



Exploration & Production

GENERAL SPECIFICATION

Field Operations

GS EP EXP 407

Identification of Safety Critical Elements

01	01/2012	Updating of generic list of SCEs, title. Section 4
00	01/2011	First Issue
Rev.	Date	Notes

Owner: OPS/EXP

Managing entity: OPS/EXP



Contents

1. Scope	3
2. Reference documents.....	3
3. Introduction	4
3.1 Purpose	4
3.2 Definitions	4
3.3 General process for managing SCE.....	6
4. Workpack 1- Identification of SCE.....	7
4.1 Step 1- Collect Risk Assessments outcomes	7
4.2 Step 2 – Identify SCEs.....	7
4.3 Step 3 – Establish SCE sponsors.....	8
4.4 Step 4 – Establish the specific list of SCE	9
5. Workpack 2 – Establish Performance Standards for SCE.....	12
5.1 Definition.....	12
5.2 Step 1 - Establish Performance Standards.....	13
5.3 Step 2 – Validation.....	13
5.4 Step 3 – Loading and management of SCEs in the CMMS	13
Bibliography.....	14
Glossary of terms	15
Appendix 1 Generic List of SCE.....	18
Appendix 2 Example Major Risk Register (from PRA).....	25
Appendix 3 Example of Bow Tie Representation.....	27
Appendix 4 Example format of SCE registers	29
Appendix 5 Example format of Performance Standards	34



1. Scope

This document intends to provide Maintenance and Inspection Engineering Contractors with the methodology for identifying Safety Critical Elements (SCE) and preparing the baseframe requirements for managing SCEs.

This document applies to all Total E&P projects and operated installations.

2. Reference documents

The reference documents listed below form an integral part of this General Specification. Unless otherwise stipulated, the applicable version of these documents, including relevant appendices and supplements, is the latest revision published at the EFFECTIVE DATE of the CONTRACT.

Standards

Reference	Title
Not applicable	

Professional Documents

Reference	Title
Not applicable	

Regulations

Reference	Title
Not applicable	

Codes

Reference	Title
Not applicable	

Other documents

Reference	Title
Not applicable	



Total General Specifications

Reference	Title
GS EP SAF 041	Technological Risk Assessment Methodology
GS EP EXP 311	Plant Integrity, Minimum Inspection Requirements

3. Introduction

3.1 Purpose

Total E&P have defined the requirements to manage Asset Integrity. The objective is to ensure that the people, systems, processes & resources, which deliver integrity, are in place, in use and fit for purpose over the whole lifecycle of the assets.

To achieve this while considering the vast inventory of assets and activities the general principle is to concentrate management efforts on those elements being the most critical to safety, the objective being to minimize the risk of major accidents. These elements are designated as Safety Critical Elements (SCE).

Total's Integrity Management (IM) expectations are also to take benefit from improved safe operation practices to maximize production performance. The improvement is expected to result from increased facilities availability and more robust operational processes. Elements having a major impact on production performance or financial aspects are designated as Business Critical Elements (BCE).

This document defines how SCEs should be identified and how their minimum performance requirements should be formalised. Requirements for identifying and managing BCEs are not described in this document.

Present General Specification is intended to be used by Contractors mandated by Total Project Groups. It can be included as part of Maintenance & Inspection Engineering Contracts (MIEC) or separately.

3.2 Definitions

Definitions adopted by Total E&P are as follows:

An element can designate a physical piece of equipment, an activity, a work process, a person or an organisation.

Safety Critical Elements (SCE) are any element (as defined above) whose failure will either cause or contribute to a major accident, the purpose of which is to prevent or limit the effect of a major accident (UKOOA). SCE are equivalent to Safety Critical Measures (SCM) introduced in [GS EP SAF 041](#).

Business Critical Elements (BCE) include elements whose failure would have a major impact on production or asset value.

