

Development of a safety assessment process for in-vehicle information systems

David D Ward^{*1}, Mark Fowkes¹, Peter H Jesty²

1. MIRA Ltd, Nuneaton, CV10 0TU, UK, + 44 24 7635 5430/5443, david.ward/mark.fowkes@mira.co.uk

2. PJCL, Warwick Lodge, Towton, LS24 9PB, UK, + 44 1937 833640, phj@peterjesty.com

ABSTRACT

This paper presents a technique that has been developed for assessing potential safety implications of the way that information is presented to a driver by an in-vehicle information system (IVIS). This technique, developed during the European HASTE project, uses analysis techniques alone and complements the other parts of the HASTE project that have used simulators and field trials to assess the safety impacts of such systems on driving. The technique is based on the HAZOP (hazard and operability) approach that has been successfully applied to safety analysis in a number of different domains. As with any use of HAZOP, interpretation and application is required (particularly for the guidewords) and an overview of how this is achieved is presented. The technique has been trialled by applying it to two example IVIS, and the results are presented. A comparison of these results with an existing checklist based approach shows that the new approach complements existing processes and is a useful additional assessment method to investigate the potential risks of a proposed IVIS HMI at an early stage in product development.

KEYWORDS

Safety assessment, preliminary safety analysis, human-machine interface, HMI, HAZOP, in-vehicle information systems, IVIS

INTRODUCTION

Over the last decade many technologies and systems designed to deliver an increasing amount of information about traffic conditions and other travel related factors to road vehicle drivers have been developed. Some of these systems are now emerging into products for the mass market. Such systems may be of benefit to drivers and support safer and more efficient journeys through increasingly complex and congested road conditions.

However the additional information provided by such systems has to be integrated by the driver into the already demanding task of driving. If such information is difficult for the driver to acquire, control or understand then there may be a negative impact on driving performance that

outweighs the benefits. In light of such concerns it has to be considered how any such negative impacts of these future systems, and by inference driving performance, can be minimized.

The aim of the EC HASTE (Human Machine Interface And the Safety of Traffic in Europe) project was to develop methods and guidelines for the assessment of In-Vehicle Information Systems (IVIS). In this context an IVIS is defined in accordance with the European Statement of Principles on HMI [1] as:

An IVIS (In-Vehicle Information System) is an In-vehicle Information and Communication System designed for use by the driver while driving.

In this paper a process is presented that has been developed for assessing potential safety implications of the way that information is presented to a driver by an IVIS using analysis techniques alone. This work complements the other parts of the HASTE project that have used simulators and field trials to assess the safety impacts of such systems on driving.

SCOPE

Many attempts have been made to provide manufacturers and testing authorities with guidelines and/or assessment methods to assess the likely impacts of IVIS on the driving task. Most of these approaches involve the use of some form of checklist that facilitates an audit of the design of an IVIS HMI. Such checklists potentially provide a tool that enables the identification of likely problems, but they do not attempt to quantify safety problems. There is therefore still a requirement for the development of a valid, reliable and efficient tool that will aid manufacturers and testing authorities in their safety evaluation of IVIS before systems are put into production.

Typical product development lifecycles show a sequential progression from initial concepts to mock-ups, engineering prototypes and eventual manufacture ready approved design. They indicate that in an industrial context design processes have to operate within a complex procedure that includes incremental development of systems and integration, to refine a design from an “idea” to a finally accepted defined product.

If no relevant HMI evaluations are carried out within this process then it is possible that HMI operability risks may become built-in to the design and be difficult or impossible to remedy close to manufacture. It is therefore relevant to consider how such a risk assessment or operability study can be scheduled and delivered within a development process.

The HASTE project has therefore developed such a procedure (called a Driver Operability Procedure – DOP) and has considered how it can be used within the design and development process for an IVIS. Figure 1 shows the scope of the area of applicability for the DOP process. It identifies that very early concept stages may not contain enough detail of HMI design to enable a meaningful analysis to take place. At this initial stage, concept development should take appropriate note of published design guidelines, standards and regulations to guide development. When a more detailed concept specification has been developed prior to prototype development then a DOP can be applied. In parallel, a preliminary safety analysis approach can

be used to identify issues relating to functional system safety. Once prototypes of the system are available, then established experimental protocols can be used to evaluate HMI performance. Future legislative requirements (e.g. Primary NCAP in Europe) may also require HMI performance to be evaluated as part of the regulatory approval of vehicles.

