

A METHOD FOR PROJECT SAFETY DESIGN VERIFICATION ACROSS A GLOBAL ORGANISATION

John Martin, Chris Flower.
ABB Consulting, Daresbury Park, Daresbury, Warrington WA4 4BT; Email: john.s.martin@gb.abb.com

Safe and environmentally responsible operation of assets is a major consideration for owners and operators of major accident hazard process plant and this requires equipment which has been competently designed in accordance with appropriate standards and good practice.

Many operating companies have a global asset base and, as well as acquiring new plant, existing assets are regularly bought and sold. Joint ventures are common with partners and stakeholders often changing over time. Projects are generally designed and constructed, and sometimes commissioned, by contractors who will themselves operate to a set of standards which may not entirely coincide with those of a particular client.

Many operators are committed to designing, constructing, commissioning and operating assets to the highest standards globally and will tolerate no reduction of standard with geographic location. There is a major challenge for an operator to demonstrate that these commitments are realised at the detailed level when this may be in a remote location and may require the involvement and commitment of joint venture partners or third party contractors.

This paper will describe a methodology of process safety design verification or peer review for process plant. The methodology is intended to confirm that the detailed documentation is in accordance with relevant standards, calculations have been correctly performed and to establish whether there are any specific design areas that are flawed or unsafe. Results may be reported in summary tables against specific questions and issues, which ensure consistency across sites and projects. In particular gaps are reported – these may be a failure to carry out a key study or calculation or serious concern over information provided. A scoring system may be used to highlight the level of concern, if any, for each section.

Timing is flexible and it is possible to use this technique at any stage of the project providing the criteria are modified appropriately, although generally the review is based on the front end engineering package (FEEP). Earlier review can result in early warning and can be used to guide a potentially unsatisfactory project to success. Later review considers a more complete picture of the design and so gives a more comprehensive appraisal.

Design of process plant is an amazingly complex operation. Designs routinely take years from initial concept to beneficial production, involve large teams spanning multiple disciplines and may cost sums of money up to billions of dollars. Location may change several times as the design progresses from corporate office to contractor's office to constructor's site(s) to operational site and in today's global environment this change of location may span continents. Large numbers of vendors tender for and supply almost countless items of equipment which must be assembled to provide the final finished production unit.

Throughout this process innumerable decisions are taken by designers and these decisions will be reflected in the reality of the final plant. In some cases poor decisions will have little or no effect on the cost, efficiency, throughput or safety of the process. In other cases poor decisions can have a profound effect, even if this is only realised after many years of operation. For instance the consequences of the design decisions around the Flixborough control room did not become apparent until the catastrophic event in 1974 which showed that the structure was inadequate to withstand the blast of the explosion (Lees P, 1980).

In response to this the industry has developed numerous guides and standards covering all aspects of design and companies have developed their own internal standards which often attempt to ensure that the best of the industry standards are incorporated into their designs. In addition industry recognised techniques such as HAZID, HAZOP and risk assessment are routinely used to identify hazardous scenarios and to either design out the scenario or provide adequate mitigation within the design.

The requirement for contractors, suppliers, constructors and operators to deliver safe plant and operate it safely and in an environmentally responsible manner has never been greater and throughout the industry there is a genuine desire and determination to deliver this. Nevertheless accidents continue to happen and aspects of design continue to be found to contribute to those accidents.

In this environment of scale, complexity and geographical spread organisations which will ultimately own and operate assets may wish to consider some form of design verification or peer review, coordinated internally or externally, to provide a level of assurance that the design has been carried out competently and conscientiously.

The scale of the design to be considered for review can vary from a relatively minor project controlled by a local management of change procedure to a large capital project with multiple parties involved.

PURPOSE OF DESIGN VERIFICATION OR PEER REVIEW

An organisation must be clear why it commissions such an exercise. Design verification or peer review can be thought of as analogous to a layer of protection. It cannot guarantee that the facility is safe but if carried out competently it should reduce the likelihood of design errors being carried through into construction and operation.

Throughout the design process safeguards are used to protect against errors:

Competent and qualified staff are used.

The project identifies the correct standards and procedures to be used in the design

Appropriate studies such as HAZID and HAZOP are used to systematically identify hazards within the process which are either eliminated or mitigated.

All of these can be thought of as layers of protection. Each one reduces the likelihood of a hazardous scenario being realised during operation of the asset. It is important to acknowledge that these measures do not guarantee that no hazardous scenario will ever be realised. The level of risk reduction is dependent on how comprehensive and well executed these layers of protection are.

In the same way a review of design is an additional layer of protection and again the level of risk reduction will be a function of how comprehensive, how well thought through, how relevant and how well executed the review exercise is.

