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.

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](image)

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

<table>
<thead>
<tr>
<th>FMEA Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>The signaller’s generic operational activity, taken from the task analysis.</td>
</tr>
<tr>
<td>Failure mode</td>
<td>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).</td>
</tr>
<tr>
<td>Effects</td>
<td>Records the consequences of the signaller error upon the safety or operational performance of the system.</td>
</tr>
<tr>
<td>Protection</td>
<td>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.</td>
</tr>
<tr>
<td>Analysis</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Activity</th>
<th>Failure Mode</th>
<th>Error</th>
<th>PSF</th>
<th>Safety</th>
<th>Operational</th>
<th>Protection</th>
<th>Mitigation</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Manage control system</td>
<td>Log in/off</td>
<td>Fail to set password</td>
<td>Reaction</td>
<td>Wrong information</td>
<td>Complexity of log in process/ frequency of use</td>
<td>Operation by incorrect personnel</td>
<td>Authorised personnel unable to operate</td>
<td>VOA</td>
</tr>
<tr>
<td></td>
<td>Configure operating modes</td>
<td>Sets SCC in wrong operating mode of configuration</td>
<td>Wrong action</td>
<td>Complexity of setup or configuration</td>
<td>Instructions regarding correct setup for service</td>
<td>Operation of system with incorrect mode/configuration</td>
<td>Operation of system with incorrect mode/configuration</td>
<td>Operating modes and setup published in periodic operating notice issued to supervisor and discussed with staff</td>
</tr>
<tr>
<td>2. Monitor railway under control</td>
<td>Monitor location and status of services</td>
<td>Fails to identify significant change in location or status of services</td>
<td>No information</td>
<td>Wrong information</td>
<td>Partial information</td>
<td>Design of HMI displays accuracy of information</td>
<td>Distraction/workload</td>
<td>Incorrect understanding of location/status of services (range of safety and operational consequences arise from decisions made based on incorrect understanding)</td>
</tr>
<tr>
<td></td>
<td>Monitor status of infrastructure</td>
<td>Fails to identify significant change in status of infrastructure</td>
<td>No information</td>
<td>Wrong information</td>
<td>Partial information</td>
<td>Design of HMI displays accuracy of information</td>
<td>Distraction/workload</td>
<td>Incorrect understanding of status of infrastructure (range of safety and operational consequences arise from decisions made based on incorrect understanding)</td>
</tr>
<tr>
<td></td>
<td>Monitor conditions</td>
<td>Fails to identify significant change in status of infrastructure</td>
<td>No information</td>
<td>Wrong information</td>
<td>Partial information</td>
<td>Design of HMI displays accuracy of information</td>
<td>Distraction/workload</td>
<td>Incorrect understanding of environmental conditions (range of safety and operational consequences arise from decisions made based on incorrect understanding)</td>
</tr>
<tr>
<td></td>
<td>Apply reminders</td>
<td>Fails to apply reminders when required</td>
<td>No action</td>
<td>No action</td>
<td>No action</td>
<td>Design of HMI reminder</td>
<td>Operational procedures for use of reminders</td>
<td>Function to recall important service information arising from incorrect understanding</td>
</tr>
<tr>
<td>3. Manage traffic</td>
<td>Manage transitions onto/off</td>
<td>Fails to accept/release service onto/from area</td>
<td>No action</td>
<td>No action</td>
<td>No action</td>
<td>Design of HMI – supports tools (automation, simplicity of traffic light settings)</td>
<td>Service enters section that is not safe</td>
<td>Service interrupted unnecessarily</td>
</tr>
<tr>
<td></td>
<td>Manage movement authority</td>
<td>Fails to provide movement authority to train when required</td>
<td>No action</td>
<td>No action</td>
<td>No action</td>
<td>Operational procedures for normal service provision</td>
<td>Service enters section that is not safe</td>
<td>Unnecessary train protection intervention</td>
</tr>
<tr>
<td></td>
<td>Manage services</td>
<td>Misroutes services at conflict point</td>
<td>No action</td>
<td>No action</td>
<td>No action</td>
<td>Design of HMI – supports tools (automation, simplicity of traffic light settings)</td>
<td>Service runs late</td>
<td>Service runs late out of order</td>
</tr>
</tbody>
</table>

