Interlocking isolation valves – less is more

Dr Andy Brazier, AB Risk Limited, www.abrisk.co.uk

Interlocks provide a means of coordinating the function of different components so that task steps have to be performed in a specified sequence or certain conditions have to be met before a task can proceed. Valves used to create process isolations can be interlocked so that it is physically impossible to manoeuvre them in an incorrect sequence. This is often seen as a method of eliminating the potential for human error.

Advances in technology have allowed more extensive and complex interlocks to be used, which on the face of it, appears to provide the opportunity to make isolations safer than ever before. However, interlocks do not actually eliminate errors; and complexity can be a source of risk. In fact, when all factors are considered there may be an argument to say 'less is more.'

Whilst there is some guidance available about when interlocks can or should be used; there is very little to say which or how many components should be interlocked. This leaves designers with a dilemma. Do they attempt to apply a 'sensible' approach, which may leave them open to criticism because their design is not totally 'error proof?' Or do they go to an interlock vendor and ask them to interlock everything,?

One of the problems is that the reason for using interlocks is not always clearly understood or defined. Are they provided to:

- Ensure a 'spared' item (e.g. relief valve, filter) remains available at all times and is not interrupted when changing over duty/standby?
- Ensure isolation valves are in the correct position before carrying out a task?
- Ensure the item has been fully isolated and prepared for the task by ensuring valves are manoeuvred in a defined sequence and secured in the correct position;
- All of the above?

Extensive and complex interlock systems are expensive to purchase, install and maintain. They are often only effective for performing one task, and so cause significant problems when other activities have to be performed or if a problem occurs (e.g. valve passes or pipework is blocked). Also, they can create a false sense of security that introduces human factors risks. This paper will discuss these issues using real life examples and suggest that less really can be more.

Key words: Human factors, process isolation, interlocks

Introduction

"Those bloody interlocks. They are fine if you are starting in exactly the right place, doing exactly the right task and everything is working perfectly. Most of the time they are a complete nightmare."

I only mentioned pigging to a process operator whilst talking about procedures and this is the response I got. Further discussion uncovered issues with operator 'work arounds,' use of 'master keys' and being forced to proceed with a task despite key conditions not being achieved.

I have observed that more interlocks are being used on process plants, and systems are becoming more complex as a result. I have queried the reason for this on a number of occasions and not received a satisfactory response. It appears that because it is possible to interlock a function there is an assumption that it must be a good idea. But there are no philosophies or policies being applied. This means that there is no benchmark that can be used to demonstrate that a simpler solution is acceptable. When decisions have to be made, people feel that they may be criticised if they do not select the more complete system. But this does not take into account that complexity is a source of risk in its own right and that at some point this negates the potential safety benefits of using interlocks.

This paper discusses the role of interlocks in safety in the process industry. It aims to encourage a 'sensible' approach to interlocking and a view that 'less is more' in most applications.

What is interlocking?

Interlocking is a means of making the state of components dependent on each other. In general terms it means that one item cannot be operated unless another item is in its required state. Interlocks can be electrical, electronic or mechanical. Everyday examples include machines that will not operate unless their safety guard is in position, doors that cannot be opened whilst a machine is running and so called 'dead mans' switches that have to be kept pressed in at all times to confirm a person is present and in control.

Interlocks can have a role in safety by preventing control actions from being undertaken that might initiate a hazard (HSE website). They can reduce the likelihood that people will do things that put themselves or others in danger.

How are interlocks used in the process industry?

Interlocks are used widely in the process industry. Specific applications are often attractive as they are considered to provide a risk reduction at a relatively modest cost (Ellis 2003).

Trapped key interlocking is a commonly used method of ensuring valves are opened and closed in the required sequence. A key is required to operate an interlocked valve. When this valve has been operated another key becomes available. This is then inserted into the next valve in the sequence. This ensures that valves are operated in a sequence and can prevent the wrong valve from being operated (if it is interlocked).

Advances in technology have provided new ways of applying trapped key interlocks, beyond mechanical devices. For example, control systems have been employed that trap keys until certain process conditions have been met.

