iESM

BROUGHT TO YOU BY ARC

international Engineering Safety Management

GOOD PRACTICE GUIDANCE

APPLICATION NOTE 8
APPLICATION FOR HUMAN FACTORS WITHIN ENGINEERING SAFETY MANAGEMENT

Published on behalf of the international railway industry
by Abbott Risk Consulting Ltd.
Issue 1.2 October 2022

arc

CONTENTS

Issue 1.2

DISCLAIMER

Abbott Risk Consulting Limited (ARC) and the other organizations and individuals involved in preparing this handbook have taken trouble to make sure that the handbook is accurate and useful, but it is only a guide. We do not give any form of guarantee that following the guidance in this handbook will be enough to ensure safety. We will not be liable to pay compensation to anyone who uses this handbook.

ACKNOWLEDGEMENTS

This handbook has been written with help from the people listed below.

- D Beacham
- Dr G Bearfield
- S Bickley
- N Bowley
- M Castles
- P Cheeseman
- Dr Chen Roger Lei
- J-M Cloarec
- Dr R Davis
- B Elliott
- Ms S Heape
- T Jones
- Dr KM Leung
- C Lowe
- Ms S Milner
- Ms J Myde
- Ng Nelson Wai Hung
- G Parris
- Sen Paul HB
- Mrs Shi Lisa
- G Topham
- N Winchester
- Dr Fei Yan
- Dr Zhang Simon

These people worked for the organizations listed below.

- Abbott Risk Consulting Ltd.
- Acmena Group Pty Ltd
- Arbutus Technical Consulting
- Beijing Metro Construction Corporation
- Beijing National Railway Research and Design Institute of Signal and Communication Co. Ltd.
- Beijing Traffic Control Technology Company
- Bombardier Transportation
- Crossrail
- EC Harris
- Electrical and Mechanical Services Department Hong Kong Government
- Liv Systems
- Lloyd’s Register
- London Underground
- MTR Corporation, Hong Kong
- RSSB, UK
- Rio Tinto
- Siemens Rail Automation
- Technical Programme Delivery Group

This handbook does not necessarily represent the opinion of any of these people or organizations.

1 INTRODUCTION

This Application Note (AN) is a component of the international Engineering Safety Management Good Practice Handbook, or 'iESM', for short. The handbook as a whole describes good practice in railway Engineering Safety Management (ESM) on projects. It covers both projects that build new railways and projects that change existing railways.

The iESM handbook is structured in three layers:

- Layer 1: Principles and process
- Layer 2: Methods, tools and techniques
- Layer 3: Specialized guidance

Layer 1 contains Volume 1. Volume 1 describes some of the safety obligations on people involved in changing the railway or developing new railway products. It describes a generic ESM process designed to help discharge these obligations.

Volume 2 provides guidance on implementing the generic ESM process presented in Volume 1 on projects. Volume 2 belongs in the second layer. At the time of writing, Volume 2 was the only document in the second layer but further volumes may be added to this layer later.

The third layer comprises a number of Application Notes providing guidance in specialized areas, guidance specific to geographical regions and case studies illustrating the practical application of the guidance in this handbook. The structure of the handbook is illustrated in the figure on the right.

This document is Application Note 8. It supports the main body of the handbook by providing guidance on how to consider Human Factors within Engineering Safety Management.

If you have any comments on this Application Note or suggestions for improving it, we should be glad to hear from you. You will find our contact details on our web site, www.intesm.org. This web site contains the most up-to-date version of this Application Note. We intend to revise the handbook periodically and your comments and suggestions will help us to make the Application Note more useful.

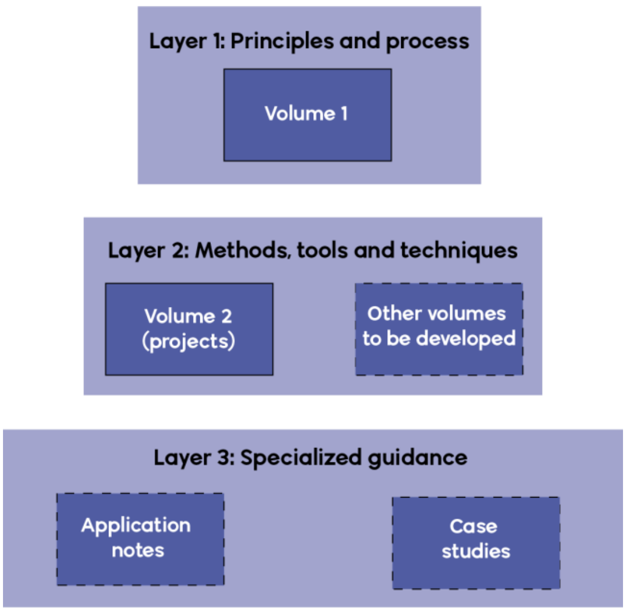


Figure 1 The Structure of iESM Guidance

2 WHY CONSIDER HUMAN FACTORS IN ENGINEERING SAFETY MANAGEMENT?

Even the most highly automated systems are designed, installed, and maintained by people. Human factors play a part in most, if not all accidents [8]. Understanding how people behave when things go wrong – and when things go right – is important in understanding safety.

Everybody makes mistakes. Most human errors can only be described as such after the fact, with the benefit of hindsight. Often, human error is the result of a poor system design rather than a failing of the person [16]. Human error should be seen as the result of a deeper problem in the system, not as the main cause of a hazard ('user interface error' may be a more accurate term). Therefore, consideration of human factors in Engineering Safety Management (ESM) is essential.

If you have not considered human factors when you need to consider Engineering Safety Management, it will be difficult to show that you have controlled risk properly.

Some of the ways people behave and some of the reasons for their behaviour are understood. Some ways of preventing or influencing the situations where humans can contribute to hazards are known. People prevent accidents as well as contributing to them, and this can be taken into account.

'Human factors' refers to the range of ways that operators, maintainers, passengers, and other stakeholders can influence the safety of the railway system. This is not just in terms of human errors and violations, but also in positive contributions to system safety through resilience, adaptability, and recovery actions that restore safe situations.

Aside from safety, the security, availability, and efficiency of the railway also depend on people. The human contribution to safety should be understood in relation to the wider role of people within the railway system [15]. Your organisation may have other initiatives associated with improving human performance, such as an Operability programme, or a Human Factors Integration programme. You should integrate your human-related ESM work with these other programmes, if they exist.

This document is intended for a manager or engineer that has been assigned responsibility for ensuring integration of human factors considerations into the generic ESM process [5]. It is not intended as detailed guidance for experienced Human Factors (HF) Specialists. It assumes a basic (but not advanced) appreciation of Human Factors Engineering knowledge and methods.

3 PROCESS FOR ADDRESSING HUMAN FACTORS IN ESM

3.1 Overview

Figure 2 shows the generic ESM process from Level 1 [5]. The process has been expanded to show how human factors can be considered in ESM.

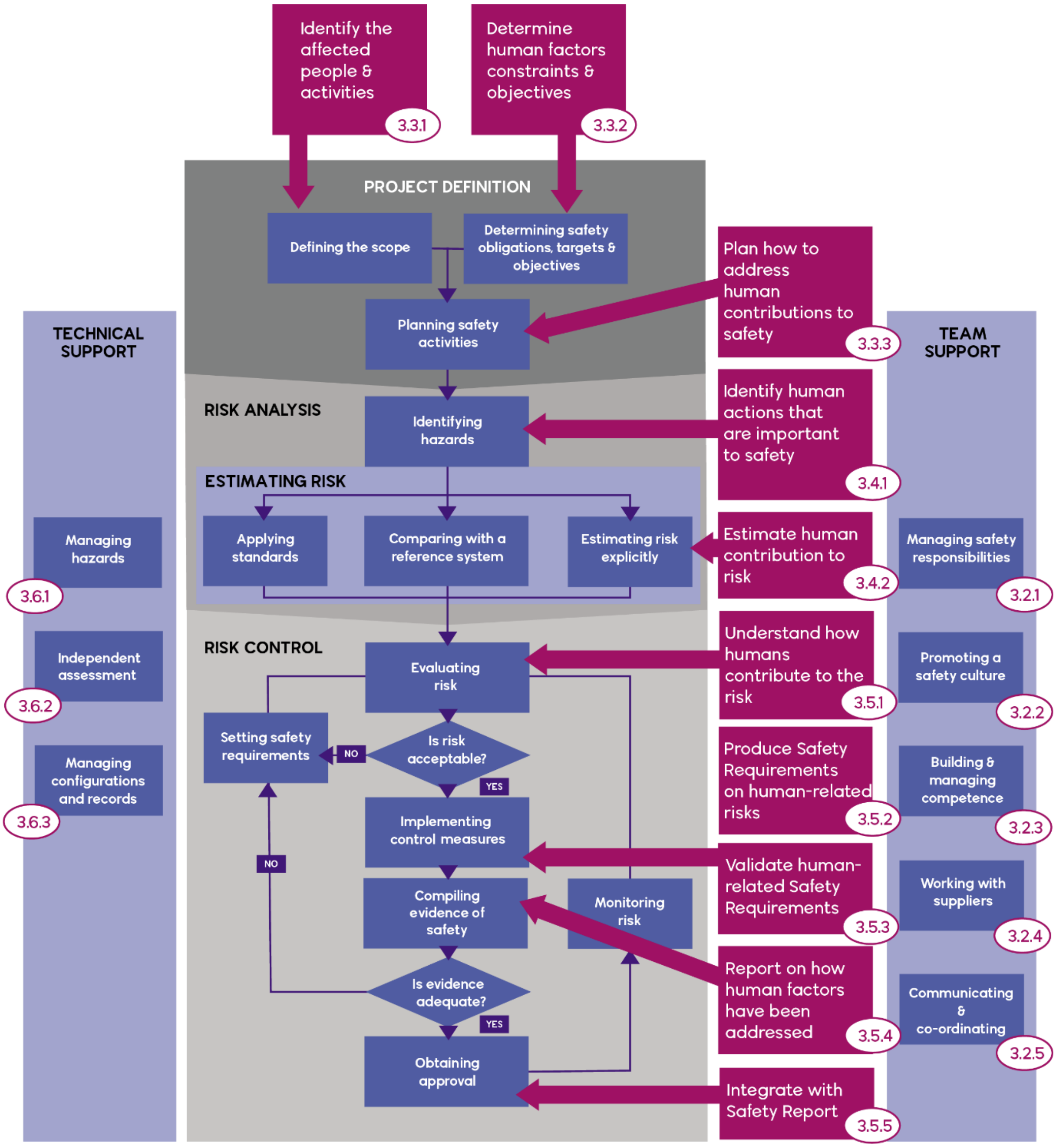


Figure 2 – ESM Generic Process and Human Factors Considerations

The following sections provide guidance on how to address safety-related human factors at each stage of the process captured in Figure 2. Given the importance of team support in addressing human factors in ESM, guidance on these activities is presented first.

3.2 Team Support

Team support is used to ensure that the people carrying out ESM activities are competent and well organised.

The guidance in the Level 1 ESM [5] also applies to the consideration of the human contribution to safety. The sections below give specific guidance to follow when addressing the human contributions to system safety.

3.2.1 Safety responsibility

Your organisation must assign a person to be responsible for co-ordinating the consideration of human factors within ESM.

This person should be given the resources and authority that they need to carry out those responsibilities.

In order to prevent confusion resulting in mistakes or missed work, you should have a competent person responsible for coordinating the consideration of human factors within the ESM project or programme. This person should have the same level of authority as any comparable engineering or assurance discipline lead. The coordinator may be the project or programme manager, or someone assigned by them.

3.2.2 Safety culture

You should treat human factors with the same importance as any other part of safety engineering.

Any organisation that professes to have a safety culture should treat human factors as an important contributor to system safety. While human factors can contribute to incidents and accidents, most of the time people make a positive improvement to the safety of the railway.

Your organisation should treat human-related safety with as much seriousness as any other aspect of safety, such as component reliability, or systematic integrity. The management of your organisation must share this commitment and make the appropriate resources available to address the human factor in safety.

3.2.3 Competence and training

People that assess and manage the human contribution to the safety of the change should be competent to do so.

Without competent people, the results of the ESM process may be unreliable. The competence necessary to perform the assessment and to manage the outcomes may be different.

The level and type of competence required will depend upon the project and the work to be carried out. It is not necessary that trained specialists carry out all work that considers human factors in relation to safety. However, your organisation should work out what training, technical knowledge, skills, experience and qualifications are required to perform these types of ESM activities.

There is training and professional accreditation schemes available for individuals involved with assessing the human contribution to risk. A local Human Factors or Ergonomics society may be able to provide details on available training and accreditation. The International Ergonomics Association (a federation of ergonomics and human factors societies from around the world – see https://iea.cc/) maintains a register of federated societies.

3.2.4 Working with suppliers

You should ensure that all supplier agreements are clear and unambiguous about how each organisation will address the human contribution to safety.

You will need to decide who does what in the supply chain, and ensure that all the parties understand their responsibilities.

You should ensure that contracts with suppliers are adequate, being clear about what is expected and what will be delivered.

You cannot give accountability for safety away, and this includes the human aspect. You can only devolve responsibility for conducting the work. It is your responsibility to ensure that those carrying out the work are competent and have the necessary resources.

3.2.5 Communicating and co-ordinating

You should identify and coordinate with other projects and organisations that could affect or be affected by your project.

It is common for a single individual on the railways to use a number of systems. It is important that work is coordinated to ensure that one system does not adversely affect the ability of users to use other systems. For example: where two systems use the same noise to alert the driver to a problem, confusion is likely to result.

You should provide access to stakeholders for the organisations that are to perform the work.

Without the actual stakeholders, especially the end-users, it is difficult to perform an accurate assessment and management of the human-related risks.

To improve communication and visibility of human factors within a programme consisting of many projects, a programme wide human factors coordinator is advised. They will have responsibility to ensure that projects coordinate their activities wherever possible and to aid the discovery of conflicting projects.

3.3 Project Definition

Project Definition is concerned with establishing clear objectives and a clear scope for the project and planning out a program of activities to deliver these.

3.3.1 Define the scope

Identify affected people and activities

An important factor in the definition of a change is the people who will be affected by it.

You should identify the affected people and activities by producing a scoping statement that contains:

A. A list of the end-users affected by the change;
B. A description of how the end-users will be affected by the change;
C. A description of how the abnormal or degraded modes of the change will affect the identified end-users[1];

[1] In this sense, 'abnormal' operations are planned but infrequent changes to the railway. 'Degraded' mode is a state of continuing railway operations with notable equipment failures.

D. What role the end-users will play in different configurations of the change (during implementation, migration, or commissioning, for example); and,
E. The definition of the boundary of the change, and how the boundary may affect the identified end-users.

This scoping statement could be in a stand-alone report. Alternatively, it could be part of another document, such as a requirements specification, operational concept, or target audience description. You are likely to need help from other disciplines such as operations, maintenance, and systems engineering in producing this scoping statement.

You should identify and describe the people who are likely to influence safety at all stages of a project. Below is a list of possible people that you may need to consider:

- The end-users;
- The people the end-users of the system deal with, including their customers and suppliers;
- Engineers involved in producing the change;
- Maintainers;
- Regulators; and,
- Management.

You should describe how these groups would be affected by the change, which may vary at different stages of the project. You should produce your report from the perspective of the end-users, and describe the change from their terms.

You should be careful to not ignore abnormal or degraded modes of operation; this includes the transition of the system during the implementation of the change. It is important that the change should be well managed, and consideration of the human contribution to safety will influence your ability to achieve this.

Often many small changes can have a significant effect. It is important that small changes are assessed to ensure that the combined effect doesn't introduce any unexpected emergent consequences.

3.3.2 Identify safety obligations

Determine human factors constraints and objectives

You may have obligations to meet certain criteria and requirements before you can accept the risks introduced by the change. This activity will consider the system in total, rather than just the human component.

However, you may also have obligations to perform certain activities in relation to the humans involved in the system.

You should determine the people-related constraints and objectives:

A. Review applicable requirements and standards and identify your obligations with regard to the human contribution to safety;
B. Identify any requirements that are not directly associated with safety, but may have an impact on safety (e.g., the need for a Signaller to supervise a larger area);
C. Find any conflicting requirements and seek to resolve them with the appropriate stakeholder;
D. Review the safety plan and identify what needs to be demonstrated with regard to the contributions of the humans to the safety of the change.

You should identify the requirements and obligations that are relevant to the consideration of human factors. This may be found in requirements specifications, legislation, applicable standards, good practice, or agreements within the end-user organisation. You may need to resolve conflicts between the requirements from these sources.

You should make sure that you understand safety obligations in relation to the other human-related objectives of the project.

Reviewing the safety plan will help you to understand the overall safety argument in relation to the people in the system. You should take this into account when planning safety activities.

Your review may also identify what type or level of evidence you will need in the future in order to show that safety obligations have been met.

3.3.3 Plan safety activities

Plan how to address human contributions to safety

It is essential that you plan the activities that will have to be carried out to address the human contribution to safety within the ESM process.

If this work is not planned, and the necessary resources are not made available, there is a significant risk that the work will not be effective.

You should produce a written statement (plan) that describes how you will address the human contributions to ESM. This should cover the following:

- **A.** **The purpose of the plan, the process to be followed, and the associated objectives in relation to ESM;**
- **B.** **The scope of the change being considered, and any assumptions (step 1 output);**
- **C.** **The people-related constraints and objectives (step 2 output);**
- **D.** **Based on analysis of A), B) and C), descriptions of the technical work activities that will be undertaken in order to address ESM human factor considerations;**
- **E.** **The schedule of these work activities;**
- **F.** **Which person is responsible for integrating human factor considerations into ESM for this change, what their duties are, and how they are supported by the project;**
- **G.** **How the outputs of the technical work activities will be integrated into ESM reporting; and,**
- **H.** **What project management and quality management controls will be used to verify the outputs of the ESM work programme.**

This planning should be integrated with all the safety planning for the project. You can do this through discussion with the safety specialist. You should make sure that your work will address the safety strategy or argument put forward in the safety plan. You should also check that there is enough time to complete the work.

You should check that your approach to human-related safety is proportionate to your obligations and the likely risks. You should confirm that the level of effort you are assigning to the consideration of human-related risks is commensurate with your obligations and the likely risks. Any decisions on scope should be recorded and revisited should assumptions change.

At the beginning of a project you may only be able to describe the general approach that will be taken. You should use this opportunity to ensure that the correct person is assigned, and that the organisation of the project supports them in their work.

At a later stage you will have to complete the remaining sections of the plan. Terminology may vary, but you should aim to have a complete plan by the end of the concept design phase.

If you have safety obligations, you should check that your planned safety activities would generate correct and complete evidence. This will ensure that your activities to address human-related safety issues will focus on the right areas, and generate the correct type and level of evidence that you will need to show that safety requirements have been met.

You should ensure that consideration of human factors is integrated into the overall engineering process. Human Factors Integration (HFI, [6]) provides a means of achieving this. On complex projects, the HFI process may also help you produce a 'Human Factors Integration Plan' that would plan the safety activities in accordance with the guidance above.

3.4 Risk Analysis

The identification, assessment and reduction of risk are core parts of any safety process. Within this process you should address the human contribution to risk, and its mitigation (humans can recover from problems as well as cause them). Your aim is to reduce the overall system risk to an acceptable level.

It is possible to model and control the situations that lead to human contributions to hazards, and also human reactions to system failures. There are many techniques that allow a practitioner to identify human involvement in hazards, assess the risk, and devise methods to reduce that risk.

It is easy for these techniques to be abused, performed incorrectly or used inappropriately. When you report on the risk analysis, you will need to demonstrate that appropriate techniques have been used to analyse human contribution to risks, and that the practitioners involved were competent to use them.

There are many models or processes for the identification, assessment and reduction of human-related risk. Within the iESM framework, there are two main steps to support the analysis of the human contribution to system risks:

1. Identify human actions that are important to safety; and,
2. Estimate human contribution to risk.

For each step we will describe in general terms what activities are necessary. We will not describe any specific techniques. The activities described here should be performed in conjunction with the corresponding ESM activity.

3.4.1 Identifying hazards

Identify human actions that are important to safety

You must carry out work to identify and understand the human factors that are associated with system hazards.

Within the context of the overall hazard analysis, you should:

A. Conduct a task analysis;

B. Identify possible types and causes of human error; and,

C. Incorporate human error types and causes into the overall hazard identification record.

In order to identify the human actions that are important to safety, you must first understand the tasks that are being carried out, and the context in which they occur.

If you do not fully understand the tasks that people will perform, and how they are to be carried out in conjunction with other duties, you cannot comprehensively identify where risks may originate.

The process of describing the tasks that people perform in relation to usage of a system is called task analysis. There are a variety of task analysis techniques [1], and the topic is too large to provide complete guidance in this Application Note.

However, to properly support the hazard identification process, any task analysis must be:

- Accurate;
- Complete;
- Appropriate[2]; and,
- Capture what is actually done, not just what the procedure says is done.

Task analysis requires a team that understands the railway domain, the change, and the techniques. A review of relevant operational experience (such as incident reports or 'near-miss' reports) may also be useful. You should also observe and talk with end-users that currently perform tasks associated with or equivalent to the change.

The task analysis is then used to identify possible types and causes of error [13]. The main techniques used to identify errors are Human HAZOP [9] and a type of modified FMEA (SHERPA [9], TRACER [9]). The major emphasis should be placed on reviewing the operation and maintenance tasks to eliminate, as far as practicable, areas that may foster the production of human error and to identify areas where the human contribution can facilitate design efficiency and effectiveness.

You should integrate the error identification process with the general process of hazard identification within the project. Many hazards will have both human and technical causes. In order to model the causes of hazards, it is necessary to consider both classes, and the manner in which they interact. Therefore, the representation of human error should be integrated with other aspects of safety analysis. For example, event and fault trees can be used to describe the sequence of events that lead to, and from, a hazard. If these are used then human error events can be integrated into the description.

[2] e.g. use a task analysis method that is a match with the types of tasks the operators are performing. See [1] for more information on task analysis methods.

3.4.2 Estimating risk

Estimate human contribution to risk

Your estimation of risk may be incomplete if you do not account for human factors.

The iESM allows for three methods of risk estimation: applying standards, comparison with a reference system, and estimating risk explicitly.

You can account for the human contribution to risk estimates by following these steps:

- **A. Confirm the risk estimation method being used for the human-related risks of interest, and then:**
- **B. When estimating risks with reference to the application of a standard, assess that the standard covers the human-related hazard;**
- **C. When estimating risks by comparison with a reference system, confirm that the human-related tasks in the reference system are comparable;**
- **D. When estimating risk explicitly, provide an error likelihood estimate (either qualitatively or quantitatively).**

If risks are being estimated with reference to the application of a standard, the person responsible for addressing human-related risks must demonstrate that application of the standard is sufficient to adequately control the human-related hazards.

When estimating risk by comparison with a reference system, the person responsible for integrating human factors into the ESM activities must demonstrate that the reference system and the change are comparable with regard to human tasks, working environment, and performance shaping conditions. In particular, it will need to be demonstrated that the working environment (e.g., pace of work, time availability, human-computer interfaces, supervision, training and competency arrangements, etc.) are comparable across the reference system and the change.

With human error represented within the overall safety model (e.g., fault tree, event tree) for a system, it is possible to assess the likelihood of an error occurring, and of it leading to a hazard and an accident. In order to do this you will need to assess the likelihood of human actions being carried out incorrectly.

Likelihood can be expressed with or without the use of absolute numeric probabilities. When expressed without using numeric probabilities, likelihood can be graded using categorical descriptions (impossible, highly unlikely, very likely, certain, etc.). When an absolute measure of likelihood is sought, it is necessary to have probabilities of the likelihood of human error, commonly referred to as Human Error Probabilities (HEPs).

There are many methods for assigning HEPs to human actions [7]. These can be broadly divided into two classes: those that rely on recorded probabilities of occurrences to form a database (such as the Rail Action Reliability Assessment method [11]); and those that rely on expert assessment to reason about, or simulate, human performance and the likelihood of an error. Both approaches have strengths and weaknesses, and the decision of which technique to use will depend on the context.

The physical and organisational environment affects the likelihood of human error. These influences are known as Performance Shaping (or Influencing) Factors (PSFs/PIFs). Techniques exist that allow you to model the effect that these factors have on the likelihood of human error. It is possible by improving an environmental or organisational factor, that the likelihood of error at several stages in a chain of events leading to a hazard can be reduced, leading to a significant reduction in risk. By modelling the impact of PSFs on the overall risk it is possible to identify those that have the greatest effect. Tools exist to allow you to model these effects in order to identify those that have most impact on the likelihood of error.

When considering human error likelihoods, it is important to consider the possible dependencies (common failure causes) between human tasks. Because the railway is a highly interconnected system, you should not assume independence between human tasks. One error may make error in a subsequent task more likely, or a protective measure less effective. This should be accounted for in the risk estimate.

3.5 Risk Control

3.5.1 Evaluating risk

Understand how humans contribute to the risk

This activity involves applying the risk acceptance criteria to the estimated risk and concluding whether or not it can be accepted. Therefore, this activity is mainly conducted at the system level.

However, you should develop an understanding of how the human element contributes to the overall risk.

This will help you understand the extent to which human factors influence the overall system risk.

When human factors are considered within the context of quantified system risk, it is possible to use standard methods of sensitivity analysis such as fault tree cut sets to identify those human actions that have the most impact on the likelihood of a hazard.

You should bear in mind that safety is highly dependent on how well people and equipment do their job. You should avoid relying completely for safety on any one person or piece of equipment. This activity will help you avoid this problem.

3.5.2 Set safety requirements

Produce Safety Requirements on human-related risks

You should set requirements to help the user avoid or recover from hazards.

The overall aim of this activity is to reduce the overall risk associated with the change to an acceptable level.

You should consider five complementary strategies for improving the human contribution to safety:

A. **Improve the working environment by removing distractions and attending to factors which might cause fatigue and reduced performance;**
B. **Improve the design of the equipment to avoid provoking the operator into error;**
C. **Improve the design of the task and procedures to reduce the likelihood of error;**
D. **Improve the performance of the individual through attention to training, competence, fitness, motivation, and safety culture; and,**
E. **Improve the design of the system so that humans are able to recover from potentially hazardous situations.**

You will have identified the factors that influence the contribution of human factors to safety through task and error analysis (Section 3.3). From this it is possible to identify the possible safety requirements that will help to reduce errors, or to assure correct human performance.

You should consider the possible safety requirements against a hierarchy of risk controls (e.g., elimination, substitution, engineering, administrative controls, competence). Controls and mitigations can be developed to address Operations, Maintenance, and Engineering areas of a business. It is important that controls and mitigations are considered in relation to all aspects of the railway operation that are impacted by the change.

Requirements should be justified by a rationale. Requirements should be recorded at a consistent and logical level of detail, making sure that the stated requirement does not contradict other requirements.

Options analysis can be used to assess the possible safety requirements, taking into account the cost of the requirement and the effect that it will have on overall system safety. You may find it useful to involve a Human Factors Specialist at this stage, as they will be able to advise on how requirements should be implemented in the design of the changes to the system.

When considering safety requirements to control human-related risks you should involve end-user representatives. You should investigate with them how the system may be improved, either to help them avoid error, or to mitigate other system errors. A good safety process involves the user throughout the project.

It is important that any requirements that you make can be measured or judged to have been achieved at some point in the future, such as during acceptance testing or commissioning. To do this, you should state the criteria (level of performance) for completion of the human-related safety requirement at the same time as you decide on what is required. Stating the criteria and the requirement together will help you understand what you may need to do to demonstrate achievement of safety goals.

Safety-related human performance requirements should be integrated with the general safety requirements.

3.5.3 Implementing and validating control measures

Validate human related Safety Requirements

You should assure yourself that the safety requirements set on the human contributions to safety are effective and have been correctly implemented.

This involves the following actions:

A. **Where necessary, provide further guidance on your human-related safety requirements so that the project can implement them correctly and successfully;**
B. **Deal with any trade-offs if human-related safety requirements conflict with other requirements;**
C. **Be aware of any unintended consequences that may arise when human-related safety requirements are combined;**
D. **Use an appropriate method when validating that a control measure has been implemented;**
E. **Make sure that your validation activities will give you enough confidence in your evidence; and,**
F. **Check that any validation findings are still valid when you want to use them.**

Human Factors Engineering includes a wide range of methods covering different aspects of implementing and validating requirements.

There are two parts to this:

- Implementing a safety requirement correctly, effectively, and with no unintended consequences; and,
- Checking that the safety requirement is met, and continues to be met when you need to rely on the evidence.

When implementing a human-related safety requirement, you may find that some additional human factors guidance or specification is required.

Validation is carried out so that stakeholders can gain confidence that the change to the railway will perform as required when implemented in the operational environment. Part of these performance expectations may relate to the role of people (e.g., drivers, dispatchers, and maintainers) in keeping the system safe. Therefore, checking that safety requirements involving humans have been successfully implemented is important to ESM.

The main methods of checking human-related requirements are inspection and testing. Inspection involves comparing a design or plan against the requirement. For example, on a rolling stock project, you may have a safety requirement that a certain proportion of the target user population can reach a certain control from the driving position. Inspection of the detailed design will show if this requirement is met.

Testing (in particular, 'mock up trials' or 'operability testing') can help to show that other types of human-related safety requirement have been met. For example, a mock-up trial might demonstrate that passengers can leave a train quickly enough when detraining is required.

When it comes to human related requirements, the way in which validation data is collected affects the confidence that can be placed on the evidence.

3.5.4 Compiling evidence of safety

Report on how human factors have been addressed

To demonstrate that a change has been designed to be safe you must provide a safety argument.

To demonstrate that human-related safety requirements have been met, you may need to produce a report with the following information:

A. **A review of project documentation, procedures, training plans and records, transition plans, and supporting operational readiness evidence;**
B. **A review against each relevant safety requirement, showing how the requirement has been met;**
C. **For safety requirements not fully met or met through a different means, perform an impact assessment to determine the consequences; and,**
D. **A forward plan for the risk monitoring stage.**

Integrate your consideration of human factors into the safety argument for the project.

You should have evidence to support the human factors parts of the safety argument.

Without evidence for its human factors parts, the safety argument is unsupportable.

You should collect this evidence throughout the project.

This will reduce the risk of the safety argument being rejected.

During the lifetime of a project you will need to collect evidence to support the parts of the safety argument that deal with human aspects. You will need evidence to show that you followed your plan (Section 3.2.3), and that the results of any analysis support your assertion that the system meets its safety requirements. The safety case should include an audit trail for human related design decisions (for instance, the rationale for why a procedure or control/display is designed in a certain way for human use).

You should agree with your stakeholders what evidence will be required in advance, in order to reduce the risk of rejection.

3.5.5 Obtaining approval

Integrate with Safety Report

You should integrate your consideration of human factors into the safety case.

You should have evidence to support the human-related parts of the safety argument.

This evidence should relate to each specific configuration of the railway system (e.g., stages within a staged commissioning or product introduction) to which your scope applies.

3.5.6 Monitoring risk

Risk monitoring should be a proactive process, which by its nature maintains and improves the acceptable level of safety. There are two aspects to this: monitoring the effectiveness of specific safety requirements, restrictions, or assumptions that you may have placed on in-service operation or maintenance, and generic monitoring of overall safety performance.

During the early stages of the introduction of the change to the railway, you should confirm that the assumptions you made in the safety assessment were correct. You should confirm that the human performance that was assumed is present in reality.

The process for the monitoring of overall safety risk involves analysing various safety data to determine whether the railway operation can be said to be safe and healthy, and where it cannot, what corrective action is required.

Risk monitoring is a generic iESM activity, but a lot of the data you will collect will be about human factors. While this is a large topic, and overlaps with the functioning of the safety management system, it is possible to give some guidance on how the link between risk monitoring and engineering safety management can be made.

When using human factors data for risk monitoring, you should keep in mind the following points:

A. **Collect safety indicators that relate to normal operations, not just incidents;**
B. **When incidents occur, investigate what is behind the incident, and act on the findings;**
C. **Identify and investigate trends and themes in the human actions within your safety data;**
D. **Provide a way for feedback from in-service operation to influence engineering projects;**
E. **Ensure that requirements on competence and risk controls are understood and acted upon by the relevant contractors and maintainers throughout the supply chain; and,**
F. **Confirm that the requirements and assumptions made in the safety case are still appropriate and effective.**

Special care should be taken when investigating safety occurrences from a HF perspective. The main purpose for investigating an occurrence should be to prevent similar events from happening. The focus must be on understanding why it happened, and why the actions made sense to the operators at the time. While occurrence investigation often stops at the conclusion of ‘human error’, investigation of human-related safety must analyse the different facets of the situation and try to understand the mechanisms and context that led to the unsafe situation.

When a potential deterioration in safety has been identified, a corrective action plan should be identified (e.g. change to standards, implementation, procedures development, changes to HMI, or revisions to training).

Where a corrective action plan cannot be identified a refinement of the current processes may be required; or as an interim measure it may be necessary to restrict the human actions associated with the deterioration.

It is very useful if operational experience can be made available to engineering projects. Engineering projects can then be made aware of any 'user interface errors' that have happened in the past, and the new systems can be built to avoid these 'error traps'.

It should be noted that monitoring risk during the in-service phase is a large topic and only the fundamental guidance can be presented here. More information can be found in a number of sources, such as the RSSB Guide 'Practical Support for Accident Investigators' [10] and the Field Guide to Understanding Human Error [3].

3.6 Technical Support

Technical support involves activities that underpin the generic ESM risk assessment process. The consideration of human factors within ESM requires the same technical support as the main ESM activities. The sections below only present the differences that are specific to the integration of human factors considerations with the safety assessment.

3.6.1 Managing hazards

Keep a register of the human-related issues that are identified, and how these have been resolved.

You should maintain a register of the human-related issues that arise from the risk analysis and risk control processes. This register should list the issues identified and the actions taken to resolve them. Ideally, you should use any existing Project Risk or Hazard Register, with relevant issues marked as being 'human-related'. This will enable all project issues to be stored together, and ensure that the human-related issues are given the same attention as other safety issues.

Human-relates issues need to be communicated effectively across teams and managed (tracked, escalated, and resolved). Processes for hazard and safety issues management on the project need to include human-related issues.

3.6.2 Independent professional review

Any independent professional review of the project should have the skills and knowledge to assess the human contribution to the safety of the change.

Without such knowledge, the independent reviewer will not be able to make an informed judgement.

The review of how human contributions to ESM have been addressed should be an integral part of the overall review of your safety case.

An independent review may need to consider both the techniques used to assess the human contribution to safety, the outputs of the techniques, and how these have been integrated into the safety case.

3.6.3 Configuration management and records

Follow the configuration management procedure that applies to the project when issuing reports and generating evidence to support human-related safety claims.

Your configuration management procedures should cover any documents and data that relate to the consideration of the human within the safety assessment.

You may produce prototypes, mock-ups, simulations, and other types of stakeholder meetings and workshops when generating evidence to show that Safety Requirements are correct and have been implemented correctly. These activities need to follow general project management and quality processes for their occurrences and their outputs. It is important that configuration management processes cover these.

You may need to handover records to support through life management.

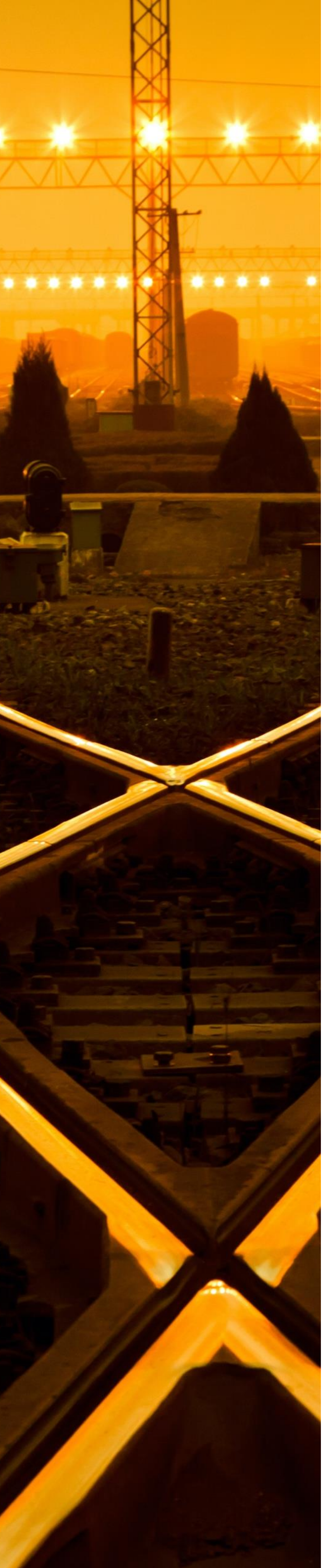
4 GUIDANCE CHECKLIST

No.	Action	How Achieved? (Write in)	Action Complete?
1	A person has been assigned to be responsible for co-ordinating the consideration of human factors within ESM.		☐
2	This person has been given the resources and authority that they need to carry out those responsibilities.		☐
3	Human factors have been treated with the same importance as any other part of safety engineering.		☐
4	People that assess and manage the human contribution to the safety of the change are competent to do so.		☐
5	All supplier agreements are clear and unambiguous about how each organisation will address the human contribution to safety.		☐
6	Other projects and organisations that could affect or be affected by your project have been identified and informed.		☐
7	Access to stakeholders and end users for the organisations that are to perform the work has been provided.		☐
8	A scoping statement has been produced to identify the affected people and activities. This contains:		☐
8a	A list of the end-users affected by the change;		☐
8b	A description of how the end-users will be affected by the change;		☐
8c	A description of how the abnormal or degraded modes of the change will affect the identified end-users;		☐
8d	What role the end-users will play in different configurations of the change (during implementation, migration, or commissioning, for example); and,		☐
8e	The definition of the boundary of the change, and how the boundary may affect the identified end-users.		☐
9	The people-related constraints and objectives have been identified.		☐
10	A written statement (plan) that describes how you will address the human contributions to ESM has been produced. This statement includes information on:		☐

No.	Action	How Achieved? (Write in)	Action Complete?
10a	The purpose of the plan, the process to be followed, and the associated objectives in relation to ESM;		☐
10b	The scope of the change being considered, and any assumptions;		☐
10c	The people-related constraints and objectives;		☐
10d	Descriptions of the technical work activities that will be undertaken in order to address ESM human factors considerations;		☐
10e	The schedule of these work activities;		☐
10f	Which person is responsible for integrating human factors considerations into ESM for this change, what their duties are, and how they are supported by the project;		☐
10g	How the outputs of the technical work activities will be integrated into ESM reporting; and,		☐
10h	What project management and quality management controls will be used to verify the outputs of the ESM work programme.		☐
11	Within the context of the overall hazard analysis, you have:		☐
11a	Conducted a task analysis to the appropriate level of detail given the anticipated safety significance of the human actions;		☐
11b	Identified possible types and causes of human error; and,		☐
11c	Incorporated human error types and causes into the overall hazard identification record.		☐
12	The human contribution to risk estimates has been accounted for. Any of the following three actions has been done:		☐
12a	When estimating risks with reference to the application of a standard, it has been confirmed that the standard covers the human-related hazard.		☐
12b	When estimating risks by comparison with a reference system, it has been confirmed that the human-related tasks in the reference system are comparable.		☐

No.	Action	How Achieved? (Write in)	Action Complete?
12c	When estimating risk explicitly, an error likelihood estimate (either qualitatively or quantitatively) has been provided.		☐
13	A statement of how the human factor contributes to the overall risk has been provided.		☐
14	You should consider three complementary strategies for improving the human contribution to safety:		☐
14a	You have considered improvements to the working environment by removing distractions and attending to factors that might cause fatigue and reduced performance.		☐
14b	You have considered improvements to the design of the task and the equipment to avoid provoking the operator into error; and,		☐
14c	You have considered improvements to the performance of the individual through attention to competence, fitness, motivation, and safety culture.		☐
15	To demonstrate that human-related safety requirements have been met, you may need to produce a report with the following information:		☐
15a	A review of project documentation, procedures, training plans and records, transition plans, and supporting operational readiness evidence;		☐
15b	A review against each relevant safety requirement, showing how the requirement has been met;		☐
15c	For safety requirements not fully met or met through a different means, perform an impact assessment to determine the consequences; and,		☐
15d	Develop a forward plan for the risk monitoring stage.		☐
16	The consideration of human factors has been integrated into the safety argument for the project.		☐
17	Safety indicators that relate to normal operations, not just incidents, have been considered for collection.		☐
18	When incidents occur, reasons behind the incident are investigated and acted upon.		☐
19	Trends and themes in the human contributions to occurrence reports are investigated.		☐

