RESPONSE 3 - CODE OF PRACTICE FOR DEVELOPMENT, VALIDATION AND MARKET INTRODUCTION OF ADAS – A PReVENT PROJECT

Juergen Schwarz
Manager System Safety
DaimlerChrysler AG
HPC: T728, 70546 Stuttgart, Germany
Tel:+49 711 17 41920, Fax: +49 711 17 47054
E-mail: juergen.s.schwarz@daimlerchrysler.com

ABSTRACT

RESPONSE 3 is elaborating a European Code of Practice for an accelerated market introduction of Advanced Driver Assistance Systems (ADAS). This implies the development of “principles” for analysis and evaluation of the human factors aspects of ADAS on a voluntary basis, as a result of a common agreement between all involved partners and stakeholders. The Code of Practice will help manufacturers to “safely” introduce new applications through an integrated perspective on human, system and legal aspects. Partners of the RESPONSE 3 project are AUDI AG, BMW group, BOSCH, CRF, DaimlerChrysler, ERTICO, FORD, PSA, TNO, TRL and Volkswagen AG.

GOAL

Existing technical limits as well as liability issues are currently delaying the market introduction of Advanced Driver Assistance Systems. RESPONSE 3 will provide the vehicle industry with the tools and common understanding to overcome and to help managing these problems. The outcome of RESPONSE 3 should result in a Code of Practice overcoming the reservations of the OEMs regarding the evaluation of the safety issues of ADAS including preventive safety applications.
On a generic level, the Code of Practice will contain descriptions of procedures for analysis of user requirements, definition of systems and validation procedures. It will have a special focus on an integrated “system safety - human factors” approach and give advice on the evaluation of driver behaviour and expectations. The application of the Code of Practice will assist in judging legal questions regarding product liability, driver responsibility and the liability of the manufacturer.

With the wide acceptance of the Code of Practice, RESPONSE 3 will contribute to an accelerated market introduction of Advanced Driver Assistance Systems which includes preventive safety applications. It will be a key instrument to help engineers develop safe products, industry to control their risks and the authorities to understand and follow the development and testing processes. The need of a Code of Practice has also been concluded by the recommendations of the e-safety initiative (#20: Develop a methodology for risk-benefit analysis, achieve a consensus on a European Code of Practice, and establish guidelines for facilitating market introduction of intelligent integrated safety systems.)

STEPS TOWARDS A CODE OF PRACTICE

Due to the new challenges of Advanced Driver Assistance Systems (ADAS) - characterised by intensive Human-Machine-Interaction, environmental “interaction” and safety relevance - it is necessary to manage not only the problem of specification, implementation or realization errors and failures but also to prevent from reasonably foreseeable operational errors and reasonably foreseeable misuse.

The importance of integrating the Human Factors science has to be realized – Human Factors integration not only into the safety assessment process but also in the whole design and development process of ADAS.

Resulting from the Response 1 project the creation of a Code of Practice (CoP) for the development and validation of ADAS was proposed. 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.

RESPONSE 2 (http://response.adase2.net/) described market introduction scenarios analyzing the gap between technological possibilities and market introduction benefits and risks using typical scenario technique procedures. Enabling and disabling factors concerning market introduction have been identified and their interactions clarified. The in-principal technological possibilities of modern ADAS implying technical, human factors, and legal risks were outlined.

The deeper understanding of enabling and disabling factors was used for the definition of risk/benefit-assessment methodologies. This was done on a 'microscopic' perspective, where the risks for the whole Human-Machine-System had to be evaluated. Further a macro-economic approach for a combined risk-benefit analysis was developed.

These risk identification and assessment strategies were translated into a requirements definition for a Code of Practice for development and testing of ADAS. This included the analysis of already existing procedures and standards as well as the derivation of need for additional ADAS-specific procedures. Content, structure and formal aspects of a future CoP were defined.

The approach was to translate the legal terms 'reasonable safety' and 'duty of care' into requirements for a Code of Practice by

- analysing existing automotive and non-automotive regulations, standards, rules, technical papers, guidelines and other relevant provisions as well as
- deriving the relevant design, performance and process aspects/elements by selecting, adapting and completing these requirements to special ADAS needs.

