



Code of Practice for the Design and Evaluation of ADAS

Foreword

The Code of Practice (CoP) comprises a suitable ADAS (Advanced Driver Assistance System) description concept including ADAS specific requirements for system development. It summarises best practices and proposes methods for risk assessment and controllability evaluation. The Code of Practice has been produced by a group of experts within the RESPONSE 3 project, a subproject of the integrated project PReVENT, a European automotive industry activity, co-funded by the European Commission, to contribute to road safety by developing and demonstrating preventive safety applications and technologies.

The RESPONSE 3 development group:

Alain Servel (PSA, F)
Andreas Knapp (DCAG, D)
Christoph Jung (BMW, D)
Eckart Donner (AUDI, D)
Elmar Dilger (BOSCH, D)
Fabio Tango (CRF, I)
Johannes Mihm (FORD, D)
Juergen Schwarz (DCAG, D)
Keith Wood (TRL, UK)
Luciano Ojeda (PSA, F)
Markus Neumann (VW, D)
Martin Brockmann (FORD subc, D)
Matthias Meyer (BMW, D)
Miklós Kiss (VW, D)
Maxime Flament (Ertico, B)
Paul Kompfner (Ertico, B)
Rainer Walz (BMW, D)
Sally Cotter (TRL, UK)
Thomas Winkle (AUDI, D)
Wiel Janssen (TNO, NL)

Revision chart and history log

Version	Date	Reason
0.1	19.01.2005	first draft by J. Schwarz, DCAG
0.2	07.06.2005	development process and structure by J. Schwarz
0.3	08.06.2005	comments on how to integrate the different chapters by A. Knapp
0.4	13.06.2005	Restructuring chapter realisation, verification and validation as well as HMI approval by J. Schwarz
0.5	02.09.2005	Included new content and questionnaire feedback from other PReVENT projects
0.6	15.09.2005	Added new chapters according to PReVENT template, restructured requirements section and added new content provided by several RESPONSE3 partners
0.62	21.09.2005	Included a proposal for annex structure and annexes 7,8,9,11
0.63	28.9.2005	Workshop modifications 27.+28.9.2005, Ingolstadt
0.64	19.9.2005	Included To Do's from workshop
0.65	10.10.2005	Included results of telephone conference from 30.9.2005 in requirements chapter, new glossary, included consistent formatting.
0.66	17.10.2005	Interims version with updates from telephone conference on 14.10. and 17.10.2005
0.67	21.10.2005	Interims version with updates from telephone conference on 21.10., Content of annexes D, R
0.7	25.10.2005	Content of annexes H, L, added executive summary and conclusion, reorganised introductory chapters and glossary
0.8	31.10.2005	Changes from review of V0.7, included Annex M
0.9	14.12.2005	Included changes from peer review <i>PR-11300-SDR-051031-v0 8-CoP_Peer_Review.doc</i>
1.0	21.12.2005	Reformatted Annexes
1.1	20.2.2006	Included new proposal for "Requirements" chapter
1.2	24.5.2006	Chapter "Requirements2 changed to Recommendations, Updated Annexes B and C, added R
1.3	7.5.2006	Included partner contributions for preparation of workshop
1.4	17.7.2006	Reworked whole CoP during workshop, accepted revisions of discussed sections
1.5	21.7.2006	updated chapter 2, 5, Annex B, D, F
1.6	10.8.2006	deleted sections that are specific to the SP deliverable from the CoP from introductory chapters; corrected grammar and inconsistent use of terms
1.7	6.9.2006	updated final proof and ADAS definition
1.8	20.9.2006	Grammar corrections
2.0	20.9.2006	no changes - workshop version
2.1	06.10.2006	post workshop error corrections – peer review version
3.0	31.10.2006	Final check and formatting by IMC; final version

Table of contents

Foreword	ii
Revision chart and history log	iii
Table of contents	iv
Figures	vi
Tables	vi
1 Introduction.....	1
1.1 Motivation	1
1.2 Scope	2
2 Terms and Definitions	4
2.1 Definition of an Advanced Driver Assistance System	4
(ADAS)	4
2.2 Glossary	4
2.3 Abbreviations.....	10
3 Development Process	12
4 Controllability.....	14
4.1 Final proof of controllability by an interdisciplinary expert	15
panel.....	15
4.2 Final proof of controllability by means of a test with naïve	16
subjects	16
4.3 Final proof - direct recommendation of Controllability	16
Sign-Off by the ADAS Development Team	16
5 Recommendations	17
5.1 Definition phase.....	18
5.2 Best concept selection	20
5.3 Proof of Concept	22
5.4 Detailed design.....	23
5.5 Verification.....	24
5.6 Validation and Sign-off	25

ANNEXES	A2
Annex A Response Procedures	A3
A.1 Checklist A – System Specification	A3
A.2 Checklist B – Evaluation concepts for system specification	A24
A.3 Hazard Analysis and Risk Assessment Procedure	A41
Annex B Recommendations for controllability evaluation	A46
B.1 Condense hazardous situations	A46
B.2 Conducting a test with subjects	A47
B.3 How to setup pass-fail criteria	A50
B.4 How to evaluate controllability by experts	A50
Annex C General methods for safety analysis	A52
C.1 Early Risk Assessment by HAZOP	A52
C.2 Failure Modes and Effects Analysis (FMEA)	A53
C.3 Fault tree analysis (FTA)	A54
C.4 Hardware in the loop (HIL) testing	A55
Annex D General Methods of Assessment	A57
D.1 Expert Panel	A57
D.2 HMI Concept Simulation	A59
D.3 Driving Simulator Test	A60
D.4 Driving Tests with Professional Test Drivers	A61
D.5 Car Clinic with Naive Subjects	A63
Annex E Definition ADAS	A66
Annex F Documentation Sheet	A72
Annex G Criteria for HMI concept selection	
(background information)	A74
G.1 Classification and Evaluation according to driving tasks	A74
G.2 Driver Information Perception	A75
G.3 Driver's Field of Work	A79
G.4 HMI Architecture Principles	A81
Annex H References	A83

Figures

Figure 1: Phases of a development process.....	12
Figure 2: Elements of a safety process and controllability concept	13
Figure 3: Controllability Workflow. Dashed lines suggest revision.... due to new information	15
Figure 4: The three driving task levels	A4
Figure 5: Level of automation	A14
Figure 6: Methodology of risk assessment	A41
Figure 7: Collection of driving situations	A46
Figure 8: Extracting controllability related situations.....	A47
Figure 9: Driving task levels	A68
Figure 10: Driver Assistance systems.....	A69
Figure 11: Examples of Driver Assistance systems.....	A70
Figure 12: Simplified demonstration of field of view limits	A77
Figure 13: Limits of acoustic perception	A78
Figure 14: Detailed description of foot well and reach areas	A79

