How to Focus on the Right Things in Complex Process Safety Systems

Ian Travers, HSE (now Lockheed Martin Information Systems & Global Solutions)
Stuart Hawksworth & Matt Clay, Health and Safety Laboratory

To manage different aspects of safety effectively, different approaches are required. For major hazard industries the consequences of not managing effectively could be an incident resulting in multiple injuries, fatalities, impact on critical infrastructure or a catastrophic environmental incident. A distinction is therefore made for the case of major hazard industries, giving particular emphasis to avoiding catastrophic events. This is also clear in safety legislation, where strict high hazard regulation applies, such as safety case regimes and/or licensing.

To meet these requirements, organisations implement a process safety management system, recognising the need for continuous checks to ensure systems function, identifying and fixing problems before they lead to incidents - in many countries this again is a regulatory requirement. Such checks are essential, as experience suggests that process safety control systems can start to deteriorate soon after they have been implemented. Major hazard businesses rely on audits to check all, or part of their process safety management systems, and implement Key Performance Indicators (KPIs) to monitor performance, working in tandem with comprehensive systems of incident reporting and investigation. While such approaches help, checking mechanisms such as audits tend not to be very well focussed and often are aimed at checking the control system itself, rather than its function and outcomes. Without careful thought, KPIs can be quite indiscriminate and vague in terms of the important performance information they provide. Incident investigation systems look at failures that have occurred and offer a valuable insight into where systematic problems may exist. However, there are often problems with robust reporting of process safety incidents because there is no serious event or injury; inadequate attention can be given to the insights from an investigation.

The Health and Safety Executive, the GB regulator, has developed a proactive inspection programme for major hazard installations. A key part of this approach is a risk targeting methodology that explores vulnerability within a process safety management system and tests that the most critical control measures to ensure it functions as intended. This methodology can also be valuable to businesses who want to ensure proper oversight of their process safety management system without having to always undertake wall-to-wall audits and inspections. A key strength is that it helps ensure that KPI programmes measure and monitor performance where it really matters. Expertise in applying this targeted approach is now available to all major hazard enterprises.

This paper describes the HSE risk targeting methodology, and an ammonia case study that has been used to train both HSE inspectors and industry on its application.

Introduction

For major hazard industries, where the potential consequences of an accident are multiple injuries or fatalities or a catastrophic environmental incident, we are accustomed to giving a particular emphasis to avoiding catastrophic events compared to say preventing slips, trips and falls. This distinction is also repeated in safety legislation where regulation includes safety case or licensing regimes for high-hazard activities. We categorise the way such high-hazard risks are addressed as 'process safety management'. This is to distinguish the specific safety approach aimed at ensuring hazardous substances or high potential energy are safely contained within the associated plant or processes or kept safe by segregation, and that the potential effects of releases are mitigated. The concepts of process safety management emerged following the disastrous chemical incident at Flixborough in 1974 and are now an embedded global framework. Catastrophic risks are systematically assessed and the appropriate control measures required to maintain containment and mitigate consequences are determined.

Although process safety management systems originally emerged from the chemical manufacturing sector the approach has subsequently been successfully applied to other industries such as power generation and transmission, mining, oil and gas exploration and even to dam safety. Derived from Deming's Plan / Do / Check / Act business management cycle (HSE, 2013) a basic process safety management system includes hazard identification, risk assessment leading to conclusions on the relevant control measures and then arrangements to check the system’s performance. It is normally expected that for any hazardous threat (e.g. of loss of containment) then it is necessary to have multiple layers of protection in the control measures. This is to provide safety in-depth and an element of redundancy within these protective systems. Control and mitigation measures are typically called barriers as per James Reason’s risk model (Reason, 1997). A process safety management system also requires a feedback loop (such as auditing, incident investigation and monitoring via key performance indicators, KPIs) to ensure the control systems continue to operate and deliver their intended outcomes. The whole system is driven by effective leadership and underpinned by an effective safety culture.

Process Safety Assurance

Most organisations who implement a process safety management system recognise the need for continuous checks to ensure the system continues to function and to identify and fix problems before they give rise to a catastrophic incident. In many countries this is a regulatory requirement.

Experience has shown that most process safety management systems start to deteriorate immediately, or very soon after they have been implemented, unless real efforts are made to maintain their effectiveness. For example, analysis carried out for HSE in 2007 showed that 81% of loss of containment incidents could be traced back to failings in maintaining the requirements of the process safety management system (Collins, 2003). Accordingly, most major hazard businesses use audits to check either the entirety or part of their process safety management systems, set a whole suite of KPIs to act as a
watchdog on performance and have comprehensive systems of incident reporting and investigation to identify where systems have failed to function.

