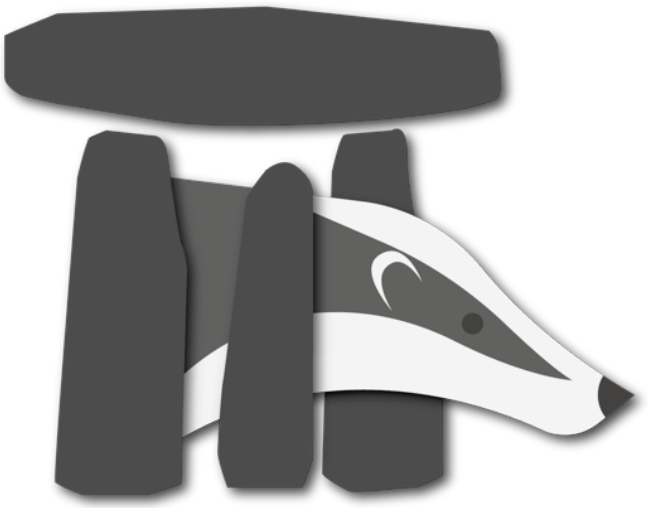

highways england

# QS2C TCMS Solutions Document

# Contents

**1.0 Introduction** ..... 1
2.0 The architecture of the TCMS ..... 3
2.1 Approach to achieving required Availability ..... 4
2.2 Implementation of the core operating functions ..... 6
2.3 Standards and protocols to be used ..... 7
2.4 Integration with The Client's National TCMS ..... 7
2.5 Integration with The Client's systems T-TOC, Dynac and ControlWorks; ..... 7
2.6 Resilience and self-recovery ..... 8
2.7 Identification of any single points of failure in the Services, Modules or Devices; ..... 9
2.8 Proposed user interface; ..... 9
2.9 Remote execution of updates and upgrades ..... 12
3.0 Implementation of TCMS functional and non-functional requirements ..... 12
4.0 TCMS security measures ..... 14
4.1 Approach to security risk management; ..... 14
4.2 Proposals for protection, including network security controls, zones, boundary controls and malware and malicious activity; ..... 14
4.3 Authentication and management of users and user profiles ..... 15
4.4 Configuration of user profiles ..... 16
4.5 Implementation of system configuration and hardening measures ..... 17
4.6 Testing for weaknesses is to be undertaken, including scope of test; ..... 17
4.7 Management and monitoring of Security Incidents ..... 17
5.0 Approach to compliance with the Client's procedures and policies ..... 18
6.0 Approach to compliance with the Clients Architecture Services Principles ..... 19
7.0 The software schedule, provided using Quality Submission Template D (Software Schedule) ..... 20

## 1.0 Introduction

The Tunnel Control and Management System (TCMS) will provide Stonehenge Tunnel operators with full control, monitoring, recording, reporting and service implementation of the services required to safely and efficiently operate the Stonehenge Tunnel. The TCMS will provide operator positions at:

- the Highways England South West ROC at Aztec West (primary operating centre);
- the Highways England South East ROC at Godstone (resilient operating centre); and
- the Tunnel Services Buildings (local operating centres).

The locations where the TCMS is to be operated from will be provided with, as a minimum, the Technology Equipment shown in the table below:

| Location | Minimum Technology Equipment |
|---|---|
| South west ROC | Five (5) No. individual operator desks with three (3) screens per terminal.<br>Video wall (CCTV, TCMS alarms, integrated M&E health, asset performance and faults). |
| South east ROC | Two (2) No. individual operator desk with three (3) screens per terminal. |
| TSB (each building) | Two (2) No. individual operator desk with three (3) screens per terminal.<br>Video wall (CCTV, TCMS alarms, integrated M&E health, asset performance and faults). |

The requirements of the video wall provided in the South West ROC as part of the TCMS operational capability will be:

- determined based on the TCMS operational requirements;
- determined in consultation with the Client;
- agreed with the Project Manager.

The local TCMS hardware will be located within the TSBs and a TCMS testing environment will be provided. The TCMS testing environment will be sandboxed (i.e. isolated from the outstation equipment) with simulated field equipment to facilitate testing.

The TCMS will enable the Client to deliver the following core operating functions:

- monitor and manage the Services; Modules and Devices;
- normal operation (including the passage of dangerous goods vehicles);
- implement diversion routes;
- manage prohibited users; livestock and wildlife;
- accommodate the safe movement of abnormal loads;
- facilitate the management of large-scale public events;
- monitor and manage the environmental conditions in Stonehenge Tunnel;
- monitor and manage the effects of weather conditions;
- monitor Stonehenge Tunnel and the tunnel approach road traffic conditions;
- manage speed of traffic;
- detect stopped vehicles within Stonehenge Tunnel;
- manage lane availability in Stonehenge Tunnel and on the approaches to the tunnel;
- support safe maintenance and emergency service access;
- communicate with Road Users;
- implement a contraflow in the non-affected bore during maintenance;

- safely manage incidents and clear vehicles from the network;
- prevent traffic from entering an individual bore of Stonehenge Tunnel in the event of an incident;
- quickly close an individual bore or complete closure of Stonehenge Tunnel;
- give advance warning to Road Users of an incident and bore / closure of Stonehenge Tunnel.

The TCMS will configure and implement the Minimum Operating Requirements (MOR) and will trigger alerts when:

- the MOR are breached;
- the number of failures or a condition is being approached which would result in the MOR being breached.

| 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 operated safely (above but approaching MOR). Faults / 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 or safe operation of the tunnel. |

Minimum Operating Requirements fault categories

The TCMS will be designed for high availability, using redundancy, diversity and automatic recovery, to allow the Client's lane availability targets to be met. Whilst a thorough functional safety analysis has yet to be carried out, analysis of similar systems has required similar TCMS to meet integrity levels between SIL1 and SIL2. As a result, the Stonehenge TCMS will achieve an availability in excess of 99.9%

## 2.0 The architecture of the TCMS

The Tunnel Control and Management System will provide a fully redundant facility to control all tunnel functions. It will be implemented using distributed processing and a highly resilient Internet Protocol (IP) network. As per clause 18.2 in the Design and Technical Requirements document, the TCMS will be connected to its operators using the Client's NRTS Telecommunications Service Provider. The high-level functional block diagram of the proposed TCMS is shown in Figure 1 Stonehenge TCMS functional Block Diagram:

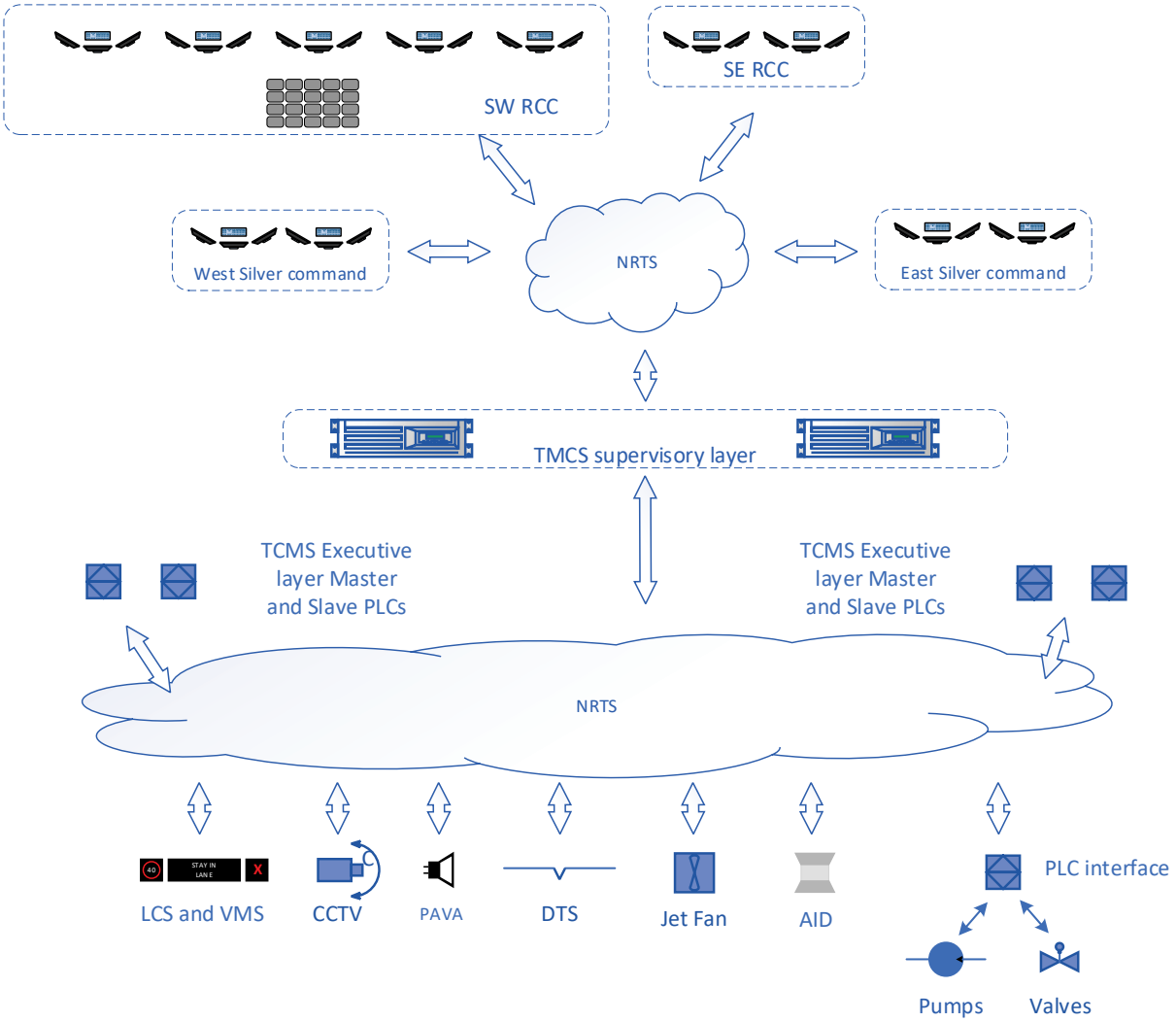


*Figure 1 Stonehenge TCMS functional Block Diagram*

The lowest layer field equipment will be connected directly to the Tunnel Network by means of an IP interface. Each of the layers in the TCMS stack will elaborate instructions coming from higher layers in the stack until direct commands to the field equipment is enacted by the equipment itself. Similarly, information flowing upwards in the stack will be combined with similar information derived from other field devices and interpreted to give intelligible, human readable operational feedback. This information will include equipment status, environmental measurements and operational parameters.

Each of the layers from the TCMS Executive layer upwards will have a degree of innate intelligence to ensure that in the event of temporary disruption to the flow of information between the TCMS layers, the TCMS field equipment ensures the safety of tunnel users. Figure 2 shows an example where the TCMS executive layer PLCs respond to a fire being

detected including a configurable pause to allow the TCMS head-end and the operators to take control.

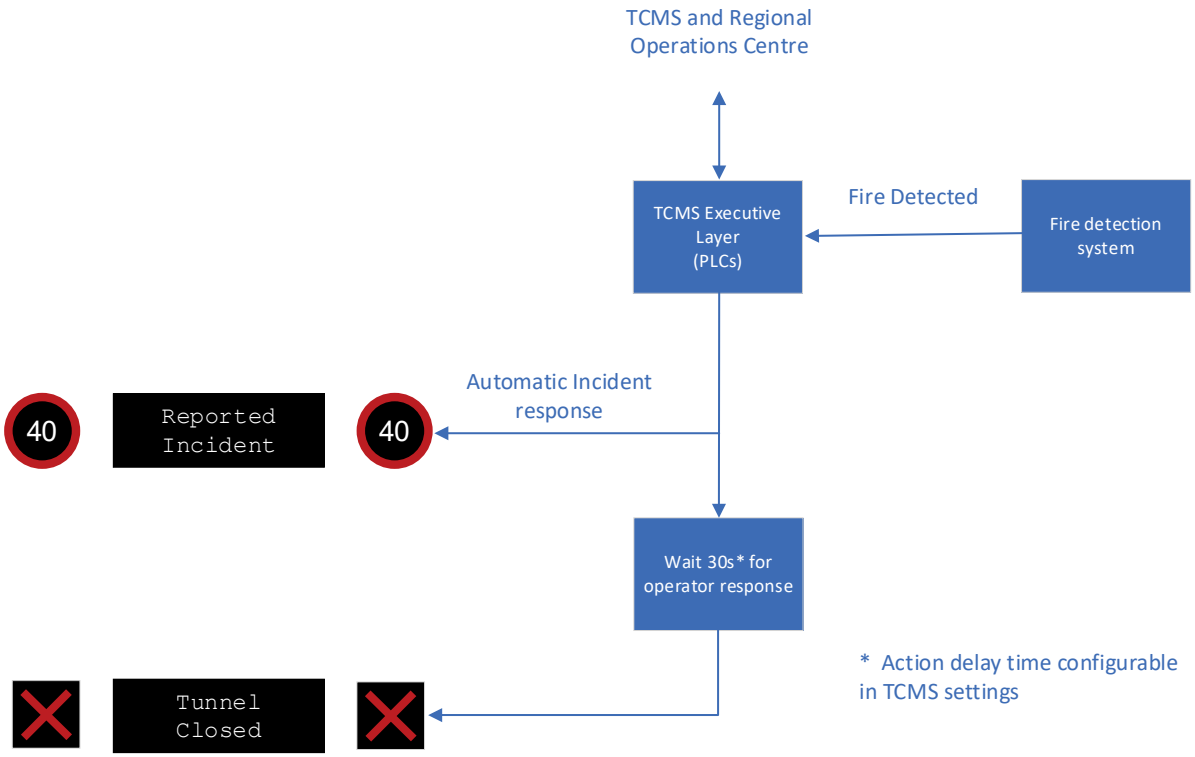


*Figure 2 Stonehenge TCMS low level system responses*

In the extreme condition that the TCMS loses communications with the remote operators, and in accordance with the requirements of Clause 20.4 of the Design and Technical requirements, the TCMS shall initiate an automatic transition to a Default Safe State and close the tunnel in a controlled manner. The exact mechanism for this transition will be defined during detailed design but, as a minimum, will include the following stages:

- Impose a reduced speed limit to the whole of the controlled section;
- Display tunnel closed aspects of the signs approaching the Countess and Longbarrow roundabouts;
- Bring up Lane Closure aspects above each lane at each portal.

## 2.1 Approach to achieving required Availability

The TCMS hosts part of the safety functions of the tunnel and as such will be subject to development and implementation processes and protocols that ensure appropriate availability to meet the safety integrity level demanded of the Safety Function. This links to the lane availability through the operation of the Minimum Operating Requirements in that to meet the MOR, the TCMS must be fully available and able to control the safety critical equipment. This is illustrated in Figure 1

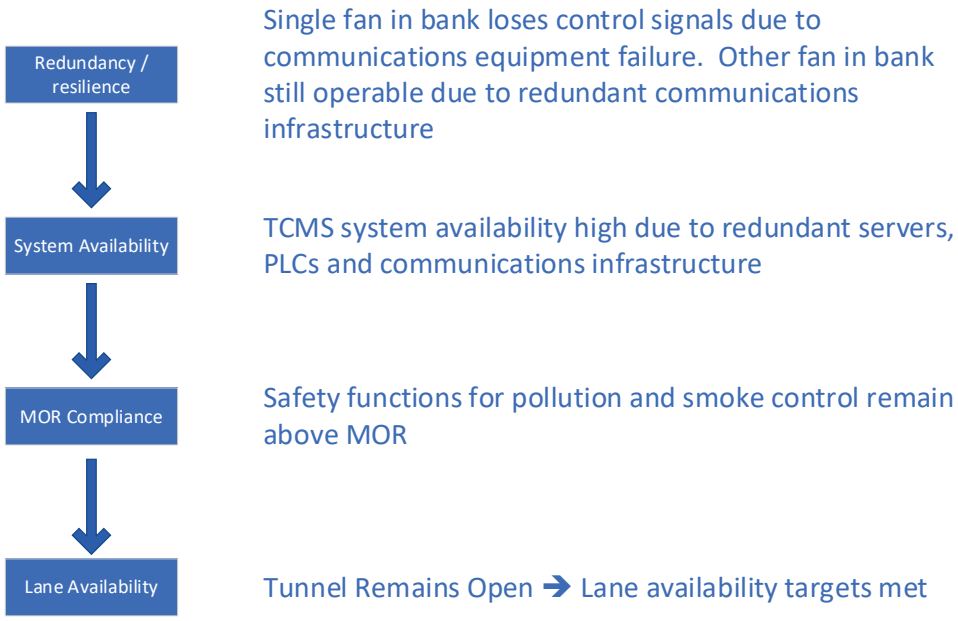


*Figure 3 Hierarchy of availability and resilience*

In addition, the TCMS will be in control of the traffic management functions and will be provided with a number of fail-safe functionality such as programming the portal lane control signs (PLCS) to revert to a Red-X in the event of the PLCS not receiving a heart-beat poll from the TCMS executive.
The approach will be in accordance with the principals outlined in BS EN 61508 parts 3 and 6 and will employ the industry standard Vee model.