Tables

Table 1: Abbreviations.....	11
Table 2: Mapping of phases from the developing process	17
Table 3: Categorisation of Severity	A43
Table 4: Categorisation of Exposure	A43
Table 5: Categorisation of Controllability for risk assessment... ..	A44
Table 6: Determination of Automotive Safety Integrity Level.....	A45
Table 7: Driver assistance systems and ADAS criteria	A67
Table 8: Concept comparison for HMI	A74
Table 9: Haptic perception.....	A79

1 Introduction

1.1 Motivation

Advanced driver assistance systems will play a major role in road safety in Europe. Experience gained from research on ADAS shows, that many ideas have been applied in prototypes with safety features, but only few have been introduced in series production.

Existing technical limits as well as liability issues are currently delaying the market introduction of Advanced Driver Assistance Systems.

Resulting from the Response 1 project (1998 - 2001) the creation of a Code of Practice (CoP) was proposed for the development and validation of ADAS. This implies to establish "principles" for the development and evaluation of ADAS on a voluntary basis, as a result of a common agreement between all involved partners and stakeholders, mainly initiated by ADAS manufacturers.

The proposal to establish such a Code of Practice was confirmed by the Commissions Communication COM(2003) 542 of 15 September 2003.

The requirements for the Code of Practice have been elaborated within the project RESPONSE 2 (2002 – 2004).

RESPONSE 3 has now finally developed the CoP to provide the vehicle industry with the tools and common understanding to overcome and to help managing the problems about safety concerns and liability of Advanced Driver Assistance Systems.

The application of the CoP is a possibility to demonstrate that state-of-the-art procedures in ADAS development have been applied, including risk identification, risk assessment and evaluation methodology.

The current status of development makes it very difficult to describe the state-of-the-art knowledge of ADAS, because there are so many systems with different technology addressing even more different assisting functions.

This links the liability discussion to the term "defective product". Risks of ADAS may be highly complex. The term "defective product" is used in the European Product Liability Directive not only in a technical sense but it is also linked to human factors including system requirements such as dependability, controllability, comprehensibility, predictability and misuse resistance. Currently the technological safety issues are standardised within ISO TC22 while RESPONSE 3 is focussing on the human-machine interaction safety issues of ADAS, in particular on driver controllability, an ADAS key issue.

The RESPONSE 3 consortium is now encouraging all people involved in the ADAS development to benefit from applying the Code of Practice in their companies

1.2 Scope

The Code of Practice applies to advanced driver assistance systems (ADAS). It is not specifically intended to be applied to systems providing vehicle stabilisation (such as ABS and ESP) or mere information and communication systems (such as navigation systems and telephones). It may be applicable to systems including vehicle to vehicle communication, but will not cover these completely.

ADAS are designed to actively support the driver in the primary driving task to either increase comfortable or safe driving. (see Table 7 in Annex E for a list of systems). Systems that support the driver by issuing warnings without intervention are not within the scope of this CoP although the recommended approach and the provided checklists may prove valuable also for these kinds of systems. If the CoP is to be applied for a warning system a tailoring by experts will be necessary.

In contrast to conventional driver assistance systems, ADAS require the detection and evaluation of the vehicle environment with the respective sensors and a complex signal processing depending on the driving task to be supported. This also includes collection and evaluation of infrastructure data if available. This functional extension means a significant increase in system design complexity since the vehicle environment is incorporated into the assistance function. Due to the system limits of environmental sensing systems, the usage of the assistance functionality will also be limited. This implies that a direct interaction between the driver and the system is necessary. This interaction has to be controllable also with regard to current legislation (Vienna Convention)

The CoP serves as a support tool for the engineer engaged in the development of ADAS. CoP not only means a compilation of currently available procedures, but also offers clues for determining activities to be performed during the individual development phases.

Focus of the CoP is the system design against the background of system controllability and the total vehicle from the field of view of Human Machine Interaction. Of course system influences due to occurring defects/errors do play an important role as well as ADAS behaviour at system limits and foreseeable misuse.

Moreover, the CoP is also intended for automotive manufacturers and suppliers dealing with specification, realisation and assessment of ADAS. The CoP has been compiled by gathering best practices of the partner companies and also considers legal requirements and the RESPONSE 2 results

The CoP deals with specification and assessment of advanced driver assistance systems during the entire development phase. Therefore, it will not address issues arising after SOP (start of production).

The CoP structure allows implementation as part of a company specific development or quality process. Requirements are supplied for each development stage and are clearly separated from checklists and method descriptions in the document in order to provide an overview for each task. The use of the checklist proce-

procedure assists in the specification of ADAS in order to also consider aspects which may not be obvious right from the beginning. The hazard and risk analysis procedure provides assistance in setting up a systematic analysis of driving situations in order to determine potential risks.

The CoP also comprises the description of methods and tools for the assessment of ADAS safety.

The CoP should not stipulate a uniform ADAS design. It should be valid for various vehicle types and systems with many complexity and integration levels for the application in all ADAS.

All in all the CoP aims at serving as a guideline assisting persons involved in ADAS development to adhere to the state-of-the-art knowledge with respect to risk identification and risk assessment as well as methodology for the evaluation of driver controllability.

2 Terms and Definitions

2.1 Definition of an Advanced Driver Assistance System (ADAS)

This definition gives an overview and classification of ADAS as a basis for the correct application of the CoP.

Driver Assistance Systems are supporting the driver in their primary driving task. They inform and warn the driver, provide feedback on driver actions, increase comfort and reduce the workload by actively stabilising or manoeuvring the car.

They assist the driver and do not take over the driving task completely, thus the responsibility always remains with the driver.

ADAS are a subset of the driver assistance systems.

ADAS are characterised by **all** of the following properties:

- support the driver in the primary driving task
- provide active support for lateral and/or longitudinal control with or without warnings
- detect and evaluate the vehicle environment
- use complex signal processing
- direct interaction between the driver and the system

With respect to the well-known categories of driving tasks, ADAS are focussing on the manoeuvring level. For a detailed description of driving tasks and typical ADAS please refer to Annex E.

