

A PRACTICAL APPLICATION OF 'HUMAN-HAZOP' FOR CRITICAL PROCEDURES

Graeme R Ellis¹ and Andrew Holt²

¹ Principle Safety Consultant, ABB Engineering Services, Daresbury Park, Warrington, Cheshire WA4 4BT, UK

² Production Manager, Chemtura Manufacturing UK Ltd, Tenax Road, Trafford Park, Manchester M17 1WT

KEYWORDS: human factors, human error, risk assessment, HAZOP, COMAH

INTRODUCTION

The accidents at Texas City and Buncefield remind us of the importance of human factors in preventing major accident hazards in the Process Industry. Much of the advice focuses on organisational factors required to ensure a motivated and competent workforce working within a good safety culture. Another key area that is often overlooked is the design of plants, processes and procedures to minimise the potential for human failures.

This paper, written jointly by ABB and Chemtura, describes a Human Reliability Assessment carried out on the Chemtura site at Trafford Park. The COMAH Safety Report describes a number of potential major accidents and their associated prevention, control and mitigation measures. Whilst many of these events are controlled by engineered protective systems, there are a few examples where actions or omissions by operating staff are critical.

A structured and qualitative risk assessment methodology was developed for these critical procedures based on guidance from HSE. The method is similar to the well proven HAZOP study for assessing new process design, but focussing on the sequence of actions carried out during a critical procedure. The key steps in the activity are identified with an experienced operator followed by a team based study to identify potential human failures at each key step, using appropriate guidewords. For credible failures the team assesses the consequences, potential to recover and other risk reduction measures. If the risk of human failure is high the team recommends improvements to minimise the likelihood for error.

This paper describes the results of the study and the key learning points for future studies. The authors believe that the 'Human-HAZOP' method developed is of wider interest for those seeking to demonstrate that the risks associated with failures of critical procedures have been reduced to 'as low as reasonably practicable'. The method could be applied retrospectively to existing operations or be used during the design stage of new processes linked to the normal HAZOP studies.

BACKGROUND

The Trafford Park site started operations as 'The Geigy Colour Company Limited' on Christmas Eve 1939. In the last 30 years the Site has been owned by Ciba Geigy and then as FMC before being bought by Great Lakes Chemical Corporation in 1999. In July 2005 Crompton Corporation merged with Great Lakes to form Chemtura Corporation. A range of speciality chemicals including phosphorus

flame retardants and fluids as well as industrial water treatment additives are manufactured on the site in a number of batch processing plants.

The site is regulated by the Health and Safety Executive (HSE) and Environmental Agency (EA) under the Control of Major Accident Hazard (COMAH) regulations as a 'top tier' site. Under the COMAH regulations, a safety report was submitted to the HSE in 2000 and this was updated in 2005.

A structured Process Hazard Review method was used to identify major accident hazards and assess the adequacy of the existing prevention, control and mitigation measures. Many of these measures are engineered safeguards such as the main control system, safety instrumented systems (SIS), relief systems, bunds, etc. Other safeguards providing risk reduction are critical procedures that require effective actions to be taken by operating and maintenance staff.

Critical procedures were also identified during a Safety Integrity Level (SIL) determination for the SIS related to major accident hazards. A quantified Layer of Protection Analysis method was used for this study. The LOPA required estimates of the probability of errors leading to hazardous events or failures to take appropriate action to halt a hazardous event sequence.

Chemtura decided to carry out further work to assess the reliability and robustness of the critical procedures identified in the COMAH and SIL studies. ABB was approached to develop a suitable methodology for the assessment, in line with HSE guidance. This method would then be trialled on one of the critical procedures associated with a major accident hazard.

HUMAN ERROR THEORY

The Process Industry has been successful in reducing the frequency of major accidents by improving equipment reliability and designing multiple layers of protection using engineered protective systems. Methods have been developed to estimate the reliability of these systems with some degree of confidence. By comparison, failures of humans involved in the process are less easy to predict.

Analysis of accidents and near misses in the industry show that a large proportion involve human failings, and it is suggested by the HSE [Ref 1] that "up to 80% of accidents may be attributed, at least in part, to the actions or omissions of people." This view is supported by detailed investigations reported by Lees [Ref 2] following major accidents such as the toxic release from the Union Carbide plant in Bhopal

and the Piper Alpha oil platform fire and explosion. These investigations identified human factors as a significant cause of the accident with failings during design, operation, maintenance and management of the facility. Various investigations into the more recent accidents at Texas City and Buncefield have also highlighted human factors as a major contributing factor.

