HSE
Health & Safety
Executive

Preventing the propagation of error and misplaced reliance on faulty systems: A guide to human error dependency

Prepared by
Greenstreet Berman Ltd
for the Health and Safety Executive

OFFSHORE TECHNOLOGY REPORT

2001/053

First published 2001

ISBN 0 7176 2104 9

Preventing the propagation of error and misplaced reliance on faulty systems: A guide to human error dependency

Greenstreet Berman Ltd
First Base
Beactonree Plaza
Gillette Way
Reading
Berkshire
RG2 0BP

HSE BOOKS

HUMAN FACTORS IN RELIABILITY GROUP

The Human Factors in Reliability Group (HFRG) is an inter-industry working group for the exchange of information concerning Human Factors issues in reliability, with emphasis on high-hazard activities. It draws its expertise from a broad spectrum of applications areas, including the Nuclear Industry, Process Control, Transport, Offshore, etc.

Its methods of working include the creation of sub-groups to consider specific issues, and to produce documents summarising current views. This document is the report of the HFRG Human Error Dependency Modelling Sub-Group (HEDMG). Its primary objectives are to:

* Develop an understanding of the causes of human error dependency and identify dependency reduction measures

* Develop a framework to guide analysts in considering the importance of dependency in a given context, and the manner in which such dependency might be controlled.

Human Error Dependency Modelling Sub-Group

The following organisations (in alphabetical order) have contributed to the work of the Sub-Group:

British Gas	HSE
BNFL	Lloyds Register
DnV Technica	Nuclear Electric
EWI	NNC
Four Elements	Rolls Royce and Associates
Greenstreet Berman	AEA Technology

The following persons (in alphabetical order) have been involved with the work of the Sub-Group for some or all of the time:

Peter Ackroyd	Angela Jenkins
Jon Berman	Keith Mitchell
Andy Dolby	Gary Munley
Bill Gall	Martin Ridal
Steve Harris	Sam Samuel
Paul Hollywell	Trevor Waters
Gareth Hughes	Barry Whittingham
	Jerry Williams

Specific questions can be addressed to the following authors of the guidance:

Jonathan Berman and Michael Wright, Greenstreet Berman Ltd
Tel: 0118-931-9609 Fax: 0118-931-9607 Email: jonathan.berman@greenstreet.co.uk
michael.wright@greenstreet.co.uk

The preparation of this guidance document, based on the work of the HEDMG, has been sponsored by the UK Health and Safety Executive.

Acknowledgements

The authors and contributors also wish to thank the following organisations for their assistance during the drafting of this guide: Health and Safety Executive, Transport for London, Railtrack Safety and Standards Directorate, Shell Exploration and Production, Maritime and Coastguard Agency, BNFL plc and British Energy. We would like to acknowledge the unpublished work of Paul Hollywell completed under the Nuclear Research Programme (ref 6) which has been drawn on in this guide.

CONTENTS

Introduction

- Have you ever made a mistake because you thought someone else had done something when in fact they had not?

- Have you ever got to the end of a series of actions, and then realised that you had missed out the same step on each one?

- Have you ever been a part of a group who have all missed an obvious issue when considering a problem?

If so – you are aware of human error dependency.

Human error dependency is particularly serious because it can "defeat" multiple independent safety defences, thereby undermining safety in what would otherwise be a high reliability system. This is demonstrated by cases where independent safety systems have failed simultaneously, teams of operators have misdiagnosed emergency situations and staff have relied on inoperative warning systems.

This guide is aimed at two audiences:

For management it provides:

- an introduction to dependency issues, to explain what they are and why they arise

- an explanation of the impact of human error dependency and the need to take proper account of it throughout all aspects of the system lifecycle - design, management, operations, maintenance, plant modifications, and decommissioning

- a framework for identifying and assessing the significance of dependencies associated with human actions and activities.

For analysts and designers it provides:

- a framework for assessing the relative contributions to dependency of different aspects of the tasks and situations;

- guidance on defences against dependency;

- a method for identifying and assessing potential error dependencies.

The guide draws on practical examples of error defences and accident case studies to show that it is practical to guard against these types of errors.

How to use this guide

Human Factors specialists with the aid and input of risk analysts and safety managers have produced this guide. It is intended for use in–house by organisations and as such the contents can be freely copied and modified for internal use. Indeed as with all other forms of risk assessment, it is the organisation's responsibility to ensure a suitable and sufficient risk assessment is completed.

The first two sections explain the nature and impact of dependent errors with the aim of enabling readers to understand how such errors may affect their operations.

The third section provides an overview of the role of managers in assessing and controlling dependent errors.

The fourth and fifth sections are aimed at persons involved in assessing safety and developing safety recommendations. They provide a method for identifying dependent human errors, assessing their likelihood, consequences and causes as well as potential defences.

Worked examples are given in the Appendix.

As this guidance has been developed for application across a wide range of industries, it does not provide an exhaustive set of solutions and examples. It is expected though that readers will be able to acquire a sufficient understanding of the issues from this guide to be able to assess their own operations and develop their own solutions.

Moreover, it is expected that users will wish to integrate the ideas and methods contained in this guide into their own risk assessments, reviews and audits. We do not suppose that users of this guide will carry out a stand-alone assessment of human error dependency. Accordingly we have sought to structure the assessment method around the steps commonly followed in risk assessment.

The impact of dependent errors

High-hazard operations and activities require commensurately high standards of safety and reliability. One way of achieving these standards is to have multiple *independent* safety "defences", so that even if one fails, another should prevent an accident. These "defences" need to be independent, whereby the failure of one will not lead to the failure of another - otherwise the benefit of providing multiple defences is greatly reduced.

The benefit of multiple safety defences is shown by the simple example of having two instead of one pressure relief valve on a pressurised vessel, each of which is capable on its own of keeping the vessel safe. With a valve failure rate of (say) 1 in 1,000, the provision of two (independent) valves would give a combined failure rate of 1 in 1,000,000. In other words, the likelihood of <u>both</u> valves failing at the same time, and therefore leaving the vessel with no protection is one in a million.

In the same way as many systems have multiple "hardware" safety devices, such as machinery guards and automatic shutdown devices, the reliability of many safety critical operations relies on "administrative", people-based and procedural controls (see Box 1). In some cases there may be a combination of "hard" and "soft" defences, such as automatic warning systems combined with a train driver monitoring (say) railway signals. In all cases, the aim is to reduce the possibility of an accident to a very low level by designing a system that would only result in an accident if multiple independent failures were to happen simultaneously.

Box 1: Common examples of "independent" and "diverse" human safety defences

- Appointing supervisors to make independent checks of work completed by fitters
- Having a "buddy" check your personal safety equipment before attempting a hazardous task
- Having a team of people diagnose a problem rather than relying on one individual
- Having two pilots operate an aeroplane rather than one
- Train drivers monitoring railway signals along with an automatic warning system

However, there have been serious incidents and disasters (see Box 2) where the provision of multiple defences has either offered no additional protection or, in some cases, reduced the reliability of defences. These cases demonstrate that, under certain conditions, a "dependency" develops between the actions of people and / or the operation of a system and other people. Such dependencies can undermine the whole basis on which an operation is thought to be "safe". At best the benefit of multiple defences is lost.

"Group think" is a good example of dependency, where people, such as control room staff or pilots, wrongly accept each others judgement without question – such that an error made by one person is unwittingly carried through by others. This negates the value of a team of people exploring alternative opinions and detecting each other's errors and misconceptions.

Box 2

Recalling the Clapham Junction railway disaster, the required independent verification of wiring was not completed because of the supervisor's "good opinion" of the technician's quality and because it had become common practice to expect technicians to check their own work – thereby allowing errors to remain undetected. Such "checking" oversights can lead management to place undue confidence in the level of operational safety, as they will remain unaware of the true level of error.

The phenomenon of group think was observed during the Three Mile Island nuclear power incident, where it took a new shift of operators to spot an anomaly that the first shift had overlooked, in part due to a "fixation" on other explanations of the abnormality. A similar phenomenon appeared more recently during the Kegworth air crash when the Captain accepted the judgement of the co-pilot without adequately questioning – resulting in the wrong (i.e. good) engine being shut down. It had been assumed that the two pilots would each assess the situation independently, and hence a mistake by one pilot would probably be detected by the other pilot. However, in practice it can be seen that their decisions were dependent on each other.

Another example involves "mind set", where a person, having made one error, repeats this error after becoming "convinced" that this action "must have been right". Such an error was observed on a nuclear power site when a person was sent to change over the fuel supply from a low duty tank to a standby fuel tank for an emergency generator. By mistake he went to the wrong valve on the standby tank, namely the inlet valve for filling the standby tank rather than the outlet to the generator. However, he had expected that the valve would be locked, and finding that he had a key that fitted the lock, he decided that this was the correct valve and opened it (i.e. leaving the correct valve shut). It would appear that he got into a mind set, believing he had correctly opened the outlet valve on the standby tank, the operator therefore compounded the mistake by closing the equivalent inlet valve on the low duty tank. Consequently neither of the tanks was able to supply the generators when required.

The impact of such dependencies on overall reliability is illustrated in Figures 1 and 2 using the example of a supervisor checking that a maintenance technician has correctly calibrated a piece of equipment. In the first figure the two errors are independent as the supervisor is considered routinely to check the calibration. In the second figure the supervisor assumes the technician is competent, perhaps due to the technician's many years of experience and qualification, and consequently systematically fails to check the calibration, perhaps just asking the technician whether the equipment has been calibrated. In the latter case of (assumed) complete dependence, the overall error likelihood is the same as the likelihood of technician error. Thus, the dependency leads to a thousand-fold increase in the overall likelihood of error.

It is the reason why the supervisor fails to check the technician's work that makes the issue of dependency significant. If it is simply that the supervisor is not aware of his responsibilities, this is a predictable error, and its likelihood can be assessed, and then reduced through appropriate training etc. However, if the supervisor's behaviour is due to his perception of another person's capabilities, it becomes more difficult to predict the likelihood of this form of error interaction.

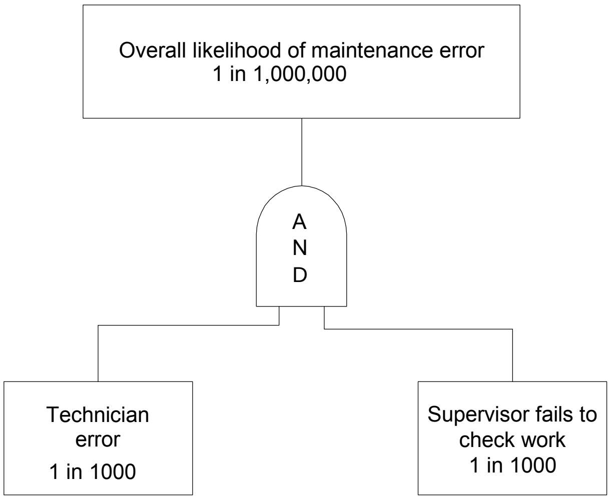


Figure 1: Independent Maintenance Errors

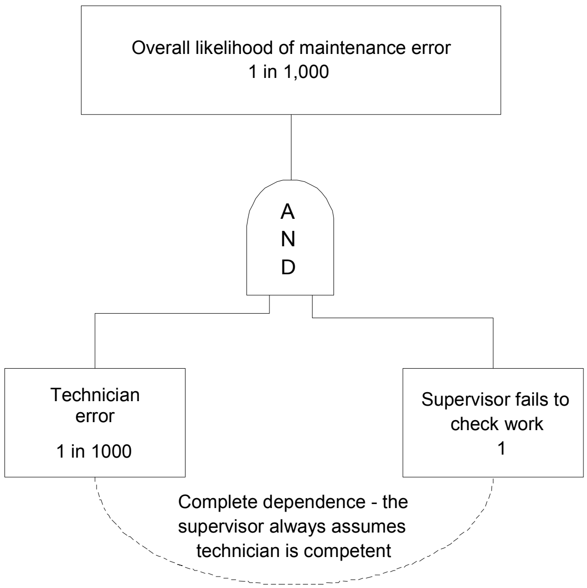


Figure 2: Dependent Errors

Another type of dependency is where people come to rely on (say) a new automatic warning system (see Box 3), such that when that fails they lack either the vigilance or competence to work unaided. Paradoxically the reliability of the operator may be inversely related to the reliability of the automatic system – the more reliable the automatic system, the less you may be able to depend on the operator.

Box 3: Over-reliance on integrated navigation system led to grounding of cruise vessel.

The 1995 grounding of the Royal Majesty passenger vessel with 1,509 persons on board about 10 miles east of Nantucket Island, Massachusetts (causing $7m damage and lost revenue) demonstrates the perils of relying on automatic warning systems. The Global Positioning System (GPS) had become partly disconnected causing the navigation system to switch to an approximate position mode of operation. This mode calculates an approximate position based on a number of factors, and does not provide accurate location information from the satellite. The auto-pilot continued to react to the GPS, causing an increasing deviation from the planned track. The watchkeepers relied on the automated features of the integrated bridge system. There was no cross-checking of the GPS derived ship's position and they relied on the position-fix alarm for warning of deviation from the vessel's intended track.

A fundamental rule of safe navigation is always to check the primary method of navigation by an independent source. Radio aids, astro navigation, visual fixing and use of the echo sounder were all available in this case. In addition, it is normal practice to take special care when making a landfall (coming into port).

Despite their experience and qualification the watchkeepers remained unaware of the deviation for 34 hours - until the vessel grounded! This was in part due to inadequate training in the technical capabilities and limitations of the system, which normally determine a ship's position with great accuracy.

The requirement for multiple administrative checks may unwittingly create a situation where everyone relies on someone else to complete a proper check – such that no one takes personal responsibility for checking. One such example was illustrated at a hospital department that dispensed drugs, where one nurse was meant to check what another nurse had dispensed. It transpired that dispensing errors were being made because everyone relied on others to do a proper check. Subsequently, responsibility for checking each prescription was placed in the person who dispensed the drugs – i.e. self-checking, and the incidence of mis-dispensing reduced. This type of dependency is of particular note when it is recognised that incident investigators often recommend additional administrative checks in the aftermath of individual errors.

Concluding point

There is an ever-increasing pressure to improve standards of safety at the same time as reducing staff costs. This is often achieved by using new technology and / or improved staff competence to balance a reduction in the level of supervision and staff. These and other trends show that there is a continued and perhaps even greater need to consider the interaction of safety "defences", i.e. how can you ensure that steps taken to improve safety do not adversely impact the reliability of other defences? For example;

- How might an improvement in the standard of staff competence affect the behaviour of supervisors?
- How might the introduction of automatic systems effect staff vigilance?
- How can you ensure colleagues continue to monitor each other's work and challenge possible errors even after they have developed a sense of mutual trust and confidence?
- How can you ensure administrative controls are effective?

