energy INSTITUTE

Guidance on quantified human reliability analysis (QHRA)

Guidance on quantified human reliability analysis (QHRA)

November 2012

Published by
ENERGY INSTITUTE, LONDON
The Energy Institute is a professional membership body incorporated by Royal Charter 2003
Registered charity number 1097899

The Energy Institute (EI) is the leading chartered professional membership body supporting individuals and organisations across the energy industry. With a combined membership of over 14 000 individuals and 300 companies in 100 countries, it provides an independent focal point for the energy community and a powerful voice to engage business and industry, government, academia and the public internationally.

As a Royal Charter organisation, the EI offers professional recognition and sustains personal career development through the accreditation and delivery of training courses, conferences and publications and networking opportunities. It also runs a highly valued technical work programme, comprising original independent research and investigations, and the provision of EI technical publications to provide the international industry with information and guidance on key current and future issues.

The EI promotes the safe, environmentally responsible and efficient supply and use of energy in all its forms and applications. In fulfilling this purpose the EI addresses the depth and breadth of energy and the energy system, from upstream and downstream hydrocarbons and other primary fuels and renewables, to power generation, transmission and distribution to sustainable development, demand side management and energy efficiency. Offering learning and networking opportunities to support career development, the EI provides a home to all those working in energy, and a scientific and technical reservoir of knowledge for industry.

This publication has been produced as a result of work carried out within the Technical Team of the EI, funded by the EI's Technical Partners. The EI's Technical Work Programme provides industry with cost-effective, value-adding knowledge on key current and future issues affecting those operating in the energy sector, both in the UK and internationally.

For further information, please visit **http://www.energyinst.org**

The EI gratefully acknowledges the financial contributions towards the scientific and technical programme
from the following companies

BG Group
BP Exploration Operating Co Ltd
BP Oil UK Ltd
Centrica
Chevron
ConocoPhillips Ltd
EDF Energy
ENI
E. ON UK
ExxonMobil International Ltd
International Power
Kuwait Petroleum International Ltd
Maersk Oil North Sea UK Limited
Murco Petroleum Ltd
Nexen
Phillips 66
Premier Oil
RWE npower
Saudi Aramco
Shell UK Oil Products Limited
Shell U.K. Exploration and Production Ltd
SSE
Statoil
Talisman Energy (UK) Ltd
Total E&P UK Limited
Total UK Limited
Valero
World Fuel Services

However, it should be noted that the above organisations have not all been directly involved in the development of this publication, nor do they necessarily endorse its content.

ISBN 978 0 85293 635 1

Published by the Energy Institute
The information contained in this publication is provided for general information purposes only. Whilst the Energy Institute and the contributors have applied reasonable care in developing this publication, no representations or warranties, express or implied, are made by the Energy Institute or any of the contributors concerning the applicability, suitability, accuracy or completeness of the information contained herein and the Energy Institute and the contributors accept no responsibility whatsoever for the use of this information. Neither the Energy Institute nor any of the contributors shall be liable in any way for any liability, loss, cost or damage incurred as a result of the receipt or use of the information contained herein.

Further copies can be obtained from: Portland Customer Services, Commerce Way, Whitehall Industrial Estate, Colchester CO2 8HP, UK.
t: +44 (0)1206 796 351 e: **sales@portland-services.com**

Electronic access to EI and IP publications is available via our website, **www.energypublishing.org**.
Documents can be purchased online as downloadable pdfs or on an annual subscription for single users and companies.
For more information, contact the EI Publications Team.
e: **pubs@energyinst.org**

CONTENTS

Page

Annexes:

FOREWORD

Major accidents in the energy and kindred process industries have illustrated the influence of people upon the performance of safety (and environmental) critical systems. Consequently, there is an increasing requirement for major accident hazard installations to demonstrate that human factors issues are being properly managed.

Many of the risk assessment techniques used in industry involve quantification, and the value of their outputs relies heavily on the quality of the data they use. Whilst there are some human reliability analysis (HRA) techniques and human error probability (HEP) data available to support the integration of human factors issues in these analyses, their application can be difficult. In particular, HEPs are often used without sufficient justification.

HRA techniques are designed to support the assessment and minimisation of risks associated with human failures. They have both qualitative (e.g. task analysis, failure identification) and quantitative (e.g. human error estimation) components. This publication focuses primarily on techniques that provide support for quantification.

EI *Guidance on quantified human reliability analysis (QHRA)* aims to reduce the instances of poorly conceived or executed analyses by equipping organisations that plan to undertake, or commission, HRAs with an overview of important practical considerations. It proceeds to outline some of the difficulties with the application of HRA techniques. It promotes the real value of an HRA coming not from the generated HEP, but from the in-depth understanding of task issues that results from the analysis.

This publication is intended for three main audiences:

1. Plant managers or general engineering managers, responsible for commissioning HRA studies.
2. Risk analysis practitioners who need to undertake HRA studies on behalf of their clients and who wish to refresh their knowledge.
3. Senior managers looking for a concise overview of the main issues associated with HRAs.

This publication makes no explicit reference to the requirements of legislative frameworks; however, the intent is that it should be particularly applicable to installations with major accident hazards (i.e. those subject to safety cases) that warrant robust assurance of human performance. Consequently, its guidance should be internationally applicable provided it is read, interpreted and applied in conjunction with relevant national and local requirements.

The information contained in this publication is provided for general information purposes only. Whilst the Energy Institute and the contributors have applied reasonable care in developing this publication, no representations or warranties, express or implied, are made by the Energy Institute or any of the contributors concerning the applicability, suitability, accuracy or completeness of the information contained herein and the Energy Institute and the contributors accept no responsibility whatsoever for the use of this information. Neither the Energy Institute nor any of the contributors shall be liable in any way for any liability, loss, cost or damage incurred as a result of the receipt or use of the information contained herein.

This publication may be further reviewed from time to time. It would be of considerable assistance in any future revision if users would send comments or suggestions for improvement to:

The Technical Department
Energy Institute
61 New Cavendish Street
LONDON, W1G 7AR
e: technical@energyinst.org.uk

ACKNOWLEDGEMENTS

EI *Guidance on quantified human reliability analysis (QHRA)* was commissioned at the request of the Human and Organisational Factors Committee and contracted to Human Reliability Associates, whose authors were Jamie Henderson and Dr David Embrey. Technical direction was provided by the Process Safety Committee's SILs/LOPAs Working Group, which also comprised during the project:

Ron Bell	Engineering Safety Consultants
Ian Bradby	ABB Engineering Services
Peter Davidson	UKPIA (member, Process Safety Committee)
Bill Gall	Kingsley Management (member, Human and Organisational Factors Committee)
Dr Alan King	ABB Engineering Services
King Lee (Chairperson)	Lloyd's Register (member, Process Safety Committee)
Dr Mike Nicholas	Environment Agency
Tom Ramsey	Esso Petroleum (Chair, Electrical Committee)
Graham Reeves	BP (Chair, Human and Organisational Factors Committee)
Dr Mark Scanlon (Secretary)	Energy Institute
Toby St. Leger	ConocoPhillips/BOL (member, Process Safety Committee)
Dr John Symonds	ExxonMobil (member, Human and Organisational Factors Committee)
Chris Wheeler	Valero Pembroke Refinery

The Institute wishes to record its appreciation of the work carried out by them in providing technical direction to the project.

Significant comments on the drafts of this publication that were issued for technical reviews were received from:

Peter Davidson	UKPIA
Bill Gall	Kingsley Management
Dr Alan King	ABB Engineering Services
Neil Macnaughton	BP
Tom Ramsey	Esso Petroleum
Dr Mark Scanlon	Energy Institute
Toby St. Leger	ConocoPhillips/BOL
Chris Venn	Chevron

Such comments have been considered and, where appropriate, incorporated. The Institute wishes to record its appreciation of the work carried out by them and others who participated during the technical reviews.

Project co-ordination and technical editing was carried out by Dr Mark Scanlon (Energy Institute).

Affiliations refer to time of participation.

1 INTRODUCTION

1.1 PURPOSE

Major accidents, such as Three Mile Island, Piper Alpha, Longford and Texas City, have illustrated the influence of people upon the performance of safety (and environmental) critical systems. Consequently, there is an increasing requirement for major accident hazard installations to demonstrate that human factors issues are being properly managed.

Many of the risk assessment techniques used in industry involve quantification, and the value of their outputs relies heavily on the quality of the data they use. Whilst there are some human reliability analysis (HRA) techniques and human error probability (HEP) data available to support the integration of human factors issues in these analyses, their application can be difficult. In particular, HEPs are often used without sufficient justification.

HRA techniques are designed to support the assessment and minimisation of risks associated with human failures. They have both qualitative (e.g. task analysis, failure identification) and quantitative (e.g. human error estimation) components. This publication focuses primarily on techniques that provide support for quantification. Therefore when the term HRA is used it includes quantification, unless otherwise stated.

The guidance outlines some of the difficulties with the application of HRA techniques. In particular, without context-specific data, it is hard ever to have true confidence in the output of a quantified HRA: the uncertainties inherent in all HRA techniques mean that the generated HEP can only ever be a best estimate. Often, therefore, the real value of an HRA comes not from the generated HEP, but from the in-depth understanding of task issues that results from the analysis.

The aim of this guidance is to reduce the instances of poorly conceived or executed analyses by equipping organisations that plan to undertake, or commission, HRAs with an overview of important practical considerations.

1.2 SCOPE

This publication:

- Provides readers with guidance in the use of HRA techniques. In particular, with regard to the use of HEP data.
- Explains the difference between qualitative and quantitative HRA techniques.
- Sets out the issues that should be considered before undertaking an HRA.
- Explains some common pitfalls in the use of HEP data, and limitations in its use.
- Supports these explanations with examples from commonly used HRA techniques.
- Helps clients review HRA outputs developed by specialists.

This publication does not:

- Directly address the relative merits of HRA techniques. References are provided to such work.
- Provide a single worked example of an HRA for readers to use as a template, or reference tables of HEP probabilities. A key goal of this guidance is to emphasise the problem of analysts using techniques or HEPs without fully considering the operating context.

1.3 APPLICATION

1.3.1 Intended audience

This guidance is directed at three main audiences in the energy and kindred process industries:

1. Plant managers or general engineering managers, responsible for commissioning HRA studies. The guidance should enable them to:
   - Determine whether studies should be undertaken in-house by suitably qualified and experienced risk analyst practitioners, or with external assistance.
   - Understand the main inputs and processes involved.
   - Review HRA outputs and identify omissions or faults in analyses.

2. Risk analysis practitioners who need to undertake HRA studies on behalf of their clients and who wish to refresh their knowledge.

3. Senior managers looking for a concise overview of the main issues associated with HRAs.

This publication makes no explicit reference to the requirements of legislative frameworks; however, the intent is that it should be particularly applicable to installations with major accident hazards (i.e. those subject to safety cases) that warrant robust assessment and assurance of human performance. Consequently, its guidance should be internationally applicable provided it is read, interpreted and applied in conjunction with relevant national and local requirements.

1.3.2 How to use this publication

This publication is set out in four main sections:

1. Introduction (i.e. this section).
2. Introduction to HRA techniques.
3. Issues to consider before using HRA techniques.
4. The HRA process.

Section 2 introduces some commonly used HRA techniques, whereas Section 3 describes some typical pitfalls in the use of these techniques. These sections should give readers an appreciation of the topic, and assist them in deciding whether or not a quantified analysis is necessary and whether external support is required.

Section 4 sets out a generic HRA process, explains the main elements of the process, and further illustrates typical issues. This section will be of most use to readers that are making a direct contribution to, or have commissioned, an HRA analysis.

Annex A comprises three checklists that summarise some of the main points to consider when planning an HRA analysis:

– Checklist 1: Deciding whether to undertake HRA.
– Checklist 2: Preparing to undertake HRA.
– Checklist 3: Reviewing HRA outputs.

Using these checklists should help to ensure that the HRAs are only performed where necessary, and that, when they are carried out, they are as robust as possible.

Annex B, which provides detailed examples of QHRA analyses, and Annex F, which discusses issues related to the modelling of human failures, should be of most use to practitioners, rather than readers seeking an appreciation of the topic.

2 INTRODUCTION TO HRA TECHNIQUES

2.1 COMMONLY USED HRA TECHNIQUES

There are a large number of different HRA techniques that include quantification: HSE RR679 which was undertaken by Health & Safety Laboratory (HSL) on behalf of the Health & Safety Executive (HSE) identified 72 different HRA methods. However, only 17 of these were considered to be of potential use to the regulator, and only nine of those 17 are publicly available. None of the techniques has been conclusively validated. Annex D summarises these publicly available techniques along with their areas of development and application.

The respective merits of these techniques are purposely not addressed in this publication. However, HSE RR679 summarises the techniques' strengths and weaknesses. Further discussion of the concept of HRA, and of many of the techniques, can be found in specialist textbooks (e.g. Kirwan (1994) and CCPS *Guidelines for preventing human error in process safety*).

2.2 HISTORY OF QUANTIFIED HUMAN RELIABILITY ANALYSIS[1]

In the 1960s, once the impact of human performance on overall system risk had been appreciated, there was a drive to integrate human factors considerations into reliability assessments. These early attempts treated people like any other component in a reliability assessment (e.g. what is the probability of an operator failing to respond to an alarm?). Because these assessments were often quantified, there was a requirement for HEP data, which in turn led to attempts to develop HEP databases.

For several reasons, but mainly because of the realisation that people are not like other components - that they can make choices, and are influenced by a wide range of environmental factors - the database effort receded. Instead, so called, first generation HRA techniques were developed through the 1970s and 1980s. These were hybrid techniques, which used expert judgement to modify base HEPs to take account of contextual factors, known as performance influencing factors (PIFs) or performance shaping factors (PSFs) (e.g. time pressure, distractions and quality of training). Technique for Human Error Rate Prediction (THERP) and Human Error Assessment and Reduction Technique (HEART) are examples of these techniques.

A parallel strand of development was in the area of expert judgement. These techniques, such as Paired Comparisons (PCs) and Absolute Probability Judgement (APJ), addressed the data problem by fully embracing the use of expert judgement to develop HEPs.

As these techniques developed, it was recognised that critical actions in tasks are not always routine responses, but often involve decision-making and problem solving in unfamiliar situations. This led to an increased interest in not just the probability of a failure (e.g. an operator failing to close a valve) but also the reasons for its occurrence. This better understanding of the psychology of human failures resulted in less emphasis on quantification and more interest in modelling and understanding potential human failures – with the goal of identifying ways to make them less likely to occur.

[1] This section is partially based on the overview presented in SRD *Human reliability assessor's guide*.

During the 1990s so-called second generation HRA techniques built on these developments by extending the consideration of contextual factors and addressing deficiencies with first generation HRA techniques. Cognitive Reliability Error Analysis Method (CREAM) and A Technique for Human Error Analysis (ATHEANA) are examples of these techniques.

More recently, new tools, based on first generation techniques, have been developed. However, in practice, and despite some well-known issues with their application (see section 3.5), first generation techniques such as THERP and HEART, are still the most widely used techniques.

All HRA techniques have been most extensively applied to manage process safety risk (many were initially developed in the nuclear industry). However, most, if not all of the techniques could also be applied to environmental or commercial risk issues.

One common problem is that, rather than use HRA techniques, risk analysts requiring HEP data simply take figures directly from available databases. HSE RR716 provides a review of layers of protection analysis (LOPA) for a particular scenario: it cites several examples of this practice that used, for example, HEPs taken from tables in the functional safety standard IEC 61511-3. In many cases, these HEPs were presented without any justification or consideration of local factors that might influence their applicability.

This approach might arise from a lack of awareness of the issues HRA techniques seek to address, or from perceived difficulty with their application. However, whatever the reason, serious inaccuracies in the final risk assessment are the likely result. Equally importantly, however, failure to fully engage with human factors issues affecting HEPs will leave the analyst with little insight into how to reduce failure probabilities.

Whilst not a widespread practice, it is possible to overcome the problem of lack of relevant data by generating specific databases. Installations could generate their own data by using simulators, collecting field data, or by using formalised expert judgement methods.

Finally, the concept of human error itself has been the subject of discussion in the human factors community for many years. Therefore, in the context of HRA, the term human failure event may be more useful. In this publication, the term failure is used (this is not always possible as the term error is heavily enshrined in the HRA techniques discussed in this guidance, and in the unit of measurement – HEP). Where the term failure is used, the reader should assume it refers to human actions (and covers both errors and non-compliances) unless otherwise stated. Annex C contains a more detailed discussion of some of the issues related to the definition and classification of human failures.

3 ISSUES TO CONSIDER BEFORE USING HRA

3.1 QUALITATIVE AND QUANTITATIVE ANALYSES

One of the first issues to consider when planning a human reliability study is whether the analysis should be qualitative or quantitative. This publication focuses on quantification. However, there are many situations where a qualitative review will be more appropriate.

HRA is best seen as an in-depth assessment of risk, as a function of human performance, whereby a system's vulnerabilities to human failure can be identified, and defences improved accordingly (Kirwan (1994). Consequently, in many situations, a qualitative analysis should be sufficient: see EI *Guidance on human factors safety critical task analysis*.