Based on research by Reason [Ref 3], the human failures that have the potential to lead to catastrophic failures are similar to those we make in everyday life. The difference is whether the mistakes are made in an environment that is forgiving. Swain [Ref 4] comments that it is less likely that human failures are due to incompetence, poor motivation or carelessness, but rather as a result of the work situation in which the error has been made. This has led to the view that when trying to reduce the likelihood of human errors, it is more effective to concentrate on improving the work situation rather than trying to change the individual.

Human failures have been categorised by the HSE [Ref 1] as either unintentional errors or intentional breaking of the rules, known as violations. A basic assumption is that workers will continue to make unintentional errors despite being well trained and motivated. These failures are thought to be an inevitable result of skilled based activities. Errors are further divided by Reason [Ref 5] into execution failures known as slips or lapses or planning failures known as mistakes.

The importance of defining the type of human failure that could occur is to allow more suitable means of error reduction to be specified. For violations or mistakes further training of operators may be most appropriate whereas for errors by skilled operators, improvement of the work environment or design of the man-machine interface is more likely to be effective.

CCPS [Ref 6] defines performance influencing factors (PIF) as those factors that influence the likelihood of error. When all the PIFs relevant to a specific situation have been optimised it can be said that the potential for human error has been minimised. Table 1 shows a guide diagram of PIFs that were used in this study.

HSE GUIDANCE

To comply with the COMAH regulations there is a requirement to demonstrate that risks have been reduced as low as reasonably practicable. HSE is looking for operators to show that relevant good practice has been followed for all the critical prevention, control and mitigation measures.

When assessing safety instrumented systems (SIS) for example, it is possible to demonstrate compliance with an appropriate standard such as IEC61508/61511. This standard covers the lifecycle of the SIS including aspects such as specification of the safety function, design architecture, and proof testing during the operational phase.

For critical procedures relevant good practice is not as well established and many safety reports have been criticised by the HSE for failing to make an adequate

Table 1. Performance influencing factors

Factor	Sub-factor
Operating environment	Chemical process environment
	Physical work environment
	Work pattern
Task characteristics	Equipment design
	Control panel design
	Job aids and procedures
	Training
Operator characteristics	Experience
	Personality factors
	Physical condition and age
Organisation and social	Teamwork and communications
	Management policies

demonstration of robustness. This is particularly relevant for procedures as these can go into an effectively failed state very rapidly. This could happen for example, following an organisational change where the person who carried out a critical inspection is redeployed.

Companies looking to improve their demonstration of how human factors contribute to major accident hazards are referred by the HSE to their general guidance [Ref 1]. This defines human factors as covering three distinct aspects: the job, the individual and the organisation and how these impact on safety-related behaviour. The latter two factors cover the attitudes of individuals and the safety culture of the organisation. These are important aspects to consider in any human factor assessment but are not the focus of this assessment because the focus is on specific hazardous event scenarios.

Following HSE guidance [Ref 1] for job aspects, tasks should be designed following ergonomic principles and matching the job to the physical and mental capabilities of the person. This includes both the design of the workplace and working environment and matching the individual's decision-making requirements and their perception of risks. It is argued that mismatches between job requirements and people's capabilities provide the potential for human error.

HSE has provided more detailed guidance [Ref 7] on methods to identify human failures and their potential effect on major accident hazards. It is argued from their experience that very few sites will proactively seek out potential human performance problems. This guidance refers to two kinds of unintentional failures, i.e. not doing what you meant to do and doing the wrong thing believing it to be right by making a wrong decision. The other types of human failures are intentional failures or violations, knowingly taking short cuts or not following known procedures.

HSE Inspectors are being encouraged to probe companies on human factor issues, for example asking how response to a process alarm is ensured. They will be interested in how companies ensure the reliability of the operator who is tasked with responding to the alarm and how they know that the operator will always respond in the correct manner. They will expect some assessment of factors may

affect an inappropriate response, e.g. tiredness, distractions, overload, prominence of the alarm, etc.

A methodology is given by HSE [Ref 7] to carry out a Human Reliability Assessment (HRA) to determine the human contribution to risk. It is recognised that HRA has traditionally been carried out quantitatively as part of fault tree analysis. Their expectation is for qualitative assessment in the first instance, with an experienced team identifying what can go wrong and putting remedial measures in place. A 7-step procedure is outlined and described as a form of 'Human-HAZOP'. This approach was developed with ABB's standard hazard and operability (HAZOP) methods for batch processes to produce the methodology used for this study.

