2006-01-0600

Controllability of active steering system hazards: From standards to driving tests

Wolfgang Reinelt, Christian Lundquist
ZF Lenksysteme GmbH, Schwäbisch Gmünd, Germany

ABSTRACT

When developing new automotive systems a great deal of the development effort is devoted to ensure a sufficient functional safety of the system. A question that arises during early risk analyses of such a system is that of the controllability of possible system hazards. While this question is answered in early stages very often using worst-case risk graphs, the question comes back later in a much more precise way: in case of active steering systems component failures would produce a deviation between desired and actual road wheel position, the deviation can be measured in terms of amplitude and/or time. The central question is how much deviation can be controlled by the driver? Note, that there will always be a certain, even small, deviation between desired and actual road wheel position since the steering systems controller contains feedback control algorithms aiming at minimising the regulation error but not actually making it disappear totally.

The contribution reviews the different notions of controllability used in safety standards such as MISRA Guidelines, IEC61508 [1], DIN V 19250 [6] and DS 00-55 [3]. The role of the operator/driver as a potential source of failure or as a safety measure is touched as well. Goal of this paper is to bridge the gap between safety standards and driving tests, recently applied during development of electronically controlled steering systems.

INTRODUCTION AND MOTIVATION

When developing new electronic systems for automotive applications, quite a few questions arise with respect to their safety and safety case. These questions will differ dependent on the type of the system: on the one side, systems that control the vehicle in critical situations such as ABS, ESP are designed to stabilise the vehicle, the aspect of driver interaction is closely connected to the driver as one actor in a feedback loop. Note that this kind of action happens rarely (over vehicle lifetime), since vehicle stabilisation occurs rarely.

On the other side, for driver assistance systems that continuously support the driver and also give some comfort features like active steering systems the aspect of driver interaction can be discussed as the driver being the only actor in a feedback loop (since the assistance system typically consists of feed-forward functionality – at least on the system level that is notable to the driver). Note that these systems act continuously, in contrast to the above named stabilisations functions.

Either way, for both systems it has to be worked out that the nominal (intended) behaviour is well suited, in particular not hazardous, for potential drivers of the vehicle. Then one has to investigate the system's hazards that are, for this discussion, divided into the categories "sudden and unintended shutdown" and "unintended actuator functionality". Obviously, the first question is of particular interest when having a system at hand that cannot fall into a safe state, but note that this issue has to be investigated as well for fail safe systems. A discussion on the second category could be started by noting that, all systems will introduce a certain, even small, deviation between desired and actual behaviour since the systems actuator usually contains feedback control algorithms aiming at minimising regulation errors but not actually making them disappear totally (because of limited performance, noise, robustness etc) [15]. Expressing this imperfectness by control engineering terms such as steady state error, overshoot etc (or short: regulation error), the question the is: where is the border between a properly working controller, leaving the driver with some regulation error and an actuator functionality, that is hazardous for the system consisting of vehicle, driver and its environment. Obviously both events can be expressed by the same control engineering term "regulation error" as a matter of different numbers, the latter one called "unintended actuator functionality" in what follows. Note, that for a hazardous behaviour one does not necessarily need an unstable behaviour of the vehicle.

The scope of this contribution is to discuss

- different natures of unintended actuator functionalities for comfort (i.e. feed-forward) and stability (i.e. feedback) systems,
- the role of the driver as the outer feedback loop in particular,
- guidance given by safety standards on these questions.

The outline of the paper follows the opposite direction, finishing with the link to driving experiments. Another question, somewhat related to this complex topic is not touched here: since nowadays vehicles often carry some ten electronic chassis systems that modify the dynamics one way or the other, one system could make up for failures of a second. If so, how, and how can this be addressed during design phase. This contribution argues from the point of view of a system within the vehicle.

Finally, a link to the EU research programme RESPONSE shall be made, which focuses on advanced driver assistance systems such as automatic cruise control (ACC), heading control etc. While the first part of the project [17] focused on how the driver copes with nominal behaviour of these systems, the second part raised the question of how to introduce the driver aspect [18]. In the next step (cf. http://response.adase2.net) these questions shall be addressed. The focus of this contribution is more on unintended behaviour of systems, and active steering systems will be the system in the focus of the work, serving as an example.

