CHEMICAL ENGINEERING TRANSACTIONS

VOL. 31, 2013

Guest Editors: Eddy De Rademaeker, Bruno Fabiano, Simberto Senni Buratti
Copyright © 2013, AIDIC Servizi S.r.l.,
ISBN 978-88-95608-22-8; **ISSN** 1974-9791

A publication of
AIDIC
The Italian Association
of Chemical Engineering
Online at: www.aidic.it/cet

DOI: 10.3303/CET1331051

Incorporating Human Error Analysis into Process Plant Safety Analysis

John R.Taylor

ITSA, 39 Prunusvej, Alleroed Denmark
JRT@ITSA.DK

A description is provided of a human error analysis methodology which is intended to mesh smoothly with other process plant hazards analysis methods, especially HAZOP. Also provided is a description of data collection to support the method over a period of 35 years.

1. Introduction

It is a generally recognised fact that human error plays a large role in causing process plant accidents, including major hazards accidents. However, in contrast to the situation in the nuclear and aerospace industries, very little human error analysis is carried out in the petroleum, petrochemical and chemical industries. Where it is performed, it is largely unrelated to the HAZOPs and QRAs which are the heart of process plant safety assessment.

There are several reasons for this. Firstly, it is quite hard to do, requiring considerable effort from already hard pressed engineers. Secondly, exiting methodologies do not mesh well with existing safety analysis practice. Thirdly, for new plants, the timing of preparation of operations descriptions and procedures comes at the end of detailed design, sometimes with finalisation after commissioning is complete. With no operations information to work with, it is not possible to carry out analysis.

It is often claimed that this does not matter because releases caused by human error are already included in release frequency databases. Examination of several such databases reveals that this is true only to a limited extent. More problematically, there are many human errors which bypass designed safety measures, and create completely new scenarios. Further, when operators or maintenance technicians are a cause of accidents, they are almost always present, so that the risk to employees is higher because of higher exposure. Most importantly of all, with no consideration of human error, there is no incentive, and very little possibility, of applying risk reduction techniques.

The approach described here uses the action error analysis method, which was developed and validated in the period 1978-1980 at the Risø National Laboratory in Denmark (Rasmussen, Taylor., 1976, Taylor, 1978, Taylor et al. 1982). It combines one of the original methods of Hazop described in the Chemical Industries Association guidebook of 1976, the SKR model of human error developed by Pr. Jens Rasmussen (Rasmussen 1974), and data collected by the present author in a long series of projects extending over the last 32 years (Taylor, 2012). The method was chosen because it fits very well with the Hazop analysis approach, and can be applied by process and instrument engineers, rather than requiring HRA specialists because it combines human error analysis with equipment failure analysis, and because it allows analysis of latent failures and hazards triggered by correct operator and maintenance technician actions.

2. The action error analysis method

The action error analysis method is most easily described as applied to a standard procedure, such as draining water from an oil storage tank, or replacing a filter. The starting point is a written procedure, describing how the task should be done, together with piping and instrumentation diagrams , cause and effect matrices for control description and similar documentation typically required for HAZOP studies.

The analysis proceeds in a similar way to HAZOP studies, and will often be part of a HAZOP study since this conveniently establishes the context for the analysis. .Each step in the operating procedure regarded as a

Please cite this article as: Taylor J.R., 2013, Incorporating human error analysis into process plant safety analysis, Chemical Engineering Transactions, 31, 301-306 DOI: 10.3303/CET1331051

HAZOP node, and the deviations considered in the analysis are the error modes applicable for operations , drawn from the list in Table 1.

Table 1 Standard error modes for action error analysis

Omission
Too early/too late
Too fast/too slow
Too much/too little
Too hard/too slight
In wrong direction
In wrong sequence
Repetition
Wrong object
Wrong substance
Wrong materials
Wrong tool
Wrong value
Extraneous action (one unrelated to the task but interfering with it)
Wrong action
Other similar wrong choices for each aspect of the task step (E.g. wrong label placed on a product package)

The consequences of the erroneous actions are then noted, together with safety measures in place. These may include the operators own error recovery actions. If the measures are deemed to be inadequate, recommendations for improvement are made (as in any HAZOP)

It is convenient to enter the data initially into a cause consequence diagram format, rather than usual HAZOP tables because this allows the sequence of actions, effects and safeguards to be defined. A standard template for this is shown in fFigure 1. When the analysis is recorded on computer the cause consequence diagram can be extended conveniently, so that longer lists of consequence events and mitigating measures can be taken into account.

