AN ANALYSIS OF COMMON CAUSES OF MAJOR LOSSES IN THE ONSHORE OIL, GAS & PETROCHEMICAL INDUSTRIES

IMPLICATIONS FOR INSURANCE RISK ENGINEERING SURVEYS

SEPTEMBER 2016

INSIGHT CONSENSUS INFLUENCE

Authors
Ron Jarvis CEng MIChemE, Swiss Re, London
Andy Goddard CEng MIChemE, Talbot Underwriting, London

Contributions
Contributions made by Kevin Gormley CEng FIChemE of QBE and John Munnings-Tomes CEng MIChemE of Navigators who are members of the LMA Onshore Energy Business Panel Engineering Sub-Group, are acknowledged.

If there are any technical queries regarding this document please contact the LMA: patrick.davison@lmalloyds.com.

LMA OG&P Loss Analysis – Version 1.0 (September 2016)

Disclaimer

CONTENTS

1 INTRODUCTION

1.1 BACKGROUND

A review has been carried out of 100 major losses in the onshore oil, gas and petrochemical industries over the past 20 years. The information contained in this study is intended to analyse the common causes of major losses in a way that it will be of practical use to insurance risk engineers.

The energy insurance industry is in a unique position in that it has experience and detailed knowledge of many industry losses, unlike many individual operators who may never experience a major loss. This study may therefore also be of interest to those working in the oil, gas and petrochemical industries who are looking for lessons learned opportunities to assist in their own risk management programmes.

The analysis comprised a review of available loss information, primarily from insurance industry reports, as well as public domain sources.

1.2 PURPOSE

It is (Re)Insurers' belief that risk engineering surveys should be conducted with a detailed awareness of the common causes of major losses in the industry. The purpose of this study is therefore primarily to guide insurance risk engineers on which loss control areas to focus on during a typical risk engineering survey of onshore oil, gas and petrochemical facilities.

This study supports the Lloyd's Market Association's key information guidelines for risk engineering survey reports[1] and guidelines for the conduct of risk engineering surveys[2] and builds upon previous studies[3].

1.3 SCOPE

For this study 100 major onshore oil, gas and petrochemical losses over a 20 year period from 1996 to 2015 were analysed. Only 'man-made' fire and explosion losses were considered (natural catastrophe events were excluded). It should be noted that, since the focus of the study is on losses with significant monetary impact, some major events resulting in large numbers of fatalities or injuries might not be included.

Although numerical data is provided and trends have been identified where possible, this should not be considered a detailed statistical analysis.

This report includes the development and details of the analysis methodology used, the results of the analysis and recommended focus areas for insurance risk engineers.

No attempt has been made to identify underlying or root causes since this information is usually not available to (Re)Insurers. Instead, the aim is to identify the most important risk control elements that can be most easily assessed by an insurance risk engineer during a typical 2-3 day risk engineering survey.

1.4 ACRONYMS

API	American Petroleum Institute
CoW	Control of Work
EOP	Emergency Operating Procedure
ESD	Emergency Shut Down
HAZOP	Hazard & Operability Study
IPL	Independent Protection Layer
ITPM	Inspection, Testing & Preventative Maintenance
LMA	Lloyd's Market Association
LOPA	Layers Of Protection Analysis
LPG	Liquefied Petroleum Gas
MoC	Management of Change
MSF	Management System Failure
PHA	Process Hazard Analysis
P&ID	Piping & Instrumentation Drawing
PMI	Positive Material Identification
PtW	Permit to Work
QA/QC	Quality Assurance/Quality Control
ROEIV	Remotely Operated Emergency Isolation Valve
SCD	Safety Critical Device
SIL	Safety Integrity Level
SOL	Safe Operating Limit
SOP	Standard Operating Procedure
WELD	Willis Energy Loss Database

2 METHODOLOGY

2.1 LOSS INFORMATION

The Willis Energy Loss Database (WELD)[4] was used to identify onshore oil, gas and petrochemicals losses from 1996 to 2015 with a total loss value exceeding USD 50 million. This loss amount was the sum of the ground up property damage plus the associated business interruption costs, excess of the insurance waiting period and only where this cover was provided. Other costs were excluded e.g. environmental clean-up, civil fines, reputational damage, personal liabilities, etc. Only "man-made" fire and explosion losses were considered (i.e. natural catastrophe events were excluded).

The losses within WELD are anonymous with only basic details provided and significant work was undertaken to ascertain the actual case in question in order to review the causes of loss. However, this report only identifies the losses by occupancy. Individual loss amounts ranged from USD 50 to 1,500 million. In total 100 losses were identified for analysis, including all of the top 50 losses in WELD (by total loss value).

Information on the background and causes of these losses was obtained from available loss information, primarily from insurance industry reports, other insurance industry publications and data sources[5] as well as public domain sources. Losses were only included where there was sufficient information to determine causation to the level required by the analysis methodology.

Total property damage and business interruption values of the losses analysed are shown in Table 1:

Table 1

	Property Damage*	Business Interruption**	Combined Loss
Total Losses (All Figures USD)	11,000,000,000	14,000,000,000	25,000,000,000

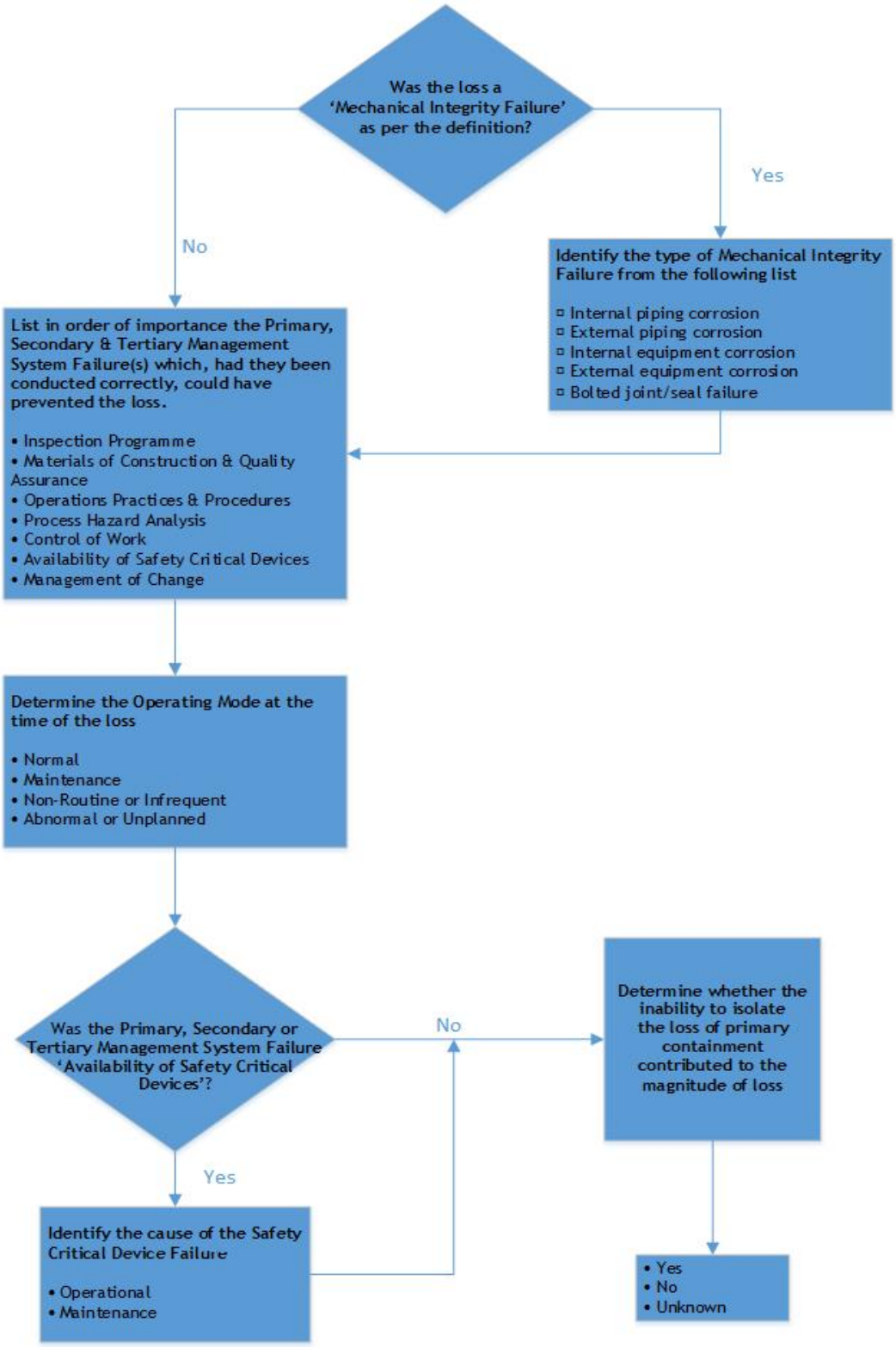
* *Property Damage figures are adjusted for inflation to end 2015 but exclude policy deductibles*

** *Business Interruption figures are actual loss to (Re)Insurers net of waiting period deductible and are only provided where cover is in place and therefore are an under estimate of actual losses sustained*

2.2 LOSS ANALYSIS METHODOLOGY

A flowchart of the process is provided in Figure 1 with the various elements of the process described in the following sections.

Figure 1



'Mechanical Integrity Failure' Losses

It was deemed important to separate out mechanical integrity failure losses as these were identified during a previous loss analysis as being responsible for a large proportion of the losses analysed[6]. The losses were therefore initially filtered to distinguish between 'Mechanical Integrity Failure' losses and 'Non-Mechanical Integrity Failure' losses based on the following definition:

Mechanical Integrity Failure	Failure of the primary pressure-containing envelope due to a specified failure mechanism. This largely relates to corrosion through metal although also includes any bolted joint or seal failures. This excludes failures induced by operation outside of safe operating limits.

The types of 'Mechanical Integrity Failure' were classified as follows:

a) Piping internal corrosion

b) Piping external corrosion

c) Equipment internal corrosion

d) Equipment external corrosion

e) Bolted joint/seal failure

For the purpose of this document, corrosion is considered to include all damage mechanisms that lead to mechanical integrity failures of equipment and piping as more fully described in API RP 571[7]

Every loss, whether caused by 'Mechanical Integrity Failure' or not, was analysed using the Management System Failure Model described below.

Management System Failure Model

Major losses are considered to occur because of simultaneous failures of loss prevention or mitigation barriers, in line with the 'Swiss Cheese' accident model[8]. Rather than attempt to analyse all of the barrier failures associated with each particular loss analysed, those loss prevention barrier failures perceived to have made the most significant contribution to the loss, were identified. **Up to three of these so called 'Management System Failures (MSFs)' were assigned to each loss in order of perceived contribution and termed Primary, Secondary and Tertiary MSFs.**

Identifying the MSFs and their order of importance was based on engineering judgement supported by peer review. Identifying the order of MSFs due to 'Mechanical Integrity Failure' was generally straightforward as the MSFs were usually clear and limited in number.

The MSFs developed and their definitions are listed below.

