SAFETY CRITICAL ELEMENT (SCE) MANAGEMENT GUIDELINE

EGPC-PSM-GL-007

PSM GUIDELINES

The Egyptian Process Safety Management Steering Committee (PSMSC Egypt)
PSM TECHNICAL SUBCOMMITTEE (PSMTC)

Acknowledgments

This publication has been produced as a result of the comprehensive efforts carried out by the PSM Technical Subcommittee on behalf of the Egypt PSM Steering Committee, formed per the Memorandum of Understanding signed between the Ministry of Petroleum and Mineral Resources and Methanex Egypt in February 2020 overseeing the design and implementation of a detailed PSM program to promote and enhance PSM culture for Ministry of Petroleum and Mineral Resources (MOP) and its affiliated COMPANIES following industry best practice, international codes and standards. The Egyptian Process Safety Management Steering Committee comprises MOP, EGPC, ECHEM, EGAS, GANOPE, and Methanex Egypt representatives.

PSM Technical Subcommittee team members during the project comprised:

Amr Moawad Hassan	**PSM Senior Consultant – Methanex Egypt**	**Team leader**
Mohamed Hamouda	HSE Department Head – Pharaonic Pet. Co.	Member
Ahmed Mostafa	Operations Section Head – ELAB	Member
Ahmed Roustom	Risk Management and Loss Prevention Studies Assistant General Manager – GASCO	Member
Hany Tawfik	OHS & PS General Manager – ETHYDCO	Member
Mohamed Ashraf Aboul-Dahb	Safety Section Head for Upstream – EGPC	Member
Mohamed Mesbah	Operations Department Head – KPC	Member
Mohammed Sabry	Risk Management and Loss Prevention Studies Executive General Manager – GASCO	Member
Sayed Eid	HSE A. General Manager – Agiba Pet. Co.	Member
Tamer Abdel Fatah	QHSE Senior – UGDC	Member

All PSM technical subcommittee documents are subjected to a thorough technical peer-review process during development and prior approval. The PSM technical subcommittee gratefully appreciates the thoughtful comments and suggestions of the peer reviewers. Their contributions enhanced the accuracy and clarity of the documents. The PSM Technical Subcommittee acknowledges the following reviewers from major Process Safety consultants as well as major operators & EPC contractors who provided valuable comments during the technical peer reviews that resulted in an outstanding product structure and quality:

Process Safety Consultant (in alphabetical order):

- Ahmed Omar, Commissioning and Startup Manager (Saipem).
- Exida - By: Greg Chantler, Principal Consultant.
- Process Safety & Reliability Group (PSRG)- By: Robert Weber, President / CEO.

Major IOCs & EPCs (in alphabetical order):

- Shell - By: Yasser Fathy, Asset Integrity Technical Manager.

It should be noted that the above have not all been directly involved in developing this document, nor do they necessarily fully endorse its content.

Egypt PSM Steering Committee team members during the project comprised:

Gamal Fathy	EGPC CEO Consultant for HSE – EGPC	Member
Mohamed Mahmoud Zaki	Executive Vice President – ECHEM	Member
Salah El Din Riad	Q&HSE Chairman Assistance – ECHEM	Member
Dr. Ashraf Ramadan	Assistant Chairman for HSE – EGAS	Member
Emad Kilany	OHS & Fire Fighting Technical Studies GM - EGAS	Member
Mohamed Sayed Suliman	HSE General Manager – GANOPE	Member
Mohamed Mostafa	Inspection & External Audit GM – ECHEM	Member
Mohamed Shindy	Managing Director – Methanex Egypt	Member
Manal El Jesri	Public Affairs Manager – Methanex Egypt	Member
Mohamed Hanno	RC Manager – Methanex Egypt	Member
Amr Moawad Hassan	PSM Senior Consultant – Methanex Egypt	Member
Mourad Hassan	PSM Consultant – Methanex Egypt	Member

DOCUMENT NO. EGPC-PSM-GL-007	TITLE SAFETY CRITICAL ELEMENT (SCE) MANAGEMENT GUIDELINE	ISSUE DATE DEC-2022

Approval

NAME	TITLE	DATE	SIGNATURE
Amr Moawad Hassan	PSM Senior Consultant - Methanex Egypt PSM Technical Subcommittee TL	DEC-2022	Amr Hassan Digitally signed by Amr Hassan Date: 2022.12.29 09:03:40 -06'00'
Gamal Fathy	EGPC CEO Consultant for HSE	DEC-2022	Gamal Fathy

Endorsement

NAME	TITLE	DATE	SIGNATURE
Alaa El Batal	CEO - Egyptian General Petroleum Corporation (EGPC)	DEC-2022	

Copyright

Disclaimer

Controlled Intranet Copy

The intranet copy of this document is the only controlled document. Copies or extracts of this document, downloaded from the intranet, are uncontrolled copies and cannot be guaranteed to be the latest version. All printed paper copies should be treated as uncontrolled copies of this document.

All administrative queries must be directed to the Egyptian Process Safety Technical Subcommittee.

Table of Contents

1. Introduction

This guideline establishes good practices for managing critical safety elements (SCEs). This includes the identification, operation, maintenance, inspection, and testing of the SCEs to assure their operational integrity and to maintain the required protection level of the industrial facilities as per the design specifications or Performance standards. Management should ensure that SCEs are identified and appropriately managed to be in service/operational, healthy, and functioning properly.

In addition to assuring and verifying the initial suitability of the SCEs, all facilities shall have a program of maintenance, inspection, and testing to ensure the ongoing suitability of safety-critical equipment and their respective barriers. A documented process shall also be in place describing the course of actions to be followed in case of one or more barrier impairments. The documented process shall address the risk assessment process required to demonstrate the ability to continue operations, the additional safeguards that may require to be put in place, and how this change in the facility operations will be approved and regularly reviewed.

2. Purpose

The purpose of this document is to define the requirements for managing SCE. This includes the identification of SCE on the system and tag level, defining and ensuring both initial and ongoing suitability of the SCE through the development of SCE performance standards, and the implementation of assurance and verification activities. The document also describes a proposed method to manage SCE impairment, including the development of Operational Risk Assessment (ORA) and cumulative barriers model health status.

3. Scope

This document stipulates the requirements applicable to the Egyptian General Petroleum Corporation (EGPC) and Oil and Gas Holding Companies, including the Egyptian Natural Gas Holding Company (EGAS), the Egyptian Petrochemicals Holding Company (ECHEM), and the South Valley Petroleum Holding Company (GANOPE) covering all of their operational subsidiaries, state-owned companies, affiliates, and joint ventures. ENTITIES and their COMPANIES and contractors shall ensure that all requirements listed herein are fully understood, implemented, complied with, and always monitored, including current operations and existing and future projects during the whole projects' lifecycle from feasibility to decommissioning.

4. Definitions

ASSET REGISTER: An inventory of tangible assets such as buildings, structures, machinery, plant, and equipment.

ASSURANCE: Activities performed by the operating company (1st party) to demonstrate that an SCE meets its Performance Standard. This includes activities in all asset life cycle phases, i.e., to demonstrate initial and ongoing suitability.

CUMULATIVE RISK MANAGEMENT: Proactive management of multiple deviations in Performance and the risks from/associated with them, including their interactions.

DEFERMENT: Delay in carrying out/performing SCE assurance tasks. A type of SCE impairment.

IMPAIRED SAFETY CRITICAL ELEMENT: A critical safety element (SCE) that does not fully meet or may not meet one or more of its performance standard criteria. Impairment includes:

- SCE overdue maintenance, inspection, and testing.
- Failed SCE (not meeting the performance standard criteria).
- Degraded SCE (partial failure to meet its functionality).
- Unavailable SCE (i.e., Inhibits or overrides).

MAINTENANCE MANAGEMENT SYSTEM: Administrative, financial, and technical framework for assessing and planning maintenance operations on a scheduled basis. Often these are computer-based systems integrated with enterprise resource planning (ERP) and called Computer-Based Maintenance Management Systems (CMMS).

MEAN TIME BETWEEN FAILURE (MTBF): Anticipated lapsed time between two consecutive system failures when in operation. Relates to the reliability aspect of the performance standard.

MEAN TIME TO REPAIR (MTTR): Mean time before the item is repaired. This relates to the availability aspect of the performance standard.

OPERATIONAL RISK ASSESSMENT (ORA): Risk assessment carried out for an impaired SCE that aims to identify, if possible, the conditions under which operation of a facility may continue at an elevated MAH risk (such as by implementing additional or different risk reduction measures), and for what period. The scope of the risk assessment should also consider the impacts of the impaired SCE on other dependent SCEs.

SAFETY CRITICAL ELEMENT BACKLOG: List of maintenance, Inspection or Testing work orders of SCE that have passed their planned execution date.

SAFETY CRITICAL EQUIPMENT: Equipment forming part of a broader system that is safety critical, e.g., portable fire-fighting equipment that is part of an active fire protection SCE or

one of many gas detectors that is part of a gas detection SCE that also comprises a control system.

VERIFICATION: Activities that seek to confirm by independent examination, testing, and review of evidence that specified requirements have been fulfilled. In the context of SCEs, these activities seek to confirm whether SCEs will be, and are, suitable or not. These activities are in addition to the operating company's (1st party) assurance processes. They are performed by an independent verifier (often an organization such as a classification society, inspection company (a 3rd party), or an independent person (a 2nd party) within the operating company's organization appointed by the operating company. A verification scheme defines how these verification activities are carried out.

5. Abbreviations

ACP	Asset Care Policy
ALARP	As Low As Reasonably Practicable
BDV	Blowdown Valve
CM	Corrective Maintenance
ESD	Emergency Shutdown
FARSI	Functionality, Availability, Reliability, Survivability & Interdependency
FEED	Front-End Engineering Design
ICP	Independent Competent Person
IOGP	International Association of Oil & Gas Producers
MAH	Major Accident Hazard
MIT	Maintenance, Inspection, and Testing
ORA	Operational Risk Assessment
PM	Preventive Maintenance
PS	Performance Standard
SCE	Safety Critical Element

For other definitions and abbreviations, refer to the PSM Glossary of Definitions and Abbreviations Guideline (EGPC-PSM-GL-011).

6. Safety Critical Element Management Flowchart

Figure 1 provides a logical process flowchart for the activities that should be in place to manage the SCEs. The management process starts with identifying the SCE at a system level until the review of assurance and verification activities for the Safety Critical Equipment are required to assure the initial and ongoing suitability of the SCE. The process also includes managing SCE impairment and reflecting on the cumulative risk figure/model and barriers to health status. Annex A includes SCE management processes along the project life phases.