However, there will still be situations where quantification is necessary. For example, in a LOPA study for safety integrity level (SIL) determination, a particular human failure may have been identified as an initiating event and, in order to complete the analysis, a human failure frequency may be required (see 3.4).

3.2 USING HRA TECHNIQUES TO IMPROVE TASK PERFORMANCE

The following sections outline some of the difficulties in the application of HRA techniques. One consequence of these difficulties is that, without context-specific data, it is hard ever to have true confidence in the output of a quantified HRA: the uncertainties inherent in all HRA techniques mean that the generated HEP can only ever be a best estimate. Whilst this is true of all quantified risk assessment (QRA), it is a particular issue for HRA (see 3.5).

A specific danger is that, even if the analyst and the commissioning team are aware of the limitations of the analysis, over time the generated probability comes to be seen as a true, accurate reflection of the operating risk, and used to support risk management decisions. Therefore, when considering a quantified analysis, the commissioning manager should always be clear about what the analysis is trying to achieve and ensure that any caveats and assumptions are carefully documented.

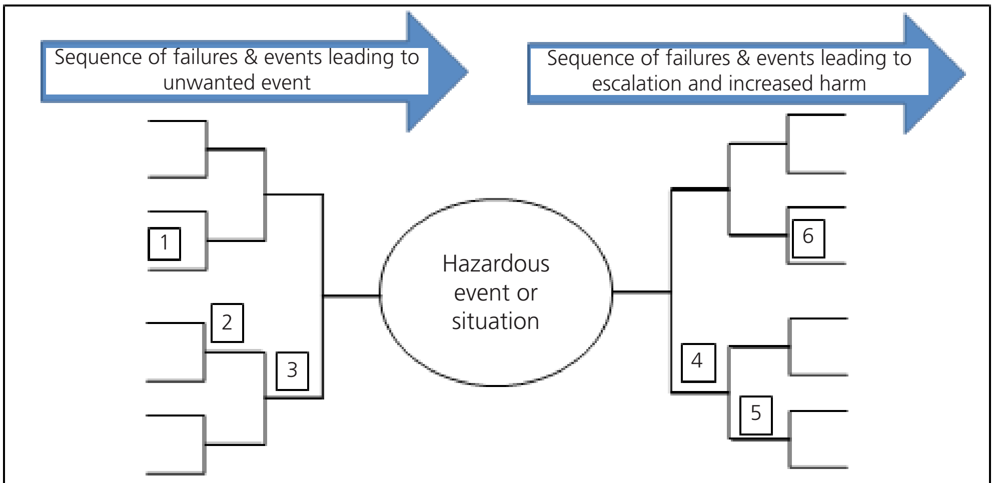
However, despite these limitations, many HRA techniques do provide the opportunity to consider and model the impact of PIFs upon safety (and environmental) critical tasks. Therefore, whilst the generated probability should ultimately be treated with caution, the consideration of different failure types and the impact of different PIFs should be assessed and used to reduce risk. For example, an HRA may indicate that quality of communication and equipment layout have a considerable influence over the probability of a specific task being performed correctly. Moreover, the scale of their influence in relation to other factors may be assessed. Therefore, whilst we may not be ultimately confident in the generated probability, we do have detailed evidence to support risk management decisions by focusing on the most significant PIFs.

3.3 INTEGRATION WITH BROADER RISK ANALYSES

Often HRA is performed in the context of a probabilistic safety analysis (PSA). HRA techniques vary in the support they provide for this integration process. For example, THERP provides a procedure for the complete analysis process, including development of event trees, whereas APJ only provides a way of generating an HEP.

Human failures can have an influence on risk at a variety of points in any given scenario.

Figure 1 Examples of potential impact of human failures on an event sequence


Sequence of failures & events leading to unwanted event
Sequence of failures & events leading to escalation and increased harm
Hazardous event or situation
1
2
3
4
5
6

1	Planning failure - latent (e.g. order incorrect chemicals)	4	Maintenance failure - latent (e.g. failure to calibrate gas detector correctly)
2	Maintenance reinstatement failure - active (e.g. failure to close drain valve after vessel maintenance)	5	Maintenance failure - latent (e.g. failure to reinstate deluge system following maintenance)
3	Operating failure - active (e.g. too great an amount into loading meter)	6	Operating failure - active (e.g. failure to operate manual emergency shutdown for correct section of plant)

The left hand side of the bow-tie diagram (Figure 1) shows events prior to the hazardous event or situation of concern; the right hand side illustrates events related to mitigation and potential escalation. The example failures provided in the diagram are illustrative rather than exhaustive, but they indicate that human failures can occur at any stage in a scenario. In particular, note that failures may be active, where consequences are realised almost immediately, or latent, meaning that they occur some time before the incident takes place. For example, a failure to reinstate a level switch after a function test may only become apparent at the time of the next demand on that system (i.e. when the level rises). Latent failures may also occur in the design process, or in management decisions.

3.4 OPERATOR RESPONSE IN SAFETY INSTRUMENTED SYSTEMS (SIS)

A specific situation where HRA quantification may be necessary is when an operator carries out part of the safety instrumented function (SIF) of the SIS to a specified SIL. It is outside the scope of this publication to describe how such a specific assessment might be carried out: see EI *Guidance on safety integrity level (SIL) determination* and UKPIA *Gap analysis and self assessment for operators & SIL 1 safety systems for overfill protection systems*. However, this section discusses some of the issues specific to this situation.

Whilst a fully automatic SIS (e.g. where a sensor detects a problem and responds automatically to prevent a hazardous event) would eliminate systematic failures due to operator error, there are occasions where it may be advantageous to include an operator in the loop (e.g. if an automated response generates a greater potential risk). The normative part of the standard IEC 61511 does not preclude an operator from carrying out part of a SIF. The supporting guidance in IEC 61511-2 clause 8.2.1 on this point states:

> "Where an operator, as a result of an alarm, takes action and the risk reduction claimed is greater than a factor of 10, then the overall system will need to be designed according to IEC 61511-1. The system that undertakes the safety function would then comprise the sensor detecting the hazardous condition, the alarm presentation, the human response and the equipment used by the operator to terminate any hazard. It should be noted that a risk reduction of up to a factor of 10 might be claimed without the need to comply with IEC 61511. Where such claims are made, the human factor issues will need to be carefully considered. Any claims for risk reduction from an alarm should be supported by documenting a description of the necessary response for the alarm and that there is sufficient time for the operator to take the corrective action and assurance that the operator will be trained to take the preventive actions."

In practice, a more common situation will be an operator responding to a basic process control system (BPCS) alarm outside the range of SIL 1 (i.e. with a probability of failure on demand (PFD) average in the range 1,0 to 0,1). However, even in this situation all claims of risk reduction should be justified, for example by the application of good engineering and operational practices. Even in this situation, the impact of human factors issues should be considered.

Of particular importance in the context of SIL determination is IEC 61511-1 clause 11.9.2 (i) which states:

> "The calculated probability of failure of each safety instrumented function due to hardware failure shall take into account:
>
> i). The estimated rate ['rate' should read 'probability'] of a dangerous failure of any human response in any modes which would cause a dangerous failure of the SIS (both detected and undetected by diagnostic test);"

Wherever an operator is proposed as part of a SIL 1 rated SIF, everything possible should be done to ensure the required human performance. In particular, it should be recognised that, in order to respond successfully to an alarm, an operator has to detect, interpret and respond to it correctly, and that failures could occur at each of these stages. Moreover, as HEPs are affected by contextual factors in the specific operating environment (see 3.5.3), any assessment should consider the potential impact of these factors upon the failure probability, and how their variation over the life of the system might influence the failure probability. The use of HEPs taken directly from tables, without awareness and consideration of the issues covered in this guidance, should be avoided. Sometimes, conservative HEPs are used in an attempt to avoid the need for detailed consideration of human factors issues; however, even where this is justified, the analyst should be wary of potential pitfalls. For example, recognising and addressing issues of dependence (see section 4.2.4).

Finally, it should be remembered that the probability of an operator failing to respond to an alarm is just one aspect of the PFD for the safety function. The PFD calculation should also include the sensors and alarms used to alert the operator, as well as the final element and the means by which the operator initiates this final element (e.g. the pushbutton which in turn closes the valve). Therefore, the PFD calculation should include all elements of the SIF and, in addition to the calculation of random events (i.e. the PFD), it will also be necessary to address systematic failures associated with human factors issues.

3.5 PRACTICAL ISSUES IN HRA

3.5.1 Expert judgement

Every HRA technique entails some degree of expert judgement. In some techniques, such as APJ, this is obvious to the casual reader, whereas in others, such as HEART, it may be less apparent. The practical implication of this is that, in order to get the best results, the HRA team should have a well-developed understanding of the task and operating environment and that, often, the skills and experience of the analyst are as important as the technique being used.

3.5.2 Lack of available HEP data

As previously discussed, the development of comprehensive HEP databases stalled early in the development of HRA. This may have been because of issues of confidentiality, an unwillingness to publish data on poor performance, or a lack of resources for collecting such data (Kirwan (1994)). However, the result is that it is difficult to find an HEP that exactly matches the specific task being considered.

3.5.3 Impact of task context upon HEPs

It may be argued that only data collected from the actual context in which a task is performed should be used to predict future failures in that situation. This is because human performance is extremely dependent upon task conditions. For example, a simple task, under optimal laboratory conditions, might have a failure probability of 0,0001; however, this probability could easily be degraded to 0,1 if the person was subjected to high levels of stress or distractions, or other PIFs/PSFs. Other examples of PIFs/PSFs include quality of procedures, quality of training, usability of equipment, and availability of information. More comprehensive lists of PIFs are provided in EI *Guidance on human factors safety critical task analysis.* There have been very few attempts to develop context specific HEP databases. Instead, the usual approach has been to take data from other sources, such as laboratory experiments, and modify HEPs to suit specific situations.

3.5.4 Sources of data in HRA techniques

A related issue is that, depending on the technique used, it can be difficult to establish the exact source of the base HEP data. It might be from operating experience, experimental research, simulator studies, expert judgement, or some combination of these sources. This has implications for the analyst being able to determine the relevance of the data source to the situation they are analysing. The question of whether generic laboratory based data, as opposed to context specific data, can be validly used as the basis for an analysis is outside the scope of this publication but is discussed in more detail in Kirwan (1994).

3.5.5 Variation in PIFs over time

The status of PIFs identified as influencing a specific HEP may vary over time. For example, some PIFs, such as equipment design, will remain relatively constant (i.e. the equipment configuration is largely fixed). However, other PIFs, such as time pressure or workload, may well vary from day-to-day, or even hour-to-hour. Any HRA should take care to consider the likely impact of such variation upon the results. In addition, if a particular PIF has been identified in an analysis as having an impact on the successful performance of a task, then consideration should be given to how this factor should be controlled at all times. For example, if successful response to a situation relies on a full complement of staff being available, then management systems should clarify how to maintain this status.

3.5.6 Effects of interactions between PIFs

Most human reliability techniques assume that PIFs affect HEPs in a linear manner (i.e. there is no interaction between the PIFs in terms of their effects on failure probability). In reality, combinations of negative PIFs which occur at the same time (e.g. lack of experience and time stress) are likely to have a greater adverse impact on error probability than their individual contributions suggest. This is true even if the quantification technique uses a multiplicative combination of the effects of the PIFs (e.g. HEART). This can to some extent be addressed by modifying the weights of the contributions of the PIFs to reflect this interaction. Although some techniques, such as those based on Influence Diagrams, address this issue, it is not taken into account by popular techniques such as HEART and THERP (Phillips et al (1990)).

3.6 COMPETENCE REQUIREMENTS

To ensure a successful HRA there should be expertise in a range of different areas. The main areas include:

- Understanding of the HRA process and human factors issues (e.g. by using a safety and reliability engineer with human factors expertise or a human factors consultant).
- Understanding of operational practices and the operating environment (e.g. by using experienced operators).
- Understanding of the system design and behaviour (e.g. by involving a control and instrumentation engineer).

Some of these areas of expertise may be held by the same individual. For example, one individual may have an understanding of the HRA process and human factors issues. If the analysis is to be part of a broader risk analysis, then expertise related to that analysis is also required. Some areas of expertise are more useful at specific stages of the HRA process. For example, there should be an experienced operator in the task analysis stage (Step 2 in process described in section 4.1), but this is less critical during modelling (Step 4 in that process).

The question of the extent to which organisations should attempt to undertake HRAs themselves, or engage external support, is difficult to answer. As this publication highlights, there is a range of practical and theoretical issues that should be taken into consideration when applying HRA techniques. This publication provides an introduction to some of these issues, but, even with this information, it may still be difficult for an individual with no previous human factors expertise to carry out a quantified HRA that will produce meaningful and defensible results. Therefore, when deciding whether to engage a consultancy, a customer may wish to enquire about their past experience with HRA analysis. In the UK, the Institute of Ergonomics and Human Factors (IEHF) maintains a list a consultancies who claim experience in the area of human reliability assessment.

Checklist – Competence requirements:

- Does the analysis team have at least one individual with an understanding of human factors issues?
- Does the analysis team have at least one individual with experience in the application of HRA techniques?
- Does the analysis team have at least one individual with experience of operational practices and the operating environment (for an existing installation)?
- Does the analysis team have at least one individual with an understanding of the process system design and behaviour?

4 THE HRA PROCESS

4.1 OVERVIEW OF PROCESS

Table 1 outlines the main steps of a generic HRA process based on Kirwan (1994). These steps are described in more detail in the following sections along with some common potential pitfalls.

Table 1 Generic HRA process

1. Preparation and problem definition
2. Task analysis
3. Failure identification
4. Modelling
5. Quantification
6. Impact assessment
7. Failure reduction
8. Review

As there is already published guidance on the qualitative aspects of HRA (EI *Guidance on human factors safety critical task analysis*), these areas are not covered in detail here. Annex E includes a discussion of the overlap with this publication. However, specific issues that might directly affect the quantification process are discussed in this section. More detailed coverage of these steps can be found in a variety of sources (e.g. Kirwan (1994) and CCPS *Guidelines for preventing human error in process safety*). Annex B includes two example analyses following the process set out in this section, along with a commentary highlighting some common issues in their application.

4.2 DESCRIPTION OF PROCESS

4.2.1 Step 1: Preparation and problem definition

An HRA can be used both to understand the relative impact of different failures upon system safety and prioritise risk reduction effort accordingly and to develop HEPs (e.g. as an input to a broader risk analysis or as a standalone HRA). Some of the issues related to the choice between a qualitative or quantitative HRA are discussed further in section 3.1.

Whilst the Annex B examples show analyses for existing plant, HRA can be applied at different stages in the system-design life cycle, and the earlier potential human factors issues are identified, the easier they will be to address. However, prior to detailed design, the process is unlikely to be sufficiently well defined to allow, for example, detailed task or PIF analysis. Therefore potential human factors issues, including requirements for HRA, should be identified at an early stage of a project and revisited throughout. Guidance is available on the integration of human factors in projects (e.g. OGP Report 454).

If the analysis is part of a larger PSA then the scope of the assessment may already be clear. However, the following items should be specified[2]:

- The risk metric to be used.
- Whether the analysis is to address likelihood, consequences, or both.
- The target audience for the output (e.g. regulators, design engineers).
- The scope of analysis (e.g. in terms of systems to be covered, modes of operation to be considered).
- The stage in plant lifecycle.

Finally, the problem definition should consider where, in the scenario in question, human actions may have an impact, and the relative importance of the actions to overall risk. Examples of possible actions could include[3]:

- Actions that cause equipment or systems to be unavailable when required (e.g. failure to reinstate a level switch following a function test).
- Actions that, either by themselves or in combination with system failures, initiate events (e.g. failure to close drain valve post-maintenance).
- Actions that exacerbate an event as it develops (e.g. opening the wrong valve and venting hydrocarbons directly to atmosphere).

If the main purpose of the HRA is to identify and reduce system vulnerabilities then, for the vast majority of situations, a qualitative analysis should be appropriate and sufficient. If human actions have a small impact on overall risk then an HRA may not be required.

Checklist – Preparation & problem definition:

- Is there a compelling reason for choosing a quantitative, rather than qualitative, analysis?
- Is it clear what value a quantitative analysis adds over a qualitative analysis?
- Are the terms and scope of the analysis clearly specified?
- If part of a PSA, has the interface with the PSA study been defined (e.g. the outputs required of the HRA by the PSA study, the scope of the HRA)?
- Has the impact of human reliability on different aspects of the scenario been considered (e.g. maintenance failures that affect layers of protection, failures that initiate event sequences, failures with the potential to make developing situations worse, and failures in recovery)?
- Have relevant previous incidents or studies been identified for reference?
- Have relevant input documents been identified and obtained (e.g. procedures, piping and instrumentation diagrams (P&IDs), vendors' instructions)?
- Has the analyst specified the HRA techniques they intend to use and explained why they feel those techniques are appropriate?
- Is human reliability a dominant variable in the overall risk?

[2] Adapted from USNRC NUREG-1880.