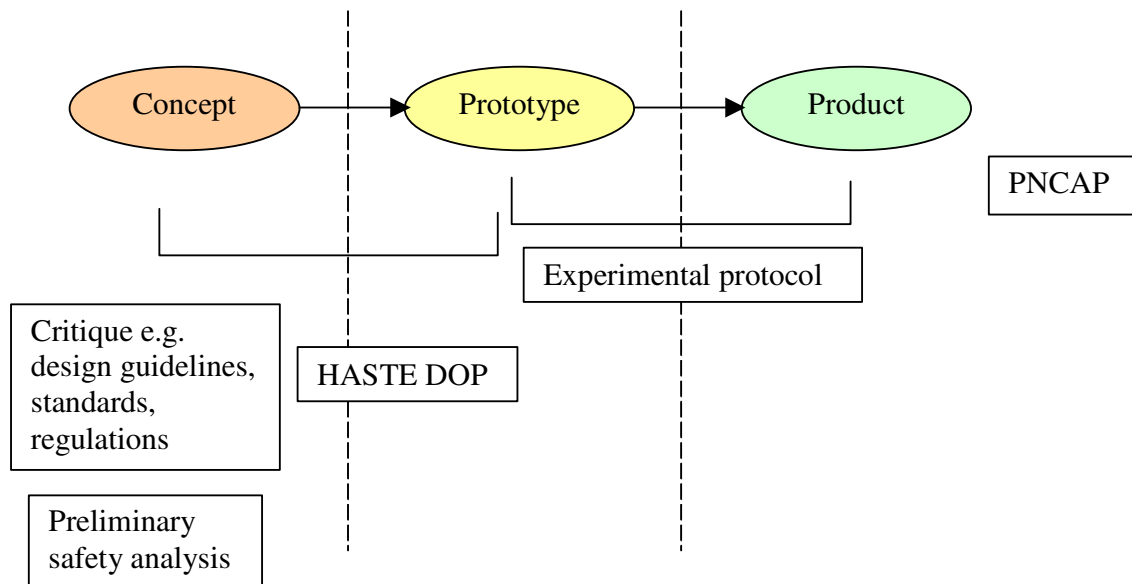


Figure 1: Scope of HASTE Driver Operability Procedure

DRIVER OPERABILITY PROCEDURE

A number of possible assessment methods were considered that could provide a useful basis for an assessment technique for human operability issues. After considering various candidates, the Hazard and Operability Study (HAZOP) was selected as a suitable basic technique. HAZOP was originally developed in the chemical engineering industry, but has been subsequently applied to a wide variety of systems including human-centric tasks [2]. More recently, it has been applied to analyse the design of traffic systems [3]. HAZOP requires at least an outline design, and is typically applied to the flow of information or data between the elements of a system. This therefore makes it an ideal technique for examining issues at the human-machine interface.

HAZOP asks structured questions, based on guidewords that describe the deviation of a system from the design intent. Each question is then used to explore the causes of the particular deviation and the consequences. The scope and extent of this exploration will depend on the application and the scope of the analysis.

There are 11 generic HAZOP guidewords that are applicable to all analyses in all domains, though it is often necessary to interpret the generic words appropriately for a given flow of information.

In applying a HAZOP-based assessment process, guidance was developed on how to produce a model of the IVIS that is suitable for the HAZOP technique, and then on how the generic guidewords might be interpreted for the human-machine interaction. For example, consider how the generic guideword “No”, meaning that no part of the design intent is achieved, could be applied to information that has to appear on a visual display that is part of an IVIS. In this case “No” could mean either that the information does not appear on the display, or that the human does not acquire the information from the display.

It should be noted that since this analysis is about HMI issues only, malfunctions of the equipment are ignored, though they should be included as part of a functional system hazard analysis. The concerns of a DOP are the consequences of a driver using the full functioning IVIS as it is currently being designed, and whether this could have an effect on the primary driving task. Typically this will be due to a need to concentrate on interpreting the output of the IVIS, to the detriment of the need to concentrate on what is happening to the vehicle and/or on the road.

Modelling the IVIS

A HAZOP study is performed on a design of the system under investigation. IVIS's are Information and Communication Technology (ICT) systems and, whilst there are a number of possible design representations, or models, that could be used by the Software Engineers, not all of them are a suitable target for a HAZOP study. A suitable model needs to show the following features:

- The key phases of the operation of the IVIS, including:
- Those interactions that a driver can perform when the vehicle is parked;
- Those interactions that a driver can/needs to perform when the vehicle is moving.
- The basic operation of the IVIS.

