Lessons learnt on inherent safety in legacy high-hazard plant – a case study

Dr Malcolm Toft, Principal Mechanical Engineer, and Peter Hunt FIChemE, Process Safety Director, Axiom Engineering Associates, Woodstock Court, 14-17 Bowesfield Crescent, Stockton-on-Tees TS18 3BL.

Abstract

This paper builds on extensive experience of managing asset integrity across multiple sites in the Chemicals, Oil & Gas, Energy, Pharmaceuticals industries including lower tier and top-tier COMAH sites, some with unusual and highly toxic inventories.

On one top-tier COMAH site, inspection revealed mechanical defects requiring rework in a sizeable population of large, mature vessels, and including the investigation of contributory factors and potential systemic remediations. The paper presents this case study highlighting with key findings and learnings.

Our approach starts from legal and codal frameworks, and considers the requirements of a COMAH report to assess "worst-case" scenarios, and to demonstrate that risks are ALARP through the evaluation of the risk reductions obtained by the implemented mitigation measures. Interaction between COMAH (concerned with all Major Accident Hazards, MAH) and PSSR (concerned with pressure hazards) is studied, and the effect that a PSSR-oriented procedural system can have on the prioritization and highlighting of COMAH toxicity risks.

Implementation of guidance in PD 5500 for prioritizing critical components of vessels on the site is reviewed, rather than applying a single construction category to an entire vessel. We find the guidance helpful but are not convinced that it is universally applied.

The study reviews a sample of corporate processes and identifies some safety input as potentially relatively generic or adjunct, rather than being central and critical from the outset. The question of how Inherent Safety was applied in the design stage is also considered. A number of PSSR-based systems which did not prioritise large vessels of highly hazardous contents at relatively low pressure are also identified.

Data dossiers are also reviewed, and note a general lack of integration with risk documentation, weakness in capturing design decisions, and iteration justifying each position taken e.g. regarding weldability.

Lessons learnt are identified regarding understanding of responsibilities under COMAH and PSSR, and relevant guidance in PD 5500. Considering risk. The operator's PHRs and the COMAH Safety Report together with project and design documentation are also reviewed, finding a range of factors including the selection of scenarios considered, approach to demonstration of ALARP, and strategy for demonstration of the basis for inherent safety.

Lessons identify working with procedural conflict, incomplete documentation and strategic risk visibility. They address management systems for their prioritization of COMAH vs PSSR, and project processes for their level of integration, as well as to what extent they genuinely embedded process safety in an effective manner. How procedural implementation followed through for the vessels and features of interest are also tracked.

In summary, we do not believe the findings to be unique to the particular site with many similar aging assets operating, and offer this case study to stimulate discussion about expectations in our industry, norms and practicalities around approaches to risk management, consideration of inherent asset integrity, proportionate pragmatism, and use of both good and best practice.

Keywords:

Assurance, COMAH, integrity, 5500, PSSR, welding, inspection, vessels, process safety.

1. Introduction

Following discovery of unexpected defects in service on a number of large, high-consequence pressure vessels, a top-tier COMAH operator commissioned us to investigate the underlying contributory factors. We therefore sought to carry out a top-level review of relevant provisions in key client processes, in particular considering the potential relevance of each of the following aspects:

- Risk assessment (HAZOP etc.);
- Projects/design;
- Procurement;
- Prescription of inspection criteria;
- Verification of third-party documentation and competence;
- Staff handover/induction processes;
- Any processes relevant to the implementation and integration of the above;
- Any other processes identified as pertinent during consultations with the client;
- Relevant process safety guidance for high-hazard plant.

Areas addressed are considered for their potential contribution to a barrier-type model of risk management as illustrated in Figure 1 below.

