Intelligent Operating Procedures: A Human Factors Safety Analysis Based Approach to Work Instruction Development

Dr David Embrey, Managing Director, Human Reliability Associates, 1 School House, Higher Lane, Dalton, Wigan, Lancs WN87RP, UK

Richard Marshall, Human Factors Specialist, Essar Oil (UK) Limited, Stanlow Manufacturing Complex, PO Box 3, Ellesmere Port, Cheshire, CH65 4HB UK

Many deficiencies have been identified in the standard operating procedures found in the oil, gas and chemical processing sectors. These include poor structuring, and significant differences between the way in which a plant operated in reality, and the information contained in the procedures. These problems arise from a lack of a systematic process which gathers information from the end users of the procedures and structures this information in a manner which makes them easy to understand and learn. A new approach is needed in which process hazards arising from potential human errors are explicitly identified and incorporated into the procedures.

This paper describes a process called Intelligent Operating Procedures (IOPS) design, which is linked to the human factors safety critical task reviews that are required for COMAH safety reviews. This enables both procedures design and competence management systems to be linked to a systematic human factors risk analysis process. A case study showing the application of this process to a petrochemical task will be described.

Keywords: Operating procedures, Human factors, COMAH safety Reports

Introduction

Standard operating procedures (SOPs) are intended to specify the way in which a plant is to be operated and maintained in order to ensure safe and efficient production. Procedures should ensure that a hazardous safety critical task is carried out in a standardized manner in which potential failures with serious consequences have been identified and mitigated. Unfortunately, many SOPs used in high hazard industries fall short of these objectives. Procedures often comprise long lists of task steps which bear little relationship to how the plant is actually operated. This is because they are often written by personnel who have limited practical operating experience. This creates a number of significant safety and operational problems. If the procedures are impractical and inaccurate, they may lose credibility with operating staff, leading to untested and possibly unsafe methods being be adopted in order to get the task completed. Reliance on informal operating practices may also lead to inconsistencies between different shifts and to variations between trainers in the information they transmit to trainees. Failure to document the tacit knowledge possessed by operating staff based on operating experience also represents a lost opportunity to capitalize on their experience.

Procedures are frequently poorly structured in terms of identifying the objectives that need to be achieved during the different stages of a process. This makes the procedure difficult to understand and harder to learn. Frequently, no distinctions are made between information intended to tell the user specifically what to do, and supplementary information which would be more appropriate in a training context. In addition, there is rarely any real attempt to link the content of procedures with human factors risk analyses, so that the knowledge of potential failures with significant consequences that emerges from these analyses can be transmitted to the operator in a systematic manner.

In this paper we describe a structured, risk based process called the ‘Intelligent Operating Procedures System’ (IOPS). The term ‘Intelligent’ refers to a process that systematically identifies the risks that the users of the procedure need to be aware of in the operating environment, and delivers this information at the appropriate point in the procedure. Another ‘intelligent’ aspect of the IOS process aspect of the IOPS process is the structuring of a task in a hierarchical manner, that identifies the overall task objectives, and the subtasks required to achieve these objectives. The IOPS process develops plans which describe how these subtasks are executed based on operational conditions. The structure provided by the process makes the resulting procedures easier to understand and also much easier to learn.

The core methodology within the IOPS design process is SHERPA, (Systematic Human Error Reduction and Prediction Approach) was originally developed in nuclear power generation safety analyses (Embrey, 1986), and has subsequently been used as a safety analysis tool within many safety critical industries. A recent review of this methodology illustrating its application in chemical industry safety analyses is available in Embrey, (2013).

The IOPS process mirrors the Human Factors Critical Task Reviews (HFCTR) carried out as part of COMAH (Control of Major Accident Hazards) safety reviews (Energy Institute, 2011, Health and Safety Executive, 2012). As a result, very little additional effort is required to utilize the information generated during the HFCTR as the primary input to the IOPS process. Apart from the saving in the resources by only having to gather this information once, the IOPS process satisfies the HSE requirement to demonstrate that the results of HFCTR are reflected in the Procedures and the Competency Management systems.

