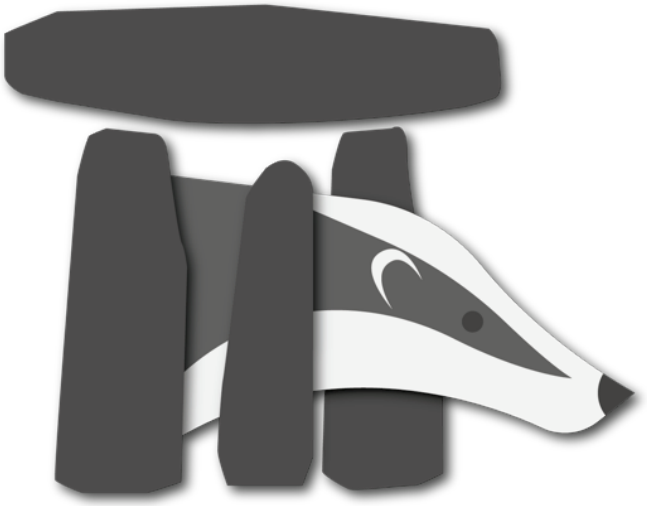


highways england

QS2B
Outline Minimum Operating Requirements

Contents

1 Introduction

1.1 General

Highways England has opened a tender period to Design, Build and Maintain contract for the A303 Stonehenge Tunnel.

Highways England requires that the contractor, when appointed, is focused on maximising the availability of the tunnel to road users. Tunnel availability is determined by the contractor meeting the Minimum Operating Requirements (MOR) which is based on safety performance and response to events in an appropriate and timely manner.

The MOR serves as a definitive minimum requirement that the Operator must not allow the tunnel and its approaches to fall below and for which a design approach and operation and maintenance strategy may be developed to avoid.

This document introduces the overarching approach to how MOR is determined (referred to as the Tunnel Safety Management System for A303 Tunnel) and describes the direct relationship between the tunnel systems and equipment, and their contribution to safety functions.

1.2 Purpose

The purpose of the work described in this report is to:

- Define the approach and framework for defining MOR; and
- Present a preliminary set of outline MORs at Tender Design for A303 Stonehenge Tunnel.

1.3 Approach

Team Badger (project team) is using previous experience from developing MORs based on key principles developed by them and other collaborators including Tunnel Operators.

At this stage (tender design), the full set of MORs for the A303 tunnel cannot be prepared because of uncertainty in the systems and equipment to be installed, and the overall contribution of those systems to the Safety Functions. Instead, this stage is focused on providing the structure, principles and outline of the Safety Functions and MORs based on the equipment required[1] that are to be included in the design. MOR shall be defined in consultation with the Tunnel Manager and Safety Officer (when appointed) and developed through the tender design and detailed design stages and subject to periodic review once the tunnel is operational.

In addition, to facilitate the tunnel safety management elements - such as fault events; fault likelihood; fault effects; mitigation actions; response time; recover time; and repair time - are considered for individual items of equipment but taking into consideration the individual element contribution to the overall safety level and safety function.

As there are aspects that will be developed as design evolves, not only during design stage but also construction, commissioning and subject to change once the tunnel is open and operating, the MOR document is considered a ‘live’ document that will require to be updated as tunnel systems/processes change.

The implementation of the MOR and Safety Functions will be supported through the programming of the tunnel monitoring and control systems, presentation to operators through SCADA, and through control room documentation. The challenge of refinement and

[1] Part 2-Design and Technical Requirements (Contract Version 1 – 28.04.22)

interpretation of complex processes (and agreements thereof) and the presentation of live operational documents in a way that provides the operator with a clear decision making process in the control room, is one which will be afforded appropriate attention in detailed design, following the framework set out in this document.

2 MOR concepts

2.1 Requirements

The Invitation to Participate in Dialogue (ITDP) (version 4) states, with regards the topic of this report:

Scope Area	Ref.	Quality submission/ Category	Requirements of quality submission	Required format and Allowable size	Key References (not limited to)
Tunnel Safety, Systems and Operations	QS-2B	Technical solution/ Outline Minimum Operating Requirements	4. Your *outline minimum operating requirements* shall provide a summary of the systems which are provided to maintain the safe operation of the tunnel.	Mandatory Maximum of twenty (20) sides at A4 size.	Volume 2 Part 2 (Design and Technical Requirements): Section 17, Section 18, Section 19, Section 20

With regards the design and Technical requirements in Volume 2 (version 3)-Section 19 paragraph 19.1.2 requires that MOR shall define:

- the systems[2] which maintain the safe operation of Stonehenge Tunnel;
- the minimum combinations of conditions, availability of systems and procedures for the safe continued operation of Stonehenge Tunnel (to be developed as design progresses);
- when a suspension or restriction in the operation of Stonehenge Tunnel (individual lane, bore or tunnel) is required (to be developed as design progresses) and;
- the actions to be undertaken in the event of a failure of a system (to be developed as design progresses).

Additional commentary on the MOR technical requirements are given throughout this document and in Appendix A.

2.2 General

The MOR establishes what is required for the tunnel to remain open and operational at an acceptable level of safety in relation to the baseline design level of safety. It does not define the baseline design level of safety (that is developed as part of the design); nor does it define a strategy for preventative or corrective action (that is developed as part of the operation and maintenance strategy).

The approach to maintaining safety levels above MOR should be considered from an early stage to include a combination of design for redundancy, reliability and resilience, and the development of strategy for rapid response and recovery from traffic incidents and equipment degradation or failure (events).

In the context of MOR, ‘events’ are anything that creates a threat to Safety Functions (e.g., if a fan is unavailable it doesn’t matter if it is unavailable due to a fault or a vehicle strike – the

[2] Tunnel systems can comprise any individual Device, Module and Service, including the TCMS, or combination thereof.

impact on safety is the same). The concept of safety functions is further explained in section 3.2 below.

2.3 Current practice

Guidance and standards exist for the development of tunnel design for operational safety (e.g. Highways England Standard CD352 and the EU Directive on Minimum Safety Requirements for Road Tunnels). However, no standards or guidance prescribe how to manage and respond to the degradation, failure or unavailability of systems, facilities or equipment that contribute to the tunnel's safety functions. There is no definitive standard that prescribes the point at which degradation or system failure is unacceptable; and there is no definitive standard that provides guidance on the acceptability or tolerability of safety risk associated with such system unavailability in road tunnels. The standard CD352 includes a note making reference to risk assessment which can be carried out to consider a set of hazard events on the continuity of the tunnel availability, including a development of MORs.

The process of deriving MORs is complex because of the scale of systems and procedures required for the safe operation of road tunnels and the inter-dependency between those systems and procedures. When a piece of equipment, a system, procedure, or other element of the tunnel operating condition fails or degrades, the impact on safety is not always clear and judgement is often required, resulting in the potential for uncertain or inconsistent outcomes.

For example, if a single zone of 25m of the fixed firefighting system (FFFS) is not operational, the impact on tunnel safety risk may not be obvious. Consideration is required of the arguably low likelihood of a fire occurring during the time of the outage, in that particular 25m zone and the potential consequences should that event occur. This then needs to be considered in the context of what other safety systems are available or can be made available to bridge any gap between the safety level in the tunnel with the zone not operational and the acceptable level of safety in the tunnel.

The MOR provides for systematic and immediate decision making (supported with information presented to operators through SCADA) based on an agreed and pre-established framework, thus minimising the need for judgement and debate at the time of an event that can create risk to users.

Pre-agreed MORs provide the tunnel Operator with a clear response action for events that could cause a safety derogation in the tunnel. In this way, the MOR serves as a definitive minimum requirement that the Operator must not allow the tunnel to fall below and for which an operation and maintenance strategy may be developed to avoid.