SCOPE OF THE STUDY

It is important at the earliest possible stage to agree the scope of the review study. The scope of a design may seem to be obvious but it may also be necessary to ensure that impact on other existing equipment has been adequately considered. For instance, if an oil refinery installs a new unit the physical modifications may terminate at the point where the blowdown line from the new unit meets the existing flare. However it is vital to ensure that the impact of the new unit on the flare header and flare capacity has been considered. Similarly it is important to ensure that backflow from the new unit into existing services such as air and nitrogen has been adequately considered. Drawing the scope too tightly may impact on the quality of the study result. Drawing an unnecessarily large boundary may result in a very expensive, time consuming and overly complex study.

It will also be important to determine whether this is a purely process engineering review or whether it will extend to electrical, instrument, mechanical and civil engineering aspects of the design.

METHODOLOGY

Most of the study will be based on documentation which has been issued by the design team. There are three reasons for this – the design may be developed through ideas and discussion but is finally defined by documentation, it helps to maintain the independence of the review team and it prevents them getting in the way of the project team who are often still busy. It can be useful to carry out a gap analysis to determine what documentation has been generated versus what would be expected. The process safety related documentation that a major project might be expected to generate would include:

- Terms of reference for the design
- Basis of design data
- HAZID (Hazard identification), HAZOP (Hazard and Operability) studies
- Detailed process design data
- PFDs, P&IDs
- Project safety and environmental philosophy
- Process design philosophy, process control philosophy
- Relief and blowdown study
- Cause & effect diagrams, emergency shutdown philosophy
- Layers of protection analysis/SIL determination

There could be additional documentation such as:

- Materials selection
- Operation and maintenance philosophy
- Outline operating instructions
- Other safety studies

Additionally there will be significant documentation generated in the mechanical, electrical and civil design. Eventually the project would be expected to generate a commissioning philosophy and plan with detailed instructions.

An operating organisation may wish to confine the review exercise to a limited area, such as the Hazop, or may ask for a comprehensive review of all process safety, and possibly some other, aspects of the design. It is important that this scope is established as early as possible since it will determine the list of documentation required by the review team, the composition of that team and the appropriate contacts within the operator or contractor organisation. It will also of course be significant in determining the size, cost and timescale of the study.

TIMING

Generally design review is carried out at the point where the front end engineering package (FEEP) has been completed. This normally represents a break point in projects, often with a reduction activity as stakeholders consider their willingness to progress to the next and more expensive stage of design – construction. Indeed the output from review exercise may be part of the assurance the stakeholders seek before committing further resources. It is also possible to use the review process at earlier points in the project – for instance as the major hazards are identified and the basis of safety is settled. Sometimes the review methodology is used for a completed and operating asset – possibly as part of due diligence for an asset purchase or as part of a gap or benchmarking exercise for a newly acquired asset.

DATA

Once the scope of the review has been agreed data must be requested. In the best systems the contractor or operator will have a database in which each document is listed and its scope can be clearly understood from the title, which allows rapid and efficient identification and retrieval of the required data. Often this is not the case and the review team must generate its own lists. One of the problems with this is that a clerk must take data requests from the review team and match them with what is found in the project file registry and the match is not always perfect. The review exercise can be compromised early on by a failure to supply data which is available but not clearly labelled leading the review team to believe that the requested data does not exist. This type of misunderstanding is often cleared up as the study progresses but it makes the exercise more confused and increases the time and effort required.

TERMS OF REFERENCE

Terms of reference (TOR) documents are extremely important particularly where there are joint ventures or contractors are involved. It is highly likely that all parties in a design will have their own guides and standards and by default their own employees will work to these. The TOR document is essential in these circumstances since it defines the agreed standards, codes and methodology used in the project. Without it the review team cannot say whether or not the work produced conforms with the agreed terms of reference and cannot comment on whether or not these are appropriate. For instance most organisations will have a risk matrix but there can be significant differences between them. Without a TOR document stating which one has been adopted for the project a review of a risk assessment could be very difficult. It is also essential that the TOR document(s) have clearly been accepted by all parties at an appropriate level.

STRUCTURE

The design package is likely to generate significant quantities of data for the design of individual items of equipment which are normally subject to internal design review. There are also likely to be a number of studies, particularly process safety studies, which span the entire project. When the objective of the review is to provide assurance regarding the process safety of the facility then it is these studies which will probably be the subject of that review. For instance it might be agreed with the process operator that the process safety aspects of the design will be studied under the following headings:

- HAZOP (Hazard and Operability studies)
- Relief and blowdown study
- Emergency shutdown philosophy

One approach is to generate questions which when answered will provide an insight into the quality and robustness of this aspect of the design. As an example it might be agreed that the study of the project relief and blowdown will answer the questions in the sections shown in Table 1.