Eventually, in a consensus formation process between project partners it was defined

- what is content and scope of the future CoP
- what are the formal requirements of the future CoP
- which are the steps towards a Code of Practice.

The RESPONSE 2 project has been the first move towards agreed validation procedures to be incorporated in a Code of Practice. Further methodological developments for validation (of system

safety and safety of usage) and the final definition of the CoP are part of the current ongoing project RESPONSE 3, that is a subproject of the integrated EU-project PReVENT.
All in all the voluntary agreement towards a Human Factors based Code of Practice shall

- give guidance in the user centred ADAS design process, helping to accelerate safe ADAS development on a “state of the art” level,
- promote positive public opinion concerning ADAS technology and its corresponding safety benefits as well as
- provide the basis for market introduction of ADAS and therewith a significant reduction of accident rates in Europe.

THE LEGAL SITUATION

A Three-Level-Classification of ADAS has been used within the legal analysis:

• Information and warning systems

Systems only providing information to the driver, as for example warning the driver that the vehicle is too close to another, do not physically take over the driver's role in any way. The driver remains in full control of the vehicle at all times with no physical driving functions assumed by the system. Instead, visible and audible information is provided to the driver in order to assist careful and proper driving. The driver is therefore responsible for exercising due care when driving.
However, there is a possibility that the information provided by the system may be incorrect or inaccurate. If this is the case, manufacturer or distributor liability should also be taken into consideration.

• Intervention systems which the driver may override at any time (“Overridable intervention systems”)

Potential driver liability concerning the overridable intervention system will very much depend on the individual case. Important factors will include inherent system limitations and driver perception of warnings and limitation consequences as well as reasonable driver behaviour like overriding the system in order to avoid critical traffic situations. System malfunction may also lead to liability of the manufacturer.

• Intervention systems which the driver cannot theoretically and/or practically (due to reaction time!) override at any time (“Non-overridable intervention systems).

If the driver is not able to override the system due to the ADAS design, liability due to inappropriate driver behaviour caused by the system arises, because such liability requires that the driver is not able to influence the system.

If the driver cannot override the driving support system manufacturer liability is more likely. If the driver cannot override the system, the manufacturer is confronted with a liability case.

With respect to liability issues, vehicle manufacturers have already had experience with the introduction of other systems, e. g. passive safety systems, which led to product liability claims regarding e.g. the deployment of airbags (too early, too late, inappropriately). Compared to ADAS, passive safety systems have been on the market for a long time, which means that the automotive industry has a lot of experience with these systems. What is more, these conventional systems do not take over driving tasks.

In the field of system safety:
In the field of system safety:
Today in general there is no risk scale for possible ADAS malfunctions which can be regarded acceptable by an OEM. Moreover, the OEM cannot refer to a guideline that shows the implications for the development and validation process. If a specific risk has been identified for a specific application, the OEM has no approved guideline to deal with this situation. In particular, all ADAS with interaction of driver and driver tasks are difficult to assess with respect to safe function in each and every driving situation.
In the field of system specification:
What are the characteristics of a least informed consumer that have to be taken into consideration by proving the robustness of the realised Human Machine Interaction-concept? What has to be considered a customer expectation and foreseeable misuse that will have a major impact on all possible liability claims? The possible misunderstanding of ADAS might also lead to problems for the OEM. Having the individual driver in the loop makes it very difficult to provide absolute design guidelines, i. e. it is not possible at the moment to define comparable guidelines on driver behaviour that would be valid for the whole variety of possible ADAS. There is no validated model which answers the question “What does the behaviour of a representative driver look like?” and an OEM can refer to. Many activities are conducted to investigate the impact of ADAS on traffic safety, for example evaluation of human factors, system design and accident research. However, there is still no guideline to assist the OEM in deciding what is an acceptable risk of a particular application.
In general, it became clear that conventional design standards are not an adequate answer to the complexity of advanced driver assistance systems. Therefore, guidelines must be established defining the duty of care necessary for the development of a reasonably safe product.
Regarding further development of ADAS (based on environmental sensors such as RADAR, LIDAR, video etc.), different safety issues for the development and validation of relevant systems become evident.