Most IVIS react to events as and when they occur. Thus a possible suitable model is a state machine. An example is shown in Figure 2, which is a simplified state machine representation of a portable in-car navigation device based on a PDA. Since the user is often able to enter any command at any time, this model could become very complex indeed, but it can be simplified by omitting:

- Those commands that are unlikely when the IVIS is in certain states
- Long complex commands which should not be entered by a driver when the vehicle is moving (though these should be noted in the HMI analysis report).

Colour can be used to distinguish between those states that are normally used when the vehicle is parked, and those that are used when the vehicle is stationary.

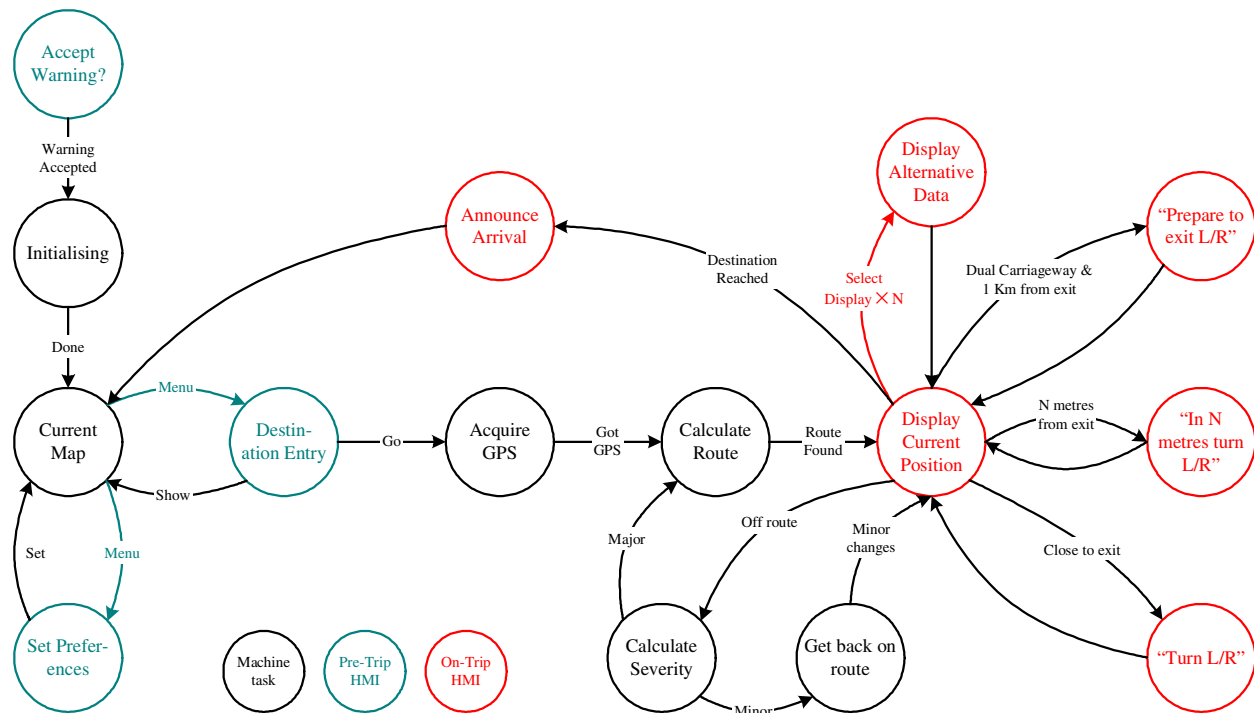


Figure 2: Simplified state machine for a navigation device

In order to identify the entities to analyse, it may also be necessary to use a data flow diagram to model the data flows in the system (see [2]).

Adapting HAZOP to an IVIS DOP

The generic HAZOP process is based on exploring deviations from the design intent of a system using a series of entities, attributes and guidewords.

An **entity** is the lowest level of component, system or function that will be examined in the analysis. As originally envisaged, the entities were flows of a physical agent; for example, a chemical agent moving in a pipe. In the more general application of HAZOP, the “flows” can be interpreted a component responsible for the movement of data or information. The following definition has therefore adopted in the context of the DOP:

Entity: an information flow or signal that passes between the IVIS and the driver or other operator. The entity is defined at the system HMI.

Entities will need to be defined for each specific application or class of applications. A generic entity could be “visual display message”. This might be further decomposed into information messages, modal dialogs, etc. Then for a specific system the classes or even the individual messages could be identified and analysed. See Figure 3.

