HAZARD BASED APPROACH TO THE MANAGEMENT OF OPERATIONAL SAFETY RISK ON HIGHWAYS SCHEMES

Ryszard Gorell & Lucy Wickham
Mouchel, UK, Export House, Cawsey Way, Woking, Surrey, UK
lucy.wickham@mouchel.com & ryszard.gorell@mouchel.com

ABSTRACT

The paper examines the approach that has been adopted by the UK Highways Agency (HA) to the definition and management of operational risk on Managed Motorway schemes. It will demonstrate and evidence the success of the adoption of this approach where it has been applied on operational schemes to date.

The role of the Highway Authority has migrated over recent years to one of Network Operator. More complex and flexible systems are being introduced with dynamic management capabilities (increasing role of technology). The operation of the road space has been fundamentally altered. There are new demands on motorists and the Operator needs to demonstrate that projects are implemented with an appropriate level of safety. This is necessitated in order to provide road users, road workers and additional 3rd parties with adequate risk protection

Setting safety objectives for a project provides a means of ensuring that the project is aiming to achieve an appropriate level of safety. Safety objectives should balance road user safety, road worker safety and third party safety with Project Cost. Safety objectives should take into account any global safety objectives.

It is essential that one starts by understanding the problem and defining what success looks like. There needs to be a clear understanding of how the network will operate and recognition that safety is one of the keys to this and may drive the design. Evidence sources need to be identified along with the project constraints. This leads to definition of the operational characteristics (known as regimes) and a common understanding of how the scheme is expected to operate. Following such a process in a systematic manner, underpinned by application of the hazard based approach will lead to successful scheme outcomes

The paper will present the methodology that has been developed and applied to achieve successful scheme outcomes. It will also present the approach and the monitoring and review strategy that has contributed to creation of the evidence base that assists in informing and shaping future interventions on the network.

1. INTRODUCTION

This paper examines the approach that has been adopted in the UK to the management of operational risk on Managed Motorway schemes. These schemes facilitate the dynamic control of traffic for congestion and incident management. The road space is managed in different ways for varying conditions to maximise capacity while providing a safe and informed environment for the travelling public and on-road resources (emergency services, maintenance workers, recovery operators and traffic officers). An example of a Managed Motorways scheme is the controlled use of the hard shoulder for congestion management. This paper will demonstrate the success of this approach where it has been applied on operational schemes to date.

New systems place new demands on motorists and as a result there is uncertainty about how the system will perform, especially in terms of providing road users, road workers and additional third parties with adequate risk protection. This uncertainty may also have an impact on the political acceptability of such systems, especially if they involve changing a fundamental component of the road, for example, dynamic use of the hard shoulder. In addition, legal responsibilities (duty of care) of the network operator towards these parties must also be adequately addressed. Therefore, before these systems are launched, there is a need to demonstrate, in a form that is auditable, that they can be implemented with an appropriate level of safety. A structured approach should be adopted to ensure that this is achieved.

2. AGREEING APPROACHES TO THE MANAGEMENT OF OPERATIONAL RISK ON THE HIGHWAY NETWORK

Whereas the traditional approach to a road scheme focuses on infrastructure and then considers the technology to support its use, the approach adopted here is to define as early as possible how the road space will be operated. This is achieved by considering how engineering, enforcement, education and encouragement (the four ‘Es’) can be applied given the constraints of the site, the expected traffic demand during the lifetime of the scheme and the outcomes that need to be achieved (e.g. reliable journey times, compliant driver behaviour, political acceptability and safety maintained). The way that the road is operated should be intuitive, with relevant and accurate information provided at timely intervals promoting ‘driver compliance’ (i.e. desired driver behaviour).

Once the operational approach is agreed (or at least narrowed to a small number of potential approaches), an appropriate safety management system (SMS) is implemented.

The systematic approach that has been developed to guide this design process is illustrated overleaf.