In the next section, we will describe the stages of the IOPS process and illustrate how these parallel the application of SHERPA in COMAH Human Factors safety reviews. A similar process can also be used to develop Competency Management Systems.

Overview of the IOPS process within COMAH task reviews

The IOPS development process consists of the following stages:

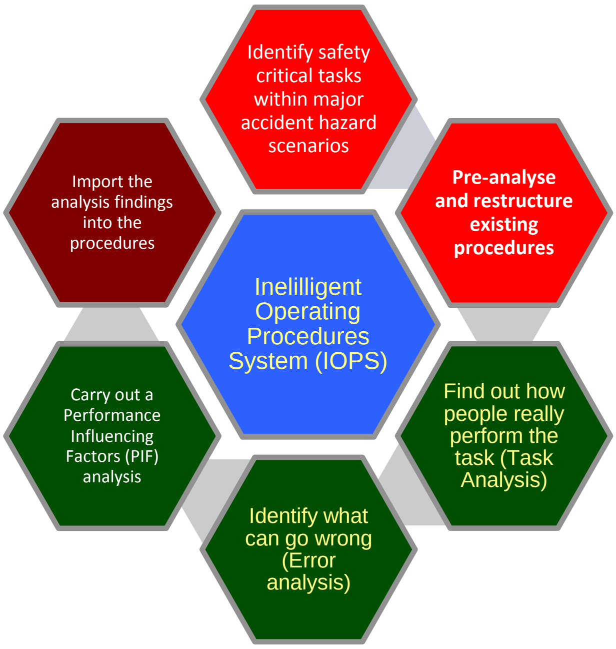
Identify safety critical tasks within major accident hazard scenarios
Pre-analyse and restructure existing procedures
Find out how people really perform the task (Task Analysis)
Identify what can go wrong (Error analysis)
Carry out a Performance Influencing Factors (PIF) analysis
Import the analysis findings into the procedures
Inelilligent Operating Procedures System (IOPS)

Figure 1: Overview of the IOPS process

Identify safety critical tasks within major accident hazard scenarios

The first step in both COMAH task reviews and IOPS development process is a workshop in which the Major Accident Hazard (MAH) scenarios identified from previous engineering risk analyses such as HAZOPs are reviewed to identify human activities which could:

- Initiate the accident sequence (e.g. an object dropped by a crane operator could rupture a pipeline)
- Affect the ability of engineering safeguards to mitigate the accident scenario (e,g. by failing to correctly maintain gas detectors or high level trips).
- Fail to carry out mitigation activities such as post release emergency plan implementation

If a previous safety analysis such as a HAZOP is not available, an alternative approach is to first identify plant areas where activities with potential MAH risks could exist. These could include areas where toxic or flammable substances are involved, and where tasks are carried out where layers of protection are removed, e.g. during maintenance. A scoring process can then be used (Health and Safety Executive 2000) to risk rank tasks so that analysis resources can be prioritized according to the ranking assigned to each task.

Pre-analyse and restructure existing procedures

The objective of the pre-analysis process is to organise the existing procedure and other relevant documents into a structure which provides a starting point for a later workshop analysis involving operating staff. Carrying out a pre-analysis also identifies operational issues that will need to be explored in the Stage 3 workshop described below. The pre-analysis process also reduces the time required to conduct this later analysis. The pre-analysis involves the IOPS facilitator conducting a preliminary task analysis of the existing procedure using a methodology called Hierarchical Task Analysis (HTA). This is described in detail in Kirwan and Ainsworth (1992) and Embrey (1994). The HTA is essentially a graphical representation of the task structure. It breaks complex tasks down into a series of subtasks, governed by a plan that specifies how these are performed in order to achieve the overall task objective. If necessary, subtasks are broken down to finer levels of detail, and a new plan is developed at each stage of the breakdown.

A detailed example of an HTA will be provided in the Case study in the last section of this paper. The HTA process is re-applied in Stage 3 of IOPS which is described below.

Develop a Hierarchical Task Analysis using a Consensus Group workshop

The Consensus Group workshop is intended to reach agreement about how tasks are carried out in practice, based on inputs from experienced operating personnel. The starting point is the preliminary task analysis developed during the pre-analysis.