The problem with these mechanisms of checking is that audits can tend not to be very well focussed and often are aimed at checking the format of a control system rather than its function and outcome. KPIs can frequently be quite indiscriminate and vague in providing valuable information on performance. Incident investigation systems look at failures that have occurred and offer a valuable insight into where systematic problems may exist. However, there are problems with robust reporting of process safety incidents because often there is no serious event or injury and so less attention is given to the insight provided by an effective investigation of a process safety incident even where the definition of an incident has been properly established.

Overlaying these three types of process safety checks is the complexity of the industrial activity typically covered by a process safety management system and the problem of how to determine where best to focus when checking that a complex and elaborate system is functioning and delivering the intended outcomes e.g. minimising the chance of a major accident.

The Health and Safety Executive recognises these issues: to plan its inspections it has developed a proactive inspection program for major hazard installations. A key part of the approach is a risk targeting methodology that explores vulnerability within a process safety management system and tests the most critical control measures to ensure it functions as intended. The methodology used by HSE can also be valuable to major hazard businesses who want to ensure proper oversight of their process safety management system without having to undertake wall-to-wall audits and safety inspections. It is especially helpful in ensuring that KPI programs measure and monitor performance where it really matters. Expertise in applying this targeted approach is now available to all major hazard enterprises.

**Targeted Risk Assurance**

HSE is currently employing an approach developed by Ian Travers during his time at HSE, known as the ‘Hazardous Installations, HID, Regulatory Model: Safety Management in Major Hazard Industries’ (HSE, 2013), which was published in 2013. It sets out the way HSE inspectors sample major hazard control measures and also gives HSE’s overview of a Process Safety Management System. This is shown in Figure 1 with overlays of the concept of Plan, Do, Check and Act onto this system description.
Figure 1: HSE’s process safety management system (3)
Targeting Vulnerability

Targeting involves an analysis of the site’s risk profile, selecting for close examination those control measures, barriers, which are safety critical in the prevention of a major accident and which are also most vulnerable to deterioration and failure.

Applying a series of guide questions leads to identification of the key aspects of process safety management to validate. The most important questions are:

- What can go wrong?
- Where or when is it likely to happen?
- What would be the consequences?
- What preventative systems are in place to prevent a failure?
- What information is available and what checks are made to ensure the preventative systems are operating as intended?

As shown in Figure 2 the starting point is to identify the major hazard scenarios for the site and then, based on risk assessment, to decide which represents either the largest event with the greatest potential consequences or to determine which major hazard scenario is the most credible event so that large but extremely low probability scenarios are excluded. This is aimed at answering the question ‘what can go wrong?’ and lead to a major accident.

![Figure 2: Targeting Assurance](image)

The aim is to check the operational integrity rather than the initial design or construction aspects of a process safety management system. The focus is on the dynamic challenges to the day to day integrity of the plant or process.

Sampling a specific plant or process with a credible major hazard scenario to check the functioning of the overall process safety management works because it is usual for an organisation to apply the same generic control measures regardless of the location of the plant or process. For instance, there will be one inspection and maintenance system, one management of change system, a single competence management system throughout the installation or even across multiple installations.

Evidence of Safety and Integrity Outcomes

Once a target plant or process is selected the next stages involve drilling down into the detail of the specific control measures relevant to preventing a major accident hazard associated with that process to get evidence that the most important control measures are working as intended and delivering the desired safety and operational integrity outcomes. This involves five stages of analysis.

1. Describe the installation, the main components of the process and their function and identify the main hazards present. Draw a simplified block diagram of the installation and process capturing the main process conditions such as temperature and pressure.
2. Identify the challenges to the integrity of the installation by listing the main ways that containment of the hazardous materials, substances or stored energy may be accidentally released. Record the type of failure and the probable location on to the process diagram.

3. Identify the important risk control measures (barriers) that should be in place to prevent the challenges to the loss of containment identified in Step 1. Record these on the process diagram in the location where the loss could occur. This helps later on to check information, intelligence and records in a focussed way to demonstrate the correct operation of these risk control systems.

