MOVING FORWARD FROM ASSESSMENT TO INSPECTION - HOW GOOD IS COMAH?

Phil Scott, HM Principal Inspector
Hazardous Installations Directorate, Health & Safety Executive, Government Buildings, Ty Glas, Llanishen, Cardiff CF14 5SH

The COMAH Regulations 1999 set dates by which operators of 'Top-Tier' sites have to produce safety reports, and the key one of February 2001 having passed means that the majority of UK operators have now completed their first reports. Only those that were not designated new major accident hazard sites prior to COMAH need not yet have done so, and these have until February 2002. So what has been the experience so far of the standard of reports and the likely effectiveness of them in preventing major accidents? Certainly the first two years has not been trouble free, as the two parts of the Competent Authority (CA) have begun to work together, operators have struggled with the requirement for demonstration of safe operation, and both operators and regulators alike have met the challenge of the workload involved in COMAH.

The paper will review the outcome of the first round of safety reports, and the CA's priorities for dealing with initial assessments. Most importantly, the paper will look forward to the next phase, as the CA begins to move from assessment of reports to inspection of COMAH establishments. Using case studies of two actual incidents that occurred at top tier sites before submission of the safety reports, the question of how likely it was that the incidents might have been prevented if the safety reports had been available and assessed will be examined. Finally the paper will outline some of the particular challenges for the future, for both the CA and industry, as COMAH develops and the public become more aware of the changes it introduces to control of major accidents.

Keywords: COMAH; Competent Authority; Inspection

INTRODUCTION

Many view the COMAH bandwagon as having got off to a somewhat shaky start along the route to delivering improved control of major accident hazards, and cite a range of problems that have afflicted industry and both sides of the Competent Authority (CA) over the first couple of years. When difficulties are highlighted (and before they have had a realistic chance for solutions to filter through) it is easy to lose sight of the progress made so far in developing the systems COMAH calls for both within the CA and industry. It is also equally easy to lose sight of the 'bigger picture' around COMAH – it's not just about safety reports and their assessment, but a longer-term mechanism for combining assessment with inspection.

There have undoubtedly been (and continue to be) some operational problems with COMAH. This is hardly surprising given the enormity of the jump from the previous regime, CIMAH, to COMAH. In its implementation of the Seveso II Directive, the UK has led the field and encountering operational problems associated with this has followed with a certain inevitability.

This paper presents a personal view, from a regulator's perspective, of the state of the game so far and based on experience of dealing with safety reports and inspection arrangements to date. It also considers the relative importance of inspection in the combined assessment / inspection / improvement cycle: the stage has currently been reached where many COMAH top-tier companies have had their safety reports assessed and there is a move now to much greater emphasis on inspection after the prevalence of assessment so far. A central proposition of this paper is that the inspection phase is the most important element in judging the relative success of COMAH in being able to prevent or at least control major accidents.

EARLY EXPERIENCE WITH COMAH AND SAFETY REPORTS

The 'first round' of safety reports, i.e. those submitted and which began assessment around February 2000, included a substantial number where the quality of presentation and level of information anticipated and expected by the regulators fell well short of expectations, and did not meet the minimum requirements set in Schedule 4 Part 2 of the COMAH regulations. Equally, it has to be said, most were at least acceptable and some were very good quality – so it is, and was, clearly possible for the required standard to be produced. A figure of 40% has been quoted for the level of safety reports from that first round being 'rejected' or returned to operators as requiring further work. That figure is somewhat misleading, as it was affected by a few operators submitting many volumes or modules for the same site or sites that all suffered from the same intrinsic deficiencies in approach – but nevertheless, the 'safety reports returned' rate was higher than anticipated.