REVIEW OF SAFETY STANDARDS

Generic safety standards such as IEC 61508 [1] give some guidelines how to identify hazards, derive integrity measures from this analysis, verify this and integrate this into the development process. Since this standard is not an automotive one, it has to be applied to this application sector (which is currently under investigation).

On the system level, the so-called **risk analysis** maps system hazards to accidents (on vehicle level) and comes quite early in every safety related development process [9,10]. Procedures for doing this are described in [1, part 5] or [6]. As pointed out above, here the supplier of one system needs assistance by the vehicle manufacturer in order to assess the system's implications on a vehicle level (together with the other systems that are onboard).

Based on the discussion above on “rarely” used stabilisation functions and “continuously” used assistance or comfort systems a remark can be made on the notions of “low demand mode of operation” and “high demand (continuous) mode of operation” as established in [1]. Even rarely used stabilisation functions (and the respective parts of the state machine and driving situation evaluation attached to this functionality) are in a high demand (continuous) mode of operation in the very sense of [1], since they are activated all the time (but usually not acting on the system). The fact that theses systems are *correctly not doing anything* most of the (vehicle-)time makes them systems of continuous mode of operation.

CONTROLLABILITY

A particular part of the risk analysis is the notion of “controllability”. One definition of the so-called controllability categories according to [8] and [7] respectively is:

Uncontrollable failures whose effects are not controllable by the vehicle occupants.

Difficult to Control failures whose effects are not normally controllable by the vehicle occupants but could, under favourable circumstances, be influenced by a mature human response.

Debilitating failures whose effects are usually controllable by a sensible human response

Distracting failures which produce operational limitations, but a normal human response will limit the outcome to no worse than minor.

A well known issue is how to distinguish between the three types of human responses involved (mature and favourable circumstance, sensible and normal). To assess the controllability of a hazard has to be done in very early design stages in order to properly design a safety concept that is appropriate to the system. Since the above named categories are not well-measurable, judgements may vary from “difficult” to “distracting” for the same experimental setup.

This dilemma has already been acknowledged by generic safety standards:

... Capturing the important human factors aspect is still an active research area [3, p.8].

And for the automotive domain in particular:

In particular, the relationship between controllability and severity could be tested out by means of experiments in a driving simulator, which would enable realistic testing of driver behaviour, and its results, in the presence of hazards. Additionally, further investigation is needed into how the risk model can be affected by human factors, some of which could be addressed by experiments using a driving simulator. [16]

Based on the discussion so far, the question arises whether there are controllability categories/rating that are better suited in terms of applicability, measurability and broad acceptance. We will discuss this question during the course of the contribution.

ROLE OF THE DRIVER

The last paragraph implicitly poses the question what the role of the driver is. [1, part 5, p.23] puts the driver somewhere between the system (called EUC, Equipment Under Control) and the safety measures:

The general model assumes that

- *there is an EUC and an EUC control system;*
- *there are associated human factor issues;*
- *the safety protective features comprise*
    - *external risk reduction facilities,*
    - *E/E/PE safety-related systems,*
    - *other technology safety-related systems.*

As a clarification, the definition of risk in the same standard associates even a residual risk for the driver:

Residual risk [actual risk]: in the context of this standard, the residual risk is that remaining for the specified hazardous events for the EUC, the EUC control system, human factor issues but with the addition of external risk reduction facilities, E/E/PE safety-related systems and other technology safety-related systems [1, part 4, sec.3.1.7]

A similar formulation appears when talking about frequency of risk, cf. [1, part 5, p.37].

Consequence from analysis of [1] with respect to human factors: Human beings are considered as part of a safety related system but not part of the protective features. Human factor requirements as such are not considered in detail in the standard. Other recent works [21] draw conclusions in similar directions.

THE DRIVER CLOSES THE LOOP

The discussion so far has been rather general on arbitrary vehicle systems. From now on the focus will be on electronic steering systems such as electronic power steering [14], steer by wire [13] and active front steering [11]. The discussion so far revealed that much depends on the drivers reaction being inside the system during a hazardous event.