[3] Adapted from IAEA *Basic level 1 PSA course for analysts – Human reliability analysis.*

4.2.2 Step 2: Task analysis

Task analysis is the process used to describe how tasks are carried out. Before identifying possible failures, a good understanding of how the task is performed in practice should be developed. The UK Office of Nuclear Regulation (ONR), for example, considers an HRA to be incomplete if a task analysis has not been completed (HSE *Human reliability analysis*). In some cases (e.g. if the analysis is part of a larger PSA and if the failure of concern has already been identified), there may be a temptation to move directly to quantification (Step 5). However, care should be taken with this approach as the analysis team should have an in-depth knowledge of the task context (see section 3.5.3), and the task analysis process is a good way of developing this understanding.

There are many different task analysis techniques available (for a review, see Kirwan & Ainsworth (1992)). One commonly used method is Hierarchical Task Analysis (HTA), which is well-suited to planned, sequential tasks, such as preparation of a system for maintenance or start-up, of the type that are often found in process industries.

Existing procedures can be used as an input to task analysis. However, failure to develop a task analysis based on the practical realities of the task will affect the quality of the resulting HRA.

Potential pitfalls – Failure to develop a task analysis that takes account of task practicalities

A task involving the drainage of settled water from the base of a hydrocarbon storage tank had been selected for HRA review. One particular concern was a loss of containment (LOC) resulting from a failure to close the drain valve. The procedure stated that a sample should be taken to establish the interface between the drained water and the hydrocarbon. However, following discussion with operators, it emerged that none of the operating team took samples. Instead, they relied on their experience to identify the difference between water and hydrocarbon - they could smell, hear and see the difference. Furthermore, a task walkthrough established that there was no simple way of taking a sample, as access to the draining water was impeded by the tundish. A task analysis developed without this insight would have resulted in an inaccurate representation of the task as performed, and would have had a negative impact on the value of the remaining stages of the HRA.

A thorough task analysis provides an invaluable opportunity to understand the task under consideration. A good understanding of practical issues may suggest possible improvements even before the full HRA process has been completed.

Checklist – task analysis:

- Was a task analysis developed?
- Did the development of the task analysis involve task experts (i.e. people with experience of the task)?
- Did the task analysis involve a walkthrough of the operating environment?
- Is there a record of the inputs to the task analysis (e.g. operator experience, operating instructions, P&IDs, work control documentation)?

4.2.3 Step 3: Human failure identification

Once a description of how the task is carried out has been developed, the next stage is to identify potential human failures. The omission of a failure at this stage will have a significant impact on the validity of the HRA; therefore a formal identification process should be used.

To achieve this, a set of guidewords is typically applied to the steps identified in the task analysis to identify failures of concern (e.g. action omitted, action too late, action in wrong order). EI *Guidance on human factors safety critical task analysis* describes this process in more detail.

The initial focus is normally on the observable failure (e.g. failure to close a valve) rather than on the underlying failure mechanism. In other words, the description is most likely to be of what can go wrong, rather than why it might occur (a more detailed discussion of failure classifications is provided in Annex C).

A comprehensive list of observable failures should be developed as an input to a full HRA analysis. However, at this stage, probable reasons for these failures should also be considered (e.g. a non-compliance arising from a poor understanding of the task risks, inadvertently omitting a step from a well-practised task sequence, choosing the wrong response to a set of plant conditions). Understanding possible reasons for these failures helps with risk reduction (Annex C has further information). Similarly, whilst some HRA techniques include identification of PIFs later in the analysis process, it is good practice to consider factors that might influence the probability of failure at this stage, whilst the detail of the task is being considered.

If the analysis is purely qualitative in nature, then at this stage the analyst might proceed directly to Step 7 (failure reduction). Again for more detail, see EI *Guidance on human factors safety critical task analysis.*

Commentary – Identifying failures

Using a set of guidewords to identify potential deviations is a common approach to this stage of the analysis. In a qualitative analysis, a common issue is the time that this takes, if, for example, a workshop team works systematically through every step in a task analysis, and identifies all possible observable failures for each step. This can also have implications for a quantitative analysis, in that the more failures that are identified the more complex the subsequent modelling and quantification becomes. Moreover, the failures that are identified, or not identified, will have a significant influence on the final output. There are some steps that can be taken to reduce this complexity, and simplify the subsequent modelling stage:

- Being clear about the consequences of identified failures. If the outcomes of concern are specified at the project preparation stage then those failures that result in consequences that are not of immediate concern to the project (e.g. production and occupational safety issues) can be excluded.
- Documenting any planned opportunities for recovery of the failure before the consequences are realised (e.g. planned checks).
- Taking care to identify planned or existing control measures that prevent or mitigate the consequences of the identified failures. It will often be the case that, for the consequences of a failure to be realised, an additional hardware failure may be necessary. This information can be used as an input to the modelling phase.
- Grouping failures with similar outcomes together. For example, not doing something at all may be equivalent, in terms of outcome, to doing it too late. Care should be taken here, however, as whilst the outcomes may be the same, the reasons for the failures may be different.

Checklist – failure identification:

- Was a formal identification process used to identify all important failures?
- Does the analysis represent all obvious failures in the scenario, or explain why the analysis has been limited to a sub-set of possible failures?
- Was there consideration of possible underlying reasons for the identified failure?

4.2.4 Step 4: Human failure modelling

This is the point in the process where, if required, the HRA is integrated with a broader risk assessment. For example, failures identified during the previous stage might be represented alongside hardware and software failures in the chosen risk assessment format (e.g. fault tree, event tree).

If the HRA is being undertaken as a standalone activity, modelling is still important in order to identify the relative importance of individual failures and to consider issues such as dependency.

The degree of decomposition of the analysis should also be considered at this stage in the analysis. Quantification can take place at the level of the specific failure (e.g. probability of failure to close valve) or at a more global level (e.g. probability of failure to perform whole task). This is a complex consideration; Annex F contains a detailed discussion of related issues.

Potential pitfalls – Failure to model dependence

There are two aspects of dependence. One is concerned with the fact that checks being carried by a second person are rarely truly independent. The other is that activities performed by the same operator or team may be subject to systematic biases which mean that certain failure modes may be repeated. As both of these mechanisms may have an impact on the accuracy of the quantification, they need to be addressed in the qualitative modelling of the scenario, and/or the values that are selected for quantification of the HEP. Examples of these mechanisms follow.

A commonly-used control, to help increase the probability of a critical step being performed, is to include a requirement for a second check. For example, a supervisor may be asked to check that an instrument technician has reinstated a level trip following a function test. However, if the supervisor is busy, and has high regard for the ability of the technician, there is a possibility that they may assume the step has been performed, without properly checking the status themselves. Similarly, if an operator fails to appreciate that, to prevent long-term damage, a piece of equipment needs to be warmed-up for half an hour before start-up and shortens the warm-up time to 10 minutes accordingly, then that operator is likely to repeat this approach for all equipment of this type (a so-called common cause failure).

These steps are, therefore, dependent on each other, and pose a challenge to the HRA analyst. If dependency is not addressed, then the reliability of the system may be overestimated.

Support for modelling dependence is limited in established HRA techniques (e.g. THERP and Standardized Plant Analysis Risk Human Reliability Method (SPAR-H) have dependence modelling elements). However, an HRA should demonstrate that account has been taken of dependence issues. A more detailed discussion of this topic can be found in HSE OTO 2001/053.

Potential pitfalls – Overly-optimistic HRA outputs

Because of issues such as dependence, common cause failures and the difficulty in ensuring that a HRA model reflects the reality of a situation, HRAs should not make overly optimistic claims for human performance. There have been attempts to estimate human performance limiting values (HPLVs) based on performance limits and modelling uncertainty (Kirwan et al (1990)), essentially an estimate of the analyst's uncertainty in the modelling process. However, as these values are not data, but limits on the level of reliability that can be claimed in a risk assessment, then they should not be used as a substitute for a proper HRA.

Once the modelling process is complete it is possible to assign pessimistic probabilities to failures to determine those with the most influence on the overall scenario - this process is known as screening. Failures with the greatest influence may require more detailed evaluation.

However, if this approach is taken, and consequently HRA modelling is not used, on the basis that very low HEPs will result, or if HPLVs are used without HEP modelling, then care should be taken to ensure that the following issues are considered (HSE *Human reliability analysis*):

- There is no common cause potential between the initial failure and recovery actions.
- Availability of instrumentation, equipment and personnel will not be affected by the initial failure.
- Recovery factors are feasible under the conditions that will arise as a consequence of the initial failure.
- Possible failures during recovery have been identified.

Checklist – human failure modelling:

- If the HRA was part of a broader risk assessment, were the identified human failures modelled alongside other types of failure (e.g. hardware and software) to determine the overall system risk?
- Where several failures were identified as potentially relevant to the overall risk analysis, were these screened to determine which required the most detailed analysis?
- Were dependencies considered and, if appropriate, modelled as part of the analysis?
- Were opportunities for recovery considered and, if appropriate, captured in the scenario modelling?
- Where a decision was taken to screen out HEPs (on the basis of a low impact on the scenario), or to use HPLVs, were common cause failure and dependency issues considered?

4.2.5 Step 5: Human failure quantification

Once the scenario has been modelled, then the individual identified failures can be quantified. Section 2.2 introduced some of the principal quantification techniques and section 3.5 outlined some practical issues with their application. Many HRA techniques provide tables of base HEPs that are then modified to take account of relevant PIFs (examples of this process are shown in Annex B).

Potential pitfalls – Taking HEPs in isolation from databases or tables

Any HEP is a function of the specific operating environment under consideration. Therefore, taking an HEP from database or table without considering its applicability to the situation in question can lead to unrealistic results (see section 3.5.3).

Following the Buncefield accident, the HSE commissioned HSL to review a number of LOPA analyses (HSE RR716). A recurring issue in the 15 LOPA studies they reviewed was the use of HEPs, taken from tables (e.g. IEC 61511-3, Table F.3), without any justification for their use in the specific operating context under consideration. Therefore, a minimum requirement for any HRA using sources of data is a demonstration that the data are applicable to the task under consideration and that relevant PIFs have been reviewed.

A related issue is the use of HEP data in a LOPA analysis without adjusting for task frequency. This is important as the HEP will invariably be much lower than the figure adjusted for task frequency.

Checklist – human failure quantification:

- Were steps taken to ensure that the HEPs used were appropriate to the scenario under consideration (i.e. drawn from a similar industry and driven by the same PIFs)?
- Were the HEPs modified to take account of differences in the relevant PIFs between the source context and the area of application?
- Are all assumptions related to quantification clearly stated and justified?
- Did the analysis appear to avoid the pitfall of being unnecessarily shaped by the limitations of the HRA technique being used (e.g. focusing excessively on the available failure probabilities and PIFs supplied by the technique, when other issues not covered by the technique appear to be more important)?

4.2.6 Step 6: Impact assessment

The modelling and quantification stages should enable the overall system risk to be calculated. The next question to be answered is whether this level of risk is acceptable. This is a complex area and a detailed discussion is outside the scope of this publication. HSE *Reducing risks, protecting people* sets out the GB HSE's position on this topic; other risk impacts should be considered (e.g. on the environment).

As part of this assessment, consideration should be given to the aspects of the system that make the greatest contribution to risk. For example, human, hardware or software aspects will all contribute to the overall risk. The analysis team should decide which aspects of the system need to be addressed in order to bring the overall risk within acceptable levels. Failures that are felt to make a significant contribution to overall risk may need to be subjected to failure reduction interventions.

Potential pitfalls – Arguing for a reduced HRA requirement based on limited impact of human actions

It is possible to argue that a detailed HRA is unnecessary where conservative screening values indicate a low contribution of human action to overall risk. However, this approach requires confidence that all important failures and possible dependencies have been identified (HSE *Human reliability analysis*).

Checklist – Step 6: Impact assessment

- Have HEPs with the greatest impact on the outcome of concern been identified?
- Has the sensitivity of the HRA results to uncertainties in the data and assumptions been discussed in the analysis narrative?
- Have actions that have been identified as having a significant impact been subject to a review to identify any dependency issues?

4.2.7 Step 7: Failure reduction

There are a number of ways in which failure reduction can be addressed. However, if the HRA process has identified failures that make a significant contribution to the overall risk, then this should always prompt the analysis team to consider whether the task design is adequate, or whether other controls should be implemented.

The first approach, although this is often difficult to achieve in older facilities, should always be to consider whether the hazard can be removed. If this is not feasible, the second type of approach is to try and eliminate the possibility of the failure occurring in the first place. This may be achieved, for example, through the use of interlocks. Care should be taken, however, to ensure that these systems do not make carrying out the task too difficult, as this may increase the probability of non-compliances where safeguards are over-ridden because they conflict with ease of use or interfere with production.

The third approach is to attempt to increase the probability of the failure being recovered before the consequences are realised. This might be achieved by the addition of checks or better feedback. However, if checks are considered, issues of dependency should be addressed (see potential pitfalls, below).

Potential pitfalls – Failure to ensure the independence of proposed checks

In a batch process, where chemicals were charged manually, checks were introduced as a way of facilitating failure recovery when incorrect chemicals were selected for charging. The intention was that the checks should be performed by two separate individuals to provide an independent verification of the chemical identity. The procedure stated that the checks should be performed by two operators. However, the operating team had interpreted this to mean that the checks should be performed by two operators working as a team. In practice, this meant that one person checked the identity whilst the second person filled out the checklist. Both operators signed to say the material had been checked but, in effect, only one check had been performed.

The fourth approach is to optimise the PIFs that influence the failure probability. For example, if, during the human failure quantification step, poor labelling was identified as a significant factor affecting task performance, then better labelling might be introduced. When changes in the PIFs are contemplated, the costs of alternative interventions and the possibility of importing risks into the task by not considering the side effects of interventions should be considered. Some more sophisticated HRA quantification tools allow cost functions to be included in the analysis to guide the analyst in selecting the interventions that will produce the greatest reduction in HEPs for the minimum costs.

Checklist – Step 7: Failure reduction

- Have failures that make an unacceptable or dominant contribution to overall risk been identified?
- Has the full hierarchy of control, including the possibility of removing the hazard, been reviewed when failure reduction measures were considered?
- Has the relative impact of different proposed intervention strategies on the HEP been assessed?
- Is there a management process in place to ensure that failure reduction measures will be implemented?
- Where checks have been proposed as measures to enhance the probability of recovery, have dependence issues been addressed (e.g. dependence between task performer and checker or between two checkers)?
- Have proposed failure reduction measures been subject to a human factors review to reduce the possibility of the introduction of new risks?

4.2.8 Step 8: Review

Once the analysis is complete, and identified actions undertaken, a review process should be established. There are two main purposes of this review. Firstly, it should ensure that any changes arising from the review are having the intended effect. Secondly, it should ensure that any important assumptions made during the analysis remain true. For example, the achieved HEP may depend on maintaining a certain level of staffing at all times, or on limiting time pressure. Changing operational practices could have a detrimental impact upon the continuing validity of such assumptions.

Checklist – Step 8: Review

- Is there a review process in place to ensure that changes arising from the HRA are having the desired impact?
- Is there a process in place to ensure that assumptions made during the analysis remain true for the life of the system?

ANNEX A
CHECKLISTS

This Annex includes three checklists that summarise some of the main points to consider when undertaking an HRA analysis:

- Checklist 1: Deciding whether to undertake HRA.
- Checklist 2: Preparing to undertake HRA.
- Checklist 3: Reviewing HRA outputs.

Using these checklists should help to ensure that the HRAs are only performed where necessary, and that, when they are carried out, they are as robust as possible.