Management System Failure (MSF)	Definition
Inspection Programme	Intended to cover all aspects of a static equipment and piping inspection programme including identification and risk assessment of damage mechanisms.
Materials of Construction & Quality Assurance	Intended to cover deficiencies in mechanical design, fabrication and installation of equipment during original construction or subsequent change e.g. during maintenance. This excludes deficient design specification (a process design issue) but does include equipment not installed to specification (a quality assurance/quality control issue). The following are examples: incorrect materials installed, installation not as per design specification, fabrication defect, mechanical installation fault. Note: Losses caused by the selection of materials unsuitable for the service was considered to be an intentional (design) decision and the MSFs for these losses were therefore classified as either MoC or PHA.
Operations Practices & Procedures	Intended to cover all aspects of operational management except Control of Work and management of Safety Critical Devices (see below). Examples include manning, shift communications, supervision, training, competence assurance, Standard Operating Procedures (SOPs), Emergency Operating Procedures (EOPs), response to alarms etc. In the case of SOPs and EOPs, this covers: no procedure, incorrect or incomplete, incorrectly followed, document control
Control of Work (CoW)	This is applied to any work activity which would ordinarily require a Permit to Work (PtW) and/or safe isolation procedure. The scope includes hazard identification and risk assessment, process preparation, work execution and return to operation. The work activity could be undertaken by maintenance or contractors during operational or shutdown periods (e.g. turnaround and grade change), or by operations (e.g. operators switching equipment using operational blinds).
Process Hazard Analysis (PHA)	Intended to cover items which should be addressed through the plant's PHA programme including process design weaknesses, inherent safety and learning from losses. PHA is taken to include HAZOP, LOPA and SIL and any other hazard identification and risk assessment techniques. The PHA could be the original plant PHA at the time of construction and any subsequent PHA revalidations/reviews. Identification and analysis of Safety Critical Tasks and identification of Safety Critical Devices would fall under this category.
Management of Change (MoC)	This is applied whenever a failure in change management contributed to the loss with 'change' defined in the broadest sense including 'non-hardware-related' changes such as organisational and operational change. Change management is taken to include all aspects of MoC from initiation to close-out and specifically including the hazard identification and risk assessment of the change by whatever technique. The change could have occurred during the original construction, subsequent projects or operational plant changes.
Availability of Safety Critical Devices (SCDs)	This is applied whenever a SCD is unavailable or fails on demand during a loss scenario. The failure could be due to a lack of maintenance or the equipment had been consciously defeated (or bypassed). The definition of SCD is suitably broad and this category is also intended to capture non-SIL rated process critical instrumentation which may or may not strictly meet the definition of a SCD (e.g. distillation column level instrument) but which played a significant contributory role in the loss.

In a significant number of the losses analysed, the absence of Remotely Operated Emergency Isolation Valves (ROEIVs) was frequently cited as a factor which could have prevented escalation of the initiating event i.e. could have reduced the size of the loss. The presence (or absence) of ROEIVs has therefore also been considered in this analysis as a loss mitigation feature.

Operating Mode

The 'Operating Mode' at the time of loss was considered with one of the following descriptors assigned to each loss.

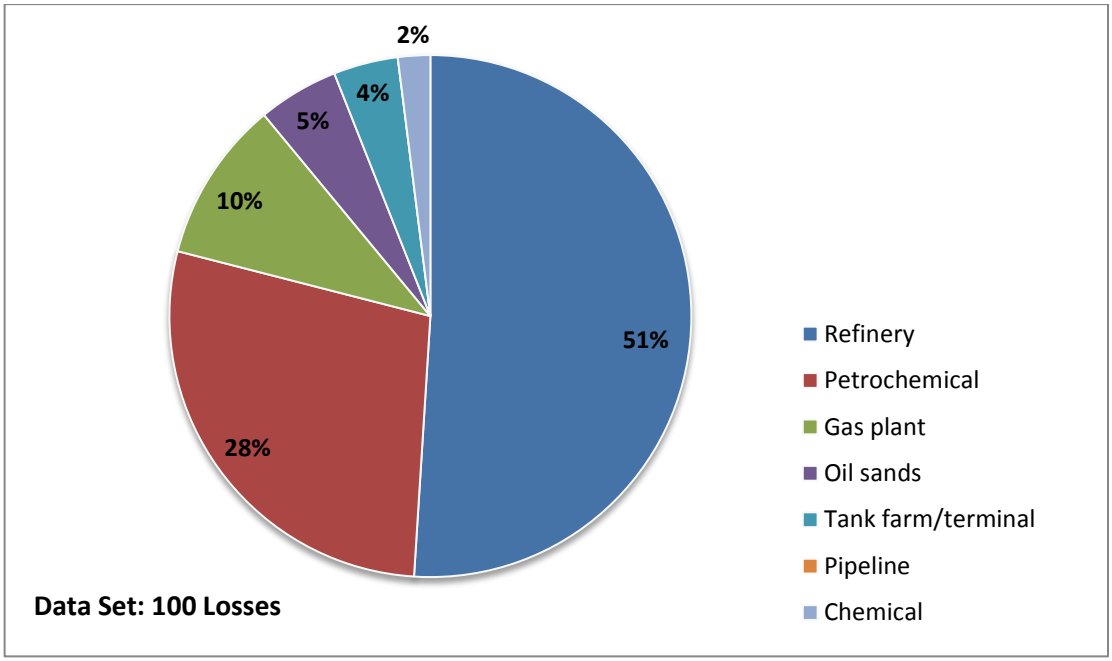
Operating Mode	Definition
Normal	Plant was running under steady state conditions and within normal operating limits.
Maintenance	A specific maintenance activity was ongoing with direct relevance to the loss. A maintenance activity is taken to be a job typically requiring a permit to work and would include the operational aspects of plant preparation and reinstatement. This includes turnaround maintenance activities and any plant modification work.
Non-Routine or Infrequent	Operations that are considered to be non-routine or planned operations that occur relatively infrequently. Examples would include plant or equipment start-up, planned plant or equipment shutdown, operation with a non-standard configuration, batch operations, equipment switching, storage tank line-up and grade changes.
Abnormal or Unplanned	Abnormal operations range from non-steady state or upset conditions through to operation outside design specification or safe operating limits. Unplanned operations are those typically in response to an initiating event such as unplanned shutdown or other emergency operational activity.

3 DATA ANALYSIS

3.1 OCCUPANCY

The occupancies of all the 100 losses analysed are distributed as shown Figure 2. Note that no attempt has been to normalise loss frequency against the relative number of each occupancy. As can be seen 51% of losses occurred at refineries and 28% on petrochemical plants.

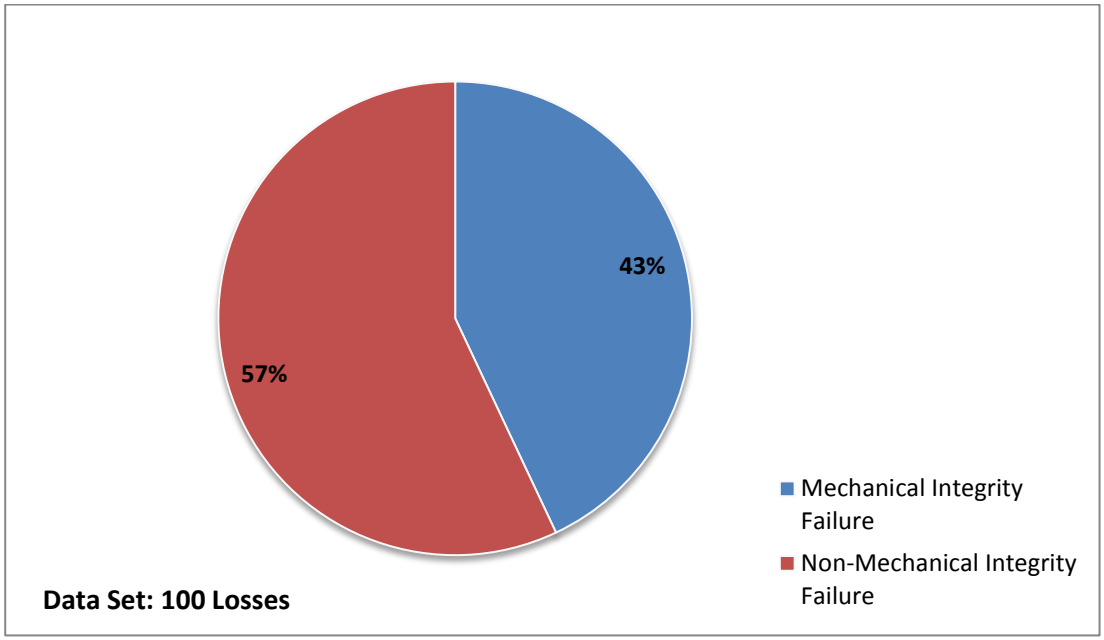
Figure 2 Occupancy Distribution of the Losses Analysed



3.2 'MECHANICAL INTEGRITY FAILURE' LOSSES

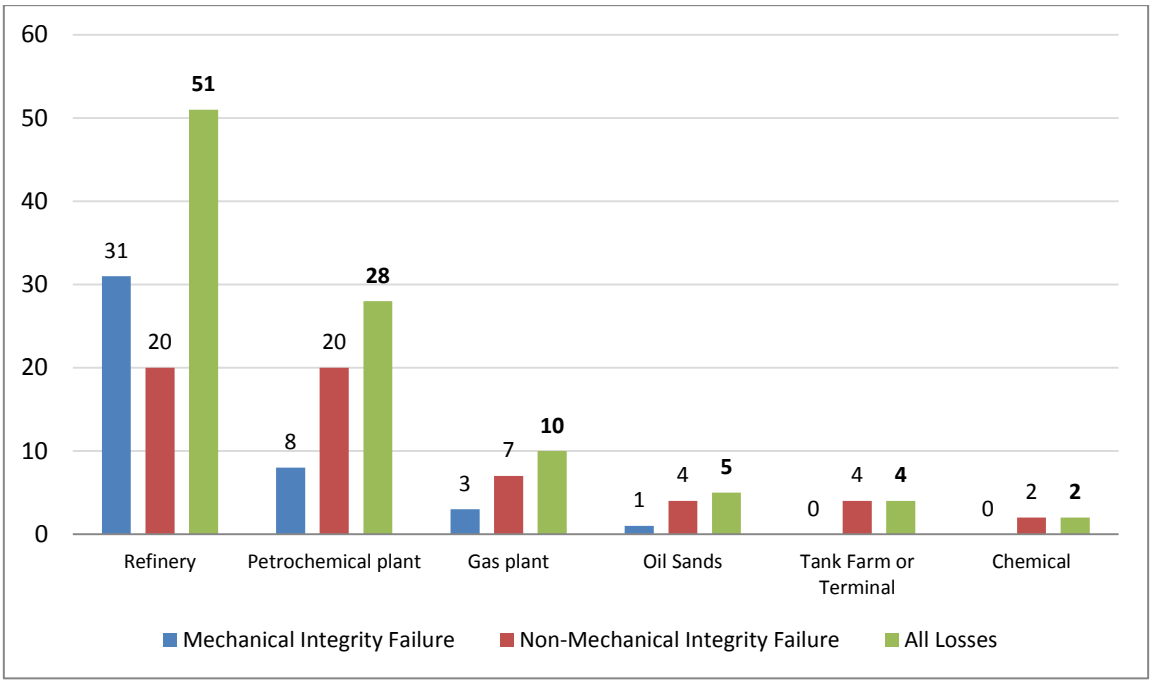
43% of the 100 losses analysed were due to 'Mechanical Integrity Failure' – Figure 3 below.

Figure 3 'Mechanical Integrity Failure' vs 'Non-Mechanical Integrity Failure' Losses



Mechanical integrity failure is a far more likely cause of major loss for refineries than for other occupancies as shown in Figure 4.