Major Accident Hazard Scenarios (MAH) are defined as "The scenarios with potential damage severity of "catastrophic" or above to people, environment or asset". According to Total rules (re. [GS EP SAF 041](#)) such situations correspond to the red squared zone of the risk matrix shown in fig. 1 below. These scenarios are also referred as Major Scenarios in this document. It should be noted that this definition implies that the severity of consequences is the leading

criteria and elements falling into the “green area” of the matrix may be SCEs even though the probability of occurrence of concerned scenario is very low.

From the above definitions, it should be understood that SCEs form the barriers protecting the personnel and assets from a major hazardous event. Operators shall then focus efforts on identifying credible major accident hazards and then identifying SCEs which will prevent, control, mitigate and facilitate the safe evacuation from the identified hazards.

Because of the essential role of SCEs, assurance activities (maintenance, inspection and testing) must be put in place to continuously demonstrate that they remain fit for purpose during the whole life of the installations.

Other equipment having a similar role but which would not be active or operated in the occurrence of major accident hazards will not be considered as SCEs. This does not mean they should not be submitted to appropriate maintenance, inspection or testing as they may be important to field operations activities.

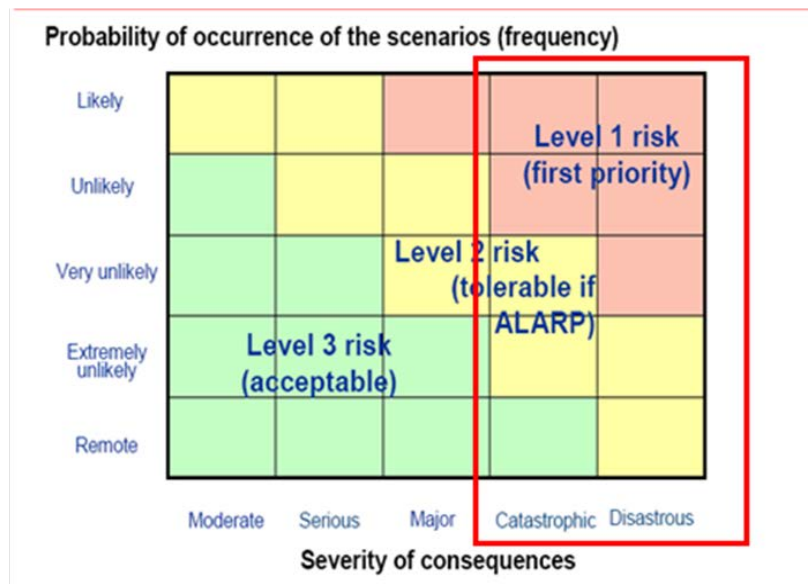
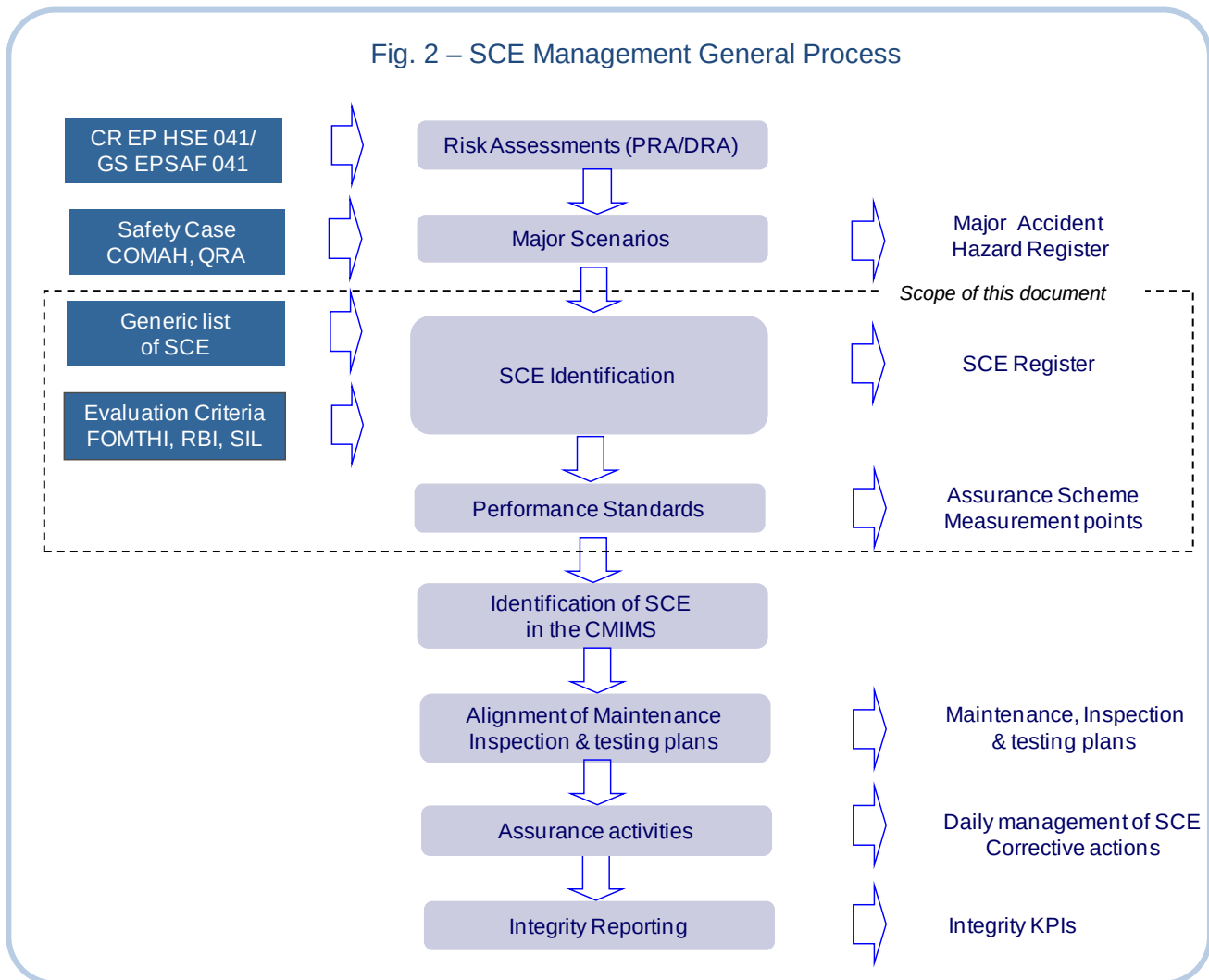


