Safety Specification of the Active Traffic Management Control System for English Motorways

A. J. Arlow*, C. J. Duffy*, J. A. McDermid†

* Systems Engineering & Assessment Ltd, Beckington Castle, PO Box 800, Beckington, Frome, BA11 6TB, UK
email: {Andrew.Arlow@sea.co.uk | Chris.Duffy@sea.co.uk}, fax: 01373 831133
† University of York, Department of Computer Science, University of York, Heslington, York YO10 5DD, UK,
email: John.McDermid@cs.york.ac.uk, fax: 01904 432708

Keywords: Active Traffic Management, FTA, Functional Hazard Analysis, HAZOP, Use Case.

Abstract

This paper describes the process by which the safety requirements for a future motorway control system were derived. Although the problem domain was found to be amenable to standard analysis techniques, it was necessary to adapt the techniques used to allow for domain specific factors and behaviours, for example, the indirect nature of the causal link between a failure within the system boundary and the subsequent occurrence of an accident on the road. The process was based on domain-specific hazard classifications, a Hazard and Operability (HAZOP) study, Fault Tree Analysis (FTA), and other tools and techniques adapted to support their use within the road transport domain. The objective of the paper is to critically review the utility of the tools and techniques used during these specification activities, and provide guidance for their future use.

1 Introduction

The Active Traffic Management (ATM) Pilot programme is a Highways Agency (HA) initiative which aims to maintain or improve safety levels whilst reducing congestion on a section of the M42 motorway, between junctions 3A (M40) and 7 (M6), through the implementation of new Operational Regimes (ORs). It will be used to develop and prove technologies and institutional arrangements in order to assess operational performance and confirm the business case for future deployment of the system. The ATM Pilot programme is a key element of the Government’s ‘10 Year Plan for Transport’.

1.1 Programme

The ATM Pilot programme started in 2001 and is scheduled to complete in 2009. The ATM Control System (CS) development project, on which this paper focuses, is a separate project within the Pilot programme, started in January 2003 and will run for the remainder of the Pilot programme.

The implementation of the ATM Pilot programme is taking place in four phases:

- Advisory 3 lane variable speed limits (VSL) – speed limits will be displayed to drivers over the running lanes but will be advisory only. The hard shoulder will not be used as a running lane except under the direction of the police. 3 lane VSL is an example of an OR.
- Mandatory 3 lane VSL – speed limits will become mandatory when displayed and enforcement is in place. The hard shoulder will not be used as a running lane.
- Mandatory 4 lane VSL with Semi-automatic Control System (SCS) – both 3 lane and 4 lane VSL operations will be possible, both with enforcement. The hard shoulder may now be used as a running lane. Monitoring and control of the motorway will be achieved using a modified existing control system and infrastructure.
- Mandatory 4 lane VSL with the ATM CS – Both 3 and 4 lane VSL operations will be provided by the ATM CS, which will replace the SCS. The ATM CS will provide improved monitoring and control features.

1.2 System Overview

The ATM CS takes data in from roadside sensors, Operator requests and other systems, and applies pre-defined rule-sets and processing algorithms to determine the most appropriate aspects to set on the signs and signals under its control, to implement the chosen OR.

Figure 1 shows the key components visible to a driver. Lightweight gantries are used to mount the signs and signals. Advanced Motorway Indicators (AMIs) over each lane display advisory and mandatory speed limits, as well as lane closure aspects and instructions for traffic to divert into another lane. Advanced Motorway Signs (AMSs) provide information to drivers, using both text and pictograms. Current sensing technology comprises closed-circuit television (CCTV) cameras, which are manually controlled and monitored in a control office, and inductive loops in the road. These loops form the main means of sensing traffic flow and provide information to algorithms which can determine when there is an incident or if queues are forming.
Speed enforcement will be introduced as part of ATM, but the ATM CS does not carry out any enforcement function itself. The ATM CS will eventually provide data to inform enforcement systems. As the hard shoulder can be used as a running lane, Emergency Refuge Areas (ERAs) are provided which are a haven for vehicles if they break down or need to stop. Each ERA has an emergency telephone to allow drivers to report problems and call for assistance.

Further details of the ATM CS may be found in [2],[3].

1.3 System Boundary

Figure 2 is a simplified representation of the boundary of the ATM CS in relation to those entities with which it interacts (actors). Actors may be people, organisations or other systems. Road Control Device (RCD) is the collective term for signs and signals. Road Monitoring Device (RMD) refers to the various sensor technologies deployed.

2 Process Overview

Figure 3 provides a simplified summary of the process by which safety requirements were derived for the ATM CS.