These considerations lead to a wider interpretation of the term “Acceptability” of ADAS. The main topics are:

TECHNICAL ACCEPTABILITY

Many of the ADAS which are currently under development, can be considered to be complex systems. The public opinion on complex technology and the corresponding safety expectations has been somehow changed to the direction of being sceptic. This might be linked to the daily experience of rebooting computer systems and radio news about computer systems crashes regulating e.g. traffic systems of big cities and other major events linked to technology problems. Considering the limits of current sensor technology, it is a difficult task to explain the limits in a way that customers can imagine an adequate model about the system, e.g. how will the RADAR or LIDAR find the relevant object (Figure 1).

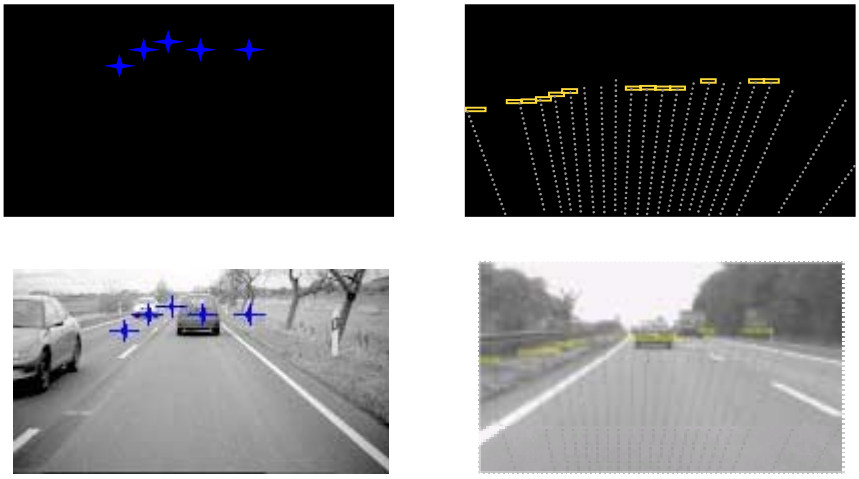

Figure 1: Environmental Sensor Capabilities

SAFETY OF USAGE

In particular systems continually assisting the primary driving task have to be tested. It cannot be expected that customers may understand the system functionality just by an explanation or by looking at the user manual. A good example to explain that issue is the experience about the ACC. This can be considered as being the first advanced driver assistance system that is designed to assist the driver continually. The development of the satisfaction index over time of using the ACC shows clearly that the driver has to learn how to use the system, and then will be happy to use it.

.