**Notes:**
- **Activity:** Includes all activities related to managing control system, monitoring railway under control, and managing traffic.
- **Failure Mode:** Lists the failure modes that can occur during each activity.
- **Error:** Specifies the type of error that can occur.
- **PSF:** Provides a list of potential safety, security, and privacy factors.
- **Safety:** Indicates the safety implications of the failure mode.
- **Operational:** Specifies the operational aspects of the failure mode.
- **Protection:** Lists the protective measures that can be taken.
- **Mitigation:** Details the mitigation strategies.
- **Analysis:** Summarizes the analysis of the failure mode and its implications.
<table>
<thead>
<tr>
<th>Activity</th>
<th>Failure Mode</th>
<th>Effects</th>
<th>Protection</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4. Manage infrastructure</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage speed restrictions</td>
<td>Fails to set TSR</td>
<td>Incorrect action</td>
<td>Services permitted to operate at excessive speed</td>
<td>Evaluate and test operation of equipment and procedures in managing normal traffic operation and the full range of anticipated abnormal, degraded and emergency modes.</td>
</tr>
<tr>
<td></td>
<td>Fails to remove TSR when no longer required</td>
<td>Incorrect action</td>
<td>Services permitted to operate at unnecessary speed restriction</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fails to set correct TSR</td>
<td>Incorrect action</td>
<td>Services permitted to operate at unnecessary speed restriction</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fails to remove TSR when no longer required</td>
<td>Incorrect action</td>
<td>Services permitted to operate at unnecessary speed restriction</td>
<td></td>
</tr>
<tr>
<td>Manage points</td>
<td>Fails to set points manually when required</td>
<td>Incorrect action</td>
<td>Services permitted to operate when points are not set correctly</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fails to protect failed points</td>
<td>Incorrect action</td>
<td>Services permitted to operate when points are not set correctly</td>
<td></td>
</tr>
<tr>
<td>Manage level crossings</td>
<td>Fails to protect failed level crossing</td>
<td>Incorrect action</td>
<td>Services permitted to operate over level crossing when it is not safe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fails to return level crossing to full service when functionality restored</td>
<td>Incorrect action</td>
<td>Services permitted to operate over level crossing when it is not safe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fails to instruct users to keep a good look out in vicinity of the railway</td>
<td>Incorrect action</td>
<td>Services permitted to operate over level crossing when it is not safe</td>
<td></td>
</tr>
<tr>
<td>Manage train detection</td>
<td>Fails to ensure train detection when required</td>
<td>Incorrect action</td>
<td>Services permitted to operate over level crossing when it is not safe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fails to ensure train detection when train is in section</td>
<td>Incorrect action</td>
<td>Services permitted to operate over level crossing when it is not safe</td>
<td></td>
</tr>
<tr>
<td>Manage possessions</td>
<td>Fails to arrange protection for engineering possession when required</td>
<td>Incorrect action</td>
<td>Services permitted to operate over level crossing when it is not safe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fails to remove protection for engineering possession before track cleared</td>
<td>Incorrect action</td>
<td>Services permitted to operate over level crossing when it is not safe</td>
<td></td>
</tr>
<tr>
<td><strong>5. Manage communications</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage digital radio</td>
<td>Fails to pass on message or instruction</td>
<td>Incorrect action</td>
<td>Services permitted to operate over level crossing when it is not safe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Passes on incorrect or incomplete instruction</td>
<td>Incorrect action</td>
<td>Services permitted to operate over level crossing when it is not safe</td>
<td></td>
</tr>
<tr>
<td>Manage analogue radio</td>
<td>Fails to pass on message or instruction</td>
<td>Incorrect action</td>
<td>Services permitted to operate over level crossing when it is not safe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Passes on incorrect or incomplete instruction</td>
<td>Incorrect action</td>
<td>Services permitted to operate over level crossing when it is not safe</td>
<td></td>
</tr>
<tr>
<td>Manage telephone</td>
<td>Fails to pass on message or instruction</td>
<td>Incorrect action</td>
<td>Services permitted to operate over level crossing when it is not safe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Passes on incorrect or incomplete instruction</td>
<td>Incorrect action</td>
<td>Services permitted to operate over level crossing when it is not safe</td>
<td></td>
</tr>
</tbody>
</table>

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**


'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.