3 The ATM Safety Objective

The HA’s safety targets, which are applicable to motorways, and which have been derived from national safety targets set by the Department for Transport (DfT), are:

- 33% reduction (1998-2010) in the number of people killed or seriously injured (KSI) in road accidents.
- Contributing to the national child casualty reduction target of a 50% reduction (1998-2010) in the number of children killed or seriously injured (child KSI) in road accidents.
1. The numbers of people, per annum, killed and seriously injured in a calendar year. The measure used as an indicator of global risk was the total requirements than is necessary. In translating the ATM Safety change the risk profile of the motorway, the ATM Safety line, has the potential to balance a reduced level of risk to one road user type against an increased level of risk to another. On the face of it, it may not be immediately obvious how GALE, which appears to provide no nett reduction in risk, can help achieve the risk reduction required by the HA’s safety targets. However, the risk baseline against which ATM is being compared improves upon the 1994-1998 baseline that features in the HA’s safety targets. Given that ATM, with its use of the hard shoulder as a running lane, has the potential to assume the worst credible outcome for each hazard can result in the specification of more onerous safety requirements than is necessary. In translating the ATM Safety Objective to a numerical target, this problem was addressed. The measure used as an indicator of global risk was the total number of accidents in a calendar year. The process by which the ATM Pilot programme has been formulated to ensure that the ATM Pilot programme contributes to the achievement of the HA’s safety targets. The ATM Safety Objective is:

The M42, between Junctions 3A (M40) and 7 (M6), with the ATM system in operation, shall present a level of risk that is at least equivalent to the global risk currently experienced by users of that section of the M42. This safety objective is usually referred to by the acronym GALE (Globally At Least Equivalent). As well as being applied at the level of all road users, GALE is applied to specific road user groups. This makes it unacceptable to compare improvements and enhancements to vehicle design.

The hazard classifications identified in Table 1 have the following features:
- They can be categorised as those that promote driver action (CS-Hzd-1 to CS-Hzd-3) and those that do not (CS-Hzd-4 to CS-Hzd-6).
- They attempt to ensure that the degree to which a driver can control his or her vehicle in a hazardous situation is considered. An approach to risk assessment that considers different degrees of ‘controllability’ has previously been discussed below).

4 Hazard Analysis
A number of devices and subsystems, such as AMIs and AMBs, inductive loops and CCTV are outside of the ATM CS boundary, the hazard identification and analysis exercise nevertheless took account of them. It is these devices and subsystems that provide the interface between road users and the ATM CS and without considering them the analysis would not have produced any meaningful outputs.

4.1 Domain-Specific Hazard Classifications
Prior to hazard identification and analysis the authors defined a series of domain-specific hazard classifications, applicable to the ATM Pilot programme. These classifications were aimed at supporting the hazard identification process and the differentiation of hazards from their causes, and are listed in Table 1.

The hazard classifications identified in Table 1 have the following features:
- They can be categorised as those that promote driver action (CS-Hzd-1 to CS-Hzd-3) and those that do not (CS-Hzd-4 to CS-Hzd-6).
- They attempt to ensure that the degree to which a driver can control his or her vehicle in a hazardous situation is considered. An approach to risk assessment that considers different degrees of ‘controllability’ has previously been

The basis for comparison for these targets is the 1994-1998 average.

The HA estimates that road safety initiatives, such as ATM, will be responsible for approximately one third of the required reductions, with the remainder provided by road improvements and enhancements to vehicle design.

The ATM Safety Objective has been formulated to ensure that the ATM Pilot programme contributes to the achievement of the HA’s safety targets. The ATM Safety Objective is:

- A 10% reduction (1998-2010) in the slight casualty rate, expressed as the number of people slightly injured per 100 million vehicle kilometres.

2. The numbers of people seriously injured were adjusted upward to take account of the findings of a study in which it was estimated that only 89% of serious injuries are reported [4]. The study compared hospital reports with STATS19 data.

3. The numbers, per annum, of people slightly injured were calculated using data from the STATS19 accident reports for the ATM Pilot site. These numbers were adjusted upward to take account of the findings of [4], in which it was estimated that only 77% of slight injuries are reported.

4. To translate from injuries to accidents, the STATS19 accident reports were analysed to determine, on average, the numbers of people killed per accident, seriously injured per accident, and slightly injured per accident. Accident numbers, for each of the years 1998 to 2002 and on average per annum, were calculated using these ratios in conjunction with the numbers of people killed, seriously and slightly injured derived in steps 1, 2 and 3.

5. Damage only accidents, based upon estimates calculated as part of the wider ATM Pilot programme, were added to the average, per annum, accident numbers calculated in step 4 to give a total number of accidents that occur on average per annum for the ATM Pilot site.

This total number of accidents per annum was used as the top-level input into the probabilistic fault trees (discussed below).

Table 1.