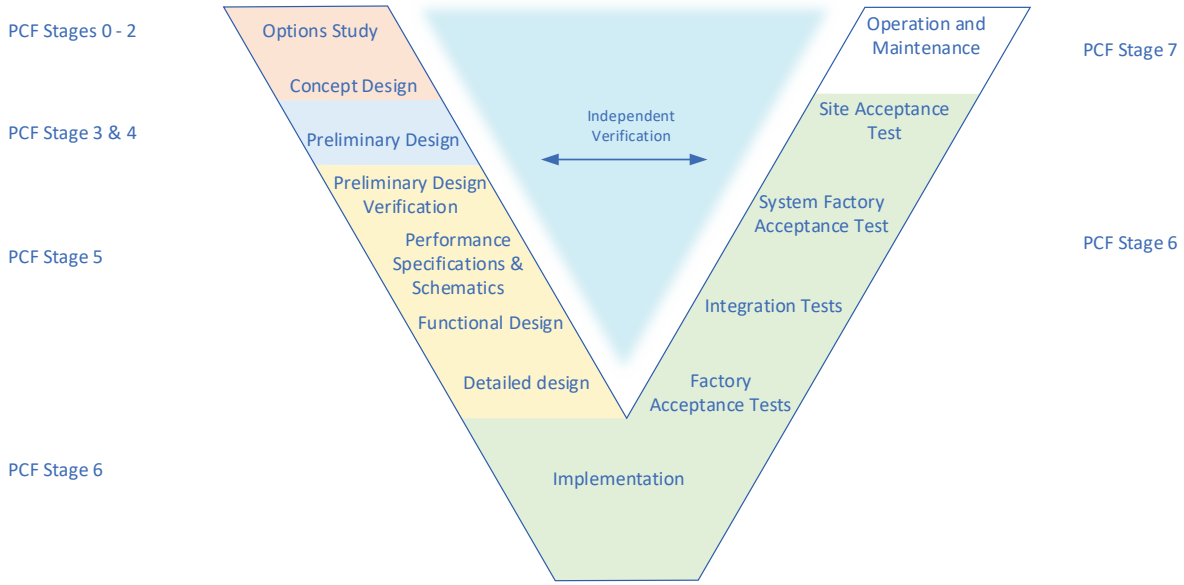


*Figure 4 Vee model with mapping to the Highways England Project Control Framework*

During the detailed design of the TCMS, we will initially validate the work already done by Highways England and their partners at PCF stages 0-2. We will carry out a functional safety analysis in accordance with BS EN 61508 in which the key stakeholders (including Highways England) will be participants. Upon completion, these functional safety requirements will be assigned to the systems that will deliver them. Finally, in coordination with the definition of the Minimum Operating Requirements, the requirement on the Safety

Functions will be used to determine the required safety integrity level of the various system components.
In parallel with the development of the functional safety process, we will carry out an information security management analysis in accordance with the guidelines contained in BS ISO 27001. Again, this analysis will be led by team Badger and will engage closely with Highways England and their key stakeholders.
Once the required safety integrity levels and information security measures have been determined, they will be added to the high-level functional requirements and decomposed to the detailed design following the steps identified on the left-hand arm of the Vee Model. At each step of the decomposition, the products will be checked, or validated, for completeness and accuracy of transcription. This will ensure that the lower level requirements are all traceable to the higher-level requirements.
Moving across the bottom of the Vee model, the various low-level systems will be integrated before being tested against their low-level requirements. As the project proceeds, the individual low-level systems are integrated together through an implement, integrate and test / validate cycle. The testing / validation activity will confirm the operation of the system against the functional specification (or detailed design requirements as appropriate) and validate that against the requirements derived from the highest-level requirements coming from the left hand half of the Vee.
At the lowest level in the implementation, techniques such as redundancy, spatial diversity, secure coding methods and anomaly detection with automatic process restart will be employed to ensure that the provided TCMS will meet the required availability. Furthermore, in order to ensure that the minimum set of safety functions can be delivered at all times, the safe-state processing will be implemented in the TCMS executive (PLC) layer and will be called if communications to the higher levels are lost. By dividing and duplicating TCMS functionality in this way, the likelihood of a single failure disabling the entire TCMS will be minimised.

## 2.2 Implementation of the core operating functions

Core operational functions will be built up from standard modules with explicitly defined interfaces. At generation, the modules will be explicitly tested against the interface specification and their functional requirements using a test harness that forms part of the module source management object. Where a module forms part of a safety function, then the module test data will include such code audit data as required to achieve the confidence of operation needed for the safety function's integrity level. As per the Vee model, individual modules will be integrated to generate higher level functionality which will be tested against the anticipated functionality and validated against the original requirements. This integrate and test / validate cycle will be repeated until the overall TCMS requirements have been met in full.
The TCMS provisioned Services will consist of discrete pieces of Software providing application functionality to other TCMS Modules and applications through well-defined services. They will be accurately described so they can be re-used by the Client and Others and they will be published using the OpenAPI Specification
At the physical level, the functionality will be provided by a layered structure shown in the Stonehenge functional block diagram (Figure 1) with each layer being functionally independent of each other. The layers will pass defined message to the layers above and below themselves. We will adopt the principle that all safety critical functionality well be carried out at the lowest level possible. In practice this will normally be at the Master and Slave PLCs of the TCMS executive layer. This will include fire responses and emergency traffic management plans (like reducing the speed limit and closing the tunnel). High level processing (such as pollution management and elective traffic management) will be carried out within the SCADA application software at the TCMS supervisory layer. The supervisory layer will also handle the user interfaces, configuration management and the data management (back-up, restore and logging) functions for the TCMS. This layer will also

provide the connection point for the user interfaces. The local Silver commands will be provided by a local hosted operator interface. The interfaces provided at the Regional Operations Centres will be provided by the national TCMS via the required DATEX 2 link.

Wherever possible, all field devices will be connected direct to NRTS service delivery points using open interfaces that fully expose the services that the device offers to the TCMS. Wherever this is not possible, for example with dry contact digital I/O, these devices will be connected to a PLC interface which will handle the translation to an open protocol and will expose the equipment functionality to the TCMS.

## 2.3 Standards and protocols to be used

During the implementation phase of the TCMS, we will employ a hierarchy of open or industry standard communication standards and protocols. The use of a standard list of protocols will ensure that the system components can be supplier agnostic and will improve maintainability (i.e. it will remove vendor lock-in). We are proposing that the following standards and protocols are used:

| Data Interchange | |
|---|---|
| Preferred | DATEX 2<br>NTCIP |
| | JSON<br>Open standard |
| | Defacto Industry std* |
| Not Preferred | Proprietary interfaces* |

| Hardware | |
|---|---|
| Preferred | Ethernet / TCPIP<br>RS485 |
| | Dry contacts*<br>4-20mA loop* |
| Not Preferred | Modbus* |

*Table 1 Interface protocol preference*

* Note in the case that the use of these non-preferred standards is unavoidable, then a PLC interface will be used to handle the translation to the agreed open protocol for the NRTS interface.

In all cases, where a suitable open standard exists, it will be adopted. Only when there is not a suitable standard will a closed standard be used.

## 2.4 Integration with The Client's National TCMS

The Stonehenge TCMS will implement a configurable interface that matches the interface disclosed in the "A303 High Level Design" document revision A/4 dated 8 April 2020 from Indra. The interface will be provided by a firewalled HTTPS socket which can be enabled or disabled individually or as whole through the TCMS configuration by the local TCMS application.

## 2.5 Integration with The Client's systems T-TOC, Dynac and ControlWorks;

The interfaces to the client's back office systems and services will also be by means of firewalled HTTPS sockets (one per service) which can be disabled individually or as a whole from within the local TCMS application. The TCMS application will provide a number of pre-defined report types to automate the sharing of relevant information with the Highways England back office systems. The predefined reports will have an automatic execution schedule to allow them to be run on a regular cadence. The contents of the reports, their destination and the execution interval will be defined within the TCMS application and will be enabled or disabled individually by the system.

The TCMS will integrate with the following *Client's* enterprise capabilities

- Advanced Traffic Management (Dynac);
- Incident Management (ControlWorks); and
- Tools for the Technology Operations Capability (T-TOC) (ServiceNow).

The TCMS will integrate with the *Client's* Technology Equipment using the *Client's* enterprise services bus (ESB). The Advanced Traffic Management (Dynac) and Technology Operations Capability (TOC) enterprise capabilities will be integrated using the ESB device or service adapters. The Incident Management (ControlWorks) enterprise capability will be integrated using an ESB direct connection.

