HAZOPS are not the only fruit

Conor Crowley, Atkins Ltd, UK

Nigel Bowker, Blackhall Consulting Ltd, UK.

Introduction

In the chemical and process industries, HAZOP may be one of the most widely used words in hazard identification, but it suffers in its ubiquity by meaning many different things to many different people. While the safety professionals are comfortable with HAZOP meaning, amongst other things:

- A systematic review of a plant design, based on the Piping and Instrumentation Diagrams, a known process design, carried out by the systematic application of guidewords to identified deviations from the steady-state which may cause hazard or operability problems. This is often known as a *Line HAZOP*
- A high level version of this method, where the design is not mature enough to have full P&IDs, but where the design can still be influenced to remove hazards by inherent safety principles. This is often known as a *Preliminary HAZOP*.
- A review of a procedure or batch process, whereby the order of the activities is important. To this end, additional key-words are often applied which focus on the time-domain, and this is often then referred to as a *Batch HAZOP* or a *Procedural HAZOP*.

There are many other variations, including "CHAZOP" for control/computer based systems, Human Factors HAZOP, etc. What they all share in common is a team-based approach, attempting to identify hazards and operability problems by identifying DEVIATIONS from the design intent. They are generally facilitated by a HAZOP Chair, who follows either a company-specific, consultant specific or internationally accepted standard procedure.

However, the word HAZOP is often extended in the industry to mean any type of hazard identification exercise. Like Humpty-Dumpty in "Through the Looking Glass", the meaning depends on the person speaking .

"`When I use a word,' Humpty Dumpty said in rather a scornful tone, `it means just what I choose it to mean -- neither more nor less.'
`The question is,' said Alice, `whether you can make words mean so many different things.'
`The question is,' said Humpty Dumpty, `which is to be master - - that's all.'"

The challenge we often face as safety professionals is what HAZOP means to the customer, and whether applying a HAZOP technique is the best approach to meeting the underlying requirement.

This paper considers a number of the pitfalls of applying HAZOP in the offshore oil and gas industry in the experience of the authors. Alternative strategies to meet the identified shortfalls are presented.

It is assumed that for the purposes of this paper, the intrinsic HAZOP method is generally understood, and that it would be specious to summarise the technique in this area. Where applicable, the wording used in the paper is in line with the International Standard ISO-61882 (reference 1).

HAZOP as a brainstorming technique

The ISO Standard refers to HAZOP as a "creative process", and is sometimes referred to as a systematic brainstorm technique. However, it generally follows a strongly structured approach, and is a lot less like a traditional brainstorm than, say, a HAZID.

In their recent book (reference 2), Dave Gray et al discuss the fundamentals of creative meeting processes, and present a model of creative meeting processes in three distinct phases as follows:

- Opening (Divergent)
- Exploring (Emergent)
- Closing (Convergent)

The *Opening Phase* in the HAZOP Process is the call to identified potential causes of a deviation. It is assumed for the purposes of the exercise that the steady-state design is safe (although this is often examined implicitly), and the team is invited to identify whether it is possible to deviate from that design. The combination of guide-word (e.g. MORE) and parameter (PRESSURE) gives a deviation, and once one or more credible causes are identified, these are then considered in turn.

The *Exploring Phase* asks the team to determine the consequences of each cause of the deviation. This is generally confined by the method to within a single small area of plant, or a node, to allow the exploration to be comprehensive but also

bounded within what a team can consider at the same time. This is the time to consider the "what if" combinations, the history of the plant operation, the team experience of similar systems, etc.

The "Closing Phase" concentrates on the safeguards in place to deal with the particular hazard, and whether these are adequate. If there are concerns with the design, the understanding of the consequences, or the adequacy of the safeguards, these are recorded as actions from the meeting.

The process then continues with the next cause of the deviation, and explores and closes these as before.

The process is systematic and attempts to be comprehensive by application of a large number of guidewords and suitably sized nodes. Also, it does by design separate the idea creation (the identification of the causes of the hazards) from the evaluation of these causes, as it is not generally considered possible to be able create an idea and evaluate it at the same time, as these involve different mental processes. However, in contrast to other brainstorming techniques, where the sessions are designed to create ideas initially without critical evaluation, the HAZOP method does switch between these thinking modes regularly, which may well be one of the reasons HAZOPs can be very tiring for the participants.