2.4 Tunnel Safety Risk

The failure or degradation of any element of equipment or system that has a contribution to a Safety Function has, by definition, an impact on safety.

Risk contribution figures (the level of safety scores) are proposed to be developed for the Tunnel Safety Management System (TSMS) for the A303 Stonehenge tunnel, as derived from a risk assessment process comprising:

- Judgement based on experience; and/or
- Qualitative risk assessment, where a systematic assessment of hazards and risk is required to demonstrate equivalence; and/or
- Quantitative risk analysis, where sufficient and suitable data are available for such analysis

The approach to the assessment of the safety impact of a degradation or failure is to:

- Judge, with common-sense and experience whether the degradation or loss of functionality is clearly offset, or compensated for, by the functionality of another element of equipment already in place, or processes that could be put in place. If this is the case, no further risk analysis is required to be undertaken and the compensation levels can be defined in the TSMS through the level of safety scores. This may be the case, for example, if a section of the tunnel's CCTV has failed but is also covered by video incident detection cameras which may be supplemented with increased operator vigilance to demonstrate equivalence. The challenge here, for example, would be to ensure that a process by which the video detection system may be seamlessly brought in to compensate for the loss of CCTV without major further works or modifications.
- Judge, with the aid of risk analysis data (qualitative or quantitative) whether the degradation or loss of functionality is counter-balanced by an alternative risk reducing measure that may be put in place. This may be the case, for example, if the PA/VA system has failed (not available in all tunnel zones), causing a quantifiable increase in risk of a certain quantum of theoretical statistical fatalities per year, then a counter-balancing risk reduction may be required by implementing a mitigation measure (e.g. speed limit reduction with lane closure) that causes a quantified decrease in risk of fatalities per year (under the circumstances of the system failure or degradation under assessment) that is of a higher quantum than the increase caused by the PA/VA degradation.

Where risk reduction figures are quantified and form part of the TSMS (in Appendix A), these are to be initially derived as described above to inform discussion and review by the Tunnel Manager (TM) and Safety officer (TSO), the TDSCG if appropriate, and those involved with tunnel operations when appointed. MOR will be refined and finalised throughout the project to ensure that their implementation drives the required outcomes, in terms of Highways England's aim to appropriately focus the project on tunnel safety and availability.

2.5 Risk Transfer

Where full/partial tunnel closure is implemented, the potential transfer of risk from the A303 Stonehenge Tunnel to an alternative route, or to a single bore in contraflow, needs to be considered.

Traffic diverted from the A303 Stonehenge Tunnel as a result of closure of both bores (i.e. no contraflow) may be reasonably expected to re-direct to route options that include local diversion routes via the A360/The Packway/A345, regional routes via Salisbury and strategic diversion routes via M4/ M5.

Tunnel safety risk may be considered to be proportional to traffic flow volumes so, in terms of overall network safety risk, the increase in risk on the alternative route due to the additional traffic, will need to be carefully considered.

3 MOR process

3.1 Key principles

The key principles defined in this Section 3 have been derived to establish the framework for MORs. These are illustrated with examples from the Tunnel Safety Management System (TSMS) developed for the A303 Stonehenge Tunnel under these principles.

When a piece of equipment, a system, procedure, or other element of the tunnel operating condition fails or degrades, the impact on safety is not always clear and judgement is often required, resulting in the potential for uncertain or inconsistent outcomes.

Pre-agreed MORs provide the Operator with a clear response action for events that could cause a safety derogation in the tunnel, without recourse to protracted deliberation and

uncertainty on the action required. In this way, the MOR serves as a definitive minimum requirement that the Operator must not allow the tunnel to fall below and for which an operation and maintenance strategy may be developed to avoid.

The MOR may be defined as the level at which all the tunnel's **Safety Functions** continue to be met. Key safety functions are as follows:

- Overall, critical tunnel functioning;
- Maintain Safe Driving Conditions;
- Maintain operator visual coverage and information;
- Maintain ability to alert tunnel users of an incident requiring their evacuation;
- Maintain ability to facilitate and manage a safe evacuation; and
- Maintain ability to facilitate effective emergency services intervention.

There are a number of safety sub-functions beneath these top level functions.

Figure 1 below illustrates some of the principles of MORs adopted by the Badger Team, illustrating the proposed commitment to the maintenance of *safety*, at the same time as maximising *availability*. where the green line represents the normal operation safety level and the red one is the minimum operating requirement safety level. Between these lines, the tunnel is in a degraded operation area but is above the MOR and may continue to operate. Below the red line, the tunnel is below the minimum operating safety level and the tunnel needs to be closed.

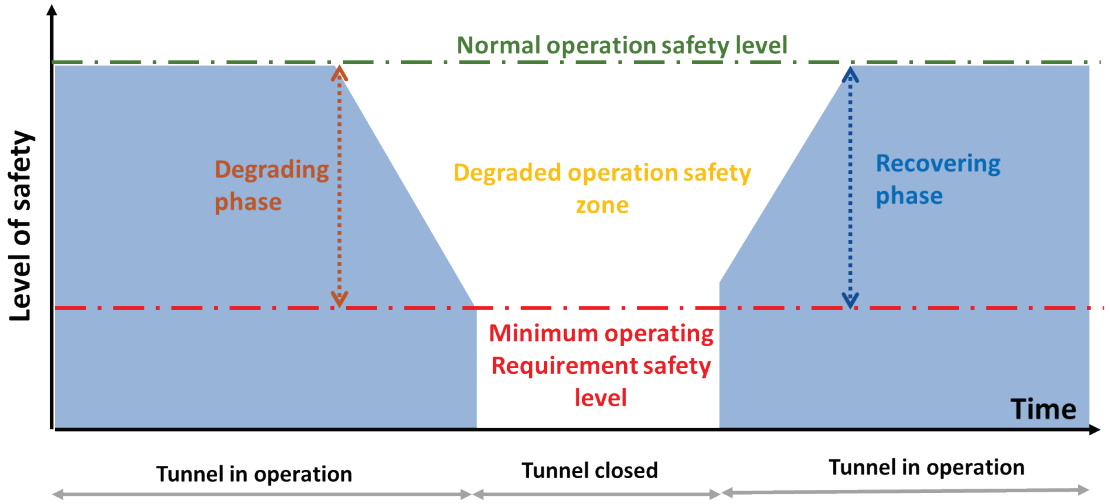


Figure 1 Illustration of MOR principle

There are scenarios where there may be a sudden loss of safety function e.g. a complete power loss, meaning that MORs are breached much sooner in which case procedures are required to be in place to enable a prompt closure of the tunnel (Figure 2), or a prompt evaluation of the situation to inform a decision on whether to close, or to mitigate risk. For these scenarios, the focus of attention is on minimising the likelihood of such a sudden loss through design for resilience and appropriate redundancy.

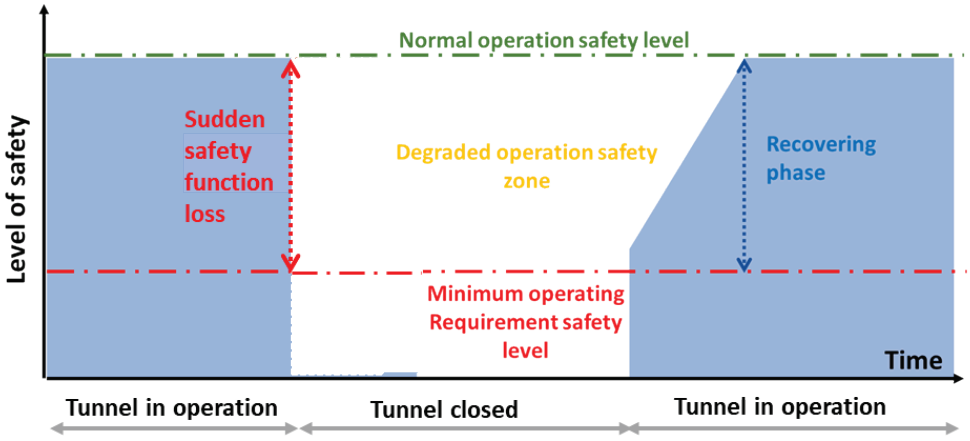


Figure 2 Sudden system failure

3.2 Safety Functions

The MOR may be defined as the level at which all the tunnels Safety Functions continue to be met. Key top-level safety categories consist of the following:

- Global systems;
- Manage incident likelihood;
- Incident detection; and
- Manage incident consequence.

