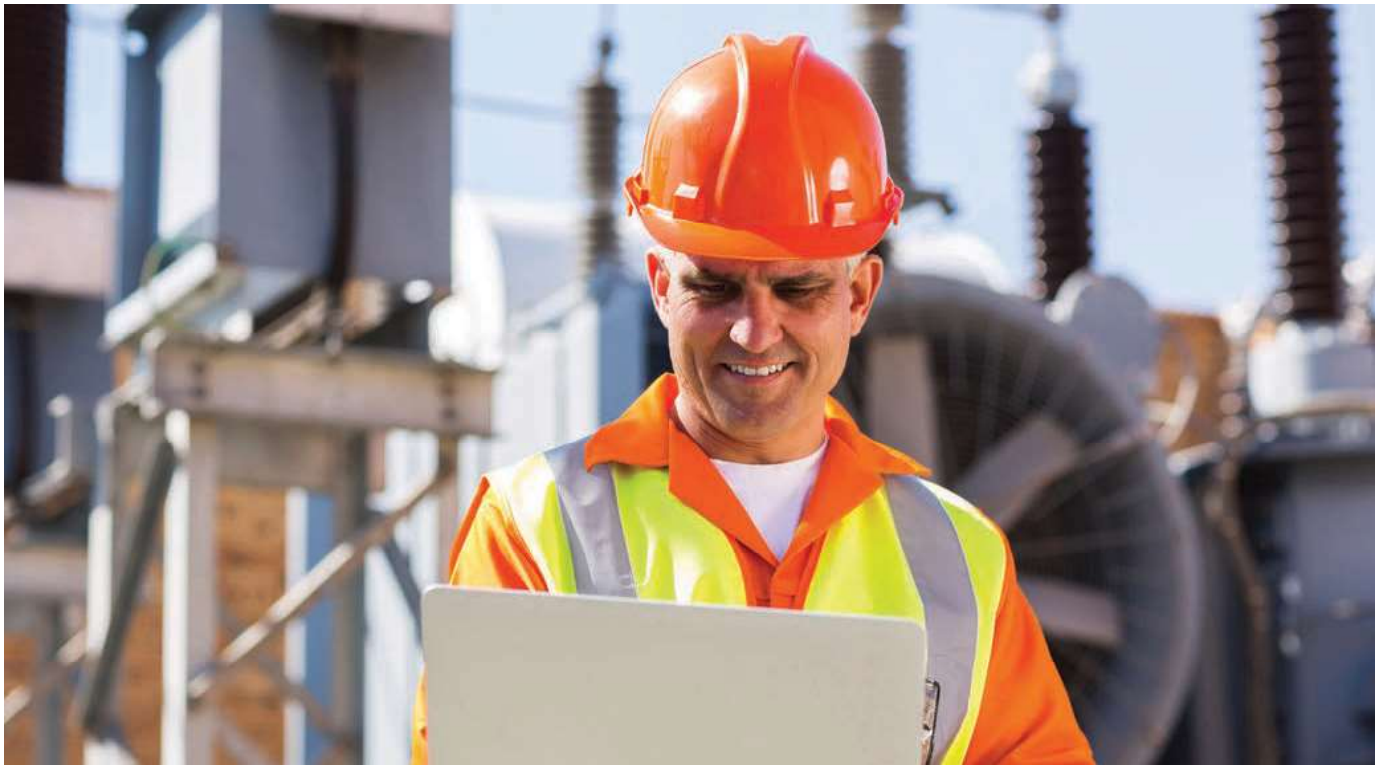


What Safety Studies Have You Got on Your Menu?

Andy Brazier and Nick Wise introduce a series looking at ALARP

THE process industry has been carrying out safety studies for decades. But can they ever prove that your plant is safe? In a case study (which is intended to illustrate some general issues and presents a simplified description of the plant and safety studies) we looked at several studies that had been carried out for a particular piece of process equipment. We were satisfied that the safety studies had followed good practices, were comprehensive and had resulted in reasonable outcomes. However, individually, none demonstrated that risks were as low as reasonably practicable (ALARP) and it was not clear how an overall picture could be obtained from the combined results. Also, we noted that inherent safety had received very little attention but at least one additional engineered control had been introduced as a result of carrying out the studies.

CASE STUDY

Process gas is heated by passing it through three parallel coils inside a heater fired by natural gas (*see Figure 1*). Operation is largely automatic, with a burner management system (BMS) providing startup and shutdown sequences; and controlling the process gas exit temperature.

THE SAFETY STUDIES

The process heater had been in service for many years without significant incident. During its lifetime it had been subject to a number of safety studies using different methods. The three most recent had been: process hazard review (PHR); layers of protection analysis (LOPA); and safety critical task analysis (SCTA).