<table>
<thead>
<tr>
<th>Hazard Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS-Hzd-1</td>
<td>Driver-related actions leading to hazardous situations.</td>
</tr>
<tr>
<td>CS-Hzd-2</td>
<td>Road user actions leading to hazardous situations.</td>
</tr>
<tr>
<td>CS-Hzd-3</td>
<td>Subsystem actions leading to hazardous situations.</td>
</tr>
<tr>
<td>CS-Hzd-4</td>
<td>Actions of road users and sub-systems that do not lead to hazardous situations.</td>
</tr>
<tr>
<td>CS-Hzd-5</td>
<td>Actions of other road users and sub-systems that may lead to hazardous situations.</td>
</tr>
<tr>
<td>CS-Hzd-6</td>
<td>Actions of other road users and sub-systems that do not lead to hazardous situations.</td>
</tr>
</tbody>
</table>

The data was supplied to the authors from data gathered as part of the ‘Before and After’ study being undertaken to measure the impact of ATM. For each of the years 1998 to 2002 and on average per annum, were calculated using these ratios in conjunction with the numbers of people killed, seriously and slightly injured derived in steps 1, 2 and 3.
used within the automotive industry [5]. The approach used within the specification of the ATM CS does however differ from that described in [5].

<table>
<thead>
<tr>
<th>ID</th>
<th>Hazard Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS-Hzd-1</td>
<td>Direction of vehicle towards a pedestrian or pedestrians, where better than normal driver skill is needed to avoid an impact.</td>
</tr>
<tr>
<td>CS-Hzd-2</td>
<td>Direction of vehicle towards an occupied vehicle or vehicles, where better than ...</td>
</tr>
<tr>
<td>CS-Hzd-3</td>
<td>Direction of vehicle towards an unoccupied vehicle or passive object, where better than ...</td>
</tr>
<tr>
<td>CS-Hzd-4</td>
<td>Failure to direct vehicle away from a pedestrian or pedestrians, where better than ...</td>
</tr>
<tr>
<td>CS-Hzd-5</td>
<td>Failure to direct vehicle away from an occupied vehicle or vehicles, where better than ...</td>
</tr>
<tr>
<td>CS-Hzd-6</td>
<td>Failure to direct vehicle away from an unoccupied vehicle or passive object, where better than ...</td>
</tr>
</tbody>
</table>

Table 1: ATM CS Hazard Classifications

The classical approach to controllability considers the ability of drivers to cope with technical failures, for example, how readily they can control the vehicle given the loss of ABS. Our approach has been to adopt the same underlying philosophy, but to apply it to the driver’s ability to respond properly to misinformation such as sudden reductions in speed or lane closure. This, we believe, is much more effective than treating technical failures, for example the loss of an AMI, as the top-level hazards. This approach not only helps in hazard analysis but helps in identifying hazard mitigations – which generally involve changing the state of other signs or signals to produce a situation which is controllable. We believe that this approach to hazard identification is one of the key innovations in our process, and there is also a general message for those analysing safety of novel systems: design hazard categories so they are appropriate to the domain.

4.2 Hazard Identification and Analysis using Use Cases

In [1] an approach to hazard identification and analysis is proposed based upon analysis of the use cases of a system within the setting of a HAZOP study. Use cases describe the functional behaviour of the system and as such are useful during system level hazard analysis, where the functions of the system may be known but not its exact logical or physical composition. An example use case, relevant to the ATM Pilot programme, is shown in Table 2.

In common with [1], a refined set of HAZOP guidewords, which are due to Pumfrey [6], was used:

- Omission – the service is never delivered.
- Commission – the service is delivered when not required.
- Early – the service occurs earlier than intended.
- Late – the service occurs later than intended.
- Value – the information delivered has the wrong value.

[1] proposes application of the guidewords to each use case element (stimulus, pre-conditions, system response, post-conditions) as part of the following process:

1. Apply and interpret each of the guidewords.
2. Identify possible failure causes.
3. Interpret the deviation in terms of the use case.
4. Interpret the real world effect of deviation on the system.
5. Assign a failure classification based on the system level effect.
6. Identify necessary integrity constraints on the core function.
7. Identify where the failure classification merits the incorporation of new, safety-related use cases.

For this HAZOP study, this process was tailored to increase the speed with which each deviation was considered and so reduce the time being spent in the HAZOP workshops – of particular importance given the difficulty in getting all workshop participants together at the same time. The following tailoring measures were applied:

Table 2: Manage VSL Use Case

<table>
<thead>
<tr>
<th>Use Case Title</th>
<th>Manage VSL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stimulus</strong></td>
<td>A flow measurement or an occupancy measurement is received from the monitoring devices</td>
</tr>
<tr>
<td><strong>Pre-conditions</strong></td>
<td>VSL has been successfully deployed</td>
</tr>
<tr>
<td><strong>System Response</strong></td>
<td>• IF occupancy measurement is greater than the stationary traffic threshold THEN</td>
</tr>
<tr>
<td></td>
<td>• Set AMIs (main carriageway and hard shoulder) immediately upstream from the occupancy measurement to 40 (enforced), and the AMIs two gantries upstream from this to 60 (enforced)</td>
</tr>
<tr>
<td></td>
<td>• On the AMS immediately upstream from the occupancy measurement display the queue pictogram and the text “Slow Down” (non-enforced)</td>
</tr>
<tr>
<td></td>
<td>• ELSE IF &lt;alternative conditions omitted&gt;</td>
</tr>
<tr>
<td></td>
<td>• Report sign and signal settings to the Operator</td>
</tr>
<tr>
<td><strong>Post-conditions</strong></td>
<td>AMIs and possibly AMSs have been set in response to a received flow measurement or an occupancy measurement</td>
</tr>
</tbody>
</table>
• Guidewords were not applied to post-conditions since it was felt that this would duplicate their application to the system response.