Services to be integrated with the wider *Client's* technology systems will be in accordance with Table 2.

| Services | Dynac and ControlWorks | T-TOC |
|---|---|---|
| Integrated M&E | | ✓ |
| Queue Detection | ✓ | |
| Speed Control | ✓ | |
| Lane Control | ✓ | |
| Diversionary Routing | ✓ | |
| Traffic Monitoring and Management | ✓ | |
| Incident Management | ✓ | |
| Asset Performance Monitoring and Fault Management | | ✓ |
| Configuration Management | | ✓ |

*Table 2 TCMS Services Integration*

## 2.6 Resilience and self-recovery

The provision of system resilience underpins the availability provisions outlined in section 2.1 by ensuring the system will continue to operate normally despite some level of degradation. Under these conditions the resilience of the system will be provided by the layer isolations and the system redundancy already described which will ensure that the system remains fully operational. The system will implement a trust based vertical functional isolation scheme, isolating faults to the individual affected system and trapping invalid or inconsistent data. It will be possible to independently restart elements within the vertically isolated elements from within the TCMS without adversely affecting other systems. This will be coordinated with the security isolations defined in BS IEC 62443.

This section describes the response of the system to extreme events. Two conditions have been considered explicitly: TCMS platform failures and black-start conditions.

Considering TCMS platform failures, we will employ redundancy, spatial diversity, functional isolation and functional layering, will ensure that whilst some part of the TCMS remains operational, the impact of a failure will be minimised. However, built into the TCMS components and layers will be a number of measures to ensure that if any of the components stop functioning correctly, they will be restarted or returned to a known state. Mechanisms such as watchdogs and system heartbeats will be used to detect any operational impairment and the TCMS supervisory layer will take charge of managing the restarting of the nonperforming elements. In the case of system supervisory elements, one

half of the redundant pair will be responsible for re-initialising its counterpart if it is determined to be non-responsive. If the counterpart does not respond to a software initialisation or software initialisation is not available, then a hardware watchdog will reset the failed system. Regardless of the source of the reinitialisation / reset, the recovered system will attempt to generate a crash-dump / recovery log event to permit later diagnosis and will alert the operators to the event.

In the event of a recovery from a complete system failure (for example from a complete power failure with UPS exhaustion), the TCMS will immediately alert the operator to a 'black-start' condition and attempt to recover the last known state of the TCMS. If the recovery is successful, the TCMS will prompt the operator to set the TCMS to the last known state as a system proposal. From this point, the operator can accept that proposal, can edit that proposal to suit the prevailing tunnel conditions that the operator knows at that time or can make a completely new proposal using a 'new plan' option.

In the event that the system can't recover a last known state successfully or that the operator does not respond to the recovery proposal in a predetermined timeframe, the TCMS will automatically move to the default safe state and close the tunnel.

Disruption to the TCMS functionality or a failure of the TCMS will not result in data loss. To ensure this requirement is met, the TCMS data will be automatically backed up

- a minimum once (1) per day;
- to achieve the Recovery Point Objective;
- prior to a change and immediately after any successful change to the TCMS (including upgrades or patches).

The TCMS will be designed so that system operation can be quickly and efficiently restored following a failure of the TCMS to achieve the Recovery Time Objective.

The TCMS will be provided with the capability for the detection and prevention of malware and other malicious activity and will implement the recommendations and guidance: produced by the UK Government's National Cyber Security Centre, of the UK Government's Cyber Essentials Scheme and contained in the Cabinet Office's Minimum Cyber Security Standard.

## 2.7 Identification of any single points of failure in the Services, Modules or Devices;

Throughout the development of the TCMS and its supporting hardware platform, the presence of single points of failure will be avoided. The systems will employ redundancy and hot standby functionality. It should be noted that although some of the field devices may be single entities (such as individual fans or individual sensors) the system will be designed such that the failure of a number of such single entities will not compromise the overall objectives of the system. The overall approach to mitigation of failures will be through the application of functional safety analysis and the allocation of safety functions to system elements. It is during this process that the tolerability of all anticipated failure modes will be explicitly considered and the measures required to prevent unacceptable single points of failure defined. It should be noted that in certain circumstances a single point of failure may be tolerated if either the effect of the failure can be mitigated to an acceptable level or that the equipment concerned can be assured to have an adequate safety integrity level.

## 2.8 Proposed user interface;

The user interface will be mouse / touch screen point and click based using a geographic and / or schematic hierarchical graphical user interface. In its home state, the GUI will show

an overview of the tunnel and its approaches, it will show any abnormal conditions using colour, text characteristics (e.g. **bold**, *italics* and underlining) and flashing icons to alert the operator. The fundamental principals of the user interface and its configuration will be to adopt the principle of least privilege (i.e. that individuals will have the minimum set of facilities that permit to complete their duties) for all users and to minimise the number of roles an individual log-in can have (principally that an individual with both operator and administrator duties should have two log-in identities).

**Alarm management**
In addition to the colour / flashing status of the relevant equipment icon on the home screen, there will be a clickable text based alarm banner that will appear for a configurable period immediately that an abnormal condition is detected. Clicking on the alarm text banner will move the operator focus to the relevant alarm handler interface. A similar result will occur if the operator clicks on the coloured / flashing icon on the home screen. The alarm management screen will provide the operator with a diagnosis of the fault and any secondary alarms that the TCMS associated with that alert. The operator will be prompted to take whatever action is required of them within the alarm management screen (e.g. send a remote reset, transfer duty or raise a maintenance ticket) and will be able to acknowledge the alarm The TCMS will provide the operator with context sensitive access to the TCMS user manual and diagnostic fault trees by means of appropriate help buttons.

In addition to the graphical interaction with the system alarms, it will be possible for the operator to interact with the alarm log directly. This will be a text based representation of the alarm queue which the operator will be able to sort and filter to suit the information that they are seeking. A number of preconfigured sort and filter templates will be provided. Once loaded, the preconfigured template will allow the operator to configure the parameters of the search. Options will be provided to show all alarms or collapse secondary alarms into threads relating to the root cause. Clicking on any alarm will display the alarm management window and will provide clickable links showing whether it is ‘the parent of’ or ‘the child of’ the alarms lower down or higher up the alarm hierarchy respectively.

Where alarms relate to equipment failure or non-availability, the TCMS will compare the current non-availability, together with any other known non-availability with the Minimum Operating Requirements for the tunnel and advise the operator what actions are required based on MOR mitigations. In the event that the combination of non availability means that the MOR requires the tunnel to be closed, the TCMS will propose a closure plan that can be implemented immediately by the operator. If the operator takes no action, the closure plan will automatically implement after a predefined delay. The closure proposal can be dismissed by the operator but a justification will need to be entered into a text box that appears if the plan is dismissed. Whenever a new operator logs in and an MOR violation is in place, a closure proposal will be shown and the system operation described above will take place.

**Equipment Control**
Equipment control mode can be entered by two mechanisms from the home screen. Clicking on a controllable item of field equipment will bring up a context sensitive menu. If there are no outstanding faults on the selected equipment, then, the TCMS will enter control mode for that type of equipment. If there are outstanding faults, the operator will have to note the outstanding alarm before progressing to set mode. When the operator notes the outstanding alarm, the system will provide guidance on what restrictions the outstanding fault might impose. Once in equipment control mode, the operator will be presented

The second method of entering equipment control mode is to select one of the predefined equipment plans direct from the home screen. It is likely that these plans will be to select particular tunnel operation traffic configurations or to select ventilation, drainage or lighting

automatic modes. It should be noted that the tunnel's emergency response actions will be managed based on the traffic configuration. For example, if the traffic mode is normal / both carriageways open, unrestricted, then the fire response will be different to the fire response if the tunnel mode was one bore maintenance / other bore in contraflow.

**Equipment management**
It will be possible to interrogate the current status of any of the equipment within the tunnel estate. Upon interrogation, the current status will be shown both graphically (including, where appropriate, animation) and in text form. The operator will be able to request enhanced diagnostic information and, if necessary, request a maintenance intervention. The status enquiry screen shall provide links to the equipment control screen for that type of equipment by means of a simple link.

**Emergency Management**
The TCMS will provide facilities for communicating the presence of an emergency in the tunnel. This will be achieved by providing an emergency banner on all operator screens. This emergency banner will make clear the nature of the emergency and a prompt as to the action that is required. Clicking on the emergency banner will bring up a new operator window that provides access to all the information required by the operator to manage the emergency. This will include full integration with the CCTV and traffic surveillance / incident detection systems. The window will also provide access to the emergency actions that the operator might consider employing. This will include the ventilation, the lighting, the PAVA, the fixed firefighting and the emergency wayfinding systems. The operator will also be able to create a manual emergency condition. This manual emergency can be linked by the operator to a particular location or to a whole region (e.g. bore). Upon creation of the manual emergency, the system will bring up the emergency management screen as if the operator had responded to a system generated emergency condition.