In order to be able to formulate the scope of the investigations to be done in this direction we will apply a systematic method, namely Hazard and Operability Studies HAZOP [5] to different functionalities of the active steering system: the variable steering ratio that varies the ratio between hand steering wheel and road wheel, as for instance described in [11] and vehicle stabilisation, e.g. yaw rate control as for example described in [12]. Note that both functionalities use the same actuator, namely the electronically controlled superposition of an angle to the hand steering wheel angle, but realise different functionalities. Variable steering ration falls into the category of assistance (feed-forward) functions, while yaw rate control clearly is a stabilisation (feedback) function. The goal of this section is to highlight the different nature of these two functions with particular respect to unintended actuator functionality and to quantify this.

HAZOP studies aim at, among other goals, finding out how a change in certain attribute of an entity is reflected at the boundary of the entity. Since this study is aiming at early design stages of the system, when not much deeper insight into the system is present, guidewords are provided to systematically carry out the study. The generic question posed is: What if [entity] [attribute] is [guideword]? Typical guidewords used are: no, more, less, as well as, part of, reverse, other than, early, late, before and after [5, part 2]. Since this discussion is about highlighting the differences between the systems and the driver behaviour because of them, the following analysis is exemplary rather than complete.

In the first step, we intend to work out the difference between feed forward and feedback systems on vehicle level, when hazards occur. The entities under investigation therefore are *variable steering ratio* and *stabilisation*; the attributes are, in both cases, *command*. Table 1 describes the vehicle behaviour for selected guidewords (interpretation in brackets).

Table 1: Early design stage HAZOP 1 for variable steering ratio (VSR) and yaw rate control (YRC) according to [5].

WHAT IF…	**…Variable Steering Ratio command IS...**	**…Stabilisation command IS…**
…no? [zero angle added]	Falls back to mechanical steering. Step depends on VSR layout. Depends on driving situation.	Same as for VSR when no command applied. Otherwise YRC not finished correctly, vehicle not stabilised.
…more? [amplitude than correct]	Steering too direct. Depends on driving situation and amplitude.	Vehicle destabilised or not stabilised correctly, depends on amplitude.
…less? [amplitude than correct, but same direction]	Steering too indirect. Depends on driving situation and amplitude.	YRC not carried correctly, vehicle not stabilised. Depends on amplitude.
…reverse? [opposite direction]	Vehicle steers in wrong direction.	Vehicle not stabilised.
…late? [in time]	Steering with time delay, feels awkward. Depends on delay.	YRC too late, vehicle not stabilised.

Quite a few conclusions can be drawn from the HAZOP shown in Table 1. In the "no" case, there seems to be a design implication on the VSR function, but not for the YRC. While for the VSR functions all comments include driving situation and amplitude, only amplitude is mentioned in the YRC case. This is due to the fact that the YRC commands an action (unequal to zero) when an unstable driving situation occurs. In contrast, VSR function is always active and consequences of the hazard depend on the very situation as well (city traffic, motorway etc).

The first HAZOP was focusing on the systems as such, minimising –if possible- feedback by the driver. A second has been carried out to detail the driver's reaction in these situations. Hence, the entity under investigation is the *driver reaction* and the attributes are *too much VSR command* and *too much YRC command* (reflecting the guideword "more" situation in the first HAZOP) and the goal is to detail the result described in Table 1. The result is given in Table 2, again not aiming at completeness.

Table 2: Early design stage HAZOP 2 for driver reactions to variable steering ratio (VSR) and yaw rate control (YRC) hazards according to [5].

WHAT IF driver reaction…	**…to too much Variable Steering Ratio command IS...**	**… to too much Stabilisation command IS…**
…no? [freezes hand wheel angle]	Steering too direct. Depends on driving situation and amplitude.	Vehicle destabilised or not stabilised correctly, depends on amplitude.
…fast? [almost releases hand wheel angle]	No vehicle reaction, since hazard evolves towards hand wheel.	Vehicle destabilised or not stabilised correctly, depends on amplitude.
…more? [turns hand wheel in same direction as hazard]	Makes steering even more direct. Depends on driving situation and amplitude.	Vehicle destabilised or not stabilised correctly, depends on amplitude.
…reverse? [turns hand wheel in opposite direction as hazard]	May correct steering ratio. Depends on driving situation and amplitude.	May stabilise vehicle.

