TURBOMACHINERY & PUMP SYMPOSIA | VIRTUAL
DECEMBER 8-10, 2020
SHORT COURSES: DECEMBER 7, 2020

INTEGRITY MANAGEMENT OF SAFETY CRITICAL ROTATING EQUIPMENT AND SYSTEMS

Girish Kamal
Principal Rotating Equipment Engineer
PETRONAS Carigali Sdn. Bhd.
Kuala Lumpur, MALAYSIA

Girish Kamal is currently working as Principal Rotating Equipment Engineer with the Centre of Excellence Division of PETRONAS Carigali Sdn. Bhd. in Kuala Lumpur. He has more than 30 years of extensive and diversified experience in the Oil and Gas Industry in the fields of rotating equipment management for onshore and offshore applications including specifications, design approvals, witness testing, inspection, commissioning, installation, maintenance and technical services. Prior to joining PETRONAS Carigali, he worked with Dolphin Energy Gas Plant in Qatar as Head of Machinery Reliability, with PETRONAS Carigali in Peninsular Malaysia Office as Unit Head for the Condition Based Maintenance department, with Engineers India Limited as Deputy Manager (Rotating Equipment) and also with Oil and Natural Gas Corporation Limited in India as Executive Mechanical Engineer. He holds a BE degree in Mechanical Engineering and an MBA qualification. He is also a Certified Reliability Professional.

ABSTRACT

Safety Critical Elements (SCEs) are the equipment and systems that provide the basis of risk management associated with Major Accident Hazards (MAHs). A SCE is classified as an equipment, structure or system whose failure could cause or contribute to a major accident, or the purpose of which is to prevent or limit the effect of a major accident.

Once the SCE has been identified, it is necessary to define its critical function in terms of a Performance Standard. Based on the Performance Standard, assurance tasks can be defined in the maintenance system to ensure that the required performance is confirmed. By analyzing the data in the maintenance system, confidence can be gained that all the SCEs required to manage Major Accidents and Major Environmental Hazards are functioning correctly. Alternatively, corrective actions can be taken to restore the integrity of the systems if deficiencies are identified.

This tutorial shall detail out how the MAH and SCE Management process is initiated to follow the best industry practice in the identification and integrity management of major accident hazards as well as safety critical equipment (rotating equipment in particular). The tutorial shall describe in detail the following important stages:

- Identification of Major Accident Hazards
- Identification of Safety Critical Equipment, involved in managing Major Accident Hazards
- Define Performance Standards for these Safety Critical Rotating Equipment
- Execution of the Assurance processes that maintain or ensure the continued suitability of the SCE Equipment, and that these are meeting the Performance Standards
- Verification that all stages have been undertaken, any deviations being managed and thus that Major Accident Hazards are being controlled.
- Analyze and Improve

Through the diligent application of these stages, it is possible to meet the requirements for MAH and SCE Management process giving a better understanding and control of risks in the industry.

INTRODUCTION

Effective management of Technical Integrity of all Assets' is a fundamental part of the business and a key area for continuous improvement across the whole of Organization.

Technical Integrity is defined as follows:
Integrity of an Asset is achieved when, under specified operating conditions, the risk of failure occurring which would endanger the safety of personnel, the environment or Asset value is tolerable and has been reduced to as low as reasonably practicable (ALARP).

The objective of this tutorial paper is to describe a standardized process which is applied during an Asset's Operation phase to:

- provide assurance that the physical hardware barriers (SCEs) are in place and working to prevent initiation or escalation of major incidents or, if they are not, that risks are properly assessed, and mitigation actions taken.
- provide transparency and visibility of the management of SCE performance assurance.
- standardize the processes and use of the available supporting tools.

The term 'SCE Management' covers the method of providing workable, sustainable, measurable and standardized processes and tools to assure the performance of SCEs to demonstrate that these hardware barriers are in place and effective.

The SCE Management process summarized in Figure 1 is divided into six sections, each of which is outlined below and described in more detail later in the tutorial.

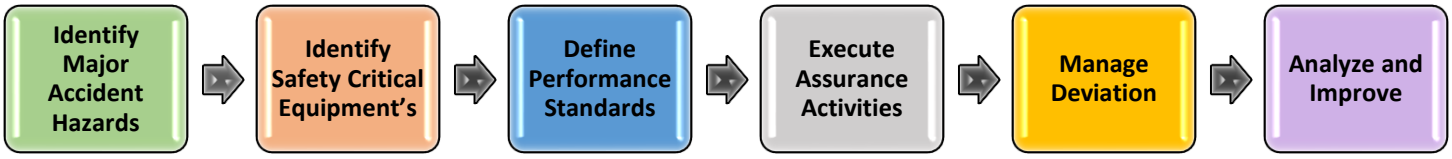

Figure 1 Safety Critical Element Management Process - Overview

1.0 IDENTIFY MAJOR ACCIDENT HAZARDS (MAH)

A Major Accident Hazard (MAH) is typically a hazard that can lead to a low probability, high consequence event which requires a different approach to the occupational, or personal, safety management processes and programmes which are associated with higher frequency but lower consequence events. This is mainly due to the fact that while single failures can cause dangerous occurrences, Major Accidents do not normally happen as a result of a failure of one piece of equipment or one wrong action by an individual. Instead, they are characterized by a series of failures of plant, personnel functions & processes as well as procedures.

Once a major accident happens, upon detailed investigation, it is often noticed that although all the signs of the likelihood of the eventual accident were evident but the operating company and personnel had not been able to recognize this and make the necessary changes to plant, people and processes, which become obvious and natural to do, after such an accident. Only major accidents that have the potential to cause harm from the occurrence of a single, unexpected and unplanned, acute exposure, release or event (e.g. fire, explosion or major environmental impact) shall be considered in the MAH and SCE Management Process. These include:

- Fire, explosion or other release of a dangerous substance involving death or serious injury
- Any event involving major damage to the structure or loss of stability
- Helicopter collision
- Failure of diver systems
- Any other work activity event involving death or serious injury to multiple persons
- Accidents with catastrophic environmental impact Major Accident to the Environment (MATTE events)

The severity of accidents is given in the Risk Ranking Matrix (RRM), shown in Figure 2. MAHs are effectively any incident with a severity level of 5 as well as scenarios considered to be more likely, but with a severity level 3 or 4, i.e. E4, D4 and E3 in Figure 2.