In addition to individual feedback to operators on their safety reports, in summer 2000 the CA produced a letter on the early lessons from safety reports, that it circulated to all COMAH TT operators. The intention was to be as open as possible and to draw attention to the emerging problems. The letter highlighted the following main issues from safety reports:

a) Descriptions of safety management systems (SMS) which failed to focus specifically upon the **management** of major accident hazards;

b) A failure to demonstrate the link between the major accident hazards and the measures for prevention control and mitigation. This was a key issue.

c) Descriptions in the reports of what the SMS looked like, rather than why and how it demonstrates that all necessary measures have been taken to control major accident hazards.

d) A failure to demonstrate that there is a systematic approach to evaluating major accident risks.

e) A failure to show that human factors, in particular the part that human failure can play in initiating major accidents and the reliability of safeguards which depend on human action were understood and addressed adequately.

f) The risk assessment process had not been robust enough. Operators had not demonstrated that the results from the assessment of the major accident risks had been taken forward and used as the basis of the

process to select, prioritise and schedule further risk reduction measures to reduce risks as low as is reasonably practicable (ALARP). This was also a key issue.

Fuller details were given in the letter on the main problems. The hope was that this information would assist in the process of getting better quality safety reports, both for those operators who had had them returned and also for those who were in the process of preparing them for February 2001 submission.

It was disappointing to say the least, therefore, to find that with the February 2001 reports there was still a substantial number where the information was inadequate and they were returned to the operators. In the area covered by one operational Unit for example (Merseyside, Wales, West Midlands and West of England), out of 52 safety reports received in the first quarter 13 have been returned to the operators – 25%. After an initial assessment (the CA carries out an initial read of all safety reports to ensure the presence of the essential information required by the Regs, before committing to a full and detailed assessment process) this was undoubtedly the appropriate action in the circumstances – the reports were clearly deficient in their coverage. It is the intention of the CA to operate in a cost-effective way both in terms of using its resources on viable reports and also to save operators unnecessary charges for work on reports that would patently fail to meet the assessment criteria.

In many cases, whether reports have been rejected or not, there have been serious concerns amongst assessors that the information presented in reports indicates that necessary measures to prevent major accidents (i.e. safety management systems or hardware controls) may not be present on the plant. Where this concern exists, the course of action is to carry out an early inspection to check – and invariably, experience has been that the conditions or provision on plant is substantially better than that presented in the safety report. Many operators are not doing themselves justice, and certainly not doing the company any favours, by failing to properly describe and present in a logical fashion the information about how they control major accident potential. The concept of demonstration is at the heart of this, and clearly the CA has not got over in all cases what it is expecting to see, and some operators have failed to make a reasonable attempt at showing that what they have on site to prevent major accidents will work.

CURRENT DEVELOPMENTS WITH COMAH

The section above focussed on some of the early experiences of dealing with safety reports, and clearly there have been some problems. So what is being done to develop COMAH to address these issues?

The large jump involved in moving from the previous CIMAH regime to implementing the Seveso II Directive by the COMAH Regulations is epitomised by the following fundamental changes that COMAH has brought, and which were at least contributory to the early experiences:

- Formation of the CA by amalgamating HSE and Environment Agency input;
- A Safety Report Assessment Manual, used by the CA and available also to industry and anyone else via the Internet, which sets down the criteria against which safety reports will be assessed;
- The requirement for Demonstration in safety reports of safe operation;
- The concept of ‘Domino’ or knock-on effects from one major hazard site to another.

The most recent (and forthcoming) developments in each of these aspects will now be summarised.

COMPETENT AUTHORITY

The early challenges in bringing together the Environment Agency (concentrating on the environmental hazard potential) and HSE (taking the lead on safety and health) into an efficient joint regulator have been well documented, and there has been very good progress towards meeting these challenges. This has happened at the strategic level, via a Single Implementation Project that has set a framework for commonality between the two organisations. But it has also happened at local level, by individual HSE and EA teams coming together to produce joint working on COMAH safety reports and to present a more unified approach to operators. The COMAH system provided from the very early stages for common assessment of safety reports – inspectors from EA and HSE being part of the same assessment team, using the same criteria set out in the Safety Report Assessment Manual, and providing a single conclusion to an operator.

