Available online at www.sciencedirect.com
ScienceDirect
Safety Science 45 (2007) 231–251
SAFETY SCIENCE
www.elsevier.com/locate/ssci

Safety learning and imagination versus safety bureaucracy in design of the traffic sector

Ellen Jagtman *, Andrew Hale

Safety Science Group, Delft University of Technology, Postbus 5015, 2600 GA Delft, Netherlands

Abstract

This paper deals with the processes of evaluating the possible safety effects of measures introduced either in the road infrastructure or in the electronic and information systems in cars. It uses speed control measures (speed bumps and the Intelligent Speed Adapter [ISA]) as cases to describe and test the approach. The paper describes and critically assesses the current methods of ex-ante design and evaluation of such measures, which relies on design to national and international standards. It criticises this approach, particularly from the point of view of predicting unexpected and unwanted effects of the new designs. It proposes an adapted form of hazard and operability study as a tool to help predict these effects and validates this approach against the experiences of a field study of an ISA instrument.

Keywords: HAZOP; Design standards; Intelligent Speed Adapter

1. Introduction: evaluating road traffic information technology

The use of information and communication technology in traffic is increasing. Advanced Driver Assistance Systems (ADAS) have been developed to support the driver by providing information or even to temporarily take over part of the driving task. For instance systems for lane keeping in trucks and for distance keeping for cars on motorways have already been introduced to the market. ADAS for other driving tasks are expected. These future ADAS will support many tasks at the same time. Such an integrated system

* Corresponding author.
E-mail addresses: h.m.jagtman@tudelft.nl (E. Jagtman), a.r.hale@tudelft.nl (A. Hale).

0925-7535/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ssci.2006.08.009

may for example include route guidance, distance and speed keeping. Although car manufacturers sell these systems as 'comfort extensions' the applications have the potential to influence the safety of the user and/or the safety of the road traffic system as a whole.

Up to now safety assessments of ADAS mostly occur by testing a more or less standard set of possible safety issues in various simulations and field trials, based on checklists and guidelines. The emphasis in (larger) field tests for ADAS has focused on acceptance of the specific system under study and on predictable safety effects (Jagtman et al., 2001). These mainly consist of testing for known technical problems, for the usability of the system and for effects on safety resulting from the desired (normative, designed) operation of the system. The criteria available in all current evaluation frameworks have mainly been derived from this intended operation process (see, Carsten, 1993; Morello, 1995; European Transport Safety Council, 2001). However effects on safety can also result from all kinds of deviations from the process that is intended. When we are dealing with new technologies, not yet introduced to the market, the range of safety effects is particularly uncertain. Apart from unexpected modes in which the ADAS may operate and all sorts of user violations, the system settings may generate deviations. The driver may use a device in a way that does not comply with the limited conditions in which it should be used according to the designed intended process. For example, distance-keeping systems, which are extensions of the conventional cruise control, are, according to the instruction manuals, designed for motorway environments in which a steady speed can be driven for a prolonged period. However one can switch-on such ADAS at any speed from 30 or 40 km/h or faster (see e.g., BMW, 2002; Mercedes Benz, undated; Nissan, undated), which could be in a congested traffic situation without a steady speed. A safety assessment should identify and incorporate all such plausible scenarios resulting not only from the intended operation processes, but also from deviations from them.

1.1. Strategies for evaluation

For designers and policy makers an assessment of safety effects in the design stage may follow two extreme strategies: proactive or bureaucratic.

- The proactive strategy seeks to learn throughout the design process of an ADAS about all plausible safety problems and to decide upon preventing or controlling these problems while the system is still under design. The responsibility to try to cover all plausible scenarios is assigned in this strategy to the designer, while policy makers check if this assessment has been done, preferably in the ongoing design process. This is a closed loop, feedback process, relying on the designer providing the input and creativity for the proposed solutions. It is a regime found typically in the safety cases for major hazard sites (European Commission, 1997).
- In the bureaucratic strategy designers make use of standards or guidelines, which are imposed in some way on the manufacturer/designer and which they must follow as a prerequisite for the design. This is a feed-forward system, where the standard setter provides the main input and requirement for solutions and checks at the end the detailed compliance. The car industry in Europe is exempt from the European machine directive (European Commission, 1991; CEN, 1992). Instead makes use of a type approval procedure in which an independent approval authority evaluates whether a type of vehicle, a component or a separate technical unit satisfies the relevant technical requirements