HAZOP in Design

HAZOP is arguably at its best when considering a green-field detailed design project. With a mature design, and a mix of operations and design engineers and specialists, HAZOP allows the design to be tested and will generally reveal deficiencies in the design, and inform other safety related studies such as SIL Assessments etc. The Design HAZOP is generally a major set-piece in the design process, and forms much of the focus of designers and project management. Use of HAZOP at this stage in the project is a mature approach, and has a large part to play in testing a detail design.

The use of HAZOP followed by SIL/LOPA Assessment meetings has been introduced by a number of operators and design houses in recent years in order to align the design with the requirements of IEC 61508/61511. We have seen a number of people trying to combine the sessions, and others to run the sessions in series to use a consistent set of understanding for the two studies, which should in theory use the same hazards and assessments to inform the criticality of safety systems.

In practice, however, this process is not currently being carried out efficiently, with in some cases, an iterative approach required to converge on a solution for high hazard items. In these cases, our experience has been that there is a tendency to leave the design of higher integrity level shutdown systems to after the HAZOP, whereas the issues driving a SIL 2 or higher system are generally known during the development of the P&IDs throughout the detail design process. The feasibility of these designs tend not to be driven by whether a suitable architecture could be found, but rather whether there is sufficient time for shutdown systems to operate while preventing a hazard escalating, and these aspects of the design could realistically be carried out prior to a HAZOP, with the decisions on higher SIL rated systems made first on a functional basis by the process safety discussions, supported by the formal design and certification process in due course.

Another significant issue which we have come across in recent years has been the trend towards additional facilities being installed by means of bridge-linked platforms: these have recently been installed in the UKCS for Forties Alpha Satellite Platform by Apache, Jasmine over Judy by ConocoPhillips, Montrose Area Redevelopment by Talisman Sinopec etc.

A feature common to a number of these installations has been that the *greenfield* and *brownfield* parts of the design are carried out by separate contractors, and this has proved difficult to handle from a HAZOP point of view. In one extreme case, the extent of the changes in the brownfield section of the plant was limited to pipework and ESDVs, and within the brownfield project scope, the HAZOP initially was carried out focusing only on the individual pieces of pipe within the brownfield contractors scope. This did not produce any meaningful hazard analysis. The team were required to reconvene with a wider node definition to allow some of the cross-field operations hazards to be considered. Even then, the silo mind-set of each team was difficult to break down.

HAZOP in Commissioning

A number of our clients in the UKCS use their facilities as hubs for processing from a network of sub-sea wells. Additional wells are proposed and added to the infrastructure, and while a common design approach is taken to each well, the exact configuration is seldom identical to the previous designs, and hence it is required to carry out a HAZOP, under the control of change procedures.

This example is one whereby the HAZOP technique is really understood to be more of a "something the project must do, and I guess a HAZOP would something we could do…." We carried out a series of these HAZOPs for a client, and increasing found less and less to document, in one case ending up with a HAZOP with no recorded actions. This illustrated that the approach was not the optimum one for such designs, and that requiring for example the lead process engineer to justify why the HAZOP should not be carried out in regard to the existing hazard identification for the infrastructure in the area would have been more straightforward and arguably more cost effective. But at present, the operator's procedures have not changed, and each new addition to the facility does require to be HAZOPed. This will be considered further below.

HAZOP in Operation

Offshore oil and gas processing is arguably unique amongst the processing industries in that there is no certainty in the plant design that the fluids being processed are the same as designed for, even from day one: it is not unusual for plants to be designed for a particular composition which is based not on real measurement, but from tests from wells drilled in a similar region, sometimes years or decades previously, and even sometimes with only a lab report to go on, rather than a real fluid. Add to that, the fact that the feed to the plant will almost certainly change in composition, flow, pressure and water content over the field life, the facilities involved need to be robust against a wide range of operating conditions and fluids.

This introduces the subtle problem that the HAZOP process assumes that deviation from the steady state is required to create a hazard, however, that is predicated on a steady-state existing in a meaningful way. It is quite possible for an upstream production facility to change from a hazard point of view even if the equipment and the well configuration do not change.

