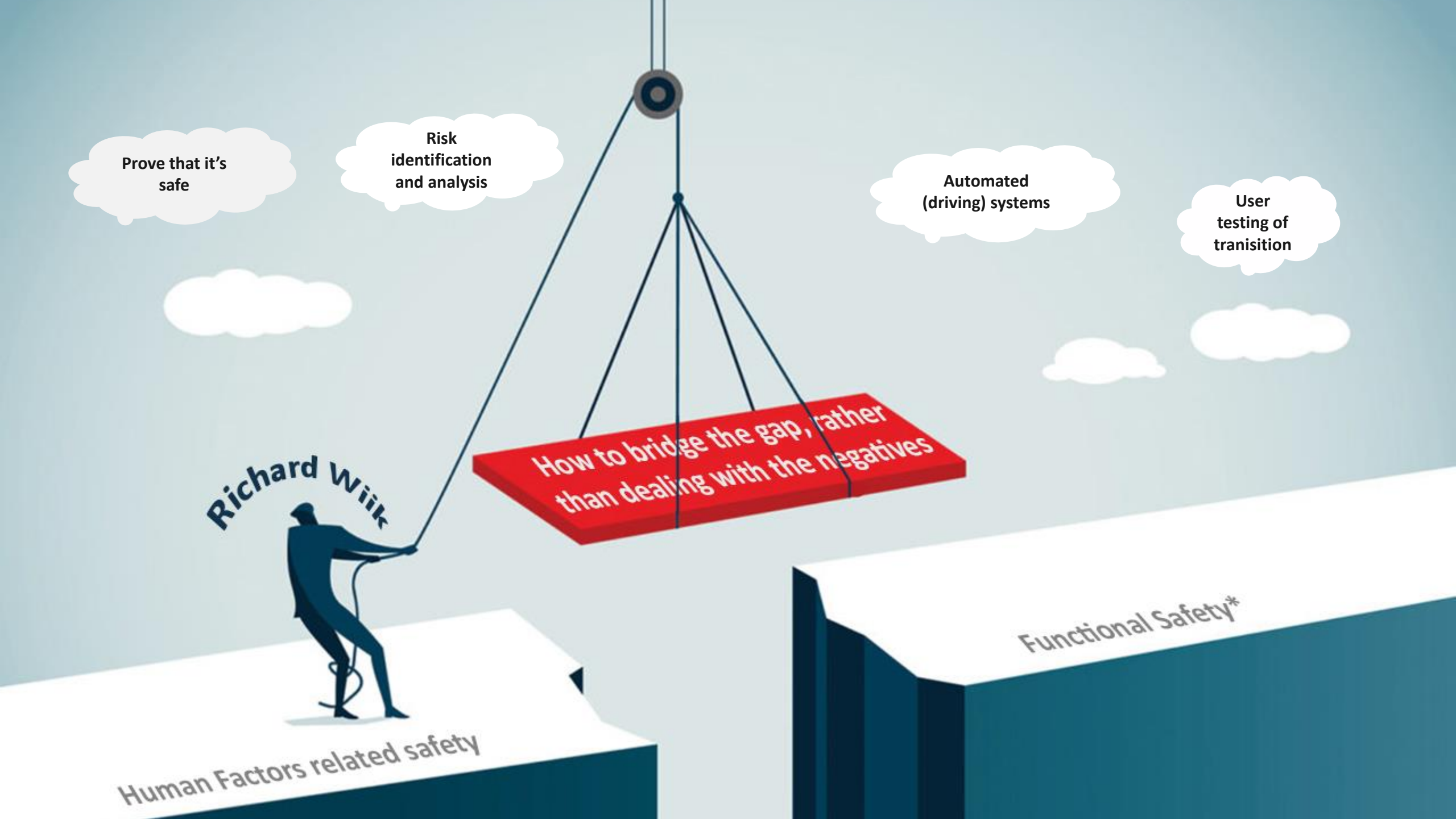
Richard Wiik

2022-08-25

TRAFIKVERKET

Att nyttogöra digitaliseringens fördelar, utan att behöva kämpa med dess baksidor

Or rather...