Fig. 1 – Scenarios generated or controlled by SCEs

3.3 General process for managing SCE

The overall process can be illustrated by the following diagram:

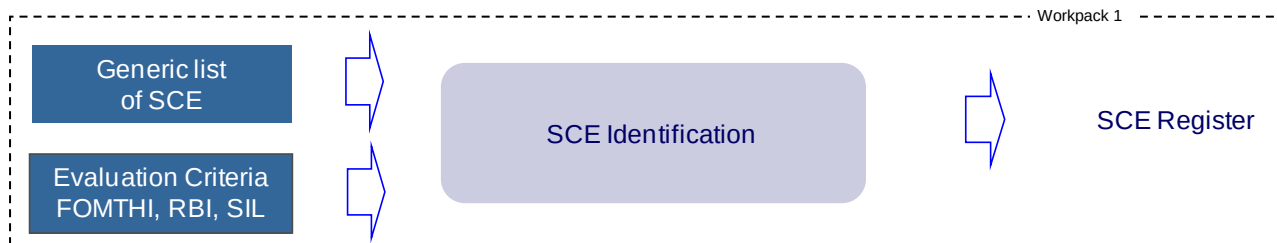


The process is based on a step by step approach, each step requiring separate work packs and dedicated competences.

The dotted line in the above diagram shows the scope of this document

The following sections segregate the process in successive workpacks, each workpack being split into several steps that are to be conducted in sequence. Workpacks may be left to different contractors as the nature of the work varies significantly from one to the other. The given split and scope of workpacks is indicative only, and can be adjusted to project needs or to the organization of the affiliate, especially when the work is partially done using internal resources.

