Lloyd's Register: Human Engineering Limited

# Human Error Assessment in the Design of New Signalling Control Centres

IRSC 2010 – Hong Kong, 5th October, PM Session 1

Harry Blanchard – Senior Human Factors Consultant
Human Engineering Limited

250 YEARS OF SERVICE

Lloyd's Register
LIFE MATTERS

# Human Error

- Human error is important
  - Regulatory: *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.* (Yellow Book 4, Section 3.3, p.26)

- Human error is particularly important in new signalling systems
  - For example: ETCS, TVM-430, LBZ, CTCS-3
  - New equipment, new responsibilities and new tasks
  - Late identification can result in:
    - Higher rate of incidents, reduced system availability
    - Expensive remedial work, additional operating restriction, compromised procedures, additional staffing, increased preventative and corrective maintenance
    - Unexpected catastrophic failures

- Human error is complex, but it is not mysterious!
  - Method we have developed in working in new signalling systems

# A word about the problem

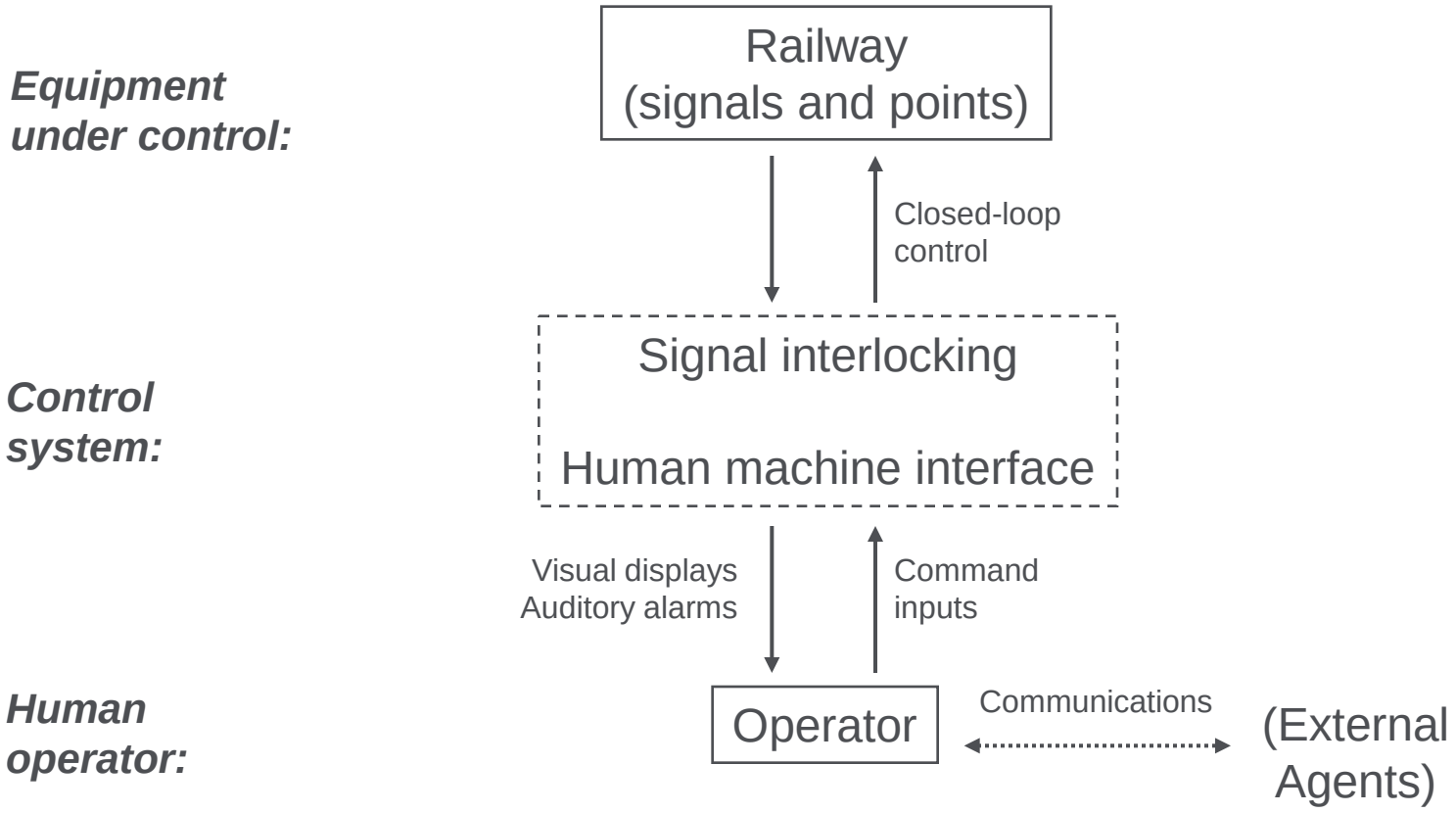
- A word about the problem: *prospective* human error analysis
  - Cannot be directly observed must be derived by analysis of the proposed system, inference from past systems, reference to similar systems
  - Systems are new, must be adapted to local operating circumstances, projects are subject to cost and technical constraints
- How to address the problem
  - Systematic error identification process, driven by the operating tasks
  - Identify the potential safety and operational consequences for the system
  - Explicitly represent the protection made available through the procedures and equipment
- Existing techniques include SHERPA and THERP
  - Strengths and weaknesses