IMPACT		Severity	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophic
		People	Slight Injury	Minor Injury	Major Injury	Single Fatality	Multiple Fatalities
		Asset	Slight Damage	Minor Damage	Local Damage	Major Damage	Extensive Damage
		Environment	Slight Impact	Minor Impact	Localized Impact	Major Impact	Massive Impact
		Reputation	Slight Impact	Limited Impact	Considerable Impact	Major National Impact	Major International Impact
LIKELIHOOD	E Almost Certain	Happens several times per year at location	E1	E2	E3	E4	E5
	D Likely	Happens several times per year in company	D1	D2	D3	D4	D5
	C Possible	Incident has occurred in our company	C1	C2	C3	C4	C5
	B Unlikely	Heard of incident in industry	B1	B2	B3	B4	B5
	A Remotely likely to happen	Never heard of in industry	A1	A2	A3	A4	A5

Figure 2 Risk Ranking Matrix

The above definition of an MAH deliberately excludes occupational hazards. Major Accident Hazards are identified through the use of systematic identification processes, such as Hazard Identification (HAZID) studies, and quantified through such techniques as Quantitative Risk Assessment (QRA). To follow best established industry practice, it is necessary to both identify and quantify the Major Accident Hazards. Major Accident Hazards should be identified in a specific subsection of the asset's Health, Safety and Environment Case (HSE Case) together with the means used to prevent, detect, control, mitigate, rescue or help recover from a Major Accident (which effectively become the Safety Critical Elements). All personnel should develop a level of understanding of how safety is assured through the implementation of the HSE Case. This understanding will help personnel appreciate the importance of the Safety Critical Elements and help understand how they can support and assure safety within their own job roles, bringing benefits in safety to all involved.

All assets need to have an HSE case that identifies the Major Hazards and related hardware barriers necessary for the asset, derived from the Hazard and Effect Management Process (HEMP) which provides the framework for managing the major HSE risks to be tolerable and ALARP, and identify the controls needed to manage the residual risks. During this process, various HSE studies are undertaken and risks identified, minimized and recorded in the risk register which is ultimately recorded in the HSE Case.

Where the HEMP identifies Major Hazards, Bow-Tie models (see figure 3) are required to be developed to:

- Identify the potential Major Hazards release, escalation and consequence scenarios
- Identify the controls i.e. barriers and escalation factor controls, required to effectively manage these hazards to be tolerable and reduced to ALARP.

Barriers shown in Bowtie prevent or reduce the probability of the Threats to cause the Top Event and/or limit the severity, or provide for quick recovery from the consequences of the Top Event. Escalation Factor Controls manage conditions that can reduce the effectiveness of barriers.

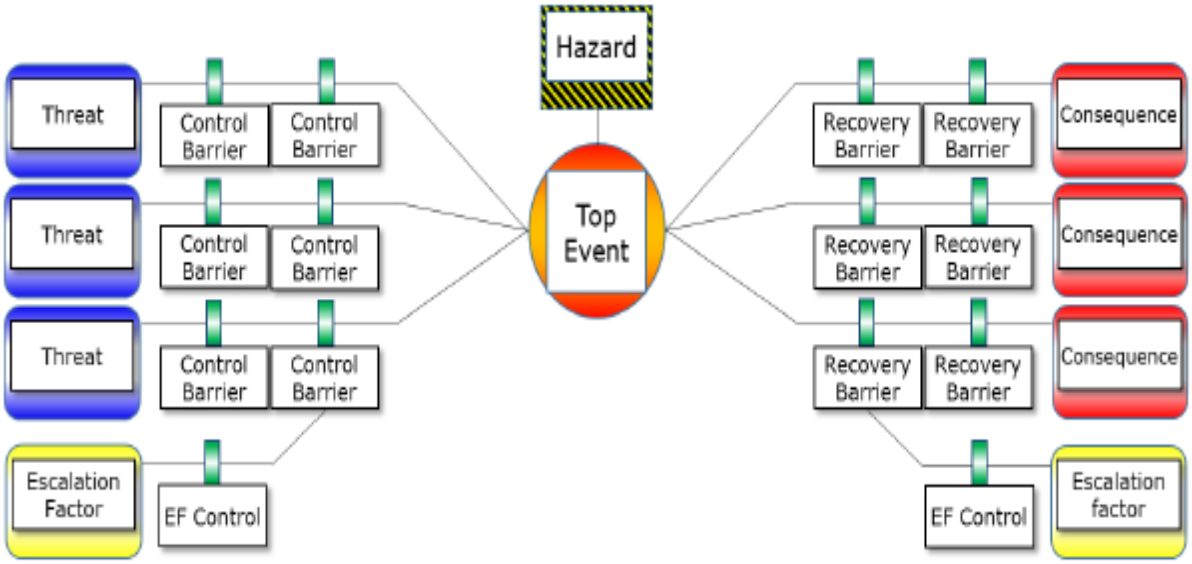

Figure 3 Bowtie Diagram

2.0 IDENTIFY SAFETY CRITICAL EQUIPMENT (SCE)

The key safety plant, systems and equipment required to manage Major Accident Hazards are collectively known as Safety Critical Elements (SCEs). The definition given in the United Kingdom Safety Case Regulations (UKSCR) of a Safety Critical Element is:

"Such parts of an installation and such of its plant (including computer programs), or any part there:

- the failure of which could cause or contribute substantially to; or
- a purpose of which is to prevent, or limit the effect of - a major accident"

Basically, it can be seen that:

- If by failing an item would cause a major accident, then it is to be considered safety-critical
- If by failing an item would significantly add to a major accident, then it is to be considered safety-critical
- If the purpose of an item is to prevent a major accident, then it is to be considered safety-critical
- Finally, if the purpose of an item is to limit the effect of a major accident, then it shall be considered safety-critical.