'HUMAN-HAZOP' METHOD

A structured and qualitative risk based approach was developed for the HRA of critical procedures, referred to as a 'Human-HAZOP'. The objective is to identify human failures during an activity and assess the potential for operator recovery or other risk reduction measures that stop this failure escalating to a major accident. When the human failure makes a significant contribution to the risk of a major accident, improvements are considered with the aim of reducing the risk of human failure to 'as low as reasonably practicable' (ALARP).

The methodology detailed in this section is qualitative and involves a team of experienced staff, broadly following the method in HSE guidance [Ref 7]. This is a general methodology that can in principle be applied to any operating or maintenance procedure.

STEP 1 – IDENTIFY 'SAFETY CRITICAL' ACTIVITIES

Safety critical activities are defined as operating or maintenance procedures with the potential to cause or limit the escalation of major accident hazards (MAH). These are hazardous events generally associated with 'loss of containment' of dangerous substances that have the potential for serious consequences, e.g. a major injury on-site or worse.

MAH associated with 'safety critical' procedures can generally be found with reference to the COMAH Safety Report risk assessment, or similar process safety study. They are also likely to be found in Layer of Protection Analysis (LOPA) carried out for SIL determination of safety instrumented systems. Whilst many hazards on process plants are usually 'engineered out' with automatic protective systems, there usually remain a proportion of hazards where procedural controls are essential to achieve the required level of risk reduction.

Safety critical procedures include physical or mental activities that:

- have the potential to initiate an event sequence, or
- stop an incident sequence, or
- prevent the escalation of an incident

For some MAH the risk of human failure may be very high, particularly when it is not mitigated by other risk reduction measures. This would be the case where the human error probability required to meet the risk criteria is lower than can be claimed using conservative data. In these cases the qualitative methodology in this procedure is not appropriate and a quantitative assessment is required using methods such as those described by Kirwan [Ref 8].

STEP 2 – HIERARCHICAL TASK ANALYSIS

A Hierarchical Task Analysis is used to list the key steps in the activity that will be used for the human failure identification stage. The level of detail at each step in the procedure is related to the specific hazardous event under assessment. There will be a number of broad steps involved in the activity, some of which will be broken down into more detailed sub-steps where required. It is therefore not a requirement to list all the steps involved in the written procedure.

The key steps are prepared in advance of the hazard identification meeting. This is done by talking to operators about how the activity is carried out in practice, watching the activity where possible, plus a review of the written procedure, check-list, job aids, training material and relevant risk assessment. The key steps will include a description of what is done, what information is needed (and where this comes from) and any interactions with other people.

STEP 3 – IDENTIFY POTENTIAL HUMAN FAILURES

A team of knowledgeable and experienced staff from the plant are required to carry out the hazard identification study. This follows a similar approach required for a traditional batch HAZOP. The team includes the following functions:

- Leader, independent process safety specialist
- Site Process Safety Specialist
- Supervisor for operation under review
- Operator or Technician with direct experience of operation

The 'Human-HAZOP' team consider each key step in the activity from the HTA, with the aim of identifying the following types of human failure:

- physical errors, 'not doing what you meant to do'
- mental errors or mistakes, 'making the wrong decision'
- procedural violations, 'knowingly taking short cuts'

To aid the team with the identification of credible human failures the following (Table 2) 'Human-HAZOP' guidewords are applied to each key step.

STEP 4 – ASSESS CONSEQUENCES

For all credible human failures the team assesses the initial and ultimate consequences assuming that there is no recovery and that other non-passive risk reduction measures fail

Table 2. 'Human-HAZOP' guidewords

Guideword	Prompt
No/none	Not completed at all
More/less	Too fast/much/long Too slow/little/short
Reverse	In the wrong direction
Sooner/later	Too early/too late At the wrong time In the wrong order
Part of	Partially completed
Other than	On the wrong object
As well as	Wrong task selected Task repeated

to prevent escalation. In many the consequences will be obtained from existing process safety studies such as the COMAH Safety Report. Any low severity events can be screened from further assessment.

STEP 5 – ASSESS POTENTIAL FOR RECOVERY

For failures with significant consequences, the team assesses the potential for human recovery from the initial failure. This could be at a later stage by the person who made the error or by an independent person such as a supervisor. The recovery process generally follows three phases: detection of the error, diagnosis of what went wrong and how, and correction of the problem. The team should ensure that all these elements can be achieved within a timescale that prevents the hazardous event occurring.

