Horizon 2020
European Union Funding
for Research & Innovation

In2Rail

Project Title:	**INNOVATIVE INTELLIGENT RAIL**
Starting date:	01/05/2015
Duration in months:	36
Call (part) identifier:	H2020-MG-2014
Grant agreement no:	635900

Deliverable D7.3

Specifications of the Standard Operator Workstation

Due date of deliverable	Month 16
Actual submission date	31-08-2016
Organization name of lead contractor for this deliverable	THA
Dissemination level	Public
Revision	FINAL

Authors

	Partner	Contribtuions
Author(s)	**Partner 10 (THL)** Joanna Evans Mark Lowten	Owners of deliverable 7.3. Lead on subtasks 7.2.4, 7.2.5 and 7.2.3.3, (sections 4, 6 and 4.5 of this document). Collated all partners' outputs to produce this document, the final output for deliverable 7.3.
Contributor(s)	**Partner 1 (NR)** Richard Bye Mike Carey Amanda Webster Nadia Hoodbhoy Tom Tivey	Attended meetings to contribute to and review content for subtasks 7.2.4 and 7.2.5, (sections 4 and 6 of this document). Reviewed final output for deliverable 7.3.
	Partner 7 (SIE) Antonio Planells Munoz Hector Garcia Esteban	Lead on secondary subtask 7.2.4.4, (section 4.10 of this document).
	Partner 24 (INDRA) Ángel Pérez Bartolomé, Carlos Monton Gomez	Lead on subtask 7.2.2, (section 5 of this document).
	Partner 3 (ASTS) Marco Giaroli	Lead on subtasks 7.2.1 and 7.2.3, (sections; 4.4.4, 4.4.5 and 4.4.6 of this document).
	Partner 5 (RFI) Simone Petralli	Attended concept review workshop to contribute to and review content for subtask 7.2.4.

Executive Summary

Over the coming years, there are expected to be a number of developments in the technology available to be used within rail operator's workstation design. The changes in technology used will have an effect on people, (the users), and the processes that support the users in utilising the technology available. This report has been produced to determine the key considerations for future workstation design. When defining these key principles, it was essential to consider workstation design in the context of Traffic Management (TM) Systems. The report captures not only best practice in workstation design but also security management systems and operator workload as they are seen as closely related in the context of TM Systems.

The overriding findings from this report are that systems of the future will need an increase in flexibility in order to adapt to the:

- Changing operational cultures to use more flexible roles,
- Changing operational conditions that contain more varied scenarios,
- Rapid advances in technology that should be utilised to solve current and future user needs,
- Increasing need for cyber security to be integrated into the entire lifecycle of system design through to operation,
- Use of automation and intelligent systems and their effect on workload.

A number of concepts for future TM workstation design and Human Machine Interface (HMI) design have been developed to enable a road map of future TM workstations to be produced based on technological readiness and cost. The advantages and disadvantages of each concept are evaluated and are discussed in order to provide guidance to operating companies or future deployments of TM To ensure the selection of technology is appropriate it is important to keep a holistic view of the application of the technology in the context of the railway and also how it relates to people and process. Therefore the selection of technologies should be based around the user needs and ensure they enhance the safety and performance of the railway.

Due to the expected changes in types of tasks required by operators, an increase in collaborative working styles and shared responsibilities, future TM workstation and HMI designs need to have greater flexibility in order to react to changing operational demands and user needs. TM Workstations and HMI displays therefore need to be configurable to support the information requirements for each specific role as well as support each role during different scenarios.

It is predicted at this stage that integrated desktops, an increase in automation and intelligent systems or artificial intelligence is where the value proposition will be as it will

enable a holistic and meaningful view of the railway to be created to enable effective decision making and management of the railway.

The review of security measures proposes a methodology that builds upon a traditional Information Security Management System to create a railway specific Railway Information Security Management System. The need for this is ever increasing, as railways, networks and partners attempt to work in a more collaborative manner to increase the capacity and efficiency of the railway. This increase in collaboration means that information needs to be shared digitally which increases the risk of cyber-attacks.

Being able to accurately measure and predict operational workload means that TM control centres of the future can be appropriately sized and manned. The findings from the workload tool set proposes a comprehensive set of techniques that can be used to measure workload. It then shows how these measurements can be used to predict the impact on staff or future TM systems so that changes can be proposed, evaluated and decided upon in a controlled manner.

It is expected that as different technologies continue to develop in maturity and their respective value propositions are determined, concept of operations will also continue to evolve to make use of the technology available in any given deployment of TM. Therefore the recommendations in this report should be reviewed for each deployment of TM to ensure they meet the needs of each project and most importantly the end user.

TABLE OF CONTENTS

Abbreviations and Acronyms

Abbreviation / Acronyms	Description
ISMS	Information Security Management System
ASTS	Ansaldo STS
AoC	Area of Control
AR	Augmented Reality
DRAWS	Defence Research Agency Workload Scales
EEG	Electroencephalograph
EOG	Electrooculogram
EU	European Union
HF	Human Factors
HMI	Human Machine Interface
INDRA	INDRA Sistemas S.A
ISA	Instantaneous Self-Assessment
ISMS	Information Security Management System
IWS	Instant Workload Scale
IXL	Interlocking
I²M	Intelligent Mobility Management: information developed as a strategically critical asset: • A standardised approach to information management and dispatching systems enabling an integrated Traffic Management System (TMS). • An Information and Communication Technology (ICT) environment supporting all transport operational systems with standardised interfaces and with a plug and play framework for TMS applications. An advanced asset information system with the ability to 'nowcast' and forecast network asset statuses with the associated uncertainties from heterogeneous data sources.
In2Rail	Innovative Intelligent Rail
NASA TLX	NASA Task Load Index
NHS	National Health Service
NR	Network Rail
MACE	Malvern Capacity Estimate
MCH	Modified Hooper Scales
ODEC	Operational Demand Evaluation Checklist
PRESTO	Predictor of Signaller Time Occupancy
RISMS	Railway Information Security Management Systems
RFI	Rete Ferroviaria Italiana
SIE	Siemens Aktieengesellschaft
SME	Subject Matter Experts
SWAT	Subjective Workload Assessment Technique
SWORD	Subjective Workload Dominance
THA	Thales

Abbreviation / Acronyms	**Description**
TM	Traffic Management
TMS	Traffic Management System: a traffic control-command and supervision/management system, such as ERTMS in the railway sector.
UC	Use Case
UK	United Kingdom
USD	User Centred Design
WP7	Work Package 7: System Engineering of Intelligent Mobility Management (I²M) of In2Rail.
WP8	Work Package 8: Integration Layer of Intelligent Mobility Management (I²M) of In2Rail.
WS	Operator Workstation
VR	Virtual Reality

1 Background

This document constitutes the first issue of Deliverable D7.3 “Specifications of the Standard Operator’s Workstation” in the framework of the Project titled “Innovative Intelligent Rail” (Project Acronym: In2Rail; Grant Agreement No 635900).

D7.3 is main output of Task 7.2 “Standardised Operator’s Workstation”, of In2Rail Work Package 7 “Intelligent Mobility Management (I2M) – System Engineering”. The overall objective of Work Package 7 (WP7) is to provide the specification to validate the Intelligent Mobility Management (I^{2}M) open integrated platform for Traffic Management Systems (TMS). WP7 covers three topics, which come at different development stages of the future Traffic Management System:

- *WP7: Task 7.1*: to carry out the requirement analysis;
- *WP7: Task 7.2*: to specify a Standard Operators’ Workstation allowing the display and control of all services and functions applied in an integrated traffic control centre;
- *WP7: Task 7.3*: to validate an integrated I^{2}M TRL3 proof-of-concept built around the Integration and Application Layer, the Demand Management functionalities and the ‘now casting’ and forecasting of the network assets status.

This report is the main output of Task 7.2.

1.1 Partners Involved

The following companies are involved in Task 7.2:

- Thales (THA);
- Network Rail (NR);
- Siemens Aktieengesellschaft (SIE);
- INDRA Sistemas S.A (INDRA);
- Ansaldo (ASTS);
- Rete Ferroviaria Italiana (RFI).

1.2 Summary of Task 7.2 subtasks

Five sub-tasks have been identified to meet the goals of In2Rail task 7.2. These subtasks are defined as:

- Subtask 7.2.1 – User Requirement Specification: Operator Workstation user requirements are captured and defined; define the end user population, establish use cases, carry out link analysis and review appropriate standards.
- Subtask 7.2.2 – Specification of Security Measures: define security measures for standardised desk: review the current best practice, define audit requirements, define access control and define regulatory compliance.

- Subtask 7.2.3 – Design Guidelines for Standardised Desk: define design guidelines for standardised desk: define maintenance and environmental requirements and ensure inclusive design principles are followed.
- Subtask 7.2.4 – Conceptual Workstation Design: produce conceptual design for standardised desk: identify appropriate case study from industry and develop sketch of standardised desk; define conceptual design for the Workstation Application.
- Subtask 7.2.5 – Workload Analysis for Operators: define Workload analysis context: review current best practice, define key variables for operational workload, propose framework and test workload toolset.

In order to provide a structure for the partners involved and make clear the lead and support for each task, Table 1.1 was produced. This shows the secondary subtasks that make up the subtasks. For example, 7.2.1.1 (define the end user population) is a secondary subtask of subtask 7.2.1 (User requirements specification). Table 1.1 also indicates which partner was leading (YL blue) and which of the remaining partners were providing support (Y yellow).

This split and allocation of secondary subtasks allowed the work to be shared appropriately between the partners to enable a collaborative approach to be taken. It also allowed cross fertilization of ideas and solutions when addressing complex issues.

During Task 7.2 it became clear that there was a lot of overlap between subtasks 7.2.1, 7.2.3 and 7.2.4. In order to keep the deliverable for this task usable the outputs from these subtasks have been combined to form one section, section 4: Considerations for Future TM Workstation. The result is that the output from all of the subtasks in the above table will be presented in three sections in this report:

- Section 4: Considerations for future TM workstation (combination of subtasks 7.2.1, 7.2.3 and 7.2.4);
- Section 5: Specification of Security Measures (subtask 7.2.2);
- Section 6: Workload Analysis for Operators (subtask 7.2.5).

	Updated task definition	Partner Involvement per subtask					
		Thales	Ansaldo	NR	Siemens	RFI	Indra
7.2.1	User Requirement Specification						
7.2.1.1	Define the end user population for the equipment (roles both operations and engineering)	Y	YL	Y	Y	Y	N
7.2.1.2	Establish the use cases (including consideration for the railway usage (metro Vs highspeed) and operational scenario (normal, abnormal, degraded and emergency) for the equipment such that the tasks required of the various roles can be established.	Y	YL	Y	Y	Y	N
7.2.1.3	Carry out a link analysis of the equipment required to be located on the desk such that functional grouping can be defined	Y	YL	Y	N	Y	N
7.2.1.4	Review appropriate standards to define the current recognised best practice in control room equipment design	Y	YL	Y	N	N	N
7.2.1.5	Derive Workstation requirements to fill gap from 7.1 - Request NR & RFI current TMS workstation requirements and align with functional requirements	Y	YL	Y	N	N	N
7.2.2	Specification of Security Measures						
7.2.2.1	State of the art related to Information Security Management Systems	N	Y	N	Y	Y	YL
7.2.2.2	Definition and design of a Train Traffic Information Security Management System	N	Y	N	Y	Y	YL
7.2.2.3	Synthesis and documentation	N	Y	N	Y	Y	YL
7.2.3	Design guidelines for standardised desk						
7.2.3.1	Defining the maintenance requirements of the equipment (hardware/software)	Y	YL	Y	Y	Y	N
7.2.3.2	Define the environmental requirements for the room and the equipment within the room	Y	YL	N	N	Y	N
7.2.3.3	Consultation with disability groups to define the specific needs of users with special needs	YL	N	N	N	N	N
7.2.3.4	Hold requirements review workshops to rationalise the output from the above tasks to ensure a usable deliverable	Y	YL	N	N	Y	N
7.2.4	Conceptual Workstation Design						
7.2.4.1	Identify appropriate case study from industry	YL	N	N	N	Y	N
7.2.4.2	Develop Sketch of standardised desk based on guidelines & Case study	YL	N	N	N	N	N
7.2.4.3	Develop AutoCad drawings	YL	N	N	N	N	N
7.2.4.4	Operator workstation application: definition of list of views, layout of those views in the screens, and explore the possibility of standardizing any of the views	Y	N	N	YL	Y	N
7.2.5	Workload Analysis for Operators						
7.2.5.1	Review current best practise for workload assessment within the rail industry	YL	Y	Y	Y	Y	N
7.2.5.2	Define the key variables for operational workload such that they can be considered during the design of the assessment	YL	Y	Y	Y	Y	N
7.2.5.3	Propose a framework / tool set for assessing operational workload that could be applied consistently across deployments	YL	Y	Y	Y	Y	N
7.2.5.4	The final task will be to test the workload tool set under controlled conditions against the use cases established as part of 7.2.1	YL	Y	Y	Y	Y	N

Table 1.1: A table to show the detailed subtask and secondary subtask breakdown per partner

2 Objective / Aim

2.1 Objective

The objective of Task 7.2 is to design a Traffic Management (TM) "Standard Operator's Workstation" that allows the user to display and manage all services and functions applied in an integrated Traffic Control Centre.

The solution draws upon best practice in the principles of workstation design, use of emerging technologies where possible but most importantly, the design must have the flexibility to support the future needs of TM control room operators.

2.2 Document Structure

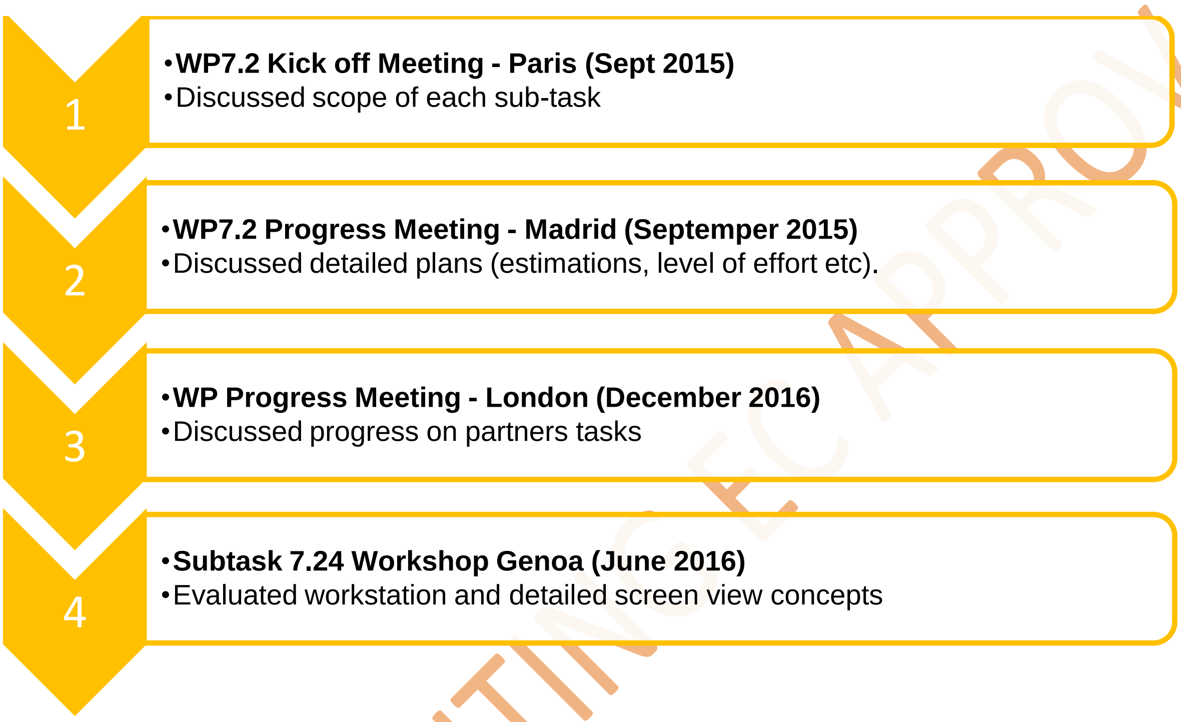
This document contains the following sections:

- **Section 3: The design process followed:** this section gives an overview of the key workshops and meetings held in order to produce this report and evaluate TM workstation design and HMI concepts;
- **Section 4: Considerations for future TM workstations:** this section contains the output of subtasks 7.2.1 "User Requirements Specification", subtask 7.2.3: "Design Guidelines or Standardised Workstation" and Subtask 7.2.4: "Conceptual Workstation Design". As stated in Section 1.2, the output from these subtasks has been combined as there is a natural link between them. It was therefore felt that it would provide an improved reader experience to combine them;
- **Section 5: Specification of security measures:** this section provides the output of subtask 7.2.2 and gives an overview of security measures and security measures in the context of traffic management;
- **Section 6: Workload analysis for operators:** this section provides the output of subtask 7.2.5 and gives an overview of generic workload principles, workload principles in the context of traffic management and provides an In2Rail toolset to measure and predict workload in future TM systems.
- **Section 7: Conclusion:** this section provides a summary of each of the key subtasks findings; Considerations for traffic management workstations (Section 4), Specification of security measure (Section 5) and Workload analysis for operators (section 6).

3 Design Process

This section gives an overview of the workshops and meetings that have taken place as part of Task 7.2.

There have been four major workshops and face to face meetings that have taken place throughout Task 7.2. A summary of these workshops and meetings can be seen below:



1
- **WP7.2 Kick off Meeting - Paris (Sept 2015)**
- Discussed scope of each sub-task

2
- **WP7.2 Progress Meeting - Madrid (Septemper 2015)**
- Discussed detailed plans (estimations, level of effort etc).

3
- **WP Progress Meeting - London (December 2016)**
- Discussed progress on partners tasks

4
- **Subtask 7.24 Workshop Genoa (June 2016)**
- Evaluated workstation and detailed screen view concepts

Note as well as the above workshops and meetings, monthly teleconferences were held between all partners to review progress and raise any project risks or issues.

4 Considerations for Future TM Workstations

This section contains the output of the following subtasks:

- Considerations for future TM workstation (Combination of subtasks 7.2.1, 7.2.3 and 7.2.4);
- Specification of Security Measures (Subtask 7.2.2);
- Workload Analysis for Operators (Subtask 7.2.5).

4.1 Key terminology

The following terminology is used throughout this report and it is important that everybody has the same understanding:

The **operator workstation** is a key component of the integrated traffic control centre that allows the display and control of all services and functions by an Operator. It consists of:

- **Hardware**, constituted by a processor unit and a set of input and output devices (HMI) aimed to facilitate physically the interaction with the operator.
- **Software**, usually organized in a layered structure, where the application occupies the top level.

In the context of the In2Rail WP7, "integrated traffic control centre" is a term that refers to the Traffic Management Systems (TMS) and dispatching systems of the future, for the next 25 years.

An **operator** is any person that is allowed to interact with the TMS. It is assumed that Operators are employees of a Railways Infrastructure Manager (IM). Operators may play at least one defined role according to the organization in the IM.

The **application** is the main component from a functional point of view of Operator Workstation. It implements the functional requirements specification as well as the human-machine interface (HMI) with Operator.

The HMI comprises of:

- **Input devices:** which are the means that the Operator can use to release commands and control the railways signalling system. Input devices may be implemented by different technologies;
- **A graphical user interface:** where the railways signalling system is represented as well as the operational status of the TMS components, through a set of graphical resources such as layouts and views.

4.2 Design Journey

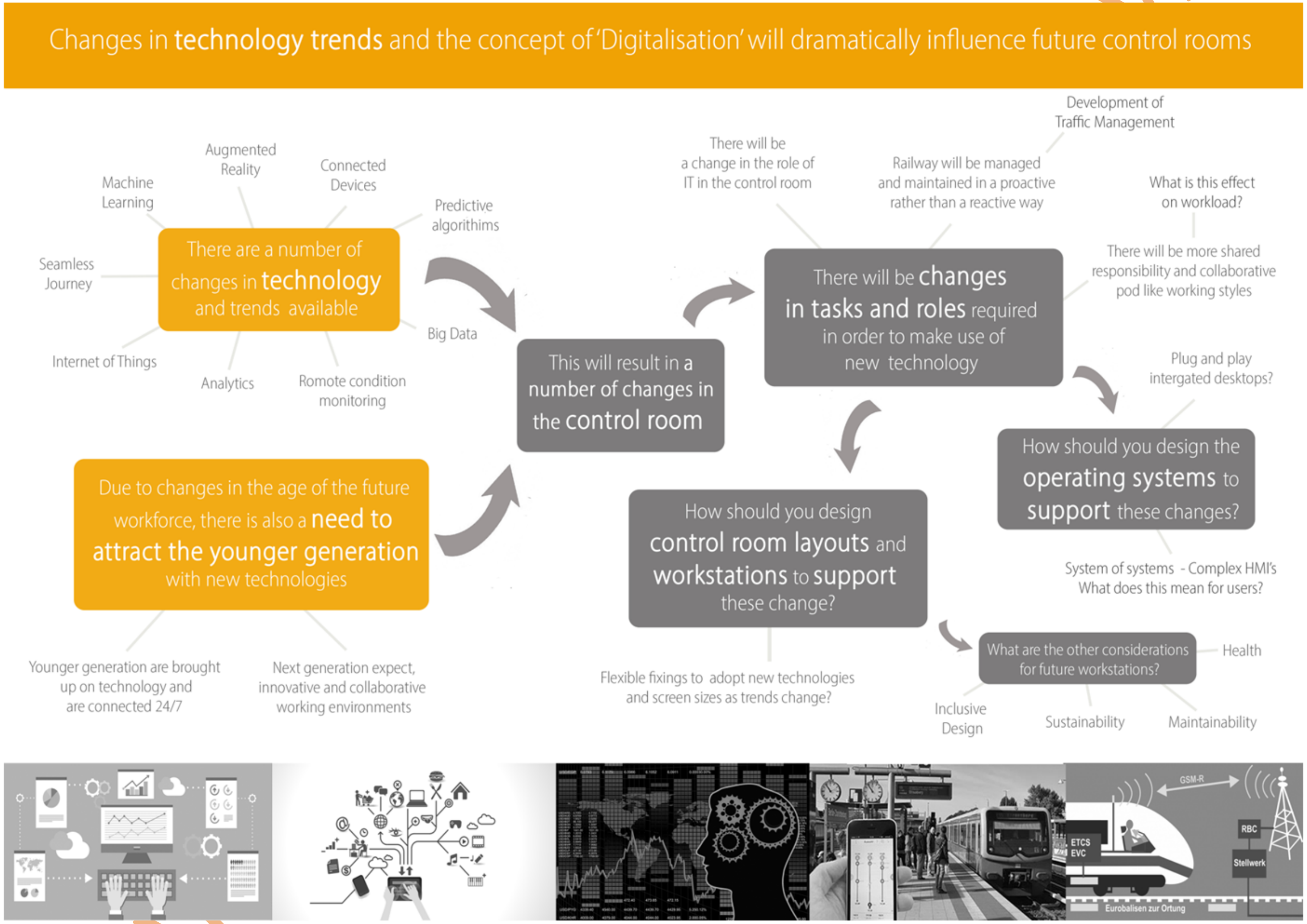
Throughout the document are a number of graphical images aiming to explain concepts or considerations. These images will be referred to as 'the design journey' and set the scene for the problem space that needs to be resolved by future workstation design and operational role requirements. They should help the reader understand the thought process of the partnership during the analysis and decision making.

Figure 4.1 describes the problem space and the impact that technology changes will have on future control room considerations.

Figure 4.2 describes the high level model of future control room's concept of operations. Operators in the control room are expected to form multi-disciplinary, collaborative teams that are able to proactively monitor and control the railway.

Figure 4.3 describes how the future 'pod working' is expected to operate in normal operation. Task boundaries and responsibilities will be well defined and clear. Pod working is the concept that a group of individuals work closely together as a team in order to work towards common goals in a collaborative working style.

Figure 4.4 describes how the future 'pod working' is expected to operate in degraded operation. The pod will use shared information to collaboratively problem solve during incidents and degraded modes. There will be shared responsibility.



Changes in **technology trends** and the concept of 'Digitalisation' will dramatically influence future control rooms

There are a number of changes in **technology** and trends available

Augmented Reality

Connected Devices

Machine Learning

Predictive algorithms

Seamless Journey

Big Data

Internet of Things

Analytics

Romote condition monitoring

This will result in **a number of changes in the control room**

Due to changes in the age of the future workforce, there is also a **need to attract the younger generation** with new technologies

Younger generation are brought up on technology and are connected 24/7

Next generation expect, innovative and collaborative working environments

There will be a change in the role of IT in the control room

Railway will be managed and maintained in a proactive rather than a reactive way

Development of Traffic Management

There will be **changes in tasks and roles** required in order to make use of new technology

What is this effect on workload?

There will be more shared responsibility and collaborative pod like working styles

Plug and play intergated desktops?

How should you design the **operating systems** to **support** these changes?

System of systems - Complex HMI's
What does this mean for users?

How should you design **control room layouts** and **workstations** to **support** these change?

Flexible fixings to adopt new technologies and screen sizes as trends change?

What are the other considerations for future workstations?

Health

Inclusive Design

Sustainability

Maintainability

Figure 4.1: Design Journey Image 1 - Future control room considerations

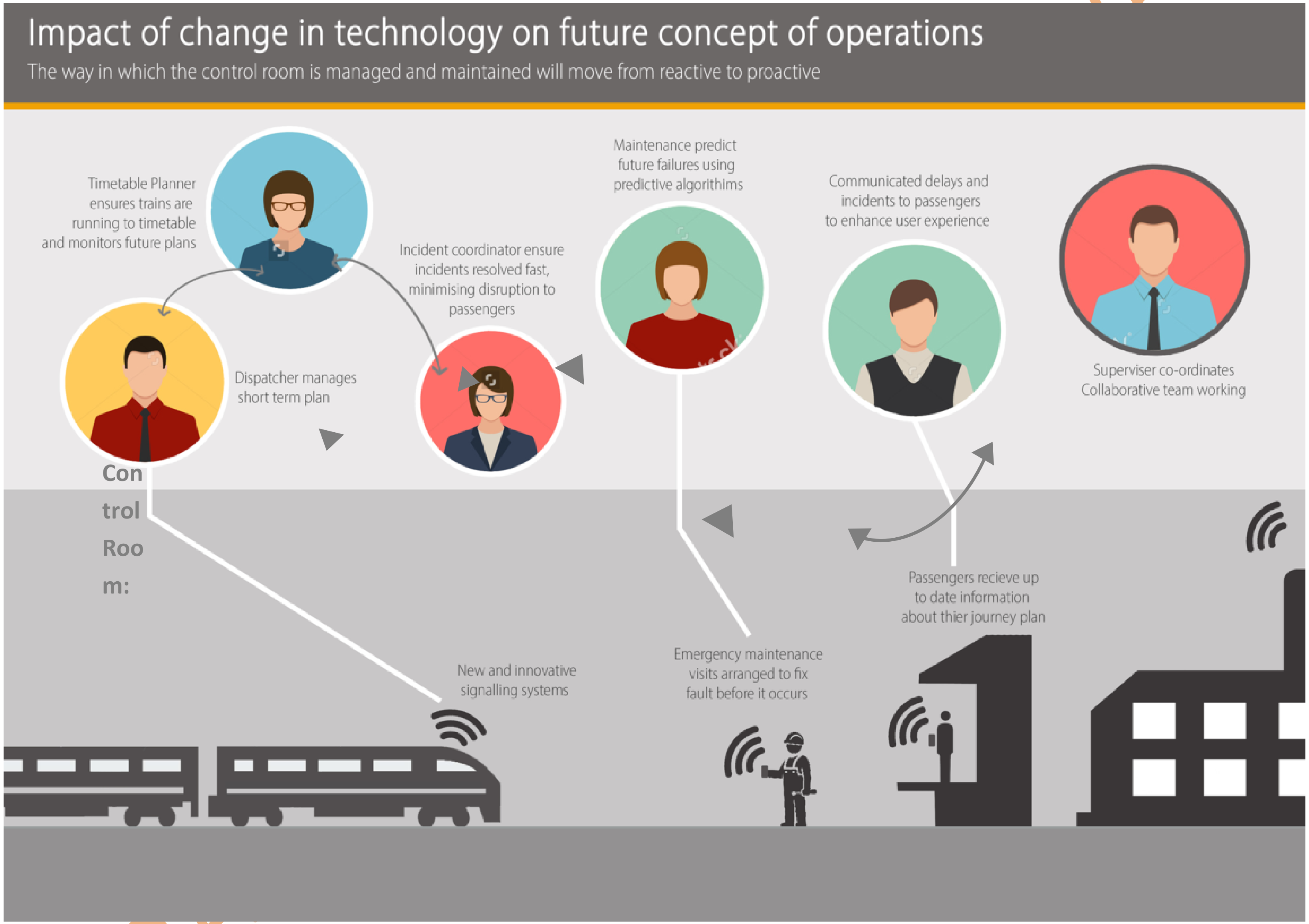
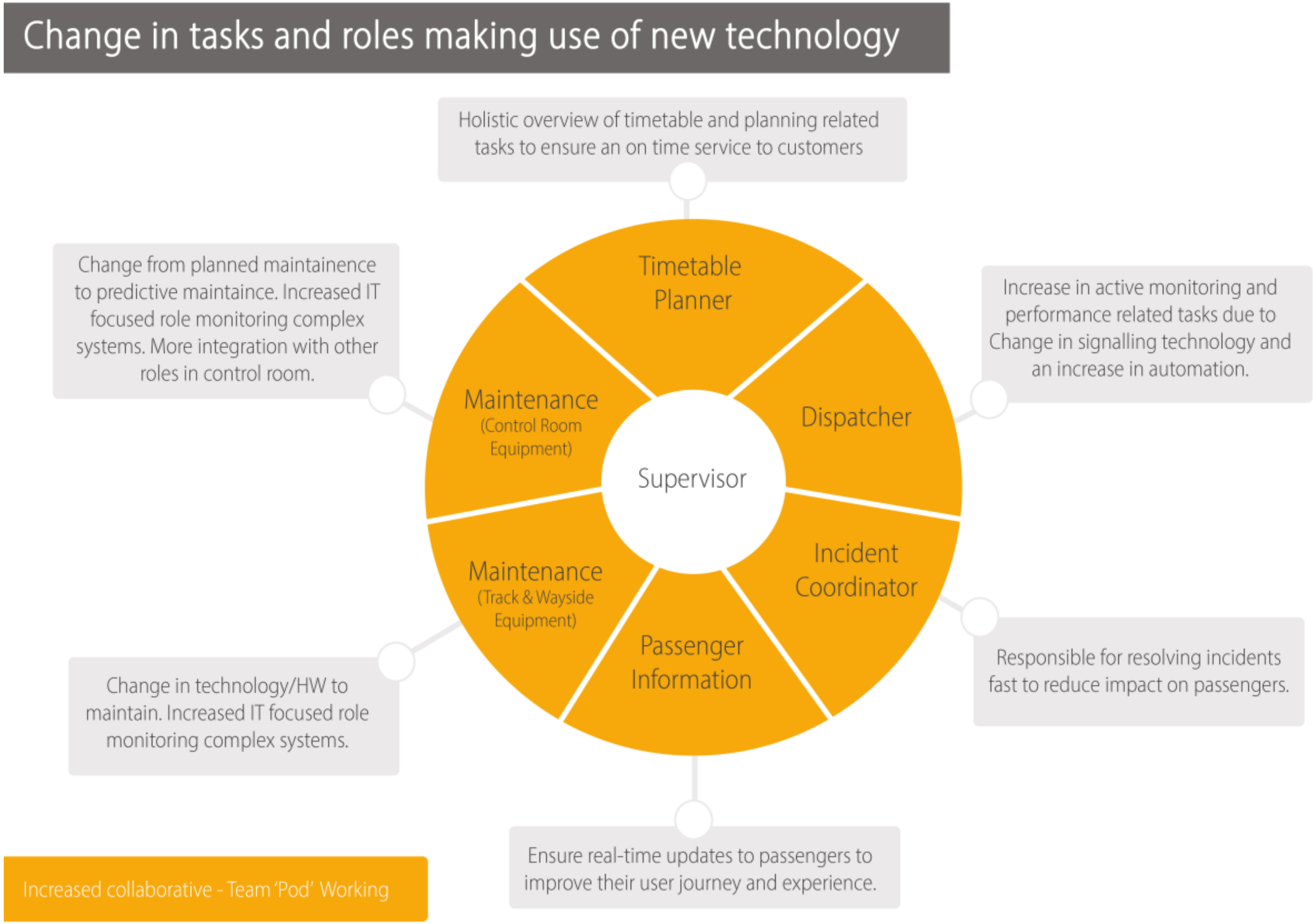

Impact of change in technology on future concept of operations
The way in which the control room is managed and maintained will move from reactive to proactive
Timetable Planner ensures trains are running to timetable and monitors future plans
Dispatcher manages short term plan
Incident coordinator ensure incidents resolved fast, minimising disruption to passengers
Maintenance predict future failures using predictive algorithms
Communicated delays and incidents to passengers to enhance user experience
Superviser co-ordinates Collaborative team working
Control Room:
New and innovative signalling systems
Emergency maintenance visits arranged to fix fault before it occurs
Passengers recieve up to date information about thier journey plan

Figure 4.2: Design Journey Image 2 - Changes to concept of operations



Change in tasks and roles making use of new technology

Holistic overview of timetable and planning related tasks to ensure an on time service to customers

Change from planned maintainence to predictive maintaince. Increased IT focused role monitoring complex systems. More integration with other roles in control room.

Increase in active monitoring and performance related tasks due to Change in signalling technology and an increase in automation.

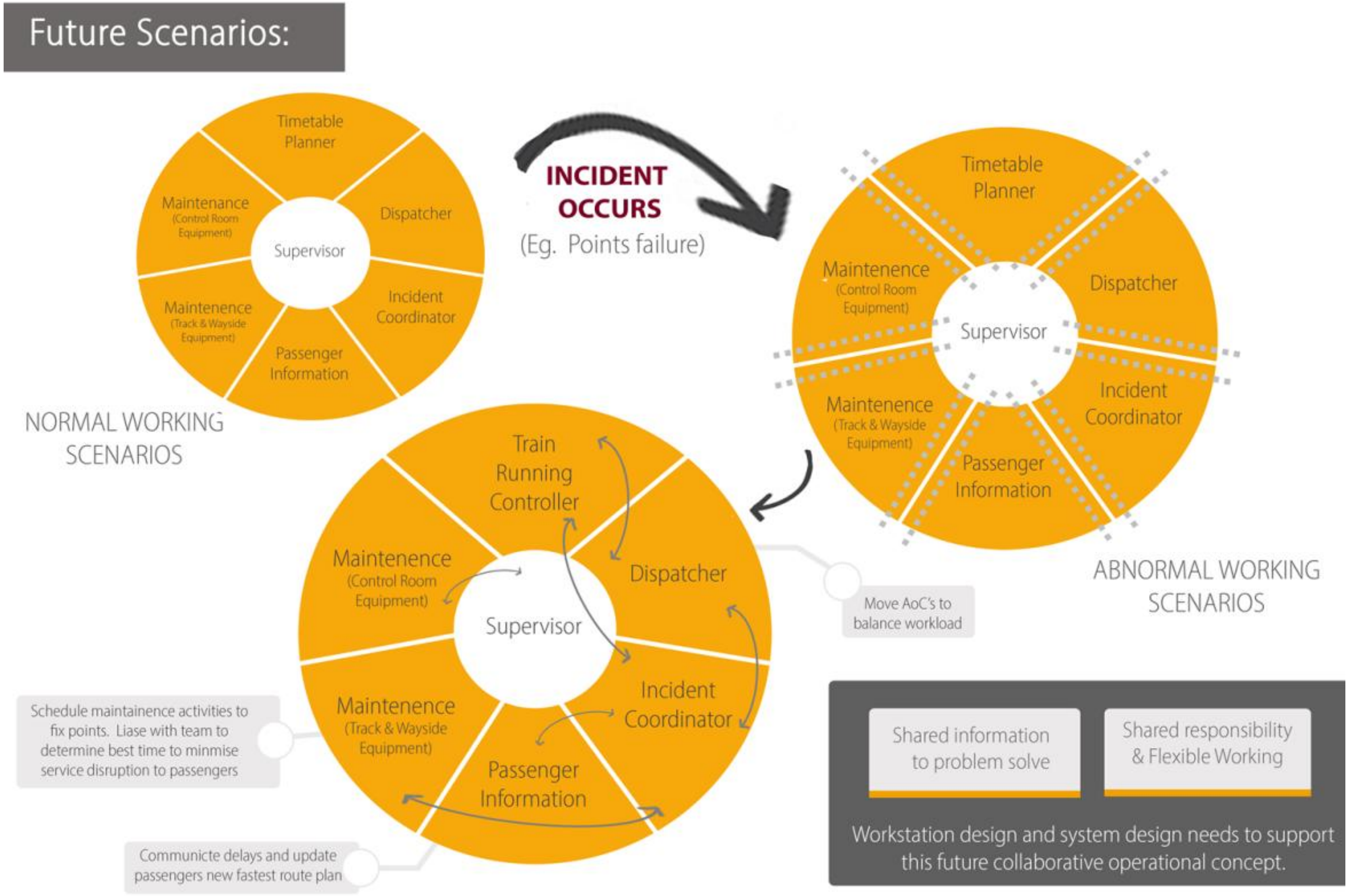
Change in technology/HW to maintain. Increased IT focused role monitoring complex systems.

Responsible for resolving incidents fast to reduce impact on passengers.

Ensure real-time updates to passengers to improve their user journey and experience.

Increased collaborative - Team 'Pod' Working

Figure 4.3: Design Journey Image 3 - Changes to concept of operations



Future Scenarios:

NORMAL WORKING SCENARIOS

Timetable Planner
Dispatcher
Incident Coordinator
Passenger Information
Maintenence (Track & Wayside Equipment)
Maintenance (Control Room Equipment)
Supervisor

INCIDENT OCCURS
(Eg. Points failure)

ABNORMAL WORKING SCENARIOS

Timetable Planner
Dispatcher
Incident Coordinator
Passenger Information
Maintenence (Track & Wayside Equipment)
Maintenence (Control Room Equipment)
Supervisor

Train Running Controller
Dispatcher
Incident Coordinator
Passenger Information
Maintenence (Track & Wayside Equipment)
Maintenence (Control Room Equipment)
Supervisor

Move AoC's to balance workload

Schedule maintainance activities to fix points. Liase with team to determine best time to minmise service disruption to passengers

Communicte delays and update passengers new fastest route plan

Shared information to problem solve

Shared responsibility & Flexible Working

Workstation design and system design needs to support this future collaborative operational concept.

Figure 4.4: Design Journey Image 3 - Changes to concept of operations

4.3 User Requirements

The number of roles and the different types of roles change depending on the size of the geographical area, the complexity of track and volume of traffic. In the future there will be an increase in multi-skilled teams working together on a wider area increasing the complexity of defining user requirements.

During the Concept Workstation Review – (which took place on the 6th June 2016) a number of differences regarding roles required by NR and RFI were discussed. These differences are as a result of how the railway is managed in different counties and the size and complexity of different geographical areas.

As a result of these differences, this section aims to summarise best practice in roles and high level tasks, however it should be noted that these user roles may need to be adapted for each deployment of TM. As a result of differences in roles per deployment, it is useful for user requirements specification to be "function oriented". Each deployment of TM can then allocate the functions to different roles as required.

4.3.1 Roles and Functions

The below roles have largely been developed taking best practice from the NR TMS 1st deployment project in the UK. However, it is important that the concept of operations in the UK supports other countries concepts of operations. See section 4.3.2 for how these roles were reviewed with RFI to determine suitability for RFI current concept of operations.

Operational Roles:

Dispatcher(s):

- Access the traffic control functionality
- Access the train tracking functionality such a s track diagram,
- Access the overview and detailed views
- Perform the management of protections on the Interlocking (IXL)
- Access the traffic management functionality
- Manage short term plan

Note: a dispatcher is normally referred to as a signaller in the UK.

Timetable Manager/Planner

- Manage mid-term and long term planning
- Access the Integrated Train Planning System (ITPS)
- Access the Possession Planning System (PPS)

Incident Co-ordinator

- Perform actions and coordination of countermeasures in case of accident
- Access the Control centre integrated log (CCIL)
- Access the Fault management system (FMS)
- Ensures incidents are resolved fast to minimise impact and delays to passengers

Supervisor

- Co-ordinates collaborative team working
- Operate on the controlled geographical area
- Access the traffic management functionality
- Access the train tracking functionality
- Access the overview and detailed views
- View the status of the protections set on the IXL
- Handover to another supervisor on the same workstations

Customer Information Manager

- Update customers journey plan
- Provide information on delays or incidents to customers to manage user experience

Support Roles:

Administrator:

- Manage users and passwords of the personnel authorized to access and operate on the workstations (and on the TMS itself)
- Manage the roles of the personnel authorized to access and operate on the workstations (and on the TMS itself).

Maintainer (Control Room Equipment):

- Manage the alarms of faulty equipment in the control room
- Maintain equipment to prevent faults
- React to and resolve hardware or software failures in the control room

Maintainer (Infrastructure and Assets):

- Manage maintenance of rail assets e.g. points, track, signals etc.
- Work with incident co-coordinator to resolve incidents quickly with minimal impact to service.

4.3.2 Evaluation of Roles

The roles as proposed in section 4.3.1 were reviewed by RFI to determine how they compare to RFI's current concept of operations. This was carried out to highlight the business change required in order to make use of the future TM roles.

RFI's current functional roles:

- Rail undertakings contact person (RIF);
- Dispatcher (DCO);
- Regulator;
- Public address responsible (RIC);
- Infrastructure diagnostic responsible (CEI).

Roles and tasks proposed in section 4.3.1 compared to RFI's current roles:

- Monitor the running of the service and monitor a number of information sources to determine if they need to intervene to achieve as close to the plan as possible. (Regulator/RIF);
- Make medium-term and long-term re-planning decisions to resolve train conflicts. (Regulator);
- Work with the Signaller (Dispatcher - DCO) to determine the impact of any medium-term and long-term re-planning decisions on the future plan. (Regulator);
- Operate on the controlled geographical area. (Regulator);
- Access the traffic management functionality. (Regulator);
- Access the train tracking functionality. (Regulator);
- Access the overview and detailed views. (Regulator);
- View the status of the protections set on the IXL. (Regulator);
- Traffic control functionality. (DCO);
- Train tracking functionality. (DCO);
- Overview and detailed views. (DCO);
- Perform the management of protections on the IXL. (DCO);
- Access the traffic management functionality. (DCO);
- Responsible for managing incidents, creating plans to resolve incidents and disruptive events. (DCCM);
- Track response to resolve incidents. (DCCM/Regulator);
- Liaise with control centre technician (maintainer) when incidents are related to failures from trackside/wayside equipment etc. (DCCM/DCO/CEI);
- Provide customers with update information regarding the service, if it is on time, delayed or if there has been an incident. (RIC);
- During disruptions organise alternative transport for passengers. (DCCM/RIC/Regulator);
- Manage users and passwords of the personnel authorized to access and operate on the workstations (and on the TMS itself). (Technical Department);
- Manage the roles of the personnel authorized to access and operate on the workstations (and on the TMS itself). (Technical Department);
- The TMS allow the maintenance operator to manage the alarms. (CEI).

The above summary shows there are a number of differences of how tasks are allocated to different roles. The list of roles in section 4.3.1 suggests generic EU suitable roles for In2Rail, however as stated, it is useful for user requirements specification or tasks to be "function oriented". Each deployment can then assign tasks to roles that support their concept of operations and business processes.

It should be noted that as TM is introduced, current and future concept of operations are likely to change, therefore business processes that are implemented today, are likely to change in the future. Any change to concept of operations due to TM should be carefully managed by business change experts, training and efficient processes and procedures.

4.3.3 Use Cases

Based on the roles in section 4.3.1, a number of uses cases were generated, see the Use Case document inserted below.

In2Rail_WP7
2.1_UseCases.xlsx

The use cases captured in the above document were used to influence workstation concepts and detailed view concepts in sections 4.9 and 4.10 respectively.

4.4 Design Guidelines for Standardised TM Workstation

This sections details some design guidance and best practice that should be referred to as part of future TM workstations. This guidance covers:

- Workstation design;
- Guidance for associated equipment;
- Environmental requirements;
- Maintenance considerations;
- Common control centre issues to be resolved.

4.4.1 Workstation design considerations

There are a number of components regarding workstation design to consider such as:

- The user and their tasks required;
- The size and shape of the workstation;
- The hardware and layout of equipment on the workstation;
- The different systems displayed to the user, such as planning or signalling software.

Within these components, there are a number of key principles to consider for future workstation design relating to technology changes, roles and concept of operations changes, the need to provide an ergonomic workstation and a healthy working environment.

Although it is important to address the above principles in future workstation design, the key and most challenging issues to resolve are the future user issues such as enabling intelligent decision support and supporting distributed cognition.

4.4.2 Approach to Workstation Design

Ergonomic best practice for workstation design is to ‘fit the equipment to the user’. This approach can be achieved by following a user centred design process to determine initial concepts, right the way through to assuring final designs. However, due to project constraints there are often two approaches to workstation design:

- Approach 1: What size or shape can a workstation be?
- Approach 2: What size or shape should a workstation be?

Approach 1: What size or shape can a workstation be?

This approach is often constrained by the size of the control room available, the number of roles required and or the workstation itself, i.e. there may be scope for equipment changes or equipment layout changes but no scope to change the desk itself.

Example of constrained design process:

1. Size of the control room is defined.

2. Determine how many roles are required in the control room based on forecasting or predictive workload methods.
3. Determine the maximum size of each desk to ensure all desks required fit in the allocated space available.
4. Determine the size and layout of the equipment based on the footprint of required desk size.

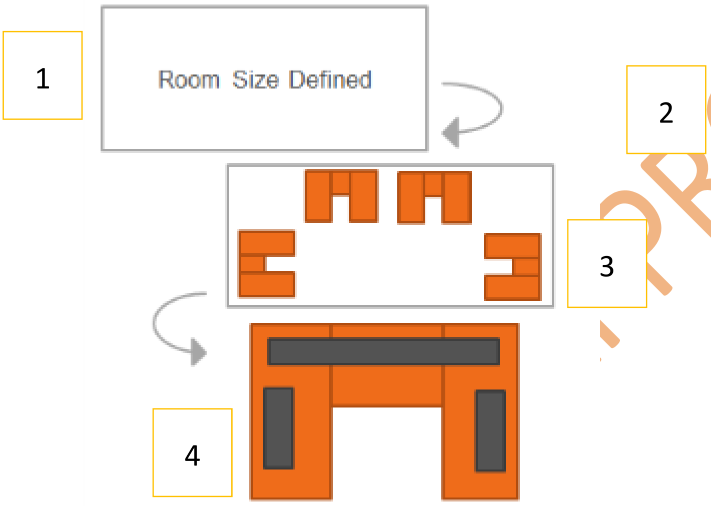


Figure 4.5: Image to Constrained Workstation Design Process

Although this is not best ergonomic practice, this is a common constraint and a method needs to be developed to ensure ergonomic principles are applied as far as practically possible in this instance.

Where there is scope to alter the workstation equipment or layout of equipment but the workstation itself is fixed, assistive devices can be used to support the user in simulating the effect of a sit stand workstation. For example, a free-standing sit-stand adaptor can be used that raises a monitor and keyboard and enables a sit-and-stand working style to be achieved.

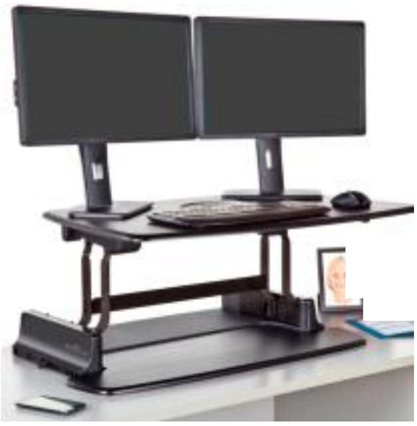


Figure 4.6: Example of Free-Standing Sit-Stand Adaptor

Approach 2: What size or shape should a workstation be?

In this approach, the workstation design should be determined based on the user, their tasks and the equipment required enabling the user to perform their tasks effectively. This is best ergonomic practice as it fits the equipment to the user.

User Centred Design Process:

1. Determine what tasks each user needs to achieve and therefore determine the equipment required and size of equipment required, (within ergonomic constraints).
2. Design system and workstation based on user's tasks and review workstation concepts with end users to gather their feedback and improve designs based on their feedback.
3. Determine how many roles are required in the control room based on forecasting and predictive workload methods.
4. Determine control room size based on the number of roles required and the size of desk required.

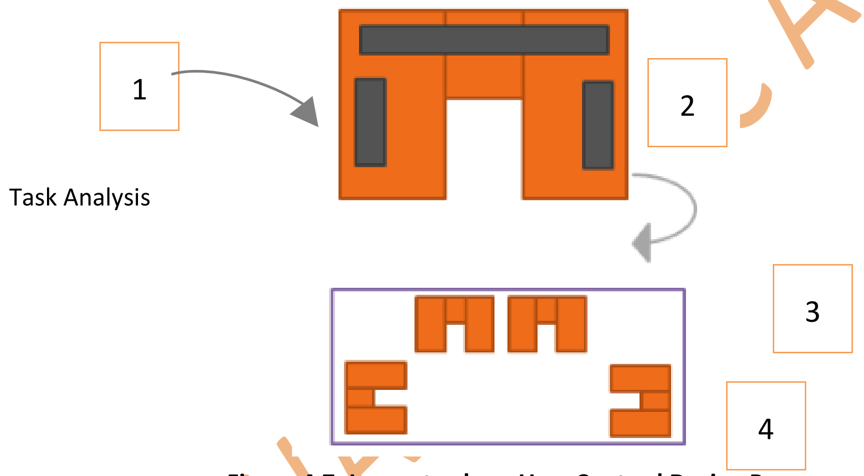


Figure 4.7: Image to show User Centred Design Process

Due to the challenge that within each future TM project the approach to determining workstation size will differ, there is a need to identify key ergonomics principles that apply to approach one and two and should be considered in order to determine a 'base design'. However, it should be noted that although there are often two approaches to workstation design as stated above, for the purpose of this subtask the design of the conceptual workstation will follow approach two as far as possible within the scope of deliverable 7.3.

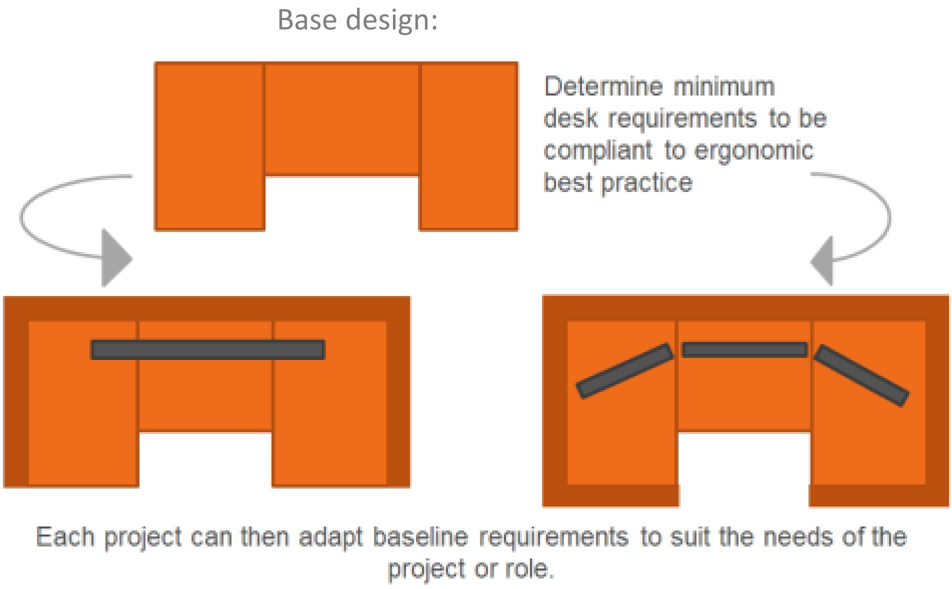

Base design:
Determine minimum desk requirements to be compliant to ergonomic best practice
Each project can then adapt baseline requirements to suit the needs of the project or role.

Figure 4.8: Ergonomic Base Design

4.4.3 Ergonomic Principles to be applied to the TM Workstation

There are a number of useful standards and guidelines for workstation design. A list of these useful guidelines can be seen below:

- Ergonomic design of control centres – Layout and dimensions of workstations: ISO 11064-4;
- Office furniture – work tables and desks BS EN 527-1:2001;
- Office work VDTS's: ISO 9241 Part 1, 2, 4, 5, 6 and 9.