Prove that it's safe
Risk identification and analysis
Automated (driving) systems
User testing of tranisition
How to bridge the gap, rather than dealing with the negatives
Richard Wiik
Human Factors related safety
Functional Safety*

TRAFIKVERKET

Background

- Cognitive Science, Human Factors & Ergonomics
- Work experience within E/E standards within different domains
- Functional Safety* & HF related safety

LINKÖPINGS UNIVERSITET

Magisterprogram, Ergonomi och Människa-Teknik-Organisation


Ps
Mitt kära
Tålamod
Har lämnat mig
i stor sorg och saknad
KTH
VETENSKAP
OCH KONST
KOGNITIONSVETENSKAP
LINKÖPINGS UNIVERSITET
Richard Wiik
Estrella Damm
Estrella Damm
WORLD PADEL TO
GRANADA OP
IRONY
TRAFIKVERKET

TRAFIKVERKET

Today’s content

- Centered around automated driving systems
- I think and hope methods and practical experience presented today can be used on a wider scale

- Functional safety* standards differs across domains but are in large ”similar”

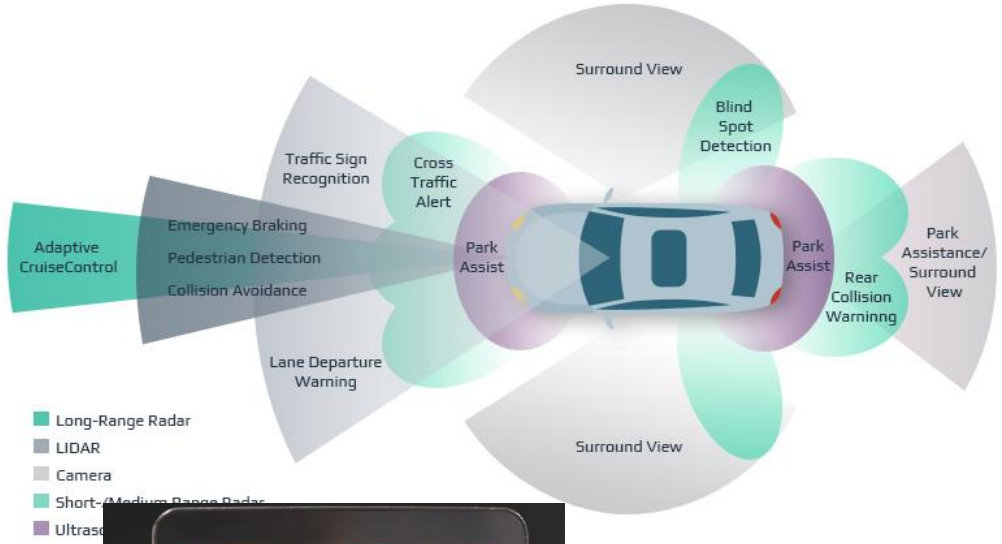
61508-4: Functional safety
part of the overall safety relating to the Equipment Under Control and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures

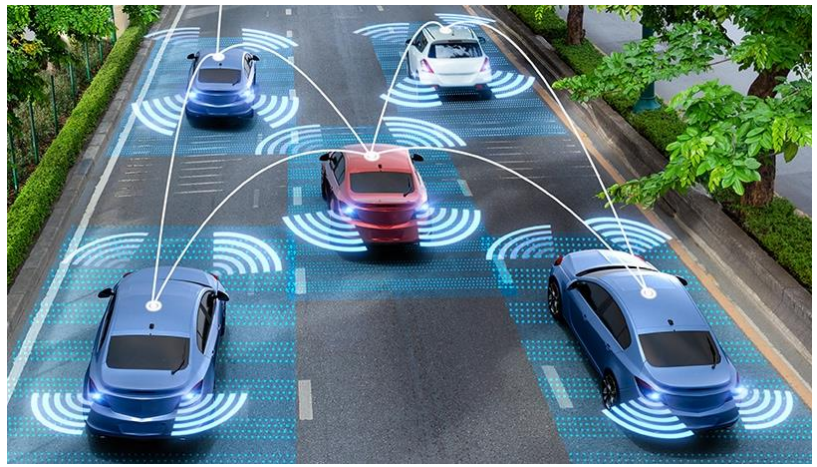
TRAFIKVERKET

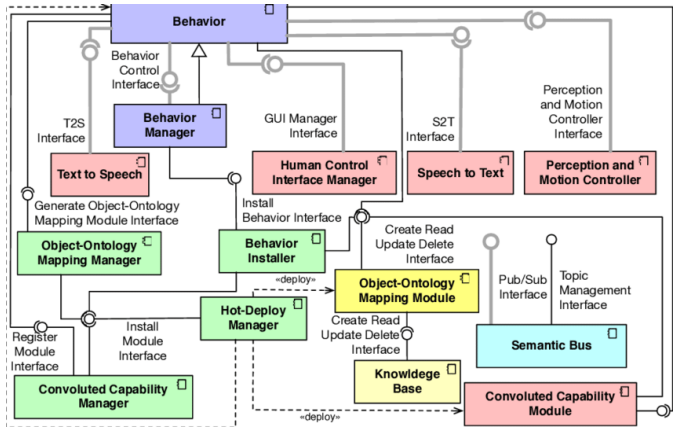
What does the sensors see?

TRAFIKVERKET

Within the realm of functional* safety







TRAFIKVERKET

Functional safety* takes many forms

- IEC 61508
- SS-EN 50126/8/9
- ISO 26262
- ISO/PAS 21448
- SS-EN 62061
- SS-EN ISO 13849
- SIS-ISO/TR 14121
- SS-EN ISO 12100
- ISO 20474
- SS-ISO 17757
- DO-278A
- DO-178C
- ED-153
- MIL-STD 882E
- FMV H Progsäk

Automated (driving) systems


Within its Operational Design Domain

Its ODD is in Gothenburg!

TRAFIKVERKET

5 Levels of driving automation

”Med hänsyn till utvecklingen i omvärlden bedömer Trafikverket att det högst troligen kommer att finnas kommersiella fordon med automatiseringsnivå 4 i trafik i Sverige inom en tioårsperiod, åtminstone i begränsad skala och främst inom yrkestrafiken.”

Trafikverket - Vägens stöd till automatiserade fordon
diva-portal.org/smash/get/diva2:1680517/FULLTEXT01.pdf

TRAFIKVERKET

Safety of high automated driving (L4) decomposed into three sub-problems

(1) Safe driving when the human is responsible

(2) Safe driving when the Automated Driving System is responsible

Human in control

ADS in control

(3) Safe transitions between the human and the ADS

- Stuck in transition
- Unfair transition
- Mode confusion

TRAFIKVERKET

Mode confusion during transitions

- Hazardous situation where either non is driving or both are
- Methodology to find safety issues in HMI protocols
  - Human
  - HMI
  - ADS
- Using Fault Tree Analysis to identify causes

Towards Safety Analysis of Interactions Between Human Users and Automated Driving Systems

TRAFIKVERKET

Who is driving?

- An agreement between ADS and human driver of how the transition is allowed

- To identify possible interaction failures during the transition we need…
  - a transition protocol
  - an interaction sequence

Adding to the procotol

TRAFIKVERKET

A simple transition protocol

But who is doing what?