The IOPS facilitator develops a graphical representation of the task structure using Hierarchical Task Analysis. This can be performed using manual methods such as Post-it notes. However, for complex tasks, specialist software tools such as the Human Factors Risk Manager (HFRM), developed for HFCTRs by Human Reliability Associates, and other tools such as Task Architect are available, which facilitate the interaction with the workshop participants, and which automatically document the analysis in the form of a Word table or spreadsheet. The development of the HTA using the Consensus group is one of the most important stages of the IOPS process as it provides the information to structure the task in a clear and understandable manner. It is also the vehicle identifying the potential risk information such as errors with serious consequences, which needs to be embedded in the final version of the procedures.

Perform a Predictive Human Error and Consequence Analysis (PHECA)

This stage of IOPS uses the graphical task analysis developed during stage 4 to identify potential errors leading to Major Accident Hazard (MAH) consequences. This is achieved by first identifying the Activity types involved in the procedures. Examples of Activity types include Actions, Checking, Monitoring and Communication. Each activity type has an associated set of failure modes, for example Action omitted, Right action wrong object (Actions), Monitoring omitted, wrong variable monitored (Monitoring) and check omitted, wrong object checked, check too late (Checking). These failure modes are used by the analysts during the workshop to provide a prompt for the workshop participants with regard to whether the failure mode could occur, and if so, what would be the consequences. These failure modes perform a similar function to the Guidewords used in HAZOPs. The failure modes are documented in the COMAH human factors report and are also subsequently transferred into the procedure which is developed by the IOPS process to provide the basis for warnings and comments.

Carry out a Performance Influencing Factors (PIF) analysis

PIFs are the factors which increase or decrease the likelihood that the failures identified during the previous stage will actually arise. The results of the analysis can provide recommendations to modify the PIFs to reduce the likelihood of errors. Task specific PIFs are error inducing factors that are unique to the task environment being studied. They might include factors such as the quality of the alarm system, organisation of the DCS displays, and the labelling of plant items such as valves. In the analysis documentation, PIFs descriptions are preceded by the labels -ve or +ve indicating that the PIFs are likely to have positive or negative effect on the likelihood of error. An example of such a PIF analysis is shown in Figure 2 below. Some of the PIF deficiencies identified at this stage of the process will have implications for procedures development process. The example shown in Figure 2 provides information that could potentially be included in the procedure, e.g. that the low pressure alarm on 25-PC-005 may indicate a problem with the surge tank seal.

Generic PIFs are factors influencing error probability associated with each activity type. Example include levels of distractions, fatigue, and time pressure. These types of PIF are important for optimizing operational conditions and hence reducing error likelihood, but are less relevant for procedures development.

-ve: Alarm (for low pressure) on 25-PC-005 is a low priority alarm. This provides the first indication of a potential problem with the surge tank seal - this prioritisation may affect how quickly this problem is identified by the Control Room Operator (CRO) (i.e. during times of high alarm load)
+ve: Rate of opening of 24-PC-005 is clearly presented on the DCS (this enables the initial verification of a seal pot leak).
+ve: Large alarm overview screen is available in the CR (and actively used by most operators)
-ve: Several CRTs were unaware as to how to access point-of-use alarm response manuals within the DCS.

Figure 2: Example of Task specific PIF analysis

Import the analysis findings into the procedures

In this final stage, the ‘Intelligence’ gathered during the preceding stages of the IOPS process is incorporated into the procedure. Although the exporting of the task analysis information into the procedure is greatly facilitated by the use of software tools, it can be done by hand if only a small number of tasks is being analysed.

The main types of information that are imported are as follows:

Standard headings, ‘boilerplate’ information and procedures formatting conventions

Most organisations have a standard procedures format which includes standard headings, logos and quality control information. In addition, there may be standard information about the hazards in the substances being used in the task, the PPE required and global risk management information. All of this information can be incorporated into a software template, and automatically added to the content derived from the task analysis to produce a fully customised procedure.