2.2 Glossary

1. **Abbreviated Injury Scale:** An anatomical scoring system for ranking the severity of injury (Association for the Advancement of Automotive Medicine).
2. **Adaptive Cruise Control:** Enhancement to conventional cruise control systems, which allows the subject vehicle to follow a forward vehicle at an appropriate distance by controlling the engine and/or power train and potentially the brake. (ISO 15622)
3. **Advanced Driving Assistance Systems (ADAS):** See chapter 2.1 for a definition of ADAS.
4. **Action:** An event initiated by the driver or the application
5. **Action slip:** A human action deviating from the intended plan, e.g. the driver want to shift gears but unintentionally pressed the brake pedal due to a missing clutch in cars with automatic transmission. An action slip often occurs if the driver is absentminded and may increase in frequency under stress. [Red 97]¹

¹ [Red 97]: Redmill, F ; Rajan, J: Human factors in safety critical systems; butterworth-Heinemann 1997, p. 49

6. **Architecture:** The fundamental organisation (both HW and SW) of a system embodied in its components, interaction among components, and to the environment, and the principles guiding its design and evolution.
7. **Automotive safety integrity level (ASIL):** One of four steps to specify the risk and its requirements for risk reduction with *D* representing the highest and *A* the lowest risk reduction class (ISO/WD 26262-1).
8. **Behavioural Changes (Adaptation):** Behaviour which may occur following the introduction of changes to the road-vehicle-driver system and which were not intended by the initiators of the change or by the system developers.
9. **Code of Practice (CoP):** Guidelines for procedures and processes that may be used during specification and realisation of ADAS in order to state reasonable safety and duty of care. [IP_D4 06]²
10. **Collision Avoidance:** System for warning and avoidance of a pending collision. [IP_D4 06]²
11. **Collision Mitigation:** System that helps vehicle occupants or unprotected road users to survive in crash and to minimise its effect by activating vehicle functions that reduce the retardation forces in an impact. However, it must be remembered that systems may also reduce the vehicle impact velocity, and thereby increase vehicle retardation by means of autonomic braking manoeuvres before the crash. [IP_D4 06]²
12. **Concept phase:** The first phase of a project in which the need is examined, alternatives are assessed, the goal and objectives of the project are established and a sponsor is identified.
13. **Comprehensibility:** Degree to which information is understood that is conveyed to the driver; the quality to be comprehensible; capability to be understood
14. **Controllability:** likelihood that the driver can cope with driving situations including ADAS-assisted driving, system limits and system failures (for a detailed discussion see chapter 4).
NOTE: this definition differs from ISO 17287
15. **Defective Product:** A product is defective when it does not provide the safety a person is entitled to expect, taking into account all circumstances, including: (a) the presentation of the product; (b) the use to which it could reasonably be expected that the product would be put; (c) the time when the product was put into circulation (product liability law).
16. **Definition Phase** The first development subphase of the concept phase where the system definition is drafted (see Figure 1).

² [IP_D4 06]: PReVENT IP public deliverable IP D4 on Functional Requirements

17. **Dependability:** The trustworthiness of a computing system, which allows reliance to be justifiably placed on the service it delivers. [IFIP]³
18. **Development phase:** The time in the product life cycle where the system is developed from the first idea to production.
19. **Driver Distraction:** The process of diverting the attention of the driver from the driving-task to something else.
20. **Driver Intent:** The aim of the driver to perform an action.
21. **Equipped Vehicle:** vehicle equipped with the ADAS applications in question and related to the topic of discussion (ISO 15622).
22. **Error:** The difference between the desired and actual value or performance of a system or human action.
23. **Failure:** The inability of a component or system to perform its intended function as designed. Failure may be the result of one or many faults.
24. **Failure Mode And Effect Analysis (FMEA):** A method to examine potential failures in a system or process, to evaluate consequences and define remedial actions (see C.2 for a detailed description).
25. **Fault:** An abnormal condition or defect at the component or sub-system level which may lead to a failure.
26. **Fault Tree Analysis (FTA):** A deductive analysis method that begins with a general conclusion (a system-level undesirable event) and then attempts to determine the specific causes of this conclusion (see C.3 for a detailed description).
27. **Function:** a) A description of what something does or is used for; b) A routine that returns a result.
28. **Functional Requirements:** A description what the system is required to do. Functional requirements make the basis of the scope of work of the project, defining user functions, system limitations, types of inputs and outputs, etc.
29. **Functionality:** A set of functions associated with software or hardware.
30. **Harm:** Physical injury or damage to the health of people either directly or indirectly as a result of damage to property or to the environment (EN 61508).
31. **Hazard:** Potential source of harm (EN 61508).
32. **Hazard and Operability Study (HAZOP):** A systematic qualitative technique to identify process hazards and potential operating problems using a series of guide words to study process deviations (see C.1 for a detailed description).

³ [IFIP]: IFIP WG10.4 on Dependable Computing and Fault Tolerance (www.dependability.org)

33. **Hazardous Situation:** Circumstance in which a person is exposed to hazard(s) (EN 61508)
34. **Homologation:** The granting of approval by an official authority based on a set of strict rules or standards to determine whether such approval should be given
35. **Human Factors:** A profession that focuses on how people interact with products, tools, procedures, and any processes likely to be encountered in the modern world. Also referred to as “ergonomics”.
36. **Human Machine Interaction (HM Interaction):** All the possible modes by which an interaction (direct or indirect) between the driver and one or more vehicle systems occurs.
37. **Human Machine Interface (HMI):** Element or sub-element of a system with which the driver can interact, i.e. all the input and output devices (e.g. knobs, switches, levers, displays), which permit the interaction between the driver and one or more vehicle systems.
38. **Impact analysis:** Determines which areas and previous work products are impacted by an intended change.
39. **Intervening system:** A system that triggers actuators like a braking or steering system based on environmental sensor information to avoid e.g. a lane departure or to mitigate a forward collision. Intervening systems usually include a preceding warning phase, therefore showing characteristics of both, ADAS and active safety systems.
40. **In-vehicle Information System (IVIS):** A system supporting the driver in the navigation task, i.e. giving information to support the driver in reaching their destination. Also referred to as “driver information system”.
41. **Macroscopic Effects:** Effects (and consequences) that are shown by a system considered as a whole. In other words, they are the “global behaviour”, due to the interactions between the single elements of a system; opposite to macroscopic effects, there are the microscopic ones, which are due to the single elements constituting a system. In this CoP the “system as a whole” is often considered to be the traffic system while the “single elements” are the cars.
42. **Malfunction:** Referring to a system that is not performing its intended function.
43. **Manoeuvring Level:** The second of the three levels of a driving task (see also stabilisation and navigation level). Tasks related with adhering to traffic rules and avoiding collisions are within this category.
44. **Misuse:** Use of the (TICS) functions intended by the manufacturer to be used while driving in a way or manner not intended by the manufacturer and which may lead to adverse consequences (ISO 17287). Note the difference to “abuse” which is not covered by the CoP.