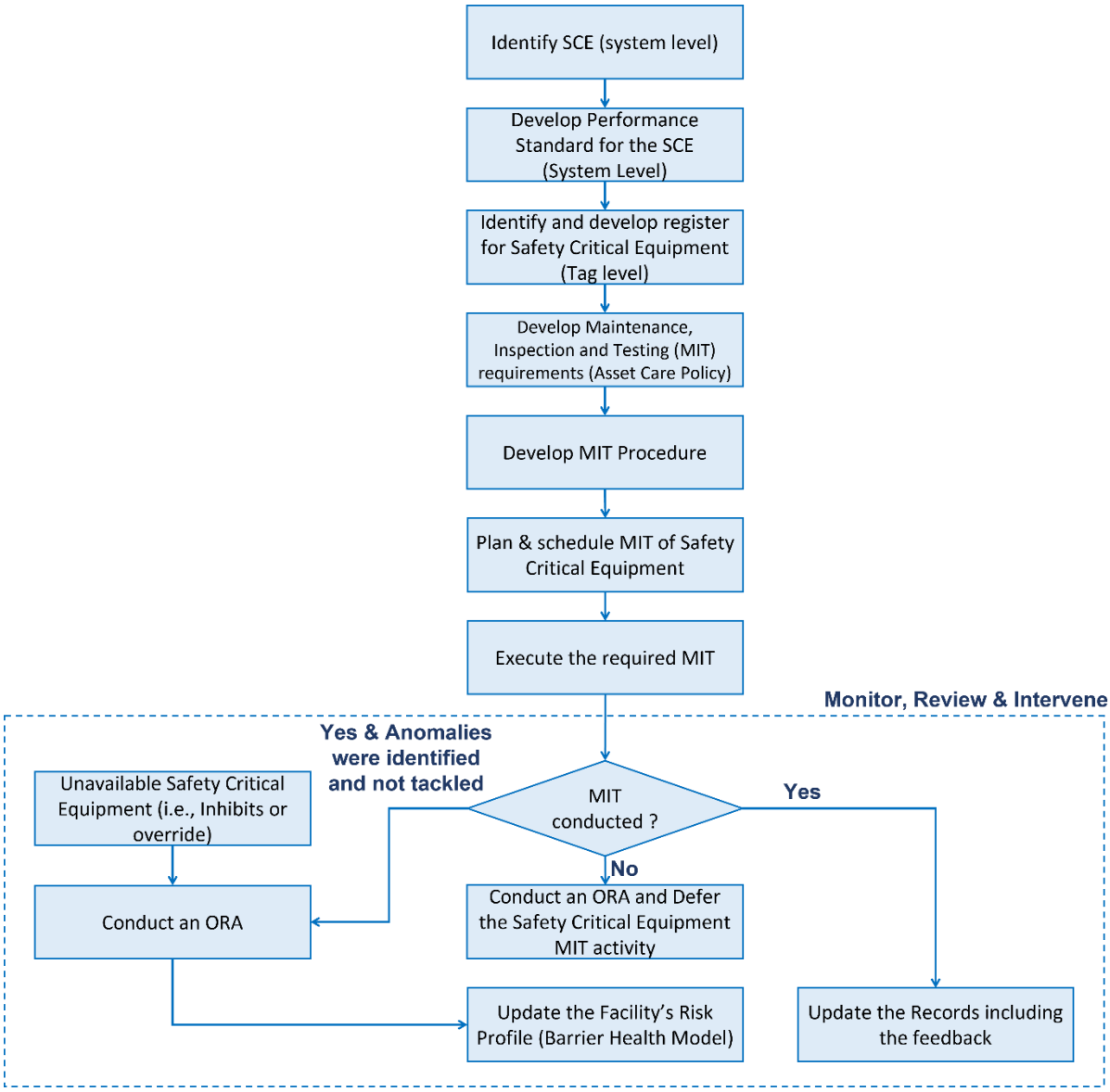

Figure 1. *SCE management process flowchart.*

7. Identify Safety Critical Elements

The starting step in identifying the SCEs is to identify the MAH scenarios. SCE identification should start in the design stages of a project, often FEED; lists of identified SCEs should be refined iteratively through subsequent project phases. Based on IOGP, the hardware barriers implemented by the oil and gas industry for process safety to prevent/control Major Accidents can be broadly categorized under eight hardware barriers:

1. Structural Integrity.
2. Process Containment.
3. Ignition Control.
4. Detection Systems.
5. Protection Systems.
6. Shutdown Systems.
7. Emergency Response.
8. Lifesaving Equipment.

Each barrier is divided into separate systems that form part of the same high-level functional group called Safety Critical Elements (SCEs). SCE is any part of a facility, plant, or computer program, the failure of which could cause or contribute substantially to a MAH or the purpose of which is to prevent or limit the effect of a MAH.

To assure effective SCEs management, a robust and appropriate process for MAH identification and risk assessment should be used. MAH list screening should start in the Evaluation/Concept selection phase. However, this MAH list is refined as the design progresses. Lists of MAHs are then used to identify required SCEs. SCEs should be identified and selected using Bowtie methodology. Refer to Major Accident Hazard Management Guideline (EGPC-PSM-GL-006) for more details about the identification of MAHs and subsequent SCE selection. If the defined SCEs are inappropriate for the MAH they are intended to prevent, control, or mitigate, then there is an increased vulnerability to a major accident.

SCEs fall into one of the following two groups:

- Passive systems (i.e., process containment, passive fire protection, escape routes, etc.)
- Active systems (i.e., Fire detection, ESD, deluge, etc.).

8. Develop Safety Critical Element Performance Standards

Performance standards (PS) shall be developed for each identified SCE. PSs should state the overall MAH management goals (or objectives) of the SCE. Using these goals, designers and risk specialists should be able to assess and define the required function and level of performance of the SCE during the design stage.

PS sets out the performance levels SCE must achieve in terms of functionality, availability, reliability, survivability, and interdependency (FARSI). This ensures that the critical barriers remain in place and effectively continue to manage the Major Hazard over time.

Performance Standard document shall include:

- The levels of Performance that SCE must achieve.
- The assurance activities required to meet the required Performance.
- The verification activities are required to assure assurance activities' implementation and meeting performance criteria.

SCE performance criteria usually remain appropriate for all facility life cycle phases, but SCE assurances and verifications are not fixed and change with the facility life cycle phase, such as:

- Design: engineering calculation and analysis.
- Project implementation (procurement, fabrication, construction, and commissioning): equipment type testing and commissioning performance testing.
- Operation: inspection, maintenance, and testing.

Therefore, PSs for establishing initial suitability may differ from those used to assess the ongoing suitability of SCEs; hence, separate PSs should be developed for initial and ongoing suitability for the same SCE. Refer to Annex B for more details about Performance Standard development.

9. Identify Safety Critical Equipment– Tag Level

The next step is to identify the SCE on the tag level. For the sake of differentiation, the SCE on the tag level will be referred to as "Safety Critical Equipment." Therefore, Safety Critical Equipment is the equipment forming part of a broader safety-critical system, e.g., one of many gas detectors that is part of a gas detection SCE.

Before starting up the operation, the facility should ensure that all Safety Critical Equipment is identified, listed, and included as part of a comprehensive, structured asset register listing all assets and work equipment at each location and within each area of operation. Each Safety Critical Equipment should be uniquely identified and easily identified on the asset register.

Identification of SCE at the tag level is not simple. Typically, an item of Safety Critical Equipment could be the 'child' of a system already identified as an SCE, but it does not follow that it is an SCE itself. The failure of an individual item (Equipment) within a system will not necessarily stop the SCE from performing its functional role. The following decision-making principles (see Figure 2) could be applied to ascertain whether an item or equipment is a safety critical itself:

- Does the Safety Critical Equipment/component item belong to an SCE system (i.e., as a child of an SCE)?
- Will the failure of the Safety Critical Equipment/component item prevent the SCE from meeting its performance standard?

The facility should ensure a common understanding of which equipment should be considered safety critical. The decisions for the inclusion and/or exclusion of equipment as "safety critical" should be suitably and formally documented inside the facility.

If this analysis is not done, there will be far too many or too few Safety Critical Equipment. If there are too many, some may not strictly meet the criteria of being safety-critical, and this may mean that some receive unnecessary assurance effort causing potential detriment to those that are safety critical.

Every Safety Critical Equipment belongs to at least one SCE group/system, all to be identified in the company's asset register along with the relevant SCE group/system reference. In cases where more than one SCE group may be relevant to a single Safety Critical Equipment, only one can be assigned to the asset register. In these cases, a judgment must be made on selecting the most appropriate SCE group. For example, a certified junction box within a fire and gas system loop could be assigned fire and gas detection. However, as it is passive in its fire and gas functionality, its most likely failure mode would be related to its EX-design. Therefore, assigning it to certified electrical equipment would be more appropriate. Assigning an SCE group in the asset register is used only for reporting purposes. It should not preclude any other relevant performance assurance tasks from being assigned to the SCE. Effective SCE assurance during the operating phase depends on the alignment between the asset register and the Performance Standards.

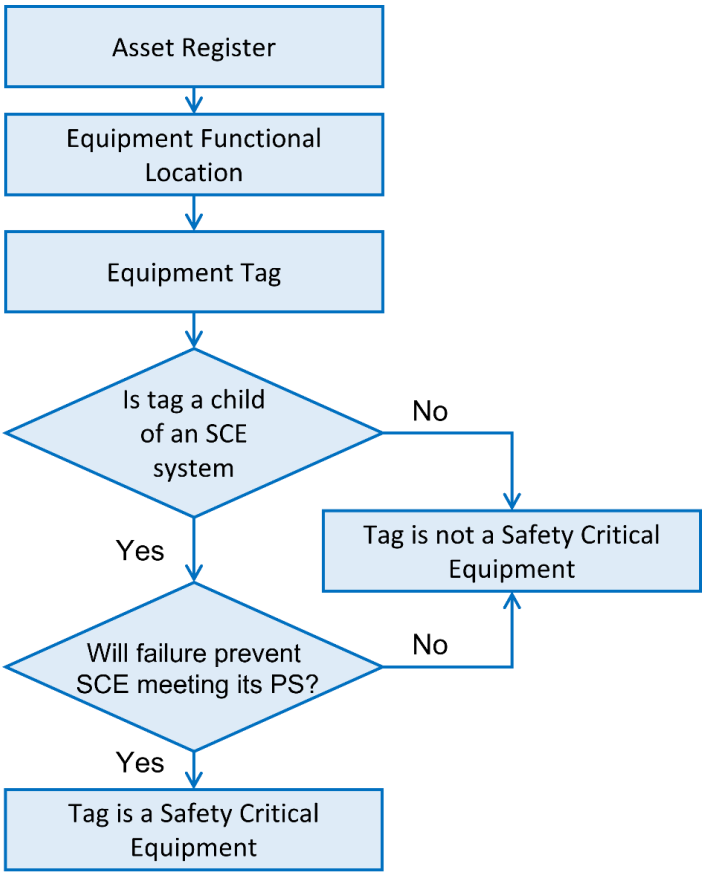

Figure 2. *Safety Critical Equipment decision-making process.*

10. Develop Maintenance, Inspection, and Testing Requirements

The company shall develop maintenance, inspection, and testing requirements/Asset Care Policies (ACPs) for each identified Safety Critical Equipment to ensure their ongoing suitability during the operation phase. This ACP should adopt risk management principles to define the appropriate equipment care approach and specific maintenance, inspection, and testing interventions necessary to deliver the required level of performance/reliability from each Safety Critical Equipment. It should establish the most appropriate balance between 'run to failure,' 'condition-based,' and 'time-based' interventions.

A generic ACP will likely cover several identical or similar equipment in many cases. In these cases, the team developing the ACPs should consider the type of equipment and the operating environment when deciding whether it is appropriate to develop a generic ACP to cover a class of Safety Critical Equipment.