PHR

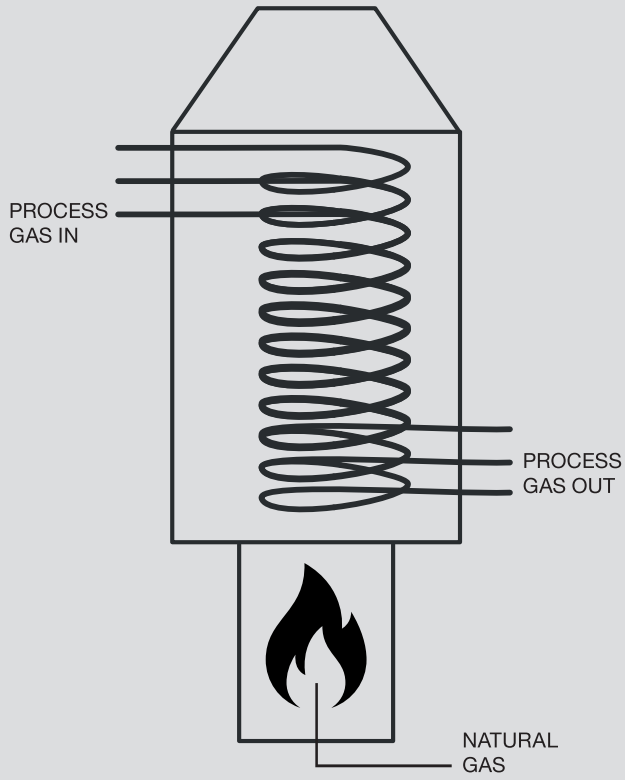
PHR is a systematic identification and assessment of hazards and risk controls. It is similar to HAZOP but requires less resource and is generally carried out retrospectively. The study of the process gas heater had identified the following major accident hazards:

- heater coil failure due to firing with no process flow;
- heater coil failure due to flame impingement;
- explosion inside the heater due to flammable atmosphere during startup;
- failure of downstream pipework due to high exit temperature of process gas.

Focussing on the first scenario (coil failure due to no process flow) the PHR identified the following risk control 'safeguards':

- burner management system;
- low process gas flow alarms;
- low process flow trip;
- coil high temperature alarms;
- coil high temperature trip; and
- procedures for heater de-isolation and startup after maintenance.

FIGURE 1: SIMPLIFIED DRAWING OF THE PROCESS HEATER



No improvement actions were raised as a result of studying this scenario. This may imply that everyone was satisfied with existing arrangements. Also, there was an ongoing project to review and potentially upgrade the coil high temperature trip following a LOPA study (*see below*). The PHR will be revisited on a regular basis (every five years) and future revisions will have the benefit of input from the LOPA.

The PHR achieved its objectives by identifying major accident hazard (MAH) scenarios and reviewing safeguards and included some prompts to consider whether risks for certain scenarios are ALARP. Although the study report demonstrated a thorough review of hazards and risks, it did not make any explicit claims regarding overall risks being ALARP.

LOPA

LOPA is a semi-quantitative assessment of hazardous scenarios. One of its main uses has been to determine the required safety integrity level (SIL) for safety instrumented systems (SIS). The method provides clear guidance that credit can be taken for layers of protection if they are independent and reliable. The method allows the calculated overall risk of the scenario to be reduced because those layers of protection are considered reliable enough to prevent an initiating event from developing into a hazardous outcome.

The LOPA study of the process heater had been completed following the PHR. The likelihood of blockages in coils stopping process gas flows (initiating causes) and the potential impact in terms of harm to people were considered. The LOPA only took credit for one existing safeguard, the heater trip acting on low process flow. The existing flow and temperature alarms were acknowledged but minimal credit was taken because there was no certainty that operators would always be able to react quickly enough. No credit was taken for the burner management system or operating procedures; or any mitigation controls.

The LOPA assessment team concluded that the existing risk was not acceptable. They repeated the risk calculations with an additional, independent SIS rated as SIL-1 and concluded that the risks would then be acceptable. This addition was accepted and an SIS acting on coil temperature that closes a valve in the fuel supply to the heater was developed. This required new instrumentation, logic solver and a valve to be installed.

The LOPA was carried out conservatively, which may be considered the safest approach. But it is not entirely clear whether the LOPA demonstrates whether the overall risks have really been reduced. Particular issues remained unanswered, including:

- additional risks introduced by the SIL-1 high coil temperature SIS, particularly associated with routine testing and maintenance; and greater likelihood of process trips;
- the maintenance strategy for the low process flow trip because some credit was taken for this in the LOPA;

- the PHR identified the high coil temperature alarm and burner management system as safeguards but these were not taken into account in the LOPA.