# Method

- Procedure
  1. Description of proposed operation
  2. Task analysis
  3. Failure Modes Effects Analysis

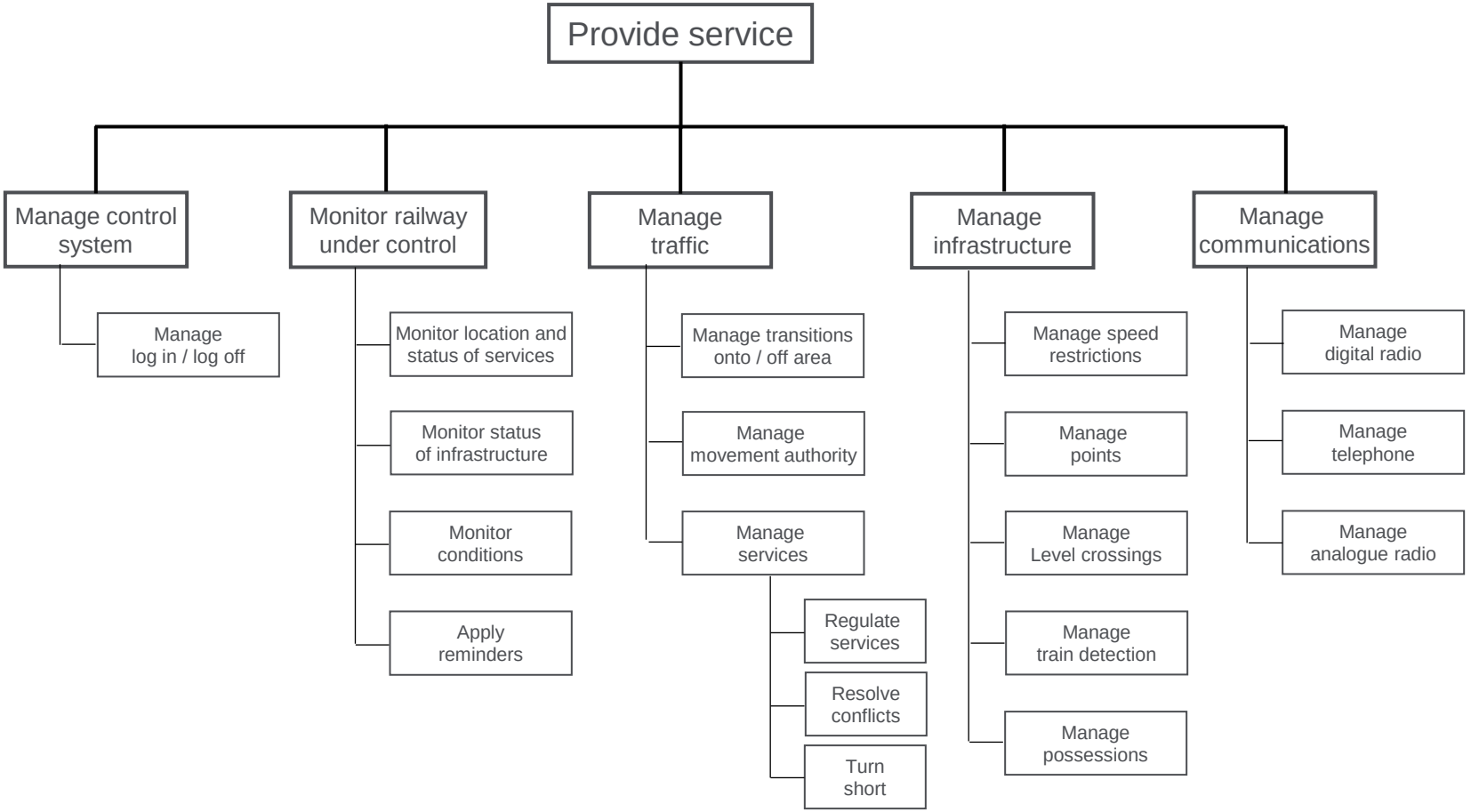
- Application
  - Through the project design cycle
    - Planning the work
    - Supporting design
    - Submitting the design
  - In supporting other human factors analyses