The concept of Safety Critical Elements is perhaps made easier to understand if they are considered as hardware barriers between the hazard and the consequence of the incident. This is best explained by illustrating the SCEs as eight plant barriers as shown in Figure 4. The holes in the barriers reflect a path or route through which the hazard is realized. This is commonly referred to as the "Swiss cheese model". This pictorial representation is also commonly used in various other Industries than the offshore oil and gas (e.g. Health and Aviation) to illustrate how a combination of failures can lead to an accident event occurring.

Major Accident investigations indicate that such events do not occur because of a single failure of plant or one individual's mistake. It has been consistently demonstrated that for a Major Accident to arise a combination of process, plant integrity and personnel failures needs to happen. This arrangement of processes, plant and people are often referred to as the barriers between a threat being present and an accident occurring. Any one of the barriers can prevent the accident and multiple failures are required before a major accident can happen. It should be noted that the barriers referred to here should not be confused with the barriers referred to in the Bow-Tie process for the identification of individual SCEs. The Barriers here refer to the discrete grouping of SCEs or identified failure mechanisms.

It is not necessary for all eight barriers to fail to lead to a major incident. For example, failure of a single barrier such as structural integrity or process containment or shutdown systems may lead directly to a major incident.

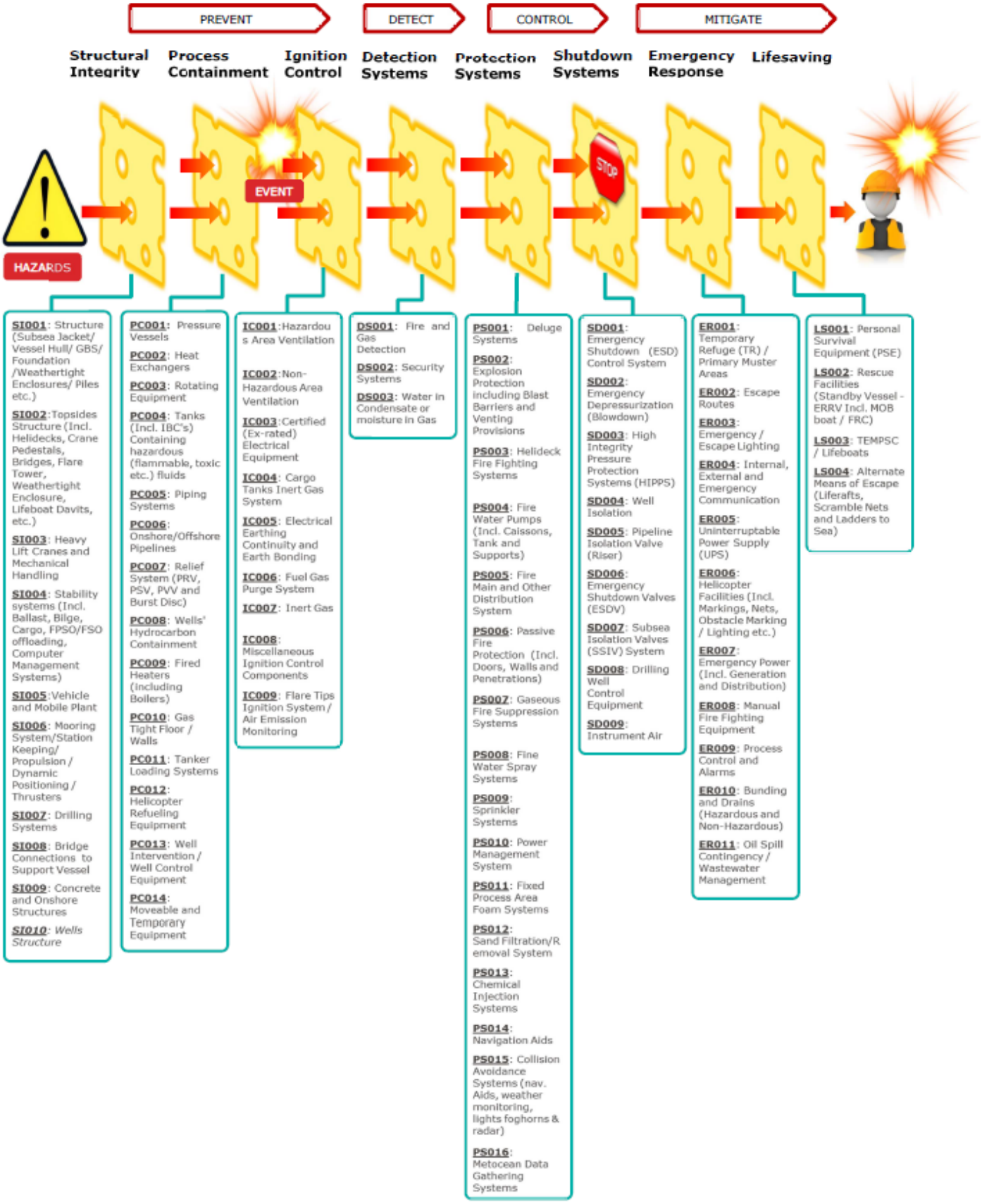

Figure 4 Barrier Groups and typical safety critical elements

In a Major Accident Hazard, each barrier type is represented by one or more Safety Critical Elements and is designed to stop or minimize the effects of a hazard. In a loss of containment of hydrocarbon for example, the barrier types are:

- Process Containment. In this case, keeping the hydrocarbon inside the process rotating equipment e.g. a gas compressor means there is no escalation – the hazard is being managed.

- Detection Systems. If the first barrier fails, then the hydrocarbon is released, and may ignite. It is the job of the detection systems to warn of this event before the hazard can escalate, and initiate controlling measures - allowing management of the hazard.

- Shutdown Systems. The identification and escalation of the hazard (either through the detection SCE, or through the hazard now being self-evident) should then be managed through use of such systems as Emergency Shutdown, and Process Blowdown to minimize the inventory that can fuel the on-going incident.

- Protection Systems. As the event continues, management of the consequences of the incident are being managed through active and passive fire protection (such as deluge, blast walls and fire retardant materials).

- Emergency Response. Should the incident escalate sufficiently, it may be necessary to control the risk to personnel by removing them from proximity to the hazard.

It should be noted that barriers often work in parallel, whether People, Process or Plant and this demonstrates the importance of maintaining the health of such barriers to avoid the initiation and escalation of events leading to Major Accidents. Further, it may be possible for a number of barriers to fail and yet a major accident does not occur. In the Swiss cheese model the hardware barriers are depicted with a number of small holes that represent a design flaw or some potential degradation of their performance. On their own, these degradations may not be significant but, if the holes line up, there may be no effective barriers in place between safe operations and escalating consequences, leading to a major incident. The illustration is used to show the importance of maintaining and knowing the integrity status of all the hardware barriers, so that what might be considered to be relatively small faults in individual barriers do not combine together in an unforeseen manner that compromises the ability of the barriers to prevent or control a major incident.

In the example above in the event of a hydrocarbon gas release i.e. failure of process containment barrier, the ignition control barrier should come into action to prevent a Major Accident. Even the occurrence of multiple barrier failures, such as process containment and detection systems, does not necessarily lead to a major accident if subsequent barriers such as mitigation (e.g. protection systems and shutdown systems) do not fail. The converse is also true however. A loss of process containment involving toxic gas could lead to a major accident event without any other barrier failures, if the area is manned at the time.

Effective barrier performance can be achieved through the adoption of well written Performance Standards; and assurance & verification procedures. These procedures must be adhered to by personnel who are competent in their defined roles in maintaining and assuring the performance of Safety Critical Elements for a specific asset.

2.1 Identification of SCE's for a given MAH

The Oil & Gas industry has had its fair share of disasters and as a result most countries require some form of safety management for their plants. The Bow-Tie Model or Bow-Tie Analysis is considered best industry practice for the identification of SCEs associated with a given hazard. Every SCE belongs to at least one SCE group, the most appropriate of which shall be identified in the Asset Register along with the relevant SCE group reference. In cases where more than one SCE group may be relevant to a single SCE, only one can be assigned in the Asset Register. In these cases, a judgment must be made on the most appropriate SCE group to select. This should take into account the prime function of the item and likely failure modes as well as the maintenance and / or inspection that will be applied to the item and hence how any failure would be detected. For example:

- A process isolation ESD valve could conceivably be safety critical in terms of its hydrocarbon containment role (PC005) and its role as an ESD system end element (SD001). However, its prime role is to be able to close to isolate process inventories and, therefore, the most appropriate SCE group for it to be assigned to would be SD006 (Process ESD valve).
- A certified junction box within a fire and gas system loop could be assigned DS001 fire and gas detection. However, as it is passive in its fire and gas functionality and its most likely failure mode would be of it's EX classification. Therefore, it would be more appropriate to assign it to IC003 (certified electrical equipment). Note that assigning an SCE group in the Asset Register is used only for reporting purposes. It should not preclude any other relevant performance assurance tasks being assigned to the SCE.

The decision tree in Figure 5 can be used to determine SCEs by considering whether the system or equipment is linked to the HSE bow-ties in any way and using the output of any RRM assessments.

