Theme: Global Perspective for Managing Human Performance

Title: Human Error Assessment in the Design of Signalling Control Centres

Presenters: Harry Blanchard, Senior Human Factors Consultant,
Human Engineering Limited, part of the Lloyd's Register Group

Synopsis

Humans allow rail systems to operate in a flexible, adaptable manner. However, operators are also subject to errors that may result in safety incidents or reduced operational performance.

Rail systems have protection to minimise human error through a combination of safety features, interface and display design and operational procedures. Rapid growth and technical innovation in rail systems introduce new equipment and new responsibilities for the operators and may result in unexpected operator errors if human factors are not adequately considered in design.

This paper describes a method for assessing the opportunities for human error in signalling centres using an approach based upon the established techniques of Task Analysis and Failure Modes Effects Analysis. The method allows systematic identification of signaller errors in the future signalling operation, the derivation of consequences for safety or operational performance of the system, and the influence of different protection measures to be considered.

The method consists of the following steps:

1. An assessment of the architecture of the proposed signalling system, to understand the safety and operational role played by the different system elements. The influence of different safety features, for example system interlocking, can be captured in this description. This allows the role of the signaller, and the relationship with the signalling equipment to be understood.

2. A description of the signaller’s task (Task Analysis) to represent the actions required of the signaller under different operating conditions (for example normal, abnormal, degraded and emergency operations). The task analysis will be based upon the operational procedures developed for the signalling centre.

3. The Failure Modes Effects Analysis technique is then used to systematically identify the human errors that may occur for each of the signaller activities described in the task analysis, and the safety and operational consequences for the system to be derived.

This analysis allows system managers to identify any new errors, and to decide if the proposed system provides sufficient protection for the potential error opportunities that exist. This paper provides a generic case study of the application of the system to a novel signalling system in the UK, and describes how it was used to refine operational procedures and provide assurance to the infrastructure owner and regulator that the system was suitable for operation.

Introduction

Investment in new signalling systems is often justified by the enhanced performance and greater safety made available as a result of their implementation, but experience has shown they can also introduce new problems.

Rapid innovation in technology brings new responsibilities and tasks to the human operators. For example, new signalling systems such as ETCS (part of the European ERTMS), LBZ in Germany, TVM-430 in France and the Channel Tunnel, CTCS-3 in China have introduced in-cab signalling, sophisticated Automatic Train Protection, and introduced a high degree of automated route setting, conflict resolution and track protection functionality provided directly through the train control infrastructure. All of these innovations offer great benefits, but must be carefully developed for those benefits to be realised.

The failure to manage the human factors relating to such developments can result in unexpected performance bottlenecks and safety incidents. When such issues are identified only late in the project, even in service, this will result in:

- Higher rate of incidents (injuries, fatalities, equipment losses) and reduced system availability than were anticipated in design, arising from a failure to consider likely operator errors;
- Expensive remedial work, additional operating restrictions, compromised procedures, additional staffing and increased preventative and corrective maintenance in service to control these issues; and
- Unexpected catastrophic failures arising from a failure to consider operator performance (and additional potential errors) under all operating conditions or minority use cases.

Modern rail Engineering Safety Management standards are increasingly making specific requirements for the consideration of human factors within the design process, recognising the contribution of human action to system safety. For example, Yellow Book 4 (RSSB, 2007) makes a requirement for a step within the design process to:

> *Refine understanding of hazards of the system and the system's effect on overall risk to the railway […] Identify contribution of human error to risk.*
> (Section 3.3, p.26)

This paper describes a method we have developed, drawing upon established human factors and safety techniques, to evaluate the contribution of the human operators to the safe and efficient operation of new signalling systems. We believe the method satisfies regulatory requirements, follows best-practice and conducts the human factors work within a structure that can be readily aligned with safety and operational cases.

We have found this approach to be more suitable for the *prospective* human error analysis of proposed designs (as opposed to *retrospective* analysis of past events, such as safety incidents on existing systems) than other approaches. Compared to human hazard identification workshops that might be conducted as part of general safety assessment, this method offers a more coherent structure and is more amenable to development through the project. Compared to the Systematic Human Error Reduction and Reduction Approach (SHERPA, Embrey 1986) this method offers a similar structured approach to the identification of human errors, but is able to represent the protection provided by the equipment more explicitly in the analysis – a feature that is particularly useful for evaluating signalling systems.