# 1. Description of proposed operation




- Populated by review of system supplier manuals, proposed operating procedures, interview and observation
- Reviewed in workshop to confirm accurate and realistic
- Periodic updates to reflect design developments

# 2. Task analysis




- Populated by review of system supplier manuals, proposed operating procedures, interview and observation
- Reviewed in workshop to confirm accurate and realistic
- Periodic updates to reflect design developments

# 3. Failure Mode Effects Analysis

| Activity | Failure Mode | | | Effects | | Protection | | | Analysis |
|---|---|---|---|---|---|---|---|---|---|
| | Error | Keyword | PSF | Safety | Operational | Prevention | Detection | Mitigation | |
| **Manage control system** | | | | | | | | | |
| Log in/off | Fail to set password protection<br>Forgets password | No action<br>Wrong information | Complexity of log in process<br>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<br>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 |
| **Monitor railway under control** | | | | | | | | | |
| Monitor location and status of services | Fails to identify significant change in location or status of services<br>Misinterprets location or status of services | No information<br>Wrong information<br>Partial information | Design of HMI information displays<br>Accuracy of information<br>Distraction/workload | *Incorrect understanding of location and status of services*<br>(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.<br><br>Difficult to detect and correct a misunderstanding by the operator, but other staff may help identify error.<br><br>Should ensure that operators are trained to anticipate emerging situations ("situational awareness"), emphasise in supervision, and remedial and refresher training.<br><br>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<br>Misinterprets location or status of infrastructure | | | *Incorrect understanding of status of infrastructure*<br>(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<br>Misinterprets location or status of infrastructure | | | *Incorrect understanding of environmental conditions*<br>(range of safety and operational consequences arise from decisions made based on incorrect understanding) | | | | | |
| Apply reminders | Fails to apply reminders when required<br>Misunderstands reminders<br>Fails to remove reminders when no longer required | No/wrong action<br>No/wrong/partial information | Design of HMI reminder function<br>Operational procedures for use of reminders | *Failure to recall important service information*<br>(range of safety and operational consequences arise from decisions made based on incorrect understanding) | | | | | |
| **Manage traffic** | | | | | | | | | |
| Manage transitions onto/off | Fails to accept/release service onto/from area<br>Accepts or releases service from area when it should be held | No/wrong action | Design of HMI - operator controls<br>Design of HMI - support tools (automation)<br>Complexity of traffic routing<br>Operational procedures for normal service provision<br>Operational procedures for abnormal, degraded, emergency conditions<br>Distraction/workload | Service enters section that is not safe | Service interrupted unnecessarily | Interlocking prevents unsafe routes being set under normal circumstances<br>Restrictive operational procedures maintain safety of movements under abnormal, degraded and emergency circumstances | SPAD alarms<br>Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding. | Action of train protection system under normal operating conditions<br>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.<br><br>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<br>Fails to remove movement authority/order train stop when required<br>Misroutes service | No/wrong action | | Service enters section that is not safe<br>Unnecessary train protection intervention | Service interrupted unnecessarily<br>Unnecessary train protection intervention<br>Service set to wrong destination | | | | |
| Manage services | Misprioritises services at conflict point<br>Fails to turn service early to maintain timetable | No/wrong action | | n/a | Service runs late<br>Service runs out of order | n/a | Timetable display indicating delay minutes<br>Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding. | Recovery time in the timetable | |
| **Manage infrastructure** | | | | | | | | | |
| Manage speed restrictions | Fails to set TSR<br>Sets incorrect TSR<br>Fails to remove TSR when no longer required | No/wrong action<br>No/wrong/partial information | Design of HMI - operator controls<br>Complexity of infrastructure under control<br>Operational procedures for managing infrastructure under abnormal, degraded and emergency conditions<br>Distraction/workload | Services permitted to operate at excessive speed | Services operating with unnecessary speed restriction | Interlocking prevents unsafe routes being set under normal circumstances<br>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<br>Movements under abnormal, degraded, emergency conditions are conducted at low speed<br>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.<br><br>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<br>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<br>Fails to return level crossing to full service when functionality restored<br>Authorises user to cross when it is not safe to do so<br>Instructs user to cross when it would otherwise be safe | No/wrong action<br>No/wrong/partial information | | Services permitted to operate over level crossing when it is not safe<br>Road users permitted to use crossing when it is not safe | Service interrupted unnecessarily<br>Road users prevented from using crossing unnecessarily | | | | |
| Manage train detection | Fails to reset train detection when required<br>Resets train detection when train is in section | No/wrong action<br>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<br>Removes protection for engineering possession before track cleared | No/wrong action<br>No/wrong/partial information | | Exposure of on track workers to collision risk | Service interrupted unnecessarily<br>Engineering work interrupted unnecessarily | | | | |
| **Manage communications** | | | | | | | | | |
| Manage digital radio<br>Manage analogue radio<br>Manage telephone | Fails to pass on message or instruction<br>Passes on incorrect or incomplete instruction | No/wrong action<br>No/wrong/partial information | Design of HMI - communication system<br>Distraction/workload | *Critical message not delivered or received*<br>(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 |