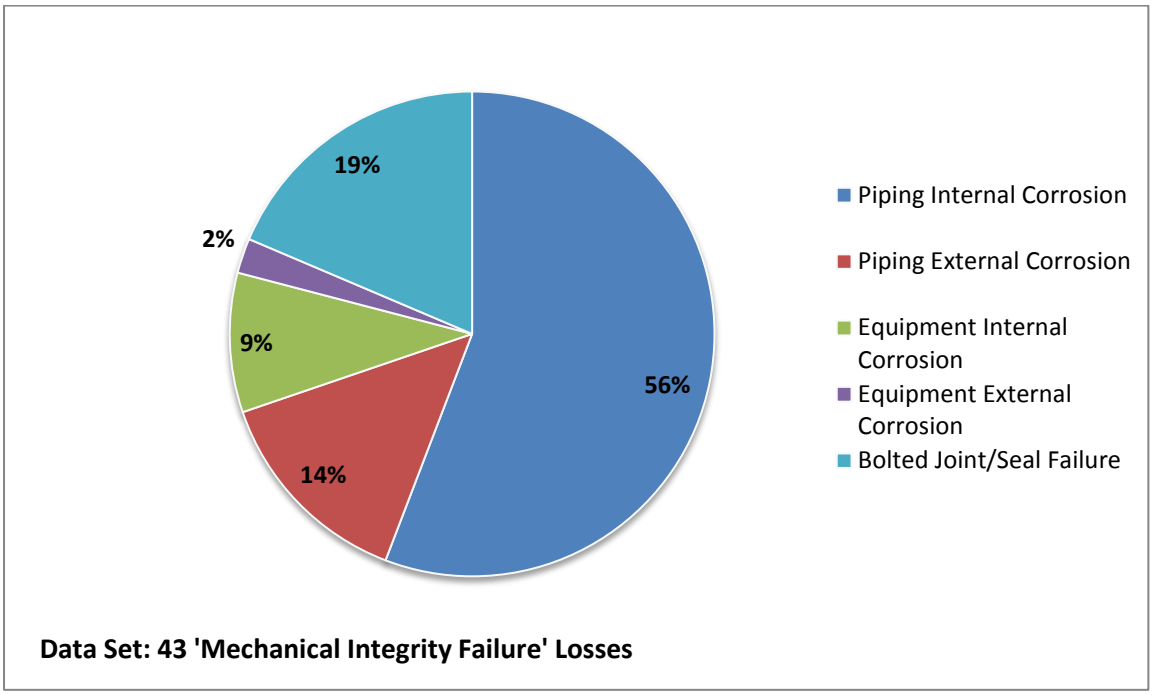
Figure 4 Occupancy breakdown by number of losses



3.3 'MECHANICAL INTEGRITY FAILURE' TYPES

The types of 'Mechanical Integrity Failure' are split as shown in Figure 5.

Figure 5 Types of 'Mechanical Integrity Failure'



Regarding the types of 'Mechanical Integrity Failure', the following observations are made:

- 70% of all 'Mechanical Integrity Failures' were due to corrosion (as defined previously) of process piping, mostly due to internal corrosion. External corrosion was primarily due to corrosion under insulation.

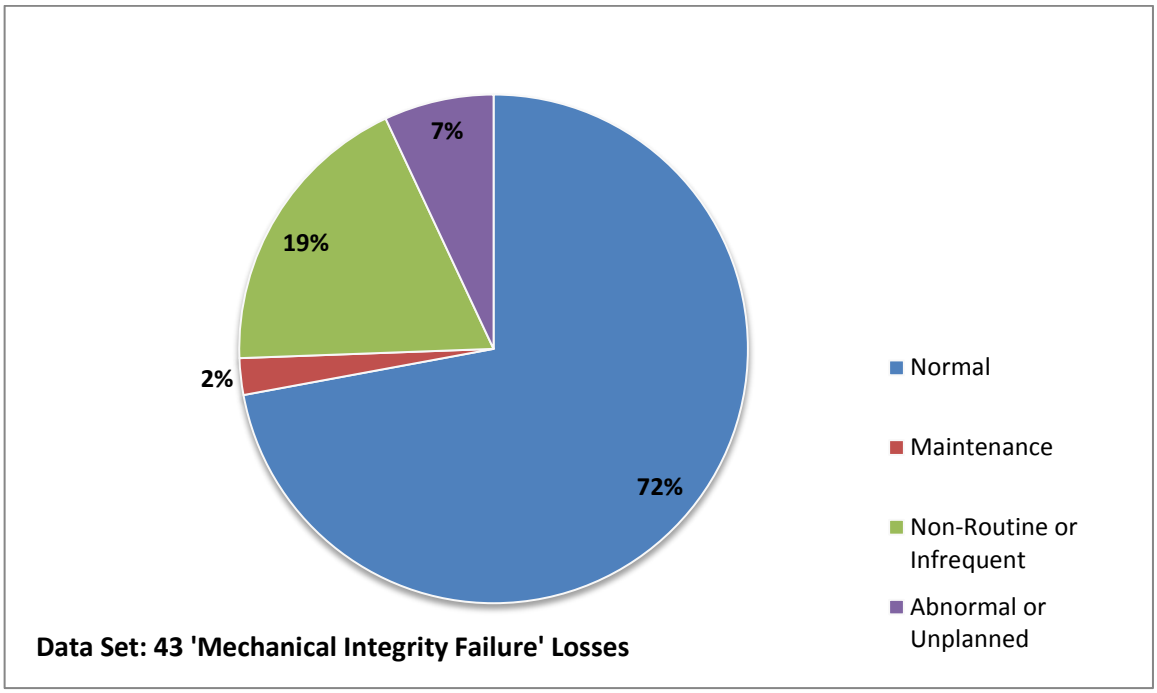
- 'Mechanical Integrity Failure' of static equipment (including pressure vessels) is far less common (approximately 10%).
- There were five bolted joint failures in the data set due to inadequate bolting. In two cases flange bolts became loose due to pressure relief valve chattering or excessive pipe vibration following a significant operations event. In these cases it was impossible to determine whether the bolting was inadequate or whether the vibration was so severe that inadequate bolting could not be blamed. However, it does raise an important issue regarding the adequacy of joint bolting, particularly in critical services.
- There were three valve component/valve seal failures.

With respect to piping and equipment corrosion, these results are in line with insurance risk engineers experience i.e. that the mechanical integrity of pressure vessels is generally well enforced worldwide, primarily driven by regulation. Process piping, on the other hand, is generally not as highly regulated and is therefore left to the operator to devise an appropriate inspection programme, introducing the opportunity for inconsistency. Another factor is the vast amount of process piping on a typical refinery or petrochemical plant.

3.4 OPERATING MODE

Figure 6 summarises the distribution of 'Mechanical Integrity Failure' losses by operating mode.

Figure 6 Operating Mode - 'Mechanical Integrity Failure' Losses

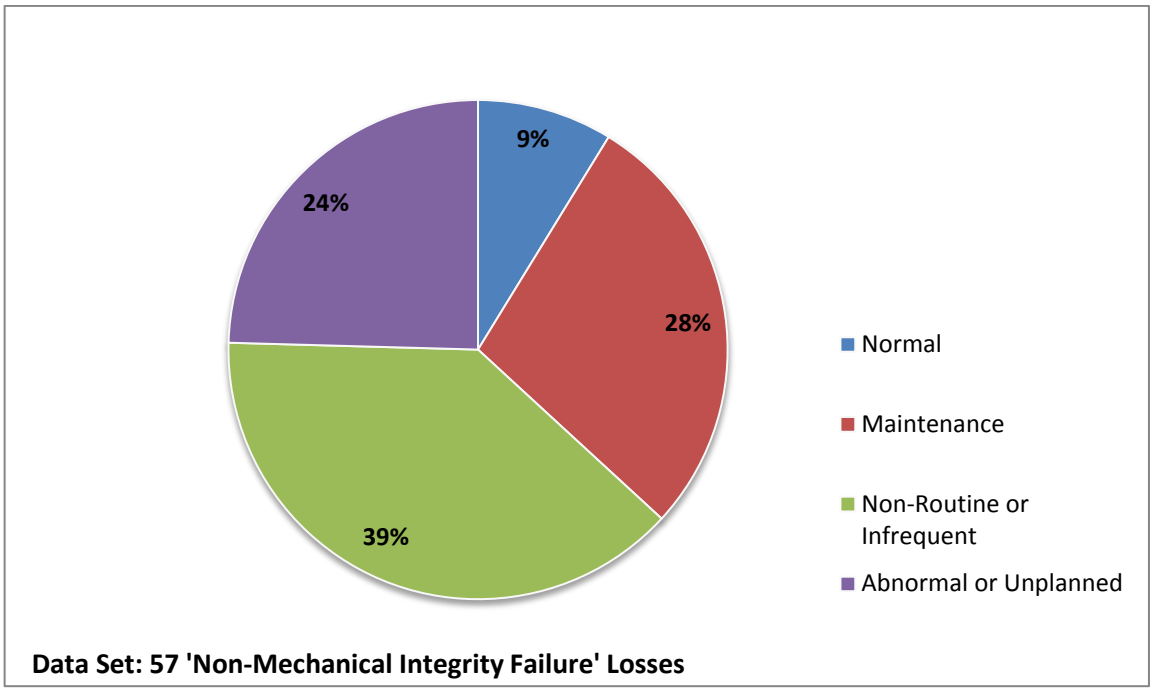


As can be seen more than 70% of 'Mechanical Integrity Failure' losses occurred during normal operation. This is not surprising as losses of this type are generally unexpected and sudden.

Eight 'Mechanical Integrity Failure' losses occurred during start-up operations (classified as 'Non-Routine or Infrequent') where the transient process conditions revealed weaknesses in the plant previously unnoticed under steady state conditions.

Figure 7 summarises the distribution of 'Non-Mechanical Integrity Failure' losses by operating mode.

Figure 7 Operating Mode - 'Non-Mechanical Integrity Failure' Losses



Data Set: 57 'Non-Mechanical Integrity Failure' Losses

As can be seen less than 10% of 'Non-Mechanical Integrity Failure' losses occurred during Normal operation. What is also significant is the high combined contribution of 'Non-Routine or Infrequent' and 'Abnormal or Unplanned' operating modes which could collectively be termed 'Transient' operations. These accounted for more than 60% of 'Non-Mechanical Integrity Failure' losses **i.e. there is a strong relationship between 'non-normal' operation (of various types) and the likelihood of a major loss.**

Nearly 30% of 'Non-Mechanical Integrity Failure' losses occurred during maintenance activity, typically due to inadequate control of work.

3.5 PRECURSORS TO TRANSIENT EVENT-RELATED LOSSES

In terms of 'Transient events', Table 2 provides a summary of the events which lead to these losses.