4. Workpack 1- Identification of SCE



4.1 Step 1- Collect Risk Assessments outcomes

In Total E&P risk assessment (RA) is a mandatory requirement being part of the control of major Technological Risks. **GS EP SAF 041** defines dedicated methodologies and responsibilities for conducting preliminary and detailed risk assessments (PRA/DRA), during the project phase and during the operation phase. RA studies are generally performed by specialist contractors.

The outcome of these studies is the creation of a Risk Register and action plan. The Risk Register describes the major risks and provides clear links between the identified risks and control measures, systems, processes and procedures implemented to manage/mitigate the risk.

For some projects, conducting these assessments is already subject to local regulatory requirements. They are sanctioned by e.g. COMAH/HSEIA processes (UK, NL, UAE). Reports are available and can be used, although assessments may not fully comply with **GS EP SAF 041**.

In other cases Quantitative Risk Assessments (QRA) may have been conducted as part of project requirements.

All available RA realized by the project or the affiliate shall be collected and gathered within a dedicated "Risk Assessment Dossier" for future reference.

4.2 Step 2 – Identify SCEs

By principle, and in compliance with **GS EP SAF 041**, the identification of SCEs shall be directly derived from the major scenarios that have been analysed during the Detailed Risk Assessment (DRA) stage of the risk assessment process. Comprehensive assessment is needed to identify SCE on the basis of their quantified influence on risks, considering especially the impact when they fail on demand.

In order to simplify the evaluation, an acceptable approach will be to identify SCE from a generic list instead of considering the whole inventory of facilities and activities. With the growing experience gained over the recent years, especially in the North Sea, such an approach is becoming a standard practice for operators. At this stage, it is considered that SCEs are identified at the function level, not at the single equipment TAG level. In other words, a detailed identification of all the components constituting SCEs is not required. The objective of the task is to identify individual SCE functions effectively present within the installations.

The list of SCE functions specific to concerned facilities shall be based on the generic list provided in appendix 1.

The generic list shall be screened in detail and tailored to comply with actual facilities asset register, by removing assets that do not exist in the concerned installations e.g. offshore related assets if concerned development is onshore. Additions may be done as deemed necessary for project specific items.

SCE classification given in attached generic list shall be respected so as to ensure system coherence throughout affiliates.

- Level 1: Protective role
 - P Hazard Prevention*
 - C Hazard Control*
 - M Hazard Mitigation*
 - E Evacuation, Escape & Rescue*
 - S Staff competency*
- Level 2 : Critical Function
 - P1 to P18**
 - C1 to C14**
 - M1 to M10**
 - E1 to E12**
 - S1**
- Level 3: SCE
 - P1.1 to P1.n**
 - C1.1 to C1.n**
 - Etc.*

The classification shall be used in all aspects of SCE management, especially for identifying SCE in the CIMMS and reporting on Asset Integrity.

4.3 Step 3 – Establish SCE sponsors

Once the generic list is established, it is important to clearly define who shall be the lead discipline in charge of the establishment of the requirements attached to each SCE. In general, the proposed SCE classification allows one key discipline per class to be easily identified, a single discipline quite often being in charge of several classes of SCEs. For example Instruments are usually in charge of Process Control SCEs (P7) and Hazard Control (C1, C2, C3, etc.).

During the project phase, Key SCE sponsors shall be identified within project organisation. Their role is to establish the detailed list of SCEs being within their area of work, verify/establish generic performance standards, ensure adequacy of design solutions and supplies, validate assurance activities, etc.

It is important that a Task leader is formally nominated in order to ensure the coordination, the consistency and timely delivery of the task. The Project Lead Integrity Engineer or the Integrity Manager of the affiliate (as relevant) are the natural candidates.

4.4 Step 4 – Establish the specific list of SCE

Identifying individual SCE by simply screening and tailoring the asset inventory as per the elements of the generic list of SCE does not identify those elements that are potentially involved in major scenarios nor those which control or mitigate the risks associated with major scenarios. Many items from the generic list may be involved in non-major scenarios outside the squared “major risk area” shown in fig. 1 section 1.2.