# Failure Mode Effects Analysis - headings

| 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. |

# Failure Mode Effects Analysis - detail

| Activity | Failure Mode | | | Effects | | Protection | | | Analysis |
|---|---|---|---|---|---|---|---|---|---|
| | Error | Keyword | PSF | Safety | Operational | Prevention | Detection | Mitigation | |
| **Monitor railway under control** | | | | | | | | | |
| Monitor location and status of services | Fails to identify significant change in location or status of services<br>Misinterprets location or status of services | No information<br>Wrong information<br>Partial information | Design of HMI information displays<br>Accuracy of information<br>Distraction/workload | *Incorrect understanding of location and status of services*<br>(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.<br><br>Difficult to detect and correct a misunderstanding by the operator, but other staff may help identify error.<br><br>Should ensure that operators are trained to anticipate emerging situations ("situational awareness"), emphasise in supervision, and remedial and refresher training.<br><br>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<br>Misinterprets location or status of infrastructure | | | *Incorrect understanding of status of infrastructure*<br>(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<br>Misinterprets location or status of infrastructure | | | *Incorrect understanding of environmental conditions*<br>(range of safety and operational consequences arise from decisions made based on incorrect understanding) | | | | | |
| Apply reminders | Fails to apply reminders when required<br>Misunderstands reminders<br>Fails to remove reminders when no longer required | No/wrong action<br>No/wrong/partial information | Design of HMI reminder function<br>Operational procedures for use of reminders | *Failure to recall important service information*<br>(range of safety and operational consequences arise from decisions made based on incorrect understanding) | | | | | |
| **Manage traffic** | | | | | | | | | |
| Manage transitions onto/off | Fails to accept/release service onto/from area<br>Accepts or releases service from area when it should be held | No/wrong action | Design of HMI - operator controls<br>Design of HMI - support tools (automation)<br>Complexity of traffic routing<br>Operational procedures for normal service provision<br>Operational procedures for abnormal, degraded, emergency conditions<br>Distraction/workload | Service enters section that is not safe | Service interrupted unnecessarily | Interlocking prevents unsafe routes being set under normal circumstances<br>Restrictive operational procedures maintain safety of movements under abnormal, degraded and emergency circumstances | SPAD alarms<br>Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding. | Action of train protection system under normal operating conditions<br>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.<br><br>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<br>Fails to remove movement authority/order train stop when required<br>Misroutes service | No/wrong action | | Service enters section that is not safe<br>Unnecessary train protection intervention | Service interrupted unnecessarily<br>Unnecessary train protection intervention<br>Service set to wrong destination | | | | |
| Manage services | Misprioritises services at conflict point<br>Fails to turn service early to maintain timetable | No/wrong action | | n/a | Service runs late<br>Service runs out of order | n/a | Timetable display indicating delay minutes<br>Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding. | Recovery time in the timetable | |