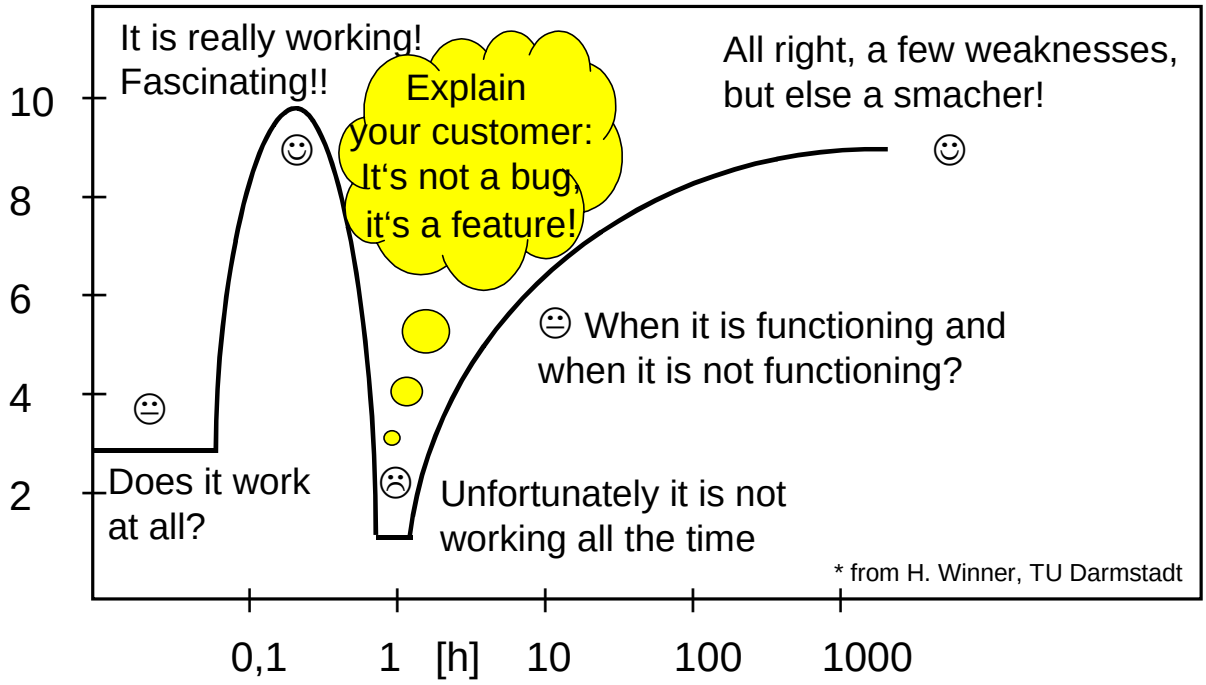

Figure 2: Satisfaction index (ACC) over time of usage

A principle to avoid critical situations of the ACC was the layout to give the driver always enough time for adequate reaction, when the system limits are reached. This will limit the possible range of the system, but will also assure that the driver will experience the limits often enough that he will stay in the loop. This is also linked to the next topic, the question of driver's responsibility.

DRIVING AT THE LIMITS - OVERRIDABILITY - RESPONSIBILITY?

What could be done about systems that will not allow the driver to react. That is certainly the case with systems that are designed for acting in emergency situations, where the driver clearly did not react to avoid critical situations by himself. What can be said about the legal point of view? Is there a shift of liability to the manufacturer? Is the manufacturer responsible, if there is a critical situation and the system does not intervene due to sensor limits? Is it possible to activate the brakes in order to warn the driver, because he is just about to cross a red traffic light? What if the system acts in a situation where no reason can be found and an accident occurs? All these questions are linked to the topics overridability and responsibility. The current status of responsibility can be explained as follows. The driver is responsible for his vehicle. This includes studying the information about the equipment of the vehicle. But manufacturer have to keep in mind the "rental car scenario". Nobody expects customer to study the complete user manual of the vehicle before starting. That means, that it should be made obvious to the customer, if a driver assistance system is mounted.

Regarding intervening systems, there is also a basic principle that the correct behaviour within traffic is protected. A good example would be a crossing assistant. To activate the brakes if the driver is just about to cross a red traffic light or a stopping sign, either for warning the driver to act by himself or at the end to perform the braking manoeuvre is in line with traffic rules. On the other hand it will certainly

not be accepted, if emergency manoeuvres will be performed without reason. But how to make the system design safe, knowing the limited reliability of sensor data?

SYSTEM RELIABILITY

Considering the reliability of technical systems, it is well-known that there is no 100% reliability. But is a 100% reliability required in order to market ADAS? The possible complexity of traffic situations shows clearly, that there is no sensor system that could cover all possible traffic situations that can occur. Therefore a good principle of designing intervening systems is not to try to cover all situations, where the system could help, but try to cover some situations, where redundancy or plausibility mechanisms can be used to make sure that the performed intervention will do a good job.

RISK AND SYSTEM SAFETY

Besides the principles of designing the positive functionality of systems, like it is described above, complex systems have also to cope with system failures, that are always to be considered with these systems. What are the requirements for the electric/electronic system design? This is a wide field and the answer will focus on a system safety process. As the automotive industry has already started to standardise such a safety process of complex electronic systems for safety applications on an ISO level, RESPONSE 3 will refer to these activities. Basically, it is important to consider the risk of malfunctions will be considered. Depending on the possible outcome of malfunctions in various traffic situations, safety requirements have to be derived. As there is no standard risk assessment at the moment available, the automotive industry is currently proposing a methodology for risk assessment. This proposal will consider risk being expressed by a combination of severity for a specific situation outcome, the probability to be in that situation and the controllability of the driver to avoid a critical outcome. RESPONSE 3 will focus on the issue of controllability to assist in finding possible methods to describe this controllability issue.

