Ensuring Asset Integrity - A Risk-based Approach

By Sandy Dunn,
Director, Assetivity Pty Ltd

Summary

There are many improvement methodologies and techniques available to improve plant reliability and availability, including such techniques as Reliability Centred Maintenance, PM Optimisation, Weibull analysis and others. However all of these techniques have significant limitations when it comes to dealing with high consequence, low probability events – those events that have potentially catastrophic impacts on plant integrity.

This paper discusses these limitations, and outlines an alternative approach which Assetivity has used to effectively identify, and manage, asset integrity risks.

Keywords

Asset Integrity, Risk Management, Reliability Centred Maintenance, PM Optimisation, AS4360, Methodology, Case Study, Behavioural Factors.

Introduction

The primary objective of an Asset Integrity Assurance process could be stated as:

> *To ensure the ongoing commercial viability of operations by ensuring that the risks associated with equipment failure are within tolerable levels.*

These risks could be related to:

- Production – equipment failure leads to the asset not being capable of producing saleable product
- Environment – equipment failure leads to a breach of an environmental standard, regulation or license condition
- Safety – equipment failure leads to injury or death of employees or other people

AS/NZS 4360:1999 – the Australian standard for Risk Management (which is currently held to be the leading standard in the world in this area) introduces risk as being the product of Consequences x Likelihood. It is therefore possible that an event which has minor consequences, but which happens frequently could be assessed as having the same overall level of risk as another event which happens less frequently, but which has more severe consequences.

One of the key outcomes of the Royal Commission into the Esso Longford explosion was the realisation that low probability – high consequence events need to be managed in a different manner to high probability - low consequence events – **even though both events may have the same overall level of risk**. Esso was deemed to have a highly effective safety management system in place which successfully dealt with the high probability, low consequences safety events, but which was simply incapable of dealing with a low probability, high consequence event such as a major gas leak. One of the results of this finding has been the introduction of Hazardous

Facilities legislation in Victoria, as well as Industrial Manslaughter legislation. Put simply, as humans, we tend to ignore low probability events – no matter how serious the potential consequences. For example, the probability of any one Australian being killed on the roads this year is (on average) about 1 in 8,000 – a risk that most of us do not even think about when we hop in our cars to drive to work every morning.

So, in managing Asset Integrity, we need similarly separate processes for dealing with high probability-low consequence events and low probability-high consequence events. The former is probably best managed through existing Maintenance Management processes and systems. The latter requires more proactive risk identification and management activities.

Root Cause Analysis thinking leads us to the realisation that there are generally three levels of root cause of system failure

- Physical Root Cause (the equipment broke)
- Human Root Cause (something someone did caused the equipment to break), and
- Latent Root Cause (the organisational system that someone used to make a decision led to the system failure)

There is very often a temptation to deal with equipment failure at the top level (Physical Root Cause), and occasionally at the second level (Human Root Cause). However, to successfully and permanently eliminate the risks associated with equipment failure, we must deal with the Latent Root Causes. This involves ensuring that a wide range of organisational processes, cultures, reward systems etc are all aligned to ensure that risks are successfully managed.

Given the objective of the Asset Integrity Assurance Process given above, as well as the significance of the preceding paragraph, it may be best to consider the Asset Integrity Process as a "meta-process" which incorporates a number of other management processes that may already be in place within an organisation, including:

- Risk Management processes
- Environmental Management processes
- Maintenance Management processes
- Safety Management processes

The challenge is to make sure that all of the activities of these processes are pulled together in a cohesive manner to ensure overall Asset Integrity.

So what may an effective Asset Integrity Process look like?