Based on the above standards the following key ergonomic areas to be considered at a minimum to determine the base design are:

- Type of workstation;
- The end user population;
- Postures;
- Reach;
- Viewing cones and distances;
- Monitor arrangement and layout.

Note the above areas are summarised in sections 4.4.3.1– 4.4.3.7.

Other additional areas to consider in workstation design are environmental and maintenance principles. Examples of relevant environmental standards include:

- ISO 7731, Ergonomics — Danger signals for public and work areas — Auditory danger signals;
- ISO 7779, Acoustics — Measurement of airborne noise emitted by information technology and telecommunications equipment;

- ISO/CIE 8995, Lighting of indoor work places;
- ISO 13731, Ergonomics of the thermal environment — Vocabulary and symbols;
- IEC 60651, Sound level meters — Electromagnetic and electrostatic compatibility and test procedures.

Note the environmental and maintenance principles to consider are summarised in sections 4.4.5 and 4.4.6.

4.4.3.1 Types of workstations

There are two main types of workstations, fixed height and flexible height. The majority of current signaller workstations make use of fixed height workstations, however it is highly recommended that the In2Rail workstation should support sit stand functionality due to health and performance benefits, [References 4-11]. The following principles should be considered in sit stand workstations, [Ref 1]:

- Sit-stand workstations should have an adjustable floor to work surface height between 650mm and 1250mm measured at the work surface front top edge;
- The rise-fall mechanism needs to be capable of being operated reliably over the target lifetime of the desk;
- The desk needs to be designed to prevent undue mechanical strain or damage to any equipment or cabling.

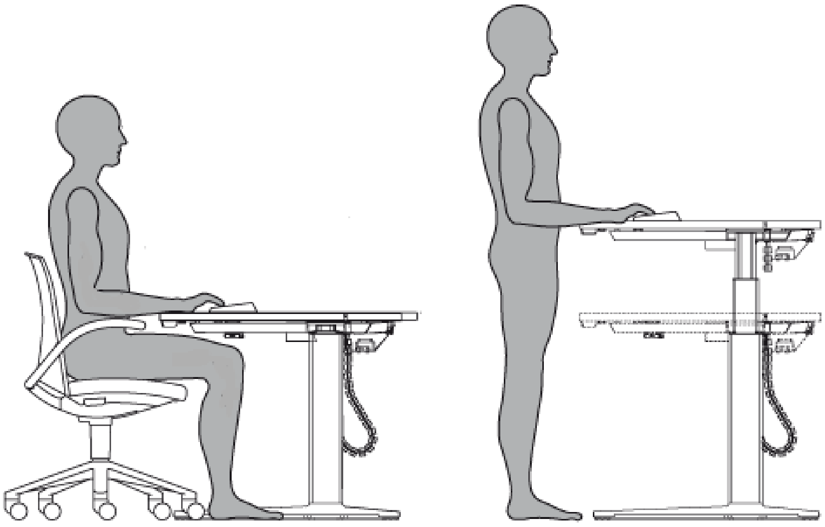


Figure 4.9: Sit Stand Workstation Side profile

Benefits and rationale for sit stand workstations, [References 4-11]:

- Prolonged static postures in the workplace increase the risk of health problems such as diabetes and musculoskeletal disorders;
- The National Health Service (NHS) in the UK recommends taking breaks and moving every 30 – 40 minutes, however it is unknown whether this is also a European guideline for this recommendation;

- Working in a perched or standing position burns more calories, than sitting and recent research shows it encourage users to be more alert which in turn improves performance.

4.4.3.2 End user population

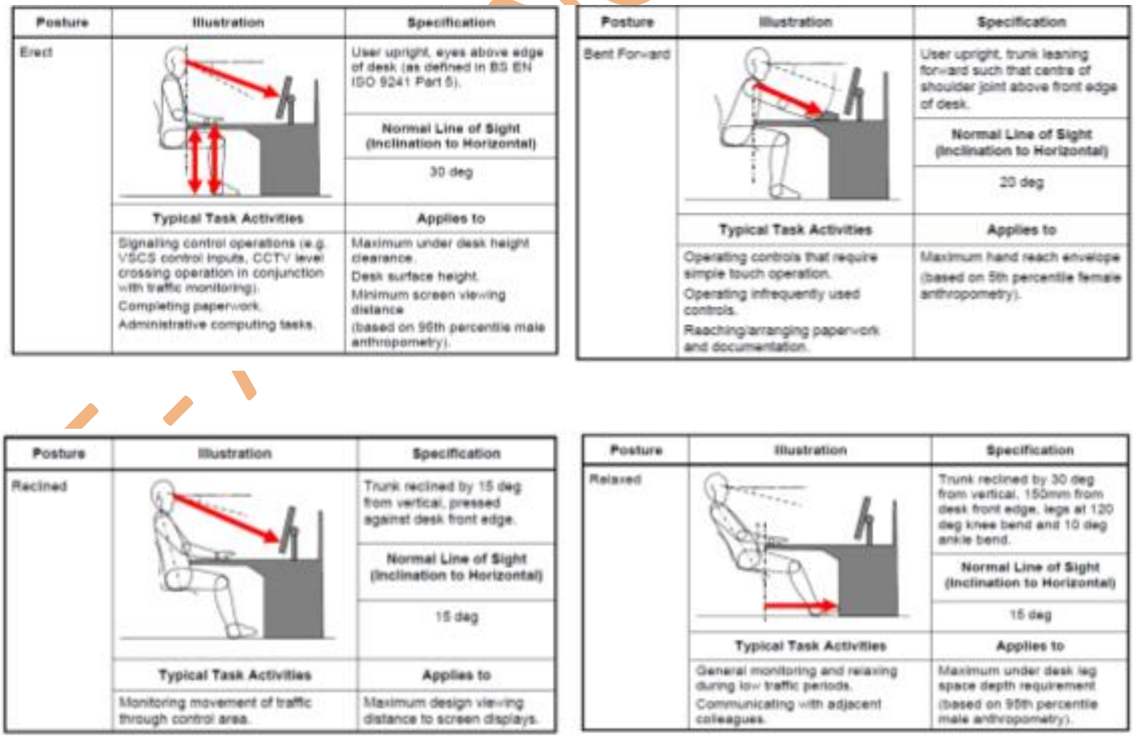
Desks should be designed for use by a target population[1] of users defined by the following anthropometric limits:

- Shortest/smallest: 5th percentile Female (18-65 years);
- Tallest/largest: 95th percentile Male (18-65 years).

Desks should support impairments defined applicable to TM, see the output from section 4.5.

4.4.3.3 Postures

To ensure the workstation design is suitable, the monitors and equipment available must take into account the needs and constraints of the user via analysis of the top view (plan) and from the vertical (elevation view). When evaluating the users via plan and elevation view analysis, the following postures should be taken into account and used to evaluate workstation designs layout of equipment (UNI EN 11064).



Posture	Illustration	Specification
Erect		User upright, eyes above edge of desk (as defined in BS EN ISO 9241 Part 5).
		Normal Line of Sight (Inclination to Horizontal)
		30 deg
	Typical Task Activities	**Applies to**
	Signaling control operations (e.g. VSCS control inputs, CCTV level crossing operation in conjunction with traffic monitoring). Completing paperwork. Administrative computing tasks.	Maximum under desk height clearance. Desk surface height. Minimum screen viewing distance (based on 95th percentile male anthropometry).

Posture	Illustration	Specification
Bent Forward		User upright, trunk leaning forward such that centre of shoulder joint above front edge of desk.
		Normal Line of Sight (Inclination to Horizontal)
		20 deg
	Typical Task Activities	**Applies to**
	Operating controls that require simple touch operation. Operating infrequently used controls. Reaching/arranging paperwork and documentation.	Maximum hand reach envelope (based on 5th percentile female anthropometry).

Posture	Illustration	Specification
Reclined		Trunk reclined by 15 deg from vertical, pressed against desk front edge.
		Normal Line of Sight (Inclination to Horizontal)
		15 deg
	Typical Task Activities	**Applies to**
	Monitoring movement of traffic through control area.	Maximum design viewing distance to screen displays.

Posture	Illustration	Specification
Relaxed		Trunk reclined by 30 deg from vertical, 150mm from desk front edge, legs at 120 deg knee bend and 10 deg ankle bend.
		Normal Line of Sight (Inclination to Horizontal)
		15 deg
	Typical Task Activities	**Applies to**
	General monitoring and relaxing during low traffic periods. Communicating with adjacent colleagues.	Maximum under desk leg space depth requirement (based on 95th percentile male anthropometry).

Figure 4.10: References Posture to Consider [Ref 1]

[1] The anthropometric data used should be the same as or similar to the country of deployment

It should be noted that it is good practice that the referenced postures above should be analysed and documented to ensure equipment layout satisfies requirements. From each reference posture, the following should be considered reach, horizontal and vertical viewing cones, (see sections 4.4.3.4 – 4.4.3.6).

4.4.3.4 Reach

Acceptable reach should be determined according to two reach envelopes - 'Normal Reach Envelope' and 'Extended Reach Envelope', [Ref 1]:

1. The 'normal reach envelope' should be defined where any In2Rail devices lie within the reach envelope of the smallest member of the user population when seated in the 'erect' position with forearms resting horizontally on the desk work surface.
2. The 'extended reach envelope' shall be defined where the In2Rail device lies within the reach envelope of the smallest member of the user population when seated in the 'bent forward' position.

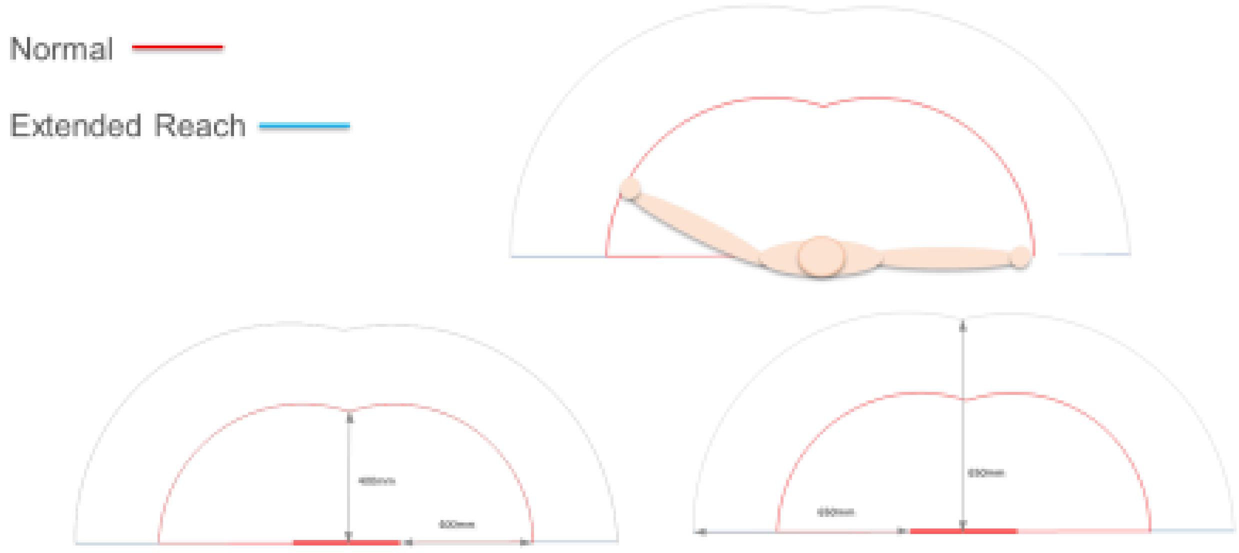


Figure 4.11: 5th percentile Female Normal and Extended Reach

4.4.3.5 Viewing Cones and Distances

4.4.3.5.1 Vertical Viewing Cones

- The normal line-of-sight is defined as a perpendicular to the centre of the screen array;
- The acceptable vertical viewing zone for the upright position is defined as 40 degrees above and 40 degrees below (80 degree cone) the normal line-of-sight;
- The recommended viewing zone for the upright position is defined as 15 degrees above and 15 degrees below (30 degree cone) the normal line-of sight;

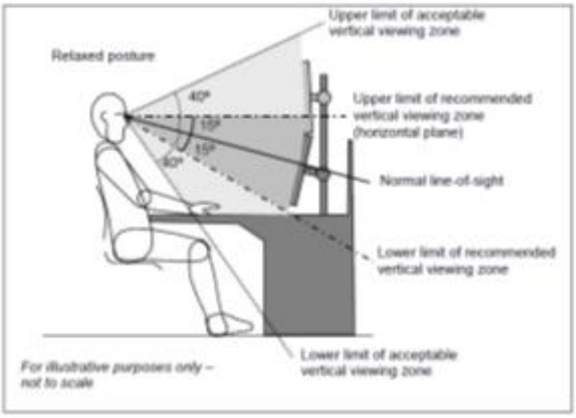

Upper limit of acceptable vertical viewing zone
Relaxed posture
40°
15°
15°
60°
Upper limit of recommended vertical viewing zone (horizontal plane)
Normal line-of-sight
Lower limit of recommended vertical viewing zone
Lower limit of acceptable vertical viewing zone
For illustrative purposes only – not to scale

Figure 4.12: Vertical Viewing Cones [Ref 1]

- Screens used for data entry or monitoring the railway should be placed within the acceptable vertical viewing zone when in the 'reclined' position;
- Screens which do not display items of a critical nature may be placed outside of the acceptable vertical viewing zone.

4.4.3.5.2 Horizontal viewing cones

- The acceptable horizontal viewing zone is defined as 35 degrees to the left and 35 degrees to the right (70 degree cone) of the normal line-of-sight;
- Screens which are frequently used for monitoring the railway should be positioned so that they are within the acceptable horizontal viewing zone when in the 'reclined' position;
- Screens where audible signals draw the user's attention to the display may be positions outside the acceptable horizontal viewing zone.

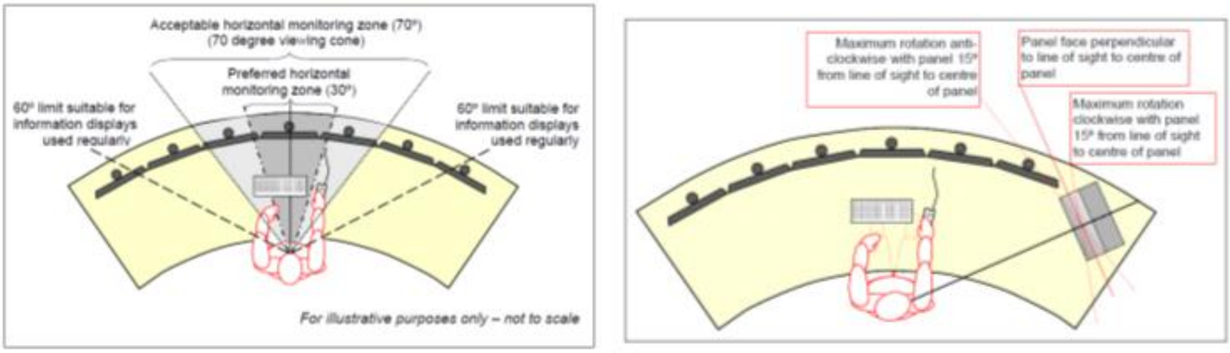

Acceptable horizontal monitoring zone (70°) (70 degree viewing cone)
Preferred horizontal monitoring zone (30°)
60° limit suitable for information displays used regularly
60° limit suitable for information displays used regularly
For illustrative purposes only – not to scale
Maximum rotation anti-clockwise with panel 15° from line of sight to centre of panel
Panel face perpendicular to line of sight to centre of panel
Maximum rotation clockwise with panel 15° from line of sight to centre of panel

Figure 4.13: Horizontal Viewing Cones [Ref 1]

4.4.3.5.3 Viewing Distance

- Dynamic textual information that is critical for In2Rail safety and performance should be a minimum of 15 minutes of arc at the maximum viewing distance for a user seated in the 'reclined' position;
- Static labels and other non-critical textual information displayed on the In2Rail screens should be sized to meet a minimum of 10 minutes of arc at the maximum screen viewing distance.

4.4.3.6 Clearance

- The In2Rail workstation should have a minimum legroom depth of 750 mm at under-surface and at floor-level.
- The In2Rail workstation should enable a seated user with a minimum 300mm lateral leg clearance from the centre line of any computer or control workstation input device(s) to any equipment enclosure or shelving under end sections of the work surface.

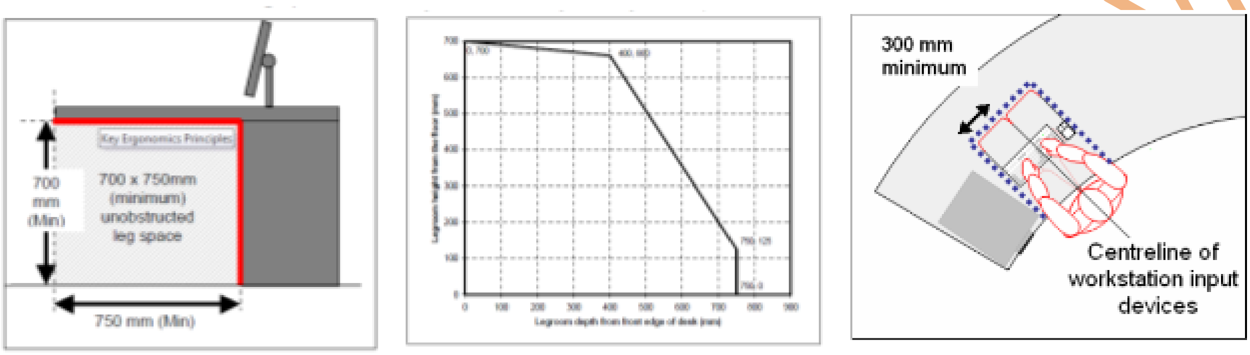

Key Ergonomics Principles
700 mm (Min)
700 x 750mm (minimum) unobstructed leg space
750 mm (Min)
0, 700
400, 660
750, 125
750, 0
0
100
200
300
400
500
600
700
800
900
Legroom height from the floor (mm)
Legroom depth from front edge of desk (mm)
300 mm minimum
Centreline of workstation input devices

Figure 4.14: **Leg clearance principles to consider [Ref 1]**

4.4.3.7 Monitor Arrangement and Layout principles

As the visual field scanned by the human eye affects the number of devices that can be kept under control at the same time, it's important to consider that additional monitors outside the 160° line of a user's vision "straight-ahead" requires a rotation of the head and the lower body in order to view the information displayed. This places strain on the user and can lead to fatigue or musculoskeletal disorders.

Monitors should be placed by first utilising the central portions of the field of view and proceeding gradually to the sides whilst also considering vertical viewing angles.

As well as the principles of vision, reach and clearance already discussed, the monitor arrangement for the workstation depends on the factors listed below:

- The size and shape of the workstation;
- the number of expected and predicted monitors (including future expansion);
- the size of each display;
- the adjustability of each display,
  - The support mechanisms and fixings of the monitor must ensure adjustability. To achieve adjustability, monitor arms and fixings should be selected with appropriate degrees of freedom. It should be noted that the ability to make adjustments of monitor positions is easier with smaller monitors as the size and weight of larger monitors can limit the possibility of adjusting the angle and position of the monitors. In the case of large monitors lateral movement should be made possible as a minimum.

- The hierarchy of information, different operational priority of the information displayed and the frequency of use of monitors or equipment,
  - The most frequently used devices and the most important ones, should have higher priority and must be placed as close to the normal line of vision of the operator as possible. The devices with less priority can be placed in the periphery visual field.
  - The frequently used controls should not be positioned above the height of the 5th percentile users shoulders,
- The controls and displays that are used together should be located near each other,
  - The controls and displays must be organized into functional groups that allow clear and simple identification,
  - The display and the controls that are frequently used in a particular sequence should be arranged according that sequence,
  - If displays are not used in sequence, it is preferable that they are positioned so as to tell the operator the most important information in relation to the task that is expected to be carried out,
- Type of equipment required;
  - Appropriate input devices, (such as mouse, keyboard, numeric keypad etc.), should be selected depending on the type of task required.
- Equipment layout design should take into consideration left handed and right handed users.
- The input devices should not compete for the work surface with other devices:
  - The telephone should be easily accessed in case of emergency,
  - There should be a minimum of 150mm of clear work surface between the work surface front edge and any frequently used input devices,
  - There should have space to enable keyboards to be rotated 30 degrees in the clockwise or anti-clockwise direction,
  - The In2Rail workstation should provide a minimum space of 200mm wide and 240mm length for mouse input devices,
  - The In2Rail workstation should provide space to enable the mouse to be rotated 30 degrees in a clockwise or counter-clockwise direction,
  - Input devices used infrequently may be stored at the back of the desk and moved forward when they are required to be used.

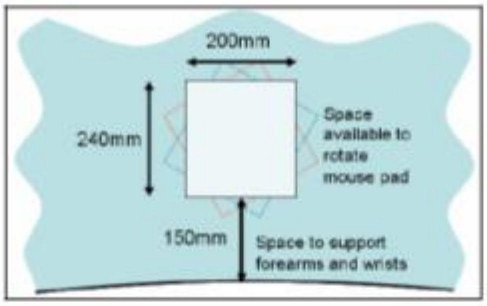

200mm
240mm
Space available to rotate mouse pad
150mm
Space to support forearms and wrists

Figure 4.15: Keyboard required area on workstation [Ref 1]

- Types of tasks required to complete:
  - Signalling screens are often the most frequently used screens for the signaller and will be the most important for the majority of safety related actions.

Therefore these screens should generally be centrally located on the workstation. However, it should be noted that due to the introduction of TM, this principle is likely to change due to greater automation and an increase in planning related tasks required. It is also important to consider the differences in layout of equipment for other roles, not just the signaller role.

4.4.4 Best Practice for Conventional Workstation Equipment and Input Devices

4.4.4.1 Monitor characteristics

The following principles should be considered with regards to monitor selection:

- It is recommended that monitors make use of LCD technology and anti-reflective screens;
- The type, extent and frequency of the control activities are some of the factors to consider in monitors selection;
- Since there is a continuous and prolonged use, (24h operation for 7 days a week), it is necessary to prevent the deterioration of the visual characteristics of the monitor over time;
- In order to display the required information clearly a monitor of suitable size and resolution should be used.
  - Note as the amount of information to display to the user is increasing, monitors sizes used are also increasing which is leading to increased viewing distances. Therefore there is a need to better utilise the monitor sizes displays in order to reduce this issue occurring in future TM workstations;
- Large monitors require particularly robust rear support casings and they involve special activities for handling, installation, repair and replacement.

Additional relevant technical aspects to consider are:

- Brightness (cd / m²);
- the pixel size (mm);
- contrast ratio (e.g. 400: 1, 600: 1);
- the wide viewing angle;
- heat dissipation;
- level of electromagnetic emission.

4.4.4.2 Keyboard principles

The following principles should be considered with regards to keyboard selection and location:

- The keyboard should be placed at the centre of the operator's working space, in relation to the number and controlled positioning of the display;
- The keyboard should be placed a minimum of 15 cm from the edge of the workstation;
- The keyboard shall form shall support the forearm / hand;
- The angle of the keyboard must be user adjustable between 5° and 15°;

- Some of the keys should be marked by a slight relief (tactile feedback), so that they can be recognised by touch without looking at the keyboard;
- The surface finish of the keyboard must be opaque, and must not have reflective parts;
- Black symbols or text on a light background are preferred.

4.4.4.3 Mouse

There are a number of different types of mouse; "trackball", "dial" or "space mouse". The following general guidelines regarding mice should be considered:

- The shape of the mouse must be such as to allow a comfortable grip and a smooth actuation;
- The surface on which the mouse is placed must allow a friction with the sensor command (ball, light beam, etc.);
- The mouse must possess high strength characteristics.

4.4.4.4 Footrest

The seat must be equipped, if necessary, with a separate footrest, to support the lower limbs of the operator. The following should be considered with respect to footrests;

- The footrest can be used to support users falling in smaller anthropometric bands or operators who so request them;
- The footrest must have an inclination of between 10 and 15 degree;
- The depth should be equal to the area of use of the feet and the width equal to the space reserved in the lower limbs;
- The construction material and/or coating must be non-slip and low conductivity to ensure the footrest itself does not easily slip or move out of position.

4.4.4.5 Document Storage or Holders

The following principles should be considered:

- A port-document should be used for documentation that is frequently used to support operators;
- They must be sufficiently strong and resistant to all of the handling;
- It must be able to be easily moved and oriented in order to achieve the most suitable position for the user to read documents.

The port -documents must be able to be positioned to the right or left of the screen and at the same height of the monitor of reference, (if possible).

4.4.5 Environmental Considerations

Part 6 of ISO 11064 gives environmental requirements as well as recommendations for the ergonomic design, upgrading or refurbishment of control rooms and other functional areas within the control suite.

The following aspects are covered here to support this work:

- Thermal environment;
- Air quality;
- Lighting environment;
- Acoustic environment;
- Vibration.

4.4.5.1 General Environmental Principles

- In order to optimize operator performance and comfort, levels of illumination as well as temperature shall be adjustable in accordance with the operators' needs;
- Where conflicting demands exist between different environmental features (i.e. thermal conditions, air quality, lighting, acoustics, vibration, and interior design and aesthetics), a balance shall be sought which favours operational needs;
- Environmental factors work in combination and shall be taken into account in a holistic way, i.e. the whole environmental entity needs to be taken into account, (e.g. interaction between air conditioning systems generating noise and the acoustic environment);
- Environmental design shall be used to mitigate the detrimental effects of shift work, e.g. raising ambient air temperature early in the morning;
- The design of environmental systems shall take account of future change (e.g. equipment, workstation layouts and work organisation).

4.4.5.2 Thermal Conditions

The following factors should be taken into account regarding thermal conditions:

- Climatic factors;
- Heat generated from equipment in use (including equipment and lighting);
- Physical movement required by operators;
- Typical clothing to be worn by operators;
- Operator number and shift patterns;
- The orientation of the control room in respect of solar gain (including thermal transfer from external walls);
- The number of doors and windows;
- Shielding properties of construction materials;
- The potential for shielding direct sunlight;
- The geographical location of the building.

4.4.5.3 Air Quality Guidance

The following factors should be taken into account regarding air quality:

- Airflows shall not cause direct draughts to operator, in order to do this, air velocity shall be checked;
- Extractor grilles should be located to avoid short-circuits between inlets and outlets and to even the distribution of air throughout the room;
- Minimal noise and no vibration to be emitted by the air conditioning system;
- The rate of air change shall be suitable for maintaining good air quality;
- Ingress of dust into the HVAC system ducts should be minimal, as such, ducts should be easily accessible for cleaning and maintenance purposes;
- Operators shall be protected from external air pollution and harmful substances through the air supply.

4.4.5.4 Lighting

The following factors should be taken into account regarding lighting:

- Optimise visual performance for VDU tasks being undertaken by operators;
- Minimize degradation in human performance and enhance safety;
- Enhance legibility of information from both active and passive displays, self-illuminated VDTs (Visual Display Terminal) on and away from workstations, and of printed material;
- Enhance the comfort and health of the operator;
- Operators should have some level of control of local task lighting at their workstation but this must not cause glare or discomfort to other operators in the OCR;
- Ceiling lighting shall avoid veiling reflections and not cause reflected glare off screens;
- Lighting systems should take into account future changes in equipment, workstation layouts, operating procedures, and team working; options for rearrangement of lighting and methods for maintenance should be examined;
- Suitable methods of control over natural light shall be in place to avoid difficulties of intense natural light.

4.4.5.5 Acoustics Guidelines

The following factors should be taken into account regarding acoustics:

The control room should be designed to optimize the acoustic environment:

- Reduce noise levels;
- Reduce sound levels;
- Reduce reverberation times.

The following operational needs should be considered when designing for acoustic optimisation:

- Verbal communication between operators telephone conversations;
- Hearing of alarms, alarms need to be distinguishable from background noise;
- Minimise operator annoyance (e.g. from noisy equipment).
    - If noisy equipment is identified, it should be housed separately in acoustically modified rooms or surrounded with sound shielding

It should be noted that the layout and operational concept can help in optimising acoustics by grouping teams of operators together to improve communication channels and by building telephone use into processes to prevent loud conversations across the room.

4.4.5.6 Vibration

Vibration should be minimised to prevent impacting the working environment; large vibrations can cause operators difficulties in physical tasks e.g. typing on a keyboard. Vibration can be minimised by:

- Positioning the control rooms as far as possible from sources of vibration such as back-up generators and compressors,
- Insulation shall be used to protect operators and their associated equipment from vibration transmitted from the general environment.
- If necessary, the control-room floor, walls and ceilings should be isolated from vibrating structures by vibration absorbers.

4.4.6 Maintenance Considerations

Maintenance of Hardware and software is usually determined by a contract between the customer and supplier where the following aspects are covered:

- Assistance and maintenance: managing the system software or hardware faults reported by the Customer's Maintenance Operators, by implementing a number of diagnosis and maintenance activities aimed at solving the reported problem;
- Repair: organizing the collection of broken components; monitoring the repair progress; replenishing the stock at the customer's warehouses;
- Support: providing the user with technical information support (telephone assistance), collaboration and additional training (if necessary).

The main goals of the above aspects are:

- Maximum speed in resolving the problems;
- Top coordination among all the boards normally involved in the assistance and maintenance activities.

In the event that a fault cannot be fixed through telephone assistance, remote diagnosis or by having the customer personnel replace the faulty components with spare parts the supplier shall carry out on-site work at the customer's request.

4.4.6.1 Recommended Maintenance Principles

Usually every contract for systems and services defines guidelines and procedures for maintenance. However, this section aims to define best practice of maintenance and describes a possible organization of the customer service with roles and responsibilities.

4.4.6.1.1 Call Centre

A Call Centre shall be the user's only point of contact with the Maintenance Service. This ensures greater service efficiency, as well as a prompter response and better coordination of the activities performed both inside and outside the Maintenance Service, including the ones performed by external suppliers in connection with the hardware/software repair and assistance services delivered.

The Call Centre shall be contacted through a dedicated telephone number and the operators shall be available on a 24-hour basis, every day of the year. Moreover, a number of operators will be working simultaneously, so as to ensure no waiting time on the telephone.

Below are the main functions to be performed by a Call Centre:

- Identifying the troubles and problems;
- Recording a telephone call and assigning a ticket number;
- Activating the personnel in charge of coping with the reported trouble or problem;
- Handling the reminders and the requests for information on the tickets being processed.

The Call Centre operator will, due to his/her being the first person who gets in touch both with the user and the problem, have a general knowledge of the systems and will also rely on his/her own competence and experience as well as on suitable supporting tools such as the manuals and the telephone call history records.

The operator in charge of receiving the calls will also make a preliminary analysis of the problem or request for information. Such preliminary classification may be changed when the problem analysis progresses, if the preliminary analysis has not led to a clear result.

Though all the Customer's maintenance operators are allowed to report a malfunction, it is assumed that this responsibility will lie only with the customer's maintenance manager.

4.4.6.1.2 Repair Line

The Repair Line consists of a team of operators entrusted with ticket management. This team includes industrial technicians and engineers who have gained long experience of the systems forming the scope of supply.

Below are the functions to be carried out by the Repair Line:

- Telephone assistance;
- Remote diagnosis;
- Remote assistance;
- Data-processing security management;
- Issue of assistance call statistics and reports.

4.4.6.1.3 Field Service

The Field Service consists of a team of specialized technicians who have gained long experience of system commissioning. These technicians come into action when an on-site intervention is requested following an assistance call, in the event that the situation requires so.

Below are the main functions carried out by the Field Service:

- On-site intervention for corrective maintenance purposes (at request);
- Inspection visits;
- On-field collaboration.

4.4.6.1.4 Logistics

The logistics functions deal with the following:

- Spare part supply,
- Component repair or replenishment,
- Warehouse and stock handling.

The tickets concerning the requests for component repair will be forwarded to the Logistics function, which will arrange for the parts to be shipped from the plant to the ASTS laboratories (or suppliers); they will check the repair work progress and arrange for the same to be restored at the Customer’s warehouse. All of the above will be performed by taking care that the contractual deadlines agreed upon with the Customer will be met.

4.4.7 Principles to Consider for Future Workstation Design

As well as considering principles as captured in sections 4.4.3 – 4.4.6, there are a number of other principles to consider for future workstation design related to changes in people, process and technology:

- Technology is constantly changing faster than ever before. There are new technologies available for signalling systems, TM systems and technologies to be utilised in control rooms. All of these changes have an impact on workstation design, and how operators may control the railway in the future;
- There is the potential that different input devices may be used such as eye or gesture controls and touchscreens that have the potential to increase effectiveness as well as support users with impairments;
- Roles and concept of operations will evolve and there will be an increase in collaborative team working, and a need for multi-skilled teams;
- There will be more flexibility required in workstation configuration based on users and tasks required;
- There will be an increase in use of IT and more intelligent systems and decision making tools. This will change user’s tasks from proactive rather than reactive monitoring;
- There will be a need for cyber security to ensure correct authorisation and authentication of users;

- The role of ergonomics, following a user centred design process and enhancing user experience will continue to grow in importance in order to distinguish solutions from their competitors;
- Employees have a duty of care to provide safe, healthy and comfortable workstations and these environments also have a contributing factor to job satisfaction, motivation and efficiencies;
- Workstations need to be maintainable and the effect of obsolescence due to fast changing technologies needs to be reduced by having flexible fixings to easily replace components when required, rather than entire workstations;
- The rail industry has a responsibility to apply sustainable best practice to reduce its effect on the ecological footprint from workstation or system design.

4.4.7.1 User Problems to Resolve

It should be noted that although it is important to consider the principles in section 4.4.7 in future workstation design, the key and most challenging issues to resolve are the future user issues. See below examples of user issues to resolve:

- Enable intelligent decision support:
  - Support pro-active, rather than reactive monitoring and tasks;
- Reduce complacency from automation:
  - The user should be considered as part of the system to minimise lack of situational awareness and to enhance decision making;
- Use automation and decision support to reduce burden on user to make complex decisions;
- Use automation and intelligent information decision support to inform users decision making effectively to improve the performance of the railway;
- Reduce silo working:
  - Support communication tasks and collaborative decision making,
  - Support distributed cognition,
  - Ensure complex information is presented to the right person(s), at the right time and in the right format;
- Ensure suitable workload to support performance and safety of railway:
  - Ensure tools support the change from fixed areas of control to flexible working;
- Ensure flexibility in workstation design and ensure the user can make changes to the:
  - Position of equipment e.g. distance and angle to user,
  - Height of the workstation,
  - Thermal environment,
  - Lighting environment,
  - Their personalised set up e.g. the user should also have the ability to save favourite set ups which can be either role dependant and or task/scenario dependant.

4.5 Inclusive Design Considerations

This section describes the output of sub-task 7.2.3.3.

It is estimated between 12 and 13 per cent of the population have some degree of impairment.

The aim of section is to capture the needs of individuals with special needs to feed into the design of future TM systems, identify any limitations in supporting individuals with special needs in this context and determine what additional support may be required.

4.5.1 Definitions

The following definitions are taken from BS 8878:

Special needs: 'A condition, such as an illness or an injury, which damages or limits a person's physical or mental abilities'.

Accessibility: 'Usability of a product, service, environment or facility by people within the widest range of capabilities'.

Assistive Technology: 'Hardware or software added to, or incorporated within, a system that increases accessibility for an individual'.

Disability: 'Physical or mental impairment which has a substantial and long-term adverse effect on a person's ability to carry out normal day-to-day activities'.

Impairment: The main types of impairments include; Physical, sensory or cognitive impairments. It should be noted that people may have a number of different impairments where the combined effect of these impairments are likely to be more severe than the individual impairments might indicate in on individually.

Impairments can change in severity across each individual and each person's impairment can fluctuate in severity and impact.

Usability: 'Extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use'.

4.5.2 Determining special needs to consider in the context of Traffic Management

The recruitment policies for disabilities in Nuclear, Healthcare, Aviation and Rail were reviewed via web searches however this resulted in little information found on recruitment policies in rail.

Therefore, as part of this subtask 7.2.3.3, the partners reviewed a range of impairments to determine which were considered to be applicable for TM. The following were deemed applicable:

- **Physical:**
  - Hearing impediments and deafness,
  - Visual Impairments and blindness (e.g. colour blindness),

  - Physical disabilities and restricted mobility including missing limbs;
- **Psychological:**
  - Reading and learning disabilities (e.g. dyslexia),
  - Speech and language impairments (e.g. stutter);
- **Excluded:**
  - All other conditions defined as special needs / disabilities, e.g. Down syndrome, ADHD, Cystic fibrosis etc.

4.5.3 Assistive Technologies to support special needs applicable to Traffic Management and In2Rail

Based on the special needs deemed applicable to TM, a number of assistive technologies that could support these impairments were reviewed. This section summarises the range of assistive technologies reviewed and highlights suggested initial design principles.

Psychological:

- Speech and Language impairments:
  - Sign Language support or draw upon sign language principles,
  - Automated messages and predefined text to select and send as messages;
- Reading and Learning difficulties:
  - Use simple language,
  - 'Narrator' voices: hover over screen to read text aloud,
  - Speech to text convertors: speak into microphone to turn voice into text. Supports those who find typing difficult e.g. Windows 7 Voice text,
  - Live scribe pen: write on a special pad of electronic paper and system types text on to screen,
  - Text-to-speech converters: reads text aloud to user,
  - 'Dragon naturally thinking' product: give the product ideas by speaking into it and it translates speech into text and paragraphs,
  - Alternative input devices such as joysticks;

Physical:

- Hearing impairments and deafness:
  - Use other methods to attract attention e.g. haptic (vibrate through chair or on desk top), or flashing icons,
  - Increase volume to a suitable level of hearing for each user;
- Visual impairments:
  - Toggle on or off colour blind mode, (change colours to suit needs of colour blind users),
  - Use programmes such as 'Vistech': upload html or images to show how the HMI would appear to a colour blind user,
  - Do not use colour as primary meaning,
  - Screen reader: magnifies text and views x 32 e.g. windows eyes 9.4,
  - Make each page configurable to various text sizes and colours,
  - Dynamic touchscreens: able to recreate feeling of brail on touchscreens.
- Physical disabilities and restricted disabilities:

- Reduce the overall size equipment takes up on desk so it is in normal reach envelope,
- Increase ease of moving up and down desk e.g. hand rails or the material of the floor to make sliding up and down easier,
- Electronic pointing devices to interact with interface,
- Use gestures tracking technologies to perform commands,
- Mouth stick to control interface,
- Enable wheel chair access,
- Use sit stand desk suitable for smallest and tallest users (not just 5%-95%),
- Alternative keyboards.

It is important to consider that if you adapt the system or workstation design to support a range of special needs it should also improve the system for all other users. If alterations of a workstation are required that do not support other uses tasks then it is not inclusive design. Therefore, the In2Rail system and workstation design must be flexible and configurable to suit a range of needs. It must also be determined from SME's if there is a need to define requirements for a varying range of special needs to be role specific. There is also a need to determine if there are any of the impairments stated in section 4.5.2which are not suitable for all safety critical roles.

4.5.4 Inclusive Design Recommendations or Legislation

This section defines regulations and recommendations for inclusive design taken from a variety of legislation and ergonomics standards. See section 4.5.5for the requirements generated for the In2Rail system and workstation design based on the recommendations captured in this section of the report.

4.5.4.1 UK legislation important to consider

The following UK legislation is important to consider:

- Equality Act 2010;
- Disability Discrimination Act 1995;
- Disabled peoples protection policies 2014 – ORR;
- 'Disability Discrimination Act (DDA) 1995, Section III.

Note: These policies focus on support for passengers with disabilities however there is no reference to inclusion policies for operators in the control room.

4.5.4.2 Ergonomic standards and recommendations to consider

The following standards or guidelines should be considered:

- ISO/IEC 40500:2012 - Information technology -- W3C Web Content Accessibility Guidelines (WCAG) 2.0;
- BS 8878:2010 Web Accessibility – Code of Practice;
- Core web accessibility guidelines from W3C WAI;
- Web Content Accessibility Guidelines (WCAG);

- Various ISO Standards; 9241-11, 9241-12, 9241-171, 9241-129;
- BS 8300:2009+A1:2010 - Design of buildings and their approaches to meet the needs of disabled people –Code of practice;
- Website Accessibility Initiative (WAI);
- ISO standard (ISO 7193) for Wheelchairs.

A summary of principles from the above references can be found below:

- System design should enable accessibility without the need for special adaption, other than the use of assistive technologies;
- The accessibility of systems depends on the operating systems and assistive technologies impaired people use;
- The system should have the ability to zoom in on a page, zoom in on just the text on the page, and the ability to change the system colours specified by enabling the use of a custom cascading stylesheet (CSS);
- Ideally the HMI and workstation design should be reviewed with older or disabled users to gather requirements or run usability assessments. If access to these end users is not available, ethnographic research methods should be followed to accurately capture their particular needs. To support this process, expert reviews should be conducted with early designs and prototypes and as a minimum a heuristic evaluation should be conducted to evaluate the HMI under development to ensure it meets the needs of impaired end users;
- Blind and Partially sighted people:
  - Colour blinded individuals cannot read certain colour combinations that have a low contrast level. Therefore you should never use colour as the only way to convey the meaning of something,
  - The user should have the ability to resize fonts, (or select from a number of pre-defined texts size options),
  - The user should have the ability to adjust the contrast levels as some users benefit from high contrast levels while others find the glare and brightness of a light background hard to read and prefer lower contrast levels;
- Learning difficulties users benefit from:
  - Having information displayed in manageable sections and use clear and consistent navigation and layouts,
  - Having the ability to control colour and text size,
  - Clear and simple displays as they can be sensitive to clutter,
  - Note: These principles are common ergonomic display principles relevant for all users;
- Cognitive Impairments:
  - Users benefit from clear and simple displays, ability to alter colour and text size;
- Physical Impairment:
  - System needs to be usable by a number of different methods of interaction such as keyboard and mouse, touchpad or eye gestures;
- Older generation users:

  - Due to the demographics of an aging workforce in rail, it may also be useful to consider design principles suitable for older users;
- Wheel chair users:
  - Manual wheelchair users need sufficient space and clearance to be able to drive the chair without striking their elbows or knuckles on surrounding obstacles. The ISO standard (ISO 7193) for wheelchairs states there needs to be a clearance of no less than 50mm and preferably 100mm, on both sides,
  - There are a number of different sizes and types of wheelchairs to consider,
  - Other measurements to consider when accommodating wheelchair users are:
    - Eye height, which is around 120-130mm below seated height giving a 5th-95th percentile range for wheelchair users,
    - Knee height, 500mm to 690mm,
    - Seat height, 460mm to 490mm,
    - Height to bottom of foot support, 60mm to 150mm.
  - The ability of a person in a wheelchair to reach sideways or reach forward.

4.5.4.3 Other Useful Strategies or Literature to Consider

- **Network Rail Diversion and Inclusion Policy**

Network Rail has a diversion and Inclusion Policy that the In2Rail system and workstation should support or comply with. The policy states that there are work stream leads and a team of experts within NR focusing on diversity and inclusion. The In2Rail project or Shift2Rail should utilise these resources where possible to review In2Rail concepts and identify requirements for special needs users.

Currently the inclusion policy focuses on ensuring more inclusive and accessible services and stations for passengers and is less focused on supporting operators in the control room. Therefore, this shows the need for further collaboration required with operating companies to ensure that inclusions policies support impaired users as well as the designs themselves.

- **Government Inclusive Mobility Policy**

The Government has set out a policy regarding accessible public transport and infrastructure, however this policy again shows that the inclusion policy focuses on ensuring more inclusive and accessible services and stations for passengers and is less focused on supporting operators in the control room.

4.5.5 Inclusive design requirements

Based on the recommendations captured in sections 4.5.3 - 4.5.4, this section gives examples of inclusive design requirements required for the In2Rail system and workstation design.

Requirement	Category	Impairment supports	Comment
In2Rail workstation design shall support sit-stand functionality.	Workstation Design	Physical impairments e.g. height and supports healthy working principles	
In2Rail equipment layout and workstation fixtures shall be configurable to support specific roles tasks required and each user's physical mobility capabilities e.g. enable all equipment to be within normal reach envelope for an individual with restricted mobility.	Equipment Layout	Restricted mobility	
Regularly used In2Rail equipment shall be within the normal reach envelope to support users with restricted mobility.	Equipment Layout	Restricted mobility	
The In2Rail HMI shall make use of simple displays.	Software Design	psychological e.g. dyslexia	Support users with psychological impairments such as dyslexia
The In2Rail HMI shall make use of configurable displays principles such that the user can easily reconfigure text size, font style, zoom level, colours and contrast levels.	Software Design	psychological e.g. dyslexia and Physical e.g. visual impairments	
The In2Rail HMI shall make use of multiple feedback methods such as change of state e.g. change in button colour or shape, haptic feedback and audible feedback.	Software Design	Physical and psychological	
In2Rail alerting functions e.g. alarms shall make use of multiple alerting principles e.g. sound (varying volume to suit users hearing abilities), haptic (e.g. chair or desk vibrations), visual (e.g. flashing information).	Software Design	Physical and psychological	
The In2Rail system shall enable multiple input methods such as keyboard and mouse, touchscreen and tracker ball to support different user's physical needs.	Software Design	Physical and psychological	
The In2Rail system shall be configurable to use with external assistive technologies e.g. pen to text, speech to text, text to speech, gesture or eye control technologies etc.	Software Design	Physical and psychological	Issue in safety critical systems - does external device need to be safety critical?
In2Rail workstation design shall be suitable for wheel chair users.	Workstation Design	Restricted mobility	

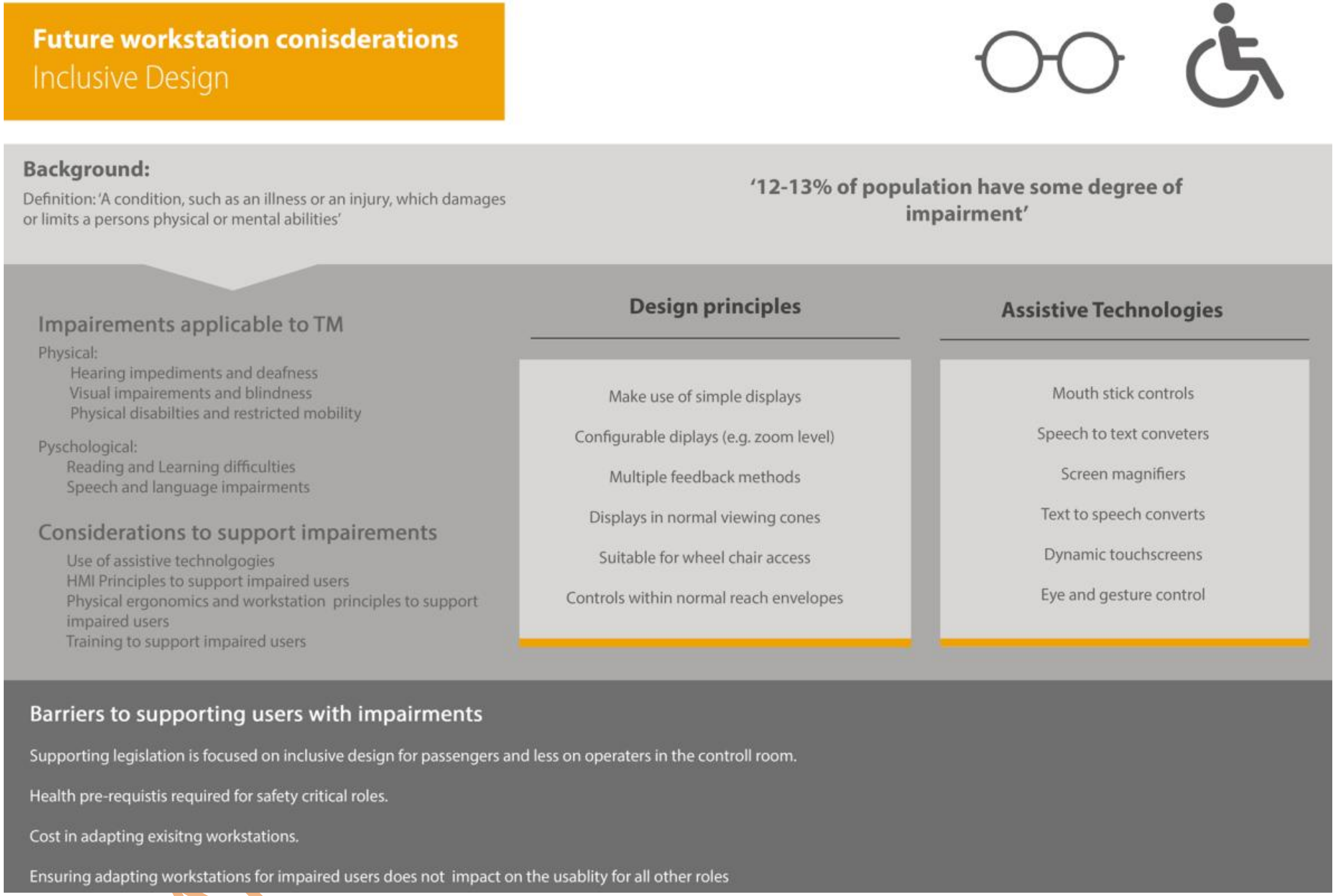
Table 4.1: Design Requirements to support users with special needs

4.5.6 Workshops and consultations with SME's in Inclusive Design

The first step in ensuring that future TM workstations and systems will meet the needs of users with impairments is to design a workstation that builds upon design principles and requirements captured in Table 6.1. However, the next step is to ensure that recruitment policies, pre-health requisites and concept of operations in a control room also meet their needs. Although it is out of scope in sub-task 7.2.3.3 to modify these, the following next steps outline how future work packages in In2Rail or Shift2Rail could start to explore this issue further.

Proposed next activities:

1. Identify experts in rail across the EU to arrange workshops with to identify policies and barriers in rail to implementing inclusive design principles in control rooms.
2. Determine if there are any initiatives to improve inclusive design in rail control rooms.
3. Determine if there are any current recruitment policies around hiring individuals who work in control rooms with special needs.
4. Contact diversity and inclusion functions and local work stream functions to support planning for future control room design and workstation design.



Future workstation conisderations
Inclusive Design

Background:
Definition: 'A condition, such as an illness or an injury, which damages or limits a persons physical or mental abilities'

'12-13% of population have some degree of impairment'

Impairements applicable to TM

Physical:
- Hearing impediments and deafness
- Visual impairements and blindness
- Physical disabilties and restricted mobility

Pyschological:
- Reading and Learning difficulties
- Speech and language impairments

Considerations to support impairements
- Use of assistive technolgogies
- HMI Principles to support impaired users
- Physical ergonomics and workstation principles to support impaired users
- Training to support impaired users

Design principles

- Make use of simple displays
- Configurable diplays (e.g. zoom level)
- Multiple feedback methods
- Displays in normal viewing cones
- Suitable for wheel chair access
- Controls within normal reach envelopes

Assistive Technologies

- Mouth stick controls
- Speech to text conveters
- Screen magnifiers
- Text to speech converts
- Dynamic touchscreens
- Eye and gesture control

Barriers to supporting users with impairments

Supporting legislation is focused on inclusive design for passengers and less on operaters in the controll room.

Health pre-requistis required for safety critical roles.

Cost in adapting exisitng workstations.

Ensuring adapting workstations for impaired users does not impact on the usablity for all other roles

Figure 4.16: Design Journey Image 4 - Summary of Inclusive Design Considerations

4.6 In2Rail Workstation Design

4.6.1 Innovative Technologies to Consider

As shown in the design journey image Figure 4.17, there is a range of technology that the rail industry could utilise. However, the user should always be at the centre of the decision for change and technology should not just be used for the sake of using technology if it doesn't support a user need.

Therefore before deciding which technologies the future workstation should use, it's essential to determine which technologies the user would benefit from. In order to determine this it is important to:

- First, identify the key user issues you're trying to solve, see section 4.4.7.1;
- Identify what the advantages and disadvantages of each technology are and identify potential applications, see the 'Comparison of technologies to utilise for In2Rail Workstation; in section 4.10.2;
- Identify which technologies support or solve each user need,
- Evaluate whole-system design concepts to consider the interactions between the people, process and technology elements of the system.

There is also a need for the rail industry to stay current with user's expectations of how systems work and their experience with common operating systems like windows or applications used on hand held devices. The focus in the design of rail systems has always been on usability with regards to performance and safety and less focused on user experience. However, operators will use systems for 12 hours day, which is longer than lots of commercial products so the design of future workstations and systems should enhance user experience to improve motivation, attract younger generation and ensure competitive advantage.