There is also a general requirement to carry out suitable and sufficient risk assessment, having proper regard for the possibility of human error. In the situation where the provision of additional safety defences and checks may actually adversely affect other defences it is important to ask, "How do you factor human error dependency into your risk assessment?" Otherwise risk assessments may make overly optimistic assumptions about the benefit to be gained from (say) administrative checks and thereby underestimate the risk of incidents occurring.

This guide aims to help managers and specialists answer these points by providing an understanding of the phenomenon of human error dependency and how to manage and guard against it.

Types and causes of dependent errors

Defining error dependency

Dependency is used as a general term to describe the situation where the probabilities of failure of 'independent' components are not in fact independent, but are in some way conditional. **Human Error Dependency** (HED) is one particular form of dependency. HED exists wherever the probabilities of human actions or errors, or series of actions or errors, are linked together more closely than if they were random events (i.e. their probabilities are conditional).

The term Human Error Dependency is used in the context of three forms of dependency, of which we are only concerned with one in this guide.

> The form of dependency we are concerned with in this guide is where the probability of an error is dependent on other actions, behaviours, systems and operations. There is a need for some form of "coupling mechanism" to exist between the error and other events, errors, operations and people - such that the occurrence of one influences the likelihood of the error.

The term is also used to describe two other forms of "dependency" defined below which are important reliability factors. These forms of dependency are not considered as issues in their own right in this guide because they are amenable to "standard" Human Factors assessment and risk assessment.

1. Common cause errors, where (for example) a series of people commit one or more errors due to (say) commonly poor training or a poorly designed control panel. In this situation the probability of each person committing an error is dependent on a common condition, namely the poor training.

2. Human induced (inter-system) dependency, where human action creates a "dependency" between two or more otherwise independent hardware systems, such as a poorly trained technician making the same error on each of four standby generators such that they all fail to start when required.

Not discussed in this guide as issues in their own right

In both of the latter cases, two or more errors may occur but they may not be "dependent" on one another. However, where the human induced (inter system) dependency occurs due to dependent human errors, these are within the scope of this guide. For example, a technician makes an uncharacteristic slip when maintaining one standby generator. When the technician comes to the next generator they carry out the same action, as they remember doing it that way. Likewise, there may be some dependency between errors that also happen to share common causes. For example, poor instrumentation may cause two operators to misread a dial at the same time as a dependency between the two operators leads one operator to trust the reading of the other.

Also, factors that give rise to common cause errors are of concern if they also affect the possibility of people being influenced by the actions of others or, their own previous actions. For example, obscure instrumentation may deter one person from checking the judgement of another person and thereby contribute to a dependent human error.

What causes human error dependency?

There are a number of ways in which human errors may become dependent on other actions, phenomena and operations. Each of these can be described as a form of **"coupling"**. For example, pilots' decision making is "coupled" by the level of faith they have in each other's expertise. However, the likelihood of such a "potential" coupling to be realised is influenced by factors such as the degree of stress posed by the situation. For example, the stress posed by an emergency might lead pilots to take each others word at face value due to a desire to take rapid control of the situation. Thus, along with different forms of "coupling" there are **"contributory factors"** (sometimes referred to as Performance Shaping Factors) influencing the likelihood of such couplings occurring. Finally, as with all forms of error, people might **detect and correct** their errors. For example, out of limits alarms may alert operators to the unexpected consequences of their error.

These terms are elaborated overleaf as well as being illustrated in Figure 3.

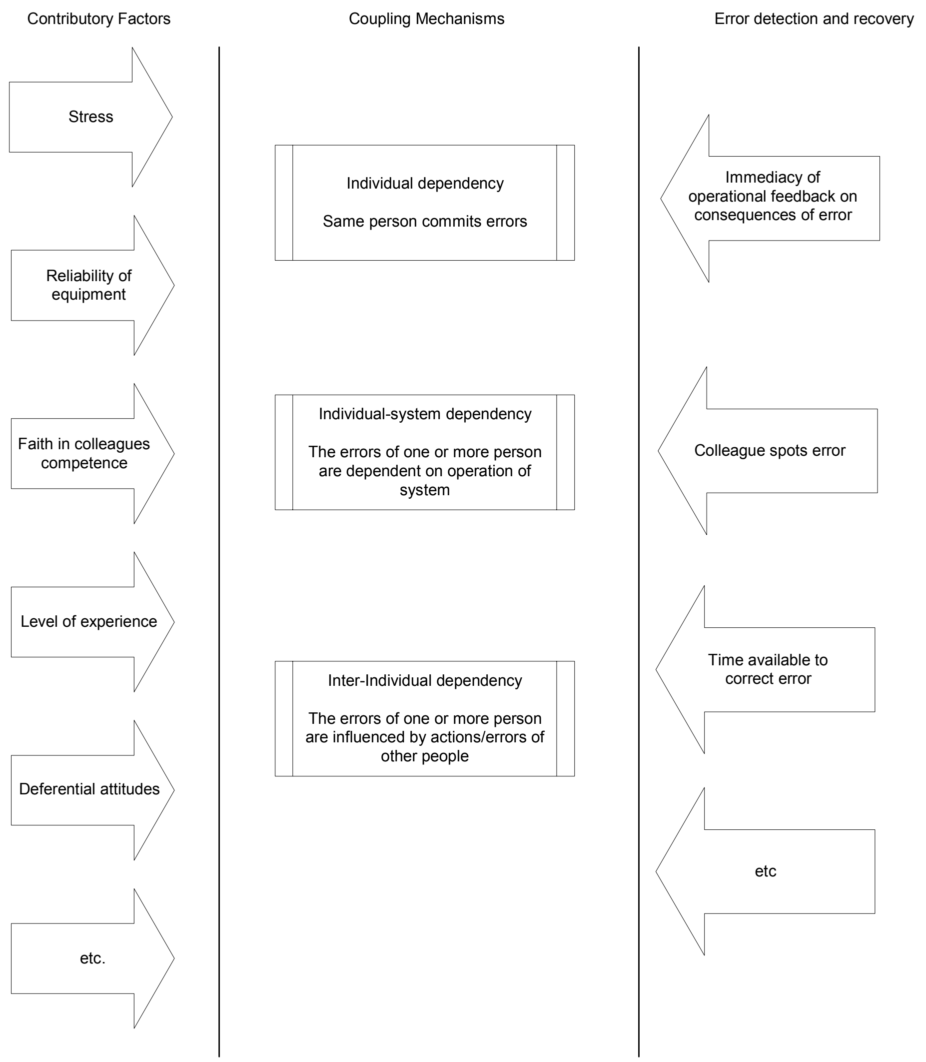


Figure 3: Types and causes of dependent errors

Individual dependency

This category covers situations where there is the potential for psychological / physiological factor(s) to cause the operator to make and / or repeat an error, or at least creates a conditional probability of error. One example was noted in the introduction, where an operator apparently convinced himself that his initial action "must have been right", thereby getting himself into a "mind set". The latter type of error is particularly likely if the thought of making an error makes you feel "uncomfortable".

Other modes of individual dependency include:

- Overconfidence in own ability - This is the tendency to place a higher level of confidence in one's own ability than is justified, perhaps because the situation has never arisen where your ability is challenged. It can lead to people omitting checks on their work, not being diligent in reviewing one's own work etc. This is illustrated in Case Study 1.

- Focusing (tunnel vision) - This is the tendency to only seek information that confirms your initial perceptions and / or be unwilling to re-analyse beliefs in the face of new information. Such a tendency is related to a wish to avoid uncertainty and / or mental "conflict" that may occur if we acknowledge information that contradicts our beliefs. In this situation the probability of a person failing to respond to apparently unambiguous information would be much higher than may appear at first sight.

- Confirmation bias – A reluctance to change one's mind in the face of contradictory evidence (thereby avoiding the anxiety created by "knowing you have got it wrong").

- Complacency – The conscious repetition of a violation or repeated lack of care and attention because such behaviour has not led to an incident before.

Case study 1

Following maintenance on the cooling system of a diesel driven pump, the system had to be re-commissioned and then the pump restarted. Once running normally, the pump temperature had to be regularly monitored and logged. The maintenance, re-commissioning and temperature monitoring were all performed by the same person.

On one occasion, having restarted the pump, the over-confident operator failed to log its temperature, assuming the cooling system to be functioning correctly. However, due to a valve being left shut, cooling water was not getting to the pump. Eventually the pump overheated and tripped due to a high temperature.

The second two modes of individual dependency may be more likely when people are executing complex plans and procedures, as the emotional "cost" of changing direction is high if you have made a large personal investment in the plan. This can lead to "escalation of commitment" when individuals continue on their chosen course in the face of negative feedback whilst another person (who was not party to devising the plan) would have changed course by now.

Individual – system dependency

Another type of dependency is illustrated by the Southall Train disaster, as described below in Case Study 2, where the driver apparently became reliant on new technology. In this example, the likelihood of driver error was affected by (and thereafter dependent on) the introduction of the automatic warning system. This mode of dependency involves one or more individuals forming an attitude that the system is sufficiently reliable that they no longer need to monitor operation of the system or maintain past levels of diligence. Such errors have been discussed in terms of "ironies of automation" – whereby the supposed benefits of automation (i.e. better reliability) are reduced due to an unintended decline in operator reliability.

Another example further illustrates how this mode of dependency could appear, namely the falsification of fuel pellet records by operators at the BNFL MOX Demonstration Facility in Sellafield. The HSE report indicated that operators regarded their manual inspection of a sample of fuel pellets to be unnecessary due to the high reliability of automated checks. In addition, the manual inspection was a highly repetitive unstimulating task completed in a poor ergonomic environment, and operators had not been advised as to the importance of the manual inspections. Accordingly, some operators falsified fuel check records by copying old inspection data.

Case Study 2: The Southall train disaster
Train driver become dependent on the security of an automatic warning to alert him to signals at danger

On the 19th September 1997 a high-speed train went through a signal at danger and collided with a freight train crossing the line near Southall, causing seven deaths and 139 injuries.

The inquiry found that the driver had probably become reliant on the automatic warning system to alert him to signals at danger, causing him to be less vigilant. The AWS normally emits an auditory signal when signals are passed at yellow or danger and has to be acknowledged, otherwise there is an automatic brake application. On this occasion though, the AWS had been isolated due to a fault and so provided no warning or brake activation. The inquiry indicated that the tendency to rely on the AWS meant the driver was less vigilant even when the AWS was inoperative, as stated below:

"While drivers accepted the traditional view that Automatic Warning System was merely an "aid" the reality was somewhat different, as the Southall accident has demonstrated. While it must be emphasised that the primary duty of a driver is to keep a vigilant lookout at all times, there must be a tendency for drivers, to an extent, to become dependent on the security of an automatic warning on the approach to every signal…. The absence of AWS was a contributory factor to the failure of Driver Harrison to respond to signals…. at the crucial time". (p 86, The Southall Rail Accident Inquiry Report, 2000)

Thus, whilst the automatic systems might provide higher standards of safety when operating, the likelihood of error whilst driving without automatic warning is higher having previously relied on them than if they had not been provided.

Inter-individual dependency

This can occur where two or more people are involved in completing a task, such as a team of control room operators, pilots, or supervisors checking the work of team members. Inter-individual dependency is typified by some of the effects which teams can have on individual performance, such as peer pressure, conformity, false consensus, risky shift, etc. There are a number of forms of inter-individual dependency. These include:

- Failing to check another person's work;
- People may accept the opinion or judgement of colleagues without question, rather than developing their own opinion, offering alternative opinions or challenging other peoples' views;
- Changing one's own opinion to "fit in" with other people.

This can occur for a number of reasons.

- Mutual trust: An individual accepts the judgement of another due to their faith in their competence.
- Group think: A group of people arrives at a consensus without adequately evaluating all alternatives, perhaps with individuals' self-censoring doubt and thereby giving an illusion of unanimity. Members' desire for unanimity and "team spirit" may override their motivation to appraise alternatives, leading to a suppression of disagreement to preserve group solidarity and a wish to avoid "rocking the boat".
- Deferential attitudes: Social pressures may operate to dissuade individuals from participating and contributions from low status members may be rejected.
- Failure to share information leading to either a false consensus (thinking you have agreed when in fact you have not) or pluralistic ignorance (thinking everyone has the same information, when some people are not aware of key facts)
- Collective rationalisation or a wish for conformity may lead people to "go along" with group pressures – this can lead to a false consensus, as individuals do not wish to be the "odd one out".
- Risky shift involves individuals placing greater confidence in their opinion or a chosen line of action when it appears to have majority support ("if everyone else agrees I must be right"). Individuals are willing to accept a greater risk when working as part of a group than when required to take sole responsibility for a decision.

Case study 3 provides an example of one person acting, without question, on the word of another. Case study 4 entails one person presuming that another person is competent and so failing to check their work. In situations where people are placed in the role of checking the performance of another, then factors such as trust reliance and subordination may reduce overall performance. Indeed there may be some situations where such factors become dominant with the result that the overall performance with two operators is actually worse than the performance of a single operator.

Case Study 3: The Kegworth aircraft crash
Flight commander accepted first pilot's diagnosis and shut down wrong engine without checking indicators himself

After an uneventful take off and climb the crew suddenly heard an unusual noise accompanied by vibration, followed by a smell of fire and possibly some visible smoke in the cockpit. This combination was interpreted by the pilots as evidence of a serious engine malfunction, with an associated fire, and appears to have driven them to act very quickly to contain this perceived condition without assimilating from the engine instruments any positive indication of malfunction.

When asked which engine was at fault the first officer half formed the word "left" before saying "right". The first officer then accordingly (but wrongly) throttled back the No.2 (right) engine. The misdiagnosis was reinforced by the noise and shuddering ceasing when the No.2 engine was throttled back, although an indicator still showed high vibration levels. They failed to notice continuing maximum reading on the No.1 engine vibration indicator, fluctuating fuel flow and continuing vibration felt by passengers. The shuddering and noise probably ceased because the autopilot had been disengaged, thereby decreasing the demands on the No.1 engine.

The Commander is thought to have believed that the first officer had seen positive indications on the engine instruments, and accepted the first pilot's assessment / diagnosis.