Historians will recognise the procedure so far as a variant of the original manufacturing Chemists association guidelines for HAZOP analysis, with a more elaborate and specific check list. So far there is no need for any special human reliability expertise, only understanding of process engineering and control.

3. Supervisory control and Emergency response

Not all operator actions involve step by step procedures. A large part of the operators time in the control room is spent in monitoring the process. If a parameter deviation shows on the display or an annunciation or an alarm does occur the operator should generally respond. This kind of activity can be incorporated into the action error analysis by regarding each alarm, annunciation or process parameter disturbance as a hazop node, and applying the error check list as a deviation in the alarm response.

4. Latent failures and latent hazards

It is convenient during the action error analysis to include latent hazards and latent failures triggered by the operator performing task steps correctly. An example is filling of reactants into a kettle type reactor which is already too hot due to steam leakage from a failed control valve into the reactor jacket.

There is a good heuristic for identifying such latent failures and hazards. For each step in the procedure, the sequence of events resulting from the task step is recorded. For example in starting a motor, the operator pressing the start button is followed by the contacts closing, electrical current flowing, the motor turning the impeller, flow starting and liquid being transferred e.g. to a vessel. Then for each step, the failure modes of equipment (those which would be tabulated in an FMEA for example) may be recorded in the cause consequence diagram. Similarly, hazardous states, such as the receiving tank already being full, can be identified using standard HAZOP keyword lists. It should be noted that in tracing sequences of events in a P&ID, loop diagram or an electrical single line diagram etc. events may progress against the fluid or electrical flow. For example the pump may fail to start when the start button is pressed not only because the contact is failed, but also because there is an open circuit between the button and the pump, an open circuit in the electrical supply or the power supply failed.