The human factors of interlocking

Interlocking appears to provide a 'fail safe' means of ensuring safety because people cannot perform actions (operate valves) in the wrong sequence. One manufacturer claims that their proprietary interlocking systems "remove the 'human factor' by ensuring dangerous processes happen only in a designated sequence." Another claims that their products are able to "enforce and guarantee a pre-defined sequence of operation and so eliminate human error."

The reality is that it is never possible to remove the human factor or eliminate human error. Whilst it is acceptable to claim some reduction in the likelihood of some specific operational errors, there are many other factors that need to be considered. An interlock is only as good as the person maintaining it (Edmonds 2016) and when it fails the operator is usually the only line of defence (Marsden et al 2003).

Examples of issues encountered when examining the wider human factors of interlocks include:

- Assuming it is safe to operate a valve because the key fits. Design and maintenance errors can mean that a key can fit in the wrong valve. Interlock systems may not have considered every task or set of circumstances;
- Being forced to continue with a sequence of steps that may not be the most effective or safe. A good example of this is where the integrity of an isolation cannot be confirmed because the sequence does not allow it;
- Using 'master' keys to override interlocks due to equipment problems or carrying out non-routine activities; without understanding the risks;
- Paying less attention to the task because of a perception that interlocking means it cannot be done wrong (believing the marketing hype).

All interlocks can be defeated. Whilst this is often viewed as a violation, human factors tells us that most violations are caused by job or organisational factors (i.e. people feel that they have to defeat the interlock to get the job done). This becomes more of an issue as routine reliance on interlocks can reduce awareness of the criticality of certain operations and the associated safety implications (Marsden et al 2003).

One of the direct causes of the Formosa Plastics Corporation 2004 explosion that killed five workers (CSB 2007) was that an operator used an air hose to open an interlocked valve on a drain valve on a reactor. He believed this was necessary because he believed that there was a problem with the sequence control. The real reason was that he had gone to the wrong reactor. The air hose was readily available because it was required to complete transfers in an emergency. From a design and management perspective it was easy to assume that the operation was safe because critical steps were interlocked. In practice, the risk reduction achieved was less than anticipated. Another factor in this case was that diagnosis of the causes of the initial release was affected because personnel believed it could not be the drain on the vessel because it was interlocked. This may have affected the effectiveness of their emergency response.

The increased use of interlocks

Advances in technology have allowed extensive and complex interlocks to be used. Vendors have software that allows them to develop a more 'complete' solution, which generally means more valves are interlocked. Devices such as 'key exchange' units are available that allow multiple keys to be trapped or released and allow more complex sets of conditions and task steps to be interlocked. And electronic systems are being introduced where interlocks are integrated with instruments, Programmable Logic Controllers (PLC), Distributed Controls Systems (DCS) and Safety Instruments Systems (SIS).

Risk aversion is another factor leading to the increased use of interlocks. Now that technical systems allow it, people assume that more interlocks must be safer, or at least they cannot be criticised for choosing the more complete solution. However, as illustrated above, this is not necessarily the case and design decisions are often made without fully understanding all of the potential risks.

Standards and guidance related to interlocks

There appears to be very little in industry standards or guidance that can be referred to by companies wishing to use interlocks to manage their risks.

Even for pigging operations, where interlocking has been considered as a standard requirement for many years the details are minimal. For example:

- The guideline to the Pipelines Safety Regulations 1996 (HSE 1996) states that "Interlock arrangements may be provided as safety systems, particularly where they prevent inadvertent operation. For example, valve interlocks may be used in conjunction with bleed devices on pig trap door mechanisms to prevent opening up under pressure."

- The NORSOK Standard P-100 for Process Systems (NORSOK 2001) states "Pig launcher and pig receiver shall be equipped with an interlock system to prevent opening of isolation valves around the launcher when the launcher door is open."

The problem with this lack of information is that it is difficult for people to benchmark their approach to interlocking in order to determine it is sensible. Again, this makes it difficult to decide if they have 'done enough' and often results in more interlocks being introduced.

Examples illustrating the issues with interlocks

Three examples are discussed below where interlocks are often used in the process industry. The purpose is to illustrate that there are different options when deciding how much to interlock, and that more interlocks does not necessarily mean safer when all potential risks are considered.