Within each safety category are defined top-level Safety Functions (SFs), and within each SF a range of safety sub-functions (SSFs) are defined. At the same time under each safety sub-function there are different items of equipment, systems, facilities and/or procedures that support that sub-function (and perhaps other sub-functions). See Figure 3 below:

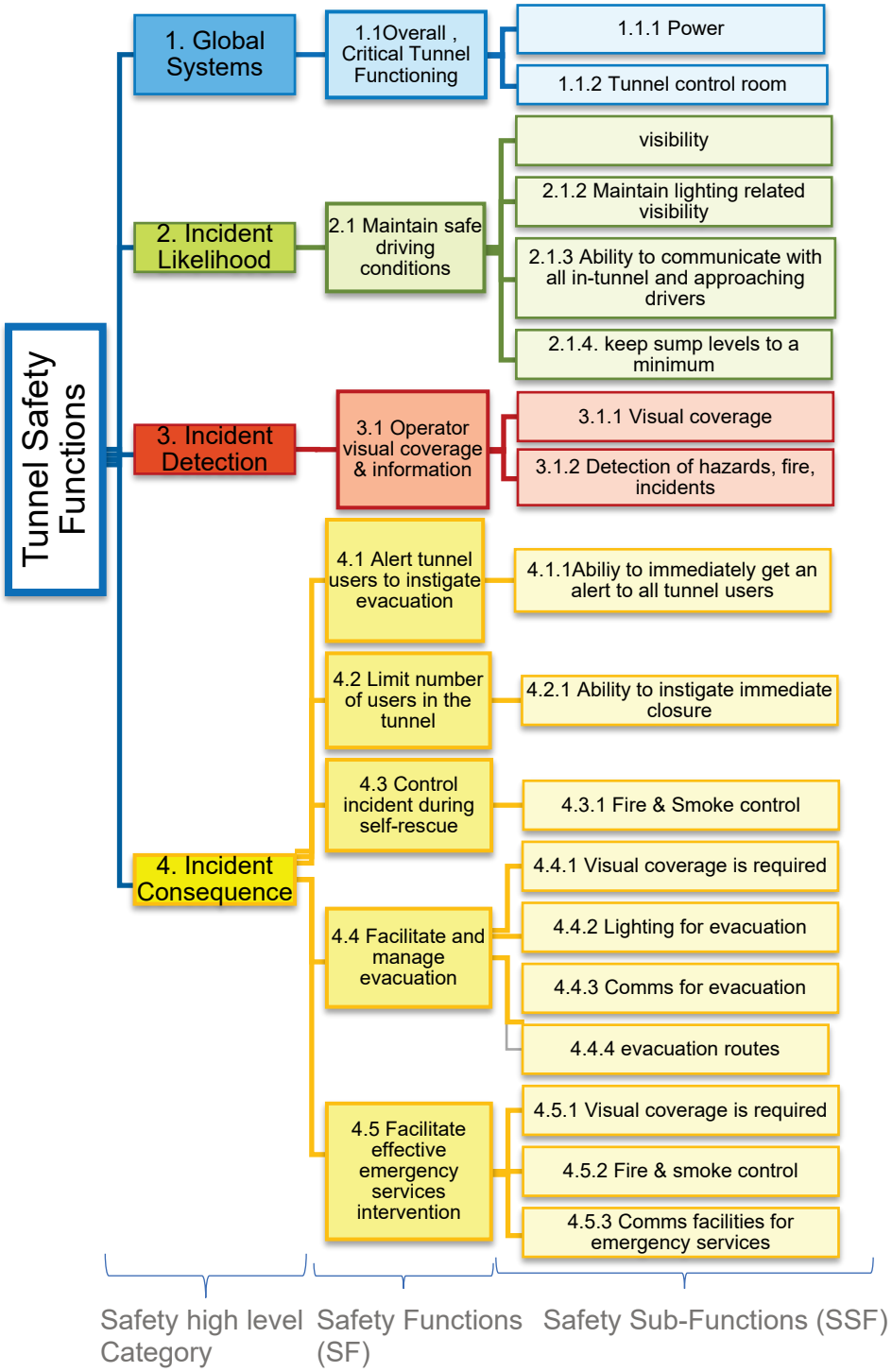
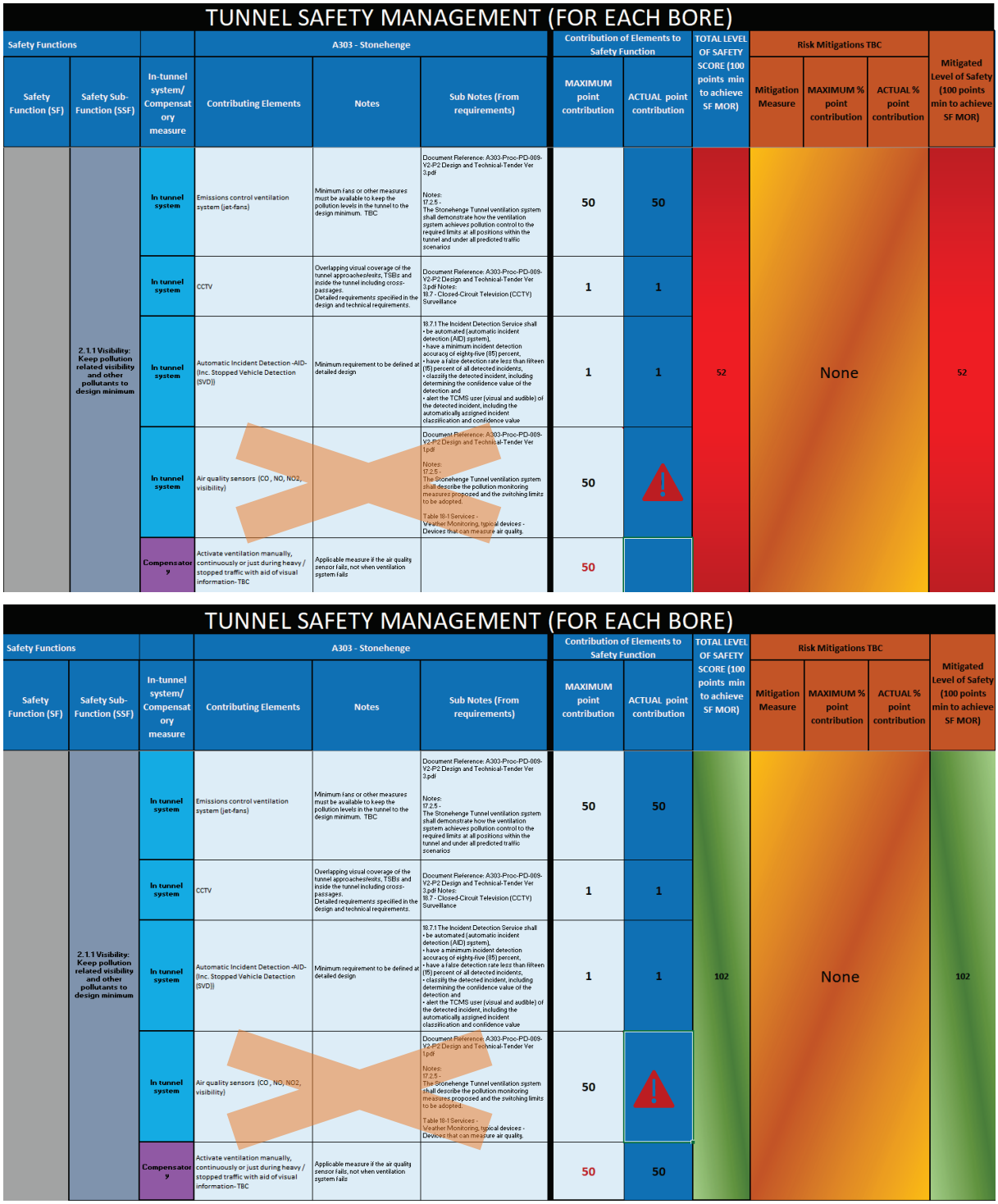


Figure 3 Safety categories, functions and sub-functions for MOR definition.