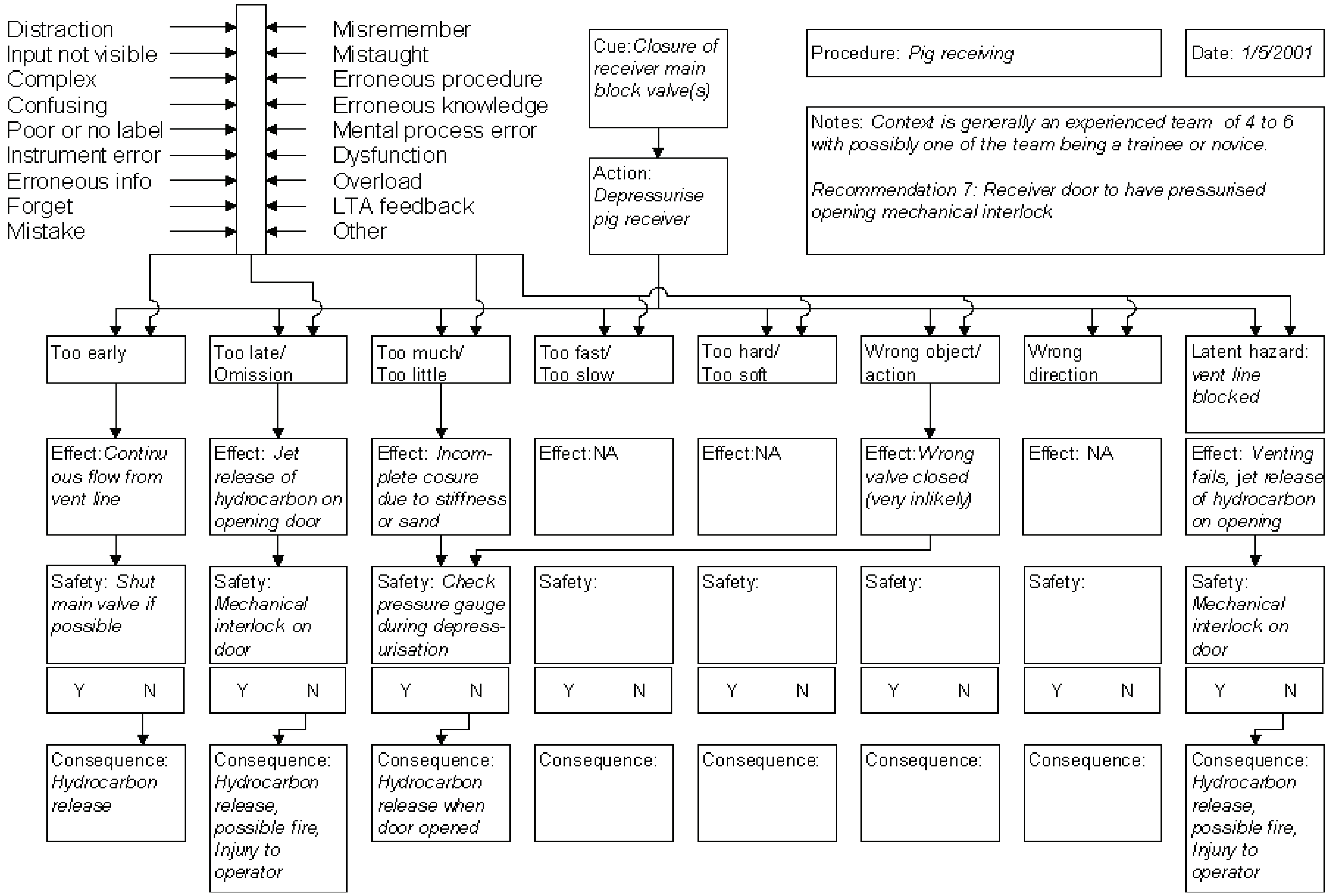
Distraction
Input not visible
Complex
Confusing
Poor or no label
Instrument error
Erroneous info
Forget
Mistake
Misremember
Mistaught
Erroneous procedure
Erroneous knowledge
Mental process error
Dysfunction
Overload
LTA feedback
Other
Cue: Closure of receiver main block valve(s)
Action: Depressurise pig receiver
Procedure: Pig receiving
Date: 1/5/2001
Notes: Context is generally an experienced team of 4 to 6 with possibly one of the team being a trainee or novice.
Recommendation 7: Receiver door to have pressurised opening mechanical interlock
Too early
Too late/ Omission
Too much/ Too little
Too fast/ Too slow
Too hard/ Too soft
Wrong object/ action
Wrong direction
Latent hazard: vent line blocked
Effect: Continu ous flow from vent line
Effect: Jet release of hydrocarbon on opening door
Effect: Incom- plete cosure due to stiffness or sand
Effect:NA
Effect:NA
Effect: Wrong valve closed (very inlikely)
Effect: NA
Effect: Venting fails, jet release of hydrocarbon on opening
Safety: Shut main valve if possible
Safety: Mechanical interlock on door
Safety: Check pressure gauge during depress- urisation
Safety:
Safety:
Safety:
Safety:
Safety: Mechanical interlock on door
Y N
Y N
Y N
Y N
Y N
Y N
Y N
Y N
Consequence: Hydrocarbon release
Consequence: Hydrocarbon release, possible fire, Injury to operator
Consequence: Hydrocarbon release when door opened
Consequence:
Consequence:
Consequence:
Consequence:
Consequence: Hydrocarbon release, possible fire, Injury to operator

Figure : Action error analysis format for one step

Latent failures are generally ignored in QRA. This is an important omission, because a large fraction of the major accidents occurring in process plant actually involve latent failures and hazards . HAZOP analysis captures some, but generally not all, of these, mostly those which are localised to the current node, and mostly those related to the process itself.