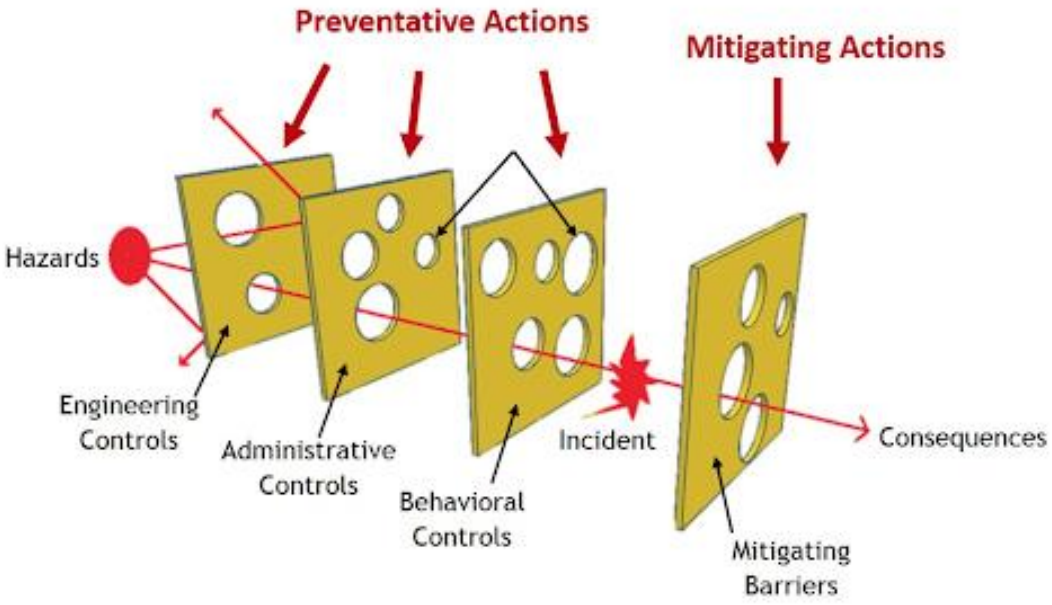

Figure 1. Barrier-type model showing action interactions for risk management

Each section investigates one of the following aspects or project stages in turn, finishing with suggested learning points. These are summarized at the end of our paper.

The next section sets out the legal and codal context for the work.

2. Legal and codal guidance

We first review key aspects of the legal and codal framework for plant, and share our experience of how well these are understood and applied in practice.

2.1 COMAH

(The Control of Major Accident Hazards Regulations 2015, Statutory Instrument No. 483)

These regulations place numerous duties on the operators of hazardous plant. Many of these have to be collated in the safety report. The words of clause 8 are relevant here:

"Every operator of an upper tier establishment must prepare a safety report for the purposes of—

(a) demonstrating that a major accident prevention policy and a safety management system for implementing it have been put into effect in accordance with the information set out in Schedule 3;

(b) demonstrating that the major accident hazards and possible major accident scenarios in relation to the establishment have been identified and that the necessary measures have been taken to prevent such accidents and to limit their consequences for human health and the environment;

(c) demonstrating that adequate safety and reliability have been taken into account in the design, construction, operation and maintenance of any installation, storage facility, equipment and infrastructure connected with the establishment's operation which are linked to major accident hazards inside the establishment;"

This requires operators to identify hazards, MAH scenarios, and demonstrate adequate safety and reliability in design, construction etc.

Terminology such as "limit consequences" etc. is usually interpreted as incorporating measures to reduce risks to a level which can be shown to be As Low As Reasonably Practicable (ALARP).

2.2 PSSR

(The Pressure Systems Safety Regulations 2000, Statutory Instrument No. 128)

PSSR has roots in historic boiler safety legislation, and is primarily concerned with hazards due to pressure. We have found, across a number of plant operators, that any procedures primarily focused on PSSR, or prioritizing using mainly PSSR as a guide, can sometimes not highlight vessels or features with particularly toxic contents, simply because they do not represent a significant pressure hazard. COMAH sites therefore need to prioritize considering factors from the COMAH report (see next section), not just PSSR. A top-tier COMAH site may appear to have a relatively low level of pressure hazard when compared to, for example, a high-pressure gas plant: but PSSR should not be the governing legislation in isolation from other requirements.

2.3 PD5500

(PD 5500: 2018 + A1: 2018 Specification for unfired fusion welded pressure vessels)

PD5500 gives guidance on levels of inspection required for different construction categories as follows:

"3.4.1 Construction categories

For each pressure-containing component of the vessel, the manufacturer shall select a construction category in accordance with Table 3.4-1. *The purchaser may require a minimum construction category in which case it shall be specified in the purchase specification. A component is defined as a part of pressure equipment which can be considered as an individual item for the purpose of calculation* e.g. flange, end, cylindrical strake." *(our italics)*

This text therefore specifically states that categorization should not necessarily apply to a vessel as a whole, but is specifically permitted to apply differently to different parts of a vessel, depending on criticality, ease of fabrication etc., as discussed in the following notes to PD5500 Table 3.4-1 (Table 2 here):