The output from a completed assessment is an inspection plan, phased over anything up to 4 years after the assessment in the first year. These are joint inspection plans that combine the identified needs from the assessment team covering HSE (regulatory inspector as well as specialist inspectors) and EA inspectors. The system is transparent to the operator, who has broad details of what the inspection issues are to be. These inspections are now beginning to be carried out.

The process has been less progressive for COMAH lower-tier sites, but EA and HSE teams are now developing and implementing joint inspection plans for these sites too - developed from a hazard-based approach by inspectors from each part of the CA sitting down to review past intelligence about a particular site and determining which aspects of an operation need to be inspected and with what priority. It will take some time for these inspection plans to be produced and implemented for all lower-tier sites, but the process has begun.

DEMONSTRATION

The problems with identifying exactly what is required for a demonstration of safe operation in a safety report has been an issue that has dogged COMAH from the start. These concerns have been expressed extensively within the CA, but quite properly industry representatives have also voiced their concern long and loud. There has been a very reasonable call for better clarification and examples of what a good demonstration comprises. It is in response to this latter stimulus that some action is being taken.

Earlier this year, a Working Group was convened at Huddersfield jointly by the CA and industry representatives via the Chemicals Industry Association, to explore the issues and to identify a way forward. 4 sub-Groups were formed with the task of developing guidance in specific areas on the level of detail required when providing information on the prevention and limitation of major accidents. At the time of writing this guidance is shortly to be published, and the results are awaited with interest both by regulators and industry in the anticipation of some much-needed clarification.

DOMINO

The concept of Domino was introduced for the first time with COMAH. The basic proposition is that if there are 2 or more major hazard sites close to each other with the potential for an incident to happen with effects outside the site boundary, there is a potential for an incident at one site to escalate by causing an incident at an adjacent site also. The COMAH regulations require the CA to identify such sites, by writing to operators and Emergency Planners, so as to stimulate a transfer of information between operators and emergency planners that can be taken into account in off-site emergency plans.

The CA identified Domino sites by means of the Consultation Distances used for assessing the suitability of land-use planning applications in the vicinity of major hazard installations. Each major hazard site has a zone assigned to it the size of which is based on the nature, quantity and usage of hazardous substances; this is used between the local planning authority and HSE to identify and provide advice on land-use planning proposals. The zones provided a rough-and-ready but viable way of identifying Domino sites. Where Consultation Distances from 2 or more sites overlap, and particularly where the overlap encompasses a hazardous installation such as a major storage or process vessel, the sites concerned have been designated Domino sites and required to begin the information exchange and consider what steps need to be taken. At the time of writing the sites have been identified and the activity is currently between operators and emergency planners to consider the implications. Full details are now included as a separate Chapter of the Safety Report Assessment Manual.

SAFETY REPORT ASSESSMENT MANUAL (SRAM)

Changes are afoot with the Safety Report Assessment Manual, which sets out the detailed criteria that the CA uses to assess safety reports against and also provides the process steps the CA operates under. The SRAM has been made fully available via the Internet, and operators who have to prepare safety reports are strongly encouraged to use it to inform the development of their reports.

A review was planned from the outset, to take account of lessons the CA had learned from the first round of safety reports and also feedback from industry. This will be an iterative process of monitoring, reviewing and implementing which will continue indefinitely in response to changing needs and changing information, but the first round of changes are now imminent. The full changes will be publicised through various committees such as Advisory Committee for Dangerous Substances, Chemical Industries Forum, and through industry contacts. Some of the key areas of change however are expected to be:

- Providing a view from assessors dealing with predictive or consequence analysis in safety reports at an early stage, to ensure that the measures considered in a report are proportionate to the level of risk from an operation;
- Greater emphasis on meeting company management where information in safety reports is insufficient and more is needed, to explain exactly what is needed;
- Where ‘further information’ is requested and provided, this information being part of the safety report and consequently being included on the public register;
- A better targeted Conclusions Letter after assessment, which sets out clearly the main elements of the planned inspection and verification programme.