• Step 1 was undertaken by the authors prior to the HAZOP workshops, and confirmed, or otherwise, by workshop participants.

• Step 3 was omitted altogether from the HAZOP study on the grounds that the real world effect of the deviation was, in any case, considered (step 4)

• Step 5 was omitted from the HAZOP study but undertaken within the FTA activity. This was considered permissible in the context of this programme since the ATM Safety Objective is expressed in terms of a global target. As such, the impact of all hazards must be considered collectively. This is discussed below.

• Steps 6 and 7 were merged but undertaken by the authors outside of the workshop setting. This allowed an holistic approach to the development of safety requirements, rather than safety requirements being developed on a deviation by deviation basis.

Tailoring of the process described in [1] and outlined above took place following the first workshop. Seven workshops were held in all, by the end of which each deviation was being considered in 6-7 minutes, compared with more than double this at the start. While the authors believe there is a time benefit provided by the tailoring outlined above, it should be recognised that HAZOP studies have a natural tendency toward greater efficiency (and hence speed) as they proceed, and this will have contributed to the improvement noted.

The HAZOP workshops were attended by a range of transport domain specialists and ATM project stakeholders, invited on the basis of their ability to provide specific areas of expertise. This ensured that a wide range of applicable expertise was used in the analysis.

Application of the approach proposed within [1] allowed analysis of the safety implications of the system’s proposed functionality before (in principle) any design decisions were made. It also created a strong linkage between the systems and safety engineering processes. The safety engineering team were able to access directly the use cases defined within the system model created by the systems engineering team, and use them within the HAZOP study.

In adopting the approach described above, care must be exercised in the selection of use cases to be analysed: a large system can have a large number of use cases which, if all were to be analysed would almost certainly take more time than is available within the schedule. This was the case within this safety programme. The goal of the analyst, therefore, is to identify the use cases, the analysis of which will yield the maximum number of hazards and/or causes – in effect a cost/benefit trade-off.

Prior to the workshops the authors, in conjunction with the systems engineering team, identified the so-called ‘core’ functions of the system: functions considered to provide control over the motorway. The application of this criterion reduced the number of use cases to be analysed from just over 300 to just over 100. Of these core functions, 14 described the ORs identified at that point (Table 2 is an example of a partial OR described by a use case), with the remainder describing general and user operational elements of system functionality in a more abstract manner. Only the use cases describing the ORs were analysed within the workshops. The general and user operational elements of system functionality were analysed separately by members of the safety engineering team.

The hazard log was generated from the use case deviations analysed within the HAZOP study. Each of the hazards can be identified with use cases defining the ORs and the general and user operational functions. Of the use case deviations from which hazard causes were generated, approximately 69% are associated with the OR use cases, while the remaining 31% are associated with the general and user operational functions. While these figures should be interpreted with care since there will inevitably be some overlap between the various categories of deviation, they do provide a general indication that the OR use cases provided a noticeably more effective way of identifying hazards and their causes. The reason for this is likely to lie in their specificity, when compared with the more abstract general and user operational use cases. An example, the Manage VSL use case shown in Table 2 ultimately ends up setting specific aspects (60 or 40) which affect driver behaviour. Within the general system functions the Set Aspects use case provides comparable functionality, however this use case includes the more general step: Send aspect requests to RCDs. The context provided by the specific setting requests in Manage VSL is lost.

4.3 ATM CS Hazards

The outputs of the HAZOP study were cross checked against the fault trees, generated by a process described in Section 5, to ensure mutual consistency, and the hazards documented in Table 3 identified.

A point to note about the hazards is that none of them relate to specific road user populations. Recall that the ATM Safety Objective does not allow risk to one population to be balanced against risk to another. Similarly, none of the hazards differentiates between adults and children. This reflects the fact that the ATM CS does not make any of these distinctions in its application of the currently envisaged ORs. Conversely, the ATM CS can only reduce the overall accident rate and by doing so reduce the casualty rate for specific populations.

