





MAJOR ACCIDENT HAZARD MANAGEMENT GUIDELINE

EGPC-PSM-GL-006

PSM GUIDELINE

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

 EGPC	Major Accident Hazard Management Guideline	
	Document No: EGPC-PSM-GL-006	

Acknowledgements

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 MOP and its affiliated companies following industry best practice, international codes and standards. The Egyptian Process Safety Management Steering Committee is formed of representatives from MOP, EGPC, EICHEM, EGAS, Ganope and Methanex Egypt.

PSM Technical Subcommittee team members during the project comprised:



Amr Fathy Hassan	PSM Consultant – Methanex Egypt	Team leader
Mohamed Hamouda	HSE Section Head – Pharaonic Pet. Co.	Member
Mohamed Ashraf AboulDahab	Safety Section Head for Upstream – EGPC	Member
Tamer AbdelFatah	PS & DM Sites QHSE Senior – UGDC	Member
Mohammed Sabry	Projects Safety A. General Manager – GASCO	Member
Hany Tawfik	OHS & PS General Manager – Ethydco	Member
Sayed Eid	HSE A. General Manager – Agiba Pet. Co.	Member

During developments and prior approval, all PSM technical subcommittee documents are subjected to a thorough technical peer-review process. 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 sub-committee acknowledges the following reviewers from major Process Safety consultants as well as major operators & EPC who provided valuable comments during the technical peer reviews that resulted in an outstanding product structure and quality:

Process Safety Consultants (in alphabetical order)

Bell Energy Services	Amey Kulkarni	Technical Director
DNV	Cees de Regt	Senior Principal Consultant
Process Safety & Reliability Group (PSRG)	Robert J. Weber	President/CEO
Risktec Solutions - TÜV Rheinland		

 EGPC	Major Accident Hazard Management Guideline	
	Document No: EGPC-PSM-GL-006	



Major IOCs & EPCs (in alphabetical order)

Eni	Ahmed Omar	LNG Operations Manager
Methanex Egypt	Ihab Fikry	Process Safety Management Lead
SHELL Egypt	Yasser Fathi	Process Safety Manager

It should be noted that the above have not all been directly involved in the development of 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
Osama Abdou Ahmed Hassanin	HSE General Manager – EGPC	Member
Emad Kilany	OHS & Fire Fighting Technical Studies GM – EGAS	Member
Mohamed Sayed Suliman	HSE General Manager – Ganope	Member
Mohamed Mostafa	Inspection & External Audit AGM – 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
Ihab Fikry	PSM Lead, Methanex Egypt	Member
Amr Moawad Hassan	PSM Consultant – Methanex Egypt	Member
Mourad Hassan	PSM Consultant – Methanex Egypt	Member


 EGPC	Major Accident Hazard Management Guideline	
	Document No: EGPC-PSM-GL-006	

DOCUMENT NO. EGPC-PSM-GL-006	TITLE Major Accident Hazard Management Guideline	ISSUE DATE 28-10-2021
--	---	---------------------------------

Approval

NAME	TITLE	DATE	SIGNATURE
Amr Moawad Hassan	PSM Consultant - Methanex Egypt PSM Technical Subcommittee TL	28-10-2021	 <small>Digitally signed by Amr Moawad Date: 2021.11.04 02:47:02 +0200</small>
Gamal Fathy	EGPC CEO Consultant for HSE		

Endorsement

NAME	TITLE	DATE	SIGNATURE
Abed Ezz El Regal	CEO - Egyptian General Petroleum Corporation (EGPC)		

Copyright

The copyright and all other rights of a like nature of this document are vested in EGPC and Egyptian Oil and Gas Holding Companies – refers hereinafter as ENTITIES –. This document is issued as part of the Process Safety Management (PSM) System Framework establishing requirements for their operating company, subsidiary, affiliated and joint ventures – refers hereinafter as COMPANIES –. Either ENTITIES or their COMPANIES may give copies of the entire document or selected parts thereof to their contractors implementing PSM standards or guidelines to qualify for the award of contract or execution of awarded contracts. Such copies should carry a statement that they are reproduced by permission relevant ENTITY or COMPANY. This document cannot be used except for the purposes it is issued for.

Disclaimer

No liability whatsoever in contract, tort, or otherwise is accepted by ENTITIES or its COMPANIES, their respective shareholders, directors, officers, and employees whether or not involved in the preparation of the document for any consequences whatsoever resulting directly or indirectly from reliance on or from the use of the document or for any error or omission therein even if such error or omission is caused by a failure to exercise reasonable care.

Controlled Intranet Copy



The intranet copy of this document is the only controlled document. Copies or extracts of this document, which have been 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.....	6
2. Purpose and scope.....	6
2.1 Purpose.....	6
2.2 Scope	6
3. Definitions and Abbreviations	7
4. Major Accident Hazard Management Process	8
5. Definition of Major Accident Hazard (MAH)	9
6. Risk Assessment Matrix and Major Accident Hazard	9
7. Identification of Major Accident Hazard	10
8. List of Major Accident Hazards	10
9. Bowtie Development – Bowtie workshop	11
9.1. Validity of Safety Barrier	11
9.2. Barrier Adequacy	12
10. Identification of Safety Critical Elements (SCEs).....	13
11. Performance Standard (PS)	13
12. Reflecting Performance Standard in maintenance program.....	14
13. Safety Critical Tasks	15
14. Verification of Performance Standard Assurance tasks	15
15. References	16
16. Annexes	17
Annex (1) typical examples for the Major Accident Hazards	17
Annex (2) – Bowtie methodology and examples	18
Annex (3) Bowtie checklist	34
Annex (4) Barrier Effectiveness Criteria	36
Annex (5) Barrier Adequacy Criteria	37
Annex (6) SCE Group for Each Barrier	39
Annex (7) Operation Performance Standard example.....	41
Annex (8) Safety Critical Tasks example	43

	Major Accident Hazard Management Guideline	
	Document No: EGPC-PSM-GL-006	

1. Introduction

This guideline establishes the principles, methodology and guidance for the management of Major Accident Hazards (MAHs), using bowties which are typically used as part of safety case development taking into consideration creating a balance between maximum sustained value and minimum lowest sustained risk.

2. Purpose and scope

2.1 Purpose

The main purpose of this document is to establish requirements and provide guidance for the effective management of Major Accident Hazards (MAHs) during the project life cycle, including design and the operation phases, of a Facility/Entity. This guideline aims to:

- Develop a clear definition of Major Accident Hazard (MAH);
- Provide MAH Bow tie development rules;
- Develop criteria for MAH safety barriers concerning effectiveness, independence, and adequacy; and,
- Detail the process for identifying Safety-Critical Element (SCE), developing SCE Performance standards (SCEPS), and developing Safety Critical Tasks (SCTs).



This guideline supports the development of a safety case document.

While this guideline has been developed for the purpose of providing an overview of MAH management with a focus on of identification of MAH within the facility, risk management process and related barriers & controls for the purpose of managing Major Accident Hazards. Thus it does not include the full process for managing SCE i.e. the impairment management of SCE, the SCE criticality ranking, the KPI's. This guideline also does not cover the full scope of formal safety assessment studies, which shall be addressed in details in other guidelines.

2.2 Scope

This document applies to the Oil and Gas Holding companies including the Egyptian General Petroleum Corporation (EGPC), the Egyptian Natural Gas Holding Company (EGAS), the Egyptian Petrochemical Holding Company (ECHEM), and the Ganoub El Wadi Holding Company (GANOPE) covering all of their operational subsidiaries, state-owned companies, affiliates, and Joint Ventures and their Contractors.

This guideline supports the development of the safety case document and shall be implemented by those companies required to develop a safety case.

	<p style="text-align: center;">Major Accident Hazard Management Guideline</p> <p style="text-align: center;">Document No: EGPC-PSM-GL-006</p>	
---	---	---

3. Definitions and Abbreviations

Bow tie Model

A risk diagram showing how various threats can lead to a loss of control of a hazard and allow this unsafe condition to develop into a number of undesired consequences. The diagram can show all the barriers and degradation controls deployed.

Hazards and effects register (H&ER)

A risk assessment record that demonstrates that all hazards and effects have been identified, are understood, and are being properly controlled. This Register is kept current throughout the life cycle of a project or activity. H&ER covers Major Accident Hazards (MAH) and other hazards which are not rated as MAH.

HSE Critical Position

The Person who carries out a Safety Critical Task (SCT).

Major Accident

A Hazardous event that results in:

- Multiple fatalities or severe injuries; or
- Extensive damage to structure, installation or plant; or
- Large-scale impact on the environment (e.g. persistent and severe environmental damage that can lead to loss of commercial or recreational use, loss of natural resources over a wide area or severe environmental damage that will require extensive measures to restore beneficial uses of the environment).

Major Accident Hazard could be substances, activities, operations or conditions.

Major Accident Hazard

A hazard with the potential, if realized, to result in a major accident. Hazards that are initially assessed (without any control measure) as having a consequence severity of (A - Disastrous) or risk ranking of red, as defined in the corporate risk matrix, are categorized as major accident hazards.

Performance standard (PS)

A qualitative or quantitative statement of the required performance of a safety critical element (SCE) that contains the information necessary to validate its effectiveness during design, construction, testing, commissioning, operation and decommissioning.

Performance Standards for establishing initial suitability may differ from those used to assess the ongoing suitability of SCEs and hence separate Performance Standards should be developed for initial and ongoing suitability for the same SCE.

Safety Critical Element (SCE)

Any part of a facility, plant, or computer program, the failure of which could cause or contribute substantially to an MAH; or the purpose of which is to prevent or limit the effect of an MAH.