3.3 MOR process

The MOR is applied to the Safety Functions, rather than to specific items of equipment or systems. This means that a system or item of equipment may degrade or fail but if the relevant Safety Function is being achieved by other equipment or systems, then the MOR may not necessarily be breached (**TQ2C2.1** led by our Design Manager).

An illustrative, simplified example as a snapshot of the MOR Table is given in the Figure below where the Air Quality sensor has failed; affecting *SSF 2.1.1 Maintain pollution related visibility* and therefore affecting *SF 2.1 Maintain safe driving conditions*. It can be observed that the tunnel should be closed to public because the level of safety is less than 100 points. However, if a compensatory measure is applied, in this case, manual activation of the ventilation system (50 points), a level of safety above the MOR (102 points) is recovered.



TUNNEL SAFETY MANAGEMENT (FOR EACH BORE)

Safety Functions			A303 - Stonehenge			Contribution of Elements to Safety Function		TOTAL LEVEL OF SAFETY SCORE (100 points min to achieve SF MOR)	Risk Mitigations TBC			Mitigated Level of Safety (100 points min to achieve SF MOR)
Safety Function (SF)	Safety Sub-Function (SSF)	In-tunnel system/ Compensatory measure	Contributing Elements	Notes	Sub Notes (From requirements)	MAXIMUM point contribution	ACTUAL point contribution		Mitigation Measure	MAXIMUM % point contribution	ACTUAL % point contribution	
	2.1.1 Visibility: Keep pollution related visibility and other pollutants to design minimum	In tunnel system	Emissions control ventilation system (jet-fans)	Minimum fans or other measures must be available to keep the pollution levels in the tunnel to the design minimum. TBC	Document Reference: A303-Proc-PD-009-V2-P2 Design and Technical-Tender Ver 3.pdf Notes: 17.2.5 - The Stonehenge Tunnel ventilation system shall demonstrate how the ventilation system achieves pollution control to the required limits at all positions within the tunnel and under all predicted traffic scenarios	50	50	52	None			52
		In tunnel system	CCTV	Overlapping visual coverage of the tunnel approaches/exits, TSBs and inside the tunnel including cross-passages. Detailed requirements specified in the design and technical requirements.	Document Reference: A303-Proc-PD-009-V2-P2 Design and Technical-Tender Ver 3.pdf Notes: 18.7 - Closed-Circuit Television (CCTV) Surveillance	1	1					
		In tunnel system	Automatic Incident Detection -AID- (Inc. Stopped Vehicle Detection (SVD))	Minimum requirement to be defined at detailed design	18.7.1 The Incident Detection Service shall • be automated (automatic incident detection (AID) system), • have a minimum incident detection accuracy of eighty-five (85) percent, • have a false detection rate less than fifteen (15) percent of all detected incidents, • classify the detected incident, including determining the confidence value of the detection and • alert the TCMS user (visual and audible) of the detected incident, including the automatically assigned incident classification and confidence value	1	1					
		In tunnel system	Air quality sensors (CO , NO, NO2, visibility)		Document Reference: A303-Proc-PD-009-V2-P2 Design and Technical-Tender Ver 1.pdf Notes: 17.2.5 - The Stonehenge Tunnel ventilation system shall describe the pollution monitoring measures proposed and the switching limits to be adopted. Table 18-1 Services - Weather Monitoring, typical devices - Devices that can measure air quality.	50						
		Compensatory	Activate ventilation manually, continuously or just during heavy / stopped traffic with aid of visual information- TBC	Applicable measure if the air quality sensor fails, not when ventilation system fails		50						

TUNNEL SAFETY MANAGEMENT (FOR EACH BORE)

Safety Functions			A303 - Stonehenge			Contribution of Elements to Safety Function		TOTAL LEVEL OF SAFETY SCORE (100 points min to achieve SF MOR)	Risk Mitigations TBC			Mitigated Level of Safety (100 points min to achieve SF MOR)
Safety Function (SF)	Safety Sub-Function (SSF)	In-tunnel system/ Compensatory measure	Contributing Elements	Notes	Sub Notes (From requirements)	MAXIMUM point contribution	ACTUAL point contribution		Mitigation Measure	MAXIMUM % point contribution	ACTUAL % point contribution	
	2.1.1 Visibility: Keep pollution related visibility and other pollutants to design minimum	In tunnel system	Emissions control ventilation system (jet-fans)	Minimum fans or other measures must be available to keep the pollution levels in the tunnel to the design minimum. TBC	Document Reference: A303-Proc-PD-009-V2-P2 Design and Technical-Tender Ver 3.pdf Notes: 17.2.5 - The Stonehenge Tunnel ventilation system shall demonstrate how the ventilation system achieves pollution control to the required limits at all positions within the tunnel and under all predicted traffic scenarios	50	50	102	None			102
		In tunnel system	CCTV	Overlapping visual coverage of the tunnel approaches/exits, TSBs and inside the tunnel including cross-passages. Detailed requirements specified in the design and technical requirements.	Document Reference: A303-Proc-PD-009-V2-P2 Design and Technical-Tender Ver 3.pdf Notes: 18.7 - Closed-Circuit Television (CCTV) Surveillance	1	1					
		In tunnel system	Automatic Incident Detection -AID- (Inc. Stopped Vehicle Detection (SVD))	Minimum requirement to be defined at detailed design	18.7.1 The Incident Detection Service shall • be automated (automatic incident detection (AID) system), • have a minimum incident detection accuracy of eighty-five (85) percent, • have a false detection rate less than fifteen (15) percent of all detected incidents, • classify the detected incident, including determining the confidence value of the detection and • alert the TCMS user (visual and audible) of the detected incident, including the automatically assigned incident classification and confidence value	1	1					
		In tunnel system	Air quality sensors (CO , NO, NO2, visibility)		Document Reference: A303-Proc-PD-009-V2-P2 Design and Technical-Tender Ver 1.pdf Notes: 17.2.5 - The Stonehenge Tunnel ventilation system shall describe the pollution monitoring measures proposed and the switching limits to be adopted. Table 18-1 Services - Weather Monitoring, typical devices - Devices that can measure air quality.	50						
		Compensatory	Activate ventilation manually, continuously or just during heavy / stopped traffic with aid of visual information- TBC	Applicable measure if the air quality sensor fails, not when ventilation system fails		50	50					

Figure 4 Illustration of MOR principles for sudden system failure. a) Contributing element failure; b) compensatory measure in place.