Checklist 1: Deciding whether to undertake HRA	Section	Yes/No
1.1 Is there a compelling reason for choosing a quantitative, rather than qualitative, analysis?	Step 1 – Preparation & problem definition	
1.2 Is it clear what value a quantitative analysis adds over a qualitative analysis?	Step 1 – Preparation & problem definition	

Checklist 2: Preparing to undertake HRA	**Section**	**Yes/No**
2.1 Does the analysis team have at least one individual with an understanding of human factors issues?	Section 3.6 - competence requirements	
2.2 Does the analysis team have at least one individual with experience in the application of HRA techniques?	Step 3.6 – competence requirements	
2.3 Does the analysis team have at least one individual with experience of operational practices and the operating environment (for an existing installation)?	Step 3.6 – competence requirements	
2.4 Does the analysis team have at least one individual with an understanding of the process system design and behaviour?	Step 3.6 – competence requirements	
2.5 Are the terms and scope of the analysis clearly specified?	Step 1 – Preparation & problem definition	
2.6 If part of a PSA, has the interface with the PSA study been defined (e.g. the outputs required of the HRA by the PSA study, the scope of the HRA)?	Step 1 – Preparation & problem definition	
2.7 If relevant, will the impact of human reliability on different aspects of the scenario be considered (e.g. maintenance failures that affect layers of protection, failures that initiate event sequences, failures with the potential to make developing situations worse, and failures in recovery)?	Step 1 – Preparation & problem definition	
2.8 If available, have relevant previous incidents or studies been identified for reference?	Step 1 – Preparation & problem definition	
2.9 Have relevant input documents been identified and obtained (e.g. procedures, P&IDs, vendors' instructions)?	Step 1 – Preparation & problem definition	
2.10 Has the analyst specified the HRA technique(s) they intend to use and explained why they feel those techniques are appropriate?	Step 1 – Preparation & problem definition	
2.11 Is HRA a dominant variable in overall risk?	Step 1 – Preparation & problem definition	

Checklist 3: Reviewing HRA outputs	Section	Yes/No
3.1 Was a task analysis developed?	Step 2 - Task analysis	
3.2 Did the development of the task analysis involve task experts (i.e. people with experience of the task)?	Step 2 - Task analysis	
3.3 Did the task analysis involve a walkthrough of the operating environment?	Step 2 - Task analysis	
3.4 Is there a record of the inputs to the task analysis (e.g. operator experience, operating instructions, P&IDs, work control documentation)?	Step 2 - Task analysis	
3.5 Was a formal identification process used to identify all important failures?	Step 3 - Failure identification	
3.6 Does the analysis represent all obvious errors in the scenario, or explain why the analysis has been limited to a sub-set of possible failures?	Step 3 - Failure identification	
3.7 Was there consideration of possible underlying reasons for the identified failures?	Step 3 - Failure identification	
3.8 If the HRA was part of a broader risk assessment, were the identified human failures modelled alongside other types of failure (e.g. hardware and software) to determine the overall system risk?	Step 4 - Modelling	
3.9 If several failures were identified as potentially relevant to the overall risk analysis, were these screened to determine which failures required the most detailed analysis?	Step 4 - Modelling	
3.10 Were dependencies considered and, if appropriate, modelled as part of the analysis?	Step 4 - Modelling	
3.11 Were opportunities for recovery considered and, if appropriate, captured in the scenario representation?	Step 4 - Representation	
3.12 Where a decision was taken to screen out HEPs (on the basis of a low impact on the scenario), or to use HPLVs, were common cause failure and dependency issues considered?	Step 4 - Modelling	
3.13 Were steps taken to ensure that the HEPs used were appropriate to the scenario under consideration (i.e. drawn from a similar industry and driven by the same PIFs)?	Step 5 - Quantification	
3.14 Were the HEPs modified to take account of differences in the relevant PIFs between the source context and the area of application?	Step 5 - Quantification	
3.15 Are all assumptions related to quantification clearly stated and justified?	Step 5 - Quantification	

Checklist 3: Reviewing HRA outputs (continued)	Section	Yes/No
3.16 Did the analysis appear to avoid the pitfall of being unnecessarily shaped by the limitations of the HRA technique being used (e.g. focusing excessively on the available failure probabilities and PIFs supplied by the technique, when other issues not covered by the technique appear to be more important)?	Step 5 - Quantification	
3.17 Have HEPs with the greatest impact on the outcome of concern been identified?	Step 6 - Impact assessment	
3.18 Has the sensitivity of the results of the HRA to uncertainties in the data and assumptions been discussed in the analysis narrative?	Step 6 - Impact assessment	
3.19 Have actions that have been identified as having a significant impact been subject to a review to identify any dependency issues?	Step 6 - Impact assessment	
3.20 Have failures that make an unacceptable or dominant contribution to overall risk been identified?	Step 7 - Failure reduction	
3.21 Has the hierarchy of control, including the possibility of removing the hazard, been reviewed when error reduction measures were considered?	Step 7 - Failure reduction	
3.22 Has the relative impact of different proposed intervention strategies on the HEP been assessed?	Step 7 - Error reduction	
3.23 Is there a management process in place to ensure that error reduction measures will be implemented?	Step 7 - Failure reduction	
3.24 Where checks have been proposed as measures to enhance the probability of recovery, have dependence issues been addressed (e.g. dependence between task performer and checker or between two checkers)?	Step 7 - Failure reduction	
3.25 Have proposed error reduction measures been subject to a human factors review to reduce the possibility of the introduction of new risks?	Step 7 - Failure reduction	
3.26 Is there a review process in place to ensure that changes arising from the HRA are having the desired impact?	Step 8 - Review	
3.27 Is there a process in place to ensure that assumptions made during the analysis remain true for the life of the system?	Step 8 - Review	

ANNEX B ILLUSTRATIVE EXAMPLES

The primary purpose of this publication is to equip organisations that are thinking of undertaking, or commissioning, HRAs with an overview of practical considerations, with the aim of reducing the instances of poorly conceived or executed analyses. The following sections include outlines of two illustrative HRA examples developed in response to specific requests. References to more detailed descriptions of these methods used, and others, are provided in Annex D. These analyses are supplemented by commentaries identifying strengths and weaknesses of the analyses, linked to the issues raised in the publication.

Two examples are provided: a scenario where a failure could initiate an event sequence, and a post-fault scenario, where an operating team needs to respond to an incident. These are typical of the types of situations for which HRA studies are often commissioned. For the reader's convenience, the analysis report has been organised according to the generic eight-stage HRA process outlined in section 4.1. The comments in the accompanying commentary have been cross-referenced with the checklists provided in Annex A. Comments are provided for every stage of the process, with the exception of Step 8, which addresses issues related to the review of outputs.

Note: These examples should not be used as templates for real-world analyses. The examples, whilst based on real scenarios, are designed to illustrate practical issues in the application of HRA and, consequently, contain intentional flaws and inaccuracies.

B.1 POST-FAULT EXAMPLE[4]

The following example details an HRA performed by an external consultant at the request of an installation manager.

B.1.1 Step 1: Preparation and problem definition

A process hazard analysis (PHA) has identified the potential for an operator failure causing a rupture of a propane condenser and a serious incident. The manager of the area has commissioned this HRA study to estimate the likelihood of the condenser rupturing as the result of such a failure, and to identify ways to reduce the expected frequency of such ruptures.

System description:

The system has four parallel propane condensers that have a 450 psig shell pressure rating and a 125 psig tube pressure rating. The propane vapour pressure is controlled at 400 psig; the cooling water flowing through the condenser tubes is normally maintained at 75 psig. Liquid propane flows out of the condenser as soon as it condenses; there is no significant inventory of liquid propane in the condenser. The two propane isolation valves for each condenser are rising-stem gate valves with no labels. The two water isolation valves for each condenser are butterfly valves with no labels. Their hand-wheel actuators have position indicators.

[4] This scenario was originally presented in ACC *A manager's guide to reducing human errors*; however, this example has been revised to show some potential issues with the application of HRA techniques.

> On average, a tube has failed in one of the four condensers about once every three years. If a condenser tube fails, the affected condenser can be removed from service by closing four isolation valves: the propane vapour inlet valve (PIV), liquid propane outlet valve (POV), cooling water supply valve, and cooling water return valve. However, if a tube fails, it is essential that the operator closes the two propane isolation valves before closing the two water isolation valves (this was the particular failure identified in the PHA). Closing the two water valves first allows pressure to build on the tube side of the condenser, resulting in a rupture of the tube head.

The specification for the HRA also stated that:

- It can be assumed that the field operator (FO) has already correctly identified the propane condenser with the failed tube.
- There is a checklist procedure for the task, available in the control room, describing the steps the field operator should carry out.

Commentary:

- Whilst the system is described clearly, there is no description here of the team that undertook the analysis or the inputs to the analysis process (e.g. versions of procedures and P&IDs used). ***Checklist reference 2.1-2.4 & 2.9***.

B.1.2 Step 2: Task analysis

A simple HTA for the task in question was developed with the input of an experienced operator and by visiting the task location (see Table B1).

Table B1 HTA for tube rupture response task

No.	Description	Who	Notes
Pre-conditions:	Low de-propaniser pressure alarm sounding in the control room	N/A	
Plan 0	Do in sequence		These steps were not within the scope of the analysis.
1	Identify low pressure alarm	CRO	
2	Recognise cause of low pressure alarm	CRO	
3	Ask FO to isolate failed condenser	CRO	
4	Identify failed condenser	FO	
5	Isolate failed condenser	FO	Propane valves should be closed before the water valves to prevent pressure build-up on the tube side of the condenser.
Plan 5	Do in sequence		
5.1	Close PIV	FO	All valves are closed by hand. The propane isolation valves are unlabelled rising stem gate valves.
5.2	Close POV	FO	
5.3	Close cooling water supply valve	FO	The water isolation valves are unlabelled butterfly valves.
5.4	Close cooling water return valve	FO	

Commentary:

- The HTA indicates that there are number of other elements of the task that could make a significant contribution to the overall failure probability. For example, there could be failures during the identification and interpretation of the alarm, in the process of communication between the control room operator (CRO) and FO, or when the FO identifies the condenser. Whilst the problem definition states that these issues are outside the scope of the analysis, they clearly could have an impact on probability of successfully completing the task. Therefore, the analyst should raise this point with the commissioning manager at an early stage to discuss their potential inclusion. ***Checklist reference 2.7***.
- The involvement of an experienced operator and a walkthrough of the operating area help the analyst to gain an appreciation of the issues faced by the FO when responding to this event. ***Checklist reference 3.2 & 3.3.***

B.1.3 Step 3: Human failure identification

Using the task analysis as an input the main failures related to the isolation action (Step 5 in the HTA) were identified (see Table B2). In addition, PSFs relevant to the identified failures were captured when raised by the workshop team.

Table B2 Main failures identified for isolation step of task

No.	Step	Identified failures	Description	PSFs
5	Isolate failed condenser (FO)	Operation in wrong order	Close water valves before propane valves - pressure build-up on tube side of condenser - possible rupture and LOC	- VE time pressure: FO will be aware that isolation must happen quickly to avert requirement for unit shutdown. - VE stress: Possibility of visible propane vapour cloud likely to increase the stress on the FO. - VE procedures: There is a checklist procedure available for this task. However, operator feedback was that this would be unlikely to be used because of time pressure to respond quickly. +VE valve design: Valve has a rising steam design which clearly indicates the valve position. -VE valve labelling: The different isolation valves have no labels.
		Operation incomplete	Fail to fully close either propane valve (and then close water valves) - pressure build-up on tube side of condenser - possible rupture and LOC	

Commentary:

- The process description does not discuss whether formal checklists for failure types and PIFs were used by the analysis team. ***Checklist reference 3.5***.
- The analyst has taken care to undertake a qualitative review to identify credible failures. However, there are a number of other obvious failures that are not described in this output. For example, the analysis does not pursue the possibility of the FO closing only one of the two propane isolation valves, before moving on to close the water isolation valves. It is possible that the analysis team considered this event but decided not to document it (e.g. because the consequences were less severe than for the documented failures). However, for a detailed analysis of a simple task it is useful to document all credible failures and then indicate those that have been discounted from further consideration. This gives the reader greater confidence that the analysis is comprehensive. ***Checklist reference 3.6.***
- Another possibility is that the analyst felt that the failure to close both propane isolation valves was addressed by the overall failure to close the propane valves before the water valves. However, there may be different reasons for these failures, meaning that they should be considered separately. For example, closing the water isolation valves first may be a mistake resulting from a lack of understanding of the system, whereas closing only one propane isolation valve may be the result of a lapse, where the stress of the situation results in the inadvertent omission of a step. The remedial measures that would be proposed to reduce the failure probability to an acceptable level might differ in these two cases. Since one of the objectives of human reliability analyses is to determine how to achieve particular risk target levels,

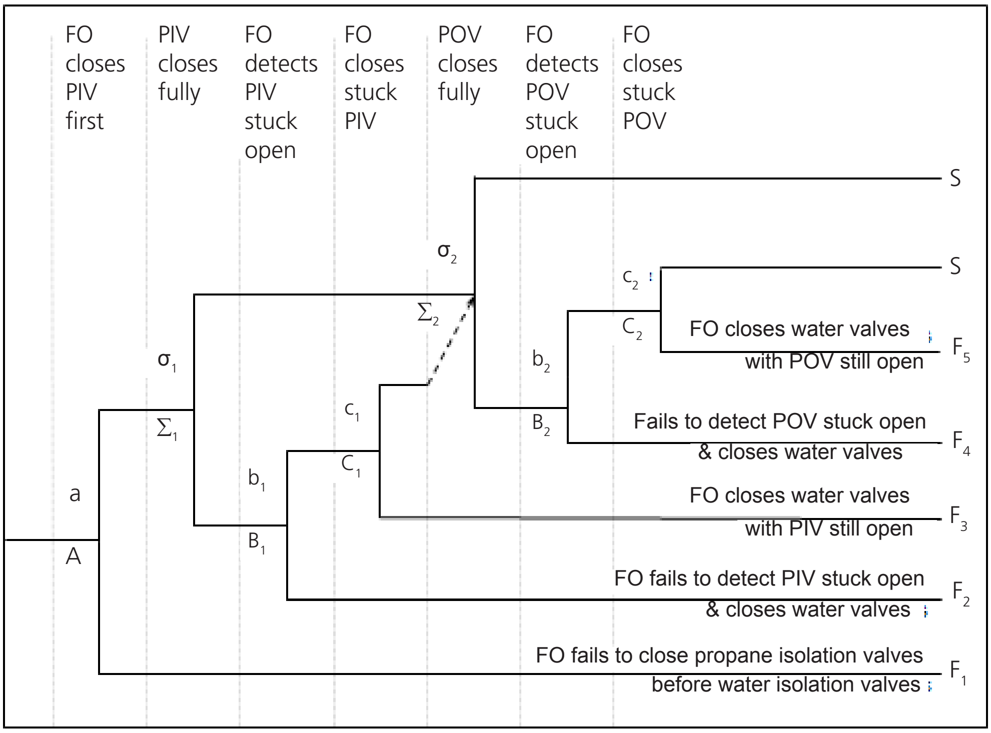
the nature of failures (i.e. slips, lapses, mistakes or non-compliances (see Annex C.3)) should be identified so that appropriate remedial measures can be specified. ***Checklist reference 3.7***.

– It is clear, even before the quantification process has been undertaken, that the most important failure is closing the water isolation valves before the propane isolation valves. The analyst should consider discussing this finding with the commissioning manager before proceeding with the analysis. It is possible that this may provide sufficient information for the manager to address the risks associated with the task, without undertaking a more detailed analysis. ***Checklist reference 3.9***.

B.1.4 Step 4: Human failure modelling

Using the task analysis and the outputs of the failure identification exercise, an HRA event tree was developed, as shown in Figure B1. The event tree follows the THERP convention of using Greek letters to indicate potential equipment failures and English letters to indicate potential human failures. In addition, upper case letters are used to indicate failure and lower case success. The event tree illustrates another convention that is sometimes used, which is to represent a recovery (either of a hardware failure or a previous human failure) as a re-entrant branch of the tree, where the path following a recovery rejoins the path that would have been traversed if the failure had not occurred. This is represented by the dotted arrow in the event tree.

Figure B1 HRA event tree for response to condenser tube rupture


FO closes PIV first
PIV closes fully
FO detects PIV stuck open
FO closes stuck PIV
POV closes fully
FO detects POV stuck open
FO closes stuck POV
S
σ_2
S
c_2
Σ_2
C_2
FO closes water valves with POV still open
F_5
σ_1
b_2
c_1
B_2
Fails to detect POV stuck open & closes water valves
F_4
Σ_1
C_1
b_1
a
FO closes water valves with PIV still open
F_3
A
B_1
FO fails to detect PIV stuck open & closes water valves
F_2
FO fails to close propane isolation valves before water isolation valves
F_1

Notes:

1 S = success, F = failure

Commentary:

- The modelling of the event sequence does not fully address the options that are available to the FO in the event of the valve sticking open. If the valve is identified as stuck open, the FO can try and close the valve manually and, if this fails, either decide to close water isolation valves anyway, or shut down the system. More fundamentally, the analysis does not address the failure identified in Step 3, where the operator closes the PIV but then fails to close the POV (the assumption in the event tree is that the operator will always try to close the second valve having closed the first valve, but this is by no means certain). These choices and actions do not appear to be fully modelled in the event tree. Consequently, the event sequence modelling is incomplete and may have a significant impact on the overall analysis. This also illustrates the importance of a robust qualitative analysis ***Checklist reference 3.6***
- There is no discussion in the analysis narrative about opportunities for recovery during the event sequence. For example, one might assume from the analysis that closing the water isolation valves before the propane isolation valves would result in immediate over-pressurisation of the system. In fact some time might elapse before this outcome was realised, which might provide an opportunity for the operator to recognise the failure and reverse the action. ***Checklist reference 3.11***.
- Occasionally there is a danger of an analyst allowing the HRA technique to shape the analysis. For example, in this analysis, THERP data are available on the probability of failing to identify stuck open valves, and this is modelled in the analysis. However, there are more important failures, such as recognising that the valve has stuck open but deciding to proceed with closing the water valves anyway, that are not modelled in the analysis. The decision not to include this failure mode might have been influenced by the fact that THERP does not provide an explicit HEP for decision failures of this type. ***Checklist reference 3.16***.

B.1.5 Step 5: Human failure quantification

Having identified the failures of concern, these were then quantified using THERP. This technique was selected as the analyst has extensive experience in its application. The following table shows the failure probabilities obtained using the THERP technique.