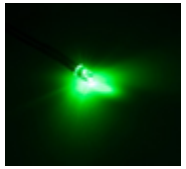
TRAFIKVERKET

A proposed protocol for the transition

Human

Human control

Human actions
HMI signals



HMI shows ADS available

Human requests ADS

HMI shows ADS prepared

Human selects ADS

ADS state

ADS un-available

ADS available

ADS requested

ADS prepared

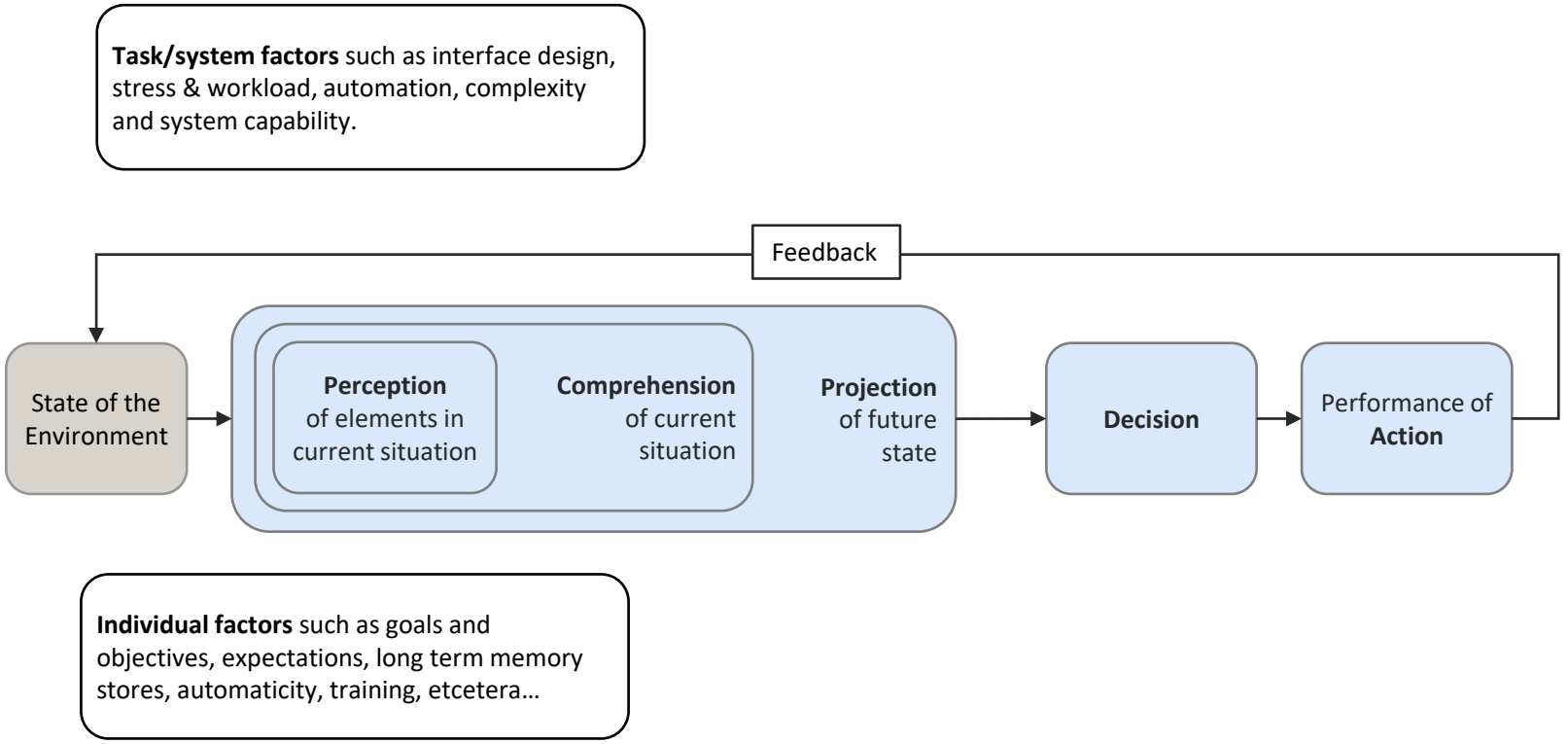
ADS control

1 2 3 4 5

TRAFIKVERKET

Situation awareness

Mica Endsley model for SA as a way to adding human factors to the protocol



M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," Human factors, vol. 37, no. 1, pp. 32–64, 1995

TRAFIKVERKET

A proposed protocol for the transition

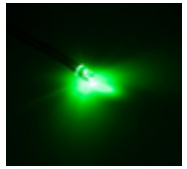
…And then adding the SA model to the protocol

Human

Human actions
HMI signals

ADS state

	1	2	3	4	5
Human	Human control				
Human actions HMI signals		HMI shows ADS available	Human requests ADS	HMI shows ADS prepared	Human selects ADS
ADS state	ADS un-available	ADS available	ADS requested	ADS prepared	ADS control



TRAFIKVERKET

A HMI-protocol for the transition… with interaction sequence!