# Failure Mode Effects Analysis - activity

| Activity | Failure Mode | | | Effects | | Protection | | | Analysis |
|---|---|---|---|---|---|---|---|---|---|
| | Error | Keyword | PSF | Safety | Operational | Prevention | Detection | Mitigation | |
| **Monitor railway under control** | | | | | | | | | |
| Monitor location and status of services | Fails to identify significant change in location or status of services<br>Misinterprets location or status of services | No information<br>Wrong information<br>Partial information | Design of HMI information displays<br>Accuracy of information<br>Distraction/workload | *Incorrect understanding of location and status of services*<br>(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.<br><br>Difficult to detect and correct a misunderstanding by the operator, but other staff may help identify error.<br><br>Should ensure that operators are trained to anticipate emerging situations ("situational awareness"), emphasise in supervision, and remedial and refresher training.<br><br>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<br>Misinterprets location or status of infrastructure | | | *Incorrect understanding of status of infrastructure*<br>(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<br>Misinterprets location or status of infrastructure | | | *Incorrect understanding of environmental conditions*<br>(range of safety and operational consequences arise from decisions made based on incorrect understanding) | | | | | |
| Apply reminders | Fails to apply reminders when required<br>Misunderstands reminders<br>Fails to remove reminders when no longer required | No/wrong action<br>No/wrong/partial information | Design of HMI reminder function<br>Operational procedures for use of reminders | *Failure to recall important service information*<br>(range of safety and operational consequences arise from decisions made based on incorrect understanding) | | | | | |
| **Manage traffic** | | | | | | | | | |
| Manage transitions onto/off | Fails to accept/release service onto/from area<br>Accepts or releases service from area when it should be held | No/wrong action | Design of HMI - operator controls<br>Design of HMI - support tools (automation)<br>Complexity of traffic routing<br>Operational procedures for normal service provision<br>Operational procedures for abnormal, degraded, emergency conditions | Service enters section that is not safe | Service interrupted unnecessarily | Interlocking prevents unsafe routes being set under normal circumstances<br>Restrictive operational procedures maintain safety of movements under abnormal, degraded and emergency circumstances | SPAD alarms<br>Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding. | Action of train protection system under normal operating conditions<br>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.<br><br>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<br>Fails to remove movement authority/order train stop when required<br>Misroutes service | No/wrong action | | Service enters section that is not safe<br>Unnecessary train protection intervention | Service interrupted unnecessarily<br>Unnecessary train protection intervention<br>Service set to wrong destination | | | | |
| Manage services | Misprioritises services at conflict point<br>Fails to turn service early to maintain timetable | No/wrong action | Distraction/workload | n/a | Service runs late<br>Service runs out of order | n/a | Timetable display indicating delay minutes<br>Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding. | Recovery time in the timetable | |

- "Activity" column, taken from task analysis

# Failure Mode Effects Analysis – failure modes

| Activity | Failure Mode | | | Effects | | Protection | | | Analysis |
|---|---|---|---|---|---|---|---|---|---|
| | Error | Keyword | PSF | Safety | Operational | Prevention | Detection | Mitigation | |
| **Monitor railway under control** | | | | | | | | | |
| Monitor location and status of services | Fails to identify significant change in location or status of services<br>Misinterprets location or status of services | No information<br>Wrong information<br>Partial information | Design of HMI information displays<br>Accuracy of information<br>Distraction/workload | *Incorrect understanding of location and status of services*<br>(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.<br><br>Difficult to detect and correct a misunderstanding by the operator, but other staff may help identify error.<br><br>Should ensure that operators are trained to anticipate emerging situations ("situational awareness"), emphasise in supervision, and remedial and refresher training.<br><br>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<br>Misinterprets location or status of infrastructure | | | *Incorrect understanding of status of infrastructure*<br>(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<br>Misinterprets location or status of infrastructure | | | *Incorrect understanding of environmental conditions*<br>(range of safety and operational consequences arise from decisions made based on incorrect understanding) | | | | | |
| Apply reminders | Fails to apply reminders when required<br>Misunderstands reminders<br>Fails to remove reminders when no longer required | No/wrong action<br>No/wrong/partial information | Design of HMI reminder function<br>Operational procedures for use of reminders | *Failure to recall important service information*<br>(range of safety and operational consequences arise from decisions made based on incorrect understanding) | | | | | |
| **Manage traffic** | | | | | | | | | |
| Manage transitions onto/off | Fails to accept/release service onto/from area<br>Accepts or releases service from area when it should be held | No/wrong action | Design of HMI - operator controls<br>Design of HMI - support tools (automation)<br>Complexity of traffic routing<br>Operational procedures for normal service provision<br>Operational procedures for abnormal, degraded, emergency conditions | Service enters section that is not safe | Service interrupted unnecessarily | Interlocking prevents unsafe routes being set under normal circumstances<br>Restrictive operational procedures maintain safety of movements under abnormal, degraded and emergency circumstances | SPAD alarms<br>Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding. | Action of train protection system under normal operating conditions<br>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.<br><br>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<br>Fails to remove movement authority/order train stop when required<br>Misroutes service | No/wrong action | | Service enters section that is not safe<br>Unnecessary train protection intervention | Service interrupted unnecessarily<br>Unnecessary train protection intervention<br>Service set to wrong destination | | | | |
| Manage services | Misprioritises services at conflict point<br>Fails to turn service early to maintain timetable | No/wrong action | Distraction/workload | n/a | Service runs late<br>Service runs out of order | n/a | Timetable display indicating delay minutes<br>Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding. | Recovery time in the timetable | |

- Failure modes identified through application of error keywords, first by analyst, then at workshop (hazop)

# Failure Mode Effects Analysis – effects and protection

| Activity | Failure Mode | | | Effects | | Protection | | | Analysis |
|---|---|---|---|---|---|---|---|---|---|
| | Error | Keyword | PSF | Safety | Operational | Prevention | Detection | Mitigation | |
| **Monitor railway under control** | | | | | | | | | |
| Monitor location and status of services | Fails to identify significant change in location or status of services<br>Misinterprets location or status of services | No information<br>Wrong information<br>Partial information | Design of HMI information displays<br>Accuracy of information<br>Distraction/workload | *Incorrect understanding of location and status of services*<br>(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.<br><br>Difficult to detect and correct a misunderstanding by the operator, but other staff may help identify error.<br><br>Should ensure that operators are trained to anticipate emerging situations ("situational awareness"), emphasise in supervision, and remedial and refresher training.<br><br>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<br>Misinterprets location or status of infrastructure | | | *Incorrect understanding of status of infrastructure*<br>(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<br>Misinterprets location or status of infrastructure | | | *Incorrect understanding of environmental conditions*<br>(range of safety and operational consequences arise from decisions made based on incorrect understanding) | | | | | |
| Apply reminders | Fails to apply reminders when required<br>Misunderstands reminders<br>Fails to remove reminders when no longer required | No/wrong action<br>No/wrong/partial information | Design of HMI reminder function<br>Operational procedures for use of reminders | *Failure to recall important service information*<br>(range of safety and operational consequences arise from decisions made based on incorrect understanding) | | | | | |
| **Manage traffic** | | | | | | | | | |
| Manage transitions onto/off | Fails to accept/release service onto/from area<br>Accepts or releases service from area when it should be held | No/wrong action | Design of HMI - operator controls<br>Design of HMI - support tools (automation)<br>Complexity of traffic routing<br>Operational procedures for normal service provision<br>Operational procedures for abnormal, degraded emergency conditions | Service enters section that is not safe | Service interrupted unnecessarily | Interlocking prevents unsafe routes being set under normal circumstances<br>Restrictive operational procedures maintain safety of movements under abnormal, degraded and emergency circumstances | SPAD alarms<br>Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding. | Action of train protection system under normal operating conditions<br>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.<br><br>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<br>Fails to remove movement authority/order train stop when required<br>Misroutes service | No/wrong action | | Service enters section that is not safe<br>Unnecessary train protection intervention | Service interrupted unnecessarily<br>Unnecessary train protection intervention<br>Service set to wrong destination | | | | |
| Manage services | Misprioritises services at conflict point<br>Fails to turn service early to maintain timetable | No/wrong action | Distraction/workload | n/a | Service runs late<br>Service runs out of order | n/a | Timetable display indicating delay minutes<br>Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding. | Recovery time in the timetable | |

- Effects and protection derived from understanding of system architecture

# Failure Mode Effects Analysis - analysis

| Activity | Failure Mode | | | Effects | | Protection | | | Analysis |
|---|---|---|---|---|---|---|---|---|---|
| | Error | Keyword | PSF | Safety | Operational | Prevention | Detection | Mitigation | |
| **Monitor railway under control** | | | | | | | | | |
| Monitor location and status of services | Fails to identify significant change in location or status of services<br>Misinterprets location or status of services | No information<br>Wrong information<br>Partial information | Design of HMI information displays<br>Accuracy of information<br>Distraction/workload | *Incorrect understanding of location and status of services*<br>(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 consequence, 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.<br><br>Difficult to detect and correct a misunderstanding by the operator, but other staff may help identify error.<br><br>Should ensure that operators are trained to anticipate emerging situations ("situational awareness"), emphasise in supervision, and remedial and refresher training.<br><br>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<br>Misinterprets location or status of infrastructure | | | *Incorrect understanding of status of infrastructure*<br>(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<br>Misinterprets location or status of infrastructure | | | *Incorrect understanding of environmental conditions*<br>(range of safety and operational consequences arise from decisions made based on incorrect understanding) | | | | | |
| Apply reminders | Fails to apply reminders when required<br>Misunderstands reminders<br>Fails to remove reminders when no longer required | No/wrong action<br>No/wrong/partial information | Design of HMI reminder function<br>Operational procedures for use of reminders | *Failure to recall important service information*<br>(range of safety and operational consequences arise from decisions made based on incorrect understanding) | | | | | |
| **Manage traffic** | | | | | | | | | |
| Manage transitions onto/off | Fails to accept/release service onto/from area<br>Accepts or releases service from area when it should be held | No/wrong action | Design of HMI - operator controls<br>Design of HMI - support tools (automation)<br>Complexity of traffic routing<br>Operational procedures for normal service provision<br>Operational procedures for abnormal, degraded, emergency conditions | Service enters section that is not safe | Service interrupted unnecessarily | Interlocking prevents unsafe routes being set under normal circumstances<br>Restrictive operational procedures maintain safety of movements under abnormal, degraded and emergency circumstances | SPAD alarms<br>Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding. | Action of train protection system under normal operating conditions<br>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.<br><br>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<br>Fails to remove movement authority/order train stop when required<br>Misroutes service | No/wrong action | | Service enters section that is not safe<br>Unnecessary train protection intervention | Service interrupted unnecessarily<br>Unnecessary train protection intervention<br>Service set to wrong destination | | | | |
| Manage services | Misprioritises services at conflict point<br>Fails to turn service early to maintain timetable | No/wrong action | Distraction/workload | n/a | Service runs late<br>Service runs out of order | n/a | Timetable display indicating delay minutes<br>Reporting from driver, fellow signallers, or monitoring by supervisor correct mistaken understanding. | Recovery time in the timetable | |

- Analysis column – direct by stage of development…

# Applying the method

- At different project stages
  - Concept stage: high level operator requirements, initial human factors issues
  - In design: iterative, update and make recommendations for design and procedures, identify supporting analyses
  - Final submission: demonstration that errors identified have been controlled
    - *Tolerable and ALARP*
    - Also, *No worse or better than*

# Further human factors analysis

- Leading into other human factors analyses:
  - Evaluation of equipment usability, ensure HMIs are suitable
    - Best practice in design, user review, interactive evaluation in realistic environment
    - FMEA identifies operations where HMI usability contributes to safe efficient performance
  - Analysis of workload, ensure tasks are feasible
    - Through workload analysis, past performance or observation in simulator
    - FMEA identifies scenarios where high workload can disrupt safe operations
  - Quantitative human error, ensure tasks can be completed reliably
    - Through error analysis, past performance or observation in simulator
    - FMEA identifies critical human errors, where protection is reduced and consequences are severe
  - Support development of operational procedures
    - FMEA identifies circumstances where reduced protection is available from the equipment, and robust procedures must be in place

# Conclusion

- Combination of
  - human factors techniques (task analysis, error identification) and system safety management technique (FMEA)
- Has proved suitable for managing operator error in new signalling systems
  - Structured error identification
  - Represents potential consequences of different errors
  - Represents protection provided by equipment and procedures
- Follows best-practice, satisfies regulatory requirements and fits in with other safety and performance management work
  - Flexible enough to be used throughout project design cycle
  - Supports other human factors work

For more information, please contact:


## Karl Rich
Principal Human Factors Consultant

Human Engineering Limited
Shore House, 68 Westbury Hill
Bristol, BS9 3AA

T +44 (0) 117 962 0888
E Karl.Rich@humaneng.co.uk

## Harry Blanchard
Senior Human Factors Consultant

Human Engineering Limited
71 Fenchurch Street
London, EC3M 4BS

T +44 (0) 207 423 2320
E Harry.Blanchard@humaneng.co.uk