When browsing the result of the second HAZOP, it does not seem possible to detail the results in the YRC case compared to the first one. In the case of "reverse" reaction one might ask why the driver should be able to stabilise the vehicle now when he was not able to stabilise it when the YRC occurred (which would have prevented it at all). On the other hand, the VSR results also reflect particular properties of the active front steering system, i.e. to allow the hazard to propagate towards the hand wheel (which would not be the case with a steer by wire system).

Assuming that one intends to develop as system that display the VSR function only, HAZOP 1 gives advice to prevent the “reverse” case by the safety concept and investigate the other ones in terms of allowed failures, or regulations errors (see above), more carefully. However, when comparing the VSR results to the YRC results it becomes clear that the results obtained here cannot be applied to the YRC case in a one-to-one fashion.

For the VSR function, even this simple HAZOP gives us pretty accurate questions to answer for design of the safety measures:

- What should mechanical and variable ratio layout look like (case: “no” in HAZOP 1)?
- How to map the terms “more” and “less” (HAZOP 1), onto the regulation error (amplitude, speed)?
- How to map the terms “late” (HAZOP 1) onto the regulation error (timing issues, delays)?
- Do we have to react differently in different driving situations or is there a reasonable worst case assumption?
- Should we consider message encouraging the driver to release the hand wheel (case “fast” in HAZOP 2)?
- What is the variation in the driver behaviour (case “reverse” in HAZOP 2)?

We will briefly outline how to answer these questions in the next section.

ASSESSING CONTROLLABILITY USING DRIVING TESTS

After having bridged the gap between standards and driving experiments by having worked out how to derive particular questions to assess controllability, we will now give a hint to recent works [19, 20] that have been successfully carried out during the development of active front steering systems. As mentioned above, dealing with hazards of the variable steering ratio is somewhat easier and we concentrate on this question.

Instead of the conventional controllability categories as in [6, 7], a modification of the modified Cooper-Harper-Rating Scale has been used in [19, 20]. This scale is well known form the aircraft domain and is based on a decision tree that has been modified for automotive applications. It ends up in eleven (including the “not perceived” category) ratings which are roughly defined like these:

- rating 10 (vehicle not controllable)
- rating 9-7 (dangerous)
- rating 6-4 (annoyance)
- rating 3-1 (noticeable)

Finally, rating 0 (not perceived) has to be added to complete the picture. Note that the main categories are sub-divided in three categories each (all of them defined verbally), which makes apparently easier to apply for the persons involved in driving tests. Note also, that decision-tree type of questions as known from the Cooper Harper scale are not present as well. For details, we refer to [19, 20].

The next question arising then is how to choose the relevant failure scenarios, which is straightforward given the list of questions derived using the HAZOPs in the last chapter. The task of the driving experiment programme is then to carefully derive target numbers that are statistically reliable, see [19].

CONCLUSIONS

The notion of controllability as given in well established safety standards has been discussed. A systematic approach, namely HAZOP, has been used to detail the questions that are typically open after a risk analysis. This has also been highlighted by a practical example based on an active front steering system. Recent works have been linked to this analysis stage. In these works, an alternative controllability scheme was used.

ACKNOWLEDGEMENTS

Valuable discussions with Alexandra Neukum during the course of this paper and the related works are gratefully acknowledged as well as the input given by the unknown reviewers.

REFERENCES

1. IEC 61508: Functional Safety of E/E/PES Systems. International Electrotechnical Commission IEC, Geneve, Switzerland. Dec 1998.
2. IEC 60300: Dependability management. Part 3: Application guide. Section 8: human reliability. International Standard. International Electrotechnical Commission IEC. Geneve, Switzerland. 1995
3. DS 00-55 Requirements for Safety Related Software in Defence Equipment. DEFSTAN. UK Ministry of Defence. Defence Procurement Agency, Glasgow, UK.