5. Error causes

Identifying error causes is important because identification of causes allows prevention measures to be incorporated into procedures and equipment designs. One of the first applications of the method, for example, was development of interlocks and permissives, and physical barriers, for a sodium methylate batch reactor after a serious accident.

Error causes are identified in the action error analysis method using a check list based on the SKR model developed by (Rasmussen 1974). The list of possible human error causes was originally developed by applying the FMEA process to this model. The list of causes was validated by checking the list against accident case stories. Some confidence was gained by the identification of unanticipated error causes which were later identified in accident root cause analyses.

The full list of causes is extensive and will not be given here since it is very long. An excerpt is given in Table 2 as an example.

The error cause check list allows prevention measures to be defined, and more importantly, to be taught, so that human reliability techniques can be incorporated naturally into the design process.

6. Quantification

In modern safety engineering practice, accident frequency calculation is required for land use planning QRA, fire and blast risk assessment, SIL review and many design calculations. Human error probabilities and frequencies are needed to support these analyses.

Collecting human reliability data is far from easy. It should preferably be collected in place from actual operating plant, with real plant operators. The frequency of occurrence of errors in this type of environment is low, several thousand hours of observation has proved insufficient to allow capture of more than a few serious errors.

Actually working in plants over a period of some 30 years, as safety engineer, commissioning engineer and occasionally as plant manager has allowed collection of data from incident and near miss investigations. There is still a problem that data for only a fraction of possible error causes and situations can be identified, even over this extended time.

Table 2 Excerpt from operator error cause list

Cause groups	Error causes	Error reduction measures
Action prevented	Attention failure Comfort call Operator sheltering Distraction Overload Priority error Action hindered	Proper manning, with alternate operator. Sheltered operator station in the field for tasks involving waiting. Good telephone discipline. Good access for operations, stairs rather than ladders, access platforms. Avoid creating locked off areas. Disturbance response training based on hazop analysis.
Observation error	Hidden cue, symptom Mistaken cue, symptom Cue overlooked Symptom overlooked Missing cue or symptom Parallax Mistake Mislearning	All cues for action should be clearly visible on displays. Physical fidelity in display Human factors criteria for alarm frequency, display size. Unit specific training with good training material. Procedural display

The solution to this problem, described by (Kirwan 1994), is to determine “anchor points”, that is cases with similar errors for which the frequency or probability can be determined, from the number of incidents and frequency of the operation. Then the ratio of occurrence of these errors to that of other error types can be determined from the much more extensive data bases of incidents (such as national labour inspectorate data bases)for which the frequency of task performance is not known A methodology called the Accident Anatomy method was developed. In this method consequence diagrams of typical accidents, and then records on these the actual occurrences, giving the relative frequency of different aspects of the accidents. This allows several statistical data points to be extracted from each incident report. To date some 60 anchor points and over 200 typical accident types have been quantified in this way (Taylor 2012)

7. Validation

The action error analysis method was validated qualitatively in a study in 1978 to 1991 in which a urethane reactor and multi-product batch distillation plant were designed with the aid of hazop, action error analysis and a few other methods and then the plant was built and followed for several years. The analyses were performed by several teams to allow comparisons. The results are shown in Figure 3. (Taylor 2012)

Validation of quantitative results has only recently been possible with access to a large body of accident and near miss reports, and the possibility to interview many operations supervisors. A number of standard process plant operations were studied using action error analysis, and then comparing with historical records for accidents for the overall procedure. Results are given in Table 3.

Even though the results are quite uncertain, they are well within the bounds of typical process risk analysis uncertainties. The pattern of causes of the incidents was also reasonably well reproduced. One of the observations from the studies was that human error caused incidents varied very much according to equipment design, which was not unexpected; and the very large dependence on experience and knowledge, which was larger than anticipated. Experience of earlier accidents, in particular was important.

8. Practical aspects

The practical difficulties of cost and timing mentioned in the introduction still represent a problem. To overcome the timing difficulty, that procedures and sanding orders are not available at the design time when analyses would be most effective, generic procedures were developed and assessed. The recommendations from these were listed, along with lessons learned from accidents and near misses, and proven risk reduction measures.