Safety Critical Task (SCT)

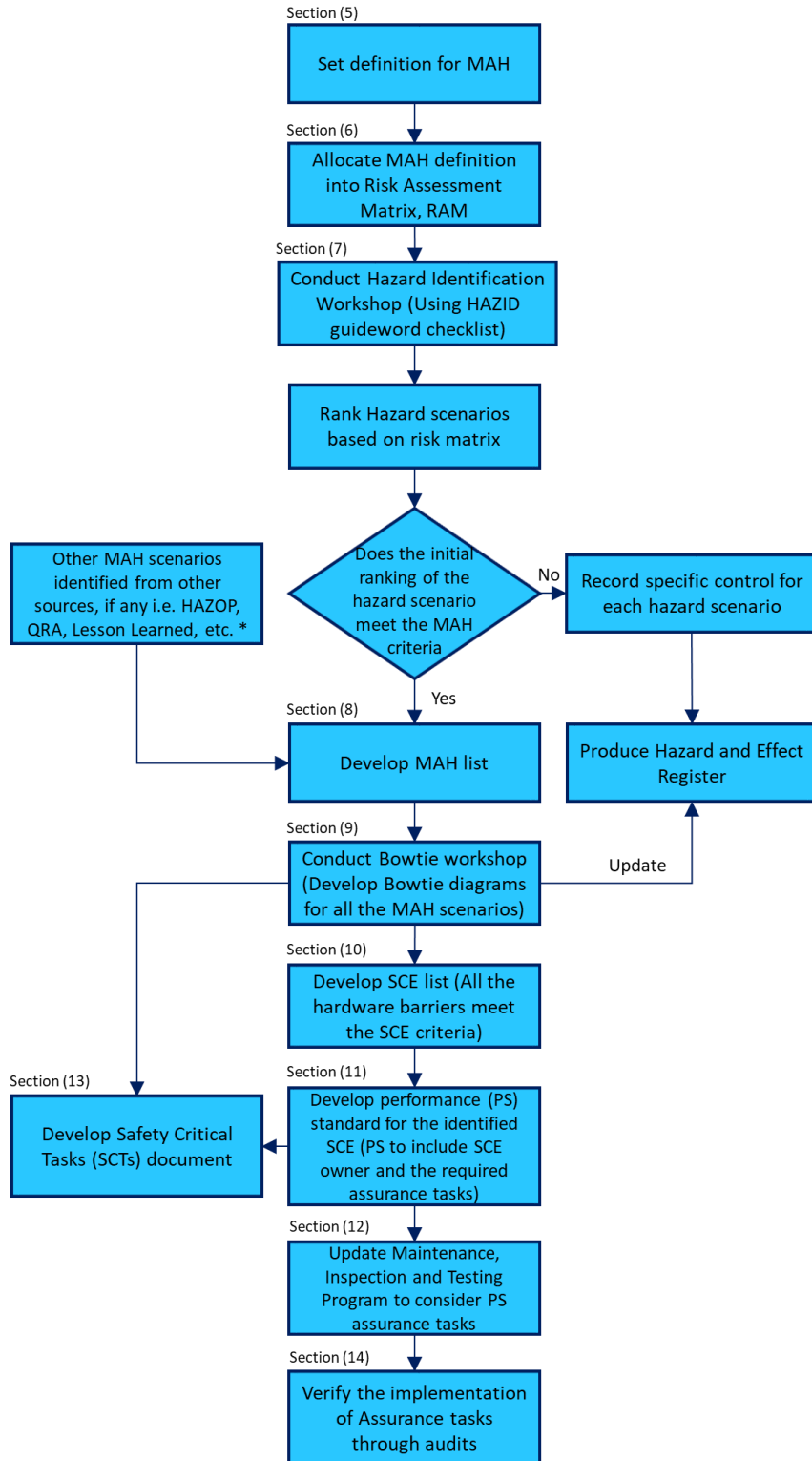
Tasks / Action necessary for the development, implementation, operation or maintenance of a barrier established for managing Major Hazards.

Refer to PSM Glossary document EGPC-PSM-GL-011 for more definitions and abbreviations.



4. Major Accident Hazard Management Process

The below chart details the Major Accident Hazard management process starting from setting a definition for MAH. Each step is mentioned in detail in the document body.



(*) Input is explored and evaluated during HAZID workshop

Fig. (1) - MAH management process flowchart

5. Definition of Major Accident Hazard (MAH)

Major Accident Hazard is the hazard with the potential, if realized, to result in a major accident.

A Major Accident is Hazardous event that results in:

- Multiple fatalities or severe injuries; or
- Extensive damage to structure, installation or plant; or
- Large-scale impact on the environment (e.g. persistent and severe environmental damage that can lead to loss of commercial or recreational use, loss of natural resources over a wide area or severe environmental damage that will require extensive measures to restore beneficial uses of the environment)."

(ISO 17776 definition) [1]

Major Accident Hazard could be substances, activities, operations or conditions.

Annex (1) includes typical examples for the Major Accident Hazards.

6. Risk Assessment Matrix and Major Accident Hazard

Based on the definition of Major Accident Hazard and reference to the Corporate Risk Assessment Matrix (RAM), the region of MAH could be allocated and marked on the RAM.

Any hazard assessed as having a Disastrous Consequence (Severity A) should be considered as a MAH regardless of the likelihood of the event.



The below figure shows the MAH mapped on Corporate RAM.

Likelihood		Rare	Unlikely	Possible	Likely	Very Likely	Almost Certain
Severity	#	1	2	3	4	5	6
Disastrous	A	1A	2A	3A	4A	5A	6A
Catastrophic	B	1B	2B	3B	MAH Area		
Major	C	1C	2C	3C			
Serious	D	1D	2D	3D	4D	5D	6D
Minor	E	1E	2E	3E	4E	5E	6E
Notable	F	1F	2F	3F	4F	5F	6F

Non-MAH Area

Fig. (2) - MAH reflected on RAM

- All MAH scenarios shall be managed and adequate risk control measures shall be demonstrated via bowties diagrams and Safety Critical Elements SCEs and tasks. All Safety Critical Elements (SCEs) and tasks shall be identified for the MAH Bowties diagram.
- The rest of the hazard scenarios identified in the HAZID workshop (section 7), shall be managed and adequate risk measures shall be identified and demonstrated in the facility

 EGPC	Major Accident Hazard Management Guideline Document No: EGPC-PSM-GL-006	 PSM
--	--	---

hazard and effect register. Note: Hazard and effect register template is included in the HAZID guideline.

7. Identification of Major Accident Hazard

A Hazard Identification (HAZID) study is commonly used as the basis for identifying the major hazards and developing the MAH list.

HAZID is a team-based brainstorming analysis used to identify potential process and non-process hazards. HAZID typically examines all reasonably possible sources of hazard, including the process design itself and hazards external to the process design.

ISO 17776 provides an extensive checklist of hazards that can be encountered in the petroleum and natural gas industries. The HAZID team could utilize this checklist and risk assess only the applicable hazards to the facility/entity or process.

For the scope of the safety case, the main objective of the HAZID study is to identify the credible MAH scenarios. MAH screening starts in an Evaluation / Concept selection study and should be continually assessed and defined as the design evolves.

MAH risks may change, especially during the operational phase. New MAH could be introduced, or the risk associated with existing MAHs could change because of changing operational conditions. If these changes occur, then the MAH risks should be re-evaluated. Examples of events, changes or activities that should trigger MAHs reviews include:



- Major project changes (e.g. process, inventories, production fluids, etc.);
- CAPEX projects (e.g., extensions, new builds);
- Ageing of the facility;
- New or amended legislation, regulations, standards, etc; and,
- Lessons learned from incidents.

During the operation phase and as a minimum, the MAH review process should be conducted every five years.

8. List of Major Accident Hazards

MAH list is generated as one of the deliverables of the HAZID study. Initial risk ranking, before considering the proposed /existing control measures, determines those hazards that are qualified as Major Accident Hazards, refer to (section 6).

Note: During the early design phase, evaluations will necessarily be less detailed than those undertaken during later design and operation phases. So, any MAH identified from other studies i.e., HAZOP, QRA, etc. is to be explored during the HAZID session and to be added to the MAH list.

	Major Accident Hazard Management Guideline	
	Document No: EGPC-PSM-GL-006	

Each MAH requires further in-depth studying through bowtie. Before starting bowtie development, the MAH list shall be reviewed to consider any MAH raised from any other studies and not discussed during the HAZID workshop.

9. Bowtie Development – Bowtie workshop

Bowtie is a method of identifying prevention and mitigation risk reduction control measures. An advantage of the Bow tie methodology is its simplicity in delivering a pictorial representation of the MAHs, top event, consequences and risk reduction measures, which in Bow tie terminology are called barriers.

For those hazards that are classified to be Major Accident Hazards, Bow tie models are required to be developed to:

- Identify the potential Major Hazard release, escalation and consequence scenarios,
- Identify the prevention and mitigation barriers and ensure their adequacy, and
- Identify the Safety Critical Elements and Safety Critical Tasks required to effectively manage these hazards.

Bowties can demonstrate the link between controls and the management system, specifically those relevant to the management of risks (e.g., safety critical elements, critical positions / tasks).

Explanation of Bowtie elements with examples are detailed in Annex (2).

9.1. Validity of Safety Barrier

Barriers must have the capability on their own to prevent or mitigate a Bow tie sequence and meet all the validity requirements for a barrier to be effective, independent, and auditable.

Effective:



For the barrier to be effective and considered for bowtie presentation, it has to be ‘big enough’, ‘strong enough’ and react ‘fast enough’ to stop the threat leading to the top event or to mitigate the consequence when it functions as designed.

If the barrier achieves this criterion, then effectiveness rating could be decided. Effectiveness option to characterize the effectiveness of a barrier is a qualitative rating.

The effectiveness of each barrier is assessed considering both the effectiveness of the hardware controls that will be possible and also the controls that will rely on human intervention.

The basic process undertaken for each control barrier Effectiveness will consider the following aspects :

- Effectiveness; whether or not the control will be in place and how good it is at doing its job;
- How independent it is of the human factor, and
- How reliable it is, how easy to defeat the top event

	Major Accident Hazard Management Guideline	
	Document No: EGPC-PSM-GL-006	

Barrier effectiveness ratings is colour-coded in the bowtie diagrams to allow shortcomings in hazard control to be readily identified, thereby demonstrating of the level of control and allowing identification of areas where additional control measures can, or require to, be practicably implemented. Annex (4) shows the barrier effectiveness criteria.

Independent:

For a Barrier to be independent it needs to be:

- Independent of the threat;
- Independent of other barriers on that pathway; and,
- Not sharing the common mode failure with other barriers.

The barriers are not independent if the effective performance of one barrier is dependent on the successful operation of another.

For example, alarm and trip functions sharing one instrument is one barrier only. An additional hardwired trip, hence independent from the other instrument, would count as a separate control measure. If there is no trip, shutdown or executive action initiated by the safety function, operator intervention using aimed to follow-up and response to the instrument alarms should be regarded as part of the one total risk reduction measure.

Auditable:

Barriers should be capable of being audited to check that they work on demand or when it is called to respond to certain changes or set points. The Auditability of safety barriers will ensure the presence of an audit trail of the safety barriers performance which reflects the ability of an organization to:

- Establish and maintain inspection procedures;
- Records previous validation assessments, and other documented information to ensure that safety design intent is met;
- Testing, maintenance, and operation continue to conform to expectations.



Barrier can be evaluated to verify that it can and will operate when it is called upon (e.g. through testing and inspection, or through audit of the hardware performance criteria or Safety Critical Tasks (SCTs) needed to maintain an effective barrier).