In the initial stages of implementation, extensive use will likely be made of generic ACPs; however, although the degradation mechanisms are likely to remain the same across a class of equipment, the failure consequences may differ depending on how it is used. With time, as more comprehensive testing, inspection, and maintenance history develop for each Safety

Critical Equipment, it may be possible to differentiate the likelihood of failure. This will allow ACPs to be optimized for each identified Safety Critical Equipment.

It is important to ensure that the ACP complies with legislative requirements and requirements from the company and industry standards. SCE Performance standard documents shall be considered while the development of the ACPs to ensure that maintenance and testing meet the requirements of the SCE performance standards.

11. Develop Maintenance, Inspection, and Testing Procedures

Based on the ACPs, procedures (or work packs) should be developed for SCE maintenance, inspection, and testing to assure a consistent approach and achieve maximum efficiency and effectiveness from the available technical and planning resources.

When a procedure or work pack is developed for maintenance, inspection, and testing, it will assemble or reference many different sources of information. Sometimes, this information may have to be developed from the basics.

In addition to these procedures and work packs, there may be other reference information such as basic Safety Critical Equipment records, specification sheets, parts lists, drawings, maintenance procedures, vendor manuals, and Safety Critical Equipment maintenance, inspection, and testing history. It should be decided what information is required, how it will be stored and maintained up to date, and how it will be made available.

This reference information may be assembled on an ongoing basis as procedures/work plans/ packs are developed, or it may be appropriate for the resource to be assigned to address this as a specific initiative. The choice of approach will typically be based on the current status and accessibility of the required reference material.

12. Plan and Schedule Maintenance, Inspection, and Testing

Planning the work activities should identify how the work will be carried out and develop the work packs, which should put everything required to execute the work safely, efficiently, and fully.

The work pack for Safety Critical Equipment maintenance, inspection, and testing might contain a risk assessment and a procedure incorporating the necessary control measures to maintain a tolerable risk during the period that the Safety Critical Equipment is bypassed or defeated for testing, inspection, and maintenance. The work packs should define the feedback required from the execution group to carry out the work.

Whereas the plan should set out how the work will be carried out, the schedule should set out when it will be carried out (start, finish, and duration) and who will carry it out. The schedule also provides a means of coordinating activities, forecasting and optimizing resource requirements, and understanding the overall business impacts of the planned activities.

Sometimes, Safety Critical Equipment maintenance, inspection, and testing activities address the frequency of testing and the type of test to be carried out (e.g., proof, function) but not how that testing should be done. The result is that technicians may only have their standard competence to do the testing (e.g., electrical), but there is no recognition of its limitations when applied to SCEs.

The planning and scheduling of the maintenance, inspection, and testing of Safety Critical Equipment should be coordinated with other activities which may be planned on the same assets or using the same resource groups. It should be ensured that the work plans and schedules are reviewed and agreed upon with the line managers/supervisors/technicians who will be required to execute them.

Any amendments to job plan or work order scheduling frequency shall be controlled to ensure that any effects of extending or increasing maintenance intervals are fully understood and risk assessed. The maintenance management system should be configured with the SCE assurance activities before implementing SCE integrity assurance activities, during the Construction/ Commissioning / Start-Up phase, and before the operate phase.

13. Execute Required Maintenance, Inspection, and Testing

If work is effectively planned and scheduled, its execution becomes a matter of ensuring everything goes to plan, i.e., ensuring that all identified testing, inspection, and maintenance activities are completed in full, on schedule, and in line with the plan.

The people carrying out the work should be appropriately briefed, and everything should be set up in line with the plan.

It will also be necessary to address any issues arising from work, such as:

- The management of emergent work is identified by the testing, inspection, and maintenance activities.
- The resolution of any deficiencies in the plan. In this case, it should be ensured that the plan is updated to correct these deficiencies and improve its efficiency for future use.

Following the completion of maintenance, inspection, and testing work, the necessary feedback should be provided. Specific feedback requirements should be defined in the work pack for each activity. Typically, this feedback will include the following:

- As found condition.
- As a left condition.
- Performance against the plan.
- Performance against schedule.

It should be ensured that the equipment history is updated and reviewed to incorporate the feedback from execution. Some active SCEs may have insufficient recorded data to demonstrate whether the PS criterion is being met. For this reason, operations personnel should record the 'as found' condition and any details of SCE repairs needed to achieve the required PS. For example, if an ESDV had to be stroked (and greased) several times during routine testing to close it properly, but it did not close properly several times during routine testing, and this wasn't recorded and acted upon by the implementation of a long-term remedy, the fault could recur and potentially impair the SCE's functionality.

Responsibility for maintaining and updating records should be clearly defined inside the facility. The records and information should be held in a defined and agreed place(s) to ensure they are easily accessible.

In cases where it is necessary to delay scheduled maintenance, inspection, and testing of Safety Critical Equipment, this should be formally deferred using a risk-managed approach, tracked appropriately, and approved by personnel with the required level of authority.

14. Review Feedback from Maintenance, Inspection, and Testing

The company should ensure that the feedback from maintenance, inspection, and testing is monitored, analyzed, and regularly reviewed to identify the following:

- Necessary modifications to ACPs:
  - Increase inspection or maintenance intervals – where the as-found condition is as or better than expected.
  - Reduction of inspection or maintenance intervals or a revised intervention – where the as-found condition is worse than expected.
- Bad actors/poor performing Safety Critical Equipment:
  - Poor performing equipment where there is a justification (issue or opportunity) to change the inspection and maintenance approach or upgrade the assets/work equipment to reduce the cost.
- High-cost inspection or maintenance interventions where there is a justification (opportunity) to change the inspection/maintenance approach or upgrade the Safety Critical Equipment to reduce the cost.

Identified requirements for improvement should be assessed to evaluate the justification, priority, and feasibility. Where justified, the improvement should be developed and implemented in line with the company's MOC process.

15. SCE Impairment Management

An impaired safety critical element is an SCE that does not fully meet, or may not fully meet, one or more of its Performance Standard criteria. SCE Impairment includes:

- SCE overdue maintenance, inspection, and testing.
- Failed SCE (not meeting the performance criteria).
- Degraded SCE (partial failure to meet its functionality).
- Unavailable SCE (i.e., inhibits or overrides).

The identification of SCE impairment may result from any of the following circumstances/ processes:

- Through observation during routine plant operations and maintenance activities.
- While conducting SCE assurance activities.
- During verification witness testing.
- An unplanned event that reveals SCE impairment.

Impairment of the SCE increases the conditional probability of failure to prevent, detect, mitigate, or control a major accident event or impedes evacuation, escape or rescue, or could also increase the potential consequences of an event.

It should be ensured that appropriate risk assessment is carried out for any SCE impairment, applying appropriate compensating control measures and review and, approval by authorized persons. The Safety-Critical Equipment is there to prevent an unsafe condition from developing. Suppose it is impaired while the asset or work equipment designed to protect it is in service. In that case, it should be ensured that there are appropriate alternative robust controls in place to ensure that the risk of an unsafe condition developing is managed to a tolerable level.

The company should decide who will have delegated management authority to approve the impairment of Safety Critical Equipment and maintain an up-to-date list of these delegated authorities. In parallel with the management authority, there should be a list of technical authorities. Approval to impairment should require authorization by both a technical and management authority.

The risk assessment and the demonstration of suitable mitigation measures should be a requirement to gain formal approval for safe continued operations of the facility when not complying with Performance Standards, e.g., deviation from the Performance Standard or deferment of Safety Critical work orders beyond their scheduled compliance dates.

The requirement to perform a risk assessment is prompted by any scenario in which a barrier is identified as unavailable, degraded, or failed or where assurance activities are deferred. These scenarios maybe:

- Overrides or inhibits on Safety Critical Equipment:
  Suppose any Safety Critical Equipment is inhibited or over-ridden. In that case, it will fail to perform some/full part of its safety-critical function, e.g., the Safety Critical control loop is inhibited for testing purposes. A risk assessment should be performed to assess the risks where any Safety Critical Equipment is over-ridden or inhibited, and suitable risk mitigation measures should be established.

- Deferral of SCE assurance:
  Maintenance, inspection, and testing activities provide assurance of SCE and hence the barrier effectiveness. All backlog (deferral) of planned assurance activities on SCEs should be risk assessed. Based on the associated risk level the related maintenance, inspection, or testing activity may be authorized for deferral for a specified interval. In all cases, a request for deferral must be issued and present adequate justification for deferment. Where it is agreed that the risks and implications of the deferral are acceptable, the deferral request form shall be circulated to the relevant level for endorsement. The new execution date should be reflected in the maintenance planning program and hence the assurance activity will not be counted in the SCE backlog. All approved deferrals should be recorded on a deferral register. In the case that the maintenance deferral is deemed unacceptable, the request form shall be rejected.
- Deviation from the Performance Standard (Failure or Degradation):
  The failure of an SCE to meet the specified performance standard may be disclosed by planned assurance activities (i.e., testing) or by an actual demand on the system (such as a shutdown event). All requirements for corrective maintenance of the element to restore full effectiveness should be considered in a formal risk assessment.

In some cases, impairment of the SCE will trigger a MOC, so the companies should define the situations where the MOC process shall be followed, i.e., long-term isolation of an SCE longer than six months. Isolation of safety-critical equipment shall be managed through the company's safe work practices, including using an isolation certificate, even during turnarounds.

16. Operational Risk Assessment (ORA)

The company's procedures for risk management need to be dynamic to accommodate and account for adverse changes in Safety Critical Element provision, conditions, or other abnormal situations that may potentially increase levels of major accident risk. This dynamic

approach to risk management takes several forms and has various titles applied to the processes. In this guideline, the term Operational Risk Assessment (ORA) will be used.

The application of the ORA process commences at facility start-up and continues throughout the Operate and Decommission stages. The most common trigger for ORA is the identification of impaired SCE. Other triggers include the up-normal operational situations and changes to the organizational capability that may compromise the facility's safe operation.

Each company should develop, maintain and implement ORA procedures that guarantee a systematic and effective approach to operational risk management such that:

- A thorough assessment of Major Accident Hazards associated with SCE impairment or other abnormal operational situations is carried out. Risks are identified and evaluated; effective risk control and mitigation measures to manage risks arising from impaired SCE are properly identified, documented, implemented, and monitored.
- Steps are taken to ensure that interdependent SCE or other control measures associated with or affected by the ORA are adequate, available, and fully functional or being managed/controlled under a separate ORA.
- The assessment and documented outputs are reviewed, endorsed, and approved by relevant technically competent personnel.
- Awareness of the abnormal conditions and changes arising from an ORA is maintained and monitored until permanent remediation/ restoration of SCE performance is completed.
- There is a reliable basis / good reasoning for operational control and decision-making.
- Permanent remediation of impaired SCE or recovery actions from the abnormal situation is identified, prioritized, and tracked to closure in an appropriate time scale.
- Operational risk management processes are managed and executed by suitably competent personnel.
- All ORAs is presented and reflected in the facility cumulative barriers health model.