The cost of running hazop workshops is currently between $500 and $1,000 per person per day, in countries with western salary rates, and typical hazop teams vary in size from 5 to 20 persons. More importantly, taking experienced people from a design team for a period is seriously painful for most project managers and their completion schedules. Adding a new procedure to the already long list of safety studies in modern safety engineering practice is not likely to be popular. On the other hand, analyses performed by a single specialist have generally proved unsatisfactory due to incompleteness. In practice the analyses have proved to fully justify the cost, in terms of problems eliminated.

Some steps were made to reduce the costs, including providing action error analysis support tools; developing an intelligent P&ID and procedure display system which can trace system which can display disturbance propagation through a complete set of drawings; automated generation of alarm sets from disturbance simulation; and automated sneak analysis. The most effective tool for time and cost reduction though has proved to be the generic analyse, along with guidelines for adapting them to actual situations.

Table 3 Validation studies for prediction accuracy of action error analysis

Operator or maintenance task	Ratio of prediction to observation
Pig receiving on oil pipelines	2.4:1
Changing a large bucket filter	1.8:1
Isolating an H2Sabsorber unit in preparation for maintenance	0.62:1
Replacing a motor for repair	3.1:1
Changing out a heat exchanger tube bundle	7.7:1
Taking a sample of hydrocarbon condensate	1.6:1
Taking down a pressure safety valve for testing	0.87:1

9. Conclusions

Human error analysis has been claimed to be important for over forty years, with no counter argument. In some industries, such as the nuclear industry, human error analysis is a standard technique. With a few honourable exceptions, human error analysis has been neglected on the oil, gas and chemical industries. Certainly in risk assessments, human error, although agreed to be important, is ignored. The standard procedures for process plant risk analysis do not even mention the issue.

Risk analysis and safety engineering has come a long way in the 40 years or so that techniques have existed. The conclusions from the present extended project are that it is possible to make human reliability assessment methods practical, and that they can be applied by working engineers and safety specialists as a part of standard engineering procedures, even in the hectic world of process plant design and operation.

References

Rasmussen J., Taylor J.R., 1976, Notes on Human Factors Problems in Process Plant Reliability and Safety Prediction, Risø-M-1894, www.risoe.dk/rispubl/reports/ris-m-1894.pdf (15 January 2013)

Taylor J R, 1978, A Background to Risk Analysis, Risø National Laboratory, Denmark

Taylor,J.R., Hansen, O.M., Jensen C., Jacobsen O.F., Justesen M., Kjærgård S., 1982, Risk Analysis of a Distillation Unit, Risø-M-2319,Risoe National Laboratory, Denmark www.risoe.dk/rispubl/reports/ris-m-2319.pdf, (15 January 2013)

Chemical Industries Association, 1977 A Guide to Hazard and Operability Studies, UKRasmussen J., 1974, The Human Data Processor as a System Component, Bits and Pieces of a Model Risø Report R-8-74, Risø National Laboratory, Denmarkwww.risoe.dk/rispubl/reports/ris-r-74.pdf (15 January 2013)

Taylor J.R., 2012, Human Error in Process Plant Operations, ITSA, Denmark, 2012

Rasmussen J., 1982, Skills, Rules & Knowledge; Signals, Signs & Symbols and Other Distinctions in Human Performance Models., Risø-N-4-82. www.risoe.dk/rispubl/reports/ris-n-4-82.pdf (15 January 2013)

Rasmussen J., Mancini G., Carnino A., Griffon M., Gagnolet P., 1981 Classification System for Reporting Events Involving Human Malfunctions, RISØ-M-2240, www.risoe.dk/rispubl/reports/ris-m-22240.pdf, (15 January 2013)

Taylor J.R., 1976, Interlock Design Using Fault Tree and Cause Consequence Analysis, Risø-M-1890, Risoe National Laboratory, Denmark

Taylor J.R., 1992 Risk Analysis for Process Plant, Pipelines and Transport, Taylor and Francis/Spon

Kirwan B., 1994, A Guide to Practical Human Reliability Assessment, Taylor and Francis, London, UK