9.2. Barrier Adequacy

In establishing the number of barriers required, care should be taken to count only the independent barriers.

To ensure consistency in all bowtie studies across the Egyptian companies, a criterion for barrier adequacy and sufficiency must be available to take in consideration the barriers Independency and strength/effectiveness.

The barrier adequacy criteria specify what is deemed suitable and sufficient control of threats and mitigation of / recovery from consequences. This criterion should be considered as a minimum number of barriers and not an absolute requirement. Where less barriers are identified, additional controls / actions (Risk Reduction Measures) should be identified to reduce the risks to ALARP. Annex (5) shows the barrier adequacy criteria.

	<p style="text-align: center;">Major Accident Hazard Management Guideline</p> <p style="text-align: center;">Document No: EGPC-PSM-GL-006</p>	
---	---	---

Where it is not possible to utilize this technique (adequacy criteria) as the introduction of a new barrier is not reasonably practicable, Team should include a suitable and sufficient narrative explanation of all the factors considered, and the underlying rationale for the final judgment and the barriers considered sufficient.

Annex (3) contains a checklist that could be used in the bowtie workshop to ensure bowties are meeting the criteria mentioned in this document.

10. Identification of Safety Critical Elements (SCEs)

In principle, all barriers in a Bow tie diagram are important and need an ongoing management process to ensure their effectiveness however, some barriers can be more important than others and frequently some barrier components are designated SCEs and their associated human actions as safety-critical tasks. This is why Barriers could be categorized as critical and non-critical barriers.

The purpose of this categorization is to indicate which barriers need more focus and ongoing monitoring, maintenance and immediate rectification when required. When a critical barrier fails, it can be assumed that the risks associated with the threat under consideration are greater so the chance of an undesired event occurring increases significantly, warranting the additional focus and attention on that barrier.

The basis for determining barrier criticality is whether the barrier components include Safety Critical Element (SCE). SCE is defined by Energy Institute as *“any part of a facility, plant, or computer program, the failure of which could cause or contribute substantially to an MAH; or the purpose of which is to prevent or limit the effect of an MAH”* [2].



Each hardware barrier is sub-divided into SCE groups, for reporting and management purposes. These groups are defined by their function ensuring the barrier remains in place (they are not defined by location, equipment type, medium or service, construction type or technical authority responsibility).

One of the deliverables from bowtie workshop is the SCE group list. The purpose of developing such a list of SCE group is that the equipment involved would be ranked higher on the integrity priority program for inspection, maintenance and repair, together with measures such as holding parts in stock to reduce the time for repair.

Annex (6) lists some SCE groups against their respective barriers. It is preferable at the end of the Bowtie workshop to review this SCE list to ensure that no applicable SCE has been missed during the workshop.

11. Performance Standard (PS)

For each SCE identified during the bowtie workshop, a performance standard must be developed. This standard sets out the levels of performance it 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

 EGPC	Major Accident Hazard Management Guideline	
Document No: EGPC-PSM-GL-006		

time. PSs for SCEs should be described in a safety case for MAHs that demonstrates the basis of safe operation.

Energy Institute guidelines defined Performance standard (PS) as “A qualitative or quantitative statement of the required performance of a safety critical element (SCE) that contains the information necessary to validate its effectiveness during design, construction, testing, commissioning, operation and decommissioning” [2].

In the context of SCE, Performance standard defines the performance criteria for the SCE and contains the information necessary to verify the effectiveness of SCE during design, construction and operation of the system.

Each SCE should have its own Performance Standard. For example, Active Fire Protection can be viewed as an SCE at a system level or broken down into its safety-critical equipment and components, such as pumps, valves, ring-main, associated branch piping systems, and nozzles. Active Fire Water Protection system functionality performance criteria is measured to the firewater demand to the worst-case scenario for a certain duration while functionality performance criteria for fire pump is pressure and flow measured at the pump discharge. The advantage of viewing such sets of safety-critical equipment and components on a system level is that it is easier to manage them together.

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. Operating companies should define PSs for their SCEs to define the required assurance activities, i.e., maintenance, inspection and testing to maintain the integrity of the SCEs. In this way, there should be a transparent linkage between MAHs, SCEs and the PSs.

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; and,
- Operate: inspection, maintenance and testing.

Therefore, PSs for establishing initial suitability may differ from those used to assess the ongoing suitability of SCEs and hence separate PSs should be developed for initial and ongoing suitability for the same SCE. The requirement contained in PSs should be to assure that SCEs do meet defined PS criteria across the facility life cycle and so MAH risks meet the defined risk acceptance criterion.

Annex (7) shows example for operation performance standard.

12. Reflecting Performance Standard in maintenance program

During the operation phase, performance standard assurance requirements should be reflected in the company’s maintenance, inspection and testing program so that SCEs retain ongoing suitability and continue to meet their PS criteria.

 EGPC	Major Accident Hazard Management Guideline Document No: EGPC-PSM-GL-006	
--	--	---

In order to apply performance standard requirement and to facilitate scheduling and executing assurance tasks at tag level, an asset register shall be developed. Asset register comprising Safety Critical Equipment or Components that are part of a system-based SCE, identified at tag level with a unique identification number.

Effective SCE assurance during the operate phase is dependent upon the alignment between the asset register and the PSs.

13. Safety Critical Tasks

Safety Critical Tasks (SCTs) are a group or set of tasks / actions necessary for the development, implementation, operation or maintenance of a barrier established for managing Major Hazards.

Each Safety Critical Task should be assigned to a responsible HSE Critical Position. Personnel in these positions should be competent in executing the activity allocated to them. Note: HSE Critical Position is any position who is required to carry out a Safety Critical Task. i.e. Field operator, HSE engineer, maintenance technician.

Safety Critical Tasks should have safety critical procedures that have been properly designed and are supported by appropriate training programmes to ensure successful operation. Good communication of operational instructions should equip personnel to better fulfil duties for safe operation and maintenance of the plant. Safety Critical Tasks (SCTs) should be used as a basis for defining the competency criteria for those HSE critical positions.

Several SCTs could be derived from a single barrier. All critical barriers on the Bowtie must be supported by at least one Safety Critical Task to maintain the Barrier performance.

Safety Critical Tasks should be written in the active form (e.g. Initiate Emergency Response according to an Emergency Response Plan), and should be linked to procedures or processes which are identified to ensure that the activity is carried out when, and as, required and be written in the form of (who does what when and how often).

One of the deliverables from bowtie workshop and performance standard documents is the list of SCTs and the associated HSE Critical Position that is responsible for executing the SCT.



SCT could be derived from:

- A Human Barrier where a human action is required to prevent or limit the consequences of major accidents,
- Performance standard document where people are required to inspect, maintain or test an SCE, or
- From any other general requirement i.e. PSM element.

Annex (8) shows examples for Safety Critical tasks.

14. Verification of Performance Standard Assurance tasks

SCE verification activities should be defined both for the project phase and operate phase; those for the project phase aim to ensure initial suitability of the SCEs, whereas those for the operate phase aim to ensure their ongoing suitability.

	Major Accident Hazard Management Guideline	
	Document No: EGPC-PSM-GL-006	

Verification process shall be done by an independent party, not the party who is responsible for the assurance 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 assurance activities are done properly.



Verification aims to confirm that the company's SCE assurance processes are:

- Defined, implemented and complied with;
- Executed by competent persons;
- Providing suitable SCEs (i.e. initial suitability); and,
- Demonstrating that SCEs continue to perform as required (i.e. ongoing suitability, and not undermined by change).

Verification should be governed by the verification scheme stated in the performance standard document. The company could incorporate the verification requirement in its audit program.

15. References

[1]	CCPS, 2018. <i>BOW TIES IN RISK MANAGEMENT - A Concept Book for Process Safety</i> . New York: John Wiley & Sons, Inc..
[2]	Energy Institute, 2020. <i>Guidelines for management of safety critical Elements (SCEs)</i> . 3rd ed. London.: Energy Institute.
[3]	ISO, 2016. <i>Petroleum and natural gas industries - Offshore production installations - Major Accident Hazard management during the design of new installations (ISO17776)</i> . Brussels: EUROPEAN COMMITTEE FOR STANDARDIZATION.

	Major Accident Hazard Management Guideline	
	Document No: EGPC-PSM-GL-006	

16. Annexes

Annex (1) typical examples for the Major Accident Hazards

Hazard Number (ref. ISO 17776)	Examples	Sources
H-01.01	Oil under pressure	Flowlines, pipelines, pressure vessels and piping
H-01.02	Hydrocarbons in formation	Oil wells especially during well drilling and entry/workover operations
H-01.03	LPGs (e.g. propane)	Process fractionating equipment, storage tanks, transport trucks and rail cars
H-01.04	LNGs	Cryogenic plants, tankers
H-01.05	Condensate, NGL	Gas wells, gas pipelines, gas separation vessels
H-01.06	Hydrocarbon gas	Oil/gas separators, gas processing plants, compressors, gas pipelines
H-08.01	On-land transport (driving)	Driving to and from locations and camps, transporting materials, supplies and products, seismic operations, moving drilling rigs and workover rigs
H-08.02	On-water transport (boating)	Boat transport to and from locations and camps, transporting materials, supplies and products, marine seismic operations, barges moving drilling rigs and workover rigs
H-08.03	In-air transport (flying)	Helicopter and fixed wing travel to and from locations and camps, transporting materials, supplies and products
H-20.01	H ₂ S (hydrogen sulphide, sour gas)	Sour gas production, bacterial activity in stagnant water, confined spaces in sour operations
H-20.05	Chlorine	Water treatment facilities
H-21.04	Methanol	Gas drying and hydrate control

Note: Not all Major Accident Hazards listed are applicable at all facilities, and others not listed may be applicable.

Annex (2) – Bowtie methodology and examples

Note: This annex is extracted from the AIChE CCPS bowtie concept book-2018 [3].

The Bow tie model contains eight elements; these elements are: (1) hazard, (2) top event, (3) consequences, (4) threats, (5) prevention barriers, (6) mitigation barriers, (7) degradation factors, and (8) degradation controls.