It should be noted though that within any changes to technology or a system, training is required. Although using common user interaction principles from applications that lots of users are used to may reduce the training needs for some users, there may be some users where barriers in digital technology causes an increase in training needs.

Figure 4.17 describes a summary of considerations for future technologies, examples of technologies to consider and they there is a need to attract the young, technology savvy future generation.

Future Workstation Considerations
Innovative Technologies

Quesions to Conisder:

What technologies would a future control room benefit from?

Why would they benefit from them?

Which roles would benefit from using these technologies the most?

What are the barriers of implementing them in safety critical systems?

Technologies to Conisder

Touchscreens
Augmented Realtiy
Virtural Reality
Mutlitouch Tables

Eye Gesture
Gesture Control
Curved screens
Integrated desktops

Attract the Next Generation

- There is a need to showcase the rail industries capabilities and attract the next generation, (Generation 'Gamers' & `Connected') to balance out the rate at which the 'Baby Boomers' will retire and leave a gap in years of knowledge and experience .
- Gen G & C are technologically minded and expect high envionemental workplace standards. They are brought up in a world of rapidly developing technology enabling them to interact with complex HMI's and have learnt to problem solve through gaming learning.

Figure 4.17: Design Journey Image 5 - Innovative Technologies to Consider

4.7 Case Study from Industry: CGM

The following company was identified as a useful case study for workstation design as their desk design concepts follow the principle that adjustability and flexibility is key to enhance user experience. Examples of key functions that CGM workstations have are described below:

In the the CGM workstation below, the user has full control over the adjustability of the workstation. They are able to adjust the height of the workstation to support sit stand operation. They are able to adjust the screen height, the distance the screen is from themselves and also the angle at which the screen is presented at. This enables the users to find a comfortable working position that suits their individuals needs depending on time of day or type of task completing.

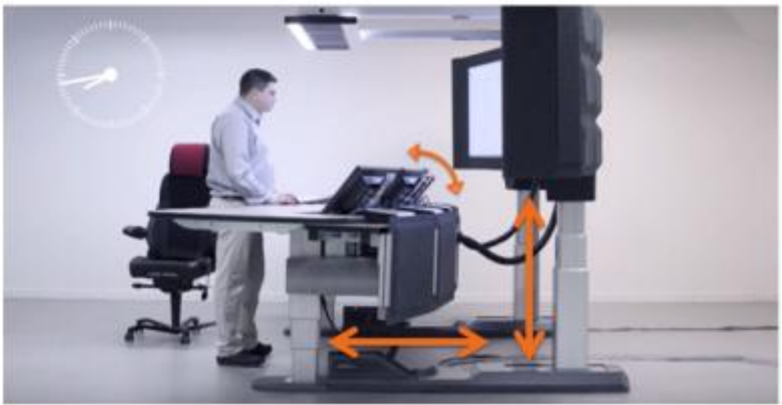


Figure 4.18: CGM Workstation Functionality - Adjustability

The ability to adjust their workstation set up is quick and easy to do so via a touch pad that can be accessed under the desk surface. This enables small adjustments to be made easily, without the need for manual adjustments.

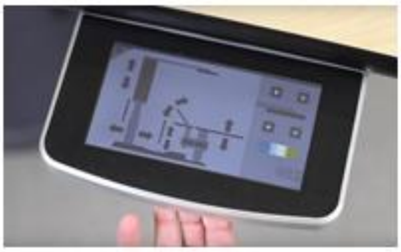


Figure 4.19: CGM Workstation Functionality - Adjustment Touchpad

The Workstation also has the ability to store individual user's workstation preferences so that when they log into the workstation via a unique bracelet identifier, the workstation is quickly set up to the user's needs.

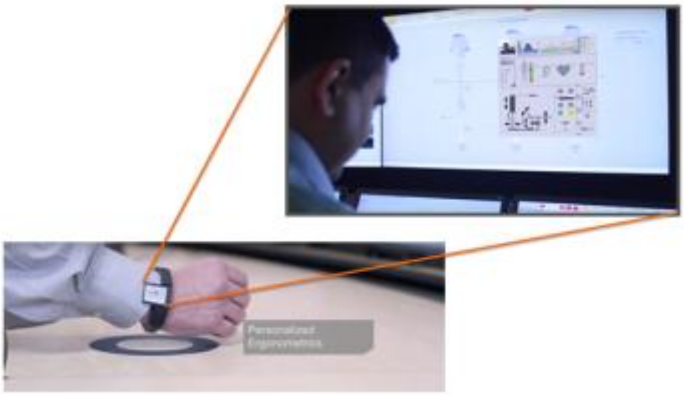


Figure 4.20: CGM Workstation Functionality - Personalised Set Ups

The workstation also has the ability to be placed into a ‘night mode’ to adjust the light settings to be more suitable to night shift tasks.

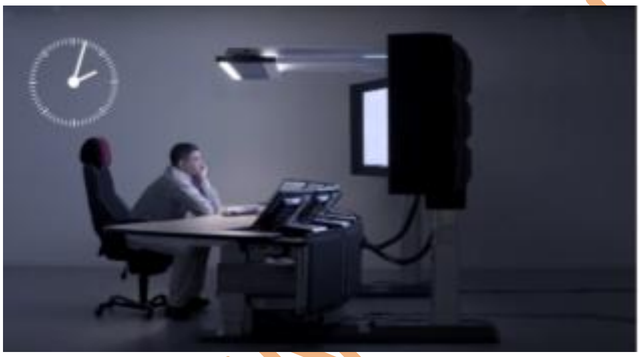


Figure 4.21: CGM Workstation Functionality - Night Mode

Finally, the workstation has the ability to adjust not only the lighting into a night mode, but also make small adjustments during the day via a direct sound system.

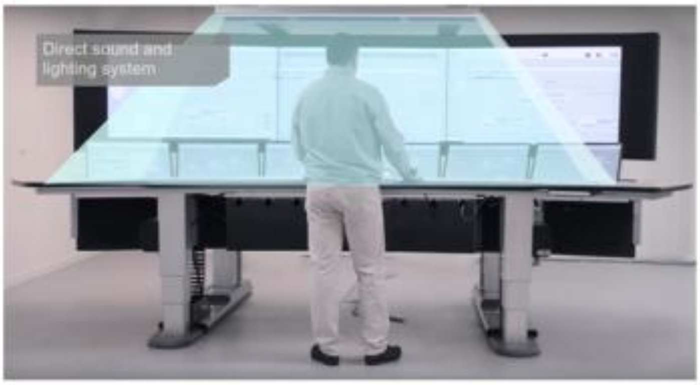


Figure 4.22: CGM Workstation Functionality - Lighting and Sound System

Note this CGM case study was presented and evaluated at the In2Rail Concept Review Workshop in Genoa on the 6th June 2016 to determine which principle should be captured in the In2Rail workstation concepts.

4.8 Workstation Design Process

The following design process was followed to generate and evaluate the conceptual workstation designs for future TM Workstations:

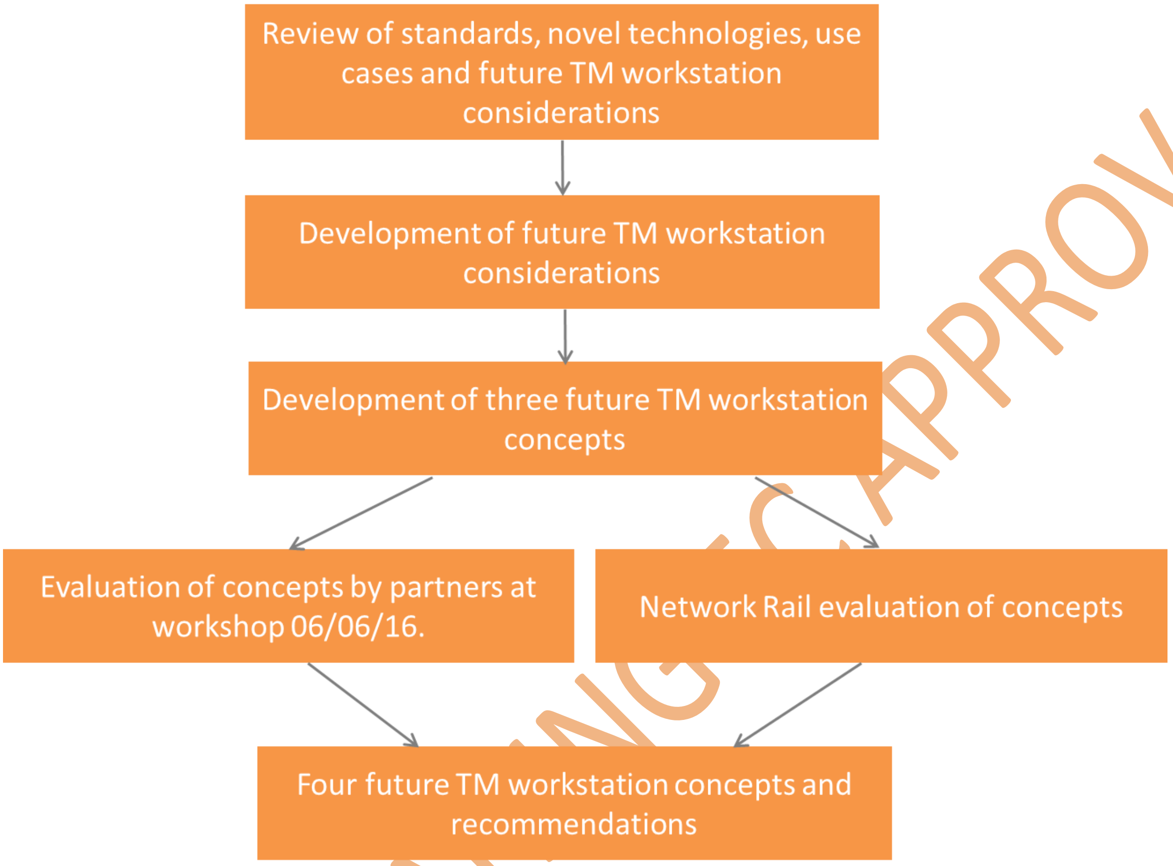

Review of standards, novel technologies, use cases and future TM workstation considerations
Development of future TM workstation considerations
Development of three future TM workstation concepts
Evaluation of concepts by partners at workshop 06/06/16.
Network Rail evaluation of concepts
Four future TM workstation concepts and recommendations

Figure 4.23: In2Rail Workstation Design Process

When developing the workstation concepts, key principles to consider were the future user needs as discussed in section 4.4.7.1.

Initially, three concepts were presented during the Concept Review Workshop in Genoa on the 6th June2016. As a result of this workshop, a fourth concept was then developed as a further future concept that a TM workstation could aspire to.

The above design process shows the process followed to determine future TM workstation designs based on HF best practice principles and 'approach 2' to workstation design in section 4.4.2. The next steps to progress these concepts and to ensure a user centred design process is continued to be followed can be found in section 4.10.8.

4.9 In2Rail Workstation Concepts

At this stage of In2Rail and TM system development; it is challenging to define an end state TM Workstation as there are many uncertainties with respect to the most appropriate technology to be used, roles and tasks required by operators and the exact functions of the system required. Therefore technology, roles and tasks are likely to change from what we expect today and may be different across countries and finally the budget and scope for workstation design is different for each deployment.

Therefore a number of concepts have been developed to enable a road map of future workstations to be produced based on technological readiness and cost.

The advantages and disadvantages of each concept were evaluated during the Concept Review Workshop and are discussed in order to provide guidance to operating companies or future deployments of TM. Future deployments of TM, and through Shift2Rail, can select principles from each concept that are applicable to and support that specific project requirements and user needs.

In Figure 4.24, it shows where each workstation concept is positioned on the road map in terms of cost and technological readiness. The figure shows that the higher the technological readiness, the lower the cost to implement and the lower the technological readiness, the higher the cost to develop the solution.

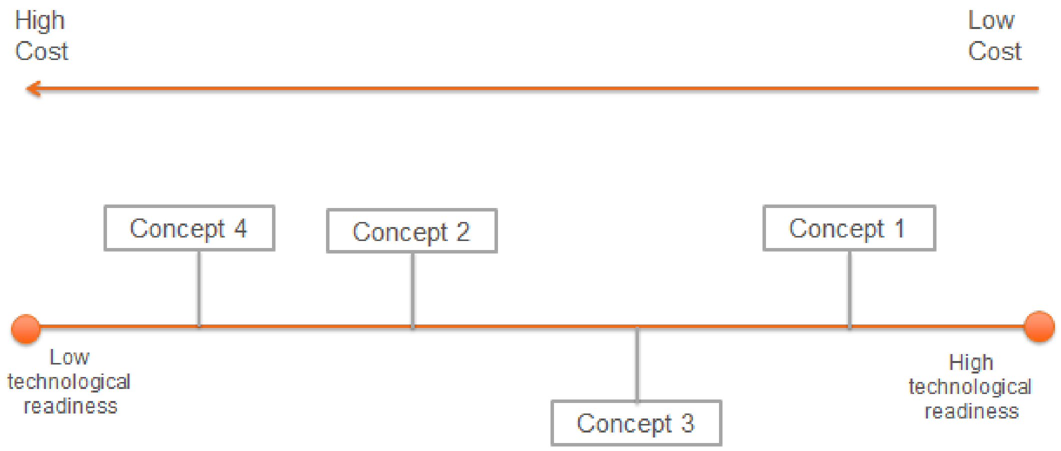


Figure 4.24: Road Map of In2Rail Concepts

4.9.1 Concept 1

Concept 1 builds upon principles and workstation dimensions from the TMS 1st Deployment Workstation currently being deployed in the UK; however, it has been modified to make use of a large singular displays and integrated desktop capabilities, see Figure 4.25.

Although the workstation could also make use of smaller individual screens that are commonly used in workstations today, there are a number of benefits to using large singular displays. These benefits are captured in the evaluation of concept 1, however an example benefit would be the ability to utilise integrated desktops to enable a seamless display.

This concept is the lowest cost option of the four concepts. Although sit stand workstations are generally more expensive than fixed height workstations, the benefits justify the cost as they have the ability to reduce static postures and support healthy working principles. This brings benefits to both the user and the operating company as sit stand workstations have been shown to reduce the development of musculoskeletal disorders and therefore reduce the amount of absence from work. Finally these types of workstations have also been shown to enhance performance. [See references 4-11]

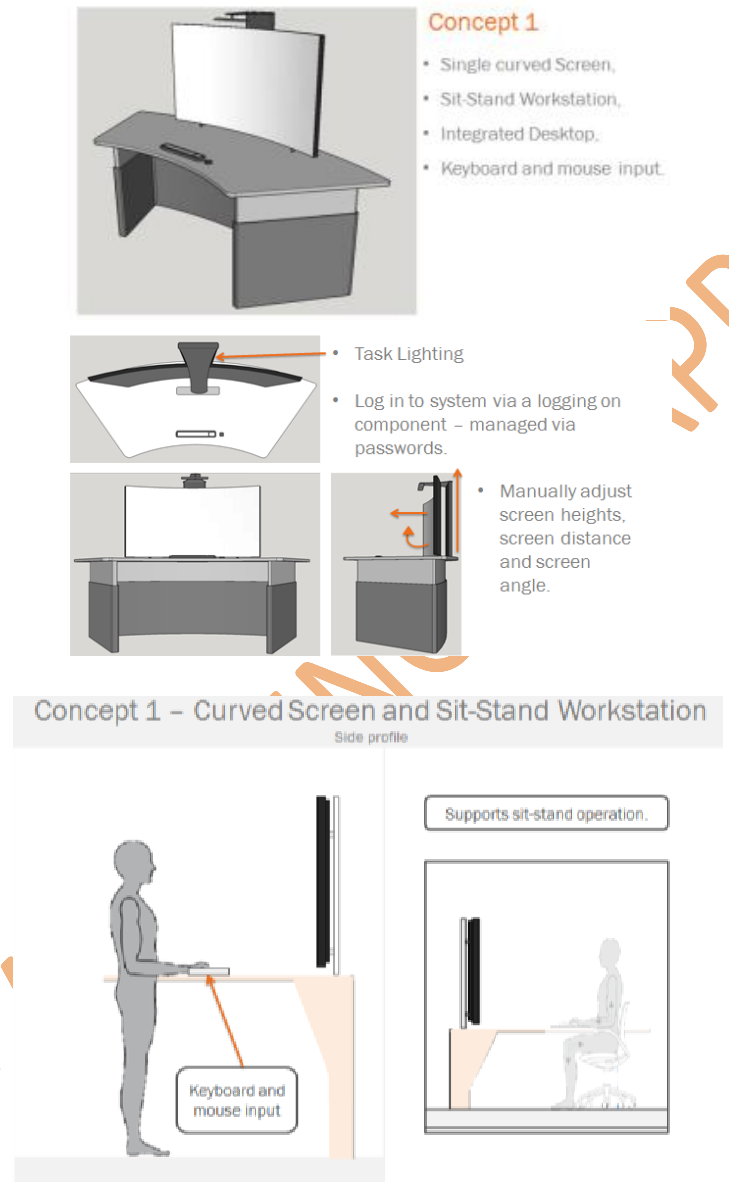

Concept 1
Single curved Screen.
Sit-Stand Workstation.
Integrated Desktop.
Keyboard and mouse input.
Task Lighting
Log in to system via a logging on component – managed via passwords.
Manually adjust screen heights, screen distance and screen angle.
Concept 1 – Curved Screen and Sit-Stand Workstation
Side profile
Supports sit-stand operation.
Keyboard and mouse input

Figure 4.25: Key Features of Concept 1

The size of this workstation has been developed using best practice from number of standards used to develp the TM Workstation for TMS 1st Deployment in the UK. However due to the use of the singualr sceen and intgerated desktop, the width of the screen array has been reduced which in turn has reduced the overal desk surface of the workstation required.

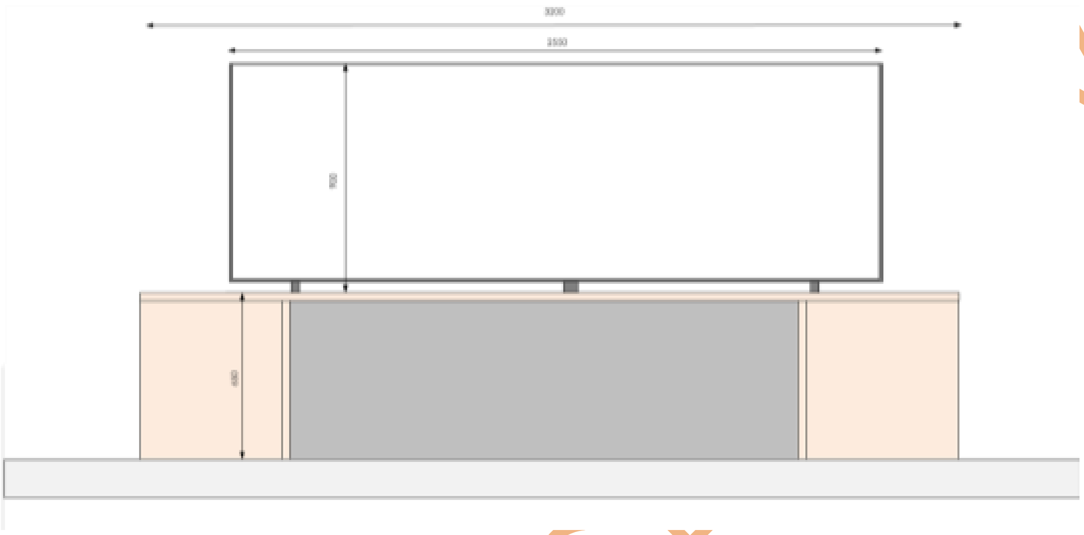


Figure 4.26: Concept 1 Dimensions

The workstation dimensions and screen size has been optimised to ensure it is compliant with key ergonomic requirements stated in Section 4.4.3, see Figure 4.27 and Figure 4.28.

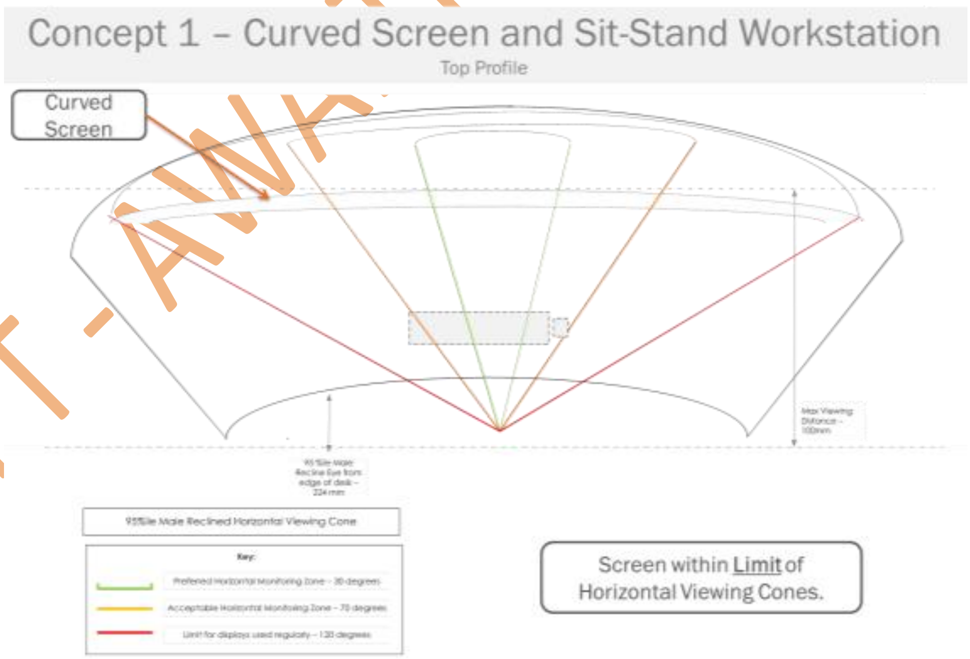

Concept 1 – Curved Screen and Sit-Stand Workstation
Top Profile
Curved Screen
Max Viewing Distance - 100mm
95 %ile Male Recline Eye from edge of desk – 224 mm
95%ile Male Reclined Horizontal Viewing Cone
Key:
Preferred Horizontal Monitoring Zone – 30 degrees
Acceptable Horizontal Monitoring Zone – 70 degrees
Limit for displays used regularly – 120 degrees
Screen within Limit of Horizontal Viewing Cones.

Figure 4.27: Horizontal Viewing Cones Evaluation of Concept 1

Concept 1 – Curved Screen and Sit-Stand Workstation
Side Profile

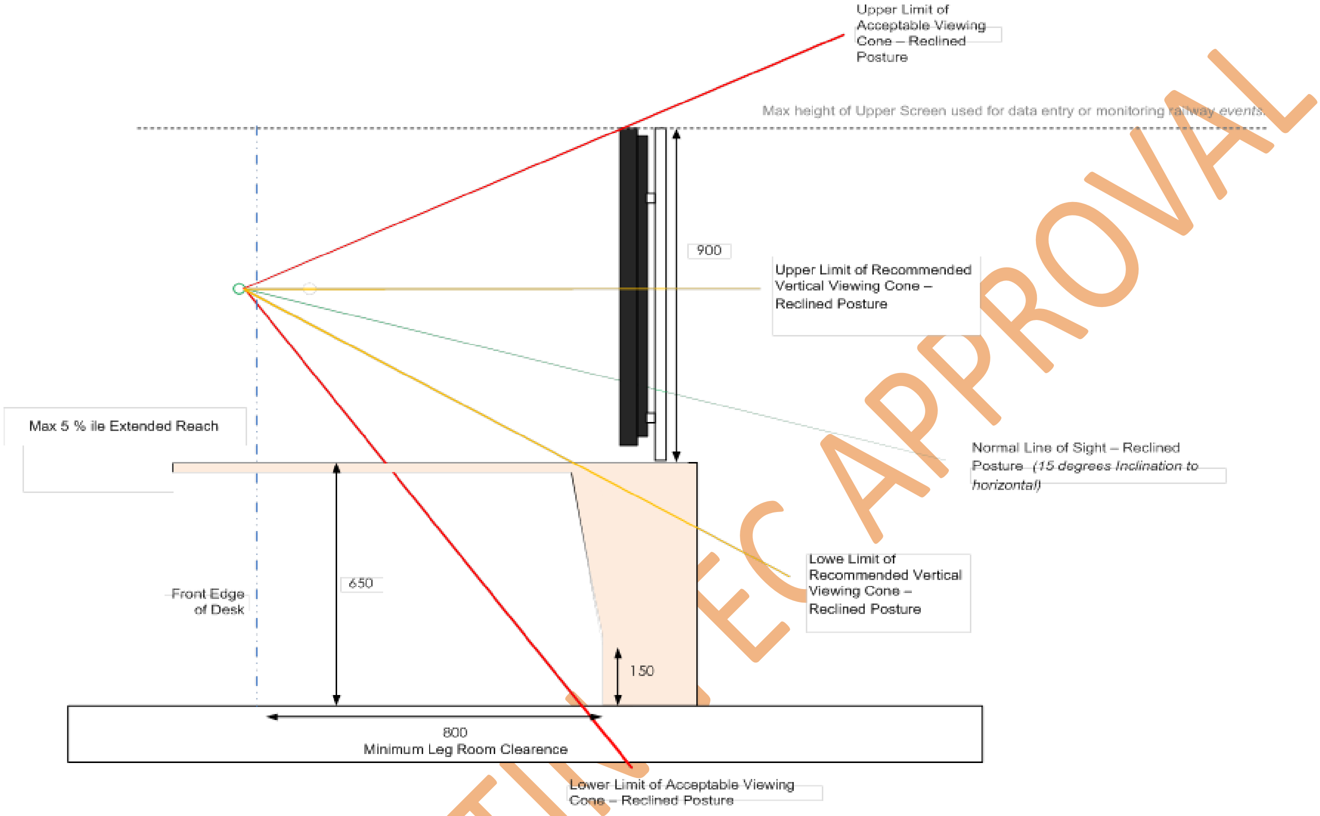

Upper Limit of Acceptable Viewing Cone – Reclined Posture
Max height of Upper Screen used for data entry or monitoring railway events.
900
Upper Limit of Recommended Vertical Viewing Cone – Reclined Posture
Max 5 % ile Extended Reach
Normal Line of Sight – Reclined Posture (15 degrees Inclination to horizontal)
Lowe Limit of Recommended Vertical Viewing Cone – Reclined Posture
Front Edge of Desk
650
150
800
Minimum Leg Room Clearence
Lower Limit of Acceptable Viewing Cone – Reclined Posture

Figure 4.28: Vertical Viewing Cones Assessment of Concept 1

	Concept 1 - Evaluation		
Consideration	**Advantages**	**Disadvantages**	**Suggestions**
Ergonomics	• One singular screen – no breaks in information on the screen and across critical information. • Benefits of integrated desktop; Dynamic views, widgets and customisation of windows for each user – supporting individual needs and decision making by role and task required etc. • Adjustable screen angles and distance to user. • Screens between acceptable and limits of horizontal viewing cones, reduces the need for head rotation. • Curved screens support operators field of view	• Manual adjustments to screen difficult for individuals to alter due to size and weight of screen would need to be supported by maintenance. This might discourage users to alter screen to suit their individual's needs. • Issues in manual handling of large screens would need multiple users to install and maintain one large screen. • Single input method, (keyboard), has limited flexibility in supporting different users preference for input device. However note that the concept could be easily adapted to use touchscreen if required.	• Need to ensure lighting is suitable above curved screens to reduce light reflections.

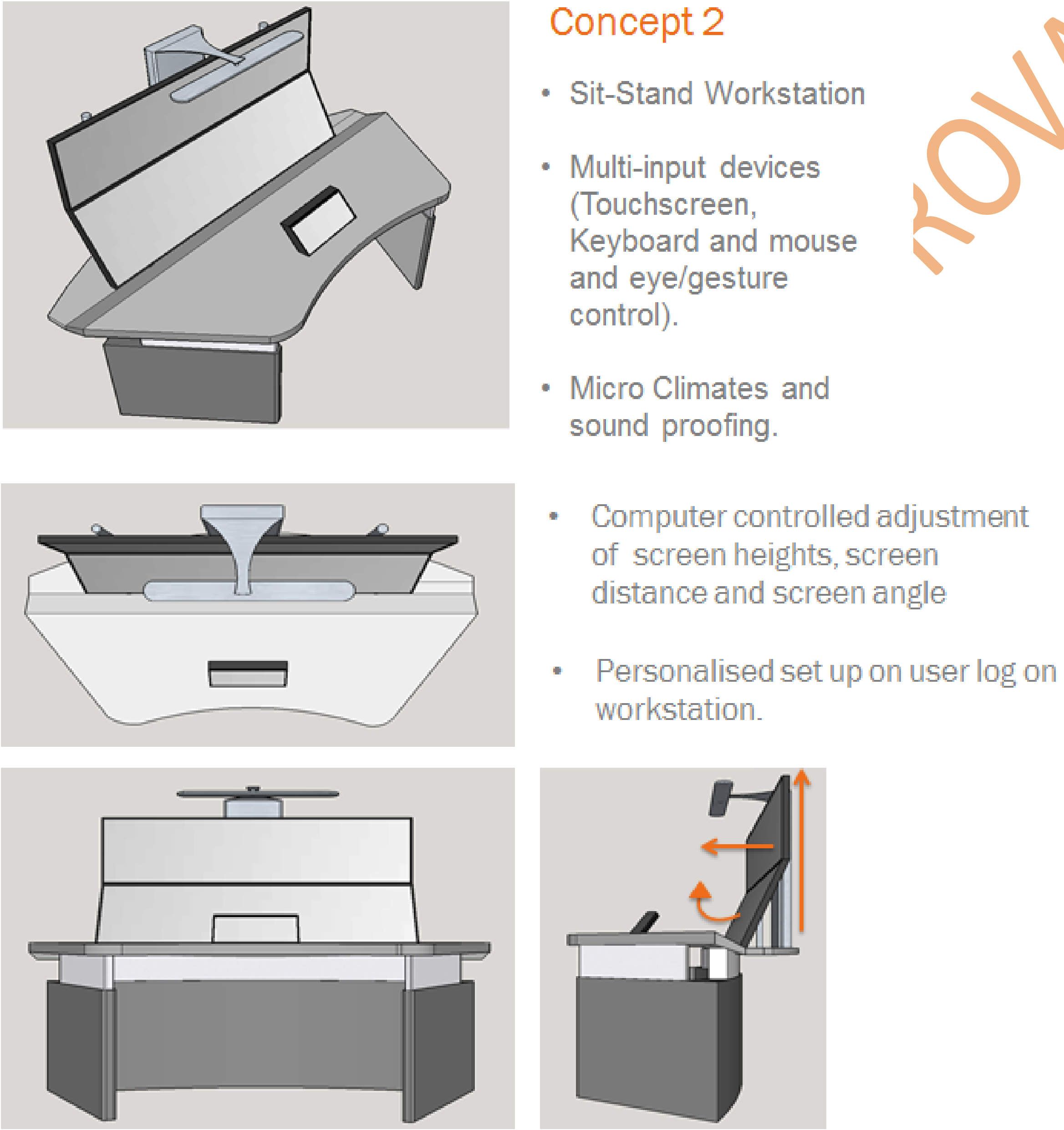
	Concept 1 - Evaluation		
Consideration	**Advantages**	**Disadvantages**	**Suggestions**
Inclusive design	• Sit stand workstation supports wheel chair users.	• The use of keyboard and mouse does not support users with reduced dexterity.	
Healthy working principles	• Sit-Stand desk enables users to operate workstation in both sitting and standing postures, reducing effects of prolonged static postures. • Enables adjustments of work surface height to enable each user to find a comfortable height which supports arm rest on the work surface.	• Adjustable micro-climates expensive.	
Technology	• Larger screens support integrated desktop – seamless display – 'plug and play' architecture. • Quick and easy to configure personalised dashboards. • Technology readiness: Integrated desktop and 'plug and play' architecture predicted to be commercially available within next 5 years due to rapid development of operating systems and applications. • Show cases rail industry capabilities	• Technology readiness: Large screen sizes used in gaming but less readily available commercially – high cost now but expected to become commercially available in next 5 years. • Difficulty if multiple suppliers are supplying each application to ensure seamless design	

	Concept 1 - Evaluation		
Consideration	**Advantages**	**Disadvantages**	**Suggestions**
	– novel technologies to rail sector: Touchscreens, eye gesture and gesture control etc. Attract next generation of users.	and have consistent design principles.	
Security	• Log into whole system once – no need to log onto each application separately. • Prevents unauthorised users accessing applications.		
Maintainability		• One large screen creates difficulties in manual handling in installation and maintenance, multiple users will be required. • If the one screen fails, the whole workstation is offline. (This can be mitigated by spare workstations).	• Suggested spare screen as an option behind the primary screen so if one fails, the secondary screen is available for use.
Sustainability	• Cost of one large screen predicted to be less than the cost of multiple smaller screens.		

Table 4.2: Concept 1 Evaluation

4.9.2 Concept 2

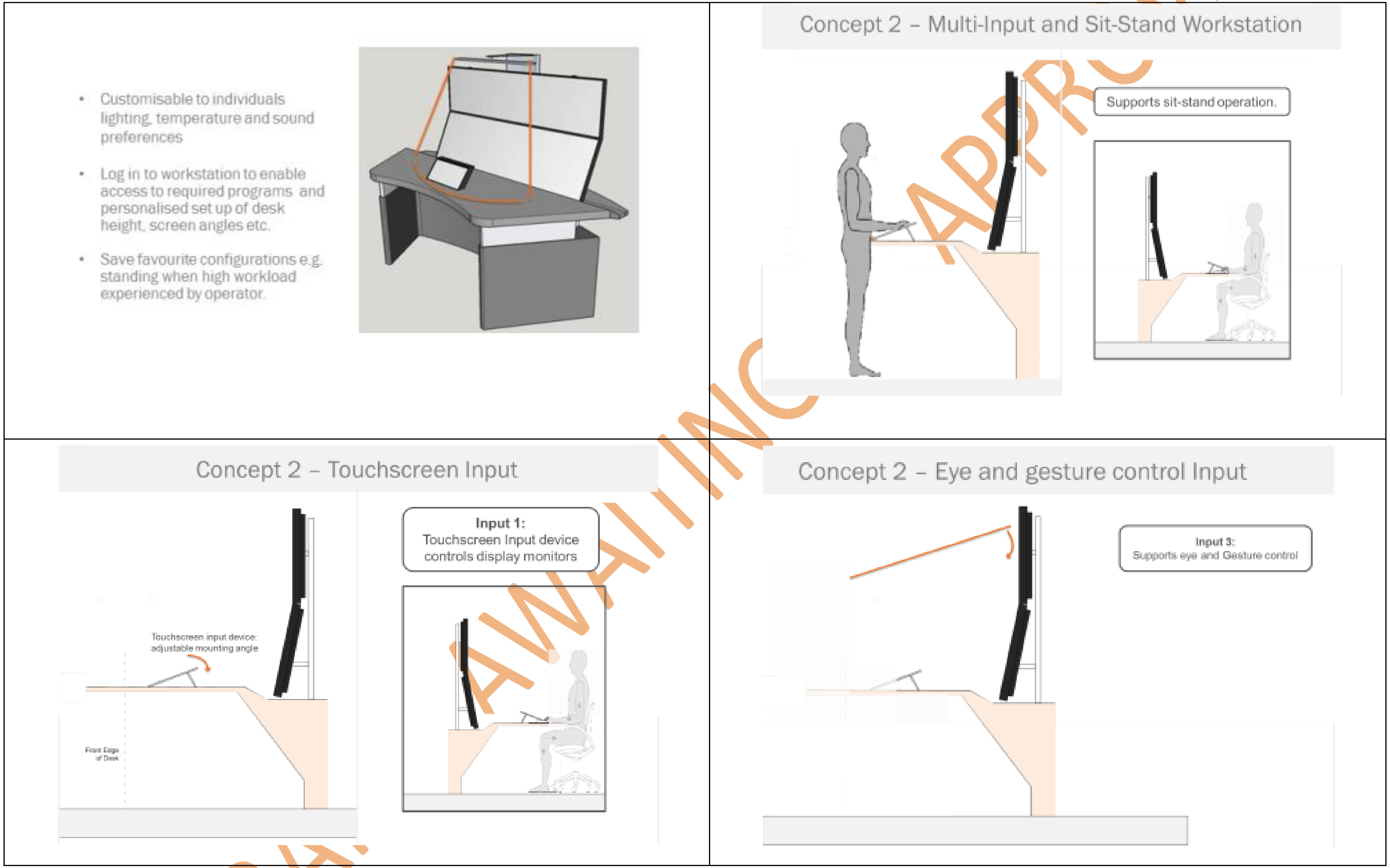
Concept 2 has a similar plan view as Concept 1; however, it has a stepped profile at the back of the workstation. This enables the bottom screen to be placed lower down, which in turn enables the centre of the bottom screen to be in line with the user's normal line of sight.



Concept 2

- Sit-Stand Workstation
- Multi-input devices (Touchscreen, Keyboard and mouse and eye/gesture control).
- Micro Climates and sound proofing.
- Computer controlled adjustment of screen heights, screen distance and screen angle
- Personalised set up on user log on workstation.

Figure 4.29: Key Features of Concept 2



- Customisable to individuals lighting, temperature and sound preferences
- Log in to workstation to enable access to required programs and personalised set up of desk height, screen angles etc.
- Save favourite configurations e.g. standing when high workload experienced by operator.

Concept 2 – Multi-Input and Sit-Stand Workstation

Supports sit-stand operation.

Concept 2 – Touchscreen Input

Input 1:
Touchscreen Input device controls display monitors

Concept 2 – Eye and gesture control Input

Input 3:
Supports eye and Gesture control

Figure 4.30: Key Features of Concept 2 Continued

Similar to Concept 1, the size of this workstation has been developed using best practice from number of standards used to develop the TM Workstation for TMS 1st Deployment in the UK. However due to the use of an integrated desktop, the width of the screen array has been reduced which in turn has reduced the overall desk surface of the workstation required.

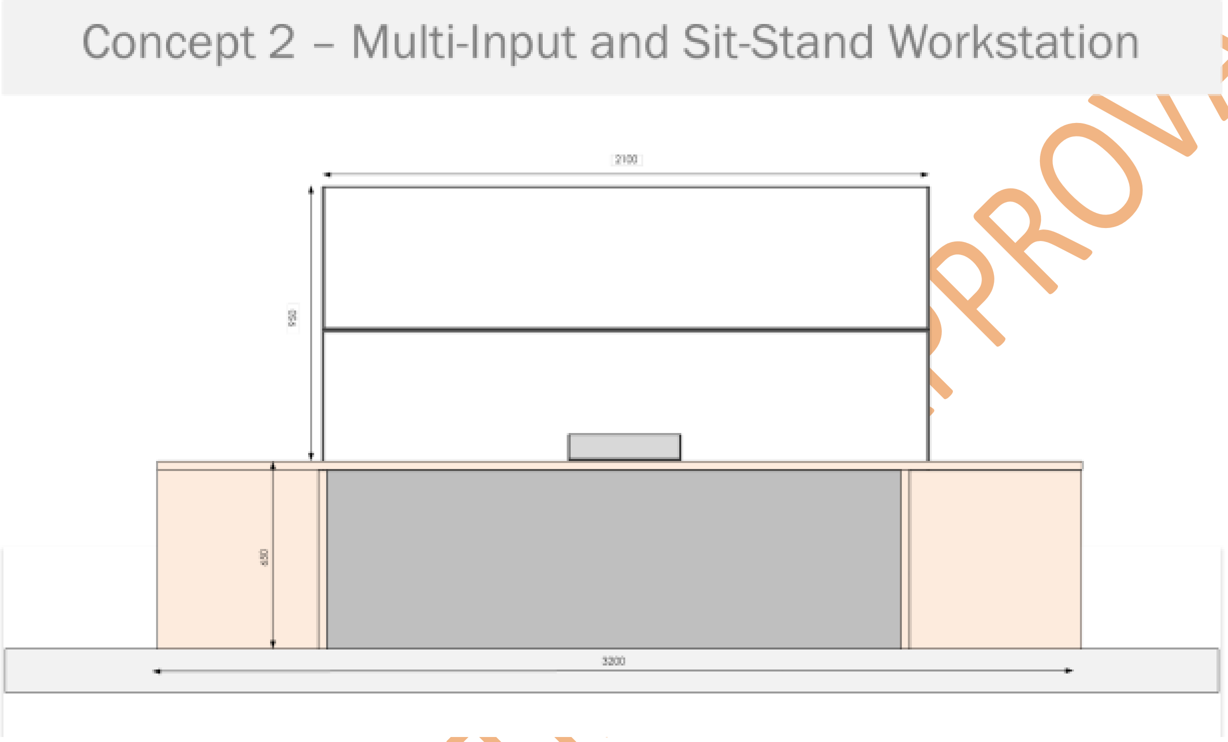
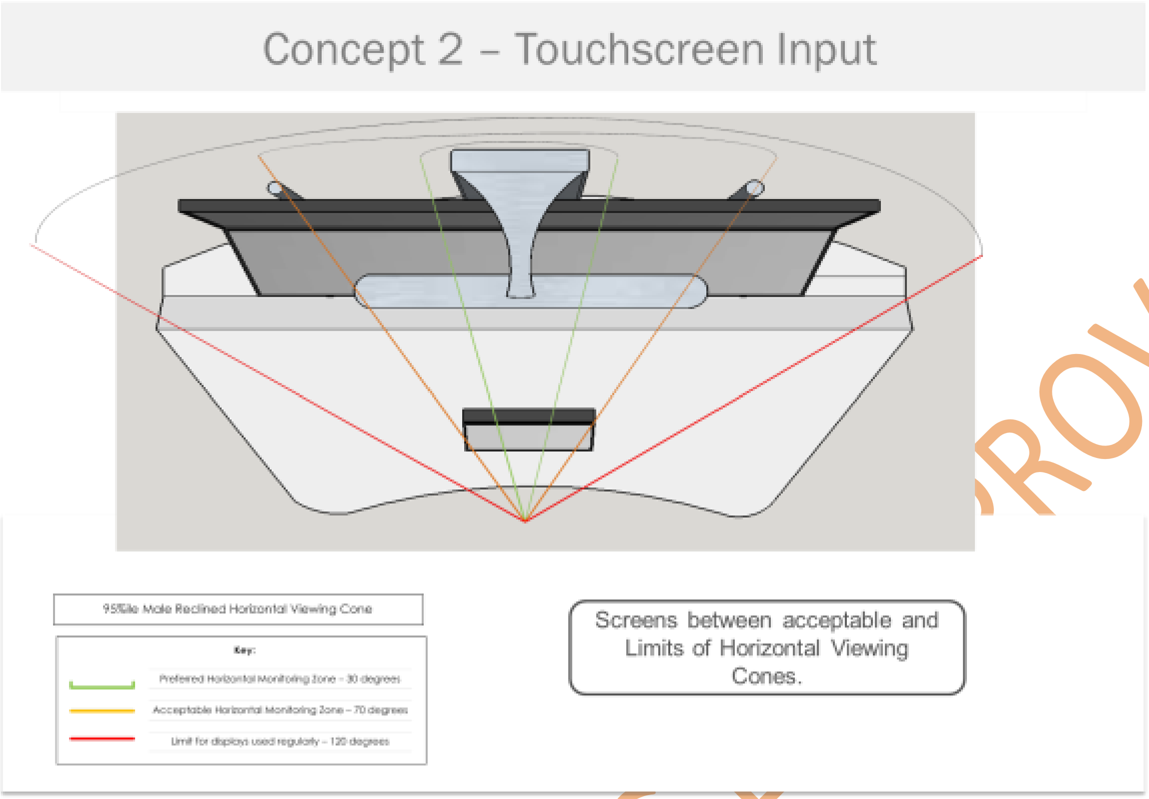


Figure 4.31: Dimensions of Concept 2 - Front Profile

The workstation dimensions and screen size has been optimised to ensure it is compliant with key ergonomic requirements stated in Section 4.4.3 (see Figure 4.32, Figure 4.33 and Figure 4.34).



Concept 2 – Touchscreen Input

95%ile Male Reclined Horizontal Viewing Cone

Key:

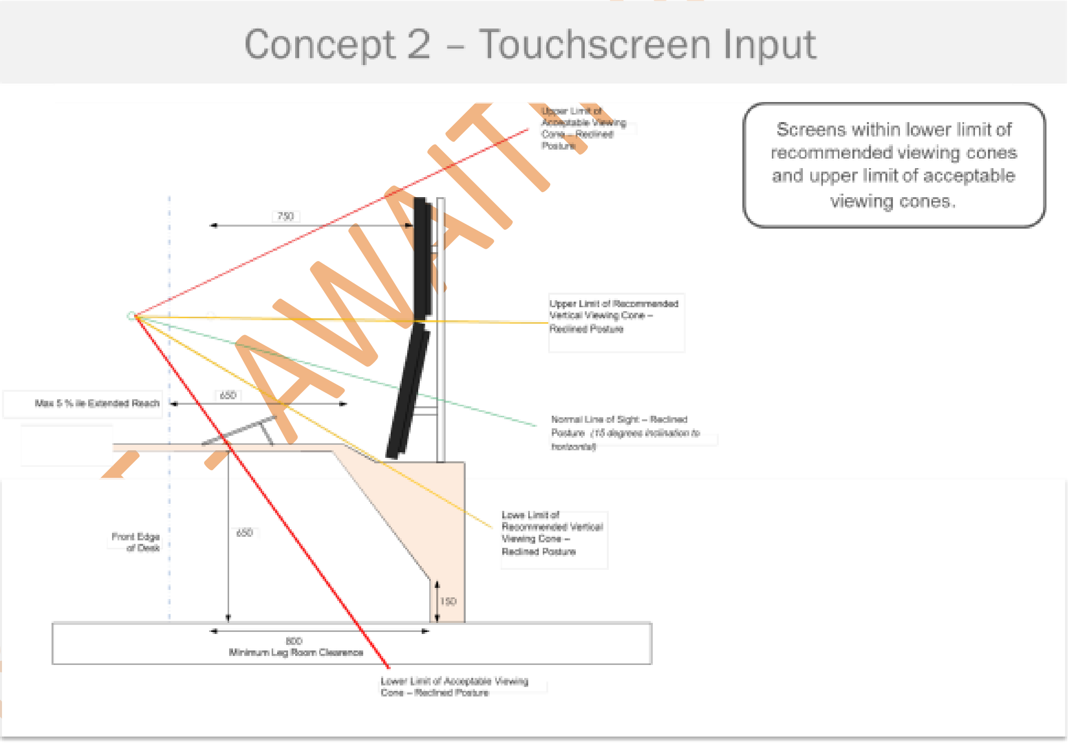
🟩 Preferred Horizontal Monitoring Zone – 30 degrees

🟨 Acceptable Horizontal Monitoring Zone – 70 degrees

🟥 Limit for displays used regularly – 120 degrees

Screens between acceptable and Limits of Horizontal Viewing Cones.

Figure 4.32: Horizontal Viewing Cone Analysis of Concept 2

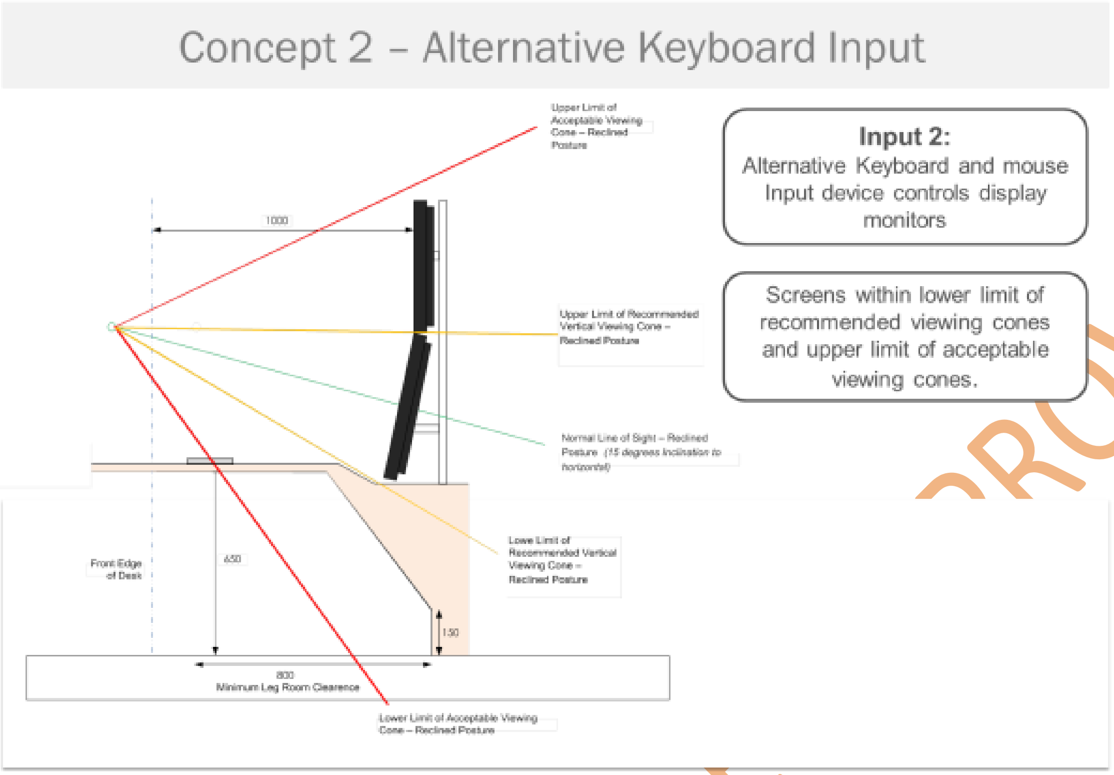


Concept 2 – Touchscreen Input

Screens within lower limit of recommended viewing cones and upper limit of acceptable viewing cones.

Upper Limit of Acceptable Viewing Cone – Reclined Posture
750
Upper Limit of Recommended Vertical Viewing Cone – Reclined Posture
Max 5 % ile Extended Reach
650
Normal Line of Sight – Reclined Posture (15 degrees inclination to horizontal)
Front Edge of Desk
650
Lowe Limit of Recommended Vertical Viewing Cone – Reclined Posture
150
800
Minimum Leg Room Clearance
Lower Limit of Acceptable Viewing Cone – Reclined Posture

Figure 4.33: Vertical Viewing Cone Analysis of Concept 2



Concept 2 – Alternative Keyboard Input

Input 2:
Alternative Keyboard and mouse Input device controls display monitors

Screens within lower limit of recommended viewing cones and upper limit of acceptable viewing cones.

Upper Limit of Acceptable Viewing Cone – Reclined Posture
1000
Upper Limit of Recommended Vertical Viewing Cone – Reclined Posture
Normal Line of Sight – Reclined Posture (15 degrees Inclination to horizontal)
Front Edge of Desk
650
Lowe Limit of Recommended Vertical Viewing Cone – Reclined Posture
150
800
Minimum Leg Room Clearence
Lower Limit of Acceptable Viewing Cone – Reclined Posture

Figure 4.34: **Vertical Viewing Cone Analysis of Concept 2**

	Concept 2 - Evaluation		
Consideration	**Advantages**	**Disadvantages**	**Suggestions**
Ergonomics	• Multiple input methods – suits each user's need and preferences as well as customisable to support specific tasks required. • Reduce number of screens – reduces the number of breaks in information on the screen and across critical information. • Benefits of integrated desktop; Dynamic views, widgets and customisation of windows for each user – supporting individual needs and decision making by role and task required etc. • Centre of main lower screen is at user's normal line of sight. • Customisable to individuals lighting, temperature and sound preferences	• Potential resistance by users used to current technologies and training required. • Training may be required to ensure all generations have technical skills to use new technologies.	
Inclusive design	• Eye and gesture control benefits; Using this process, human can interface with the machine without any mechanical devices, therefore beneficial for users which physical impairments or mobility restrictions.		
Healthy working principles	• Sit-Stand desk enables users to operate workstation in both sitting and standing postures, reducing effects of prolonged static postures. • Enables small adjustments of work surface height to enable each user to find a comfortable height	• Adjustable micro-climates are expensive and difficult to control.	