Human control

ADS un-available

ADS available

Perception

Comprehension

Projection

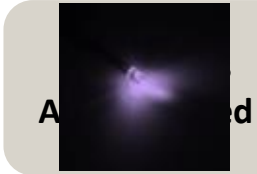
Decision

S1

A1

ADS requested

S2



ADS prepared

Perception

Comprehension

Projection

Decision

A2

ADS control

Mode confusion in the A HMI-protocol

Human control

ADS un-available

ADS available

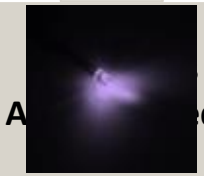
Perception
Comprehension
Projection
Decision

S1

A1

ADS requested

S2



ADS prepared

Perception
Comprehension
Projection
Decision

A2

ADS control

1 | 2 | 3 | 4 | 5

Human control

ADS un-available

ADS available

HMI shows ADS available

S1

Perception

Comprehension

Projection

Decision

Human requests ADS

A1

ADS requested

ADS prepared

HMI shows ADS prepared

S2

Perception

Comprehension

Projection

Decision

Human selects ADS

A2

ADS control

1 | 2 | 3 | 1 | 1

1 | 2 | 3 | 4 | 5

Human

Human control

Perception
Comprehension
Projection
Decision

S1

HMI shows ADS available

Human requests ADS

A1

S2

HMI shows ADS prepared

Perception
Comprehension
Projection
Decision

Human selects ADS

A2

Human actions
HMI signals

ADS state

ADS un-available

ADS available

ADS requested

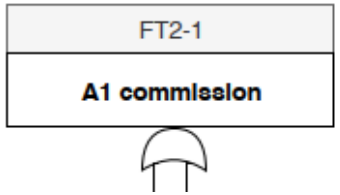
ADS prepared

ADS control

1 | 1 | 1 | 1 | 5

Fault tree analysis

- Perception - failure to correctly perceive the information.
- Comprehension - failure to comprehend the situation.
- Projection - failure to project the situation into the future.



Decision - Incorrect selection of action to reach a goal, or incorrect execution of that action.

Action - Unintentional substitution of a correct performance segment (action) with an incorrect one.