Method

The method has been developed to include three steps.

1. Description of the proposed operation

The analyst should agree with the safety management representatives how the work can best contribute to the safety and operational cases. It is expected that the analysis would be conducted in support of defined project safety and operational targets, set at a strategic level. Closely related to the aim of the study is the definition of the operators, equipment and operating conditions to be assessed.

The analyst should then capture all of the available data about the proposed operation, particularly:

- The level of service to be supported by the new system
- The strengths and weaknesses of the technology
- The responsibilities assigned to the signaller
- The operating circumstances – for example:
    - a period of transition during which the function of the system is incomplete and temporary working methods are to be used;
    - daily or seasonal variation in working methods, such as different manning levels and traffic between day and night, higher levels of road traffic on level crossings at particular times of year; and
    - mixed stock operation, in which different services must be managed in different ways.

At an early stage in development of a new signalling system much of this information will be presented in an *operational concept* document describing how the system is intended to be operated. As the system design matures, further documents will add further detail. A particularly useful system description for human factors analysis is a *system architecture*, describing the relationships and functional allocation between different equipment components and different operators.

A generic architecture for a signalling control system is presented at Figure 1. Signalling control systems generally resemble a *supervisory control system* as defined in *the Human Factors Framework for IEC 61508* (HSE, 2001). The electronic control system of the signalling system exercises closed-loop control over the railway equipment (signals and points), and may follow a programmed timetable to set routes for the passage of services and applies algorithms to resolve conflicts. A system of interlocking prevents track configurations being set that may lead to unsafe movements.

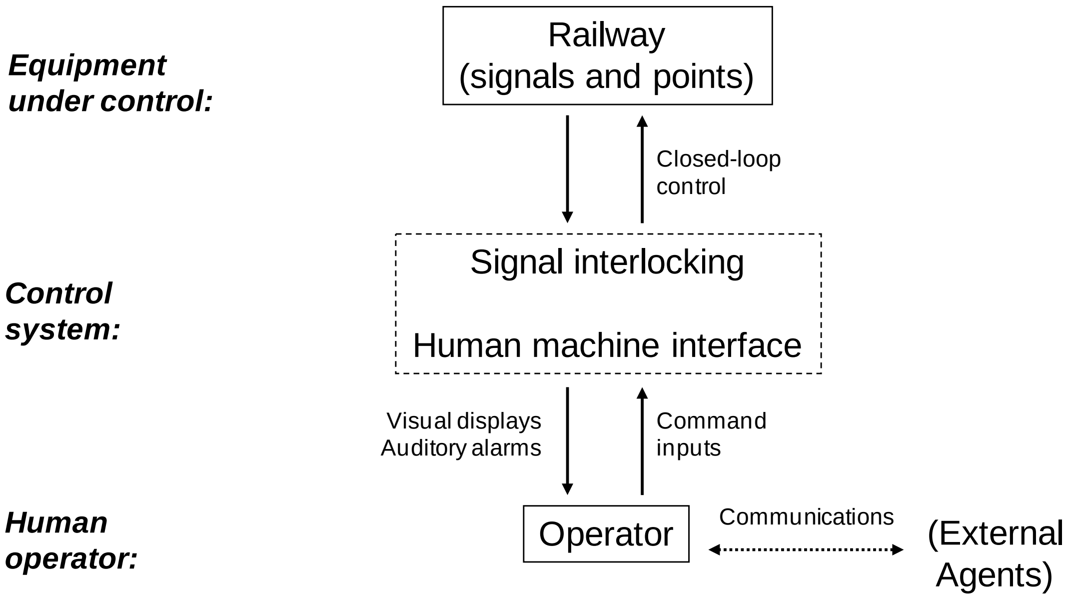

Figure 1 – Generic system diagram for a signalling control system

In this arrangement the operator acts in a supervisory capacity, monitoring the status of the railway and the action of the Service Control System:

- In normal (and abnormal) operation the operator will primarily act to optimise service delivery, rescheduling services and intervening to resolve emerging conflicts.
- Under degraded circumstances the operator is involved in maintaining safety by protecting parts of the railway affected by equipment failures or to support the protection of track workers, and authorising train movements as required to allow service to be maintained.
- Under emergency circumstances the operator may activate a train stop order, as required and alert management and emergency services to the incident.