	Concept 2 - Evaluation		
Consideration	**Advantages**	**Disadvantages**	**Suggestions**
	which supports arm rest on the work surface.		
Technology	• Larger screens support integrated desktop – seamless displays – 'Plug and Play' architecture. • Show cases rail industry capabilities – novel technologies to rail sector: Touchscreens, eye gesture and gesture control etc. Attract next generation of users. • Quick and easy for the users to adjust angle of screens,	• Technology readiness: Large screen sizes used in gaming but less readily available commercially – high cost now but expected to become commercially available in next 5 years. • Technology readiness: Types of tasks that can be controlled by eye and gesture control need to be defined and tested to ensure suitable for safety critical tasks. • Technology readiness: Lack of proof of concept of Integrated desktop and 'plug and play' architecture in Rail industry.	• Select screens with no bevels to further reduce breaks on the screen and across critical information. • Need to ensure suitable design mitigations are in place to ensure technologies are suitable for safety critical commands.
Security	• Log in via assistive tool (e.g. bracelet) for quick and easy access to system and personalised set ups.	• Potential breach of security if assistive tool is lost or stolen.	
Maintainability		• Customised solution for moving components, need to ensure RAMS	• Need to ensure moving parts can be

	Concept 2 - Evaluation		
Consideration	**Advantages**	**Disadvantages**	**Suggestions**
		and moving components are reliable.	easily accessed to be maintained and need to protect from dust and grime. • Predictive maintenance - predict failure before failure occurs.
Sustainability		• Cost of pneumatic and sensor controls.	• Ensure spare components are easily accessible and suitable through life support.

Table 4.3: Concept 2 Evaluation

4.9.3 Concept 3

Concept 3 was developed not to replace the conventional workstation but to be used as a collaborative support decision tool during certain scenarios such resolving incidents or de-briefing at the end of the day.

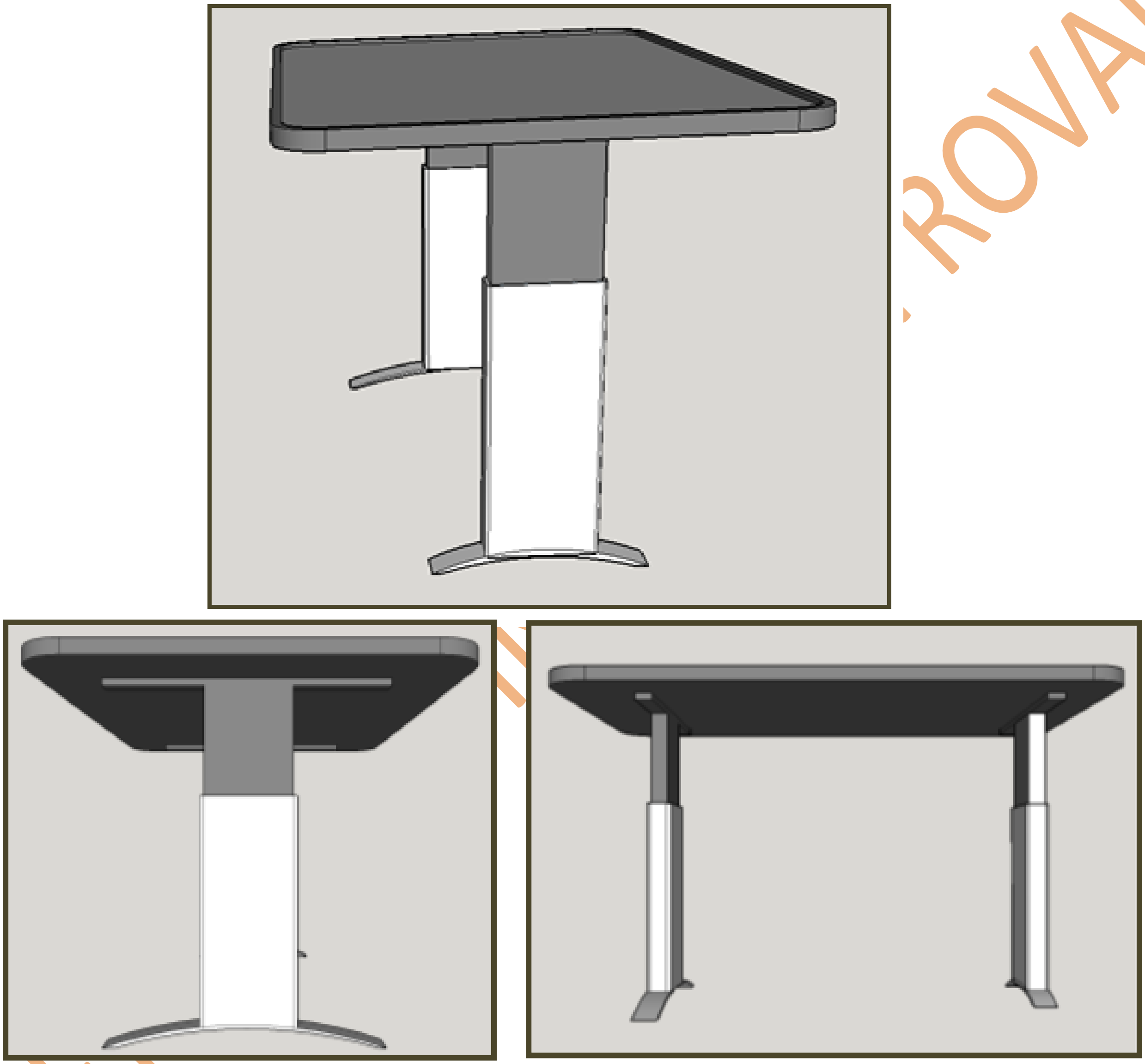
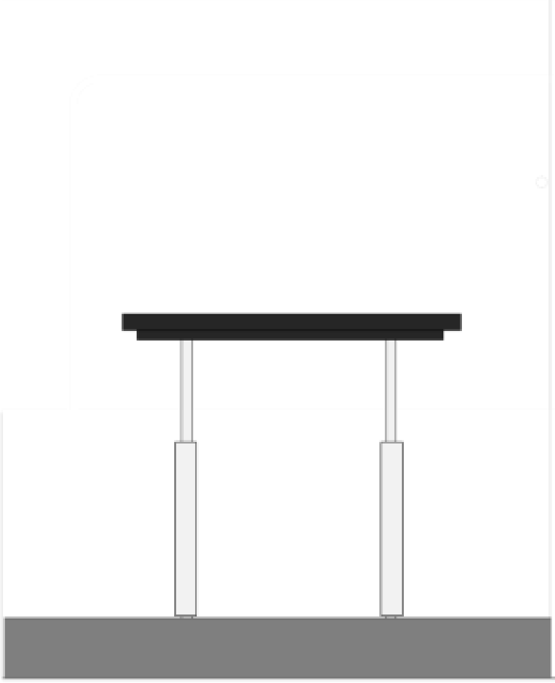
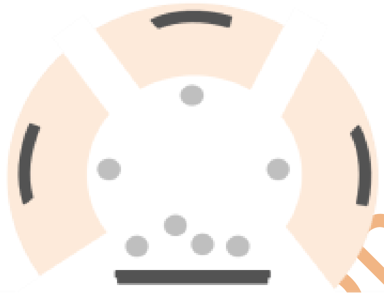


Figure 4.35: Concept 3

During the Concept Review Workshop, it was discussed whether this support tool could be achieved by using spare conventional workstation's in the standing position to enable multiple users to use a singular workstation at once to resolve incidents. Although this was agreed possible, the stand alone support tool was liked by RFI and was seen as a credible solution in its own right.

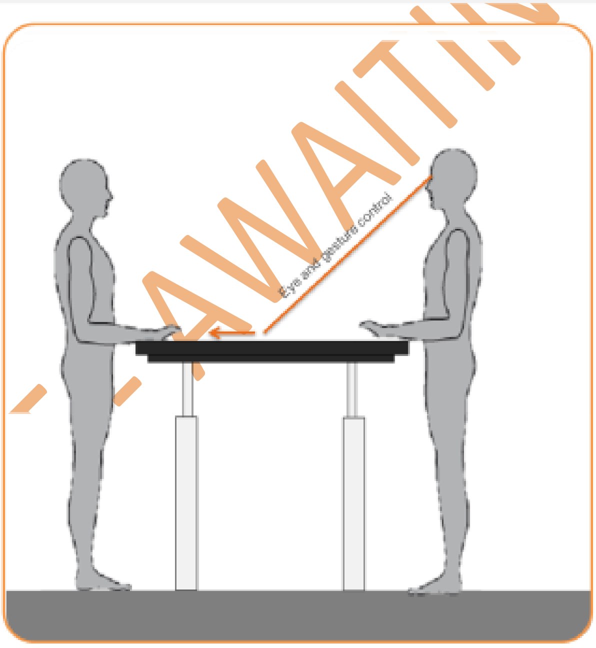
Concept 3 – Pod and Scenario Support Tool (Table)





Multi-touch interactive touch tables located on the control floor to support collaborative working scenarios.

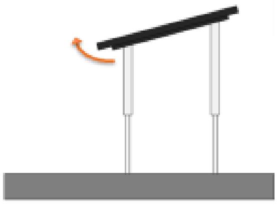
Concept 3 – Pod and Scenario Support Tool (Table)



Multi-touch screens

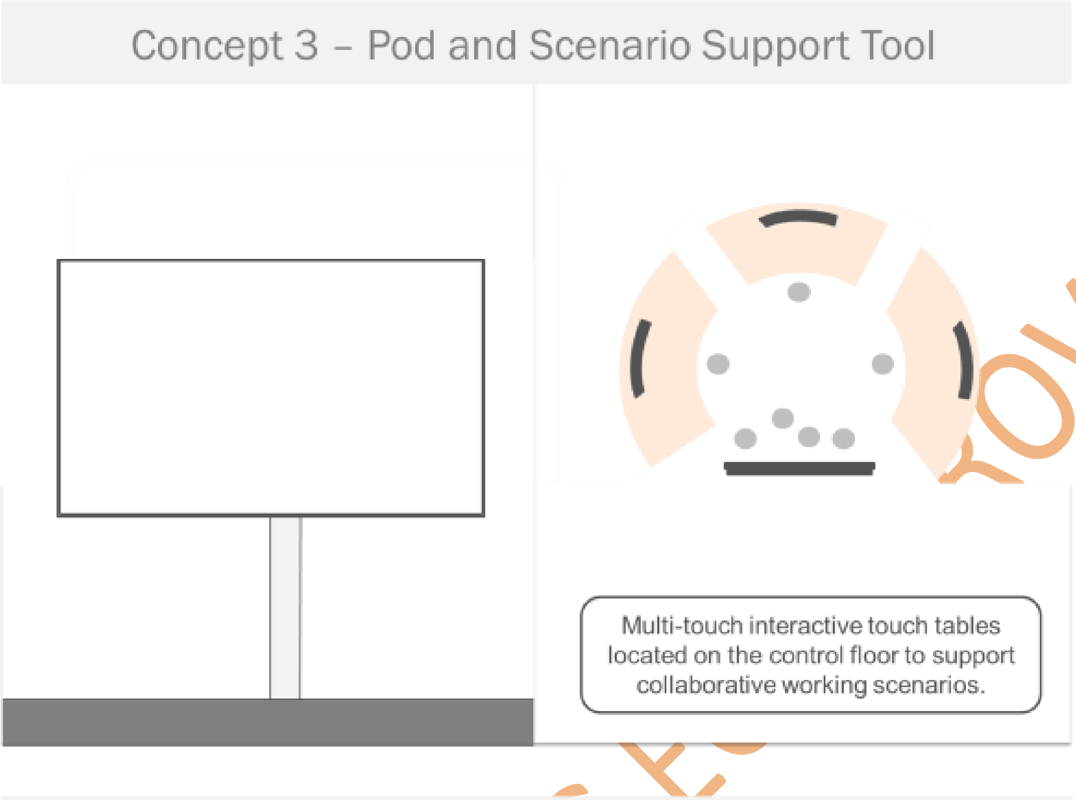
Supports collaborative working during certain scenarios:

- Resolving Incidents
- Training, *(in addition to/ to compliment training on users required workstations).*
- De-briefing/Lessons Learnt



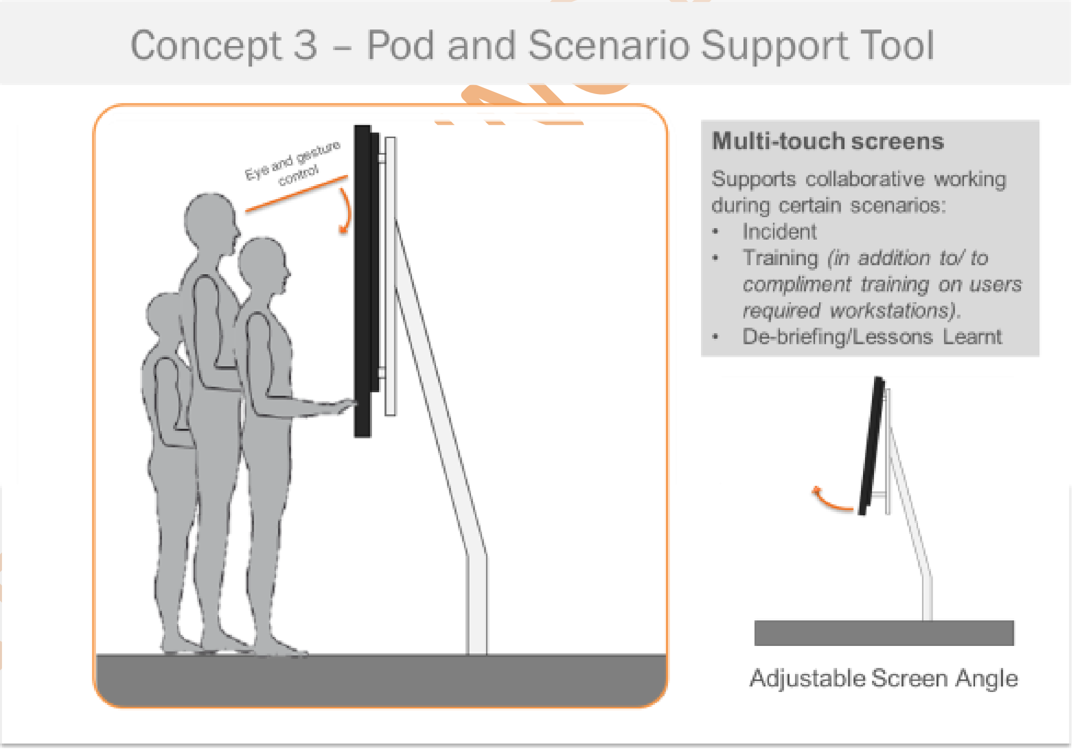
Adjustable Screen Angle

Figure 4.36: Features of Concept 3



Concept 3 – Pod and Scenario Support Tool

Multi-touch interactive touch tables located on the control floor to support collaborative working scenarios.



Concept 3 – Pod and Scenario Support Tool

Multi-touch screens

Supports collaborative working during certain scenarios:

- Incident
- Training *(in addition to/ to compliment training on users required workstations).*
- De-briefing/Lessons Learnt

Adjustable Screen Angle

Figure 4.37: Features of Concept 3 Continued

	Concept 3 - Evaluation		
Consideration	**Advantages**	**Disadvantages**	**Suggestions**
Ergonomics	• Support users in resolving major performance or safety related incidents collaboratively. • Enables users to share information quickly and manipulate information easily to resolve complex issues quickly. • Useful for de-briefing at the end of a day to learn from key scenarios and improve efficiencies in performance.	• Size of interactive table limited by 5%ile users reach. • Difficult to reach far corners when sat down, would need to interact with alternative methods e.g. eye control.	• Due to issues in security and/or human error in multiple users interacting with table, type of tasks that users should be able to perform should be information related only, no safety critical inputs. • Use play – back facilities so can re-run scenarios
Inclusive design	• Multiple input devices support users in completing tasks in a variety of methods depending on impairment.		
Healthy working principles	• Encourages users to be active and move around the interactive table/stand. • Enables users to move from their normal workstation.		

	Concept 3 - Evaluation		
Consideration	**Advantages**	**Disadvantages**	**Suggestions**
Technology	• Multiple input devices support users in completing tasks in a variety of methods depending on the type of task. • Supports the use of AR for maintenance activities. • Multi-touch tables enable multiple users to interact with the table/stand. • Show cases rail industry capabilities – novel technologies to rail sector: Touchscreens, eye gesture and gesture control etc. Attract next generation of users. • Larger screens support integrated desktop – seamless displays – 'plug and play' architecture. • Touchscreen benefits; enhances comfort, increased control, quick and easy to manipulate interface etc.	• Training may be required to ensure all generations have technical skills to use new technologies. • Need to ensure suitable design mitigations are in place to ensure technologies are suitable for safety critical commands.	
Security		• If multiple users are interacting with table, loose ability to know who performed command. • Need to determine what types of commands/functions would be suitable to perform.	• Log on required to ensure only authorised personnel have access.

	Concept 3 - Evaluation		
Consideration	**Advantages**	**Disadvantages**	**Suggestions**
Maintainability		• Bespoke equipment, low number of units. Need to ensure spare parts are easily available and not too expensive.	
Sustainability		• Bespoke equipment and specific application. (The same effect is nearly achieved by having a spare workstation for multiple users to use during specific critical scenarios).	

Table 4.4: Concept 3 Evaluation

4.9.4 Concept 4

During the Concept Workstation Review, a final fourth concept was discussed based on a future workstation concept developed by Rolls Royce that was presented by Siemens.

Key principles that were agreed to be useful from the Rolls Royce future concept were utilised where possible and areas where partners thought the design could be improved were captured and applied to the concept.

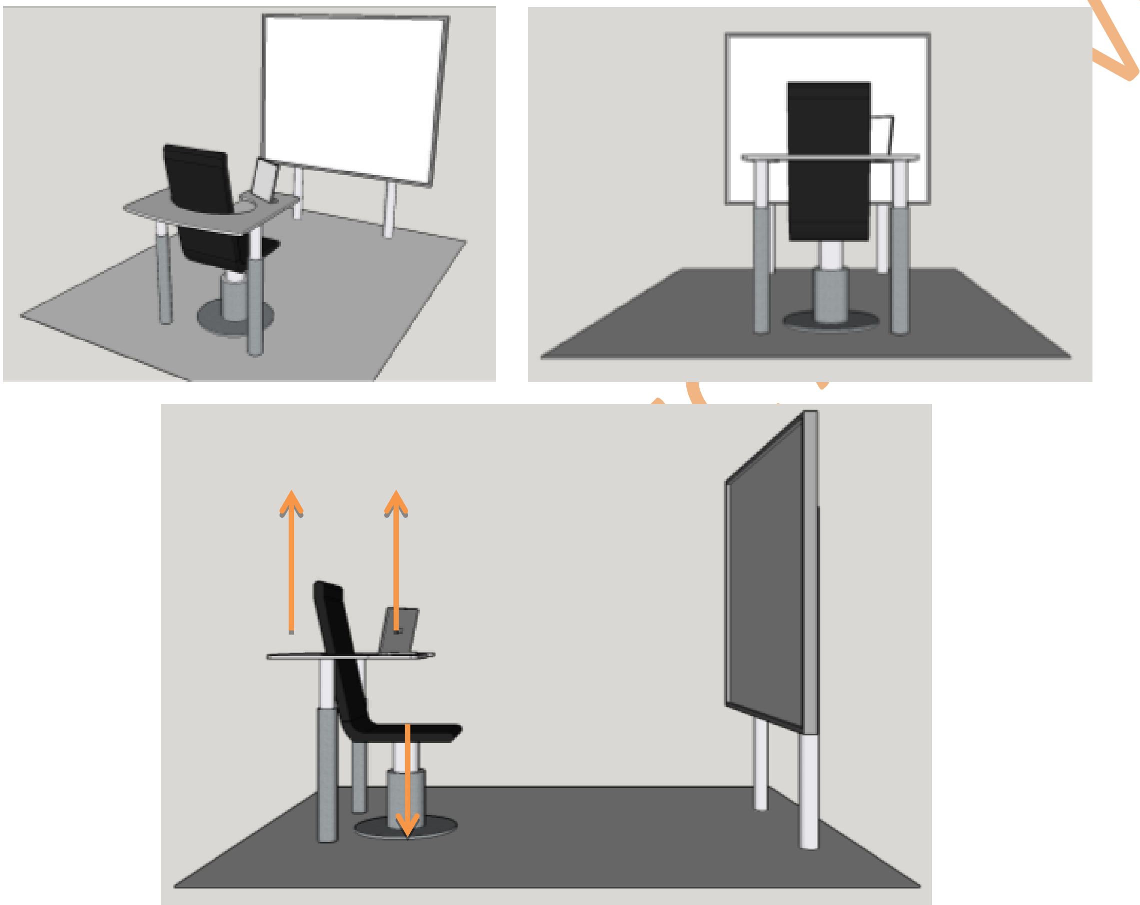


Figure 4.38: Concept 4

Key principles of Concept 4 include:

- The need for requiring a large work surface has been replaced by a central touchscreen control system that can be placed either to the left or the right of the user depending on their needs. The user can interact with the system either via, the touchscreen control, voice commands and eye gesture control.
- It utilises a large singular screen than can be raised or lowered in height, or brought closer to the user if required,
- The chair can be lowered or raised and the work surface can be raised to above the chair level to also provide a standing workstation position.

	Concept 4 - Evaluation		
Consideration	**Advantages**	**Disadvantages**	**Suggestions**
Ergonomics	• Enables users to share information quickly and manipulate information easily to resolve complex issues quickly. • Multiple input methods – suits each user’s need and preferences as well as customisable to support specific tasks required. • Reduce number of screens – reduces the number of breaks in information on the screen and across critical information. • Benefits of integrated desktop; Dynamic views, widgets and customisation of windows for each user – supporting individual needs and decision making by role and task required etc.	• Potential resistance by users used to current technologies and training required. • Training may be required to ensure all generations have technical skills to use new technologies.	
Inclusive design	• Multiple input devices support users in completing tasks in a variety of methods depending on impairment. • Eye and gesture control benefits; Using this process, human can interface with the machine without any mechanical devices, therefore beneficial for users which physical impairments or mobility restrictions.		
Healthy working principles	• Enables users to move from their normal workstation position. • Sit-Stand desk enables users to operate		

	Concept 4 - Evaluation		
Consideration	**Advantages**	**Disadvantages**	**Suggestions**
	workstation in both sitting and standing postures, reducing effects of prolonged static postures. - Enables small adjustments of work surface height to enable each user to find a comfortable height which supports arm rest on the work surface.		
Technology	- Multiple input devices support users in completing tasks in a variety of methods depending on the type of task. - Show cases rail industry capabilities – novel technologies to rail sector: Touchscreens, eye gesture and gesture control etc. Attract next generation of users. - Larger screens support integrated desktop – seamless displays – 'Plug and Play' architecture. - Touchscreen benefits; enhances comfort, increased control, quick and easy to manipulate interface etc. - Quick and easy for the users to adjust angle of screens,	- Training may be required to ensure all generations have technical skills to use new technologies. - Need to ensure suitable design mitigations are in place to ensure technologies are suitable for safety critical commands.	
Security		- Need to determine what types of commands/functions would be suitable to perform via each input method.	- Log on required to ensure only authorised personnel have access.

	Concept 4 - Evaluation		
Consideration	**Advantages**	**Disadvantages**	**Suggestions**
Maintainability		• Customised solution for moving components, need to ensure RAMS – ensure moving components are reliable.	• Need to ensure moving parts can be easily accessed to be maintained and need to protect from dust and grime. • Predictive maintenance - predict failure before failure occurs.
Sustainability		• Cost of pneumatic and sensor controls.	• Ensure spare components are easily accessible and suitable through life support.

Table 4.5: Concept 4 Evaluation

4.9.5 Workstation Principles

The optimal TM workstation solution is likely to be a combination of components set out in the four options. To support future applications where the processes and user needs are not well defined, a set of design principles has been developed as a guide. Therefore, based on the advantages collected for each of the four concepts, the following generic principles have been gathered that should be applied to future TM workstation design as far as possible.

Consideration	Examples
Ergonomics	**Physical:** • Controls or input devices shall be within the normal reach envelopes for the 5 % percentile female. • Screens shall be within acceptable horizontal and vertical viewing Cones. • Screens and displays shall be within acceptable viewing distances. • The workstation shall meet the needs of shortest/tallest anthropometric limits. • The workstation shall support under work surface leg clearance, (both laterally and for leg room depth). • The micro-climate and thermal environment shall be customisable by each user. • The user shall be able to configure their desktop and set up personalised dashboards role and task dependant. • One singular screen should be used where possible to reduce the number of breaks in information on the screen and across critical information. (Note where large singular screens are used, manual handling principles need to be considered). **Cognitive:** • The workstation shall support users in pro-active rather than reactive decision making. • The users should be considered as part of the system to reduce the effects of complacency by keeping users informed on key decisions deemed required, e.g. have a large performance or safety impact. • The workstation shall support distributed cognition, support communication and sharing of information to enable collaborative decision making. • Information shall be presented to the right person(s) at the right time and in the right format to create the optimum level of workload to enable high performance and safe management of the railway.
Inclusive design	• Suitable for wheelchair access. • Support users with restricted mobility or visual impairments. • Ensure multiple input devices can be used. • Ensure multiple feedback methods and multiple methods of attention. • Configurable display to support individual user's needs. • Enable use of assistive technologies where possible.

Consideration	Examples
Healthy working principles	• The workstation shall support sit-stand operation • The workstation shall encourage movement where possible and reduce length of prolonged static postures • The workstation shall enable breaks or work to be shared collaboratively • The workstation shall enhance comfort, thereby improving motivation and performance.
Technology	• Technologies used shall support key future user needs defined for In2Rail e.g. support distributed cognition • Technologies used shall enhance user experience and attract younger generation • The workstation shall make use of integrated desktop technologies. • It should be quick and easy to configure personalised dashboards and workstation set ups.
Security	• Due to changes in concept of operations to flexible and collaborative working styles - need to ensure there are correct process and procedures / technology to ensure correct authorisation/authentication of users.
Maintainability	• Plug and play architecture, parts in stock and available, software releases when required for update e.g. change in standards, change in rules, bug in software.

Table 4.6: Workstation Principles

4.10 Operator Workstation Application HMI Displays

This section will describe the output of subtask 7.2.4.4, “Operator Workstation Application”, led by Siemens. The scope of this subtask is focused in the Application and the definition of the HMI and is primarily aimed to propose a conceptual design for application, as a first step for a future standardization.

4.10.1 Design Principles

All of the workstation concepts in Section 4.9 make use of one or two large seamless displays and novel technologies such as touchscreens. Based on this principle, the Workstation Application concept has been developed following four main principles:

1. Comprehensibility:

As the TMS will become more and more automatic and will require less manual intervention, it is likely that a fewer number of workstations will be necessary to control large railway areas. Therefore, future workstations should contain better, more efficient software and hardware resources. Increased intelligent features in workstations and system design should lead to more comprehensive applications and a holistic view of the railway.

2. Versatility:

As everything will be centralized, and the same workstation room will be used for controlling and monitoring all the different systems, workstations should be multi-purpose. Both hardware and software shall be designed to support any use case and/or role at the TMS.

3. Portability:

TMS personnel are expected to take more responsibilities than today. Moreover extensive collaborative work is suggested as the way to work in the future for taking decisions and managing the railway. Therefore, the workstation should support the “portable” concept, giving the freedom to the operator to leave his/her place and attend other tasks while he/she is still able of acting in case of emergency.

4. Dynamic:

Any input from the operator or output to the operator shall be supported by the workstation using a dynamic behaviour, meaning:

- Login/ logoff, predefined configurations and personal configurations shall be quick, automatic and easy to change, using also new technologies that will ensure more security and will simplify the operator’s effort at the same time;
- Views and layouts shall be flexible so each user can adapt them to his/her needs. Bespoke scenarios shall be also provided by the workstation to focus the operator’s attention under certain circumstances, such as emergency situations.

As well as these four considerations, it’s essential that the information systems and HMI support the cognitive user needs and problems identified in section 4.4.7.1 such as:

- Enable intelligent decision support: support pro-active, rather than reactive monitoring and tasks;
- Reduce complacency from automation: The user should be considered as part of the system to minimise lack of situational awareness and to enhance decision making;
- Use automation and decision support to reduce the burden on the user to enable them to make complex decisions effectively to improve the performance of the railway;
- Support communication tasks and collaborative decision making through the sharing of information across different roles, and during different scenarios via different applications;
- Support distributed cognition: The TM pod will be made up of a number of operators, all using different information systems for different scenarios, The TM pod needs to be considered as a holistic model to ensure complex information is presented to the right person(s), at the right time and in the right format.

4.10.2 Comparison of technologies to consider

The benefits or disadvantages of technologies that have been considered in the workstation design in section 4.6 and the workstation application concept in this section, section 4.10, are summarised in Table 6.7.

It should be noted that although it is useful to determine the advantages and disadvantages of technologies, it is important to keep a holistic view of the application of the technology in the railway and also how it relates to people and process. Therefore the selection of technologies should be based around the user needs and ensuring they enhance safety and performance of the railway.

4.10.3 Proposal of Conceptual Design

Figure 4.39 shows that the application concept is based on the principle of one operating system where multiple applications can be utilised.

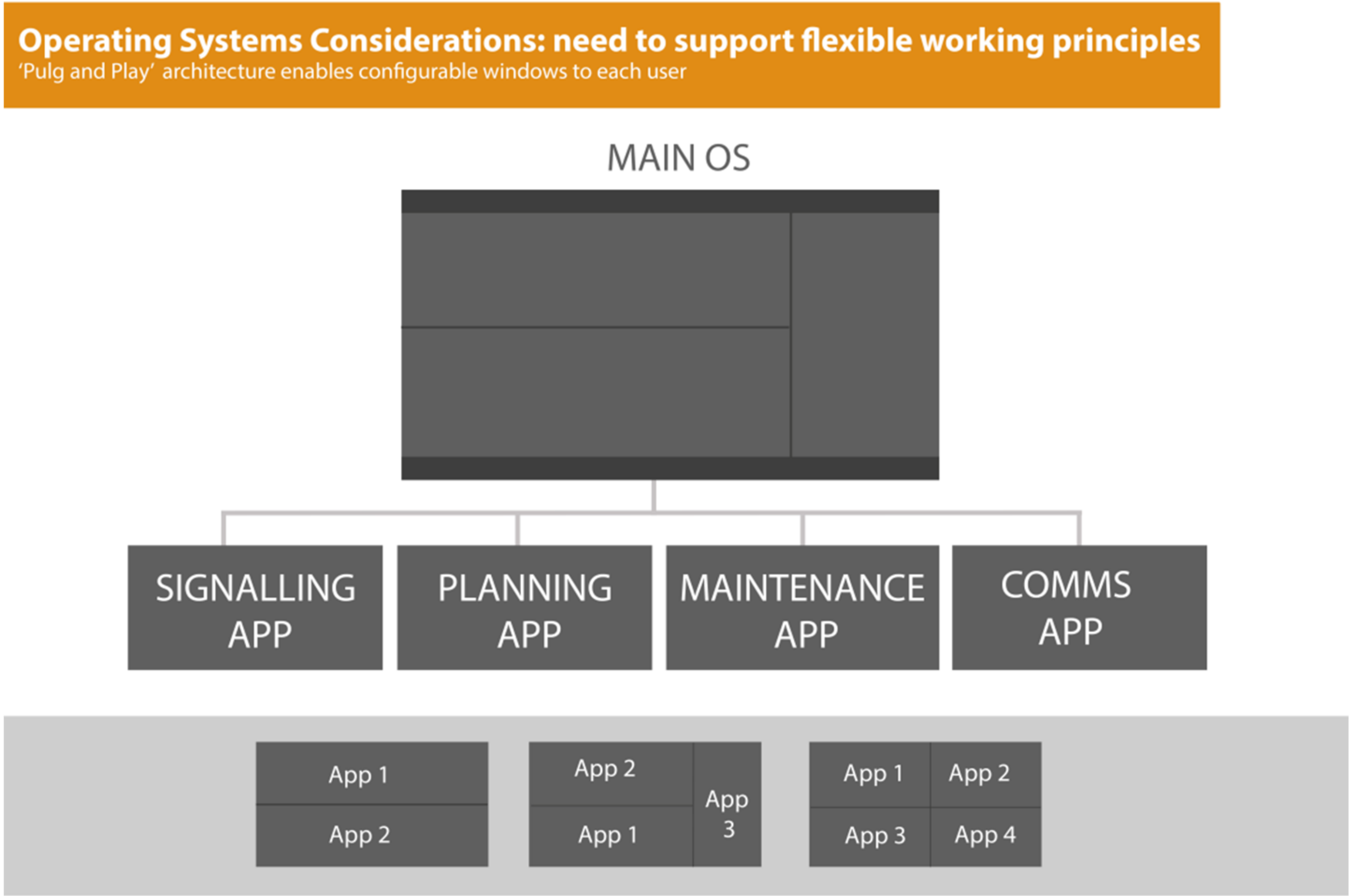
Technology	Benefits / Opportunities	Negatives / Barriers to implement
Touchscreens	• Update software as standards change • Update software as procedures change • Accuracy of selection (cursor directly under finger) • Reduces biomechanical load (improve comfort) - (depending on angle and position of screen) • Supports transferable zones of control or transferable information • Quick and easy to manipulate interface • Younger generation brought up on touchscreen technology • Development of 'raised' touchscreens • If fail, can more easily replace than physical controls •	• Resistance by users used to current technologies and training required • Information must be presented larger to be suitable for touch operation reducing amount of information on screen • Higher sensitivity – safety critical controls may need secondary input or confirmation • Effects of dust, grime and light reflections need to be taken into account.
Augmented Reality	• 'An enhanced view of real life by overlaying computer generated content' - Overlaid information to support users decision making e.g. Dashboard information or support maintenance activities. • Support product development and concept design phases to engage customers. • Increases engagement and provides richer user experience • Inexpensive as no specific media needs to be purchased • Enables operators to 'drag and drop' information onto any surface • Potential to partner with Universities for AR skills and expertise • An example use of AR could be via augmented reality.	• Resistance by users used to current technologies and training required. • Lack of acceptance or proof of concept in rail industry in control room environment • Current usage more applicable for maintenance on track side and in cab displays than in control room. • Need in house skills to use AR or sub-contract out

Technology	Benefits / Opportunities	Negatives / Barriers to implement
Multi-touch Tables	• Easy and quick manipulation of information • Multiple people can interact with table – support collaborative behaviour and share decision making • Update software as standards change • Update software as procedures change • Accuracy of selection (cursor directly under finger) • Reduces biomechanical load (improve comfort) – (depending on angle and position of screen) • Younger generation brought up on touch technology	• Resistance by users used to current desktop technologies • Information must be presented larger to be suitable for touch operation reducing amount of information on screen • Higher sensitivity – safety critical controls may need secondary input or confirmation • Effects of dust, grime and light reflections need to be taken into account. • Might not be suitable for all roles and tasks • Lack of acceptance or proof of concept in rail industry in control room environment
Wireless/Bluetooth Technology	• An example use of wireless or blue tooth technology could be via a headset, tablet device or keyboard and mouse. • Enables flexibility for operators to be able to move around their workstation or the control room while still using their input devices or communication devices.	• Adds a level of complexity in process to if devices are being used away from an operator's workstation. • Security and reliability in information transferred across wireless and Bluetooth technology.
Eye Gesture and Gesture Control	• A gesture is a 'non-verbal communication made with a part of the body', its uses a combination of different tools of technologies such as camera, graphics, vision etc. • Humans naturally use gesture to communicate • Using this process, human can interface with the machine without any mechanical devices, therefore beneficial for users which physical impairments or mobility restrictions. • Gesture types; hand, head, finger, body etc. • Examples; Pointing to items on the large screen with	• Movements vary person to person • Need in house skills to use or sub-contract out • Lack of acceptance or proof of concept in rail industry in control room environment • Resistance by users used to current technologies and training required.

Technology	Benefits / Opportunities	Negatives / Barriers to implement
	voice, Text editing, manipulating objects, controlling maps etc.	
Virtual Reality	• Useful technique in training by using 3D and virtual reality environments as part of training methodology • Use e-learning to teach/learn the theoretical understanding and knowledge then virtual reality scenarios to test the information learned in a life-like situation • Safe and effective learning environment • Reduce cost • Highly immersive • 'Bring the site to the office' • Engage tech-savvy learners • Potential to partner with Universities for VR skills and expertise	• Resistance by users used to current technologies and training required. • Lack of acceptance or proof of concept in rail industry in control room environment • Current usage more applicable for maintenance on track side and in cab displays than in control room. • Need in house skills to use VR or sub-contract out
Integrated desktops	• Integrated Desktop enables ability to create customer/user friendly HMI's from existing applications - existing applications are interwoven instead of forcing existing application behaviour and complexity. • Enables reduction in the amount of legacy systems or separate screens and/or PC's per system. Therefore reducing number of screens, enabling screens to be within user's field of view. • Quick set-up of desktop – reduce training needs. • Dynamic views, widgets and customisation of windows for each user – supporting individual needs and decision making by role and task required.	• Creating 'open block' architecture is beneficial to Customer as multiple suppliers can 'plug and play' into architecture. Potentially disadvantages the supplier as no longer dependant on by customer for entire solution. • Lack of acceptance or proof of concept in rail industry in control room environment

Technology	Benefits / Opportunities	Negatives / Barriers to implement
	• Enables information across multiple systems to be shared to create holistic view of railway and present accurate representation of railway to support users decision making.	
Large Curved Screens	• Curved screen supports viewing angles. • Most curved screens in 4K resolution – clear displays. • 55" + screen sizes – Therefore all information can be viewed on one large screen, enabling information to be displayed in appropriate viewing cones.	Depending on curvature of screens, multiple may not be used in series. (Where end of curved screens meet – potential to skew information reading across screens).
Data analytics and intelligent systems (AI)	• Gather metrics on railway assets and operational performance. • Present complex information in clear and user friendly manner in order to support user's decision making. • Have the ability to present the right information to the right user at the right time. • System maturity and intelligence grows as environment and user needs are more understood.	• Expensive and complex to develop intelligent algorithms which present useful information. • Has the potential for information and displays to be too complex and not show the user relevant or too much information, resulting in overload

Table 4.7: Technologies to Consider for workstation and application design



Operating Systems Considerations: need to support flexible working principles

'Pulg and Play' architecture enables configurable windows to each user

Figure 4.39: Design Journey Image 6 - Operating system considerations

The Workstation Application concept consists of the following hardware components. It is noted that such hardware components constitute the Human-Machine Interface (HMI) for Standardized Operator's Workstation:

1. Screens: three (3) screens are provided per Workstation, namely:
   - Overview screen.
   - Close-up screen.
   - Portable screen.
2. Login-logoff devices:

Devices providing automated biometric identification, such as:

- Finger point
- Iris recognition.
- Voice recognition.
- SMART bracelet access, tec.

3. Extra devices:
   - Wireless headset (integrated telephony system and voice recognition).
   - Smart glasses.

4.10.3.1 Screens

Three different screens are proposed for Standardized Operator's Workstation. Screens shall be integrated in the Workstation Desk, according to ergonomics principles as considered in section 4.4.3. It should be noted that every screen is characterized by a particular layout.

4.10.3.1.1 Overview Screen

- The overview screen shall display all the information available. The overview includes new information to appear in the railway environment, such as:
  - widget-like views for issues like the weather forecast,
  - map view to physically allocate trains and associated/nearby services;
- Predefined layout of views per role shall be available and developed through end user engagement;
- Each layout consists of fixed panel locations but flexible sized windows. The user can change only the content of some of the panels, such as widgets, or CCTV images.

The Overview Screen would have a pre-defined layout of standard views per role, but the layout of windows on the screen should be configurable to authorized personnel.

The following picture shows the Overview Screen standard layout for dispatcher, as proposed in Section 4.10.5.1.

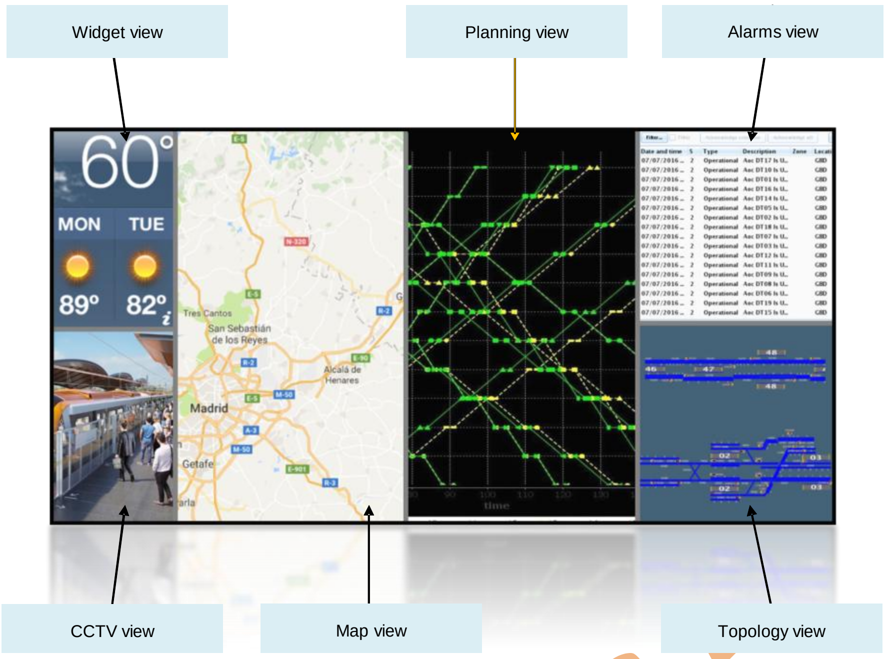


Figure 4.40: Overview Screen: standard layout for dispatcher

4.10.3.1.2 Close-up screen

- The close-up screen is a touchscreen which can be used to control the Overview Screen;
- It is noted that the Overview Screen should also be able to be controlled via a keyboard and mouse to support the desk design concept 1;
- The set of views is also predefined per role;
- The layout, size and number of views is not fixed and the user can resize and place the views wherever he/she wants;
- The look & feel is similar to the overview screen.

Using the touchscreen, operators could manipulate the size of the views as well as the information shown in each view on the Overview Screens.

For instance, the operator would be able to minimize views, change the size of windows and change the size or amount of information shown in each view on the touchscreen.

The following picture shows the Close-up Screen standard layout for dispatcher, as proposed in Section 4.10.5.1.

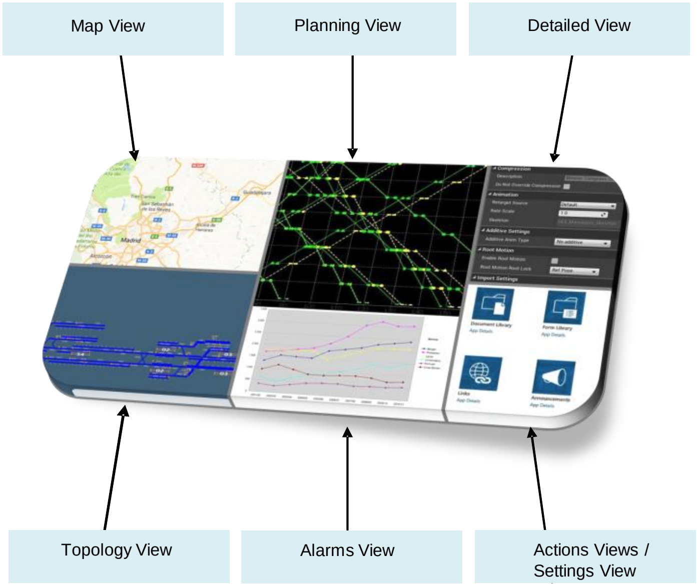


Figure 4.41: Close-up Screen: standard layout for dispatcher

4.10.3.1.3 Portable screen

- Tablet-like device;
- When docked (i.e. the operator is seated), it is disabled. When undocked, the close-up screen becomes locked and the tablet is enabled;
- The information displayed is the same as in the close-up view at all times.

Figure 4.42: Portable screen

The portable screen (tablet) could be used for operators to carry information from workstation to workstation to discuss scenarios. If an incident was to happen in their area of control, they would be alerted via the tablet device.

4.10.3.2 Login-logoff devices

Devices providing automated biometric identification are proposed to ensure restricted access to the workstation to authorized personnel only. This would help to improve IT Security and it also releases the users from the “passwords”.

For instance, if a fingerprint device is used for login, once the system recognizes the fingerprint of an authorized use, the layout of all screens would be updated according to the user preferences.

4.10.3.3 Extra devices

4.10.3.3.1 Headset

It may act as telephony system and input device substituting keyboard by voice commands.

For instance, the operator could activate voice commands to control the interface during the session. Another possibility is the use of noise cancellation headphones to reduce the environmental noise for the operators who prefer lower noise levels.

Figure 4.43: Headset

4.10.3.3.2 Smart glasses

This device can provide critical information during the management of an emergency scenario.

For instance, smart glasses could present operators with the most important information, drawing her/his attention to certain failure modes or alarms.

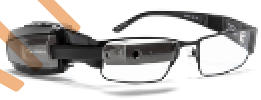


Figure 4.44: Smart glasses

4.10.4 Details of Views

According to the use cases, roles and FRS from WP7.1, and also taking into account the trends and new technologies that will be in the market in the future; see below the list of views that shall be available in a Standardized Operator’s Workstation.

View name	Summary	Information shown	Interaction	Roles
Widget view	• This view offers different widgets, connected to internet, which provide to the user complementary information that may be useful depending on the use case/operational scenario.	Example list of different widgets that can be included in the workstation: • Weather forecast widget: provides weather information related to the area being controlled at the TMS. It also may alert regarding future weather events that can impact railway operation. • News widget: provides a list of news related to the area being controlled at the TMS. • Social networks: provides connectors to social networks. This will help the users to get feedback and alerts from the railway users on real time.	• The user can select which widget is shown at each time.	• All
Map view	• This view provides an animated map containing static and dynamic information. Layer-concept shall be used to group different kinds of information, such as: information related to crew management, to consist management, to train operation,	Example list of different kinds of information that can be included in the map: • Crew management related information: driver's locations, crew facilities, driver's destinations. • Rolling stock management: rolling stock location, workshop facilities, etc. • Train operation: location of each running train. • Evacuation facilities: location of	• User shall be able to zoom and move the map; activate/deactivate layers displayed	• All

View name	Summary	Information shown	Interaction	Roles
	evacuation facilities, etc.	emergency exists, routes for rescue plans, location of other entities such as Police or Firefighter Stations, etc.		
Topology view	- A schematic view of the railway is provided, allowing the user to concentrate on railway operation when needed	- All elements associated to railway operation: trains, signals, points, etc. The information is grouped in layers, following the same concept as for the Map View	- User shall be able to zoom and move the map; activate/deactivate layers displayed; interact with the elements shown sending commands to remote controllers for changing the status of the railway	Supervisor Dispatcher
CCTV view	- This view shall offer CCTV images of the different cameras installed in the area being controlled at the TMS	- CCTV images	User shall be able to select any CCTV image at any time. Images can be also displayed using different layouts in the view, combining two or more images at the same time	Supervisor Dispatcher Maintainer
Alarms and events view	- List of alarms and events that are being processed by the TMS displayed as a tabular view	- The alarms and events processed by the TMS. These alarms and events are being provided by several systems, including the TMS	- Alarms can be acknowledged by the users; alarms and events can be commented; list can be filtered; each alarm/event shall be associated with the field element that triggers it, so the user can jump from the alarm view to a topology or map view	- All
Planning view	- This view shall provide schedule and regulation information of the railway	- The information shall comprise schedule and regulation functions of the TMS, providing detailed and comprehensive images in different	- The user can select the type of display at any time (tabular, time-distance graph, etc.). The view shall also allow the user to edit current	Supervisor - Dispatcher

View name	Summary	Information shown	Interaction	Roles
	operation	formats: tabular view, time-distance graphs, quality of service in real time, etc.	regulation parameters and schedule and validate the changes	
Settings view	View for allowing the user to customize the workstation	• The view provide controls for resizing and moving views on the different screens of the workstation; it also displays a set of pre-defined and stored layouts assigned to the users' current role	• The user can edit the layout of each screen to suit his/her needs; the editing comprises resize, location and number of views. The user can also store different layouts via this view	• All
Actions view	This is a dynamic view, automatically activated when the user wants to send a command to a certain element or group of elements	• The available commands that the user can send to a certain element	• User can input the commands using this view. Graphically the commands will be represented as buttons or something similar, but the user shall be able to also input commands via voice recognition	• All
Detailed view	A view for displaying details of a certain element. The details vary depending on the selection done	• Each element provides different information to be displayed on the detailed view	• The user can open the detailed view by selecting an element on other views such as map, topology, etc. Selection can be done manually using the touch screen of via voice recognition	• All
Assets view	View for displaying assets information in real time that can be used by maintenance personnel	• Assets related to maintenance are provided in graphical view using a schematic graph similar to the topology view; also a tabular form is provided	• The user can select elements on the view, apply available commands on each element, and finally show/hide elements or filter out the tabular form to concentrate on certain assets	Supervisor • Maintainer

View name	Summary	Information shown	Interaction	Roles
Logistics view	View for displaying logistic information associated with the maintenance of the railway	The logistic information comprises: • Spare parts supply • Component repair/replenishment manuals and procedures • Warehouse and stock handling	• The user can check and edit the information of the view	Maintainer
Reports and stats view	View for creating and displaying reports and stats of the TMS. The view provides support for both "operation of the railway" information and maintenance information	Statistics on real time generated by TMS Report facility for creating and managing reports	• The user can select which statistics to display at any time; the user can also create reports on demand, schedule report generation at a certain hour, and manage the archive of reports on the TMS	Supervisor Maintainer
Customer information view	View for graphically displayed the customer information infrastructure	Customer information elements on a schematic view with additional information relevant for customer information service	• User shall be able to zoom and move the map; activate/deactivate layers displayed; interact with the elements shown sending commands to remote controllers	Supervisor Customer information

Table 4.8: Details of Workstation Views

4.10.5 Layout of Views

Each layout is defined by a set of views according the role that it shall satisfy.

The layout shall be configured based on each TM deployments needs, and within this, each roles needs. The layout and views displayed to each user should be developed through workshops with each type of user to determine a layout which best supports their tasks required and decision making.

The following sections give examples of standard layouts per role, according to the generic functions defined for each role in In2Rail.

“Overview” stands for “Overview Screen”, whose concept is proposed in Section.4.10.3.1.1.

“Close-up” stands for “Close-up Screen”, as shown in Section 4.10.3.1.2.

4.10.5.1 Layout for dispatcher

Overview			
Widget view	Map view	Planning view	Alarms view
CCTV view			Topology view

Rationale: The map view and planning view make up the central display as these will be the most commonly used displays for the dispatcher. The less commonly used displays, such as the widget, the CCTV view and the topology view can be displayed towards the outer of the screen as they display less critical information. During system development, the alarms view should be developed such that it is clear to the user when a new alarm is generated and the viewing distance is suitable to interact with the alarm view to prevent human error or lack of decision support.

Close-up		
Map view	Planning view / Alarms view	Detailed view
Topology view		Actions view/Settings view

Rationale: The left part of the screen provides the geographical information (map and topology view). The central display is intended to be a tab-like panel where the dispatcher can combine or maximize the planning view and the alarms view depending on the operational scenario that he/she is managing.
On the right side, the detailed view and the actions view are updated automatically depending on the element selected by the dispatcher in the other views. Moreover, the Actions view panel can be used for displaying the Settings view.

4.10.5.2 Layout for supervisor

<table>
<tr><th colspan="4">Overview</th></tr>
<tr><td>Widget view</td><td rowspan="2">Map view</td><td rowspan="2">Planning view</td><td>Alarms view</td></tr>
<tr><td>Topology view</td><td>Reports and stats view</td></tr>
</table>

Rationale: The map view and planning view will also make up the central display as these will be the most commonly used displays for the supervisor, however these views may only be required in a read only form due to tasks required. The less commonly used displays, such as the widget, the topology view and reports can be displayed towards the outer of the screen as they display less critical information. During system development, the alarms view should be developed such that it is clear to the user when a new alarm is generated and the viewing distance is suitable to interact with the alarm view to prevent human error or lack of decision support.

<table>
<tr><th colspan="3">Close-up</th></tr>
<tr><td>Map view / Topology view</td><td rowspan="2">Planning view</td><td>Alarms view / Detailed view</td></tr>
<tr><td>Reports and stats view / Assets view / Customer information view</td><td>Actions view /Settings view</td></tr>
</table>

Rationale: The left upper part of the screen provides the geographical information (map and topology view). The left bottom panel is intended to be a multi-purpose area where the supervisor can open any view that he/she may want to check depending on the operational scenario. Normally this panel will display the Reports and Stats view but Maintainer's and Customer Information's views could be also shown here.
The central display focuses on the planning information as it is the most accurate view for the supervisor to check the railway operation. On the right side, the detailed view and the actions view are updated automatically depending on the element selected by the supervisor in the other views. Moreover the Detailed view can be used for displaying the Alarms view; and the Actions view panel can be used for displaying the Settings view.