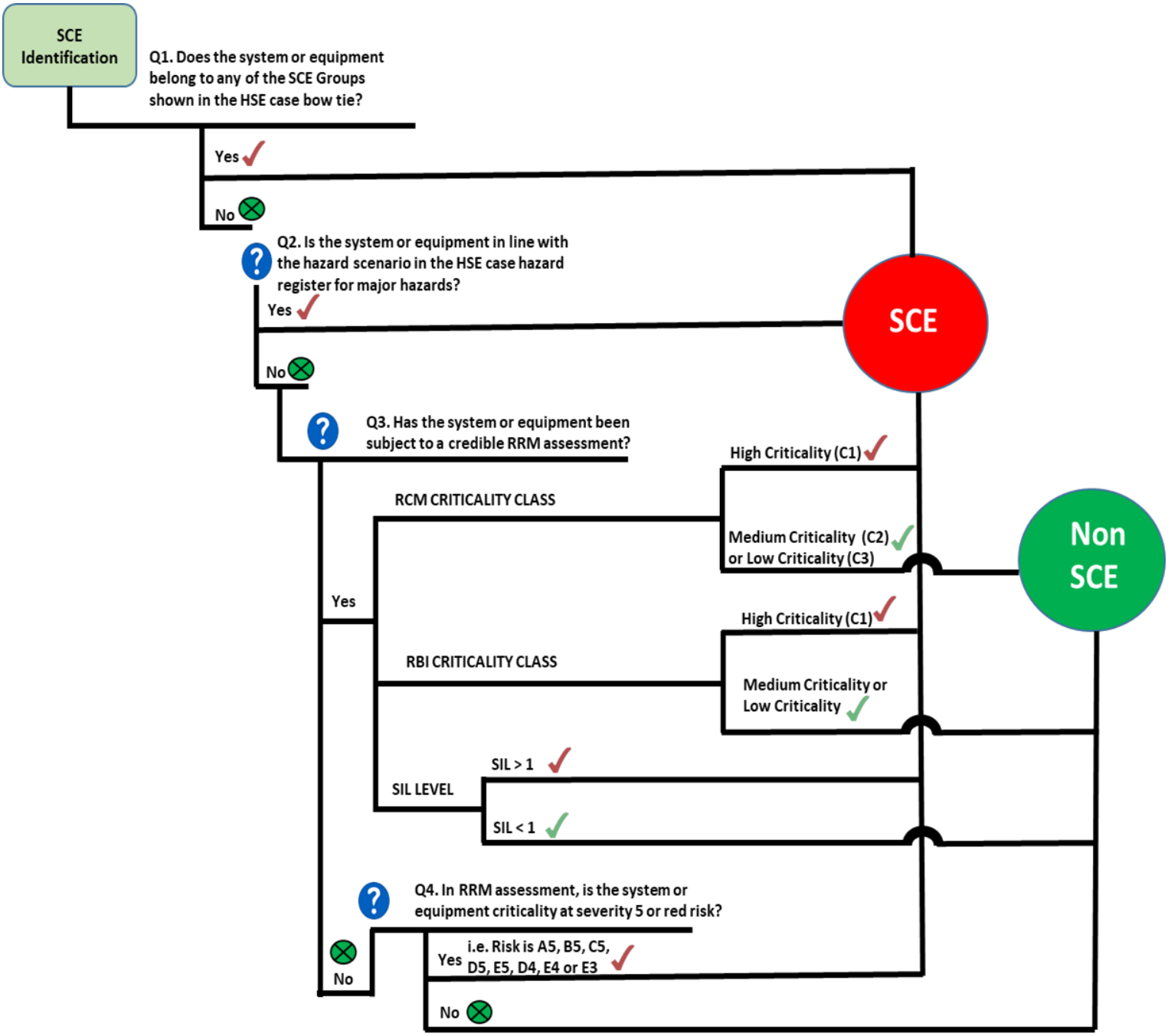

Figure 5 SCE Identification decision tree

3.0 DEFINE PERFORMANCE STANDARD FOR SCE

The next step in the process is the definition of the functions that each SCE is required to perform. This enables confirmation that the SCE is capable of consistently and continuously performing those functions. It has become accepted industry practice that the method of describing what each individual SCE must achieve be defined in a "Performance Standard" which is an Asset specific document. These shall include acceptance criteria that the SCEs must meet and shall be developed in detail to enable the practical verification that all barriers are in place and effective. They are initiated during the asset's define phase and finalized with specific performance requirements and performance assurance tasks during the Execute phase as part of the detailed design. These are the SCE performance standards to be used and maintained during the asset's operate phase. The performance standards should not be confused with either the design specifications required to establish Technical Integrity or the preventive maintenance strategy required for the maintenance of equipment, e.g. lubrication. They specifically cover only the tasks necessary to validate that SCEs perform the function necessary for the barrier to be effective.

The development of Performance Standards is an important element in the MAH and SCE Management Process in order to gain confidence that SCEs will fulfil their intended purpose whenever required, which is achieved by assessing SCEs against the relevant Performance Standard criteria, through Assurance and Verification activities. All the information related to a specific SCE (goal, functionality as well as specific acceptance criteria) are found in the PS and must be captured by the asset-specific PMMS / SAP system. Asset-specific PS should contain measurable acceptance criteria wherever possible.

Performance standards and acceptance criteria are set at anything from a system and / or area to an individual maintainable item. Examples of SCEs at system level are:

- fire detection system
- emergency escape lighting system
- fire water pump system

And at item level:

- pressure vessel containing hydrocarbon
- hydrocarbon process pumps, compressors and turbo expanders
- pipeline emergency valve
- electrical motor operating in a potentially hazardous zone
- Emergency generator

Results are specified as either a yes / no confirmation of an acceptance criteria being met or a specific quantitative measured value. Examples of yes / no confirmation are visual integrity inspection for any unacceptable leaks of produced or non-produced hydrocarbons for a SCE critical system / area and fire water pump functional check. Examples of measured values would be ESD valve closure time or a relief valve lift pressure. It is very important to differentiate between a pass and a pass after fix i.e. to record that a remedial action was required before achieving a successful test.

A suitable Performance Standard need to satisfy all of the following conditions:

- The goal or function of the SCE
- The functional performance requirement for the following criteria: Functionality, Availability / Reliability and Survivability
- Any dependencies on other SCEs
- The pass / fail acceptance criteria by which performance of the SCE will be measured and recorded
- The reference material from which the acceptance criteria should be derived
- Any contingency actions that may be taken into consideration when performance criteria are not met.

An overview of SCEs, their goals and boundaries with typical rotating equipment types is shown in Table 1 below:

TABLE 1 - GUIDANCE ON SCE GOALS AND BOUNDARIES WITH TYPICAL ROTATING EQUIPMENT TYPES

Description	SCE Goal	Typical Equipment Types	System Level/Boundaries
SCE Group : PC003 **SCE Group Title : Rotating Equipment**			
Continued Integrity of rotating equipment (Pumps & compressors) including all fittings and fixtures mounted directly on the equipment and the equipment supports, are vital in the containment of hydrocarbons	To maintain leak tight integrity.	Process hydrocarbon pumps, compressors, turbines and turbo expanders in following services: • oil or gas production, processing, handling and export • condensate / NGL processing, handling and export • gas injection • fuel gas, treatment, heating and distribution • flare scrubber / knock out drum • handling flammable or hazardous chemical • inert gas transfer • gas turbines (including blade	At item level, e.g. per compressor

		containment)	
SCE Group : IC008 **SCE Group Title : Miscellaneous Ignition Control Components**			
Prevention of igniting explosive or flammable atmospheres is a fundamental aspect of ignition control including the provision of facilities to safely contain and dispose of blowdown gas by controlled combustion (i.e. Flare System).	Component installed to minimize the risk of a source ignition in a hazardous area.	• Vent / exhaust flame traps • Anti-static devices, e.g. fan belts • Diesel / turbine exhaust temperature control	At system level
SCE Group : PS004 **SCE Group Title: Fire Water Pumps (Include. Caissons, Tank & Supports)**			
Firewater systems mitigate the effects of fires by cooling exposed surfaces and / or applying foam blankets with water supplied from dedicated pumps.	1. To provide sufficient firewater on demand to extinguish or limit the spread and effects of a fire. 2. To provide cooling to structures and process plant.	Firewater pumping system including Motors, Pumps, Couplings, Starter, etc.	At pump set skid level from intake to inlet into ring main

A complete set of generic PS for the Safety Critical Rotating Equipment is listed in Table 2 below:

Table 2 - OPERATIONAL PERFORMANCE STANDARD AND ASSURANCE TASK – PROCESS CONTAINMENT

SCE Group : PC003
SCE Group Title : Rotating Equipment

FUNCTIONALITY

Functional Criteria	Assurance Task	Minimum Acceptance Criteria	Frequency (Monthly)	Measurable Unit	Verification Task	Supporting documents for verification
1. To maintain the pressure envelope for conditions within design basis.	**Non- Enclosure Equipment** 1.1 Perform Visual Integrity Inspection (Produced Hydrocarbons) There shall be no detectable produced hydrocarbon leaks from the rotating equipment including equipment package pipes & valves, shaft seals or casings. A leak is defined as: GAS: 20% LEL measured at 4" (100mm) "downwind". Seal barrier LIQUID: 4 drips per minute or 1 litre in 24 hrs.	No unacceptable leaks.	03	Y/N	1.1.1 Review the inspection report for both produced and non-produced applicable rotating equipment. 1.1.2 Review the anomalies report and verify that no equipment is operating under unacceptable condition (no unacceptable leaks).	Function tests and inspection reports for rotating equipment and its associated supporting equipment, and PMMS records ● Inspection strategy and leak check records ● Anomalies reports (if any)
	Non- Enclosure Equipment 1.2 Perform Visual Integrity Inspection (Non-Produced Hydrocarbons) There shall be no 'non-produced' hydrocarbon leaks: i. in the vicinity of or onto hot surfaces or ii. Onto lagging or turbine	No unacceptable accumulations.	03	Y/N	Refer to 1.1.1 - 1.1.2 above.	

	insulation. There shall be no unacceptable 'non-produced' hydrocarbon accumulations on equipment base plates. Seal barrier LIQUID: 4 drips per minute or 1 litre in 24 hrs. NOTES: 'Non-produced' hydrocarbons are considered to be: Hydraulic, seal & lubricating oils and liquid fuels. Applicable rotating equipment types = pumps, compressors, turbo expanders					
	Enclosure Equipment **1.3 Perform function test for Safeguarding Detectors of Enclosure Equipment (i.e. IR/UV/Gas Detectors).** The detector shall alarm and operate (i.e. trip the unit) at the correct set point. Cross refers to instrument PPM records and ensures preventive maintenance have been executed as per schedule or approved deviation and records are updated. Applicable rotating equipment types = engines & turbines or equipment that has permanent enclosure Note: This Assurance Task can be executed at a frequency of six (6) months/4K PM as applicable.	Detector alarms and operational.	06 / 4K PM	Y/N	1.3.1 Review a sample of historical flammable gas detector functional test records to ensure that detectors operate in accordance with the correct preset levels and voting logic. 1.3.2 Witness the testing of randomly selected flammable gas detectors to verify alarm set points where opportunity arises.	
	1.4 Perform Seal Protection System Function Test The seal protection system(s) shall alarm and operate (i.e. trip the unit) at the correct set point. Note: a. The Seal Protection System shall be applicable for all the seals for Rotating Equipment that has protection system such as: • mechanical seal for Centrifugal Pumps, • pressure packing for Reciprocating Compressors • dry gas seal for Centrifugal Compressors.	Seal protection alarms and operational.	12 / 8K PM	Y/N	1.4.1 Review a sample of Seal Protection System Function Test records to verify functionality at correct set points.	

	b. The Assurance Task can be executed at a frequency of twelve (12) months / 8k PM as applicable.					
	1.5 Perform Overspeed Trip Protection Function Test The unit overspeed trip protection function shall trip and operate (i.e. trip the unit) at the correct set point. Note: This Assurance Task can be executed at a frequency of twelve (12) months/8K PM as applicable.	Over-speed trip operational.	12 / 8K PM	Y/N	1.5.1 Review a sample of Over-speed Trip Protection Function Test records to verify functionality at correct set points.	
	1.6 Perform Vibration Monitoring Trip Protection (where present) All vibration monitoring protection trip channels shall be operational and effective. Applicable for turbines, compressors & pumps Note: This Assurance Task can be executed at a frequency of twelve (12) months/8K PM as applicable.	Vibration monitoring trips operational.	12 / 8K PM	Y/N	1.6.1 Verify that the detection means are operational and not in bypass mode. Check that periodical CBM is accordingly implemented and records are interpreted to detect onset of failure modes. 1.6.2 Review the Vibration Monitoring Trip Protection records to verify functionality at correct set points.	
	1.7 Perform a Condition Check of Compressor Surge Control System To confirm that the surge control capability is in acceptable condition via: i. Anti-surge control system is in Auto mode ii. No visible alarms on Anti-surge control system iii. Perform anti-surge valve stroke testing including checking valve response time to fully open Note: This Assurance Task can be executed at a frequency of twelve (12) months/8K PM as applicable.	Surge control System in acceptable condition.	12 / 8K PM	Y/N	1.7.1 Verify that Compressor Surge Control System integrity check is being conducted on periodical basis.	
	1.8 Perform Electrical and Fuel	Fuel cut-off valve or mains	12 / 8K PM	Y/N	1.8.1 Verify that all electrical and	

	Driven Rotating Equipment Inspection Check that all electrical and fuel driven rotating equipment is provided with the means to stop the driver if the normal means of stopping fails. Note: This Assurance Task can be executed at a frequency of twelve (12) months/8K PM as applicable.	breaker fitted and functional (emergency stop)			fuel driven rotating equipment is being inspected for fuel cut-off or breaker availability and functionality	
	1.9 Perform Visual inspection on exhaust flexible joint integrity (if applicable). Visual inspection to ensure that exhaust bellows have no cracks, corrosion, leaks or deformation and comply with OEM standards Note: 1. This Assurance Task can be executed at a frequency of twelve (12) months/8K PM as applicable. 2. Inspection standard to determine the level of inspection required for exhaust flexible joint including inspection methods (e.g. NDT needed)	Exhaust flexible joints are in good working condition	12 / 8K PM	Y/N	1.9.1 Perform sample visual inspection on selected exhaust bellows to ensure no cracks, corrosion, leaks, deformation and complies to the design intent, where opportunity arises. 1.9.2 Review PM tasks, PMMS records, inspection checklists and Anomaly management (including reporting, rectification, repair and modification work, by-pass, temporary repairs etc.) where applicable. 1.9.3 Conduct physical spot check on anomaly (where applicable) to confirm quality of rectification.	
	1.10 Perform Visual inspection on Prime mover (e.g. turbine) enclosure to ensure its integrity (if applicable). Visual inspection to ensure that Prime mover (e.g. turbine) enclosure have no holes or leak paths and that the ventilation system is functioning as intended. Verify that doors and associated seals are in suitable condition. Note: This Assurance Task can be executed at a frequency of twelve (12) months/8K PM as applicable.	Prime mover (e.g. turbine) enclosure are in good working condition	12 / 8K PM	Y/N	1.10.1 Perform visual inspection on selected prime mover (turbine) enclosure to ensure its pressurized/ventilated enclosure have no holes or leak paths 1.10.2 Review PM task, PMMS records, inspection checklist and Anomaly management (including reporting, rectification, repair and modification work, by-pass, temporary repairs etc.) where applicable.	