A hazard which does relate to a specific road user type has been identified within the wider ATM Pilot programme, namely the hazard presented to motorcyclists by repeated crossing of the ‘rumble strip’ onto an actively managed hard shoulder. This hazard is being addressed through infrastructure design measures.
<table>
<thead>
<tr>
<th>ID</th>
<th>Hazard Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSH-01</td>
<td>Driver directed onto Hard Shoulder</td>
</tr>
<tr>
<td>CSH-02</td>
<td>Driver exits motorway abruptly</td>
</tr>
<tr>
<td>CSH-03</td>
<td>Driver changes lane abruptly from the Hard Shoulder</td>
</tr>
<tr>
<td>CSH-04</td>
<td>Driver uses Hard Shoulder when it is closed</td>
</tr>
<tr>
<td>CSH-05</td>
<td>Stationary vehicle unprotected</td>
</tr>
<tr>
<td>CSH-06</td>
<td>Vehicle directed into an existing incident</td>
</tr>
<tr>
<td>CSH-07</td>
<td>Driver changes lane abruptly on main carriageway</td>
</tr>
<tr>
<td>CSH-08</td>
<td>Driver brakes heavily</td>
</tr>
<tr>
<td>CSH-09</td>
<td>Opposing lane diverts</td>
</tr>
<tr>
<td>CSH-10</td>
<td>Queuing traffic not protected</td>
</tr>
<tr>
<td>CSH-11</td>
<td>Hard Shoulder opened with stationary vehicles or debris present</td>
</tr>
<tr>
<td>CSH-12</td>
<td>Vehicles are directed by AMIs toward an ERA (lane divert left immediately before an ERA)</td>
</tr>
</tbody>
</table>

**Table 3: ATM CS Hazards**

### 4.4 Analysis of Unsafe Aspect Combinations

The hazards identified all relate to aspects (instructions) that are or are not displayed to road users. It is therefore only possible to claim that all hazards and their causes have been identified if all combinations of aspects may be displayed as a result of failures within the system are considered. This observation reflects the experience of the HAZOP study when considering value deviations of RCD settings: it is only really possible to get a full understanding of the likely outcomes of such a deviation by considering each possible setting in turn and how it relates to the aspects already set around it. Unfortunately, there are a large number of possible RCD settings and to consider them all within the workshop setting would take a prohibitively long time. The various possible RCD settings were therefore considered exhaustively outside of the workshop setting. The number of aspect combinations to be considered is large and therefore the goal was to analyse a minimal but sufficient set. The various aspect combinations considered fell into four groups, identified by the relative positioning of the RCD types upon which they can be displayed:

- One AMI and one AMS, adjacent to each other.
- Two AMIs on consecutive gantries, over the same lane.
- Three AMIs on a single gantry, transversally (to the flow of traffic) adjacent to each other, with the Hard Shoulder closed.
- One AMI over lane 1 and one AMI over the Hard Shoulder with the Hard Shoulder open.

Table 4 provides a fragment of the analysis of aspect combinations that may be displayed on two longitudinally consecutive gantries.

**Table 4: Fragment of Analysis of Aspect Combinations**

(us) means upstream and (ds) downstream, and both relate to the direction of traffic flow. Since each RCD can display the same aspects, the table from which Table 4 is extracted is simply a square matrix in which the contents of the first row and first column (the aspect identifiers) are the same. Within Table 4, a tick indicates that the aspect combination is considered acceptably safe, while an exclamation mark indicates the converse.

The findings of this analysis were incorporated into the hazard log as additional or more specific hazard causes. No additional hazards were identified.

### 4.5 Functional Failure Modes

The hazard identification process identified hazard causes at two distinct levels labelled, for convenience, intermediate and atomic causes. The latter are in fact functional failure modes of the system.

- **RMD Failure/Error**: RMD software failure/error, RMD hardware failure/error, RMD data error
- **RCD Failure/Error**: RCD software failure/error, RCD hardware failure/error, RCD data error
- **CS Failure/Error**: CS software failure/error, CS hardware failure/error, CS data error
- **Operator Interface failure/error**
- **Communications failure/error**
- **Installation Error**: RMD Installation Error, RCD Installation Error, CS Installation Error
- **Power Failure**: RMD Power Failure, RCD Power Failure, CS Power Failure, Communications Power Failure
- **Overload**: CS overload, Comms overload
- **Human Failure/Error**: Operator failure/error, Maintainer failure/error, On-road resources failure/error
- **Malicious Action**: Malicious Operator action, Malicious Maintainer action, Malicious damage by third party
- **Breach of computer security**

The functional failure modes were identified as a ‘by-product’ of the hazard analysis activities. Effort was expended during hazard analysis to refine the classification of failure types to ensure consistency in identification of hazards and hazard...
causes. If these functional failure modes had been determined at the start of hazard analysis this would have reduced the time spent on this activity. Further, although the functional failure modes provide a useful checklist identifying deviations in a HAZOP study, they need to be refined when recorded as hazard causes in a hazard log, to enable effective mitigation. For example, a hazard caused by a communications failure may be mitigated in different ways depending upon whether the failure is a complete message loss or a message corruption.

5 Risk Assessment

In parallel to the HAZOP study, a FTA was undertaken starting with the various accident types that may occur on the road and deducing their causes. The FTA fulfilled two roles. Firstly, it allowed a cross check to be made on the completeness of the hazard causes and secondly it provided a means for deriving safety integrity requirements.

5.1 Generic Accident Types

A workshop setting was initially used to identify the various accident types and to derive a set of ‘qualitative’ fault trees for each accident type. These qualitative fault trees were derived without reference to the findings of the HAZOP study, to ensure an independence of view. Additionally, they were not populated with any numerical data. In common with the HAZOP workshops, the FTA workshops were attended by a range of transport domain specialists and ATM project stakeholders.