4.10.5.3 Timetable Manager/Planner

<table>
<tr><th colspan="3">Overview</th></tr>
<tr><td rowspan="2">Map view</td><td rowspan="2">Planning view</td><td>Alarms view</td></tr>
<tr><td>Reports and stats view</td></tr>
</table>

Rationale: The planning view make up the central display as this will be the most commonly used display for the planner. Map view on the left side will help also the planner to check the situation of trains and how they move through the railway. The right side of the screen is composed of the alarms view and the reports and stats view for supporting the planner's decisions. During system development, the alarms view should be developed such that it is clear to the user when a new alarm is generated and the viewing distance is suitable to interact with the alarm view to prevent human error or lack of decision support.

<table>
<tr><th colspan="3">Close-up</th></tr>
<tr><td rowspan="2">Map view / Topology view</td><td rowspan="2">Planning view</td><td>Detailed view / Reports and stats view</td></tr>
<tr><td>Actions view/Settings view</td></tr>
</table>

Rationale: The left part of the screen provides the geographical information (map and topology view). The central display focuses on the planning information as it is the most important view for the planner. On the right side, the detailed view and the actions view are updated automatically depending on the element selected by the planner in the other views. Moreover the Detailed view can be used for displaying the Reports and stats view; and the Actions view panel can be used for displaying the Settings view.

4.10.5.4 Incident Coordinator

<table>
<tr><th colspan="3">Overview</th></tr>
<tr><td rowspan="2">Map view</td><td>Topology view</td><td>Alarms view</td></tr>
<tr><td>Assets view</td><td>CCTV view</td></tr>
</table>

Rationale: The topology view and assets view make up the central display as these will be the most commonly used displays for the incident coordinator. The less commonly used displays, such as the map and the CCTV view can be displayed towards the outer of the screen as they display less critical information. During system development, the alarms view should be developed such that it is clear to the user when a new alarm is generated and the viewing distance is suitable to interact with the alarm view to prevent human error or lack of decision support.

<table>
<tr><th colspan="4">Close-up</th></tr>
<tr><td rowspan="2">Alarms view</td><td rowspan="2">Map view</td><td rowspan="2">Topology view / Assets view</td><td>Detailed view</td></tr>
<tr><td>Actions view/Settings view</td></tr>
</table>

Rationale: The left upper part of the screen provides the Alarms view which is permanently displayed for the Incident coordinator. The geographical information (map and topology/assets views) is shown in the center part of the screen. On the right side, the detailed view and the actions view are updated automatically depending on the element selected by the incident coordinator in the other views. Moreover Actions view panel can be used for displaying the Settings view.

4.10.5.5 Layout for customer information

Overview		
Widget view	Map view	Alarms view
	Customer information view	CCTV view

Rationale: The map view and customer information view will make up the central display as these will be the most commonly used displays for customer information users. The less commonly used displays, such as the widget and the CCTV View can be displayed towards the outer of the screen as they display less critical information. However the widget view is larger for the customer information users as they will be monitoring and providing updates via social media channels. During system development, the alarms view should be developed such that it is clear to the user when a new alarm is generated and the viewing distance is suitable to interact with the alarm view to prevent human error or lack of decision support.

Close-up			
Widget view / Alarms view	Map view	Customer information view	Detailed view
			Actions view/Settings view

Rationale: The left part of the screen provides the widget and alarms view. The widget view is intended to be an important display for the customer information role as it will provide useful information of press news and feedback/comments from railway passengers through social networks.
The central display is divided in two sections for providing the geographical information (map view) and the customer information view. On the right side, the detailed view and the actions view are updated automatically depending on the element selected by the user in the other views. Moreover the Actions view panel can be used for displaying the Settings view.

4.10.5.6 Layout for maintainer

Overview		
Topology view	Map view	Alarms view
Reports and stats view	Assets view	CCTV view

Rationale: The map view and assets view make up the central display as these will be the most commonly used displays for the maintainer. The less commonly used displays, such as the topology view, the reports and stats, the alarms view and the CCTV view can be displayed towards the outer of the screen as they display less critical information. During system development, the alarms view should be developed such that it is clear to the user when a new alarm is generated and the viewing distance is suitable to interact with the alarm view to prevent human error or lack of decision support.

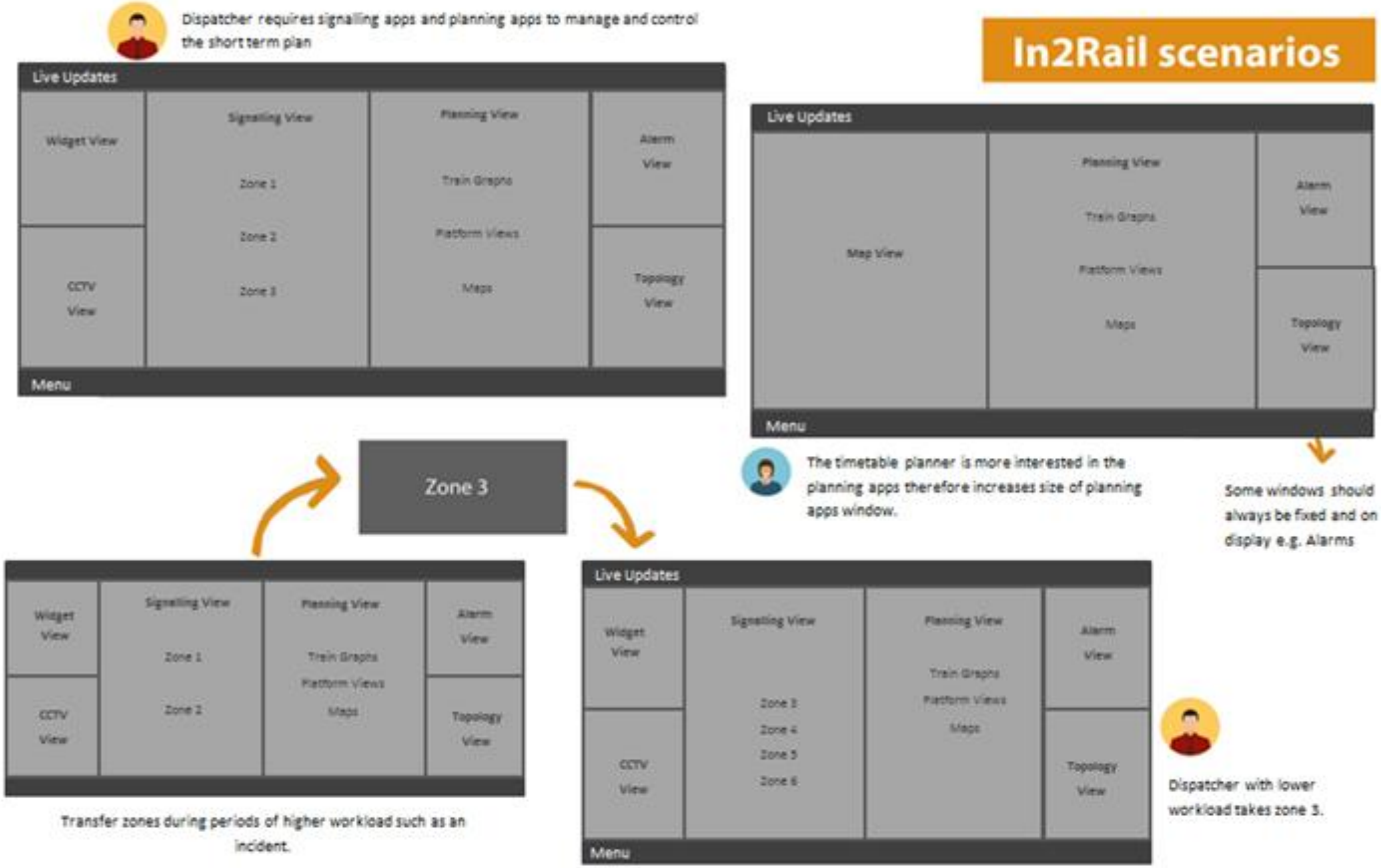
Close-up

Alarms view	Map view / Topology view		Detailed view
	Assets view	Logistics view	Actions view /Settings view

Rationale: The left part of the screen provides the Alarms view which is permanently shown to the maintainer. The upper part of the central display focuses on the geographical information (map and topology view). The lower part of the central display contains the bespoke views for the maintainer (Assets view and Logistics view). On the right side, the detailed view and the actions view are updated automatically depending on the element selected by the dispatcher in the other views. Moreover Actions view panel can be used for displaying the Settings view.

4.10.6 Scenarios

Figure 4.45 and Figure 4.46 on the following pages build upon sections 4.10.1 - 4.10.3 but describe how the overview screen could be used by different roles during certain scenarios.



In2Rail scenarios

Dispatcher requires signalling apps and planning apps to manage and control the short term plan

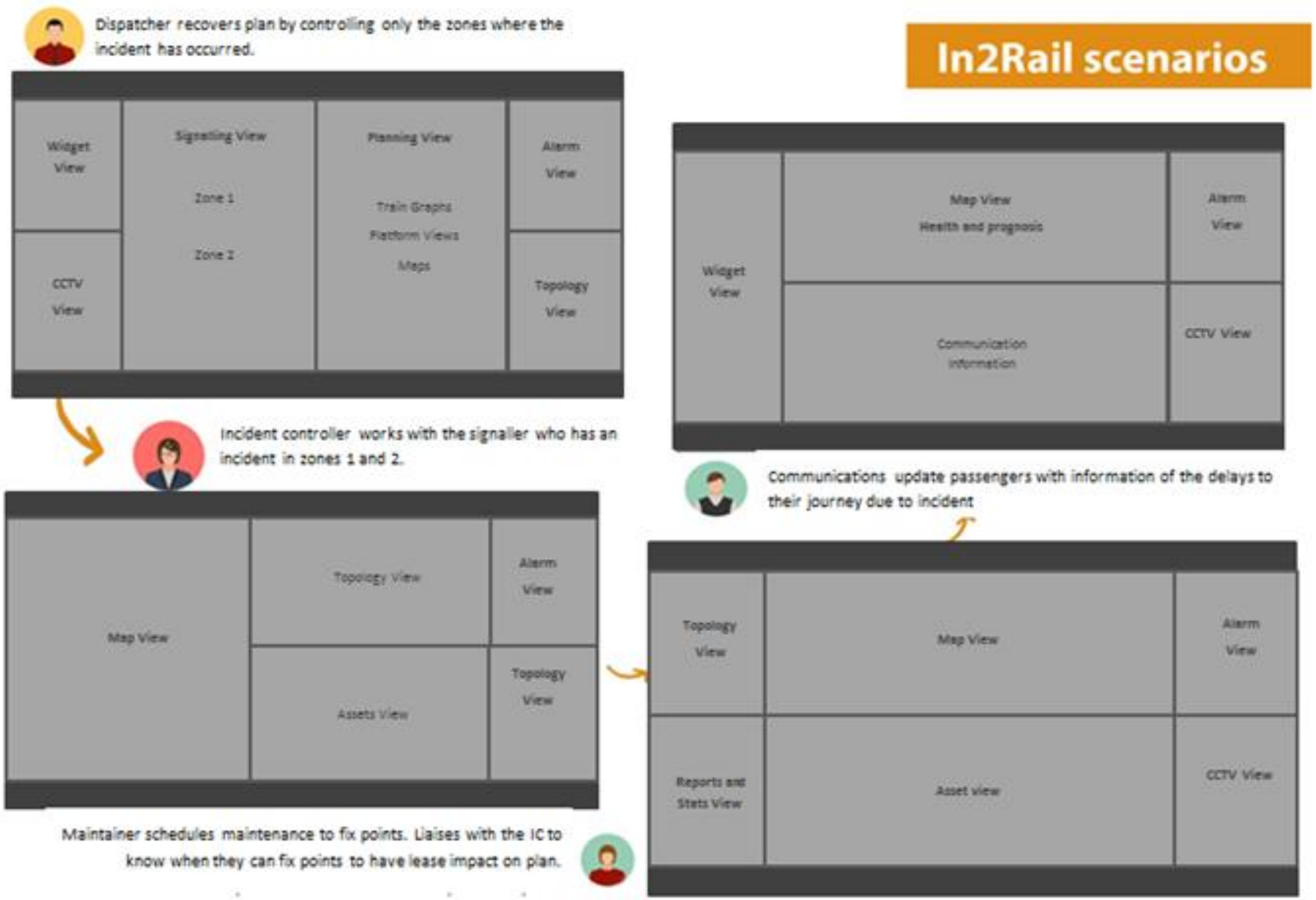
The timetable planner is more interested in the planning apps therefore increases size of planning apps window.

Some windows should always be fixed and on display e.g. Alarms

Transfer zones during periods of higher workload such as an incident.

Dispatcher with lower workload takes zone 3.

Figure 4.45: Use case examples for specific user tasks



In2Rail scenarios

Dispatcher recovers plan by controlling only the zones where the incident has occurred.

Incident controller works with the signaller who has an incident in zones 1 and 2.

Maintainer schedules maintenance to fix points. Liaises with the IC to know when they can fix points to have lease impact on plan.

Communications update passengers with information of the delays to their journey due to incident

Figure 4.46: Use case examples for specific user tasks

4.10.7 Traceability from other tasks

The following links to other tasks performed in WP7.2 can be identified.

4.10.7.1 Roles

Roles for Standardized Operator's Workstation were defined in Subtask 7.2 in Section 4.3 in this report. The following assignment of standard views to generic roles is proposed:

Role	Views
Dispatcher	Widget view Map view Topology view CCTV view Alarms and events view Planning view Settings view Actions view Detailed view
Supervisor	Widget view Map view Topology view CCTV view Alarms and events view Planning view Settings view Actions view Detailed view Assets view Reports and stats view Customer information view
Timetable Planner	Widget view Map view Topology view CCTV view Alarms and events view Planning View Settings view Actions view Detailed view
Incident coordinator	Widget view Map view Topology view CCTV view Alarms and events view Planning View Settings view Actions view Detailed view
Customer Information	Widget view Map view CCTV view Alarms and events view Settings view

Role	Views
	Actions view Detailed view Customer information view
Maintainer	Widget view Map view CCTV view Alarms and events view Settings view Actions view Detailed view Assets view Logistics view Reports and stats view

Please note that role “Administrator” is not considered in the table above, given that the functions realised by such roles are included in the Supervisor’s functions.

4.10.7.2 Uses cases

Use Cases for Standardized Operator’s Workstation were also defined in Subtask 7.2.1. Further analysis of use cases and roles involved may help to optimize the standard layout definition as proposed in section 4.3.3.

4.10.7.3 IT Security

IT Security specifications applicable to Standardized Operator’s Workstation are defined in section 5, Specification of Security Measures.

Device providing automated biometric identification are proposed as login-logoff devices of the standardized Workstation. In this case the use of state-of-the-art technology can help to improve the security levels required for the future TMS.

4.10.8 Further Development

In order to ensure the concepts discussed in this report, both workstation design in section 4.6 and the application HMI design in this section, continue to develop in maturity and follow the user centred design process, the following steps are recommended to be taken:

- Build low fidelity mock ups of each concept; (Workstation and HMI);
- Review mock ups using the In2Rail use cases in Task 7.2.1 with end users or subject matter experts;
- Use feedback from mock up review to identify areas of improvements, ensure concepts meet the user needs, or determine where further development is required in order to ensure technological readiness,
- Operating companies and specific TM Deployments select a concept suitable to their specific project and further refine the design based on those projects individual needs or user needs.

5 Specification of Security Measures

This section describes the following elements of information security:

- A review of key principles relating to Information Security Management Systems (ISMS);
- A design of an Information Security Management System for Traffic Management Systems.

The security measures will refer to current best practice for security measures, taking lessons learned from existing research and rail industry knowledge in this topic.

It should be noted that in the design of the ISMS, the following security measures will not be included as they are part of the wider organisational security model:

- Physical security of locations – such as buildings, operational control centres, IT server rooms;
- Environment security – such as electrical power, heating ventilation and air conditioning, water, lighting;
- Human resources security – beyond the HMI considerations of human factors when working at the operator workstation;
- Business continuity management – beyond that required to assure that a particular operator workstation is the active control point for a section of the operational rail service.

5.1 Information Security Management Systems

5.1.1 Introduction

Whenever we talk about security we think of the idea of protecting something however security is more complex than this. Security is the state of being free from danger or threat. There are many types of attacks that make a system insecure and at a very high level these types can be categorised as physical and logical attacks:

- Physical attacks: are those that involve producing an injury to a building or facility;
- Logical attacks: are those produced to a system or to the information managed.

Both types of attacks have a negative impact on the service provided. Initially, it may seem that physical attacks have a greater effect than logical attacks but it has been shown that the impact of logical attacks can cause the collapse of an entire service.

Physical attacks are more targeted while logical attacks are intended to have an impact on the entire operation. For the railway operation the attack to a powered substation can close a section of the rail network but the attack over a part of the centralized control system or the information that is managed can produce the collapse of the entire network.

Due to an increase in digital and software based technology and the centralization of systems it has increased the motives of attackers. This is due to the consequence of being able to manage many trains and the impact of an attack is much higher than in the past.

Therefore one of the major objectives to be achieved in the transport sector is making management systems more secure and in particular ensure that the information they manage has an adequate level of security that does not limit their application.

This section of the report addresses the risks of logical attacks to the systems in a TM system and mechanisms and methodology to identify these risks and ensure the ability to mitigate them. It should be noted that physical attacks are not part of the scope of this document.

When introducing the general concept of security, it is important to consider the following questions:

- What is a threat?
- Who is involved in a threat?
- What is the motivation to attack a system?
- How do we mitigate threats?

Responses to the above questions and a detailed explanation of general key principles of security can be found in the security appendix.

There are also number of guidelines and standards that are useful to reference when understanding general security issues. Descriptions of some of these guidelines can be found in the security appendix.

5.1.2 Overview of Information Security Management Systems

Information is an asset that has value to an organization and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of increasing interconnectivity, information is now exposed to a growing number and wider variety of threats and vulnerabilities. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form information takes, or means by which it is shared or stored, it should always be appropriately protected. Information security management systems is the method or mechanism to protect the information from a wide range of threats to ensure business continuity, minimize business risk and maximize return on investment and trade opportunities. Information security management systems are achieved by implementing a suitable set of controls; including policies, processes, procedures, organizational structures, and software and hardware functions.

Information and processes are important business assets. Defining, achieving, maintaining and improving information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance and commercial image. Organizations and their information systems and networks face security threats from a wide range of sources; including computer fraud, espionage, sabotage and vandalism. The causes of damage of malicious code, computer hacking or denial of service attacks are becoming more common, more ambitious and increasingly sophisticated. The information security is important to both business and private sectors of the public, and to protect critical infrastructure. The interconnection of public and private networks and sharing of information sources increases the difficulty of achieving access control. The trend to distributed computing has also weakened the effectiveness of central and specialized control. Many information systems have not been designed to be safe.

Security can be achieved through technical means however it should also be supported by appropriate management and procedures. Identifying which controls setting requires careful planning and attention to detail. The management of information security requires at least the participation of shareholders, suppliers, third parties, customers, other external groups and of course all internal staff involved in the system.

The current Information Security Management System follows the methodology based on four areas or phases:

- The **Plan** phase is about designing the Information Security Management System, assessing information security risks and selecting appropriate controls;
- The **Protect** phase involves implementing and operating the controls;
- The **Check** phase objective is to review and evaluate the performance (efficiency and effectiveness) of the Information Security Management System;
- In the **Act** phase, changes are made where necessary to bring the Information Security Management System back to peak performance

These four areas have a continuous execution because the security task has to be continuous cycle of evolution.

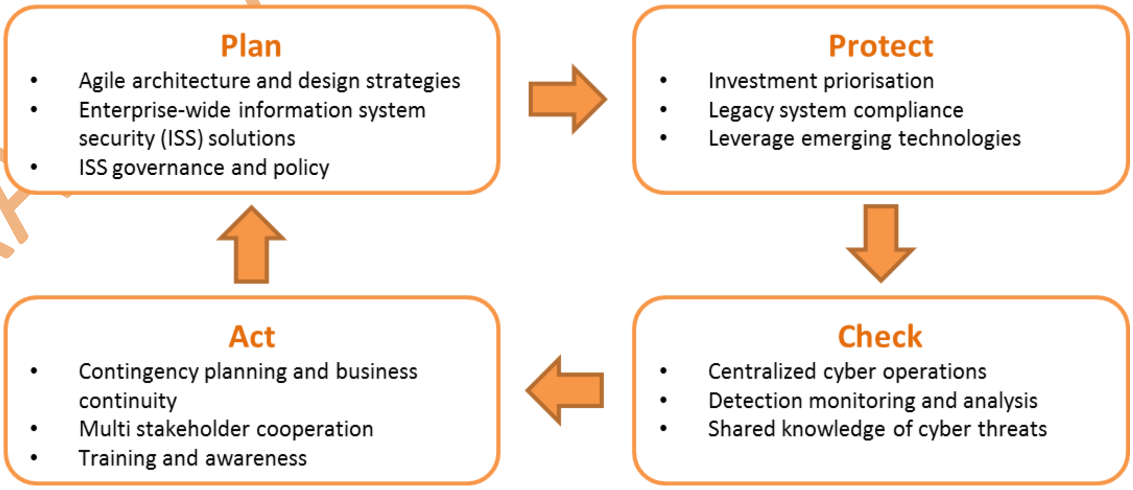

Plan
Agile architecture and design strategies
Enterprise-wide information system security (ISS) solutions
ISS governance and policy
Protect
Investment priorisation
Legacy system compliance
Leverage emerging technologies
Check
Centralized cyber operations
Detection monitoring and analysis
Shared knowledge of cyber threats
Act
Contingency planning and business continuity
Multi stakeholder cooperation
Training and awareness

Figure 5.1: Four Phases of ISMS

The **Plan** quadrant includes the creation of design strategies and an enterprise-wide or overall system-of-systems architecture that enhances security, provides agility, and reduces overall costs. To effectively implement the architecture, organisations must develop policy and fund security solutions throughout the enterprise with total management commitment.

The **Protect** quadrant includes prioritising information security investments in both new and legacy systems. Protection techniques must be agile; that is, they must be able to quickly change and adapt to an ever-changing threat. This requires the organisation to leverage emerging technologies and implement them at an enterprise-wide level. While some aspects of security must be built into individual systems, enterprise solutions can be shared throughout an organisation and are a key underlying element of an effective architecture. Enterprise security solutions reduce overall costs and, just as importantly, make it possible for new and evolving threats to be addressed centrally rather than having to introduce new measures into every part of the system. The success of any information technology security programme is, in part, dependent on the ability to detect and respond to a cyber-security event.

Protecting the integrity and availability of our information will help to ensure that the correct information is available to staff and customers at the time they require it. Confidentiality allows us to control the flow of information into the public domain so to not disappoint or confuse stakeholders by accidentally leaking immature information at inappropriate moments.

Typical information assurance requirements have to take into account:

- **Confidentiality:** the assurance that information is not disclosed to unauthorised persons, processes, or devices. It includes both the protection of operational information and the information assurance of password or configuration files.
- **Integrity:** assures that information is not modified by unauthorised entities or through unauthorised processes. Integrity supports the assurance that information is not accidentally or maliciously manipulated, altered, or corrupted. Integrity also means that detection occurs with no or minimal false alarms when information has been altered; the alteration source must be identifiable.
- **Availability:** assures timely, reliable, continued access to data and information systems by authorised users. Availability controls protect against degraded capabilities and denial of service conditions.
- **Authentication:** assurance of the identity of message senders and receivers. Authentication supports the validation of messages and information system requests.
- **Authorisation:** the verifiable identity of each entity handling any asset must be checked to possess appropriate permission and privilege.

- **Non-repudiation:** assurance that the data sender is provided with proof of delivery, and the recipient is provided with proof of the sender's identity, assuring that sender and receiver processing of the data.
- **Traceability:** all actions performed on each asset must be logged in a format and for a time period that can satisfy both regulatory and consumer needs.

The need for the next two quadrants – **Check and Act**– reflects the unfortunate reality that no matter how much planning and protection is put in place, failures will occur and determined attackers will gain access to protected systems. This fact does not minimise the need for good architecture design and investment, both of which reduce the susceptibility to compromise. Adequate intrusion-detection capability is required to monitor and detect potential cyber security incidents. Detection requires a centralised cyber security operations centre staffed by experts with up-to-date knowledge of the evolving cyber threat. This cyber security operations centre must be supported by analysis tools fed by intrusion monitoring sensors installed throughout the enterprise, which provide the ability to detect when an organisation's information system has been compromised.

The **Act** quadrant includes contingency planning, procedures, and training and awareness, which allow an organisation to quickly and effectively respond to a compromise and minimise the possible impact on mission operations. Cyber security content is almost non-existent in the curriculum of current training programmes, and what might be needed in regards to cyber security knowledge, skills, and abilities of engineers, technicians, and other staffs needs to be identified. The combination of detection and response provide the organisation with an ability to know when cyber compromise is a problem, and assist the organisation in executing cyber procedures to ensure the operational mission is fulfilled throughout an attack. On the other hand, the "response" action also requires an appropriate evaluation of lessons learned to prevent any re-occurrence and thus promote a cycle of continuous improvement through each of the four quadrants.

There are lots of types of enterprises that use Information Security Management Systems to improve the quality of their processes or systems. In particular, systems that control critical infrastructures such as Air Traffic Management Systems follow their own ISMS to take into account the potential attacks they can suffer.

However historically, train traffic management systems have previously not been typical consumers or users of ISMS compared to the aviation industry. Although the rail industry has been previously more focused on physical attacks than logical attacks, it is expected over the next few years that the importance of information security in train TM systems will increase.

5.1.3 Information Security in the Context of Traffic Management Systems

Traffic management systems, regardless of the type of transport, are becoming more complex and more dependent on computer systems that allow the automation of tasks to enable a better quality of service.

Specifically within the railway management, evolution has allowed the increase of the offer provided to end customers and has also allowed more efficient use of the infrastructure required for this type of transport. This development is not only technological but also operational, from a more distributed operation along the entire rail network to a centralized management and lately a hierarchical management. These changes in railway management result in the principle that the railway is managed from control centres through complex computer systems that make it possible to monitor, control and manage efficiently many kilometres of network by a small number of operators.

Unfortunately, this evolution involves a number of risks and the systems that manage the railway are becoming more vulnerable. Therefore it is essential to ensure that TM systems take into account the need to improve information security.

The following summarises where there is a need to improve the information security of TM systems:

- There is an increase in current trends to share across collaborative systems;
- There is a need to share information to:
  - Encourage the use of intermodal systems,
  - Increase the attractiveness of rail transport,
  - Compete against other modes of transport,
  - Have a modern interconnected system;
- There is an move from information distribution systems based on point to point interfaces to information intelligent distribution systems;
- The information must be reliable and adapted to each recipient;
- It is mandatory to provide quality information, coherent information, compressible information and consistent information;
- The system cannot distribute conflicting information to different stakeholders;
- The system cannot distribute conflicting information through different delivery mechanisms;
- It is necessary to filter information for each stakeholder;
- It is necessary to provide the appropriate level of detail for each stakeholder;
- Information consumers require much more information and there are many more ways to distribute this information. A few years passengers only had information systems at stations to access real time information about the state of the railway but now passengers can access information through the internet and using mobile applications;

- Given the growing increase in the exchange of information between different systems, it is necessary to have a security feature to assure a safe exchange of information. The main aim of these security features is to ensure the control of the managed information and ensure that information exchanged is correct and it has not been distorted.

5.2 Information Security Management Systems for Traffic Management Systems

5.2.1 Objective

Information is the most important element of an organization, which is the reason why it is necessary to protect. The protection mechanism must provide a high level of confidentiality without interfering with the access of the authorized actors involved in the system. This balance is achieved through analysis phases of the system itself and the environment.

Information security is the protection of information from a wide range of threats to ensure business continuity, minimize business risk and maximize return on investment and trade opportunities.

The main aim of an Information Security Management System (ISMS) is to provide mechanisms, processes and methodologies to be implemented at an organization to eliminate or minimize the probability of suffer an attack, the successful of this attack and the impact of a success attack.

All the security measures proposed by an ISMS are intended for preserve the integrity and the confidentiality of the data managed by the organization and maintain the availability of the service provides by the organization.

An ISMS should not only be taken into account during the design of the system bu the following must also be taken into account within an organization:

- Security depends on people more than on technology;
- Employees are a far greater threat to information security than outsiders;
- Security is like a chain. It is as strong as its weakest link;
- The degree of security depends on three factors: the risk you are willing to take, the functionality of the system and the costs you are prepared to pay;
- Security is not a status or a snapshot but a running process.

An ISMS must provide a pattern of work of all the actors that interact with the system, developing policies and procedures, performing security reviews and analysing risk, addressing contingency planning and promoting security awareness.

The following sections describe a specific modification of a traditional ISMS in the context of railway infrastructure. This specialization of a ISMS is the Railway Information Security Management Systems (RISMS).

This RISMS propose a methodology, process and tasks that are adapted to the systems that control a railway infrastructure in order to reduce the probability of an attack and the impact of a successful attack to the information that is managed.

The RISMS proposed can be implemented in future Traffic Management Systems or in existing legacy systems. The systems deployed several years ago typically didn't have security measures because at the time they were deployed the risks and the attacks were very different and the inter-connexion of the control centre was limited. The RISMS aim to provide general methodologies that can be applied for all the Traffic Management Systems deployed for the control of the railway infrastructure.

5.2.2 Railway Information Security Management System

The Railway Information Security Management System (RISMS) is based on the traditional ISMS used by the industry and on the ISO/IEC 27001:2005, but aims to highlight some specifics in relation to Traffic Management Systems.

The following elements should be considered in RISMS:

- **Flexible:** Provide a framework that can be adapted to the continuous change of the systems;
- **Centralized:** The management of the RISMS has to be in a central model to insure a level of coherence;
- **Distributed:** The RISMS must be adopted by all the organizational levels of the TMS;
- Important for the responsible supplier of the TMS: The control and the evolution of the RISMS must be one of the objectives of the suppliers responsible for TMS;
- **Continuous:** The RISMS life cycle must be executed without disruption to be able to adapt it to the possible new risks;
- **Selective:** The effort must be centred around the main tasks and at the main risk points identified;
- **Continuous evolution:** Must provide mechanisms to assure appropriate training of staff providing different safety polices.

The proposed life cycle at the ISO/IEC 27001:2005 is based on the Deming cycle and divides the ISMS actions into four main processes:

- **Plan:** This phase has all the tasks related to the design of the ISMS;
- **Do:** This phase contains the implementing and operating controls task;
- **Check:** The objective of this phase is the evaluation of the ISMS performance;
- **Act:** This phase has the tasks to ensure that the ISMS is in continuous evolution and is flexible to adapted to the continuous evolution of the environment.

Based on this life cycle phase and taken into account the particularities of a railway TMS, the RISMS has the following breakdown of processes:

- **Identify:** The main aim of this phase is detect the most exposed part of the TMS that has to be protected to assure the correct system execution;
- **Assess:** This phase has to assess the risk of possible threats at the exposed parts identified at the previous phase;
- **Strategy:** The main aim of this phase is to apply mechanisms to mitigate the risk detected at the previous phase;
- **React:** This phase has the tasks related about who and what to do when an attack is on-going;
- **Learn:** This phase has the learning tasks to improve the RISMS.

Figure 5.2 represents the global process of the RISMS that is divided on two phases.

- **Preparation phase:** This phase covers all the RISMS activities to prepare the TMS in order to provide more level of security;
- **Execution phase:** This phase covers all the RISMS activities when an attack is produced over the TMS.

The first phase has to be executed periodically to be able to assure that the system is analysed continually to provide a high level of security.

The execution phase is triggered when an attack is produced over the TMS and at the end of this phase the RISMS is prepared to execute a new cycle of the preparation phase in order to take into account the new scenario after the attack.

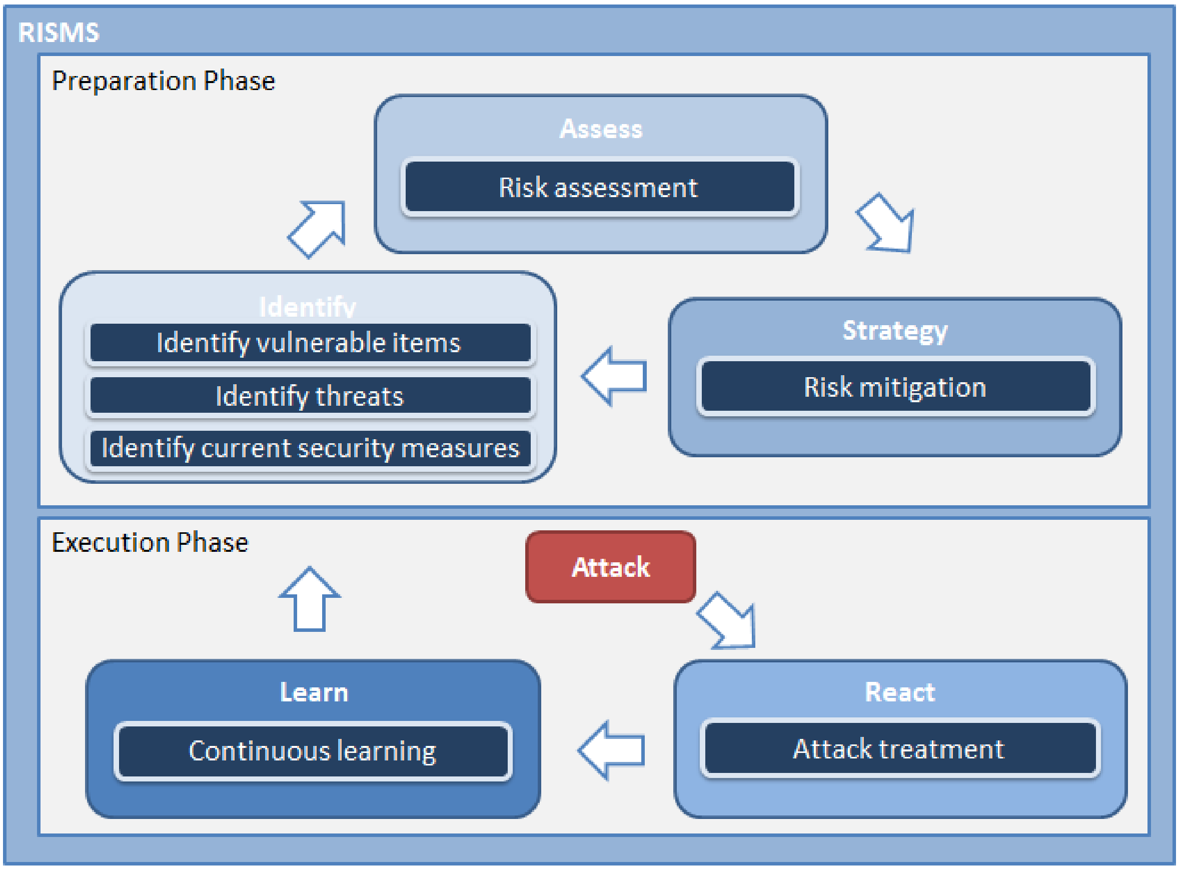


Figure 5.2: Railway Information Security Management System

Each process (identify, assess, strategy, react and learn) has several activities that have to be executed sequentially in order to follow the RISMS methodology.

The following chapters explain each process with all the activities that are necessary to produce the expected results.

5.2.2.1 Preparation phase

This phase of the RISMS contains all the necessary processes to prepare and adapt the system to control and manage the risk associated to the system.

This phase includes the processes of identify, assess and strategy that are processes that must be executed before the system has an attack.

These three processes must be executed periodically to try to refine all the security aspects of the system independently if the system suffer or not attacks.

5.2.2.1.1 Identify

The desired result at the "identify" process of the RISMS are the following lists:

- List of TMS vulnerable items;
- List of threats that can provoke an attack over the TMS;
- List of current security measures.

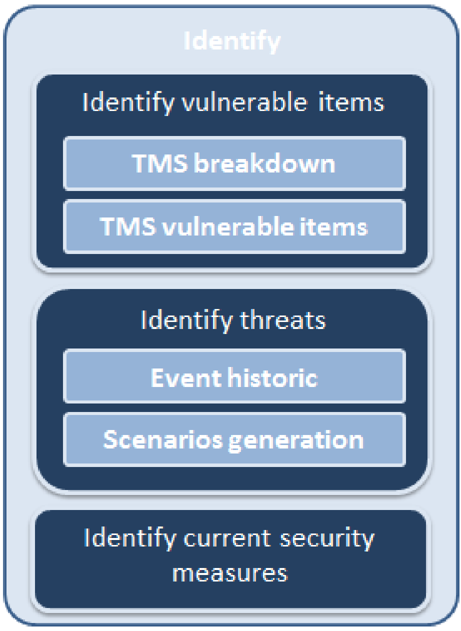


Figure 5.3: Process of Identify

5.2.2.1.1.1 Identify vulnerable items methodology

The identification of potential vulnerable items of a TMS is one of the most important phase of the RISMS process. Over the TMS parts detected at this phase is based all the next processes of the RISMS.

The methodology to identify the vulnerable items of a TMS is based on two sequential steps:

- **Identification of TMS parts:** The main aim of this subtask of the process is identify the different parts of the systems. Then the result of this subtask is a breakdown of the TMS based on several rules;
- **Assess the vulnerability of TMS parts:** This subtask has the assess process to detent which parts of the TMS are vulnerable and have to be taken into account along the execution of the RISMS.

5.2.2.1.1.2 Methodology to make the TMS breakdown

The aim of this subtask is to provide a methodology or rules to be able to make an effective breakdown of the TMS parts to be used by following process of the RISMS.

The breakdown result of this methodology must be based on these ideas:

- The different parts of the TMS identified must have a similar importance. This homogeneous division is important to be able to determine the minimal unit to be taken into account along the entire process;
- Each part identified must attend to an atomic function inside the TMS but it does not necessarily need to be a full functionality of the system;
- Each part must provide a logical function inside the TMS;

- The function provided by each part must be unique inside the TMS. If two parts have the same functions they must be identified at this breakdown level as one, although these parts are used by other different parts of the TMS. At the end of the process the breakdown must provide a set of different modules or functional parts not necessarily linked to the low level of implementation of the TMS;
- A good practice to make this breakdown is to divide process modules of the TMS, interfaces between internal modules and interfaces between internal modules and external modules or systems.

The difficulty of this breakdown, and one of the main objectives of this subtask, is to divide the system into parts of the same entity. An excessive breakdown leads to inefficiency in the following subtask and processes of the RISMS. This is because the following analysis of the vulnerability of these parts will have a higher cost, and a breakdown of a high level (few parts identified). Therefore the action that will be proposed to mitigate the risk at the next steps of the RISMS will need more effort and will not be efficient.

The breakdown task is a very subjective task, depending the actor that makes this functional modules division the result may be very different. The start point, the experience and the knowledge of the system involved are the main factors that produce a different result. Therefore the most appropriate techniques to do this breakdown are based on a group of experts.

To identify the TMS parts there are several techniques that can be used:

- **Brainstorming:** The definition is, “a method of shared problem solving in which all members of a group spontaneously contribute ideas”.
  - There is a need to involve a group of experts with high functional knowledge of the system (TMS). They must talk about their ideas of a correct breakdown and must produce the definitive modules division of the TMS.
- **Delphi technique:** The definition is, “A systematic forecasting method that involves structured interaction among a group of experts on a subject”.
  - The Delphi Technique typically includes at least two rounds of experts answering questions and giving justification for their answers, providing the opportunity between rounds for changes and revisions. The multiple rounds, which are stopped after a pre-defined criterion is reached, enable the group of experts to arrive at a consensus forecast on the subject being discussed.

These two techniques must take into account these guidelines:

- A good **selection of the experts** is necessary. All experts must know in deep the functional characteristics of the system;
- **Correct level of breakdown:** The expert group must take into account the main objective of the breakdown. It is common for experts to produce a very detailed breakdown but this is a very common error and it is important that the result of this

process is a high-medium level of breakdown of the system. This is because a high-medium breakdown is the most appropriate level to be effective in the next steps;

- **Identify main global functionalities:** The experts must identify the main functionalities of the system in order to try to divide the processes that the system makes to execute them. The processes identified will be part of the breakdown.

The result of this TMS breakdown has to be:

- The different functional modules that compound the full TMS solution;
- Identification of these modules;
- Characteristics of these modules, identifying if they are internal or have communications with the external systems;
- A short functional description of each module identified;
- Identification of the connection between these modules;
- Characteristics of the connection with other internal or external modules/systems. The communication method, protocols, information exchange, the actors involved at this communication, the access method to these modules and any other communication characteristics that may be taken into account in order to determine the vulnerability of the module.

This breakdown information must model the complete TMS functionality and will be used during the next RISMS steps.

Methodology to identify the TMS vulnerable item:

The process of the RISMS must use the modules or the different parts of the TMS to identify which ones have characteristics that require a special treatment and are more vulnerable. At this phase it is not important to identify the level of an impact or the probability of a potential attack. The methodology must provide a method to identify all vulnerable parts independently of the impact level.

The methodology is based on an evaluation process for each module or part identified as part of the TMS.

There are two different types of TMS parts, internal and external.

- The internal modules have communication with other TMS modules but they don't have communication with other systems and they don't exchange of information with TMS staff or with external staff;
- The external modules have communication with different actors, like external systems or TMS internal or external staff.

The analysis phase of each module includes the evaluation of several different specific aspects by this modules classification.

For each internal module it is necessary to assess:

- The protocol used to the exchange of information:
  - Protocol type: Commercial or standard protocol or Specific or ad-hoc protocol,
  - Safety characteristics;
- Connection characteristics:
  - Direct connection between TMS modules,
  - Known connection net,
  - Unknown connection net.

For each external module is necessary to assess:

- The type of actor involved:
  - System:
    - Known and authorized system, the systems that can access the TMS must be authorized by an administrational procedure previously to the first connection. The connection time, the period of the connection or the simultaneous access must be limited by a contractual document,
    - Unknown system, there may be external systems connecting to the TMS but they are not known previously. For example, the TMS can provide external modules to allow the connection of external systems to get the train running information in real time;
  - Staff:
    - TMS staff, the actors that connect to the module are known because are part of the TMS staff. This staff must be considered as internal staff as part of the TMS,
    - Known external staff, it is a possible scenario when the actors that exchange information or interact with the module are not part of the TMS staff. This staff is known because are part of the staff of other organization or other external system that has an authorized access,
    - Unknown personnel, it happens when the entity, actor or personnel that access to the TMS is an unknown external entity from the point of view that the people that need for example get a TMS information can access to it but this entities are unknown;
- The protocol used to the exchange of information:
  - Protocol type: commercial or standard protocol or specific or ad-hoc protocol;
  - Safety characteristics;
- Connection characteristics:
  - Direct connection between TMS module and external module;
  - Known connection net;
  - Unknown connection net.

All of the above points must be assessed for each identified modules to provide a value for each module.

The methodology provides a threshold to particularize the vulnerability grade. All modules that have an evaluation upper to the threshold established will be classified as vulnerable modules and will be used at the next steps of the RISMS.

The next table shows the questions and the possible responses used to classify each TMS module. The grey boxes are used to insert the value of each response by the TMS expert staff.

For internal modules			
What is the type of protocol?	Commercial or standard protocol	Specific or ad-hoc protocol	
The protocol used has security characteristics?	Yes	No	
What are the connection characteristics?	Direct Link	Known net	Unknown net
For external modules			
The connection is with known external system?	Yes	No	
The connection is with unknown external system?	Yes	No	
The connection is with TMS internal staff?	Yes	No	
The connection is with known external staff?	Yes	No	
The connection is with unknown external staff?	Yes	No	
What is the type of protocol?	Commercial or standard protocol	Specific or ad-hoc protocol	
The protocol used has security characteristics?	Yes	No	
What are the connection characteristics?	Direct link	Known net	Unknown net

Table 5.1: Form to identify the TMS vulnerable items

When all TMS internal modules are assessed with this form it is necessary to order them from the maximum value to the minimum to identify which ones are over the threshold imposed.

5.2.2.1.1.3 Identify threats methodology

Identify threats is a very difficult task because the actors involved at this phase determine on internal and external issues. It is very important to have a deep knowledge of the TMS and a good knowledge of the external environment to try to find the most possible attacks that can be executed over the TMS.

This process has to be systematic and comprehensive enough to ensure that no threats are unwittingly excluded. Identifying threats to information security is performed based on the analysis of external and internal sources of risk taking into account the historical, political and social context of where the analysed system is. Therefore the threats that a traffic control system has, can be very dependent on where it is providing the service.

There are a lot of classifications of threats taking into account several characteristics:

- **By the origin:**
  - Internal TMS staff. The attacks produced by internal staff have a low probability but the impact of attacks produced by them can be high because they have

knowledge to produce the attack and the probability of a successful attack is higher,

- External person. The attacks produced by these external actors have allowed success probability but there are a lot of attacks produced by this kind of actors. The most common motivation to produce these attacks is only to achieve a success attack,
- External organization. When an actor like that produce an attack the success of probability is higher than in previous attackers because they have a deep knowledge of the system and they have a high level of motivation for a success attack;

- **By the activity** that produces it, like an unauthorized dissemination of confidential data, competitor deploys a new marketing policy, new or revised data protection regulations, an extensive power failure, etc;
- **By the consequences**, results or impact like a service disruption (partial or complete), delay at the trains, service unavailability and loss of confidence in the railway operator or in the infrastructure manager company;
- **By a specific reason** of the occurrence like system design error, human intervention;
- **By protective mechanisms** and controls like access control and detection systems, policies, security training;
- **By the time and place of occurrence**, like during extreme environmental conditions there is a flood in the computer room.

There are two big groups of threats, physical and logical, however this document only considers the logical threads. The logical threats can be classified at:

- **Cybercrime:** A cybercrime is a cyber-attack to a computer, to the information managed by a computerised system or to a complete computerised system, convenient, anonymous, quick, diverse, and relatively low-risk and with low impact;
- **Cyber terrorism:** A cyber-attack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or intimidate a society into an ideological goal (NATO). A cyber terrorism is a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies. (US National Infrastructure Protection Centre);
- **Industrial espionage:** It is the action of collecting information illegally (intrusion, security, theft) about competitors or potential customers. The main target is only the information, not to produce a problem to the service provided by the system.

The most frequently tools used at the logical threats are:

- **Viruses:** is a computer program usually hidden within another seemingly innocuous program that produces copies of it and inserts them into other programs or files, and that usually performs a malicious action.
- **Trojan horses:** is any program that invites the user to run it, concealing harmful or malicious executable code of any description. The code may take effect immediately

and can lead to many undesirable effects. In the case of some spyware, adware, etc. the supplier may require the user to acknowledge or accept its installation, describing its behaviour in loose terms that may easily be misunderstood or ignored, with the intention of deceiving the user into installing it without the supplier technically in breach of the law.

- **Rootkits:** is a collection of computer software, designed to enable access to a computer or areas of its software that would not otherwise be allowed.
- **Backdoors:** is a method of bypassing normal authentication procedures, usually over a connection to a network such as the Internet. Once a system has been compromised, one or more backdoors may be installed in order to allow access in the future, invisibly to the user.

There are several good practices to find possible threats:

- Good quality information and thorough knowledge of the organization and its internal and external environment are very important in identifying risks. Historical information about this or similar organizations (competitors or not) may also prove very useful as they can lead to safe predictions about current and evolving issues that have not yet been faced by the organization;
- It is necessary to have a deep knowledge of the system and the most common attacks produced in the past in similar systems.

Methods and tools used to identify threats and their occurrence include checklists, judgments based on experience and records, flow charts, brainstorming, systems analysis, scenario analysis and systems engineering techniques.

For the RISMS we consider that the most appropriate techniques are:

- **Event historic:** used when we have a lot of information about threats of similar systems;
- **Scenarios generation:** used for analysis of possible situations when it is not clear the possible threats.

All these techniques must be executed by expert staff in order to ensure that all aspects of the TMS have been taken into account.

Each identified threat must be classified as one of the following categories:

- **Integrity:** when the threat can affect to the correct execution of the system (performance, functionality, operations);
- **Audit operations:** when the threat can affect to the register of the managed information;
- **Authentication:** when the threat can affect to the system access;
- **Authorization:** when the threat can affect to the privileges management.

Event historic

This technique is based on the analysis of one big data source of historical attacks produced against other rail traffic management systems or similar systems that controls other infrastructures.

This historical data can have multiple internal or external factors to the organization sources but all the information should be standardized and centralized in order to use it efficiently.

To achieve this objective it is necessary to recover a lot of information of each attack. This is a complex task because it is difficult to have access to the right information because it is often classified information for a lot of agencies and when the information is accessible it can be incomplete or inexact.

The information that has to be recovered for each attack is at least the following:

- Date and time;
- Any special aspect of the day and time that is produced the attack, for example when the attack is produced at the time that there is a planned maintenance of the system;
- Attacker agency/person/group, in some cases it is difficult to obtain;
- The reason, it is important to try to understand which the attacker motivation is. This information will be used to try to make a mitigation plan to this kind of attacks;
- The objective, this is the attack aim. It is important to register the item, module or functionality of the system that is attacked;
- The consequences, (if an attack is successful);
- The reaction to the attack, the actions that were made to mitigate the impact of the attack;
- The corrective actions, that have been implemented to the system in order to improve the security level and prevent other similar attacks.

The sources to collect these attacks are:

- Internal infrastructure manager departments;
- Specific infrastructure manager departments involved at safety issues;
- Public entities that are involved at the management of critical systems as:
  - National Centre for Critical Infrastructure (CNPIC - Centro Nacional de Infraestructuras Críticas),
  - ENISA - European Network and Information Security Agency,
  - Federal Office for Information Security (BSI - Bundesamt für Sicherheit in der Informationstechnik),
  - CPNI - Centre for the Protection of National Infrastructure,
  - NATO Agency Cyber Security.

Scenarios generation

This technique is based on creating possible situations/scenarios where a potential attacker can have to try to attack to the system.

In each scenario the security analyst must try to take the place of each one of the attackers identified in previous steps to try to imagine what actions take place to make a successful attack the system.

These scenarios must be designed by experts of the TMS in order to take the place of an expert attacker but the attacks used at each scenario must cover all the possibilities that the security analyst can imagine because a minor attack and a big one can produce serious impacts in the system if it is not designed to prevent them.

When the security analyst has the scenarios designed it the time to evaluate which are the system items that needs to implement safety measures to try to prevent similar attacks. The design of the measures is a very important process because it has to take into account all aspects in order to prevent the system from attack.

5.2.2.1.1.4 Identify current security measures

The main aim of this process is to identify the security measures that the TMS has developed. It is very important to identify these security measures because it is necessary to take it into account to be able to evaluate the risk associated.

In the In2Rail project there is a document about data management that defines the basic security measures that the system must provide.

The TMS must follow the best practices described at the "In2Rail Data Management Plan" document.

There are two kind of security measures, this type must be identified to each implemented security measures:

- **Deterrents measures:** to show the attackers show there is low probability they will be able to attack. Therefore attackers will think before making the attack;
- **Blocking measures:** to block and attack so that is does not succeed.

The expert team that is evaluating the security measures of the TMS must provide a list of these measures classified providing the following information of each one:

- Measure name: Arbitrary name to identify it;
- Measure description: Description of the measure implemented;
- Measure reason: Main reasons to implement this measure;
- Aim of the measure: The mechanism used to react to a threat;
- TMS item that protect: The TMS parts where this measure is implemented;
- Potential attacks where it is effective: The list of attacks where this security measure works effectively.

The main tool to provide this list of security measures is the brainstorming composed by TMS experts involved at TMS security issues.

5.2.2.1.2 Assess

The desired result at the "assess" process of the system are the list of items that must be treated to be able to reduce the risk identified.

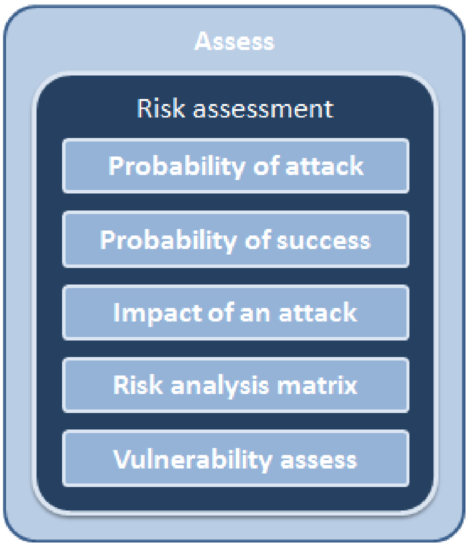


Figure 5.4: Process of Assess

5.2.2.1.2.1 Risk assessment methodology

The main aim of this phase is obtain the risk level to each vulnerable part or module of the TMS.

It is very important that as a result of this phase all current risks are identified and recorded but always thinking that there will be unknown risks at the analysis time. These unknown risks will be included at next iteration of the RISMS.