This latter point is key to providing a link from the assessment process to the inspection phase, the importance of which is considered in the next part of this paper.

FROM ASSESSMENT TO INSPECTION

The Safety report assessment process by a multi-disciplinary assessment team is intended to achieve two basic things: firstly, to conclude on whether the safety report provides an adequate picture of control of major accident hazards at a site, including whether or not there are any serious deficiencies indicated in the measures taken on site to prevent major accidents. And secondly, to identify a programme of issues that members of the team need to inspect on site to verify the information in the report and to check on the physical and safety managerial standards of control. These latter inspection issues will be prioritised so that the most pressing are done soonest and the remainder programmed over anything up to 4 years after assessment. In some cases the issues can be dealt with on site by one inspector, in other cases a team approach (for example, an audit) may be necessary.

An important feature of the inspection plan is that it should be transparent to the operator, both in terms of content and approximate timings so that the operator knows what is in store. Indeed, 'best practice' in this area is for good liaison and exchange of information from the CA to the operator and vice versa so that issues are fully in the open.

The two essential parts of COMAH implemented by the CA, assessment and inspection, have to be seen as working in tandem. COMAH is not just about assessment, and it certainly does not finish with the conclusion of the assessment process – it is only beginning. The effectiveness of COMAH in identifying the potential for major incidents and for preventing them is more likely to derive from the inspection part of the process than from the assessment stage – this is increasingly becoming clear from the assessments completed so far, the inspections carried out after them, and perhaps most importantly incidents that occur. Incidents often provide a very good indicator, albeit after the event, of how well or how badly an operator manages safety to the degree of thoroughness needed for the highest hazard sites.

The next part of this paper will look at two recent incidents as a form of case study to evaluate whether assessment of a safety report alone would be likely to indicate problems that the regulator (or indeed industry) could act on, and hence prevent incidents. While two incidents are not capable of making a case one way or another, they are relevant here for several reasons:

- Both involved COMAH top-tier sites;
- Both involved serious incidents at companies where management thought they had good safety management and control systems;
- Both involved issues that needed to be considered in COMAH safety reports.

Both incidents also resulted in prosecution by HSE under the Health and Safety at Work etc. Act after detailed (and costly!) investigation, and fines imposed after guilty pleas. In as much as they have been dealt with by the courts the facts are therefore a matter of public record, however for the purposes of this paper the circumstances have been anonymised so as not to identify the companies concerned – the principles are what are relevant here to the point being made.

CASE 1 – IGNITION OF TOXIC AND FLAMMABLE GAS

In this incident, two contract welders were burned while working to repair a leak on a pipework system carrying a gas that was both toxic and flammable, when an escaping gas cloud ignited. A system of gas blowers was used to draw gas from one part of the process to another. One of the gas blowers was to be taken off line by the fitting of blanking plates while another put on line by the removal of blanking plates. To achieve this, isolation valves were used to isolate the parts of the plant concerned.

When re-instating a gas blower on line, a leak was detected at a flange. The contractors, under the supervision of a Shift Manager, attempted to seal the leak but a large release occurred which ignited and engulfed the two men. They escaped with burns and problems from inhalation of combustion fumes and the toxic gas, and fortunately made a full recovery.

The investigation revealed a number of factors that led to the accident:

(i) A special operating procedure was in use for the work, which had been done many times before. The procedure called for a very accurate control of pressure within the gas circuit, to reduce the possibility of leak on the part being worked on. It was clear from the investigation however that the instrumentation provided was neither designed nor capable of balancing pressures with sufficient accuracy and reliability to be able to perform such an operation reliably.

(ii) In any event, the instruments were not noted on any inspection and maintenance schedules, and no records of any maintenance could be produced.

(iii) The work also relied upon the closure of isolation valves to prevent the movement of gas. In the investigation it transpired that the isolation valve on the inlet side could not be closed, as it had not been maintained. Indeed, the Permit to Work issued for the job noted that the valve was "passing gas".

