Human Factors Safety Information

Prepared by the Safety Advisory Council

Safety Info HF 13/12

# Organisation

# Human Reliability

## Human Reliability

There are many terms that are used to describe how people contribute to safety events, including human failure and human error. In this document we use the term 'Human Reliability' to describe an area of safety management that considers the human contribution to risk and the systems we need to reduce that risk.

Human failures, as the name suggests, is a general term for where the actions of people have been deficient in some way and this has led to an accident or loss. Human failures are recognised as being a major contributor to accidents and incidents as they frequently result in immediate or latent hazardous situations (unsafe behaviours and conditions). Consequences can include injury, loss of containment, loss of process integrity, failure of plant and equipment.

The two main types of human failure are errors and violations, and these are described later.

Human Reliability is therefore concerned about understanding where humans can contribute to safety risks and reducing both the likelihood and severity of the potential outcomes.

## Human Reliability Assessment

The likelihood of a human error occurring during a task is directly related to the way the task itself is designed and the quality of the following key factors:

- Organisation, including the safety culture;
- Job/task, including complexity, design and documentation (e.g. written procedures); and
- Individual, including operator competence and behavioural factors.

Other sheets in the EIGA Human Factors series provide further details on these factors.

Human reliability assessment (can also be known as Human Error Analysis) is used to gather and present



***EUROPEAN INDUSTRIAL GASES ASSOCIATION*** *AISBL*
AVENUE DES ARTS 3 – 5 ♦ B-1210 BRUSSELS
PHONE +32 2 217 70 98 - FAX + 32 2 219 85 14 - E-mail : info@eiga.eu - www.eiga.eu

information on these factors in a logical way. Organisations use human reliability assessment to examine the extent to which they have these factors under good control. If the level of control (and therefore human reliability) can be improved, the assessment will point to how this may be achieved.

Certain techniques are available to generate 'human error probabilities' for tasks giving an estimate of the risk of human error. Different tools and techniques are also available for examining violations (e.g. 'ABC analysis').

## Learning more about Human Reliability

### Management questions:

1. Does the organisation understand the term 'human failure'?
2. Does the organisation recognise the difference between intentional failures (violations) and unintentional failures (errors)?
3. Does the organisation consider that human error is inevitable, or that failures cannot be managed? In other words, can we only eliminate human error through process design?
4. Is there a formal procedure for conducting human reliability assessments?
   - Is there any science/method as to how the organisation assesses human failures, or is it seen as 'common sense'?
5. Does the organisation identify those critical operations (not just manual) that impact on major accident hazards and the risks of human error?
   - e.g. maintenance, start-up, shut down, valve movements, temporary connections.
6. Does the organisation identify the key steps in the operations?
   - e.g. by talking through the task with operators, walking through the operation, reviewing documentation.
7. Does the organisation identify potential human failures that can occur in the key steps in the operations?
   - e.g. failure to complete the task, completing tasks in the wrong order.
   - Does the organisation include unintentional errors as well as intentional violations?
   - Does the organisation address mental failures (decision making) or communication failures, as well as physical failures?
8. Does the organisation identify factors that make these failures more or less likely (such as workload, working time arrangements, training and competence, clarity of interfaces/labelling)?
9. Does the organisation apply the hierarchy of control measures in addressing the human failure (e.g. by eliminating the hazard, rather than simply providing training)?
10. Do assessments lead to new control measures, or confirmation that failures are addressed by existing controls?
11. Are operators involved in assessments of activities for which they are responsible (e.g. task analysis or identifying potential failures)?
12. Are human reliability assessments recorded?
13. Do the assessors have training and experience to demonstrate that they are able to identify potential human failures and the means to manage them?
    - How do they know that they have identified all of the failures and influencing factors?
14. Does the organisation consider human failures in process deviations or emergency situations?
    - Does the organisation consider how the influences on behaviour may be different under these circumstances? (e.g. people can experience higher levels of stress in dangerous or unusual situations, or their workload might be greatly increased in a deviation from normal operation).
15. Does the assessment focus only on operator failure, or does the assessment also consider management and system failures?
    - e.g. failures in planning, allocation of resources, selection of staff, provision of suitable tools and procedures, communications, allocation of roles/responsibilities, provision of training and competency

assessment, organisational memory.