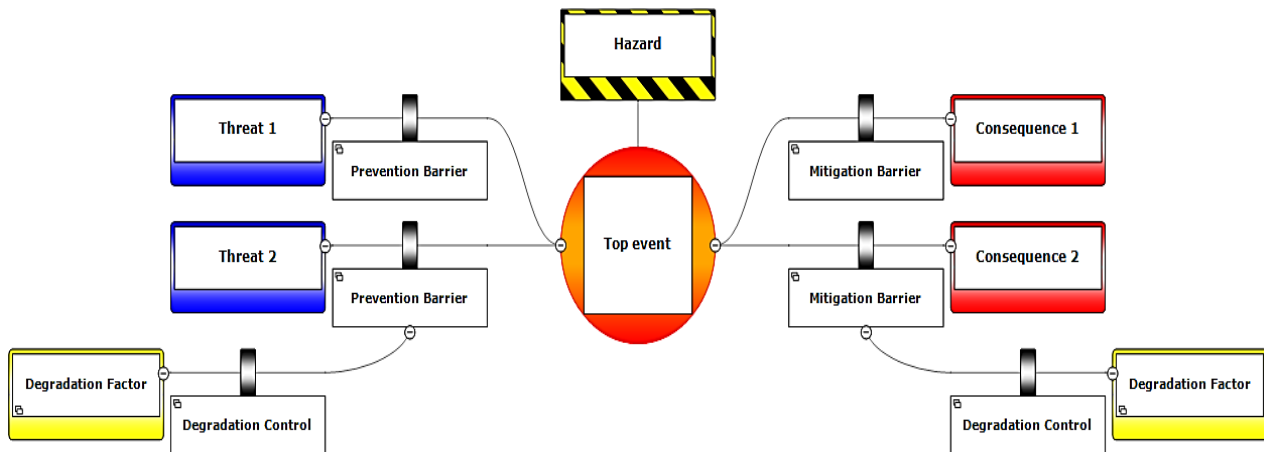


Fig. (3) - Bowtie Diagram

- **Hazard:** the Bow tie starts with the hazard.
- **Top Event:** the loss of control of the hazard.
- **Threats** are depicted on the left side (customarily the prevention side) of the Bow tie diagram.
- **Consequences** of loss of control of the hazard are depicted on the right side (customarily the mitigation side) of the Bow tie diagram.
- **Prevention Barriers** on the left side of the diagram represent prevention barriers, which stop threats from resulting in the top event.
- **Mitigation Barriers** shown to the right of the top event represent mitigation barriers, which mitigate the top event (i.e., reduce the scale of and possibly stop undesired consequences).
- **Degradation Factors** can be applied to both prevention and mitigation barriers and these are the factors that if realized can lead to impairment or failure of the barrier to which they are attached.
- **Degradation Controls** act to control the Degradation factors, helping maintain the main pathway barrier at its intended function. Degradation controls can, but do not necessarily satisfy, the effective, independent, and auditable criteria for barriers.

Constructing the Bowtie - General Information

1. Defining the Hazard:

The 'hazard' is an operation, activity or material with the potential to cause harm.

It is shown on the diagram to provide clarity to the reader as to the source of risk.

Hazards are part of normal business and are often necessary to run an operation.

Some examples of hazards are toxic materials, high pressure gases, rotating equipment, flammable liquids in atmospheric storage tanks, loading a tanker truck, manufacturing polyethylene, or processing hydrocarbons that are flammable and under pressure.

Generic hazards can lead to generic Bow ties and thus the hazard should be specific.



Hazards would normally be identified in a HAZID process. The hazard checklist in ISO 17776 (2016) can provide guidance on a wide range of potential hazards – see also Annex (1). Although it is an offshore standard, it provides good general guidance for onshore facilities as well.

Hazards should be formulated in a controlled state. A hazard description should be “transporting fuel in a truck from A to B” and not “fuel truck explosion”. A hazard describes a potentially harmful substance / process / activity and not the loss of control of the hazard.

Add detail to the hazard to determine scope and desired Bow tie detail level. If the hazard is well defined this will support more useful Bow ties. Be specific, as the level of detail set in the hazard will influence the level of detail in the rest of the Bow tie.

Well-Worded Hazard Examples are given in the table below.

Hazard	Comment – why this is well worded
Drilling in a formation with hydrocarbons under pressure	Drilling in a rock formation with hydrocarbons is part of normal business for oil and gas companies, but does have the potential to cause harm (e.g., blowouts).
Processing hydrocarbons containing H2S gas	Hydrocarbons have the usual flammable properties; the H2S gas is an additional toxic hazard that points to wider safety issues. Since these hazards are different with some possible differences in barriers, this might justify two Bow ties with one focusing on flammable hazards and one on toxic hazards.
Pressurized propane storage in sphere	Normal operational state is defined and volume in sphere will be known to those using the Bow tie
Driving a tanker on the highway	Driving a tanker on the highway is a normal requirement to get from A to B. This in itself is not a problem, but it does have the potential for loss of control.
Transporting people to and from a work site via helicopter	The activity of flying in a helicopter to a work location is well defined.

	Major Accident Hazard Management Guideline	
	Document No: EGPC-PSM-GL-006	

Poorly worded hazard examples are given in the table below.

Hazard	Comment – why this is poorly worded
Chlorine	This is too vague is it product chlorine in small cylinders, in piping, or in the main storage tank.
Uncontrolled fire	'Uncontrolled fire' is a consequence it is not a part of normal business. However, 'fighting a fire at a chemical facility' is a possible hazard, as it is an accepted part of business for the firefighting unit.
Ignition	This is part of an incident sequence it is associated with the top event 'loss of containment' of the hazard 'hydrocarbons in the process'.
Control system failure	This can be a threat, a top event, or a barrier failure, depending on the context. It does not specify the actual hazard perhaps high-pressure process fluid.
Derailment	'Derailment' is not a good description of a hazard, because it is not a part of normal business it is in fact a top event. A better hazard would be transport of crude oil by train.

2. Defining the Top Event:

Given a well-selected hazard description, the next step is to define the top event in the center of the diagram.

The top event is the moment when control over the hazard or its containment is lost, releasing its harmful potential. While the top event may have occurred, there may still be time for barriers to act to stop or mitigate the consequences.

It is possible to identify multiple top events for one hazard control can be lost over the hazard in different ways. Therefore, one hazard can result in multiple Bow tie diagrams.

The top event describes an event in which control of the hazard is lost. Common generic top events are loss of containment, loss of stability (e.g., of a floating drill rig) or loss of control (e.g., of a chemical reaction). In process safety applications dealing with hydrocarbons, the most common top event is Loss Of Containment (LOC).

Give an indication of scale if possible. As with the hazard specification, it is often good practice to quantify the top event. Thus, rather than just 'hydrocarbon leak', it might be better to differentiate rupture and small leak as many of the barriers and consequences will be different.

In formulating the hazard and top event, the analyst should always be thinking, "Is this top event too narrow so that we will need several diagrams to cover the risks surrounding this asset or operation? Can we do the same analysis using one Bow tie rather than several? Or is it too broad, and should we split it up to several Bow ties?" A test is to ask: "How many threats and consequences can we build for this top event?" If it is only one or two, the top event may be too narrow. If it is more than ten, perhaps it is too broad (or by its nature, it is possible that there are many valid threats). However, there can be cases where a single threat or consequence is worthy of analysis if their magnitude is sufficiently large.

Well-Worded Top Event Examples are given in the table below.



Hazard	Top Event	Comment – why this is well worded
Drilling into formation containing hydrocarbons under pressure	Loss of well control Influx of hydrocarbons	The loss of well control can be due to either an influx of hydrocarbons into the well or a loss of drilling fluids into a permeable formation. Since the barriers are different, two Bow ties are appropriate one for the influx of hydrocarbons and the other for loss of drilling fluids. The top event makes clear which is the causal mechanism.
Gasoline stored in a tank	Tank overflow and gasoline spill onto dike floor	The hazard links directly to the loss of containment event. Multiple consequences are possible which will be explored on the right side of the Bow tie.
Driving a tanker on the highway	Loss of control of the tanker	In this case, loss of control is literal losing control of the tanker is the top event.
Loads suspended by a crane	Dropped object	The dropped object is the loss of control over the lift. It leads to several possible undesired consequences, but with multiple mitigations; hence this is a good top event. It may be appended by 'or swinging loads' or be changed to 'loss of control of the load'.

Poorly Worded Top Event Examples are given in the table below.

Hazard	Top Event	Comment – why this is poorly worded
Gasoline stored in a tank	Tank overflow and major dike fire	This top event combines the actual top event with one of the possible consequences. It bypasses all the various mitigation barriers that aim to prevent ignition and reduce the consequence of a major fire.
Gasoline stored in a tank	Corrosion of the tank	'Corrosion of the tank' can be a good top event, but is not correct for this hazard. 'Corrosion of the tank' does not describe how control is lost over 'storing hydrocarbons in an atmospheric tank'. 'Corrosion of the tank' describes one of the threats that can lead to loss of control over the hazard (e.g., loss of containment).
Driving a tanker on the highway	Crashing into a tree	'Crashing into a tree' is not a good top event. A crash is not a way we lose control over our hazard, but the unwanted result of losing control over our hazard. We can identify our real top event by asking 'What was the initial loss of control that led to the crash?'

3. Defining the Consequences:

Consequences are unwanted outcomes that could result from the top event and lead to damage or harm. Generally, these would be major accident outcomes.

One top event may have multiple consequences, but normally only important consequences would be developed to show the mitigation barriers, not trivial ones.

Consequences should be described as '[Damage] due to [Event]'. It is important to include the event leading to the damage, as different barriers can be required to stop or mitigate damage depending on the event leading to the damage. 'Fatalities due to fire' might, for example, call for different mitigation barriers than 'fatalities due to toxic gases', and 'environmental damage due to smoke' can require different barriers than 'environmental damage due to liquid spill'.

Care should be taken to avoid being too specific in defining consequences, such as splitting injuries from fatalities. When reviewing a Bow tie, if all the barriers are the same on different pathways, they could normally be combined, unless differences in the risk assessments are worth noting.

Care should be taken to avoid developing a consequence that does not flow directly from the top event. This may be a temptation to address an orphan consequence that otherwise might be missed. For example, in a tank overflow top event a consequence of internal tank explosion would not be appropriate. It is better to develop a Bow tie specifically for this consequence, with a suitable hazard, top event, and threats.

Well-Worded Consequence Examples are given in the table below.

Top event	One Consequence	Comment – why this is well worded
Loss of well control	Major harm to marine wildlife due to oil pollution.	This consequence is acceptable as it defines the scale of environmental damage. Most company risk matrices include categories ranging from minor through to catastrophic, so indicating scale is useful.
Tank roof sinks	Asset damage from full surface tank fire	The consequence links directly to the top event and will allow all the various mitigation barriers to be properly included. It is specific in the type of consequence.
Loss of control over the vehicle	Driver injury / fatality due to crash into object	This range of outcomes is also a suitable consequence. Since the mitigation barriers would be the same, it is sensible to combine both injury and fatality into one consequence.
Dropped object	Impact damage and total loss of object that is dropped	This consequence is clear and directly results from the top event.