45. **Naïve subject:** An expression for a person that tests the ADAS under evaluation with no more experience and prior knowledge of the system than a later customer would have.
46. **Navigation Level:** The highest of the three levels of a driving task (see also stabilisation and manoeuvring level). Tasks related with finding a route to the driver's destination are within this category.
47. **Normal Operation:** a system working under standard conditions (inside its operative range).
48. **Open item list:** Means to collect track issues or questions that cannot immediately be answered while working on a certain topic (e.g. an open question from a checklist). See also Figure 3.
49. **Outlier:** In statistics, an outlier is a single observation "far away" from the rest of the data.

In most samplings of data, some data points will be further away from their expected values than what is deemed reasonable. This can be due to systematic error, faults in the theory that generated the expected values, or it can simply be the case that some observations happen to be a long way from the centre of the data. Outlier points can therefore indicate faulty data, erroneous procedures, or areas where a certain theory might not be valid. However, a small number of outliers is expected in normal distribution.

Outliers have to be removed from the dataset in order to achieve correct results and draw the correct conclusions after an experiment.

50. **Perceptibility:** The possibility for the driver to perceive information that is presented to them by the system (see also: perception)
51. **Perception:** In psychology and in cognitive sciences, it is the process of acquiring, interpreting, selecting, and organizing sensory information. Methods of studying perception range from essentially biological or physiological approaches, through psychological approaches to the often abstract 'thought-experiments' of mental philosophy.
52. **Physical Control Loop:** A control loop describes algorithms arranged as to regulate the output at a setpoint. The algorithms are using feedback to continuously optimise the output. The term "physical" describes the fact that the driver is within the loop, i.e. the feedback of the driver to the system action (or warning) is needed in order for the algorithm the work as intended.
53. **Predictability:** The degree to which a correct prediction of a system's state can be made either qualitatively or quantitatively.
54. **Primary Driving Task:** Those activities that the driver has to undertake to maintain longitudinal and lateral vehicle control within the traffic environment (ISO 17287). Namely, all aspects involved in mastering a vehicle to obtain a certain goal (e.g.

reach a destination). This corresponds to the primary task in a driving situation.

55. **Proof of Concept:** The (optional) last development subphase of the concept phase where the preceding steps are justified (see Figure 1).
56. **Risk:** Combination of the probability of occurrence of harm and the severity of that harm (EN 61508).
57. **Road Users:** All type of subjects (including vehicles, pedestrians, cyclists etc.), which use the road and its layout.
58. **Secondary Driving Task:** Additional driver activities that are not directly related to the vehicle control e.g. tuning the radio, changing settings of the air conditioning, programming the navigation system.
59. **Series Development:** The development phase after the concept phase. The targeted development of a system concept for a specific car series.
60. **Sign-off:** The last step during product development concluding that the system is ready for production; based on evidence collected during development.
61. **Situational Awareness:** The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future.
62. **Specification (framework):** A set of requirements that have to be met by a system.
63. **Stabilisation Level:** The lowest of the three levels of a driving task (see also stabilisation and manoeuvring level). Tasks related with finding keep the car under control (lateral and longitudinal).
64. **System:** A collection of components organised to accomplish a specific function or set of functions.
65. **System Limit:** The operational limitations of a system. A limitation is defined during development or implicitly introduced due to physical/technical constraints, a restriction of operative scenarios, intrinsic functionality of hardware components etc.
66. **System State:** The state in which a system (or its sub-system) actually is.
67. **Transport information and control system (TICS):** Single function, such as route guidance, or number of functions designed to work together as a system (ISO 17287).
68. **Usability:** Concept comprising the effectiveness, efficiency and satisfaction with which specified users can achieve specified goals in a particular environment (ISO 17287).

NOTE As well as effectiveness, efficiency and satisfaction, usability involves learnability, controllability, error robustness and adaptability.

69. **Use Cases:** An intended or desired flow of events or tasks that occur within the vehicle and are directed to or coming from the driver in order to accomplish a certain system-driver interaction
70. **Valid subject:** A valid subject is a participant of an experiment who took part in the whole experiment, where the complete dataset is available and no reason for declaring the dataset as an outlier is given.
71. **Validation:** The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies the expectations.
72. **Vehicle:** In the CoP specifically motorised road vehicles, i.e. cars, trucks, buses and motorcycles.
73. **Verification:** Assuring, e.g. by testing, that a component, a sub-system, a system or a process is working as required and specified.
74. **Vigilance:** The process of paying close and continuous attention or readiness to detect and effect an adequate response to unforeseen, small and specific changes of environment; proper attention in proper time
75. **Workload:** Degree of mental, physical and perceptual effort required by the driver to undertake a particular task (ISO 17287).
Also **mental workload:** the specification of the amount of information processing capacity that is used for task performance.

2.3 Abbreviations

Abbreviation	Meaning
AAM	Alliance of Automobile Manufacturers (US)
ACC	Adaptive Cruise Control
ADAS	Advanced Driver Assistance System
AIS	Abbreviated Injury Scale
ASIL	Automotive Safety Integrity Level
C	Controllability
CoP	Code of Practice
DAS	Driver Assistance System
DIN	Deutsches Institut für Normung e.V. (German organisation for standardisation)
DUT	Device Under Test
E	Exposure to a situation where hazards exist
ECU	Electronic Control Unit
ESoP	European Statement of Principles on the Design of Human Machine Interaction
ESP	Electronic Stabilisation Programme

f	frequency (of occurrence of a hazardous event)
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
FTA	Fault Tree Analysis
H&R	Hazard analysis and Risk assessment
HAZOP	HAZard and OPerability study
HIL	Hardware In the Loop
HMI	Human Machine Interface
ISO	International Organisation for Standardisation
IVIS	In-Vehicle Information System
MAIS	Maximum AIS (Abbreviated Injury Scale)
POST	Power On Self Test
R	Risk
S	potential Severity of the resulting harm or damage
TICS	Transport Information and Control System
AIDE	Adaptive Integrated Driver-vehicle InterfacE
I/O	Inputs/Outputs
SUV	Sport Utility Vehicles
SoP	Start of Production

Table 1: Abbreviations

3 Development Process

Following, please find a generic development process provided to facilitate a classification of the elements described in the CoP. This generic development process reflects in general the logical sequence of product development phases of a product development as well as selected milestones, but not necessarily their time sequence (Figure 1). Therefore, it corresponds to a simplified presentation of reality. Possible iteration loops accompanying individual development phases are not shown.