STEP 6 – ASSESS RISK REDUCTION MEASURES

The team identifies the 'engineered' risk reduction measures currently in place, including inherent, passive and active protection systems. These measures should be designed to reduce the risk of the human failure to an acceptable level of risk. The team should consider improvement options to eliminate or reduce the risk associated with human failure, following the hierarchy below:

- Can the hazard be removed by applying an inherently safe design?
- Can the human contribution be removed?
- Can the risk of human failure be reduced by further measures?

If the risk of human failure can be significantly reduced by recommendations for improvements no further assessment is required, otherwise the team consider how the likelihood of human failure can be reduced in the next step. The recommendations made at this stage will potentially involve significant expenditure and it is therefore likely that some form of cost-benefit assessment will be required of the options.

STEP 7 – IMPROVEMENTS TO PREVENT HUMAN FAILURES

Based on the causes of human failure and the potential for recovery, the likelihood is assessed by the team. This should make reference to the operational experience of the team based on incidents, near misses or audits. The objective is to assess whether events or near misses are occurring more frequently than would be anticipated from generic data. Typical human error probabilities from Kirwan [Ref 8] can be used to determine generic error rates as a benchmark for this assessment.

Factors that could affect the likelihood of the identified human failure are assessed by the team. Table 1 gives Performance Influencing Factors (PIFs) to be used as a prompt for key factors, some of which will be generic to the whole activity. PIFs are the characteristics of people, tasks and organisations that influence the likelihood of human failure. They vary on a continuum from the best practicable to worst possible. When all the PIFs relevant to a particular situation are optimal, then error likelihood can be said to be minimised, and this should be the aim of the team.

The team should consider improvements for any human failures considered to present a significant risk, such as:

- Improved or clearer written procedure
- Job aids such as checklists
- Clear signs at workplace
- Improved training and competence of staff
- Regular auditing to demonstrate compliance

Reliable and usable written procedures are important when avoiding 'mistake' type errors. A typical procedure should have the following elements:

- Purpose of the procedure;
- Precautions which must be observed to avoid potential hazards;
- Special tools or equipment needed;
- Initial conditions which must be satisfied before starting;
- References to other relevant documents, e.g. data sheets or manuals; and
- Procedural steps to perform the task safely and efficiently

The improvements at this stage are likely to be relatively low cost and within the budget and capability of the operational team. The justification for implementation should therefore be based on a qualitative team judgement of practicality and benefits.

STEP 8 – RECORD OF 'HUMAN-HAZOP'

The results of the HRA are recorded on a 'Human-HAZOP' record table with the following columns:

- Step: Description of task by person carrying out activity
- Human Failure: Description of credible human failures when carrying out this task based on guide diagram

- Consequences/Severity: Ultimate consequences of the human failure if there is a failure to recover or mitigate the event
- Potential to recover/Likelihood: Potential for human recovery involving detection of problem, diagnosis and correction of failure
- Risk Reduction Measures: Risk reducing measures to prevent escalation of the incident that do not involve human intervention
- Recommendations: Practical actions to reduce the potential for failure based on the PIFs or for further risk reduction measures based on the hierarchy of measures

PRACTICAL EXPERIENCE SELECTED ACTIVITY

The methodology described in this paper was trialled on a COMAH scenario selected from the site Safety Report where human factors were known to be significant. This involved offloading of organic peroxide from 200 litre drums from a dedicated unloading bay into storage tanks. This operation has the potential for ignition of an explosive atmosphere within the drums. A serious explosion and fire occurred on the facility a few years ago and the design of the unloading process had been improved in light of this experience. Nevertheless, this scenario was judged to present a risk at the upper end of the ALARP band during the COMAH risk assessment.

The basis of safety for this operation is to purge the drums with nitrogen prior to inserting a dip-pipe into the drum and starting the pump-out stage. A key step is the operator connecting a flexible nitrogen hose to the drum vent hole. Interlocks have been installed to prevent the dip-pipe being removed from its mount or the offloading pump running before the nitrogen purge flow and purge time are completed. It was realised prior to the HRA that errors could still be made by the operator that would cause the basis of safety to be compromised.

HIERARCHICAL TASK ANALYSIS

The written procedure for the peroxide drum offloading operation was reviewed prior to the 'Human-HAZOP'. This includes a number of steps that were judged to have little relevance to the hazardous event of interest. The procedure was therefore broken down into the key steps that could either prevent or mitigate the effects of a drum explosion/fire. For example, the procedure requires the pallets of full and empty drums to be kept on the delivery lorry at all times, except the pallet that is currently being unloaded. As the lorry is separated from the unloading bay this limits the size of a fire to the 4 drums on the pallet in the worst case.