The accident types are believed to represent the range of accidents that may occur within the ATM Pilot site. They are shown in Table 5. Throughout the table, V1 is used to indicate the vehicle responsible for the accident, RC, the Running Carriageway and HS, the Hard Shoulder.

<table>
<thead>
<tr>
<th>ID</th>
<th>Accident Type</th>
<th>Sub-type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acc-01</td>
<td>Rear Collision:</td>
<td>a) V2 stationary (RC, HS or ERA).</td>
</tr>
<tr>
<td></td>
<td>Collision between two vehicles</td>
<td>b) V2 moving slower than V1 (RC, HS or ERA).</td>
</tr>
<tr>
<td></td>
<td>travelling in the same direction.</td>
<td></td>
</tr>
<tr>
<td>Acc-02</td>
<td>Chain Collision:</td>
<td>a) V2 stationary on carriageway at rear of queue (RC or HS).</td>
</tr>
<tr>
<td></td>
<td>Collision between more than two</td>
<td>b) V2 decelerating to join queue (RC or HS).</td>
</tr>
<tr>
<td></td>
<td>vehicles travelling in the same</td>
<td></td>
</tr>
<tr>
<td></td>
<td>direction.</td>
<td></td>
</tr>
<tr>
<td>Acc-03</td>
<td>Frontal Collision:</td>
<td>a) V1 crosses central reservation.</td>
</tr>
<tr>
<td></td>
<td>Collision between two vehicles</td>
<td>b) V1 crosses temporary barrier in contra-flow.</td>
</tr>
<tr>
<td></td>
<td>travelling in opposite directions.</td>
<td>c) V1 driving normally against traffic flow (RC, HS or ERA).</td>
</tr>
<tr>
<td>Acc-04</td>
<td>Lateral Collision:</td>
<td>a) V1 changes lane to right (RC or HS).</td>
</tr>
<tr>
<td></td>
<td>Includes angle collision, side by side</td>
<td>b) V1 changes lane to left (RC, HS or ERA).</td>
</tr>
</tbody>
</table>

Table 5: Generic Accident Types

5.2 Qualitative Fault Trees

In addition to system failure, the qualitative fault trees generated by the domain experts during the workshops contain entries relating to the environment and driver response. They were originally to be used for the derivation of the safety integrity levels. However, neither the ATM Pilot site accident data used to deduce the accident rate in Section 3, nor the other data reviewed during the course of the analysis (e.g. rate of carriageway debris egress, vehicle breakdown rates), supported the detail of these fault trees, particularly in relation to environmental and driver behaviour effects. As a consequence it was not possible to populate the qualitative fault trees in a uniform manner.

Hence, an alternative approach to the FTA was developed which used significant elements of both the ATM Pilot site accident data, other data analysed and the original workshop fault trees. Firstly, by examining the accident descriptions contained within the STATS19 data, it was possible to make a judgement on whether the ATM CS, if it had been in place at the time of the accident, could have made a difference as to whether the accident occurred. These were typically accidents that involved collisions with stationary vehicles on the running carriageway or hard shoulder. For other accidents, such as single vehicle accidents in the middle of the night, accidents involving mechanical failure, accidents involving drunk drivers, etc., it can be assumed that the ATM CS would have had no impact. By comparing this figure with the ATM Safety Objective, it was possible to deduce a figure for the number of accidents which can be assigned to a malfunctioning ATM CS. To examine this in more detail, ‘probabilistic’ fault trees were developed.

5.3 Probabilistic Fault Trees

The probabilistic fault trees use many elements of the qualitative fault trees. At the top level, they link directly to the accident types. They also share common elements in terms of the presence of objects within the motorway environment (e.g. stationary vehicle on the Running Carriageway). Where they diverge from the qualitative fault trees is that that they focus solely on ATM system component faults including the ATM CS hardware and software. These
specific faults were derived directly from the outputs of the HAZOP described in Section 4.

Typically the probabilistic fault trees take the form shown in Figure 4.

![Figure 4: Form of Probabilistic Fault Trees](image)

The resultant fault trees were populated using the available accident and failure data, and linked to the numerical target derived from the ATM Safety Objective. These probabilistic fault trees were used as the basis for risk assessment, indicating when safety risk had been sufficiently mitigated and providing numerical safety integrity requirements. Derived safety integrity requirements are identified in Section 6.

A feature of the fault trees is that they include driver response (or more correctly, the lack of an appropriate response) to the presence of the hazard. This event can be used to indicate the degree to which the driver can control his or her vehicle within the situation, and provides a parallel to the approach based on ‘controllability’ used elsewhere in the automotive industry. It is, however, difficult to estimate what probability should be apportioned to this event. Moreover, the fault trees are highly sensitive to the probability used. While not done during this safety programme, it would be instructive to investigate driver response in a driver simulator.