Generally, the scope of detailed analysis is limited to the role of the primary operator (the signaller), which has fitted the requirements of the projects seeking to demonstrate the acceptability of the equipment to deliver service. More complete studies may consider further roles, for example the contribution of maintenance, trackside and administrative staff. Different system architectures may require consideration of different signaller roles (for example a strategic and tactical controller).

We would recommend that the equipment scope includes all equipment that the signaller may be required to use for the operating conditions as real operations require all the equipment to be used together. Consideration of only a subset of the equipment would be rather artificial, as it would not be able to consider the contribution made by another equipment set (for example communications) to reducing errors in conducting the signalling task.

We would recommend that the full range of operating conditions is considered. The signalling system must be suitable for a wide range of operating conditions and circumstances. To focus only on normal operations, for example, would result in operator errors that may be committed under abnormal, degraded and emergency conditions. In more detailed design consideration should also be given to operation transition periods when equipment may be only partially functional and additional procedures are required to control additional opportunities for error.

2. Task analysis

In this step the analyst describes the signaller's task, using some form of task analysis – a method to decompose an overall goal (such as *Providing Signaller Service*) into a series of sub-goals and tasks. This allows the analyst to represent all of the signaller's tasks, under different operating conditions, in a structured way. The task analysis structure will also be used to order the error analysis.

Under a particular method, Hierarchical Task Analysis (Shepherd, 1992), each sub-goal or task is re-described in terms of its constituent sub-goals, task and plans until the task is thoroughly described, or until it is not useful to re-describe the task further. A generic task analysis for a signaller is provided in Figure 2, represented in HTA format. The structure of this TA aims to reflect the *input-output-communication* division of the system architecture. Other useful structures would include dividing *normal-abnormal-degraded-emergency* operations.