The speed with which the pilots acted was contrary to both their training and the instructions in the Operations Manual, both of which required them to evaluate all evidence available before taking action. If they had taken more time to study the engine instruments it should have been apparent that the No. 2 engine indications were normal and that the No. 1 engine was behaving erratically. The commander himself may have had a better chance to observe these abnormal indications if he had not disengaged the autopilot.

"Both pilots reacted to the emergency before they had any positive evidence of which engine was operating abnormally. Their incorrect diagnosis of the problem must therefore be attributed to their too rapid reaction and not to any failure of the engine instrument system…"

In the terms of this guide, it is important to consider whether the commander would have checked the flight indicators himself if the first officer had not voiced an opinion. The presence of two pilots did not increase the level of reliability, as the commander simply acted on the word of the first pilot.

Case study 4: A freight train derailment
Train driver assumed that the guard was competent and so failed to check guard's investigation of an alarm.

A freight train passing an axle hot box detector initiated an alarm. It was reported to the train guard that the hot axle box in question was on a pulpwood wagon. The train was stopped and the guard investigated but went to the wrong wagon and hence found no abnormality. Shortly afterwards the train passed another hot box detector which alarmed. The guard went to investigate, checking all axles, but did not detect the faulty axle box. Whereas the driver should then have independently checked the axles, he decided that the guard was competent, and hence it must be another false alarm. Shortly afterwards the axle box failed and the train derailed.

The driver's perception of the guard's competence and the previous apparent false alarm led him to omit the required independent check of the alarm.

Contributory factors

As illustrated in Figure 4, the likelihood of error dependencies occurring is influenced by a variety of factors. Some of these factors are specific to particular modes of error, whilst other factors are common to all modes of error dependency.

For example, the "culture of deference" in an organisation is likely to influence the extent of inter-individual dependence but is unlikely to influence individual-system dependency. On the other hand, a lack of time, poor motivation, awkward / unreliable instrumentation and so on may all contribute to a tendency to avoid double checking your own judgements, actions of colleagues or operation of systems. In one sense, any factor that has a bearing on human performance may also have a bearing on the possibility of dependent errors. In the case of the Kegworth aircrash the poor quality and past unreliability of instrumentation may have contributed to the commander failing to double check the co-pilot's judgement of which engine was faulty. Thus, on the one hand you trust your colleague's judgement and on the other hand it is difficult to double-check the situation for yourself.

A fuller listing of factors is given later in this guide as part of the HFRG method.

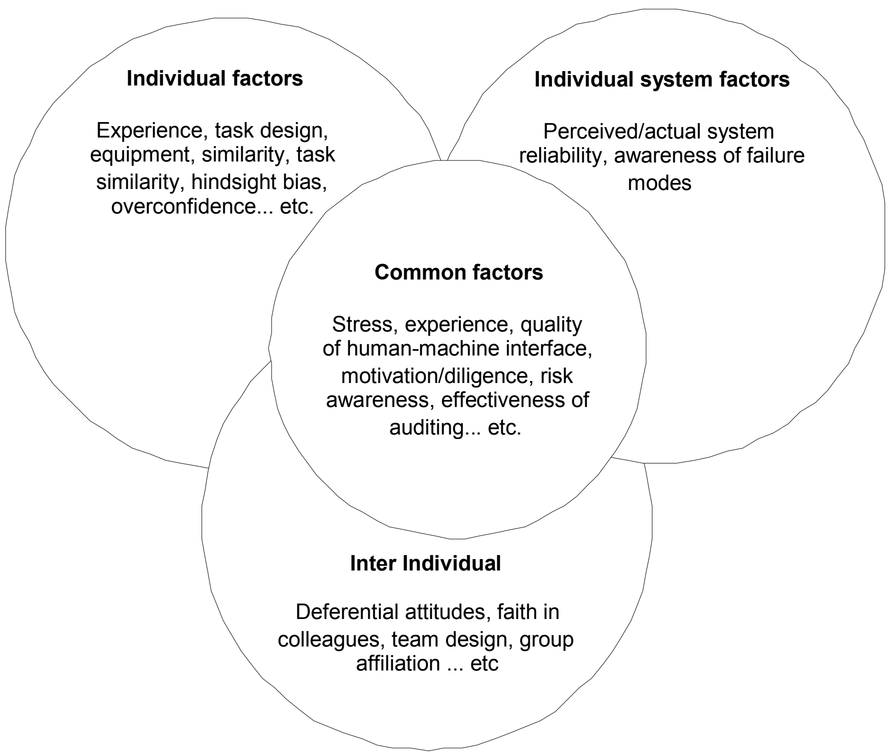


Figure 4: Examples of contributory factors

Detection and recovery of dependent errors

As with all forms of human error, people may or may not detect and correct their mistakes. Turning back to the example of the Royal Majesty passenger vessel, described further in Case Study 5, the remoteness of the GPS receiver and the short duration of the audible alarm which sounds when switched to the dead reckoning mode, contributed to the failure of the watchkeepers to notice the change. Some of the factors affecting the likelihood of detecting and correcting errors will be common to all forms of human error, such as:

- Is there enough time between committing the error and its consequence to intervene?
- Are there "obvious" indications of the error, such as an audible alarm?

In the case of dependent errors, it is important to consider how the mode of error may influence the likelihood of detecting it. In particular, in the absence of obvious indications of an error, dependent errors may go undetected if all persons present are party to the error as no one will be expecting such errors.

Case study 5
Inadequate alarm failed to alert crew to erroneous change in course

As previously noted the crew of the Royal Majesty passenger vessel over-relied on the automated features of the integrated bridge system, failing to notice the course deviation or the partly disconnected Global Positioning System.

Aside from their over reliance on the automatic system, the remoteness of the GPS receiver and the short duration of the audible alarm which sounds when switched to the dead reckoning mode, contributed to the failure of the watchkeepers to notice the change.

Concluding point

Whilst there are many forms of dependency, human error dependency primarily concerns the situation where some form of individual, inter-personal or external factor creates a "coupling" between two otherwise independent actions or events. These errors can be distinguished from common cause errors in that the occurrence of one error or phenomenon has a direct bearing on the occurrence of another error – whilst common cause errors simply share a common origin such as poor training or wrong procedures. Contributory factors such as the quality of human-machine interfaces may influence both the likelihood of dependencies occurring and the likelihood of such errors being detected. Operational factors such as the time available to detect and correct errors will influence the likelihood of errors leading to an actual incident.

The role of management

This section of the guide provides advice on what steps managers, such as operations managers, engineering managers and safety managers, might take to assess and control human error dependency. The guidance focuses on policy level issues that managers should have regard for.

Management is responsible for setting policy, defining required performance standards and ensuring appropriate arrangements are implemented to achieve and maintain these standards. In the same way that organisations should explicitly assess and guard against the potential for hardware failure, they should equally assess and guard against error dependency. In addition, as many forms of error dependency arise from the style of supervision, management has a wider, less tangible role in promoting a culture that guards against human error dependency. In the context of human error dependency, these roles translate into a set of tasks as described below. A checklist is given that encapsulates these.

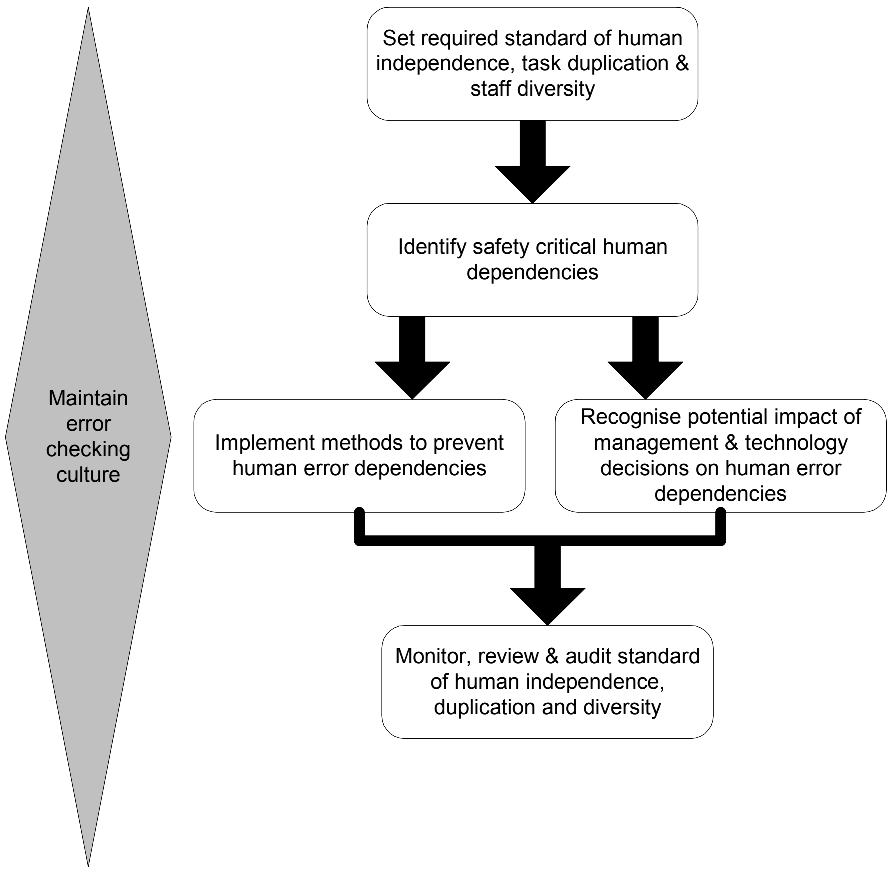


Figure 5: The management of human error dependency

Setting standard of duplication, diversity and independence

As noted in the introduction, the levels of duplication, diversity and independence required depend on the level of potential risk posed by operations. Higher risk operations require higher levels of duplication, diversity and independence to ensure that a single point failure does not cause an accident. Accordingly, a judgement needs to be reached regarding the level of duplication, diversity and independence the organisation needs to achieve and hence the importance of guarding against human error dependency. This judgement should be based on an understanding of risks and consequences of operational failure, with higher levels of independence typically required for higher risk activities.

Identify safety critical human error dependencies

Where the achievement of safety standards depends on a "defence in depth" strategy, the organisation should identify safety critical tasks that are sensitive to dependency and ensure proportionate steps are in place to prevent or reduce the likelihood of dependencies emerging. For example, where supervisory checks are proposed as a means of ensuring (say) adequate workmanship on safety critical systems, such checks should be classed as safety critical and managed accordingly.

As part of this, due allowance should be made for the possibility of human error dependency in risk assessment, so that unrealistic assumptions about the effectiveness of (say) supervisory checks and secondary checks are avoided.

Implement methods to prevent human error dependencies

Management should identify methods for preventing human error dependency and ensure these are implemented effectively. For example, it is recognised within the aviation sector that pilots may (wrongly) defer to colleagues. This is countered by the technique of "Crew Resource Management" that develops effective team working skills amongst crew, including a non-deferential attitude. Thus, in aviation, a method specifically aimed at a particular source of dependent errors has been developed and implemented.

Recognise potential impact of management and technology decisions on human error dependencies

Many "routine" business decisions may incidentally impact upon the likelihood of human error dependencies, such as automated control systems decreasing operator vigilance or new "team" based ways of working eroding the effectiveness supervisory checks. Management should recognise the potential of such changes to impact the true level of duplication, diversity and independence, and take account of these.

For example, in the event that new automatic warning systems are introduced the question "What should staff do when automatic systems are not available" should be raised. It is possible that personnel will become reliant on automatic systems leading to the erosion of skills and / or loss of vigilance. In the event that the system is unavailable, it might be that staff will perform inadvertently at a lower standard than they did before the introduction of automatic systems, and may have a lower level of vigilance and skills. One option is to adopt "as policy" the practice of withdrawing the plant / railway train etc from service in the event of system failure even if staff would previously have operated the process manually. Another option is to ensure staff maintain skills by providing regular hands-on experience by use of either simulators or manual operation, or require additional staff to be deployed when automatic systems fail. A third option may be to make the detection of system failure / error obvious – to address low levels of staff vigilance, such as prominently displaying aircraft route so that course deviation is obvious at a glance.

Monitor, review and audit standard of human independence, duplication and diversity

Rather than assuming supervisory checks etc are operating effectively, arrangements should be put in place to proactively test the standard of staff performance. For example, the conduct of supervisory checks could be externally audited.

Maintaining an "error checking" culture

As previously noted, the attitudes of staff, their awareness of risks and appreciation of the rationale behind "secondary" safety controls influence many forms of human error dependency, such as deferential attitudes leading staff to take colleagues judgements at face value. Accordingly, there is a need to recognise those aspects of the organisation's culture that influences such behaviour and manage it accordingly. Two examples are noted below in Boxes 4 and 5.

Box 4: An example from the coastguard – the buddy system

Regardless of rank or period of service, it is a recognised and accepted practice that colleagues check that you have donned your personal safety equipment correctly. An attitude that your equipment should be checked regardless of your perceived or actual level of competence or experience is actively promoted and applauded – to ensure that colleagues are not inhibited from spotting errors by your rank etc. In this way, the culture of the organisation acts as a barrier against personnel presuming that they do not need to check the actions and judgements of colleagues due to their competence or rank.

Box 5: An example from the US Navy

The US Navy reportedly operates a culture that actively encourages personnel to monitor and challenge colleagues actions and decisions regardless of rank - to help ensure that errors are not overlooked due to a deferential attitude.

Key messages

Management has a key role to play in minimising human error dependency – directly by policies aimed specifically at human error dependency and indirectly by ensuring general management / technology decisions and organisational culture do not inadvertently encourage error dependencies.

Management checklist

1. Do managers understand (perhaps via risk assessment) how safety controls, such as administrative checks, automatic warning systems, procedural requirements etc, interact such that the overall level of reliability may be reduced by dependencies between such controls?

2. Have managers formed a clear understanding (perhaps via risk assessment) of what level of "defence in depth", independence and diversity is required to achieve targeted safety standards?

3. Are managers aware of which aspects of the organisational culture influences the likelihood of dependent errors, such as deferential attitudes, trust and peer group affiliation?

4. Are managers aware of which aspects of management, administrative, procedural and hardware arrangements play a significant role in achieving targeted levels of "defence in depth", independence and diversity?

5. Have you recognised the potential for dependencies within risk assessment, such that inappropriate assumptions about the benefit of multiple safe guards are avoided?

6. Are there appropriate checks within the safety management system of the continued integrity of administrative / procedural and other forms of independence, diversity and duplication, such as the verification of supervisory checks on maintenance work?