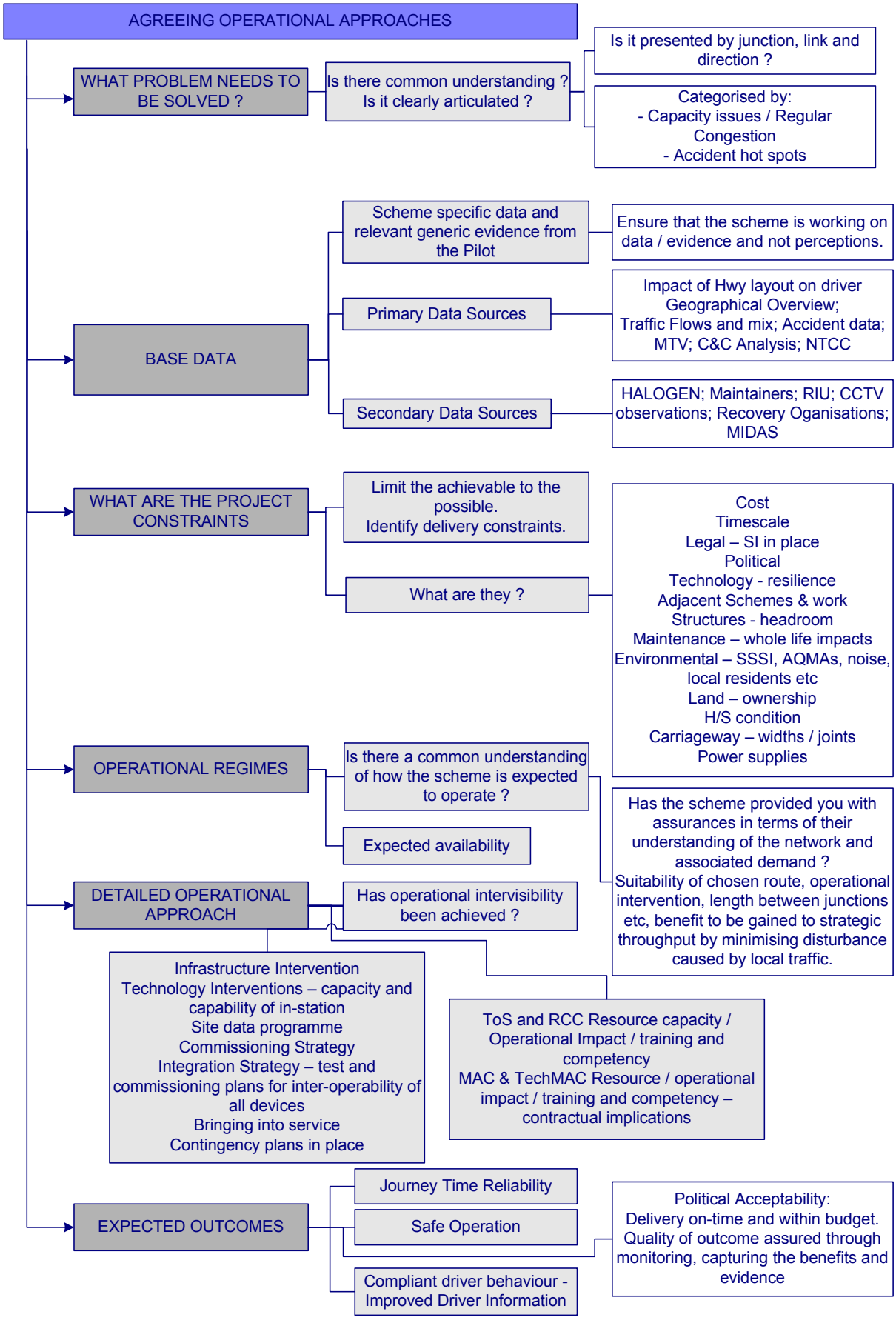

Figure 1 Agreeing Operational Approaches

HCKDBIYTOKLN

3. PRINCIPLES FOR SAFETY MANAGEMENT

The road 'system' can be seen as being made up of a number of separate entities, which include the road itself, communications infrastructure, the operator of any control systems in place, the driver and the vehicle. Safety can be seen as an emergent project feature in that the level of risk that will affect those on the road arises through the interaction of the above entities. Therefore an approach to safety management that is appropriate for the highways needs to be a system-orientated approach. In other words, any risk model that is generated must take into account the necessary entity interactions rather than studying each in isolation.

A system orientated approach can also be used to build up an overall picture of the risk (i.e. a risk model or profile) that a type of road section will present, enabling those areas that remain at a higher level of risk to be more readily identified.

As more work goes on to reduce the risk experienced by both the workforce and road users, the difficulty in identifying areas that can be targeted for further improvement tends to increase. The availability of a risk model, or risk profile, to help highlight areas that are appropriate for further mitigation then becomes a significant help.

Safety management principles exist in international standards such as IEC 61508[1], which are already applied to other industry sectors, including sectors of transport such as rail. Such standards can therefore be used to provide the foundation for safety management in the highways sector. Useful principles that IEC 61508 embodies, which we can transfer to the highways include:

- The need to conduct a comprehensive risk assessment
- That all aspects of the system require assessment
- The need to document activities thoroughly such that a clear record of all decisions is available
- The need to cover all stages of a system's lifecycle, from conception to decommissioning.

However, there are differences that apply to highways, as opposed to other transport sectors such as rail and aviation. Foremost among these is the degree of control that the Highway Authority has in respect of risk. It was noted above that safety as a project feature emerges from the interaction of a number of separate entities in a system and the Transport Authority has little / limited control over some of these entities, chiefly the vehicle and its driver. This situation is different from that in sectors such as rail and aviation, where those being transported do not have control over the way in which they are transported and can make only limited decisions that influence the risk that they experience (such as where they sit in a train carriage or aircraft).

---

[1] International Electrotechnical Committee, Functional safety of electrical/electronic/ programmable electronic safety-related systems, IEC 61508 parts 1-7 (1999).

A further requirement of the Highway Authority, and something that is not greatly emphasised in IEC 61508, is the need for appropriate analysis of the procedures carried out by maintainers and operators.

There is significant workload on operators which needs to be adequately specified and controlled, particularly as more sophisticated operational regimes are introduced. Maintainers often work while traffic is flowing and their work must be controlled by use of appropriate procedures.

Given road users and vehicles are independent parts of the road 'system', the Highway Authority can only affect a limited amount of the risk that road users are exposed to. As a result, there is a greater spread of safety criticality in systems that are deployed on the highways. There is no argument that a railway interlocking or Automatic Train Protection system is of anything other than the highest level of integrity. However, it is not always clear that traffic management systems are controlling similar levels of risk. Any safety management system (SMS) for the highway needs to be able to accommodate this range of safety criticality and ideally provide for a less onerous approach where the level of risk warrants it.

A safety management approach that is too onerous for a given situation can be as damaging as one that is insufficiently onerous, in that it undermines the credibility of such safety work and takes resources away from elsewhere where they could be better used.

The key requirements of an SMS for the Highway Authority are therefore to:

- Provide compliance with legal requirements
- Reflect the system aspects that characterise the highways
- Build upon the principles captured in recognised international standards such as IEC 61508 0
- Recognise the type of future developments that are expected, especially in respect of technology development and integration
- Provide flexibility in approach to match the safety criticality of the system in question.

4. SAFETY MANAGEMENT SYSTEM (SMS) – SELECTION AND APPLICATION

The UK approach to safety management consists of two stages: an initial analysis of the project being considered to determine what level of SMS is appropriate, and then the application of the SMS.