It should be noted that it is difficult to make a 100% secure system because the threats are not finite and they may appear new threats continuously.

The result of this risk assessment determines where to focus efforts to make the analysed system safer. Risk mitigation requires effort, time, resources and thus money. These needs are not unlimited thus is necessary to identify a line in order to establish the threshold at which you can decide what parts of the system must be treated to reduce or eliminate the measured risk.

The risk assessment has to be implemented as part of the RISMS loop to be sure that the continuous new threats are evaluated at each execution.

The risk can be calculated as a mathematical formula where it is involved three aspects; **probability of attack**, **probability of success** and **impact of an attack**.

Risk = Probability of attack (PA) * Probability of success (PS) * Impact of an attack (IA)

To do this risk assessment the RISMS uses a **risk analysis matrix** in order to have a graphical representation of the risk detected. This matrix will be used to identify the system items that have a high risk and the threats involved at this risk. This information will be used to decide the vulnerable system items and how to implement measures to try to reduce the risk at the system at the **vulnerability assess** process.

Definitions of the elements of risk can be seen below:

- (PA) Probability of attack:

A TMS is a system that has a high level of interest for attackers because the possible impact of an attack to this system is high. A TMS is a centralized point of the control of a very large infrastructure installation. If an attacker can make an attack at a single point of the infrastructure the service provided by the railway enterprise will be reduced at this single point. But if the attack on the TMS is at the centre of the actions, the impact will be global and could cause the entire service to collapse.

The probability of attack represents the probability that someone (person, group, organization) decides to attack a specific target or in this case a part of the TMS (module, functionality, service), using one of the methods presented as threats in the previous process (Identify). The value of an attack can be decreased by introducing disincentives to make the attacker think that the attack will not succeed. These actions are described at the risk mitigation methodology at the strategy process.

- (PS) Probability of success:

This concept is the measure of the vulnerability of the system or part of the system. These measures are used to know if the security measures can avoid an attack.

The main difference between probability of attack and probability of success is that the first one measures the possible attacks and the second one measure the success once an attack is on execution.

- (IA) Impact of an attack

The impact is the measures of the consequences of a successful attack. This measure does not have to consider the previous probabilities.

The impact can be reduced by introducing systems that minimize the consequences of an attack. These measures can be very different to the measures used to mitigate the probability of attack or the success of an attack.

Risk analysis matrix:

A risk assessment in the context of this document is the analysis of the probability of attack, the probability of a successful attack and the level of impact of a threat over a vulnerable TMS item. Then when we have identified the threats that are involved in the TMS it is necessary to assess each one at the vulnerable parts identified at the previous phase of the RISMS. This evaluation must take into account several aspects, probability of occurrence, probability of success and impact of the threat over each vulnerable item of the system.

The tool used at the RISMS to assess the risk is the risk analysis matrix. This tool is an analysis and visual mechanism to be able to assess each threat over each vulnerable item of the TMS.

The matrix has a vulnerable item of the TMS, (identified at previous phases), per each row and a threat identified, (at previous phase), per each column.
The methodology used to assess the risk is divided into three aspects:

- **Probability of an attack (PA):** This parameter represents the probability of an attack of the threat over the vulnerable item. This value represents the interest of an attacker (threat) to attack part of the TMS. It is necessary to take into account all security measures that provide mechanisms to dissuade an attack;
- **Probability of a success attack (PS):** This parameter represents the probability that a real attack has success. This value has to take into account all the measures that the TMS has to block a real attack. These measures are part of the security measures identified at the previous phase as blocked measures;
- **Impact of a success attack (IA):** This parameter represents the impact level that a successful attack can produce to the TMS operation. An example of possible values are:
  - **1:** Complete loss of the system control;
  - **0,9:** Loss of information managed by the system;
  - **(0,9 – 0,5):** Partial loss of the system control (Different values for different parts of the system, automatic operation, manual operation, traffic control operations, management operation, etc.);
  - **(0,7 – 0,3):** Loss of system performance (Different values for different reduction level of performance).

An example of a risk matrix is seen below:

Risk Matrix	**Threat**															
	Threat 1				Threat 2				Threat 3				Threat 4			
Vulnerable item	PA	PS	IA	Risk	PA	PS	IA	Risk	PA	PS	IA	Risk	PA	PS	IA	Risk
Item 1				0				0				0				0
Item 2				0				0				0				0
Item 3				0				0				0				0
Item 4				0				0				0				0
Item 5				0				0				0				0
Item 6				0				0				0				0
Item 7				0				0				0				0
Item 8				0				0				0				0
Item 9				0				0				0				0
Item 10				0				0				0				0

Table 5.2: Example of a risk matrix

This risk matrix must be evaluated by experts on the TMS with a medium/high level of knowledge of the design of the system because is necessary to take into account all the security measures that the TMS implements in order to dissuade potential attacks and mitigate the impact of attacks.

The values for PA, PS and IA are decimal numbers from 0 to 1 and the risk measure has a possible value between this values interval (0-1).

The result of this matrix is the risk value for each row/column but there is not part of this matrix get the conclusion of the risk. Each intolerable risk must then be assessed, see 'vulnerability assessment'.

Vulnerability assessment

This is the process of identifying those risks that are considered intolerable and must be addressed in the strategy phase to reduce them using a number of different techniques.

In order to accomplish this task it is necessary to:

- Establish risk intervals: This allows you to specify ranges of values that are considered low, medium or high risk;
- Set the value of the assumed risk: This value determines the threshold of risk that can be assumed. All calculated risks that are below the threshold value should not be considered as priorities in establishing additional security measures on parts of the system involved and all that have a higher value should be treated.

The ranges of values established for the risk should be coloured in the matrix so that the calculated risks can be displayed graphically according these established risk ranges. Each risk exceeding the determined threshold must be marked so that it is visually identified. The matrix should also always display the specific values of calculated risk.

The following matrix represents an example of a risk matrix with risk values associated for a generic list of items and a generic list of threats.

Risk Matrix	Threat															
	Threat 1				Threat 2				Threat 3				Threat 4			
Vulnerable item	PA	PS	IA	Risk	PA	PS	IA	Risk	PA	PS	IA	Risk	PA	PS	IA	Risk
Item 1	0,2	0,5	0,1	0,01	0,1	0,6	0,3	0	0,2	0,5	0,1	0	0,8	0,8	0,8	0,5
Item 2	0,3	0,4	0,2	0,02	0,9	0,5	0,9	0,4	0,1	0,4	0,5	0	0,1	0,4	0,5	0
Item 3	0,5	0,1	0,1	0,01	0,6	0,5	0,8	0,2	0,8	0,8	0,8	0,5	0,3	0,4	0,2	0
Item 4	0,6	0,9	0,8	0,43	0,3	0,4	0,2	0	0,6	0,5	0,8	0,2	0,6	0,5	0,8	0,2
Item 5	0,8	0,9	0,8	0,54	0,1	0,4	0,5	0	0,9	0,5	0,9	0,4	0,3	0,5	0,3	0
Item 6	0,9	0,2	0,9	0,16	0,6	0,5	0,8	0,2	0,1	0,6	0,3	0	0,8	0,9	0,9	0,7
Item 7	0,1	0,4	0,5	0,02	0,6	0,5	0,8	0,2	0,3	0,4	0,2	0	0,6	0,5	0,8	0,2
Item 8	0,1	0,6	0,3	0,02	0,5	0,1	0,1	0	0,6	0,7	0,8	0,3	0,6	0,5	0,8	0,2
Item 9	0,3	0,5	0,3	0,05	0,9	0,8	0,9	0,6	0,1	0,6	0,3	0	0,5	0,1	0,1	0
Item 10	0,5	0,2	0,1	0,01	0,8	0,3	0,8	0,2	0,6	0,5	0,8	0,2	0,9	0,2	0,9	0,2

Risk ranges		
Low	0	0,09
Medium	0,1	0,5
High	0,51	1

Risk acceptance threshold	0,4

Table 5.3: Example of a risk matrix with values

At above risk matrix example, there are 8 risks that are identified with an unacceptable risk as they are above the risk threshold of 0.4. The next step is to mitigate these intolerable risks.

The assessment phase and process mitigates risks captured in a standard format so that the report can be used for quality assurance and post analysis phases.

The aim of this report is to provide an overview of the main risks detected and the recommendations and guidelines to take into in the next phase, the strategy phase.

5.2.2.1.3 Strategy

This process will use the report provided by the assess process. This report will be the trigger that starts this phase where the main aim is to identify the most appropriate security measures to implement in order to reduce the risk to have an acceptable risk value for all vulnerable items in the TMS.

The result of this phase must be a report with these main points:

- Which measures shall be implemented, when and where;
- The type of each identified measure;

- The rationale behind the measures;
- The organisation and/or personnel in charge of implementation;
- The resources required for implementation;
- A new evaluation of the risk matrix taking into account the security measures proposed.

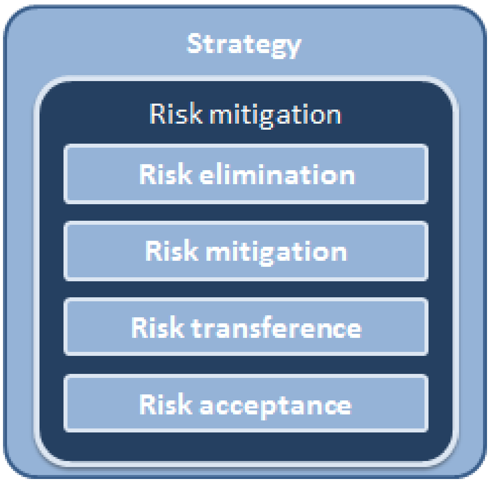


Figure 5.5: Process of Strategy

5.2.2.1.3.1 Risk mitigation methodology

Once the requirements and security risks are identified, the next step is to decide what additional security measures must be implemented in the system to reduce or eliminate the risk identified and thus ensure that the risk is always below the threshold of acceptable risk.

This task of identifying security measures to adopt is called risk treatment. Steps to take to carry out this phase are:

- Identification of options;
- Develop action plan;
- Approval of the action plan;
- Implementation of action plan;
- Identification of residual risk.

The measures to be taken to reduce the risk must be done to any vulnerable parts that have detected an unacceptable risk. It should be noted that the security measures adopted after this phase may cause a reduction in risk in other parts of the system. Therefore the risks should be re-evaluated in the entire system after the execution phase to determine if risks have been reduced or if new risks have been introduced.

This cycle must run on a recurring basis for several reasons:

- Threats are changing and there may be new or change already detected;
- The TMS is a system that can evolve to provide new features, new interfaces, etc. involving the appearance of new vulnerable parts;

- The control process for the information security must be continuous, because that continuous executions cause these good practices that are part of the process applied.

There are several ways to reduce the risk:

(a) Risk elimination
(b) Risk mitigation
(c) Risk Transfer
(d) Risk acceptance

These types of measures to be taken are described below:

(a) Risk elimination

Risk elimination is the most difficult measure to be able to adopt. The reason is that to do this it is necessary to reduce to zero one of the parameters of the risk formula to zero.

The three parameters to aim to reduce to zero are:

- Probability of attack: Reducing this parameter to zero is not possible because it depends on the attackers more than the TMS characteristics;
- Probability of success: This parameter can be reduced adding specific security measures;
- Impact of an attack: This parameter can be reduced with attack detection measures.

(b) Risk mitigation

Risk mitigation involves the implementation of measures that reduce one or all of the following; the probability of an attack occurring, the probability of a successful attack, the impact of a successful attack.

(c) Risk transference

Risk transference assumes that responsibility of the risk treatment falls over another entity or institution. A good example would transfer to state institutions or insurance companies, which assume responsibility and economic consequences of the impact of a successful attack.

(d) Risk acceptance

Risk acceptance means accepting that a detected threat in the future may occur, causing some level of impact.

It is a valid strategy for small risks whose protection entails higher cost than the damage it would cause if the threat did materialize, or for those risks that are so unlikely and the cost of cover is so high that is unacceptable for the company to cover the costs.

By definition all risks that are not mitigated, or avoided or transferred are accepted.

All the risks that are below the risk acceptance threshold should be accepted by the security department but these risks should still be monitored and assessed at the next cycle of the RISKS to ensure they remain below the risk acceptance threshold.

5.2.2.2 Execution phase

This phase of the RISMS is executed when an attack is produced. The processes involved at this phase is to react and learn and the results of these processes must be used at the next execution cycle of the preparation phase processes.

5.2.2.2.1 React

The first step to be able to react to an attack is detecting it. There are some mechanisms to detect an attack before is successful but sometimes the attack is detected across due to the consequences it produces.

At the TMS environment, the direct consequences of a logical attack can be:

- **Loss of control:** This is the most dangerous consequences in the TMS. An attack that produces it can produce a complete disruption of the traffic;
- **Corrupted information:** This is another dangerous consequence because all of the operations in a TMS are based on the information received from other external systems and centralized traffic control systems;
- **Loss of information:** This could be a big problem for the TMS post-operation. A TMS must register all the information related with the events produced at the railway exploitation, if an attack produces a loss of this information it will be impossible to recover it;
- **Change of system operation:** These consequences could change the desired behaviour of the trains. The attacks that produce these kinds of consequences are very difficult to detect because usually they are interpreted as faults in the system and not as consequences of attacks;
- **System crash:** Produce a partial or complete reduction of the system capabilities.

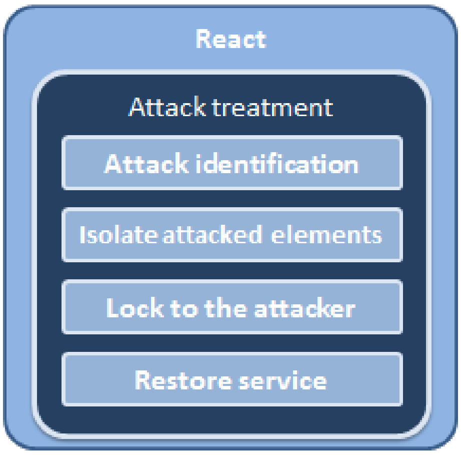


Figure 5.6: Process of Reacting to a threat

5.2.2.2.1.1 Attack treatment methodology

The attack treatment process is known as the contingency plan of an organization. This plan defines the procedures and alternative processes that an organization must implement when a risk manifests into a real situation. In this case activation of the contingency plan should cover three main activities:

- Coordinate crisis management;
- Ensuring the use of alternative processes that enable business continuity;
- Resolve the incident to restore normality in the processes and operations.

The treatment of an attack includes several steps that compound this methodology:

(a) Attack identification: It includes actions to be executed periodically to try to detect an attack before it produces a system error or malfunction;

(b) Isolate attacked elements: It includes all the actions involved to reduce the impact of an attack success;

(c) Lock to the attacker: When the attack is isolate and then the impact is known and controlled, the next step will be detect and block the attack;

(d) Restores service: When the attack is blocked it is necessary restore the complete system in a controlled way.

(a) Attack identification

The main problem in identifying an attack is the interference with the system. It is also necessary to detect the attacks but with a minimum impact to the system operation.

There are a lot of methodologies to do this identification:

- **Sniffers:** They are software or hardware devices that detect information patterns that are not used in the system. These kinds of items are focused on the network system and on the information exchanged between modules and subsystems. The main problem of this methodology is that it requires specific resources to analyse all information flows and may produce a delay in the exchange of information between different parts of the system;
- **Audit system status:** This methodology is based on periodical analysis of the system or subsystems status. The main problem with this method is the complexity to detect if a module or subsystem is working correctly or not. Each module or subsystem to be analysed must have the ability to auto-diagnosis to provide their status without a reduction in performance.

The proposed methodology for TMS systems is to detect attacks deemed intolerable based on parts identified at previous RISMS phases.

The most efficient method to detect possible attacks in a TMS is to include periodical check operations in order to assure that the system is working according to the specifications and performance of all the parts of the system.

The different TMS subsystems, especially the parts of the system identified as vulnerable, must provide mechanisms to evaluate their own performance in order to be able to detect deviations. This data will be used by the experts to evaluate if the system is working correctly or not.

It is important to analyse the behaviour of the system in order to make a database with all the performance results. These performance indicators will be used to make a relation between them and the different indicators of the railway exploitation. For example, the performance level of a single part or module of the system can be directly related with the number of simultaneous trains that are running. This kind of information must be analysed to try to detect the different thresholds of performance to be able to determinate when the performance level is anomalous. The experts must then evaluate the state of the system has and include the results of the database in order to detect patterns of the behaviour of the system. As part of this analysis phase, the experts must analyse the historical data to be able to identify deviations in the system to try to detect possible attacks to the system.

Other important actors involved at this identification process are the users of the TMS. Operators are using the system 24 hours and can detect a loss of performance or a strange behaviour of the system or part of the functionality provided by the system. The periodical checks can detect deviations in the system and can be reported by the operators.

When an attack is detected, is important to identify the modules or parts of the system affected, if the part affected is one of the vulnerable parts identified at previous phases of the RISMS. The reaction to this identified attack can be different taking into account the level of vulnerability assigned. For example, if the level of vulnerability is low it is possible that the reaction will be delayed to an interval of low traffic but if the level of vulnerability is high then the reaction should be applied immediately.

(b) Isolate attacked elements

There are several technics to try to minimize the impact of an attack. The use of the different alternatives is directly related with the impact level of an attack and the parts of the system affected. If the attack affects a fundamental part of the system, the measures to take in order to minimize the impact of an attack will be more drastic than if the parts affected are minimal.

The measures to minimize the impact of a successful attack have to be decided by experts in security and by the staff that use the system. This double team required to take the decision is necessary because the actions required from the point of view of the security can produce a catastrophic result from the point of view if the railway exploitation. The security staff will provide the measures to reduce the impact of the attack and the staff responsible for the operation of the system will provide their opinion about the impact of these actions to the system and to the railway exploitation.

Possible measures to take when an attack is detected are:

- **Completely stop the system:** this action will be implemented when the impact of the attack is unacceptable;
- **Stop of the affected parts of the system:** this action will be implemented when the attack is selective to a specific part of the system. It is important to take into account that the system must be prepared to do this in different parts of the system;
- **Not use the affected parts of the system:** if a functionality of the system works incorrectly as an effect of an attack, a possible measure will be not use this specific functionality and make the necessary actions to try to minimize the possible impact of not to use the affected functionality;
- **Use other alternative systems:** one measure to apply can be to transfer the operation to an alternative system. When the operation is restored it will be necessary to merge the information managed by this alternative system to the main system in order to have all the information in the same system;
- **Transit the system to a degraded mode of operation:** some of the current Traffic Management Systems have degraded modes in order to provide the most important functionality to be able to continue with the railway operation. These degraded modes usually have to use manual operations versus automatic functions of the system, but the operation can be assumed in a manual mode and then the impact of the attack can be minimized.

(c) Lock to the attacker

Once the attack is detected and once the effect of the attack is isolated to prevent an increase in impact, the attacker should be blocked.

This phase is important in order to make it possible to restore the system with guaranties to assure that the system will work correctly and ensue that the system doesn't suffer the same attack in the near future.

It may also be necessary to continue with this process of studying the attack to take measures to minimize the probability of future similar attacks.

(d) Restore service

There are two alternative actions to restore the system operation.

- **Partial:** This action will be applied to try to restore the operation by parts. This method allows assuring that the attack is not active yet or the measures applied to block is working correctly. Each module is executed and tested before starting the next module or part of the system. This is the preferred option because it provides more control over the state of the system;
- **Complete:** When the system doesn't provide different modules to execute independently, it is necessary to use this option. When the system is on execution it

is necessary to analyse each module, functionality or part of the system in order to try to assure that is working correctly.

Independently of the action used, at the end of this phase the system has to provide the complete functionality with the performance expected.

5.2.2.2.2 Learn

The main aim of this process is identify new aspects that must be taken into account at the next execution cycles of the RISMS and in particular at the next cycle of the execution phase of the RISMS.

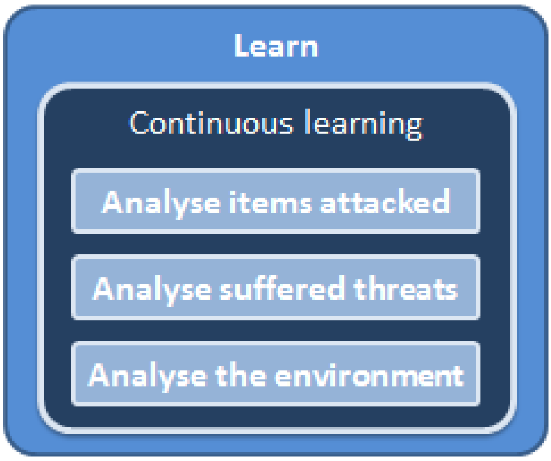


Figure 5.7: Process of Learn

5.2.2.2.2.1 Continuous learning

This process must analyse the attacked suffered in order to detect new vulnerable items and new threats that were not detected at previous preparation phase cycles.

The result of this analysis will be used at the next execution cycle of the preparation phase in order to refine the RISMS and provide a TMS prepared to future attacks. It is good practice for continuous learning to take place across the following areas:

- Analyse items attacked

This task must provide the list of items or part of the system affected by the attack suffered.

The experts must analyse which modules of the system are involved in the attack and detect if these ones are included in the list of vulnerable items of the previous execution cycle of the Identify process of the RISMS.

The items affected by the attack must be taking into account at the next execution cycle of the preparation phase of the RISMS.

- Analyse suffered threats

This task aims to detect and identify if the threat suffered was identified at the previous execution of the preparation phase.

The experts must analyse the attack suffered in order to detect if the attack was one of the possible threats identified at the previous tasks. It is important that the experts not only focus on the attack suffered but must also identify similar threats that can affect to the TMS.

All these new threats must be taken into account at the next cycle execution of the preparation phase of the RISMS.

- Analyse the environment

This task aim to detect all environmental aspects that can affect to the value associated to each threat and vulnerable item regarding probability of attack, probability of success and impact of the attack.

The experts must analyse the environmental reasons that led that to somebody trying to make the attack (probability of attack), the chain of events that made the attack a success (probability of success) and the reasons that made the attack produce the suffered effect (impact of an attack).

The result of this analysis will be used at the next execution of the Assess process in order to make a re-evaluation of the values associated to the Risk analysis matrix.

6 Workload Analysis for Operators

6.1 Introduction to Workload

6.1.1 Workload Principles

Across many sources of workload literature, there is much dispute around the definition of workload and methods in which best quantify the experience of workload [Ref 1]. Workload can be defined as 'the amount of work assigned to or expected in a specified time period' [Ref 2] and so is most simply thought of as a ratio of time required to do tasks to time available to do them in [Ref 3]. However, changes in workload are not only influenced by time and so the element of 'effort' is also used to assess its effects [Ref 3].

There are a number of models to help define mental workload such as; limited resources model and multiple resources model. These models describe the workload as being the difference between resources available in a person and resources demanded by a task situation [Ref 1]. Therefore performance is affected by either task demand or resources available. Some tasks however are time consuming but are not particularly demanding on cognitive resources or effort [Ref 3]. As well as this there are a number of different influences that effect workload; these include individual's skills, expertise and attitudes, as well as work circumstances [Ref 1]. Therefore personal, technical and organisational factors and the effects of their interactions must be taken into account [Ref 4].

There are number of different workload variables, examples of these variables are explained by the NASA-TLX Model; Mental, Physical, Temporal Demands, Frustration, Effort, and Performance, see section 9.2.1.2 in the appendix.

Although workload may not directly impact performance, both acute and chronic periods of very high, very low, or variable work demand can have undesired consequences and wider impact on situational awareness, fatigue and decision making.

Workload is multidimensional and is made up of the following individual, technical, organisational and social components and influences, [Ref 4 and 5]:

- Task and or job design:
  - E.g. Task difficulty, task allocation, avoid time sharing, task variety, avoid constant attention, provide sub-goals, job enrichment etc.
- Work equipment:
  - E.g Reduce ambiguity of presented information and design for operator not machine based decisions etc.
- Environment:
  - E.g. Illumination, temperature, colours etc.
- Organisational:
  - E.g. Reduce time pressures, job enlargement/rotation etc.

- Operator:
  - E.g. Motivation, experience, fatigue etc.
- Time:
  - E.g. Actual time available vs. time perceived available.

Generally, higher workload can be associated with more errors; however it has been shown that a higher workload doesn't always correlate with lower levels of performance [Ref 1]. This is explained by the Yerkes-Dodson law and it should be noted that there is an optimum level of arousal when describing the effects of the level of arousal on performance [Ref 3]. This law explains that the effects of under load can also have a negative impact on performance. Therefore the design of systems and tasks should enable operators to complete tasks required, in the time required, retaining some spare capacity for additional tasks. The task load should also not be too high as it can result in fatigue or mistakes but also, should not be too low that operators suffer from boredom due to under load of attention [Ref 11].

Therefore based on the above theories, some key design principles include:

- Task/systems should be designed such that operators should not be overloaded due to being required to perform multiple tasks at once or one very complex task;
- Task/systems should be designed such that operators should not be under loaded as this can result in lack of concentration and reduced situational awareness;
- System design should support users in their decision making tasks to reduce the effect of workload.

6.1.2 Workload Measurement Techniques

There is no single best way to measure or assess mental workload and so a combination of methods should be used together. There are four main techniques of workload assessment:

- **Physiological measurements**: records and evaluates changes in physiological states as a result of different levels of workload;
- **Subjective ratings:** how participants subjectively assess the effect of mental workload for example how they feel about specific scenarios or tasks;
- **Performance assessment:** evaluate variation in performance as a result of different levels of workload;
- **Job and tasks analysis**: assess task elements, physical and psychosocial work conditions, environmental conditions and the organisation factors effect on workload.

For a more detailed list of types of workload measurement techniques as well as specific measurement techniques used in the context of rail, see appendix 9.2.

6.2 Workload in the Context of Traffic Management

This section discusses how the introduction of TM will increase the complexity of how workload is predicted and measured in the future.

6.2.1 Effects of Future TM Systems on Workload

There is a large amount of supporting literature regarding workload measurement techniques for the signaller role using conventional rail systems. However, as a result of the development of TM systems there will be a number of factors of workload that change from conventional rail signalling systems, these changes include:

- Increase in automation;
- System design;
- Roles and processes;
- The type and quantity of tasks that the operator is required to perform;
- The characteristics of the operators (including training and experience);
- The complexity of the task(s) that the operator has to perform;
- Timetable (traffic type and density);
- Network (track features and signalling technologies) etc.

All of the above changing factors will have different effects on workload, for example;

- Some elements of workload will be reduced or eliminated;
- Some elements of workload will remain unchanged;
- Some elements of workload will be exaggerated, and
- Some new elements or sources of workload will be introduced.

It is important to clearly identify the above factors and how they might change as a result of TM in order to influence system design, task design and process design. Test Cases to measure workload should be developed to identify the tasks required in both normal and degraded modes of working. This will allow the expected sources of workload to be defined due to changes in technology, changes in tasks and changes in process.

6.2.2 Aim of Designing for Optimum Workload

The aim of designing for an optimum workload in TM systems is unchanged from conventional systems; however the capabilities in achieving these goals have the potential to be enhanced.

The aim of designing for an optimum workload is to:

- ensure the human is supported by the system;
- ensure the number of errors are reduced that could lead to safety related incidents;
- ensure optimum capacity of the running of the railway but have sufficient spare capacity and flexibility to manage an incident if it occurs;
- balance between operational cost and safety, performance or reputational risk.

The ability to design for an optimum workload in conventional systems is well understood. There are well established methods to develop systems, roles and processes to ensure there is a suitable level of workload and there is a huge amount of supporting workload data from previous deployments of conventional systems to baseline levels of workload to. However, due to the introduction of TM and functionality such as flexible areas of control, the concept of measuring the workload experienced by an individual to ensure it is at an optimum level to support safe and efficient management of the railway has become more complex.

The concept of operations of the railway is changing from silo working, where individual signallers have the responsibility of controlling a defined area of the railway, to a more collaborative team working approach. Therefore it is no longer enough to measure the workload experienced by each individual separately, but there is a need to consider the effects of workload experienced by the team and the entire system.

The below diagram aims to show how in the future, workload will need to be measured in the context of the entire system:

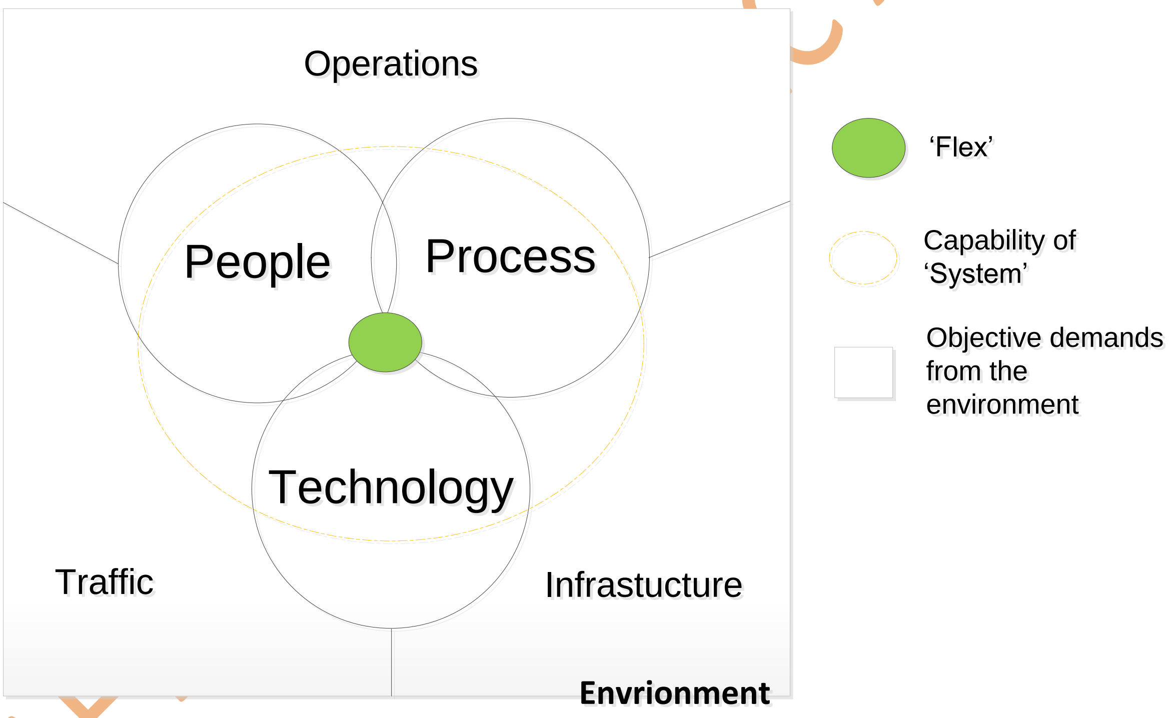


Figure 6.1: Workload in the Context of TM

Based on the above diagram, the following should be considered:

- The environment consists of objective workload demands related to traffic, infrastructure and operations. For example, the amount of traffic and the complexity of infrastructure in an area of control impacts on demand;
- The capability of the system is made up of people, process and technology;
- The system can experience different levels of workload depending on the objective demands from the environment;

- When the capabilities of the system cannot cope with the objective demands, this is when higher workload is experienced by the system;
- The system must be designed so that an optimum level of workload is achieved and there is a suitable level of resilience to cope with the changing objective demands;
- The 'Flex' of the system is the ability to flex people, process or technology to meet the objective demands of the system. For example, a flexible area of control enables workload to be distributed across the system depending on each sub-systems current experience of workload.

The overall goal of the system is to reduce delays and maximise safety. Therefore, people, processes and technology should adapt in order to meet this goal.

6.2.3 Predicting Future Workload for TM Systems

At this stage of TM implementation there is a lack of data to baseline the effect that TM systems have on the experience of workload. It is also difficult to predict the effect that TM systems will have on workload. This is due to the fact that there are a number of variables with a level of uncertainty related to expected sources of future workload which have not yet been assessed in practice.

In order to reach a stage where we are able to make predictions of workload for future TM systems with a higher level of confidence, the following activities must occur:

1. Identify variables we believe, based on current understanding, will affect workload in the future due to TM,
2. For each project or deployment of TM, develop a forecast of expected workload to be experienced by the system,
3. Use this forecast to make assumptions about the number of roles required, to influence system design and develop processes,
4. Develop the TM system and measure the level of workload experienced by the system to ensure it is suitable to commission the system,
5. Continuously measure the experience of workload and use data to feed into subsequent TM deployments, process improvements and system design.

The In2Rail toolset, see Section 6.3, describes in more detail how the above steps should be followed.

6.3 In2Rail Workload Framework and Toolset

This section describes a suggested tool set to be followed to forecast and measure workload in future TM Systems. The In2Rail Tool set has been developed, in order to reach a stage where we are able to make predictions of workload for future TM systems with a higher level of confidence. The toolset has also been developed to highlight where existing rail workload measurement techniques need to be adapted in order to support continuous development of people, process and technology.

6.3.1 Introduction to In2Rail Toolset

The In2Rail Toolset is spilt into three main phases:

Phase of TM	Description of In2Rail Workload Phase
First deployment of TM	**Phase 1: Forecasting** Phase 1 has the following characteristics: • There is high uncertainty and a lack of previous TM workload measures[2] to baseline and inform decisions such as determining type and number of roles required, suitable size of areas of control and changes to concept of operations required. • Predictive methods to determine the above are nearly impossible due to the number of uncertainties, number of changing variables and lack of TM workload baseline. Therefore a 'forecasting method' has been developed to help inform initial first deployments people, process and technology decisions. See Section 6.4 for details of the forecasting model.
Live system of first TM deployment is available	**Phase 2: Measure** • Once the first deployment of TM has been implemented and commissioned onto the live railway, workload should be continuously reviewed by both the supplier and the operating company. • Data collected from this continuous review cycle should be used to develop the forecasting model so that it is more mature to be used in subsequent TM deployments as well as influence people, process and technology enhancements for TM.
Subsequent TM deployments	**Phase 3: Predict** • Once a suitable number of TM deployments have occurred and the workload experienced by the system has been evaluated, the forecasting method will become more mature and reach a state where the forecasting tool output matches the measured workload of the final system. • Once the forecasting method has reached this 'steady state' it can now be used as a predictive model with higher level of confidence for subsequent deployments.

Table 6.1: Alignment of In2Rail Toolset Phases to TM Deployment Phase

[2] Relevant to that location, type or scale of deployment

6.3.2 Overview of In2Rail Toolset

Figure 6.2 shows an overview of the three phases in the In2Rail workload toolset. To see further details of each phase; Phase 1, 2 and 3, see sections 6.3.3, 6.3.4 and 6.3.5 respectively.

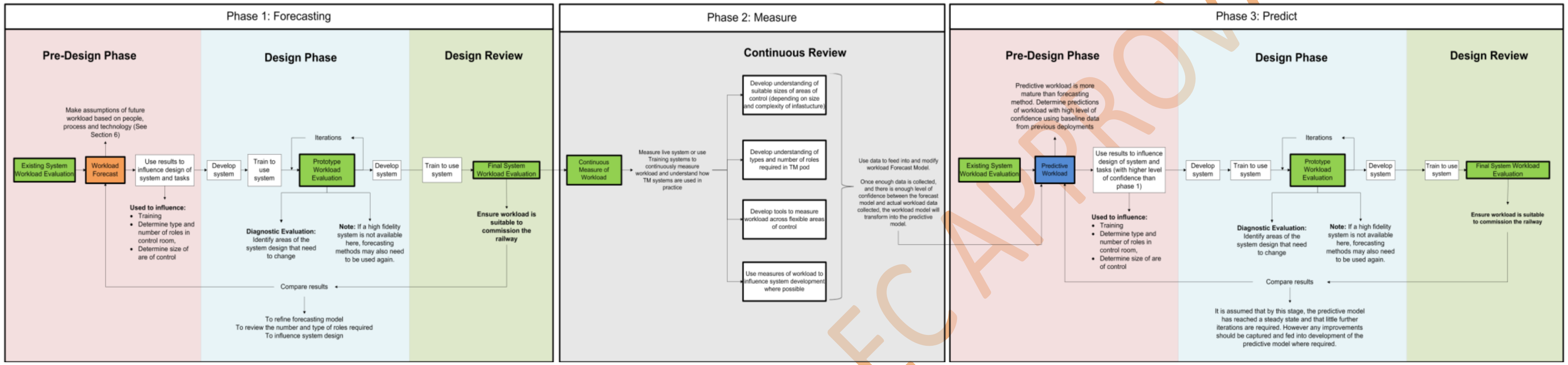

Phase 1: Forecasting
Pre-Design Phase
Design Phase
Design Review
Make assumptions of future workload based on people, process and technology (See Section 6)
Existing System Workload Evaluation
Workload Forecast
Use results to influence design of system and tasks
Develop system
Train to use system
Iterations
Prototype Workload Evaluation
Develop system
Train to use system
Final System Workload Evaluation
Used to influence:
• Training
• Determine type and number of roles in control room,
• Determine size of are of control
Diagnostic Evaluation: Identify areas of the system design that need to change
Note: If a high fidelity system is not available here, forecasting methods may also need to be used again.
Ensure workload is suitable to commission the railway
Compare results
To refine forecasting model
To review the number and type of roles required
To influence system design
Phase 2: Measure
Continuous Review
Continuous Measure of Workload
Measure live system or use Training systems to continuously measure workload and understand how TM systems are used in practice
Develop understanding of suitable sizes of areas of control (depending on size and complexity of infastucture)
Develop understanding of types and number of roles required in TM pod
Develop tools to measure workload across flexible areas of control
Use measures of workload to influence system development where possible
Use data to feed into and modify workload Forecast Model.
Once enough data is collected, and there is enough level of confidence between the forecast model and actual workload data collected, the workload model will transform into the predictive model.
Phase 3: Predict
Pre-Design Phase
Design Phase
Design Review
Predictive workload is more mature than forecasting method. Determine predictions of workload with high level of confidence using baseline data from previous deployments
Existing System Workload Evaluation
Predictive Workload
Use results to influence design of system and tasks (with higher level of confidence than phase 1)
Develop system
Train to use system
Iterations
Prototype Workload Evaluation
Develop system
Train to use system
Final System Workload Evaluation
Used to influence:
• Training
• Determine type and number of roles in control room,
• Determine size of are of control
Diagnostic Evaluation: Identify areas of the system design that need to change
Note: If a high fidelity system is not available here, forecasting methods may also need to be used again.
Ensure workload is suitable to commission the railway
Compare results
It is assumed that by this stage, the predictive model has reached a steady state and that little further iterations are required. However any improvements should be captured and fed into development of the predictive model where required.

Figure 6.3: Overview of In2Rail Toolset Phases

Across the three phases there are three elements to also consider:

- Workload Measurement Techniques,
- A Forecasting Model
- A Predictive Workload Model

Key

🟩 Workload Measurement

🟧 Workload Forecast

🟦 Predictive Workload

Workload Measurement Techniques: The different phases where workload measurement techniques need to be considered are indicated by the green boxes then gives guidance on how individual workload assessment should be conducted in each of the stages highlighted in green in Phase 1, 2 and 3. Details of how types of measurement techniques need to be enhanced to support continuous improvement of people, process and technology is also given in Section 6.3.7.

Forecasting Model: The Forecasting technique developed as part of the In2Rail Toolset is indicated by the orange box in Phase 1. See Section 6.4 for details of how this forecasting method has been developed and evaluated.

Predictive Model: Prediction methods are indicated by the blue box in Phase 3. Although this is not possible to do at this stage, the aim is that overtime due to continuous improvements of the forecasting model this will be possible.

6.3.3 In2Rail Toolset Phase 1 - First Deployment of TM

Phase 1 has been split into three main stages:

Pre design Stage:

- Evaluate Existing Systems: Evaluate existing systems to baseline current workload experienced and use the results to identify areas of overload or under load the future system can support, or mitigate the effects of;
- Forecasting: Forecast future levels of workload, based on assumptions of known changes related to equipment or technology changes, role and task changes. See section 6 for details of forecasting;
- Use the output from the forecasting to influence the number of roles required, the areas of control require, the design of the system itself and training required.

Design Phase Stage:

- Develop System: TM system development, made up of people, process and technology.
- Prior to conducting workload assessments, it's necessary to train participants in new functionality or changes in system design as unfamiliarity can have an impact on usability and workload.
- Prototype Workload Evaluation: Using either prototype systems or low fidelity systems, initial workload assessments should be conducted to identify early areas of under load or overload. Results from these assessments can then be used to influence the TM system design further, (including people, process and the technology). In the phase a number of iterations are likely to take place as the technical system design develops and as it becomes more understood how the system will be used in practice.
- It should be noted that if a simulator is not available at this stage then forecasting may be required to be completed again using more mature information regarding people, process and technology.

Design Review and Evaluation Stage:

- Similar to in the design phase, prior to conducting workload assessments, it's necessary to train participants in new functionality or changes in system design as unfamiliarity can have an impact on usability and workload.
- Final System Workload Evaluation: Measure the workload of the system, (people, process and technology); to ensure final design has appropriate levels of workload in order to commission the system.

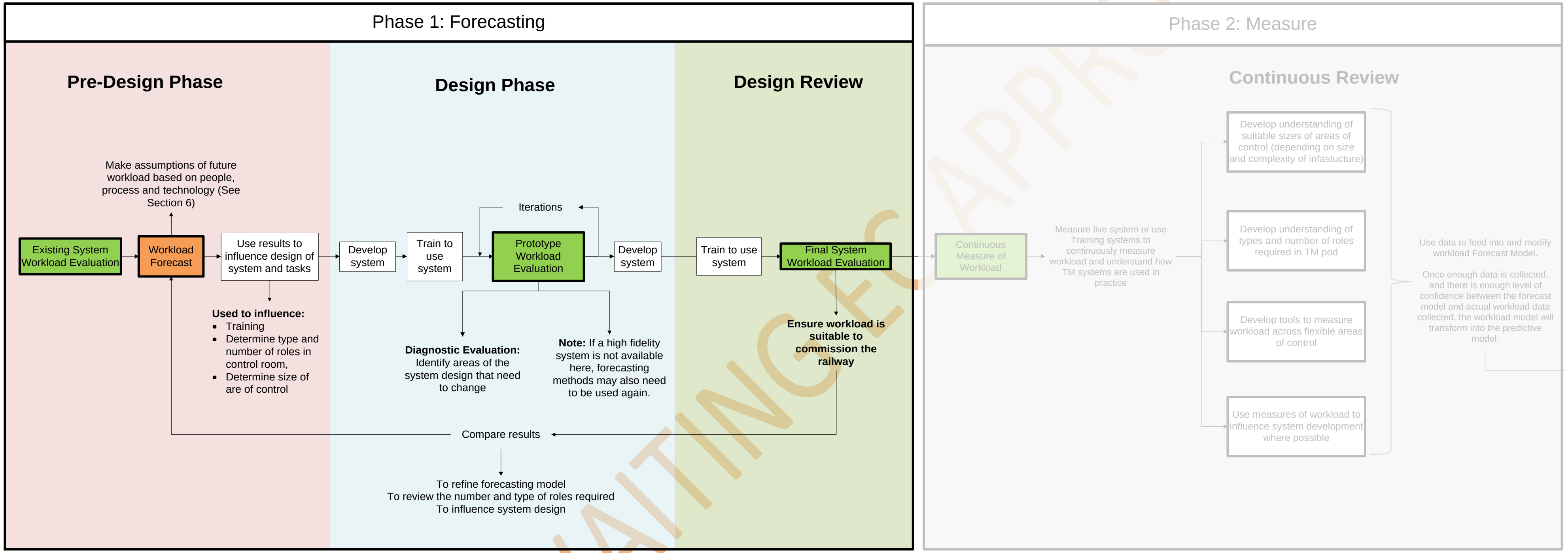

Phase 1: Forecasting
Pre-Design Phase
Design Phase
Design Review
Make assumptions of future workload based on people, process and technology (See Section 6)
Existing System Workload Evaluation
Workload Forecast
Use results to influence design of system and tasks
Used to influence:
• Training
• Determine type and number of roles in control room,
• Determine size of are of control
Develop system
Train to use system
Iterations
Prototype Workload Evaluation
Develop system
Train to use system
Final System Workload Evaluation
Diagnostic Evaluation: Identify areas of the system design that need to change
Note: If a high fidelity system is not available here, forecasting methods may also need to be used again.
Ensure workload is suitable to commission the railway
Compare results
To refine forecasting model
To review the number and type of roles required
To influence system design
Phase 2: Measure
Continuous Review
Continuous Measure of Workload
Measure live system or use Training systems to continuously measure workload and understand how TM systems are used in practice
Develop understanding of suitable sizes of areas of control (depending on size and complexity of infastucture)
Develop understanding of types and number of roles required in TM pod
Develop tools to measure workload across flexible areas of control
Use measures of workload to influence system development where possible
Use data to feed into and modify workload Forecast Model.
Once enough data is collected, and there is enough level of confidence between the forecast model and actual workload data collected, the workload model will transform into the predictive model.

Figure 6.4: Phase 1 of In2Rail Toolset and how it links to Phase 2

6.3.4 In2Rail Toolset Phase 2 – Live System of TM First Deployment Available

During phase 2, the forecasting method in Phase 1 will form the predictive model in phase 3. Once the first deployment of TM has been implemented and commissioned onto the live railway, workload should be continuously reviewed by both the supplier and the operating company. Note that data could also be collected from any training simulators that were developed during the project if rail operating centres chose to continue to use these systems for further training or process enhancements. Data collected from this continuous review cycle should be used to develop the forecasting model so that it is more mature to be used in subsequent TM deployments as well as influence people, process and technology enhancements for TM. The main areas that should be considered in continuous review are:

- Develop a better understanding of suitable sizes of areas of control (depending on size and complexity of infrastructure) - determine if there is more or less workload than expected and if areas of control can be increased in size;
- Develop a better understanding of types and number of roles required in the TM pod, and ensure processes are adapted to support new ways of working;
- Develop the tools to measure workload across flexible areas of control, and collaborative TM pods;
- Use measures of workload to influence system development.

The above data, and any additional data or findings collected from assessing the impact of TM in practice should be fed into the workload Forecast Model for further development. Once enough data is collected, and there is enough level of confidence between the forecast model and actual workload data collected, the workload model will form into the predictive model in phase 3.

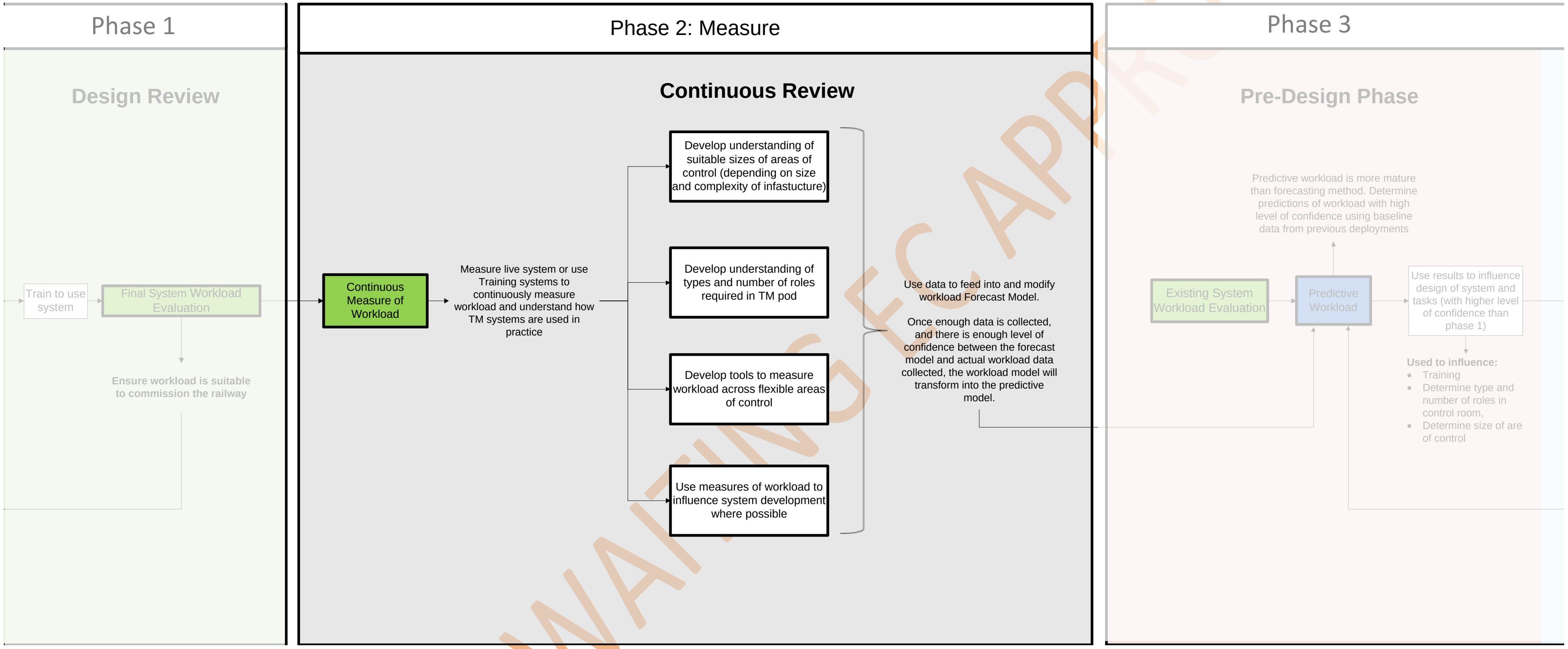

Phase 1
Design Review
Train to use system
Final System Workload Evaluation
Ensure workload is suitable to commission the railway
Phase 2: Measure
Continuous Review
Continuous Measure of Workload
Measure live system or use Training systems to continuously measure workload and understand how TM systems are used in practice
Develop understanding of suitable sizes of areas of control (depending on size and complexity of infastucture)
Develop understanding of types and number of roles required in TM pod
Develop tools to measure workload across flexible areas of control
Use measures of workload to influence system development where possible
Use data to feed into and modify workload Forecast Model.
Once enough data is collected, and there is enough level of confidence between the forecast model and actual workload data collected, the workload model will transform into the predictive model.
Phase 3
Pre-Design Phase
Predictive workload is more mature than forecasting method. Determine predictions of workload with high level of confidence using baseline data from previous deployments
Existing System Workload Evaluation
Predictive Workload
Use results to influence design of system and tasks (with higher level of confidence than phase 1)
Used to influence:
Training
Determine type and number of roles in control room,
Determine size of are of control

Figure 6.5: Phase 2 of In2Rail Toolset and how it links to Phase 1 and 2

6.3.5 In2Rail Toolset Phase 3 – Subsequent TM Deployments

Phase 3 is similar to Phase 1 in that it is also split into three main stages, however the key difference is that the forecasting method from phase 1 is assumed to of now formed a predictive model.

Pre design Stage:

- Evaluate Existing Systems: Evaluate existing systems to baseline current workload experienced and use the results to identify areas of overload or under load the future system can support, or mitigate the effects of;
- Predicting Model: Once a suitable number of TM deployments have occurred and the workload experienced by the system has been evaluated, the forecasting method will become more mature and reach a state where the forecasting tool output matches the measured workload of the final system. Once the forecasting method has reached this 'steady state' it can now be used as a predictive model with higher level of confidence. Using the predictive model, you will be able to predict future levels of workload, based on workload data captured in Phase 2 as well as known changes related to equipment or technology changes, role and task changes based on Phase 2;
- The output from the prediction model can then be used to influence the number of roles required, the size of the areas of control required etc. with a higher level of confidence than in Phase 1 to more accurately influence design.

Design Phase Stage:

- Develop System: TM system development; made up of people, process and technology;
- Prior to conducting workload assessments, it's necessary to train participants in new functionality or changes in system design as unfamiliarity can have an impact on usability and workload;
- Prototype Workload Evaluation: Using either prototype systems or low fidelity systems, initial workload assessments should be conducted to identify early areas of under load or overload. Results from these assessments can then be used to influence the TM system design further, (including people, process and the technology). A number of iterations are likely to take place as the technical system design develops and as it becomes more understood how the system will be used in practice. However less iteration is likely to take place than in Phase 1 due to previous evaluations of TM in practice;
- It should be noted that if a simulator is not available at this stage then prediction may be required to be completed again using more mature information regarding people, process and technology.

Design Review and Evaluation Stage:

- Similar to in the design phase, prior to conducting workload assessments, it's necessary to train participants in new functionality or changes in system design as unfamiliarity can have an impact on usability and workload;
- Final Workload Evaluation: Measure the workload of the system, (people, process and technology); to ensure final design has appropriate levels of workload in order to commission the system;
- Compare Results: It is assumed that by this stage, the predictive model has reached a steady state and that little further iterations are required when comparing the final workload output with the predictive model. However any improvements should be captured and fed into development of the predictive model where required.