4. Of the risk control measures identified in Step 3 assess which are the most important to audit by identifying whether:
   - the system is safety critical – that is, if it failed and there was an associated loss of containment would this potentially lead to a major accident or a serious incident? Note: Major accidents such as Buncefield showed that instruments and sensors which measure process conditions such as tank level gauges are just as safety critical as protective devices such as pressure relief valves and emergency shut down systems.
   - the control measure is towards or is ‘the last in line’ using the bow-tie analogy;
   - the system provides any ‘early warning, of failure e.g. leak before fail, excess vibration to flag up a potential component failure. Systems that fail catastrophically without early warning are more vulnerable than systems or controls that gradually and detectably deteriorate before failure,
   - there is opportunity to recover the loss of containment, e.g. limit the extent of release, rapidly shut down the system or to capture or contain the release through bunding or other secondary containment measures, and
   - the correct functioning of the control measure relies partly or wholly on human intervention. This is especially important where human intervention includes both detection and then taking effecting corrective action.

Figure 3: Identification of the most vulnerable and safety critical barriers

5. For this sub-set of vulnerable barriers HSE aims to check on site for evidence that the controls continue to operate. HSE also looks to see that appropriate leading and lagging KPI’s have been set for these most vulnerable barriers. Figure 3 shows how to plot vulnerability and safety criticality onto a simple matrix. The control barriers in the top right hand box should be the focus of a targeted assurance check.

Example – Ammonia Plant

An example is now presented that has been used by HSE and HSL to successfully train inspectors and industry on the application of the HID Regulatory Model. In this hypothetical example, a large scale loss of ammonia represents the worst case major hazard scenario for the whole site, as 20,000te of liquid anhydrous ammonia is present Therefore the ammonia production and storage process was selected as the most important process to examine and test the operation of the process safety management system. This example uses a hypothetical but realistic process plant layout (see Figure 4) and any resemblance to an existing installation is coincidental.
Stage 1: Process Description

Imported hydrogen is compressed and then washed with liquid nitrogen at -190 deg C and 28 barg to remove carbon monoxide which is a contaminant. The hydrogen is then mixed with more nitrogen and compressed further before being transferred to the reaction vessel. The reaction is carried out at 500°C and 140 barg over an iron catalyst. The anhydrous ammonia product is cooled to -33°C and sent along a 2 km pipeline to the 15000 tonnes storage tank. The pipeline from the ammonia plant to the ammonia storage tank has a safety shutdown system associated with it, which isolates the tank and jetty line in the event of a release. It is despatched by ship from the jetty. The ammonia storage tank stores 20,000 tonnes of anhydrous liquid ammonia at -33°C in a double-skinned and insulated tank. As vapours boil off they are compressed, refrigerated and returned to the tank as liquid, so maintaining a nominal pressure of 60 mbarg. Only cold ammonia should be transferred to the storage tank. The tank has pressure relief valves and vacuum valves to prevent over pressure and vacuum formation. The tank is also fitted with high pressure alarms to warn of rising pressure in the tank, so it can be vented to the scrubber if necessary.

Specialised cryogenic gaskets and bolts are used on the cryogenic sections of the plant such as the coldbox. Spiral wound graphite gaskets are used across the plant on medium pressure joints and metal ring joints are used on high pressure systems.

Stage 2: Challenges to Integrity

Stage 2 is about answering the question ‘how and where can a loss of containment occur?’ The main challenges to the integrity, likely to lead to a loss of containment for this plant are corrosion including stress corrosion, mechanical failure (including wear and tear), cold embrittlement, over filling, over pressure, physical impact and human error. Figure 5 illustrates how mapping these onto the process description in Figure 4 (zooming in on key areas) identifies the location of such challenges and also reveals clusters or nodes where such challenges will impact to degrade the integrity of the plant.
Stage 3. Identifying the control measures – barriers to prevent a loss of containment

Each type of challenge must have a least one control measure to prevent a loss of containment but preferably several for each failure mode. This stage is important because in practice when applying this analysis it is often discovered that there is a failure mechanism that has not been recognised or addressed by a suitable control measure. The main control measures are set out in Table 1 and shown on the process diagram in Figure 6.