PUBLIC OPINION

Besides all the technical requirements, it is also important to consider the public opinion. Regarding the vehicle, we have a high emotional product. Everything in context with the vehicle must be perfect. This also applies to the high quality standards, which do exist in the automotive industry. Although there is a discussion on electronic reliability, we have to consider the high complexity of today’s vehicles. And if we consider the safety aspects, we can clearly show that we do not face problems with the safety of systems in the first place but with driver errors (Figure 3). And this shows on the other hand, that we should introduce advanced driver assistance systems that may help to reduce the negative consequences of driver errors.

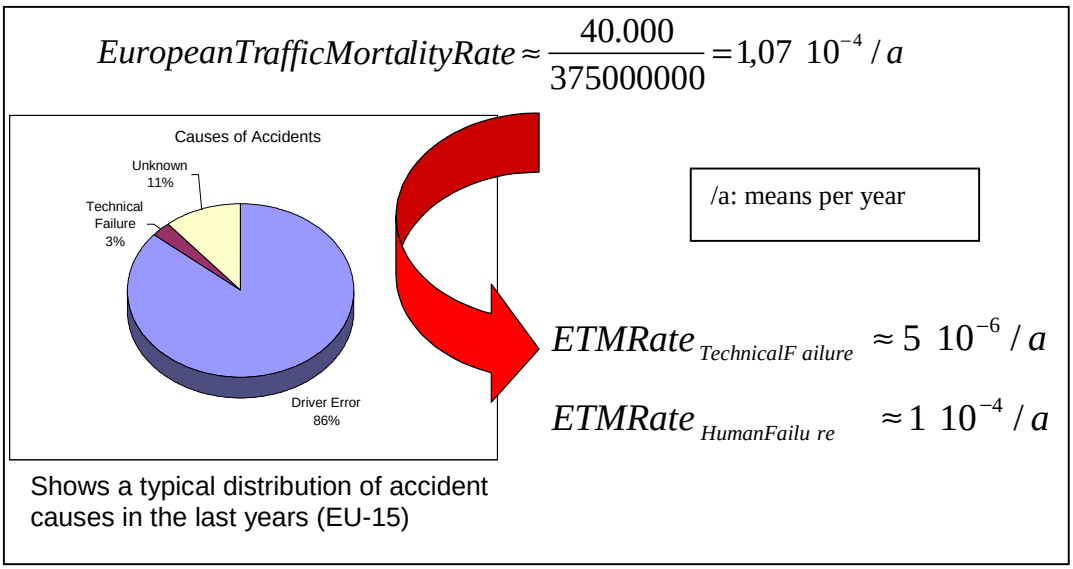

Figure 3: European Traffic Mortality Rate

This leads us to the discussion of naming the systems. People often translate the system name into a mental model. Therefore, the term safety system should not be used too often. In spite of the fact that we are aware that all of the planned ADAS have a safety aspect, it would be advisable not to call them safety systems, as the implication might be misleading for customers.

CODE OF PRACTICE

All these aspects shall be complied in the Code of Practice and subsequently be translated into a specification framework, helping to establish systems considering the different safety issues..

It will help to perform risk analysis and finding the possible methods to clarify these risks. In doing so the Code of Practice shall help to consider state of the art for ADAS with respect to safety issues. This will also help to argue the reasonable safety and duty of care within the development of ADAS, which is a crucial point with respect to liability risk.

ACKNOWLEDGEMENTS

The author wants to thank the partners of the RESPONSE 3 consortium, especially, Hans-Lothar Schollinski and Thomas Winkle from AUDI AG, Christoph Jung from BMW group and Markus Neumann from Volkswagen AG for constructive discussions. The RESPONSE 3 consortium wants to thank EC DG Information Society and Media for the active interest and support of the project.