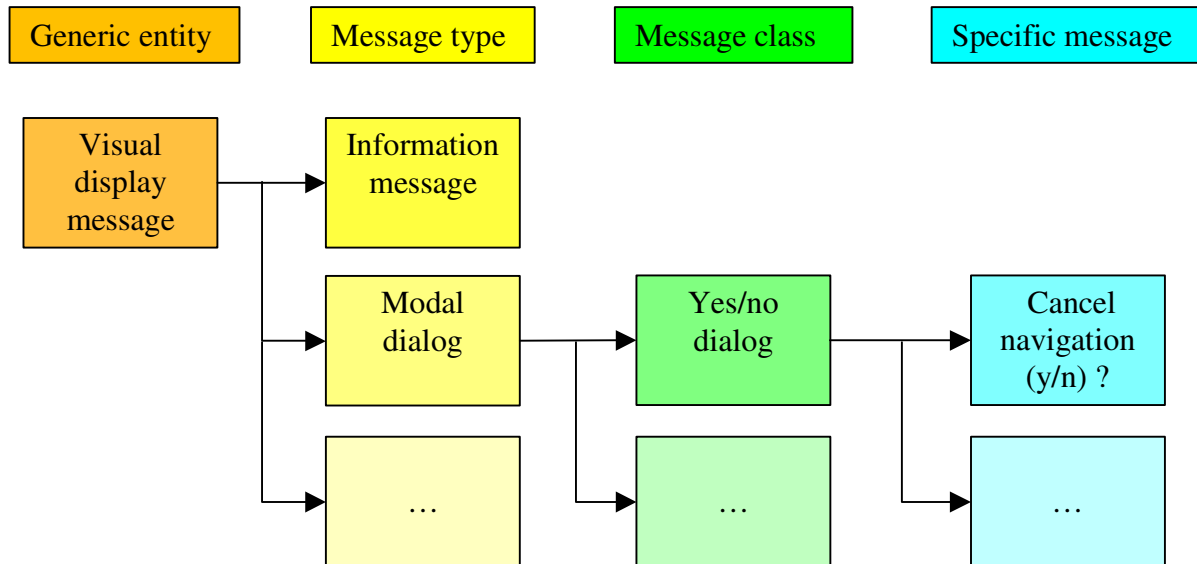


Figure 3: Example classification of entities

The **attribute** is an identifiable state or property of the entity. The interpretation will depend on the specific data flow but could include:

- Value – the numerical or textual or other content of the data flow
- Time – the relative time in which the data flow occurs
- Sequence – the sequence or order related to the data flow (e.g. a message may have several stages which are intended to occur in a pre-defined order).

The **guideword** describes a deviation from the intended design behaviour. There is a basic standard set of guidewords although these need to be interpreted in the context of the analysis being undertaken. The authors' experience with HAZOP shows that the generic guidewords always provide a complete set that describes all possible deviations, even though they will usually need to be interpreted in each application domain. The standard guidewords and their generic meanings are shown in Table 1 [see 2, 4].

Table 1: Generic HAZOP guidewords

Generic properties	Meaning
<i>No</i>	The complete negation of the design intention – no part of the intention is achieved and nothing else happens
<i>More</i>	A quantitative increase over what was intended
<i>Less</i>	A quantitative decrease over what was intended
<i>As well as</i>	All the design intention is achieved together with additions (i.e. a qualitative increase over what was intended)
<i>Part of</i>	Only some of the design intention is achieved (i.e. a qualitative decrease over what was intended)
<i>Reverse</i>	The logical opposite of the intention is achieved
<i>Other than</i>	Complete substitution, where no part of the original intention is achieved but something quite different happens
Timing	Meaning
<i>Early</i>	Something happens earlier than expected relative to clock time
<i>Late</i>	Something happens later than expected relative to clock time
<i>Before</i>	Something happens before it is expected, relating to order or sequence
<i>After</i>	Something happens after it is expected, relating to order or sequence

EVALUATING THE DOP

The DOP was evaluated by trialling it on two real IVIS systems – a speed limit warning system and a navigation application running on a GPS-equipped PDA. Both of these are aftermarket devices readily available to consumers. These devices were used as examples of the type of system to which the DOP could be applied, and the DOP was applied as if these were new concepts that were being developed. For both devices, the system behaviour was first modelled with a state machine to represent the different display states, and a data flow diagram that was used to identify the entities for the analysis. Figure 2 above shows the state machine for the navigation device. Figure 4 below shows the corresponding data flow diagram.