***If the answer to any of the above is 'no', then you need to take action!***

## Types of Human Failures

It is important to remember that human failures are not random, and are usually familiar and predictable. It is also important to understand the different failure types because they have different causes and influencing factors and the ways of preventing or reducing the failures are also different.

The types of human failure that can lead to incidents may be categorised as follows:

**Unintentional**

**Errors** are an action that was not intended or a decision that resulted in an unintended outcome. There are two important types of error:

- action errors, where the action was not as planned, through either a slip (e.g. pressing the wrong button or reading the wrong gauge) or a lapse (e.g. forgetting to carry out a step in a procedure); and
- thinking errors, commonly known as mistakes, are errors of judgement or decision-making where the intended actions are wrong (i.e. where we do the wrong thing believing it to be right)

**Intentional**

**Violations** are a deliberate deviation from a rule or procedure or established behavioural norm. They differ from the above in that they are intentional (but usually well-meaning) failures, such as taking a short-cut or non-compliance, e.g. deliberate deviations from the rules or procedures. They are rarely wilful (e.g. sabotage) and usually result from an intention to get the job done despite the consequences.

- **Unintended violations:** a breach of a rule or procedure, but the person was unaware or did not understand the rule or procedure. The person commits the violation because of their lack of knowledge, training or skill. Note that this is a similar failure to a 'mistake' – the distinction being a rule or procedure is breached in a violation.
- **Situational violation:** a person chose to break a rule or procedure as they considered compliance with rules or procedures would make the task or activity unworkable e.g. special tools or equipment such as work platform were not available.
- **Organisational benefit violations:** a person chose to break a rule or procedure as they felt it would benefit the organisation e.g. quicker and cheaper.
- **Personal benefit violation:** a person chose to break a rule or procedure because they personally benefited e.g. taking short cuts to finish the work so they can go home early.
- **Reckless violation:** person chose to break a rule or procedure without any or proper regard to the consequences, including malicious acts.

As previously stated, there are various other models that classify violations in a different way. For example, the UK HSE classifies violations as follows:

- **Routine violations:** a behaviour in opposition to a rule, procedure, or instruction that

has become the normal way of behaving within the person's peer/work group. This term applies to any type of violation and raises issues about the role of supervisors / management.

- **Exceptional violations:** these violations are rare and happen only in unusual and particular circumstances, often when something goes wrong in unpredicted circumstances e.g. during an emergency situation. Acts of sabotage, ranging from vandalism by a de-motivated employee to terrorism could be included in this category.
- **Situational violations:** these violations occur as a result of factors dictated by the worker's immediate work space or environment (physical or organisational).

The motivation for violations also vary, including where there is personal benefit (e.g. taking short cuts or rushing so as to go home early), organisational benefit (e.g. where the individual believes their manager or supervisor want it done that way, or their behaviour action will result in a better outcome for the company) or reckless violations (e.g. the individual simply does not care or consider the outcomes from their actions).