Elements of an Effective Asset Integrity Process

All good processes should contain all of the elements of the "Plan-Do-Check-Act" cycle. Possible items that could be contained in each of these elements are:

Plan

- Formal Risk Identification and Assessment (either using Quantitative techniques, such as Quantitative Risk Assessment (QRA), or qualitative assessment techniques, such as contained in AS/NZS 4360:1999)
- Criteria for categorising events into high probability-low consequence or low probability-high consequence events
- Reliability Centred Maintenance or PM Optimisation processes for identification of tasks to address high probability-low consequence events
- Protective Devices and Systems analysis process to determine appropriate methods and frequencies of testing/maintaining critical protective systems, such as fire systems etc.
- Formal inclusion of Asset Integrity considerations in budgeting processes

Do

- Project Management of tasks identified in planning stage
- Maintenance Planning and Scheduling Process

Check

- Monitoring of achievement of activities identified in planning stage
- Monitoring of PM schedule compliance
- Monitoring of results of routine equipment inspections
- Monitoring of results of Protective system functional tests
- Asset Integrity Inspections (using visual inspections, assessment of NDT/Condition Monitoring results, assessment of current vs. expected equipment life, assessment of current vs. design operating parameters)

Act

- Root Cause Analysis of equipment failures
- Identification of significant variances from above (e.g. assets that are about to fail), and identification of appropriate corrective actions

Of course, all of this must occur within a corporate framework which has the following elements:

- Leadership – a strong sense of direction and focus on longer-term asset integrity, safety and environmental compliance
- Rewards – Financial and other rewards that encourage a focus on longer term plant integrity, rather than short term plant performance and/or cost cutting
- Culture – Encouragement of a sensible, risk-aware culture that identifies and manages equipment-related risks, rather than ignoring them or believing that "it can't happen here".

Putting It Into Practice – A Case Study

A client of ours had recently experienced some unexpected, catastrophic, and high-profile failures. As a result, they were keen to ensure that similar failures were not repeated, and they were also keen to identify any other, potential, catastrophic failures that may have existed, but of which they were unaware.

We worked with them to develop an approach to managing plant integrity which is currently being implemented.

The first aspect of this approach recognises that, in identifying and assessing equipment-related risks, inspections and controls can occur at four levels:

- **Level 1-** Routine Operator Inspections (up to several times per day)
- **Level 2-** Routine Maintenance Inspections (typically daily, weekly, monthly or quarterly)
- **Level 3-** Internal Audits/Inspections (conducted by professional engineering staff, nominally annually)
- **Level 4-** External Audits/Inspections (conducted by external specialists, and usually limited to specific equipment items or systems)

Our client had recently been through a process to identify and optimise the first two sets of tasks, using Reliability Centred Maintenance principles in a PM Optimisation approach, and so was comfortable that these aspects of Plant Integrity Management were under control. They also conducted a number of external audits/inspections, usually dictated as a result of legislative and/or Occupational Health and Safety regulations, and were less concerned about the adequacy of those. Their prime concern related to the conduct of Internal Audits and Inspections, and so it was in this area that we assisted them to develop and implement a more robust process.

Why are these internal audits and inspections necessary? Some would argue that if the RCM/PMO process had been properly conducted, then it would identify **all** the routine maintenance actions that were necessary, and that, therefore, Internal Audits would not be required – indeed that they could be counter-productive. For our client, these additional inspections were considered to be necessary because:

- Our client operated in a hazardous industry, and the consequences of missing a potential failure mode in the RCM/PMO analysis could, potentially, be extremely serious. Our client wanted to ensure that any missing failure modes were identified early, through an independent inspection process.
- Our client was concerned that there may be increasing acceptance of risk with the passage of time on the part of those that worked continually in the area. This phenomenon has been identified in the analysis of many catastrophic failures, including the Challenger Space Shuttle disaster, and others. Our client wanted to make sure that inspections were performed using an independent, fresh set of eyes, that came from another area within their operations, and that could provide a reality check on potential hazards that may exist.
- Our client also wanted to make sure that this process was used to ensure that the first two levels of inspections were being performed effectively – on time, and to the required level of quality.

- Finally, our client was keen to ensure that any changes to operating conditions or equipment design standards were properly assessed, and sensible decisions made regarding the potential impact of these on regulatory compliance and asset integrity. It was felt that it was best to do this on a formal, regular basis.