A combination of these factors therefore led to the release of the gas, and its subsequent ignition, from which 2 men were fortunate to escape alive. But could these factors have been identified before the event?

The safety report would have been required to contain details of a number of relevant factors. As part of the safety management system description, details of the maintenance and inspection systems and the control and supervision of contractors would have to be documented. There would also need to be details of how risk assessments were organised and undertaken, both for routine and maintenance work. The Permit to Work system would also have to be described. There would need to be a demonstration in the report that the measures taken by the company were proportionate to the hazard, and were effective i.e. were working. For a site such as this, both Process Safety and Mechanical Engineering assessors would have been included in the safety report assessment team and would have looked at many of the circumstances surrounding the work being done during this incident.

In most cases operators describe systems in place on the basis of how they anticipate they will work, rather than thinking about how they might not. At this site, as an example, the operator would have been able to highlight a maintenance and inspection system that was ostensibly detailed, well structured and computer-based. The company used a criticality approach to items to be maintained, and reasonable frequencies for inspection of items on the schedules had been set. Some of this could even have been demonstrated, for example by choosing suitably representative areas and detailing the actions taken. All very reasonable – except that in practice it was not working! The company's own investigation concluded among other things that the planning of the job was inadequate, the operating procedure was inadequate, there were deviations from procedures, the maintenance strategy for isolation valves was inadequate, and there were errors of judgement by personnel involved in the task.

If the company had done a sufficiently rigorous job in looking at it's own systems, it may (but would not with certainty) have discovered its own failings and could then have plugged the gaps. But the CA assessors, faced with an outwardly reasonable description of what was otherwise a comprehensive system, would have had little chance at the assessment stage of uncovering the true picture. This is only likely to have been possible during inspection, when the maintenance system would be given a thorough site inspection by examining systems, checking records, and asking questions of responsible individuals about how things worked in practice and where they sometimes might not.

If the system of balancing the gas pressures across the plant had been described, that is likely to have been sufficiently unusual for it to have raised queries at the assessment stage or more likely for it to be noted as an inspection issue for more detailed consideration under the inspection plan.

In terms of the relative effectiveness of assessment or inspection in preventing this accident, 1 – 0 to inspection.

CASE 2 – RELEASE OF HYDROCHLORIC ACID FROM A STORAGE VESSEL

The second incident relates to a release of concentrated (35%) hydrochloric acid (HCl) from a storage vessel, after bolts securing a flange at the base of the vessel failed and allowed a release of 20 tonnes of acid into the vessel bund.

The vessel was a 40-tonne capacity vertical storage vessel, in a common bund with five other vessels. At the base of the vessel was a nozzle and flange for a level measurement transmitter. The incident happened without warning, when two flange studs failed under acid attack and allowed the flange to open. HCl sprayed due to the head of hydrostatic pressure from the flange and into the bund; an acid mist also began to form and to drift off-site, where it was later smelled a few hundred metres away. Water curtains were set up around the bund, to knock down the acid mist and prevent it leaving the site, and the combined acid and water spray began to fill the bund.

After an hour or so, when the bund level had risen to about half full, part of the bund lining (specifically, the sealant in the expansion joints of the bund) failed under acid attack and the contents of the bund were lost onto adjacent concrete and eventually into the ground.

The investigation revealed the following failings that led directly to the accident and its consequences:

(i) The flange gasket had been passing acid for some time; this had been playing on the flange stud bolts until they had completely corroded through and failed.

(ii) There was visual evidence of substantial corrosion around the flange and adjacent pipework, as well as other nearby metalwork including the base of the vessel itself, and evidence of dripping acid on the concrete of the bund floor. This evidence could and should have been noted and acted upon.

(iii) The bund itself had not been coated to resist acid, and the sealant in the expansion joints of the concrete forming the bund had not been maintained and gave practically no resistance to acid/water mix in the bund.

