

HUMAN ERROR ANALYSIS AT A REFINERY

John Gould[1] and Sandra Lovell[2]
[1]Environmental Resources Management (ERM) 5 Exchange Quay, Manchester, M5 3EF, UK
[2]ERM Llandarcy House 11A, The Courtyard, Swansea Bay, Neath, SA10 6EJ, UK

Good operating procedures are a key part in the safe operation of a process plant. Procedures can be both a source and a safeguard of human error and it is important to identify what might go wrong. Identifying human error is an essential part of producing instructions. Existing HAZOPs based on P&IDs do not adequately address human error because the focus is on the engineering process itself rather than the interaction of the process with human operators. A methodology developed by ERM has been applied to major hazard industries. This has identified human errors and actions to prevent major accident hazards. The methodology uses a system of prioritising the tasks based on risk. The human error guidewords are based on HSE human factors guidance.

INTRODUCTION

The Health & Safety Executive (HSE) states that although the human contribution to major incidents is widely accepted, few major hazard sites will proactively seek out potential human performance issues (HSE 2008). By actively looking for potential sources of human error, they can be identified, controlled and ultimately minimised.

Amongst other safe systems of work, good operating procedures are key in the safe operation of a process plant. As both a source of and a safeguard against human error, operating procedures are integral to the overall management of process safety.

ERM have established an approach to identifying the critical procedures in preventing major accidents and the types of human error associated with these critical procedures as well as controls that need to be in place to reduce the likelihood of those errors occurring. Figure 1 illustrates the overall approach.

Existing procedures and activities are risk-ranked to identify those that have the largest potential to cause a major accident. The risk-ranking identifies those procedures that require human error assessment. Procedures categorised as Integrity Critical undergo human error analyses to identify the errors, causes and potential controls that critical procedures must take into to account. The analysis seeks to identify risk reduction measures other than purely procedure design. The analysis also comprises a cross-reference to the hazards identified in the initial risk assessment as well as to the original HAZOP analysis. Cross-checking with the P&IDs play a central role also, particularly where controls identified result in changes to the content or order of the procedural steps.

RISK RANKING

The procedures and activities were categorised based on risk assessments to identify and assess the major hazard potential for each operation. The initial risk assessment methodology was developed based on ExxonMobil's Competency Assurance Standards (EXXON 2002), (EXXON 2003) and industry best practice.

Each procedure was assessed separately by a specialist team knowledgeable about the operation and led by an experienced risk assessor. The potential consequences for each procedure were identified. The scenarios that could lead to the adverse impacts were identified and recorded, along with the existing controls designed to ensure that the impacts were not realised.

In identifying the hazardous scenarios, the team also considered the possibility that the procedure was not correctly followed and included failures such as:

- equipment being in the wrong or failed state for the operation to be undertaken safely
- equipment failure during the operation
- procedure started or finished too late
- procedure started or finished too early
- procedure omitted
- procedure (or part of it) performed twice or too much
- procedure partially completed or too little
- procedure in the wrong direction (e.g. start up instead of shut down)
- procedure on wrong equipment
- information required by the procedure not obtained
- wrong information required by the procedure obtained
- incomplete information required by the procedure
- information required by the procedure incorrectly interpreted
- information obtained during the operation incorrectly communicated

The existing mitigation measures were also identified and recorded. Mitigation measures could include, for example, engineering controls to limit the consequences (e.g. fire and gas sensors) or feedback to inform the operator of the success or failure of the operations (e.g. checks by an independent person).

PROBABILITY & COMPLEXITY

The probability that the harmful event will occur was assessed and categorised against the descriptions listed in Table 1.

The probability of the harmful event was assumed to increase in the case of complex or infrequently used procedures. The categorisation adopted for estimating the complexity of the operation is listed in Table 2.

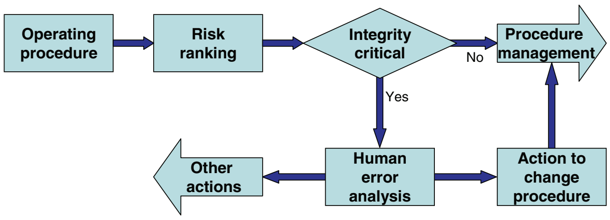

Figure 1. Human error assessment in operating procedures

Table 1. Probabilities used for the risk ranking

Category	Description (typically 10 to 30 years)	Numerical probability range	Numerical probability mid-point
A	Possibility of repeated incidents	1/10–1/1	1/3
B	Possibility of isolated incidents	1/100–1/10	1/30
C	Possibility of occurring sometime	1/1000–1/100	1/300
D	Not likely to occur	1/10000–1/1000	1/3000
E	Practically impossible	<1/10000	1/30000

The highest probability or complexity value was taken forward in the assessment.