Operational risk assessment is one element of a wider suite of management system elements, processes, and practices to manage Major Accident Hazards. As an example of interdependence, impaired SCE may be revealed by integrity management activities, and remediation of the impairment will become part of the maintenance management or action management systems.

It is particularly important to stress that the application of task risk assessment procedures, criteria, and guidewords focusing on personal injury outcomes only is inappropriate in Operational Risk Assessment (ORA).

Clear routes and levels of authority must be specified and adhered to for the review, endorsement, and approval of documented operational risk assessments. Levels of authority should reflect and align with the assessed risk levels of the impaired SCE.

Relevant personnel must be aware of operational risk assessments and associated changes to SCE Performance. Personnel such as Process Operators, Control Room Operators, and Emergency Response Team members should be made aware of changes and any new or additional actions that may be required by them or others as part of ORA mitigation measures. Annex C includes more details on the ORA development process.

17. Cumulative Risk Profile and Barriers Health Model

The cumulative risk profile process provides an overview of the overall operational risk that results from the combined impairments to more than one barrier at the facility. The objective of the cumulative risk profile is to provide a means to assess the ongoing effectiveness of the barriers, their systems and equipment, and the increase in the baseline level of risk resulting from failed, defective, or untested barriers.

Determining if the barriers can perform according to their performance standards is based on information gathered from maintenance, inspection and testing, independent verification activities, periodic safety case/process hazard reviews, and a knowledge of other activities affecting the barriers, such as inhibits or overrides.

Gathering this information and assessing the potential or actual impact on barrier effectiveness will provide oversight of the potential increases in major hazard risk that a facility is subject to during operation and provide a reliable basis for operational decision-making and control.

It is a pre-requisite for the development of the cumulative risk profiling and barrier health model that the following are implemented and functioning effectively:

- Applicable Major Accident Hazards scenarios are identified.
- Barriers required to manage risks associated with these hazards are identified.
- The minimum acceptable performance standards for these barriers are documented.
- The performance standards requirements are integrated into the management system and form the basis for the planned maintenance, inspection, and testing of the barriers at the facility.
- A clear procedure describing the processes for operational risk assessment of impaired barriers is in place.

The Major Accident Hazard Management Guideline (EGPC-PSM-GL-006) provides detailed guidance on identifying barriers. Figure 3 below shows the generic barrier model for managing process safety-related hazards.

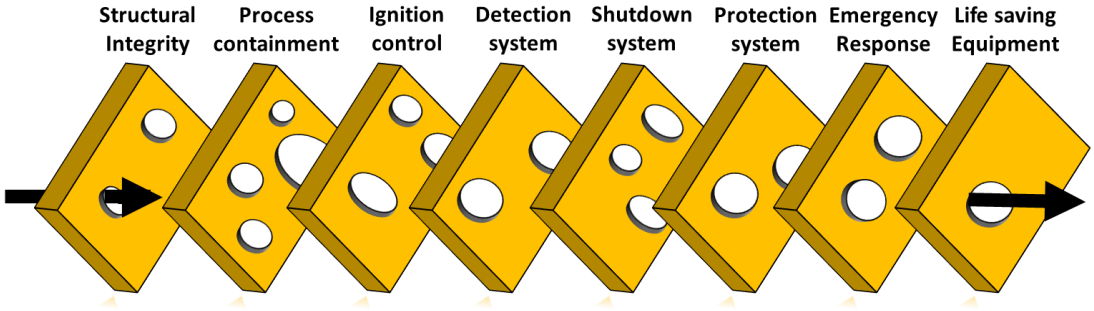

Figure 3. *Barrier model.*

When the specific barriers have been identified and agreed upon, they can be represented in a visual model similar to that shown above. This can provide the basis for a visual representation of the overall barrier effectiveness for a facility.

Barriers' integrity is assured based on three key elements:

- Design and build integrity.
- Sustain integrity.
- Operate with integrity.

Each of these three elements should be considered in determining the overall effectiveness of the barriers; however, the three elements may not all be reviewed on the same timescale.

17.1 Design and Build Integrity

During the design stage, the objective is to build integrity by identifying and specifying the barriers that will manage the risks. This is typically achieved by compliance with codes and standards and suitable risk assessment studies conducted at the design stage on how the barriers will deliver a facility that can operate with As Low-risk levels As Reasonably Practicable (ALARP) and is documented in the facility design Safety Case.

However, once the facility commences operation, there is a need for periodic reviews to ensure that circumstances at the facility have not changed such that new hazards exist, or risks associated with existing hazards have not increased. Therefore, EGPC requires Safety Case thorough Reviews (5 yearly), which will involve Process Hazard Reviews, and HAZID & HAZOP activities as appropriate.

Collectively, these reviews ensure that the facility's design is still suitable to deliver a level of risk that is As Low As Reasonably Practicable (ALARP). The reviews should identify missing barriers required to manage specific hazards or deficiencies in the design of the existing barriers. As a result of these activities, some re-design, modification, replacement, or

upgrading of barriers may be required to reduce the risk if it is reasonably practicable to do so and to meet the EGPC's barriers adequacy criteria.

Before this work is completed (which may take some time if facility modifications are required), the barrier model would be used to show which barriers are deficient and document the ORAs and mitigation measures that need to be put in place until the work is complete. The model would also show any ongoing operational issues on the same barriers.

17.2 Sustain Integrity

The condition of barriers can refer to their physical state of repair or ability to function per their performance standard. Information on this aspect can be gathered from maintenance systems and the routine inspection and monitoring activities associated with day-to-day operations.

The barrier model should be updated to show the effects of actual barrier failures, whether on a test or because of actual demand. Consideration should be given to the impact of any overdue maintenance, inspection, or testing activities on the level of confidence the operator has in the barrier's effectiveness; the barrier model should be adjusted accordingly.

17.3 Operate with Integrity

Assessment of barrier effectiveness should consider how the barriers are being operated about their normal and safe operating limits on a day-to-day basis. The impact of any deviations from these limits or any known inhibits or overrides that are in place are a vital input to this assessment.

The assessment of barrier effectiveness should involve the personnel responsible for operating or maintaining barriers; consideration of the personnel involved with the operation or maintenance of barriers is required where resource requirements may be compromised regarding personnel availability or adequate competence.

Finally, assessing the barriers should consider the quality and completeness of the input information required and, where there is a lack of suitable information, make allowance for this when considering the current barrier effectiveness.

Based on the Operational Risk Assessment's risk ranking, each barrier can be classified based on its current effectiveness/condition (ability to meet the performance standard) and the mitigation measures in place. The classification can be represented visually in the barrier model using a simple color coding, such as traffic lighting (Red, Amber, and Green).

Where the barrier is considered fully effective (no impairments, inhibits, or deferred assurance activities), it will be classified as green. A risk assessment will be carried out as described above for any barrier that is not fully effective. The effectiveness of the barrier should be assessed on an initial and residual basis, with the difference between the initial and

residual risk ratings being attributed to the quality (e.g., effectiveness, reliability, assurability/robustness) of the agreed interim risk mitigation measures that are applied.

Based on risk ranking, where the initial risk shows a significant increase above the design baseline level and where the mitigation measures are only partially effective in reducing the risk (such that there is only a small difference between the initial and residual risk rating) then this may be the basis for the barrier to be classified as red.

For the same scenario, if the mitigation measures are effective at reducing the risk (creating a significant reduction between the initial and residual risk rating) and where the mitigation measures can be readily assured, then this may be the basis for the barrier to be classified in the amber category.

Figure 4 illustrates the barrier model showing hypothetical barriers' health status, considering the initial risk figure and residual risk figure, after applying the mitigation measure. This barrier model could be presented to the senior management and site management on a suggested monthly basis.

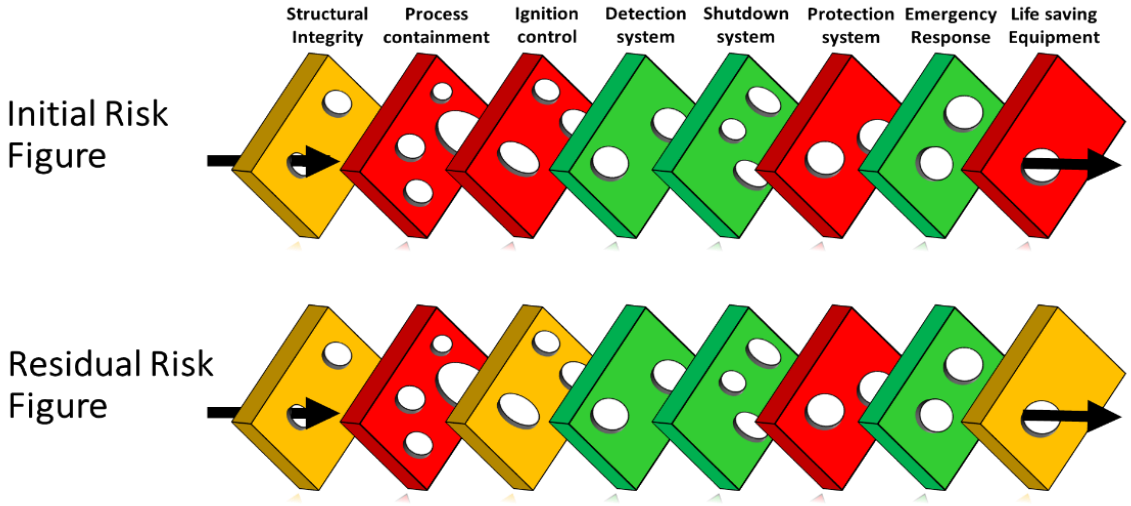

Figure 4. *Barriers Health Status-Example.*

It is important to note that the barrier model supports decision-making by assessing a facility's overall operating risk. Still, the relevant personnel must make the decisions in the facility based on the information available – the process itself has no means to indicate or dictate the actions that should be taken, or the risk reduction measures that should be employed – it cannot indicate if the risk of continued operation is tolerable or not.

Frequent reviews of the barrier model should be carried out in the asset to ensure the validity of the information used and establish the "everyday use" of the tool as a 'business as usual' practice. Those involved in the review process must take prompt action based on the evolving information and not wait for the situation to escalate.

Everyone involved in the review process is responsible for intervening and challenging the information and decisions made. Using a cumulative risk barrier model correctly should allow the early identification of potential threats, prompting the correct conversations and timely intervention to ensure that developing risks are effectively managed.

Facilities should consider the following frequencies and drivers for assessing the barrier conditions using the cumulative risk model:

- In the event of significant change, as deemed by a technical expert and technical support functions.
- Weekly as part of ORA reviews conducted by the facility-based team.
- Biweekly through functional support roles, including technical experts and technical asset authorities.
- Monthly through a combination of asset senior management and site management as part of process safety and asset integrity governance review.

Figure 5 shows the relation between cumulative risk and ORA.