The approach used to select an SMS involves assessing the scheme against six characteristics or project features: stakeholder interest, operation experience, technology, standards and legislation, impact on organization and project scale.

Formal agreement will need to be reached with the Highway Authority as to what features should be used for this selection and what weighting may be applied to each. For illustrative purposes set of features that is typical of that used for highways are shown in the figure below.

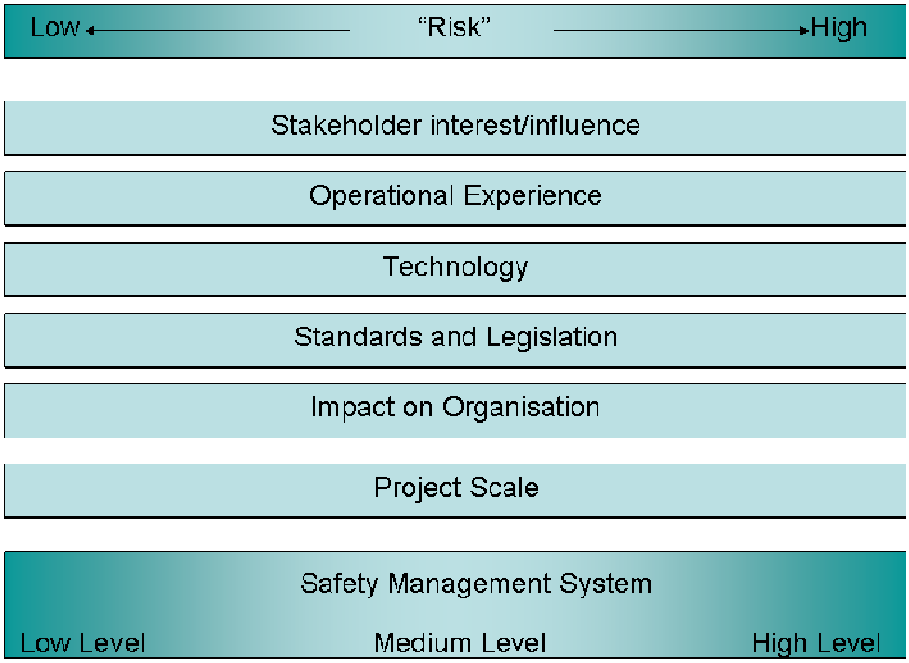

Figure 2: Typical features used to categorise a project's SMS requirements

Using appropriate definitions each feature can be categorised as being Low, Medium or High Level 'Risk', In this context risk mainly means safety risk but can mean other types of risk for example failure of the scheme due to public pressure or the risk of damage to the reputation of the Highway Authority implementing the scheme. Using a suitably agreed set of criteria, each is assessed as ranging from 'Simple' (least onerous), through 'Moderate' to 'Rigorous' (most onerous).

The features under consideration are presented in more descriptive detail below.

Feature
Stakeholder interest: The degree of interest that an individual or group have in the success of the project Stakeholders can be both internal and external. Internal stakeholders can be considered as those within the Highway Authority or contracted by them and associated operational staff. External Stakeholders are generally people outside the Highway Authority such as the emergency services, local authorities, breakdown support organisations and people who live nearby.
Operational experience: The degree of knowledge available from operating or running a similar project
Technology: Measure of technical novelty the project brings.
Standards and legislation: Consideration as to the applicability of current standards and legislation and to whether new standards or changes in legislation will be required.
Impact on Organisation: The effect that the project will have on the current organisational arrangements and in particular and changes in roles and responsibilities.
Project Scale: Consideration of the size of the project to be implemented.

Table 1: Project Features

Broadly speaking, the SMS chosen is that corresponding to the most popular category (e.g. mostly Medium Level means a 'Moderate' SMS). The choice of three potential outputs is essentially empirical and based on balance between providing sufficient choice in the type of SMS available and keeping the approach as simple as possible. The selected SMS indicates the safety activities that are necessary for a given project and the documented evidence that will need to be produced. The three types of SMS are summarised below:

- Simple – Existing standards capture sufficient safety management activities or specify requirements comprehensively enough to mean that little or no additional input is required.

- Medium – There is a requirement to go beyond the requirements of existing standards meaning that further safety management activities are required and activities may need to be carried out in more depth.

- Robust – All recognised aspects of a safety management lifecycle as given in standards such as IEC 61508 0 will need to be carried out.

It is noted that this moderate approach is that which is now being applied in England – following successful implementation of a number of 'Controlled Motorway', 'Active Traffic Management' and 'Managed Motorway' interventions on the strategic road network. Evidence from these schemes suggests safety advantages and decreased risk as a result of these interventions on the English motorway network.

5. SAFETY MANAGEMENT APPROACH

The previous section has described the need for an SMS that is appropriate for the scheme in question. While some activities are omitted from a Simple SMS that are required for a Rigorous SMS, changes in SMS mainly concern the complexity with which a particular activity is undertaken and the depth of analysis that must be carried out.

The key elements of an SMS are shown in the figure below.