CONSEQUENCE

The consequence was assessed for health and safety, environment and financial loss. The highest category was taken forward in the assessment. Table 3 lists the consequence categories.

The highest consequence value was taken forward in the assessment.

Table 2. Complexity categorisation

Category	Complexity
A	Unfamiliar, highly complex, immediate response and analysis required
B	Highly complex, prompt response, knowledge and analysis required
C	Complex, knowledge required and some time to respond
D	Less complex but has the potential for human error to occur
E	Common, familiar and non-complex task

RISK MATRIX

The probability and consequence categories assigned to the procedure were assessed against the matrix illustrated in Figure 2.

Procedures categorised as WA (Work Aid) could be written using industry best practice without further reference to the risk assessment. They could be downgraded to work aids if appropriate.

Procedures categorised as N (Normal) could be written using industry best practice still taking into account the hazards identified in the risk assessment and including them within the safety information provided to the operators.

Procedures categorised as IC (Integrity Critical) underwent a human error analysis. The relevant human error and risk analysis results were included in the safety information provided to operators

HUMAN ERROR ANALYSIS

The human error analysis method was based on the familiar techniques of Task Analysis and HAZOP, using a system of prioritising the tasks and identifying the types of error by task.

The first part of the human error assessment included a Hierarchical Task Analysis (HTA). The HTA provided a systematic description of the nature of human activities under consideration. For some areas, the HTA provided a flow diagram of work activities that could be used to provide situational awareness of the procedures relating one part of the overall system. Existing procedures were typically set out in chronological steps, however, it was sometimes necessary to group the steps in a procedure into meaningful sets of tasks suitable for analysis.

ERROR TYPES

The Human Error Analysis covered all the steps in the critical operating procedures, taking each step (or groups of steps) separately and discussing the relevant error type. Table 4 contains an example of error categories and specific error types used to classify the potential human errors during the analysis. This is a comprehensive list based on the Health & Safety Executive Guidance Document on Human Failures provided on their web site.

ERROR CAUSES, CONSEQUENCES AND CONTROLS

Once a human error was identified as being relevant, the assessment continued to identify:

- Cause of error
- Consequence of error
- Existing controls and recovery actions

The cause was restricted to human failures, such as closing the wrong valve. The consequence was based on the worst case scenario, rather than the most likely consequence of the error.

The controls already in place to prevent the error from occurring were recorded, such as feedback before final

Table 3. Consequence categories

	Health & safety	Public disruption	Environmental impact	Examples
i	Fatalities or serious impact on public	Large community	Major/extended duration full scale response	Major fire or explosion significant H/C release toxic release
ii	Serious injury to personnel/ limited impact on public	Small community	Serious/significant resource commitment	Fire small H/C release spill to water large spill to land
iii	Medical treatment for personnel/no impact on public	Minor	Moderate/limited response of short duration	Non-toxic release minor fire environmental exceedence small spill to land
iv	Minor impact on personnel	Minimal to none	Minor/little or no response needed	Minor leak, with negligible impact

Consequence \ Probability	A	B	C	D	E
i	IC	IC	IC	IC	IC
ii	IC	IC	N	N	N
iii	IC	N	N	WA	WA
iv	N	WA	WA	WA	WA

Figure 2. Risk matrix

selection. Recovery actions were considered where they either prevented the consequences from occurring following the error or mitigated the consequences, for example, high level alarms. Factors like operator competence and good training were assumed as an organisational control for all steps in the procedure.

The assessment team of operational staff led by a human factors specialist, talked through procedural steps and recorded findings in a workshop format. The potential consequence and existing recovery controls were discussed and agreed upon before agreeing recommended actions to reduce the likelihood of and better control for human error. Most of the actions identified improvements in the procedure, as there were a good level of control systems already in place. However, a significant proportion identified other ways to reduce human error and these actions were used to produce an improvement plan for implementation by different departments on site.

It should be noted that no quantification of error likelihood was undertaken. The likelihood of most of the errors occurring was small, yet the premise of the analyses is that it is often these infrequent errors which can lead to the most

Table 4. Example of human error types

Error type	Error
Action errors	• Operation too long/short • Operation mistimed • Operation in wrong direction • Operation too little/too much • Operation too fast/too slow • Misalign • Right operation on wrong object • Wrong operation on right object • Operation omitted • Operation incomplete • Operation too early/late
Checking errors	• Check omitted • Check incomplete • Right check on wrong object • Wrong check on right object • Check too early/late
Information retrieval errors	• Information not obtained • Wrong information obtained • Information retrieval incomplete • Information incorrectly interpreted
Information communication errors	• Information not communicated • Wrong information communicated • Information communication incomplete • Information communication unclear
Selection errors	• Selection omitted • Wrong selection made
Planning errors	• Plan omitted • Plan incorrect
Violations	• Deliberate routine • Deliberate exceptional

serious consequences. Therefore all errors, no matter how infrequent or unusual, were considered.