The quantification element of LOPA can be reassuring because it appears to give tangible targets and evidence that risks have been reduced. However, it is not clear whether numbers like these ever demonstrate that risks are ALARP.

SCTA

SCTA provides a structured and systematic way of identifying tasks associated with MAH. The most critical tasks are assessed, potential human errors identified and risks evaluated qualitatively.

Operations and maintenance tasks related to the process heater were identified and ranked according to their potential to cause or contribute to MAH. Information from the PHR and LOPA was cross-referenced with operational experience to ensure all credible scenarios were considered.

De-isolating the process heater and returning to service after maintenance was the only operations task with a credible potential to result in the heater operating with no process flow through the coil. This could occur if a valve was left closed in error. Procedural controls including pre-startup line walks were considered effective at preventing this with the various alarms and trips being sufficient to prevent an accident if the error occurred and was not detected before the heater was started.

SCTA IS EFFECTIVE FOR ANALYSING SPECIFIC TASKS AND CAN INCLUDE A CONSIDERATION OF WHETHER THE RISKS ASSOCIATED WITH THAT TASK ARE ALARP. HOWEVER, IT IS CLEAR THAT MANY HUMAN ACTIONS AND POTENTIAL ERRORS ARE NOT ASSOCIATED WITH SPECIFIC TASKS AND SO NOT CAPTURED BY SCTA

Function testing the coil high temperature SIS was the only maintenance task identified related to the scenario that warranted SCTA because it has a high reliance on human performance, and consequences in the event of error could be significant. However, the analysis of this task highlighted that it did not involve anything particularly different to other SIS testing tasks carried out on the plant. All other instrumented systems including the process gas low flow and various alarms were considered to be standard items and covered by generic task analyses.

The SCTA provided useful validation that the way tasks are being performed is effective at managing the known risks of MAH. Only a small number of tasks could be identified with a direct link to the scenario of interest. However, people make a much greater contribution to the risk (in positive and negative ways). For example:

- manual valves could in theory be operated at any time (ie not just startup and shutdown) but this is avoided because everyone knows that they should not operate valves without a specific reason;
- operators are monitoring the process continually and can be effective at detecting problems early, based on subtle changes. An example is the formation of hydrocarbon hydrate in instrument process lines resulting in false readings. Instrumented systems can be designed with health check facilities but operators can often detect early indications of hydrate formation far earlier;
- general maintenance will be carried out on the process heater on a regular basis. Much of this is generic and so is very difficult to link this to the scenario.

SCTA is effective for analysing specific tasks and can include a consideration of whether the risks associated with that task are ALARP. However, it is clear that many human actions and potential errors are not associated with specific tasks and so not captured by SCTA.

SEEING THE BIGGER PICTURE

There was enough consistency between the findings of the PHR, LOPA and SCTA to confirm that the current understanding of MAH potential for the process heater was accurate. On

FIGURE 2: ARRANGEMENTS IN PLACE TO PREVENT 'NO FLOW' RESULTING IN 'COIL FAILURE'

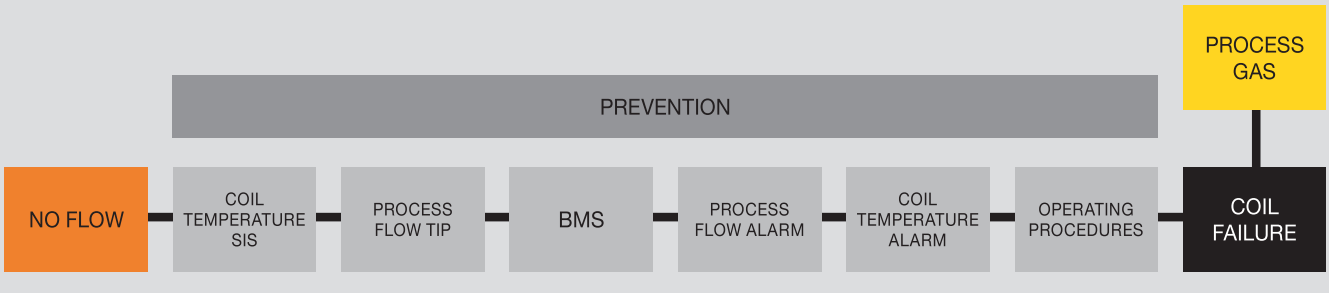
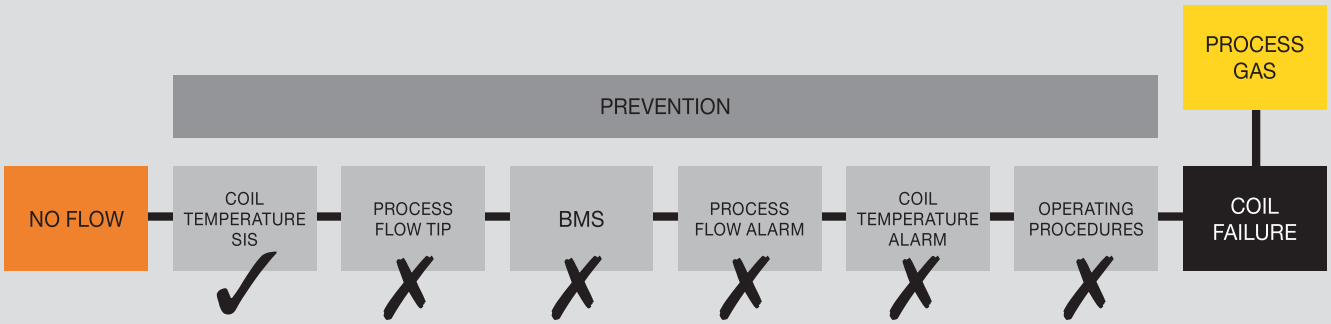


