Safety practice

Shared isolations

Andy Brazier, AB Risk Limited, UK

Summary

Removal of an isolation was identified as one of the causes of the Piper Alpha disaster. The operators did this to start a pump without realising its relief valve had been removed for maintenance. The underlying cause was that the pump isolation was not cross referenced with the removal of the relief valve.

This paper summarises several issues with process isolations based on the events at Piper Alpha, namely use of shared isolations and management of change. Process isolation is a critical and complex subject, and this paper only touches on the subject. A key message is that people can often perceive an isolation as guaranteeing safety when the reality is that it is only a means of reducing rather than eliminating a risk.

Keywords: Isolation

Introduction

Maintenance on process plant introduces the potential for people to be exposed to a hazard (personal safety incident) or for a loss of containment of hazardous material (process safety incident or major accident). In an ideal world the hazard would be completely eliminated from a facility before any intrusive work took place. In practice this is normally impossible and so the risks are managed by isolating the plant where work is being carried from sources of hazard.

On process plant the sources of hazard that need to be considered when planning work include process fluids, electricity, stored energy and radioactive sources. Isolation procedures (whether written or not) will usually involve the following steps:

- create a barrier between the source of hazard and the worksite;
- prove the integrity of the barrier;
- remove any stored process hazard (e.g. flammable or toxic substance remaining in the system);
- discharge any stored energy (e.g. hydraulic or pneumatic pressure, mechanical spring, electrical charge);
- secure the isolation;
- record the status of the plant so that it can be handed over for maintenance to take place.

This is usually relatively easy for electrical supplies. Isolation will usually involve switching off the supply at source, locking the switch in the off position and 'testing for dead' at the worksite to confirm the supply has been stopped. Process isolations can be more complex and will often involve closing and securing multiple valves, venting to relieve any trapped pressure, draining and purging to remove the process fluids and testing to confirm the worksite is free of hazard and to prove the integrity of the isolation valves. Accounting for stored energy when preparing to carry out work can be particularly difficult as it is not always very easy to identify where it may be. Radioactive sources, on the other hand, are generally quite straight forward as their use is highly regulated and design and use is standardised.

What happened at Piper Alpha?

The release of hydrocarbon condensate that caused the initial fire at Piper Alpha occurred because a pump was started whilst its relief valve was missing. Hydrocarbon condensate leaked from the flange where the relief valve was normally connected.

The relief valve had been removed during the previous day shift for maintenance. This had been done without incident, indicating that it had been successfully isolated at the time. The relief valve did not have its own isolation points (i.e. there were no valves at its inlet) so these had to be created at other points in the system. In this case an isolation put on to allow maintenance work to be carried out on Condensate Pump A was also suitable for removing the relief valve.

The operators on the night shift did not realise that the relief valve was missing because this had not been communicated at the shift handover. They knew that Pump A had been isolated, but there was no indication at the pump's isolation points that they were also being used for the work on the relief valve. Removing the isolations and starting the pump resulted in condensate flowing from the flange where the relief valve had been removed.

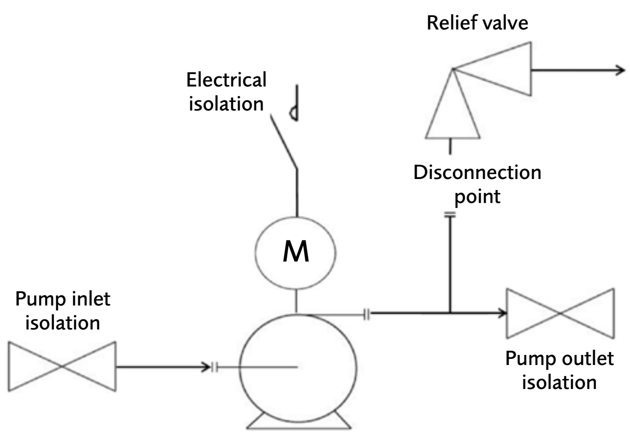


Figure 1– Simplified diagram of the Condensate Pump and relief valve

engineering and design

systems and procedures

0260-9576/18/$17.63 + 0.00

IChemE

Poor cross-referencing of work — a key cause of the disaster

The Public Inquiry into the Piper Alpha disaster concluded that Condensate Pump A had been "electrically and mechanically isolated"[1] during the day. This would have involved switching off the electrical switchgear and shutting a number of valves.

The inquiry identified that two separate permits to work had been issued. One to carry out maintenance on the pump. The other to allow the relief valve to be removed.

To issue a permit it would have been necessary to consider any isolation requirements. There was no evidence to suggest that permits were issued at Piper Alpha without doing this, so it is assumed that the permit to remove the relief valve was relying on the isolation put in place to carry out the pump maintenance. The problem was that the two pieces of work were not cross referenced, meaning that the shared isolation was not recorded. Combined with failures at shift handover, the night shift were not aware of the plant status.