Spared relief valves

It is very common to protect plant against over pressure using Relief Valves (RV). If an RV's calibration expires, either because of the time since it was last calibrated or because it activates (lifts) it needs to be taken out of service. In order to avoid a full plant shutdown a spare RV is often included in the design (see diagram below). Manual valves are provided so that the duty/standby RV can be swapped.

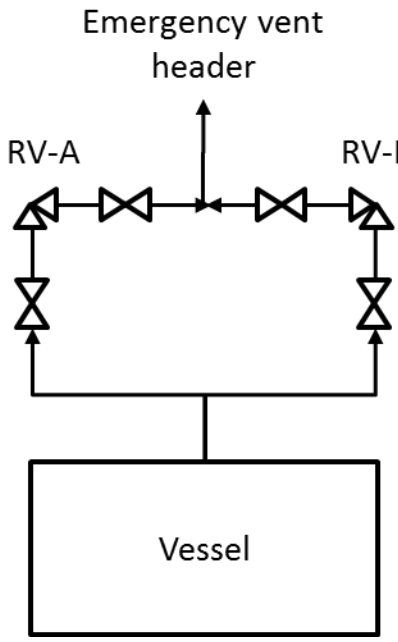

Figure 1: Spared relief valves with isolation

The problem is that the manual valves included in the design mean that an error can occur where both RV are isolated and the vessel is not protected against over pressure. To overcome this it is common to use interlocks to restrict valve operations so that at least one RV is always lined up for duty.

In this application the role of the interlock and the associated safety implications are very clear if they can ensure over pressure protection is always available. However, identifying that an interlock will be of benefit does not define what needs to be interlocked. In this case the main options are to interlock:

- Inlet valves (i.e. vessel side);
- Outlet valves (i.e. vent header side);
- Both inlet and outlet valves.

It is normal for the inlet valve of the standby RV to be closed. This prevents the internal components being exposed to contaminants from the process and avoids any potential issues with over pressurising the RV outlet if it is not fully rated to process pressure. The outlet may be left open or closed. Obviously both valves on the duty RV need to be open.

Assuming the outlet valve of the standby RV is left open it is possible to interlock the inlet valves so that at least one of them is open at all times. However, the outlet valves on both RV will need to be secured open so that they cannot be closed inadvertently. This would normally involve them being 'normally' locked open with controls in place to manage any closure. Most companies have effective means of managing the status of critical valves, which would apply in this case.

If the outlet valve of the standby RV is left closed there needs to be additional controls to make sure that it is open before changing over the duty/standby RV. This could be achieved via procedures and competence, which may be considered as relatively unreliable. This may be used as a justification to increase the number of interlocks so that the position of all inlet and outlet valves is controlled.

Interlocking all inlet and outlet valves can be effective at ensuring the vessel is always protected. But it increases complexity and may contribute to the other human factors issues discussed above.

Another issue with interlocking routine tasks is that they can restrict the performance of non-routine activities. In this example, isolating the vessel will not be possible because the interlock does not allow both RVs to be isolated at the same time. A master key (or equivalent) would be required to close all the valves so that the vessel is isolated from the emergency vent header. Once a master key exists the potential for interlocks to be defeated has to be considered.

In this scenario, the safety role of RVs probably justifies the use of interlocks. But as discussed above, even in this apparently ‘obvious’ case there are still issues to consider. Whilst interlocking the inlet valves appears to be a requirement, there appears to be no clear benefit in interlocking the outlet valves as well. The ‘Less is more’ philosophy would result in a simpler and cheaper solution, and may reduce the likelihood of over reliance and complacency.

Duplex filter

Duplex filters are similar to RVs in that one is duty and the other standby. Again valves are provided to allow changeover if the duty filter becomes blocked.

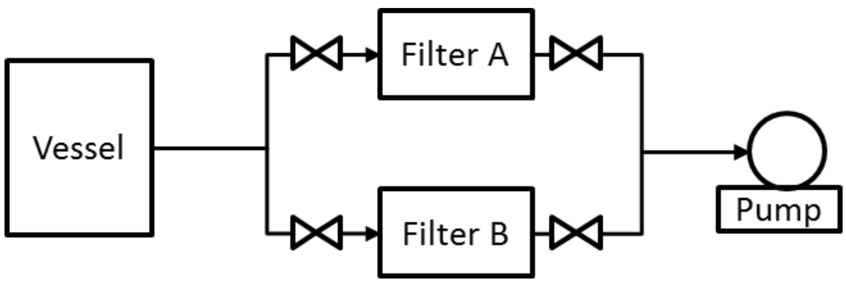

Figure 2: Duplex filters with isolation

To maintain production it is essential that at least one filter is lined up at all times. This can be achieved by interlocking the inlet and/or outlet valves. Whilst this appears to be a similar case to the RVs it is important to note that this is usually for production, not safety, so the justification is not so clear.