The Nature of Equipment-related risks

While Level 1 and 2 maintenance interventions may cover many of the more frequently occurring (and often lower consequence) equipment failure events, our focus on the Level 3 inspection processes meant that we needed to ensure that we identified, and addressed, the less frequent and higher consequence events. In achieving this, we considered that the major sources of these larger, less frequently occurring, risks were in the areas of:

Equipment Design

Over time, equipment design standards change. These could be both externally generated standards (such as Australian Standards) and internally generated standards, which are based on local experience at this site or other sites within the corporate group.

Further, it is possible that modifications that have been made to equipment do not comply with current standards. In our experience, in many industries, there are no, or ineffective configuration management processes to ensure that this does not happen. Occasionally, even in normally well managed industries, these configuration management processes are not followed, with catastrophic results.

It is also possible that when equipment was first designed and installed, that it did not meet those standards, although if sound engineering design and commissioning processes are followed, this should be extremely unlikely.

Compliance with some standards may be mandatory, with others, it may merely be recommended practice. In some cases there is a honeymoon clause, which permits existing equipment that no longer complies with a changed standard to remain unaltered, but which requires that any new, or modified equipment must comply with the standards.

It is important, therefore, to periodically review the extent to which existing equipment complies with current design standards, and to assess the risk of any non-compliance that may exist.

Equipment Operation

All equipment is designed and installed assuming that the equipment will be operated within certain operating parameters. If the equipment is operated outside those parameters, then the consequent risk of equipment failure is increased.

The nature of this operation of equipment outside the design “envelope” can be either:

- Intended, or
- Unintended

And can also be either:

- Sustained, or
- Occasional

When we say that operating equipment outside the design envelope is intended, this is not to say that the operators set out to deliberately break the equipment, but rather there has been a conscious decision to (say) increase production output, without checking whether the equipment was actually capable of reliably sustaining this increase. On the other hand, an unintended breach of the design "envelope" is one where there has been no conscious decision to increase (or reduce) the particular operating parameter – it has normally been a by-product of other decisions.

Sustained breach of the equipment design limits is where the safe operating margins are consistently breached, often by a small, but significant amount. For example, an engine with its "red line" at 6,000 rpm may be consistently operated at 6,200 rpm. The Auckland Power Failure is a typical example of failure in this area.

On the other hand, occasional breach of design limits is where a sudden, intermittent "spike" in the operating parameter is experienced (such as a large voltage spike down an electrical cable).

In almost all cases, exceeding the published design limits for equipment does not lead to instantaneous failure – rather, it sets the conditions for later, premature failure, or for a later failure where the design (and maintenance) parameters had not envisaged failure and these may be catastrophic. Operating an internal combustion engine at speeds consistently above its maximum design rpm rarely leads to instantaneous failure, but it does significantly reduce engine life by applying stresses that lead to premature failure of key components.

Equipment Maintenance

The Level 1 and 2 maintenance interventions, if established using sound Reliability Engineering principles and processes, such as RCM or PM Optimisation, should avoid all expected, intolerable repetitive failures that are economic to predict, prevent or detect. However if these routine maintenance interventions are not performed at the required frequency, or to the required quality standard, then the risk of unexpected failure increases significantly.

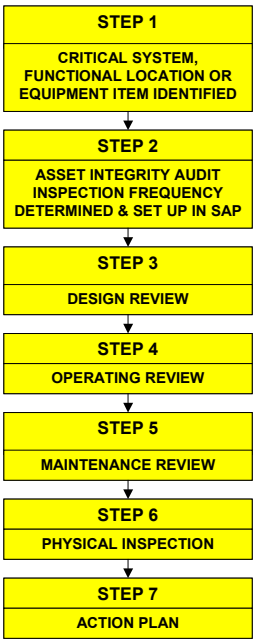
In addition, if high-risk corrective maintenance tasks are not performed according to sound repair and quality principles, then the risk of subsequent equipment failure is also increased.

It is important, therefore, in conducting the Level 3 audit, to ensure that:

- The Level 1 and 2 maintenance interventions have been established using sound Reliability Engineering principles
- That these maintenance interventions are being performed at the required frequency and to the required quality standard, and
- There are properly documented repair procedures for high-risk corrective maintenance actions, and that these repair procedures are effectively used.

The Asset Risk Assessment Process

Based on the above principles, the Asset Risk Assessment process that was used at our client is illustrated diagrammatically on the right.