The following principles are required to be followed for Safety Function based MORs. The focus of these principles is to provide the level of safety required (by legislation and standards, and a level expected by society) whilst maintaining maximum availability:

- The MOR is considered to reflect the minimum level of safety accepted by tunnel users so if the tunnel is below its MOR (100 points) then it should not normally be open to traffic;
- If a system failure or unavailability results in a Safety Function not being fully met (100 points), then measures are required to offset that degradation and provide equivalence in order to remain above MOR for that Safety Function;
- The availability of some tunnel systems will compensate for other tunnel system failures, either fully or in part where Safety Functions are performed by several systems. Compensatory systems may enable the tunnel to stay above the MOR;
- Where insufficient compensatory systems are in place, additional mitigation (if available for that safety function) will be required to provide the equivalent level of safety to stay above MOR;
- The equivalence of compensatory or mitigation systems may be established and demonstrated through common sense, qualitative risk assessment or more detailed quantitative risk analysis where appropriate;
- Compensating and/or mitigating systems should be available and implemented immediately in order that MOR is not breached and the tunnel can remain open; and

Action to close the tunnel should be preceded by appropriate prior consideration of the potential transfer of risk from the tunnel route to an alternative route.

3.4 Compensation and Mitigation

In the event of a degradation in tunnel operation such that the normal operating state no longer applies, the Minimum Operating Requirements (MOR) process needs to be invoked so that any risks associated with the degradation or failure are compensated or mitigated such that tunnel safety levels can be maintained, and the tunnel can be kept open in some capacity.

Compensatory measures may be defined as a measure or a combination of measures that in the event of a degradation, provide adequate coverage to maintain equivalent user safety levels, as shown in Figure 4 above.

Additional 'mitigation measures' may be applied if the compensation measures alone do not provide for equivalent levels of safety. Mitigation Measures here are distinct from Compensatory Measures by virtue of their impact on traffic and users such that some form of restriction is required on the Tunnel. In this way, 'mitigation measures' are, by definition, more impactful than compensation measures, and are therefore considered more as a 'last resort' to maintaining safety and availability under extreme circumstances.

Mitigation measures may be, for example:

1. Speed limit reduction (reduce likelihood and consequences of incidents); and

2. Tunnel lane closure (reduce traffic volumes and therefore risk, e.g., by batching traffic)[3]
3. Traffic restrictions (reduce vehicle size and fire size potential or exclude vehicles transporting larger number of users, e.g., buses).

The process involves the identification of Safety Functions being delivered by tunnel systems, the identification of where and when Compensatory Measures are available due to availability of other systems and where Mitigation Measures can be put in place in the event that Compensatory Measures are not available or not adequate to fully compensate for the loss of functionality due to the degradation. More detail of suggested systems, compensation and mitigation measures are presented in Appendix A.

3.5 Fault events and response times

Fault categories are defined by the project requirements into three categories (red, amber, green). These are shown and defined below.

Fault category	Definition
A	Stonehenge tunnel cannot be operated safely (breach of MOR). Major faults/ system deficiencies or complete loss of functionality of the system.
B	Stonehenge Tunnel can be opened safely (above but approaching MOR). Fault/ system deficiencies resulting in limited or no redundancy in the system. Further faults would result in MOR being breached.
C	Stonehenge Tunnel can be operated safely (above MOR). Small number of minor faults/system deficiencies which do not affect the redundancy of the system of safe operation of the tunnel.

Fault event elements are proposed to be incorporated into the MOR as follows:

- Safety system: This first step will consider the potential deficiency in the individual safety system (i.e., mechanical, electrical or other and these can range from minor fault to complete system loss);
- Mitigation and compensation actions: The second step evaluates the available mitigation and compensation measures (if any) and further updates the overall safety function fault (post mitigation). If mitigation/compensation measures for a specific safety function are available, then the tunnel safety management will provide visibility of time scales to implement such measures and confirmation of follow up actions.
- Lastly, the time to permanent repair (and removal of mitigation when the safety function is fully restored, see Figures 1 and 2) is provided.

This approach is illustrated in Figure 5 below:

[3] Within the context of MORs, the only reason for a single lane closure through the tunnel would be to reduce traffic throughput in order to reduce risk. This is a mitigation for increased risk due to a system failure or degradation (subject to verification and agreement in this measure as a reasonable risk reduction measure during consultation). It is not intended that this be for repair of the system failure.

Step 1 (individual safety system)

Step 2 (compensation/mitigation action , repair times)

System	Safety Functions	Other systems	Element of system	Failure cause		Failure likelihood	Effect of failure	CAT of fault (no mit)	Mitigation/ compensation & Action	Category of fault (with mit)		Time to fault diagnosis (& implement mitigation)	Further action	Time to stage 1 recovery / impl. mitigation	Time to permanent repair (or removal of mitigation)
TVS	Safety Functions: SF 2.2 SF 4.3 SF 4.5	-FFFS -Fire systems -Pollution sensors -Water systems -Others	1 Fan (or small number of fans within redundancy provision)	Elec	1		Reduced ventilation capacity	C	Enable redundant fan(s) Fault diagnosis Schedule repair	C	1	1 week	TBC	1 month	Within normal fan maintenance schedules
					2						2				Within next set of 2 or 3 closures
					3						3				Urgent repairs / replacements in next closure
					4										
				Mech	1										
					2										
					3										
					4										
				Comm.	1										
					2										
					3										
					4										
			Multiple Fans (beyond redundancy)	Elec	1		Reduced ventilation capacity beyond minimum	A	Apply mitigation measure (e.g., speed limit, lane closure, HGV diversion, DGV diversion; other ops measures) Other systems available Fault diagnosis Schedule repair	B (if Safety Functions are met)	1	2hrs (implement mitigation)	Manage mitigation performance	4hrs (decide whether to close)	Urgent repairs / replacements in next closure
											2				Urgent repairs / replacements in next closure
				Mech	2						3				Special closure required
				Comm	3				No mitigation available Fault diagnosis Schedule repair	A (if SF cannot be verified)	1	2hrs	CLOSE TUNNEL (unless mitigation can be implemented to change category to B)	TBC Tunnel is CLOSED	Special closure required
											2				Special closure required
											3				Special closure required
			All Fans	Elec	1		No ventilation capacity	A		A	1				Special closure required
				Mech	2						2				Special closure required
				Comm	3						3				24hrs

Subject to detailed design

Subject to consultation

Figure 5 Illustration of process for implementation of fault event response within MOR context

Figure 5 above illustrates the two-step approach for a potential failure within the main tunnel ventilation system. It is noted the tunnel ventilation system serves three safety sub-functions:

- maintain pollution control,
- fire and smoke control during self-rescue stage, and
- fire and smoke control for emergency services intervention.

Failure in the ventilation system could affect one fan or a small number of fans within redundancy provision, in which case may be considered as acceptable (*GREEN* zone, as the safety function is still fulfilled), actions are generated to trigger repair and timescale requirements.

When multiple fans (beyond redundancy levels) fail this (when unmitigated) would constitute a MOR breach (*RED* zone), triggering a series of actions and timelines to: a) get the fault rectified and b) verify whether other mitigation and compensation measures are available for *all the safety functions* covered by the ventilation system.

There may be certain circumstances whereby a compensating system is not available (e.g., a power failure resulting in loss of ventilation and the FFFS) in which case a breach of the safety function and therefore MOR would require actions for a controlled tunnel closure (in this case under safe conditions ensured by UPS protection of key systems).

4 The Tunnel Safety Management System (TSMS) and application to the A303 Stonehenge Tunnel

4.1 Implementation

A developing TSM Table with figures included that relate to the project team design is given in Appendix A, with examples of compensation measure approach given in Figure 4 above. This Appendix A table shows the full range of functions for which systems, equipment and procedures are required to be provided in order that they be fulfilled and meet the “100 point” level of acceptability.

As the design develops, this MOR / Safety Function process will guide the design development and options evaluation with a focus on operability and resilience. The ‘scores’ for various systems contribution to Safety Function may be derived through:

- Workshops with the participation of stakeholders; and
- Further risk assessment / analysis for various degraded states.

The contributing systems identified are required to be fully operational to their minimum Safety Requirement in order to contribute to the Safety Function(s).