When a filter becomes blocked it needs to be cleaned. This involves opening the filter to remove its element, which is either replaced or cleaned. This is often a fairly frequent activity and involves breaking containment on a live system. If it is in hazardous service there will be a number of safety issues to be considered and it will normally be necessary to isolate, drain, vent and purge the filter before it can be opened. Hence a number of additional valves and connections are provided.

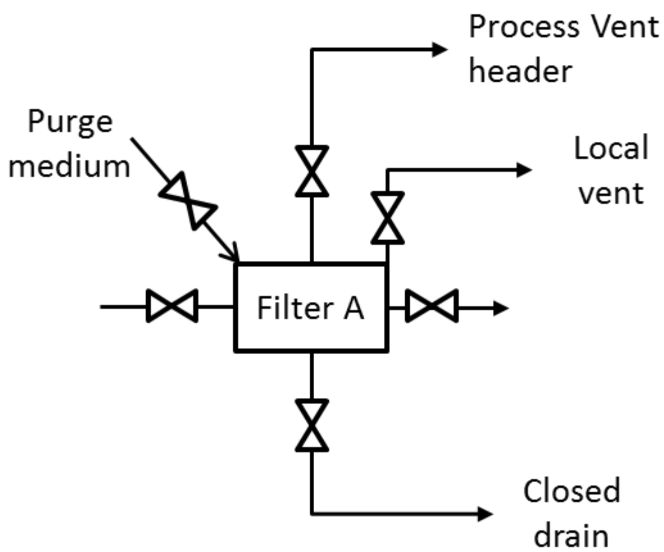

Figure 3: Filter drain, purge and vent connections

There are a number of potential errors that can occur and so it is reasonable to consider interlocks as a method of controlling the risks.

One error is that the filter may not be isolated from the process because its inlet and/or outlet valve are open. Interlocks can be used to confirm the valves are closed before the filter door can be opened.

Ensuring the filter has been drained and vented is not so easy to control via interlocks. Although the drain and vent valves have to be opened for this activity, they need to be closed before opening the filter so that it is isolated from the closed drain and process vent header systems. Hence the status of these valves is not a confirmation of the filter status. More advanced interlock systems, such as using multiple keys in some valves, can address this. But this increases complexity. The danger is that people will think less about what they are doing and why they are doing it; and start concentrating on what they need to do to get the right key to proceed.

In this case the 'Less is more' philosophy may help to focus on the most important safety concern, which is making sure there is not a release of hazardous material when the filter door is opened. It can be argued that opening the local vent immediately before opening the door will give a good indication that the filter is isolated from the process and depressurised. Hence, a simple interlock could be used that links the local vent status with the door securing mechanism. Proprietary closure mechanisms used on filter doors often include such an arrangement, and may suggest that additional interlocks is of relatively little benefit.

It is important to recognise that the filter being depressurised is not an indication that it is in the correct safe condition; and securing isolations is an important consideration. Whilst interlocks can be used to address this, they are not the only option. Most companies have effective means of controlling isolations, which could be used in this case. In fact, in a real-life example it is very likely that isolation of the filter would require double-block and bleed; and a requirement to confirm the integrity of individual valves before any break of containment. To interlock this operation is likely to be very complex, and so the human factors risks discussed above are of particular relevance.

For duplex filters the requirement to keep one online at all times is critical to production and not safety. Given that the main safety concerns are related to preparing the filter for opening, the case for interlocks of process valves is relatively weak. However, an interlock on a local vent that releases a key to open the filter door may be appropriate.