Table B3 Quantification of events in HRA event tree

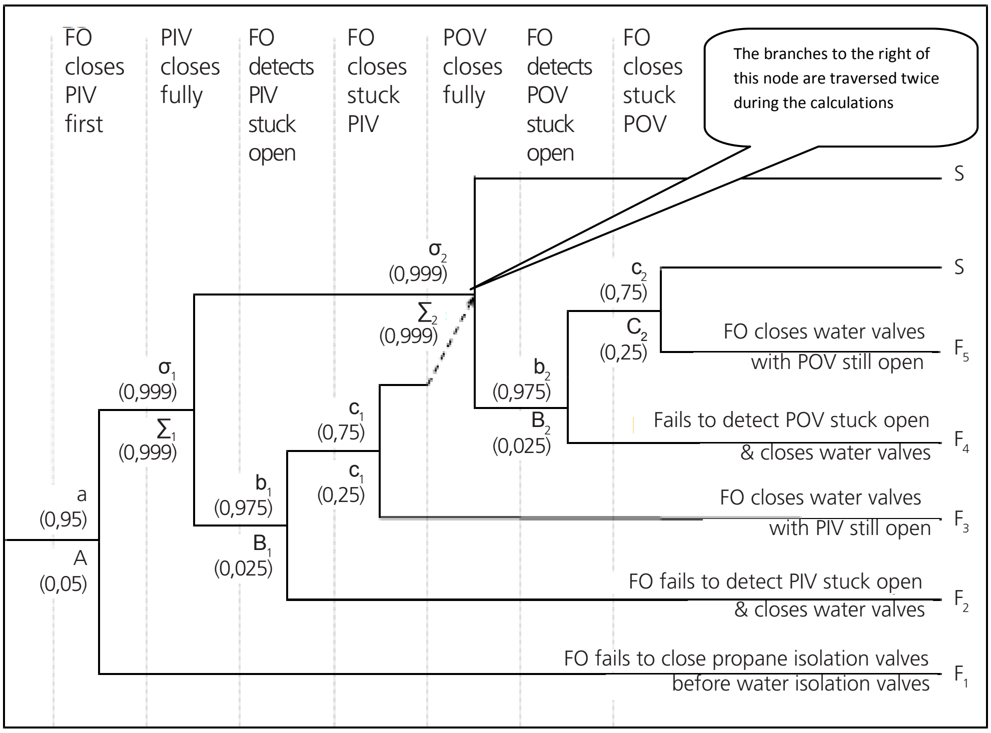
Failure symbol	Failure description	Estimated probability	Data source (THERP) (Note 1)	Notes
A	FO fails to close propane isolation valves first	0,05	T20-7 #5 footnote x5, per T20-16 #6a	An error of omission when use of procedures is specified but they are not used (modified to take account of the effects of stress),
Σ_1	PIV fails to close	0,001	T20-14 footnote	Probability of a valve of this type sticking open,
Σ_2	POV fails to close	0,001	T20-14 footnote	See Σ_1
B_1	FO fails to detect PIV stuck open	0,025	T20-14 #3 x5, per T20-16 #6a	Failure to detect rising stem valve,with no position indication, stuck open (modified to take account of effects of stress)
B_2	FO fails to close stuck PIV	0,025	T20-14 #3 x 5, per T20-16 #6a	See B_1
C_1	FO fails to close stuck PIV	0,25	T20-16 #7a	Dynamic task carried out under stressful conditions
C_2	FO fails to close stuck POV	0,25	T20-16 #7a	See C_1

Notes:

1. Data from USNRC NUREG/CR-1278.
2. THERP uses the same approach as many HRA techniques, where a base HEP is modified to take account of contextual factors (PIFs/PSFs). This column lists the source table in the THERP handbook of the HEP (i.e. T20-7 #5 footnote) as well as any modifications to take account of PSFs. In this case the base HEP is multiplied by 5 to take account of the stressful nature of the situation (as per tab T20-16 #6a in the THERP handbook).

The failure probabilities from the THERP database were then used to populate the event tree.

Figure B2 Quantified HRA event tree for response to tube rupture


FO closes PIV first
PIV closes fully
FO detects PIV stuck open
FO closes stuck PIV
POV closes fully
FO detects POV stuck open
FO closes stuck POV
The branches to the right of this node are traversed twice during the calculations
a (0,95)
A (0,05)
σ1 (0,999)
Σ1 (0,999)
b1 (0,975)
B1 (0,025)
c1 (0,75)
c1 (0,25)
σ2 (0,999)
Σ2 (0,999)
b2 (0,975)
B2 (0,025)
c2 (0,75)
C2 (0,25)
S
S
FO closes water valves with POV still open
F5
Fails to detect POV stuck open & closes water valves
F4
FO closes water valves with PIV still open
F3
FO fails to detect PIV stuck open & closes water valves
F2
FO fails to close propane isolation valves before water isolation valves
F1

Notes:

1 S = success, F = failure

The event tree was then used to calculate an overall failure probability. The calculation of the probabilities for the various success and failure outcomes, to the right of the event tree is derived by multiplying the probabilities along the paths via which these outcomes are reached. This should take into account both the recovery path and the path that would have been traversed had the recovered failure (C) not occurred. Thus, the branch of the event tree to the right of the dotted arrow head has to be included twice in the calculations. This is taken into account in the calculations set out in Table B4.

Table B4 Results of HRA quantification

$F_1 = A$	5,0E-2
$F_2 = a\Sigma_1 B_1$	2,4E-5
$F_3 = a\Sigma_1 b_1 C_1$	2,4E-4
$F_4 = a(\sigma_1+\Sigma_1 b_1 c_1)\Sigma_2 B_2$	2,4E-5
$F_5 = a(\sigma_1+\Sigma_1 b_1 c_1)\Sigma_2 b_2 C_2$	2,3E-4
$F_T = F_1 +\ldots+ F_5 = 0,05$	

Commentary:

- The report does not contain any real discussion or justification as to why THERP has been selected as the most appropriate technique for this analysis. In particular, there is no comment on its relevance to the scenario in question in terms of the sources of data in THERP (e.g. was the data obtained in similar industrial setting? Was there reference to the THERP explanatory chapters?). ***Checklist reference 2.10.***
- The issue of dependence is not discussed at all in the analysis. There is no indication that the analyst has considered whether dependence is an issue, and no attempt to use the dependence modelling facility within THERP to address any identified issues. ***Checklist reference 3.10.***
- The specific THERP table that the failure probability for 'closing the water isolation valves before the propane isolation valves' is taken from is for 'errors of omission when use of procedures is specified but they are not used'. This implies that the use of procedure is appropriate for this task. However, as the FO is likely to be away from the control room, and given the inherent time pressure of the task, it is unlikely that an FO would return to the control room to obtain the procedure before undertaking the task. Therefore, when undertaking an HRA the analysis team should always be careful to question the underlying task assumptions. In this case, for example, the best way of supporting performance may be a local sign warning of the importance of sequence when closing the valves. ***Checklist reference 3.16***.
- The use of THERP enables the analyst some limited modification of the base HEPs based on the prevailing PIFs. In this analysis, the primary PIF that is assessed is stress. However, the qualitative analysis identified the absence of valve labelling as a particular issue, a factor that is likely to have an impact on the probability of closing the water valves first, and yet it is not modelled in the analysis. This can sometimes be an issue with the application of HRA techniques; important PIFs for which the technique has no data may not be modelled, whereas less important issues, for which data exist, may be included. ***Checklist reference 3.16***.

B.1.6 Step 6: Impact assessment

Inspection of the HRA tree (Figure B2) indicates that the dominant human failure (i.e. the one with greatest impact on the overall failure probability) is the first failure (A), where the FO fails to isolate the propane valves before the water valves. If it is not possible to remove the hazard, then steps should be taken to minimise the probability of this failure.

As the frequency of condenser tube ruptures, for all four condensers, is known to be approximately once every three years, then the expected frequency of incorrect isolation of a failed condenser, leading to a condenser rupture, can be calculated as shown in Table B5:

Table B5 Frequency of condenser ruptures

Probability of incorrect isolation (from THERP)	0,05 x
Frequency of tube ruptures (from data)	0,33/year
= Frequency of condenser ruptures	= 0,017/year (or approximately about once every 60 years)

Commentary:

- Since no specific target frequency had been specified in the project brief, this information can be fed back to the commissioning manager to determine whether the calculated frequency is acceptable. Even if it is within an acceptable range, there are a number of specific failure reduction steps that could be taken to further improve the system (see B1.7).
- The output does not provide any indication of the range of possible outputs that might be possible depending on uncertainties in the data. Some HRA techniques allow the analyst to indicate ranges within which the HEP may fall, rather than give a specific value. ***Checklist reference 3.18.***

B.1.7 Step 7: Failure reduction

There are a number of possible actions that might be taken in order to reduce the frequency of condenser failures arising from incorrect isolation. The first approach should be to consider whether the hazard could be removed, or additional technical controls put in place (e.g. pressure relief system, automatic system shutdown in the event of tube rupture). Such considerations are best left to the PHA team.

If these types of interventions prove impractical, then other possible interventions might include:

- Improved labelling of the valves to support identification of propane and water isolation valves.
- A locally maintained job-aid to support the FO in selecting the correct valves under time pressure.
- Refresher training to ensure that the operating team understand the importance of closing the valves in the correct sequence.
- An improved maintenance regime to reduce the probability of valves sticking in the open position.

Commentary:

- Whilst a range of possible interventions are suggested, the output does not stress the importance of prioritising interventions towards the top of the hierarchy of control. This is particularly important for a task such as this, where the possibility of human failure under time pressure resulting in a serious outcome will remain, even with the proposed interventions. ***Checklist reference 3.21.***
- No attempt is made to indicate the relative impact of making the suggested improvements upon the overall frequency of failure. Such information could assist the commissioning manager in making cost-benefit decisions related to possible interventions. THERP does not provide particular support for this issue, whereas other techniques such as HEART, and in particular, the Success Likelihood Index Method (SLIM), do. ***Checklist reference 3.22.***

B.2 INITIATION EXAMPLE

The following example details an HRA performed by an external consultant at the request of an installation manager following a near-miss.

B.2.1 Step 1: Preparation and problem definition

This HRA review has been developed in response to a request from the installation manager following a near miss at the rail loading area. The specific request was to undertake an HRA to determine the likelihood of a LOC arising from a drive-away incident at a railcar loading bay.

System description:

> The loading bay is a top-loading facility, with three loading arms arranged on a gantry. The loading arms can be used to transfer diesel and petrol, depending on the requirements for the specific train being loaded.
>
> There are three operators working in the loading area. Typically, loading takes place three days per week, with trains, of up to 12 railcars in length, leaving once per day on loading days. During loading, two of the operators work in the rail loading area, whilst the third undertakes other duties. One of the operators manages the loading gantry, whilst the other takes responsibility for shunting the railcars into position. The gantry operator talks to the shunter via radio, to move the railcars into the correct position under the loading arm, and to advise the shunter when loading is complete. Each railcar takes approximately 20 minutes to load.

One of the issues identified in the near-miss review was that the task relies heavily upon the quality of communication between the gantry operator and the shunter. As the shunter driver cannot see the position of the loading arms, the gantry operator must advise the shunter via radio when the loading arms are clear of the railcars. Following the incident, the installation is considering fitting in-cab closed-circuit television (CCTV) to help the shunter to establish when loading arms are clear of the railcars. Therefore, this analysis will consider the possible impact of this proposed change on the frequency of such incidents.

Commentary:

– The request is for a very specific review of a particular type of failure. It would be possible to extend this analysis to examine the overall risk of LOC in this area. If this were the case, the analyst would also need to consider other types of failure such as overfilling the railcars. ***Checklist reference 2.7***

B.2.2 Step 2: Task analysis

The analyst spent half-a-day observing the loading operation and speaking to operators. The main stages of the loading process, based on the procedure and task observation, are:

- Shunter checks condition of railcars to be loaded.
- Shunter (with direction from loader) moves railcar into position and applies brakes.
- Gantry operator removes inspection cover from railcar and inserts loading arm.
- Gantry operator opens isolation valve on loading arm and starts the transfer.
- When loading is complete, gantry operator closes the isolation valve on the loading arm, removes loading arm and replaces inspection chamber cover.
- Gantry operator advises shunter, via radio, that loading is complete.
- Shunter disengages brakes and pushes railcars clear of gantry. (N.B. there is space for up to ten railcars to be positioned for loading at any one time. Therefore, the 10 railcars will be filled sequentially until all are full.)

Notes:

1. Whilst the procedure suggests that the railcars should be loaded one at a time, the configuration of the loading bay means that up to three railcars can be loaded simultaneously. In practice, this means that the gantry operator will insert three loading arms in three railcars, and then start the loading processes in parallel. This has significant time advantages for the loading team.
2. The shunter cannot see the position of the loading arms from the cab.
3. The shunter tends to stay in the vicinity of the cab for the duration of loading operation.
4. There is no training in radio communication and each pair of shunters/gantry loaders have their own ways of communicating with each other.

Commentary:

- The analyst has chosen not to develop a full task analysis for this review. Given that the failure of concern is very specific, this is a reasonable approach. However, the analyst has still made sure to undertake a walkthrough of the loading area task and has identified some important issues (e.g. the inability of the shunter to see the position of the loading arms). This illustrates that, even with a narrow band of inquiry, it is always worth spending time on the qualitative parts of an HRA review. ***Checklist reference 3.1***

B.2.3 Step 3: Human failure identification

The brief for this review is to examine the possibility of a LOC arising from a shunting movement whilst a loading arm is in place in a railcar. There are two main ways in which the railcar could move whilst a loading arm is in place. The shunter could omit to apply the railcar brakes or the shunter could move the railcar in the belief that the loading arm(s) are clear of the railcars.

The former failure is not felt to pose a significant risk; as the track in the vicinity of the loading area is very flat, the railcars are unlikely to move without some additional force being applied. Moreover, the railcars need to be stationary to allow the loading arm to be inserted, and it appears, following discussion with the loading team, that the only way that this can be achieved is by the application of the handbrake.

The focus of this analysis therefore is on the possibility of a shunter moving the railcars in the belief that the loading arm has been removed.

Commentary:

- The analyst has chosen to describe the failures of concern for this specific task informally rather than apply a systematic failure identification technique. Given the limited scope of the analysis this is a reasonable approach. ***Checklist reference 3.6***
- However, whilst the outcome of concern seems straightforward (i.e. that the shunter moves the railcars before the loading arm(s) is removed), there is no discussion of exactly how this situation might arise. For example, the movement might be a result of the shunter mishearing a communication from the gantry operator. ***Checklist reference 3.7***

B.2.4 Step 4: Human failure modelling

Commentary:

- As the brief for the analysis focuses on a very specific failure, there is no requirement for the analyst to model the event sequence. However, for this type of scenario, it may also have been useful for the analyst to discuss whether there are any hardware issues with the potential to affect the outcome. For example, the probability of the worst case outcome may be a function of both the human failure (i.e. moving the railcar before the arm is moved) and the design of the system (e.g. the loading arm may be designed to breakaway when moved, to prevent LOC). If this was the case then this could be modelled (e.g. in a fault tree).

B.2.5 Step 5: Human failure quantification

The HEP for this failure was derived using HEART technique (Williams (1986)).

The first part of the HEART process is to select the generic task type that best suits the task under consideration. In this case the closest match was found with Type G (see Table B6).

Table B6 Generic task type as defined in HEART

HEART element	Features of failure 'moving railcars with loading arm still in place'
Proposed generic task type	Type G - Completely familiar, well-designed, highly practised, routine task occurring several times per hour, performed to highest possible standards by highly motivated, highly trained and experienced persons, totally aware of the implications of failure, with time to correct potential error, but without benefit of significant job aids – this task is mission oriented and could involve a great many discrete elements or actions, but would normally only involve one basic activity.
Nominal human unreliability for generic task type	0,0004
5th-95th percentile bands	0,00008 - 0,007

Task type G was felt to be the closest match for the shunting task. The only significant discrepancy between the HEART description and the actual task is that there is no time for recovery before the consequences of the failure are realised (i.e. as soon as the railcars moves the loading arm will be damaged).

Relevant associated error producing conditions (EPCs) were then identified and assessed from the list in the HEART handbook. The EPCs selected in this case are shown in Table B7.