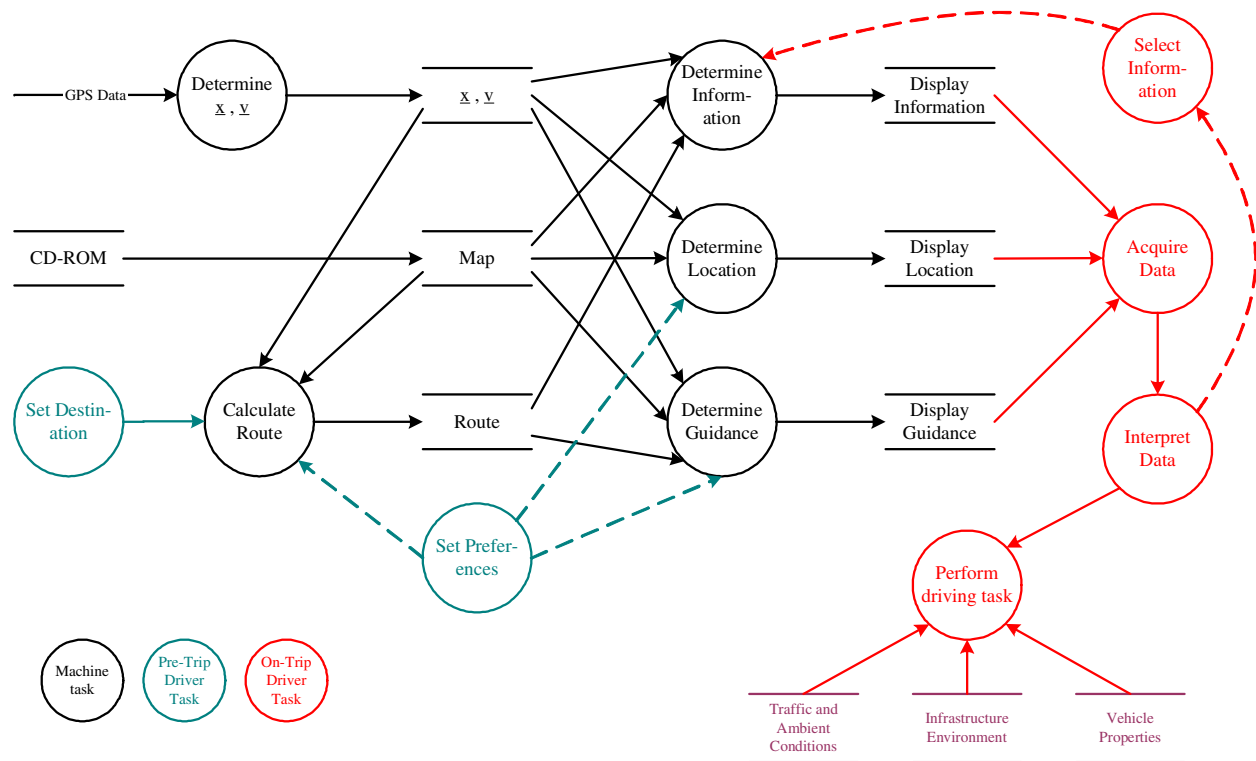


Figure 4: Simplified data flow diagram for a navigation device

The analysis first identified appropriate entities and attributes. The generic guidewords were applied and interpreted in the context of the navigation application. It was then possible to explore possible deviations from the design intent, explore the causes and consequences, and make recommendations for the design to mitigate these findings. The results are shown in the Table 2.

Table 2: Results of trial application of DOP

Entity	Attribute	Guide word	Interpretation	Cause	Consequence	Recommendation
IVIS display	General image	Less	Driver doesn't (can't) see display	Ambient lighting conditions	Inappropriate driver reaction	Design – shading/contrast protection
Local map	Graphic image	Less	Not enough information	Inappropriate scale	Inadequate guidance Distraction	Ensure large scale maps have the most information
Local map	Graphic image	More	Too much information	Inappropriate scale	Inadequate guidance Distraction	Ensure small scale maps have less information