When Condensate Pump B tripped due to a blockage caused by hydrate formation the operators determined that although isolated, Pump A was in an operable state as the planned maintenance had not commenced. The inquiry found evidence that the permit for the pump maintenance was formally cancelled so that it could be returned to service. Unfortunately, the people doing this did not know that the relief valve was missing because this was not referenced on the permit for the pump maintenance or the record of isolations.

Issues to consider when managing isolations

Management of electrical isolations is fairly standardised. Sometimes described as 'Lock Out Tag Out' (LOTO), it involves anyone using an isolation (i.e. working on the piece of equipment that has been isolated) to attach a personal lock to the electrical switchgear, which will be in the 'off' position. Special hasps are used to allow multiple locks to be attached if there is more than one piece of work taking place. This means that the isolation cannot be removed until everyone has removed their personal lock, which they would only do once their work is complete. Tags are also applied to identify whose locks are attached.

Process isolations are not so easy to secure. Not all valves have the facility to be locked in position and isolations will often involve a large number of valves and so it is impractical for everyone to attach personal locks at every isolation point. Also, achieving an isolation is less certain. Valves will often fail to isolate due to physical issues with seals etc., whereas problems with electrical switchgear will usually cause it fail to a safe condition (i.e. power supply isolated).

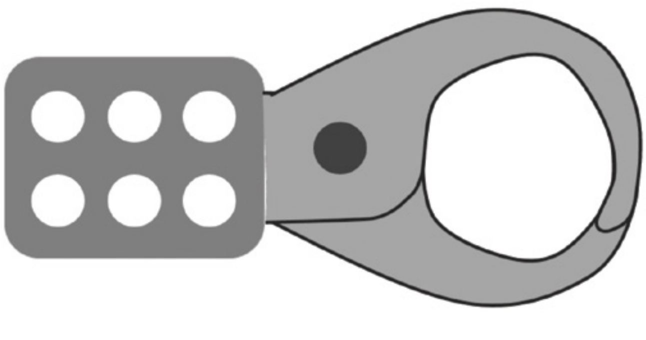
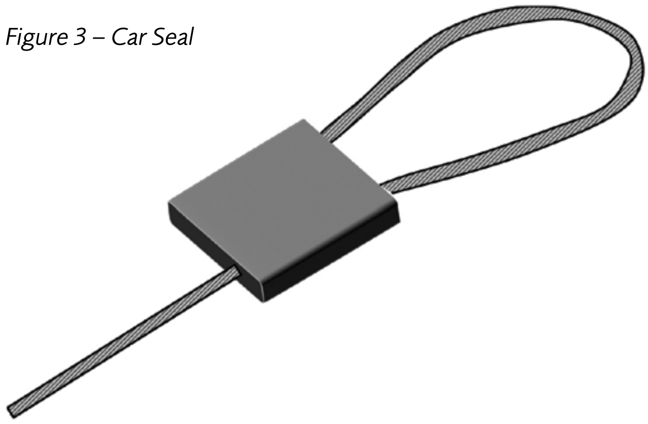


Figure 2 – Hasp allowing multiple locks to be attached

Figure 3 – Car Seal



There are two main reasons for securing valves used to create a process isolation:

- prevent accidental operation of the valve (e.g. being inadvertently opened);
- prevent people operating the valves for a purpose unrelated to the work requiring the isolation.

A physical means of securing a valve is generally preferred because it addresses both concerns. But, whilst this may be achieved by a standard key operated padlock (or similar) other devices are often used including cable ties and 'car seals.' These alternatives may appear to be less secure because they can be opened without a key. But they do have some advantages because they can only be used once and so every movement of a valve can be monitored; whereas a padlock can be reused indefinitely by anyone who has the key.

Any of the methods used to secure isolations can be defeated (locks can be cut off) and human error can mean that people controlling an isolation may allow them to be removed at the wrong time (as happened at Piper Alpha). For this reason, the main control of isolations is actually procedural. Isolation certificates (or similar) are often used. They provide a formal record of status and are used when returning plant to service to ensure all isolation points are removed.

Managing isolations for a single piece of work is relatively straightforward. But Piper Alpha highlighted that complications often arise due to sharing of isolations and changes to plans and scope of work. This means it is essential that people have a full overview of all work that is going on and remain alert to potentially adverse interactions.

Ensuring process isolations are managed properly

The issues with process isolations that contributed to the Piper Alpha disaster still remain relevant. There is relatively little guidance available on the subject, and what makes sense on paper does not always work in practice[2, 3].

Use of shared isolations is common and often a practical necessity. The term 'boundary isolation' is sometimes used. Guidance document HSG 253[4] states that these involve use of "fully pressure rated spades or spectacle blinds at every point of the plant boundary." In practice other forms of isolation (e.g. double block and bleed) may be used, depending on the nature of the hazard and the work being carried out.