One of the main deficiencies in the operational phase from a HAZOP point of view is the use of the understanding of the plant which has been gained in a HAZOP to inform how the plant is operated in practice. The hazards identified in the HAZOP are seldom presented to the plant operator in a format that is useful for day-to-day operation, and as a result, the cognitive model that each operator has on the way the plant operates is likely to be informed by previous experience and any patterns they have developed between cause and effect on the plant. Where these are incorrect, it can have significant implications in preventing the development of hazard causes into consequences. However, the HAZOP can often become a "write-only" document, doomed to sit on a shelf but not referred to.

Another significant issue is minor modifications: while these can often be HAZOPed in the area where the modification is made, the wider implications of the design change may not be seen within the modification "cloud", and again care has to be taken to ensure that the traditional HAZOP approach does not give a false sense of security about the coverage against major hazards.

HAZOP as a Tool for Plant Validation

To combat the issue of plant drift, many oil companies have written standards that require a plant to be completely re-HAZOPed periodically, say every 5 or 10 years. These HAZOPs can become major exercises in their own rights, taking dedicated teams of operations and support engineering functions many months as the facility is subjected to a detailed HAZOP.

Again such exercises are not cheap to carry out, tying up key resources for significant periods. They also risk being used to solve relatively minor operability problems, without adding significantly to the understanding of the hazards under review. While they will almost certainly create lots of activity and actions, it is less clear that they add significant value to the management of risk, and often are a "lowest common denominator" approach, in that they are a well-understood methodology, and therefore carrying one out can keep a regulator happy.

What Else is in the Toolkit?

The well-known motivational theorist, Abraham Maslow, once commented: "If the only tool you have is a hammer, you will see every problem as a nail". As safety professionals, we have much more available in the toolkit, and variations of these are also possible to produce which give the equivalent or greater value as a HAZOP, but are more appropriate for the task. These include:

- Previous Incident Analysis
    - It is one of the truisms of process safety that no major incident re-occurs in exactly the same way. But, as Judith Hackett, HSE Chair, points out, there are no new accidents either. It is not difficult to take the progression of a well-known incident, such as Piper Alpha, and go through each part of the incident development, documenting how this would be prevented, controlled, or mitigated by a facility design or management system. Indeed, such a process was postulated at the Piper 25 Conference in Aberdeen in 2013 by Andrew Hopkins, Emeritus Professor of Australian National University. It was clear in the discussion of the presentations that this simple approach was not generally applied.
- Human Error Modelling and Risk Reduction
    - It is widely stated that the majority of accidents have a human involvement, but yet a classic HAZOP does not always systematically address the different ways that humans can cause deviations from the steady state design.
    - A number of structured Human Factors Methods exist, where error-causing guidewords are used to prompt deviations from normal operation, and prompt identification of hazards. This formal method is most often used for procedures, however, it is less used for steady state HAZOPs.
- Integrity Management and Review
    - Management of aging plant has been a focus of the industry for a number of years ago, and there is a wide variety of industry experience behind this. Oil and Gas UK published a guideline to managing

ageing installations, which contains recommended strategies and practices for the management of obscolescence in the oil and gas industry, which have significant wider applicability.