When the table is populated with the answers generated in the review study it becomes the report table. When the completed report tables are put together they form the basis of the study report.

It is important to note that the review study cannot repeat certain aspects of the design. If time is available calculations may be re-created but some of the project studies are a record of key interactions. For instance the HAZOP is a live exercise involving a team with appropriate experience and qualifications and the interaction and dialogue between the

Table 1. A possible report table pro-forma for Relief & Blowdown

Scope	Have all vessels that may be subject to over or under pressure been identified and included in the relief study?
Generation of relief cases.	Has a structured methodology been used to ensure that all causes of over and under pressure been identified?
Codes and standards	Have the relevant codes and standards been referenced and used in the identification of relief cases and the calculation of required relief rates?
Calculations	Have the calculations been written and are they legible and understandable. Is the process data consistent with the P&I diagrams and the project heat and mass balance? Have the calculations used recognised and referenced methods? Are the calculation conclusions clear and correct? Has the calculation been checked and approved?
Data Sheets	Have the results of the calculations been correctly transferred to data sheets which specify the mechanical and process aspects of the required relief devices?
Instrumented systems	Were instrumented systems used to protect against over or under pressure. If so have these been subject to the appropriate studies to ensure the required integrity is achieved?
Blowdown	Has the relief device blowdown been considered? If a vent has been used has the capacity of the vent and its location been considered? If the relief device vents to flare has its impact on the flare total capacity been considered? Has the flare backpressure been considered?

team is essential in ensuring that the hazards have been identified. The reviewer can comment on the HAZOP methodology and report – whether or not it has been effective in identifying causes of hazards, mitigations and assigning actions and the quality of the record but the HAZOP itself cannot be re-created. Even so the reviewer is also likely to want to be satisfied that the major hazards associated with the process and their consequences have been correctly identified.

LEVELS OF DETAIL

An appropriate level of detail must be agreed between the review team and the operator of the process. In the ultimate the review team could be asked to repeat, from scratch, the work of the design team. This is unlikely to be efficient and sometimes can be quite unhelpful. There is likely to be a need to agree a filter – for instance it is likely that all pressure relief calculations have been carried out by a competent person, checked by an experienced competent person and approved by someone with appropriate seniority. Hence it may be decided that only calculations corresponding to potential major accident scenarios will go through the review process. Of course this means that there is an initial exercise to identify those relief calculations which fall into this category but it is likely that the project will be able to do this anyway or if not it should be possible to screen the process for these cases fairly efficiently.

As well as agreeing which pieces of work are to be reviewed it is very important to agree the depth of the review. It may be appropriate to agree to carry out some key calculations from scratch whilst others are re-checked and for others the philosophy and approach of the calculation alone will be checked, accepting that the numbers have already been adequately checked as part of the normal design process. Again just as the design safety review exercise is a layer of safety so is the normal calculation checking and approval process.

Certain forms of calculation, such as LOPA, may not have been subject to checking and approval in the design although the results are profoundly important in designing the safety systems for the process. LOPA and other calculations may be carried out with spreadsheets and order of magnitude errors are possible but such a calculation is sometimes not independently checked either because of the difficulty and complexity of doing so or because it is not presented on formal calculation sheets – this may also mean that it doesn't appear on the calculation register. Hence all calculations, both formal and less formal, which impact significantly on the safety of the process should be considered for review.

As well as numerical errors which can, of course, be significant there are also errors of approach to consider – such an error can be very fundamental and can have profound implications for the design. For instance in a pressure relief calculation it would be expected that the engineer would identify all the possible relief cases and then calculate the relief rate values and size the relief valve based on the dominant case. A structured approach to considering all potential causes of over and under pressure should be used and an example of how this might be achieved is populating the matrix found in Ref 1 and is shown in Fig 2. Too often the relief calculation makes an assumption of the dominant case e.g. "external fire" and does not consider any other cause of relief – this assumption may be correct but the failure to have demonstrated that other causes have been considered would be a serious flaw in the calculation and should attract comment from the reviewer even if the calculation result is correct.