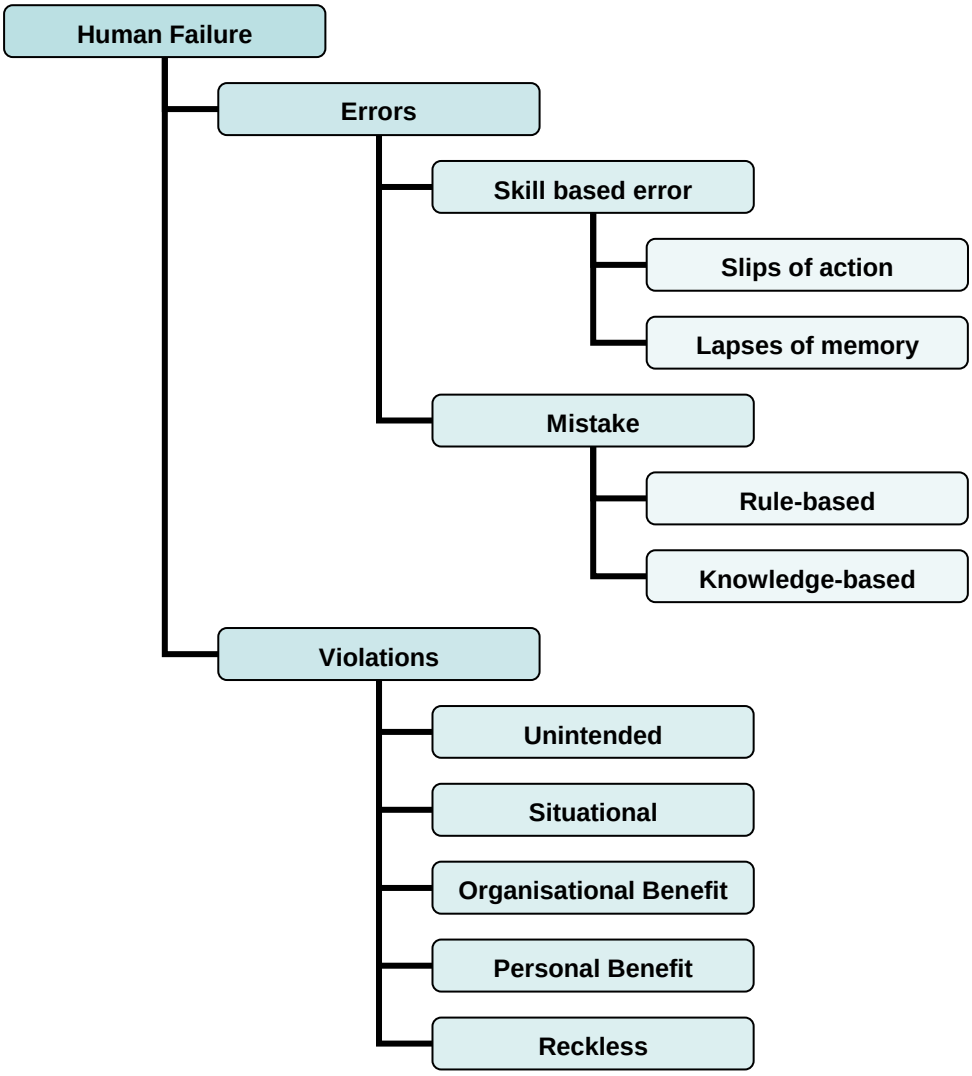


*Figure 1: Hierarchy of Human Failures*

## How Human Failures contribute to incidents

People can cause or contribute to incidents (or mitigate the consequences) in a number of ways:

- Through a failure a person can directly cause an accident. However, people do not make errors deliberately. We are often 'set up to fail' by the way our brain processes information, by our training, through the design of equipment and procedures and even through the culture of the organisation we work for.
- People can make disastrous decisions even when they are aware of the risks. We can also misinterpret a situation and act inappropriately as a result. Both of these can lead to the escalation of an incident.
- We can intervene to stop potential incidents. Many companies have their own anecdotes about recovery from a potential incident through the timely actions of individuals. Mitigation of the possible effects of an incident can result from human resourcefulness and ingenuity.
- The severity of injury can be reduced by the emergency response of management/supervisors and operators. Emergency planning and response including appropriate training can significantly mitigate the impact of the emergency situations and improve the speed of recovery to normal operations.

The consequences of human failures can be immediate or delayed:

| | |
|---|---|
| **Active** | Active failures often have an immediate consequence or at-risk situation and are usually made by front-line people such as drivers, control room staff or machine operators. In a situation where there is no room for error these active failures have an immediate impact on health and safety. |

| | |
|---|---|
| **Latent** | Latent failures are made by people whose tasks are removed in time and space from operational activities, e.g. designers, decision makers and managers. Latent failures are typically failures in operational and health and safety management systems (design, implementation or monitoring). Examples of latent failures are:<br>• poor design of plant and equipment;<br>• ineffective training;<br>• inadequate supervision;<br>• ineffective communications; and<br>• uncertainties in roles and responsibilities.<br>Latent failures provide a greater risk to the effectiveness of an organisation's health and safety management than active failures. Latent failures are usually hidden within an organisation until they are triggered or revealed by an event likely to have serious consequences (e.g. an active failure). |

## Managing human failures – common pitfalls

There is more to managing human failure in complex systems than simply considering the actions of individual operators. However, there is obvious merit in managing the performance of the personnel who play an important role in preventing and controlling major incidents, as long as the context in which this behaviour occurs is also considered.