Table 2 Transient Events - All Losses ('Mechanical Integrity Failure' and 'Non-Mechanical Integrity Failure' Losses)

Non-Routine or Infrequent Activities	#	Unplanned Events	#	Abnormal Situations	#
Start-up	19	Power failure	4	Blockage	4
Equipment switching	9	Equipment trip	2	SOL excursion	2
Shutdown (planned)	0	Steam failure	1	Other	3
Other	2	Cooling water failure	1		
		Other	0		

The following observations are made:

- For 'Non-Routine or Infrequent Activities':
  - **'Plant Start-up'** accounted for 19 losses and is by far the most important transient precursor.
  - **'Equipment Switching' is also an important precursor resulting in 9 losses.** This is a broad categorisation covering numerous types of equipment switching including such operational activities as:
    - Reactor switching (batch reactors, coke drums, etc.)
    - Storage tank switching during filling operations
    - Olefins cracking furnace decoke cycles
    - Switching parallel heat exchangers or pumps
  - Planned shutdown does not feature in any of the losses analysed.
- **For 'Unplanned Events'** losses, **'Power Failure'** was the most common precursor.
- In terms of the 'Abnormal Situations' losses, 'Blockage' was the most significant precursor.

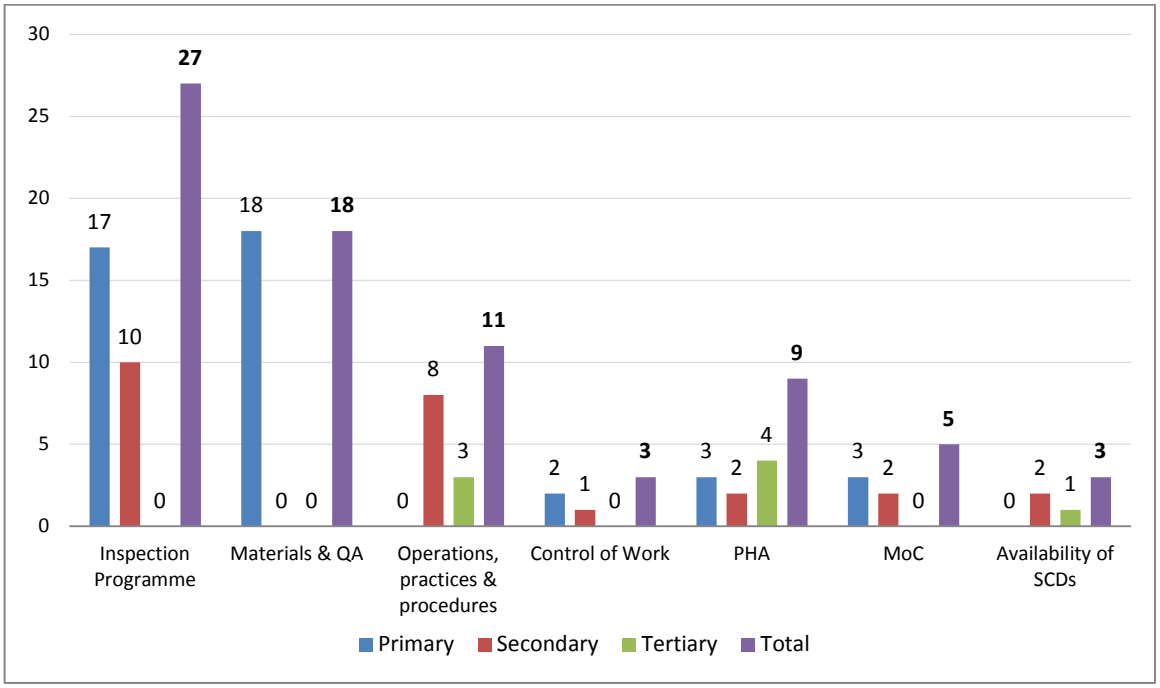
Losses due to transient operations are discussed in Section 4.3.

3.6 MANAGEMENT SYSTEM FAILURES

Primary, Secondary & Tertiary MSFs – Mechanical Integrity Failure

Figure 8 summarises the number of Primary, Secondary and Tertiary MSFs for 'Mechanical Integrity Failure' losses.

Figure 8 Number of Primary, Secondary & Tertiary MSFs

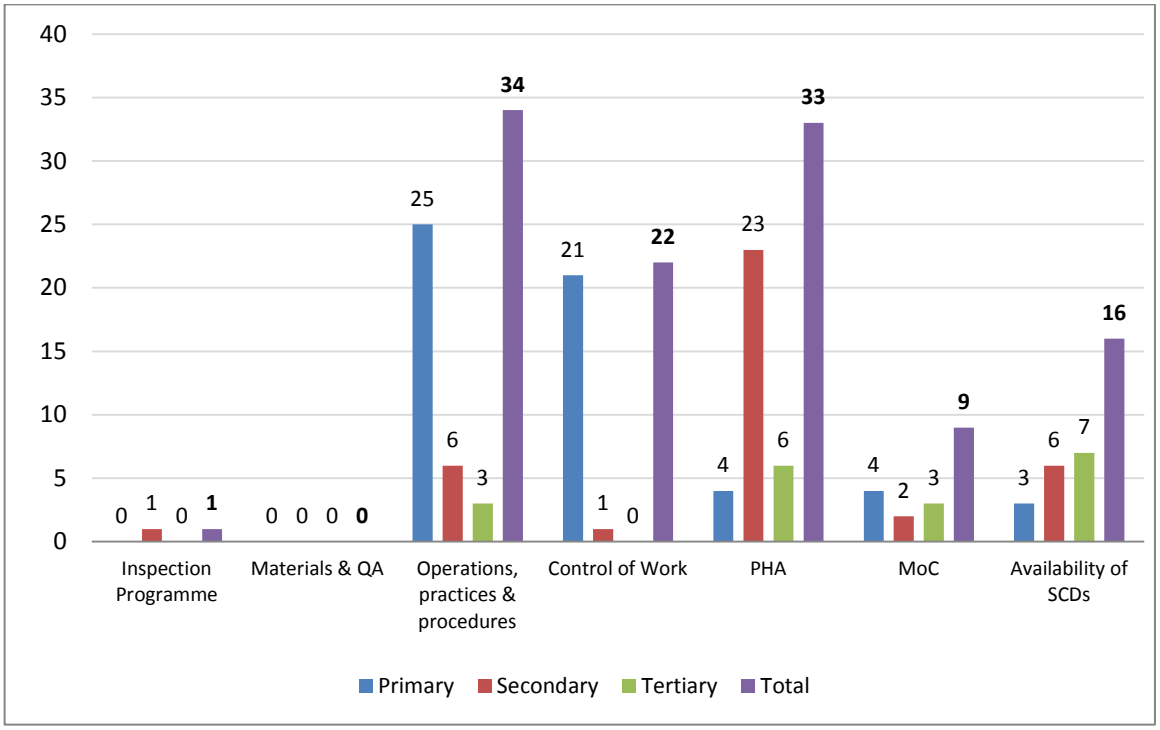


It is noted that Mechanical Integrity-related MSFs, i.e. Inspection Programme and Materials & QA, are dominated by their Primary MSFs. This is because generally a major loss of integrity has few other MSF layers of protection to prevent the loss.

Primary, Secondary & Tertiary MSFs – Non-Mechanical Integrity Failure

Figure 9 summarises the number of Primary, Secondary and Tertiary MSFs for 'Non-Mechanical Integrity Failure' losses.

Figure 9 Number of Primary, Secondary & Tertiary MSFs



As can be seen, the Primary MSF is dominated by Operations Practices & Procedures and Control of Work (safe maintenance) i.e. these MSFs are the first line of defence. PHA is typically a second line of defence as shown by the dominance as a Secondary MSF, demonstrating the importance of effective PHA to prevent major losses. The Availability of SCDs and MoC become more important as a Tertiary MSF, i.e. where other barriers have already failed.

Primary, Secondary & Tertiary MSFs – Combined Analysis

Based on the combined number of Primary, Secondary and Tertiary MSFs (assuming equal weighting), the relative importance of each MSF is as follows:

a) Inspection Programme and Materials & QA (Mechanical Integrity-related MSFs)

b) Operations Practices & Procedures

c) PHA

d) Control of Work

e) Availability of SCDs

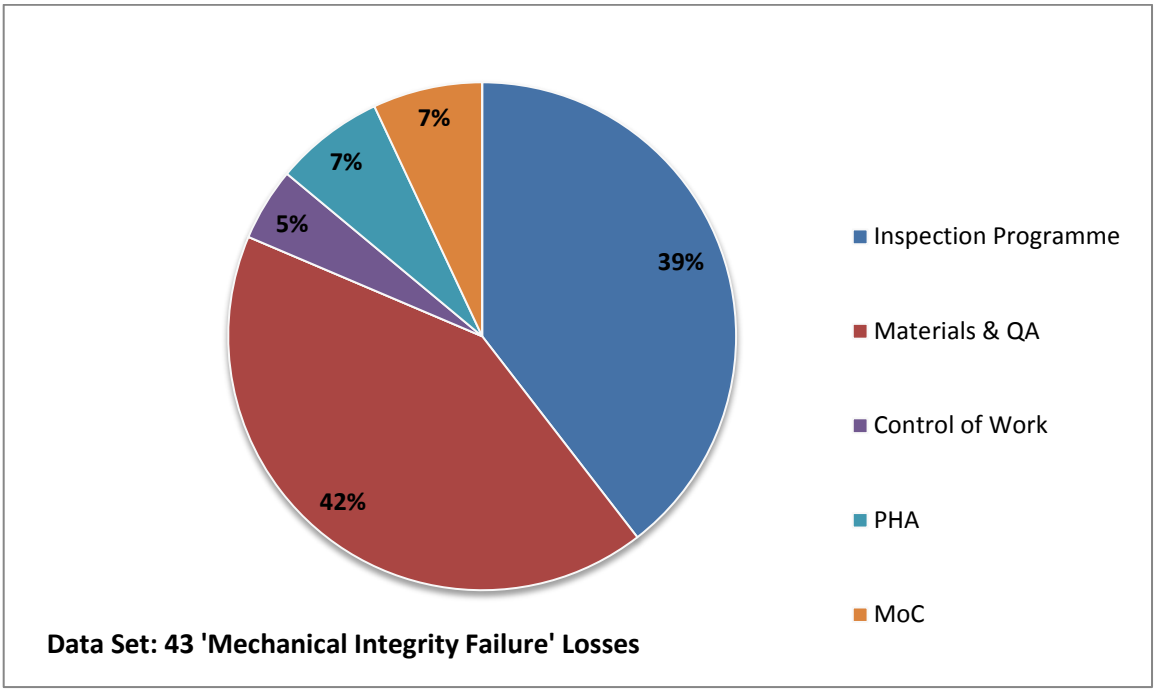
f) MoC.

4 MANAGEMENT SYSTEM FAILURE ANALYSIS

4.1 INSPECTION PROGRAMME

As shown in Figure 10, 39% of Primary MSFs for 'Mechanical Integrity Failure' losses were attributed to an inadequate or incomplete inspection programme i.e. the potential for mechanical integrity failure could have been identified before the loss occurred if a more thorough and effective inspection programme had been in place.

Figure 10 'Mechanical Integrity Failure' Losses Primary MSFs



Many of the inspection-related losses resulted from the failure to identify potential damage mechanisms and then implement appropriate inspection programmes to suit (in fact this is considered a fundamental issue underlying most of the losses). Of particular note are localised damage mechanisms which can be difficult to detect. For some of the losses analysed, corrosion had been detected before the loss but there was a failure to act on this information. Some examples are as follows:

- Refinery (fire) - partial replacement of piping had occurred in a piping circuit of a refinery unit following internal corrosion. However the whole circuit was not replaced as some parts were considered to be above minimum allowable thickness. There were also differing material specifications within the pipe circuit. The piping failed because the subsequent inspections did not include all of the more corroded sections of piping.
- Petrochemicals plant (fire) - piping failure due to localized corrosion under insulation which was not identified by the inspection programme.
- Refinery (vapour cloud explosion) – column overheads piping failure due to internal corrosion.