7. Have the risks associated with breaching / eroding "defence in depth", independent checks etc been effectively communicated to people at all levels of the organisation?

8. Are managers aware of how technical, organisational and administrative / procedural changes may increase the possibility of human error dependencies, such as:

   - New technology eroding staff vigilance / skills;
   - Additional administrative checks eroding diligence of current checks;
   - Refocus of supervisors onto "leadership" tasks eroding conduct of task checking;
   - And so on.

9. Have strategies been developed to identify and manage the potential impacts of new technical, organisational and administrative / procedural arrangements on human error dependency?

10. Are managers aware that behaviour may change over time and that a process of continued review is required to check the integrity of "defence in depth" strategies?

The HFRG error dependency approach

Overview of method

The key steps in assessing human error dependencies are shown in Figure 5. It is anticipated that users of this guide would normally integrate an assessment of human error dependency into other broader assessments rather than complete a standalone assessment of error dependency. Accordingly, the process broadly follows the steps of risk assessment. Some examples of when users of this guide might need to consider human error dependency are given in Box 6. Users of this guide may wish to "tailor" the approach outlined herein to fit their own particular form of risk assessment and /or extract parts of this approach. Guidance is provided herein on the special factors and considerations to take into account in the case of human error dependencies.

Box 6: For example, you should consider the issue of human error dependency upon:

- Introduction of new automatic control systems or other equipment
- Changes in organisational structure, supervisory / team leader roles
- Changes in ways of working, task design etc
- Introduction of new administrative checks and procedures
- During completion of risk assessments, HAZOP, What-if analysis etc
- Auditing and review of safety management arrangements
- Design of processes and equipment
- Reviews of operating / maintenance procedures & practices

The process cannot be applied by rote as it relies on judgement. Therefore, the assessor needs to have a valid understanding of the task and how people behave. This understanding may come from direct experience, such as managers assessing operations within their own department, or indirectly by interviewing operational staff and / or supervisors. In the case of new tasks, techniques such as Task Analysis should help provide an understanding of the tasks.

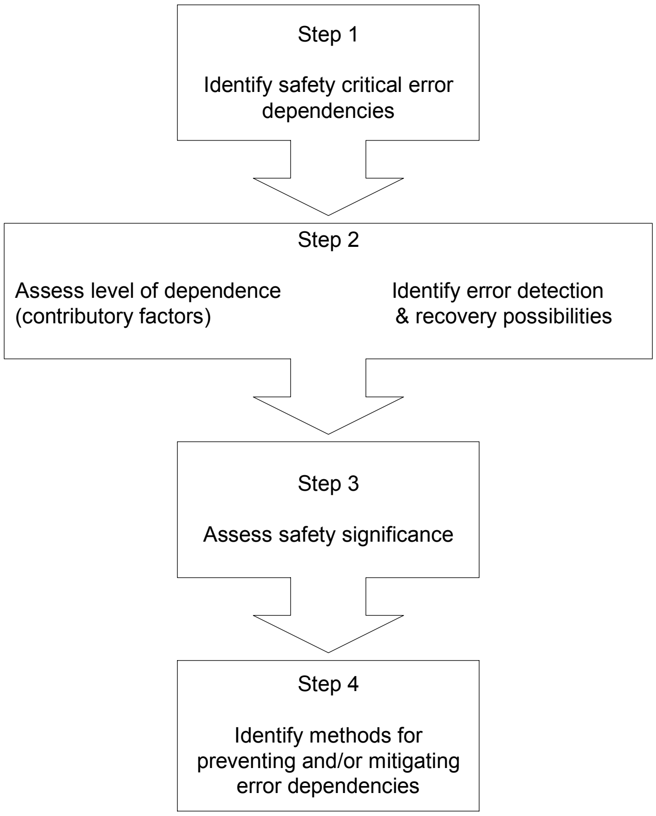


Figure 6: HFRG Human Error Dependency Assessment

Step 1 is comparable to Hazard Identification / HAZOP wherein the analyst identifies the presence of a hazard or the possibility of a fault without appraising its likelihood. The completion of step 1 ensures that only errors that have the potential to adversely impact safety are taken further. It also entails characterising the type of error dependency, thereby enhancing the analyst's understanding of the error(s) in question. Step 1 provides a list of potential error dependencies classified into types, i.e types of coupling mechanisms.

Step 2 is comparable to Hazard Analysis wherein the analyst judges the likelihood of an incident occurring. However, Step 2 involves consideration of those factors that are specific to human error dependency, thereby ensuring an accurate assessment and an understanding of why the dependency may occur. Step 2 provides a likelihood judgement for each error dependency and a list of those factors underlying the dependency.

The judged likelihood is combined with an assessment of consequences in Step 3 to give a risk estimate, thereby allowing decisions to be made about the need to identify methods of preventing these errors. As the consequences of human error dependency may be similar to those of other types of failures, they can be assessed using the same risk assessment methods. Notwithstanding this, guidance is provided on how to characterise the impact of human error dependency on the extent of "system" diversity and independence. This characterisation augments the "standard" assessment of risk and aims to help analysts understand the impact on the system. Thus, Step 3 provides a risk rating for each error and a view of how it may impact "system" diversity and independence.

Step 4 is analogous to the "reduce risk" stage of risk assessment in that it entails identifying methods for preventing or mitigating error dependencies. Those errors judged to pose the highest risk in Step 3 should be given priority. Also, the assessment of the causes of dependency and the type of dependency from Steps 1 and 2 should be taken into account when identifying how best to prevent the error in question. Step 4 provides a set of options on how to prevent or mitigate those error dependencies assessed in Steps 1 to 3.

Guidance on the process of assessment is given below along with a set of tables and figures. As previously noted, it is expected that users of this guide will fit the approach into their own risk assessment methods. Accordingly, whilst we recommend the use of a minimum set of tables, some of the tables (as noted) are optional.

Two worked examples are given in the appendix. The examples illustrate two alternative ways in which the potential for dependency can be assessed. The first example has applied a simpler version of the method, taking each potential type of error dependency in turn and appraising the Contributory Factors as a whole for each error. The second example has applied the optional tables and appraised each Contributory Factor in turn, in respect to a specific task step. The latter approach may be preferred where a complex task and / or alternative solutions are being considered. The former approach may be preferred for less complex tasks.

Step 1: Identifying safety critical human error dependencies

The key question at this stage is "what dependent errors may occur that could have a significant impact on safety?" Thus, the identification of safety critical human error dependencies entails two questions, namely could a dependency occur and, if so, might it impact safety? These questions are elaborated below.

The outputs from this step are shown in the first column of the examples in Appendix A and B. In Appendix A a description is given of each error along with the type of Coupling Mechanism. In Appendix B, the Task Condition is defined using Table 1 along with the error description and Coupling Mechanism.

a) Do task "conditions" present a possibility of dependency?

It is necessary to identify whether the task "conditions" present a possibility of dependency. For example, do two people work together to perform a task or does one person work alone unaided by control systems? If two people work together they could influence one another. But if the two people complete tasks at different times, without directly communicating, their actions may be independent.

The identification of possible dependencies can be achieved by the analyst's judgement, drawing on the explanation of human error dependency in the introductory sections of this guide.

b) Could the dependency impact safety?

Secondly a distinction should be made between those errors that could impact safety and those of no safety significance. It is possible for errors/actions to be dependent but for such dependencies to be of no safety significance. Clearly it is only situations where errors have an impact on safety, reliability or system availability that dependency requires attention. Any dependent errors that do not pose such a risk may be disregarded at this point.

Some examples of significant dependent errors include:

- Errors that negate the independence of duplicate safety systems, such as mis-maintaining two pressure relief valves;
- Errors that could lead to coincident failures of diverse safety systems, such as ignoring fire and smoke alarms assuming that they are false alarms;
- Errors by a team of people that causes mis-diagnosis of an emergency leading to an inappropriate response.

A set of examples is given below (see Box 7) to help identify potential Human Error Dependencies that could have a significant impact on safety. The examples are sub-divided according to their Coupling Mechanism. It should be noted that the examples are not exhaustive and that the assessor should identify and define the type of coupling mechanism with reference to a specific task. It may also be useful to define the mode of dependency, namely Individual, Individual-System or Inter-Individual.

This could include stating the job titles of relevant persons, describing the task and the error, as per the examples defined below.

Box 7: Examples of safety critical human error dependencies

Individual

1. Is one person involved in completing a series of tasks wherein errors may cause safety critical failures?

   For example:

   - A technician commits the same maintenance error on each of a series of independent safety systems.
   - A fitter operates valves on all instances of (say) fuel supplies, such that the individual could repeat the same error across (say) otherwise independent fuel supplies.
   - A surgeon repairs third degree burns on a variety of patients, with the potential of committing the same surgical error.

Individual – system

2. Does one or more person utilise automatic (or semi-automatic) control systems to aid the operation of systems?

   Examples include:

   - Ship's crew presume the automatic navigation system will safely keep the ship on course
   - Midwife relies on a sonicaid (electronic sound detector) to hear fetal heart beat (which may be confused by the sonicaid with the mother's heart beat) without double checking using a pinnard (an ear trumpet)

3. Does one or more person utilise automatic warning systems to aid the detection of hazards etc?

   Examples include:

   - Control room operators fail to check that the process has been shutdown safely by automatic systems
   - A train driver does not monitor the status of signals normally annunciated by automatic warning systems
   - An anaesthetist relies on automatic alarms to monitor vital signs of life during a surgical procedure rather than checking readouts/displays.

4. Do staff replicate tasks already completed by (say) computerised systems?

   Examples include:

   - Technician fails to double check the calibration of automatically calibrated equipment
   - Quality control staff fail to double check the quality of material already checked by computerised equipment

Box 7: Examples of safety critical human error dependencies

Inter-individual

5. Does the completion of a safety critical task involve co-operation and co-ordination of two or more people?

   For example:

   - The successful completion of a complex emergency procedure on a chemical process plant requires good communication and co-ordination between all members of a team of operators, engineers and supervisors.

6. Does the task entail cross-checking of work and/or double-checking of information/ indicators etc?

   Examples include:

   - A supervisor fails to check the maintenance work of (say) fitters and technicians
   - A control room operator fails to check status of indicators already checked by a colleague

7. Are two or more people involved in interpreting safety critical information and making related decisions?

   Examples include:

   - A team of 5 operators and a shift supervisor fail to question the leading technician's diagnosis of a process upset on a chemical plant
   - A flight commander accepts co-pilot's diagnosis of control system fault on aircraft
   - A junior doctor fails to question a consultant's diagnosis of a rare or unusual condition despite believing the consultant has overlooked certain symptoms and an alternative diagnosis.

Optional judgement aid for Step 1

Figure 7 presents a classification of Task Conditions that can be used to help prompt identification of possible dependencies. The classification presents every possible combination of people, task, equipment and time (when tasks are completed) that may occur. The conditions are presented in the form of an event tree. You need to ask if the activity involves the same or different people, then the same or different task and so on. Depending on your answers you are routed down one of the branches of the tree and are led to a certain Task Condition. Examples are given for each possible Task Condition.

There are 16 combinations of:

- Person (same/different);
- Task (same/different);
- Action/Device (same or similar/different);
- Time (same or same shift/different- time is considered to be 'same' if the tasks occur on the same shift).

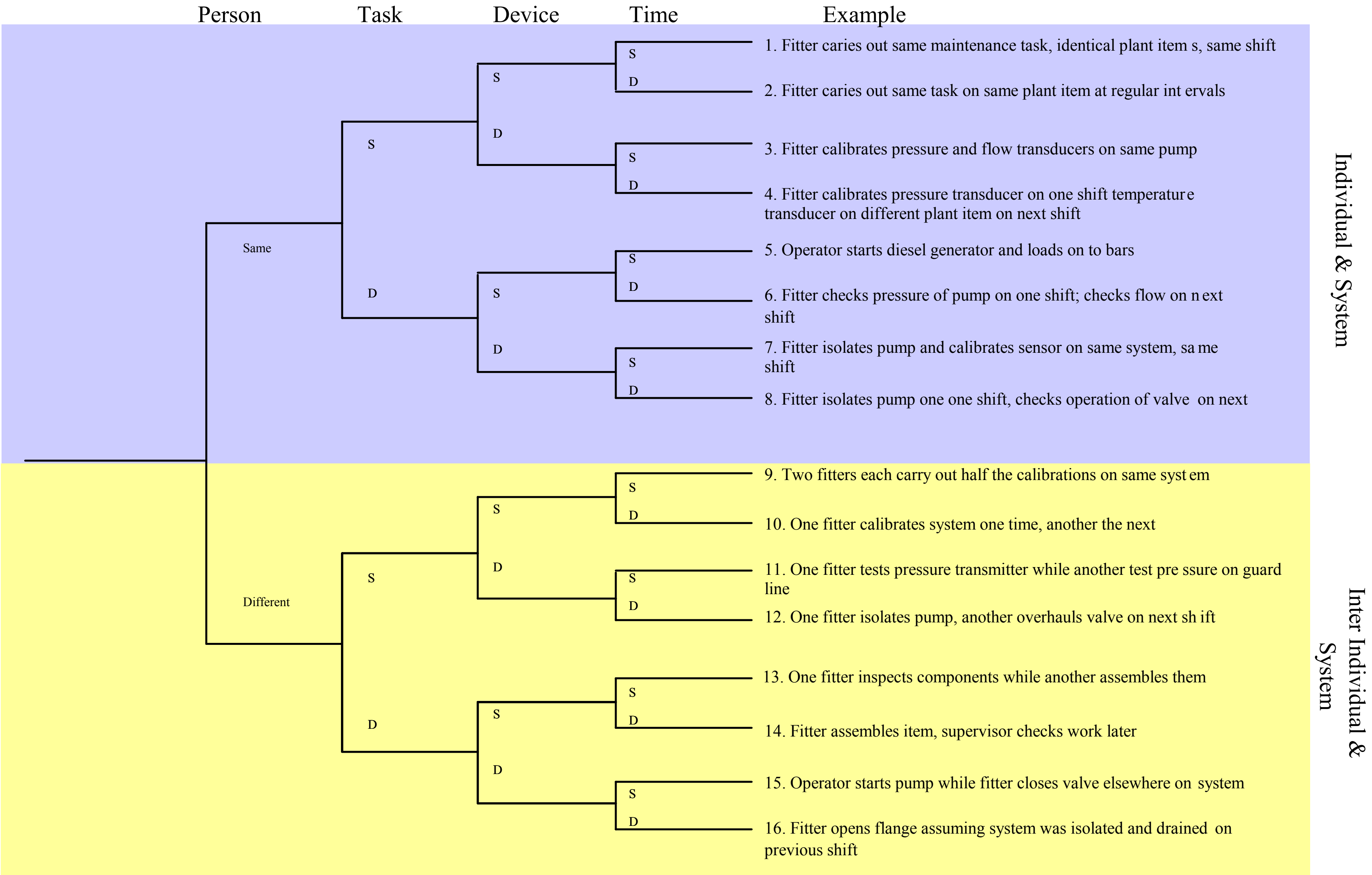
These combinations range from one person undertaking the same task on identical devices during the course of a single shift, to different fitters undertaking different tasks on different systems at different times.