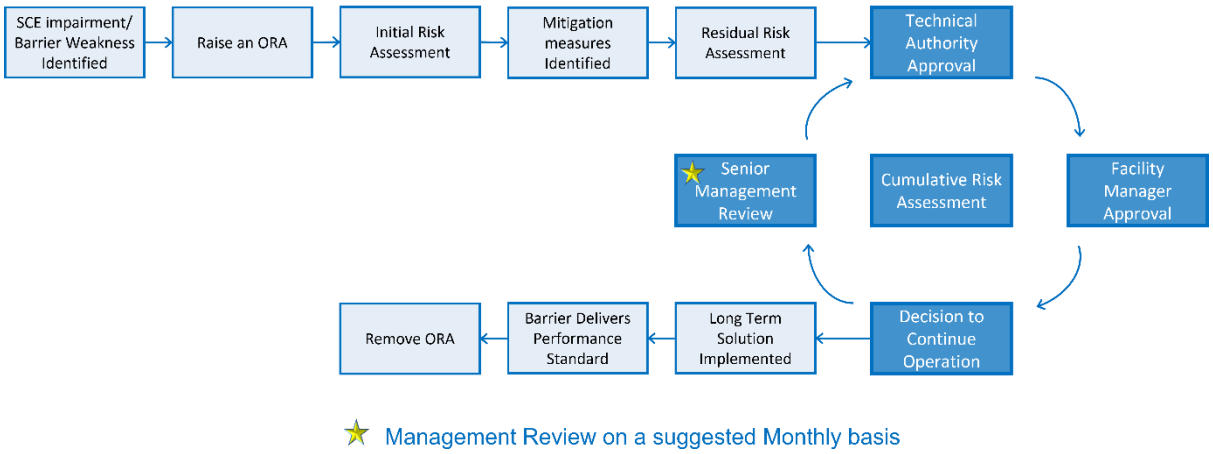

Figure 5. *Typical cumulative risk and ORA process map.*

18. Managing Temporary Equipment

Introducing temporary equipment may create new hazards or impact existing risk assessment assumptions. Procedure for introducing temporary equipment should be developed is a key requirement to assess any impacts upon SCEs. Procedure should define how any temporary risk reduction measures will be managed. For example, introducing a transportable/mobile air compressor creates a potential ignition source, which may coincide with potential hydrocarbon releases to affect the likelihood of ignition of hydrocarbon release / realizing the MAH consequences.

If temporary equipment is:

- Part of an SCE.
- An SCE itself (e.g., demountable drilling equipment not permanently held on an E&P facility).
- Impacts on an existing SCE, either due to its:
  - Planned location on the facility (e.g., an engine-driven transportable air compressor or skid-mounted temporary generator required to operate in a designated hazardous area).
  - Proposed application (e.g., well intervention equipment once it becomes part of the reservoir pressure envelope).

Then, temporary equipment proposed introduction should be subjected to the MOC process. If appropriate, it should be included in the asset register of the maintenance management system, have a PS, and be subjected to SCE assurance.

19. Safety Critical Equipment Criticality

Within the identified SCEs, some companies prefer to be further criticality ranking. The main purpose of ranking the criticality of SCEs is to manage the equipment inventories and to decide the size, type, and frequency of the verification activities.

There are various methods of evaluating SCE criticality. The example method described in Annex E allocates scores based on the following factors:

- The MAH management functional role of the SCE (prevention through to emergency response).
- The consequence of the failure of the SCE.
- The extent to which an alternative SCE can take over the function of the SCE in the event of its failure or its unavailability, and/or whether the SCE has inherent redundancy (i.e., defense in depth).

20. References

[1] Energy Institute, “Element 16: Management of Safety Critical Devices”, Energy Institute, 2015.

[2] British Gas, “Cumulative operational risk assessment”, British Gas, 2012.

[3] Energy Institute, “Guidelines for management of safety critical elements, Energy Institute”, 2020.

[4] Egyptian General Petroleum Corporaton (EGPC), “Major Accident Hazard Management Guideline (EGPC-PSM-GL-006)”, EGPC, 2021.

[5] Oil & Gas UK, “Guidance on the Conduct and Management of Operational Risk Assessment for UKCS Offshore Oil and Gas Operations”, Oil & Gas UK, 2012.

21. List of Annexes

- **Annex A -** SCE Management Through the Asset Life Cycle.
- **Annex B -** Performance Standard.
- **Annex C -** Operational Risk Assessment (ORA).
- **Annex D -** Example for the ORA and Cumulative Barrier Model.
- **Annex E -** SCE Safety Criticality Ranking.

Annex A - SCE Management Through the Asset Life Cycle

During the facility's life, the integrity of SCE is established by the project team and safeguarded by the operating team. Table A1 shows the points at which key deliverables in the SCE management process are completed against each phase of the facility life cycle.

Table A1. *SCE Management activities across the facility life cycle.*

Evaluation / Concept selection	Basic Engineering /FEED	Detailed Engineering	Construction/ Commissioning / Start-Up	Operate
1. SCE Management Activities				
Initial analysis of MAHs	Formal MAHs Identification Bow-tie analysis Identify, group, and describe the extent of SCEs and identify interactions Develop SCE Design PSs Define design Phase assurance and verification measures	Refine MAHs Re-check Bowties Refine SCE identification Implement design phase assurance activities	Implement the assurance in procurement, fabrication/ construction, and commissioning and control deviations Develop SCE Operations PSs Define operate phase assurance and verification measures Define Safety Critical Equipment in the asset register Configure and implement SCE-planned inspection, maintenance, and testing in a maintenance management system	Implement operation phase assurance activities (inspection, maintenance, testing) as per PSs Identification and remedy of failures, degraded performance, deviations, and deferred assurance activities Control deviations through MOC Report on SCE performance Review MAHs and manage changes, including to SCEs
2. SCE Verification Activities				
	Review MAHs Review the SCE selection methodology and list	Review MAHs Review the SCE selection methodology and list Review the suitability of PS FARSI criteria	Review the initial suitability of PS FARSI criteria Review SCE performance and condition	Review critical function tests and maintenance Review SCE performance and condition

The wide verification process could be carried out through the facility's life cycle. The verification part inside the standard performance document does not cover the whole verification process to verify the initial and ongoing suitability of the SCE. Table A1 presents some other verification activities, including the performance standard verification activities.

An Independent competent person shall carry out verification activities. During the project phase to verify the initial suitability of the SCE, verifications are carried out by an independent person from outside the company. During the operation phase, verification of the assurance activities carried out on the SCE could be done by personal from inside the company independent from those carried out the assurance activities.

Annex B - Performance Standard

B.1. Performance Standard FARSI

The performance standard is a mandatory document for each SCE identified to manage a Major Accident scenario. Table B1 illustrates a proposed template for the performance standard considering FARSI criteria.

Table B1. *Performance standard template.*

SCE Name	
Reference	
Revision	
Goal	
Scope/System boundaries	
Project Phase	

Functionality			
Function	**Criteria**	**Assurance**	**Verification**

Availability

Reliability

Survivability

Interdependency	
PS	**Criteria**

Performance Standards goals should be taken as the starting point for building the PS in terms of functionality, availability, reliability, survivability, and independency (FARSI) criteria:

1. **Functionality:**
   - What the SCE is required to do concerning MAH management.
   - The SCE functionality aspect of the PS should define the appropriate performance to enable management of the pertinent MAH safety risks such that they meet a defined risk criterion, such as ALARP.
   - Functionality criteria may cover a wide range of performance requirements, e.g., the functionality of a firewater system SCE may cover the delivery rate, the

quantity of fire-fighting water, and the response time to deploying the fire-fighting water.

- Functionality criteria may have associated limits (e.g., for temperature or pressure) under which the required Performance should be able to be delivered with confidence. Outside such criteria, the functionality may be undermined.

2. **Availability:**
   - The proportion of time that the SCE is required to be capable of performing its function on demand.
   - Availability is affected by the need to maintain the equipment, either planned or unplanned. This may be stated as, e.g., unavailability of [number] hours per annum, indicating whether the SCE will be ready to function when required. Most SCEs should always be available. Availability typically is described in terms of mean time to repair (MTTR).
   - If an SCE is being maintained and is out of use, an operational risk assessment (ORA) should be raised if this is for a significant period.
3. **Reliability**
   - The allowable failure rate of the SCE (or conversely, the likelihood of the SCE performing on demand).
   - In the operating phase, reliability targets should apply to active SCEs operating on demand in direct response to a MAH through either automatic or manual initiation, e.g., an ESDV actuation. As well as initiating, the SCE may need to function for a further period.
   - Reliability targets should cover all aspects of detecting, deciding, and acting, which may necessitate consideration of human reliability (e.g., whether a control room operator will correctly diagnose a plant deviation) before the operation of the SCE.
   - Typically, reliability targets should be defined for SCEs such as ESDVs, F&G detection systems (including individual detectors), firewater pumps, emergency lighting systems (and individual luminaires), safety-critical systems such as instrumentation and temporary refuge heating, ventilation, and air conditioning (HVAC) systems (e.g., for dampers to close and fans to stop). For system-based SCEs, there may be different reliability targets for the SCE and individual equipment items.
   - Reliability targets should be measurable such that corrective action can be taken if the target is not achieved. Reliability is typically described as the mean time between failure (MTBF).
4. **Survivability**
   - The MAHs that the SCE can survive and still perform its functionality.
   - The survivability criterion should only apply to SCEs that need to function after a major accident (by providing mitigation and reducing the effects of the event).

- The SCE may need to survive events such as fire, blast, collision (e.g., ship impact), adverse weather, dropped objects, etc.
- Examples of survivability include:
  - Support structures that enable escape and evacuation routes to remain in use.
  - Firewater deluge system withstanding a defined blast overpressure.
  - The pressurized enclosure that protects people from toxic gas ingress is defined as blast overpressure and thermal radiation.
  - Pressure relief system that reduces the hydrocarbon inventory that otherwise provides fuel for a jet fire.

5. **Independency**
   - Interfaces with other systems (usually also SCEs) required to function at the same time or those upon which the functions directly depend.
   - The independency criterion considers both the Interactions and dependencies.
   - 'Interactions' refers to interfaces of an SCE with other systems, which usually are also SCEs.
   - Examples of interactions for an emergency power supply SCE are:
     - Active Fire Protection – emergency power supply SCE provides power to the fire pumps, and
     - Emergency shutdown and blowdown system – emergency power supply SCE provides power to the ESD system.
   - 'Dependencies' refers to the degree of reliance of the SCE on other systems (usually SCEs) to perform its function. A common cause failure (CCF) is where several SCEs are impaired due to one failure mechanism – these are not independent and should be considered a combined system. The diversity of SCEs (passive and active) should reduce the risk of common mode failure.
   - Examples of dependencies for an emergency power supply SCE are:
     - Hydrocarbon containment – to provide fuel for the emergency power supply's generator.
     - Temporary Refuge – to house the essential equipment of the emergency power supply.

B.2 Defining Performance Standard (PS) Criteria

To establish PS criteria, a clear hierarchy of preference should be used, such as:

- Applying national and international design and construction technical publications (e.g., codes, standards, and good industry practice) where risk is relatively well understood. A good practice is a minimum requirement in demonstrating ALARP for

new facilities, and it should be considered with existing facilities to enable compliance with EGPC requirements.

- Risk assessment is when no appropriate technical publications are available, a good practice is not well defined, and there is uncertainty or complexity, so there should be a specific study or analysis.
- Precautionary approach, where there is excessive uncertainty or complexity, even after completing a risk assessment. The application may be innovative.