Poorly Worded Consequence Examples are given in the table below.

Top event	One Consequence	Comment – why this is Poorly worded
Gasoline tank overflow	Environmental damage Or Pollution	The consequence links directly to the top event but it is vague, and not specific as to the nature or severity of the environmental damage. Is the damage to land or water (small stream or large river?) or to specific species? Consequences should name the receptor affected. Inclusion of the scale is useful to design an adequate response from the mitigation barriers.
Loss of containment	Evacuation of the facility	A plant will be evacuated when a loss of containment of hydrocarbons escalates to a stage that recovery is no longer possible. The evacuation is however not the actual consequence but a barrier to prevent worse consequences such as multiple injuries.
Loss of control over the vehicle	Crash barrier damage	This is a possible consequence, but it is likely to be unimportant compared to other consequences and might be better grouped (e.g., 'asset damage to car and road infrastructure').
Dropped object	Delay	This consequence is also too vague. If this is a heavy lift of a critical piece of infrastructure, then delay is an important consequence and some magnitude will be important, e.g., 'project delay for over months'.

4. Defining the Threats:

Threats are potential reasons for loss of control of the hazard leading to the top event. For each top event there are normally multiple threats placed on the left side of the diagram, each representing a single scenario that could directly and independently lead to the subject top event.

When a team is brainstorming threats, a HAZOP review or HAZID study is often a valuable input as these document causes leading to major accident events, but not necessarily all potential causes.

It is important to remember that the threat, if the pathway is not prevented, must lead to the top event. In addition, (3) categories are helpful to initiate discussion in identifying threats:

- Primary equipment not performing within normal operating limits (e.g., mechanical fault - pump seal failure),
- Environmental influence (e.g., overpressure due to solar heating of blocked in pipeline),
- Operational issues (e.g., insufficient personnel present to support all required human barriers during unit start up).

Loss of containment is generally the result of one of the following issues:

- overfilling / underfilling;
- overpressure / under pressure;
- corrosion;
- stress / fatigue;
- incorrect flange torqueing;
- embrittlement;
- erosion;
- wear and tear;
- physical damage / impact; or
- Subsidence / settlement / earthquake.

Besides using these categories as inspiration, it can also be helpful to ask the question as to why a certain procedure or protocol exists there is usually a good reason.

The use of 'human error' as a threat leading directly to a top event is generally not recommended as this commonly leads to structural errors in the Bow tie as the barriers suggested are more often degradation controls. Experience shows human error is better treated as a degradation factor leading to impairment of a main pathway barrier.

Where threats use identical barriers, these can be combined on a single threat pathway.

Threats should have a direct causation and should be specific. A threat is direct when the causal relationship between the threat and the top event is clear without additional explanation. For example, direct threats for the top event 'loss of control of vehicle' can be 'driving on slippery road' and 'reduced visibility'. 'Bad weather conditions' does itself not describe what will cause someone to lose control over their vehicle.

Threats should be sufficient. Each threat itself should be sufficient to lead to the top event. If a threat can only cause the top event in combination with another threat, it is not sufficient in itself and therefore incorrect.

Threats are not barrier failures. Formulating a threat as the failure of a barrier is one of the most frequent mistakes when constructing a Bow tie diagram. A barrier failure on its own does not lead to a top event, because the barrier failure is a control that stops the actual threat from reaching the top event. A failed barrier, such as a broken lock in a Lock out Tag out, has no 'energy' and does not initiate or accelerate an unwanted chain of events by contrast, a threat, such as mechanical impact, actually contains the energy to lead to a top event.

Well-Worded Threat Examples are given in the table below.

Threat	Top event	Comment – why this is well worded
Excess filling of tank	Tank overflow	The threat links directly to the top event without the need for other combination threats and it is a credible cause.
Excess speed for road conditions	Loss of control over the vehicle	The threat links directly to the top event. The hazard would be driving a vehicle.

Lifting unbalanced load	Dropped object	An unbalanced load on lifting equipment can cause a load to fall and thus is a direct cause of the top event.
-------------------------	----------------	---

Poorly Worded Threat Examples are given in the table below.

Threat	Top event	Comment – why this is Poorly worded
High pressure well	Loss of well control	This could be a threat, but it is poorly worded. All wells increase in pressure at greater depths, so this is a normal condition. A better threat for this issue would be ‘unexpected pressure increase in well’.
Level gauge out of Preventive maintenance cycle	Tank overflow	The threat is not a direct cause of tank overflow just because it is late on a preventive maintenance cycle. The threat is excess flow into the tank and the barrier is associated with operator vigilance using the level gauge.
Failure of anti-lock braking system (ABS)	Loss of control over the car	This is a safety system which has failed. It does not cause the top event on its own. A better threat would be a sudden burst tire.
Wind during lift operation	Dropped object	Wind can lead to swinging load and ultimately to a dropped object, but the threat is too generic. A better threat would be ‘Strong wind (> 9m/sec)’ as this is a much clearer indication of the challenge to the integrity of the lift.

5. Defining Barriers:

Barriers must have the capability on their own to prevent or mitigate a Bow tie sequence, they could be physical or non-physical measures. Barriers in bowtie must be: (effective, independent, and auditable) this is in order to meet the validity requirements of the barrier.

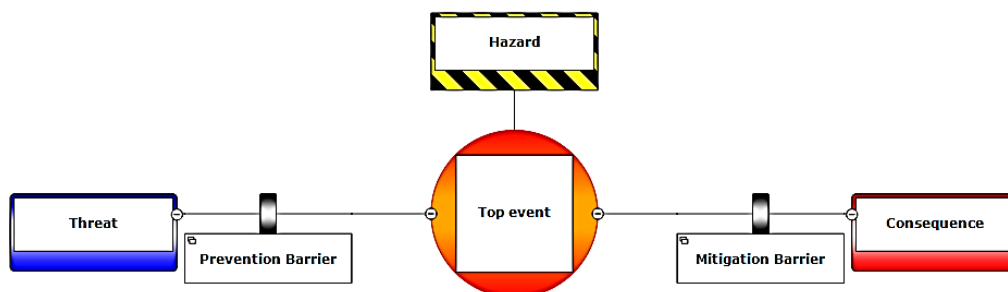


Fig. (4) - Bowtie showing Prevention and Mitigation Barriers on either side of Top Event

Prevention barriers:



A prevention barrier is a barrier that prevents the top event from occurring. A key test for a prevention barrier is that it must be capable of completely stopping the top event on its own. This does not mean that it is 100% reliable, only that in principle it can prevent or terminate a threat sequence (for example, a properly sized pressure relief valve can prevent a top event of 'pressure vessel burst', but it can fail if the degradation control 'routine recalibration of relief valve' does not occur).

There are two main ways in which a prevention barrier can have effect: either to prevent the threat from occurring in the first place, or to stop an occurring threat from leading to the top event.

Mitigation barriers:

Mitigation barriers (on the consequence side of the Bow tie) are employed after the top event has occurred and should help an organization prevent or reduce losses and regain control after it has been lost.

There are two main ways in which a mitigation barrier can have effect either to stop the consequence from occurring (ignition prevention), or to reduce the magnitude of the consequence (detection, response, and ESD). A mitigation barrier can have a lower weight in calculating / evaluation the risk reduction achieved than a prevention barrier in that it may only mitigate, not terminate, a consequence.

Barriers types:

Barrier type identifies the main operating characteristic of the barrier. There are five possible types of barriers:

- Passive hardware;
- Active hardware;
- Active hardware + human;
- Active human;
- Continuous hardware.

Active barriers must have separate elements of 'detect-decide-act', i.e., 'detect' a change in condition or what is going wrong, 'decide' what action is required to rectify the change and 'act' to stop the threat from progressing further.

If any of the detect-decide-act elements is missing from an active barrier, the barrier will not be able to stop the threat. For example:

- A firefighting system could be perfectly designed for realistic fire scenarios, but it will not function if no 'detect' element is present to allow a person or controller to decide that the system is required and then to activate it.
- A very good alarm (detect) is ineffective if it does not lead to a suitable response action. Thus, the barrier would be 'alarm and operator response'. Operator response includes both the decide and act elements.
- An 'emergency shutdown valve' (act) on its own is not a barrier. The system must include 'detect and decide' elements or the barrier will not function.





If any element of detect-decide-act is missing, then showing this as a barrier gives a false sense of security by portraying a barrier that is not fully functional.

An overview of barrier types and the associated 'detect-decide-act' elements are given in the table below.

Barrier Type	Description	Detect	Decide	Act	Examples
Passive Hardware	The barrier works by virtue of its presence.	N/A	N/A	N/A	Dike, blast wall, crash barrier, anticorrosion paint
Active Hardware	All elements of the barrier are executed by technology.	Technology (e.g., pressure sensor)	Technology (e.g., logic controller)	Technology (e.g., emergency shutdown valve)	Process control systems and Safety Instrumented Systems
Active Hardware + Human (Predominately hardware)	The barrier is a combination of human behavior and technological execution.	Technology (e.g., high high-level indicator and alarm)	Human (e.g., operator hears and responds to alarm)	Technology (e.g., emergency shutdown valve) Or Human (e.g., operator manually shuts valve)	Operator activated ESD valve Gas alarm and decision by human to evacuate
Active Human (Predominately human)	The barrier consists of human actions, often interacting with technology.	Human observation (e.g., operator walk around detects leak)	Human evaluation (e.g., decides to shut down and isolate the equipment)	Human - but acting on technology (e.g., operator presses stop button or manually shuts a valve)	Operator detection and response (e.g., during structured walk arounds)
Continuous Hardware	The barrier is always operating.	N/A	N/A	Technological	Ventilation system, impressed current cathodic protection

Note: Not all barriers can fit exactly within the barrier type model, particularly for mitigation barriers (e.g., ignition control is a blend of passive (electrical switch cubicles) and active hardware (shutdown of powered systems)).

Barrier Properties:

 EGPC	Major Accident Hazard Management Guideline Document No: EGPC-PSM-GL-006	
--	--	---

In order for a barrier to be a valid barrier, it should be effective, independent, and auditable.

Effective:

A prevention barrier is described as ‘effective’ if it performs the intended function when demanded and to the standard intended, and it is capable on its own of preventing a threat from developing into the top event. A mitigation barrier is described as ‘effective’ if it is capable of either completely mitigating the consequences of a top event, or significantly reducing the severity.