Figure 7 aims to help you describe the task condition in a way that prompts you to consider whether there is potential for human error dependency in each condition. Thus, you may ascertain that in condition 16 (where for example a fitter opens a valve on one section of pipe the day after operators isolate a different section of pipe) there is no potential for dependency, as there is no connection between the two tasks or people. However, the conclusion may be different in another example of condition 16. For example, in the situation where a fitter opens a valve on a section of pipe the day after operators are meant to have isolated it, the likelihood of the fitter checking the isolation before opening the valve may depend on how much the fitter trusts the operators to have completed the isolation.

Also, the susceptibility to dependency effects will be different for each condition, as will the causal factors. In particular, in conditions 1 to 8, there is potential for Individual dependency but not for Inter-Individual Dependency. In contrast, there is potential for Inter-Individual Dependency in conditions 9 to 16 but not for Individual dependency. There may be a potential for Individual-System dependency in all task conditions.

This classification may be of particular value in screening complex tasks or identifying errors for a probabilistic or quantitative risk assessment. In these situations it is particularly important to screen tasks in a systematic manner.

Figure 7: Classification of task conditions (optional aid)



Step 2: Assess likelihood of dependence and error detection opportunities.

Having identified the potential for a dependent error in Step 1, this stage entails a judgement of the likelihood of the dependencies. The likelihood judgement is combined with a judgement of consequences to derive a risk rating in Step 3. An understanding of how and why a dependent error may occur is also required to guide the selection of error prevention strategies (Step 4).

The outputs from this step are shown in the second columns of the examples in Appendix A and B. In Appendix A a judgement of the error dependency is given along with a note regarding the potential for error detection. In the Appendix B example the Contributory Factors are listed and evaluated one by one.

At a minimum, it is recommended that a judgement be made, in the terms given in Table 1, of the likelihood of error dependency causing an incident. This judgement should have regard for what Contributory Factors apply to the activity, the extent to which they may lead to individuals making dependent errors and how likely it is that errors will be detected and corrected before causing incidents.

Table 1: Judgement scale for level of dependency

Level of dependence	Description
Complete	The actions of one person are entirely dependent on the actions / errors of another person or operation of equipment or their own previous actions, i.e. the error will ALWAYS be repeated by the same or another person.
High	On most but not all occasions the individual(s) behaviour will be influenced by the operation of systems or other people.
Moderate	Individuals' actions will often be influenced by the operation of systems or other people.
Low	Individuals' actions will rarely be influenced by the operation of systems or other people.
Not at all	No reason at all can be identified for one person's actions to be influenced by the operation of systems or other people.

The level of detail of analyses is decided at the analyst's discretion, although it is advised that each error be considered separately. More detailed analysis, perhaps considering each Contributory Factor separately (as per Appendix B) may be preferred when completing Probabilistic or Quantitative Risk Assessment, when evaluating a complex task or when alternative solutions are being compared. In the latter case, it might be useful to have a deeper understanding of the Contributory Factors to allow the effectiveness of alternative solutions to be assessed. In the case of "standard" workplace risk assessment a coarser assessment of errors may be preferred wherein a composite view of Contributory Factors is taken (as per Appendix A), i.e. making a single judgement of dependency likelihood for an error rather than considering factors one by one.

In the case of current operations, information required on the behaviour of staff to help guide this judgement may be acquired from:

- Near miss and accident/incident reports
- Interviews with staff to explore their attitudes regarding (for example) the need to double check operation of automatic systems
- Interviews with staff to verify how they "really work", such as whether they really check each others' work
- Results of audits and reviews of staff behaviour and compliance with procedures, such as adherence to task checking requirements

Where you are dealing with new systems and operations, the likelihood of dependencies could be assessed by:

- drawing analogies with comparable situations and lessons learnt from past experience

- completing a task analysis (see reference 1 for further guidance on task analysis) of sufficient detail to allow the nature of the tasks and interactions of people/equipment to be profiled

Optional judgement aid for step 2

A checklist of factors is shown overleaf in Table 2. With regard to Table 2, you should ask:

- Which of these factors apply to the task / error being assessed?
- Depending on your knowledge of the task in question, does the factor(s) induce a low or high level of dependency?
- Are there opportunities for error detection and correction?

If there are opportunities for error detection these may be taken into account by concluding that there is a lower likelihood of the dependency causing an incident, effectively by assigning a lower level of dependency to the error. However, dependency also needs to be considered in the context of error detection. That is, will the likelihood of error detection be reduced by a dependency between the initial error and the likelihood of people detecting it?

As previously mentioned, the assessment can be completed at the level of individual Contributory Factors or at the level of individual errors. These two alternative ways of using Table 2 are illustrated in Appendix A and B. Thus, in Appendix A, a single judgement of the level of dependency is given for each error, such as the ship's crew relying on an automatic radar system. In Appendix A the opportunity for error detection is noted for each error but individual Contributory Factors have not been listed out or assessed separately. In this example, the table simply informed the analyst's knowledge of possible factors and was not used in a "tick box" manner.

In Appendix B those Contributory Factors that influence the likelihood of failing to administer anaesthetic gas are listed out and assessed one by one. The opportunity for error detection is implicitly covered within the assessment of each factor in Appendix B. In this example the likelihood rating for each Contributory Factor is combined with a judgement of the error consequence to derive a Risk Rating per Contributory Factor as part of Step 3.

It would be equally valid to assign a single likelihood rating to the error based on the ratings of the Contributory Factors. For example, if five factors have been rated, the overall rating could be taken to equal the rating of the Contributory Factor with the highest likelihood. Thus, if any one factor is judged to induce complete dependency it can be assumed that this applies to the task or error as a whole, even if other factors do not induce complete dependency. Similarly, if one factor were rated as High with others rated as Low, the overall likelihood would be taken to be High.

Any errors classed as "Not at all dependent" may be dropped from the assessment of dependency at this stage, although it may be important to consider these errors for other reasons.

It should be noted that some of the Contributory Factors might not apply to the task in question. For example, questions regarding the possibility of operators becoming reliant on automatic system will not apply where such systems are not used. Irrelevant factors should be omitted from this assessment.

Also, the checklist is not necessarily exhaustive. Accordingly, you may wish to add other factors to the checklist and incorporate them into the evaluation. However, it does cover the main categories of factors (Individual, Job and Organisation factors) noted in other authoritative guides, in particular HSG48 (reference 2) – although Job factors are split between Individual and System factors in Table 2 and Organisation factors are termed Inter-Individual factors. Thus, the Contributory Factors can be cross-referenced to the Coupling Mechanisms and Task Conditions in Step 1.

Table 2: Assessing the level of dependence (optional aid)

Contributory Factors	**Not at all**	**Low**	**Moderate**	**High**	**Complete**
Individual factors					
1) Individuals are unfamiliar with the task such that it will not be obvious to them that they've gone wrong?					
2) Staff involved in double-checking tasks etc are NOT aware of the importance of such checks in achieving the required standards of safety and reliability?					
3) To what extent do staff perceive the task of double-checking / signing-off (say) permits to work a monotonous duty?					
4) Is reliance placed on staff to check their own work, without an independent check or occasional spot check by colleagues / superiors?					
5) Do staff complete the same or similar tasks in quick succession?					
6) In cases where individuals work on a series of items of equipment, how similar is the design of such equipment?					
7) In cases where individuals work on a series of items of equipment, does the design of controls /valves etc permit the same action to be repeated across equipment?					
8) Could staff wrongly assume that different equipment are operated in the same way?					
9) Could staff mistakenly transfer training / practices from one task to another?					
10) Could staff develop "bad habits", repeating short cuts across tasks without any apparent risk?					
11) Do staff demonstrate a low level of diligence or commitment to complying with procedures etc?					
12) To what extent might self-confidence lead staff to become over-confident, causing them to overlook their errors or consider possibility of error?					
13) Are there reasons to suppose staff will over-simplify a problem, perhaps because it is complicated and they are time pressured, thereby making a series of mistakes?					
14) Are there reasons to suppose staff will become fixated or focused on one particular view of a problem without considering alternatives?					
15) Would the stress of the situation lead people to want to "get on with" the task?					

Table 2: Assessing the level of dependence (optional aid)

Contributory Factors	**Not at all**	**Low**	**Moderate**	**High**	**Complete**
16) Does the task difficulty (workload, awkward equipment and procedures, environmental conditions, time pressure etc) deter people from re-doing a task or checking whether they have done it correctly – even when they suspect they may have done it wrongly?					
System factors					
17) How likely is it that people will become reliant on automatic systems and presume reliability, such that they fail to monitor the situation or check for system failures?					
18) Staff are unaware of the failure modes of automatic systems and how these may be detected / recognised?					
19) To what extent will staff assume that equipment, processes etc are sufficiently reliable to render double-checking of equipment unnecessary, such as checking plant at the start and part way through a shift?					
20) How likely is it that personnel skills and standards of vigilance will be eroded by the introduction of new technology or task duplication, such that they cannot be relied on to perform to the same standards in the absence of such technology?					
21) How likely is it that the use of automatic control and warning systems will mean that people will fail to monitor operations such that when they do need to intervene they do not have an appreciation of the situation?					
22) Does the design of control and instrumentation, complexity of procedures etc dissuade people from double-checking the actions, decisions and judgements of colleagues?					
Inter-Individual factors					
23) How likely are staff to accept the opinion of colleagues without question, perhaps due to a deferential attitude, a presumption of competence or a wish for peer approval / consensus?					
24) How likely are staff to "go along" with the mainstream opinion rather than challenge opinions, check information etc?					

Table 2: Assessing the level of dependence (optional aid)

Contributory Factors	**Not at all**	**Low**	**Moderate**	**High**	**Complete**
25) Does the wish to maintain group cohesion inhibit people from "rocking the boat", expressing doubts, offering contrary information etc?					
26) How likely are peers, supervisors, senior officers etc to presume that the level of competence of other staff is enough to mean they do not need to check for errors or omissions?					
27) How likely are team leaders to solicit and seek out alternative opinions in a way that avoids self-censorship and false consensus?					
28) Are staff aware that they may suffer from "tunnel vision" and "group think" in stressful situations and that they need to retain a degree of individual perspective, situation awareness and actively consider alternative views of what is happening?					
29) To what extent may staff assume that they do not need to double-check (as stipulated in procedures) whether (say) the correct part has been issued by stores as someone else will have done so already or will do so before the part is used?					
30) Do staff assume that colleagues will, at shift hand-over for example, inform them of anything important, rather than actively request information / status information?					
Error detection and recovery					
31) Is time between an error and its consequence so short that people do not have time to reflect on their actions and decisions, thereby detecting their own and others errors?					
32) Is the indication of the status of plant, equipment, and processes etc ambiguous or poorly presented?					
33) Does the task difficulty (workload, awkward equipment and procedures, time pressure) deter people from checking one another?					
34) Do staff mistrust instrumentation?					

Step 3: Assessing safety significance of dependency

Having appraised the likelihood of error dependency in Step 2, it is important to consider the consequence of such errors so that the safety significance can be determined. An assessment of the safety significance of the error helps to guide decisions on the need to implement additional strategies for preventing or mitigating such dependencies, i.e. priority should be awarded to higher likelihood / consequence errors.

Before determining the safety significance of the error it may also be useful to characterise consequences in qualitative terms such as:

- Undetected fault in safety critical equipment
- Failure to correctly respond to impending major incident

Such a characterisation should help form a view of the consequence of the error.

The outputs from this step are shown in the fourth and fifth columns of the examples in Appendix A and B. The simpler example in Appendix A provides a judgement of the consequence and a Risk Rating. The Appendix B example also provides qualitative description of the impact of the error dependency on task diversity and independence.

It is recommended that, as a minimum, a judgement is made of the scale of consequences and a Risk Rating is derived by combining the consequence and likelihood judgements of Step 2 as follows:

Likelihood x Consequence = Safety Significance (risk)

The assessment of consequences can be completed using the same method applied to other causes of failure. This is a matter for the user of the guide. Thus, in the case of "standard risk assessment" it may be adequate to apply a simple scale of consequences, such as Minor, Serious and Major loss. This could be combined with the Level of Dependence scale as follows:

Table 3: Illustrative Risk Rating matrix

Level of dependence	Minor	Serious	Major loss
Complete	High risk		Very High risk
High		High risk	
Moderate	Medium risk		High risk
Low			
Not at all	Low risk		

Where the level of system diversity is being considered, it may also be useful to describe the consequences in terms such as:

- Human Dependent Failure – where a single error can lead to an incident due to (say) ineffective error checking by supervisors, error repetition etc
- Common Cause Failure - A series of system failures occurring for the same reason;
- Common Mode Failure - A series of system failures occurring in the same way;
- Human Induced Dependency – Two "independent" systems fail due to a common human error.

