

# ADAS risk assessment: Safety methods and countermeasures

Dr. Evangelos BEKIARIS



# Extended FMEA

- Based upon a Failure Mode and Effects Analysis methodology.
- The relevant indicators of *severity, occurrence probability, delectability* and *recoverability* have been expanded to cover not only technical risk but also *behavioural, legal and organisational - related* risks.
- For each identified type of problem, the failure effect, cause, detection and recognition, and mitigation strategy are also defined.



# Methodology for ADAS multiparameter risk analysis

- Risk = Severity x Probability x  $((\text{Detectability} + \text{Recoverability})/2)$
- Calculate separately a Technical Risk Number (RNT), a Behavioural Risk Number (RNB), a Legal Risk Number (RNL) and an Organisational Risk Number (RNO).
- Overall Risk Number (ORN) =  $[RNT + RNB + (RNL + RNO)/2]/3$
- Further analysis of issues with higher risks and proposal of appropriate mitigation strategies.

# Behavioural risks analysis steps

- System definition.
- System familiarisation.
- Definition of the top event.
- Construction of the fault tree.
- Analysis of the fault tree.



# Severity levels for ADAS behavioural analysis

- **Extremely severe:** Human error is intolerable, as it could cause loss of vehicle safety resulting in significant serious injury and significant vehicle or environmental damage.
- **Severe:** The expected costs (training, design changes, etc.) to reduce human error will far exceed the profit/benefit from the ADAS / Human behavioural adaptation may abort the system benefits (completely or slightly) / Changes in driver behaviour has negative safety effects.
- **Moderate:** Human behavioural changes may significantly reduce the positive effects of the system.
- **Slight:** Human error could cause customer dissatisfaction without resulting in injury or vehicle or environmental damage.
- **Insignificant:** Human error is very unlikely to happen and the consequences would be insignificant.

# Example: Behavioural adaptation due to ACC

- Short term: Distrusting the ACC system / Increasing brake pedal forces / Unequipped vehicles imitate equipped vehicles / Reliance on vehicle in front
- Long term: Using spare capacity for other in-vehicle tasks / Over-reliance / Fatigue / Quick approach to vehicle in front / Shorter time-headway / Use ACC as an indication of when to overtake / Difficulties with overtaking and being overtaken



# Example: Behavioural adaptation due to driver monitoring systems

- Drivers will use such a system as an alarm clock and rely on it to alert them when they fall asleep. This will allow them to drive closer to the limits of impairment than they might have without the system.
- Drivers will depend on the system rather than themselves to diagnosis their fitness to drive. So drivers may continue driving with a system even when they themselves feel impaired.
- Drivers will change their driving style to avoid being warned.
- Drivers will ignore or sabotage the systems in order to continue driving even when they are impaired.



# Example: Behavioural adaptation due to CAS

- Drivers may try to prevent warnings or interventions by changing their driving behaviour, such as starting an overtaking manoeuvre sooner, or staying longer in the left driving lane.
- An effective CAS system can be assumed to contain an intervention function. It may, however, also be fitted with a warning function, preferably in the form of tactile stimulation. How to integrate these two functions for optimal performance?



# Example: Technical risk regarding ADAS HMI

Function	Failure mode	Failure effect	Failure cause	Mitigation Measures
<i>Icons /Leds + wiring + connectors + ECU-CCL output chain</i>	Permanently active	Wrong information to the driver	Problems of connections. ECU output chain broken.	Use redundant means of warning.
	Permanently inactive	No communication to the driver	Connector got off. Problems of connections. Defect of led. ECU output chain broken.	Use redundant means of warning.
	Intermittent operation	Wrong information to the driver	Poor contact. Led wear out. ECU output chain broken.	Use redundant means of warning.

# Example: Behavioural risk regarding ADAS HMI

Function	Function purpose	Behavioural problem	Failure effect	Failure cause	Mitigation Measures
Confirm button	Reply of driver to system	Unjustified press of the confirm button in the cautionary phase	Red phase is prohibited even if required, safety management	Inadvertent press of the confirm button. Confusion with Repeat button. Misunderstood system request. Wrong self-estimate of the driver's own state.	Try to eliminate the orange phase by appropriate system design.
Emergency button	Human triggered transition to imminent phase	Inadvertent press of the emergency button	Red phase is initiated, when not required Automatic driving occurs	Confusion of the emergency button with a simple "emergency call" button. Passengers are playing with buttons.	