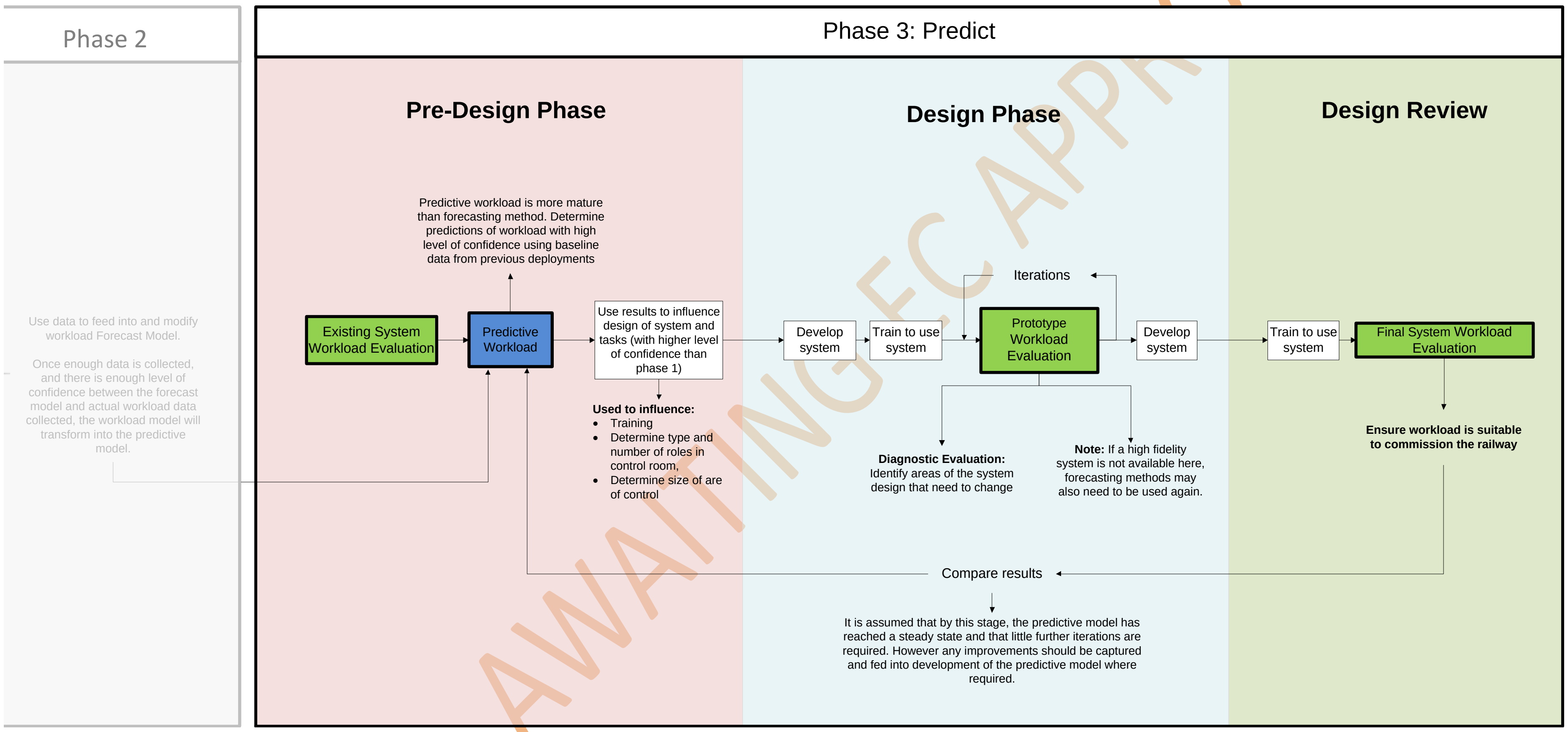

Phase 2
Use data to feed into and modify workload Forecast Model.
Once enough data is collected, and there is enough level of confidence between the forecast model and actual workload data collected, the workload model will transform into the predictive model.
Phase 3: Predict
Pre-Design Phase
Design Phase
Design Review
Predictive workload is more mature than forecasting method. Determine predictions of workload with high level of confidence using baseline data from previous deployments
Existing System Workload Evaluation
Predictive Workload
Use results to influence design of system and tasks (with higher level of confidence than phase 1)
Used to influence:
Training
Determine type and number of roles in control room,
Determine size of are of control
Develop system
Train to use system
Iterations
Prototype Workload Evaluation
Develop system
Train to use system
Final System Workload Evaluation
Diagnostic Evaluation: Identify areas of the system design that need to change
Note: If a high fidelity system is not available here, forecasting methods may also need to be used again.
Ensure workload is suitable to commission the railway
Compare results
It is assumed that by this stage, the predictive model has reached a steady state and that little further iterations are required. However any improvements should be captured and fed into development of the predictive model where required.

Figure 6.6: Phase 3 of In2Rail Toolset and how it links to Phase 2

6.3.6 TM Deployment Additional Use Case

This section describes an additional use case that could be considered and describes how the In2rail toolset supports it.

Change to existing TM Deployment area Use Case:

There a number of changes that an operating company may need to implement post commissioning of TM such as:

- Add a certain amount of geography into an existing Rail Operating Centre and TMS System;
- Modify the size of the areas of control to determine its impact on workload;
- Modify the number and type of roles in the TM pod and determine its impact on workload.

Phase 3 of the In2rail toolset supports this process of further TM software drops into existing deployments. By this phase, the predictive methods are expected to have an even greater level of confidence due to the ability to baseline against the current workload experienced for that TM deployment. The changes in variables can be inputted into the predictive model to determine whether the workload of the system will be higher, lower, or unchanged due to the changes required. Therefore the need for extensive simulation and prototype reviews may not be required. However, if a training system is still available from development stage, the updated software could be added to the existing training system to simulate how tasks or processes may be required to change as a result of the system update.

6.3.7 Workload Measurement Techniques for Traffic Management

During each of the In2Rail Toolset Phases 1, 2 and 3, there are a number of different times when workload measurement assessments were required. These were indicated by the green boxes in figures (from Figure 6.3 to Figure 6.5). This section describes how to conduct these workload assessments. Figure 6.7 provides guidance on how an individual workload assessment could be run and gives examples of the types of workload assessment methods that should be used to measure workload. This builds upon best practice as captured in the Workload Appendix.

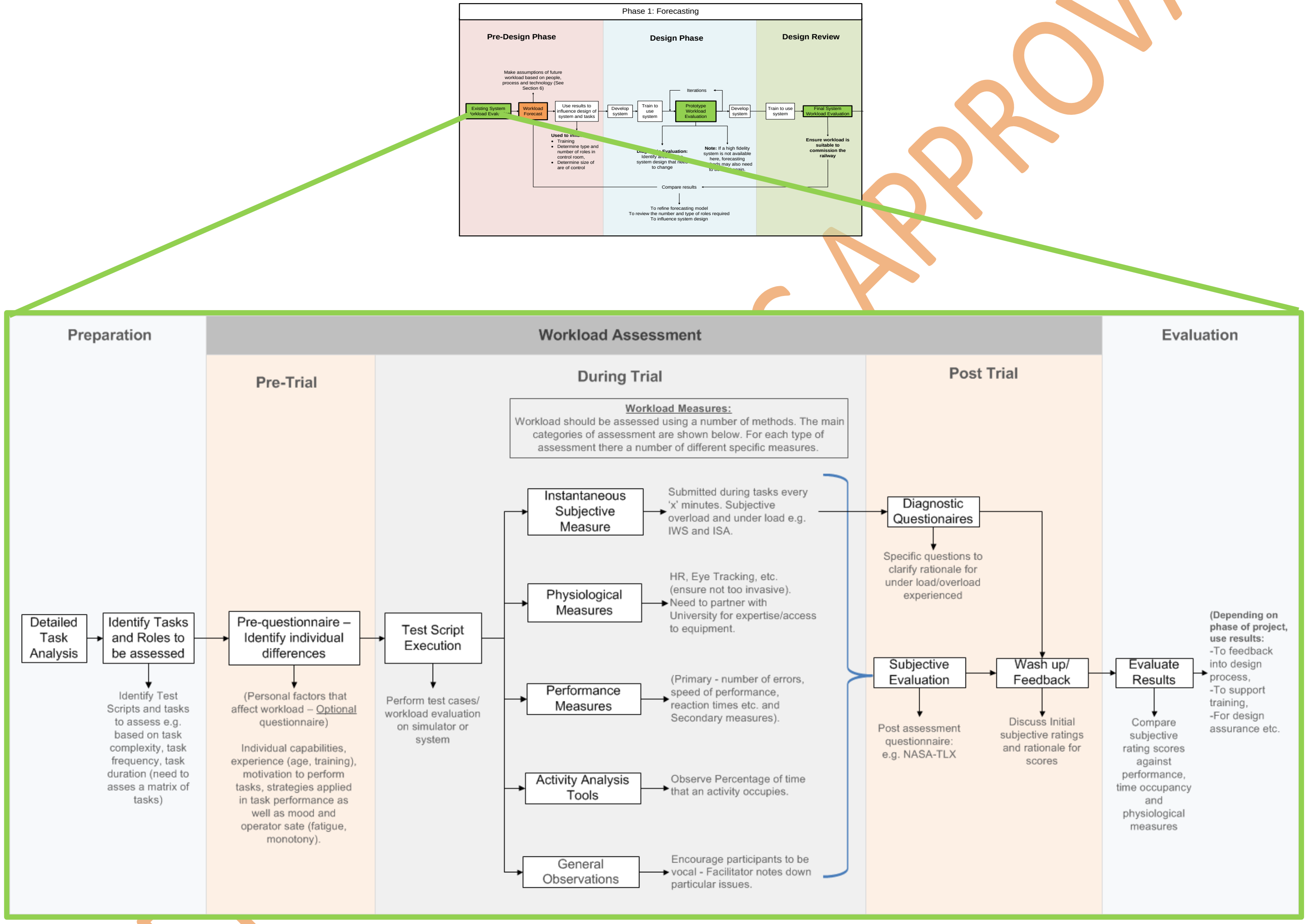

Phase 1: Forecasting
Pre-Design Phase
Design Phase
Design Review
Make assumptions of future workload based on people, process and technology (See Section 6)
Existing System Workload Evaluation
Workload Forecast
Use results to influence design of system and tasks
Develop system
Train to use system
Iterations
Prototype Workload Evaluation
Develop system
Train to use system
Final System Workload Evaluation
Used to influ...
• Training
• Determine type and number of roles in control room,
• Determine size of are of control
Diagnostic Evaluation: Identify areas of the system design that need to change
Note: If a high fidelity system is not available here, forecasting methods may also need to be ... again.
Ensure workload is suitable to commission the railway
Compare results
To refine forecasting model
To review the number and type of roles required
To influence system design
Preparation
Workload Assessment
Evaluation
Pre-Trial
During Trial
Post Trial
Workload Measures:
Workload should be assessed using a number of methods. The main categories of assessment are shown below. For each type of assessment there a number of different specific measures.
Detailed Task Analysis
Identify Tasks and Roles to be assessed
Identify Test Scripts and tasks to assess e.g. based on task complexity, task frequency, task duration (need to asses a matrix of tasks)
Pre-questionnaire – Identify individual differences
(Personal factors that affect workload – Optional questionnaire)
Individual capabilities, experience (age, training), motivation to perform tasks, strategies applied in task performance as well as mood and operator sate (fatigue, monotony).
Test Script Execution
Perform test cases/ workload evaluation on simulator or system
Instantaneous Subjective Measure
Submitted during tasks every 'x' minutes. Subjective overload and under load e.g. IWS and ISA.
Physiological Measures
HR, Eye Tracking, etc. (ensure not too invasive). Need to partner with University for expertise/access to equipment.
Performance Measures
(Primary - number of errors, speed of performance, reaction times etc. and Secondary measures).
Activity Analysis Tools
Observe Percentage of time that an activity occupies.
General Observations
Encourage participants to be vocal - Facilitator notes down particular issues.
Diagnostic Questionnaires
Specific questions to clarify rationale for under load/overload experienced
Subjective Evaluation
Post assessment questionnaire: e.g. NASA-TLX
Wash up/ Feedback
Discuss Initial subjective ratings and rationale for scores
Evaluate Results
Compare subjective rating scores against performance, time occupancy and physiological measures
(Depending on phase of project, use results:
-To feedback into design process,
-To support training,
-For design assurance etc.

Figure 6.7: Workload Measurement Assessment Guidance

Although the workload measurements methods described in Figure 6.7 are not expected to need to be modified too much in order to be suitable for the measurement of workload for TM systems, there are some elements to consider.

The most common workload measurement techniques where there is most supporting evidence in rail are subjective tools, activity analysis tools, performance measures and general observations. However, there is less supporting literature that uses physiological methods as a measure for workload in rail. This may be because these methods can often be more intrusive. Therefore, although these methods could be suitable for prototype or training system evaluations, they may not be suitable for a live railway. As a result, physiological measures may need to be adapted to enable them to be used on an operational railway in order to be a technique that could be used to continuously monitor a user's workload during operation.

Subjective rating scales such as instantaneous subjective measures could also be developed to be built into the system itself so that the user can input their experienced level of workload electronically whenever the system requests it. This would support facilitators during the evaluation phase as it reduces the demand on the facilitators in terms of data collection. Digitalising IWS type tools would also support continuous improvements as it would enable workload scores to be continually collected and evaluated during operation to improve processes to reduce the number of high workload experiences.

There is also a need to consider the change from fixed areas of control to flexible areas of control and the increase in collaborative pod working. This will add to the complexity of measuring workload and therefore existing workload measurement techniques may need to be adapted to effectively measure these changes.

6.4 Assessment of Forecasting Element of In2Rail Toolset

This section provides key consideration and an explanation of the variables in the forecasting model. It also provides an evaluation of the forecasting element of the In2Rail Workload Toolset against the TMS 1st deployment project in the UK.

6.4.1 Description of Forecasting

For the initial deployment(s) of TM forecasting will be required to take place or determine future levels of workload based on assumptions of known changes related to equipment or technology changes, role and task changes. These forecasts will then be used to influence the number of roles required, the design of the system itself and training required.

So in order to forecast the future level of workload, the variables that we expect to effect workload in the future need to be defined. In order to ensure the forecast of expected workload is complete; the variables should be defined based on the entire system as defined in Figure 6.1.

Variables that affect the system's ability to cope with the objective demands of environment are:

- People;
- Process;
- Technology.

Variables that affect the objective demands of environment are:

- Operational Environment;
- Control Room Environment.

6.4.1.1 People

- **Experience:** What experiences do they have in TM systems? What experiences do they have in using predictive systems?
- **Training:** What level of training is required for individuals to be able to use TM effectively? Is there a generational gap with regards to ease of learning new technologies? What novel methods or tools for training are available to utilise? Can the training needs' be reduced through simple, user friendly, easy to use HM's that draw upon gaming or consumer design principles?
- **Competence:** How competent are individuals in using traffic management systems? How competent are individuals at working as part of a team? What are their non-technical skills? Is someone a novice or an expert? How mature is their local knowledge, system knowledge and rules knowledge?
- **Fatigue:** Are the patterns of shift work designed to reduce fatigue? Do the normal operations of the role generate high levels of physical or cognitive strain that could result in fatigue? Are there wider factors such as commuting time or pressures outside of work which could affect their experiences of workload?

- **Culture:** Are individuals supported if they are over or under loaded? How do individuals get support if they are overloaded?
- **Roles:** Are there a sufficient number of roles? What should the type of roles be?
- **Shift Patterns**: How long has a user been working for? Has a sufficient hand over occurred?

6.4.1.2 Process

- **Communication:** What are the changes in communication required to support team working?
- **Team working:** how is team working managed? Does team working to problem solve reduce workload in some circumstances, but increase it in others? Does shared responsibility spread the effect of workload?
- **Process and Procedures:** Are processes well defined to reduce miscommunication, duplication of effort or complacency? Are the allocations of functions efficient?

6.4.1.3 Technology

- **Automation:** What is the effect of new technologies level of automation on workload? Does automation reduce some experiences of workload but increase other areas? Does automation lead to complacency and errors? Do the tools support conflict detection? What is the complexity and frequency of conflict detections?
- **Usable Interface:** Does the HMI support the user in their decision making process? Does the HMI present the right users, with the right information at the right time? Is the HMI easy to use?
- **Equipment Layout:** Is equipment in an accessible location? Is equipment arranged to match the limitations of the user?

6.4.1.4 Operational Environment

Operations:

- **Areas of Control (AoC):** How does the change from fixed to flexible areas of control effect workload? How do you define what is a suitable workload for each workstation when each area of control may have a different level of associated workload?
- **Tasks:** Have the number of tasks, the types of tasks e.g. complexity and the frequency of tasks changed? How does the change from reactive to proactive tasks effect workload?
- **Degraded Modes:** Are the effects of degraded modes supported by TM?

Infrastructure:

- **Track:** Is the complexity of infrastructure staying the same? How can you compare workload across each location or deployment of TM if the size of the geographical area or complexity of infrastructure changes?
- **Assets:** How many points, LX Controls, signals, interlocking's and stations should be in an AoC? Are these assets changing as a result of TM? Does TM help monitor these assets?

Traffic:

- **Traffic:** Has the type and frequency of traffic changed due to TM?
- **Timetable:** Is the timetable conflict free and high in quality?

6.4.1.5 Control Room Environment

- **Lighting:** Can the lighting be adjusted to meet users individual or task needs? Is there glare?
- **Temperature:** Are they comfortable?
- **Noise levels:** Are noise levels increased due to increased communication?

6.4.2 Evaluating the Forecasting Method

To ensure that the considerations and variables in section 6.4.1 were complete and useful to forecast the effects of TM, they were reviewed by Thales and Network Rail against the TMS 1st deployment project in the UK. The output of this review can be seen in Table 6.1 and Table 6.2. The forecasting model aimed to summarise how the changes in system; (people, process and technology), and the operation demands; (Operations, Infrastructure and Traffic) are expected to affect workload and in turn safety and performance.

Variables that affect the system's ability to cope with the objective demands of environment are described in Table 6.2 while variables that affect the objective demands of environment are described in Table 6.3.

A summary of the findings from the evaluation can be seen below:

- The evaluation of the forecasting model showed there a number of areas of workload that may be higher at the start when TM is first commissioned due to lack of experience, such as system knowledge. However over time the effect of this should be reduced and performance should be enhanced;
- In general the experience of workload is predicted to be lower due to increased collaborative problem solving and functions such as flexible areas of control;
- There are a number of areas of high uncertainty that need to be evaluated further once a training or live system is available for testing such as the effects of automation and areas of control.

Workload High Level Variable	Detailed Workload variable	Description of effect on Workload	Summary of Workload Change	Description of effect on Safety or Performance	Recommendations for TM Project
People	Experience	Signalling level of experience or local knowledge is assumed to stay the same however the level of experience of using a TM or integrated system will be low at the start which may increase workload but over time as operators use TM effectively to plan railway in proactive manner, workload will decrease.	Higher then Lower	Potential to reduce performance marginally at the start but then improve over time.	There needs to be a suitable training period to allow operators to learn how to use TM effectively across a range of scenarios.
	Training	It is assumed that a suitable level of training will be achieved by the rail operating company so that operators can effectively use both the TM system and integrated system.	No change	No change	No comment.
		Generational gaps and or experience with novel technologies should be considered and more training may be required for different individuals to ensure their level of workload is suitable when using a new system.	Higher then Lower	Potential to reduce performance marginally at the start but then improve over time.	New technologies should be introduced as early as possible to end users.
		It is assumed that the TMS system will have an intuitive user interface and therefore training needs will be able to be reduced. (Note: If the user interface is not simple, suitable training will be required to ensure that workload is not too high).	Lower (if intuitive interface)	Potential to improve performance (if intuitive interface).	A number of iterations of system design should take place with end users and there should be sufficient time, budget and project support to implement required changes so system is usable.
	Competence	It is assumed that operators will have a suitable level of competence (Technical knowledge, system and route knowledge).	No change	No change	No comment.
		Similar to experience, when operator's first start to use TM, their competence will be lower and will have a greater impact on workload than when they have more experience with the system and their competence is higher.	Higher then Lower	Potential to reduce performance marginally at the start but then improve over time.	There needs to be a suitable training period to allow operators to learn how to use TM effectively across a range of scenarios.

Workload High Level Variable	Detailed Workload variable	Description of effect on Workload	Summary of Workload Change	Description of effect on Safety or Performance	Recommendations for TM Project
	Fatigue	It is assumed that physical fatigue will stay the same due to TM, with the potential to be lowered due to better workstation design	No change/potential Lower	Potential to improve performance.	Workstation design should be introduced as early as possible to end users. A number of iterations of system design should take place with end users and there should be sufficient time, budget and project support to implement required changes so system is usable.
		There is the potential that cognitive fatigue will be higher at the start due to lack of experience in using integrated, complex systems. However, this cognitive fatigue and impact on workload should reduce over time.	Higher then Lower	Potential to reduce performance marginally at the start but then improve over time.	There needs to be a suitable training period to allow operators to learn how to use TM effectively across a range of scenarios.
	Culture	Support from supervisors will be provided such as to reconfigure areas of control due to higher workload; this will spread the effect of workload more easily across the system.	Lower	Potential to improve performance.	This should be managed by process and training. Should assist technologies become mature enough these could be used to support this.
		Work will need to be done to ensure operators are willing to express feelings of over or under load to supervisors so that the system can be reconfigured accordingly.	Lower (if culture changed)	Potential to improve performance.	This should be managed by process and training. Should assist technologies become mature enough these could be used to support this.
	Roles	It assumed that at the start of TM deployment the number of roles will stay the same due to uncertainty and therefore due to the increased automation, workload is expected to be lower in the system. However, due to the changes in roles, and the increased communication required between roles, some elements of workload may increase during certain tasks.	Mostly Lower, (some elements higher)	Potential to improve performance.	This should be managed by process and training. Should assist technologies become mature enough these could be used to support this..

Workload High Level Variable	Detailed Workload variable	Description of effect on Workload	Summary of Workload Change	Description of effect on Safety or Performance	Recommendations for TM Project
	Shift Patterns	The shift patterns are assumed to be the same as today therefore no effect on workload.	No change	No change	No comment.
		Shift handover will need to be carefully managed to ensure that information is clearly past between operators so that have sufficient situational awareness of the system. If this is not managed, workload may increase due to lack of SA and a reduced ability to cope with sudden incidents.	No change (if process supports)	No change (if process supports)	This should be managed by process and training. Should assist technologies become mature enough these could be used to support this.
	Job Design	Job design and flexibility of tasks should enhance motivation and distribute workload across teams more evenly, therefore reducing the workload experience by certain operators in the system.	Lower	Potential to improve performance.	There needs to be a suitable training period to allow operators to learn how to use TM effectively across a range of scenarios to inform effective route operating models.
Process	Communication	It is expected that more communications will be required between roles in the TM pod. Therefore this may increase the communicating element of workload but reduce other elements of workload such as task complexity as tasks will be solved more collaboratively.	Higher	Although workload may be higher for communication, it is not expected that will have a negative impact on performance.	This should be managed by process and training.
	Team Working	It is assumed that team working will be managed effectively and that this will reduce workload in all modes of working, (normal, degraded and emergency).	Lower	Potential to improve performance.	This should be managed by process and training. Should assist technologies become mature enough these could be used to support this.
		Shared responsibilities across the team is forecasted to reduce workload.	Lower	Potential to improve performance.	This should be managed by process and training.
	Process and Procedures	It is assumed that processes and improvements are well defined to support operators during all scenarios.	Lower	Potential to improve performance.	There needs to be a suitable training period to allow operators to learn how to use TM effectively across a range of scenarios to inform effective

Workload High Level Variable	Detailed Workload variable	Description of effect on Workload	Summary of Workload Change	Description of effect on Safety or Performance	Recommendations for TM Project
					route operating models.
		It is assumed that processes will be well defined so that there is no miscommunication between responsibilities so the workload is managed effectively and there is no duplication of tasks or complacency.	Lower	Potential to improve performance.	This should be managed by process and training.
	Rules and Standards	It is assumed that the system meets rules and standards and the rules and standards are sufficient for the specific deployment.	No change	No change	No comment.
Technology	Automation	It is assumed that automation will reduce the number of manual tasks and therefore workload in this area but not completely.	Lower	Potential to improve performance.	The effect of automation needs to be carefully measured when assessing workload of the final system as this is an uncertain variable.
		Until there is full trust in the system, manual interventions will still be required, and will still be required in certain degraded modes. Due to lack of practice in manual tasks, this may increase workload in this scenario.	Higher	This should not lead to safety errors as the system should be prevented by interlocking, however may lead to performance reductions.	The effect of automation needs to be carefully measured when assessing workload of the final system as this is an uncertain variable.
		It is assumed that the automation will keep the human in the decision loop and therefore complacency will not occur and therefore workload will be reduced.	Lower	Potential to improve performance.	The effect of automation needs to be carefully measured when assessing workload of the final system as this is an uncertain variable.
		It's assumed that the number of proactive/monitoring tasks will increase but as they will support decision making to prevent incidents from occurring, workload will be reduced.	Lower	Potential to improve performance.	The effect of automation needs to be carefully measured when assessing workload of the final system as this is an uncertain variable.

Workload High Level Variable	Detailed Workload variable	Description of effect on Workload	Summary of Workload Change	Description of effect on Safety or Performance	Recommendations for TM Project
	Usable Interface	It's assumed that the display is simple and easy to use therefore workload will be no worse than today and potentially less.	Lower	Potential to improve performance.	A number of iterations of system design should take place with end users and there should be sufficient time, budget and project support to implement required changes so system is usable.
		It's assumed that the right information is presented to the right user at the right time supporting their decision making process and therefore reducing workload.	Lower	Potential to improve performance.	A number of iterations of system design should take place with end users and there should be sufficient time, budget and project support to implement required changes so system is usable.
	Equipment Layout	It is assumed that the layout is in accessible location and matches the limitations of the user therefore workload will be no worse than today and potentially less.	No Change to Less	No Change to Less	A number of iterations of equipment design should take place with end users and there should be sufficient time, budget and project support to implement required changes so system is usable.

Table 6.2: Variables that affect the system's ability to cope with the objective demands of environment

Workload High Level Variable	Detailed Workload variable	Description of effect on Workload		Description of effect on Safety or Performance	Recommendations for TM Project
Operations	Areas of Control (AoC)	It's assumed that flexible areas of control will more evenly distribute workload experienced by the system and reduce individual operator's experience of workload.	Lower	Potential to improve performance.	The effect of this needs to be carefully measured when assessing workload of the final system as this is an uncertain variable.
		It's expected that at the start of TM deployment, to reduce risk, AoC's will stay a similar size to today and therefore may not be large enough which could lead to operators being under loaded. It's expected that over time as workload is more understood, operators will control large areas.	Lower	Potential to improve performance.	The effect of this needs to be carefully measured when assessing workload of the final system as this is an uncertain variable.
	Tasks	It's assumed that the types of tasks will change; there will be less manual tasks and more monitoring tasks. There will be a change from reactive to proactive. Although there will be more information to the operator, they can use this to manage the railway and prevent disruptions and therefore reducing their workload.	Lower	Potential to improve performance.	The effect of this needs to be carefully measured when assessing workload of the final system as this is an uncertain variable.
	Degraded Modes	It is assumed that the effects of degraded modes are supported by TM by presenting the right information at the right time to the right user.	Lower	Potential to improve performance.	A number of iterations of alarm design should take place with end users and there should be sufficient time, budget and project support to implement required changes so system is usable. The training system should be used to further develop the design.
Infrastructure	Track	The infrastructure is staying the same therefore no change to workload.	No Change	No Change	No comment.
	Assets	The assets are not changing and the areas of control are staying the same to start with therefore no change to workload.	No Change	No Change	No comment.

Workload High Level Variable	Detailed Workload variable	Description of effect on Workload		Description of effect on Safety or Performance	Recommendations for TM Project
		Information is provided about failed assets via alarms which should reduce impact of incidents as operators will be able to respond quicker and more effectively and therefore reduce workload.	Lower	Potential to improve performance.	A number of iterations of alarm design should take place with end users and there should be sufficient time, budget and project support to implement required changes so system is usable. The training system should be used to further develop the design.
Traffic	Traffic volume	The type and frequency of traffic has not changed due to TM therefore no change to workload.	No Change	No Change	No comment.
	Timetable	It is assumed that the timetable quality is high and therefore workload is made no worse than today.	No Change	No Change	No comment.
		Due to features such as conflict resolution detection, the management of the timetable should be enhanced, reducing delays and therefore reducing workload.	Lower	Potential to improve performance.	The effect of this needs to be carefully measured when assessing workload of the final system as this is an uncertain variable.
Control Room Environment	Lighting	The lighting in the control room will be assessed so that it does not affect the use of the system, therefore no change to day.	No Change	No Change	No comment.
	Temperature	The temperature in the control room will be assessed so that it does not affect the use of the system, therefore no change to day.	No Change	No Change	No comment.
	Noise	The noise in the control room will be greater due to increased communication which may increase the feeling of workload. However, this is mitigated by the room layout to ensure the correct operators are located next to each other.	Higher	Although workload may be higher for communication, it is not expected that will have a negative impact on performance.	Room layout should ensure the correct operators are located next to each other. Interaction between roles should be assessed during workload assessments.

Table 6.3: Variables that affect the objective demands of environment

6.4.3 Next Steps to Develop Forecasting Model

The next steps to develop this forecasting method are out of scope for subtask 7.2.5, however, suggested steps for future In2Rail deliverables are:

- When a training system is available and or live system, the workload of the system should be measured. The workload assessment should include all elements in the In2rail forecasting model;
- The data captured from the workload assessment should be compared against the forecasting model to clarify assumptions, modify assumptions where required and add additional relevant variables or considerations where required;
- The forecasting model should be continuously reviewed against actual workload data collected until the forecast matches the actual workload measured from the system;
- Once the forecast model has reached a steady state it will form the predictive model that will be used to influence future TM deployments with a higher level of confidence.

7 Conclusions

7.1 Overall Conclusions

The key objective of task 7.2 was to define the Specification for Traffic Management (TM) "Standard Operator's Workstation" allowing the user to display and manage all services and functions applied in an integrated Traffic Control Centre.

The overriding findings from this report are that systems of the future will need an increase in flexibility in order to adapt to the:

- Changing operational cultures to use more flexible roles;
- Changing operational conditions to contain more flexible scenarios;
- Rapid advances in technology that should be utilised to solve current and future user needs;
- Increasing need for cyber security to be integrated into the entire lifecycle of system design through to operation;
- Use of automation and intelligent systems and their effect on workload.

This document provides recommendations in how to achieve the above via the potential new roles, design processes, current industry guidance or by use of future technologies.

7.2 Considerations for Future TM Workstation Design

This section of the report provides a set of principles and guidelines for the design of a future TM Operator's Workstation and HMI for the display and management of all services and functions applied in an integrated Traffic Control Centre.

At this stage of In2rail and TM system development; it is challenging to define a final TM Workstation as there are many uncertainties with respect to the most appropriate technology to be used, roles and tasks required by operators and the exact functions of the system required. As well as this, technology is constantly changing, roles and tasks are likely to change from what we expect today and may be different across countries and finally the budget and scope for workstation design is different for each deployment. Therefore a number of concepts have been developed to enable a road map of future workstations to be produced based on technological readiness and cost.

The advantages and disadvantages of each concept were evaluated during the Concept Review Workshop and are discussed in order to provide guidance to operating companies or future deployments of Traffic Management. Future deployments of Traffic Management, and through Shift2Rail, can then select principles from each concept that are applicable to and support that specific project requirements and user needs. It should be noted that it is important to keep a holistic view of the application of the technology in the context of the railway and also how it relates to people and process. Therefore the selection of technologies should be based around the user needs and ensure they enhance the safety and performance of the railway.

A number of different HMI layouts are proposed for each user role and the rationale for the applications they are expected to require are captured. However the next step is to ensure a detailed list of tasks are generated for each user role that are made possible with the technologies selected. The detailed task list should then be compared against the user needs to ensure that the technologies selected have a real benefit to both the user and business needs.

It is predicted at this stage that technologies such as integrated desktops, increased automation and intelligent systems or artificial intelligence is where the value proposition will be as it will enable a holistic and meaningful view of the railway to be created to enable effective decision making and management of the railway.

The next steps to develop the HMI and workstation concepts in this report should be to review the concepts and technologies with wider stakeholders. Once the value proposition is further defined from the technologies discussed, a multidisciplinary team of experts will then be required to develop a proof of concept to prove the solutions are affordable to rail operating companies and provide a real benefit.

7.3 Specification of Security Measures

The review of security measures proposes a methodology that builds upon a traditional Information Security Management System to create a railway specific Railway Information Security Management System. The need for this is ever increasing, as railways, networks and partners attempt to work in a more collaborative manner to increase the capacity and efficiency of the railway. This increase in collaboration means that information needs to be shared digitally which increases the risk of cyber-attacks.

The main aim of the Railway Information Security Management System is to provide mechanisms, processes and methodologies to eliminate or minimise the probability of an attack, the ability for an attack to be successful and the impact of a successful attack. It also highlights the fact that security does not just depend on technology and system design but people and processes within an organisation have a major role to play in ensuring a system is secure.

The process of identifying risks and eliminating or minimising them through system design or via a process is not a one shot process. System and process design should be continuously reviewed both during development of Traffic Management systems, but also, during operation to ensure the vulnerability of a system is continuously reviewed. This is to ensure that lessons are learnt from any attacks that have occurred in a suppliers Traffic Management system or any similar Traffic Management Systems to prevent future attacks from occurring.

7.4 Workload Analysis for Operators

Being able to accurately measure and predict operational workload means that control centres of the future can be appropriately sized and manned. The findings from the workload tool set proposes a comprehensive set of techniques that can be used to measure workload. It then shows how these measurements can be used to predict the impact on staff or future systems so that changes can be proposed, evaluated and decided upon in a controlled manner.

Across many sources of workload literature, there is much dispute around the definition of workload and methods in which best quantify the experience of workload. Therefore this report provides a generic definition of workload and defines key principles of workload to consider. It then describes advantages and disadvantages of the main types of generic workload measurement techniques; physiological, subjective and performance measures of workload.

There is a large amount of supporting literature regarding workload measurement techniques for the signaller role using conventional rail systems. However, as a result of the development of TM systems there will be a number of factors of workload that change from conventional rail signalling systems. Therefore the report describes how the introduction of TM will increase the complexity of how workload is predicted and measured.

It is important to clearly identify the workload variables and how they might change as a result of TM in order to influence system design, task design and process design. Based on the expected changes in workload variables, it was necessary to define an In2Rail toolset to forecast and measure workload in future TM systems. It should be noted that during this project phase of In2rail, it is difficult to define a detailed workload toolset as there are still a number of unknown variables in future technology used and role changes required. Nevertheless, it is useful to develop a generic tool set which draws upon established workload principles from supporting literature as well us current TM projects. This is to ensure that the system and workstation design meets the operational future needs of control rooms, taking into account workload principles and Human Factors best practice.

The In2Rail Tool set was developed in order to reach a stage where we are able to make predictions of workload for future TM systems with a higher level of confidence. The toolset also highlights where existing rail workload measurement techniques need to be adapted in order to support continuous development of people, process and technology.

7.5 Closing Comments

The completion of this report has captured best practice in Workstation Design, Security Management Systems and Operator Workload in the context of Traffic Management Systems. It provides recommendations in how to achieve the key findings either through the development of role and process design, system or workstation design and through the use of future technologies.

It is expected that as different technologies continue to develop in maturity and their respective value propositions are determined, concept of operations will also continue to evolve to make use of the technology available in any given deployment of TM. Therefore the recommendations in this report should be reviewed for each deployment of TM to ensure they meet the needs of the project and most importantly the end user.

8 References

As well as the references discussed in each respective section of the report, the below references have been used. It should be noted that the references section is split into two sections, references for section 4: Considerations for Future TM Workstations and references for section 6: Workload Analysis for Operators.

Section 4: Considerations for Future TM Workstations

[1] NR Signalling Centre Desks - NR/SP/ERG/00005: April 2007.

[2] CGM: http://www.cgm.se/.

[3] Rolls Royce future shore control centre. [Online]. Available at: http://www.rolls-royce.com/media/press-releases/yr-2016/pr-2016-03-22-rr-reveals-future-shore-control-centre.aspx.

[4] Hedge A, 2004, Effects Of An Electric Height-Adjustable Worksurface On Self-Assessed Musculoskeletal Discomfort And Productivity In Computer Workers, Cornell University Human Factors and Ergonomics Research Laboratory

[5] National Health Service, 2014. NHS Choices – Why sitting too much is bad for your health: http://www.nhs.uk/Livewell/fitness/Pages/sitting-and-sedentary-behaviour-are-bad-for-your-health.aspx

[6] Just Stand.Org, 2015. – Online Calorie Counter (http://www.juststand.org/tabid/637/default.aspx)

[7] National Health Service, 2014. NHS Choices Health A-Z, Obesity (http://www.nhs.uk/Conditions/Obesity/Pages/Introduction.aspx)

[8] Roelofs, A. and Straker, L., 2002. The Experience of Musculoskeletal Discomfort amongst Bank Tellers Who Just Sit, Just Stand or Sit and Stand at Work, Ergonomics SA, 14 (2), 11-29.

[9] Paul, R.D. and Helander, M.G. 1995. Effect of Sit-Stand Schedule on Spinal Shrinkage in VDT Operators, Designing for the Global Village. Proceedings of the Human Factors and Ergonomics Society 39th Annual M

[10] Chau et al. BMC Public Health 2014. Desk-based workers' perspectives on using sit-stand workstations: a qualitative analysis of the Stand@Work study

[11] Neuhaus M et al, 2014. Workplace Sitting and Height-Adjustable Workstations – A Randomised Controlled Trial

Section 6: Workload Analysis for Operators

[1] O'BRIEN, Thomas G. CHARLTON, Samuel G. Handbook of human factors testing and evaluation. New Jersey: Lawrence Erlbaum associates 1996.

[2] Anonymous. Workload [online]. Viewed 26.11.13. Available from: http://www.thefreedictionary.com/workload.

[3] WICKENS, Christopher D. GORDN, Sallie E. LIU, Yili. An introduction to Human Factors Engineering. 3rd Edition. Addition-Wesley Educational Publishers. Chapter 13 pages 388-394.

[4] ISO 10075-2 - Ergonomics principles related to mental workload - Design principles.

[5] ISO 10075-3 - Ergonomics principles related to mental workload - Measuring & assessing.

[6] Human Factors Methods: A Practical Guide for Engineering and Design – Chapter 8.

[7] W/INDEX: A predictive model of operator workload, Robert A. North.

[8] Fundamental examination of mental workload in the rail industry.

[9] Development and implementation of a predictive tool for optimising workload of train dispatchers, *Melcher Zeilstra et al, Integro, The Netherlands.*

[10] Sarah Miller, Literature Review – Workload Measures – 2001.

[11] NRTMS Traffic Management – Workload Assessment Tools and Process - NR/TM/PRO/RPH/0016: 2013.

[12] Network Rail Ergo tools [online] - Signaller Workload Toolkit. Available from: http://ergotools.co.uk/SWT/.

9 Appendices

9.1 Security

Sections 9.1.1– 9.1.4 contains a more detailed description of key principles to consider in relation to security as stated in section 5.1.

Section 9.1.5 contains a more detailed description of standards to consider in relation to security as stated in section 5.1.

9.1.1 Threat Definitions

There are a lot of definitions and interpretations for the concept of a threat. This is because threat is used differently in different contexts and the approach is very different at each case.

One extended definition of a threat is "A statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done".

A threat regarding information managed in systems is a cyber-threat. One extended definition made by the US Department of Homeland Security "any identified effort directed toward access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or a federal system, without lawful authority".

It is important to note that a threat can be a combination of a cyber and physical attack, for example, a physical intrusion into the control centre of an infrastructure and a modification of the software within it. This would be an intentional cyber and physical attack. Or, when authorized personnel do not follow procedure to check the infrastructure, and the infrastructure generates and transmits incorrect data. This is both a cyber and unintentional physical attack.

A cyber threat can be intentional or unintentional, targeted or non-targeted, and can come from a variety of sources, including: foreign nations engaged in espionage and information warfare; criminals; hackers; virus writers; and disgruntled employees or contractors working within an organization.

- **Unintentional threats** can be caused by inattentive or untrained employees, software upgrades, maintenance procedures and equipment failures that inadvertently disrupt computer systems or corrupt data;
- **Intentional threats** include both targeted and non-targeted attacks:
  - A targeted attack is when a group or individual specifically attacks a critical infrastructure system,
  - A non-targeted attack occurs when the intended target of the attack is uncertain, such as when a virus, worm, or malware is released on the Internet with no specific target;

The attacker that causes the threat is other way to classify the different types of threat:

- **Natural disaster:** these include severe floods, earthquakes, snow, and ice storms, hurricanes and other hazardous natural processes that may disturb the business continuity of an airport or even completely shut down businesses for an indefinite amount of time;
- **Unknown attacker:** It could be a group or a single person that try to make any disruption at the service. This is a generic actor and the control systems of the infrastructures must provide mechanism to detect this kind of intrusions, and mitigate the effects. These attacks are taking place all around the world almost every minute and the targets vary from banking systems to e-mail servers or to control systems of several kinds of industries;
- **Known attacker:** The most worrisome threat is the "insider", someone who has authorized and legitimate access to a system or network. Other malefactors may make use of insiders, such as organized crime or a terrorist group suborning a willing insider, or making use of an unwitting insider. These kinds of threats can be guarded against and deterred by an organization via a security policy, by authentication mechanisms and physical controls with restricted proximity card access;
- **Malfunction and unintentional human error:** Sometimes the systems may suffer from random errors or accidental failures like power loss, equipment shutdown or damage, loss of internet and phone lines; this type of incident would be called a malfunction and unintentional human error.

9.1.2 Types of Attackers

There are a lot of different classifications of potential attackers. One of the most frequently classification on studies of cyber security is the following. There are five levels of potential attackers, the first level is formed by attackers with lowest the expertise level and the fifth level is formed by the highest expertise level:

- Level 1 - Cyber vandalism: Adversaries with very limited expertise; non-targeted attacks, primarily focused on organization's perimeter;
- Level 2 – Cybercrime: Adversaries with limited technical expertise; intent is to acquire critical information;
- Level 3 – Cyber surveillance: Adversaries with moderate expertise capable of launching multiple attacks, seek to gain foothold in the organization's infrastructure;
- Level 4 – Cyber espionage: Sophisticated adversaries, capable of multiple, coordinated attacks, able to establish persistent footholds within the organization's infrastructure;
- Level 5 – Cyber warfare: Very sophisticated adversaries, capable of multiple, coordinated, continuous attacks.

All these possible attackers can be external or internal staff. The attackers that are internal staff too can be the most dangerous attacker because they can have a lot of information about the security system and the operational actions that are part of the information security management system. This knowledge can be very important for the attackers to be able to enter the system, and most importantly, to be able to come and go undetected.

One important action to start the analysis of the possible vulnerabilities of a system or a critical infrastructure is to identify these different groups of possible attackers that could pose a risk, and this needs to be done through a thorough threat assessment.

A definition of a "threat actor group" is *a group of people who can reasonably be considered to have the same characteristics in terms of capability, motivation and opportunity to perform an attack*.

For example, an organisation's set of cleaners may be grouped together as one threat actor group, rather than conducting a threat assessment for each individual cleaner. The IT department staff of an enterprise can be considered as another group and even the security department staff can be considered as another different group. These three example groups are very different because they have different knowledge characteristics different access level to the infrastructure system. For example, usually the cleaners group has less technical knowledge than the IT staff but they can access all the floors and rooms of the building. These access privileges should be taken into account when the security system is being designed.

It should be noted that the classification of external staff is more difficult and requires more effort to be able to make an analysis of all possible types of involved actors.

When all the groups are identified, the next step is to inform to each one about their security responsibilities. Part 7 of the ISO 27002 standard provides controls relating to human resources security and ensures that the employee understands, is aware of and fulfils his security responsibilities. This also ensures that only those employees with the right personality and motivations are identified for certain roles. This is done through screening, testing, awareness education and training, as well as having in place the disciplinary processes to deal with an employee who commits an information security breach. The ISO standard provides for the basic controls; any residual risk can be minimised by a number of other controls, such as restricting access to certain employees and thereby limiting their capability to be a risk.

One extended methodology to make this task more effective to identify and classify the different groups that interact with the system is to take into account the different access modes that the system has. The identified groups are:

- **Normal users:** these are the users that use the system and access to the information that is managed by the system. They use the information that the system provide but without special access right or permissions;
- **Advanced users:** these are the group involved in the configuration and admin tasks within the system, e.g. system specialists, administrators or configuration managers.

They have special access rights and can be involved at hardware administration, system configuration operations or security control tasks;

- **Service consumer:** they are the group of people or external systems that consumes or uses the information provided by the system, but they cannot modify the managed information. They are not part of the systems or staff that provides information to the system;
- **Indirect consumer:** they are external systems or external personnel that exchange information with a system that is connected to the system. This group can use the information provided by the system but indirectly and usually the system doesn't know about these systems. They are considered as unauthorized systems but can access to the information indirectly by other authorized system,
- **Handlers:** this is the group of people required to handle, transport, supply or deliver the systems e.g. the designers, developers and testers of the system;
- **Service providers:** this usually interacts with the system through a service level agreement and contractual processes. They are the providers of a service or of specific software that is used by the system;
- **Beholder:** these are users that may have been granted physical access to areas but with no access rights to the systems or information. Cleaners, visitors or maintenance personnel would typically fit this group.

The first responsibility of the security department is to classify the internal and external potential attackers as one or several of these groups with the main aim to design mechanisms to mitigate the possible attacks of each one.

9.1.3 Motivation to Attack a System

The motivations to try to execute an attack are very different but at a high level can be classified into two types of actions:

- **Intentional:** people carry out negative actions for different reasons, often based on their motivations. Motivations can be influenced though communications, education, money, beliefs, etc. However, "negative" beliefs are hard to change and can only be identified through screening and monitoring. Third parties can influence the motivations of people through direct contact and persuasive communication. The motivation of intentional actions in attacks may emerge from a variety of sources – a foreign State or terrorist, criminal, or social-issue organisations. Threat agents performing such intentional actions may be unauthorised entities or insiders, and their primary objective is to engineer potential hazards and performance losses in the system;
- **Unintentional:** how people behave is also influenced by motivations and personality. This can be due to lack of care, lack of pride, lack of training, time pressures, a belief they know better. This kind of attacks are more frequently between internal staff but can be executed by external personnel.

Following the previous classification of potential attackers, we can try to find the different motives to plan and execute and attack to the system:

- Level 1 - **Cyber vandalism:** the aim of the attacks are not directly to provoke damage, they are seeking access to the system to show that the system is vulnerable;
- Level 2 - **Cybercrime:** this group try to get information managed by the system but without a concrete aim, they try to demonstrate that they can access to this system when they want. Usually this kind of person wants the security department to know the existence of the attack but not know how they are doing it;
- Level 3 - **Cyber surveillance:** the motivation at this level is access to the system to produce damage. They are looking for a break in the service provided by the system or to damage the public image of the organizational owners of the system. Usually they are funded by other group and they provide the technical knowledge to execute the attack;
- Level 4 - **Cyber espionage**: the motivation of this group is to get important information managed by the system with the aim to obtain a benefit using or selling it to other group. The information theft may also carry a loss in the service provided by the system;
- Level 5 - **Cyber warfare:** this level of actors has the motivation to gain the control of the system, not only the information managed, but they want to take complete control of the operation. Usually they make continuous attacks to try to break the security barriers and try to get control of the system.

There are other common motivations for the attacks that don't correspond to a concrete group; these reasons are political or ideological causes.

Infrastructure control systems are potentially one of the most exposed systems to these kinds of attacks because the consequences of the attacks are larger and have bigger repercussions.

The real impact of an attack can be classified taking into account the importance of the effect of the attack, it is not necessary to collapse of the entire system, but a reduction of the capacity of a system can be a disaster because the customer perception of the service provided can be catastrophic.

In a TMS the loss of operations for any period of time or a reduction of throughput, would seriously harm the business. Other kinds of attacks to a TMS such as the leakage or destruction of data is also very attractive because usually there is a lot of information managed by the system that is private because it has a security component.

Attacks that are successful require time to be solved; this time inevitably leads to a financial loss. For example if there are delays or cancellation of trains the railway often has to give economical compensations to the passengers. Furthermore, this situation would be aggravated by the press and have an immediate negative effect on social media. This is can result in the loss of potential passengers in the future due to the quality of service provided.

9.1.4 Threat Mitigations

There are a number of different threats and the sophistication and resources available to attackers are so great that this problem cannot be addressed with a single solution, nor can it be addressed only at a single point in time. The tools, tactics, and strategies of attackers at all levels are readily available and will continue to evolve, and the threat will continue to increase. It would be naive to believe that the proliferation of these tools can be controlled through legislation or regulations. Responding effectively to the threat will require a long-term commitment from senior leadership to an on-going process of building and operating increasing levels of information system security capabilities.

All the current methodologies of Information Security Management Systems has two method to mitigate the threats:

- Decrease the probability of an attack;
- Minimizing the negative effect of an attack.

Once the mechanisms are established to mitigate the threats, it is important to know how to respond to an attack but the first step is to have attack detection mechanisms.

Taking into account the potential attackers identified in previous sections, security departments need to design specific mechanisms to mitigate the impact of an attack and / or reduce their probability of occurrence for each attack group.

To mitigate a typical attack from each identified group of potential attackers it is necessary to take into account the following mechanisms:

- Level 1 - **Cyber vandalism:** defences at this level are focused on establishing a perimeter around an organisation's information system infrastructure, and defending that perimeter using firewalls and other commercially available tools like antivirus software;
- Level 2 - **Cybercrime:** defences at this level include protecting information and systems not just at the perimeter but wherever it resides within the enterprise, using techniques such as encryption of wireless traffic and hard drive encryption;
- Level 3 - **Cyber surveillance:** defence at this level requires continuous internal monitoring and system hardening throughout the enterprise;
- Level 4 - **Cyber espionage:** defence at this level requires an enterprise architecture that can impede an attacker's actions within the organisation's information system infrastructure and ensure continuity of critical mission operations;
- Level 5 - **Cyber warfare:** defence at this level requires agility, adaptation, and flexibility to dynamically reshape operations and maintain mission continuity even while under continuous attack.

To help organise efforts for responding to the cyber threat, most relevant international standards suggest applying an approach that divides the on-going security process into four complementary areas or phases that are the breakdown of an Information Security Management System.

9.1.5 International Standards References for Security

In the following section the below standards and other security frameworks are described:

- ISO 27000 series;
- ISO/IEC 17799:2005;
- Cyber security Framework of the US Commerce Department's National Institute of Standards and Technology (NIST).

9.1.5.1 ISO 27000 series

The ISO 27000 was published in May 2009 and was revised at December 2012 and at January 2014. This series of standards provides an overview of the rules that comprise the 27000 series, indicating for each its scope of action and purpose of publication. Collect all the definitions for the 27000 series of standards and provides the basis for why it is important to implement an Information Security Management System, an introduction to ISMS, a brief description of the steps for setting, monitoring, maintaining and improving an ISMS.

The ISO 27001 standard, originally published in October 2005 and revised at September 2013, provides the specification for an information security management system (ISMS). The objective of the standard is to "provide requirements for establishing, implementing, maintaining and continuously improving an ISMS". Regarding its adoption, this should be a strategic decision and is influenced by an organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization. While the 2005 version of the standard heavily employed the Plan-Do-Check-Act (PDCA) model to structure the processes, the latest 2013 version places more emphasis on measuring and evaluating how well an organization's ISMS is performing.

The ISO 27002 standard, also published in 2005 and re-published at July 2007, provides a code of practice for information security and outlines the potential controls and control mechanisms, which may be implemented, subject to the guidance provided within ISO 27001.

The ISO 27003 published in February 2010, it is a guide that focuses on the critical aspects needed for successful design and implementation of an ISMS ISO / IEC 27001 agreement: 2005. Describes the specification and design process from conception to implementation of implementation plans and the process of obtaining approval by management to implement an ISMS.

The ISO 27004 published in December 2009, it is a guide for the development and use of metrics and measurement techniques applicable to determine the effectiveness of an ISMS and controls or groups of controls implemented to ISO / IEC 27001.

The ISO 27005 published in June 2011, provides guidelines for risk management in information security. It supports the general concepts specified in ISO / IEC 27001: 2005 and is designed to help the successful implementation of information security based on a risk management approach. The ISO 27005 standard does not provide or recommend a specific methodology, but provides an overview of the Information Security Risk Management process including risk assessment, risk treatment, risk acceptance, risk communication and risk monitoring and review.