Table 3.4-1 **Construction categories**

Construction category	Non-destructive testing (NDT)	Permitted material groups and sub-groups	Maximum nominal thickness of component[a] (see 1.6) (mm)	Temperature limits	
				Upper	Lower
1	100% (see **5.6.4.1**)	All	None, except where NDT method limits	See **2.3.1.1**, **K.1.4.1.2** and Note 2 to **3.2.2**	See Annex D limitations for temperatures below 0 °C
2	Limited random (spot) (see **5.6.4.2**)	1[d], 2 and 4	40	See **2.3.1.1**, **K.1.4.1.2** and Note 2 to **3.2.2**	See Annex D limitations for temperatures below 0 °C
		1.2 CMo	30		
		8	40	None	None
3	Visual only (see **5.6.4.3**)	C and CMn steel (R_m[b] ≤ 432 N/mm^2)	13[c]	300 °C	0 °C
		8	25	300 °C	None

Figure 2. PD 5500 construction categories for pressure-containing components of vessels

"NOTE 1 Any one of the three construction categories in Table 3.4-1 will provide adequate integrity for normal purposes within the material and temperature limitations specified therein. *The justification for any special precautions (e.g. additional inspection and/or test requirements, secondary containment) to reduce external risks in the postulated event of an escape of hazardous vessel contents involves consideration of matters by the purchaser* (and Regulating Authority) which are beyond the scope of this specification. Any modifications to the requirements of this specification which are required for the purpose should be covered in the purchase specification." *(our italics)*

"NOTE 2 *Construction categories*, as defined in Table 3.4-1 *are intended to apply to components of a vessel and not necessarily only to complete vessels which may therefore comprise components in two or more categories*. Category 3, however, is commonly applied to complete vessels so that design stresses and inspection requirements are consistent throughout the vessel." (*our italics)*

We therefore conclude that there need be no such thing as a "Cat. 2 vessel", for example, but that the intent of PD5500 is specifically that different levels of NDT may be specified for different parts of a vessel, depending on risk. In our experience with a number of plant operators, this does not appear to be universally understood or applied in practice, but generic categorization of vessels (which may be either conservative or non-conservative for particular sections) remains common.

3. Risk assessment

We review a sample plant operator's Corporate risk guidance and the site's COMAH report risk assessments, in the light of the preceding guidance.

3.1 COMAH Report

COMAH reports are unsurprisingly geared to the *operation* of the site, rather than its *design*. We would ideally expect to see larger vessels itemised, but this is often not the case.

We would also generally expect to see some systematic exposition of the basis of safety for key vessels, building on their early hazard studies – what philosophy was applied e.g. total/secondary containment, all-welded, layers of protection etc.

The Quantified Risk Assessment should evaluate the worst-case consequences. For example, for high-profile sites, we expect to see the FN curves extending up to the theoretical maximum number of potential fatalities, in order to demonstrate that the probability of such catastrophic events is acceptably low (see e.g. HSE "R2P2").

QRAs in COMAH reports usually focus on consequence modelling, and there can be relatively little to justify the probabilities assigned to each potential event scenario. In particular, there is sometimes little demonstration of risk reduction by mitigation measures such as design control etc. In our view, such demonstration is a key component in giving confidence that risks are being managed to a level which is As Low As Reasonably Practicable (ALARP).

Assessments (especially if performed by an external body, using standard software) may consider available public properties of the material for both toxicity and mobility, which may produce a conservative assessment in dispersion characteristics, but not discuss the fundamental characteristics of any hazardous but non-standard product. Leak detection often forms part of the basis of safety for standard materials, with this normally being focussed on SIL-rated gas detection systems and, in cases of non-standard/detectable materials, reliance on operator observation and by camera is common. However, these measures are likely to have a larger threshold, and lower reliability, than most SIL-rated instruments.

Mitigation descriptions can sometimes be perfunctory, e.g. where the main reference to initial NDT as a risk mitigation might simply say that this shall be "appropriate". We expect to see some reference to systemic guidance correlating levels of inspection and potential consequence or criticality. This could usefully highlight key vessels. HSE guidance on COMAH reports is good, and should be followed.

It is therefore possible for both the probability and the consequence of potential leaks to be underestimated, leading to potential non-conservatism in the overall assessment of risk in the COMAH report.

We have reviewed a number of COMAH reports for various operators over the years. Our review of these documents indicates that many do not appear to consider unmitigated risk as a baseline from which to demonstrate risk reduction, and therefore struggle to demonstrate the benefit of alternative risk reduction strategies, which is a key component of demonstrating that risks are ALARP. An operator is required to do everything reasonably practicable to reduce risks – and it is possible that a particular plant configuration may not be able to be brought within the ALARP region of the FN curves in the QRA, if the particular volumes and processes onsite are intrinsically sufficiently hazardous to large numbers of people. Practices applied in the nuclear industry can become necessary in severe cases.