Several failures occurred partly because external inspection would have been difficult. Examples are as follows:

- Refinery (vapour cloud explosion) - an encased (underground) propylene pump failed due to corrosion of the casing because of a historic defect which would have required pump removal to be apparent.
- Refinery (vapour cloud explosion) – a hydrocarbon condensate pipe ruptured due to internal corrosion. Inspection of the pipe at the point of failure would have been difficult as it was resting on a concrete sleeper pipe support in a piperack.
- Gas plant (vapour cloud explosion) – a sub-sea gas import pipe ruptured at an interface between the sea and the beach which was difficult to inspect externally due to the presence of external pipe wrapping.
- Petrochemical plant (fire) – gas feed pipe failure caused by localised corrosion under insulation (the area affected covered an area of less than one square foot). The pipe was located about 18 feet above the ground and obscured from view.

In some cases, operational changes impacted the damage mechanism:

- Refinery (vapour cloud explosion) – overhead vapour line ruptured due to internal erosion & corrosion at a bend just downstream of a water injection point. The installation and operation of the injection point did not go through a formal MoC. This pipe was also difficult to access for inspection.
- Gas plant (fire) – failure of a heat exchanger nozzle due to liquid metal embrittlement of aluminium by elemental mercury present in the feed gas which had increased in concentration over time.

These and some other losses emphasise the importance of identifying damage mechanisms and their associated risk and the need to establish Integrity Operating Windows.

There were five bolted joint failures due to inadequate bolting. Although mentioned here, their Primary MSFs were either PHA (3) or Control of Work (2) since the initiation of these bolted joint leaks was directly related to these MSFs. Examples are as follows:

- Refinery tank farm (vapour cloud explosion) - a propylene pump flange in an off-sites area had apparently been leaking for several days, possibly due to short-bolting. A subsequent failure due to fatigue of the bolted joint caused a major release of propylene.
- Refinery (fire) – a fire occurred in a bank of shell and tube heat exchangers on a refinery unit. Due to the heavy fouling duty, the exchanger pairs were frequently switched over for bundle pulls. Cleaning and leaks often occurred on the exchanger heads following switchover which were tightened up online. However one such small leak escalated to a major fire. Operators were unable to access the isolation valves due to the fire which prolonged the fire event. Aside from the undesirable requirement for frequent cleaning (a function of process conditions), follow-up after the loss focused on improving bolting practices.
- Petrochemical plant (fire) - the loss of cooling water flow to a petrochemical unit resulted in pressure increase in the propylene splitter column. The operator response was unable to prevent the pressure safety valves relieving to the flare. Due to excessive chattering and vibration the inlet flange to one of the PSVs failed resulting in the release of a propylene vapour cloud and a vapour cloud explosion. It is unknown whether bolting standards contributed towards the loss or whether the bolts became loose due to excessive vibration during opening of the PSVs.

4.2 MATERIALS OF CONSTRUCTION & QUALITY ASSURANCE

As shown in Figure 10, 42% of Primary MSFs for 'Mechanical Integrity Failure' losses were attributed to Materials of Construction & Quality Assurance. These were split as follows:

Table 3

No of losses	Materials of Construction & Quality Assurance Failure Mechanism
8	Premature corrosion due to the presence of incorrect materials of construction i.e. not in accordance with the design specification, primarily due to a failure of QA/QC practices and procedures during construction or maintenance
7	Weld defects or material out of specification e.g. excessive hardness in piping or equipment (failure of QA/QC practices & procedures)
3	Valve component failure (design/specification related)

In many of these cases a more effective inspection programme could have identified a potential loss of integrity indicated by accelerated/unexpected corrosion rates. However in these cases 'Materials of Construction & Quality Assurance' rather than 'Inspection Programme' was chosen as the Primary MSF since it was the initiating cause of failure.

There were several cases of incorrect materials installed either when the plant was built or at a later, often undocumented, stage in the plant's history, resulting in premature failure. In all cases there were found to be individual 'rogue' components in piping systems, predominantly in ageing refineries (6 of the 8 losses caused by premature corrosion were in ageing refineries). Examples are as follows:

- Petrochemical plant (explosion) – high pressure piping ruptured during compressor start-up. Investigation found that the piping had suffered high temperature hydrogen attack and subsequent PMI discovered the piping was not the specified Cr/Mo alloy (the piping was installed over 30 years earlier).
- Refinery (fire) - hydrogen induced embrittlement of a control valve in a HDS unit resulting in a fire. A carbon steel control valve was installed by mistake instead of stainless steel some years before the loss.
- Refinery (fire) - an 8" diameter carbon steel elbow inadvertently installed in a high pressure, high temperature hydrogen line ruptured after operating for only 3 months. The failure occurred as a maintenance contractor accidentally switched a carbon steel elbow with an alloy steel elbow during a scheduled heat exchanger overhaul.

It should be noted that a further 3 'Mechanical Integrity Failure' losses were attributed to inappropriate materials of construction intentionally installed as a plant change leading to premature failure due to corrosion. Although the primary cause of failure was installation of incorrect materials of construction, these have been classified under Management of Change in this report.

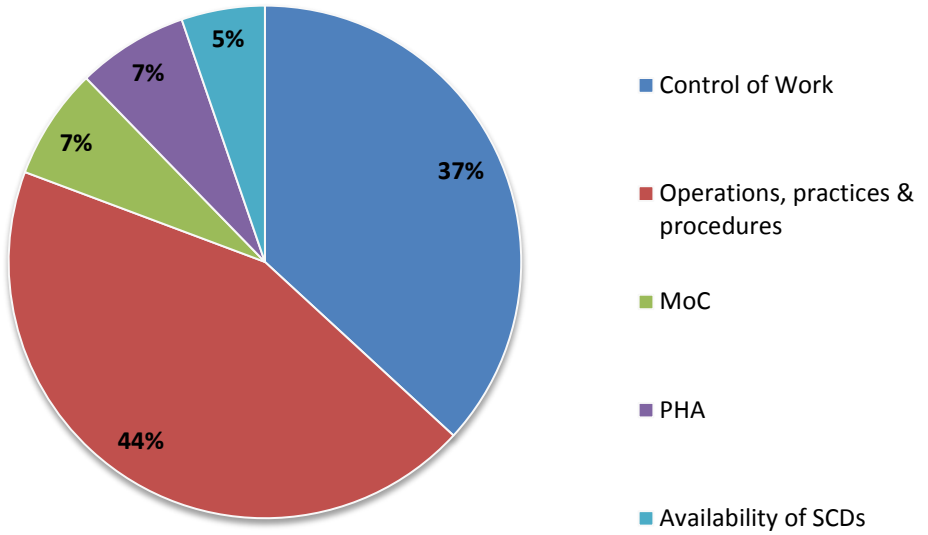
There were 3 losses attributed to valve component failure (design/specification related). For example:

- Refinery (fire) - during the start-up of a compressor on an olefins plant (following repeated compressor trips), a suction check valve shaft 'blow-out' occurred due to a valve design fault. It is reported that failures of similar valves had occurred previously at other plants worldwide.

4.3 OPERATIONS PRACTICES & PROCEDURES

As shown in Figure 11, 44% of Primary MSFs for 'Non-Mechanical Integrity Failure' losses were attributed to Operations Practices & Procedures.

Figure 11 'Non-Mechanical Integrity Failure Losses Primary MSFs



Data Set: 57 'Non-Mechanical Integrity Failure' Losses

In general, when the plant is running in normal or steady state conditions, losses due to Operations Practices & Procedures MSF are unusual. Losses tend to occur during infrequent activities or unsteady state conditions. The most common causes of the losses associated with this MSF were as follows:

- **Non-Routine of Infrequent Activities**

  Lack of compliance with (or absence of) operating procedures (including checklists) for infrequent activities such as unit and equipment start-up, discontinuous operations such as equipment switching, etc.

- **Abnormal or Unplanned Events**

  Operational activities not subject to permit to work and/or safe isolation procedures, e.g. clearing blockages.

  Incorrect or inappropriate response to an abnormal or unplanned event such as an emergency situation.

- **SCD and critical bypass valve management**

  Safety critical devices defeated, not functioning (lack of maintenance) or not identified as safety critical. Lack of control of the use of bypass valves etc. (see Section 4.6).

Often too much reliance is placed upon Operations Practices and Procedures for loss prevention when the root cause is often associated with inherent design weakness, inadequate hazard identification or unavailability of safety critical devices.

Although not specifically identified from the available loss reports, operator and supervisor experience, competency and manning levels will most likely have contributed to a number of

the losses. However, this is normally an underlying issue at a level below the direct management system failures considered by this analysis. Loss of experience is evident in the industry due to a high turnover of staff in certain regions and a retiring workforce. All too often, retraining of operators only follows an incident. It would be more beneficial to define a systematic competence assurance programme with a particular focus upon critical tasks. Definition and provision of minimum safe manning levels covering all modes of operation is also an important factor.

Non-Routine or Infrequent Activities

Start-Up

As mentioned in Section 3.5, 'transient event' losses most commonly occurred during planned start-up of plant and equipment. Common failings that led to such losses were:

- Procedures not followed.
- Lack of the use of check lists.
- Communications issues usually associated with shift handover.
- Inadequate staffing for demanding activities such as start up.

For example, the use of manual valves to isolate fuel gas was the cause of a number of furnace losses. The lack of formal checklists to ensure that these operations were carried out in the correct sequence was an important factor, as was operator competency leading to incorrect diagnosis of the problem - Refinery (fire) - and weaknesses in shift handover procedures.

Equipment Switching

Several losses occurred during what has been classified as equipment switching of various types. Examples are as follows:

- Upgrader (fire) - fire occurred during coke drum switching.
- Tank farms (fires) - two major tank farm fires occurred during the filling operations (switching tanks on line).

In all these losses, although there were failures of several management system barriers, the use of specific and well-designed, operating procedures and check lists for these discontinuous activities would have provided a level of protection.

A number of losses resulted from poor control of bypass valves. Some examples are as follows:

- Refinery (explosion) – an explosion occurred in a crude unit furnace during start-up. Hydrocarbon reached the furnace during line-up of the downstream vessels. Although a high-level trip device had been fitted to the vessel the bypass valve was open thereby defeating the trip device.
- Refinery (fire) - a fire occurred on a crude unit shell & tube heat exchanger. The tube-side bypass valve was manually opened because a lighter crude was being processed. This procedure had not been documented. A subsequent leak in the piping could not be isolated due to the bypass valve. Note that the leak was caused by a bolted joint design/installation issue.

Abnormal or Unplanned Events

Blockages

As mentioned in Section 3.5, there were several losses initiated by operators attempting to clear blockages in equipment. For example:

- Petrochemical plant (vapour cloud explosion) - during start-up after an unplanned shutdown on a polymer unit, dissolved wax caused blockages. In order to remove the wax, some in-line filters were repeatedly opened. During one of these filter changes the operator failed to properly isolate the filter and although hydrocarbon flow was initially prevented by the wax blockage, this eventually cleared itself resulting in a significant loss of hydrocarbons which the operators were unable to isolate.
- Gas plant (fire) - Shortly after commissioning, field operators were troubleshooting process issues believed to be caused by the presence of unknown construction debris. Operators opened a low point drain in LPG service and commenced draining the debris into a bucket. Eventually LPG began to flow and the operators were unable to close the drain.
- Several other losses have occurred which were associated with piping and equipment blockages. A common factor in some of these losses was a failure to identify potential hazards as these types of interventions by operators are often not controlled by a permit to work or isolation certificate and associated risk assessment.