The details of the key steps are outlined below.

Step 1 – Critical System, Functional Location or Equipment Item identified.

In this step, critical systems, functional locations or equipment items were identified using high level criticality analysis, which, in turn, was based on a risk matrix derived from AS/NZS 4360 – Risk Management. This criticality matrix is a fairly standard matrix which assesses the likelihood and consequence of failure of the system, functional location or equipment, and allocates it an overall level of risk in terms of its potential impact on the operation in terms of Production, Safety, Environment or Costs.

Step 2 – Establish Inspection Frequency in SAP.

In this step, based on the criticality of the system, functional location or equipment, a preferred frequency for the Level 3 inspections (Internal Audit) was determined, and established in SAP. This initiates the internal audit inspection at the desired time. Establishing it within SAP ensures that, with changes in personnel, the need to conduct these inspections is not overlooked.

Higher criticality systems were inspected more frequently, and others less frequently. The frequency of these internal audits ranged from annually to never.

Step 3 – Design Review.

In this step, an appropriately qualified and experienced Maintenance Engineer, by reference to drawings, manuals, design calculations or other relevant documents, critically assesses the level of compliance with current design standards.

The standards referenced include all relevant internal and external standards, including, but not limited to, Australian Standards, OHS&W Regulations, Mines Regulations and internal Company Engineering Specifications.

The Maintenance Engineer documents, in writing, on a specially developed Asset Integrity Audit Summary Sheet, any deviation or non-compliance with the existing standards, highlighting any High or Serious risk areas for consideration. The levels of risk are assessed by estimating the likelihood and consequences of failure (following AS/NZS 4360) using the risk matrix illustrated on the following page.

Likelihood	Failure Consequences					
	0	1	2	3	4	5
Very High	Serious	Serious	High	High	High	High
High	Moderate	Serious	Serious	High	High	High
Moderate	Moderate	Moderate	Serious	Serious	High	High
Low	Low	Moderate	Moderate	Serious	Serious	High
Very Low	Low	Low	Moderate	Moderate	Serious	Serious

Where the failure consequences ratings are as tabulated below:

Consequence Rating	Consequences			
	Safety	Production	Environment	Repair Cost
0	No health effect/injury	No loss of production	No effect	No damage
1	Slight health effect/injury, Medical treatment	Slight loss of production <$10,000	Slight effect, within fence	Slight damage <$10,000
2	Minor health effect/injury, Lost Time	Minor loss of production <$100,000	Minor effect, single breach or complaint	Minor damage <$100,000
3	Significant health effect/injury, irreversible damage	Significant loss of production <$1,000,000	Significant effect, repeated breaches or many complaints	Significant damage <$1,000,000
4	Permanent Total Disability or 1 to 3 fatalities	Major loss of production <$10,000,000	Major effect, extended breach or widespread nuisance	Major damage <$10,000,000
5	Multiple fatalities	Extensive loss of production >$10,000,000	Massive effect, persistent severe damage	Extensive damage >$10,000,000

And the failure likelihood ratings are as tabulated below:

Likelihood Rating	Likelihood
Very High	Occurs several times per year at this site
High	Occurs at least once per year at this site
Moderate	Has occurred in the past at this site
Low	Not known to have occurred at this site, but likely to occur, given industry experience
Very Low	Not known to have occurred at this site, and unlikely to occur, given industry experience

In this instance, we are trying to identify the most important variations from current design standards, in terms of their potential risk to the operations. In many organisations, there may be a high number of deviations, but most, if not all, of these may have potentially low risk. It is important to identify the critical few, not the less important many, in order to successfully manage organisational risks.

Step 4 – Operational Review.

In this step, an appropriately qualified and experienced Maintenance Engineer identifies any critical operational parameters that may lead to accelerated failure of the equipment item. This could include such parameters as:

- Production output
- Flow rates
- Process liquor concentrations (both internal and external to the equipment)
- Specific Gravity
- Temperatures
- Presence of contaminants
- Pressures
- Etc

The Maintenance Engineer then, with reference to drawings, manuals, design calculations or other relevant documents, determines the maximum design capabilities of the equipment with regard to any of the critical operational parameters identified above, and compares this with current operating practice.