Data to populate the probabilistic fault trees was still comparatively sparse with a larger amount of data available to characterise what happens on the road (accidents, number of pedestrians on the motorway, amount of debris on the motorway, etc.) than the frequency with which various system components fail. The fault trees were therefore underpinned by a large number of assumptions. The authors attempted to offset this uncertainty through adoption of a conservative approach to estimation coupled with the use of error margins in the adoption of the final safety integrity requirements. In order to ensure visibility of the assumptions, they were explicitly documented within the Preliminary Safety Case.

It is worth noting that, at present, an accident requires a ‘failure of driver control’ since the ATM CS has no direct control over the driver’s vehicle. As motorway control systems become more advanced, it is possible to envisage a situation where direct control of a vehicle by the control system may remove the need for this failure of driver control.

This approach to risk assessment recognises and makes use of the global nature of the ATM Safety Objective. Each accident has a range of possible outcomes in terms of the severity of injury, and this is factored into the accident rate apportioned to the top event of the fault trees. Consequently, the fault trees consider severity implicitly and likelihood of occurrence explicitly.

6 Safety Requirements

Safety requirements were derived to mitigate the hazards and their causes. These are summarised below:

- The arbitrator function, which is responsible for setting aspects on the road, will implement a ‘signal sequencing ruleset’ that will not result in the unsafe aspect combinations being set. The arbitrator will balance competing aspect setting requests and take account of device status in the arbitration process. The arbitrator function will monitor device status (including settings made), and will re-arbitrate if necessary in the event of a device failure. If the arbitrator is not able to identify a safe set of aspects it will request Operator intervention.

- The aspect monitoring function will monitor aspect setting requests generated by the arbitrator and aspect settings on the road. By reference to its own ‘unsafe aspects ruleset’ it will determine whether the arbitrator is attempting to set unsafe aspect combinations or whether unsafe aspect combinations have been displayed on the road. Depending upon the ‘recovery mode’ defined within the unsafe aspects ruleset, the aspect monitoring function will block unsafe aspect setting requests made by the arbitrator function (automatic mode), seek Operator confirmation prior to setting (semi-automatic mode) or allow the requested settings but also request independent Operator recovery action (manual mode). Blocked aspect requests will be reported to the Operator. In addition, regardless of the recovery mode associated with detected unsafe aspect setting requests, the failure of the arbitrator function will be logged. A choice of recovery mode is provided in recognition of the fact that automatic blocking of aspects can, in some cases, give rise to an unsafe state on the road.

This is illustrated by the case in which the arbitrator is erroneously attempting to set a single STOP aspect with no lead-in signalling, in response to an incident. The lack of lead-in signalling is hazardous, however simply to block the requested STOP aspect would leave the incident unprotected.) The arbitrator function will automatically re-arbitrate when it detects a failure that affects the aspects displayed on the road. Since the Operator may wish to take action supplementary to that of the arbitrator function the aspect monitoring function will inform the Operator of
any unsafe aspect combinations detected. The system will also log the failure. The aspect monitoring function will not re-use elements of the arbitrator function, in particular, its source code or ruleset and thus will not be susceptible to any systematic errors in the arbitrator function.

- Significant user actions will be logged including, but not limited to deployment and termination of ORs, manual setting of aspects and amendment of configuration data. This provides a range of benefits but, in relation to the ATM CS hazards, will deter users from malicious use of the system.

- There is a residual risk that the CCTV system will not return the correct image, and that the ATM CS will not be able to determine that this error has occurred. To reduce the risk that the Operator fails to notice this type of fault, the CCTV camera ID will be displayed with the image returned.

- To minimise the possibility of Operator error as a result of poor user interface design, a System Operability Study will be undertaken during development of the ATM CS, aimed at establishing the optimum design for the user interface, identifying any system constraints which may impact the design of the user interface and determining optimum working practices for the users of the CS.

- To minimise the possibility of insufficient system resources leading to poor performance a system sizing study will be undertaken during development of the ATM CS. The study will determine the necessary processor, volatile and non-volatile memory requirements and confirm, or otherwise, that the internal (to the Control Room) and external communications requirements are adequate.

- The ATM CS software: no more than $1 \times 10^{-5}$ dangerous failures per hour.
- The ATM CS arbitration function: no more than $1 \times 10^{-5}$ dangerous failures per hour.
- The ATM CS aspect monitoring function: no more than $1 \times 10^{-5}$ dangerous failures per hour.
- The ATM CS users’ interface devices: no more than $5 \times 10^{-5}$ dangerous failures per hour.
- The ATM CS hardware: no more than $5 \times 10^{-5}$ dangerous failures per hour.

In addition, there are a number of procedural safety requirements, such as:

- Data will be maintained under configuration management using standards approved by the HA.
- A procedure will be defined and implemented that identifies what must be done in the event that the aspect monitoring function detects unsafe aspect setting requests or unsafe aspect combinations on the road.
- A procedure will be defined and implemented that addresses the situation where an Operator is unable to use the CCTV system to obtain visual confirmations.