Emergency Operating Procedures (EOPs)

The absence of effective EOPs, or failure to comply with the EOPs under emergency circumstances, contributed to some of the losses; in particular associated with key utility failures (EOPs are taken to cover predefined but unplanned scenarios). EOPs are also an important safeguard following loss of containment, demonstrated by a number of instances where operator action (or inaction) contributed to the magnitude of the loss. Appropriate action (rapid controlled plant shutdown) will often restrict the size of a loss. Examples are as follows:

- Petrochemical plant (runaway reaction) – during a batch oxidation reaction the steam supply failed and in response the operator activated the ESD system. As the temperature of the reactor liquid phase was not dropping as quickly as the operator expected, the ESD interlock was released allowing a switch back to the normal cooling water supply. Unbeknown to the operator, this action also stopped the nitrogen flow which was providing agitation and cooling to the reactor contents. This ultimately led to a runaway reaction and rupture of the oxidation reactor. Improvements to the EOP were recommended to ensure full understanding of the ESD functionality.
- Petrochemical plant (vapour cloud explosion) – the loss of cooling water to a propylene column overheads condenser due to a manual valve line up error. This ultimately led to a pressure relief valve bolted joint failure and vapour cloud explosion. Operators responded in the field, however there was no formally documented EOP for this particular utility failure scenario.

The following losses were specifically related to operator response to hydrocarbon leaks:

- Gas plant (fire) - delay in activating the plant ESD following a hydrocarbon release.
- Refinery (pipe trench fire) – a leak from an offsite crude oil pipeline was discovered and an attempt was made to clean up and clamp online. Hydrocarbon liquid had flowed into the pipe trench and vapours accumulated in a roadway underpass igniting on a steam line.

This was around 3 hours after the initial discovery of the leak. An extensive pool fire in the pipe trench ensued.

- Refinery (pool fire) – a significant number of personnel gathered at the leak from a crude unit piping system. Attempts were made to remove the insulation using a pole to enable the line to be clamped but this was unsuccessful and the decision was made to build a scaffold. Firefighters in breathing apparatus began to remove the insulation but a flash fire occurred and the area was evacuated. Orders were given to shut down the unit 2 hours 40 minutes after the initial leak discovery shortly after line ruptured followed by ignition. A formal leak response protocol was subsequently developed[9]

4.4 CONTROL OF WORK

As shown in Figure 11, 37% of Primary MSFs for 'Non-Mechanical Integrity Failure' losses were attributed to Control of Work. The Control of Work losses generally fall into three categories:

- Safe isolation of equipment for maintenance.
- Permit to work system including contractor management and handback to operations.
- Safe work practices.

Safe isolation of equipment for maintenance

Piper Alpha and Pasadena Texas are well known losses caused by inadequate isolation during maintenance. The failure to adequately prepare and isolate equipment prior to the first line break remains a common weakness. The following are examples of losses that occurred due to inadequate isolation:

- Refinery (fire) - incident occurred during start-up of the main crude unit following a unit turnaround. Maintenance personnel worked on the wrong flange leading to a release of hydrocarbon and major fire at the base of the main column. The work location was not adequately identified by Operations.
- Refinery (fire) - An oil spill occurred due to a failure of a block valve to seat properly during maintenance on a pump strainer in the visbreaker unit. The oil auto-ignited and the ensuing fire spread and destroyed the unit.

Reliance on remotely operated valves for safe isolation requires very careful consideration to ensure that they are not inadvertently opened, i.e. the motive force to open the device should itself be isolated as part of the overall isolation process. The following are examples of such losses:

- Gas plant (vapour cloud explosion) – a bolted joint was opened for maintenance on a pump but reliance for isolation was placed on a remotely actuated valve. The valve was inadvertently opened either from the control room or from the motor control centre resulting in a major release of propane with subsequent explosion.
- Petrochemical plant (fire) - A loss occurred during the removal of a blind following decoke of one of the ethylene cracking furnaces. The blind was located downstream of an air actuated valve which was inadvertently opened during blind removal. This released quench oil resulting in a large fire and multiple fatalities.

There were two major losses caused by the use of operator-controlled line blinds e.g. Sammi, Onis, Hamer etc. Although these incidents have been classified as 'Control of Work' they could just as easily have been classified as failure of 'Operating Practices & Procedures' or 'PHA' (both had PHA assigned as the Secondary MSF). They have been included here because although they require positive isolation either side of the blind before they are operated,

these devices were designed to be used by the operators and are often not subject to a permit to work/safe isolation certificate. Guidance on the use of these blinds is available[10].

Permit to work system

Losses due to inadequate permit to work control tend to be less severe than those due to inadequate isolation.

Fires due to hot work activities are typically characterised by inadequate supervision of contractors when undertaking hot work activities.

The following losses occurred due to inadequate PTW system management or control:

- Refinery (fire) – hot work was being conducted in a packed column by a sub-contractor under the supervision of the equipment vendor/contractor. The site hot work permit procedure was not followed and a fire occurred causing major damage and subsequent collapse of equipment.
- Refinery (fire) - a 'metal fire' occurred inside a 250ft column during replacement of the internals and packing (hot work) which ultimately led to the collapse of the column.
- Fertilizer plant (fire) - Following the completion of welding work by contractors, a fire spread due to the presence of combustible materials in the area including cable trays and conveyor belts.

The handback from job executor to plant owner is an important step and failure to verify the quality of work carried out contributed to a number of the losses. As previously mentioned in Section 3.3, five losses occurred due to inadequate joint bolting practices and verification of flange make-up should form part of any PTW handback.

Specific risk areas for oil and petrochemical plants that require special attention are hot work near column packing.

Safe Work Practices

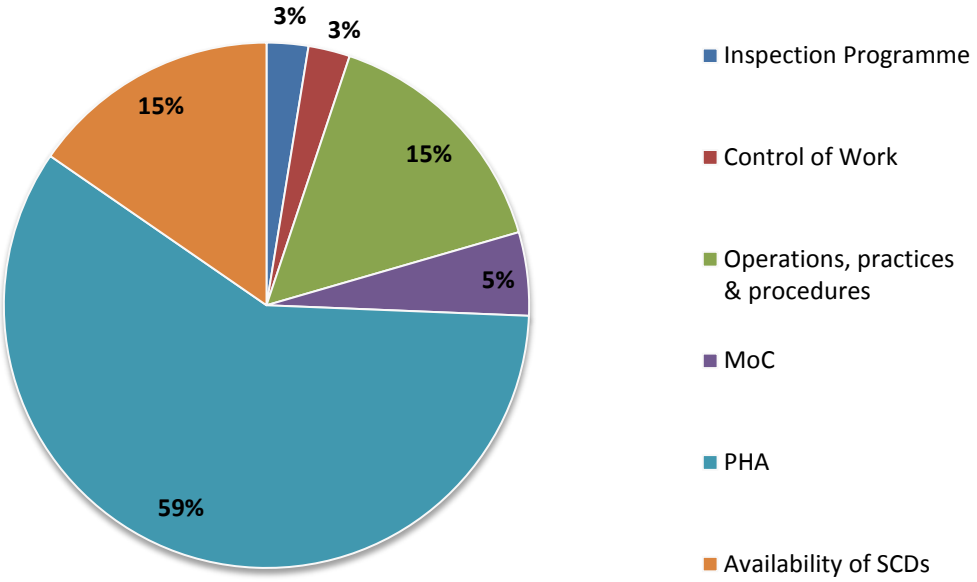
There were a few losses caused by poor work practices during maintenance. For example:

- Gas plant (fire) - Contractors were in the process of blinding pipework as part of capital project works. The contractor incorrectly supported a propane process line resulting in a crack in the pipework. The released propane auto-refrigerated the line leading to catastrophic failure.
- Petrochemical plant (vapour cloud explosion) - A trailer being towed by a forklift snagged and pulled a drain valve out of a strainer in a liquid propylene system on the Cracker. Operators were unable to isolate the leak which formed a large vapour cloud. The ensuing explosion and fire caused extensive damage.

4.5 PROCESS HAZARDS ANALYSIS

Inadequate PHA was cited as a Secondary MSF in 59% of 'Non-Mechanical Integrity Failure' losses as shown in Figure 12. This is surprising considering that HAZOP studies and other related methods are mature methodologies that have been adapted and proven to be effective in many situations including for safety-critical tasks and procedures.

Figure 12 'Non-Mechanical Integrity Failure' Losses Secondary MSFs



Data Set: 39 Secondary MSFs 'Non-Mechanical Integrity Failure' Losses

As shown by Figure 9, PHA MSF features a total of 33 times in the 57 'Non-Mechanical Integrity Failure' losses analysed in this study. The following are particular weaknesses identified:

- Inadequate quality of hazard identification studies
- HAZOP of Safety-Critical Activities/Transient Operations
- Identification of Safety Critical Devices

Inadequate quality of hazard identification studies

There were a significant number of losses partly caused by the failure to identify hazards and/or provide suitable risk mitigation controls in the form of hardware process design features. This could be considered the basic function of a PHA and would therefore suggest that the quality of PHAs could be improved.

Quality assurance processes for HAZOP studies are rarely in place. An independent review of the quality of completed HAZOP studies would be of significant benefit, for example verifying the team composition, the time spent, sampling some of the hazards identified and verifying the recommendations made were appropriate and implemented.

Specifically, a number of losses occurred due to inadequate pressure relief system design. Examples are as follows:

- Petrochemical plant (explosion and fire) – a large explosion and ensuing fire resulted when an operator was attempting to switch over two in-parallel reboilers on a fractionation column. The process design was such that it was possible to block in the reboiler boiler feed water supply without adequate pressure relief (a similar design has since been found on another plant during an insurance risk engineering survey indicating that this was not an isolated finding).
- Refinery (pool fire) – a large pool fire resulted from a loss of containment from a relief valve manifold on the discharge of the main charge pumps to the crude unit. The incident occurred following switch over of the pumps which resulted in overpressure, the relief

valves chattering and ultimately failure of a relief valve inlet bolted joint. A number of issues were identified with the relief system design (including whether or not the valves should have been installed in the first place).

- Refinery (vapour cloud explosion) – a vapour cloud explosion occurred on the isomerization unit during start-up operations. A fractionator column was inadvertently liquid filled, with pressure relief provided by an atmospheric blowdown drum and not to a closed flare system. The blowdown drum and piping was undersized leading to overfill of liquid into the process unit.

HAZOP of Safety-Critical Activities/Transient Operations

As is evident from Section 3.5, a significant proportion of the analysed losses occurred during transient operations and in many of these cases the plant design was found to be inadequate with reliance then placed upon operator response. HAZOP studies should therefore ensure that all operating modes are considered in sufficient detail to ensure suitable risk mitigation controls are in place.

With respect to operating procedures, there are well established techniques for identifying hazards associated with transient operations for which safety-critical procedures should be in place, although they are still rarely carried out in the refining and petrochemicals industries. These "procedural HAZOP" studies can often plug the gaps left by conventional HAZOPs. For instance P&IDs may not show every design detail, particularly instrumentation details such as local bypass switches, logic or vendor-specific equipment details. A procedural HAZOP will highlight these details and ensure a greater focus on their function, operation and maintenance as well as analysing in detail each step of the procedure. There would likely be more benefit in using available resources to conduct safety critical procedural HAZOPs rather than the commonly adopted 5 year revalidation HAZOPs studies, especially when a good MoC procedure is in place which should capture the vast majority of new hazards[11] [12] [13].