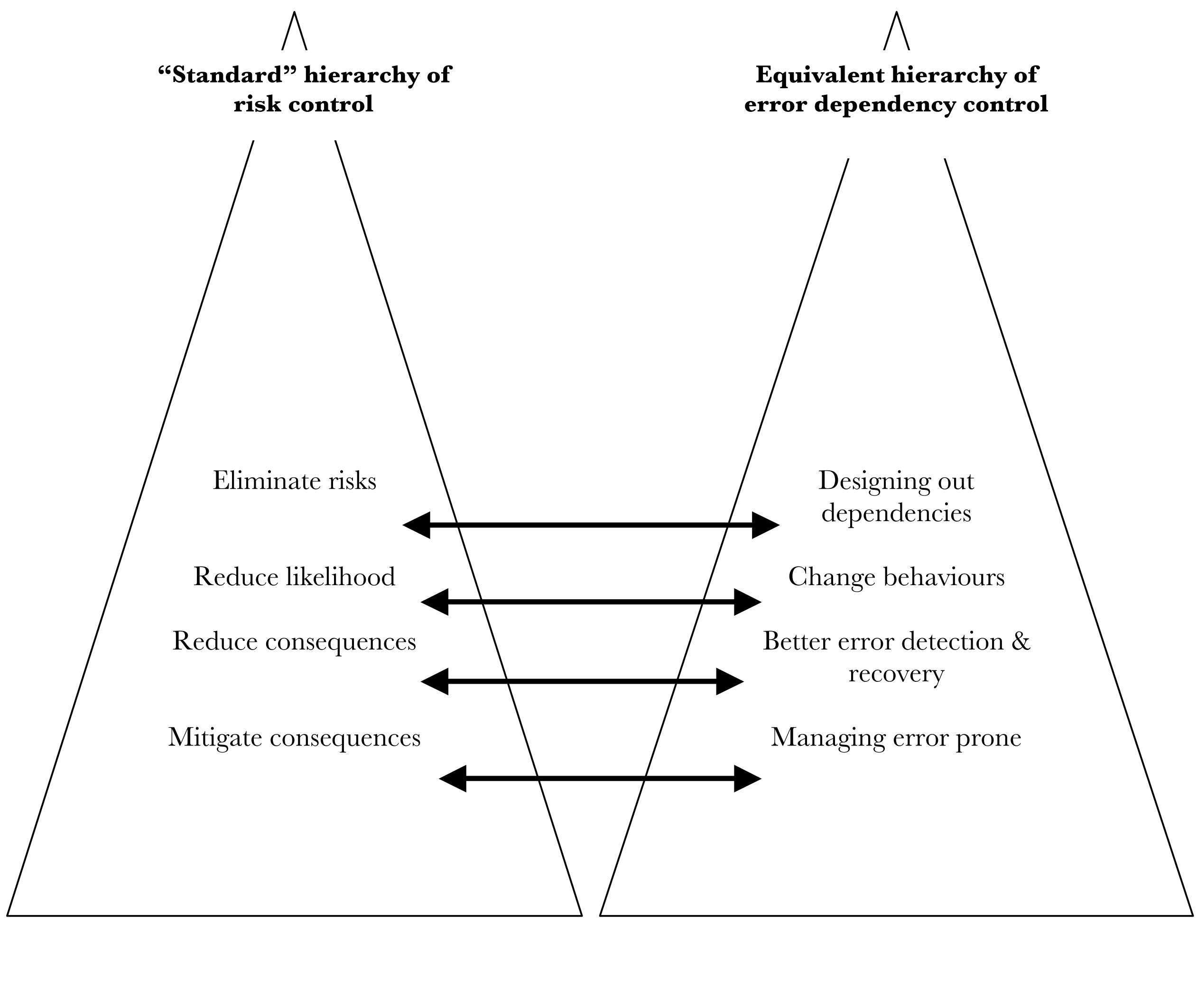
In Appendix B, the consequences of errors are first described qualitatively in these terms and then a Risk Rating is given by combining the dependency likelihood with the consequence scale.

A figure (Figure C.1) is provided in Appendix C that can be used to help identify the way (the failure mode) in which a dependent error could impact safety. This may be of particular importance when completing quantitative or probabilistic risk assessment, especially if fault trees are used.

Step 4: Choosing strategies for preventing or mitigating dependencies

Having determined the safety significance of dependent errors in Step 3, the next step is to choose one or more strategy to prevent or mitigate such errors. The output of this step is shown in the final right hand columns of the examples in Appendices A and B. The selection of strategies should take account of the safety significance of errors, their causes and the "hierarchy of control". As with all other safety management decisions, risk reduction measures should be considered in terms of the hierarchy of control, as illustrated below in Figure 6. Where possible error dependency should be eliminated as far as reasonable practicable, especially where the safety significance of errors is high. This might be achieved by re-designing equipment or re-allocating tasks such that the task does not entail any significant interaction between people and /or between people and those items of equipment of concern. In cases where elimination is not practical, consideration should be given to reducing the likelihood and / or consequences of dependent errors.

Figure 8: Hierarchy of control



Otherwise, the strategy should address the contributory factors noted in Step 2 and/ or the task conditions noted in Step 1. By considering task conditions and causal factors, the advantages and disadvantages of each potential defence can be assessed.

For example, in the event that operators are thought to rely overly on automatic warning systems, it could be proposed that they are informed of the failure modes of automatic systems to reduce their "unsuspecting" reliance on them. However, it could be that operators are influenced by their colleagues' judgements more than by their perception of automatic systems. In the latter case it might be more effective to train operators in the techniques of Crew Resource Management, such as alerting them to the possibility of misleading one another and highlighting the importance of cross-checking one another's judgements. For the latter strategy to work it may be necessary to develop a "democratic" style of team leadership so that staff challenge error in an uninhibited manner.

There might be weaknesses associated with any particular strategy. For example, whereas hardware interlocks can prevent certain errors, over-reliance on them can introduce dependencies of their own. Similarly, an excessive number of procedural checks may lead people to believe some one else will complete a check. Accordingly, it is important to consider the possibility that the proposed strategy may itself introduce dependent errors, perhaps simply replacing one set of dependencies with another set of dependencies.

The strategies noted in Figure 6 are defined below and illustrated with examples in Boxes 8 to 11.

Designing out dependencies

This entails eliminating the possibility of a dependency. For an error dependency to be eliminated there must not be any possibility of one error or process influencing the possibility of the error of concern. For example, components may be designed such that it is impossible to repeat an error across two items of equipment. Alternatively a task could be entirely automated or avoided by adoption of alternative working practices.

Change behaviours (quality strategies)

These strategies aim to reduce the likelihood that the occurrence of one error or process will influence another, such as reducing the propensity of people to rely on one anothers' judgements.

Error detection

This involves increasing the likelihood that a dependent error will be detected and / or corrected before it has an adverse impact. Detection could involve automatic alarms, such as for alerting operators to the loss of automatic warning systems, independent administrative checks on completion of tasks, functional testing and so on. These strategies aim to detect an error once it has occurred and facilitate its correction.

Managing error prone situations

These strategies apply to those occasions where no practical way of eliminating or reducing likelihood of an undetected error can be identified, or where further risk reduction is required. The aim is to manage error prone activities in such a way that the potential error is less likely to have an adverse impact. It may include halting operations in the event that automatic warning systems are not available, improving reliability of automatic systems and so on. In these cases it is recognised that error may occur. The strategies aim to either avoid these activities or compensating for the errors.

The application of these strategies is illustrated in Appendix A and B. In the first example, these sub-headings have been omitted because initial assessment determined that errors could not be eliminated or mitigated. In the second example consideration of each strategy has been prompted by including each strategy as a sub-heading in the final column of the table.

Strategies can also be described in terms of quality and diversity approaches, as defined below. These terms are defined here to further help prompt identification of strategies.

Quality strategies: these aim to "improve" the quality of "contributory factors", such as reducing the level of deferential attitudes so as to minimise the potential for (dependent) human error to occur. These may also include maximising the potential for error recovery and making the system error tolerant. As such they should help reduce the likelihood and consequence of dependent errors.

Diversity strategies: This category of defences against dependency aims to provide increased independence between human actions. Examples include:

i) the avoidance of relying on the same essential piece of 'equipment';

ii) separating the timescale between tasks;

iii) introducing additional personnel into tasks;

iv) adopting working practices which minimise the propagation of repeated human errors through the system.

Diversity strategies may, in some cases, eliminate error dependency, such as where tasks are spilt between people.

Further guidance on error prevention can be found in reference 2.

Box 8
Examples of designing out dependencies

Component Design
Component design can assist in reducing dependence between maintenance/ repair/ replacement tasks across components in, for example, redundant trains of a safety system. In circumstances where replacement of a number of identical components is necessary, for instance, the potential for the introduction of multiple faults can be reduced through sound component design by:

(i) Ensuring that the replacement component can only be physically fitted in place, in the correct orientation (e.g. by avoiding symmetry).

(ii) Ensuring that only appropriate components of the required quality/design rating, fit for the purpose intended can be utilised.

Equipment Diversity
In addition to providing the obvious benefit of minimising the potential for hardware-related common cause or common mode failure, equipment diversity has additional benefits in defending against human dependency. The use of diverse components means that operating practices and procedures will differ across the components (e.g. a turbine-driven compared with a motor-driven pump) and the potential for errors common to all components is reduced.

Staggered Testing or Maintenance
Staggering test and maintenance activities provides an increased time separation between multiple actions that could be functionally linked (e.g. contribute to the occurrence of a hazard). This could be important in, for example, redundant components across multiple trains of a safety system or in related components that together form a particular line of protection. If all pumps in a redundant system are maintained at the same time, the potential for a single, repeated error by an individual or team of operators to defeat the whole system is obviously increased. Staggering the activities would normally have the additional benefit of meaning subsequent actions are likely to be carried out by different personnel, thereby increasing the independence between tasks further.

Diverse Operational/Maintenance Teams
The use of different teams of operators for specific tasks reduces the reliance on a single team (or individual). For example, to maintain a set of functionally linked components, it may be advantageous to use two teams, each maintaining half the components. In this way, even if one of the teams makes repeated errors, it will not affect all the components of concern. It is important to note however that dependency could still exist between the two teams if, for example, they discuss and agree which procedures should be applied.

Box 9
Examples of changing behaviours

Countering social processes
Training should emphasise the pitfalls of over-reliance and trust upon other team members and the negative effects that seniority/social status can have on the questioning of other team members' decisions by junior members of the team. One leading example of this can be found in the technique of Crew Resource Management (CRM). A series of tragic accidents in the aviation sector highlighted the potential for junior staff deferring to senior officers, thereby failing to indicate errors and impending accidents. As a result many aircraft operators have implemented a programme of CRM training that encourages staff to actively check colleagues actions, decisions and interpretation of the situation, regardless of relative rank and experience. The techniques of CRM have now been introduced to the power and offshore sectors.

Active rather than passive task checking
Get staff to repeat (say) a calculation independently and compare answers, rather than asking one person to check the work of another.

Human-machine interface design
The design of control and instrumentation should not discourage individuals from scanning and interpreting information. For example:

- It should be easy for operators to scan instrumentation and quickly notice key information;
- It should be easy to tell if there has been an instrument or plant failure, to promote diagnosis and understanding of the situation.
- System design should allow competing tasks to proceed (e.g. under automatic control) while the operator deals with the task in hand.

The application of basic ergonomic principles is discussed in many human factors textbooks, and in guidelines produced by the Health and Safety Executive, such as reference 2.

Staffing level, procedures, training, general competence
Any factor that increases task difficulty may influence error dependency, by reducing staff inclination to check each other, re-do tasks etc. Accordingly, factors such as staffing levels, competence etc should be optimised to avoid inducing errors and / or inhibiting self-detection.

Risk awareness
Ensure staff have an understanding of the level of safety that needs to be achieved and the role of secondary checks to achieve these standards.

Awareness of system failure modes / true reliability
Ensure staff have an understanding of failure modes of systems so that they do not heedlessly rely on automatic systems etc.

Quality Assurance (QA)
The adoption of the principles and practices of a sound quality assurance system such as ISO 9000 should maintain and enhance the standards of the working practices throughout the plant. The QA system has obvious benefits in defending against dependent failures, including human dependency, through the control of documentation (use and upkeep), administrative control systems, technical verification, record keeping, design change procedures, etc.

Box 10
Error detection and recovery

Reliable and trustworthy information
Instrumentation should be sufficiently reliable for staff to trust indicators and so be encouraged to use instrumentation to check colleagues' decisions. The past unreliability of the vibration indicator on the 737 involved in the Kegworth air crash may have played a role in the commander's failure to double-check the co-pilots diagnosis of the engine fault by scanning flight instrumentation.

Obvious feedback

- Operators should be given clear, direct feedback of the effects of their actions to facilitate self-correction of errors.
- Communication procedures should use a standard phraseology with 'repeat back' procedures to facilitate detection of errors in verbal communication.

Truly independent task monitoring
The need to have someone performing the role of standing back and getting an overview of what is happening has been indicated in a series of accident reports as a means of countering "group think" amongst operators, including Three Mile Island and Texaco explosion. The "hands-off" person is meant to actively monitor decisions and information with the aim of checking whether other staff are overlooking key points of information or focusing on a small part of the problem.

An example of the latter strategy can be found in the US Navy, who are reported to have sufficient "spare" staff to perform a shadowing role, whereby they observe and monitor the actions and decisions of more junior staff. This is combined with a philosophy of task delegation that enables senior staff to have a "hands-off" role, allowing them to monitor achievement of their directions (orders). In this way they have separated the role of completing tasks from the role of monitoring performance, and thereby achieved independent task monitoring. The shadowing role of senior staff is a recognised and legitimate role, accepted as a means of achieving an effective "defence in depth".

Supervision and Checking
The provision of additional personnel either to supervise or check an individual's work provides a way of recovering from errors and may prevent multiple errors due to within-person dependence from leading to a hazardous situation. Supervisors should have first-hand operational experience of the task they are supervising, and the job organisation should be such as to maximise the independence between the supervisor or checker, and the operator carrying out the task. It should be noted that dependence between the operator and checker/supervisor may still exist, but (when implemented correctly) effective supervision should reduce the overall task failure probability.

Auditing behaviour
Conventional safety auditing of administrative procedures can help ensure that the standard of independent checks is not eroded. As well as ensure that procedures and SMS are being followed.

Post-Maintenance Functional Testing
The adoption of functional testing of items of equipment following maintenance provides a means of testing the components prior to making them operational. This provides a means of recovering from faults introduced during maintenance (including faults in multiple items of equipment due to repeated, systematic errors). It should be noted however, that proper functional testing may not reveal all potential defects which could have been introduced, as some defects may be slowly developing and only revealed when a component is stripped down and overhauled, for instance.

Box 11
Managing error prone operations

This entails implementing managerial / operational procedures that counter errors. For example the habit of staff relying on automatic warning systems may be managed by:

- Introducing additional personnel with the specific task of monitoring the situation when automatic systems are inoperative

- Shutting down operations / taking the equipment out of service in the event that it fails – as a matter of policy

Also, where staff are thought to rely on (say) automatic warning systems, the importance of maintaining the availability of such systems should reflect the heightened risk of error in the event of system failure.

For example, where a new automatic warning system is introduced, this should be classed as a safety critical system with appropriately prioritised maintenance, even if they had previously operated without it. This reflects the possibility that staff vigilance etc would be eroded by reliance on the new system, such that past levels of vigilance can no longer be achieved in the absence of the new system.