Pig launcher/receiver

Interlocks on pig launchers and receivers are generally considered as a requirement due to the hazards involved. The main concern is that a relatively large system is opened whilst the associated pipeline is live; and people are required to work in close proximity to the open launcher/receiver to load or remove pigs, clean and inspect internals, and to maintain components including the door seal. In some respects, the risks are similar to a confined space entry, with the added concern that it is performed under valve isolation (i.e. no spades, blanks or removed spools to create a positive isolation).

There is certainly potential for human error with very serious consequences, so interlocks would be a reasonable consideration. However, the diagram below illustrates that there are a lot of valves can be interlocked.

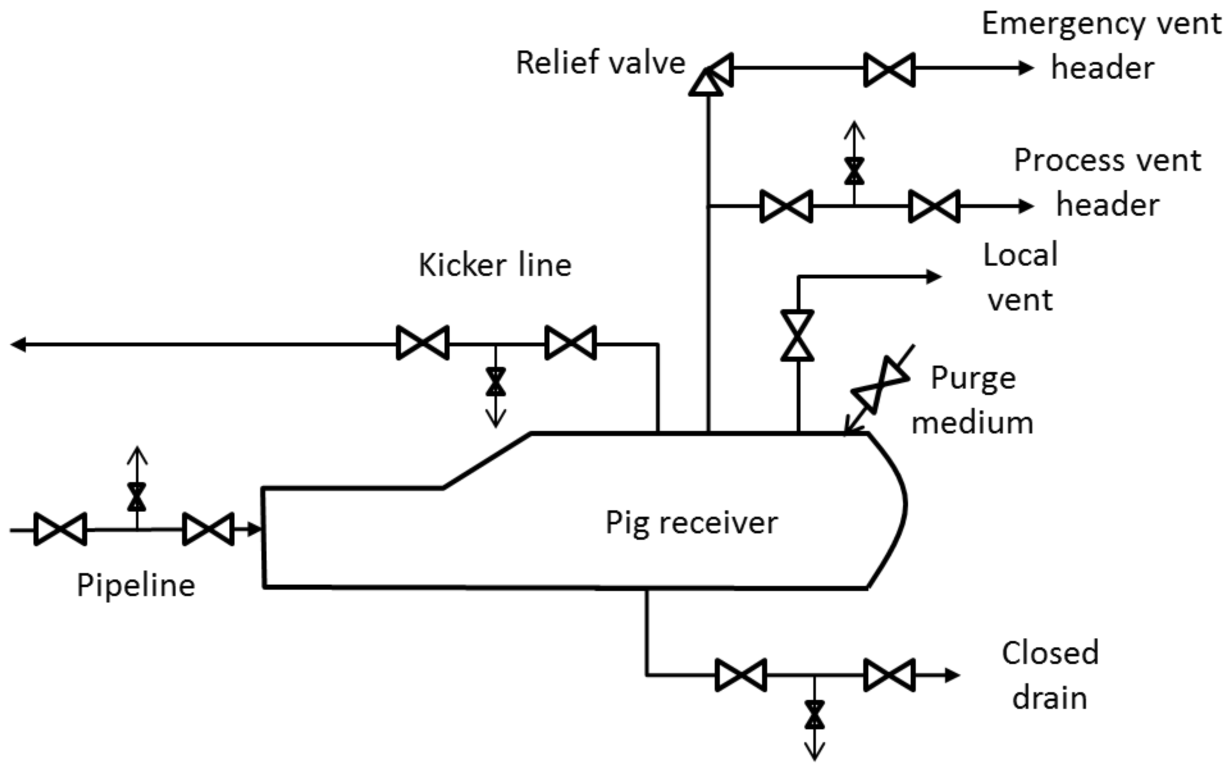

Figure 4: Example pig receiver

Whilst it is easy to decide that interlocks should be provided, this does not determine how many valves should be interlocked. There are at least three options as follows in increasing levels of complexity:

1. Interlock primary isolations – 5 valves;
2. Interlock primary and secondary isolation – 9 valves;
3. Interlock all isolation and bleed valves – 13 valves.

However, the options presented above can only confirm the status of valves and do not confirm that the launcher/receiver has been drained, vented or purged. Also, they will not confirm the requirements for safe isolation of plant as defined in HSG 253 (HSE 2006). In particular, interlocks do not prove the integrity of the isolation valves, which requires a high degree of operator understanding and vigilance (Brazier 2013).