No.	Action	How Achieved? (Write in)	Action Complete?
20	A way for feedback from in-service operation to influence engineering projects is provided.		☐
21	You have checked that requirements on competence and risk controls are understood and acted upon by the relevant contractors and maintainers throughout the supply chain.		☐
22	During transfer to operations, requirements and assumptions made in the safety case are confirmed to be still appropriate and effective.		☐
23	A register of the human-related issues that are identified, and how these have been resolved, has been kept.		☐
24	Any independent professional review of the project includes people with the skills and knowledge to assess the human contribution to the safety of the change.		☐
25	The configuration management procedure that applies to the project has been followed when issuing reports and generating evidence to support human-related safety claims.		☐



5. DOCUMENT REFERENCES

1. Annett, J. and Stanton, N. (Eds.) (2000) Task Analysis, Taylor & Francis, London.
2. Commission Regulation (EC) No 352/2009 of 24 April 2009 on the adoption of a Common Safety Method on Risk Evaluation and Assessment.
3. Dekker, S. (2006), The Field Guide to Understanding Human Error, Ashgate, Aldershot, England.
4. Engineering Safety Management, issue 4, “Yellow Book 4”, ISBN 978-0-9551435-2-6 (Note - Yellow Book 4 now has the status of a withdrawn document).
5. International Engineering Safety Management Working Group, Volume 1: Good Practice Handbook: Principles and Process
6. Heape, S., and Lowe, C., (2012) Effective Human Factors Integration in the Design of a Signalling and Train Control System for the Metro Rail Industry, in: Rail Human Factors around the World: Impacts on and of People for Successful Rail Operations, CRC Press, Taylor & Francis Group, London.
7. Kirwan, B (1994), A Guide to Practical Human Reliability Assessment, Taylor and Francis, London.
8. Kletz, T. (2001), Learning from Accidents, Butterworth-Heinemann, Oxford, England.
9. Rail Safety and Standards Board (2008), Human Factors Good Practice Guide.
10. Rail Safety and Standards Board (2011), Practical Guidance for Accident Investigators.
11. Rail Safety and Standards Board (2012), Railway Action Reliability Assessment: User Manual.
12. Reason, J (1997), Managing the Risks of Organizational Accidents, Ashgate, Aldershot, England.
13. Reason (1990) Human Error, Cambridge University Press, Cambridge, UK.
14. Rasmussen, J (1997), Risk management in a dynamic society: a modelling problem. Safety Science, 27(2/3) pp. 183-213.
15. Wilson, J (2013) “Systems Approaches in Ergonomics/Human Factors Applied within Rail Systems Engineering” in Rail Human Factors: Supporting Reliability, Safety and Cost Reduction, CRC Press, Taylor & Francis Group, London.
16. Woods, D. D, Dekker, S, Cook, R, Johannesen, L, Sarter, N (2010) Behind Human Error, Ashgate Publishing Limited, Farnham, England.

Note: This revision (Issue 1.2) of the Application Note has not modified any of the technical content present in the previous revision. Some of the standards referenced may have been revised. A full technical review is planned to be undertaken of this Application Note prior to its next revision.

GLOSSARY

This glossary defines the specialized terms and abbreviations used in this Application Note.

Engineering Safety Management (ESM)	The activities involved in making a system or product safe and showing that it is safe. Note: despite the name, ESM is not performed by engineers alone and is applicable to changes that involve more than just engineering.
Human Error	Errors are the result of actions that fail to generate the intended outcomes. A common classification is slips, lapses, and mistakes.
Human Error Probability (HEP)	A mathematical ratio between the number of errors occurring in a task and the number of tasks carried out where there is an opportunity for error.
Human Factors	The human element of any system, the manner in which human performance is affected, and the way that humans affect the performance of systems.
Human Factors Engineering	The practice of Human Factors applied to the design, operation, and evaluation of systems to ensure that that they are safe, efficient, comfortable and aesthetically pleasing to humans. Taken to be the same as 'Ergonomics'.
Human Factors Integration	A systematic process for identifying, tracking and resolving people-related considerations ensuring a balanced development of both technology and human aspects of a system.
Hazard	A condition that could lead to an accident. A potential source of harm. A hazard should be referred to a system or product definition.
Human Safety	Broad consideration of how people can affect safety (positively and negatively)
Operability	The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, safety, and satisfaction in a specified context of use.
Performance Shaping (or Influencing) Factor	A property of the person or working environment that makes a particular task outcome (error or success) more or less likely.
Safety	Safety is defined as "freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment."
System	A set of elements which interact according to a design, where an element of a system can be another system, called a subsystem and may include hardware, software and human interaction.
System Lifecycle	A sequence of phases through which a system can be considered to pass. A product may also pass through some of these phases.
Systematic Failure	A failure due to errors, which causes the product, system or process to fail deterministically under a particular combination of inputs or under particular environmental or application conditions.

Task Analysis	Task analysis describes and defines the tasks necessary to achieve a particular goal. Tasks can be described at different levels of detail according to the type of human–system issue being investigated.
Triggering Event	An event, outside the system or product of interest, which is required in order for a Hazard to result in an Accident.
Violation	Any deliberate deviation from the rules, procedures, instructions and regulations drawn up for the safe operation and maintenance of plant or equipment.

iESM

BROUGHT TO YOU BY ARC

international Engineering Safety Management

Published on behalf of the international railway industry
by Abbott Risk Consulting Ltd.
Issue 1.2 October 2022