3.2 Corporate Risk Procedures

We have reviewed risk assessments, and their governing documents, in different capacities for various plant operators. One common theme in those review has been that application of recent good practice procedures for risk assessment to legacy plant can often produce higher risk rankings than originally considered in design, as corporate, public and legal approaches to risk tolerance evolve.

We also recorded multiple instances in this case of there being both Corporate and Site documents on related subjects (again, not unique in the modern evolving chemical industry), and therefore suggest that tighter integration may improve efficiency and performance in this regard.

4. Project and design

4.1 Design for Safety

Again, many operators' recent procedures contains numerous helpful provisions which could potentially have reduced the probability of issues on existing vessels if they had been in place at the time of design, construction etc.. Whilst backdating is generally impracticable, we ask whether this should be considered in this case if original design risk documentation cannot be located, or appears insufficiently robust.

Our review (consistent with our wider experience) brought to light cases where procedures exist in isolation and do not integrate, and where process safety can appear to be a relatively generic or adjunct consideration (e.g. "approves the design pack… with design safety considerations taken"). Procedures can often usefully be strengthened to ensure the primacy and centrality of safety and risk throughout the design process. Some of these changes are part of the ongoing improvements in the industry following process safety management (PSM) developments after the Buncefield incident, which are still being embedded into operators' documents nationwide. Such changes would appear likely to ensure that the relevant features on key vessels are given higher priority and visibility "from day one".

4.2 Design of Pressure Systems

Our review of a number of corporate design procedures revealed that many were driven by PSSR, and therefore may not always optimally highlight vessels whose principal hazard is toxicity rather than pressure. We suggest that, where the governing risk assessment for the site is the COMAH report, then supporting documents could perhaps better align with the critical regulations and hazards onsite, i.e. COMAH rather than PSSR. The situation may reflect history in which boiler rules for pressure hazards (evolving into PSSR) predate work towards COMAH (considering toxicity hazards).

PER/PSSR-based systems do not necessarily dovetail easily with COMAH toxicity/criticality. A PSSR-based approach will not necessarily highlight or prioritise large vessels of highly toxic fluid which are relatively routine in terms of pressure hazards.

4.2 General Requirements for Welded Unfired Pressure Vessels

Sound technical documents may contain much good guidance, but be relatively weak on oversight or strategy regarding categorisation, considering key parts of a vessel, or those which may pose particular challenges in fabrication. Documents can often usefully be strengthened to give more specific guidance on these subjects, and to join up with other documents both upstream and downstream in the design process. The wider documentation system needs to function as an integrated whole in order to offer effective risk mitigation.

4.3 Data dossiers

Many dossiers do not include risk documentation, nor any record of design discussion, decision or iteration (e.g. no "why", markups, minutes etc.). Whilst this is conventional practice, it is nevertheless regrettable that, for example, there may be no fabrication review on record which could have readily modified the weldability of critical features, for example.

Vessel drawings often give the design code for an entire vessel as e.g. "PD5500: 2000 Cat.2", which does not therefore apply the guidance given in PD5500 (discussed earlier), to give additional priority to any components of a vessel which might be especially highly stressed or difficult to fabricate.

We therefore conclude that the features of key vessels can thus be highly stressed, difficult to fabricate, with little material margin, and code guidance not followed in singling out such features, nor in reviewing their weldability, to add design or inspection mitigations. That feedback, oversight or review aspect of design iteration is key to delivering an optimal product.

5. Procurement

We have experience of both reviewing purchased product designs, and also of tendering for work ourselves with a great variety of prospective clients. Our learning from these activities is that modern procurement practice, of qualifying vendors technically, and then choosing between qualified vendors on price, does not always enable clients to differentiate technically. This can be particularly relevant for products which are especially high-consequence, or which contain features which may require particular fabrication skill.

We reviewed how vessels were identified as being particularly critical for high-quality procurement. Continuing the thread of logic from previous sections of this paper, we found that prioritization based on PSSR would not tend to mark key vessels out for any special precautions in procurement, whereas a consideration of COMAH risk could potentially highlight their criticality and consequence.

6. Prescription of inspection criteria

NDT can often almost be specified as typical by default, with no particular consideration of the criticality or difficulty of key welds, or of the challenges of inspecting a particular thickness. The selection of MPI for key welds can be based on a general assumption that only surface-breaking defects are critical. However, for welds of problematic thickness and accessibility, even 10% radiography can make a significant difference, and should therefore be considered.