Structural information

The structure of subtasks, plans and task steps developed during the task analysis are directly translated into the structure of the procedure. This ensures that the procedure is easy to read, understand and learn. The translation process uses a to map the task structure developed in the Consensus Group HTA to the procedures preconditions, objectives, and the subtasks and steps required to achieve these objectives. The template also determines the relationship between the information in the task analysis and its location in the final procedure.

Warnings and comments

The PHECA risk analysis carried out in step 4 of the IOPS process allows the identification of task steps where potential failures that could impact on safety or production might occur. This information is captured in a spreadsheet-like data grid during the analysis and used to place warnings at appropriate points in the procedure. Comments, for example, background information about why a particular step is required are also translated from the spreadsheet into the procedure in a similar manner.

Roles and responsibilities

During the task analysis process in Step 4, the roles and responsibilities of personnel to carry out the tasks and subtasks are defined. This information is recorded in the analysis report generated by the IOPS process and can then be exported into the procedure and located in a manner determined by the template.

Document the results of the task review analyses into the COMAH safety report

In this paper we have focussed on the use of the methodology in the context of procedures development. However, as mentioned previously, the outputs from Steps 1-5 are identical to those recommended by the HSE for carrying out COMAH human factors task reviews. These are documented in a separate COMAH report which includes the task analysis in a text based format, the documentation of the failure modes identified in Step 4, and the PIF analysis in Step 5.

Case Study

In this section we will provide a simple case study to illustrate the stages of the IOPS process. We assume that the task under consideration has already been identified as being safety critical during Stage 1 of the IOPS process.

Task Analysis (Stages 2 and 3)

The top level for the HTA task analysis shown in Figure 3 is developed during Stages 2 and 3

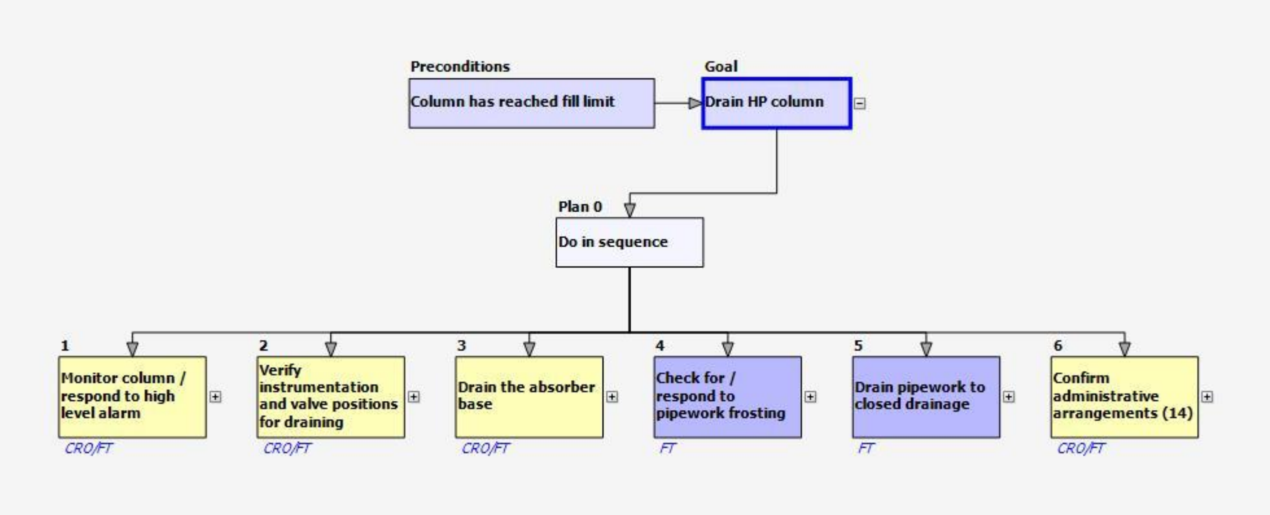
Preconditions
Column has reached fill limit
Goal
Drain HP column
Plan 0
Do in sequence
1
Monitor column / respond to high level alarm
CRO/FT
2
Verify instrumentation and valve positions for draining
CRO/FT
3
Drain the absorber base
CRO/FT
4
Check for / respond to pipework frosting
FT
5
Drain pipework to closed drainage
FT
6
Confirm administrative arrangements (14)
CRO/FT

Figure 3: Top level of HTA for drain HP column task, showing subtasks

In Figure 4 we show how subtask 2 is broken down into further detail, together with the associated plans which specify the conditions determining the order of execution for the lower level subtasks and their individual steps.