PS criteria should identify the source information (e.g., a specific standard). PS criteria should be quantitative (e.g., time, pressure, temperature) so that the performance criteria are unambiguous as regards whether SCEs pass/fail (e.g., not 'no excessive corrosion') and they facilitate measurement of actual SCE performance (e.g., creeping degradation)

Quantitative PS criteria should include the pertinent units, e.g., a quantitative functionality criterion for firewater pumps in an Active Fire Protection system may be: each firewater pump shall deliver a minimum acceptance flow of [volume] m3/hour at [pressure] barg within [number] minutes of actuation at [location].

However, other functionality criteria may be qualitative, e.g., firewater pumps shall be capable of being started by two independent means – manually from the local control panel or automatically via the emergency control system per relevant cause and effect (C&E) analysis.

For a passive SCE system, qualitative criteria only may be appropriate in the operating phase; e.g., a firewall may have a design-based duration (e.g. [value] minutes), but this cannot be measured in the operating phase. Instead, a visual degradation criterion may be all that can be declared (e.g., no visible cracks of size greater than [value] dimension).

The setting of reliability performance should be based on robust and achievable data. This should be based on the actual achieved reliability performance of the SCE for the pertinent facility using data in the maintenance management system if the facility is operational or, more generally, from a database within the operating company for similar facilities. In the absence of a representative data population (e.g., facility not yet operational, infrequently tested SCEs or small population), other means should be considered to define the reliability performance, such as using industry reliability databases, e.g., OREDA. Reliability performance targets are inappropriate for passive systems such as sub-structures or Passive Fire Protection.

B.3 Performance Standard Assurance Activities

SCE management typically comprises desk-based and facility-based assurance activities. Assurance requirements shall be stated in the performance standard for each SCE. Those requirements differ for the initial and ongoing suitability of the SCE.

Performance Standard assurance requirements in the design phase should focus on the design quality and adequate design specifications, procurement, fabrication/construction, and commissioning. These SCE assurance activities should be carried out to ensure the initial suitability of SCEs.

During the operating phase, SCE assurance activities should focus on ensuring the ongoing suitability of SCEs through maintenance, inspection, and testing.

The performance standards should not be confused with 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.

B.4. Performance Standard Verification Activities

Verification refers to activities that seek to confirm by independent review, examination, testing, and review of evidence that specified requirements have been fulfilled. In the context of SCEs, verification seeks to confirm whether SCEs will be, or are, suitable.

Verification should be carried out throughout the life cycle of a MAH facility. The scope of verification activities differs during the facility life cycle to verify the initial and ongoing suitability of the SCE.

A suitable mixture of verification activities, such as review of records, visual examination of equipment and witnessing of critical function tests, may achieve verification of SCEs.

For each PS requirement, there should be at least one verification activity to demonstrate whether the PS requirement is being met. Each verification activity should state whether it is performed by review, examination, or witnessing and the frequency of the verification process.

The verification activities in the design phase for SCEs usually comprise one or more of the following generic activities to assess whether they are initially suitable:

- Review performance standard criteria.
- Visual, physical examination of equipment procured vs. a procurement register, fabrications, construction.
- Witness and/or review factory acceptance tests, review construction records (e.g., material certification, welding, non-destructive testing (NDT), pressure testing, etc.), and examine and witness hook-up, installation, and commissioning at site.
- Verification during start-up.

Verification activities during the project phase are usually conducted by an independent competent person (ICP) from outside the company.

The verification methods for SCEs in the operation phase usually comprise one or more of the following generic activities to assess whether they are suitable:

- Review assurance records to assess the robustness of assurance processes.
- Witness and review critical function tests.
- Visual physical 'as found' examination of SCE hardware condition vs. that stated in maintenance management system records.

Operations phase verification activities could be done by the second or third part, from inside the company, independent from the department carrying out the assurance activities.

The frequency of verification activities during the operation phase should depend on factors such as:

- The overall risks of the facility's operation.
- The extent and frequency of the operating company's inspection and maintenance of different SCEs.
- The relative risk associated with failure of each SCE on MAH risks.
- The findings of previous verification activities.
- Confidence in the operating company's assurance processes.

Below is an example of the firewater SCE in the operation phase for a company (x), including the minimum requirements for the firewater pump operations performance standard. The performance standard is facility-specific, so this example is only for illustration purposes. Reference: NFPA25 Fire pump's Maintenance, Inspection, and Testing requirement.

SCE	Diesel Firewater Pump
Reference	PS16
Revision	[01/Oct. 2022]
Goal	The purpose and role of the SCE in major accident hazard management throughout its lifecycle.
Scope/system boundaries	Diesel firewater pump, including engine, daily diesel fuel tank, and batteries.

Functionality			
Function	**Criteria**	**Assurance**	**Verification**
Fire Pump Capacity: About NFPA20:2022 section 4.10.1, a centrifugal fire pump for fire protection shall be selected so that the greatest demand for any fire protection system connected to the pump is less than or equal to 150 percent of the rated capacity (flow) of the pump.	The fire pumps shall provide a flow rate of 681 m3/hr. at a discharge pressure of 11 barg.	**Fire Pump Weekly Inspection(s).** Do weekly inspections. The inspection shall cover the following: 1. Pump house conditions. 2. Pump system conditions. 3. Electrical system conditions. 4. Diesel engine system conditions. Reference: NFPA25:2020 Section 8.2.2	Per the maintenance plan, confirm by review of assurance records that the firewater pump support systems have been checked. (6 Months)
		Fire Pump Flow Testing(s): Conduct Annual test of each constant speed pump assembly. Reference: NFPA25:2020 Section 8.3.3	Witness the annual pump flow test. Ensure that the test is conducted by qualified personnel and the results are satisfactory. (Annual)
		Carry out maintenance, inspection, and testing for the fire pump per NFPA 25 and manufacturer recommendation. Reference: NFPA25:2020 Section 8	Ensure that CMMS's maintenance plan covers all NFPA requirements stated in appendix A. (Annual) Per the maintenance plan, confirm by review of assurance records that the firewater pump support systems have been checked. (Annual)
Each fire pump shall start on demand from Initiation signals.	The fire pumps shall start upon receipt of the start signal from: - Local Panel Pushbutton - F&G Panel, Pushbutton /Confirmed Fire detection - Fire Main Pressure Switch	**Weekly run test to the pump:** It is not necessary to test all three during each test performance, but the testing regime shall ensure all start signals are tested equally.	Witness the weekly pump run test. Ensure start options are included in the test instructions. (Annual)

Functionality			
Function	**Criteria**	**Assurance**	**Verification**
Pump's Engine: Diesel engines for fire pump drives shall be listed for fire pump service.	Diesel engines for fire pump drives shall be listed for fire pump service.	**Weekly Run test for fire pump (no flow):** Engines shall be designed and installed so they can be started no less than once a week and run for no less than 30 minutes to attain normal running temperature. Reference: NFPA25:2020 Sections 8.3.1.1/8.3.2	Witness the weekly pump run test. Ensure compliance with the test steps, including the minimum run time for the engine. (6 Months)
		Carry out maintenance, inspection, and testing for the Diesel engine system as per manufacturer recommendations and NFPA requirements. Reference: NFPA25:2020 Sections 8.5/Table 8.1.1.2	Ensure that the CMMS maintenance plan covers all manufacturer recommendations and NFPA requirements stated in appendix A. (Annual)
Fuel supply tank: About NFPA 20:2022 Section 11.4.1.3.1, Fuel supply tank(s) shall be sized for a minimum of 12 hours of engine run time-based on the fuel supply rate requirements of the engine, plus 5 percent volume for expansion and 5 percent volume for a sump.	Fuel supply tank(s) shall be sized for a minimum of 12 hours of engine run time based on the fuel supply rate requirements of the engine, plus 5 percent volume for expansion and 5 percent volume for a sump.	**Weekly inspection:** Ensure that the fuel tanks are kept as full as practical but never below 66 percent (two-thirds) of tank capacity. Reference: NFPA25:2020 Section 8.2.2(4)	Reviewing assurance records confirms that the pump's diesel fuel tank capacity has been checked per the weekly inspection plan. (Annual)
		Diesel Annual degradation test: Carryout degradation test for diesel fuel no less than annually. Reference: NFPA25:2020 Section 8.3.4.1	Ensure the CMMS maintenance plan covers the annual degradation test and confirm its implementation. (Annual)
Engine's Batteries: Refer to NFPA20, sections 11.2.7.2.1 and 11.2.7.2.5: • Each engine shall be provided with two storage battery units • Two means for recharging storage batteries shall be provided.	Each engine shall be provided with two storage battery units. Two means for recharging storage batteries shall be provided. One method shall be the generator or alternator furnished with the engine. The other method shall be an automatically controlled batter).' charger taking power from an ac power source.	**Batteries Annual check:** Carry out the annual check for batteries. Reference: NFPA25:2020 Section 8.1.1.2.15	Ensure that CMMS's maintenance plan covers the annual battery check and that the work instructions cover the NFPA requirements. (Annual)

Availability
No single pump shall exceed the downtime limit of 400 hours in 365 days.

Reliability
Failures of firewater pumps to start shall not exceed one failure in 25 tests/demands.

Survivability
The fire pump, driver, controller, water supply, and power supply shall be protected against possible interruption of service through damage caused by the explosion, fire, flood, earthquake, rodents, insects, windstorm, freezing, vandalism, and other adverse conditions. Reference: NFPA20:2022 Section 4.14. 1

Interdependency	
PS	**Criteria**
Firewater tank and Ring main (PS 15)	• The firewater tank supplies the fire pump and provides firewater storage capacity. • The firewater ring main supplies the end users with firewater from the firewater pumps.
Deluge & Foam Systems (PS 17)	• Firewater Pumps supply firewater to the Deluge & Foam Systems

Annex C - Operational Risk Assessment (ORA) Development Steps

Step 1: Description of SCE failure and hazard identification:

The assessment should provide a clear and sufficiently detailed description of the impaired SCE giving rise to the ORA. Reference should be made to the affected Performance Standard and describe the nature and extent of SCE degradation.

The description should state what plant and equipment are affected by the ORA, what Major Accident Hazard(s) the SCE relates to and / or the failure gives rise to, and what barrier(s) is /are affected by the failure. Significant effort should be applied to hazard identification at this stage as this provides the basis for all pursuant aspects of the ORA, and flawed hazard identification will result in an ineffective ORA output.

Step 2: Risk Evaluation:

Having identified relevant Major Accident Hazard(s) associated with the failed SCE, the team should evaluate risks that may stem from the identified Major Accident Hazard. Essentially the ORA is comparing the risk of operating with SCE in an impaired condition against normal operating risk. The evaluation process, therefore, considers four key factors, namely:

1. **Consequence:**

   The initial stage of risk evaluation should consider the potential consequences of SCE failure. The assessment should identify and list all reasonably foreseeable Major Accident Hazard scenarios linked to that SCE and describe how these are affected by the failure.

   This assessment considers the pre-mitigation condition (i.e., the consequences that may result if no additional mitigation is put in place to compensate for the impaired SCE). It should identify the reasonably foreseeable outcome for each identified hazard. The ORA team should have information from the safety case and SCE Performance Standards to support this assessment. Still, they should be especially mindful of any wider impacts of the SCE failure and the combined effect of other ORA already in place on the facility.