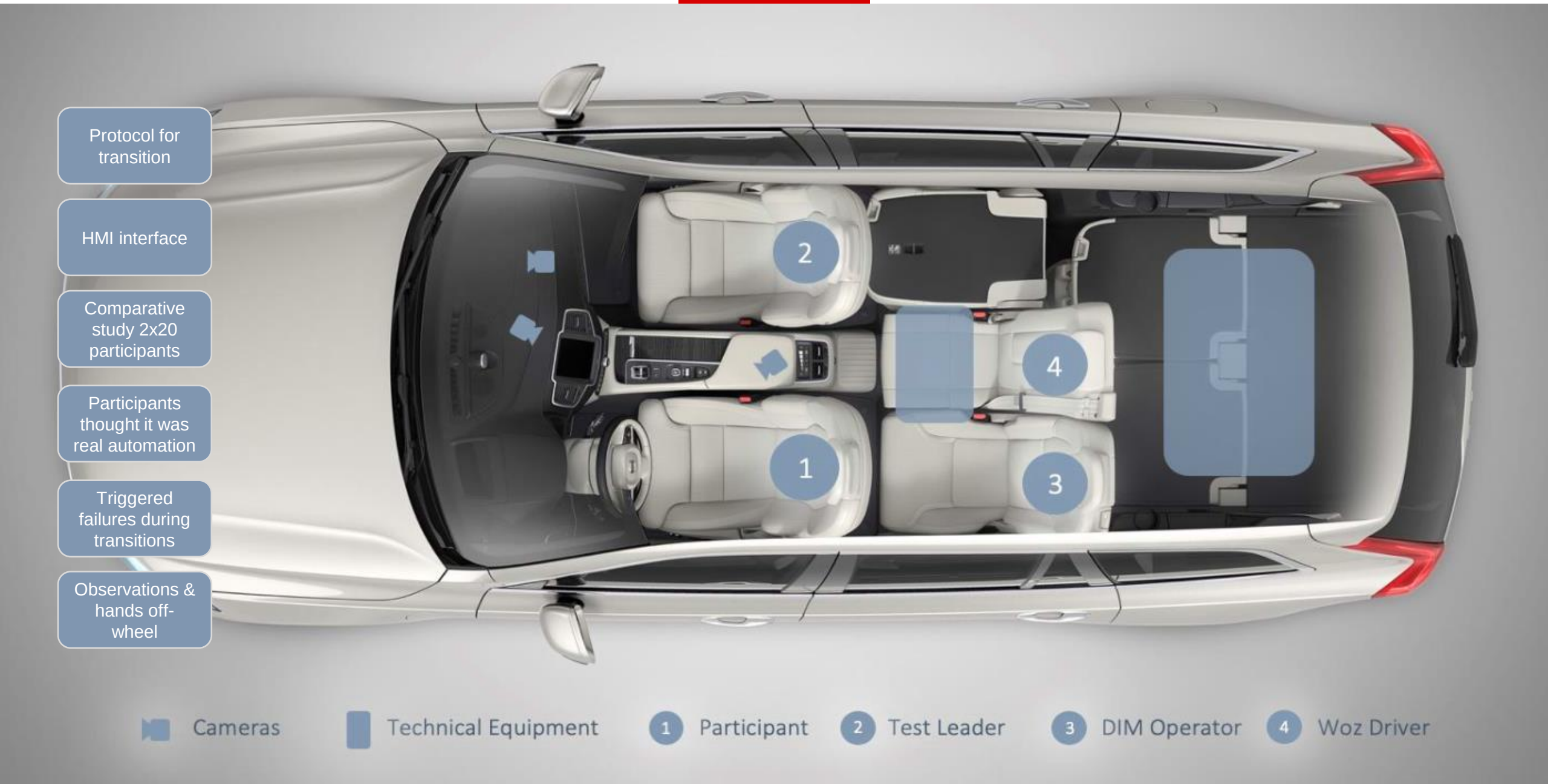
TRAFIKVERKET

Usability testing

Can the human identify if the ADS fails during transition and avoid mode confusion?

TRAFIKVERKET

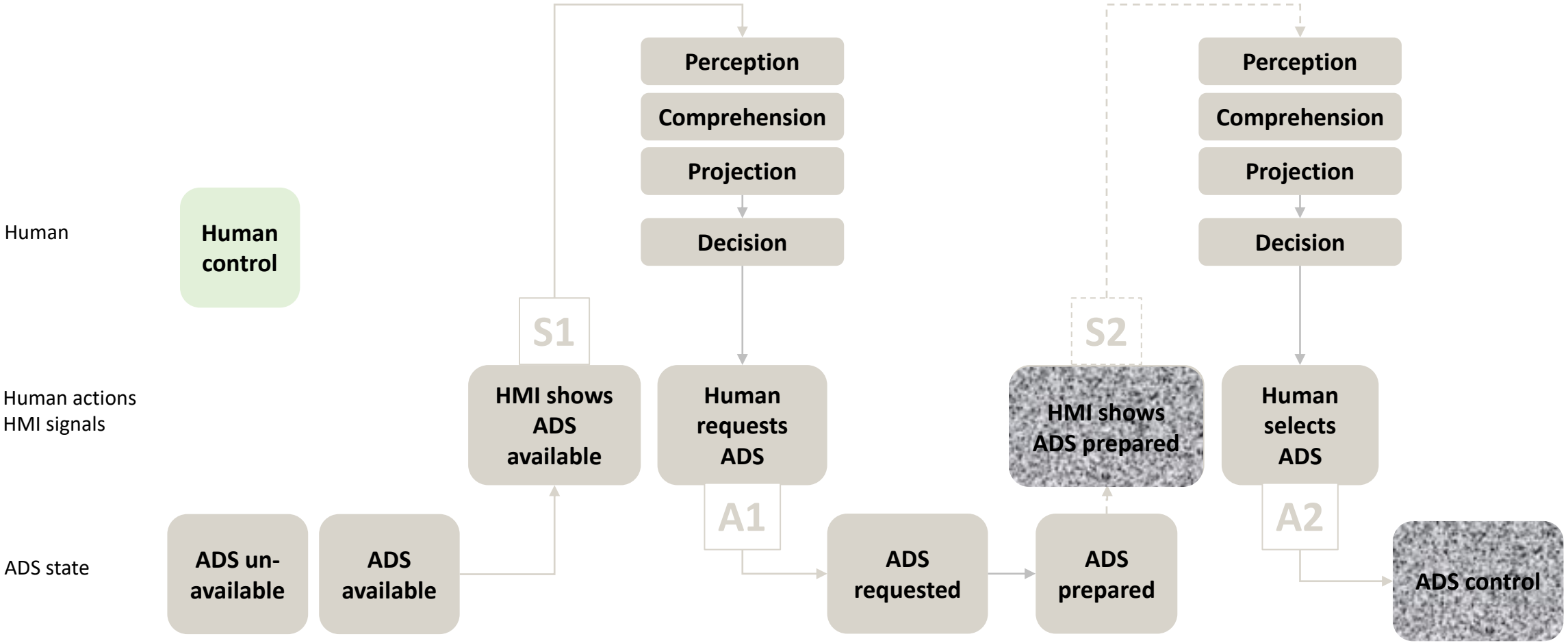
- Protocol for transition
- HMI interface
- Comparative study 2x20 participants
- Participants thought it was real automation
- Triggered failures during transitions
- Observations & hands off-wheel