(iv) The company had previous experience of corrosion problems with stud bolts used to make flange connections on hydrochloric acid duty.

As with the previous case, would any of these factors have been transparent in a safety report so as to be able to identify action necessary to prevent the incident?

The safety report would ostensibly present a very encouraging picture when describing the safety management system and in particular the maintenance inspection system. A

completely new, state of the art system was in the process of being introduced to replace an existing system that was itself apparently well structured. In addition the company management had shown a positive and progressive interest in maintaining high standards of safety and health across a range of issues.

The vessel concerned, in common with other vessels, had an external as well as an internal inspection frequency established – 2 years external and 5 years internal in this case. The inspection history showed internal inspections had been carried out in 1994 and 1996 (i.e. more than the set frequency) and a further external inspection in 1998. There was a detailed scope of inspection in a written procedure.

However on closer investigation, the procedure did not include any flanges and fittings as part of the inspections; there was no requirement in the procedure to examine these, let alone dismantle them and examine the condition of bolts, gaskets etc. There was a general pipework inspection programme, but nothing to cater for the particular hazards of hydrochloric acid duty. Apart from the failure to include the flanges and fittings as part of the inspection schedule, the weakness of the whole system was epitomised by the fact that there had been a recent painting programme for the vessels that had resulted in painting over the substantial corrosion already present.

Again in this case there was nothing in the safety report descriptions to alert assessors to the developing problems. The description of the maintenance and inspection systems would be more than adequate to satisfy the assessment criteria, and this could have been backed up by demonstration (even for the vessel concerned) that the measures were effective and were being carried out – inspection records were available for the vessel. It is highly unlikely that even the most suspicious inspector carrying out an assessment would have guessed that the procedure fell short of the flanges and fittings – though if this had been identified, then a request for further information would in all probability have drawn attention to the intrinsic weakness. What is far more likely is that an inspection programme to verify the claimed records and dealing with the condition of the storage vessels would have picked up the very obvious corrosion, and led to the right questions being asked and the appropriate action being initiated.

2 – 0 to inspection over assessment?

MOVING INSPECTION ON

A central argument of this paper is that COMAH is not just about assessment, but has to be seen in the wider context of a combined assessment and inspection scheme, the two parts of which need to work together to have the maximum chance of preventing major accidents at COMAH sites. It is the authors view that there has been a little too much made of the early problems with the assessment process and not enough about the longer term benefits of a structured, transparent system that combines an assessment process leading to the identification of inspection issues that are then examined in detail appropriate to the hazard and risk potential.

The two cases considered above do not, it is fully accepted, make a conclusive case for the value of inspection over assessment any more than they demonstrate what an effective tool COMAH in its widest sense can be. However, experience of many major incidents that have occurred at high hazard sites has shown time and time again that a structured inspection is one of the most successful ways of challenging beliefs about the effectiveness of safety measures and identifying the potential for things to go wrong. The efforts of operators to

identify these issues, and then to set them out in safety reports, is enhanced by the 'fresh pair of eyes' approach from the regulator working toward the same goal.

The challenge for the CA is how best to use its resources. The assessment process alone is extremely resource-intensive, and in the first assessments of an operator's reports ties up a substantial amount of expertise that is then not available for inspection. In the medium to longer term, the inspection plan produced from assessment has to marshal the correct mix of skills in the assessment team – specialists inspectors dealing with particular disciplines such as process safety or human factors, regulatory inspectors assessing safety management systems, and Environment Agency inspectors dealing with potential environmental impact. Furthermore, the whole process and proposed inspection strategy must be transparent to the operator so that they can see both the rationale for what is proposed as well as the detail of when it will happen and how much it will cost them.

From shaky beginnings, when neither the CA nor industry really knew what COMAH had in store, enormous progress has been made in developing the systems and understanding needed. A great deal is still to be done, but after much effort over safety report assessment the key stage has been reached where the benefits of implementing inspection plans at many COMAH sites can be realised.