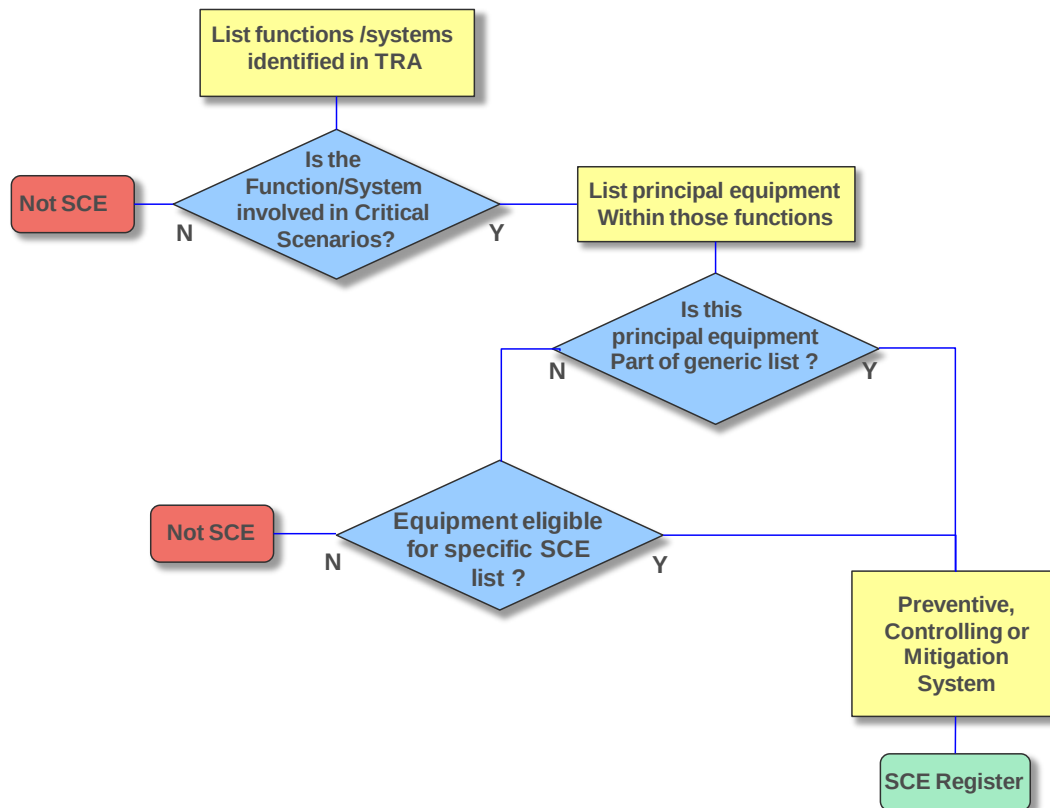
Step 4 consists in selecting for each SCE class of the generic list, those individual SCEs involved in scenarios belonging to the categories “disastrous” or “catastrophic” as per the definitions of Total E&P risk matrix.

The reference basis shall be the “Risk Assessment Dossier” established during step 1, which should include the “Major Risk Register” required by **GS EP SAF 041**. The Major Risk Register is the collection of major scenarios. A typical example is given in Appendix 2, showing the main elements of the Register i.e.

- The critical Scenarios,
- The main causes of the event,
- The associated preventive measures,
- The associated mitigation measures.

The key sources of data from which SCE shall be identified will be the PIDs for process equipment and construction files for other equipment, e.g. structures.

The general process can be illustrated by the following simplified chart.



Pending on the time at which the identification of SCE is conducted within the project overall schedule, the asset register may not be fully available at the time of implementation of present work scope. In this case the list of SCE will have to be established directly from the review of PID for process systems or from construction files for other assets (structures, wells, lifting appliances, subsea equipment, etc.).

SCE shall be identified as elements being in the same time:-

- 1- Hardware or activity belonging to the generic list of SCEs
- 2- An identified barrier in the “Disastrous” or “Catastrophic” major scenarios.