Should the TCMS detect an emergency condition and that this condition has been alerted to the operator(s) for a predetermined duration with no response forthcoming, the TCMS will initiate a preconfigure incident response based upon the alarm type, its location and the known tunnel state. The TCMS will, after a short grace period, begin to annunciate an automatic emergency response deployment warning with a count-down to enactment. For example: "Automatic incident response at Stonehenge Tunnel B bore in 15 seconds, 14, 13 …". Any acknowledgment of the emergency condition will cause the automatic response to be abandoned and control handed back to the operator.

**Engineering control**
The TCMS will provide engineering control over the system. The engineer's controls will provide the capability to install, commission, decommission and remove equipment. All engineering actions will be subject to positive confirmation before being enacted. Engineering functions will allow individual elements of equipment to be directly controlled. Where the equipment being controlled might cause any confusion to road users, the operation of the equipment will be interlocked with the tunnel mode to prevent engineering tests being carried out under live traffic conditions.

The engineering interface will permit full remote diagnostic tests to be carried out on field equipment. This will include resetting equipment, resetting tripped circuit breakers and measuring current and voltage at key points around the tunnel estate.

**Sandbox Mode**
A TCMS sandbox mode will be provided. This will provide a fully isolated TCMS simulation that can be used for testing new TCMS configurations and updated / upgrades or for training operators dependent on the log-in credentials used

## 2.9 Remote execution of updates and upgrades

The TCMS will permit an appropriately qualified operator to carry out updates and upgrades from any of the TCMS workstations. The remote user will be authenticated using two factor authentication and will only permit the new software / configuration package to be installed if its content can be authenticated using a secure hash function and a pre-supplied hash value. It will also only permit the package to be sourced from a predetermined secure location Prior to any Software (including firmware) update process on the TCMS, the provisioned Services, and connected Modules and Devices the following will be enforced by the TCMS executive system:

- file integrity checks verify that the update file has not been altered;
- authenticity checks verify that the update file has originated from the correct and expected source;
- the update file version has been validated to demonstrate it is compatible and intended for the target Device.

Validation will be carried out to all updates on the TCMS, the provisioned Services, and connected Modules and Devices to demonstrated that the updates has been successfully installed and the system is functioning as expected.

If validation of an update on the TCMS, the provisioned Services, and connected Modules and Devices fails, the system will be rolled back to the most recent known good state.

All TCMS updates and patches shall be tested in the TCMS sandbox prior to deployment onthe live TCMS.

## 3.0 Implementation of TCMS functional and non-functional requirements

The TCMS will implement the functional requirements as identified in section 2 above. The functional elements will be implemented in the form of module drivers that are specific to the device being controlled or monitored. The module drivers will carry out any module specific data manipulation before exposing a standardised device interface that implements an open protocol.

For example, a photometer device driver will manage the specific device hardware and software interface with the physical device whilst exposing light level and device status information in an agreed format. Similarly a fan driver will handle the interface with the physical fan drive equipment to start the fan in the commanded direction upon command from the TCMS. The driver will then handle the fan status information based on the physical and software interface and carrying out any manipulation required to develop the fan operational data in the agreed format. In this way, the low-level interfaces to the field equipment can be abstracted from the core TCMS functionality and should a new photometer or fan driver be required in the future, changes will be restricted to the module driver. This will allow the device driver to be developed, tested and validated without affecting the live TCMS. Only once the module driver has been fully validated will it be integrated into the sandbox for isolated ‘live’ testing. When this sandbox test has been completed successfully, the device can be integrated into the live system.

The TCMS will implement the following non functional elements:

- User management
  The system will provide facilities to permit authorised users to add, remove and suspend system users. The authorised user will be able to allocate / deallocate functional groups and privileges to users, including themselves. In the event that there is only one authorised user, it will not be possible to deallocate the only remaining administrative user.

- User Interface
  In order to provide a level of accessibility to users with diverse sensory or processing needs, the TCMS will provide an intuitive user interface that meets the requirements of Level AA of the Web Content Accessibility Guidelines and will allow this to be improved to achieve Level AAA with future development.
- System back-up and restore
  The system will provide automatic back-up of all executable elements. Full back ups will be made at preconfigured intervals without operator intervention. The system will also create a back-up and a restore point whenever any part of the system suite (including the underlying operating system) is changed, upgraded or patched. The system will permit a suitably authorised user to restore from any back-up or restore point. All back-ups will be stored locally and mirrored automatically to a cloud based back-up server. All backups will be marked as read-only and accompanied by complex authentication token that can be checked to verify each back-up is complete and uncorrupted.
- System data management
  The system will provide data management functions allowing all users access to historical data relevant to their role. This historical data can be reported in graphical, tabular and text based (including ODF) formats. Historical data will be served from a local database and mirrored to a cloud based store. All system transactions including all data exchanges with field devices, all operator messages and commands and all system management data will be copied in real time to the historical database and all entries in the historical database will be read only and have an authentication token attached.
- System management
  The system management functions will monitor the health of all system components and report their status to the operators (by exception) and the historical database. The system management functions will automatically attempt to restart any element of the system that is not responding correctly to status signals such as heartbeat and watchdog signals. Any attempts to restart any component will be alerted to the operators and recorded in the historical database.
- System Recovery
  The TCMS will provide comprehensive facilities for system recovery. The standby TCMS servers and standby PLCs will keep the current live device status and will generate ‘shadow’ outputs. As a result, the standby servers and PLCs will be able to take-over immediately in the event of a master failure. The TCMS will regularly store its current operational state to non-volatile storage. These operational state backups will be timestamped and in the event of a significant failure of the TCMS, the TCMS will offer to restore the previous operational state. Clearly this recovery method is only useful if the TCMS can be recovered in a matter of minutes. As a result, an appropriately accredited operator will have to accept the proposal within a defined (and configurable) time period or the system will proceed to implement a cold start.
- System maintainability
  The TCMS and all its supporting equipment will be built from industry standard hardware that will allow any equipment failures to be repaired from standard stock items. All the servers used in the system will be commercial off the shelf high reliability devices and the executive layer’s PLCs will, similarly, be off the shelf high integrity units. It will be a requirement on the implementation that all the software will include a hardware abstraction layer that ensures the portability of the applications between similar hardware platforms.
  In terms of the TCMS firmware and software suite, the TCMS will provide integrated tools to permit the system to be diagnosed and maintained. These will include tools to allow patches to be deployed and rolled back. Tools to allow the performance of the system to be inspected will be integrated into the TCMS.

- Information security management
  The TCMS will implement security measures as described in the following section.

The TCMS will be built of independently testable modules written in a common language and supplied with a test harness that demonstrates all the functions of the module and tests for the boundary conditions of any inputs. All such modules will be subject to version control within a secure commercial source code repository.

## 4.0 TCMS security measures

The TCMS will be provided in accordance with the requirements, guidance and recommendations contained in:

- IEC 62443 (All Parts) 'Industrial Communication Networks';
- MCH 1514 Highways England's Code of Connection;
- BS EN ISO / IEC 27001 'Information Technology - Security Techniques - Information Security Management Systems – Requirements';
- BS EN 61508-1 'Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems. General requirements.

The TCMS will be protected in accordance with the requirements, guidance and recommendations:

- produced by the UK Government's National Cyber Security Centre;
- of the UK Government's Cyber Essentials Scheme;
- contained in the Cabinet Office's Minimum Cyber Security Standard.

## 4.1 Approach to security risk management;

The TCMS and the requirements relating to the security of the systems providing its functionality will be carried out in accordance with BS EN 27001. The security assessments will be carried out by the implementation contractor with members of the client's specialist taking part. The outcome of the assessment will be built into the project's requirement schedule and validated and verified as per the other requirements according to the VEE model process. Security measure implementation will be subject to independent audit and testing throughout the implementation phase.

As a basic level, good security hygiene will be practiced. All unused services, ports (both physical and software) and applications will be disabled or disabled. Physical access to TCMS hardware will be protected by both physical and electronic software access control mechanism. All users of the system will be authenticated using 2 factor authentication and all their actions will be logged. Users will have the minimum set of functions required to carry out their required roles.

## 4.2 Proposals for protection, including network security controls, zones, boundary controls and malware and malicious activity;

Throughout the development and implementation of the TCMS, the TCMS architecture will show the network security controls implemented and demonstrate how the system has been grouped into zones based on common security requirements, as described BS IEC 62443. TCMS zones with differing trust levels will be logically or physically segregated from all other zones using boundary controls (for example firewalls, unidirectional data connections and demilitarised zones).

Firewalls used as boundary controls in the TCMS will:

- be deployed at all network perimeters and internal network boundaries;

- provide segregation of the security zone in which they are installed; and
- have the basis of firewall rules set to "deny all" with exceptions explicitly identified.