- Procedures to be implemented to minimise the possibility of malicious User action adversely affecting system operation.
- A training regime for users of the CS will be defined and implemented, aimed at minimising the chance of human error.
- HA approved installation procedures will be used for the ATM CS, RMDs and RCDs.

The key safety function identified is the so-called aspect monitoring function, which checks sign and signal setting requests made by the ATM CS against its own (diverse) ruleset, and which monitors sign and signal settings on the road. The former is primarily aimed at mitigating failures within the ATM CS boundary, while the latter is primarily aimed at mitigating failures in equipment outside of the ATM CS boundary. An alternative view is that the former is aimed primarily at mitigating hazard causes while the latter is aimed primarily at mitigating hazard effects.

The unsafe aspects ruleset is generated by the analysis of aspect combinations, discussed above within the context of hazard identification and analysis. Choice of appropriate recovery mode is simply a question of considering the implications for each hazard of automatically blocking the unsafe aspect setting requests that cause the hazard.

Neither the arbitrator or aspect monitor will be capable of detecting hazards arising from safe aspect combinations which are inappropriate for the prevailing conditions. Such hazards are mitigated by other means, for example, Operator action.

7 Discussion and Conclusions

The following observations, additional to those elsewhere in this paper, can be made about the approach adopted:

- For this application, it is not possible to argue that the HAZOP is exhaustive without considering all combinations of aspects that may be displayed by the RCDs. This is labour intensive and best undertaken outside of the HAZOP workshops.
- Within the problem domain, and particularly for this application given the change in road use, it is not always possible to define a safe state. This creates difficulty in the determination of appropriate hazard mitigation. Ultimately, the resolution of this difficulty may rely on the system’s operational personnel.

Based on the work described in this paper, the following conclusions may be drawn regarding this application:

- The domain-specific hazard classifications provide a useful tool for assessing the completeness of the identified hazards as well as providing a means to differentiate hazards from their causes.
The functional failure modes identified provide a useful checklist to support future HAZOP studies in this domain. They do, however, need to be refined when recorded as hazard causes in a hazard log, to enable effective mitigation.

The set of road accident types identified provide a useful checklist to support future FTA activities in this domain.

Accident causation is governed by driver behaviour. The role of the equipment is to influence driver behaviour, however quantifying the level of this influence is difficult. Establishing the impact of the equipment and its failure on accident rates is therefore problematic. In order to ensure that hazard analysis outputs are both correct and complete (to the extent that this can be credibly claimed), the analysis techniques employed must be able to take account of the influence that the ATM CS has on driver behaviour.

In general, standard techniques, suitably adapted have proved appropriate and effective in this problem domain. The definition of domain-specific hazard classifications in terms of a driver’s ability to respond properly to misinformation, and their subsequent application to the outputs of the HAZOP study and FTA was a key innovation in this adaptation process.

The work undertaken also allows the following more general conclusions to be drawn:

- The approach proposed in [1] proved effective in the identification and analysis of hazards, and is well suited to system specification activities in general. Not all elements of this approach were found to be necessary.
- Selection of use cases for analysis can have a significant effect on both the time taken to complete the analysis and the completeness of the outputs. Use cases that identify system behaviour specifically rather than in an abstract manner are more likely to lead to the identification of hazards or their causes.
- Production of qualitative fault trees independently of the HAZOP outputs can have some benefits in terms of providing a cross check for hazard causes identified through the HAZOP process. However, if data is sparse, it is more effective to derive probabilistic fault trees directly from HAZOP outputs. In this case, the sparseness of data to populate the fault trees meant they were reliant on a large number of assumptions.

Beyond their obvious applicability to the road traffic domain, the tools and techniques described in this paper may have wider application. In particular:

- The approach to hazard identification and analysis described in [1] is suitable for any domain, since it is domain independent. Moreover the form of the use cases make them amenable to describing human processes and as such this approach could be readily extended to the Human Factors domain.

- The ATM CS is an example of a safety related information system. The form of the fault trees developed within this safety programme factor in human response to the information presented by the system and it is reasonable to believe that this approach could be extended to analysis of safety related information systems in general.

**Acknowledgements**

The ATM CS has been specified by the ATM CS Consultant (CSC), a team comprising the HA as the Project Sponsor, WSP Civils Ltd as the Prime Contractor, and SEA. The authors acknowledge the important role of these organisations in the conduct of the project and in the review of this paper.

The authors acknowledge the specific contributions of the following people within the various workshops undertaken in support of the safety activities described within this paper: Marcus Blitz (HA), Chris Chorlton (WSP), Tim Lovell (SEA), Mel Mock (SEA), Martin Morley (WSP), Andrew Parkes (TRL), Earl Patrick (WSP), Brian Rooker (CMPG) and Steve Tucker (HA).

The authors acknowledge the assistance received in the collation of accident data from Max Halbert (Cambridge Consultants), Ray Hartshorne (Mouchel Parkman), Stefan Lotter (WSP, formerly of Mott McDonald) and Bob Meekums (Mott McDonald).

Finally, the authors thank James Catmur of Arthur D. Little for comments provided on this paper.

**References**