Key messages

Dependent errors play a significant part in accidents. Having considered several case studies, it can be seen that:

- Human error dependency has played a role in many major accidents;
- Well-intentioned improvements, such as the introduction of new automatic warning systems and team working, can inadvertently introduce error dependencies.
- Dependency factors may affect the ability of a single operator to perform correctly the same task several times or several different tasks sequentially, and they may play a part in influencing the decisions taken or actions made by a team of operators.
- When potential dependent errors are identified, their likelihood can often be reduced, though not necessarily eliminated. Many organisations have implemented strategies specifically targeted on dependent errors.
- Methods for controlling human error dependency range from "hard" measures such as engineering out dependencies to "softer" cultural and administrative measures.
- Human error dependency should be considered within both qualitative and quantitative risk assessments.
- Management play a key role in preventing error dependency both directly by policies aimed at dependent errors and indirectly by considering possible impact on human error dependency of general management and technology decisions / changes.

REFERENCES AND FURTHER INFORMATION

1) *A guide to task analysis.* B. Kirwan and L.K. Ainsworth (eds). Taylor and Francis. 1992. ISBN 0 7484 0058 3

2) *Reducing error and influencing behaviour.* HSG48. HSE books 1999 ISBN 0 7176 2452 8

3) *Handbook of Human Reliability Analysis with emphasis on Nuclear Power Plant Applications.* A.D.Swain and H.E. Guttmann. NUREG/CR-1278 SAND80-0200 RX, AN. Printed 1983. Available from U.S. Nuclear Regulatory Commission, Washington, D.C. 20555 and National Technical Information Service, Springfield, Virginia 22161.

4) *Human Reliability Assessment – a critical overview*. ACSNI Study Group on human factors. Second report. HSE Books 1991. ISBN 0 11 885695 2.

5) *A Guide to Practical Human Reliability Assessment.* Kirwan, B. Taylor and Francis, 1994.

6) *Human Dependent failures: A schema and taxonomy of behaviour*. Hollywell, P. In EJ Lovesey (ed) Contemporary Ergonomics, 1993, 171-177.

Appendix A: Example of HFRG method

Introduction

A collision occurred between two vessels off Lands End. The cause of the collision was failure by the crews of both vessels to take avoiding action in a timely manner, although the reasons for those failures were different. The HFRG method has been applied to the systems and arrangements that were in force on the two vessels. The information on which the analysis is based has been drawn from the Marine Accident Investigation Branch Safety Digest. The conclusions drawn below may not be a true reflection of the systems and the incident in question, due to the inevitable brevity of the report. Consequently, no judgement is implied or should be inferred concerning either the cause of the reported incident, or the quality of the investigation. The purpose of this case study is solely to illustrate the method.

Incident summary

It was a dark but clear night. The container ship was heading south off Lands End at 14 knots. The fishing trawler was fishing approximately 6 miles from the container ship – showing navigation lights indicating trawling, and decklights. The fishing trawler was making 3.5 knots, due east, in company with two other fishing vessels.

The Skipper of the fishing trawler observed lights (of the container ship) approximately 6 miles away, but assumed it would alter course as the trawler had right of way.

The crew on the container ship failed to observe the trawler.

The trawler skipper realised eventually that the container ship was not changing course, and took avoiding action, but too late to avert a collision, leading to minor damage to the trawler and severe bruising to the skipper. The trawler was escorted to harbour by another fishing vessel that was close by. The container ship made radio contact after the collision, but established that assistance was not required.

System

The container vessel had:

- Second Officer on Watch (took over from Chief Officer) about 30 minutes before collision;
- GPS (satellite positioning) used as primary aid for position fixing;
- Two radars, one in use;
- Lookout posted on bridge to assist in watchkeeping, and;
- ARPA (Automated Radar Plotting Aid) which helps to identify collision risk.

The Second Officer had been advised at handover of vessels in sight.

The fishing trawler had:

- Skipper on watch in wheelhouse, and;
- Navigation and deck lights making visible vessel and its intentions.

Accident causes

The immediate causes of the accident were;

- a failure by the watchkeeper and lookout on the container vessel to detect the fishing trawler, and;
- a failure by the skipper of the fishing trawler to take avoiding action early enough once it became apparent to him that the container vessel was not altering course, even though it was required to under the Collision Avoidance Rules.

The underlying causes of the accident were:

- the reliance placed by the crew of the container vessel on their electronic navigation aids, to the detriment of the use of visual scanning
- distraction of the watchkeeper on the container vessel by the need to plot a position
- the assumption by the Skipper of the trawler that the container vessel had seen his vessel, and would alter course
- the delayed recognition by the trawler Skipper that no course change was apparent.

It is known that automatic radar plotting aids (ARPA), designed to aid identification of collision risk, have been set on an inappropriate scale in other incidents, thereby giving inadequate warning of collision risk. At least one radar should be set on long range scale to give forewarning of collision risk. It is also possible for radar to "miss" small vessels that give a weak reflection. Accordingly, crews are meant to maintain a constant visual watch and judge distance / routes of other vessels by eye, rather than rely on radar to identify collision risks, especially if the radar is not constantly monitored.

Summary of assessment

The results of the assessment are shown in Table A.1. The column headings note which step of the method is reported.

Step 1: Identify safety critical human error dependencies

In this example there are 8 possible dependent errors that could impact safety, namely allow a collision to occur. These are analysed in each of the 8 rows of Table A.1. The task condition and coupling mechanism along with a description of each error is given in the first column.

Step 2: Assess likelihood of dependence

A single composite judgement of the level of dependency has been made for each of the eight errors, i.e. eight separate judgements. These judgements have been arrived at after considering the factors in Table A.1. The opportunity for detecting and correcting the errors prior to collision have been noted and taken into account when forming the likelihood judgement. Thus, if there is ample opportunity to detect and correct an error, its likelihood has been reduced. However, if the mode of dependency suggests crew may not be take steps to check their situation, the potential for error detection has been reduced. For example, whilst a second crew member might counter the first crew member's reliance on ARPA, it is equally possible that both crew members would rely on the ARPA.

Step 3: Assessing safety significance of dependency

The likelihood of each dependent error has been combined with a judgement of it consequence (in the third column) using the Consequence scale to produce a Risk Rating in the fourth column. The errors range from Medium to Very High risk. Priority should be awarded prevention of the higher risk errors.

Step 4: Choosing strategies for preventing or mitigating dependencies

The strategies have been designed to address the primary Contributory Factors judged to underlie each error. The highest risk dependency entails crew relying on the ARPA, although recommendations are offered for all errors in this example. With regards to the highest risk dependency it is proposed to mitigate reliance on ARPA by highlighting the limitations of ARPA, particularly when navigating in coastal areas and shipping lanes. No credible way of designing out this dependency can be identified. Also, there are already a number of personnel in position who are meant to double-check one another. Accordingly the strategies focus on reducing the level of dependency with the ARPA and on one another.

Table A.1: Application of HFRG method to a marine example

Step 1 (Box 7)	Step 2 (Table 1)	Step 3 (Table 3)		Step 4 (Boxes 8 – 11)
Description of dependent human error, type of coupling mechanisms & task condition	**Dependency Likelihood (& error detection)**	**Consequence (Safety Significance)**	**Risk Rating**	**Recommendations**
The Container vessel				
Type of coupling mechanism Individual ***Error description*** Ability of watchkeeper to detect another vessel influenced by his previous scan of the area (if not detected before, likelihood of detecting may be reduced)	Low Continued scanning & second lookout may spot other vessel before collision occurs	Major loss	Medium	Training should emphasis speed with which situation can change, especially in coastal waters and shipping lanes where large numbers of relatively fast moving traffic occurs as well as lane crossing. Should also stress the need to vary position on vessel to change view and perspective, including avoiding obstacles in line of sight (eg masts).
Type of coupling mechanism Individual - system **Error description** Reliance on automatic radar systems (e.g. ARPA) reduces likelihood that watchkeeper will also use visual scanning diligently	High Second lookout may also rely on ARPA	Major loss	Very High	Training and formal procedures should highlight requirement to cross-check radar against visual inspection. Also, training and procedures should highlight need for variation in radar ranges and highlight limitations of ARPA, such as missing smaller vessels and giving inadequate warning of collision if only short range radar is used.
Type of coupling mechanism Inter-individual **Error description** Information provided by off-going watchkeeper will influence detection of other vessels	Moderate Oncoming watch keeper may develop own understanding of situation, thereby spotting over sight by previous watchkeeper	Major loss	High	Training and procedures should stress need for oncoming watchkeeper to maintain a watch for a few minutes and to describe to off-going watchkeeper his perception of situation before offgoing watchkeeper updates him, and for oncoming watchkeeper to double check offgoing watchkeeper briefing

Step 1 (Box 7)	Step 2 (Table 1)	Step 3 (Table 3)		Step 4 (Boxes 8 – 11)
Description of dependent human error, type of coupling mechanisms & task condition	**Dependency Likelihood (& error detection)**	**Consequence (Safety Significance)**	**Risk Rating**	**Recommendations**
Type of coupling mechanism Inter-individual **Error description** Each person on Bridge may influence the likelihood that the other will remain fully vigilant	Moderate Attention could be returned to watchkeeping before collision occurs	Serious	Medium	Training in techniques such as Crew Resource Management whereby importance of double checking each other's performance and working as a team is stressed.
Fishing trawler				
Type of coupling mechanism Individual **Error description** Ability of watchkeeper to detect another vessel influenced by his previous scan of the area (if not detected before, likelihood of detecting may become reduced)	Moderate Watchkeeper could intermittently recheck course of other vessel before collision occurs	Major loss	High	Training should emphasis speed with which situation can change, especially in coastal waters and shipping lanes where large numbers of relatively fast moving traffic occurs as well as lane crossing. Should also stress need to vary position on vessel to change view and perspective, including avoiding obstacles in line of sight (eg masts).
Type of coupling mechanism Individual **Error description** Ability of watchkeeper to identify collision course influenced by previous decision about whether collision risk exists	Moderate Watchkeeper could intermittently recheck course of other vessel before collision occurs	Major loss	High	Training should emphasis speed with which situation can change, especially in coastal waters and shipping lanes where large numbers of relatively fast moving traffic occurs as well as lane crossing.

Step 1 (Box 7)	Step 2 (Table 1)	Step 3 (Table 3)		Step 4 (Boxes 8 – 11)
Description of dependent human error, type of coupling mechanisms & task condition	**Dependency Likelihood (& error detection)**	**Consequence (Safety Significance)**	**Risk Rating**	**Recommendations**
Type of coupling mechanism Inter-individual **Error description** Assumption that other vessel has seen you if you have seen the other vessel	Moderate Watchkeeper could intermittently recheck course of other vessel before collision occurs	Serious	Medium	Training should highlight examples of where other vessels have failed to observe smaller vessels and struck them
Type of coupling mechanism Inter-Individual **Error description** Assumption that other vessel will follow 'rules of the road'	Moderate Watchkeeper could intermittently recheck course of other vessel before collision occurs	Serious	Medium	Training should highlight examples of where other vessels have failed to follow the 'rules of the road'

Appendix B: Example of HFRG method (using optional tables)

Failure to Administer Anaesthetic Gas at start of Operation[1]

Case Summary and Chronology

Patient Mrs K (25) suffers from chronic arthritis. Over the years she has undergone many elective orthopaedic operations including bilateral hip replacements and bilateral knee replacements. The chronology is:

27.10.97 – Patient was admitted for elective elbow replacement, pre-operative visit by Consultant Anaesthetist, who knew patient and was aware of her immobility problems. Surgery planned for 28.10.97.

28.10.97 – Case postponed due to lack of theatre time.

30.10.97 – Elective total elbow replacement, incident occurred during this procedure.

Patient was a recognised operative risk; she had severe chronic arthritis, which greatly reduced her range of movements. Her neck was almost totally immobile, allowing minimal flexion. She had previously had a very difficult intubation and required resuscitation and was recognised as a Grade 4 intubation difficulty. The anaesthetist (a Senior Registrar) spoke to the patient about the anaesthetic, and explained that she would be prone (lying on her front) during the procedure.

On arrival in the anaesthetic room the patient vomited a small amount of bile stained fluid, thought to be as a result of preoperative morphine. Intravenous drugs were administered to induce anaesthesia. A laryngeal mask airway was inserted without a problem, and the patient was allowed to ventilate spontaneously on a mixture of isoflurane, a volatile anaesthetic, 50% oxygen and nitrous oxide. The patient's trachea was successfully intubated with an armoured endotracheal tube. Once intubated the patient was paralysed and mechanically ventilated.

The patient was transferred to the theatre and reconnected to the anaesthetic machine and (it was thought) the same gases were administered as in the anaesthetic room. The machine was not formally checked as there was no oxygen analyser. The patient was carefully positioned prone on the table, with her neck being held in a neutral position. The patient remained stable during this positioning procedure.

Once surgery had commenced the patient became very hypertensive and tachycardic, denoting a sympathetic response to pain. IV opiods were given. The patient did not respond to this. The breathing circuit was then checked on suspicion of a leak. The anaesthetist became aware that the patient was not receiving anaesthetic gas. The circuit was immediately changed and anaesthetic gas administered. The operation was successfully completed.

The patient recalls waking up in recovery screaming. She was immediately aware of the fact that she recalled being awake at the outset of surgery. She remembered what the surgeon said, and recalls feeling intense pain but being unable to move and alert the staff to the fact that she was awake.

Causes of incident

The hospital had kept older unalarmed equipment in use after introducing new alarmed machines. Staff appear to have became used to the alarmed machines such that they became less vigilant in the use of older unalarmed machines. This example demonstrates the risk of assuming standards of operation of current control equipment will be unaffected by the introduction of new technology. The hospital subsequently withdrew all old machines from use.

---

1 A protocol for the investigation and analysis of clinical incidents. Clinical Risk Unit and ALARM. The Royal Society of Medicine Ltd. 1999. ISBN 185315436 9

Summary of assessment

The results of the assessment are shown in Tables B.1 and B.2. The column headings note which step of the method is reported.

Step 1: Identify safety critical human error dependencies

The assessment has addressed two task steps, namely checking that the anaesthetic gas machine is connected prior to the start of the operation and then checking the gas supply at the start of the operation. These two steps are analysed in Table B.1 and B.2 respectively. In each case the type of coupling mechanism and task conditions are noted in the first column.

Step 2: Assess likelihood of dependence

The factors that are judged to apply to each task step are noted in the second column and a judgement of the level of dependence associated with each factor is given in the third column.