The TCMS will be implemented using secure coding techniques to minimise the most critical security risks to web applications identified in the OWASP Top Ten.

The TCMS will implement an approach to secure coding using one or more of the following techniques and measures:

- internal code reviews;
- use of automated tools to conduct security checks;
- use of a version control system;
- a segregated and secure development and testing environment; and
- evidence of input sanitisation, including buffer overflow prevention.

The TCMS and configuration computer will be protected from unauthorised modification or use through the implementation of physical and technical security features, including the following

- encryption;
- access control;
- event and communication logging;
- monitoring; and
- alarming.

The TCMS will be tested for security weaknesses through a security test conducted prior to Completion of section 3 and annually after Completion of section 3 until the Maintenance Completion Date. The scope of the TCMS security test will be determined through consultation with the Client and recorded in the TCMS Solutions Document. The un-abridged version of the TCMS security test report and its recommendations will be provided to the Project Manager.

A Remedial Action Plan will be prepared which proposes how vulnerabilities identified in the TCMS following security testing shall be mitigated. A Technical Vulnerability and Patch Management Plan will be provided for the TCMS, the provisioned Services, and connected Modules and Devices which includes:

- the methods to guarantee the integrity and compatibility of the systems with patches before their deployment;
- a schedule against which automated vulnerability scans are to be run on the system;
- an approach and associated capability to remediate newly reported zero-day vulnerabilities;
- procedures for patching the system after commissioning;
- a schedule against which patches are to be applied to the system;
- mitigation strategies for situations where there is a recommendation against applying a released patch;
- identification of the party responsible for the installation and update of patches;
- procedures for minimising operational disruption as a result of patching.

## 4.3 Authentication and management of users and user profiles

The TCMS will provide user profiles with defined access rights. The TCMS user profiles will be provided as follows

- maintainer;
- operator;
- manager; and

- administrator.

TCMS user profiles will be configured based on the TCMS operational functions. The TCMS will manage user credentials so that:

- default passwords are changed upon first use;
- the need for shared accounts is avoided;
- stored and in-transit credentials are secured using strong cryptographic techniques;
- concurrent logins of the same account are rejected;
- applications do not store login information between sessions;
- auto-fill functionality during login is prevented; and
- anonymous logins are disabled.

The TCMS shall be provided with a user profile password management system that allows for the configuration and setting of

- password length;
- frequency of password change;
- password complexity;
- number of login attempts;
- inactive session logout time;
- screen lock by application; and
- denial of repeated or recycled use of the same password.

The configuration requirements for the TCMS user profiles will be:

- determined in consultation with the Client; and
- agreed with the Project Manager.

The TCMS will support a minimum twenty (20) concurrent users.

Multi-Factor Authentication (MFA) will be used to authenticate all remote and privileged (for example Administrator, maintainer, etc) TCMS users.

The TCMS will provide full conflict resolution and prioritisation between multiple users.

User profile access rights will be configured to the principle of least privileged (POLP).

Role-based access controls will be implemented in the TCMS.

The TCMS will minimise the number of occurrences a user has to authenticate their credentials.

The TCMS ensure that all users have completed the Baseline Personnel Security Standard (BPSS) pre-employment controls. This will be achieved by requiring the Supervisor enabling every user account created by the Administrator upon receipt of confirmation of a valid BPSS screening.

## 4.4 Configuration of user profiles

The configuration of user profiles will be carried out by the Administrator by assigning users to a number of specific function profiles. These profiles will allow specific operations to be carried out (e.g. tunnel operation, equipment configuration and maintenance, user management sandbox only etc). In order to prevent unexpected outcomes on street, some of these may be mutually exclusive. For example, a user that can configure the system will have no control over field equipment in the live system. If an individual required both

functions, then two system accounts will be required. Within the sandboxed test system, maintainers will have 'control' functionality to allow them to test the modifications that they are making.

## 4.5 Implementation of system configuration and hardening measures

The TCMS will be implemented in an electrically and functionally isolated manner with only the interfaces necessary to carry out required system functions exposed. Where interfaces to the outside world are exposed, these will be hardened and validated using the following proposed methods:

- Physical security (preventing access to TCMS equipment);
- Endpoint verification;
- End to end Encryption;
- Data authentication (assuring that the control data is complete and unmodified)
- Originator authentication (assuring that the control data originates from an authorised source)
- Functional zoning to prevent malfunctions or intrusions in one area of the TCMS can't affect other functional areas

## 4.6 Testing for weaknesses is to be undertaken, including scope of test;

The TCMS will be tested for weaknesses in accordance with the BS EN 27001 information security management system assessment. Tests to be undertaken are likely to include:

- Independent code audits;
- Penetration / White-hat hack tests;
- Module interface boundary testing;
- Integration testing; and
- User interface bounds testing.

## 4.7 Management and monitoring of Security Incidents

The TCMS will maintain an activity log of changes to the TCMS and the TCMS provisioned Services (including automatic responses to predefined MOR rules and mitigation) with a brief description of changes made, including usernames and timestamps.

The TCMS will have a centralised Authentication, Authorisation, and Accounting (AAA) management capability which will:

- time stamp events using an authoritative time source; and
- protect audit logs from corruption and tampering.

The TCMS will maintain a time stamped log on the login status and activity of all TCMS users.

The TCMS will retain historic data within the system capturing the following information:

- system activity;
- audit logs;
- Service change of state;
- event faults; and
- user actions.

TCMS will provide capabilities for historic data to be:

- retained within the system for a minimum of two (2) years;

- archived for a minimum of six (6) years; and
- able to be exported and downloaded in SQL, CSV and ODF (for word processing and spreadsheets) formats.

System event logging will be enabled on the TCMS to monitor the activity of the TCMS, provisioned Services and connected Modules and Devices.

The TCMS will be provided with systems to detect, prevent and report on attacks on the system including denial of service attacks.

The TCMS will be provided with a security monitoring system which:

- filters system event logs and alerts users of Security Incidents;
- detects known threats by comparing system event logs against Indicators of Compromise (from threat intelligence sources);
- has procedures defined for responding to threats and Security Incidents;
- permits users to view the logs and produce reports of all detected Security Incidents;
- The TCMS security management system will be refined and improved throughout the term of the TCMS SLA to reflect the latest cyber security guidance from the National Cyber Security Centre and the Cabinet office.

All TCMS Security Incidents which are defined as Major Security Incidents will be reported to the *Project Manager* as soon as reasonably practicable. The TCMS will provide facilities to prepare the supporting data for such a report.

Any TCMS will provide facilities to capture and report the data relating to any Major Security Incident that will permit a root cause analysis to be carried out with a report produced documenting the cause of the Security Incident along with proposed remedial actions which could prevent a recur.

The TCMS will implement a full network management subsystem (NMS) that scans for unauthorised or unexpected network traffic and is able to isolate the source of that traffic by dynamically disabling its network access.

The NMS will regularly scan all the network infrastructure for unauthorised modification and will be able to restore to standard configuration and reboot any network switch that does not provide a valid configuration

## 5.0 Approach to compliance with the Client's procedures and policies

The TCMS and its development will comply with Highways England policies and procedures as described below. The design of the regular and ongoing audit and independent checking of the TCMS development, integration and testing will be in line with that required to meet the integrity requirements determined by the functional safety assessment. We propose that these audits and checks will have the same weight as the CAT3 checking of Mechanical and electrical installations required by CG 300 clause 6.3.

The functional safety assessment carried out will be done in accordance with GG 104 and BS EN 61508 with the two assessments being carried out in a synchronised manner and managed by the Project Safety Control Risk Group taking overall responsibility for the process.

As the development of the TCMS and the deployment of its field systems is completed, a Technology Commissioning Plan that relates to TCMS will be prepared in accordance with the testing and commissioning philosophy and requirements of:

- MCH 1980 'Process for Commissioning and Handover of Technology Schemes' and
- GG 182 'Major Scheme Enabling Handover into Operations and Maintenance'.

For the TCMS handover, the Consent to Implement (CTI) process will be implemented in accordance with the requirements of GG 182. Prior to the implementation of the TCMS on site and its connection to the NRTS backbone, a Code of Connection in accordance with MCH1514 will be prepared and submitted to Highways England for their acceptance. The code of connection will be supported by such cyber security data as generated by the penetration tests and any others required as part of the Information Security management system assessment (in accordance with BS ISO 27001).

The requirements contained in MCH 1349 'Technology Maintenance Instruction Operational and Maintenance Requirements for Technology Systems and Equipment' and MCH 1399 'NMCS Maintenance Instruction Notification of a Change in Equipment Quantities for Maintenance' will be complied with prior to Completion of section 3.

Prior to Completion of section 3, materials, training and handover to permit the Client to assume independent operational control of the works will be provided and coordinated.