					1.9.3 Conduct physical spot check on anomaly (where applicable) to confirm quality of rectification.	

4.0 EXECUTION OF PERFORMANCE ASSURANCE ACTIVITIES

The SCE performance assurance tasks are carried out in the field and the results are recorded and assessed for conformance with the performance standard acceptance criteria and based on assessment results any follow-up corrective work is identified.

4.1 *Prepare, schedule and execute work*

In this step, the SCE performance assurance tasks are managed through the routine maintenance process in which they are given priority over other preventive maintenance tasks. The objective is to achieve compliance with their Latest Allowable Finish Date (LAFD).

4.2 *Record results*

After the performance assurance task is completed, the Maintenance Personnel shall accurately record the results. During this step, the outcome of the task shall be recorded as:

- "passed" indicating that the SCE has met the acceptance criteria, or
- "failed and fixed" indicating that the SCE did not initially meet the acceptance criteria but a small remedial action was taken to reinstate its performance, which was also recorded in the technical history as a notification, or
- "failed" indicating that the SCE did not meet the acceptance criteria and that follow-up work will be required.

It is vital that the results are recorded accurately and in a timely manner so that the associated risks are known and the need for follow - up corrective work is made immediately visible.

4.3 *Analyze results*

The results of the performance assurance task shall be assessed in order to determine if the performance meets the acceptance criteria. If the outcome is "passed" or "failed and fixed", no further action is required. If the outcome is "failed", it is classed as a non-conformance and shall have:

- a flag in the CMMS
- a follow-up corrective maintenance notification that is raised automatically to rectify the malfunction
- a deviation raised before the LAFD if the follow-up work cannot be completed before that date.

Detailed information about the non-conformance shall also be entered into the follow-up notification to help with evaluating its impact on the Technical Integrity during the deviation management. This information should include details of the condition found and any other relevant information for problem diagnosis. The follow-up corrective maintenance notification shall be prioritized in the daily review meeting as part of the normal maintenance management process with Technical Authority input as required. The priority then sets the LAFD of the follow-up work.

If the follow-up work cannot be completed before the LAFD, a deviation shall be initiated and assessed as detailed in section 5, Manage Deviations, of this paper.

4.4. *Identify SCE performance assurance task backlogs*

When it is not possible to execute an SCE performance assurance task by the LAFD, it shall be identified as a non-conformance by raising a deviation request which is managed as detailed in the Manage Deviations section. This action should take place in advance of the LAFD being approached to ensure the risks of delaying the task are adequately assessed.

5. DEVIATION MANAGEMENT OF SCE

This section describes the management of deviations for assurance and safety critical SCE work orders which cannot be completed before their LAFD. Deviation management involves the assessment of the risks, identification and execution of mitigating actions and close out of the deviation.

5.1 ***Perform risk assessment***
In this step, the OIM or Plant Manager shall ensure that a risk assessment is executed and that mitigating actions are proposed as soon as practicable. During the assessment, it is essential to consider the cumulative risks presented by all deviations as well as the current operating situation, and not just the deviation being addressed at the time.

The assessment shall be reviewed and approved by the appropriate operations and technical persons. The OIM or Plant Manager shall assemble a risk assessment panel typically consisting of the appropriate personnel such as:

• Technical Authority
• Technical Safety Engineer
• Operations Manager
• Engineering and Maintenance Team Leader
• Offshore Installation Manager/Plant Manager.

The minimum information required to review the nonconformance is as follows:

- Details of the equipment concerned - the SCE group and hardware barrier
- The level of performance - the way it has failed.
- The acceptance criteria - the goal
- The implications of the failure - the risks.

Details of the evaluation shall be recorded including the following items:

- Possible escalations resulting from the release of each hazard
- Concurrent activities that were considered
- Constraints or weaknesses in any of the hardware barriers defending against escalation
- Other deviations, which are known at that moment and impact this deviation
- Thinking ‘out of the box’ and ahead for the duration of the deviation
- Mitigating measures proposed with timescales.

The risk assessment shall be formally recorded against the deviation.

5.2 ***Identify mitigating actions***
In this activity, any mitigating actions shall be specified to provide sufficient control over the risks identified in the risk assessment. The mitigating actions can take many forms including:

- temporary operating procedures
- increased operator checks
- increased maintenance, inspection or testing
- temporary repair
- reduction in activities that may increase the risk or demand for the system
- shutdown of the whole or part of the process.

All deviations are temporary and require an expiry date before which the corrective work shall either be completed or the situation reassessed. In the case of all temporary repairs and other non like-for-like changes, a technical specification shall be prepared and approved by the relevant Technical Authority before the deviation review and approval process can continue. The mitigating actions shall be formally recorded against the deviation.

5.3 ***Execute mitigating actions***
The relevant supervisor shall ensure that specified mitigating actions are put and kept in place through their normal work process. In the case of maintenance, e.g. for temporary repairs, this shall be covered by a suitable authorized CMMS work order.

5.4 ***Review and approve deviation***
In this step, the OIM or Plant Manager shall only approve the deviation after verifying that:

- the risk assessment has been completed
- the relevant Technical Authorities have been consulted and their requirements have been taken into account
- the mitigating actions are in place and will remain in place for the duration of the deviation.