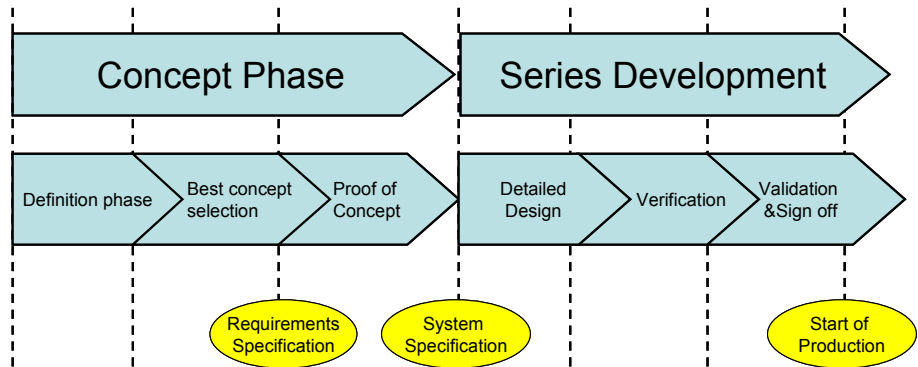


Figure 1: Phases of a development process

Since RESPONSE 3 is focussing on safety aspects of HM Interaction, Figure 2 shows activities regarding HMI development. This does not necessarily represent a separate development process, but the activities are normally integrated into the product development process.

In respect to this CoP the specific safety relevant aspects are now considered. Principally the ADAS safety aspects may be classified in three categories. HM Interaction and the related controllability is analysed

- within system limits (normal operation, ADAS assisted driving),
- at system limits and
- with system failures.

All categories are evaluated by means of measures confirming controllability with respect to possible risks 0(Annex A.3). Depending on the risk evaluation, requirements for the safety concept as well as the HMI are derived

For a system with safety implications additional safety related activities are performed. For the automobile industry requirements for a safety related development process are formulated in a domain specific safety standard. This is presently done in the ISO TC22 / SC3 / WG 16.

Figure 2 shows additional elements of a general safety process (in white) and activities regarding controllability (in yellow). The elements of a general safety process are depicted, as the elements of

the CoP may be included into a company specific safety process. The CoP itself will focus on the activities regarding controllability. The concept of controllability is described in chapter 4. Regarding the safety of ADAS (for a definition of ADAS see chapter 2.1 and Annex E) the concept of controllability is the central issue. According to legal requirements, an ADAS is considered safe, as long as the driver is able to control the vehicle.

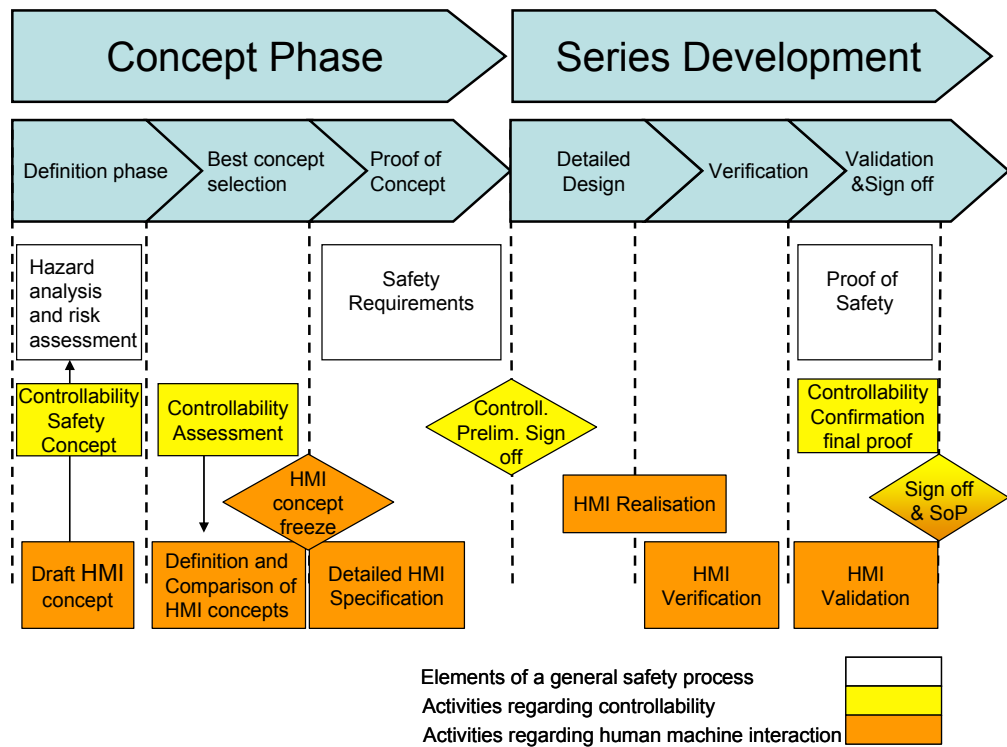


Figure 2: Elements of a safety process and controllability concept

The development process described above has only to be applied completely with regard to a new development of an ADAS system. In case of modifications (derivate or change) of existing systems, an impact analysis should be performed to assess the relevant areas affected by the modification.

The vehicle manufacturer is responsible for the application and documentation of the CoP. If development tasks and services are performed by a supplier, the supplier must be informed about the CoP and/or relevant information of the ADAS interfaces and the integration into the vehicle. Responsibilities need to be agreed between the vehicle manufacturer and the supplier.

4 Controllability

In this CoP controllability is a key requirement. Controllability refers to the entire ADAS-driver-environment interaction which comprising:

- normal system use within system limits,
- usage at and beyond exceeding system limits and
- usage during and after system failures.

Controllability is dependent on

- the possibility and driver's capability, to perceive the criticality of a situation,
- the drivers capability to decide on appropriate countermeasures (e.g. override, system switch-off) and
- the driver's ability to perform the chosen countermeasure (e.g. reaction time, sensory-motor speed, accuracy).

Safety of usage requires controllability. Compared to controllability other design requirements are of secondary importance.

Controllability is a basic parameter in the automotive risk assessment (as proposed in the draft of the functional safety standard ISO WD 26262-3). Within this future hazard analysis and risk assessment (H&R), controllability of safety relevant electronic devices has to be estimated in early development stages.

The CoP assists early controllability estimation and later confirmation by providing checklists and references to state-of-the-art evaluation methods. The annexes provide checklists responding to the input to the H&R. Results from the H&R and checklist questions lead to open items that should be compiled in an Open Item List for further tracking of the development status. The list can also be used to derive a controllability evaluation plan.

Figure 3 provides an overview of the possible workflow with regard to controllability.

At the end of the ADAS development the CoP recommends a Controllability Final Proof to confirm that sufficient controllability is achieved for the production version of the system, in particular for intervening systems.

Therefore, the ADAS Development Team has to verify that drivers will react as previously anticipated or in an appropriate way in relevant scenarios. The data utilised is from the H&R, the checklists and the test results have been conducted according to the evaluation plan.

Three equally respected ways are offered by the CoP to finally prove that the driver can react and will do so in the expected way (Figure 3):

- Final proof of controllability by an interdisciplinary expert panel (chapter 4.1)

- Final proof of controllability by a test with naive subjects (chapter 4.2)
- Final proof - direct recommendation of Controllability Sign-Off by the ADAS Development Team (chapter 4.3)

The ADAS Development Team is free to choose the appropriate way for each particular scenario. A mixed approach is possible.

When the controllability relevant design of the system is confirmed by the ADAS Development Team a recommendation for sign-off can be given from the Code of Practice point of view.

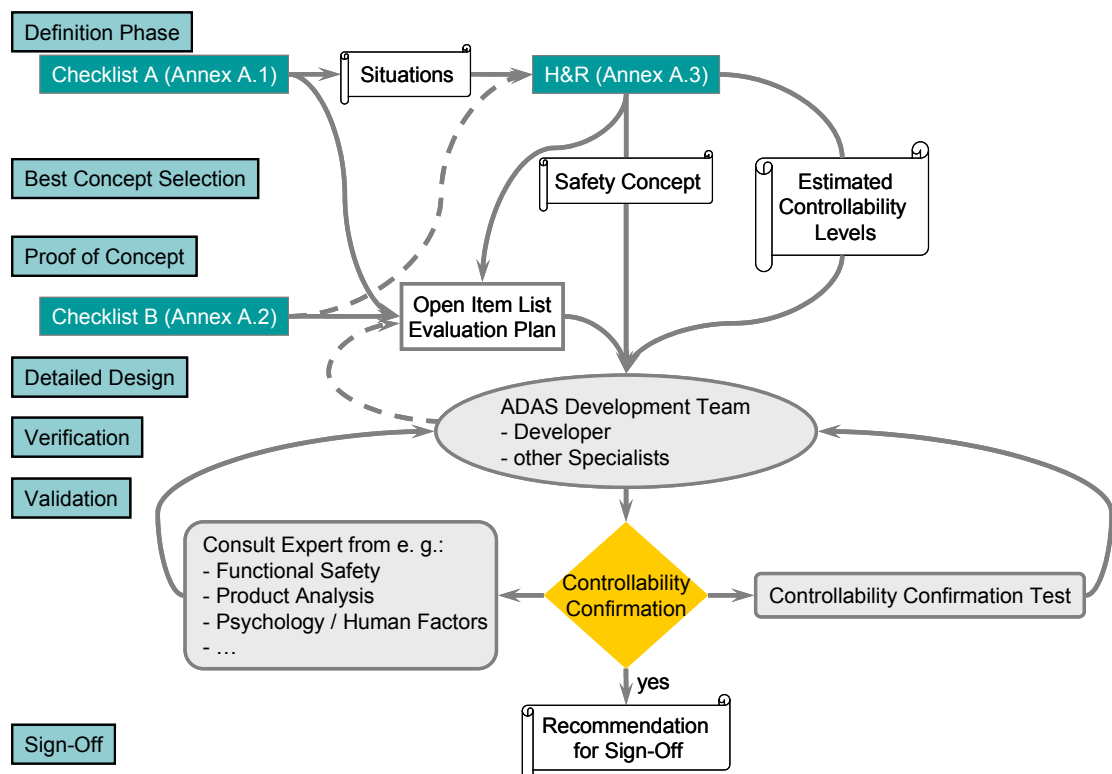


Figure 3: Controllability Workflow. Dashed lines suggest revision due to new information

4.1 Final proof of controllability by an interdisciplinary expert panel

The controllability estimations are reviewed by an interdisciplinary Expert Panel. This Expert Panel for Final Proof is a cross-functional group of individuals (the ADAS Development Team and additional specialists). It is recommended to include members of other departments in the panel to ensure “external” expertise and a third view of the controllability process.

The Expert Panel has to judge and confirm the controllability estimates. Therefore, the members of the panel must be familiar with the system in adequate situations. The judgment can be based on analogies, literature and previous studies during development phase etc. When in doubt, the Expert Panel will gather additional information for clarification. For this purpose a test might also be performed.

4.2 Final proof of controllability by means of a test with naive subjects

Statistical proof of absolute controllability is not possible. Furthermore, a test to demonstrate that 99 % of the drivers “pass” the test in a certain traffic scenario is not feasible because a huge number of test subjects would be necessary to demonstrate this.

Consequently, the Code of Practice recommends a different approach.

Practical testing experience revealed that a number of 20 valid data sets per scenario can supply a basic indication of validity. A data set is not considered as being valid if a subject fails due to a reason that is not system related (e. g. due to motion sickness in a driving simulator). The test design should also consider the possibility of the occurrence of outliers. Criteria for the classification of outliers should be established according to the state of the art in human factors testing. In order to enlarge the data basis it is possible to perform retests with the same test subjects, prerequisite is that the effect on the test subject behaviour is negligible.

To assume controllability in accordance to the CoP naive subjects should be tested in relevant scenarios. Naive means that the subjects have no more experience and prior knowledge of the system than a later customer would have. The test-scenario is “passed” if the subject reacts as previously anticipated or in an adequate way to solve the situation.

To show a controllability of the given task of at least 85 % all 20 valid data sets must fulfill the pass criteria.

Testing can be carried out in any of the following ways (see Annex D):

- On public roads,
- on proving grounds or
- in a simulator
- etc.

4.3 Final proof - direct recommendation of Controllability Sign-Off by the ADAS Development Team

In some projects all open issues on the Open Item List are easily solved by the ADAS Development Team. Additionally a sufficient number of tests in a technical status representing the final system design may have been conducted with positive results during development.

In this case the ADAS Development Team may initiate the sign-off for final proof without any further tests or consultation of an Expert Panel.

5 Recommendations

The objective of this chapter is to present the recommendations for a safe development of ADAS. The content of this chapter is structured according to the generic development process introduced in Figure 1 and Figure 2. Table 2 references the activities of the generic development process.

The entire concept phase splits into the parts 'definition phase', 'best concept selection' and 'proof of concept'. Comparison of concept alternatives and the selection of one of them is economically reasonable. Consequently, the definition phase deals with drafting HM Interaction concepts. Subsequently the drafted HM Interaction concepts are compared and the most suitable one is chosen for realisation. Finally, the concept selected has to be specified in the proof of concept section. Note that general ADAS development topics are only covered to the extent that controllability specific topics can be described.

Main phase	Sub phase	Recommended steps
Concept phase	5.1 Definition phase	5.1.2 Draft HM Interaction concept and Controllability safety concept
	5.2 Best concept selection	5.2.2 HM Interaction concept specification
		5.2.3 Selection of HM Interaction concept
	5.3 Proof of Concept	5.3.2 Preparation of preliminary sign-off
		5.3.3 Controllability preliminary
Series development	5.4 Detailed design	5.4.2 Detailed HM Interaction design
	5.5 Verification	5.5.2 Verification of HM Interaction
	5.6 Validation and Sign-off	5.6.2 Controllability confirmation & final proof
		5.6.3 Sign-off

Table 2: Mapping of phases from the developing process to sections in chapter 5

The recommendations are described as activities. Each activity is presented in the same format. The tasks of each activity are presented in chronological order.

<p>Activity A: <i>Name of activity (optional activities without grey shading)</i> requires: <i>reference to prerequisites</i></p>
<p>a) <i>Name of task</i></p> <ul style="list-style-type: none"> • <i>Explanation of subtask</i> • <i>Explanation of subtask</i> <p>▶ Annex A.1</p>
<p>a) <i>Name of task</i></p> <ul style="list-style-type: none"> • <i>Explanation of subtask</i> <p>▶ Annex A.1</p>

5.1 Definition phase

5.1.1 Objective

The objective of this section is to develop a level of comprehension of the intended system and its environment to an extent that other development cycle activities may be performed satisfactorily.

Recommendations that need to be considered at the start of a system development will be listed in this chapter.

5.1.2 Draft HM Interaction concept and Controllability safety concept

At least one ADAS concept is drafted in this subphase. Every concept should be drafted according to the set of recommendations of this section, which are related to the main aspects: ADAS functionality, ADAS HM Interaction, ADAS usage, ADAS standards and ADAS hazards & risks.

<p>Activity A: ADAS functionality</p>
<p>a) Assigning function name</p> <ul style="list-style-type: none"> • Introduce a suitable name for the ADAS function
<p>b) Drafting functionality</p> <ul style="list-style-type: none"> • Define system status, modes, transitions and actions • Characterise situational limits and initial sensor requirements • Sketch system behaviour under situational limits • Clarify interaction with other systems <p>▶ Annex A.1</p>

Activity B: HM Interaction

requires: 5.1.2 A, D

a) Drafting HM Interaction

- Sketch driver activities to operate the system
- Characterise transferred information
- Define take over procedures

▶ Annex A.1

b) Drafting physical layout

- Consider an integration of the HM Interaction concept in the vehicle
- Draft controls and displays (system input and output)

▶ Annex A.1

Activity C: Usage

requires: 5.1.2 A,, B, D

a) Defining domain

- Characterise the intended market for the ADAS
- Describe the type of vehicle for which the ADAS is intended
- Draft the environment and roads in which the ADAS is used
- Characterise the user group of the ADAS

▶ Annex A.1

b) Characterising use

- Draft operating scenarios
- Sketch user expectations, misinterpretation, overestimation

▶ Annex A.1

c) Characterising misuse

- Draft non operating scenarios
- Identify reasonably foreseeable misuse
- Find possible measures to avoid misuse

▶ Annex A.1

Activity D: Standards

requires: 5.1.2 A

a) Ensuring conformity

- Look for relevant standards and regulations

▶ Annex A.1

Activity E: Preliminary Hazard analysis and risk assessment

requires: 5.1.2 A, B, C, D

a) Identifying hazards

- Identify possible hazardous situations and the relevant sources of hazards within the drafted ADAS function for normal operation, system failure and system limits.

▶ Annex A.1, B.1

b) Analysing hazards

- Perform hazard analysis paying specific attention to the controllability aspect

▶ Annex A.3

c) Assessing risk

- Perform a risk assessment for the analyzed hazards

▶ Annex A.3

5.2 Best concept selection

5.2.1 Objective

In this part of the concept phase suitable criteria for discriminating various concepts are defined. Based on these criteria the results can be used to select a concept.

The selected HM Interaction concept will be incorporated into a detailed specification as part of the overall system requirements specification.

5.2.2 HM Interaction concept specification

The concept specification is a general development activity. The detailed definition of system limits is part of the company individual design strategy and therefore not covered here.

Activity A: Controllability concept

requires: 5.1.2 E

a) Specifying the controllability concept

- Specify HM Interaction based on the draft concept and controllability results from a risk assessment

▶ Annex A.1, A.2

Activity B: HM Interaction

requires: 5.1.2 B,

a) Specifying system transitions

- Identify driver initiated transitions that correspond to operator control actions
- Identify system initiated transitions, caused by changing environmental conditions as well as exceeding the system limits
- Identify system initiated transitions, caused by system failure or failures of other interacting systems

▶ Annex A.1

b) Specifying system dialogs

- Describe the system feedback to the driver for controllability relevant system states and transitions
- Describe the input/output modalities and dialogs

▶ Annex A.1

c) Specifying physical layout

- Consider controllability aspects of system states and transitions for specification of the controls and displays

▶ Annex A.1

5.2.3 Selection of HM Interaction concept**Activity A: Evaluation criteria**

requires: 5.1.2 E

a) Defining criteria

- Define criteria for the evaluation of the concepts considering controllability requirements based on the risk assessment

▶ Annex A.3, B.3

Activity B: Selection of concept

requires: 5.2.2 B

a) Finding a best concept

- Evaluate the concepts and select the most suitable one according to the defined requirements. Check if the HMI is suitable for the intended task in normal operation, at system limits and with system failures

▶ Annex A.2, A.3

5.3 Proof of Concept

5.3.1 Objective

In this part of the concept phase the drafted and selected ADAS concept has to be specified focusing on controllability. The structure of this activity is presented in the detailed HM Interaction specification section.