Materials and training on the operational control of the works will be in accordance with MCDHW Clause 7015, (Training) be provided to personnel from:

- the Client;
- the Client's representatives;
- those maintaining the M&E Systems and Technology Equipment;
- Emergency Services; and
- the Client's TSP.

The following materials will be provided:

- user, reference and training manuals;
- original equipment manufacturer (OEM) user manuals;
- maintenance manuals, as-built drawings, spares, software, special tools;
- Health and Safety File; and
- any additional documentation required to permit the Client to assume operational control of the works.

The following operational and training manuals for each component of the M&E Systems and Technology Equipment as well as an integrated manual will be provided with procedures covering:

- normal operating procedures and agreed mitigation to be applied when the MOR is breached or approaching a level where the MOR would be breached;
- response to emergency situations and alarms;
- incident detection system alarms;
- Plant alarms and failures and
- maintenance and renewal.

## 6.0 Approach to compliance with the Clients Architecture Services Principles

The TCMS will be implemented in accordance with the 14 principals defined in the Highways England "Enterprise Architecture (EA) Principals" document dated January 2016. The TCMS

will be built on the basis that as much of the development has been and can be re-used as possible, it will treat information as an asset that should be shared and made as accessible as it can be. The TCMS will be built on web and cloud based services.

## 7.0 The software schedule, provided using Quality Submission Template D (Software Schedule)

Template D is attached in the required form.

# A303 Amesbury to Berwick Down (Stonehenge)

## Invitation to Participate in Dialogue

### Quality Submission Template D

### Software Schedule

| TEMPLATE D – Software Schedule | |
|---|---|
| Participant allocated name | **Badger** |
| Submission version | Badger_210730_QS-2C_Final |
| Submission date | July 30th 2021 |

1. **THE SOFTWARE**

1.1 The Software below is licensed to the *Client* in accordance with clause Z13 (Intellectual Property Rights). The Parties agree that any wording contained in the columns headed "Purpose", "Number of Licences", "Restrictions", "Number of Copies" and "Other" in the tables set out in paragraphs 2, 3, 4 and 5 below is for information only and does not restrict the *Client*'s use of the Software. In the event that there is any change to the purpose for which the Software is used, or an additional number of licences or copies are required, or any restriction or other issue needs to be relaxed or amended, this is the sole responsibility of the *Contractor*.

1.2 The Parties agree that they will update this schedule periodically to record any Contractor Software, Third Party Software and OSS subsequently licensed, and any Specially Written Software created, by the *Contractor* or third parties for the purposes of the delivery of the *works*.

2. **CONTRACTOR SOFTWARE**

The Contractor Software includes the following items:

| Software | Supplier (if an Affiliate of the *Contractor*) | Purpose | Number of Licences | Restrictions | Number of Copies | Type (COTS or Non-COTS) | Deposited Software (Yes/No) |
|---|---|---|---|---|---|---|---|
| User Management Module | FCC Industrial | Manage and control user access roles and permissions to software platform modules | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |
| Variable Message Sign Management Module | FCC Industrial | Monitoring and control of fixed and variable signalling systems for user information | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |
| Lighting Control Module | FCC Industrial | Monitoring and control of tunnel lighting conditions | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |
| Road Weather Information Module | FCC Industrial Systems Division | Monitoring of meteorological conditions affecting the motorway | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |
| Access Control & Restriction Module | FCC Industrial Systems Division | Traffic access monitoring, control, and traffic restriction | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |

| Software | Supplier (if an Affiliate of the *Contractor*) | Purpose | Number of Licences | Restrictions | Number of Copies | Type (COTS or Non-COTS) | Deposited Software (Yes/No) |
|---|---|---|---|---|---|---|---|
| Tunnel Ventilation & Pressurization Module | FCC Industrial | Monitoring and control of ventilation conditions in the tunnel, working conditions of the jet fans. Control of pressurization of emergency galleries as well. | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |
| Fire Protection and Life Safety Module | FCC Industrial | Management monitoring and control of fire detection, management, evacuation, and emergency fire control | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |
| FFPS Fixed Fire Protection System Module | FCC Industrial | Management monitoring and control of pumps, valves | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |
| Emergency Power Generator & UPSs Control Module | FCC Industrial | Management and control of main and redundant emergency power generators control and UPS monitoring. | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |

| Software | Supplier (if an Affiliate of the *Contractor*) | Purpose | Number of Licences | Restrictions | Number of Copies | Type (COTS or Non-COTS) | Deposited Software (Yes/No) |
|---|---|---|---|---|---|---|---|
| Emergency Call and communication Module (ERTs) | FCC Industrial | Incident Emergency Communications Management System (ECMS) | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |
| Security PAVA Comms Module | FCC Industrial | Management of PAVA (Public Address Voice Alarm) for message transmission | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |
| Security Radio Comms Module | FCC Industrial | Management of radio frequency comms for message transmission | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |
| Alarm Management Module | FCC Industrial | Management of the complete life cycle of alarms and alerts, from their activation to their deactivation, providing a grouping by type and priority-based triggering | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |
| Video Control Module | FCC Industrial | Real-time video management and monitoring | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |

| Software | Supplier (if an Affiliate of the *Contractor*) | Purpose | Number of Licences | Restrictions | Number of Copies | Type (COTS or Non-COTS) | Deposited Software (Yes/No) |
|---|---|---|---|---|---|---|---|
| Traffic Control Module | FCC Industrial | Vehicle classification and counting for tunnel capacity management and monitoring | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |
| RTU Remote Terminal Unit Control Module | FCC Industrial | Independent local control system to communicate field elements with the Control Centre. | End User License for exclusive use in Stonehenge Tunnel TSBs | N/A | One copy per TSB | Non-COTS | Yes |

3. **THIRD PARTY SOFTWARE**

The Third-Party Software includes the following items:

**NOTE**:
Since FCC Industrial Tunnel Management Platform is an own development which means that FCC Industrial controls its development cycle, there is no restriction for integrating any third-party solution provider that could be decided in further phases. Therefore, Supplier is not identified at this stage.

| Third Party Software | Supplier | Purpose | Number of Licences | Restrictions | Number of Copies | Type (COTS or Non-COTS) | Deposited Software (Yes/No) |
|---|---|---|---|---|---|---|---|
| Automated Incident Management System | To be defined<br><br>(Candidates: FLIR, CITILOG,..) | Automatic incident detection system image-based | One license per TSB | N/A | One copy per TSB | COTS | |
| CCTV Video Management System (VMS) | To be defined (Candidates: BOSCH, HIKVISION, …) | Collect, record and interface viewing provision for video camera images | VMS manufacturer's licensing is normally based in per camera unit and management module | N/A | One copy per TSB | COTS | |
| Videowall Control System | To be defined (Candidates: RPG, NEC, MITSUBISHI) | Management of traffic information visualisation based on tiling multiple displays in the operations centres | One license per TSB | N/A | One copy per TSB | COTS | |
| Windows Server | Microsoft | Operational System | One license per TSB | N/A | One copy per TSB | COTS | |
| Windows Client | Microsoft | Operational System | One license per TSB | N/A | One copy per TSB | COTS | |

| Third Party Software | Supplier | Purpose | Number of Licences | Restrictions | Number of Copies | Type (COTS or Non-COTS) | Deposited Software (Yes/No) |
|---|---|---|---|---|---|---|---|
| SQL Server | Microsoft | Data Base Management | One license per TSB | N/A | One copy per TSB | COTS | |
| Backup and recovery management system | VMware | Backup and Recovery | One license per TSB | N/A | One copy per TSB | COTS | |
| Infrastructure and Virtualisation system | VMware | Virtualization Software | One license per TSB | N/A | One copy per TSB | COTS | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

4. **SPECIALLY WRITTEN SOFTWARE**

The Specially Written Software includes the following items:

| Specially Written Software | Supplier (if Affiliate of the Contractor) | Purpose |
|---|---|---|
| Horus-Avanza DATEX II Interface | FCC Industrial<br><br>DATEX II supplier to be decided | Interface communication for messaging interchange and platform integrating services |
| Incident Reporting System | FCC Industrial | Incident communication system with public emergency and protection authorities |
| | | |
| | | |

5. **OSS**

The OSS shall consist of the following items:

**NOTE:** there is no OSS used to be declared..

| OSS | Supplier | Purpose | [Number of Copies] | [Other] |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**ANNEX 1**

**FORM OF CONFIDENTIALITY UNDERTAKING**

**CONFIDENTIALITY AGREEMENT**

THIS AGREEMENT is made on [*date*] 20

**BETWEEN:**

(1) [*insert name*] of [*insert address*] (the "Sub-licensee"); and

(2) [*insert name*] of [*insert address*] (the "Contractor")

together, the "Parties").