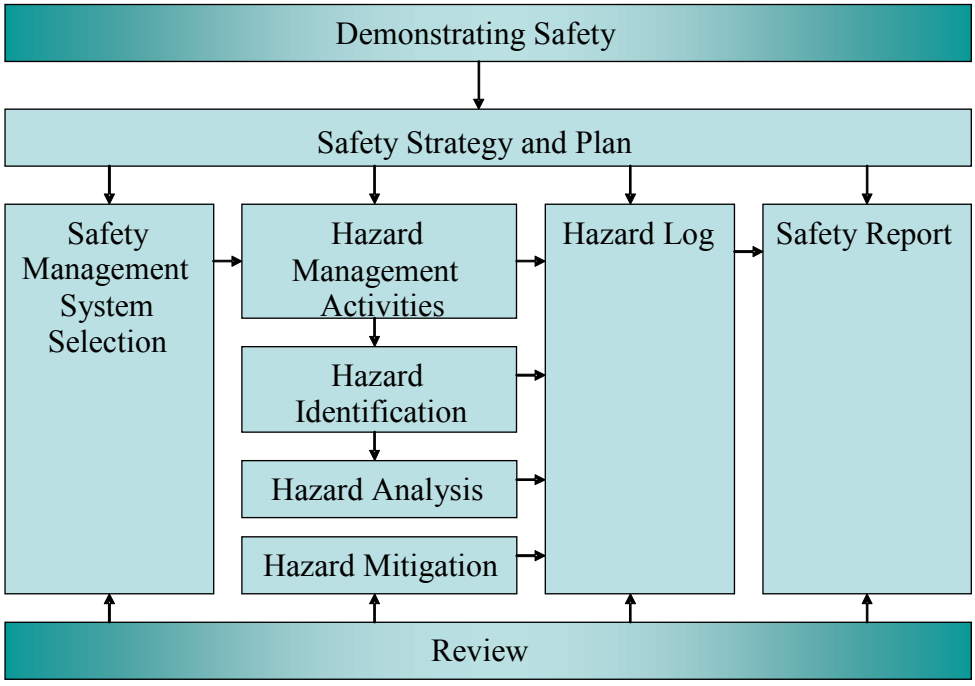

Figure 3 – Key Elements of an SMS

In addition these activities also need to fit in with the project-lifecycle. The figure below shows how the associated safety lifecycle matches up against a project development lifecycle. The stages will be recognised by those familiar with IEC61508 or similar such standards.

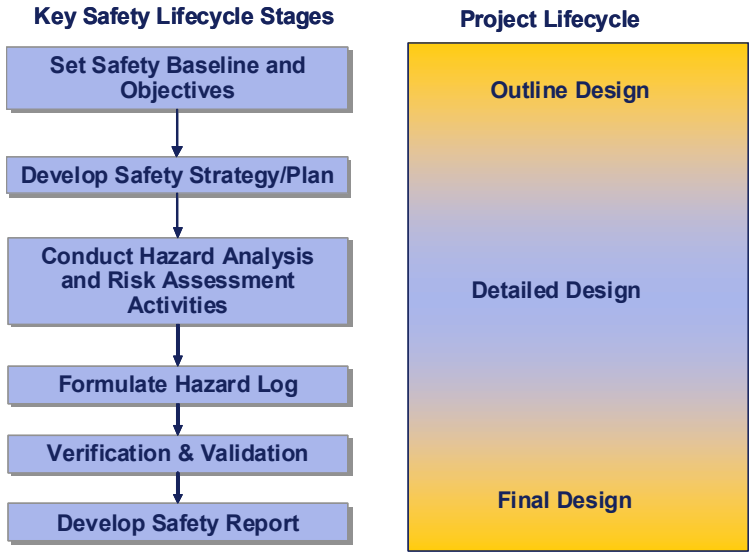

Figure 4: Safety activities and the project lifecycle

The key activities that need to be undertaken are:

5.1 Set Safety Baseline and Objectives

The Safety baseline will present the evidence to define and support the 'before' risk model / profile of the project. This will be used to assess the expected / predicted safety performance of intervention(s) proposed (the 'after' risk profile). Separate objectives are recommended for the road users and road workers. The road user objective proposed is that the scheme will aim to deliver either the same safety standard or an improvement in safety

5.2 Develop Safety Strategy and Plan

- to define an agreed approach for delivering the safety objectives of the project and define the safety activities that will be carried out throughout the project lifecycle.
- to provide a means of communicating and educating stakeholders how the project will approach safety, how it will achieve its safety objective and how the safety programme will be delivered.
- to Support the planning of safety activities and demonstrate that a defined safety management approach is being used. As such, it assists in the achievement of project safety objectives.

5.3 Hazard Analysis Activities and Risk Assessment

To identify potential hazards, their causes, risk level and to establish that appropriate mitigation is in place, or to identify additional mitigations where necessary.

5.4 Maintenance of a Comprehensive Hazard Log

All hazards that the project identifies are entered into the hazard log and are then tracked until closure. Closure of a hazard takes place once appropriate mitigations for this hazard have been demonstrated to be in place.

5.5 Verification and Validation

Safety requirements will need to be verified and assumptions validated.

5.6 Develop a Safety Report

A Safety Report is the document that summarises the evidence that a particular system is acceptably safety. The document should state the safety objective for the system and summarise how achievement of that target has been demonstrated.

It will also document how safety has been managed (processes and competent people) and how hazards have been mitigated.

Strong Documentary Records of all activities is required to ensure that evidence of all aspects of system safety is available throughout the system's life. This documentation needs to provide an audit trail of the safety activities carried out, so that, if required, an independent body could review the work and obtain a clear understanding of the activities that justify the achievement of the overall safety objective and the decision-making behind the selection, or rejection, of mitigation measures. Comprehensive records of activities and decisions are thus fundamental to the safety approach.

To provide a level of assurance about the safety decisions that are being undertaken, it is recommended that a **Safety Control Review Group** (SCRG) be established to review hazard risk level ranking and supporting information and guide the project strategy and approach to Operational Safety management. This group should consist of a cross-functional team that meets as required, with the aim of endorsing activities that have been undertaken by the project. The activities that the group will endorse are:

1. The identification and assessment of each significant hazard
2. The action plan to mitigate each significant hazard
3. Significant changes to the assessment of a hazard, or action plan
4. The closure of each significant hazard.

The group should be composed of representatives from the Project Team, the Highway Authorit, relevant specialists and consideration should be given to including relevant stakeholder representatives. A remit for this group would need to be developed, if this suggestion is supported. Such a group can present a productive forum to secure stakeholder buy-in (through engagement and involvement in the decision making process) – taking the contributors 'on the journey' to agreement / acceptance and support of the interventions proposed (particularly where complex or contentious issues arise).

To be able to provide sufficient detail, the descriptions given correspond mainly to a more rigorous This is only likely to be required for activities of the more innovative solutions that are being considered.

6. SET SAFETY BASELINE OBJECTIVES

The safety baseline identifies the level of safety against which the safety objective will be measured (i.e. in safety terms, what the scheme will be compared to). To do this it is necessary to have an understanding of the safety record of the existing highway (as covered by the scheme ‘extent) so that the safety record can be put into context.

All evidence and data that has been collected and analysed pertinent to the scheme area, together with details of relevant assumptions (and their basis) should be slearly set out and documented.

The introduction of the interventions proposed for this scheme will aim to deliver either the same safety standard or an improvement in safety.

Separate objectives are required for the road workers and road users. The need for separate objectives arises at least in part because of the different legal requirements that must be satisfied in most countries.

The principle that is applied for each project is based on the idea that globally the risk after project implementation will be at least equivalent (or better) than that which existed prior to implementation.

It is recommended that the safety baseline:

- Is scheme specific, i.e. the safety baseline for a specific scheme should be the section of highway where the scheme is going to be implemented

- Should include the average level of safety (e.g. measured as number of casualties, or Personal Injury Accidents (PIAs)) for the five-year period immediately before the implementation of any elements of ‘Active Traffic Management’. Where this information is not available, for whatever reason eg: due to major maintenance, the best available data should be used, e.g. shorter timescales, data for earlier time periods, data for comparable sections of highway or average data.

- Includes available operational data and evidence.

An analysis is being undertaken of the accident and casualty record on the links covered by the scheme based on data collected for the period up to 2009/10. The purpose of this analysis is to identify whether or not the accident or casualty rate deviates from the norm. If it is higher than the norm it may indicate the potential to reduce accidents and casualties still further. In addition there may be certain accident and casualty groups that may be more vulnerable at present that could be addressed (targeted) by the scheme.

7. DEVELOP SAFETY STRATEGY AND PLAN

The Safety Plan contains details of the safety objective of the project, the activities that will be undertaken to achieve this objective and the safety roles and responsibilities applicable.

As a project evolves so roles and responsibilities change and the level of detail with which specific activities can be described increases. Therefore the Safety Strategy and Plan should be regarded as an evolving document.

8. HAZARD ANALISYS AND RISK MANAGEMENT

These are the core activities of the SMS. As many approaches exist to identifying hazards and carrying out risk assessment, no specific approach is mandated, but certain requirements are placed on the process that is carried out, for instance to make sure that sufficient note is taken of previous work and that the necessary expertise is involved in hazard analysis activities.

The purpose of the hazard analysis is to identify potential hazards and the associated consequences. Once a hazard is identified, it can be mitigated. Through identifying hazards from an early stage and throughout the project, the design of the project can be modified to either remove hazards completely or reduce risks as soon as they are identified.

The hazard analysis process is iterative. Inevitably, new safety requirements will be derived as the system evolves. The necessary parts of the process should be repeated as the project design progresses and new functions and procedures require analysis.

This iterative nature of the hazard analysis process highlights the importance of an effective action tracking and hazard management system. Having such a process in place will increase confidence in the safety management of the system.

For Managed Motorway schemes in England, a Hazard Log Application has been developed and is made available to all. This web-browser based application is able to:

- list of all identified hazards,
- record the risk scores that apply to these hazards and any updates to these scores,
- record details of risk assessment activities carried out on the hazards and any updates to these risk assessments,
- record mitigations that are applied to each hazard, and
- record details of outstanding actions related to each hazard.

The Hazard Log Application is pre-populated with the incidents, hazards and causes that are known to be associated with Managed Motorway schemes.

An important function of the hazard log is to determine the level of risk associated with each hazard. To obtain these risk scores the risk measurement for each hazard is split into three parameters:

- frequency at which a hazard occurs,
- likelihood that a hazard will lead to an accident or collision, and
- consequences that arise from this collision.

Within the Hazard Log Application, scores are provided for the latter two parameters based on previous experience, although these can be changed if required to reflect local circumstances. As part of the scheme, there is a specific responsibility to check and complete the entry of the required information into the hazard log.

The Hazard Log Application can therefore be used to hold a record of the ‘before’ risk level and tracks progress with the predicted ‘after’ risk score, facilitating the quantitative aspect of the achievement of the safety objective.

A single project hazard log is recommended for adoption for each scheme for the following reasons:

1. A common approach across the project for tracking hazards
2. Hazards whose resolution requires interfacing between different parties can be more readily tracked
3. The current level of risk associated with the system can be identified from a single place.

The hazard log will need to be maintained throughout the lifetime of the project right through to decommissioning. Any substantial modifications to the design will require an appropriate level of analysis, and where new risks are identified or other levels change, these items will need to be documented in the hazard log. Finally, the decommissioning process itself will require examination to ensure that any risks associated with this process have been identified and adequately mitigated.

The hazard log process is shown in Figure 5 below.

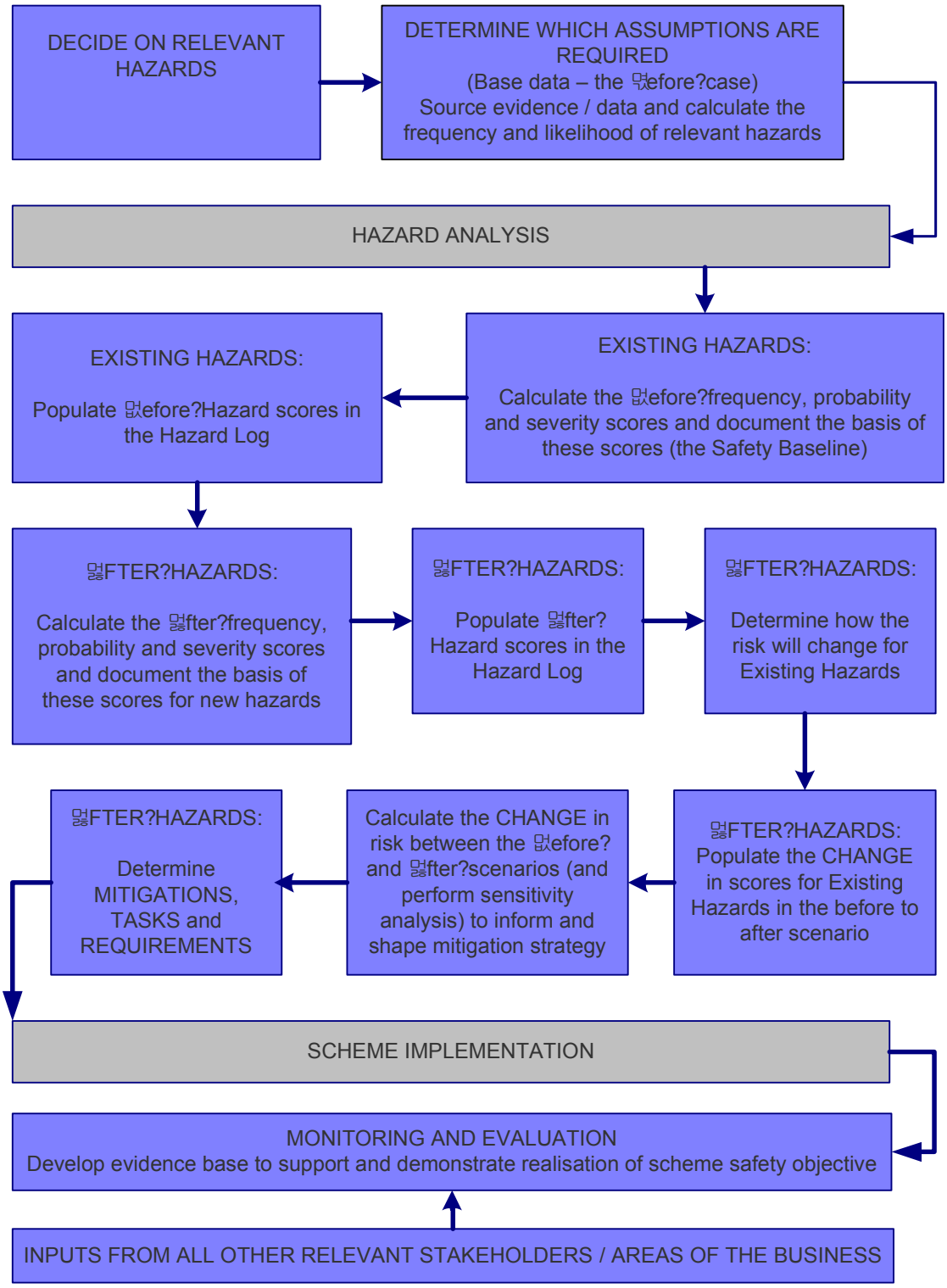

Figure 5: The Hazard Log Process

In terms of the 'After' scores, an anticipated risk profile should be prepared for each relevant intervention; this is shown in schematic form, for an illustrative scheme, in Figure 6 overleaf.

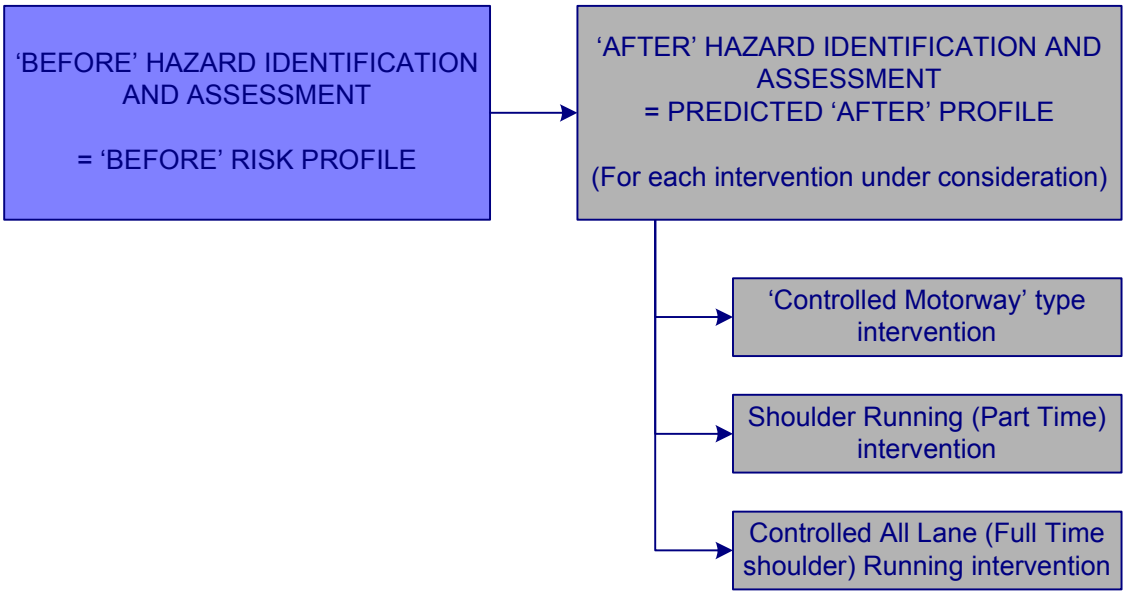

Figure 6: 'After' scoring for each proposed intervention (illustrative interventions shown)

A typical managed motorway (England) scheme risk profile is shown below.