<table>
<thead>
<tr>
<th>Challenge to Integrity</th>
<th>Control Measures / barriers</th>
</tr>
</thead>
</table>
| Corrosion              | • Design and material specification.  
                          • Corrosion protection / coating.  
                          • Inspection and maintenance of the equipment – corrosion detection or deterioration of the corrosion protection. |
| Stress Corrosion       | • Design and material specification.  
                          • Maintaining the temperature and pressure within safe design limits and avoiding excessive temperature / pressure cycling.  
                          • Competent Process Control operators.  
                          • Suitable operating procedures.  
                          • Inspection and maintenance of the temperature and pressure sensors and control system. |
| Mechanical Failure     | • Design and material specification.  
                          • Adequate spares procurement to specification.  
                          • Condition monitoring.  
                          • Risk-based inspection and maintenance. |
| Overfilling            | • Maintaining liquid levels within safe limits  
                          • Setting and maintaining suitable high level alarm limits.  
                          • Competent Process Control operators.  
                          • Suitable operating procedures.  
                          • Inspection and maintenance of level gauges, sensors, control loops and safety shut down systems. |
| Overpressure           | • Maintaining pressure within safe limits  
                          • Setting and maintaining suitable high level alarm limits.  
                          • Competent Process Control operators.  
                          • Suitable operating procedures. |
Table 1 Challenges to the integrity of the plant mapped against the expected control measures / barriers.

This mapping of control measures onto the plant diagram starts to pinpoint what evidence should be sought to validate that the process safety management system is delivering the right outcomes for this particular plant. For instance, instead of just examining the inspection and maintenance system for the whole installation it becomes clear that inspection and maintenance of say of the corrosion protection on the 1.9 km liquid ammonia filled pipeline between the chiller and the bulk storage tank will be very important. A focus of attention should therefore be seeking evidence that the inspection method is correctly followed according to the associated documented procedure, and that records show that the inspections of this pipeline were done to schedule. Even greater assurance could be obtained if completion of this inspection item was monitored by the site KPIs.

Stage 4. Identifying vulnerability

Applying the tests of safety criticality and vulnerability reduces the target number of control measures to examine and further assists in pinpointing the part of the process against which to check the control measures are fully functioning. The aim is to eliminate the control measures that do not deteriorate quickly or issues like design and construction of plant and equipment that are only done once. Focusing on dynamic elements of risk control provides the greatest degree of assurance. Next, match the vulnerable control measures to the location so that evidence of safe operation and reliability can be gathered directly.

Figure 7 shows the conclusion of this assessment, resulting in a smaller set of control measures to examine, and Table 2 illustrates how the vulnerability analysis is applied to the control measures determined at stage 4. Most importantly, the clustering indicates that, in this example, close attention should be given to the integrity of the storage tank because of the high number of challenges to the integrity that apply, coupled with the vulnerability of the control measures associated with its safe operation. It should be remembered that because a control system is judged to be vulnerable this does not mean that the plant or process is unsafe. Rather it means that special attention and more frequent assurance is needed to show that those systems continue to operate as intended.

One of the most vulnerable control measures that results from this analysis is the procurement and fitting of the right gasket to the carbon monoxide isolation valve. The right, cryogenic gasket needs to be selected and as this is a single isolation valve then it has to function without failure. Selection and fitting is the last in line barrier to prevent a leak and relies upon human intervention and competence. The gasket will give no hint that it is the wrong type before it is fitted. It will not fail and leak immediately and so shows no sign or warning of failure until it is too late.

It is equally important that the operation of these most vulnerable systems feature prominently in the company’s KPI programme. These KPIs should be the sentinel measures for common control systems such as pressure control, inspection and maintenance and staff competence which guard against the broad range of challenges to the integrity of plant and equipment.

This sample and carefully targeted assurance check provides a valuable insight into the functioning of the whole safety management system because the findings can be read across the whole installation or organisation. Faults or problems identified in this part of the system can be used to improve the whole process safety management system. Over time different samples build a picture of the adequacy or otherwise of the system because the same measures are normally deployed across the whole organisation. Figure 8 illustrates how such a picture can be built.
Figure 6. Control measures mapped against the challenges to the integrity of the plant.
Control Measures - Process
- Temperature Control
- Pressure Control
- Level Control
- Gas Detection (CO / NH₃)
- Vibration Monitoring

Control Measures - Generic
- Inspection & Maintenance
- Competence
- Spares Procurement
- Emergency Plan