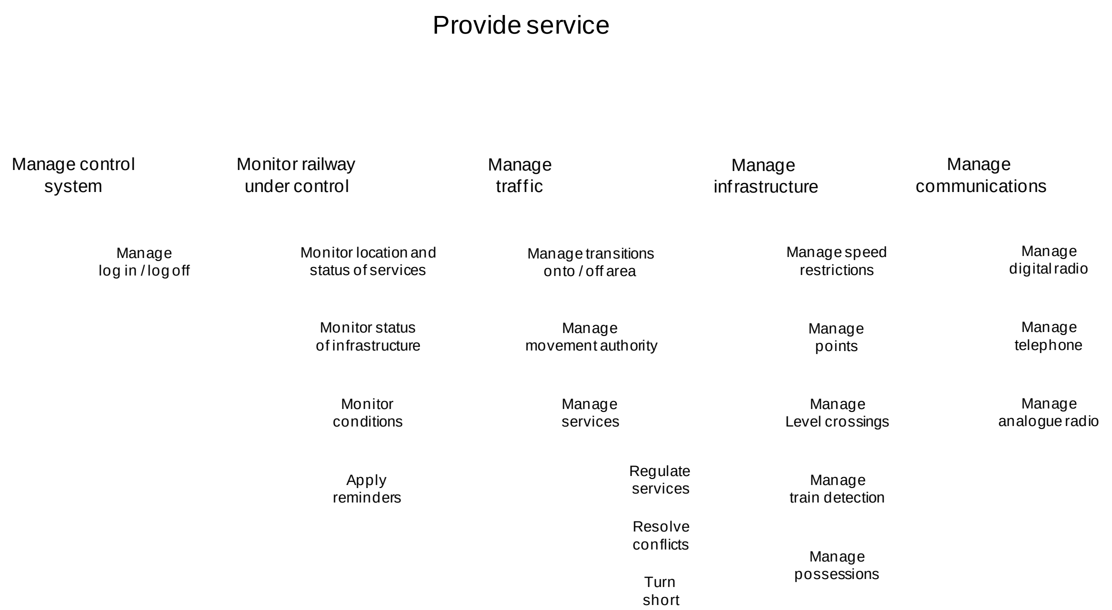

Figure 2 – Generic high-level signalling control system task analysis

The task analysis is generally populated by review of the system supplier user manuals and the proposed operating procedures. Wherever possible, the task analysis should be validated through workshops with the operators, and by observation of the operators using the equipment, for example, in a simulator. This is important to ensure that the task analysis is accurate and realistic.

3. Failure Modes Effects Analysis

Failure Modes Effects Analysis (FMEA) is a systematic procedure for assessing the failures of a component of a system (in this analysis, the signaller) and determining the effect on the system. The objective of such an analysis is to identify critical functions and related failures, and the ability of the system (through design or operational procedures) to:

- Limit the probability of failure;
- Encourage correction of the failure;
- Mitigate the consequences of failure; and
- Improve the ability of the system to recover from failure.

An example FMEA of the potential operator errors in a generic signaller control system task is presented in Figure 3. The headings used for this FMEA are described in Table 1.

Table 1 – Headings used in the FMEA analysis to identify opportunities for signaller error in ERTMS signalling operations on the Cambrian Line

FMEA Heading	Description
Activity	The signaller's generic operational activity, taken from the task analysis.
Failure mode	The signaller's credible errors ("failure modes") in each activity identified using a set of hazard identification keywords from a recognised human factors technique (for example, TRACE-r, Shorrock and Kirwan, 1999).
Effects	Records the consequences of the signaller error upon the safety or operational performance of the system.
Protection	Identifies the system-level means by which the signaller errors are mitigated. This may be through reducing the propensity of the signaller making the error, by detecting that the error has been made to provide an opportunity for the signaller to correct the error, or controlling the error by remedial action of the system itself.
Analysis	In the early design the analysis column would make recommendations for further design developments or procedures. In final design stages the analysis column could be used to make claims that particular human error hazards have been managed to an acceptable level, perhaps referencing other human factors evidence that support the claim.

The initial error analysis is usually conducted by the analyst, using the error keywords to generate errors and the system architecture to evaluate the protection available and potential system, consequences. We recommend that analysts should also review the operating experience of organisations that have previously implemented similar systems to inform their identification of errors. This should be followed by a *hazard and operability workshop* (hazop) with experienced operators and system integration engineers.

Further development of the analysis could include the evaluation of specific scenarios, perhaps in a workshop. We consider such "what-if" evaluation to be an important (and often neglected) step in identifying how specific combinations of events and operator actions can result in adverse incidents, and allow additional specific protection to be developed.

As an example of the contribution of such reviews, in a previous UK metro project, the consequences of the operator accidently misrouting a service was initially considered only to have consequences for operational efficiency. Review in the workshop revealed that safety could also be compromised in two specific scenarios – mistakenly routing fast services into crowded platforms where passengers were expecting slower stopping services, resulting in a risk of passenger injury, and misrouting resulting in services with electric traction towards track sections that have been isolated for engineering possessions, causing these protected sections to become live, and resulting in electrocution risk for track workers. These scenarios were entered into the FMEA for further evaluation, and additional protection measures were recommended.