Based on the analysis it has been concluded that several of the losses described in this report could have been prevented by improved consideration of transient operations during PHAs and conduct of safety critical procedural HAZOPs.

Identification of Safety Critical Devices

Several losses were attributed or partially attributed to safety critical devices not being available on demand. The 'Availability of SCDs' is covered in detail in Section 4.6.

HAZOP and Layer Of Protection Analysis (LOPA) studies are well established techniques for identifying SCDs which is an important step feeding into operating procedures and safety-critical maintenance programmes. Many of the losses mentioned in Section 4.6 fall into this category i.e. the SCD was not identified and therefore the defeating or maintenance of the device was not treated as safety-critical by either the operations or maintenance departments. Appropriate identification of SCDs is a forerunner to the development of appropriate Inspection, Testing & Preventive Maintenance (ITPM) programmes.

Also of importance is the identification, via HAZOP and LOPA, of what might best be described as other “critical” process devices or Independent Protection Layers (IPLs). These might not be formally SIL rated but still need to be managed as safety critical devices.

The following losses occurred due to inadequate protective controls:

- Petrochemical plant (fired heater explosion) – a firebox explosion occurred in the reformer during start-up operations effectively destroying the reformer section and shutting down the plant. The start-up of the fired heater relied upon manual sequencing of fuel gas valves and various operational errors led to the loss. Following the loss, a fully

automated burner management system was installed with previous HAZOPs failing to address this scenario.

- Tank farm (vapour cloud explosion) – overfill of a gasoline storage tank led to a major vapour cloud explosion causing significant on and offsite damage. Operators were reliant upon a basic 'float and tape' level control system which was malfunctioning at the time of the incident. A HAZOP should have considered provision of a suitable overfill protection device.

4.6 AVAILABILITY OF SAFETY CRITICAL DEVICES

The Availability of SCDs was cited as an MSF in a total of 19 losses as shown in Figure 8 and Figure 9.

As was discussed in Section 4.5 (**Identification of Safety Critical Devices**), inadequate management of SCDs is often due to a lack of formal identification in the first instance which would otherwise ensure that the associated availability controls are in place.

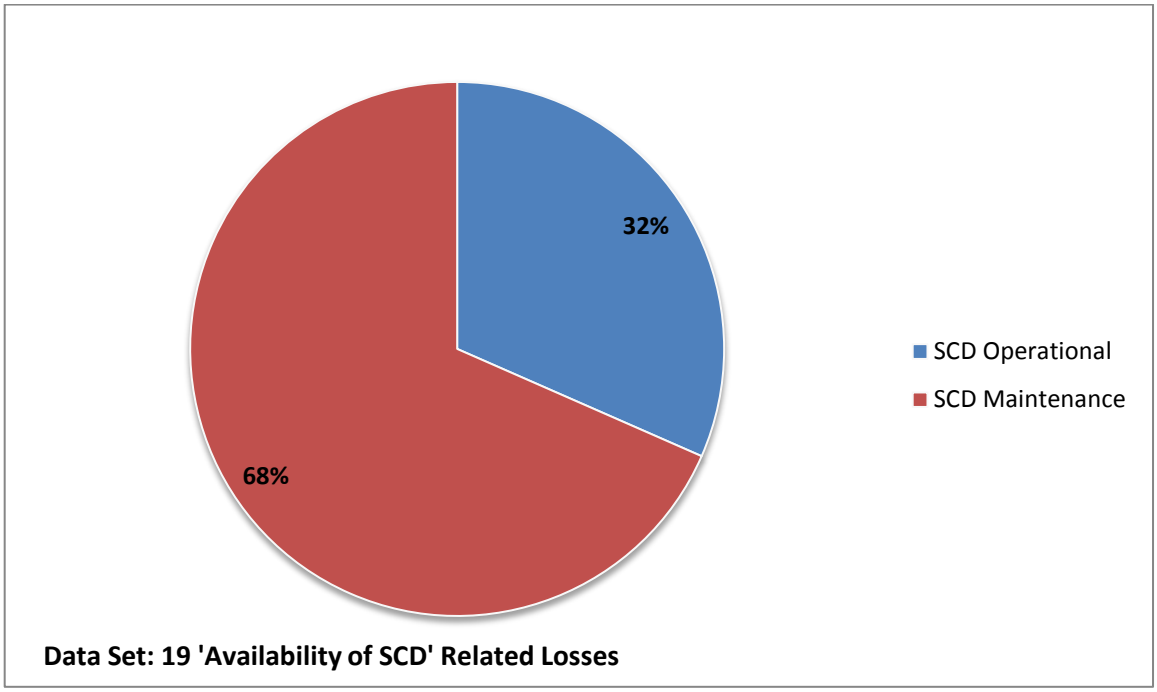
Losses related to the availability of SCDs were divided into two categories in this analysis:

a) Maintenance-related – the SCD was unavailable due to a lack of or an inadequate ITPM programme.

b) Operational-related – the SCD was unavailable as it had been intentionally defeated or bypassed.

Figure 13 below indicates the split between Maintenance-related and Operational-related SCD for the 19 **'Availability of SCD' related losses.** Most failures were due to inadequate testing and preventative maintenance.

Figure 13 Breakdown of all 'Availability of SCD' related losses



SCD Maintenance-related losses

The following are examples of SCD Maintenance related losses:

- Tank farm (vapour cloud explosion) – overfill of a gasoline storage tank led to a major vapour cloud explosion causing significant on and offsite damage. The independent high

level switch had been inadvertently disabled following testing effectively inhibiting the overfill protection device. This further emphasises that both installers and users should have a full understanding of the correct use of SCDs, and further raises questions regarding SCD design that enabled its primary function to be so easily overridden.

- Petrochemical plant (cracking furnace damage) – a regional power failure led to a complete crash shutdown of an ethylene plant causing significant damage to the cracking furnace tubes. As well as power, onsite steam and instrument air were also lost. Notably the Uninterruptible Power Supply failed to operate due to inadequate maintenance. There were a number of other findings concerning the robustness of utility supply and back-up systems.
- Refinery power plant (steam turbine overspeed) – one of the refinery's steam turbine generators tripped off load but continued to rotate and overspeed to the point of destruction. The main steam isolation valves were found to have closed and held as designed however a malfunctioning steam extraction non-return valve allowed backflow of steam from the main refinery header. The non-return valve was found to be stuck open. There was no testing and maintenance programme in place for this critical non-return valve.

What became evident during the analysis was the importance of certain critical process instrumentation which may not typically be classified as a SCD but was a key contributor to the loss as it was not functioning correctly (e.g. column level instrumentation). For this analysis, these have been included within this MSF with some examples below:

- Refinery (vapour cloud explosion) – a refinery unit was started up following a turnaround with observed faulty column level gauge. The explosion occurred following a hydrocarbon release primarily due to corrosion of an overheads piping section, although the malfunctioning level gauge was considered to be a significant contributory factor.
- Refinery (fire) - water freeze in piping dead leg partially attributed to non-functioning water level transmitter that was being used in a non-routine shutdown preparation operation. The water level instrument was not identified as being an IPL, although a redundant level transmitter/alarm was installed on the rebuilt plant.

SCD Operational-related losses

Several large losses have occurred primarily because safety critical devices (trips or interlocks) were disabled or by-passed. While these could also be classified as Management of Change or Operations Practices &Procedures in this analysis they have been classified as SCD Operational-related MSFs. There is guidance on managing the defeating of SCDs[14].

Inadequate management of the bypassing and disabling of SCDs is often a decision borne out of a lack of awareness of the importance of the system and the consequences of failure. It might be deemed necessary due to a design problem or a maintenance issue (such as a lack of spares). It is often the case that the only way of keeping the plant running in these cases is to bypass the trip or interlock. In other words a maintenance or design problem becomes an operator's problem.

The following are examples of such losses:

- Refinery (fire) - a large actuated isolation valve was opened on a live reactor using a local over-ride switch resulting in major property damage and an extended period of loss of production.
- Petrochemical plant (explosion) – an explosion occurred in an air separation unit leading to damage to the cold box. Excessive quantities of hydrocarbon from the atmosphere accumulated in the oxygen rich liquid within a reboiler resulting in a combustion process

with the aluminium heat exchanger which led to an overpressure event. Due to frequent alarms during operation, the hydrocarbon analyser on the reboiler sump was switched to calibration mode effectively inhibiting the alarm and trip function.

- Petrochemical plant (explosion) - during a batch oxidation reaction, the steam supply failed and the operator activated the ESD system switching cooling water to the emergency water supply. As the temperature of the reactor liquid phase was not dropping as quickly as the operator expected, the ESD interlock was released to allow a switch back to cooling water rather than the emergency water supply. However (and unknown to the operator), this action stopped the nitrogen flow which was used to agitate the reactor contents leading to a runaway reaction and rupture of the oxidation reactor.
- Petrochemical plant (explosion) - an explosion occurred in a polymer reactor house due to an operator incorrectly opening the bottom valve on an online reactor adjacent to the one which was offline and being cleaned. A manual field bypass was used to defeat the bottom valve interlock on the online reactor with the operator believing he was to empty the offline reactor and that the valve was stuck.

The above losses are sometimes attributed (in loss reports) to a lack of operator training, competence or supervision. However practical experience suggests that design or maintenance faults that require the disabling of trips and interlocks, or result in these systems not functioning as they should, can become the long-term norm if a formal system of risk assessment, authorisation and regular reporting of status to senior management is not in place. It is worthy of note that two of the above losses involved the use of a local field bypass which had become a routine part of the SOP and was not subject to the same control procedures other control room plant bypasses might have been.

4.7 MANAGEMENT OF CHANGE

Management of change (MoC) does not feature as often as some of the other management system failures, although this category excludes the bypassing of safety-critical trips and interlocks. In some cases, no formal MoC had been carried out whereas in other cases the hazard identification and risk assessment was found to be inadequate. The majority of MoC losses related to ‘hardware’ changes although operational and organisational changes did also feature. There exists practical guidance on Management of Change[15].

Examples of MoC losses were as follows:

- Petrochemical plant (fire) - high pressure rupture of a reactor and separation vessel with subsequent major fire caused by release of ethyl benzene due to the adoption of a new type of catalyst. During the start up in manual control mode a runaway reaction occurred because the new catalyst was far more reactive than the previous catalyst used. It does not appear that an MoC was carried out.
- Petrochemical plant (decomposition) - a decomposition reaction occurred within a low density polyethylene tubular reactor resulting in extensive damage. Previously a change was made to the ESD logic which inadvertently lengthened the time to reduce reactor pressure on detection of a decomposition.

It is observed that there have been some major losses caused during the plant design and construction phase in which changes were made after P&IDs were issued for construction i.e. after HAZOP studies had been carried out. The following major losses occurred after a decision was made (post-HAZOP) to install different materials:

- Refinery (fire) - a section of pipe failed rapidly (within months) of plant operation. The material of construction had been changed during the late design/construction phase to carbon steel despite the fact that an identical plant operating on the same site was

constructed of stainless steel. In this case, either no formal MoC was carried out, or it was ineffective.