Figure 7. Vulnerable and safety critical control measures

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Control Measures / barriers</th>
<th>SC</th>
<th>V</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corrosion</td>
<td>Design and material specification</td>
<td>H</td>
<td>L</td>
<td>A one-off design decision so no dynamic change during plant operation.</td>
</tr>
<tr>
<td>Corrosion protection / coating.</td>
<td></td>
<td>H</td>
<td>M</td>
<td>Corrosion occurs relatively slowly.</td>
</tr>
<tr>
<td>Inspections and maintenance of the equipment – corrosion detection or deterioration of the corrosion protection.</td>
<td>H</td>
<td>H</td>
<td>The 1.9 km liquid full pipeline presents the highest risk. A crack or hole in the pipeline or a leaking joint would be difficult to detect and then contain. Inspection relies on human intervention.</td>
<td></td>
</tr>
<tr>
<td>Stress Corrosion</td>
<td>Design and material specification</td>
<td>H</td>
<td>L</td>
<td>A one-off design decision so no dynamic change during plant operation.</td>
</tr>
<tr>
<td>Maintaining the temperature and pressure within safe design limits and avoiding excessive temperature / pressure cycling.</td>
<td>H</td>
<td>H</td>
<td>This is a very critical control measure as cycling represents the largest threat. This barrier relies on competent operators (below) who follow the designated control procedure. There are no automatic safety cut-offs that detect and prevent temperature / pressure cycling.</td>
<td></td>
</tr>
<tr>
<td>Competent Process Control operators.</td>
<td></td>
<td>H</td>
<td>H</td>
<td>See above - operators are the last in line for this threat.</td>
</tr>
<tr>
<td>Suitable operating procedures.</td>
<td></td>
<td>H</td>
<td>L</td>
<td>Having a written procedure is safety critical but procedures do not tend to change or deteriorate. What matters most is that process control operators follow the procedure - see above.</td>
</tr>
<tr>
<td>Inspection and maintenance of the temperature and pressure sensors and control system.</td>
<td>H</td>
<td>H</td>
<td>The entire pressure / temperature control system relies on accurate temperature / pressure sensors and control loops. This system is not SIL rated so completion of the inspection and calibration of these sensors is vital.</td>
<td></td>
</tr>
</tbody>
</table>

Table 2. Abstract of the vulnerability analysis for the ammonia plant.
## Assurance Findings Matrix: Ammonia Plant Inspection

<table>
<thead>
<tr>
<th>Control Measure</th>
<th>Plan</th>
<th>Do</th>
<th>Check</th>
<th>Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competence: Selection &amp; fitting of the correct gasket to the CO terminal valve</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Temperature Control: Ammonia tank maintained within specified range</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Pressure Control: Reactor pressure maintained within specified range</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Level Control: Liquid level in Ammonia Tank maintained within specified range</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Inspection &amp; Maintenance: Temperature Sensors and Alarms to Ammonia Tank inspected to schedule and properly maintained</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Corrosion Management: Ammonia Pipeline to Bulk Tank and Jetty inspected to schedule and properly maintained</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Corrosion Management: Inner insulated cavity to Ammonia Bulk Tank Inspected to Schedule</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Gas Detection: sensors and alarms to CO line and Ammonia Bulk Tank inspected to schedule and properly maintained</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Inspection &amp; Maintenance: Level sensors and control system to Ammonia Bulk Tank inspected to schedule and properly maintained</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Inspection &amp; Maintenance: Temperature sensors and control system to Ammonia Bulk Tank inspected to schedule and properly maintained</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Inspection &amp; Maintenance: Pressure sensors and control system to Reactor Vessel inspected to schedule and properly maintained</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

Figure 8. Building an assurance picture of the process safety management system
Stage 5: Develop KPIs

For the most vulnerable risk control measures (barriers) set focussed key performance indicators, KPIs, to provide regular information that the risk control systems continue to operate effectively and that they deliver their intended protective outcome. Undertaking routine checks or audits of these critical systems ensures that they are effective, and that those involved in associated critical tasks understand the importance of these systems and the dangers against which they provide protection. From the abstract of the criticality and vulnerability analysis in Table 2 above, those control measures categorised HH for criticality and vulnerability would be selected for the site KPIs.

Conclusion

The system developed by HSE to target its resources and inspections of high hazard installations can also provide a powerful tool for companies to use to bring a targeted focus to process safety management assurance programmes. It helps delineate and differentiate those control systems which matter most when it comes to preventing a major accident and which should be given special attention. The method also provides a logical way to determine key performance measures rather than trying to measure every aspect of safety performance.

Disclaimer

This publication and the work it describes were funded by the Health and Safety Executive (HSE). Its contents, including any opinions and/or conclusions expressed, are those of the authors alone and do not necessarily reflect HSE policy.

References