The Maintenance Engineer then assesses the potential impact of any deviation of operating practices and strategies outside the original design parameters and documents this, in writing, on a specially designed check sheet, any High or Serious risk areas for consideration. Once again, the levels of risk are assessed by estimating the likelihood and consequences of failure (following AS/NZS 4360) using the risk matrix illustrated above.

Step 5 – Maintenance Review.

In this step, an appropriately qualified and experienced Maintenance Engineer obtains from the Computerised Maintenance Management System (in this case SAP) the details of the routine maintenance program that has been established for the system, functional location or equipment. He than also obtains, also from the CMMS, work order history relating to this routine maintenance program for the last 12 months.

He documents, in writing on the specially developed check sheet, those areas where the routine maintenance program has not been completed, as planned, highlighting any High or Serious risk areas for consideration. Yet again, the levels of risk are assessed by estimating the likelihood and consequences of failure (following AS/NZS 4360) using the risk matrix illustrated above.

Finally, the Maintenance Engineer identifies any complex corrective maintenance tasks that are performed (or may be performed) on the system, functional location or equipment. He reviews the quality of work instructions that have been documented for these tasks, and again, assesses the level of risk by using the risk matrix above. Any high-risk tasks are also identified on the check sheet.

Step 6 – Physical Inspection.

In this step, we recognise that the best program may exist, on paper, but this may not have been translated into reality in the field. As a final assessment of risk, an appropriately skilled and experienced Maintenance Engineer from another area conducts a visual assessment of the physical condition of the system, functional location or equipment, using Visual Inspection Check Sheets and an Equipment Evaluation Rating System and Guidelines that were developed as part of this assignment.

For any critical potential failure mechanisms, where visual inspection alone is not likely to give sufficiently accurate prediction of failure probability, the Maintenance Engineer also obtains, from the CMMS or other relevant information sources, the results of the most recent Condition Monitoring or NDT inspections relevant to these failure mechanisms as well as any appropriate trend information that may be available.

Where critical Condition Monitoring or NDT data is not available, the Maintenance Engineer arranges for specialists to perform the necessary technical inspections at the earliest possible opportunity. This links into the Level 4 inspections referred to earlier in this paper.

The Maintenance Engineer then documents his findings, in writing, on a specially developed Check Sheet, highlighting any High or Serious risk areas for consideration. As usual, the level of risk is assessed by estimating the likelihood and consequences of failure using the risk matrix presented earlier in this paper.

Step 7 – Action Plan

The final step translates the audit into action. After the preceding assessments have been conducted, the Senior Engineer convenes a meeting attended by the relevant Maintenance, Engineering, and Production personnel. This meeting reviews each system, functional location or equipment item for which the Asset Integrity Risk is High or Serious, and develops, and agrees on, actions to reduce the Asset Integrity Risk to no more than Moderate. These actions could be:

- Shaping Actions (to reduce the likelihood of equipment failure), or
- Hedging Actions (to reduce the consequences of failure, should it occur)

The actions could include:

- Revisions to the Routine Maintenance program
- Revisions to Maintenance repair procedures
- Revisions to Operating practices or set points
- Modifications to equipment
- Rebuild, repair or replacement of the equipment
- Modifications to spare parts holding policies or stock levels
- Etc.

Agreed actions are then documented in the form of an Asset Integrity Management plan for the plant area. Agreed actions are implemented through the normal management processes that are applicable for the action – for example, equipment modifications will be managed through the Engineering Project Management process, and funds obtained through the normal processes for capital or operating budgeting.

The Senior Engineer also convenes quarterly review meetings to review progress against the agreed actions, and actions are reviewed and updated as required.

Conclusion

This paper outlines a process for managing Asset Integrity risk that is currently being successfully implemented at one of our clients. It draws on, but does not replace, the valuable work that is done to develop and optimise routine PM programs at this site. It supplements this work with reference to the currently accepted best practice standard for Risk Management, AS/NZS 4360:1999. It may be of interest and value to your organisation also.