4. DS 00-56 Safety Management Requirements for Defence Systems. DEFSTAN. UK Ministry of Defence. Defence Procurement Agency, Glasgow, UK.
5. DS 00-58 Hazop Studies on Systems Containing Programmable Electronics. DEFSTAN. UK Ministry of Defence. Defence Procurement Agency, Glasgow, UK. May 2000.
6. DIN V 19250 Vornorm: Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen. DIN Deutsches Institut für Normung e.V., May 1994.
7. MISRA - Motor Industry Software Reliability Association: Development Guidelines for Vehicle Based Software. MIRA, UK. November 1994
8. P Jesty, KM Hobley, RJ Evans, I Kendall. Safety Analysis of Vehicle-Based Systems. Proc. 8th Safety-critical Systems Symposium. Jan. 2000.
9. S Amberkar, JG D'Ambrosio, BT Murray, J Wysocki, BJ Czerny: A System-Safety Process For By-Wire Automotive Systems. SAE technical paper 2000-01-1056. SAE World Congress, Detroit, MI, USA. Mar 2000.
10. W Reinelt, A Krautstrunk. Safety related development process for electronic steering systems. SAE technical paper 2005-01-0780. SAE World Congress. Detroit, MI, USA, April 2005.
11. W Reinelt, W Klier, G Reimann, W Schuster, R Großheim: Active Front Steering for passenger cars (part 2): Safety and Functionality. SAE Technical Paper 2004-01-1101. SAE World Congress. Detroit, MI, USA, Mar 2004.
12. C Lundquist, W Reinelt, S Malinen: Vehicle dynamics control using active steering systems. SAE Technical Paper Offer 06AC-28. SAE World Congress. Detroit, MI, USA, Apr 2006
13. W Harter, W Pfeiffer, P Dominke, G Ruck, P Blessing Future Electrical Steering Systems: Realizations with Safety Requirements. SAE Technical Paper 2000-01-0822. SAE World Congress, Detroit, MI, USA, Mar 2000.
14. H Köhnle: The Electromechanical Power Steering Systems of ZF Lenksysteme - Components, Function and Application. Paper F2004F293. FISITA World Automotive Congress, Barcelona, Spain. May 2004.
15. KJ Åstrom, B Wittenmark. Computer Controlled Systems: Theory and Design, 3rd ed., Prentice Hall, 1997
16. RJ Evans and JD Moffett. Derivation of Safety Targets for Random Failures of Programmable Vehicle based systems. Proc. SAFECOMP, Rotterdam, NL. Oct. 2000
17. Commission of the European Community, Telematics Applications Programme - Sector Transport. Response 1: Advanced Driver Assistent Systems: Final report. Project 4022, Deliverable D2.2. September 2001.
18. Commission of the European Community, Telematics Applications Programme - Sector Transport. Response 2: Advanced Driver Assistent Systems: Steps towards a Code of Practice for the development and evaluation of advanced driver assistances systems Deliverable D3, Version 2.0. 29 July 2004.
19. A Neukum, HP Krüger. Driver reactions to steering system failures – methodology and criteria for evaluation (in German). VDI Tagung „Reifen-Fahrwerk-Fahrbahn“.VDI-Report 1791, pp. 297-218. October 2003.
20. A Neukum, W Reinelt. Integration des Fahrers bei der Bewertung der Ausfallsicherheit aktiver Lenksysteme (in German). VDI Tagung „ Der Fahrer im 21. Jahrhundert“. November 2005.
21. F Redmill. The significance to risk analysis of risks posed by humans. J of System Safety, Vol. 41, No. 5, Sep-Oct 2005.

CONTACT

Dr. Wolfgang Reinelt, Christian Lundquist. ZF Lenksysteme GmbH, EEMF Active Front Steering - Safety, Richard-Bullinger Straße. 77, 73527 Schwäbisch Gmünd, Germany, Phone: +49-7171-313110, Wolfgang.Reinelt@ZF-Lenksysteme.com