At this stage, there is still a non-conformance but it has been approved through the deviation management process. There is an approved and planned intention to operate outside of the normal procedure, standard or specification but the risks have been formally assessed

and mitigating actions have been taken. The OIM or Plant Manager shall ensure that deviations are closed out before their expiry date by one of the following actions.

- Completion of the preventive maintenance task or the corrective repair work
- Formal approval of a change to the SCEs performance standard or the task frequency bringing it into conformance
- Completion of a permanent change to render the deviation obsolete, e.g. permanent bypassing of the equipment approved through the MoC process.

If it is not possible to complete any of these actions by the due date, the situation shall be risk assessed again to determine the appropriate course of action.

6. ANALYZE AND IMPROVE

This section describes the approach to be followed to demonstrate that all the SCEs required to manage Technical Integrity are functioning correctly and that Technical Integrity is being safeguarded. This takes place based on the data available in the CMMS system where the current status of SCE performance assurance tasks are made visible and performance indicators are made available to identify areas for improvement.

6.1 *Status reporting*

A status report shall be available at any time and updated daily to show the integrity status of the Asset. It shall highlight safety critical preventive and corrective tasks required on SCEs that have not yet been completed and for:

- SCE preventive work orders that have:
    - green status - more than seven days until their LAFD
    - amber status - less than seven days until their LAFD
    - red status - exceeded their LAFD without an approved deviation in place.
- SCE corrective work orders that have:
    - green status - more than seven days until their LAFD
    - amber status less than seven days until their LAFD
    - red status - exceeded their LAFD without an approved deviation in place.
- deviations:
    - all deviations listing along with links to related PM & CM tasks.

The status report shall provide an overview of all safety critical tasks for each Facility and include the following drop down and filter capabilities:

- drop down through the Asset hierarchy
- drop down by hardware barrier
- drop down by SCE group
- filter by corrective and preventive tasks
- filter by deviation status (approved/not approved) and by review dates.

6.2 *Review and improve status*

The Scheduler shall ensure that forward looking workload for integrity related tasks are reviewed routinely. Plans shall be put in place to complete them by their due date or approve delays through the deviation process.

6.3 *Facility status*

To ensure that tasks, which have not been completed on time through the proactive approach, are properly addressed, the Facility status report shall be reviewed once per day, usually in the morning meetings. Any new task with a red status shall be identified and the validity of the red condition shall be confirmed with action taken as follows:

- For corrective work, ensure the priority is correctly assessed based on risk using the Corrective Maintenance Prioritization Tool
- Determine if the work is already complete, in which case the order and related notification should be confirmed as complete in the CMMS
- If the work is not complete, line supervisors shall initiate a deviation (see section 5.1) in order to schedule the work to ensure completion and discuss in the daily operations meeting.

It is important to understand the accumulation of risks from multiple ‘red’ items. Therefore, cumulative risk assessments should be undertaken to analyze, characterize, and quantify the combined risks to human health or the environment from multiple ‘reds’.

Effective Asset Integrity Management requires a complete asset register, SCE identified, clear performance standards and continuous online works management. Relationship between PMMS and Facility Status Management (FSM) is shown in figure 6 below:

Figure 6 Relation between PMMS and FSM

6.4 *Performance indicators*

Over time, statistics on the deviation process response time can be used to review where there are bottlenecks in the process and remedial action can be taken accordingly. For this process, the safety critical PM and CM compliance values and trends shall be used as key indicators as to whether the work is adequately under control. This information and snapshots of the Facility status shall be used in Asset Integrity Forums to target improvement.

CONCLUSIONS

SCEs management should be a continuous process throughout the facility life cycle of process industry. Whilst MAH screening starts during the conceptual study, SCE identification should start during the FEED stages of a project.

During detailed design, MAHs and SCEs should be continually assessed and defined as the design evolves. PSs should be developed that include the assurance and verification activities needed to demonstrate SCE suitability initially for the design phase and the assurance and verification activities required for the operate phase.

MAHs may change, especially during the long operation phase. Changes should be considered during regular reviews and evaluation of the performance requirements of SCEs. Optimistic SCE Management Deviation Process controls any deviation related to SCE in order to ensure effective quality assurance and integrity of SCE.

NOMENCLATURE

ALARP = As Low As Reasonably Practical
CBM = Condition Based Maintenance
CMMS = Computerized Maintenance Management System
ESD = Emergency Shutdown System
EX = Electrical Equipment Certified for Explosive Atmospheres
FEED = Front End Engineering Design
FSM = Facility Status Management
HAZID = Hazard Identification Study
HAZOP = Hazard and Operability Study
HER = Hazard & Effect Register
HEMP = Hazards and Effect Management Process

HSE = Health Safety & Environment
IPF = Instrumented Protective Function
LAFD = Latest Allowable Finish Date
MAH = Major Accident Hazard
MATTE = Major Accident to the Environment
MoC = Management of Change
OIM = Offshore Installation Manager
PMMS = Plant Maintenance Management System
PS = Performance Standard
QRA = Quantitative Risk Assessment
RBI = Risk Based Inspection Study
RCM = Reliability Centered Maintenance Study
SCE = Safety Critical Equipment/Element
SIL = Safety Integrity Level
UKSCR = United Kingdom Safety Case Regulations

REFERENCES

- Guidelines for the Management of Safety Critical Elements (SCEs), Third Edition – Energy Institute
- Guidance on applying inherent safety in design: Reducing process safety hazards whilst optimizing CAPEX and OPEX, Second Edition - Energy Institute
- The Offshore Installations (Offshore Safety Directive)(Safety Case etc.) Regulations 2015
- Assurance and Verification Practitioners Guide – STEP change in Safety
- The Public Enquiry into the Piper Alpha Disaster – Lord W Douglas Cullen
- Inspection of Safety Critical Element Management and Verification - HID Inspection Guide Offshore
- American Institute of Chemical Engineers, Global Congress on Process Safety, 2010, unpublished paper “Lessons Learned from Real World Application of the Bow-Tie Method”

ACKNOWLEDGEMENTS

The author would like to thank the management of PETRONAS for authorizing the publication of this tutorial paper