Table B7 Identified EPCs for task

EPC	Notes on selection of EPC	Total HEART effect	Assessed proportion of effect	Assessed effect (Note 1)
2. A shortage of time available for error detection and correction	There is no time available in the event to correct the error before the consequences are realised. EPC 7 -'No obvious means of reversing an intended action' was also considered.	x11	0,5	(11,0 - 1) x 0,5 +1 = 6
10. The need to transfer specific knowledge from task to task without loss	Communication between the shunter and gantry operator is of critical importance; this was felt to be the EPC that most closely addressed this issue.	x5.5	0.8	(5,5 - 1) x 0,8+1 = 4,6
21. An incentive to use other more dangerous procedures	The task analysis suggested that operators often load several railcars simultaneously. The procedure suggests that only one should be done at a time.	x2	0,2	(2,0 - 1) x 0,2 +1 = 1,2
36. Task pacing caused by the intervention of others	Time pressure, to get trains ready for departure, was felt to be an important factor. In addition, requests from customers for changes to train configurations can happen at short notice. HEART does not have a direct EPC for time pressure; this was felt to be the closest EPC.	x1,06	0,8	(1,06 - 1) x 0,8 +1 = 1,048

Notes:

1 The subtraction and addition of 1 in the calculation prevents the assessed effect ever being less than 1.

Therefore, the assessed nominal unreliability for this task is:

0,0004 x 6 x 4,6 x 1,2 x 1,048 = 0,01

Commentary:

- There is no discussion as to why the HEART technique has been selected for this particular analysis. ***Checklist reference 2.10***
- The proportion of effect (or 'affect' as it is sometimes called) is the part of the analysis where the analyst uses their expert judgement to determine the influence of the EPCs on the failure probability. The analyst can assess the impact in a range from maximum effect (1,0) to minimum effect (0,1), and this may significantly influence the outcome of the analysis. Here, the analyst has taken care to explain why the specific EPCs have been selected, but there is no similar narrative for the proportion of effect. This leads to questions about why, for example, the analyst has chosen to assess EPC 2 – 'A shortage of time available for error detection and correction' as having a proportion of effect of only 0.5. In this case, the failure results immediately in the unwanted consequence, with no opportunity for recovery. Therefore, it is difficult to see why this factor has not been assessed as having the maximum impact of 1. ***Checklist reference 3***
- One issue with HRA techniques that have a pre-specified list of PIFs (EPCs in this case) is that the specified factors may not map directly onto the situation being investigated. For example, in this case, the analyst states that communication is an important issue and that EPC 10 'The need to transfer specific knowledge from task to task without loss' is the closest factor to addressing this concern with communication. There is always a danger of the analyst selecting PIFs that are available and excluding PIFs that the specific tool does not cover. ***Checklist reference 3.16***
- A related point is that the number of EPCs that the analyst selects can have a significant impact on the analysis output. In this case the analyst has followed HEART guidance in choosing only a small number of EPCs. ***Checklist reference 3.16***
- The analyst has also avoided another potential pitfall with HEART, that of double-counting effects of PIFs. This can happen because the generic task types have PIFs already included within their description. For example Task G, used for this analysis, states that the task is performed 'without the benefit of significant job aids'. Therefore any EPC that was included which referenced the absence of procedures would be superfluous. ***Checklist reference 3.16***
- The output from this analysis suggests that a failure might be expected one in every hundred times that the task is carried out. To the installation manager, this is unlikely to be seen as a credible outcome. This is because there have only been two such incidents in the last five years. Moreover, the manager knows that the task is carried out upwards of 750 times per year, and that the consequences of the failure are difficult to hide. Therefore, he might have expected a result around one or two orders of magnitude less than the analysis suggests. In fact, this is a rare example of a task where data relating to this failure could be said to already exist. Rather than commissioning the HRA study, the manager could instead have reviewed the existing data, decided whether the risk was acceptable, and, if not, directed efforts at reviewing possible improvement measures. ***Checklist reference 1.1 & 1.2***

B.2.6 Step 6: Impact assessment

Whilst the nominal human unreliability for the generic task type used in this analysis is 0,0004, the HEART handbook provides uncertainty bounds for each generic task type. In this case they are 0,00008 – 0,007.

When these bounds are used as the proposed nominal unreliabilities the results are:

Table B8 Uncertainty bounds

5th percentile	0,00008 x 6 x 4,6 x 1,2 x 1,048 = 0,003
95th percentile	0,007 x 6 x 4,6 x 1,2 x 1,048 = 0,2

One train departs the loading area each day: each train is made up of up to 12 railcars. If one assumes that two railcars are loaded simultaneously, this means that there a minimum of six critical shunting movements for a 12 railcar train (i.e. movements following completion of loading of a railcar). As the length of the train varies between eight and 12 railcars, assume five movements per train.

Loading takes place three days per week. Taking this conservative estimate, there are five critical shunting movements per day (that loading takes place) and, consequently, at least 750 critical shunting movements per year. See Table B9.

Table B9 Estimated frequency of shunting movements before arm is released

	Nominal human unreliability	**5th percentile**	**95th percentile**
Probability of shunting movement before loading arm is removed (from HEART) x	0,01 x	0,003 x	0,2 x
Frequency of critical shunting movements (estimated)	750/year	750/year	750/year
= Frequency of shunting movements before loading arm is removed	= 7,5/year	= 2,25/year	= 150/year

Commentary:

- Since HEART is often used to model global analysis of failure probabilities, an event tree, like that used in THERP, is not always developed. In these cases, it is not possible to review the relative importance of the different failures that are subsumed under the global analysis. This may create problems in developing remedial measures. ***Checklist reference 3.17***
- The analyst has supplied a range of possible rates based on the uncertainty bounds supplied in the HEART technique. However, this serves to illustrate the difficulty in using these techniques to make firm decisions about risk. Based on the analysis the range of frequencies one might expect starts at two failures a year and goes all the way up to 150 failures a year. This is a large range, and could be even greater if one starts to manipulate the assessments given for the selected EPCs. The analyst does not mention that seven-and-a-half failures a year could be observed. An effort could be made to compare the HEART output and observed failures. ***Checklist reference 3.18***

B.2.7 Step 7: Failure reduction

The installation is considering fitting in-cab CCTV to assist the shunter in establishing when the loading arm is removed from the railcar. If this is installed and managed correctly, one could anticipate that the proportion of effect of EPC 10 'The need to transfer specific knowledge from task to task without loss' (see Table B7) would be minimised. Table B10 illustrates the possible impact of installing this risk reduction measure.

Table B10 Possible impact of installing CCTV on estimated frequency of shunting movements before arm is released

	Nominal human unreliability	
	Without CCTV **(with EPC 10 proportion of affect rated at existing level of 0,8)**	**With CCTV** **(with EPC 10 proportion of affect rated minimised to 0,1)**
Probability of shunting movement before arm is released (from HEART) x	0,01 x	0,004 x
Frequency of critical shunting movements (estimated)	750/year	750/year
= Frequency of shunting movements before arm is released	= 7,5/year	= 3,3/year

It appears that the installation of CCTV would have a significant impact on the frequency of dangerous shunting movements.

Commentary:

– Whilst the analyst has responded to the brief by assessing the potential impact of the introduction of CCTV, there is no discussion of other potential interventions (or indeed any consideration of the factors involved in the original near miss). For example, in an ideal world, there would be an interlock system preventing shunting movements whilst loading arms are in place. The cost of installing such a system may be prohibitively expensive. However, the potential risk reduction impact of such a system could be assessed and compared with the impact of the CCTV intervention. ***Checklist reference 3.21 & 3.22***

– Similarly, other interventions that may be easier to implement could also be considered. For example, training in radio communication protocols, or minimising management requests for last minute alterations to the train configuration, may all have an impact on the failure probability. ***Checklist reference 3.22***

– Any intervention has the potential to affect the way the task is performed in unanticipated ways, which can potentially increase as well as decrease the risk. For example, if the installation decided to take up the CCTV recommendation, it may be with the intention of supplementing radio communication. However, in practice, operators may use the CCTV in place of the radios. The analysis does not raise this as a potential issue. ***Checklist reference 3.25***

ANNEX C
DEFINING AND CLASSIFYING HUMAN FAILURES

The concept of human error itself is one that has been argued over in the human factors community for many years. Therefore, the attribution of error is as much a social as a technical process. This has implications for the discipline of HRA, which, at heart, treats systems as fundamentally safe, as systems that will only fail when someone does the wrong thing, and errors as products of individuals' weaknesses that need to be identified and eliminated (see, example, Woods et al (2010), for a more detailed discussion).

Current thinking is that there is not much difference between actions that are successful and those that are unsuccessful. And, specifically, that energy directed at identifying, classifying and quantifying failures would be better directed at developing a richer understanding of how complex systems work. For example, how they generally succeed in responding to variations in demand, reduced resources, and unexpected events. A potential irony of HRA is that the failure reduction measures suggested following an analysis (e.g. increased automation, additional supervision), could serve to inhibit the evolved adaptability of a system, making failures more, not less, likely.

Despite all of this, the term error is so heavily enshrined in the HRA techniques covered in this publication, and in the unit of measurement – HEP, that a discussion of current practices in HRA is impossible without its use.

C.1 UNIT OF MEASUREMENT

The standard unit of measurement in HRA is the HEP. This is defined as:

$$\frac{\text{Number of errors occurred}}{\text{Number of opportunities for error}}$$

This unit of measurement is necessary for human factors considerations to be incorporated in QRAs. However, the concept of human error is complex, and for the reasons discussed elsewhere in this guidance, may not be well suited to the prevailing engineering model of QRAs. Previous attempts to classify failures can be broadly grouped into those that classify failures according to their observable outcomes or those that classify them according to underlying error mechanisms.

C.2 OBSERVABLE OUTCOME-BASED FAILURE CLASSIFICATIONS

Early engineering interest in human error focused on describing observable outcomes. Such classifications provide no particular insight into why a particular failure might occur, but instead focus on the different ways in which people can fail.

These types of classifications can help a designer to design systems that protect against identified failures with significant outcomes. However, they do not help with understanding the reasons why a failure occurs. An example of such a classification can be found in EI *Guidance on human factors safety critical task analysis* (Step 5).

There is a further distinction between active and latent failures (or conditions). A latent failure is one that may be present for many years before, in combination with local conditions and active failures, it results in unwanted outcomes. This distinction was an element of the well-known 'Swiss cheese' model (see Reason (1997)).

C.3 FAILURE MECHANISMS

In the 1970s and 1980s, the discipline of cognitive engineering moved the focus away from the engineering, black-box style, approach, set out in C2, and started to examine the role that decision-making, problem solving and diagnosis played in failures.

Some of the results of this approach are summarised in EI *Human failure types.* It presents a human failure taxonomy outlining the types of mechanisms that underlie the observable, outcome-based failures described in C2.

The taxonomy distinguishes between: non-compliances, where a person acts, either knowingly or otherwise, contrary to existing rules or procedures (some HRA methodologies are poor at addressing the impact of non-compliance on overall risk); mistakes, when an incorrect course of action is chosen; and slips and lapses, when an individual chooses the correct course of action but fails to execute it as intended. The publication includes more detail about these different types of failure, as well as providing guidance on how they might be addressed.

The practical importance of these distinctions is that steps taken to reduce failure probability would be different depending on the identified type of failure. For example, mistakes might be addressed by providing better training and decision support (e.g. in the form of flow-chart decision aids), whereas slips would be more likely to be prevented by improved design of the operating environment (e.g. by setting out equipment in a logical manner).

C.4 POSSIBLE FUTURE DEVELOPMENTS

The tools outlined in this publication have a significant number of limitations. In particular, the vast majority take a deterministic approach to the management of human failure (i.e. one that relies on the identification and management of cause and effect relationships). Since the systems that they are directed at tend to be dynamic and highly complex, with individuals and managers constantly reacting to changing situations (e.g. reduced resources, interruptions, operating conflicts), it is difficult to be confident of the accuracy of any such analysis over a period of time.

Therefore, the future of human reliability management is likely to lie in approaches that recognise the complexities of working in modern industrial systems. One such model is functional resonance (see Hollnagel (2004)). This approach suggests that failure is not the breakdown of system components, as defined in reliability engineering, but instead the inability of systems, either temporarily or permanently, to adjust to their current operating conditions. Therefore, whilst systems involving people evolve the capability to cope with a wide range of different conditions (e.g. reduced staffing levels, high workload, operational problems, etc.), failures are most likely to happen when adverse conditions occur simultaneously and interact with others. However, such techniques are still to be developed into an operational form.

ANNEX D
COMMONLY USED HRA TECHNIQUES

Table D1 Openly available HRA techniques considered useful to HSE major hazards directorates (adapted from HSE RR679, (Note 1))

Tool	Description	HEP	Domain	References	Notes/ key features
First generation methods					
THERP	Uses failure event trees to represent potential human errors. These are then quantified using the THERP database, which contains both baseline HEPs for the types of task and adjustments for interdependencies between errors and the effect of predefined PSFs.	Baseline HEP is estimated and then adjusted for interdependencies and PSFs.	Developed for use in the nuclear industry but has also been applied in other sectors.	USNRC NUREG/CR-1278.	Models the interdependencies between failures. Has good explanatory material on each element in the data tables.
ASEP (Accident Sequence Evaluation Program)	A shortened version of THERP that can be used to identify tasks requiring a full THERP analysis. It comprises an analysis of pre-accident tasks, post-accident tasks, HEPs and response times.	HEPs are assigned to tasks for screening and/or sensitivity analysis. More conservative than THERP.	Developed and applied in the nuclear industry. Unlike THERP, it is not suitable for use in other sectors.	USNRC NUREG/CR-4772.	Quicker to carry out than THERP.

Table D1 continued

HEART	The premise of HEART is that the level of human reliability depends on the general nature of the task but can be degraded by a number of predefined EPCs.	Baseline HEP is assigned according to the nature of the task and then adjusted for EPCs.	Developed in the nuclear industry but intended for use in any sector. (e.g. chemical, transport and medical).	The method has been outlined in a number of conference publications and technical reports. A detailed user manual was written for Nuclear Electric (now British Energy) in 1992. Whilst it is not in the public domain, it is available on request from British Energy.	A straightforward method that requires little in the way of resources.
SPAR-H	This method assumes that human failure has two components: diagnosis failures and action failures. SPAR-H assesses the contribution of each to overall HEP, adjusted for predefined PSFs and interdependencies.	Baseline HEPs are assigned for the diagnosis and action elements, adjusted for PSFs. Overall HEP is adjusted for interdependencies.	Developed in the nuclear industry.	USNRC NUREG/CR-6883.	Lends itself to a basic reliability analysis.
Second generation methods					
ATHEANA	ATHEANA examines the effect on human reliability of error-forcing contexts (EFCs). These are situational factors (e.g. plant conditions) that make unsafe actions more likely.	HEP is calculated from the probability of EFCs combined with the probability of unsafe acts in the presence of the EFCs.	Developed in the nuclear industry.	USNRC NUREG/CR-6350 and USNRC.	USNRC NUREG/CR-6350 and USNRC.

Table D1 continued

CREAM	CREAM is a HRA method based on Hollnagel's (1998) contextual control model. It proposes that 'phenotypes' (erroneous human or system behaviours) can be traced back to three causal 'genotypes': person characteristics (e.g. cognition); system characteristics (e.g. human-machine interaction); and organisational characteristics (e.g. physical environment).	A nominal cognitive failure probability (CFP) is provided for relevant cognitive failures (phenotypes and person-specific genotypes). This is adjusted for the effect of common performance conditions (system- and organisation-specific genotypes).	Developed for generic use, particularly in process control industries.	Hollnagel (1998). A freely available software tool has been available from www.ews.uiuc.edu	Based on a comprehensive model of human performance.
Other useful techniques					
APJ	A set of methods for eliciting informed judgements of error probabilities. These involve individual or group activities with subject matter experts; in the latter, scores from individuals are either aggregated after the elicitation event or revised for consensus during the event.	HEP is directly elicited from subject matter experts.	APJ is intended for use in any domain where subject matter experts can be obtained.	USNRC NUREG INL/EXT-05-00433; Kirwan (1994).	A relatively quick and straightforward method to use.

Table D1 continued

PCs	This is based on the psychological approach known as psychophysics. Like APJ, it makes use of subject matter experts; however, the method differs in that the participants, rather than making absolute judgements about error probabilities, make binomial comparisons of different errors.	HEP is obtained by calibrating the ordinal likelihood ratings of all identified errors against those of errors with known HEPs.	PCs is intended for use in any domain where subject matter experts can be obtained.	Kirwan (1994).	A viable alternative to APJ where calibration data are available.
SLIM	SLIM assumes that the likelihood of an error is influenced by the presence of PIFs, whose relative levels and weights of effect on task performance can be estimated by subject matter experts. These estimates are used to calculate the success likelihood index (SLI) of each task.	HEP is obtained by calibrating the SLIs of all identified errors against those of errors with known HEPs.	Developed in the nuclear industry, but intended for use in any domain where subject matter experts can be obtained.	USNRC NUREG/CR-3518. A proprietary software tool is available from http://www.humanreliability.com	A more flexible method than contemporary approaches such as HEART and THERP.
Influence Diagrams	Influence diagrams are an extension of the SLIM approach, in which PIFs are organised into a hierarchy. This allows interactive effects between them to be represented.	HEP is obtained by calibrating the SLIs of all identified errors against those of errors with known HEPs.	Developed for generic use.	Phillips et al (1990).	Provides a more detailed and scalable assessment of PIFs than other HRA methods.

Notes:

1 This table is based on one presented in HSE RR679: that Research Report also evaluates the merits of the individual techniques.

ANNEX E
OVERLAP WITH EI *GUIDANCE ON HUMAN FACTORS SAFETY CRITICAL TASK ANALYSIS*

EI *Guidance on human factors safety critical task analysis* provides guidance on qualitative HRA. There is some overlap between the qualitative process set out there and the stages of quantified analysis set out in this publication. The main additional stages are shown in Table E1.