- Reliability Analysis
    - Reliability Centred Maintenance and Reliability-Availability-Maintainability Studies are mature technologies, but do suffer from the fact that the combination of failures to result in a loss of containment are relatively infrequent, and hence it is difficult to get a statistically significant estimate of the underlying failure rates.
    - The application of the international standards on instrumented protective systems into the Oil and Gas Industry has resulted in a greater focus on reliability calculation of key safety systems, although again these can get very numerically focused, and don't always take into account uncertainty in base data, and occasionally have poor treatment of common-mode/common cause failure.
- Dynamic Process Simulation
    - Increasingly, dynamic models of plants are created during design of offshore installations, and are used, amongst other things, to investigate the adequacy of control systems, and also to look at the speed of response of higher integrity systems, and relief systems, to ensure that they can operate quickly enough to mitigate the hazards.
    - A good dynamic model could be the basis for a lot of "what if" scenario evaluation, but there is limited evidence of this being used to inform hazard identification. For instance, a bank of scenarios could be investigated where the likely failure of specific instrumented protective functions could be incorporated into the analysis, and ultimately the consequences of the HAZOP deviations would be modelled and known, to confirm the team's judgement. While there is risk of confirmation bias in this approach, in that the dynamics of the deviations may be optimistic, and hence the demands on the safety systems would not be extreme, a series of "stress tests" with faster or more extreme magnitude deviations used to systematically evaluate the responses.
- Evergreen HAZOPs
    - The goal of an evergreen HAZOP is to maintain a full and comprehensive overview of the hazards in a design. In this, any modification to the plant has to be assessed in the context of the overall plant, and deviations upstream and downstream of the modified equipment revisited to ensure that changes are adequately assessed.
- Inherent Safety Review
    - The principles of inherent safety are well known throughout the industries, and the hierarchy of "prevent-control-mitigate-escape" is expressed in various ways by different constituencies. For instance, Atkins recommends incorporating an Inherent Safety Review at the early stages of concept development, as a high level way of getting operations, design and technical authorities to communicate the "known-knowns" of hazards associated with the process across the discipline pool, and attempt at the earliest stage to remove or manage the risks as appropriate.
    - This has worked particularly well where there are interfaces outside of the traditional topsides disciplines, e.g. for floating structures with associated processing equipment, where the approach to marine design and process design may not be consistent. This allows the design engineers to explain their hazard management approaches, and ensure that the other disciplines can take this into account.
- ALARP Reviews
    - Typically, the overall level of risk on an offshore installation will fall into the ALARP region while producing hydrocarbon, and as a result there is a perpetual obligation to demonstrate that the risk is as low as reasonably practicable. This approach is focused on major accident hazards, but challenges the risk owners to continuously monitor industry practice, and evaluate if engineering changes could be applied at a reasonable cost.
- Fluid Property Analysis and Review
    - One constant of the oil and gas production is change in fluid flow: as stated previously it is unusual in the process industries to have a significant uncertainty about the properties of the fluids being processed prior to start-up of a facility. Additionally, unless there is a fiscal reason to do so, the composition of inlet fluids is not necessarily measured in detail, with the focus on characterisation of the sales fluids in line with pipeline or shipper requirements. What this can result in is a significant delay in detecting significant changes to individual well compositions, as they can be masked by mixing with other well fluids, and also with other pipeline users.
    - One particular area where this has caused issues in the UKCS has been in the production of H2S, whereby wells have "soured" attributed to in some cases underground biological activity, and also introduced by mixing of seawater with production fluids.

- Barrier Analysis
    - Another popular method is to review the layers of protection against individual hazards and carry out a desk-top review of these, often in a "bow-tie" format. These can be useful operational tools as well, although as ever care needs to be taken about the true independence of layers, and whether a successful activation of a barrier is sufficient to conclude that the integrity of the barrier is proven.
    - One of the issues which is inherently difficult in the barrier analysis/layer of protection area is predicting the underlying demand rate on the system. These are generally not well understood, and can also be masked by the successful operation of other barriers/layers of protection. Atkins are currently researching using "Big Data" techniques to process historian data to measure the underlying demand rate and allow validation of the SIL/LOPA assumptions.
- Safety Critical Element Review and Performance Standards
    - The concept of "Safety Critical Elements", and the performance standards underpinning their operation is a maturing approach within the offshore industry in the UKCS, and is the topic of another Atkins paper at this conference. Fundamentally, the identification of an item as "safety critical" is intended to focus resources and attention on the key systems required to manage the major accident hazards on the installation, and ensure their continued operation.

Conclusion

HAZOP is a key process safety tool, but not the answer to all process safety and hazard identification challenges. For continued management of the safety of our processes, a wider range of approaches should be considered, both to manage the inherent weaknesses of single-cause and consequence approaches, but also to make sure that we can understand, communicate and manage the challenges of major accident hazard industries.

References

1. BS IEC 61882:2001 "Hazard and operability studies (HAZOP studies) — Application guide".
2. Dave Gray, Sunni Brown and James Macanufo, "Gamestorming, A Playbook for Innovators, Rulebreakers and Changemakers", 2010, O'Reilly Media Inc, USA.
3. Oil and Gas UK: "Guidance on the Management of Ageing and Life Extension for UKCS Oil and Gas Installations"; Issue 1; April 2012.