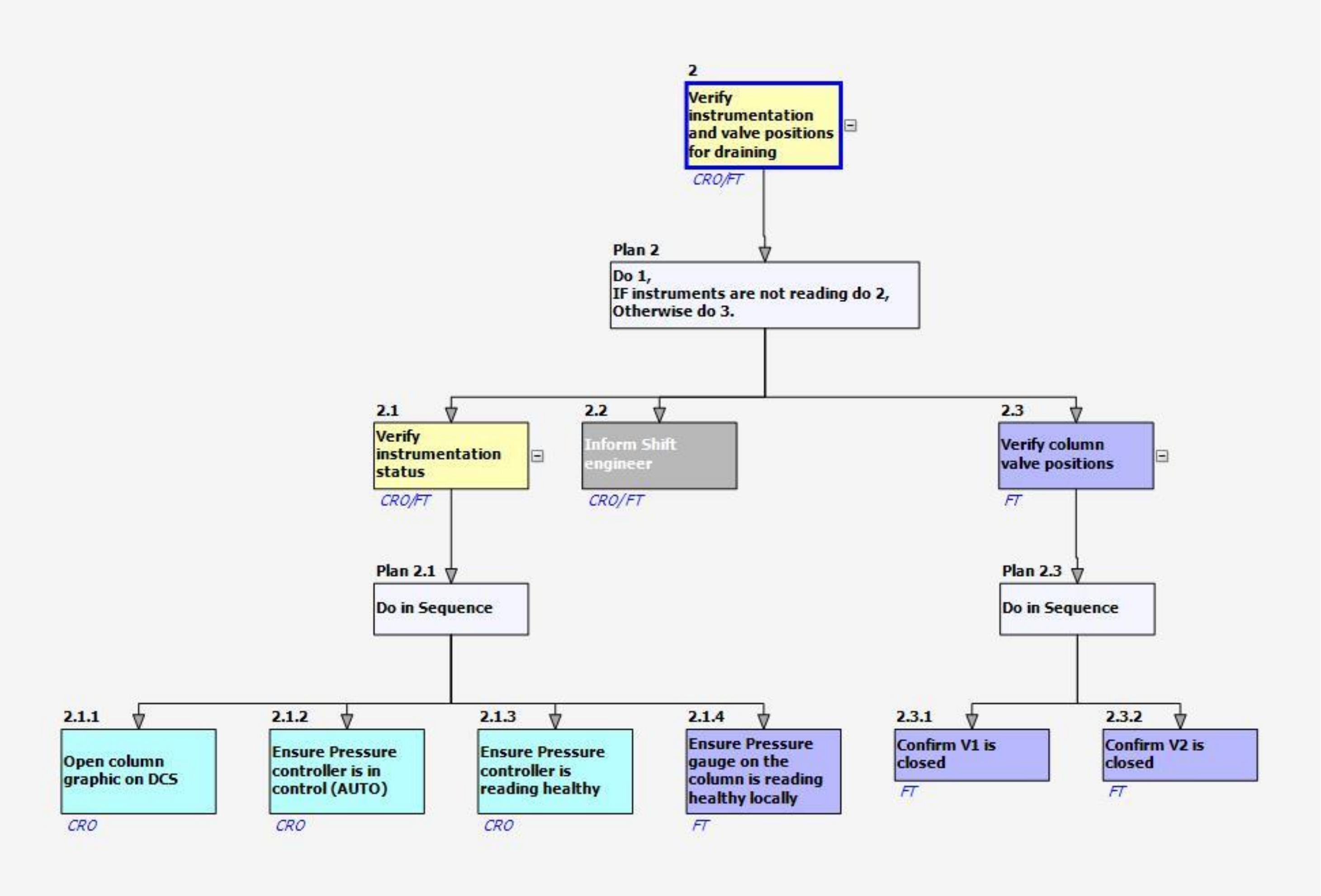
2
Verify instrumentation and valve positions for draining
CRO/FT
Plan 2
Do 1,
IF instruments are not reading do 2,
Otherwise do 3.
2.1
Verify instrumentation status
CRO/FT
2.2
Inform Shift engineer
CRO/FT
2.3
Verify column valve positions
FT
Plan 2.1
Do in Sequence
Plan 2.3
Do in Sequence
2.1.1
Open column graphic on DCS
CRO
2.1.2
Ensure Pressure controller is in control (AUTO)
CRO
2.1.3
Ensure Pressure controller is reading healthy
CRO
2.1.4
Ensure Pressure gauge on the column is reading healthy locally
FT
2.3.1
Confirm V1 is closed
FT
2.3.2
Confirm V2 is closed
FT