In order to finalise the concept specification a concept sign-off or equivalently a preliminary sign-off is recommended. The structure of this activity is supplied in the concept sign-off section.

5.3.2 Preparation of preliminary sign-off

The preliminary sign-off is an optional activity, which might be necessary or desirable for various reasons, e.g. the transfer of activities from a research to a serial development department.

Even if this is not the case it is still recommended to start with verification and validation as early as possible in order to minimise the risk of critical findings at a late stage of product development. However it is at the discretion of the developer when these activities are performed and therefore the recommended activities are optional in this early stage of product development.

Optional activities in this document have a white heading instead of a grey heading.

Activity A: Review of HM Interaction specification (optional)

requires: 5.2.2 B

a) Define a validation strategy

- Document the procedure in a preliminary review plan for the specified HM Interaction concept.

▶ Chapter 5.6 gives an overview on activities that are required in the validation phase

b) Performing the review

- Review the HM Interaction concept specification according to the plan and identify possible problem areas

▶ Chapter 5.6

<p>Activity B: Further proceeding (optional) requires: 5.1.2 A, 5.2.3 B</p>
<p>a) Considering additional tests</p> <ul style="list-style-type: none"> • Check for further tests necessary to assess controllability (controllability relevant topics that can be clearly identified as easily controllable, according to the state of the art in the area of human factors, need not be tested). • Perform necessary tests (in cases of doubt or in lack of experience tests are recommended) <p>► Annex B, Annex D</p>
<p>b) Documenting important topics</p> <ul style="list-style-type: none"> • Document the achieved results • Document the open controllability topics and the required phase of development necessary to perform a certain test. <p>► Chapter 5.6.2 Activity C, Open item list (Chapter 4, Figure 3)</p>

5.3.3 Controllability preliminary sign-off

<p>Activity A: Preliminary Sign-off (optional) requires: 5.3.2 A, B</p>
<p>a) Deciding on concept sign-off</p> <ul style="list-style-type: none"> • Sign-off the HM Interaction concept or initiate appropriate rework. (the responsible person / project manager etc.)

5.4 Detailed design

5.4.1 Objective

During the detailed design phase the development is continued based on the ADAS concept that was selected and the HM Interaction concept was specified. The main focus of this section is controllability, which is strongly related to the HM Interaction design. The comprehensive functionality of the ADAS design is part of the overall ADAS development and kept in the background.

5.4.2 Detailed HM Interaction design

<p>Activity A: HM Interaction detailed Design (optional) requires: 5.1.2 A, 5.2.3 B, 5.3.2 B</p>
<p>a) Designing HM Interaction architecture</p> <ul style="list-style-type: none"> • Develop the functional subdivision • Define which functions are performed by the driver, by hardware, software or in combinations. • Consider relevant user tasks and activities • Define input and output by systematically detailing relevant system states & transitions and the related interactions between driver and system <p>▶ Annex A.1</p>
<p>b) Designing physical layout</p> <ul style="list-style-type: none"> • decide on the appropriate physical layout of the input and output devices (controls and displays) <p>▶ Annex A.1</p>
<p>c) Integrating into overall design</p> <ul style="list-style-type: none"> • integrate ADAS HM Interaction design into overall design regarding <ul style="list-style-type: none"> - prioritisation of system outputs (e.g. warnings and messages) in relation to other functions - driver workload <p>▶ Annex A.1</p>
<p>Activity B: Update Hazard analysis and risk assessment requires: 5.1.2 E, 5.4.2 A</p>
<p>a) Updating hazard analysis and risk assessment</p> <ul style="list-style-type: none"> • update by including information from detailed design of HM interaction <p>▶ Annex A.3</p>

5.5 Verification

5.5.1 Objective

In this context verification relates to the HM Interaction design. That is, checking and documenting if and how the controllability related requirements of the developed HM Interaction design are fulfilled. Successful verification ends with the release of the HM Interaction design; otherwise rework needs to be performed.

5.5.2 Verification of HM Interaction

<p>Activity A: HM Interaction verification requires: 5.4.2 A</p>
<p>a) Verifying HM Interaction</p> <ul style="list-style-type: none"> • Verify the design based on its specification concerning HM interaction requirements for system and human performance <p>▶ Annex C</p>
<p>b) Documenting verification</p> <ul style="list-style-type: none"> • Document and report the verification results. • Initiate necessary further actions if a non-conformance to requirements is found <p>▶ Chapter 5.6.2 Activity C, Open item list (Chapter 4, Figure 3)</p>

5.6 Validation and Sign-off

5.6.1 Objective

At the end of the development process a sign-off is carried out to confirm that the system complies with the specified controllability related recommendations.

Controllability confirmation and the final proof may require specific actions and documents.

5.6.2 Controllability confirmation & final proof

The validation strategy is defined in the validation plan. It is possible to refer to earlier results e.g. from the preliminary controllability sign-off during the proof-of-concept phase, if still applicable.

<p>Activity A: Planning validation scenarios requires: 5.4.2 A, B</p>
<p>a) Identifying driving situations</p> <ul style="list-style-type: none"> • Consider the following situations <ul style="list-style-type: none"> - normal operation - behaviour at functional limits - behaviour in case of system failures • Compile a list of relevant driving situations for system validation and build reasonable clusters <p>▶ Annex B.1</p>

Activity B: Planning approach for final proof (done by the ADAS Development Team)

requires: 5.6.2 A

a) Selecting the appropriate strategy for each scenario

- Controllability confirmation by an independent expert panel (chapter 4.1)
- Controllability check by a test with naive subjects (chapter 4.2)
- Direct recommendation of Controllability Sign-Off by the ADAS Development Team (chapter 4.3)

▶ Chapter 4, Annex B.2, B.3, B.4

Activity C: Final proof

requires: 5.6.2 A, B

a) Controllability confirmation

- The experts perform the validation strategy, decide if the design has passed and give a recommendation for sign-off

▶ Annex D

b) Documenting controllability

- Document information that is sufficient to reproduce the recommendation for sign-off (e.g. approach, equipment, assumptions, decisions, test conditions)
- Compile a set of documents to confirm the controllability for the system sign-off. If the documentation is already available a collection of references is sufficient.

Documents from the risk assessment procedure, i.e.

- System and HM Interaction concept description
- Identified hazards
- Assessed risks
- Used checklists
- Assumptions

Controllability related HM Interaction requirements, i.e.

- Requirements and references to risks

5.6.3 Sign-off

Activity A: Sign-off

requires: 5.6.2 D

a) Signing-off the system

The responsible person (project manager etc.) can sign-off controllability

▶ Annex F