7. Verification of third-party documentation and competence

Reviews of key welding contractors can only prevent problems occurring if these are genuinely a listening exercise, giving contractors space to feed back (e.g. “X will be really tricky to get into”?), and ideally such discussion should have happened in the design and specification for fabrication process, upstream of this point. Unless key features had already been recognized as critical, thick or cramped, for example, we suggest that any verification would then be unlikely to be asking the right questions by this point.

Questions are often best asked “open” rather than “closed”, e.g. “can you weld that?” will generally produce a “yes”, whereas “how easy is that to weld?” will enable more discussion.

Verification can usefully include frequent visits to the fabricator, in order to enable and encourage genuine dialogue. HSE now expect an operator to be an “intelligent customer”.

8. Discussion

We highlight for discussion our finding that, throughout our investigation, approaches which appear well-established in academic or regulatory circles may still not have achieved universal uptake even after some time. For example, the familiar hierarchy of control from the Health and Safety at Work Act (HASWA) were found in this case to have been applied as follows:

1. Eliminate risk at source – often difficult to achieve once a given process/storage plant configuration/concept has been selected in principle;
2. Substitute materials or processes – ditto;
3. Engineering controls – the range of these required becomes increasingly important depending on probability and consequence, and where the preceding two options are effectively not available; engineering controls are the main focus of this paper;
4. Administrative controls – found to be of some benefit here in mitigating and managing risks, but of less benefit than the preceding options (hence “hierarchy”);
5. Personal protective clothes and equipment (PPE) – a last-resort mitigation which we would not expect to see as a primary risk reduction measure in a COMAH report, for example.

We have therefore concluded that engineering controls are often key in vessel design where other mitigation options have already become unavailable. The interaction/handover between process safety and mechanical integrity therefore faces a critical hurdle at this juncture.

The vessels under consideration predate recent process safety developments, see for example the Process Safety Leadership Group (PSLG) Principles of Process Safety Leadership. Those principles are, not unreasonably, typically now applied to the *operation* of a site rather then necessarily its *design*, which may simply be a *fait accompli* by this point. We see a need to dovetail and integrate PSLG work with vessel design which has often historically been driven by PSSR. However, revisiting foundational work on inherent safety (Mansfield, Poulter & Kletz, 1996), we suggest that this concept cannot be “retro-fitted” to existing assets already designed, and that many plants may still exist where process design has been driven by the

chemical engineering and business needs, without a project "gateway" to require demonstration of thorough consideration of risk *elimination/avoidance* or *prevention*. A large body of legacy assets are instead heavily reliant on *control* and *mitigation*, as the risk moves "downstream" in the project process and hierarchy of control. The engineering integrity measures reviewed here are thus of elevated significance for these numerous vessels across our industry. In addition, process safety cannot be ensured simply by mentioning it in procedural documents, but requires greater granularity of detailed requirements, with supporting guidance, at each stage and aspect of the asset lifecycle in order to ensure its systematic implementation and effectiveness, and avoid potential gaps aligning in successive mitigation barriers (see "Swiss cheese" model).

9. Summary of conclusions

We therefore conclude that:

1. Scope still remains to strengthen COMAH assessments of critical vessels, to demonstrate that risks are ALARP, and to ensure suitable granularity on mitigations e.g. NDT;
2. Procedures geared to PSSR may not give suitable COMAH prioritisation;
3. Inherent safety requires integration in project/vessel design procedures, with suitable supporting guidance, to ensure that risk is avoided/eliminated at source where practicable: the early involvement of a multidisciplinary team (e.g. in design HAZOP) is recommended.
4. PD 5500 guidance on prioritising critical parts of key vessels is not always understood or followed;
5. Many good procedures postdate our assets, and would have produced different plant if available during design: differences in risk assessment may be particularly significant;
6. Data dossiers and associated verification activities do not always capture or enable discussion of key risks, weldability and inspectability.

10. References

The Control of Major Accident Hazards Regulations 2015, Statutory Instrument No. 483.

The Pressure Systems Safety Regulations 2000, Statutory Instrument No. 128.

The Health and Safety at Work etc. Act 1974, Chapter 37.

PD 5500: 2018 + A1: 2018 Specification for unfired fusion welded pressure vessels.

Process Safety Leadership Group (PSLG) Principles of Process Safety Leadership.

Mansfield, D., Poulter, L., and Kletz T., Improving Inherent Safety, prepared by AEA Technology plc and Loughborough Consultants for the Health and Safety Executive, Offshore Technology Report OTH 96 521, 1996.

https://www.hse.gov.uk/humanfactors/topics/customers.htm, accessed on 22nd September 2022, 10:07.