The ISO 27006 published in March 2007 and revised in December 2011, specifies requirements for accreditation of entities of audit and certification of information security management systems.

The ISO 27007 published in November 2011, it is a guide to audit an ISMS, in addition to that specified in ISO 19011.

The ISO 27008 published in October 2011, it is a guide of audit the selected controls within the framework of implementation of an ISMS.

9.1.5.2 ISO/IEC 17799:2005

ISO/IEC 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:

- Security policy;
- Organization of information security;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development and maintenance;
- Information security incident management;
- Business continuity management;
- Compliance.

The control objectives and controls in ISO/IEC 17799:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 17799:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

9.1.5.3 NIST Cyber security Framework

The *Framework for Improving Critical Infrastructure Cyber security* was drafted by the US Commerce Department's National Institute of Standards and Technology (NIST), and was released in February 2014. It does not introduce any new standards or concepts but rather it leverages existing cyber security practices that have been developed and refined by other organizations, not limited to but including the International Organization for Standardization (ISO).

The framework itself comprises a risk-based compilation of guidelines that can help organizations identify, implement, and improve cyber security practices, and creates a common taxonomy for internal and external communication of cyber security issues, as well as an assessment mechanism which enables organizations to determine their current cyber security capabilities, a target 'state', and a plan for improving and maintaining their cyber security capabilities. The framework is also an iterative model that is designed to evolve and adapt with changes in the cyber security threat landscape, including new processes and technologies.

The framework assessment mechanism contains three key elements:

- **Core:** The Framework Core defines standardized cyber security activities, desired outcomes, and applicable references, and comprises five Functions that can be performed concurrently and continuously: Identify, Protect, Detect, Respond, and Recover. The Framework Core, in effect, describes the continuous cycle of business processes that constitute effective cyber security;
- **Implementation Tiers:** are used to create a context within which organizations can better understand how their current cyber security capabilities stand against the characteristics described by the NIST Framework. The tiers can be seen in the table below – NIST recommends that any organization planning to develop effective cyber security capabilities should be aiming to progress to Tier 3 or 4;
- **Profile:** the profile aspect of the framework recognizes that different industries and organizations have different business needs, operating models, risk appetites and available resources for developing a robust cyber security programme. The profile enables organizations to align and improve their cyber security practices based on their individual circumstances. A current and target profile can be defined and a comparison of these states can be used to identify the gaps that should be closed in order to enhance cyber security and provide the basis for a prioritized roadmap to help achieve these improvements.

9.1.6 International Programs to Improve Security

9.1.6.1 The European programme for Critical Infrastructure Protection (EPCIP)

The general objective of EPCIP is to improve the protection of critical infrastructures in the EU. This objective will be achieved by the creation of an EU framework concerning the protection of critical infrastructures which is set out in this Communication.

The three main directives follows by this program are:

- Common procedure for the identification and designation of European Critical Infrastructure (ECI);
- Common approach to the assessment of the need to improve protection;
- All-hazards approach, but priority to threat from terrorism.

This programme promotes the application of a framework to try to improve the security at critical infrastructures. The aim of this framework is to provide an action scenario following these key principles:

- **Subsidiarity:** The Commission's efforts in the CIP field will focus on infrastructure that is critical from a European, rather than a national or regional perspective. Although focusing on European Critical Infrastructures, the Commission may where requested and taking due account of existing Community competences and available resources provide support to Member States concerning National Critical Infrastructures;
- **Complementarity:** The Commission will avoid duplicating existing efforts, whether at EU, national or regional level, where these have proven to be effective in protecting critical infrastructure. EPCIP will therefore complement and build on existing sectorial measures;
- **Confidentiality:** Both at EU level and MS level, Critical Infrastructure Protection Information (CIPI) will be classified appropriately and access granted only on a need-to know basis. Information sharing regarding CI will take place in an environment of trust and security;
- **Stakeholder Cooperation:** All relevant stakeholders will, as far as possible, be involved in the development and implementation of EPCIP. This will include the owners/operators of critical infrastructures designated as ECI as well as public authorities and other relevant bodies;
- **Proportionality:** Measures will only be proposed where a need has been identified following an analysis of existing security gaps and will be proportionate to the level of risk and type of threat involved;
- **Sector-by-sector approach:** Since various sectors possess particular experience, expertise and requirements with CIP, EPCIP will be developed on a sector-by-sector basis and implemented following an agreed list of CIP sectors.

The framework will consist of:

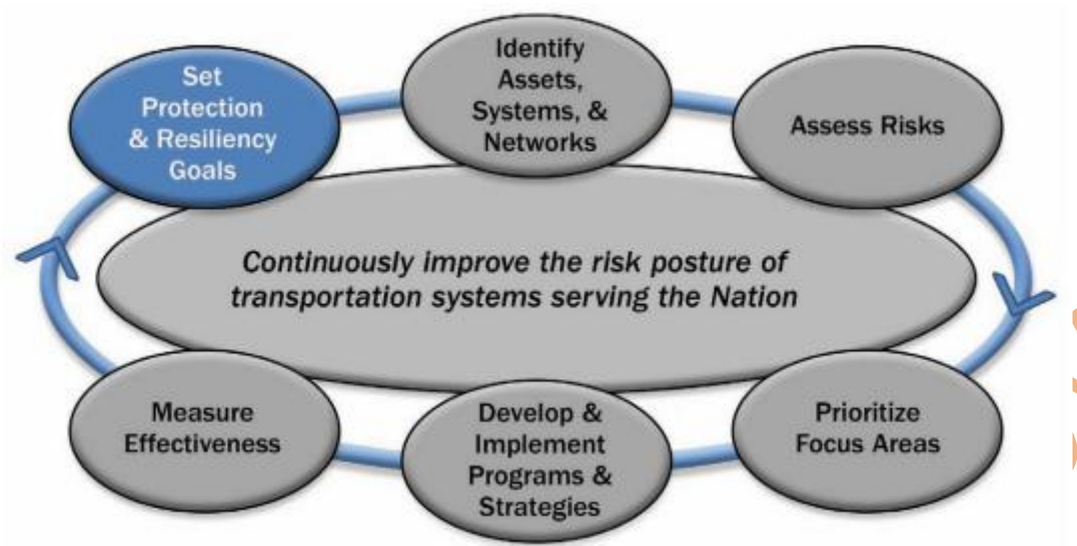
- A procedure for the **identification** and designation of European Critical Infrastructures (ECI), and a common approach to the assessment of the needs to improve the protection of such infrastructures. This will be implemented by way of a Directive;
- Measures designed to **facilitate the implementation** of EPCIP including an EPCIP Action Plan, the Critical Infrastructure Warning Information Network (CIWIN), the use of CIP expert groups at EU level, CIP information sharing processes and the identification and analysis of interdependencies;
- **Support** for EU countries regarding National Critical Infrastructures (NCIs) that may optionally be used by a particular EU country, and contingency planning;
- An **external dimension**: An important aspect of EPCIP is the external dimension of CIP. The interconnected and interdependent nature of modern economies means that disruption to or destruction of a particular infrastructure may have consequences for countries outside the Union and vice versa. It is therefore essential to strengthen international cooperation in this area through sectorial agreements;
- **Accompanying financial measures** and in particular the proposed EU programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013, which will provide funding opportunities for CIP related measures having a potential for EU transferability.

9.1.6.2 The US National Infrastructure Protection Plan (NIPP)

The Department of Homeland Security provides strategic guidance to public and private partners, promotes a national unity of effort, and coordinates the overall Federal effort to promote the security and resilience of the nation's critical infrastructure.

The National Infrastructure Protection Plan is the implementation framework of the US CIP. It provides the guidelines for the implementation of the CIP program. Among others it integrates the efforts for critical infrastructure protection measures in the various sectors; it defines the roles and responsibilities of the several actors at state and federal level and also sets the framework for a risk management framework for critical infrastructures.

These are the steps follows by this risk management framework:


Set Protection & Resiliency Goals
Identify Assets, Systems, & Networks
Assess Risks
Continuously improve the risk posture of transportation systems serving the Nation
Measure Effectiveness
Develop & Implement Programs & Strategies
Prioritize Focus Areas

The main goals of this National Infrastructure Protection Plan are:

- Assess and analyse threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities;
- Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments;
- Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, and employing effective responses to save lives and ensure the rapid recovery of essential services;
- Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk informed decision making;
- Promote learning and adaptation during and after exercises and incidents.

One of the steps of this plan is to identify which are the critical infrastructures that may apply a protection plan. There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. One of these critical infrastructure sectors is “Transportation System Sector”.

The Transportation Systems Sector consists of seven key subsectors, or modes:

- **Aviation** includes aircraft, air traffic control systems, and approximately 450 commercial airports and 19,000 additional airports, heliports, and landing strips. This mode includes civil and joint use military airports, heliports, short take-off and landing ports, and seaplane bases;
- **Highway Infrastructure and Motor Carrier** encompasses nearly 4 million miles of roadway, almost 600,000 bridges, and some 400 tunnels in 35 states. Vehicles include

automobiles, motorcycles, trucks carrying hazardous materials, other commercial freight vehicles, motor coaches, and school buses;

- **Maritime Transportation System** consists of about 95,000 miles of coastline, 361 ports, 25,000 miles of waterways, 3.4 million square miles of Exclusive Economic Zone, and intermodal landside connections, which allow the various modes of transportation to move people and goods to, from, and on the water;
- **Mass Transit and Passenger Rail** includes service by buses, rail transit (commuter rail, heavy rail--also known as subways or metros--and light rail, including trolleys and streetcars), long-distance rail--namely Amtrak and Alaska Railroad--and other, less common types of service (cable cars, inclined planes, funiculars, and automated guideway systems);
- **Pipeline Systems** consist of vast networks of pipeline that traverse hundreds of thousands of miles throughout the country, carrying nearly all of the nation's natural gas and about 65 percent of hazardous liquids, as well as various chemicals. These include approximately 2.2 million miles of natural gas distribution pipelines, about 168,900 miles of hazardous liquid pipelines, and more than 109 liquefied natural gas processing and storage facilities;
- **Freight Rail** consists of seven major carriers, hundreds of smaller railroads, over 140,000 miles of active railroad, over 1.3 million freight cars, and roughly 20,000 locomotives. Further, over 12,000 trains operate daily. The Department of Defence has designated 30,000 miles of track and structure as critical to mobilization and resupply of U.S. forces;
- **Postal and Shipping** moves over 574 million messages, products, and financial transactions each day. Postal and shipping activity is differentiated from general cargo operations by its focus on letter or flat mail, publications, or small- and medium-size packages and by service from millions of senders to nearly 152 million destinations.

To attend the specific characteristics of the transportation sector the National Infrastructure Protection Plan has a particular National Infrastructure Protection Plan risk management framework.

This framework analyse independently each transport mode and try to find the interdependences and connections between them. Inside the study of the rail transport mode there is a part that try study the impact of the cyber-attacks and the need of have mechanisms to take into account the cyber security.

Transit and passenger rail systems rely on computerized networks to facilitate operations, enable communication, and enhance efficient service delivery. This makes them vulnerable to network failure and cyber-attacks. Network failure may be caused by faulty or damaged internal components, direct cyber-attack to the agency’s network, an attack to a peripheral system or network, insider threat, unauthorized access to control centre networks, or a blanket computer virus. The result may be loss of communications or operations capabilities as well as misinformation by hacking into a website or server. The mass transit and passenger rail mode appears to be a popular target for cyber-attacks. Several attacks have made national and international news over the past few years. Because of the significance of this threat, TSA has been working with its security partners to develop a comprehensive strategy to protect, defend, and respond to cyber-attacks in the mode. The specific elements of the Mass Transit Cyber security program include:

- **Strategy Development:** Underlying the current cyber security effort in the mass transit and passenger rail mode is a broad-scoped proactive approach being coordinated with the Transportation Systems Sector Cyber Working Group (TSS CWG) to put both a strategy in place that encompasses a security methodology that will identify risk and mitigating actions to this critical element, along with a plan to identify the implementation elements needed to ensure necessary inspections and information collection is conducted. As an adjunct to the current BASE program, TSA is in the process of linking those cyber elements and processes that are contained and used within the mass transit and passenger rail mode with the periodic BASE assessment process conducted by TSIs on the largest 100 mass transit and passenger rail agencies. This addition to the BASE program will allow for a smooth transition of the cyber element into the existing inspection programs, making it the 18th element that will be examined during routine and continuing TSIs-conducted assessments. TSA will also be participating in the newly formed APTA Cyber Security Standards Development Working Group, which aims to develop standards and recommended practices for transit and passenger rail agencies.

9.1.6.3 OTA - Online Trust Alliance

Formed as an informal industry working group in 2005, today OTA is an Internal Revenue Service (IRS) approved 501c3 charitable organization with the mission to enhance online trust and empower users, while promoting innovation and the vitality of the internet. OTA is global organization supported by over 100 organizations.

OTA goals include:

- Help educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity;
- Supports collaborative public-private partnerships, benchmark reporting, meaningful self-regulation and data stewardship;
- Promote data sharing and collaboration through working groups, training and committees;
- Sponsors include individuals, technology leaders, social networks, ecommerce, financial institutions, service providers, government agencies and industry organizations;

- OTA is a member of leading organizations committed to collaboration, law enforcement and data sharing.

OTA provides best practices founded on their experience and in historic data of attacks to all kind of systems. The Traffic Management Systems usually don't implement this kind of mechanisms because they are installed in controlled networks and control centres and they have a reduced numbers of users, but now and in the near future this train traffic management systems will transit to use other networks to provide information out of the control centres and the possible threats can be numerous. It is important, for the implementation of a TMS, to take into account all these recommendations made by specialized organisms like OTA.

OTA recommends that all organizations implement the following best practices to try to minimize the risk of general attacks.

- Enforce effective password management policies. Attacks against user credentials, including brute force, sniffing, host-based access and theft of password databases, remain very strong attack vectors warranting the use of effective password management controls. Best practices for password management include:
  - Use multi-factor authentication (e.g. one-time PINs) for access to administratively privileged accounts. Administrative privileges should be unique accounts and monitored for anomalous activity and should be used only for administrative activities;
  - Require users to have a unique password for external vendor systems and refrain from reusing the same password for internal system and personal website logins;
  - Require strong passwords comprised of an 8-character minimum including a combination of alphanumeric characters, and force password changes every 90 days with limited reuse permitted;
  - Deploy a log-in abuse detection system monitoring connections, login counts, cookies, machine IDs, and other related data;
  - Avoid storing passwords unless absolutely necessary and only store passwords (and files) that are hashed with salt or are otherwise encrypted;
  - Remove or disable all default accounts from all devices and conduct regular audits to ensure that inactive accounts can no longer access your infrastructure;
  - Remove access immediately for any terminated employees or any third parties or vendors that no longer require access to your infrastructure.
- Least privilege user access (LUA) is a core security strategy component, and all accounts should run with as few privileges and access levels as possible. LUA is widely recognized as an important design consideration in enhancing data security. It also provides protections against malicious behaviour and system faults. For example, a user might have privileges to edit a specific document or email campaign, but lack permissions to download payroll data or access customer lists. Also, LUA controls help to minimize damages from exposed passwords or rogue employees.
- Harden client devices by deploying multi-layered firewall protections (both client and WAN-based hardware firewalls), using up-to-date anti-virus software, disabling by

default locally shared folders and removing default accounts. Enable automatic patch management for operating systems, applications (including mobile and web apps) and add-ons. All ports should be blocked to incoming traffic by default. Disable auto-running of removable media (e.g. USB drives, external drives, etc.). Whole disk encryption should be deployed on all laptops, mobile devices and systems hosting sensitive data.

- Conduct regular penetration tests and vulnerability scans of your infrastructure in order to identify and mitigate vulnerabilities and thwart potential attack vectors. Regularly scan your cloud providers and look for potential vulnerability points and risks of data loss or theft. Deploy solutions to detect anomalous flows of data which will to help detect attackers staging data for exfiltration.
- Require email authentication on all inbound and outbound mail streams to help detect malicious and deceptive emails including spear phishing and spoofed email. All organizations should:
  - Authenticate outbound mail with SPF and DKIM, including parked and delegated sub-domains,
  - Adopt a DMARC reject or quarantine policy once you have validated that you are authenticating all outbound mail streams,
  - Implement inbound email authentication check for SPF, DKIM, and DMARC,
  - Encourage business partners to authenticate all email sent to your organization to help minimize the risk of receiving spear-phishing and spoofed emails,
  - Require end-to-end email authentication using SPF and DKIM with a DMARC reject or quarantine policy for all mail streams managed or hosted by third parties;
- Implement a mobile device management program, requiring authentication to unlock a device, locking out a device after five failed attempts, using encrypted data communications/storage, and enabling the remote wiping of devices if a mobile device is lost or stolen;
- Continuously monitor in real-time the security of your organization’s infrastructure including collecting and analysing all network traffic in real time, and analysing centralized logs (including firewall, IDS/IPS, VPN and AV) using log management tools, as well as reviewing network statistics. Identify anomalous activity, investigate, and revise your view of anomalous activity accordingly;
- Deploy web application firewalls to detect/prevent common web attacks, such as cross-site scripting, SQL injection and directory traversal attacks. Review and mitigate the top 10 list of web application security risks identified by the Open Web Application Security Project (OWASP). If relying on third-party hosting services, require deployment of firewalls;
- Permit only authorized wireless devices to connect to your network, including point of sale terminals and credit card devices, and encrypt communications with wireless devices such as routers and printers. Keep all "guest" network access on separate servers and access devices with strong encryption such as WPA2 with AES encryption or use of an IPSec VPN;

- Implement Always On Secure Socket Layer (AOSSL) for all servers requiring log in authentication and data collection. AOSSL helps prevent sniffing data from being transmitted between client devices, wireless access points and intermediaries;
- Review server certificates for vulnerabilities and risks of your domains being hijacked. Attackers often use “Domain Validated” (DV) SSL certificates to impersonate e-commerce websites and defraud consumers. Sites are recommended to upgrade from DV certificates to “Organizationally Validated” (OV) or “Extended Validation” (EVSSL) SSL certificates. OV and EV SSL certificates are validated by the Certificate Authority to ensure the identity of the applicant. EV SSL certificates offer the highest level of authentication and verification of a website. EVSSL provides users a higher level of assurance that the site owner is who they purport to be, presenting the user a green trust indicator in a browser’s address bar;
- Develop, test and continually refine a data breach response plan. Regularly review and improve the plan based upon changes in your organization’s information technology, data collection and security posture. Take the time after an incident to conduct a post-mortem and make improvements to your plan. Conduct regular table top exercises testing your plan and personnel.

9.2 Workload Appendix

This appendix provides more details of generic workload measurement techniques as states in section 6.1.2.

It also provides examples of rail specific workload measurement techniques as stated in section 6.1.2.

9.2.1 Workload Measurement Techniques

This section describes the main types of generic workload measurement methods, (with some rail industry examples), and then describes some specific Network Rail workload measurement tools.

Mental Workload should be assessed throughout the design lifecycle. There is a need to evaluate existing systems to inform system design and task design and there is also a need to assess prototypes or final systems for assurance. However, a high-fidelity system to assess workload may not always be available during the early design phases and therefore predictive methods could be used in this instance [Ref 8].

There is no single best way to measure or assess mental workload and so a combination of methods should be used together. There are four main techniques of workload assessment:

- **Physiological measurements**: records and evaluates changes in physiological states as a result of different levels of workload;
- **Subjective ratings:** how participants subjectively assess the effect of mental workload for example how they feel about specific scenarios or tasks;

- **Performance assessment:** evaluate variation in performance as a result of different levels of workload;
- **Job and tasks analysis:** assess task elements, physical and psychosocial work conditions, environmental conditions and the organisation factors effect on workload.

When determining which method to select, some useful factors to consider are [Ref 5 and 11]:

Consideration	Comment
Time or Interval of test	Measure during, after, or continuously
Obtrusiveness of test	Obtrusive e.g. more suitable for lab testing or non-intrusive, less suitable to operational scenarios
Form of test	Verbal, written or machine gathered
Reliability	Degree of precision to which a method is able to measure what is measures
Validity	Degree of precision to which a methods measured what it intended to measure
Sensitivity	Degree to which a method is able to measure differences in workload e.g. mental strain or fatigue.
Intrusiveness	Degree in which is distracting or uncomfortable to participant.
Generalizability	Degree to which rank ordering of workload e.g. from high to low is replicable
Ease of Collection	Level of training required, time take to complete or number of facilitators required.
Ease of Processing	Level of training required or time take to complete.
Ease of Analysing	Level of training required or time take to complete.
Cost	Cost of equipment needed to time to collect, process and analyse data.
Equipment needed	Determine if additional equipment is required or if you are able to partner with external capabilities.
Confounding Variables	Workload tools causing workload, order effects etc.

Table 9.1: Considerations for Workload

9.2.1.1 Physiological

Physiological workload methods measure physiological aspects that can be affected by increased or decreased levels of workload. These methods aim to objectively measure the amount of mental workload experienced by an individual [Ref 10]. However it should be noted that the body is affected physiologically due to both mental and physical workload. Therefore, in order to examine the relationship between if the physiological responses is due to mental or physical workload, physiological methods are often compare against subjective measures.

Advantages	Disadvantages
Does not intrude on primary task performance and can be applied in the field, and in simulator setting.	High cost, physical obtrusiveness (less practically to implement on live railway/safety critical operation), issues in reliability and

	doubts in validity/sensitivity of techniques.

Table 9.2 Advantages and Disadvantages of Physiological Measures

Examples of physiological methods include:

1. **Cardiac activity measures:**

- Most common type of physiological measures as they are simple to evaluate and considered relatively reliable.
- Heart rate:
  - As workload increases, an increase in heart rate is commonly found (Wilson, Fullenkamp, & Davis, 1994).
  - It should be noted that as mean heart rate varies for each individual, it is necessary to define a baseline measurement to compare to.
  - It is also important to analyse both mental and physical workload as physical load will increase heart rate (Jorna, 1993).
- Heart rate variability:
  - Heart rate variability measures the inter-beat intervals of heartbeat over certain periods of time.
  - This method is not as common as measuring heart rate and is not as well accepted as there is less supporting evidence. However, the most common technique is to calculate the standard deviation of the inter-beat intervals over a set period of time, or a set number of beats, (Roscoe, 1992).
  - In general it is found that as workload increases, a decrease in heart rate variability is commonly found (Wilson, 1993). However, there is also some evidence to suggest that this is not always the case. This may be explained by individual differences such as physical fitness and age (Jorna, 1992).
- Blood pressure:
  - The majority of research shows that blood pressure increases as workload increases (Veltman & Gaillard, 1996).
  - Using blood pressure measuring techniques is the least common method of measuring workload as it is more intrusive than measuring heart rate or heart rate variability and is shown to provide no greater detail than when measuring heart rate.

2. **Respiratory activity measures:**

- Respiration definition: 'the interchange of oxygen and carbon dioxide between body tissues and the atmosphere' (Roscoe, 1992);
- There are a number of different respiration measures such as measuring the volume of air an individual under assessment breathes in, as well as the number of breaths in a set period of time. Some of these methods are suitable for real-world settings however, some are only suitable for lab settings;
- Respiration rate:
  - This is the most common respiration method as it is simple to conduct, is relatively non obtrusive so can be conducted in real-world settings and is sensitive to changes in workload. However, the measure of respiration rates is affected by both speech and physical workload, as physical activity increases, there is often an increase in respiration rate,

  - Most research shows that as workload increases, respiratory rate also increases (Wilson, 1993),
  - It should be noted that respiration rate has an effect on other physiological workload measures such as heart rate variability. Therefore, it is necessary to measure respiration rate if you are measuring heart rate variability so a comparison can be made (Veltman & Gaillard, 1996);
- Volume and concentration of carbon-dioxide:
  - This method aims to measure the volume of air and amount of carbon dioxide expelled during breathing,
  - It is not as common as measuring respiration rate as it is more difficult to calculate, is more obtrusive and the supporting evidence has conflicting results on workloads effect on the volume and concentration of carbon-dioxide.

3. Eye measures:

- Key measures include; horizontal eye movements and eye blink rates. These measures are primarily associated with visual workload; however, they have been shown to accurately predict mental workload (Van Orden, 1999);
- Eye Blink Rate and Interval of Closure:
  - 'Eye blink rate' is defined to be the number of eye closures in a certain period of time and 'interval of closure' is the time spent blinking,
  - The majority of supporting research shows that greater visual demand or greater visual workload is associated with less blinking (East, 2000);
- Horizontal eye activity: Most research suggests that an increase in workload results in an increase in horizontal eye movements. For example, when measuring higher workload in a car, more glances are observed to the speedometer, side mirrors and rear mirrors;
- Pupil diameter: Pupil diameter is often seen to increase as workload increases (Casali, 1983);
- Eye fixations: Measures the amount of time the eye is looking or fixated on certain objects.

4. Speech measures:

- Speech measures are the least common type of physiological workload method as it is difficult to measure the specific elements of speech such as pitch, rate, loudness and jitter etc. (Brenner, Doherty, & Shipp, 1994);
- The elements of speech most affected by workload have been found to be pitch, loudness and rate. As workload increases, pitch, loudness and rate are also seen to increase.

5. Brain activity measures:

- As decisions are made as a result of the brain processing information, making decisions and determining required actions, brain activity measures are seen as the most precise physiological measure of workload. This is because brain activity measures are classed as 'direct measures' whereas measuring cardiac, respiratory, eye and speech are as a result of 'indirect measures' as they are influenced by signals sent from the brain;

- Disadvantages of brain activity measures are that they can often be distracting or obtrusive to the individual under assessment and they also require special training to collect and analyse data;
- Common methods include Electroencephalograph (EEG) or electrooculogram (EOG).
- Electroencephalograph (EEG) aims to record electrical activity and is useful to identify workload variables that are not detected by other measures. However, this method is intrusive and extremely expensive;
- Electrooculogram (EOG) is a more sophisticated method of assessing eye blink rate however is also intrusive and extremely expensive.

9.2.1.2 Subjective Rating

Subjective rating questionnaires are administered to enable participants to provide ratings regarding their perceived mental workload. This method aims to reflect the amount of information used in their working memory e.g. if a participant feels they are experiencing a higher workload, their workload is most probably higher. However, subjective ratings should never be the only form of workload assessment, due to their subjective nature. Therefore it is always useful to follow up a subjective questionnaire with a wash up or feedback session to identify reasons why participants experienced under or overloaded in certain scenarios. Subjective measures have also been shown to correlate well with physiological measures (Tattersall & Ford, 1996).

There a number of different types of subjective rating questionnaires:

- Quantitative; type of information which is based on quantities;
- Qualitative; records descriptive and often subjective measures;
- Unidimensional; unidimensional are useful for simple tasks or while performing a task as they are fast and not too distracting;
- Multidimensional; generally considered better measures than unidimensional.

Subjective questionnaires can be administered either during or after the task(s) under assessment. It should be noted that if a questionnaire is administered during the task(s) it can interfere with the primary task under assessment. However, if administer too late e.g. 30 minutes after it can affect reporting scores. Therefore it needs to be appropriately administered depending on tasks required and context e.g. if driving a train, the driver should not fill in a long and complex questionnaire as this could have safety related consequences. When administering subjective questionnaires, it is also good practice and useful to give a trial run of filling in questionnaire and examples. This is to enable participants time to practice filling in the questionnaire so that is does no influence their perceived workload.

Advantage	Disadvantage

Low cost and ease of speed of application. Least intrusive, most flexible, most convenient, least time consuming, and least expensive form of evaluating workload (Yeh & Wickens, 1988).	Difficult to use if do not have full operating system so can be hard to use during early design stage. Can be issues in collecting data post task as participants can forget periods of higher workload.

Table 9.3: Advantages and Disadvantages of Subjective Rating

Most common methods include:

1. Subjective Workload Assessment Technique (SWAT)

This multidimensional tool is used to derive mental workload elements of workload; time, mental, and stress load [Ref 6].

- Time Load: time limit within which the task under analysis is performed and the extent to which multiple tasks must be performed concurrently;

  Mental Load: Attentional or mental demands associated with task;
- Stress Load: level of stress imposed on participant during task; including fatigue, confusion, risk frustration and anxiety.

SWAT Rating Scales:

The participant must rate the following 17 combinations into a ranking which reflects their perception of increase in workload.

Time Load	Mental Effort Load	Stress Load
1.Often have spare time	1.Very little mental effort or concentration is required	1. Little confusion, risk, frustration or anxiety.
2.Occasionally have spare time	2.Moderate mental effort or concentration required	2. Moderate stress due to confusion, frustration or anxiety.
3.Almost never have spare time	3.Extensive mental effort or concentration required	3. High to very intense stress due to confusion, frustration of anxiety.

Table 9.4: SWAT Subjective Method

Participants are then asked to weight each dimension (time, mental and stress) on a scale of 1 to 3. The scores are then converted into individual workload scores and for each swat dimension. Finally, and overall workload score is calculated.

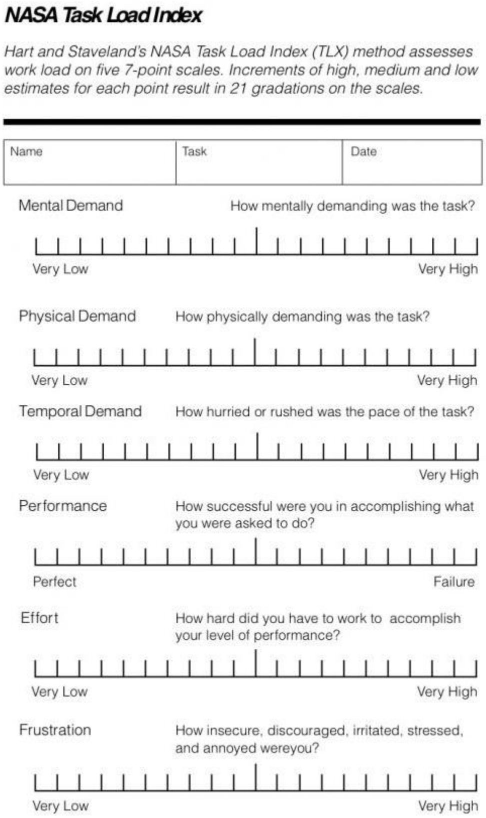
2. NASA Task Load Index (TLX):

This multidimensional tool is used to calculate overall mental workload using a weighted average of six workload sub-scale ratings; mental, physical, temporal, effort and performance [Ref 6].

- Mental Demand: How much mental and perceptual activity was required? Was the task easy or demanding, simple or complex?
- Physical Demand: How much physical activity was required? Was the task easy or demanding, slack or strenuous?
- Temporal Demand: How much time pressure did you feel due to the pace at which the tasks or task elements occurred? Was the pace slow or rapid?

- Overall Performance: How successful were you in performing the task? How satisfied were you with your performance?
- Frustration Level: How irritated, stressed, and annoyed versus content, relaxed, and complacent did you feel during the task?
- Effort: How hard did you have to work (mentally and physically) to accomplish your level of performance?

Each sub-scale is presented to participants either during or after the experimental trial and participants are asked to score each element from low (1) to high (20). Each element is then given a weighting from not relevant (0) to more important than any other factor (5). The overall workload score is then calculated by multiplying each rating by the weight. The sum of weighted ratings for each task is then divided by 15 (the total sum of weights). Therefore, a workload score from 1 to 100 is calculated.



NASA Task Load Index

Hart and Staveland's NASA Task Load Index (TLX) method assesses work load on five 7-point scales. Increments of high, medium and low estimates for each point result in 21 gradations on the scales.

Name	Task	Date

Mental Demand — How mentally demanding was the task?

Very Low — Very High

Physical Demand — How physically demanding was the task?

Very Low — Very High

Temporal Demand — How hurried or rushed was the pace of the task?

Very Low — Very High

Performance — How successful were you in accomplishing what you were asked to do?

Perfect — Failure

Effort — How hard did you have to work to accomplish your level of performance?

Very Low — Very High

Frustration — How insecure, discouraged, irritated, stressed, and annoyed wereyou?

Very Low — Very High

3. ISA (instantaneous self-assessment).

The ISA Workload technique is a simple workload assessment method, originally developed by NATS. Participants must rate their workload during a task, normally every 2 minutes, on a scale of 1 (low) to 5 (high).

Level	Workload Heading	Spare Capacity	Description
5	Excessive	None	Behind on tasks, losing the big picture.
4	High	Very Little	Non-essential tasks suffering. Could not work at this level for long.
3	Comfortable Busy Place	Some	All tasks well in hand. Busy but stimulating pace. Could keep going continuously at this level.

Level	Workload Heading	Spare Capacity	Description
2	Relaxed	Ample	More than enough time for all tasks. Active on tasks less than
1	Under Utilised	Very Much	

Table 9.5 ISA Subjective Measure

Ideally, the ISA scale is presented to the participants in a colour coded form to easily enable the participants to select their perceived workload. Alternatively to the participant having to fill in their perceived workload rating themselves, it can be given verbally. Once tasks are completed, usually a workload profile is shown via a graph to highlight the low and high workload points of the scenario.

Other methods include:

- MCH – Modified Hooper Scales;
- SWORD – Subjective Workload Dominance;
- DRAWS – Defence Research Agency Workload Scales;
- MACE – Malvern Capacity Estimate;
- Workload Profile Techniques;
- Bedford Scale.

9.2.1.3 Performance Measures:

9.2.1.3.1 Primary Task Performance Measures:

Primary task performance methods measure the ability to perform the primary task under analysis and the 'effectiveness in accomplishing a particular task', (Paas & Vanmerrienboer, 1993). Generally it has been found as mental workload increases, the performance of primary tasks is likely to decrease. However, it does not take into account spare mental capacity (Sirevaag et al., 1993). For example, two tasks may be performed with the same performance results but one person's mental capacity may not be at their maximum while another person's may be at their limits (Sirevaag et al., 1993). It should be noted that it is also hard to measure changes in performance as a result of small changes in workload. For example, when assessing low to medium workload, or a gradual change in workload, the performance may not change as much as when measuring from a low to a sudden high workload.

Typical primary task performance measures include calculating the number of errors, speed of performance and reaction times.

Advantages	Disadvantages
Direct index performance and ease of use since performance of task is usually measures anyway.	Workload is affected by individual differences and care is needed when assessing and interpreting results as performance may be affected by a lack of training or under load.

Table 9.6: Advantages and Disadvantages of Primary Performance Measures

9.2.1.3.2 Secondary Task Performance Measure:

Secondary task performance measures assesses the ability to perform an additional secondary task in addition to the primary task by determining if there is any spare mental capacity (Sirevaag et al., 1993). Therefore it calculates the difference between the mental capacity consumed by the main task, and the total available capacity (Mulder, 1979).

Typical measures include memory recall tests, mental arithmetic, reaction times and tracking tasks. In general it is found that as mental workload increases, performance of the secondary task will decrease due to reduced spare capacity to perform a secondary task. When selecting a secondary task performance measure it is necessary that the primary and secondary tasks use the same resource. For example if a primary measure is mainly visual, the secondary measure must also be visual to achieve the best measure of performance (De Waard, 1996).

As secondary tasks can often be intrusive on primary task performance, to reduce intrusion, embedded secondary task measures should be used. For example by performing a secondary task within the system under assessment, as the secondary task is not external to system, the level of intrusion is reduced.

Wickens Theory also states that some additional or secondary tasks do not interfere with primary tasks and can be done simultaneously. Therefore, these types of task should be considered in the design of the system itself to support users and enable an optimum level of workload.

Advantages	Disadvantages
Easy to use and little extra work is required to carry out a secondary task measure.	Can be intrusive to primary task performance so not suitable in certain scenarios and care is needed to ensure same resource pool of primary task is assessed.

Table 9.7: Advantages and Disadvantages of Secondary Performance Measures

9.2.1.4 Predictive Measures

More recent workload assessment methods make use of predictive techniques. These methods are often used during the system design phase when the system to be assessed is not yet available. Although these methods are more recent in sophistication, it has been found that Subject Matter Experts (SME's) predictive ratings correlate well with operator's subjective ratings when a system is available to assess [Ref 6]:

Examples of these methods:

1. **Cognitive task load analysis** is used to assess or predict the cognitive load of a task or set of tasks. This technique is based on a model of cognitive task load that describes the effects of different tasks characteristics on operator's workload. It states that task load is comprised of:
   - Percentage of time occupied,
   - Level of information processing,
   - Number of task-set switches during a task or series of tasks, [Ref 6].
2. **Variation of subjective measures SWAT and NASAT-LX**: When the system under analysis fidelity level is too low or before the system has been developed, subjective methods can be altered to be used as a predictive measure. For example, subject matter experts can be used instead of end users to rank the predictive workload for a set of tasks based on:

- Operator’s current workload,
- Expected future workload as a result of knowledge of the future system or changes in technology,
- Expected future workload as a result of known changes in tasks or procedures.

Each task can then be given a qualitative score, taking into account a number of variables (such as expected button presses, frequency of task, level of automation, change in roles and tasks) and then an expert judgement made on whether the workload is predicted to be:

- Identical workload,
- Lower workload,
- Higher workload.

For example:

	NASA TLX					
Task	**Mental**	**Physical**	**Temporal**	**Effort**	**Overall Score**	**Rationale**
Task 1	Identical	Identical	Identical	Identical	Identical	Rationale for each NASA TLX sub-score based on expert judgment
Task 2	Identical	Identical	Identical	Higher	Higher	Rationale for each NASA TLX sub-score based on expert judgment
Task 3	Lower	Higher	Identical	Identical	Identical	Rationale for each NASA TLX sub-score based on expert judgment

Table 9.8: NASA-TLX Predictive Adaptation

The rationale should include what is known and, assumptions and expectations on the system.

3. **W/INDEX** is a predictive model of operator workload used in crew station design. The method was developed by Honeywell systems research centre and it makes use of a computer based tool to predict operator workload by assessing representative scenarios. The model is useful at any stage of design from high level concepts to developed solutions. It is used to model complex environments, where an operator’s attention will be shared between multiple tasks over much of the scenario. Therefore the tool aims to use a realistic model of attention timesharing and assigns appropriate levels of workload penalties to explain for different levels of conflicts between multiple tasks, [Ref 7].

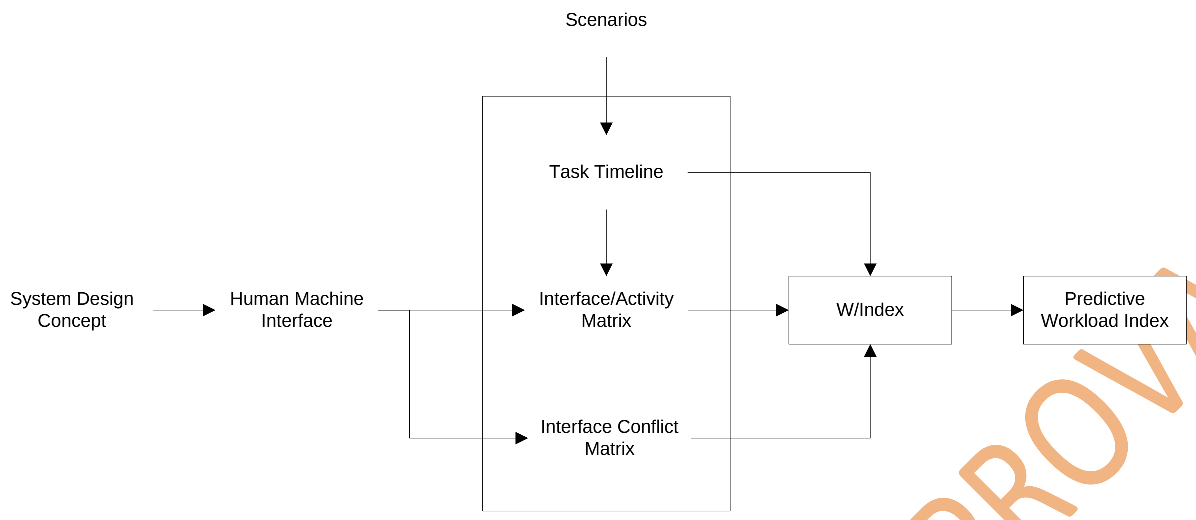

Scenarios
Task Timeline
System Design Concept
Human Machine Interface
Interface/Activity Matrix
W/Index
Predictive Workload Index
Interface Conflict Matrix

Figure 9.1: W/INDEX Method

- Task Timeline is the specific tasks performed by operator during scenario and when they occur during timeline;
- Interface/activity matrix is derived from the task timeline and specifies the amount of attention the operator must pay to each task e.g. 1 being very low and 5 being very high.

4. **BVO** [Ref 7] is based on an extended task analysis of 5 main task elements: Monitoring trains, control by preparation, communication by short messages, communication by (longer lasting) train messages and adjusting the plan. However, this method only focuses on one element of workload; task demand, and does not focus on the subjective experience of workload and working environment. It also does not have the sensitivity to highlight activation, peak demands, long lasting tasks and rule based vs. knowledge based tasks.

9.2.2 Rail Specific Workload Methods

9.2.2.1 Workload in the Context of the Rail Industry

Mental workload in rail signalling is a multi-dimensional concept and it is made up of a number of factors such as the number and complexity of tasks over a period of time and the load perceived by an individual over a period of time [Ref 8]. These factors in which can affect workload in operational centres today are generally well established and understood. For example, a greater complexity of infrastructure, an increased number of assets in an area and an increased amount of traffic in an area of control is likely to increase an operator’s experience of workload. The boundaries of each area of control are fixed and well defined in terms of workload variables and so an operator's normal level of workload can be assessed to a high degree of confidence using specific workload toolsets developed for the rail industry. As well as measuring the objective and subjective levels of workload experienced in a particular Rail Operating Centre, due to the amount of workload data collected from rail specific toolsets and current deployments, it is also possible to predict the level of workload experienced should a change to an operating system occur, or if a new operating centre is being deployed.

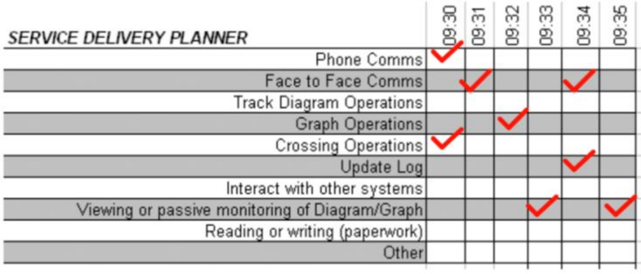
The ability to predict and measure workload due to the introduction of TM will increases in complexity. As a result, the methods used to predict and assess workload will need to be adapted and or made more intelligent to be suitable to measure workload in the future.

9.2.2.2 Current Network Rail Signalling Specific Workload Toolsets

Below are examples of specific workload tools developed by Network Rail currently used to measure signaller workload in the UK. In section 6, it will discuss how some of these tools will need to be adapted in the future to successfully measure the effects of workload as a result of TM.

1. **Network Rail Activity Analysis - Workload Profiling**

The activity analysis tool collects information about the percentage of time that a task or scenario occupies. Once the key tasks in a scenario are identified, the time or duration to complete each task should be observed during the scenario to be assessed. See example of scenario duration time sheet below.



SERVICE DELIVERY PLANNER	09:30	09:31	09:32	09:33	09:34	09:35
Phone Comms	✓					
Face to Face Comms		✓			✓	
Track Diagram Operations						
Graph Operations			✓			
Crossing Operations	✓					
Update Log					✓	
Interact with other systems						
Viewing or passive monitoring of Diagram/Graph				✓		✓
Reading or writing (paperwork)						
Other						

Figure 9.2: NR Activity Analysis Method [Ref 11]

This method is useful information to understand the effects of time pressure as it is a key element of workload. However it should be noted that there is not always a direct relationship between actions, events and level of workload. This method is also not able to capture the demand experienced due to a combination of tasks or activities and does not take into account mental processing.

Therefore, activity analysis methods should be compared with other workload tools such as subjective questionnaires. This enables a greater understanding of participant workload.

The data collected from the activity analysis can be presented in either an 'Activity Occupancy Graph' worksheet or a 'Continuous Occupancy Graph' worksheet. See below example of activity occupancy graph:

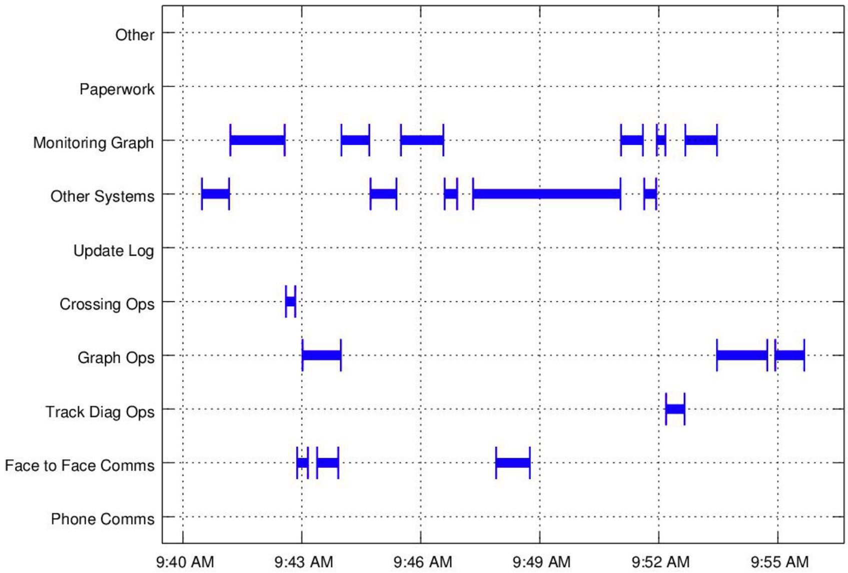


Figure 9.3: NR Activity Analysis Method [Ref 11]

2. 'Flag' Form

During scenarios to assess workload, participants should be encouraged to be vocal, and express feelings of workload. A 'Flag Form' is a form to enable observers or facilitators to note down this commentary to prompt discussions and de-brief sessions after the scenarios are complete.

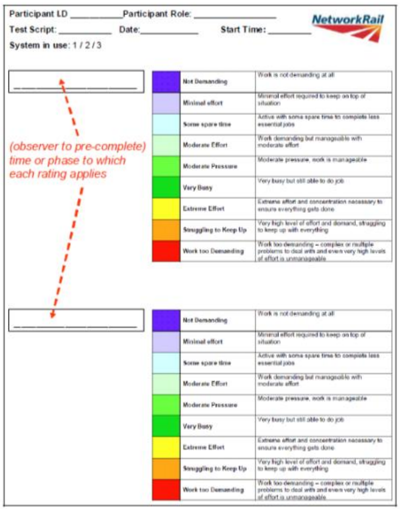
3. General Observations forms

General observations should be captured by the facilitators during scenarios to capture any interesting or unexpected behaviour. Types of observations include:

- Equipment;
- Tasks;
- Information;
- Work Design;
- Operating System;
- Infrastructure;
- Organisation;
- Timetables;
- Environment.

4. Integrated Workload Score (IWS)

The IWS is a subjective questionnaire to determine overload and under load. The participant is required to call out their perceived workload level, usually very 3 minutes, according to a rating scale made up of 9 elements. The facilitator than records this information on the sheet below:



Participant LD __________ Participant Role: ________________

Test Script: __________ Date: __________ Start Time: ________

System in use: 1 / 2 / 3

(observer to pre-complete) time or phase to which each rating applies

🟪	Not Demanding	Work is not demanding at all
🟪	Minimal effort	Minimal effort required to keep on top of situation
🟦	Some spare time	Active with some spare time to complete less essential jobs
🟩	Moderate Effort	Work demanding but manageable with moderate effort
🟩	Moderate Pressure	Moderate pressure, work is manageable
🟩	Very Busy	Very busy but still able to do job
🟨	Extreme Effort	Extreme effort and concentration necessary to ensure everything gets done
🟧	Struggling to Keep Up	Very high level of effort and demand, struggling to keep up with everything
🟥	Work too Demanding	Work too demanding – complex or multiple problems to deal with and even very high levels of effort is unmanageable

🟪	Not Demanding	Work is not demanding at all
🟪	Minimal effort	Minimal effort required to keep on top of situation
🟦	Some spare time	Active with some spare time to complete less essential jobs
🟩	Moderate Effort	Work demanding but manageable with moderate effort
🟩	Moderate Pressure	Moderate pressure, work is manageable
🟩	Very Busy	Very busy but still able to do job
🟨	Extreme Effort	Extreme effort and concentration necessary to ensure everything gets done
🟧	Struggling to Keep Up	Very high level of effort and demand, struggling to keep up with everything
🟥	Work too Demanding	Work too demanding – complex or multiple problems to deal with and even very high levels of effort is unmanageable

Figure 9.4: IWS Method [Ref 11]

<u>IWS Scoring:</u>

- An IWS rating of higher than 4 is considered that the task, scenario or enviornment is demanding a moderate level of effort from the participant;
- A score of 4 or less is considered as an 'underloaded' level of workload which can be associated with fatigue or bordem;
- A score of 7 or more is considered an 'overloaded' level of workload, associated with a decline in performance.

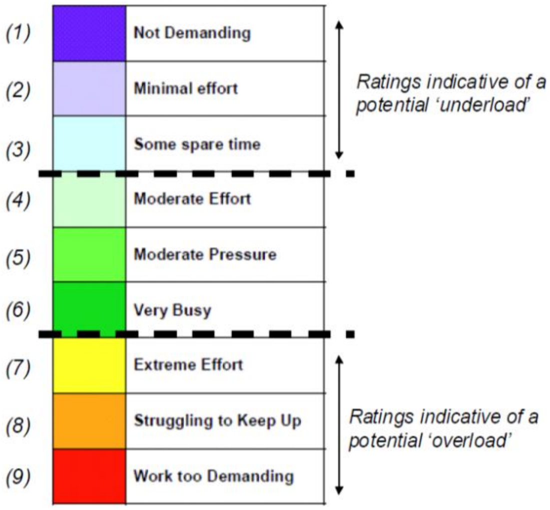
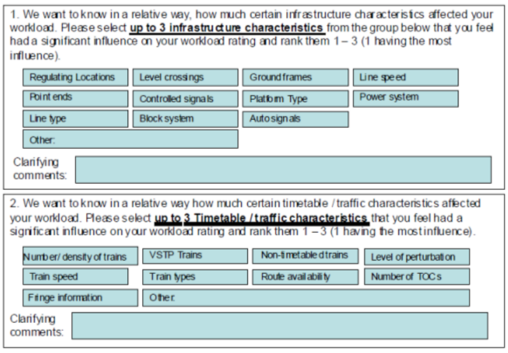


Figure 9.5: Figure 3 4 IWS Method [Ref 11]

It should be noted that as this is a subjective method, it should not be used on its own and should be used in conjunction with another workload methodology.

5. Diagnostic Questionnaire

A diagnostic questionnaire is a questionnaire specifically related to either the perceived effect of overload or under load by the participants. Therefore, depending on the IWS score, a different diagnostic questionnaire is administered. For example, if an overload IWS score was recorded for the participant, then an overload diagnostic questionnaire will be administered. Examples of questions include:



1. We want to know in a relative way, how much certain infrastructure characteristics affected your workload. Please select **up to 3 infrastructure characteristics** from the group below that you feel had a significant influence on your workload rating and rank them 1 – 3 (1 having the most influence).

Regulating Locations	Level crossings	Ground frames	Line speed
Point ends	Controlled signals	Platform Type	Power system
Line type	Block system	Auto signals	
Other:			

Clarifying comments:

2. We want to know in a relative way how much certain timetable / traffic characteristics affected your workload. Please select **up to 3 Timetable / traffic characteristics** that you feel had a significant influence on your workload rating and rank them 1 – 3 (1 having the most influence).

Number/ density of trains	VSTP Trains	Non-timetabled trains	Level of perturbation
Train speed	Train types	Route availability	Number of TOCs
Fringe information	Other:		

Clarifying comments:

Figure 9.6: Diagnostic Questionnaire [Ref 11]

6. ODEC

The Operational Demand Evaluation Checklist (ODEC) is a NR tool developed for assessing how infrastructure features and operational scenarios in an operator's area of control or responsibility affect workload. The user must provide data against 28 categories to characterise the area of control.

The output is the percentage of categories defined as having high, medium or low workload. This provides a representation of a single workstation, enabling a comparison between workstations level of workload to be mad, [Ref 12].

7. PRESTO

The Predictor of Signaller Time Occupancy (PRESTO) tool is used to enable predictions to be made regarding operators workload associated with controlling the movement of trains through a specified control area over a certain period of time.

The tool analyses train running data produced from Railsys which is a timetable modelling tool. Information regarding running times, signals, level crossings, complexity of junctions etc. is considered to determine the characteristics of an area of control.

PRESTO then calculates signaller task occupancy, (the time taken to perform tasks expressed as a percentage of the total available time), [Ref 12].