With reference to the TSMS in Appendix A, the following points define the process for establishing the MORs:

- The aim of the TSMS table is to define the operational actions to be taken depending on the system failure and provide an immediate picture of tunnel safety status (normal, degraded operations, or MOR breach) as described in section 3.5 above. These actions would be pre-agreed and then distilled into operational systems and protocols for automatic or simple implementation. Some of the actions may require increased operational vigilance (if agreed) or in the case of tunnel closure, specific protocols to be followed (e.g., does a sudden power loss require immediate closure? Is the power likely to be returned by the time a closure could be implemented?)
- Safety Functions are defined in the first three columns of the Table, based on project team experience and knowledge of tunnel safety good practise.

- The Contributing Systems to each Safety Function are identified. These may include systems that are defined as specific requirements (e.g., CCTV) and those that may be defined as compensation measures that may be deployable by the Operator (purple shaded cell on the left, e.g., increased operator vigilance)
- Each tunnel system contributes to the level of safety score for the relevant Safety Function. If the Safety Requirement is met (i.e., if the system is meeting the minimum requirement), the contribution of that system to the level of safety score is the agreed total figure identified in the relevant column of the TSMS. This figure may then be entered into the 'Actual contribution' column for that system. If the Safety Requirement for the relevant System is not met, due to degradation or failure of that System, then the 'Actual contribution' must be set to zero. The contribution figures are derived from a process as described in Section 2.3 and may be 'tuned' to reflect the agreed and verified level of safety performance.
- The Safety Requirement is the derived minimum requirement for the System to meet the overall design requirement and specification for the System, less any redundancy. As an example, if the Emergency Tunnel Ventilation jet fan design requirement is to meet the standard which prescribes a certain level of redundancy and the design includes, for example, twenty six (26) fans plus a further two (2) to allow for maintenance redundancy, then the overall design may provide twenty eight (28) fans but the Safety Requirement in the TSMS is for twenty six (26) fans only.
- The sum of contributions for every Safety Function must be at least 100. If the aggregate Level of Safety Score is greater or equal to 100, then the tunnel is operating at or above its MOR.
- If the aggregate Level of Safety Score is less than 100, then the tunnel is below its MOR and Mitigation Measures should be applied if the tunnel is to remain open (as illustrated in Figure 4b).
- Mitigation Measures offer opportunity for the (Mitigated) Level of Safety Score to be brought up to the minimum figure of 100 by implementing, for example, speed reduction or lane closure. These mitigations are available only for selected Systems and are provided contribution figures derived from a risk assessment process as described in Section 3.4.
- Where the two Mitigation Measures are combined (both implemented) their combined contribution may not be the sum of their individual contributions to the (Mitigated) Level of Safety Score. The contribution figures for the combination of mitigation measures are given in the TSMS as derived from a risk assessment process to be developed once mitigation measures are agreed.
- If the aggregate (Mitigated) Level of Safety Score is less than 100, then the tunnel is below its MOR and the tunnel should be closed.
- As the design further develops this will require scoring in agreement with the tunnel manager, tunnel safety officer and relevant approval teams.
- If the aggregate (Mitigated) Level of Safety Score is greater or equal to 100, then the tunnel is operating at or above its MOR as long as the Mitigation Measures remain in place and are verified as operational (as illustrated in Figure 4).
- In some instances, determining the contribution to a SSF will depend on whether equipment failure is full or partial, e.g.:
    - For the Emergency Ventilation System, the contribution to the Level of Safety Score reduces in steps as the number of fans available reduces. These steps will be further developed in final design. The contribution figures for the steps are derived from a risk assessment process.
    - For the Fixed Fire Fighting System (FFFS), the contribution to the Level of Safety Score reduces in steps as the number of suppression zones available reduces.
- The TSMS Table, when complete for the as-developed Contributing Systems for the Project will be used as a basis for the logic to be programmed into TCMS to provide visual and audible (fault category A or B) alarm and warning of system degradation and consequent risk of MOR breach. In addition, operational procedures will need to be

developed for MORs and actions to be taken in case of failure of equipment that reflect TSMS tables.

- The TSMS tables also include system and safety function overall faults, repair aspects and actions to be taken in relation to the aspects presented and described in section 3.5 above. Some of these are subject to detailed design (such as defining failure likelihood for specific causes of failure) while others are subject to consultation when the design progresses during next stage.

4.2 Next steps

This report provides a preliminary outline set of MORs for the A303 Stonehenge Tunnel. At the next stage (detailed design development), this MOR / Safety Function process will guide the design development with a focus on operability and resilience. The 'scores' for various systems contribution to Safety Function may be derived through:

- Workshops with the participation of the tunnel stakeholders (this will include Tunnel Manager and Tunnel Safety Officer when appointed);
- Further risk assessment / analysis for various degraded states;
- Fault categorisation before and after compensatory/mitigation measures are in place;
- Timelines to repair faults and implement compensation/mitigation measures.
- Refinement of specific actions to be taken depending on nature of element failure or when closure is required what actions need to take place.

With regards 'scores', mitigations and compensation measures given in Appendix A, these are given for illustration purposes and will need discussion and agreement with stakeholders involved with the tunnel safety (e.g., TM, TSO, TDSCG).

Appendix A- Tunnel Safety Management System Table sample for Safety functions

The Appendix below shows a selection of examples of safety sub-functions which are proposed to be further developed as design progresses.

With reference to Figure 3 above, safety sub-functions included within appendix A are within incident consequence management 4.3.1 Fire and smoke control (during self-rescue phase); 4.1.1. Ability to immediately get an alert to tunnel users, and 4.4.3 communications for evacuation.

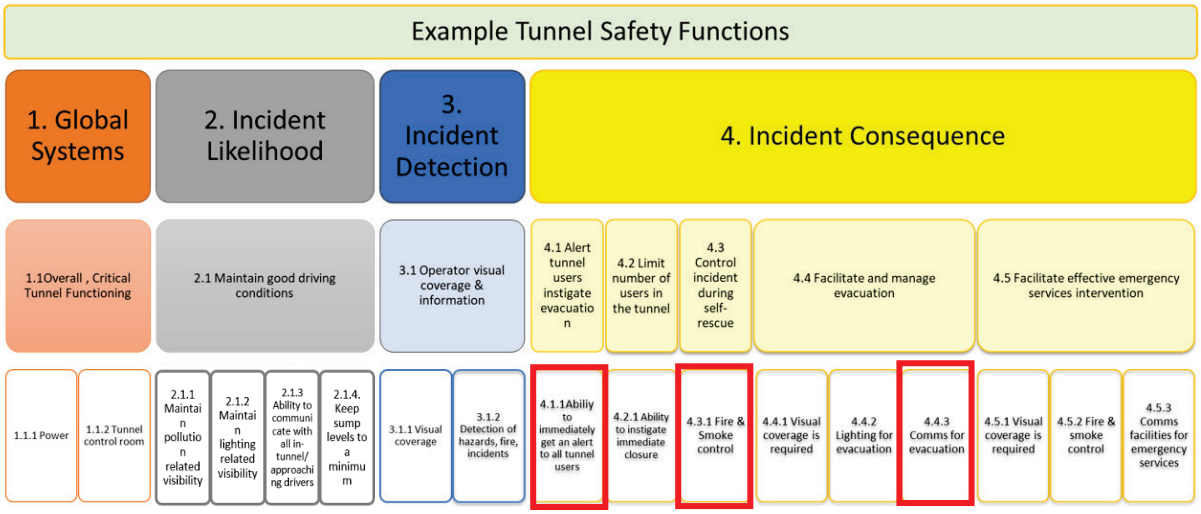


Figure 6 Tunnel safety management Functions presented in Appendix A.

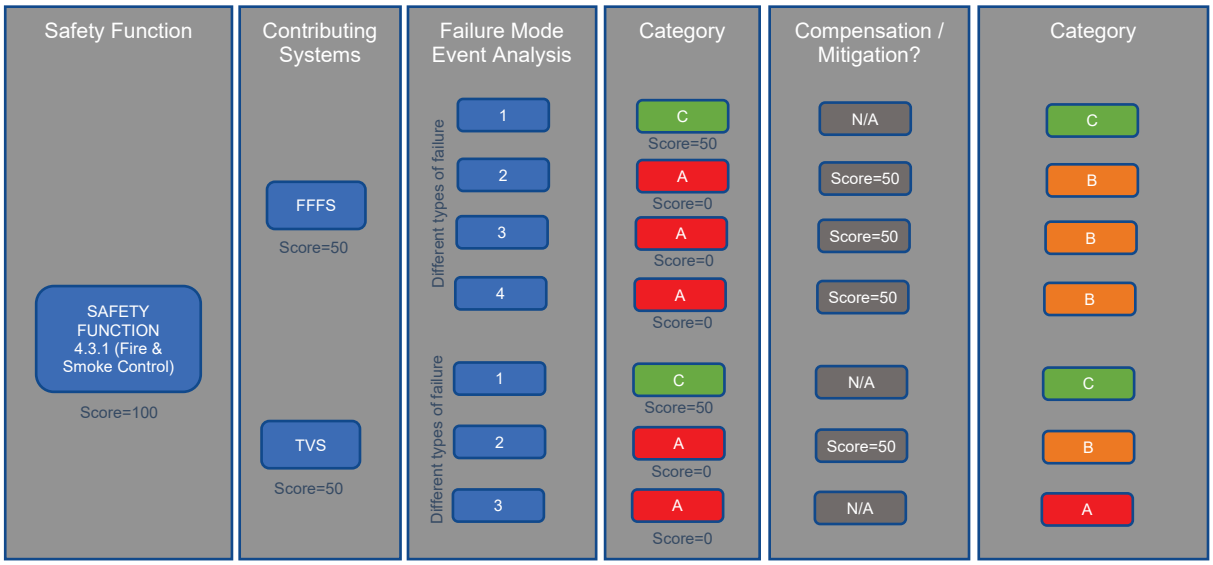


Figure 7 Schematic representation of the logic in the Tables below for the 'Fire and Smoke Control' safety sub-function.

Safety Functions					A303 - Stonehenge							Risk Mitigations TBC									Mitigated Level of Safety (100 points min to achieve SF MOR)
Top Level	Safety Function (SF)	Safety Sub-Function (SSF)	In-tunnel system/ Operational Compensatory measure	System	Contributing Elements and level 1 failure	Failure cause	Likelihood	Effect of failure on Safety Function	CATEGORY OF FAILURE (No compensation or mitigation)	MAXIMUM point contribution due to failure	ACTUAL point contribution For the system	Mitigation Measure	MAXIMUM % point contribution	ACTUAL % point contribution	Action (s)	CATEGORY (with compensation /mitigation)	Time to fault disgnosis (& Implement mitigation)	Further action	Time to stage 1 recovery/imp mitigation	time for permanent repair (or removal of mit)	
Contribution of Systems, compensatory measures and mitigation measures indicated below are illustrative. Scoring to be done in detail Design following TM/TSO input HE final approval																					
4. Incident Consequence	4.3 Control incident during self-rescue phase	4.3.1 Fire & smoke control for potential design fire	In tunnel system	FFFS	Number of pumps up to redundant levels	Electrical / Mechanical / Communications / Miscellaneous	1–4	Reduced capacity/resilience, still able to deal with Design Fire	C	50	50	N/A	N/A		Enable redundant pump Verify other systems available (TVS) Fault diagnosis Schedule repair	C	1 2 3 4	1 week	TBC	1 month	Within normal fan maintenance schedules Within next 2 or 3 closuress Urgent repairs / replacements in next closure	100
					Multiple pumps> redundancy	Electrical / Mechanical / Communications / Miscellaneous	1–4	Reduced capacity, performance of the FFFS is not complied with	A	0		advisory speed limit reduction- TBC Lane closure TBC HGV-restriction TBC	30 30 50		Implement mitigation measure of HGV restriction Verify other systems available (TVS) Fault diagnosis Schedule repair	A	1 2 3 4	2 hr	CLOSE TUNNEL (unless mitigation can be implemented to change category to B)	TBC Tunnel is closed	Special closure required (24 hs)	
					one section valve	Electrical / Mechanical / Communications	1–4	Risk of FFFS underperforming should the fire occur within the affected zone	A	20		advisory speed limit reduction- Lane closure TBC HGV-restriction TBC	30 30 50		Implement mitigation measure of advisiory speed Verify other systems available (TVS) Fault diagnosis Schedule repair	B (if safety funtions are met) A (if safety	1 2 3 4 1 2	2 hr (implement mitigation) 2 hr	Manage mitigation/ Compensation performace CLOSE TUNNEL (unless mitigation can	4 hours (decide whether to close) TBC	Urgent repairs / replacements in next closure Special closure required	

Safety Functions					A303 - Stonehenge							Risk Mitigations TBC									
Top Level	Safety Function (SF)	Safety Sub-Function (SSF)	In-tunnel system/ Operational Compensatory measure	System	Contributing Elements and level 1 failure	Failure cause	Likelihood	Effect of failure on Safety Function	CATEGORY OF FAILURE (No compensation or mitigation)	MAXIMUM point contribution due to failure	ACTUAL point contribution For the system	Mitigation Measure	MAXIMUM % point contribution	ACTUAL % point contribution	Action (s)	CATEGORY (with compensation /mitigation)	Time to fault dignosis (& Implement mitigation)	Further action	Time to stage 1 recovery/imp mitigation	time for permanent repair (or removal of mit)	Mitigated Level of Safety (100 points min to achieve SF MOR)
4. Incident Consequence	4.3 Control incident during self-rescue phase	4.3.1 Fire & smoke control for potential design fire	In tunnel syste	FFFS		Miscellaneous	1									funtion is not met)	3	2 hr	be implemented to change category to B)	Tunnel is closed		100
							2										4				
							3														
							4														
					Multiple section valves	Electrical	1	Greater Risk of FFFS underperforming should the fire occur within the affected zone (s), greater risk of fire spreading to other vehicles	A	0		advisory speed limit reduction-	30		Implement mitigation measure of HGV restriction	A	1	2 hr	CLOSE TUNNEL (unless mitigation can be implemented to change category to B)	TBC	Special closure required (24 hs)	
							2					Lane closure TBC	30		Verify other systems available (TVS)		2					
							3					HGV-restriction TBC	50		Fault diagnosis		3			Tunnel is closed		
							4								Schedule repair							
						Mechanical	1										4					
							2														
							3														
							4														
						Communications	1														
							2														
							3														
							4														
						Miscellaneous	1														
							2														
							3														
							4														
					lumber of fans up to redundant levels	Electrical	1	Reduced capacity, still able to deal with Design Fire	C	50	50	N/A	N/A		Enable redundant fan	C	1	1 week	TBC	1 month	Within normal fan maintenance schedules	100
							2								Verify other systems available (FFFS)		2				Within next 2 or 3 closuress	
							3								Fault diagnosis		3				Urgent repairs / replacements in next	
							4								Schedule repair		4					
						Mechanical	1															
							2															
							3															
							4															
						Communications	1															
							2															
							3															
							4															
						Miscellaneous	1															
							2															
							3															
							4															
			In tunnel system	TVS	Multiple fans > redundancy	Electrical	1	Reduced capacity, smaller fire	A	40		advisory speed limit reduction-	30		Aply mitigation measure	B (if safety function is met)	1	2 hr (implement mitigation)	Manage mitigation/ Compensation performace	4 hours (decide whether to close)	Urgent repairs / replacements in next closure	
							2					Lane closure TBC	30				2					
							3					HGV-restriction TBC	50		Verify other systems available (FFFS)		3				Special closure required	
							4								Fault diagnosis		4					
						Mechanical	1								Schedule repair							
							2															
							3															
							4															
						Communications	1								No mitigations/ comp available	A (if safety	1		CLOSE TUNNEL (unless mitigation can	TBC		
							2										2					
							3															
							4															