Examples of common mistakes when representing effective barriers on a Bow tie include:

- Referencing ‘training’ and ‘competency’ as barriers: these are degradation controls and would appear on a degradation pathway supporting the barrier to which they apply.
- Identifying incomplete barriers e.g., ‘fire & gas detection’. While these are important barrier elements, they do not constitute a complete barrier as they rely on other elements to completely stop the scenario from developing further. For this example, a complete barrier could be ‘fire and gas detection, automatic logic controller (or human response to alarm) and ESD’.

In order for human barriers to be effective amongst other issue there needs to be:

- Appropriate procedures that cover operational actions, and
- Operator training in the procedures.

Independent:

Barriers should be independent of the threat and of other barriers on that pathway. For example, if the threat was loss of power and a barrier requires power to operate, then that would not be a permissible barrier in that pathway.

A common mode failure occurs when one event causes two or more barriers to fail. Ideally, there should be no common mode failure possible for all the barriers in a pathway and they should satisfy the ‘independence’ property. Unfortunately, this is practically impossible. All barriers tend to have some commonality, either being maintained or operated by the same team, or even just being part of the same organization.

In most situations, common mode failures that affect all barriers are not very likely. But realistic commonalities do exist, such as barriers that are reliant on the same critical service (e.g., electricity) or the same person being responsible for or performing the procedural steps of multiple barriers.

Although it is important to have as little common mode between barriers as possible, it is not necessary to remove barriers with some minor aspect of a common mode. The barriers may have a common mode in one scenario (for example, in power outage), but work independently in other scenarios. Nonetheless, this risk of a plausible common mode failure should be managed by the addition of other barriers that do not have this common mode. Adding different types of barriers (such as active and passive, e.g., firewater system and firewalls) is advisable and usually can help avoid some general common mode failures.

In the case of two barriers that rely on the same operator to push a button, the operator is a common mode and absence of the operator could be a likely reason for failure of both. When one barrier then fails because of the absence of the operator, the second barrier provides minimal additional security and should be removed from the Bow tie.

Auditable:

Barriers should be capable of being audited to check that they work. Formally, it could be that performance standards are assigned to the functionality of a barrier. For example, a performance standard for an ESD valve would ideally include ‘periodic end to end testing’, i.e., a signal is placed upon the detection device, the logic controller responds, and activates the end device, e.g., the ESD valve.

Barrier Sequencing:

Barriers should be placed in time sequence of their effect. The most logical way of placing barriers in a diagram is in time sequence of their effect. The advice is thus to place the barriers in the order in which they are called upon, so it is clear when each barrier is needed. Often this means that design controls appear first (e.g., steel containment envelope, which includes the design criteria of material selection, pressure specification), followed by operational controls, then automatic trips, etc. An example is provided for one of the most commonly used threat lines for a loss of containment Bow tie ‘Operating outside of operating envelope’.

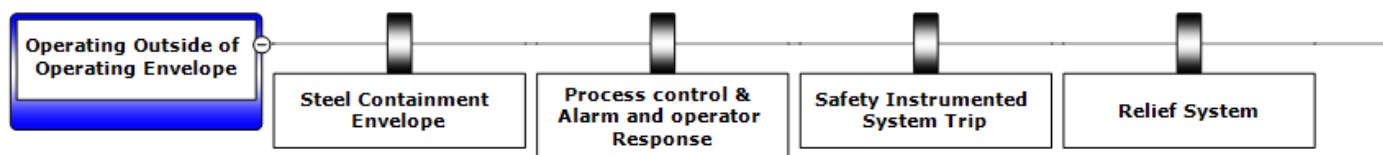


Fig. (5) - Demonstration of Time-ordered Barrier Sequence

Barrier Metadata:

Additional information, or ‘metadata’ could be added to the barriers. Several different types of information are available depending on the nature of the various Bow tie elements. Such metadata can usually be displayed or hidden by Bow tie software, depending on the communication objective. The most common types of barrier metadata include: effectiveness or strength, condition, accountability and barrier type. The preference of which metadata to display can differ during design and operation. For example, displaying effectiveness may be more important during design risk reviews, whereas condition is more important during operational risk reviews.

Barrier Examples:

Barrier titles are important to clearly communicate the specific function of the barrier. Well worded, short titles help to communicate the barriers deployed and for quality checking. The most common mistakes regarding barriers are:

- Displaying multiple barriers that are actually elements of a single barrier;
- Having barrier titles that are not informative;
- Placing barriers on the wrong side of the Bow tie top event; and,
- Including measures which are not barriers at all (e.g., degradation controls which belong on degradation factor pathways, e.g., training, competence).

Well-Worded Barrier Examples are given in the table below.

Top event – Threat / Consequence	Barrier	Comment – Barrier Type Descriptions
Tank overflow – Hydrocarbons affect environment	Mitigation: Dike	This is a passive hardware barrier as the dike is continuously present. It is somewhat of a simplification as dikes must have some way to drain rainwater and if a drain valve is used this may be left open. This should be shown as a degradation factor for the dike.
Loss of control over the car - Driver impacts dashboard	Mitigation: Air bags	This is an active hardware barrier as the air bag system must detect when deceleration is above a critical threshold and then actuate an ignition device.
Loss of containment to water – Major environmental pollution event	Mitigation: Detect leak and deploy spill response equipment	This is a Hardware + Human barrier as it combines mechanical booms and boats with operator actions.

Poorly Worded Barrier Examples are given in the table below.

Top event – Threat / Consequence	Barrier	Comment – why this is poorly worded/placed
Loss of well control – Poor cementing job	Prevention: Blowout Preventer (BOP)	This is a difficult barrier as BOPs have multiple safety devices with both a prevention function and a mitigation function the exact definition of loss of well control is also a factor (e.g., influx of hydrocarbons or uncontrolled blowout). Thus, the barrier should be renamed to make clear which part of the BOP is providing the prevention function (e.g., annular rams).
Tank overflow – Excessive flow from the upstream	Prevention: Deploy foam protection	The barrier description is poor as it does not convey Detect-Decide-Act clearly. In addition, categorization as a prevention barrier is incorrect as deploying foam protection only occurs after the spill event, so this is a mitigation barrier. Foam does have a fire prevention function, but it is still a mitigation barrier as it acts after control of the hazard has been lost (i.e., after the top event).
Loss of containment – Fatalities due to fire	Mitigation: Fire detection system	This barrier only contains a 'detect' component and no 'decide' or 'act' capability.



Leakage – Fatalities due to fire	Mitigation: Adhering to emergency response plan	Although this barrier is technically correct, it is a very generic barrier that could be placed on almost any Bow tie. Consider whether this barrier is useful in the Bow tie, given its goal and audience. A greater focus on fire response would be appropriate.
Loss of containment – Seal failure	Prevention: Maintenance plan	The maintenance plan is not a measure that can stop the threat. A better barrier would be ‘appropriate seal fitted to specification’, and the maintenance plan is then a degradation control on the degradation factor line to ensure that the seal integrity is maintained.
Loss of control over the car – Driving too quickly	Prevention: Crash barrier	The passive barrier description is good, but the placement is incorrect. It is a mitigation barrier because the crash barrier provides its function after control of the vehicle has been lost.
Dropped object – unbalanced load	Prevention: Watchman	This barrier, if it is just someone watching the activity, is not effective for prevention. It could be that the team meant that this person would verify that the crane safety systems were properly deployed and that a job safety assessment had been conducted. This would be an example of a useful control that is so poorly described that it conveys no useful information to the reader.

6. Defining Degradation Factors and Degradation Controls

Degradation factors and degradation controls are drawn in the Bow tie diagram below the barriers to which they apply. Controls along the degradation pathway are called degradation controls. The degradation factor is a condition that can reduce the effectiveness of the barrier to which it is attached. A degradation factor does not directly cause a top event or consequence, but since it degrades the main pathway barrier, the likelihood of reaching undesired consequences will be higher.

A degradation factor can apply to barriers on either side of the Bow tie diagram.

Degradation controls frequently do not fully meet the criteria of a barrier (effective, independent, and auditable) although they will be stronger if they do meet these criteria. Similarly, active degradation controls may not contain all elements of detect decide act as this is only a requirement for barriers. They are frequently human and organizational factors concerned with the management of risk and barrier assurance.

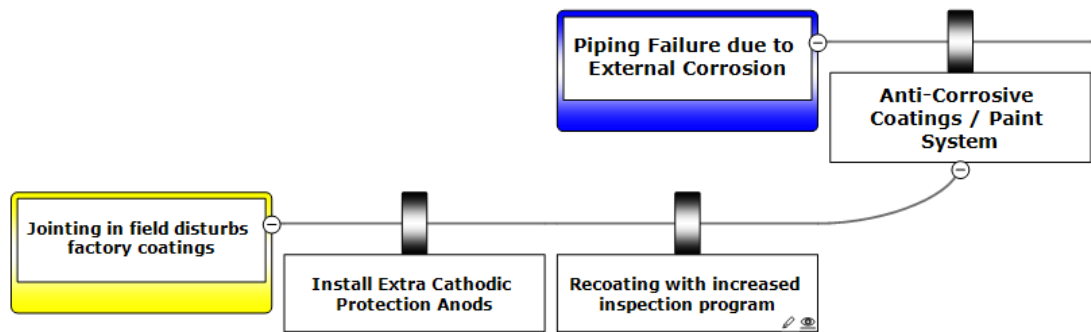


Fig. (6) - Example Placement of Degradation Control on Degradation Pathway

Examples of degradation controls that rely on human and organizational factors include engineering standards, contractor management, management of change systems, training, Job Safety Assessments, stop work authority, etc.

It is a common error to place degradation controls onto Bow tie main pathways. This causes confusion for two reasons it loses the connectivity between which degradation controls are supporting which barrier, and it presents an incorrect visualization of too many barriers on the main pathway. This can give the impression of greater defenses in depth (that many barriers protect against that threat) than actually exist, and intuitively that the risk associated with the threat is adequately controlled, when in fact there are only two barriers.

Multiple degradation factors can apply to a single barrier. It is common to have one or two degradation factors, but more than three can become complex.

Since the focus is on the more important barriers, the diagram complexity is favorably reduced by either not developing degradation pathways for less important barriers or, if these are developed for all barriers, then only displaying the less important ones when that additional level is important.

Degradation factors should not normally simply negate the barrier. It is generally not advisable to express degradation factors as the negation of the barrier. For example, if 'high level trip' is the main barrier, a degradation factor could be titled 'high level trip fails'. A better degradation factor might be 'level measurement device incorrectly calibrated' with degradation controls such as 'preventive maintenance for fluid level measuring instruments', 'instrument calibration', and then 'audit that the calibration is carried out'. The negation approach can lead to too many degradation factors and too general degradation controls making a diagram unnecessarily complex.