Figure 4: Further breakdown of subtask 2 showing plans and task steps

Predictive Human Error and Consequence Analysis (Stage 4)

Figure 5 below shows how the results of the PHECA analyses are documented. These consist of the possible failure modes and their consequences, based on the activity types associated with the task steps. It can be seen that in some cases, the consequences of an error are also recorded in the Warnings column, to indicate that this information needs to be transmitted to the procedure, in order to raise the awareness of the operator prior to carrying out this step. The table below provides some of the primary documentation to demonstrate to the regulator that a systematic and auditable process has been used for human factors task reviews such as those required for COMAH reports.

ID	Description	Role	Warnings	Comments	Activity Type	Failure Mode	Error Description	Consequences
2.1.2	Ensure Pressure controller is in control (AUTO)	CRO	If PC43340 remains in manual, it will not respond to increase in pressure in vessel F4304 - this will lead to more rapid overpressurisation in F4304.		Actions	ACT9 Action omitted	Fail to set PC in auto	If PC43340 remains in manual, it will not respond to increase in pressure in vessel F4304 - this will lead to more rapid overpressurisation in F4304.
2.1.3	Ensure Pressure controller is reading healthy	CRO	Potential over pressurisation of F4304 as control over pressure may be affected if transmitter is faulty and check omitted	Healthy will be roughly 4 Barg	Checking	CH1 Check omitted	Fail to check PT444340	Potential over pressurisation of F4304 as control over pressure may be affected if transmitter is faulty

Figure 5 Example of documentation of the PHECA analysis

Performance Influencing Factor analysis (Stage 5)

This stage of the analysis records the PIFs that might affect the probability of the errors identified in Stage 4. As can be seen from Figure 6 below, some of the PIF information such as *'Possibility that system could drain more quickly than expected'* could be transmitted to the operator in the form of a warning in the procedure.

ID	Description	Assigned Role	Activity Type	Failure Mode	Error Description	Consequences	Performance Influencing Factors
3.3.1	Monitor Pressure controller	CRO	Monitoring	MON1 Monitoring omitted	Flash drum pressure not monitored on PI43340	Possible MAH	-ve: Competing KCR tasks - possible distraction. +ve: CRO has good awareness of expected draining time (generally 10-15 mins) -ve: Possibility that system could drain more quickly than expected.

Figure 6: Example PIF analysis documentation generated during IOPS Stage 5

Import the IOPS analysis data into the procedure (Stage 6)

In his stage of the IOPS process, relevant information from stages 1-5 is imported into the procedure, based upon the designated template which maps it into the appropriate position. This is done automatically if the HFRM software has been used for the previous stages, but can also be carried out manually if required. Figure 7 Gives an example of the format of the procedure that results by importing the data described earlier into the procedures template. It should be noted that Figure 7 omits the boilerplate and other formatting information that would normally be added by the template. It can be seen that both warnings and comments that were specified in the earlier stages of the analysis have been imported into the generated procedure.