Table E1 Quantitative and qualitative HRA

Quantified HRA process set out here in section 4.1 of this publication	**Qualitative safety critical task analysis process set out in EI *Guidance on human factors safety critical task analysis***
1. Preparation & problem definition	1. Identify main hazards 2. Identify critical tasks
2. Task analysis	3. Understand the tasks 4. Represent critical tasks
3. Human failure identification	5. Identify human failures and PIFs
4. Human failure modelling	n/a
5. Human failure quantification	n/a
6. Impact assessment	n/a
7. Failure reduction	6. Determine safety measures to control human failures
8. Review	7. Review effectiveness of process

As EI *Guidance on human factors safety critical task analysis* addresses the qualitative HRA process in detail, only a brief summary of steps 1-3 is provided here. However, issues in these steps that might affect the quantification process are discussed in this publication.

ANNEX F
MODELLING ISSUES

The human failure modelling approach outlined in section 4.2.4 (Step 4 of the HRA process) is of central importance to both qualitative and quantitative HRAs. The issues that should be considered may be divided into two interrelated areas: those relating to the completeness of modelling, and those concerned with the level of decomposition of the activities that are to be assessed.

F.1 NEED TO QUANTIFY AT THE APPROPRIATE LEVEL OF DECOMPOSITION

One of the most commonly used approaches to HRA quantification involves the use of database techniques. These comprise methods that contain a specific database of HEPs that are grouped into categories such as failures associated with specific task types, e.g. 'An error of omission when use of procedures is specified but they are not used' (see THERP example in Table B3). For these techniques, the analyst matches the task type with the corresponding item in the database, and then applies the contextual PIFs specified in the database to modify these basic HEPs. In the THERP example in Table B3, the overall failure probability is calculated by combining the probabilities for possible hardware failures with failures in responding to these failures together with failures in performing the required actions.

However, the quantification exercise could have been carried out at a much more global level by simply classifying the overall scenario as a 'Dynamic task carried out under stressful circumstances' (from the THERP classification, see C1 in Table B3) and quantified as having an HEP of 0,25. However if the generic recovery probability of recovery 0,025 is applied (see B2 in Table B3), the HEP then becomes about 0,0063, i.e. about an order of magnitude less than the results (0,05) if the more comprehensive modelling used in the example is applied. The difference in these results arises because the more comprehensive model of the scenario identifies a greater number of opportunities for failure and hence produces a greater overall failure probability. This example illustrates the danger of applying a quantification process at too high a level of aggregation.

This result is particularly important when using a technique such as HEART (see Table B6). In the HEART example in Appendix B, the analyst deliberately confined the use of the technique to a single subtask. However, in order to minimise analytical resources it may be tempting to classify a complex task containing many subtasks into one task which falls into one of the overall HEART categories and then apply the HEP associated with the category. This could give rise to similar issues as in the THERP example described above.

F.2 A SYSTEMATIC MODELLING PROCESS TO SUPPORT ACCURATE QUANTIFICATION

With more complex tasks containing a number of subtasks and steps, a rigorous and systematic approach should be applied to qualitative modelling in order to obtain meaningful results.

This section describes a qualitative modelling process similar to that set out in EI *Guidance on human factors safety critical task analysis*. The process comprises the following steps:

1. Break down the task objective into the elements (e.g. subtasks, task steps) required to achieve this objective.

2. Screen these task elements (using a risk ranking process) to specify the elements to be included in subsequent more detailed analyses.

3. Classify the included task elements into an activity category (e.g. action, checking).

4. Identify the failure types (or modes) which could give rise to the task failing to achieve its objectives (N.B. issues discussed in section 4.2.4, such as dependence, should also be considered at this stage).

5. Decide if recovery from one or more of the failure types in the model is possible, and if so include these recoveries in the model, using an AND logic gate as appropriate.

6. Assign HEPs to failure modes (and recovery failures if appropriate).

7. Combine the HEPs using fault tree logic to give an overall probability of the consequences being realised.

8. Perform sensitivity and cost effectiveness analyses to evaluate alternative risk reduction options, as appropriate.

F.3 ILLUSTRATION OF THE MODELLING PROCESS

The modelling and quantification process described in F2 is illustrated in the following example.

1. Break down the task goal into its constituent elements

Figure F1 shows the top level of a hierarchical task analysis (HTA) for a ship unloading operation. In this scenario, a tanker is being unloaded to a number of onshore tanks with different capacities. Before unloading starts, the contents have to be tested to verify that they meet the required specification. A hose is then connected to the ship, the onshore receiving tanks are lined up to receive the transfer, the ship is discharged and finally the paperwork is completed.

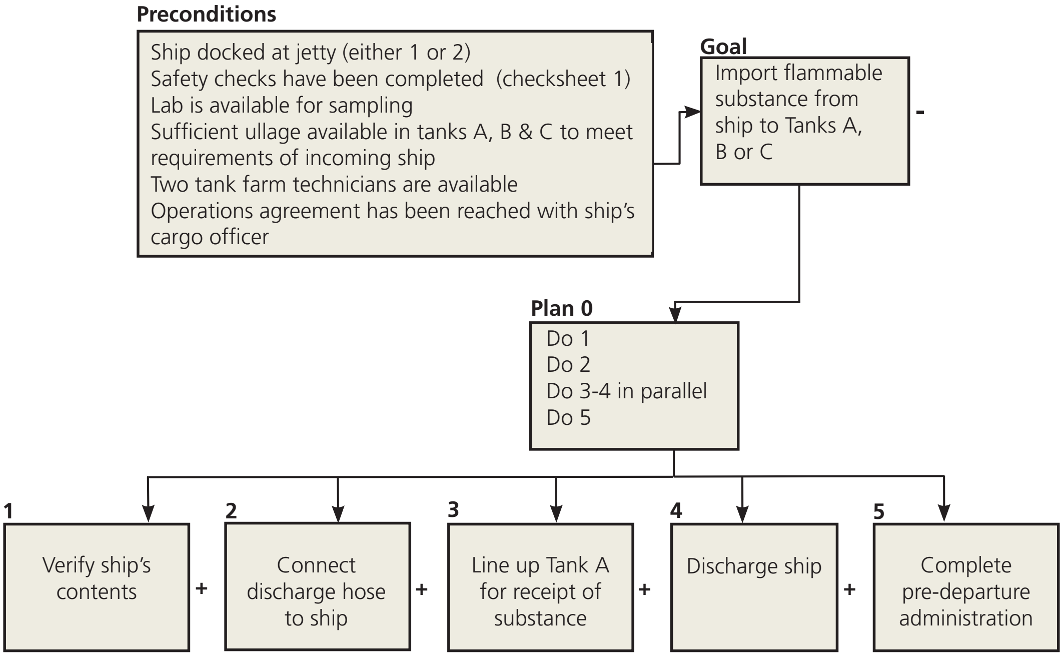

Preconditions
Ship docked at jetty (either 1 or 2)
Safety checks have been completed (checksheet 1)
Lab is available for sampling
Sufficient ullage available in tanks A, B & C to meet requirements of incoming ship
Two tank farm technicians are available
Operations agreement has been reached with ship's cargo officer
Goal
Import flammable substance from ship to Tanks A, B or C
-
Plan 0
Do 1
Do 2
Do 3-4 in parallel
Do 5
1
Verify ship's contents
+
2
Connect discharge hose to ship
+
3
Line up Tank A for receipt of substance
+
4
Discharge ship
+
5
Complete pre-departure administration

Figure F1 First level HTA breakdown for a complex task

Clearly, it would not be sensible to assess a complex scenario such as this at the global level of the overall task goal: 'Import flammable substance from ship to Tanks A, B or C'. However, it would be possible to quantify the likelihood of the overall task goal failing by first assessing the HEPs of each of the subtasks 1-5. The HTA can then be treated as a fault tree and the probabilities added by using an OR gate. This assumes that these probabilities are small and can be treated as independent. However, the subtasks can be decomposed further in order to obtain a more accurate estimate of the overall HEP for the task (this is illustrated in Figures F2 and F3).

2. Risk rank the task elements at the current level of analysis

In order to minimise the analysis effort, is useful to prioritise which of the subtasks should be selected for analysis and quantification. A number of approaches are available for screening (e.g. see HSE OTO 1999/092).

A simple method for prioritising the analysis process is to develop a risk ranking score for each of the subtasks, to make a global evaluation of the likelihood of failure (e.g. based on a subjective judgement of the nature of the task, the quality of the PIFs in the situation), and the severity of the consequences if the failure is not recovered. Assessing these parameters on a three point scale (high = 3, medium = 2, low = 1) and multiplying these assessments gives a simple risk index ranging from 1 to 9, where 9 is the highest risk). This ranking process is applied to the top five subtasks to give the results in Table F1. Based on these results, subtask 2 was selected for more detailed analysis.

Table F1 Example risk ranking scores for top level subtasks

Task element	Likelihood of failure	Severity of consequences	Risk index
1. Verify ship's contents	H (3)	L (1)	3
2. Connect discharge hose to ship	M (2)	H (3)	6
3. Line up Tank A for receipt of substance	H (3)	H (3)	9
4. Discharge ship	M (2)	M (2)	4
5. Complete pre-departure administration	L (1)	L (1)	1

In this example, it is assumed that the risk ranking score is considerably higher for subtask 3 'Line up Tank A for receipt of substance' and hence this should be decomposed further.

Following the screening process, the decomposition Step 1 is repeated for those task elements selected for more detailed analysis. This is shown in Figure F2.

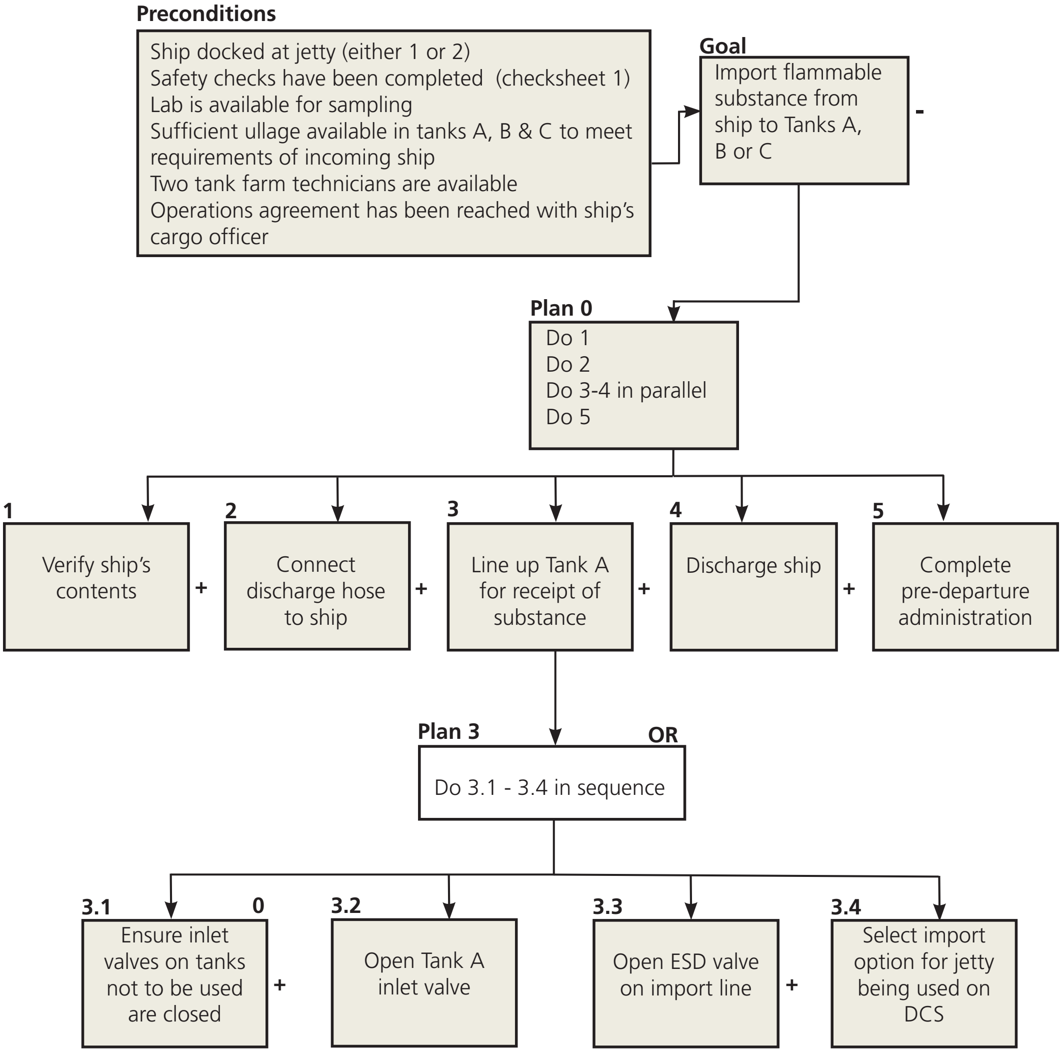

Preconditions
Ship docked at jetty (either 1 or 2)
Safety checks have been completed (checksheet 1)
Lab is available for sampling
Sufficient ullage available in tanks A, B & C to meet requirements of incoming ship
Two tank farm technicians are available
Operations agreement has been reached with ship's cargo officer
Goal
Import flammable substance from ship to Tanks A, B or C
-
Plan 0
Do 1
Do 2
Do 3-4 in parallel
Do 5
1
Verify ship's contents
+
2
Connect discharge hose to ship
+
3
Line up Tank A for receipt of substance
+
4
Discharge ship
+
5
Complete pre-departure administration
Plan 3
OR
Do 3.1 - 3.4 in sequence
3.1
0
Ensure inlet valves on tanks not to be used are closed
+
3.2
Open Tank A inlet valve
3.3
Open ESD valve on import line
+
3.4
Select import option for jetty being used on DCS

Figure F2 Second-level HTA breakdown for a complex task

Assuming that fault tree logic applies, the overall HEP for subtask 3 can then be calculated as the sum of the failure probabilities of the constituent task elements 3.1-3.4. (N.B. the calculation for this example assumes that the actions are independent.) The task breakdown to this level means that the analyst is much more likely to produce an accurate quantification. It also means that any failure reduction measures can be applied in the specific task element where the greatest risk (e.g. highest HEP) is identified.

The screening and risk ranking process described previously is then repeated again to drill down to those areas of the overall task that constitute the greatest risk. In this example, it is assumed that the application of the risk ranking process indicates that task steps '3.1 Ensure inlet valves on tanks not to be used are closed', and '3.3 Open ESD valve on import line' need to be included in the HEP evaluation, as shown in Figure F3.

3. Classify the most detailed level task elements into activity types

Once the task has been broken down to the most detailed level of task elements, a different type of decomposition may be performed. This considers the individual failure modes associated with the lowest level subtasks. In order to assign these failure modes, the task elements at the lowest level of decomposition are first classified into one of the following five activity categories:

- actions;
- checking;
- information retrieval (from a display, a procedure or memory);
- information communication (person to person, either directly or via a device such as a telephone), and
- selection (choosing from a number of similar objects or options).

4. Identify the failure types (or failure modes) which could give rise to the task failing to achieve its objectives.

This stage of the analysis uses a set of failure modes for each of the task types that appear in the analysis. Typical failure identification guidewords are reproduced in Table F2 (originally presented in Embrey (1986)).

Table F2 Failure identification guidewords

Action failures	**Checking failures**	**Communication failures**
A1 Operation too long/ short	C1 Check omitted	I1 Information not communicated
A2 Operation mistimed	C2 Check incomplete	I2 Wrong information communicated
A3 Operation in wrong direction	C3 Right check on wrong object	I3 Information communication incomplete
A4 Operation too little/ too much	C4 Wrong check on right object	I4 Information communication unclear
A5 Operation too fast/ too slow	C5 Check too early/ late	
A6 Misalign		
A7 Right operation on wrong object	**Information retrieval failures**	**Selection failures**
A8 Wrong operation on right object	R1 Information not obtained	S1 Selection omitted
A9 Operation omitted	R2 Wrong information obtained	S2 Wrong selection
A10 Operation incomplete	R3 Information retrieval incomplete	
A11 Operation too early/ late	R4 Information incorrectly interpreted	
A12 Operation in wrong order		
A13 Misplacement		

Considering failures at this level of detail ensures that the analyst evaluates as wide a range of failure modes as possible within each activity type, thus ensuring that no failures with specific consequences are omitted. Usually only a subset of these failure modes is considered, as many of them can be excluded by applying the screening process described earlier.