There are several mistakes that organisations commonly make when assessing human performance in relation to

failures. These may include:

- Assuming operators would be able to carry out all tasks during emergencies.
- Providing precise probabilities of human failure (usually indicating very low chance of failure) without documenting assumptions/data sources.
- Assuming that an operator will always be present, detect a problem and immediately take appropriate action.
- Assuming that people will always follow procedures.
- Stating that operators are well-trained, when it is not clear how the training provided relates to hazard or incident prevention or control and without understanding that training will not always affect the prevention of slips/lapses or violations, only mistakes.
- Stating that operators are highly motivated and thus not prone to unintentional failures or deliberate violations.
- Ignoring the human component completely, failing to discuss human performance at all in risk assessments, leading to the impression that the site is unmanned.
- Overcomplicating the workplace, so that operators lose sight of the critical tasks or controls.
- Making grand statements that human error is completely under control (without stating exactly how).

## Managing human failures – three serious concerns

The misconceptions discussed above can be summarised into three areas of concern, where organisations do not adequately address human factor issues:

| | |
|---|---|
| **Concern 1** | An imbalance between hardware and human issues and focusing only on engineering issues. |
| **Concern 2** | Focusing on the human contribution to personal safety rather than to the initiation and control of hazards. |
| **Concern 3** | Focusing on ‘operator error’ at the expense of ‘system and management failures’. |

## What should my organisation do about it?

**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 can influence human performance, and
- **quantitative** assessments which, in addition, aim to estimate the likelihood of such failures occurring. The results of quantitative HRAs may feed into traditional 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.

**Why carry out a human reliability assessment?**

One reason is that human failure is a major cause of 'disruption' (not just injuries, but plant downtime, defects in product quality, environmental damage etc) and needs to be controlled. Near miss reports may indicate an unacceptable level of human failure in the organisation. In some countries, regulations (e.g. Seveso/COMAH) mandate that site safety cases/reports should show that the organisation is acting responsibly to reduce human failures for major hazard scenarios.

In general, it is a positive advantage for an organisation to understand better what might be causing failures and to take steps to reduce their likelihood.

**Advantages of human reliability assessment**

- Provides a logical and comprehensive assessment of factors influencing human performance.
- Leads to recommendations for improvement.
- Supports the safety case: forces attention on safety critical tasks.
- Can increase workers engagement in safety management.

**Disadvantages of human reliability assessment**

- Can be time-consuming and costly, particularly if the risk from human failure in a task is low.
- May require specialist input.
- Some of its methods may not be validated.
- May require extensive consultation with Unions/ Workers councils etc.

## 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 those involved to understand the expectations.

A proforma for recording the Human Reliability Assessment is provided in Table 1 at the end of this document.

Overview of key steps:

- Step 1: identify main site hazards;
- Step 2: identify critical human 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/less likely;
- Step 6: manage the failures using hierarchy of control; and
- Step 7: manage failure recovery.

**Step 1: Consider main site hazards**

Identify the main hazards and risks on the site, with reference to the Site safety report and risk assessments.



***EUROPEAN INDUSTRIAL GASES ASSOCIATION*** *AISBL*
AVENUE DES ARTS 3 – 5 ♦ B-1210 BRUSSELS
PHONE +32 2 217 70 98 - FAX + 32 2 219 85 14 - E-mail : info@eiga.eu - www.eiga.eu

**Step 2:**

**Identify manual activities that affect these hazards**

Identify activities in these risk areas with a high or critical human component. The aim of this step is to identify human interactions with the system which constitute significant sources of risk if human failures occur. For example, there is usually more opportunity for human failure in filling a liquid oxygen road tanker than in operating a static liquid oxygen storage vessel due to the higher number of manual operations in tanker filling. Human interactions which shall require further assessment are:

- those that have the potential to initiate an event sequence (e.g. incorrect valve operation causing a loss of containment);
- those required to stop an incident sequence and;
- actions that can escalate an incident (e.g. inadequate maintenance of a hose).