FINDINGS

INITIAL RISK ASSESSMENT

The risk-ranking is generally a rapid process, typically considering 20 to 30 procedures per day. The benefit of this speed allowed the procedures to be considered by a single team within continuous sessions. The risk-ranking was not the forum for detailed consideration, rather, actions were frequently identified and taken forward to the human error assessment process.

ADDITIONAL BENEFITS

The integrated risk assessment process had benefits beyond the risk-ranking of procedures and activities. The assessment may be the first time that the operational teams have considered the how the existing procedures control the overall process. Missing procedures became evident, amendments in the P&IDs were identified and difficult operations were highlighted. Comments from team leaders and supervisors can surprise managers highlighting operational difficulties that have been masked by a competent and experience workforce. Examples of comments included:

> "*Start up is a real black art and the procedures are not really much use in a real situation*"
>
> "*We only use our most experience operators for this, I would not trust it to anyone else*"
>
> "*We only start this operation at night when nobody is wandering around the site just in case anything goes wrong*"

DIVERSITY OF ACTIONS

The human error assessment identified many failures that would not be identified using traditional engineering assessment methodologies. Actions included changes to how the job is undertaken, procedures, signage, and engineering changes. Most actions required trivial changes, however, many of these trivial problems can make a significant contribution to the likelihood of accidents. Examples of actions are listed below:

1. *Manual Valves: 42-MV-68-406 ... should be car sealed open.*
2. *Fit a local pressure gauge.*
3. *Ensure gauges and documentation use consistent units to measure pressure throughout the entire plant.*
4. *Include isolation diagram in procedure.*

Less frequently, engineering changes or other major changes were identified. The recommendations needed further consideration using the organisation's Management of Change system, as well as an assessment of their financial viability.

OWNERSHIP, AWARENESS AND RELIABILITY

One of the undocumented benefits of the human error analysis is the effect on the operators and their relationship with the procedures. The human error analysis increases ownership and confidence in the procedures, making deviations less likely. Operators feel that their importance has been recognised and are proud of the output from the process.

The assessment also increases the general awareness of human error within the organisation. Importantly, it shows that human error can be reduced and that error-producing environments do not need to be endured.

Feedback from the operators on the completed operating procedures was good. They felt that their issues had been addressed. The production of the written operating procedure is not the end of the story. The procedures were 'red lined' by the operators as they were put into use. Further edits were made to the procedures using the lessons learned into the human error workshops. This collection of information and improvement process closes the loop in the 'plan-do check-act' cycle so important in any management system.

The human error analysis is a time-consuming process, requiring expert input. The importance of using experienced human factors specialists cannot be overemphasised. There is a constant tension within these assessments to depend on engineering solutions, which are commonly used within industry, rather than ensuring human operators constantly know what, when and why things are in the system.

This type of analysis moves towards the ethos of High Reliability Organisations by encouraging operational teams and managers to collectively expect human errors and constantly train, update and improve ways to recognise and recover them. Such organisations continually rehearse scenarios of failure and strive to imagine new ones.

CONCLUSION

Human factors play a critical part in the prevention of major accidents. Systematic human error assessment is a labour-intensive process, requiring a significant amount of time from specialists and operators. However, the benefits of doing this analysis well increases operators' ownership, situational awareness and confidence in operational procedures. Consequently, operators use and value procedures, rather than rendering them to the nearest dusty shelf.

Human error analysis can identify numerous and diverse actions to reduce the likelihood of operational errors and produce high quality procedures that are owned, accurate and continually reviewed to ensure they are an effective barrier in preventing major accidents. This is a key part in increasing the reliability of the overall plant process.

REFERENCES

HSE, 2008. Managing human performance: Core topic 3: Identifying human failures available from HSE web site http://www.hse.gov.uk/humanfactors/comah/core3.pdf.

EXXON, 2001. Exxon Mobil's Maintenance and Reliability System section 4 Version 2.0, August 2001, Internal company standards not publicly available.

Exxon, 2002. Exxon Mobil's Production Competency Assurance Standard Version 2.0, March 2003, Internal company standards not publicly available.