<i>Entity</i>	<i>Attribute</i>	<i>Guide word</i>	<i>Interpretation</i>	<i>Cause</i>	<i>Consequence</i>	<i>Recommendation</i>
Local map	Graphic image	Less	No relevant information	Map out of date or off map	Inadequate guidance Distraction	Ensure system can be “disobeyed” without failing
IVIS display	General image	More	Display too bright for ambient conditions	Backlight too bright for ambient conditions	Distraction and glare	Implement day/night or background lighting options
IVIS display	General image	Other than	Display interruption by another application	e.g. diary reminder pops up	Temporary loss of IVIS function	IVIS function should be capable of being set as the priority application
IVIS display	General image	Other than	Display interruption by another application	e.g. diary reminder pops up	Requires additional interaction with interface to cancel and return	IVIS function should be capable of being set as the priority application
Local map	Graphic image	Late	Map scale does not change in time	e.g. delay in GPS position update	Inadequate guidance Distraction	Use map image as backup.
Turn instruction	Auditory message	No	Driver does not receive message	Low signal level compared to ambient conditions	Driver not advised of imminent turning	1. If possible, control the volume of IVIS 2. If base device not loud enough provide additional amplification
Turn instruction	Auditory message	More	Instruction to take turn when there is no turn to take	Incorrect interpretation of mapped links	Driver could be confused and/or distracted	Ensure navigation algorithm is robust
Turn instruction	Auditory message	Less	No instruction to take turn when there is potentially a turn to take	Incorrect interpretation of mapped links	Driver could be confused and/or distracted	Ensure navigation algorithm is robust

<i>Entity</i>	<i>Attribute</i>	<i>Guide word</i>	<i>Interpretation</i>	<i>Cause</i>	<i>Consequence</i>	<i>Recommendation</i>
Turn instruction	Auditory message	Other than	Message interruption by another application	e.g. diary reminder interrupts	Temporary loss of IVIS function	IVIS function should be capable of being set as the priority application
Turn instruction	Auditory message	Late	Message is not given in time	e.g. delay in GPS position update	Inadequate guidance Distraction	Use map image as backup

The DOP was further evaluated by comparing the results of the DOP analysis with an existing checklist-based approach [5]. It was found that concerns about auditory output audibility, system response time and display size were identified in both analyses. However the checklist approach identified specific input functionality and display location and rigidity issues that were not specifically noted by the DOP. It should be noted that at a concept stage of development not all such design aspects may be defined and/or known. Conversely, the DOP identified issues not found by the checklist, including possible deterioration of the display due to ambient lighting conditions and IVIS function priority.

CONCLUSIONS

This paper has presented a new approach to the assessment of potential safety implications of the way that information is presented to a driver by an IVIS, based on the HAZOP approach. HAZOP was found to be a suitable approach, although the concepts of entity and attribute need to be interpreted in each application (or class of applications). The generic guidewords of HAZOP were found to be applicable, although as with any application of HAZOP they have to be interpreted for the system under consideration,

The new approach was trialled by conducting an analysis based on two existing IVIS. For one of these analyses, the results of the DOP approach were compared with the results obtained from an existing checklist-based approach. It was found that while both approaches identified common issues, DOP found issues not identified by the checklist and vice versa. Both analysis methods are useful, and the DOP should therefore be seen as an additional method which can be used to supplement existing analysis methods in order to achieve a more complete identification of issues.

The application of a HAZOP-derived DOP to an IVIS is therefore a useful additional assessment method to investigate the potential risks of a proposed IVIS HMI at an early stage in product development. The use of the DOP in association with a preliminary safety analysis is also encouraged to develop a safety case for a new IVIS product. It will also assist in the identification of design issues that will need subsequent attention and re-evaluation as the design process proceeds prior to eventual assessment using a full experimental protocol.

REFERENCES

- [1] “Commission Recommendation of 21 December 1999 on safe and efficient in-vehicle information and communication systems: A European statement of principles on human machine interface”, *Official Journal of the European Communities*, **L19/64**, 25 January 2000.
- [2] F Redmill, M Chudleigh, and J Catmur, *System safety: HAZOP and software HAZOP*, ISBN 0-471-98280-6, John Wiley, 1999.
- [3] H.M. Jagtman, *Road safety by design*, ISBN 90-5972-045-8, Eburon Publishers, 2004.
- [4] Def Stan 00-58, *HAZOP studies on systems containing programmable electronics*, Issue 2, UK Ministry of Defence, 2000.
- [5] A Stevens *et al.*, “A safety checklist for the assessment of in-vehicle information: Scoring proforma”, TRL Project Report PA3536-A/99, 1999.

ACKNOWLEDGEMENTS

The HASTE project was funded under the “Competitive and Sustainable Growth” programme of the Fifth Framework of the European Commission, contract number GRD1/2000/25361.

© 2005 MIRA Limited.