Transportation Research Part F 21 (2013) 269–277

Contents lists available at ScienceDirect

Transportation Research Part F

journal homepage: www.elsevier.com/locate/trf

Using an integrated simulation environment for the risk based design of advanced driver assistance systems

Julian Schindler [a,*], Mirella Cassani [b]

[a] German Aerospace Center (DLR), Institute of Transportation Systems, Lilienthalplatz 7, D-38108 Braunschweig, Germany
[b] Kite Solutions SRL, Via Labiena, 93, I-21014 Laveno-Mombello, Varese, Italy

ARTICLE INFO

Keywords:
Simulation platform
DOMINION
Advanced driver assistance systems
Risk based design
Event tree
ISi-PADAS

ABSTRACT

When designing new Advanced Driver Assistance Systems (ADAS), the existing guidelines like the RESPONSE 3 Code of Practice imply intense testing of the system prior series production. Within the EU-FP7-Project ISi-PADAS a new methodology of risk based design has been established which includes an integrated simulation platform. This integration enables intense testing of new prototypes in an accelerated way and therefore enhances the design process while directly combining the simulation results with a risk matrix.

This paper describes the new methodology while focussing on the software framework and the procedure of risk assessment in detail. It shows the general approach as well as the appropriate steps taken for an ADAS prototype developed in the context of ISi-PADAS.

1. Introduction

Advanced Driver Assistance Systems (ADAS) are getting more and more complex. This is not only true for the system itself and sometimes for the involved HMI, but also for the design process of the system. The designer of the system has to merge different requirements of the ADAS, e.g. requirements in the field of functionality, usability, controllability, liability or legislation. In order to handle the complexity, different standards like ISO 26262 and guidelines like the RESPONSE 3 Code of Practice (RESPONSE 3 development group, 2006) have been established. In any case, the intense testing of the developed system is a key requirement of any guideline in order to assess possible risks of a system failure or mishandling by the user. In particular, this is getting more and more difficult and expensive when the complexity rises, as a higher number of situations have to be tested.

One focus of the EU-FP7 project ISi-PADAS was the development of a new Risk Based Design Methodology (RBDM) which includes a new way of risk assessment in ADAS design. In order to make the RBDM usable for a designer, a software framework has been established including a Graphical User Interface (GUI) for keeping track on the current stage of the development in terms of risk. The software framework also includes a flexible simulation platform, the Joint Driver-Vehicle-Environment simulation platform (JDVE). The JDVE makes it possible to perform high-speed scalable ADAS tests, e.g. for application in the Code of Practice, from desktop simulation to application in real test vehicles, from real time experiments to driver-model-driven accelerated-time-testing.

Furthermore, within the project, a new Partially Autonomous Driver Assistance System (PADAS) has been developed, consisting of an advanced Forward Collision Warning and an advanced Adaptive Cruise Control system, which takes the driver step-by-step out of the loop when the criticality of a situation rises (Tango, Alonso, Vega, Aras, & Pietquin, 2011).

* Corresponding author. Tel.: +49 5312953510.
E-mail addresses: julian.schindler@dlr.de (J. Schindler), mirella.cassani@kitesolutions.it (M. Cassani).

1369-8478/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.trf.2013.09.018

The design of this PADAS was driven by the RBDM which will be briefly described at first. Then, the integrated utilisation of the JDVE as a fundamental part of the design process is shown, focussing on the fast and easy evaluation of risk probabilities.

2. Risk based design methodology

2.1. Risk based design methodology implementation

A Risk Based Design Methodology offers the opportunity to implement a highly effective design process with reference to the safety analysis. In the case of human error evaluation in the automotive domain, the RBDM implies the development of a Driver-Vehicle-Environment simulation platform that enables to consider possible driving scenarios including different interactions between driver and vehicle.

As a starting point of a standard RBDM approach, the designer of an ADAS wants to know how much the proposed ADAS benefits the possible risks in occurring situations. Therefore, the designer has to define these situations in terms of drive scenarios. Occurrences or sequences of events are studied by combining possible human errors and/or vehicle faults, their probabilities of occurrence and interactions in order to evaluate the consequences and overall probabilities. This risk assessment leads to the evaluation of possible safety measures when the risks are considered to be unacceptable (Fig. 1).

In assessing the risk of human errors, it is of paramount importance to consider the interactions between Driver, Vehicle and Environment. These are essentially of dynamic nature and therefore the scenarios that are to be analysed must include time variability of interactions. However, the dynamic processes are particularly difficult to analyse in risk methods, due to the intrinsic complexity of dynamic reliability as well as to the scarcity of data available to account for time changing environments. On the other hand, as the automotive environment is particularly affected by rapid dynamic changes, some consideration needs to be given to this essential. For this reason, a quasi-static approach has been adopted for the implementation of human errors in the proposed risk based design methodology.

In particular, the following steps are envisaged by a designer following the RBDM:

(1) Definition of a *Scenario*. In general, a scenario can be defined as the set of elements that represent the situation, including a dynamic evolution of environment and vehicle, independent of driver behaviour. In case of the example PADAS design it has been chosen to use an urban scenario with a suddenly stopping lead car.
(2) Definition of an *Initiating Event*. In general, an event is characterised by a change in the conditions of the system which modifies the system state, characteristics or performances. In terms of human factors, an event can be defined as an action which changes the system state, characteristics or performances. An Initiating Event is a special kind of event that triggers a sequence. Other events are simply consequential or explicable follow-ups of the Initiating Event, in a logical or temporal manner. In case of the example PADAS design the point in time where the lead car starts to brake has been chosen as Initiating Event.

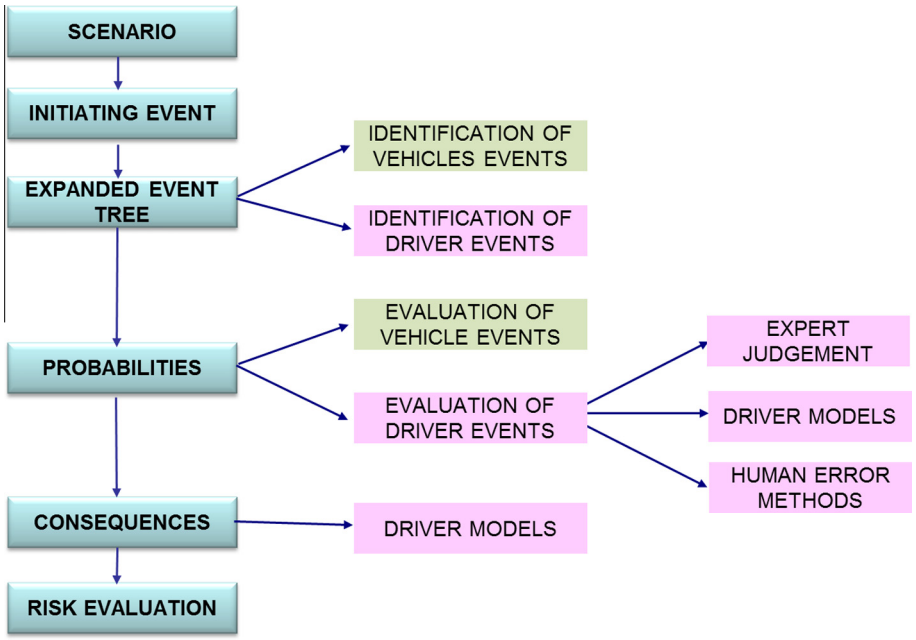

Fig. 1. Flow chart of a risk based design methodology.