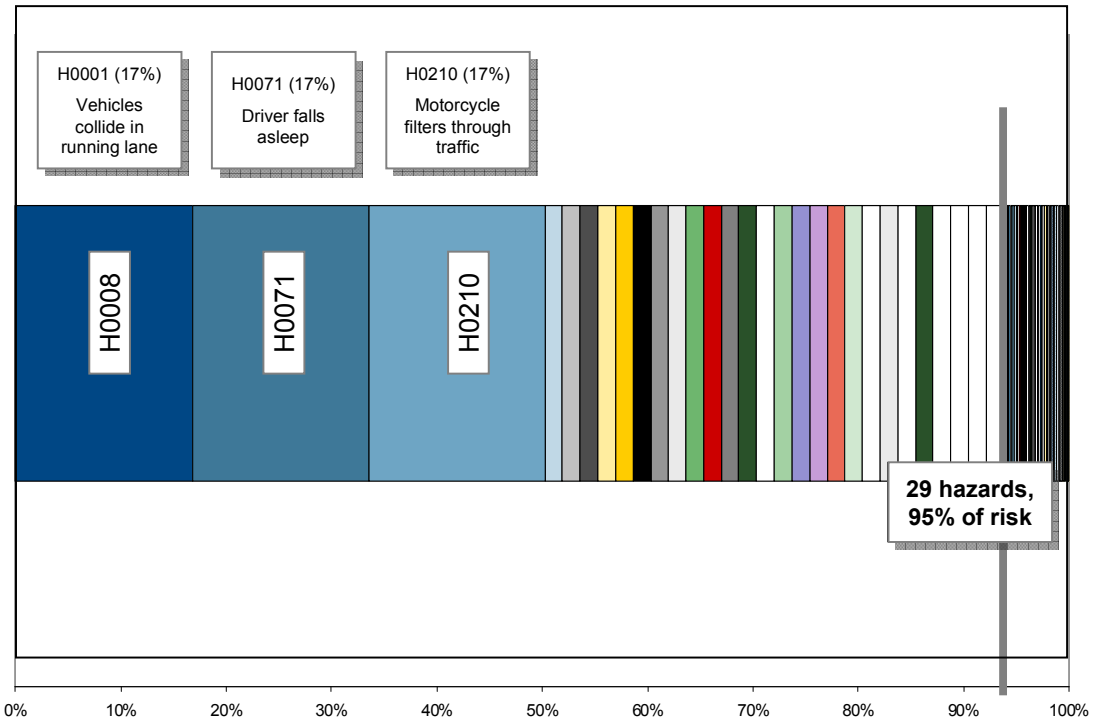

Figure 7 – typical scheme risk profile

9. VERIFICATION AND VALIDATION

The hazard analysis activities will identify a set of requirements that need to be fulfilled in order for the project to meet its safety objectives. These are the project's safety requirements. Prior to operation commencing it will be necessary to verify that these requirements have been fulfilled. Many will be verified through the testing and commissioning activities but others may require audit or

some other kind of review (for instance, making sure that appropriate training has been delivered where it is needed). Appropriate documentation of this verification will be required.

In completing risk assessment activities it is often necessary to make assumptions, for instance in regard to how road users will behave when the project becomes operational. Once operation has commenced, these assumptions need to be validated, generally through monitoring studies and incident recording. When such activities have been completed, and the associated assumptions validated, a project can really claim to have met its safety objectives.

10. SAFETY REPORT

The final deliverable that is produced to provide the evidence that a particular system is acceptably safety and that the project is likely to achieve its safety objective is the Safety Report. For a Simple SMS, such a document could be as brief as 2-3 pages. For a Rigorous SMS such a document will be significantly longer. This document is the equivalent of the Safety Case as described in IEC 61508 0 however is given a different title to reflect the range of safety projects that it is required to cover and to prevent confusion with the stricter definitions of a Safety Case that are applied in some other industry sectors.

The Safety Report provides a summary of all SMS activities carried out and need not repeat in detail information and arguments that are contained in other documents. However, the Safety Report should provide references to all such documents. It is likely that a report will be required at each major phase of the project as design is progressed and more detailed information becomes available.

11. MONITORING AND CONTROL

Once operation commences, the performance of the project must be monitored to ensure that information is obtained in respect of project performance and also to ensure that any necessary corrective action is undertaken. A procedure describing the monitoring and control actions will need to be developed. This procedure will need to define:

How monitoring will be carried out

The data that will be recorded

Who will be responsible for monitoring

The precise action that will be taken should monitoring identify a problem

A monitoring and control procedure will need to be developed in conjunction with those who will be responsible for maintenance. This procedure will be available before operation commences, allowing time for those responsible for its application to become familiar with it.

12. VERIFICATION AND VALIDATION

The hazard analysis activities undertaken within the SMS will identify a set of requirements that need to be fulfilled in order for the project to meet its safety objectives. These are the

project's safety requirements. Prior to operation, it will be necessary to verify that these requirements have been fulfilled. Many will be verified through the testing and commissioning activities, but others may require audit or some other kind of review (for instance, making sure that appropriate training has been delivered where it is needed). Appropriate documentation of this verification will be required.

In completing risk assessment activities it is often necessary to make assumptions, for instance in regard to how drivers will behave when the project becomes operational. Once operation has begun, these assumptions need to be validated, generally through monitoring studies and incident recording. When such activities have been completed, and the associated assumptions validated, a project can really claim to have met its safety objectives.