**WHEREAS:**

(A) [*insert name of Client*] (the "Client") and the Contractor are party to a contract dated [*insert date*] (the "Contract") for the provision by the Contractor of [*insert brief description of services*] to the Client.

(B) The Client wishes to grant a sub-licence to the Sub-licensee in respect of certain software and intellectual property rights licensed to the Client pursuant to the Contract (the "Sub-licence").

(C) It is a requirement of the Contract that, before the Client grants such sub licence to the Sub-licensee, the Sub-licensee execute a confidentiality agreement in favour of the Contractor in or substantially in the form of this Agreement to protect the Confidential Information of the Contractor.

**IT IS AGREED** as follows:

1. **Interpretation**

1.1 In this Agreement, unless the context otherwise requires:

**"Confidential Information**

(a) information, including all personal data within the meaning of the Data Protection Act 1998, and however it is conveyed, provided by the Client to the Sub-licensee pursuant to or in connection with the Sub-licence that relates to:

(i) the Contractor; or

(ii) the operations, business, affairs, developments, intellectual property rights, trade secrets, knowhow and/or personnel of the Contractor;

(b) the source code and the object code of the software sub-licensed to the Sub-licensee pursuant to the Sub-licence together with build information, relevant design and development information, technical specifications of all functionality including those not included in standard manuals (such as those that modify system performance and access levels), configuration details, test scripts, user manuals, operating manuals, process definitions and procedures, and all such other documentation

supplied by the Contractor to the Client pursuant to or in connection with the Sub-licence;

(c) other Information provided by the Client pursuant to this Agreement to the Sub-licensee that is clearly designated as being confidential or equivalent or that ought reasonably to be considered to be confidential which comes (or has come) to the Sub-licensee's attention or into the Sub-licensee's possession in connection with the Sub-licence; and

(d) information derived from any of the above,

but not including any Information that:

(i) was in the possession of the Sub-licensee without obligation of confidentiality prior to its disclosure by the Client;

(ii) the Sub-licensee obtained on a non-confidential basis from a third party who is not, to the Sub-licensee's knowledge or belief, bound by a confidentiality agreement with the Contractor or otherwise prohibited from disclosing the information to the Sub-licensee;

(iii) was already generally available and in the public domain at the time of disclosure otherwise than by a breach of this Agreement or breach of a duty of confidentiality; or

(iv) was independently developed without access to the confidential Information;

**"Information"** all information of whatever nature, however conveyed and in whatever form, including in writing, orally, by demonstration, electronically and in a tangible, visual or machine-readable medium (including CD-ROM, magnetic and digital form); and

**"Sub-licence"** has the meaning given to that expression in recital (B) to this Agreement.

1.2 In this Agreement:

1.2.1 a reference to any gender includes a reference to other genders;

1.2.2 the singular includes the plural and vice versa;

1.2.3 the words "include" and cognate expressions shall be construed as if they were immediately followed by the words "without limitation";

1.2.4 references to any statutory provision include a reference to that provision as modified, replaced, amended and/or re-enacted from time to time (before or after the date of this Agreement) and any prior or subsequent subordinate legislation made under it;

1.2.5 headings are included for ease of reference only and shall not affect the interpretation or construction of this Agreement; and

1.2.6 references to clauses are to clauses of this Agreement.

2. **Confidentiality Obligations**

2.1 In consideration of the Client entering into the Sub-licence, the Sub-licensee shall:

2.1.1 treat all Confidential Information as secret and confidential;

2.1.2 have in place and maintain proper security measures and procedures to protect the confidentiality of the Confidential Information (having regard to its form and nature);

2.1.3 not disclose or permit the disclosure of any of the Confidential Information to any other person without obtaining the prior written consent of the Contractor or except as expressly set out in this Agreement;

2.1.4 not transfer any of the Confidential Information outside the United Kingdom;

2.1.5 not use or exploit any of the Confidential Information for any purpose whatsoever other than as permitted under the Sub-licence;

2.1.6 immediately notify the Contractor in writing if it suspects or becomes aware of any unauthorised access, copying, use or disclosure in any form of any of the Confidential Information; and

2.1.7 upon the expiry or termination of the Sub-licence:

2.1.7.1 destroy or return to the Contractor all documents and other tangible materials that contain any of the Confidential Information;

2.1.7.2 ensure, so far as reasonably practicable, that all Confidential Information held in electronic, digital or other machine-readable form ceases to be readily accessible (other than by the information technology staff of the Sub-licensee) from any computer, word processor, voicemail system or any other device; and

2.1.7.3 make no further use of any Confidential Information.

3. **Permitted Disclosures**

3.1 The Sub-licensee may disclose Confidential Information to those of its directors, officers, employees, consultants and professional advisers who:

3.1.1 reasonably need to receive the Confidential Information in connection with the Sub-licence; and

3.1.2 have been informed by the Sub-licensee of the confidential nature of the Confidential Information; and

3.1.3 have agreed to terms similar to those in this Agreement.

3.2 The Sub-licensee shall be entitled to disclose Confidential Information to the extent that it is required to do so by applicable law or by order of a court or other public body that has jurisdiction over the Sub-licensee.

3.3 Before making a disclosure pursuant to Clause 3.2, the Sub-licensee shall, if the circumstances permit:

3.3.1 notify the Contractor in writing of the proposed disclosure as soon as possible (and if possible before the court or other public body orders the disclosure of the Confidential Information); and

3.3.2 ask the court or other public body to treat the Confidential Information as confidential.

4. **General**

4.1 The Sub-licensee acknowledges and agrees that all property, including intellectual property rights, in Confidential Information disclosed to it by the Contractor shall remain with and be vested in the Contractor.

4.2 This Agreement does not include, expressly or by implication, any representations, warranties or other obligations:

4.2.1 to grant the Sub-licensee any licence or rights other than as may be expressly stated in the Sub-licence;

4.2.2 to require the Contractor to disclose, continue disclosing or update any Confidential Information; or

4.2.3 as to the accuracy, efficacy, completeness, capabilities, safety or any other qualities whatsoever of any Information or materials provided pursuant to or in anticipation of the Sub-licence.

4.3 The rights, powers and remedies provided in this Agreement are cumulative and not exclusive of any rights, powers or remedies provided by law. No failure or delay by either Party to exercise any right, power or remedy will operate as a waiver of it nor will any partial exercise preclude any further exercise of the same, or of some other right, power or remedy.

4.4 Without prejudice to any other rights or remedies that the Contractor may have, the Sub-licensee acknowledges and agrees that damages alone may not be an adequate remedy for any breach by the Sub-licensee of any of the provisions of this Agreement. Accordingly, the Sub-licensee acknowledges that the Contractor shall be entitled to the remedies of injunction and specific performance as well as any other equitable relief for any threatened or actual breach of this Agreement and/or breach of confidence and that no proof of special damages shall be necessary for the enforcement of such remedies.

4.5 The maximum liability of the Sub-licensee to the Contractor for any breach of this Agreement shall be limited to ten million pounds (£10,000,000).

4.6 For the purposes of the Contracts (Rights of Third Parties) Act 1999 no one other than the Parties has the right to enforce the terms of this Agreement.

4.7 Each Party shall be responsible for all costs incurred by it or on its behalf in connection with this Agreement.

4.8 This Agreement may be executed in any number of counterparts and by the Parties on separate counterparts, but shall not be effective until each Party has executed at least one counterpart. Each counterpart shall constitute an original of this Agreement, but all the counterparts shall together constitute but one and the same instrument.

5. **Notices**

5.1 Any notice to be given under this Agreement (each a "Notice") shall be given in writing and shall be delivered by hand and shall be deemed to have been duly given at the time of delivery provided that such Notice is sent to the relevant physical address, and expressly marked for the attention of the relevant individual, set out in Clause 5.2.

5.2 Any Notice:

5.2.1 if to be given to the Contractor shall be sent to:

[*Address*]

Attention: [*Contact name and/or position, e.g. "The Finance Director"*]

5.2.2 if to be given to the Sub-licensee shall be sent to:

[*Name of Organisation*]

[*Address*]

Attention: [ ]

6. **Governing law**

6.1 This Agreement shall be governed by, and construed in accordance with, English law and any matter claim or dispute arising out of or in connection with this Agreement whether contractual or non-contractual, shall be governed by and determined in accordance with English law.

6.2 Each Party hereby irrevocably submits to the exclusive jurisdiction of the English courts in respect of any claim or dispute arising out of or in connection with this Agreement.

**IN WITNESS** of the above this Agreement has been signed by the duly authorised representatives of the Parties on the date which appears at the head of page 1.

For and on behalf of [*name of Contractor*]

Signature: Date:

_____

Name: Position:

For and on behalf of [*name of Sub-licensee*]

Signature: Date:

_____

Name: Position: