Introduction

Human failures are often recognised as being a contributor to incidents and accidents, and therefore this section has strong links to the section on accident investigation. Although the contributions to incidents are widely accepted, very few sites will **proactively** seek out potential human performance problems. Human failure is described fully in chapter 'Introduction to Human Factors', where different types of human failures are outlined. In summary, there are two kinds of unintentional failures - physical errors ('not doing what you meant to do') and mental errors, where you do the wrong thing believing it to be right (i.e. making the wrong decision). In addition, there are intentional failures or violations – knowingly taking short cuts or not following known procedures.

This will be a relatively new area for many dutyholders and so evidence may not be available to demonstrate that a human factors risk assessment has been completed. Therefore, the inspection will be more likely providing guidance on what is expected in such an assessment on COMAH sites. To assist in this process, a description of a method for identifying and managing human failures is attached below. However, some dutyholders will have partially addressed these issues in an unsystematic manner and the question set will tease out the aspects that they have addressed in part.

Most companies, even if aware of 'human failure', will still focus on engineering reliability. It is useful to make this point to dutyholders by asking how they ensure the reliability of an alarm in the control room – usually a detailed and robust demonstration will be made, referring to redundancy, testing etc. However, asking them how they ensure the reliability of the operator who is tasked with responding to the alarm will usually reveal some gaps. You may wish to probe **how** they know that the operator will always respond in the correct manner, and then discuss what factors may effect an inappropriate response (such as tiredness, distractions, overload, prominence of the alarm indication etc). If any factors are identified, you can ask the site how they could be improved (e.g. providing auditory as well as visual indication, providing a running log of alarms). This process is essentially a human reliability assessment and it is useful to talk through this process so that the company is clear what we mean by addressing human failures.

In assessing human performance, it is all too easy to focus (sometimes exclusively) on the behaviour of front line staff such as production operators or maintenance technicians. The site should be made aware that such focus is undesirable and unproductive. There may be management/organisational failures that have the potential to influence several front line human failures (for example, inadequacies in competency assurance). The technique outlined below can be applied to the identification of failures at the management level.

Human failures in Major Accident Hazards

It should be stressed to the site that we are concerned with how human failures can impact on major accident hazards, rather than personal safety issues.

There are two important aspects to managing human failures in the safety critical industries. First, individual human failures that may contribute to major accidents can be identified and controlled. Second, consideration needs to be given to wider issues than individual human error risk assessments; and this includes addressing the culture of an organisation. Positive characteristics that will support interventions on human failures include open communications, participative involvement of all staff, visible management commitment to safety (backed up by allocated financial, personnel and other resources), an acceptance of

underlying management / organisational failures and an appropriate balance between production and safety. These characteristics will be manifested through a strong safety management system that ensures control of major accident hazards.

Human reliability assessment

The information below is intended to assist in the first of these aspects – an assessment of the human contribution to risk, commonly known as Human Reliability Assessment (HRA). There are two distinct types of HRA:

- **qualitative** assessments that aim to identify potential human failures and optimise the factors that may influence human performance, and

- **quantitative** assessments which, in addition, aim to estimate the likelihood of such failures occurring. The results of quantitative HRAs can feed into traditional engineering risk assessment tools and methodologies, such as event and fault tree analysis.

There are difficulties in quantifying human failures (e.g. relating to a lack of data regarding the factors that influence performance); however, there are significant benefits to the qualitative approach and it is this type of HRA that is described below. The company should be informed that our expectation is that they conduct **qualitative** analyses of human performance – identifying what can go wrong and then putting remedial measures in place.

At the end of the visit, it is expected that the company will be left with a human failure risk assessment proforma, together with guidance on its completion. Agreement from the company should be obtained to undertake such analyses on safety critical operations.

Example of a method to manage human failures

The following structure is well-established and has been applied in numerous industries, including chemical, nuclear and rail. Other methods are available, but these tend to follow a similar structure to that described below. This approach is often referred to as a 'human-HAZOP', and this is a useful term to help dutyholders understand our expectations. A proforma for recording the assessment of human failures is provided at Table 1.

Overview of key steps

- Step 1: consider main site hazards;

- Step 2: identify manual activities that affect these hazards;

- Step 3: outline the key steps in these activities;

- Step 4: identify potential human failures in these steps;

- Step 5: identify factors that make these failures more likely;

- Step 6: manage the failures using hierarchy of control;

- Step 7: manage error recovery.

Step 1: consider main site hazards

Consider the main hazards and risks on the site, with reference to the safety report and/or risk assessments.

Step 2: identify manual activities that affect these hazards

Identify activities in these risk areas with a human component. The aim of this step is to identify human interactions with the system which constitute significant sources of risk if human errors occur. For example, there is more opportunity for human performance failures in chlorine bulk transfer than there is in a chlorine storage due to the number of manual operations. Human interactions which will require further analysis are:

- those that have the potential to initiate an event sequence (e.g. inappropriate valve operation causing a loss of containment);
- those required to stop an incident sequence (such as activation of ESD systems) and;
- actions that may escalate an incident (e.g. inadequate maintenance of a fire control system).

Consider tasks such as maintenance, response to upsets/emergencies, as well as normal operations. It is important to note that a task may be a physical action, a check, a decision-making activity, a communications activity or an information-gathering activity. In other words, tasks may be physical or mental activities.

Step 3: outline the key steps in these activities

In order to identify failures, it is helpful to look at the activity in detail. An understanding of the **key steps** in an activity can be obtained through talking to operators (preferably walking through the operation) and review of procedures, job aids and training materials as well as review of the relevant risk assessment. This analysis of the task steps establishes what the person needs to do to carry out a task correctly. It will include a description of what is done, what information is needed (and where this comes from) and interactions with other people.

Step 4: identify potential human failures in these steps

Identify potential human failures that may occur during these tasks – remembering that human failures may be unintentional or deliberate. Consider the guidewords below for the **key steps** of the activity. Key steps to consider would be those that could have adverse consequences should they be performed incorrectly.

A task may:

- Not be completed at all (e.g. non-communication);
- Be partially completed (e.g. too little or too short);
- Be completed at the wrong time (e.g. too early or too late);
- Be inappropriately completed (e.g. too much, too long, on the wrong object, in the wrong direction, too fast/slow);

or,

- Task steps may be completed in the wrong order;
- The wrong task or procedure may be selected and completed;

Additionally, there may be:

- A deliberate deviation from a rule or procedure (a ‘procedural violation’).

A more detailed list of ‘error types’, similar to HAZOP guidewords, is provided at the end of this section. Note that an operator may make the same failure on several occasions, known as dependency. For example, an operator may miscalibrate more than one instrument because they have made a miscalculation.

Step 5: identify factors that make these failures more likely

Where human failures are identified above, the next step is to identify the factors that make the failure more or less likely.

Performance Influencing Factors (PIFs) are the characteristics of people, tasks and organisations that influence human performance and therefore the likelihood of human failure. PIFs include time pressure, fatigue, design of controls/displays and the quality of procedures. **Evaluating and improving PIFs is the primary approach for maximising human reliability and minimising failures.** PIFs will vary on a continuum from the best practicable to worst possible. When all the PIFs relevant to a particular situation are optimal, then error likelihood will be minimised.

Some PIFs that should be considered when assessing an activity/task are outlined in the previous section on accident investigation. HSG48 also lists often-cited causes of human failures in accidents under the three headings of Job, Individual and Organisation. These ‘root causes’ of accidents are in effect the factors that can influence human performance and which should be reviewed in a human factors risk assessment. It is important to consider those factors under the control of management (such as resources, work planning and training) as they can often influence a wide range of activities across the site.

Step 6: manage the failures using hierarchy of control

In order to prevent the risks from human failure in a hazardous system, several aspects need to be considered.

- Can the hazard be removed?
- Can the human contribution be removed, e.g. by a more reliable automated system (bearing in mind the implications of introducing new human failures through maintenance etc)?
- Can the consequences of the human failure be prevented, e.g. by additional barriers in the system?
- Can human performance be assured by mechanical or electrical means? For example, the correct order of valve operation can be assured through physical key interlock systems or the sequential operation of switches on a control panel can be assured through programmable logic controllers. Actions of individuals should not be relied upon to control a major hazard.
- Can the Performance Influencing Factors be made more optimal, (e.g. improve access to equipment, increase lighting, provide more time available for the task, improve supervision, revise procedures or address training needs)?

Step 7: manage error recovery

Should it still be possible for failures to occur, improving error recovery and mitigation are the final risk reduction strategies. The objective is to ensure that, should an error occur, it can be identified and recovered from (either by the person who made the error or someone else such as a supervisor) – i.e. making the system more ‘error tolerant’. A recovery process generally

follows three phases: **detection** of the error, **diagnosis** of what went wrong and how, and **correction** of the problem.

Detection of the error may include the use of alarms, displays, direct feedback from the system and true supervisor monitoring/checking. There may be time constraints in recovering from certain errors in high-hazard industries, and it should be borne in mind that a limited time for response (particularly in an upset/emergency) is in itself a factor that increases the likelihood of error.

Specific documents

In addition to the general documents that should be requested prior to the visit (see chapter 'Aim of the Guidance') it is recommended that the following documents, which are specific to this topic, should also be requested:

- risk assessment documents outlining the main hazards on site;
- any analyses or documentation referring to safety critical tasks, roles or responsibilities.

A Classification of Human Failures

This list of failures, akin to HAZOP guidewords, can be used in place of the simplified version in Step 4 of the method above.

Action Errors

A1	Operation too long / short
A2	Operation mistimed
A3	Operation in wrong direction
A4	Operation too little / too much
A5	Operation too fast / too slow
A6	Misalign
A7	Right operation on wrong object
A8	Wrong operation on right object
A9	Operation omitted
A10	Operation incomplete
A11	Operation too early / late

Checking Errors

C1	Check omitted
C2	Check incomplete
C3	Right check on wrong object

C4	Wrong check on right object
C5	Check too early / late

Information Retrieval Errors

R1	Information not obtained
R2	Wrong information obtained
R3	Information retrieval incomplete
R4	Information incorrectly interpreted

Information Communication Errors

I1	Information not communicated
I2	Wrong information communicated
I3	Information communication incomplete
I4	Information communication unclear

Selection Errors

S1	Selection omitted
S2	Wrong selection made

Planning Errors

P1	Plan omitted
P2	Plan incorrect

Violations

V1	Deliberate actions

Table 1: Proforma for recording identification of human failures

Practical suggestions as to how to prevent the error from occurring are detailed in this column, which may include changes to rules and procedures, training, plant identification or engineering modifications.

Not all human errors or failures will lead to undesirable consequences: There may be opportunities for recovery before reaching the consequences detailed in the following column. It is important to take recovery from errors into account in the assessment, otherwise the human contribution to risk will be overestimated. A recovery process generally follows three phases: **detection** of the error, **diagnosis** of what went wrong and how, and **correction** of the problem.

Human Factors Analysis of Current Situation				**Human factors additional measures to deal with human factor issues**		**NOTES**
Task or task step description	**Likely human failures**	**Potential to recover** from the failure before consequences occur	**Potential consequences** if the failure is not recovered	Measures to **prevent the failure** from occurring	Measures to **reduce the consequences** or **improve recovery potential**	**Comments**, references, questions
Task step 1.2 – CRO initiates emergency response (within 20 minutes of detection)	**Action Too Late:** Task step performed too late, emergency response not initiated in time	CR supervisor initiates emergency response	Emergency shutdown not initiated, plant in highly unstable state, potential for scenario to escalate	Optimise CR interface so that operator is alerted rapidly and provided with info required to make decision; training; practice emergency response	Recovery potential would be improved by ensuring that the CCR is manned at all times and by clear definition of responsibilities	
Task step 1.3 – CRO checks that emergency response successfully shut down the plant	**Check Omitted:** Verification not performed	Supervisor may detect that shutdown not completed	Emergency shutdown not initiated, or only partially complete, as above	Improve feedback from CR interface	Ensure that training covers the possibility that shutdown may only be partially completed. Ensure that the supervisor performs check	
Task step 1.4.1 - CRO informs outside operator of actions to take if partial shutdown occurs	**Wrong information communicated**: CRO sends operator to wrong location	Outside operator provides feedback to CRO before taking action	Delay in performing required actions to complete the shutdown	Provide standard communication procedures to ensure comprehension Provide shutdown checklist for CRO	Correct labelling of plant and equipment would assist outside operator in recovering CRO's error	

Task steps taken from procedures, walk through of operation and from discussion with operators.