FIGURE 3: SHOWING ONLY ARRANGEMENTS THAT SATISFY THE DEFINITION OF "BARRIER"



the other hand, none of the studies had made any attempt to categorically claim that the overall risks were ALARP, which is what legislation (in the UK) actually requires.

Whilst the terminology used in each of the studies differed (ie PHR refers to safeguards, LOPA refers to layers of protection and SCTA tends to refer to risk controls) they are largely interchangeable. Is it possible to demonstrate risks as ALARP by listing all the controls in place? One way of doing this is the safety barrier or bow-tie approach (*Figure 2*).

Six barriers seems quite robust and reassuring. However, they will not all be equally effective, and common cause failures have to be considered. Recent bow tie guidance[1] published by the Center for Chemical Process Safety (CCPS) and Energy Institute (EI) states that 'barriers' can be considered only if they are:

- effective - perform the intended function when demanded and to the standard intended;
- independent - of the threat and all other barriers on the pathway; and
- auditable - to confirm the barrier works to a defined standard.

Applying this guidance to the process heater has quite a dramatic impact because most of the measures in place in this specific instance did not satisfy the definition of a barrier, for example due to a common dependence on the plant's basic process control system (*Figure 3*).

SAFETY STUDIES HAVE HELPED US TO IDENTIFY HAZARDS AND EVALUATE THE ARRANGEMENTS IN PLACE TO CONTROL THEM. THIS CASE STUDY SHOWS THAT USING DIFFERENT METHODS TO LOOK AT THE SAME EQUIPMENT GIVES A DIFFERENT PERSPECTIVE THAT IS USEFUL

This significant reduction in the number of classified barriers appears reasonable and encourages a "quality over quantity" approach to managing risk. But is it really true to say that all of the barriers that have been excluded make no contribution? The concern is that this approach will encourage the addition of more sophisticated engineered devices, which will increase complexity and is detrimental to inherent safety[2]. Also, it removes the incentive to improve other arrangements including operational controls (eg process alarms, operating procedures) that we instinctively know can make a positive difference. It is difficult to see how focussing on barriers that satisfy the definition can help when deciding if risks are ALARP.

CONCLUSIONS

Safety studies have helped us to identify hazards and evaluate the arrangements in place to control them. This case study shows that using different methods to look at the same equipment gives a different perspective that is useful.

Our concerns are that inherent safety may not be receiving the attention it deserves and it is likely that if we keep doing more studies we will actually end up with more engineered controls. This introduces significant lifetime costs and does not help us to determine whether risks are actually ALARP. Engineered controls may be preferred because they are tangible items that can be assessed during safety studies, both quantitatively and qualitatively. The problem is that being unable to take credit for less tangible operational controls removes the incentive to improve them, even though instinctively we know they can make a very valuable contribution.

Next month's article will discuss your personal responsibilities when deciding if systems are safe. ■

Andy Brazier AMIChemE is Consultant at AB Risk; Nick Wise CEng FIChemE is Business Support Manager at SSE Thermal

REFERENCES

1. CCPS/Energy Institute 2018, *Bow Ties in Risk Management*, Wiley.
2. Kletz, T, Amyotte, P, 2010, *Process Plant – A Handbook for Inherently Safer Design*, 2nd Edition, Taylor & Francis.