   A simple example of consequence assessment might be that if the failed SCE is a fire pump, deluge capacity may be reduced, leading to an increased risk of serious injuries or fatalities resulting from fire or explosion. Consequence assessment should also consider event escalation potential resulting from a failed SCE. It should be stressed that in ORA, the clear emphasis should be on determining the potential consequences of the abnormal situation.

2. **Likelihood:**

The second aspect of risk evaluation involves an assessment of the likelihood of the identified consequences of the SCE failure being realized. Again, this determination relates to the SCE failure without any mitigation measures. In most ORA circumstances, this will be a qualitative or semi-quantitative assessment, and the company's procedures should provide clear guidance on likelihood criteria specific to Major Accident Hazards. The assessment of likelihood is most relevant where the impaired SCE is preventive, e.g., ignition prevention. It should be emphasized that a determination of Low likelihood cannot be used to support continued operations without effective mitigation measures.

3. **Risk Estimation:**

The properly executed assessment of the consequence and likelihood described above enables the assessment team to arrive at a risk estimate in qualitative or semi-quantitative terms. The consequence and likelihood criteria must be relevant to Major Accident Assessment rather than task-related personal injury outcomes. Risk ranking is used to:

- Drive the requirement to shut down or limit activities or operations.
- Drive the identification and implementation of appropriate mitigation measures.
- Ensure appropriate levels of review, endorsement, and approval of the ORA.
- Identify and prioritize remedial or recovery actions (i.e., SCE time to repair).
- Specify timelines for review, revalidation, and/or closure of the ORA.

4. **Impact on other SCE:**

In considering the risks of SCE failure, assessors must be mindful of any interrelationships or dependencies between SCEs. These interrelationships and dependencies should be shown in the SCE Performance Standard, so reference should be made to that as a starting point. A simple example is that a failure of gas detection could affect alarm systems, ventilation trips, and ESD initiation.

Step 3: Identification of Mitigation Measures:

Having estimated the risk associated with the impaired SCE, the team should systematically identify and consider control measures designed to mitigate such risk. In making this determination, the team should consider the recognized hierarchy of controls and adopt the highest reasonably practicable standard of control.

Concerning SCE failure, this hierarchy can be illustrated in descending order as follows:

1. Hazard elimination by shutting down the affected plant or equipment.
2. Providing an engineering solution to replace or supplement the impaired SCE.
3. Implementing procedural controls such as prohibiting certain work activities or tasks in an affected area (e.g., stopping hot work).
4. Human intervention in the form of operator monitoring of a normally automated control function, for example.

Strict adherence to the hierarchy should be observed, and in particular, reliance on human intervention should always be the last resort. The risk assessment team should answer some specific questions along the following lines:

- Should the plant or process be shut down?
- Is an engineered solution necessary and possible to reduce risk?
- Have all available risk reduction measures been identified and properly considered?
- Where human intervention has been identified as mitigation, is there sufficient capacity and no risk of overload to the facility personnel?
- Is human intervention practical in the event of an emergency?

Finally, checks must be made to ensure that identified mitigation measures are available and reliable. This may require an SCE assurance routine to be brought forward to gain or increase confidence in the availability and reliability of that SCE in its additional mitigation role.

Step 4: Assessment of Residual Risk and Risk Determination:

The ORA team should assess residual risk by considering the risk reduction effect of identified mitigation measures. This should involve each of the identified hazards in the ORA being revisited and risks re-evaluated, taking credit for identified mitigation measures. This step should assign new qualitative or semi-quantitative values and allow the team to determine the acceptability of continued safe operation in the impaired state. The company's procedure should provide direction regarding the tolerable levels of residual risk to enable the ORA team to recommend shutdown or continued safe operation as appropriate. It should also be emphasized that lowering residual risk below that assessed as the original risk level does not necessarily mean that a proposal is acceptable. The focus on consequences should prompt serious consideration of the residual risk level and drive efforts to reduce risk further.

The facility safety case includes a demonstration that control of Major Accident Hazards complies with the relevant statutory provisions and to a level that is as low as reasonably practicable (ALARP). That compliance and the ALARP demonstration will have taken credit for existing SCE in their fully functional condition. It follows, therefore, that an impaired SCE

condition will temporarily result in a level of risk that is higher than the ALARP level defined in the Safety Case. The properly executed ORA will arrive at a position where all reasonably practicable risk reduction measures have been implemented, allowing the ORA team to determine if the residual risk is tolerable or intolerable and to make a suitably informed judgment to continue operations or to shut down on that basis. Crucial to the ORA approach is the need for a strong and continued focus on remedial actions so that the period of reliance on mitigation controls is minimized and appropriate effort and resources are applied to restore the impaired SCE effectively, as illustrated in Figure C1.

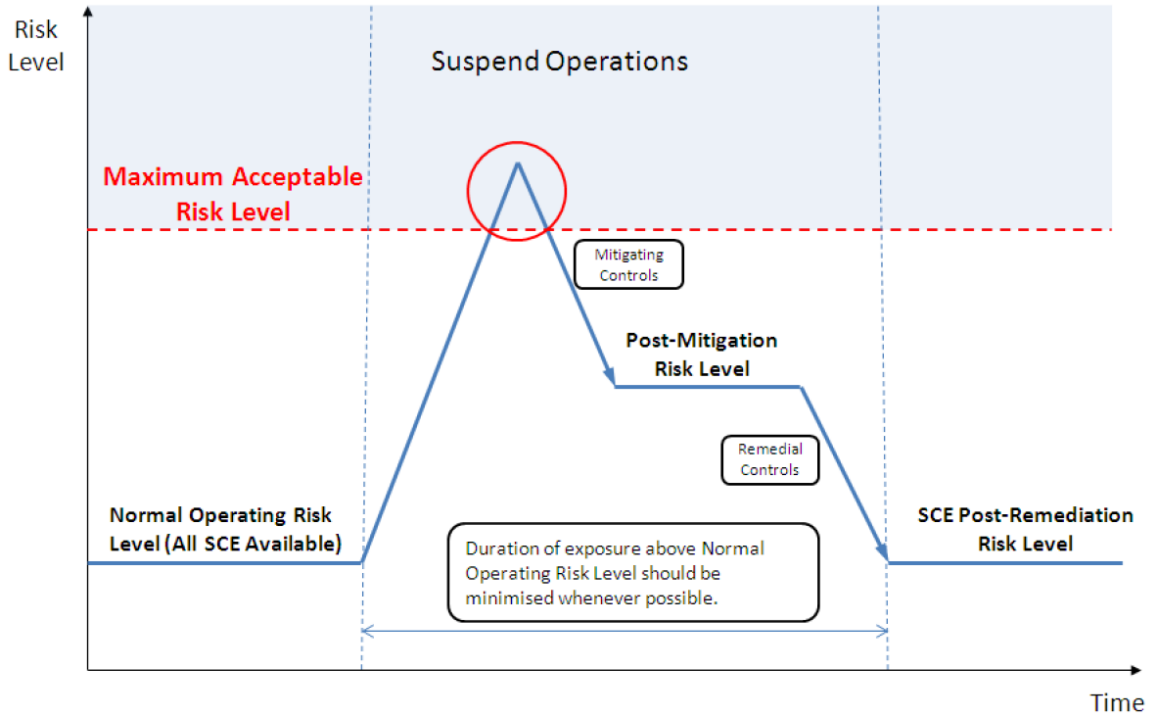

***Figure C1**. Risk tolerability judgment.*

Step 5: The Risk of Interconnected Barriers Failure:

The ORA team should have an overview of the combined effect of risks arising from interconnected SCE failure. The ORA team must be aware of other ORA in place in the facility. Other defects, such as integrity issues (e.g., temporary repairs), deferred PM or CM routines on SCE, and a specific summary of ORA where human controls are in place, should also be noted. The team should ensure that the combined effect of SCE impairment remains tolerable and mitigation measures remain manageable. This assessment aspect should also consider other demands that may already be placed on SCE affected by the ORA.

It is recommended that facilities put in place measures to record and ensure visibility of current ORA, degraded SCE, and temporary mitigation measures. The best way to achieve visibility of the inter-relationships between the threats and the potential consequences, and the role of the barriers in preventing or mitigating these events, is to use Bowtie diagrams of

the various hazards that apply. It is highly recommended that Bowtie diagrams are developed for each hazardous event and that these are used to support the overall cumulative risk model. Figure C2 diagram shows an example of a Bowtie diagram supporting an ORA conducted for a defective level trip for a gasoline storage tank.

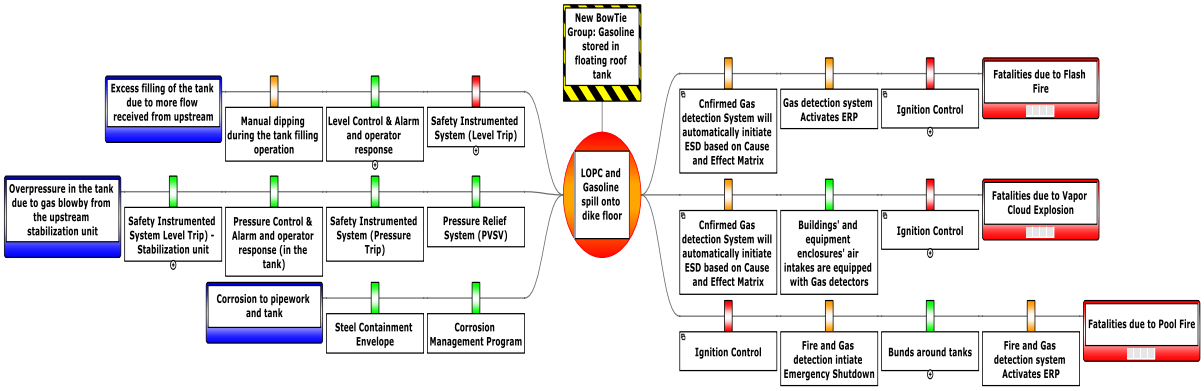

Figure C2. *Bowtie analysis for one of the ORAs of defected storage tank's level trip.*

The condition/current effectiveness of each barrier in the above example was determined based on a simple criterion, Does the barrier function as intended or not? Hence color coding was applied. In this example, the ignition control barrier was presented in red as some Ex-equipment in the tank's dike area was found to defected and assessed under separate ORA.

Based on the ORA team assessment and considering the combined risk, if it is assumed that the residual risk ranking of the above scenario was assessed as red, then, for the overall plant barrier model, the effectiveness rating (health status) of the Shutdown System barrier will be red, as this defected level trip is one of the systems under shutdown barrier.

Annex D - Example for the ORA and Cumulative Barrier Model

D.1. Means of Identification of The Deficient/Degraded Barrier

Genuine demand on critical barriers, i.e., in the event of an ESD shutdown, trip, or even test event, could reveal a barrier's failure to perform its desired function. For example, a certain level of ESD may require that some or all the main process system ESD valves move to a closed position and similarly that BDV valves open to facilitate the safe removal of hydrocarbon inventory to a vent or flare system. An accepted good practice after such an event is to establish that the plant has reached a safe position following the upset and to ascertain that elements such as ESD valves have functioned as required by their performance standard. A review of ESD valve function could reveal that valves have either not achieved their "safe" position or have done so at a time outside of the desired performance standard.