Interlock vendors will supply systems that go some way to address these issues. However, the result is complex with systems having more than 20 keys and procedures listing more than 50 interlocked steps (it was one of these systems that was causing problems for the process operator quoted in the introduction to this paper).

As with the previous examples, it must be recognised that at most companies additional controls can and will be put in place to ensure tasks are performed correctly. In this case a full procedure will be followed, along with a system for managing isolations and breaking containment. Hence, there is no reason to attempt to apply interlocks to address all potential issues.

The ‘less is more’ philosophy encourages us to consider the critical requirement, which in this case is to confirm the launcher/receiver is not pressurised when it is being opened. Modern technology provides us with an opportunity to include instruments in our interlocks. In this case an interlock that releases a key when a number of pressure instruments located on the launcher/receiver are at atmospheric may be sufficient to allow the door to be opened. This is probably an updated version of the interlock that would have been used in the past, which would have released the key when a local vent is opened.

Analytical approach to demonstrating the issues

There is clearly, in my opinion, a problem with using too many interlocks. But, there is nothing objective that people can use to inform their decision making process. One way of overcoming this would be to have a robust analysis of the issues.

Simplified system

Real-life systems have multiple components and so any analysis would be complicated. The very simple system shown below has been used to illustrate the issues raised in this paper.

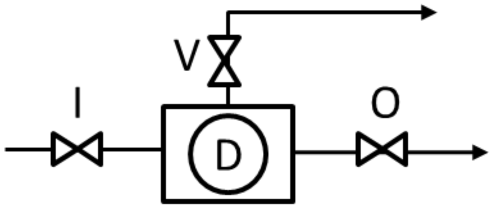

Figure 5: Simple system for analysis

The scenario here is that the door (D) must be opened. To do this safely the inlet valve (I) and outlet valve (O) must be closed; and the vent valve (V) must be opened to relieve trapped pressure. Also, the vent will need to be monitored before opening the door to confirm the integrity of the isolation.

Potential errors

The main concern is a release of process material when the door is opened. The following task and error analysis illustrates how this can occur:

1. Close inlet valve I – Action omitted - Vessel is not isolated resulting in release from process when door is opened;
2. Close inlet valve O – Action omitted - Vessel is not isolated resulting in release from process when door is opened;
3. Open vent V – Action omitted - Vessel remains pressurised resulting n release of trapped material when door is opened;
4. Monitor vent and confirm integrity of isolation – Monitoring omitted – If either isolation valve passes there will be a release from the process whilst the door is open.
5. Open the door.

Evaluating the likelihood or error

On first inspection it appears that there are four potential errors that can occur before opening the door. However, Steps 3 and 4 will be effective at detecting errors at Steps 1 and 2. In other words:

- If the vent is monitored (Step 4), as well as confirming isolation integrity it will confirm that the vent has been opened (Step 3) and that the isolation valves have been closed (Steps 1 and 2);

- If the vent is opened (Step 3) it will confirm that the isolation valves have been closed (Steps 1 and 2), but it will still be possible to omit the monitoring (Step 4).

On this basis the most interesting factors are the ones that affect the likelihood that the vent is left closed and the likelihood that the vent is not monitored to confirm isolation integrity.

Error likelihood without interlocks

If we do not have any interlocks it will be possible to open the door with the valves in any condition. Safety will rely on the technician following the correct procedure, which means there is the potential for error.

It seems reasonable to assume that because the technician has been ‘engaged’ with the task that they will be thinking quite clearly about what they are doing. Also, they will not have any device giving them any reassurance about safety. They will be quite cautious about opening the door.

In this scenario the opening of the vent will be viewed as an important by the technician and so the likelihood of error will be relatively low. However, having opened the vent the technician may assume that monitoring to prove valve integrity is not so important, and so missing that step is probably more likely.

Interlocking the isolation valves

If the isolation valves are interlocked the procedure for opening the door becomes:

1. Obtain key I;
2. Insert key I into valve I,
3. Open valve I and retrieve key O;
4. Inset key O into valve O;
5. Open valve O and retrieve key D;
6. Open the vent valve V;
7. Monitor the vent;
8. Insert key D into the door lock and open the door.