Safety Functions					A303 - Stonehenge								Risk Mitigations TBC									Mitigated Level of Safety (100 points min to achieve SF MOR)
Top Level	Safety Function (SF)	Safety Sub-Function (SSF)	In-tunnel system/ Operational Compensatory measure	System	Contributing Elements and level 1 failure	Failure cause		Likelihood	Effect of failure on Safety Function	CATEGORY OF FAILURE (No compensation or mitigation)	MAXIMUM point contribution due to failure	ACTUAL point contribution For the system	Mitigation Measure	MAXIMUM % point contribution	ACTUAL % point contribution	Action (s)	CATEGORY (with compensation /mitigation)	Time to fault disgnosis (& Implement mitigation)	Further action	Time to stage 1 recovery/imp mitigation	time for permanent repair (or removal of mit)	
4. Incident Consequence	4.3 Control incident during self-rescue phase	4.3.1 Fire & smoke control for potential design fire	In tunnel system	TVS		Miscelaneous	1									Fault diagnosis Schedule repair	function is not met)	3	2 hr	be implemented to change category to B)	Tunnel is closed		
							2											4					
					All fans	Electrical	1									No mitigations/ comp available Fault diagnosis Schedule repair		1	2 hr	CLOSE TUNNEL (unless mitigation can be implemented to change category to B)	TBC	Special closure required (24 hs)	100
							2											2					
							3																
							4																
						Mechanical	1											3			Tunnel is closed		
							2																
							3		No capacity	A	0						A						
							4											4					
						Communications	1																
							2																
							3																
							4																
						Miscelaneous	1																
							2																
							3																
							4																
					Fire extinguisher			Required by standard CD352				N/A (minor impact on MOR)											

Safety Functions					A303 - Stonehenge							Risk Mitigations TBC									Mitigated Level of Safety (100 points min to achieve SF MOR)
Top Level	Safety Function (SF)	Safety Sub-Function (SSF)	In-tunnel system/ Operational Compensatory measure	System	Contributing Elements and level 1 failure	Failure cause	Likelihood	Effect of failure on Safety Function	CATEGORY OF FAILURE (No compensation or mitigation)	MAXIMUM point contribution due to failure	ACTUAL point contribution For the system	Mitigation Measure	MAXIMUM % point contribution	ACTUAL % point contribution	Action (s)	CATEGORY (with compensation /mitigation)	Time to fault disgnosis (& Implement mitigation)		Further action	Time to stage 1 recovery/imp mitigation	time for permanent repair (or removal of mit)	
4. Incident Consequence	4.1 Alert tunnel users to instigate evacuation	4.1.1 Ability to immediately get an alert to all tunnel users - see also 4.4.3 Comms for evacuation from potential design fire	In tunnel system	Public service radio rebroadcast	Number of failures up to redundant levels (technology dependent)	Electrical 1		Reduced capacity/resilience, still able to communicate with in-tunnel users	C	50	130	N/A	N/A		Enable redundant failing element Verify other systems available (PAVA) Fault diagnosis Schedule repair	C	1	1 week	TBC	1 month	Within normal maintenance schedules	130
						Electrical 2											2				Within next 2 or 3 closures	
						Electrical 3											3				Urgent repairs / replacements in next closure	
						Electrical 4											4					
						Mechanical 1																
						Mechanical 2																
						Mechanical 3																
						Mechanical 4																
						Communications 1																
						Communications 2																
						Communications 3																
						Communications 4																
						Miscelaneous 1																
						Miscelaneous 2																
						Miscelaneous 3																
						Miscelaneous 4																
					Number of failures > redundancy levels (technology dependent)	Electrical 1		Reduced capacity/resilience, performance of radio rebroadcast is not complied with	A	0		advisory speed limit reduction- TBC	50		Implement mitigation measure of advisiory speed Verify other systems available (PAVA) Fault diagnosis Schedule repair	B (if safety functions are met)	1	2 hr (implement mitigation)	Manage mitigation/ Compensation performace	4 hours (decide whether to close)	Urgent repairs / replacements in next closure	
						Electrical 2											2				Special closure required	
						Electrical 3											3					
						Electrical 4											4					
						Mechanical 1																
						Mechanical 2																
						Mechanical 3																
						Mechanical 4																
						Communications 1																
						Communications 2																
						Communications 3																
						Communications 4																
						Miscelaneous 1																
						Miscelaneous 2																
						Miscelaneous 3																
						Miscelaneous 4										A (if safety function is not met)	1	2 hr	CLOSE TUNNEL (unless mitigation can be implemented to change category to B)	TBC Tunnel is closed	Special closure required (24 hs)	
																	2					
																	3					
																	4					
					Number of failures up to redundant levels (technology dependent)	Electrical 1		Reduced capacity/resilience, still able to communicate with in-tunnel users	C	80		N/A	N/A		Enable redundant Verify other systems available (Radio re-broadcast) Fault diagnosis Schedule repair	C	1	1 week	TBC	1 month	Within maintenance schedules	
						Electrical 3											2				Within next 2 or 3 closuress	
						Electrical 4											3					
						Mechanical 1																
						Mechanical 2																
						Mechanical 3																
						Mechanical 4																
						Communications 1																
						Communications 2																
						Communications 3																

Safety Functions					A303 - Stonehenge								Risk Mitigations TBC										Mitigated Level of Safety (100 points min to achieve SF MOR)
Top Level	Safety Function (SF)	Safety Sub-Function (SSF)	In-tunnel system/ Operational Compensatory measure	System	Contributing Elements and level 1 failure	Failure cause		Likelihood	Effect of failure on Safety Function	CATEGORY OF FAILURE (No compensation or mitigation)	MAXIMUM point contribution due to failure	ACTUAL point contribution For the system	Mitigation Measure	MAXIMUM % point contribution	ACTUAL % point contribution	Action (s)	CATEGORY (with compensation /mitigation)	Time to fault dignosis (& Implement mitigation)	Further action	Time to stage 1 recovery/imp mitigation	time for permanent repair (or removal of mit)	
4. Incident Consequence	4.1 Alert tunnel users to instigate evacuation	4.1.1 Ability to immediately get an alert to all tunnel users - see also 4.4.3 Comms for evacuation from potential design fire	In tunnel system	Public adress voice alarm	Number of failures	Commun	3											3					130
							4											4			Urgent repairs / replacements in next closure		
						Miscellaneous	1																
							2																
							3																
							4																
					Number of failures > redundancy levels (technology dependent)	Electrical	1		Reduced capacity/resilience, performance of public address voice alarm system is not complied with	A	0		advisory speed limit reduction- TBC	50		Implement mitigation measure of advisiory speed limit reduction Verify other systems available (Radio re-broadcast) Fault diagnosis Schedule repair	B (if safety funtions are met)	1	2 hr (implement mitigation)	Manage mitigation/ Compensation performace	4 hours (decide whether to close)	Urgent repairs / replacements in next closure	
							2											2					
							3											3					
							4											4			Special closure required		
						Mechanical	1											1	2 hr	CLOSE TUNNEL (unless mitigation can be implemented to change category to B)	TBC Tunnel is closed	Special closure requlred (24 hs)	
							2										A (if safety funtion is **not** met)	2					
							3											3					
							4											4					
						Communications	1																
							2																
							3																
							4																
						Miscellaneous	1																
							2																
							3																
							4																
			Compensatory	TBC-process in place																			