Step	Description	Role	Comments	Initial
2	Verify instrumentation and valve positions for draining	CRO/FT		
Plan 2	Do 1, IF instruments are not reading do 2, Otherwise do 3.			
2.1	Verify instrumentation status	CRO/FT		
Plan 2.1	Do in Sequence			
2.1.1	Open column graphic on DCS	CRO		
2.1.2	***WARNING: If PC43340 remains in manual, it will not respond to increase in pressure in vessel F4304 - this will lead to more rapid overpressurisation in F4304.***			
	Ensure Pressure controller is in control (AUTO)	CRO		
2.1.3	***WARNING: Potential over pressurisation of F4304 as control over pressure may be affected if transmitter is faulty and check omitted***			

	Ensure Pressure controller is reading healthy	CRO	Healthy will be roughly 4 Barg	
2.1.4	***WARNING: Potential over pressurisation of F4304 If check omitted***			
	Ensure Pressure gauge on the column is reading healthy locally	FT	HOLD: If any of the instruments identified in Step 3 are not reading then this procedure should be stopped and the Shift Engineer informed	

Figure 7: Example of section of procedure generated by the IOPS process (header, footer and other information omitted)

Conclusions

The IOPS process described in this paper has been applied extensively in safety critical industries such as the oil and gas sector. It provides a systematic and logical approach to ensuring that procedures development utilises all of the intelligence that is available from safety analyses conducted for regulatory purposes such as COMAH. It has particular advantages in ensuring that procedures and competency management systems are risk based, and hence are closely integrated in the risk management process. The fact that the IOPS procedures development process also achieves the objectives of the human factors task reviews required for COMAH safety reports means that considerable saving can be achieved by combining the analysis resources required for these activities. The process also satisfies the HSE requirement that organisations should demonstrate a clear and documented audit trail to show that insights from risk analyses are utilised to control risks during plant operations.

A final major benefit of the IOPS process is that it actively involves the workforce in safety and risk management efforts, and thus has the potential to contribute towards a positive and participatory safety culture.

Feedback from participants in the process has been very positive, as shown by the following comments:

> "Those involved have a greater understanding of how other shifts operate (and) improved continuity between shifts when doing tasks"
>
> "Improved my own knowledge of the task being assessed. Good cross shift communication of methods employed to identify issues of concern across the site"
>
> "Methodical by nature, in depth with genuine open discussion concerning the real issues associated with the task (i.e. safety, real world practices)"
>
> "Very good, a lot easier to understand as (the task steps) are broken down"
>
> "Has been informative and made people think more about the tasks they are doing"
>
> "I feel more involved in the development of procedures"
>
> "People have a greater understanding of why the task is done in a particular way"
>
> "People have a greater understanding of the risks associated with the task we have looked at"
>
> "I have enjoyed taking part in the IOPs process" Feedback from the operating level participants in the

We therefore recommend the IOPs design process as an ideal framework for organisations wishing to address a wide range of human factors issues such as safety reviews, procedures development and competency management across their sites in a systematic and integrated manner. We also believe that the process makes a major contribution to developing a participative and risk aware safety culture in the organisation

References

Embrey, D.E., 1986, SHERPA: A systematic human error reduction and prediction approach. Proceedings of the International Topical Meeting on Advances in Human Factors in Nuclear Power Systems, Knoxville, Tennessee American Nuclear Society La Grange Park, Illinois 60525 USA.

Embrey D.E., 1994 Guidelines for Reducing Human Error in Process Safety. Center for Chemical Process Safety New York

Embrey, D.E., 2013, SHERPA: A Systematic Human Error Reduction and Prediction Approach to Modelling and Assessing Human Reliability in Complex Tasks Proceedings of the European Safety and Reliability Conference (ESREL) Amsterdam

Energy Institute, 2011, Guidance on Human Factors Safety Critical Task Analysis Energy Institute, London

Health and Safety Executive, 2012, Human Factors: Inspectors Human Factors Toolkit http://www.hse.gov.uk/humanfactors/toolkit.htm

Health and Safety Executive, 2000, Human Factors Assessment of safety Critical Tasks http://www.hse.gov.uk/research/otopdf/1999/oto99092.pdf

Kirwan, B. and Ainsworth L. A., 1992, A Guide to Task Analysis CRC Press