D.2. Risks Presented

In the case of ESD valves, failing to achieve closure could mean that sections of the plant are not isolated as intended by design and potentially allow further escalation. Suppose the initiating event was to feature a loss of primary containment. In that case, this could mean that the release of hazardous material was sustained, and the consequences of harm were increased if there was a subsequent fire, explosion, or a significant toxic component.

D.3. Initial Operational Risk Assessment

Initial risks need to be assessed. This can be done using the company's risk matrix. Reference should be made to design documentation (including ESD valve design data and the original HAZOP and SIL reports).

Appropriate technical authorities must be involved in the assessment. In this case, a suggested minimum would be the Process, Mechanical & Process Safety Engineering Technical Authorities, and Operations management. In the initial risk assessment, no credit is taken for mitigation measures.

In this example, consequence analysis associated with the facility's Safety Case could be used to identify the likely scenarios associated with releases from the plant's various isolatable sections and the implications for escalation. It should also consider the implications if several valves in a system (or in series) did not function. Consequences should then be assessed with due consideration of potential worst-case scenarios. Assessment should be conservative. Reference to the facility Quantitative Risk Assessment (QRA) will be useful in determining the potential outcomes of loss of containment in various locations on the facility. Technical Safety should be consulted.

D.4. Mitigation Measures

Mitigation measures should be developed based on the preferred risk reduction hierarchy, seeking to identify measures that can be readily assured. These interim risk mitigation measures are only to be put in place until a permanent solution is implemented.

The selected mitigation measures and the activities required to ensure their effectiveness should be documented. In this example, if failure to isolate or safely depressurize particular inventories is identified as the main threat, the mitigation measures (in order of preference) may include:

- Additional stroke testing of the valves is carried out, closure/opening times are measured & documented, and a degradation limit is set beyond which operations may not continue (noting that this may impact the continuity of production operations and may contribute to the failure mechanism of the valves rather than ensuring reliability).
- Isolation, bypass, or a reduction of pressure, flow, or inventory in sections of the process where problematic valves are evident.
- Reduction in the permit-related activity that could lead to a spurious or genuine trip or ESD events, e.g., hot work, breaking containment, scaffolding, construction.

All the above mitigations may be required before it is considered that the residual risk has been reduced to a level that can be tolerated in the period until the permanent solution is implemented.

D.5. Residual Operational Risk Assessment

The residual risk assessment is performed considering the mitigation measures. The appropriate Technical Authorities and Operations management personnel should be involved. The overall “Shutdown barrier” effectiveness rating will be determined based on the residual risk level of this ORA.

The step is to consider the risk from defective interconnected barriers, which either allows credit to be taken for other barriers (if they are known to be effective) or may show that operational risks are significantly higher than the ALARP position when the combined effect of interconnected barrier deficiencies is considered. Any assumptions regarding risk reduction offered by other barriers should be documented; remember that the ALARP risk position is only achieved when ALL barriers function effectively, as documented in the facility Safety Case.

If the risk assessment reveals increased risk levels that cannot be acceptably managed, the risk is intolerable, and the facility should be shut down until barrier effectiveness can be improved to bring the risk profile back inside a tolerable envelope. If the decision is taken to continue operating the facility, this is based on the effectiveness of the mitigations that are proposed and the assurance of these measures becomes critical.

Figure D1 includes the bowtie developed for the LOPC scenario at the inlet facility and the status of the interconnected barriers. The status of the interconnected barriers was verified during the ORA session and the residual risk ranking was determined.

If the residual risk ranking, after considering the other interconnected barriers, was in the ALARP zone, the facility's barrier model should reflect the ORA outcome concerning this type of anomaly. Hence, the "Shutdown system barrier" in the barrier model will initially be presented in "Red color" and eventually, after considering mitigation, in "Amber color". Figure D2 includes the facility's barrier model including the health status of all barrier categories represented in colors.

D.6. Proposed Permanent Solution, Period, Approval

The details of the permanent solution (in this case, to replace the ESDV/BDV valves and/or their actuators entirely or a combination thereof with those of a sufficient rating) should be given, including the period required for implementation. Barrier deficiencies identified during genuine demand or otherwise could be a widespread, immediate failure or a longer-term issue that has grown in scale over time. Hardware changes and equipment upgrades, or modifications will likely be required. The purchase of new materials or equipment will mean that timescales could be significant but should be prioritized to be as short as practicable; some explanation of the time to implement the solution should be given. The interim risk mitigation measures must be assured throughout this period, and the cumulative risk position must be regularly reviewed. Re-approval of the ORA may be required.

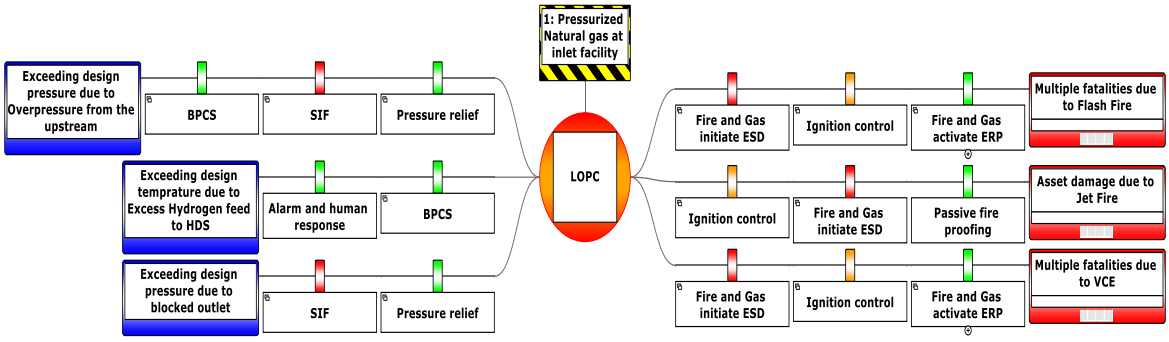

Figure D1. *ORA* for the *defective* SCE at the inlet facility.

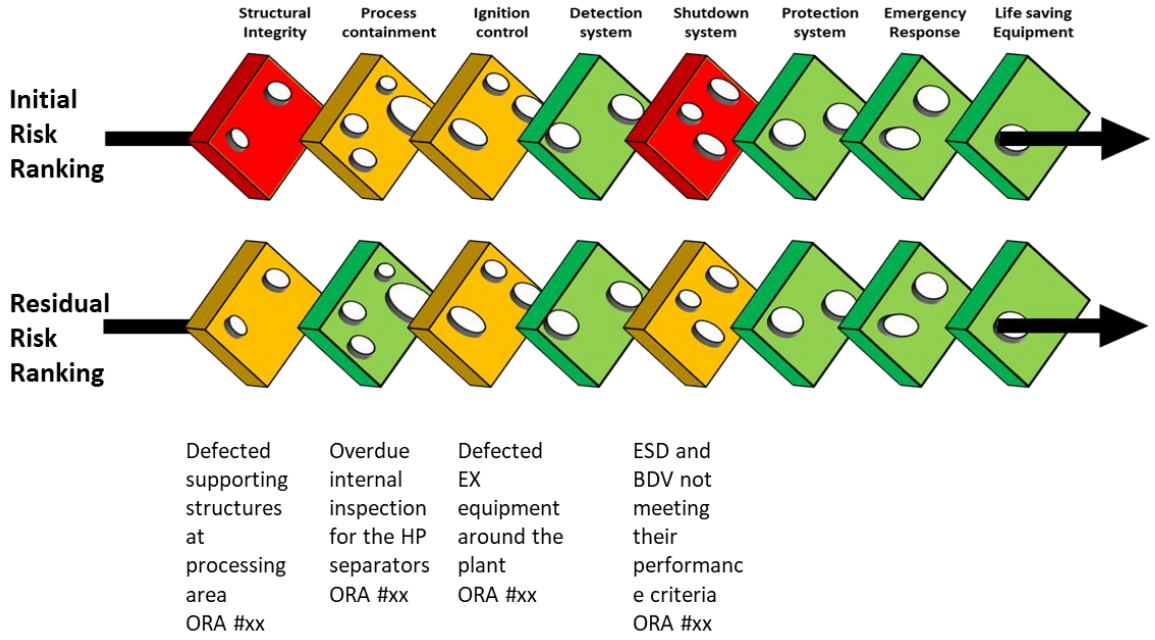

Figure D2. *Facility's cumulative barrier model showing the health status of the barriers.*

Annex E - SCE Safety Criticality Ranking

There are various methods of evaluating SCE criticality. The example method described here allocates scores based on the following factors:

- The MAH management functional role of the SCE (Fn).
- The consequence of the failure of the SCE (Cq).
- The extent to which an alternative SCE can take over the function of the SCE in the event of its failure (i.e., defense in depth) or its unavailability, and/or whether the SCE has inherent redundancy (Rn).

In the example method, each identified SCE is assessed for criticality based on its MAH management functional role, the consequence of its failure, and redundancy using the following equation:

$$SCE\ Criticaliyt = Fn \times Cq \times Rn \qquad Equation\ E1.$$

Scores are assigned for each parameter using a simple scoring system. In this example method, each score increases by integers.

The scoring system for the MAH management functional role of an SCE (Fn) in Table E1 allocates additional weight to risk reduction measures on the left-hand side of a Bowtie over those on the right-hand side.

Table E1. *Scoring system for SCE MAH management functional role.*

MAH Management Functional Role of SCE	Functional role score (Fn)
Prevention	4
Detection	3
Control and mitigation	2
Emergency response and life saving	1

The scoring system for the consequence of failure (Cq) in Table E2 is based on the severity of the consequences of SCE failure. The scope of the example method is safety only.

Table E2. *Scoring system for SCE consequence of failure.*

Severity of Consequences of Failure of SCE	Description of Severity of Consequences	Consequence of Failure Score (Cq)
Disastrous	Multiple fatalities and/or extensive plant damage.	3
Catastrophic	Single fatality and/or many serious injuries and/or significant plant damage.	2
Major	Many injuries and/or local plant damage.	1

Notes

- Data are for safety consequences only. Other risk drivers also may be applicable (e.g., business interruption).
- Organizations should apply their corporate risk criteria.
- Where the severity of consequences of failure of SCE is rated 1, the SCE should be re-evaluated as to whether it meets the criteria for being an SCE; where the review identifies that this is not the case, it should be downgraded to a conventional risk reduction measure.

The scoring system for redundancy (Rn) in Table E3 is based on the extent to which an alternative SCE can take over the function of the failed SCE or the extent to which the design incorporates redundancy.

Table E3. *Scoring system for SCE redundancy.*

Redundancy of SCE	Functional role score (Fn)
No other SCE that duplicates the full functionality of the failed/unavailable SCE	3
SCE design has provision for redundancy	2
An alternative SCE can provide full functionality of the failed/unavailable SCE	1

The criticality ranking for each SCE is determined using equation E.1, following the assessment of Fn, Cq, and Rn. SCE criticality is graded into three ranks: high, medium, and low, as set out in Table E4.

Table E4. *SCE criticality ranking.*

SCE Criticality Score	SCE Criticality Rank
17-36	High
8-16	Medium
1-7	Low