Step 3: Assessing safety significance of dependency

Failure to anaesthetise a patient is judged to be a serious event, causing extreme pain. However, as it may not cause fatal injury it is classed as Serious rather than a Major Loss. As both errors pose the same consequence they are both assigned a Serious consequence in the fourth column.

The Serious consequence is combined with the likelihood of each contributory factor to give a Risk Rating for each contributory factor, ranging from Low to Very High, in the fifth column. Those factors posing Very High risk should be prioritised when considering strategies for preventing dependencies.

In this example, the consequence has also been described qualitatively (in column four) in terms of how it may impact the level of independence in the operating procedure. This indicates that the two members of staff could both make the same mistake(s), thereby losing the benefit of involving two members of staff in this task.

Step 4: Choosing strategies for preventing or mitigating dependencies

The strategies shown in the final column have been chosen to address those factors which pose highest risk, namely assuming you can rely on colleagues to have correctly completed the task, believing equipment is reliable and poor indication of equipment status (i.e. no alarm) and wrongly assuming different equipment is operated in same way (i.e. old unalarmed and new alarmed machines). The strategies are listed under the four categories, Designing out dependencies and so on. The preferred strategies are to withdraw old machines and / or retrofit alarms / indicators to them, and formalise the equipment check by instituting verbal confirmation of equipment status. The latter verbal confirmation should be assigned to a single person to avoid the previous situation where each member of staff presumes the other one has checked the equipment. If old machines cannot be withdrawn or retrofitted, an alternative (less desirable) option is to compensate for this by instituting a special administrative check on equipment status.

TABLE B.1: CHECK ANAESTHETIC MACHINE PRE-OPERATIVELY

STEP 1 (Table 1 & Box 7)	STEP 2		STEP 3		STEP 4 (Boxes 8 – 11)
	Table 2	Table 3	Table 4	Table C.1	
Description of dependent error, coupling mechanisms & task condition	**Dependency Likelihood**	**Contributory factors**	**Risk Rating**	**Consequence (Safety Significance)**	**Recommendations**
Type of coupling mechanism Individual-system **Task condition** 14. different person, same task, same device, different time ***Error description*** Failure of anaesthetist or ODA to adequately check anaesthetic machine pre-operatively	High	4	High	**Consequence = Serious** Common Cause Failure = possible Human Induced Dependencies = possible Human Error Dependency = possible Common Mode Failure = unlikely	**Designing out Dependencies** 1. Non-standard equipment should be taken out of service. **Change Behaviour** 2. Alarms should be placed on the anaesthetic machine to bleep when a circuit is incomplete, or behaving abnormally. 3. Machine should be modified to include an oxygen monitor. 4. Adequate training for locum staff 5. ODA should be made responsible for verbally reporting the status of the anaesthetic machine pre-operatively. All anaesthetists and ODA's should receive updating on the details of the new protocol. **Better Error Detection and Recovery** 6. When using an old aneaesthetic machine an extra admin check by the ODA should be completed to ensure correct construction. **Managing Error Prone Operations** 7. Ensure all staff are aware that some machines lack alarm. 8. See 6.
	Moderate	6	Medium		
	Low	7	Medium		
	High	8	High		
	Not at all	15	Low		
	Moderate	17	Medium		
	Low	18	Medium		
	Highly	19	High		
	Not at all	21	Low		
	Moderate	22	Medium		
	Complete	26	Very high		
	Highly	29	High		
	Complete	32	Very High		
	Low	34	Medium		

TABLE B.2: CHECK GAS EMISSIONS FOLLOWING TRANSFER TO THE OPERATING TABLE

STEP 1 (Table 1 & Box 7)	STEP 2		STEP 3		STEP 4 (Boxes 8 – 11)
	Table 2	Table 3	Table 4	Table C.1	
Description of dependent error, coupling mechanisms & task condition	**Dependency Likelihood**	**Contributory factors**	**Risk Rating**	**Consequence (Safety Significance)**	**Recommendations**
Type of coupling mechanism Individual-system **Task condition** 14. different person, same task, same device, different time **Error description** Failure to check gas emissions following transfer to the operating table	High	4	High	**Consequence = Serious** Common Cause Failure = possible Human Induced Dependencies = possible Human Error Dependency = possible Common Mode Failure = unlikely	**Designing out Dependencies** 1. Non-standard equipment should be taken out of service. **Change Behaviour** 2. Alarms should be placed on the anaesthetic machine to bleep when a circuit is incomplete, or behaving abnormally. 3. Machine should be modified to include an oxygen monitor. 4. Adequate training for locum staff 5. ODA should be made responsible for verbally reporting the status of the anaesthetic machine pre-operatively. All anaesthetists and ODA's should receive updating on the details of the new protocol. **Better Error Detection and Recovery** 6. When using an old aneaesthetic machine an extra admin check by the ODA should be completed to ensure correct construction. **Managing Error Prone Operations** 7. Ensure all staff are aware that some machines lack alarm. 8. See 6.
	Moderate	6	Medium		
	Low	7	Medium		
	High	8	High		
	Not at all	15	Low		
	Moderate	17	Medium		
	Low	18	Medium		
	Highly	19	High		
	Not at all	21	Low		
	Moderate	22	Medium		
	Complete	26	Very high		
	Highly	29	High		
	Complete	32	Very High		
	Low	34	Medium		

Appendix C: Human error dependency and probabilistic risk assessment

Impact of dependency on accuracy

Human error dependency is of particular importance for reliability analysis and / or probabilistic risk assessment (PSA) (also referred to as Quantitative Risk Assessment - QRA). Typically, QRA and PSA involve task decomposition followed by the construction of fault trees against whose nodes known probabilities of failure can be assigned. Such fault trees assume independence of failure at each node, unless otherwise stated. That is to say, the outcome of one event does not influence the outcome of any other event. When this assumption does not hold true, dependency exists. If there is dependence between the probabilities of failure at two separate nodes, and this is not reflected in an adjustment to the probabilities, then the results of the analysis may be unduly optimistic. Thus, the possibility arises that, when assessing reliability in particular, a failure to take account of dependencies could result in a serious underestimate of the actual reliability. Clearly, accurate estimates of system reliability can be achieved only if human dependency is fully and properly incorporated into the analyses. For example, limiting values can be added to a top event probability.

In recognition of this, conservatisms are often incorporated into the analyses to account for undetected dependencies, amongst other reasons. However, by modelling dependencies in the way described in this guide, it should be possible to reduce reliance on what may be undue conservatisms.

Incorporating error dependency in probabilistic risk assessment

In systems reliability assessment the problem of human dependency can arise in a variety of situations. An obvious example is where an engineered standby protection system makes uses of multiple trains of identical equipment. In such situations the availability of such systems will be affected by, amongst other things, manufacture, installation, routine maintenance and testing. Clearly there is the potential in such situations for errors to systematically occur throughout the different trains thereby disabling the entire system.

Where different items of equipment have been employed to increase diversity then the potential for such systematic errors will be reduced (e.g. the need for different maintenance instructions). Nevertheless there may remain links (e.g. the use of the same maintenance team) which, to different degrees, have the effect of reducing the level of diversity.

Dependency is obviously not restricted to situations involving multiple trains of protection but can also occur between the initiating event and the availability of the protection system. For example, at Chernobyl the disabling of essential safety systems both initiated the event and aggravated its development.

When the objective relates to reliability then identification of functionally linked errors is usually simple and can be achieved simply by examination of fault trees and event trees. In the former case where a minimal cut set includes two or more human errors or actions then these are, by definition, functionally linked and it is important that any dependencies are understood. Similarly in an event tree, any two or more actions or errors occurring on a single leg of the event tree must also be functionally linked. For other situations, where there is no corresponding formal analysis of errors and their inter-relationship, then the identification of functionally linked errors or tasks requires careful thought.

Dependency between human actions can be either positive or negative. Positive dependency implies a positive relationship between human actions, although this does not mean that it is necessarily beneficial, i.e. either (i) the success of one action increases the likelihood of success of another action, or, (ii) the failure of one action increases the likelihood of failure of another action.

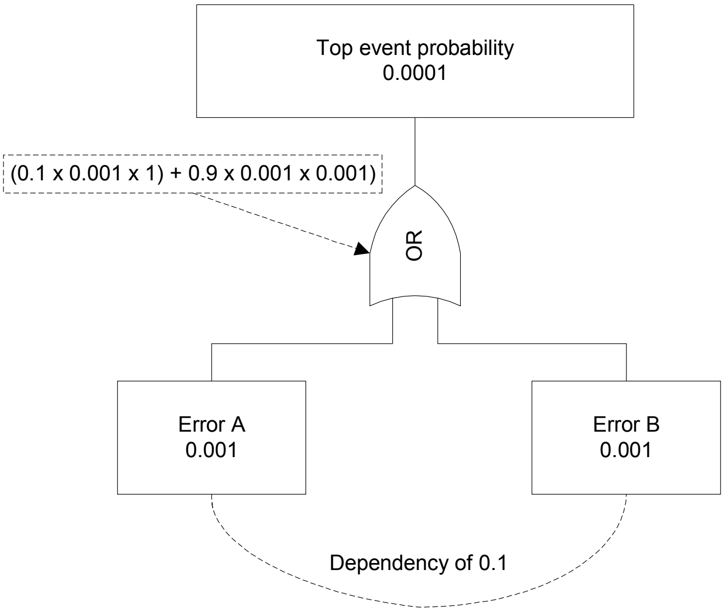
Negative dependency implies a negative relationship between human actions, ie either (i) the success of one action reduces the likelihood of success of another action, or, (ii) the failure of one action reduces the likelihood of failure of another action. In a reliability analysis it is commonly positive dependency, in failure logic, which is of most interest due to its potential for achieving an over-optimistic assessment of the level of safety.

The incorporation of dependencies into probabilistic risk assessment is covered in a number of guides, such as the Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (see chapter 10 of reference 3). The level of dependency is estimated on a scale of 0 to 1, where 0 is no dependence and 1 is total dependence. Assuming two errors have a dependence of 0.1, this means that the two errors will coincide on 10% of occasions. This is calculated as follows, assuming an error likelihood of 1 in 1,000 (0.001) for each of the two errors:

$$(0.1 \times 0.001 \times 1) + (0.9 \times 0.001 \times 0.001) = 1.0 \times 10^{-4}$$

Thus, the probabilities of the two errors are calculated as if they were independent events on 90% of occasions, but are assumed to coincide with a probability of 1 on the remaining 10% of occasions.

This is illustrated in the form of a fault tree below.



Numerical weightings are assigned to the level of dependence either by reference to historical experience or by judgement. Further guidance on the human reliability assessment can be found in references 4 and 5.

The authors of this guide are not aware of any publicly available database for human error dependency although the results of the HFRG method described in this guide could be drawn on to assign such numerical ratings, i.e. the probability assigned to a dependency could be guided by the likelihood rating derived in step 3 of the method. Some illustrative values are given below.

Level of dependence	**Example numerical value**
Complete Dependency	1.0
High	0.5
Moderate	0.1
Low	0.01
Not at all	0.0

It should be noted that the values are not based on any empirical source and are presented solely for the purpose of illustrating how numerical rating s may be related to the judged level of dependency. Users of this guide may wish to assign alternative values if they have a source of empirical data, such as an in-house incident database.

Reference 3 (page 20-38) also provides data on error detection probabilities along with a guideline that credit can only be taken of one "independent" checker. No credit is usually given for a second independent check. This allows a numerical value of error dependency to be combined with a numerical value of error detection to derive an estimate of an undetected dependent error. For example, a High dependency probability of 0.5 could be multiplied by an error detection probability of 0.05 (item 3 from page 20-38) from reference 3 to give an undetected error probability of 0.025.

Identifying possible consequences of dependent errors

Figure C.1 was developed by the Human Factors In Reliability Group. The types of failure modes that can arise in each Task Condition were determined by considering the range of failure modes that can logically occur. For example, it is unreasonable to suppose that a series of systems cannot logically fail for the same reason (i.e. a common cause failure) if there is no connection between the systems, including different people doing different tasks on different equipment. However, if the same person is completing the same task on the same equipment on different days, this person could repeat an error.

In those cases where it is logically possible for an error within a particular type of Task Condition to give rise to a specific form of failure this has been noted as "Possible". In cases where, in general, there is no significant potential for such a failure to arise, because the task condition does not logically allow a significant possibility of such failures, this has been noted as "Unlikely".

The figure is used by first defining the task condition. This may already have been done as part of Step 1. Next, you read across the row to identify which consequences are possible. This information can then be used to guide consideration of whether there is sufficient redundancy, diversity and independence in the system.

Whilst the method outlined here of incorporating human error dependency into probabilistic risk assessment requires an element of judgement, it does provide a demonstrable and systematic process and hence should be a useful aid for analysts.

Printed and published by the Health and Safety Executive
C0.50 10/01

Figure C.1. Possible consequences of dependent errors (optional aid)

Person	Task	Device	Time	Common Cause Failure	Common Mode Failure	Human Induced Dependency	Human Error Dependency
Same	S	S	S	✓	✓	✓	✓
Same	S	S	D	✓	✓	✓	✓
Same	S	D	S	✓	✓	✓	✓
Same	S	D	D	✓	✓	✓	✓
Same	D	S	S	✗	✓	✗	✓
Same	D	S	D	✗	✓	✓	✓
Same	D	D	S	✗	✓	✓	✓
Same	D	D	D	✗	✗	✗	✗
Different	S	S	S	✓	✓	✓	✓
Different	S	S	D	✗	✗	✗	✗
Different	S	D	S	✓	✗	✗	✓
Different	S	D	D	✓	✗	✓	✓
Different	D	S	S	✓	✗	✗	✓
Different	D	S	D	✓	✗	✓	✓
Different	D	D	S	✗	✗	✓	✓
Different	D	D	D	✗	✗	✓	✓

HSE
BOOKS

MAIL ORDER
HSE priced and free
publications are
available from:
HSE Books
PO Box 1999
Sudbury
Suffolk CO10 2WA
Tel: 01787 881165
Fax: 01787 313995
Website: www.hsebooks.co.uk

RETAIL
HSE priced publications
are available from booksellers

HEALTH AND SAFETY INFORMATION
HSE InfoLine
Tel: 08701 545500
Fax: 02920 859260
e-mail: hseinformationservices@natbrit.com
or write to:
HSE Information Services
Caerphilly Business Park
Caerphilly CF83 3GG

HSE website: www.hse.gov.uk

OTO 2001/053

£15.00

ISBN 0-7176-2104-9

9 780717 621040