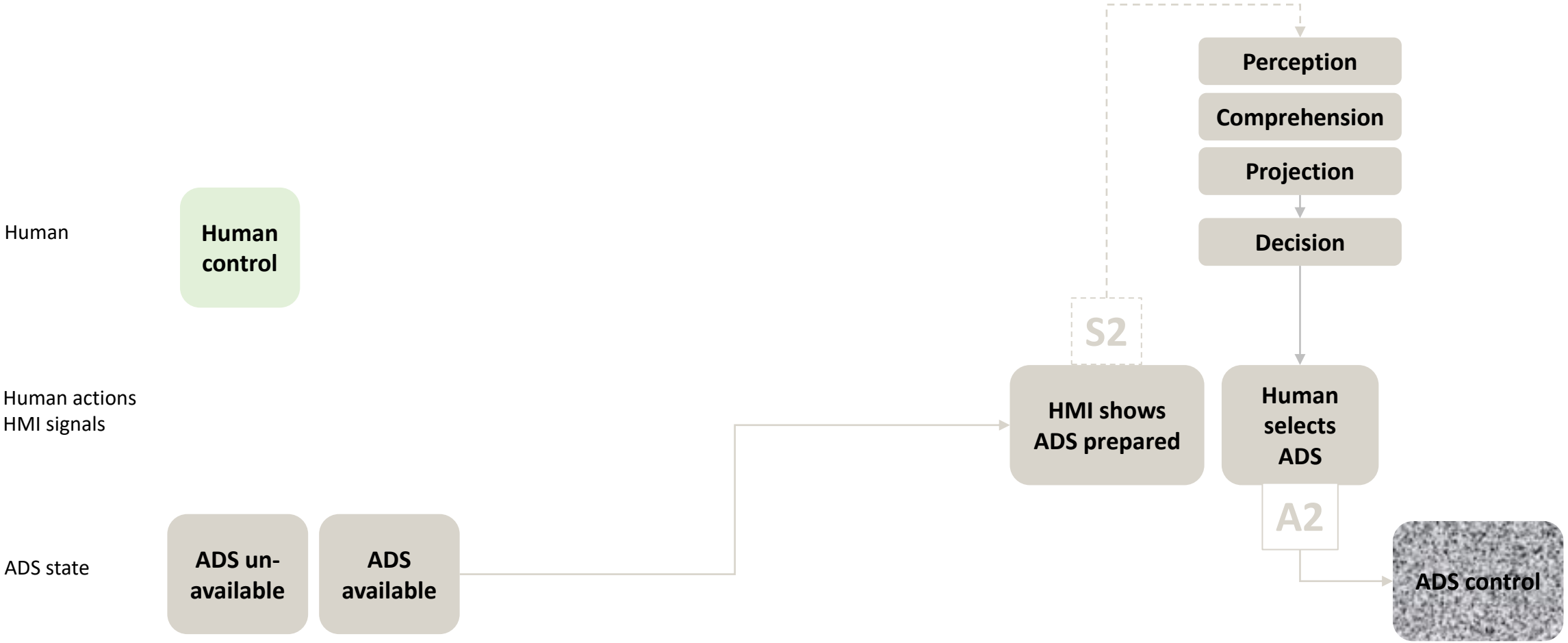


TRAFIKVERKET

Examples of protocol failures tested

TRAFIKVERKET




Perception
Comprehension
Projection
Decision
Human
Human control
S2
Human actions
HMI signals
HMI shows ADS prepared
Human selects ADS
A2
ADS state
ADS un-available
ADS available
ADS control

TRAFIKVERKET

Thanks so much for your time!

TRAFIKVERKET

Assessing risk in ISO 26262 Road vehicles — Functional safety

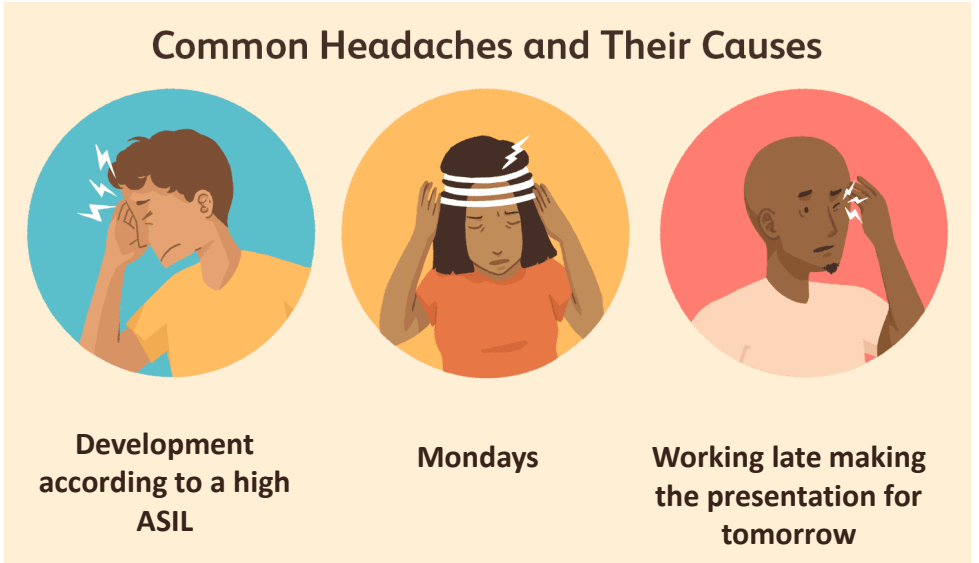
- Severity
- Exposure (probability)
- Controllability (…of the hazardous event of persons involved)

The sum of the three factors results in an ”ASIL”

TRAFIKVERKET

ISO 26262

- ASIL: required safety measure to avoid unreasonable risk of safety related functionality



TRAFIKVERKET

Usability testing to argue for controllability

Table B.6 — Examples of possibly controllable hazardous events by the driver or by the persons potentially at risk

	Class of controllability (see Table 3)			
	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable
Driving factors and scenarios	Controllable in general	More than 99 % of the average drivers or other traffic participants are able to avoid harm	Between 90 % an 99 % of the average drivers or other traffic participants are able to avoid harm	Less than 90 % of the average drivers or other traffic participants are able to avoid harm

Can the driver notice and avoid mode confusion if the transition to ADS fails?

If each of the 20 data sets complies with the pass-criteria for the test […], a level of controllability of 85 % […] can be proven. This is appropriate evidence of the rationale for a C2-estimate.

TRAFIKVERKET

Thanks again!

TRAFIKVERKET