The concern here is that at Step 5 the technician has the key they need to open the door. This means the likelihood of them forgetting to the open the vent will have increased. If they do open the vent the likelihood of them monitoring to test integrity is probably similar to the first scenario without interlocks.

Interlocking the isolation valves and vent valve

If the isolation valves and vent valve are interlocked the procedure for opening the door becomes:

1. Obtain key I;
2. Insert key I into valve I,
3. Open valve I and retrieve key O;
4. Inset key O into valve O;
5. Open valve O and retrieve key V;
6. Insert key V into vent valve V;
7. Open the vent valve V and obtain key D;
8. Monitor the vent;
9. Insert key D into the door lock and open the door.

With this option the potential action errors are eliminated. However, the potential to omit monitoring the vent remains. Given that by this stage the technician will not have had to give any great thought to the task and they will already have the key to open the door it seems reasonable that the likelihood that this step is missed is quite high.

Interlocking the vent valve only

If the vent valve is interlocked but the isolation valves are not the procedure for opening the door becomes:

1. Open valve I;
2. Open valve O;
3. Obtain key V;
4. Insert key V into vent valve V;

5. Open vent valve V and obtained key D;
6. Monitor the vent;
7. Insert key D into the door lock and open the door.

In this case it is possible to omit closing either isolation valve. However, this will be discovered when the vent valve is opened. As the door cannot be opened until the vent valve is open this effectively eliminates all error apart from monitoring the vent. Given that the technician will have had to give some thought to what they were doing as the isolation valves were interlocked it seems reasonable to assume that the likelihood of missing the monitoring step is similar to the non-interlocked example.

Quantifying error likelihood

Extreme caution is required when any attempt is made to quantify human error likelihoods. There are many potential scenarios that need to be considered, and applicable data is very difficult to obtain. However, the issues considered when attempting to quantify can be interesting for discussion purposes.

In this case the following error likelihood has been proposed. They are not based on any scientific evaluation, but used to illustrate the scenarios:

- Technician fully engaged in task and fully understands the need for the step - 0.001
- Technician engaged in task but may not appreciate step significance - 0.01
- Technician not engaged in task - 0.1

Two error scenarios are considered (vent not opened and vent not monitored). Both will result in a hazardous condition and so in a logic tree would be connected by an "OR" gate meaning the individual likelihoods should be summed. The table below shows the calculated error likelihoods.

Table 1: Error likelihood calculations

	Interlocked steps			
Error	**None**	**I+O**	**I+O+V**	**V**
Vent not opened	0.001	0.01	0	0
Vent not monitored	0.01	0.01	0.1	0.01
Error likelihood for task	**0.011**	**0.02**	**0.1**	**0.01**

Based on these very rough calculations, interlocking the vent valve results in marginally lower likelihood of error than having no interlocks. On the other end of the scale, interlocking all three valves results in the highest likelihood. The reason for this is that the technician will be less engaged in the task and so less likely to recognise the risks associated with the task leading to them overlooking the requirement to monitor the vent.

This is not the full picture. Failure to monitor the vent will not immediately result in a hazard because one of the isolation valves would also have to pass. Therefore, the likelihood of error is not a direct indication of risk. However, another factor to consider is the potential for an interlock to fail.

Interlock failure

The calculations above assume that interlocks are 100% reliable. This is not the case as mechanical devices can malfunction, interlocks to be overridden (e.g. use of 'master key') and there can be design and maintenance errors.

If technician obtains Key D it is very likely that they will assume that all interlocked steps have been completed. If Key D has become available due to a fault with an interlock and the associated valve is in the wrong position, the likelihood of this being detected will be very low. It would seem reasonable that error likelihoods would be increased by at least one order of magnitude.

The table below illustrates the calculations if a likelihood of error of 0.1 is included for interlock failure.

Table 2: Error likelihood calculations with interlock failure

	Interlocked steps			
Error	**None**	**I+O**	**I+O+V**	**V**
Vent not opened	0.001	0.01	0.1	0.1
Vent not monitored	0.01	0.01	0.1	0.01
Error likelihood for task	**0.011**	**0.02**	**0.2**	**0.11**

Again, this is not the full picture. It only considers the technician's error once the interlock has failed and they are not looking for other indications that venting has occurred (e.g. hearing the release of pressure). However, if the situation is more complex, either due to the number of interlocks or if there is a handover of personnel during the task, it is easy to see that having the key will be the overriding signal to the technician that it is safe to continue.