This column records the types of human error that are considered possible for this task. It also includes a brief description of the specific error. Note that more than one type of error may arise from each identified difference or issue.

This column records the consequences that may occur as a result of the human failure described in the previous columns.

This column details suggestions as to how the consequences of an incident may be reduced or the recovery potential increased should a failure occur.

This column provides the facility to insert additional notes or comments not included in the previous columns and may include general remarks, or references to other tasks, task steps, scenarios or detailed documentation. Areas where clarification is necessary may also be documented here.

Question set: Identifying human failures

	Question	Site response	Inspectors view	Improvements needed
1	What does the site understand by the term ‘human failure’? Do they recognise the difference between intentional and unintentional errors?			
2	Do they consider that human error is inevitable, or can failures be managed, and how?			
3	What are the typical ways to prevent human failure?			
4	What are the main hazards on the site? How has the site addressed human failures that may contribute to major accidents? (e.g.1 if a significant risk is reactions in batch processes, how has the site addressed human failure in charging incorrect amount or type of product? e.g.2 if a significant risk is transfer between storage and road/rail tankers, how has the site addressed temporary pipework/hose connection failures?)			
5	Is there a formal procedure for conducting human failure analyses? – Is there any science/method to how they assess human failures, or is it seen as ‘common sense’?			
6	Does the site identify those manual operations that impact on major accident hazards? (for example, maintenance, start-up, shut down, valve movements, temporary connections).			
7	Does the site identify the key steps in these operations? – How (e.g. by talking through the task with operators, walking through the operation, reviewing documentation)? – How do they record this analysis/what formal techniques used (if any)?			
8	Does the site identify potential failures that may occur in these key steps (e.g. failure to complete the task, completing tasks in the wrong order)?			
9	What types of failures did the site identify? - Do they include unintentional failures as well as intentional violations? – Do they address mental (decision making) failures or communication failures, as well as physical failures?			
10	If they claim to perform human failure analyses ‘as part of HAZOP’, what list of potential failures do they refer to (i.e. what is the error taxonomy – does it include action too early, too late, on wrong object, action in wrong direction etc.). - If such a structure is not used then how do they ensure that all potential errors are identified?			
11	Does the site identify factors that make these failures more or less likely (such as workload, working time arrangements, training & competence, clarity of interfaces/labelling)?			

	Question	Site response	Inspectors view	Improvements needed
12	Has the site considered the hierarchy of control measures in addressing the human failure (e.g. by eliminating the hazard, rather than simply providing training)?			
13	Do control measures focus solely on training and procedures? – Is there any recognition that people do not always follow procedures? – How do they ensure that people always follow procedures? - What factors do they consider might lead to non-compliance with procedures? – Is there awareness that training can only help to prevent mistakes (mental errors) and that training has no effect in preventing unintentional failures (slips) or intentional violations?			
14	Do analyses lead to new control measures, or are failures considered to be addressed by existing controls? - Obtain an example of a measure that was implemented as a result of human failure analysis.			
15	Have attempts been made to optimise the performance influencing factors to make failures less likely (e.g. addressing shift patterns, increasing supervision, updating P&IDs/procedures, clarifying roles)?			
16	Are operators involved in assessments of activities for which they are responsible? (e.g. task analysis or identifying potential failures).			
17	How has the site recorded such assessments?			
18	What training/experience do the assessors have to demonstrate that they are able to identify potential human failures and means of managing them? – How do they know that they have identified all of the failures and influencing factors?			
19	Have estimates of human failure probabilities been produced? - By what technique? - What were these probabilities used for? – How precise are these estimates and what are the confidence intervals?			
20	Has the site employed external help/advice in conducting these assessments?			
21	Has the site considered human failures in process upsets or emergency situations? Have they considered how the influences on behaviour may be different under these circumstances? (e.g. people may experience higher levels of stress in dangerous or unusual situations, or their workload might be greatly increased in an upset).			
22	Does the analysis focus on operator failure, or do they address management failures? – what about failures in planning, allocation of resources, selection of staff, provision of suitable tools, communications, allocation of roles/responsibilities, provision of training, organisational memory etc.)?			