Assess 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 may be obtained through:

- talking to operators (preferably going through the operation step by step);
- task observation;
- review of procedures, job aids and training materials;
- review of the relevant risk assessment.

This assessment of the task steps establishes what the person needs to do to carry out a task correctly. It should include a description of what is done, what information is needed (and where this comes from) and interactions with other people and systems.

**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 intentional. Use the guidewords below for the **key steps** of the activity. Key steps to assess 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 incorrectly 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.

Note that an operator may make the same failure on several occasions, known as dependency. E.g. an operator may wrongly calibrate more than one instrument because a miscalculation has been made.

A more detailed list of 'failure types', similar to HAZOP guidewords, can be used in place of the simplified version and is provided here:

| Action Failures | Information Retrieval Failures |
|---|---|
| A1 - Operation too long / short | R1 - Information not obtained |
| A2 - Operation mistimed | R2 - Wrong information obtained |
| A3 - Operation in wrong direction | R3 - Information retrieval incomplete |
| A4 - Operation too little / too much | R4 - Information incorrectly interpreted |
| A5 - Operation too fast / too slow | **Information Communication Failures** |
| A6 - Misalign | I1 - Information not communicated |
| A7 - Right operation on wrong object | I2 - Wrong information communicated |
| A8 - Wrong operation on right object | I3 - Information communication incomplete |
| A9 - Operation omitted | I4 - Information communication unclear |
| A10 - Operation incomplete | **Selection Failures** |
| A11 - Operation too early / late | S1 - Selection omitted |
| **Checking Failures** | S2 - Wrong selection made |
| C1 - Check omitted | **Planning Failures** |
| C2 - Check incomplete | P1 - Plan omitted |
| C3 - Right check on wrong object | P2 - Plan incorrect |
| C4 - Wrong check on right object | **Violations** |
| C5 - Check too early / late | V1 - Deliberate breach of rules or procedures |

**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 can vary on a continuation from the best practicable to worst possible outcome. When all the PIFs relevant to a particular situation are optimal, then failure likelihood will be minimised.

HSG48[3] also lists often-cited causes of human failures in incidents under the three headings of Job (or Task), Individual and Organisation.

**Step 6:**

**Manage the failures using**

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

- Can the hazard be removed?

| | |
|---|---|
| **hierarchy of control** | • 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.)?<br>• Can the consequences of the human failure be prevented, e.g. by additional barriers in the system?<br>• Can human performance be assured by mechanical or electrical means? e.g. 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.<br>• 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:**<br>**Manage failure recovery** | Should it still be possible for failures to occur, improving failure recovery and mitigation are the final risk reduction strategies. The objective is to ensure that, should a failure occur, it can be identified and recovered from (either by the person who caused the failure or someone else such as a supervisor) – i.e. making the system more 'failure tolerant'. A recovery process generally follows three phases: detection of the failure, diagnosis of what went wrong and how, and correction of the problem.<br>Detection of the failure may include the use of alarms, displays, direct feedback from the system and competent supervisor monitoring/checking. There may be time constraints in recovering from certain failures in high-hazard industries, and it should be borne in mind that a limited time for response (particularly in a deviation/emergency) is in itself a factor that increases the likelihood of failure. |



***EUROPEAN INDUSTRIAL GASES ASSOCIATION*** *AISBL*
AVENUE DES ARTS 3 – 5 ♦ B-1210 BRUSSELS
PHONE +32 2 217 70 98 - FAX + 32 2 219 85 14 - E-mail : info@eiga.eu - www.eiga.eu

**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.

## Useful Reference Information


1. Health and Safety Executive, Humans and Risks, HSE Human Factors Briefing Note No 3.
2. Health and Safety Executive, HSE Human Factors Toolkit, June 2004.
3. Health and Safety Executive, Reducing Error and Influencing Behaviour, HSG48, 2007, HSE Books ISBN 978-0-7176-2452-2
4. Institute of Petroleum, Human Reliability Analysis, Human Factors Briefing Note No 12, 2003.
5. EIGA, Human Factors Safety Information series. http://www.eiga.eu/index.php?id=317
6. Various 'Just Culture' models