LAYOUT AND CLARITY

In addition to checking the accuracy of data, the methodology used and the basis of design it is also useful for the reviewer, as an independent party, to comment on the layout, appearance and accessibility of the work. If the reviewer found the reports and calculations hard to understand, confusing in layout or information was not where expected it is likely that those who try to retrieve this information

Table 2. Pressure relief scenario matrix

	Prime Event			
Plant or process conditions	External Fire A	Process Abnormality B	Equipment & services failure C	Ambient changes D
1 System blocked in.				
2 Restricted outlet: (closed, restricted or too small) due to: valve closure, machine stoppage, solids deposition or entrainment.				
3 Restricted inlet: (closed, restricted or too small) due to: valve closure, machine stoppage, solids deposition or entrainment. under-pressure (vacuum conditions)				
4 Chemical reaction				

Table 3. An example scoring system

A	Everything satisfactory
B	Some areas of concern but these do not appear to indicate an unsafe design.
C	Significant flaw in a calculation, approach or methodology which requires re-work This may indicate a problem with safety implications which should be resolved before start up.
D	A systematic flaw in the design which requires the work to be revisited and amended before the asset is commissioned.
E	A major flaw in the design or in the safety systems which makes the design fundamentally unsafe.
X	A lack of data which makes informed comment difficult or impossible. Prior to start up it should be established whether or not the work was carried out and if the work was carried out then it should be reviewed or if the work was not carried out then it should be completed.

subsequently – possibly the process operator or a future modification project – will experience a similar problem which could lead to increased time and cost or may result in important safety information not being considered resulting in an incident.

REPORT

A project produces vast amounts of documentation. The review report must aim to be sufficiently comprehensive that all relevant points are raised but not so large and detailed that it becomes unduly onerous to fully read and act upon.

The intention of the review exercise is to provide assurance to the owner or operator of an asset that it has been competently designed to appropriate standards and that the necessary safety studies have been properly executed. Areas of weakness should be identified and commented on.

In order to make the report as brief but as comprehensive and readable as possible it should be based around the completed report tables (described above). Often a scoring

Table 4. An example of a section of a completed report table.

Overall	*C. Failure to identify some vacuum relief cases for fixed roof tanks. The relevant calculations need to be revisited and the selection of relief devices reviewed. Some calculations were not approved at the appropriate level.*
Scope	Have all vessels that may be subject to over or under pressure been identified and included in the relief study? *A comprehensive written study has identified all vessels requiring protection from over or under-pressure (reference Project A Document XYZ)*
Generation of relief cases.	Has a structured methodology been used to ensure that all causes of over and under pressure been identified? *A structured approach was used (reference Project A Document XYZ). Unfortunately vacuum protection for the low pressure storage tanks due to liquid draining at the maximum rate was not identified as a relief case.*
Codes and standards	Have the relevant codes and standards been referenced and used in the identification of relief cases and the calculation of required relief rates? *API520 /1 was used for main process items and ISO28300 was used for low pressure storage tanks.*
Calculations	Have the calculations been written and are they legible and understandable. Is the process data consistent with the P&I diagrams and the project heat and mass balance? Have the calculations used recognised and referenced methods? Are the calculation conclusions clear and correct? Has the calculation been checked and approved? *The calculations have been clearly written and well laid out. Reference to design data such as P&I Diagrams, vessel drawings and project heat and mass balance is clear.* *A detailed check on 10% of the calculations was carried out and these were found to be correct in method, arithmetic and conclusions.* *A check on the methods used in all calculations was undertaken and they were found to be consistent with the chosen codes and standards.* *The calculation conclusions are clearly summarised on the front sheet of each calculation.* *The calculations were all checked to an appropriate level within the project but the checker had also approved a number of calculations and this is not consistent with the project philosophy.*

system is useful. This may vary from a simple binary "Acceptable" or "Unacceptable" mark through to a more sophisticated system with a range of marks carrying a range of required actions. An example of a scoring system might be.

An example of a completed section of a report table for the Relief & Blowdown might be.

AFTER REPORT ISSUE

It is quite likely that the project team will want to discuss the report with the review team. This should be positive since both the project team and the review team receive feedback on their work. The design review team may find that that there is additional data available within the project which previously they had not seen but which will address some of their concerns and allow areas of the report to be rewritten. Even after the report is revised it may point to serious concerns with the design. The purpose of the review exercise is to provide additional assurance to the asset operator and a report which causes areas of the design to be revisited so that safety concerns can be addressed is at least as valuable as a report which concludes that no further action is required.

CONCLUSIONS

The design verification or peer review process does not provide a guarantee of a safe design but rather is an additional layer of protection. If used intelligently it allows a cost effective, safety focussed review of the many critical reports and calculations produced during the design.

REFERENCES

1. Process SHE Guide No.8 (PSHEG8). The Comprehensive Guide to Pressure Relief. ABB Ltd.
2. Lees F. Loss Prevention in the Process Industries. First Edition. Butterworth-Heinemann 1980.