Using these figures

The numbers quoted above must be used with great scepticism. They have no scientific basis and the analysis is by no means rigorous. However, even with this very simple example the analysis has shown that if interlocking does have a negative impact on the way the technician engages in the task it is likely to increase the likelihood of errors. Also, if there is any possibility for the interlock to fail (which there always will be) the impact can be very significant.

Conclusion

I have attempted to present a 'less is more' philosophy for interlocks. Whilst this is only my personal opinion, I believe that I have illustrated the issues associated with increasing the number of interlocks on a system and the inevitable increase in complexity. Unfortunately there are no standards or guidelines that specify what needs to be interlocked or how many interlocks should be provided. Vendors are able and willing to sell very complex systems, and risk aversion in industry means that people feel more comfortable specifying multiple interlocks in design because they may be criticised if they do not adopt a more complete solution.

The human factor can never be eliminated from a system. Devices that reduce the likelihood of operational errors generally increase vulnerability to design and maintenance errors; and can result in over-reliance leading to complacency. Complex interlocks lead to people being more concerned about doing what they have to do release the next key; and less about why they are doing things and the associated risks.

This paper has focussed on trapped key interlocks that are used to control valve operations. These are commonly used in the process industry to ensure valves are operated in the correct sequence and are in the correct status at key stages in a task. Examples from industry have been used to illustrate the issues raised in this paper. For example:

- Spared RV - ensuring an RV is lined-up at all times is critical for safety, and interlocks on isolation valves can be justified. However, this affects the ability to isolate a vessel for maintenance;
- Duplex filters – ensuring a filter is lined-up at all times is a critical for production but not safety, and so there is less justification for interlocks on the isolation valves. However, the filter will need to be opened for cleaning, and this is where interlocks may have a safety role;
- Pig launcher/receiver – this is one area where interlocks are expected, to confirm the system is safe for opening. But these are complex items and the number of interlocks can be great. Attempts to interlock every step cause very real issues.

Whilst the numbers presented in the quantified analysis of a simple system must be treated with scepticism, the approach does give some insight into the issues that need to be considered. In this case it was possible to illustrate the importance of the checking steps (opening the vent and monitoring to confirm isolation valve integrity). If interlocks affect the way a person engages with a task, the likelihood of them overlooking these checks will increase. This can easily cancel out any benefit gained from interlocking the active steps (e.g. closing isolation valves). This becomes even more significant if the potential for interlocks to fail is factored in.

The alternative to interlocks is usually a reliance on procedures. Although low on the hierarchy of risk controls, procedures can be effective if implemented effectively. On the hand interlocks, which as engineering controls appear higher on the hierarchy, they have a wide impact on human factors and can always be defeated. I believe that a 'less is more' approach will be more effective at managing the whole risk taking into account the normal and non-routine tasks (e.g. vessel isolation), dealing with unplanned situations (e.g. passing valves) and the potential for over-reliance and complacency.

References

Brazier, 2013. Process Isolation – It's more complicated than you think. Loss Prevention Bulletin 231. IChemE.

CSB 2007. Investigation report. Vinyl Chloride Monomre Explosion. Report No. 2004-10-I-IL. U.S. Chemical Safety and Hazard Investigation Board.

Edmonds, J, 2016. How to reduce human failure. The Chemical Engineer. July/August 2016.

Ellis, G, 2003. The ongoing challenge of demonstrating ALARP in COMAH safety reports. IChemE Symposium Series No. 149

HSE, 1996. A guide to the Pipelines Safety Regulations 1996. Health and Safety Executive.

HSE, 2006. The safe isolation of plant and equipment. HSG 253.

HSE Website, access 1 December 2016. Control Systems - http://www.hse.gov.uk/comah/sragtech/techmeascontsyst.htm. Health and Safety Executive.

Marsden S, Bendig M, Berman J 2003. Human factors and COMAH – the challenge of existing plant. IChemE Symposium Series No. 149

NORSOK 2001. Process Systems. Norwegian Technology Centre. Standard P-100