Results that have been obtained and verified to date on the M42 ATM Pilot scheme show that the results predicted match well with the reality of accident statistics.

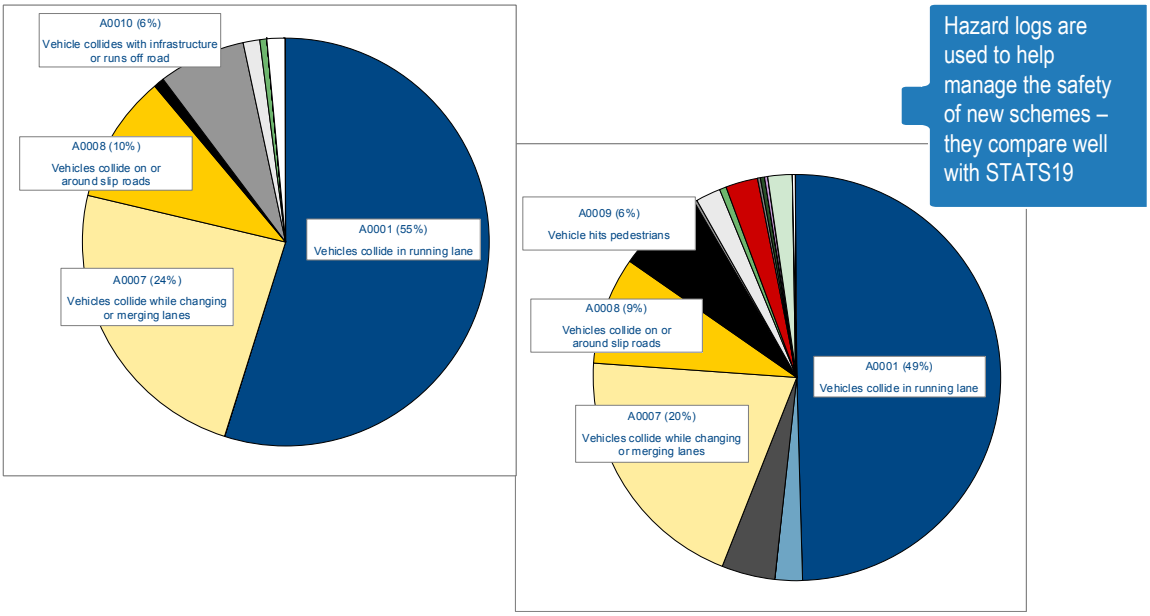

Figure 8 – M42 ATM Pilot - Results

13. SAFETY REPORT

The final deliverable that is produced to show that the safety objectives have been achieved is the 'safety report'. This provides a summary of all SMS activities carried out and need not repeat in detail information and arguments that are contained in other documents. However, the 'safety report' should provide references to all such documents. The process describing the approach to successful outcomes with respect to maintenance of safety is shown below.

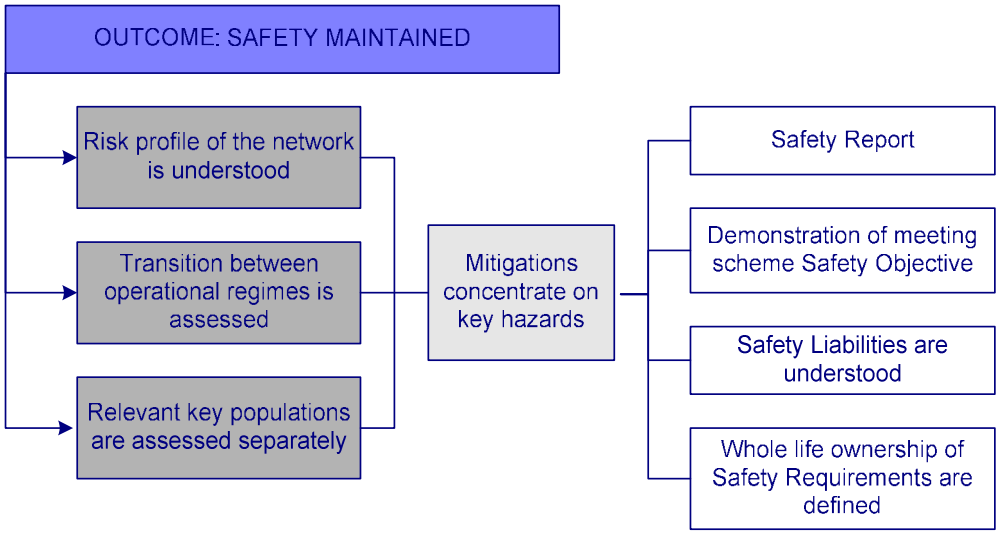

Figure 9 – Safety Maintained Outcome

CONCLUSIONS

For Managed Motorway schemes, an approach has been developed for ensuring that safety is appropriately managed. The highways specific nature of this approach is important. The highways sector has a different set of needs from other sectors so appropriate governing safety principles are needed. While most of these can be taken from existing standards, some highways specific measures are needed, thereby providing the flexibility to cover the range of safety related systems that are part of highways operation. The approach developed provides such flexibility and, while this paper summarises the basic details, there is considerably more to consider regarding the implementation of the SMS and Hazard Log Application.

Post-implementation monitoring of the first Managed Motorway scheme in the UK has demonstrated that it has provided a safer environment for road users and road workers (despite the need to maintain a greater level of equipment). The ‘safety objectives’ for the scheme have been attained, and in the case of road users exceeded. A more detailed analysis has been undertaken and will be reported in greater detail. The results indicate that the approach adopted for the management of safety is robust, and can lead to the safe implementation of complex systems and new ways of operation on the road network.