0260-9576/18/$17.63 + 0.00

Most of the problems with shared or boundary isolations are how they are perceived rather than any inherent weakness.

One perception is that a shared isolation means that the plant is 'fully isolated' so that there is no need to consider specific requirements for each piece of work. This may be acceptable as long as it can be guaranteed that the shared isolation will remain in place for the full duration of every piece of work. As demonstrated at Piper Alpha, this requires thorough cross checking of work and the isolations being relied on. As a minimum, every piece of work using the shared isolation must be identified on the isolation certificate; and permission shall not be given to remove any isolation until every piece of work has been confirmed as complete. Mandating every work-party to attach their own locks, tags or car seals to every isolation point should be considered so that none can be operated until every work party has removed their tags.

Another perception is that the plant is in a safe condition because it will have been made hazard free as part of the isolation. The scale of shared isolations means that it can be difficult to clear fluids from every part of the plant, and residual hazards may be released by one piece of work that can affect every other being carried out within the isolation. Also, some work can introduce a hazard that may affect others (e.g. nitrogen for leak testing). This issue can be mitigated by creating local isolations for individual pieces of work. This can be perceived as providing additional levels of safety. However, it is usually impossible to prove the integrity of these local isolations because the plant will already be shutdown so that there is no pressure available to check whether a valve is sealing. Care must be taken to ensure these additional, local isolations are not viewed as 'the' isolation for the work and cross checking with the shared or boundary isolation must always be carried out rigorously as discussed above.

Managing change can be particularly difficult, for example if problems occur that require a longer duration and/or a more wide-ranging isolation to be used. At one plant a gas release occurred when moving an isolation point so that more plant was covered by the isolation. The plant had been shut down, but an upstream process problem meant that return to service was going to be delayed by a considerable amount of time. This was viewed as an opportunity to increase the scope of the planned maintenance, to complete additional tasks that had been on the 'to do list' for some time. The problem occurred because the new isolation was only documented by amending the procedure for the original isolation. The person making the amendments assumed that the operators implementing the new isolation would know the full status of the plant and realise that a valve had been left open to create a bleed that would have to be closed when creating the new isolation. However, the duty operating team had not been involved in the original isolation and did not recognise this. Gas escaped from the open bleed. The key message is that all isolation procedures must include a clear definition of the original status of the plant, which must be confirmed on plant before proceeding (i.e. not rely purely on paperwork). This is particularly the case when a change is being made as the plant status will be different to normal.

Unsurprisingly, planning isolations for major maintenance shutdowns is particularly challenging. It often needs to take account of the specific pieces of work planned, particularly where higher levels of isolation are required due to confined space entries and other specialist activities. Companies generally recognise that every shutdown is different and generate a new procedure each time. Problems arise because the people tasked with generating the procedure will generally use the previous example as their starting point. But as the scope is always different this starting point will include items that need to be excluded, whilst other scope needs to be added. Procedures become very complex as a result and it becomes very difficult for people to check the procedures in advance or to implement them in practice. It is usually much better to document a standard isolation procedure that is considered to be the starting point for every subsequent procedure. Then each time a shutdown is planned the standard procedure is amended for the specific scope so that there is a robust starting point each time.

Conclusions

Piper Alpha highlights how isolations are critical to both personal and process safety. Unfortunately, there is relatively little guidance available to assist anyone setting up an isolations management system.

There are many aspects to consider with isolations and this paper has only touched on issues surrounding shared isolations and some aspects of managing change. The following may give some indication of issues to be considered when developing or reviewing an isolation management system:

- Every piece of work relying on a shared isolation must be listed on the isolation certificate.
- Requiring work-parties to attach their own locks, tags or car seals to shared isolation points should be considered.
- It is often not possible to prove the integrity of local isolations installed for specific pieces of work within a shared isolation. However, people often perceive them as providing an additional level of safety, which may not be the case.
- Particular care must be taken when modifications are made to an existing isolation, and a full procedure must be produced that covers the current status of the plant. Amending the original isolation procedure is not appropriate because the starting point will be different.
- Standard isolation procedures for major shutdowns should be developed and kept as the starting point for every shutdown. Amended versions developed for specific shutdown scopes should be archived after use and not used as the basis for the next shutdown.
- Line walks and other checks in the field must always be carried out before returning plant to service after maintenance instead of relying simply on paperwork.

References

1. Sylvester-Evans . "*Background*" - To the Piper Alpha Tragedy. IChemE Symposium Series No. 122
2. Brazier 2013. *Process Isolation - It's More Complicated than you think*. Loss Prevention Bulletin 231
3. Brazier 2016. *Double Block and Bleed - It's More Complicated than you think*. Loss Prevention Bulletin 250
4. HSE. HSG 253 The Safe Isolation of Plant and Equipment

0260-9576/18/$17.63 + 0.00