- Petrochemical plant (fire) - a change of materials of construction of pipe/fittings from Monel to stainless steel in oxygen service subsequently led to failure two years later. An identical plant alongside the one that failed employed Monel materials of construction.
- Refinery (fire) – failure of column bottoms piping due to corrosion (specified corrosion resistant material of construction appeared to have been changed to carbon steel at some stage during construction and not documented).

5 EMERGENCY ISOLATION

The absence of ROEIVs is frequently cited in loss reports. Whilst in most cases the presence of ROEIVs do not prevent losses, unless they are activated before ignition occurs, their presence, nonetheless, enables loss of containment to be isolated quickly thereby reducing the size of the loss and providing valuable loss mitigation. Many major loss investigation reports cite the absence of ROEIVs as a factor which could have prevented escalation of the initiating event. For 25% of all the losses analysed it could be demonstrated that the absence of ROEIVs resulted in a delay in the isolation or shutdown of the plant, causing subsequent escalation of the event and thereby increased the size of loss significantly. It is suspected that the true figure is probably much higher than this. Examples are as follows:

- Petrochemical plant (fire) - rupture of a propylene fractionator reboiler. The feed to the associated column could not be isolated which caused a major fire to rage for 5 hours before it could be isolated (using manual valves).
- Refinery (vapour cloud explosion) – a condensate pipeline ruptured but operators were unable to quickly isolate the flow from the upstream source.
- Refinery (vapour cloud explosion) – loss of containment within the saturates gas plant resulted in a vapour cloud explosion and ensuing fire. Only battery limit isolation could be made by the emergency response team as no internal process unit isolation was possible. A number of new ROEIVs were fitted after the loss.
- Refinery (fire) – a redundant dead-leg accumulated water, froze and cracked resulting in a high pressure propane fire on the propane deasphalting unit. The rapidly expanding fire prevented field operators from closing manually operated valves but there no ROEIVs. The lack of remote isolation significantly increased the duration and size of fire which impacted a main pipe rack and adjacent process unit.
- Refinery tank farm (vapour cloud explosion) – light ends accumulated and overfilled an atmospheric rundown storage tank during startup operations on the fluidised catalytic cracking unit. The vapour cloud ignited resulting in destruction of multiple tanks and damage to the adjacent piperack and process units. The incident continued for three days due to the inability to isolate the fuel source to the piperack fire.

Guidance on the use of ROEIVs can be found in several sources[16] [17].

6 RECOMMENDED CRITICAL FOCUS AREAS FOR RISK ENGINEERING SURVEYS

As a result of this analysis it is recommended that **insurance risk engineers should focus on the following areas during risk engineering surveys of oil, gas and petrochemical plants.** The list is by no means exhaustive and includes both general and specific focus areas.

6.1 MECHANICAL INTEGRITY

Mechanical integrity, as identified by the MSFs of Inspection Programme and Materials of Construction & Quality Assurance, is by far the most important area to focus on during risk engineering surveys as it is the cause of 43% of all the major losses analysed. Furthermore, 70% of the 'Mechanical Integrity Failure' losses occurred on refineries so is clearly of particular importance for this occupancy. Risk engineers should focus on the following:

- The adequacy of process piping inspection programmes, particularly for internal corrosion but also for corrosion under insulation. Failures due to internal corrosion tend to be more likely in refineries than at other occupancies. A good starting point is to verify that the operator has systematically identified damage mechanisms and Integrity Operating Windows, especially for process piping.
- Ensuring that critical piping which is difficult to inspect (e.g. due to its location) is included in the programme.
- Ensuring that the piping inspection programme allows for uneven corrosion rates within a piping circuit due to the presence of differing materials of construction or localised damage mechanisms.
- Ensure that there is an effective quality assurance and quality control programme in place including PMI during construction and maintenance work of critical piping and fittings[18].
- The implementation of a retrospective PMI programme of installed critical process piping and fittings where the standards of the prior QA/QC and MoC programmes are of unknown or of a questionable standard e.g. when a plant has been acquired from previous operators.
- A focus on bolting of piping and fittings as part of the maintenance and inspection programme, particularly on piping and equipment that is frequently dismantled such as filters, shell and tube heat exchangers as well as pressure relief systems as these often undergo severe mechanical vibration when called into service.

The most effective approach may be via an independent audit of the site inspection programme. Risk engineers are encouraged to make such a recommendation, especially where there are question marks regarding mechanical integrity or there is insufficient time during the survey to assess Inspection.

6.2 OPERATIONS PRACTICES & PROCEDURES

Emphasis during surveys should be on process safety management by operations during infrequent safety critical tasks/transient operations and abnormal or unplanned events, in particular:

- Unit start-up
- Equipment switching operations
- Diagnosing and clearing blockages

- Utilities failure, especially power failure.

It should be ensured that:

- Operations have identified the safety critical tasks associated with these infrequent/abnormal activities e.g. start-up or furnaces and heaters.
- That operating procedures are developed for each including using check lists.
- Additional staffing needs are identified and provided
- That emergency operating procedures are in place covering key scenarios, particularly power failure and emergency shutdown and that operators have sufficient competence and training to implement these procedures.

6.3 PROCESS HAZARDS ANALYSIS

Focus should be on the following:

- Hazard identification of safety-critical transient operational tasks using HAZOP-style techniques.
- The identification of safety critical devices (instrumented systems) as well as other critical devices/IPLs (usually via LOPA studies) and appropriate maintenance and inspection programmes allocated to these critical devices.
- A programme in place for verifying the quality of HAZOP and other PHA studies carried out supported by a clear policy and procedure for the execution of HAZOP and other PHA studies.

6.4 CONTROL OF WORK

Aside from verifying that robust control of work procedures are in place, the focus should be on the following:

- Systematic identification of hazards and their mitigation or elimination by the use of appropriate physical and procedural controls
- Verifying whether site procedures allow remotely operated valves to be used to isolate for maintenance. If so are special precautions should be in place to manage this risk.
- Safe isolation practices during maintenance and "non-standard" operator activities where a safe isolation permit to work might not be required e.g. "operational blinds".
- The control of hot work (contractor management, combustibles, housekeeping, fire watch) in high risk areas such as packed columns.
- Permit to work handback processes including verification of work quality and work area conditions.

6.5 AVAILABILITY OF SAFETY CRITICAL DEVICES

Focus should be on the following:

- Maintenance – ensuring that appropriate ITPM programmes are in place and adhered to with suitable priority attached to any corrective maintenance.
- Control - ensuring that there is a formal, robust system in place to manage the bypassing and disabling of safety critical devices comprising a risk assessment, authorisation and regular reporting of status to senior management
- Bypassing SCDs as part of a SOP

- Ensuring that other “critical” process devices are identified and appropriate Inspection, Testing & Preventive Maintenance programmes developed. Although they might not be formally SIL rated, they still need to be managed as safety critical devices.
- Of high importance is the monitoring of the status of SCDs by issuing dedicated SCD status reports including appropriate Process Safety Performance Indicators (PSPIs) to Senior Management.

6.6 MANAGEMENT OF CHANGE

The focus should be on the following:

- Changes made during construction after HAZOPs have been completed (either prior to mechanical completion or during plant testing and commissioning) as changes made at this stage are sometimes not afforded the same consideration that they would receive during the traditional design-freeze stage.
- The thoroughness of hazard identification studies carried out under an MoC including the decision process regarding whether or not a HAZOP is necessary and the inclusion of all necessary departmental functions e.g. inclusion of the inspection function in the MoC process and HAZOP study when changes are being made to materials of construction
- Changes often not captured by MoC procedures including “non-hardware” changes such as feedstock quality, Operational changes, Catalyst supplier change and Organisational change.

6.7 REMOTELY OPERATED EMERGENCY ISOLATION VALVES

It should be ensured that the site have an appropriate design standard and requirement for installing ROEIVs in new plants and retrospectively in existing plants to enable loss of containment to be isolated quickly.

7 CONCLUSIONS

This study has analysed the causes of 100 major losses in the oil, gas and petrochemical industries. It has focused on major losses, mostly known to insurers, as well as some publically known losses.

The purpose of the analysis is to guide insurance risk engineers on what to focus on during risk surveys in support to the existing Lloyd's Market Association guidance documents for risk engineers[i] [ii.] These documents will be updated, where necessary, to reflect the findings of this study.

Insurance risk engineers are encouraged to adopt the recommendations made in Section 6 of this report to shape and prioritise their risk surveys. It is also hoped that operators of oil, gas and petrochemical facilities will find the results from this analysis useful in their loss prevention and risk management programmes.

8 REFERENCES

[1] Ron Jarvis (Swiss Re, London) and Andy Goddard (Talbot Syndicate, London), *Lloyd's Market Association OG&P IGRES 2015/001 KEY INFORMATION GUIDELINES FOR OIL, GAS & PETROCHEMICAL RISK ENGINEERING SURVEY REPORTS*, May 2015

[2] Ron Jarvis (Swiss Re, London) and Andy Goddard (Talbot Syndicate, London), *Lloyd's Market Association OG&P GRES 2015/001. GUIDELINES FOR THE CONDUCT OF OIL, GAS & PETROCHEMICAL RISK ENGINEERING SURVEYS*, May 2015

[3] Ron Jarvis (Swiss Re Risk Engineering Services), *Oil Petrochemical and Energy Risks Association. London*, April 2015 & IChemE Safety & Loss Prevention Special Interest Group, *An Analysis of Common Causes of Losses in the Oil Gas & Petrochemical Industries*, July 2015

[4] Willis Engineering Loss Database

[5] Marsh, *The 100 Largest Losses. Large property damage losses in the hydrocarbon industry*, March 2016

[6] Jarvis *op. cit. An Analysis of Common Causes of Losses in the Oil Gas & Petrochemical Industries*

[7] American Petroleum Institute (API), *Recommended Practice (RP) 571 - Damage Mechanisms Affecting Fixed Equipment in the Refining Industry*, December 2003

[8] James Reason, *Managing the Risks of Organisational Accidents*, 1997

[9] U.S. Chemical Safety and Hazard Investigation Board, *Final Investigation Report Chevron Richmond Refinery Pipe Rupture and Fire*, 2015

[10] AIG, *Line Blind Valves. The inherent hazards associated with line blind valves and the steps to consider in mitigating the risks. Insight*, 2016

[11] Scott W. Ostrowski and Kelly K. Keim (ExxonMobil Chemical Company*), Tame Your Transient Operations. Use a special method to identify and address potential hazards*, Chemical Processing June 23, 2010.

[12] William Bridges & Dr. Tony Clark, *How to Efficiently Perform the Hazard Evaluation (PHA) Required for Non-Routine Modes of Operation (Startup, Shutdown, Online Maintenance)*, Process Improvement Institute, Inc. (PII)

[13] Energy Institute, *Guidance on human factors safety critical task analysis (1st edition)*, March 2011

[14] Marsh, *Risk Engineering Position Paper No 3. Managing the defeat of safety instrumented trips and alarms,* 2015

[15] Marsh, *Risk Engineering Position Paper No 5. Management of Change*, 2015

[16] American Petroleum Institute, *Recommended Practice (RP) 553 2nd Edition Refinery Valves and Accessories for Control and Safety Instrumented Systems*, November 2010

[17] Health & Safety Executive, *Contract Research Report 205/1999 Selection Criteria for the remote isolation of hazardous inventories*, 1999

[18] Chemical Safety Board (CSB), *Safety Bulletin - BP Texas City, TX Refinery Fire Positive Material Verification: Prevent Errors during Alloy Steel Systems Maintenance*, Oct 12 2006