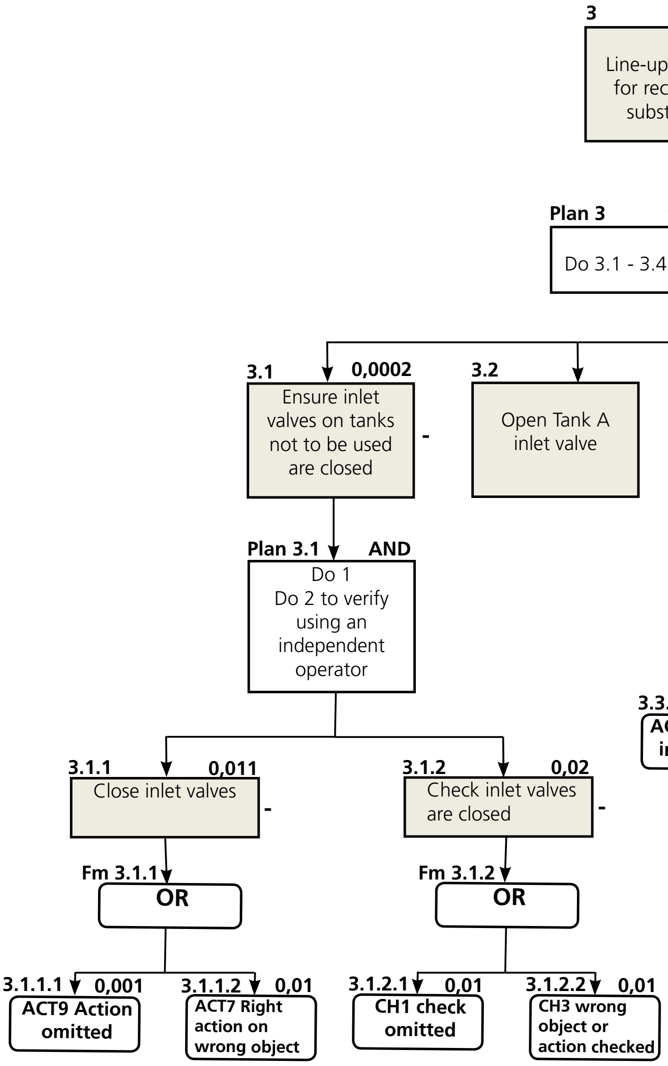


Figure F3 Third-level breakdown for a complex task

One reason for classifying task elements into activity types such as action, checking and communication failures is to apply discrete quantification models to each of these activity types. These specify the specific PIFs that influence the HEPs for each activity type. With some quantification techniques, these PIFs can then be assessed to allow baseline HEPs to be modified to reflect the context within which the task is carried out.

It should be emphasised that quantification does not necessarily require that a task is decomposed to the level of the individual failure modes. Both Steps 3 and 4 are optional, and it is common for quantification to be applied at the most detailed level of the task decomposition, rather than at the level of the failure modes themselves.

In the example analysis, the task element types being considered were checks (denoted CH) and actions (denoted ACT). The failure mode considered at 3.1 was therefore that the check fails. This in turn is broken down into two of the checking failure modes included in Figure F3, i.e. CH1 'Check omitted' or CH3 'Wrong object or action checked' (e.g. where the person tasked with monitoring the check was focusing on another part of the task). Other failure modes in the Table F2 list could have been included at this stage, e.g. C5 'Check too early/ late', but these were deemed to be low probability events.

5. Include any recovery steps in the model, using an AND logic gate as appropriate.

A recovery step was included in Figure F3 at the same level as the check failure, as it was felt that close monitoring by a second operator might detect the failure to check that the inlet valves on the tanks not to be used are closed (3.1). Both the check itself and the monitoring of the check (i.e. the recovery step) have to fail for the check not to be carried out. (Again, for the purposes of the calculation in this example, the action and check are assumed to be independent. However, in a real world situation, it is probable that there will be some degree of dependence between the initial action and the related check. This should be addressed in the analysis – see section 4.2.4).

6. Assign HEPs to failure modes (and recovery failures if appropriate).

The failure probabilities shown in Figure F3 were assigned to the failure and recovery modes. SLIM, which consists of separate models of the PIFs that influence the HEPs for each of the task types in Table F2, was used to derive these HEPs. The states of these factors were assessed for each failure mode, which produced context specific HEPs based on the state of the PIFs in the situation being assessed.

7. Combine the constituent HEPs using fault tree logic to give an overall probability of the consequences being realised.

The combination of these probabilities gave an overall failure probability of 2,0E-4 for the failure of task element 3.1. A similar calculation gave a failure probability of 3,4E-3 for task element 3.3. Assuming the failure rates for the other elements at this level are negligible, the failure probability for subtask 3 'Line-up Tank A for receipt of substance' is given by the sum of these HEPs, i.e. 3,6E-3.

8. Perform sensitivity analyses and cost effectiveness analyses to alternative risk reduction options as appropriate

Changes may be made to each of the PIFs to assess which change gives the greatest reduction in the HEPs at the lowest cost.

F.4 DISCUSSION AND SUMMARY

The first part of this annex emphasised the need for comprehensive qualitative modelling of the task or system prior to quantification. The process described in F2 provides a systematic framework to achieve this. The modelling approach decomposes a task to the most appropriate level for the specific type of assessment being performed. It should be emphasised that Steps 3 and 4 described above are optional. A task can be quantified at the level of its task elements. Where a database of HEPs is being used, e.g. such as that included with THERP, this will prescribe the level of task decomposition at which the numerical assessments are made. Essentially the degree of detail of the modelling is matched to the level of decomposition of the task elements in the database. Otherwise, the degree of detail will depend on the criticality of the task being evaluated and the level of analytical resources available.

The more detailed the modelling, the less likely it is that a significant human failure will be missed, but the greater the analytical effort required. The use of HTA to structure the task modelling has the advantage that it allows task elements to be screened and prioritised prior to quantification being applied, thus minimising the analysis resources required. The HTA structure also readily maps onto the fault tree structure, which will be familiar to engineering reliability and safety analysts. Although the generation of the qualitative model and the assignment of probabilities may appear to be a daunting task, the effort required can be reduced by the screening process described above and the application of software tools for human reliability modelling and assessment (for a description see Embrey (2011)).

ANNEX G
GLOSSARY OF TERMS AND ABBREVIATIONS

G.1 INTRODUCTION

This annex contains brief descriptions of terms and abbreviations used herein that may be encountered when working with HRA techniques.

For the purpose of this publication, the interpretations of terms in G.2 and abbreviations in G.3 apply, irrespective of the meaning they may have in other connections.

G.2 TERMS

absolute probability judgement (APJ): quantification technique that uses experts to directly estimate HEPs.

active failure: type of failure where the consequences are immediately apparent. See *latent failure*.

bow-tie diagram: visual representation of hazardous events and their causes, consequences and controls sometimes used in risk management.

cognitive error: failures in decision-making and choices of action.

common cause failure: failures in multiple parts of a system caused by a common fault. For example, in human reliability, if a technician misunderstands how a maintenance action should be carried out, it is probable that all systems maintained by that individual will have the same fault. See *dependency*.

dependency: degree to which actions are dependent on each other. For example, if the same operator has to respond to two alarms then it is unlikely that the failures associated with the response will be independent. A major issue in HRA is that it is not always immediately apparent that actions are dependent on each other, and, consequently, it can be difficult to represent dependence in HRA. See *human reliability analysis (HRA)*.

error of commission: failure resulting from an action that alters the state of the system in question. Essentially, it is when an individual does the wrong thing. It may also result in an error of omission (as the original required task remains uncompleted). See *error of omission*.

error of omission: failure to carry out a required action. See *error of commission*.

error producing condition (EPC): in HEART, a factor that can increase the probability of failure. See *performance influencing factor (PIF).*

first generation HRA techniques: HRA techniques developed through the 1970s and 1980s. These used a range of methods to modify base HEPs to reflect the context or PIFs in the specific situation being assessed. See *human reliability analysis (HRA), performance influencing factor (PIF)* and *second generation HRA techniques*.

hierarchical task analysis (HTA): technique that involves the hierarchical decomposition of tasks into goal-based sub-steps. Commonly used as an input to HRA. See *human reliability analysis (HRA)*.

human error: in reliability engineering, the term human error is used to refer to failures resulting from human actions. In cognitive psychology, the same term is often used to describe error mechanisms that underpin observable failures (see Annex C for a more detailed discussion).

human error probability (HEP): the number of failures on demand divided by the number of demands.

human factors: environmental, organisational and job factors, and human and individual characteristics which influence behaviour at work in a way which can affect health and safety (and environmental protection).

human performance limiting value (HPLV): limit on the level of human reliability that should be claimed in a risk assessment. These values are used to reduce the instances of overly optimistic claims for reliability.

human reliability analysis (HRA): techniques designed to support the assessment and minimisation of risks associated with human failures. They have both qualitative (e.g. task analysis, failure identification) and quantitative (e.g. human error quantification) components.

lapse: failure where a person forgets to do something.

latent failure (or condition): failure where the consequences only become apparent after a period of time and in combination with active failures. See *active failure*.

layers of protection analysis (LOPA): semi-quantificative technique that can be used to undertake a process hazard analysis (PHA). See *process hazard analysis (PHA)*.

mistake: type of failure occuring when an individual does what they mean to do, but should have done something else.

non-compliance (synonymous with violation): type of failure where a person acts (either knowingly or unknowingly) without complying with a rule or procedure.

performance influencing factor (PIF) (synonymous with performance shaping factors (PSF): contextual factor such as the person, team, environment or task characteristics which determine the likelihood of failure. See *error producing condition (EPC).*

performance shaping factor (PSF): see *performance influencing factor (PIF)*.

probabilistic safety analysis (PSA): analytical process used to describe and quantify potential risk associated with the design, operation and maintenance of a facility.

process hazard analysis (PHA): systematic assessment of the hazards associated with a process in order to improve safety, and reduce the consequences of incidents.

safety instrumented function (SIF): safety function with a specified SIL which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function. [Replicated from IEC 61511-1.] See *safety integrity level (SIL).*

safety instrumented system (SIS): instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor(s), logic solver(s), and final element(s). [Replicated from IEC 61511-1.] See *safety instrumented function (SIF)*.

safety integrity level (SIL): discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. SIL 4 has the highest level of safetyy integrity; SIL 1 has the lowest. [Replicated from IEC 61511-1] See *safety instrumented function (SIF)*.

screening: process to identify where the major effort in the quantification process should be focused. In particular, the analyst should avoid spending time quantifying failures that have minimal consequences (e.g. if there are diverse and reliable control measures in place).

second generation HRA techniques: techniques that extended the consideration of contextual factors and addressed some specific deficiencies with first generation HRA techniques. In particular, they addressed cognitive functions such as decision-making and diagnosis failures. See *first generation HRA techniques*.

slip (of action): type of failure where a person does something but it is not what they intended to do.

task analysis: Analysis technique which is used to represent the way a task is undertaken. See *Hierarchical Task Analysis (HTA)*.

violation: see *non-compliance*.

G.3 ABBREVIATIONS

APJ	Absolute Probability Judgement
ASEP	Accident Sequence Evaluation Program
ATHEANA	A Technique for Human Event Analysis
BPCS	basic process control system
CCTV	closed-circuit television
CFP	cognitive failure probability
CREAM	Cognitive Reliability and Error Analysis Method
CRO	control room operator
EI	Energy Institute
EPC	error producing condition
FO	field operator
HEART	Human Error Assessment and Reduction Technique
HEP	human error probability
HPLV	human probability limiting value
HRA	human reliability analysis
HSE	Health & Safety Executive
HSL	Health & Safety Laboratory
HTA	hierarchical task analysis
LOC	loss of containment
LOPA	layers of protection analysis
P&ID	piping and instrumentation diagram
PCs	Paired Comparisons
PFD	probability of failure on demand
PHA	process hazard analysis
PIF	performance influencing factor
PIV	propane vapour inlet valve
POV	liquid propane outlet valve
PSF	performance shaping factor
OGP	International Association of Oil and Gas Producers
PSA	probabilistic safety analysis
QHRA	quantified human reliability analysis
QRA	quantified risk assessment
SCTA	safety critical task analysis
SIF	safety instrumented function
SIL	safety integrity level
SLI	success likelihood index
SLIM	Success Likelihood Index Method
SPAR-H	Standardised Plant Analysis Risk Human Reliability Method
THERP	Technique for Human Error Rate Prediction
UKPIA	UK Petroleum Industry Association

ANNEX H
REFERENCES

The information provided in this annex comprises publications that are referred to herein. All were current at the time of writing. Users should consult the pertinent organisations for details of the latest versions of publications. To assist, many Internet addresses are provided.

American Chemistry Council (ACC)

www.americanchemistry.com

— *A manager's guide to reducing human errors: Improving human performance in the chemical industry* (1990).

Books

— Hollnagel E. (1998) *Cognitive Reliability and Error Analysis Method*. Oxford: Elsevier.

— Hollnagel E. (2004) *Barriers and accident prevention.* Aldershot: Ashgate.

— Kirwan B. & Ainsworth L.K. (1992) *A guide to task analysis.* London: Taylor & Francis.

— Kirwan B. (1994) *A guide to practical human reliability assessment.* London: Taylor & Francis.

— Reason J.T. (1997) *Managing the risks of organizational accidents*. Aldershot: Ashgate.

— Phillips L.D., Embrey D., Humphreys P. and Selby D.L. (1990) *A socio-technical approach to assessing human reliability,* in Oliver R.M. & Smith J.A. *Influence diagrams. Belief nets and decision making: Their influence on safety and reliability.* New York: Wiley.

— Woods D.D., Dekker S., Cook R., Johannesen L. & Sarter N. (2010) *Behind human error*. Farnham: Ashgate.

Center for Chemical Process Safety (CCPS)

www.aiche.org/ccps

— *Guidelines for preventing human error in process safety* (2004).

Conference etc. papers

— Embrey D. (2011) *The UK experience in managing risks arising from human error in the oil and gas sector*. American Institute of Chemical Engineers 2011 Spring Meeting: 7th Global Congress on Process Safety, Chicago, Illinois.

— Embrey D.E. (1986) *SHERPA: A systematic human error reduction and prediction approach*. International Meeting on Advances in Nuclear Power Systems, Knoxville, Tennessee.

— Williams J.C. (1986) *HEART – A proposed method for assessing and reducing human error.* 9th Advances in Reliability Symposium, University of Bradford.

Energy Institute (EI)

www.energyinst.org www.energypublishing.org

— *Guidance on human factors safety critical task analysis* (2011).

— *Guidance on safety integrity level (SIL) determination* (in press).

— *Human failure types* (2010). www.energyinst.org/technical/human-and-organisational-factors/human-and-organisational-factors-human-failure-types (accessed July 2012).

Health and Safety Executive (HSE)

www.hse.gov.uk

— *Human reliability analysis*, Technical Assessment Guide T/AST/063 (2010). www.hse.gov.uk/nuclear/operational/tech_asst_guides (accessed July 2012).

— Offshore Technology Report OTO 1999/092 *Human factors assessment of safety critical tasks* (2000).

— Offshore Technology Report OTO 2001/053 *Preventing the propagation of error and misplaced reliance on faulty systems: A guide to human error dependency* (2001).

— *Reducing risks, protecting people: HSE's decision making process* (2001).

— Research Report RR679 *Review of human reliability assessment methods* (2009).

— Research Report RR716 *A review of layers of protection analysis (LOPA) analyses of overfill of fuel storage tanks* (2009).

International Association of Oil & Gas Producers (OGP)

www.ogp.org.uk

— Report 454 *Human factors engineering in projects* (2011).

International Atomic Energy Agency (IAEA)

www-ns.iaea.org

— *Basic level 1 PSA course for analysts – Human reliability analysis* (1995) www-ns.iaea.org/downloads/ni/training/specific_expert_knowledge/psa-level1/III4_1%20Human%20Reliability%20Analysis.pdf (accessed May 2011).

International Electrotechnical Commission (IEC)

www.iec.ch

— IEC 61511 (series) *Functional safety. Safety instrumented systems for the process industry sector.*

Research papers

— Kirwan B., Martin B.R., Rycraft H. & Smith A. (1990) *Human error data collection and generation. International Journal of Quality and Reliability Management,* 7.4, 34-36.

The SRD Association (SRD)

— *Human reliability assessor's guide* (1995). Warrington: Human Factors in Reliability Group.

UK Petroleum Industry Association Ltd. (UKPIA)

www.ukpia.com

— *Gap analysis and self assessment for operators & SIL1 safety systems for overfill protection systems* (2011). www.ukpia.com/files/pdf/ukpia-sil1-operators-v12.pdf (accessed July 2012).

US Nuclear Regulatory Commission (USNRC)

www.nrc.gov

— INL/EXT-05-00433 *Simplified expert elicitation guideline for risk assessment of operating events* (2005).

— NUREG-1880 *ATHEANA user's guide – Final report* (2007).

— NUREG/CR-1278 *Handbook of human reliability analysis with emphasis on nuclear power applications: Final report* (1983).

— NUREG/CR-3518 *SLIM-MAUD: An approach to assessing human error probabilities using structured expert judgement* (1984).

— NUREG/CR-4772 *Accident Sequence Evaluation Program – Human reliability analysis procedure* (1987).

— NUREG/CR-6350 *A Technique for Human Error Analysis (ATHEANA)*, (1996).

— NUREG/CR-6883 *The SPAR-H human reliability analysis method* (2005).

Energy Institute
61 New Cavendish Street
London W1G 7AR, UK

t: +44 (0) 20 7467 7100
f: +44 (0) 20 7255 1472
e: **pubs@energyinst.org**
www.energyinst.org

This publication has been produced as a result of work carried out within the Technical Team of the Energy Institute (EI), funded by the EI's Technical Partners. The EI's Technical Work Programme provides industry with cost effective, value adding knowledge on key current and future issues affecting those operating in the energy sector, both in the UK and beyond.

ISBN 085293 635 1

Registered Charity Number 1097899