Activity	Failure Mode			Effects		Protection			Analysis
	Error	Keyword	PSF	Safety	Operational	Prevention	Detection	Mitigation	
1. Manage control system									
Log in/off	Fail to set password protection Forgets password	No action Wrong information	Complexity of log in process Frequency of use	Operation by incorrect or unauthorised personnel	Authorised personnel unable to operate	n/a	System cannot be used without correct password	24-hour technical support	Regular audit of system users, link to monitoring access to signalling facility
Configure operating modes	Sets SCC in wrong operating mode of configuration	Wrong action	Complexity of setup or configuration Instructions regarding correct setup for service	Operation of system with incorrect mode/configuration	Operation of system with incorrect mode/configuration	Operating modes and setup published in periodic operating notice issued to supervisor and discussed with staff	n/a	Mode configuration only permitted by supervisor / technical support	Operating modes and configuration of system should be logged and audited
2. Monitor railway under control									
Monitor location and status of services	Fails to identify significant change in location or status of services Misinterprets location or status of services	No information Wrong information Partial information	Design of HMI information displays Accuracy of information Distraction/workload	*Incorrect understanding of location and status of services* (range of safety and operational consequences arise from decisions made based on incorrect understanding)		Effective use of reminders	Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding.	n/a (no direct operational or safety consequences, but see protection provided for errors committed in managing traffic and managing infrastructure)	Evaluate and test HMI display in development to confirm it is understandable and clear to use by the operators. Difficult to detect and correct a misunderstanding by the operator, but other staff may help identify error. Should ensure that operators are trained to anticipate emerging situations ("situational awareness"), emphasise in supervision, and remedial and refresher training. Particular attention should be paid to the effective use of reminder functionality.
Monitor status of infrastructure	Fails to identify significant change in status of infrastructure Misinterprets location or status of infrastructure			*Incorrect understanding of status of infrastructure* (range of safety and operational consequences arise from decisions made based on incorrect understanding)					
Monitor conditions	Fails to identify significant change in status of infrastructure Misinterprets location or status of infrastructure			*Incorrect understanding of environmental conditions* (range of safety and operational consequences arise from decisions made based on incorrect understanding)					
Apply reminders	Fails to apply reminders when required Misunderstands reminders Fails to remove reminders when no longer required	No/wrong action No/wrong/partial information	Design of HMI reminder function Operational procedures for use of reminders	*Failure to recall important service information* (range of safety and operational consequences arise from decisions made based on incorrect understanding)					
3. Manage traffic									
Manage transitions onto/off	Fails to accept/release service onto/from area Accepts or releases service from area when it should be held	No/wrong action	Design of HMI - operator controls Design of HMI - support tools (automation) Complexity of traffic routing Operational procedures for normal service provision Operational procedures for abnormal, degraded, emergency conditions Distraction/workload	Service enters section that is not safe	Service interrupted unnecessarily	Interlocking prevents unsafe routes being set under normal circumstances Restrictive operational procedures maintain safety of movements under abnormal, degraded and emergency circumstances	SPAD alarms Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding.	Action of train protection system under normal operating conditions Movements under abnormal, degraded, emergency conditions are conducted at low speed	Evaluate and test operation of equipment and procedures in managing normal traffic operation and the full range of anticipated abnormal, degraded and emergency modes. Should liaise with Train Operating representatives to ensure that new operating procedures and service provision are suitable for all parties.
Manage movement authority	Fails to provide movement authority Fails to remove movement authority/order train stop when required Misroutes service	No/wrong action		Service enters section that is not safe Unnecessary train protection intervention	Service interrupted unnecessarily Unnecessary train protection intervention Service set to wrong destination				
Manage services	Misprioritises services at conflict point Fails to turn service early to maintain timetable	No/wrong action		n/a	Service runs late Service runs out of order	n/a	Timetable display indicating delay minutes Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding.	Recovery time in the timetable	