Well-Worded Degradation Factors and Degradation Controls Examples are given in the table below.

Main Pathway Barrier	Degradation Factor	Degradation Control	Comment
Alarm and upwind mustering of staff	Wind direction unclear in congested plant or at night	Illuminated wind indicators on elevated equipment	This degradation factor highlights a specific circumstance in which the barrier may fail.



Major Accident Hazard Management Guideline



Document No: EGPC-PSM-GL-006



Steel containment envelope	Equipment does not comply with process requirements	Formal design review against engineering standards. Asset integrity program to maintain the containment envelope.	This is a general degradation factor and it allows for the inclusion of multiple activities that need to be done to ensure proper design review.
Alarm and evacuation	New staff or visitors not trained in evacuation	Training for all new staff and visitors in evacuation.	This example highlights that training is usually a degradation control. (Note evacuation alone is not a barrier as it misses the detect element required of an active barrier).

Poorly-Worded Degradation Factors and Degradation Controls Examples are given in the table below.

Main Pathway Barrier	Degradation Factor	Degradation Control	Comment
Pressure relief valve	No pressure relief valve	Design to include pressure relief valve	The degradation factor doesn't identify the real cause of the problem. 'Pressure relief valve removed for service' is an example of a credible problem, and allows a suitable safeguard, such as 'Back up pressure relief valve'.
Pressure relief valve	Pressure relief valve blocked	Periodic PRV bench testing	This degradation control is not correct because it does not act upon the degradation factor 'Pressure relief valve blocked'. The use of a negation for the degradation factor does not make clear that the cause of blockage is due to the closing of adjacent block valves.
Wearing a seatbelt	Forgetting to wear seatbelt	Airbag	This degradation control is also not correct, because it does not act upon the 'Forgetting to wear seatbelt'. It should be a main pathway barrier.

 EGPC	Major Accident Hazard Management Guideline	
	Document No: EGPC-PSM-GL-006	

Annex (3) Bowtie checklist

1- Hazard

	Check	Yes	No	Comment
1	Is the hazard a physical situation, condition or material property that has the potential to cause harm such as injury or death to people, damage to property and investments, environmental damage, business interruption and loss of reputation.			
2	Is the hazard of the bowtie defined by considering the normal controlled state of operations, Is the hazard clearly expressed with enough details?			

2- Top Event

	Check	Yes	No	Comment
1	Is the top event a loss of control of the hazard and not a consequence?			
2	Can the top event credibly lead to the consequence of concern?			
3	Number of threats is adequate? If less than 3 that means a narrow top event, if more than 10 means a wide top event.			

3- Consequences

	Check	Yes	No	Comment
1	Is the consequence defined as '[Damage] due to [Event]'?			
2	Do all consequences cover the full range of significant outcomes?			
3	Do all consequences flow from the top event?			
4	Can all consequences be fully understood?			



4- Threats

	Check	Yes	No	Comment
1	Does the threat refer to the means by which a hazard may be realized?			
2	Does the threat lead directly to the top event and able to cause the top event independently?			
3	Is the threat considered a human error? (Shouldn't be)			
4	Is the threat properly specified?			
5	Can all threats be fully understood?			

5- Barriers

	Check	Yes	No	Comment
1	Is the barrier a physical or non-physical or a combination, and the intent is to prevent, control, mitigate or protect from accidents or undesired events?			
2	Are barriers independent of the threat and other barriers on the pathway?			
3	Are barriers effective in stopping the top event, or mitigating the consequence?			
4	Do active barriers have an element of 'Detect – Decide – Act'?			
5	Are barriers capable of being audited to check that they work and that they remain effective?			
6	Are barriers placed in sequence of their effort?			
7	Are barriers adequate (effectiveness and number)?			

5- Degradation Factor

	Check	Yes	No	Comment
1	Are degradation factors conditions which can reduce the effectiveness of the barrier to which it is attached?			
2	Are degradation factors consider the real reason behind a barrier failure?			

5- Degradation Controls

	Check	Yes	No	Comment
1	Have degradation controls been included on the main pathway instead of degradation pathways?			

Annex (4) Barrier Effectiveness Criteria

Rating	Is it used? Is it in place?	Does it work/is it effective/human dependency?	Bow tie code
Very Good	Always	Control has more than a 99.5 % chance of working when required, no human involvement	
Good	Frequently	Control has a > 90 % chance of working when required, little human involvement	
Average	Mainly	Control has a < 90 % > 60 % chance of working when required, active human involvement	
Poor	Occasionally	Control has a < 60 % > 30 % chance of working when required, very active human involvement, complex and stressful to operate	
Very Poor	Rarely	Control has less than a 30 % chance of working when required, continuous human involvement, very complex	

Example:

If a tank is surrounded by a dike and the capacity of the dike is less than the tank capacity, could not contain all the spill capacity, then this barrier is considered not effective and will not be presented in bowtie as a barrier.

If the capacity of the dike is of appropriate design for the tank capacity and the spills will be fully contained within the dike, then the dike is considered an effective barrier and effectiveness rating could be decided.

As the dike is a passive barrier with more than a 99.5 % chance of working when required and does not require any human involvement, then the effectiveness rating is “very good” and colored “dark green”.

Annex (5) Barrier Adequacy Criteria

The barrier adequacy criteria specify what is deemed suitable and sufficient control of threats and mitigation of / recovery from consequences. The following criteria should be considered as a minimum number of barriers and not an absolute requirement. Where less barriers are identified, additional controls / actions should be identified to reduce the risks to ALARP.

Table below presents the barrier criteria which shall be adopted to evaluate the barriers adequacy.

Barrier	Extreme High Risk (6A)	Very High Risk (4A, 5A, 5B, 6B, 6C)	High Risk (1A, 2A, 3A, 4B,5C,)
Threat Controls (Preventive)	Minimum of three (3) independent effective barriers to be in place for each identified threat.	Minimum of two (2) independent effective barriers to be in place for each identified threat.	Minimum of two (2) independent effective barriers to be in place for each identified threat.
Recovery Preparedness Measures (Mitigation)	Minimum of three (3) independent effective barriers for each consequence.	Minimum of two (2) independent effective barriers for each consequence.	Minimum of two (2) independent effective barriers for each consequence
Escalation Factor Controls	Minimum of two (2) independent effective escalation factor controls for each identified escalation factor.	Minimum of two (2) independent effective escalation factor controls for each identified escalation factor.	Minimum of one (1) independent effective escalation factor control for each identified escalation factor.

Below figure shows Barrier adequacy criteria mapped on RAM based on Risk Level for MAH area, (Extreme High Risk, Very High Risk & High Risk).

Likelihood		Rare	Unlikely	Possible	Likely	Very Likely	Almost Certain
Severity	#	1	2	3	4	5	6
Disastrous	A	1A	2A	3A	4A	5A	6A
Catastrophic	B	1B	2B	3B	4B	5B	6B
Major	C	1C	2C	3C	4C	5C	6C
Serious	D	1D	2D	3D	4D	5D	6D
Minor	E	1E	2E	3E	4E	5E	6E
Notable	F	1F	2F	3F	4F	5F	6F

Fig. (7) - Barrier adequacy criteria mapped on RAM

Notes:

1. To examine of barriers adequacy to demonstrate risk to ALARP. All barriers shall be independent.
2. Barrier shall be considered effective with minimum good rating (light green).
3. One (1) good barrier (light green) is considered equal = two (2) average barrier (Yellow).
4. The team can choose to compensate for a weaker barrier by strengthening the other barrier or adding an additional one.

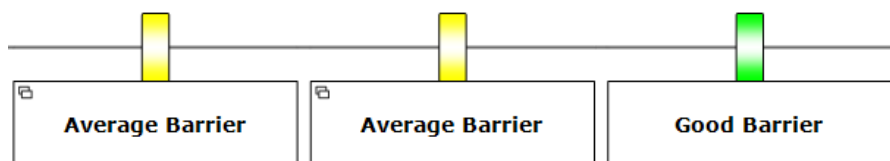
Example on how to achieve two effective barriers:



Two "Good" Barriers



If two "Good" could not be achieved, second barrier has to be stronger than "Good" to compensate for weakness in the first one



Or, two lower strength barriers "Average" are to be compensated by a higher strength barrier

Fig. (8) - Example for effective barriers

Annex (6) SCE Group for Each Barrier

Note: Below Figures for SCE groups are extracted from the Energy Institute guidelines for management of safety critical elements, 2020.