The key steps derived from the written procedure were found to be a suitable starting point for the study as the procedure was fairly up-to-date. This is unlikely to always be the case and development of the key steps is

likely to involve detailed discussions with an experienced operator and/or observation of the activity. In this case, further details were added to the key steps as the study progressed along with any departures from the written procedure.

ON-SITE OBSERVATION

The opportunity was taken for direct observation of the drum unloading activity prior to the 'Human-HAZOP' team meeting. This would not be an option for a new process but should always be done for existing processes to confirm the accuracy of the written procedures and observe the workplace environment at first hand.

On this occasion the unloading operation was being carried out by a shift operator rather than the usual 'day' operator. Although this operator had been trained for the activity he was less experienced and was found to have failed to perform a number of the key safety related steps. This finding helped to focus the team attention on the potential for human failures and raised questions on the management failures that had allowed this situation to arise. A contributing factor was a gradual change from plastic to metal drums by the supplier, with both types of drum in use at the time. This led to an over-focus on a new requirement to attach earth cables to the metal drums whilst forgetting to follow the basic safety requirements.

HUMAN-HAZOP MEETINGS

The study followed the overall methodology described in this paper with a table of results being completed in the normal style for HAZOP studies. The nodes for the HAZOP were the key steps in the drum unloading activity derived during the HTA and the site observations.

The team found it useful to focus on just the key steps that could affect the hazardous event scenario under assessment. Previous attempts on the site to review procedures had become bogged down in the detail of steps with little relevance to major accident hazards. This factor greatly assisted the completion of the study within a reasonable time period.

RECOMMENDATIONS

A number of general actions were raised that related to the entire activity:

- Written procedure to be updated to highlight the key hazards and steps identified in the study. This must also reflect the current need to unload from both plastic and metal drums, clarifying the different safety requirements.
- Review the site arrangements for training and re-validation of training for operators on safety critical tasks.
- Provide a sign in the peroxide unloading bay with the key safety steps to be followed as a visual reminder to operators.

- Implement a system for routine auditing of safety critical procedures to ensure that the key steps are being correctly followed

Other actions related to specific steps in the activity. For example, it was recognised that the nitrogen hose may not be attached to the drum because of different vent hole sizes on metal and plastic drums, and the need for an adaptor to be fitted to the drum. A recommendation was made to provide a shadow board for the adaptor in the unloading bay to ensure it would be clearly visible to the operator.

CONCLUSIONS

This paper has described a practical and structured methodology for the assessment of critical procedures, using a 'Human-HAZOP' approach that follows guidance provided by the HSE. It is intended to be used for any operating or maintenance procedure that provides critical risk reduction for major accident hazards, either on existing plants or during the development of new processes. The objective is to recognise the critical tasks in an activity, identify what can go wrong, and assess how the workplace can be designed to minimise the probability of error.

A key feature that proved beneficial in the study was to focus on the key steps in an activity that could affect the risk of a specific hazardous event. This allows the team to concentrate their efforts on issues of greatest risk and allows the study to be performed effectively within a reasonable time period.

For this study a qualitative approach using the judgement of an experienced team was found to be sufficient. This allowed a focus on relatively low cost improvement options to make the operating environment less error prone. The recommendations were therefore in the following categories;

improvements to the written procedure, a more visual workplace with appropriate signs, improving the man-machine interface design of equipment, improved training and supervision for critical tasks. Most of these improvements could be followed up by the operations team within their budgets.

In cases where a human failure is found to present a high risk of a major accident hazard a more detailed study may be required. Further 'engineered' protective systems may need to be assessed using a cost-benefit approach. Where these are not practicable a quantified HRA may be required to justify a probability of error that is much better than an estimate based on conservative generic data.

REFERENCES

1. HSE, HSG48, 2nd edition 1999, reprinted 2003, Reducing error and influencing behaviour, HSE Books.
2. Lees, F., 1996, Loss prevention in the Process Industries, Butterworth Heinemann, Oxford.
3. Reason, J and Mycielska, K., 1982, Absent Minded? The psychology of mental lapses and everyday errors, Prentice-Hall, New Jersey.
4. Swain, A.D., 1972, Design techniques for improving human performance in production, Industrial and Commercial Techniques Ltd, London.
5. Reason, J., 2002, Human Error, Cambridge University Press.
6. CCPS, 1994, Guidelines for preventing human error in process safety, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York.
7. HSE, Core Topic 3, Identifying Human Failures, Inspectors Human Factors Toolkit, HSE Web-site, updated Feb 2009.
8. Kirwan, B., 1994, A guide to practical human reliability assessment, CRC Press.