Activity	Failure Mode			Effects		Protection			Analysis
	Error	**Keyword**	**PSF**	**Safety**	**Operational**	**Prevention**	**Detection**	**Mitigation**	
4. Manage infrastructure									
Manage speed restrictions	Fails to set TSR Sets incorrect TSR Fails to remove TSR when no longer required	No/wrong action No/wrong/partial information	Design of HMI - operator controls Complexity of infrastructure under control Operational procedures for managing infrastructure under abnormal, degraded and emergency conditions Distraction/workload	Services permitted to operate at excessive speed	Services operating with unnecessary speed restriction	Interlocking prevents unsafe routes being set under normal circumstances Restrictive operational procedures maintain safety of movements under abnormal, degraded and emergency circumstances	Reporting from driver, fellow signallers, track workers or members of the public, or monitoring by supervisor correct mistaken understanding.	Action of train protection system under normal operating conditions Movements under abnormal, degraded, emergency conditions are conducted at low speed Track workers and members of the public are instructed to keep a good look out in vicinity of the railway	Evaluate and test operation of equipment and procedures in managing normal traffic operation and the full range of anticipated abnormal, degraded and emergency modes. Should liaise with Infrastructure maintenance representatives and public safety bodies to ensure that new operating procedures are suitable for all parties.
Manage points	Fails to set points manually when required Fails to protect failed points	No/wrong action		Services permitted to operate when points are not set correctly	Service interrupted unnecessarily				
Manage level crossings	Fails to protect failed level crossing Fails to return level crossing to full service when functionality restored Authorises user to cross when it is not safe to do so Instructs user to cross when it would otherwise be safe	No/wrong action No/wrong/partial information		Services permitted to operate over level crossing when it is not safe Road users permitted to use crossing when it is not safe	Service interrupted unnecessarily Road users prevented from using crossing unnecessarily				
Manage train detection	Fails to reset train detection when required Resets train detection when train is in section	No/wrong action No/wrong/partial information		Representation of service in signalling system compromised	Service interrupted unnecessarily				
Manage possessions	Fails to arrange protection for engineering possession when required Removes protection for engineering possession before track cleared	No/wrong action No/wrong/partial information		Exposure of on track workers to collision risk	Service interrupted unnecessarily Engineering work interrupted unnecessarily				
5. Manage communications									
Manage digital radio Manage analogue radio Manage telephone	Fails to pass on message or instruction Passes on incorrect or incomplete instruction	No/wrong action No/wrong/partial information	Design of HMI - communication system Distraction/workload	*Critical message not delivered or received* (range of safety and operational consequences arise from decisions made based on incorrect understanding)		Communication procedures	Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding.	n/a (no direct operational or safety consequences, but see protection provided for errors committed in managing traffic and managing infrastructure)	Should evaluate effectiveness of existing communication procedures when used with new communication systems, and ensure that all communicating parties are trained in their use

Figure 3 – Generic high-level Failure Modes Effects Analysis (FMEA) of the operator's errors in a new signalling control system task

Analysis

In this section we describe some of the details surrounding how the analysis would be conducted as part of a practical signalling project.

Development of the analysis through the project

The method can be commenced at the start of the project, and run through to its delivery. As the design matures and the signaller's role becomes better specified, the task analysis and FMEA can be continuously updated:

- *Concept stage* – high level task analysis and FMEA would allow high level operator requirements to be derived and general areas of human factors interest to be identified and entered into the project requirements database and human factors issues log for tracking through the project.
- *In design* – through each design iteration the task analysis would be updated and the FMEA would be used to make recommendations for further design developments or specification of procedures, identify additional human factors analyses to evaluate the effectiveness of the protection measures and support performance claims (detailed below).
- *Final design submission* - At the end of the design process, when all human factors issues have been addressed, the FMEA can be used to demonstrate the effective management of human hazards in the safety case. A mature version of the analysis presented in Figure 3 would show that hazards due to human error have been identified, that mitigation measures were specified and that the human hazards have been managed to a particular level, supporting a *tolerable and ALARP* safety argument. We have also applied the method to conduct an assessment of a new system compared to a baseline operation (the system that is being replaced). By presenting the different protection available under the different systems on the same chart, the additional protection available under the new system can be directly demonstrated to support an argument for relative safety and operational performance (*no worse or better than*).

Leading into other human factors activities

The FMEA, when started early in the design process can be a useful way to identify additional human factors analyses that can support design development and provide evidence to justify performance claims. Supporting human factors analyses would include:

- *Evaluation of equipment usability, to ensure that the HMI design is suitable for operations*. This can be accomplished by application of usability best-practice and following industry conventions in initial design steps, review of static prototypes by representative operators and interface experts, and the evaluation of increasingly faithful interactive prototypes under representative operating conditions. The FMEA can be used to identify particular tasks or scenarios where the usability of the system makes a contribution to overall system performance.
- *Analysis of workload to demonstrate task feasibility*. This can be accomplished either using human factors performance modelling methods (Parks and Boucek, 1988; Hamilton, Lowe and Blanchard, 2004) or by taking workload measures from operators performing the task in a simulator. The FMEA can be used to identify particular tasks or scenarios where high workload would be disruptive to the safe operation of the system.
- *Quantitative human reliability analysis*. Particularly important signaller errors, for example those for which no protection is provided, or for which the consequences of failure are severe, can be identified by screening the FMEA. These errors can be made the subject of detailed human reliability analysis to ensure that performance in these tasks is sufficiently reliable to allow overall system reliability claims to be supported. This process can either be completed as part of the human factors work, or under the safety assessment, for example in a fault tree analysis of the system. Human reliability values can be obtained either from human factors techniques (such as the Human Error Assessment and Reduction Technique, HEART, Williams, 1985), from compendia of human reliability data (Kirwin, Basra, and Taylor-Adams, 1997) or from observation of operators performing under representative conditions, for example in a simulator.
- *Supporting the development of operational procedures*. The FMEA can help identify particular situations where reduced protection is provided by the equipment (abnormal, degraded and emergency conditions) where the operational procedures must be developed to ensure safe

operation is maintained. As these procedures are developed they can be included in the analysis.

Conclusion

We have found FMEA a suitable technique for the investigation, analysis and presentation of potential operator error in new signalling system systems. We argue that such analysis is particularly important at this time when signalling systems are the subject of rapid technical development, introducing new responsibilities and tasks to the human operators.

We believe that this approach offers a project team a way to evaluate the contribution of the human operators to the safe and efficient operation of new signalling systems in a way that satisfies regulatory requirements, follows best-practice and conducts the human factors work within a structure fits in with the safety and operational case structure.

References

1. **Embrey, D.E., (1986).** SHERPA: a systematic human error reduction and prediction approach. Paper presented at the *International Topical Meeting on Advances in Human Factors in Nuclear Power Systems*, Knoxville, Tennessee.

2. **Hamilton, W. I., Lowe, C., and Blanchard, H., 2004**. Cognitive Task Analysis and Performance Modelling for Early Human Systems Integration, in *Proceedings of the Annual Meeting of the Human Factors and Ergonomics Society, 2004*.

3. **Health and Safety Executive, 2001.** *Proposed framework for addressing human factors in IEC 61508.* 373/2001. HSE Books.

4. **Kirwan, B., Basra, G., and Taylor-Adams, S.E. 1997**. CORE-DATA: a computerised human error database for human reliability support. *In Proceedings of the Sixth IEEE Conference on Human Factors and Power Plants, 1997*.

5. **Network Rail, 2004.** *Incorporating Ergonomics Within Engineering Design Projects: Guidance Note*. NR/GN/ERG/00027, issue 02, April 2004.

6. **Parks D. L. and Boucek G. P. (1988).** Workload Prediction, Diagnosis and Continuing Challenges. In G. McMillan et al. (eds) *Applications Of Human Performance Models To System Design*, New York: Plenum Press.

7. **Railway Safety and Standards Board, 2007.** *Engineering safety management: the yellow book*. Volume 1&2, Fundamentals and Guidance, Issue 04. 2007.

8. **Shepherd, A., 1992.** HTA as a framework for task analysis. *Ergonomics*, volume 41, pp. 1537-1552.

9. **Shorrock, S.T., and Kirwan, B., 1999.** TRACE-r: a technique for the restrospective identification of cognitive errors in ATM. In D. Harris (Ed.) *Engineering Psychology and Cognitive Ergonomics. Volume Three- Transportation Systems, Medical Ergonomics and Training*. Aldershot, UK: Ashgate.

10. **Williams, J.C., 1985**. A proposed method for achieving high reliability in process operation by means of human factors engineering technology. In *Proceedings of a Symposium on the Achievement of Reliability in Operating Plant*, Safety and Reliability Society. NEC, Birmingham.[i]

[i]Services are provided by members of the Lloyd's Register Group. Lloyd's Register, Lloyd's Register EMEA and Lloyd's Register Asia are exempt charities under the UK Charities Act 1993. For more information see www.lr.org/entities.