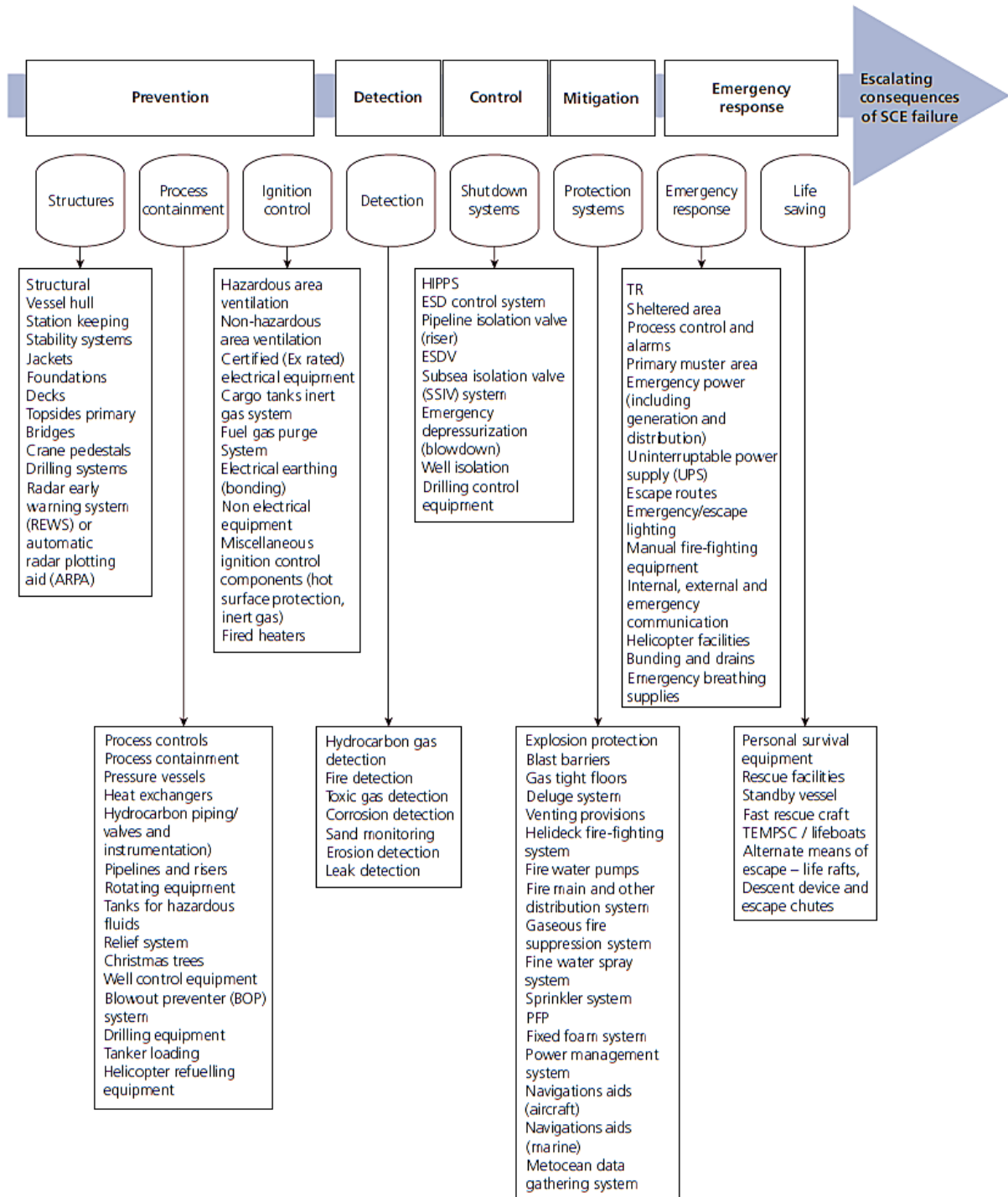


Fig. (9) - Typical SCEs for an offshore Exploration and Production facility

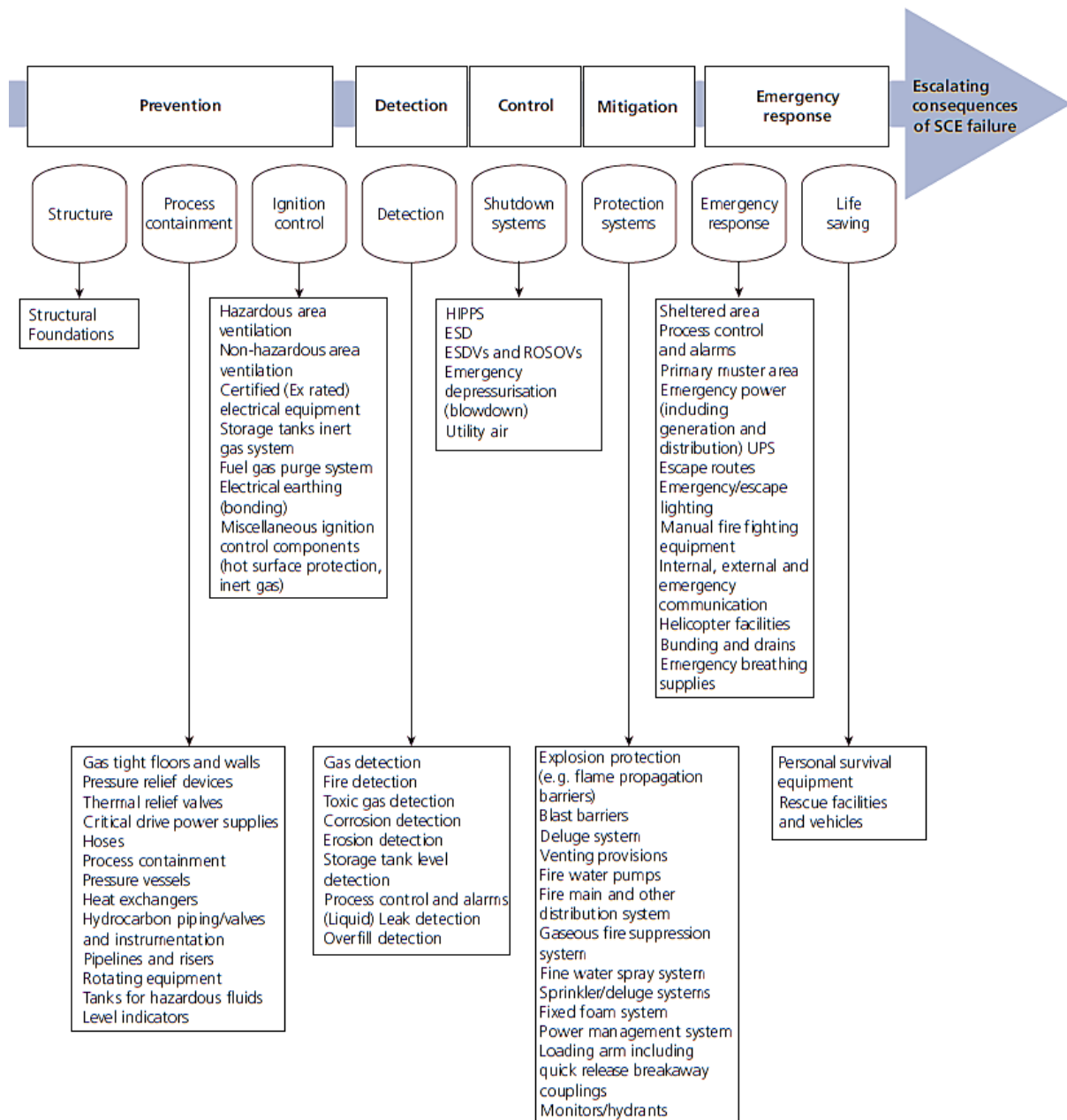




Fig. (10) - Typical SCEs for an onshore petroleum refinery

	Major Accident Hazard Management Guideline	
	Document No: EGPC-PSM-GL-006	

Annex (7) Operation Performance Standard example

SCE	Emergency lighting for a fixed offshore installation
Reference	[number]
Revision	[number/date]
Goal	To provide illumination to facilitate the successful use of control spaces, egress, evacuation and escape routes, muster and embarkation areas and evacuation systems following a major incident.
Scope/system boundaries	<p>In certain areas, lighting is considered safety critical and these luminaires are provided additionally with battery back-up and are suitable for the hazardous area in which they are located.</p> <p>Battery backed-up luminaires comprise the emergency lighting system and are installed in the following locations:</p> <ul style="list-style-type: none"> – central control room (CCR); – muster stations; – location of fire-fighting/safety equipment; – exit doorways; – incident control room (ICR); – fire team assembly areas; – all egress, evacuation and escape routes; – local electrical rooms (LERs)/switch-rooms; – radio room; – totally enclosed motor propelled survival craft (TEMPSC) and chute/ life raft.

Functionality			
Function	Criteria	Assurance	Verification
Emergency illumination levels Provide sufficient emergency illumination	<p>Illumination levels in those parts of the platform that require emergency lighting comply with CIBSE Application guide: Lighting in hostile and hazardous environments</p> <p>Compliance criteria 1:</p> <ul style="list-style-type: none"> – Emergency luminaires shall function for a minimum duration of 90 minutes – Minimum lux levels shall be: <ul style="list-style-type: none"> – egress, evacuation and escape routes: minimum 1 lux at floor; – muster, embarkation and TEMPSC area: minimum 5 lux at floor, and – LER/switch-room, CCR and ICR: minimum 15 lux at floor 	<p>Compliance criteria 1: Emergency lighting lux level and discharge test – 1 yearly</p>	<p>Attend Emergency lighting lux level and discharge test - Ensure compliance with the test plan and compare with the acceptance criteria – 1 yearly</p>



Major Accident Hazard Management Guideline



Document No: EGPC-PSM-GL-006

	<p>A PS failure is:</p> <ul style="list-style-type: none"> – Failure to achieve the minimum lux level at the end of the discharge period – Failure of three or more adjacent light fittings in any one area 		
<p>Emergency luminaires – Zone 1</p> <p>Design of emergency luminaires to suit flammable atmospheres</p>	<p>Emergency luminaires to be suitable for zone 1 hazardous areas in which they are installed</p>	<p>Consider maintaining Ex integrity of emergency luminaires</p>	<p>Review the maintenance records – 1 yearly</p>



Availability
<p>Individual emergency lighting luminaries are required to operate on battery power in the event of main power failure.</p> <p>The design and layout of the luminaries provides multiple redundancy.</p> <p>Allowing for the level of redundancy available, an availability of 90 % is required for each luminaire.</p>

Reliability
<p>Individual emergency lighting luminaries are required to operate on battery power for a period of 90 minutes.</p> <p>A reliability of 90 % for 90 minutes is required for each luminaire.</p>

Survivability
<p>Individual field devices are not expected to survive an MAH and survivability is considered in design via layout of equipment.</p>

Interactions	
PS	Criteria
Escape routes	Provide sufficient illumination for escape routes
Certified (Ex rated) electrical equipment	Selection of suitable luminaries
Primary muster area	Provide sufficient illumination for muster area
Lifeboat	Provide sufficient illumination for muster, embarkation and lifeboat
TR	Provide illumination for TR

Note: Performance standard for each SCE should focus on the relevant project phase i.e. for design performance standard should focus on the design specifications, while operation performance standard should focus on maintenance, inspection and testing.

 EGPC	Major Accident Hazard Management Guideline	
	Document No: EGPC-PSM-GL-006	

Annex (8) Safety Critical Tasks example

Bowtie Reference No.	Barrier/Degradation Control	Safety Critical Task	HSE Critical Position	Reference document
XXXX	Dipping operation is carried out to ensure the liquid level inside the tank	Carryout dipping operation for the storage tanks to estimate the liquid level	Field Operator	Operating Procedure No. xxxxxx
XXXX	Firewater pump with sufficient pumping rate activated automatically in case of fire	Perform annual performance test for the firewater pump to ensure pump status against the pump characteristics curve	Maintenance Engineer	Firewater pump manual and characteristics curve
		Perform a weekly run test for the pump to ensure its operability	Operation Engineer	Fire water system operating procedure – document No. xxxx
XXXX	Random drug and alcohol testing for professional drivers	Perform random drug and alcohol testing for professional drivers	Site Doctor	Drug and Alcohol Procedure – document No. xxxx
XXXX	Pressure relief Valve	Inspect/Test the relief valve periodically	Integrity Engineer	Relief valve inspection policy – document No. xxxx
XXXX	Safety Instrumented System with Trip function Close the inlet valves	Maintain and Test Safety Instrumented Loops (Sensor, Logic Solver & Final Element)	I&C Engineer	Maintenance Plan SIS performance standard – document No. xxxx