The Bow Tie format representation of scenarios shall be used to identify the barriers and SCEs involved and to verify they belong to a major scenario. An example is given in Appendix 3 extracted from same study as above.

There is a large part of qualitative judgment in this assessment. Many secondary pieces of equipment can theoretically be found belonging physically to a SCE and then become SCE themselves. Common sense and pragmatic judgment shall be used to define the contour of an SCE without unnecessary complication. As a general guideline, reference to Maintenance practice will generally help to define the appropriate extent of the SCE.

For example, an ESDV is composed of many elements including the valve, the actuator, the instrumented control loops, the detectors, etc. All could be individually considered as SCE as their failure could compromise the response of the protective system. However a good way to define the contour of SCEs is to consider how the system is maintained and how it is tested. In this case the valve and its actuator can hardly be segregated as they will be tested and



maintained in the same time. Detectors should be separated as they are submitted to specific testing regime, depending on their reliability and SIL. Same would apply to the control system.

In the proposed SCE Register format (see below) the lowest SCE level that reflects the above principle is designated "Principal Equipment Item Concerned"

Overall, the objective should be also to ensure that SCEs are selected with a sufficient degree of discrimination, so as to ensure that the reporting of their condition reflects a true control of the risks. This task requires sound engineering judgment. Should it be conducted by a Contractor's Team or by an affiliate task group, it is important that those teams gather all required competences, basically:

- A Field Operations representative: to identify equipment belonging to a scenario, to help understand logic controls and safety systems
- A safety engineering specialist: To help understand and analyse TRA outputs
- A Maintenance/Inspection representative: to define measuring points, routes and associated tasks
- The Asset Integrity manager (as relevant): To coordinate the task and maintain coherence over time
- Discipline specialists on demand (instruments, structures, marine, subsea, logistics, etc.) : to incorporate discipline technical input

The determination of the criticality of an SCE is not a required step of the process. However this parameter may be available as a result of specific assessments such as RBI or SIL assessments. It can therefore be used for possible more detailed evaluations.

Reporting format: The SCE Register

The minimum information to be provided in the SCE Register is:

1. The SCE Reference
2. The SCE Function
3. The General SCE Designation
4. The Principal Equipment Items
5. The Major Scenario(s) the SCE is contributing to
6. The type of contribution of the SCE (Protection, Mitigation, Escape)
7. The Sponsor of the SCE
8. Reference of associated Performance Standard

All major "Catastrophic" and "Disastrous" scenarios identified during the TRA must be referenced in the SCE Register.

The tabulated format given in Appendix 3 is provided for guidance only., Please note that only three scenarios are mentioned for the sake of clarity. In reality, several tenths of critical scenarios can be identified.

Finally, it can be noted that the proposed format will allow the easy identification of SCEs being involved in several critical scenarios.

Workpack 1 Deliverables

- 1- The Risk Assessment dossier
- 2- The SCE Register.

5. Workpack 2 – Establish Performance Standards for SCE



5.1 Definition

Performance standards are the key technical requirements to be met by SCEs in order to ensure they are effectively operable on demand, they perform as expected and they have some capacity to survive incidents.

Performance standards describe the goal of an SCE in its safety critical role and the performance requirements/thresholds (acceptance criteria) the SCE must meet during design and operational life.

As introduced earlier, assurance activities (maintenance, inspection and testing) must be put in place to continuously demonstrate that SCEs remain fit for purpose during their whole service life. It should be noted that most of assurance activities required for SCEs are usually already in place through preventive maintenance (PM) programmes and Inspection programmes. However SCEs may deserve “special treatment” i.e. specific inspection frequency, more thorough maintenance regime or possibly stricter tolerances in their management.

It is not directly implied that an SCE should be given the highest level of urgency when scheduling inspection, testing or maintenance activities. The scheduling of assurance activities should be also based on reliability aspects, so as to avoid unnecessary checks or to avoid too frequent checks that have limited added value in demonstrating fitness for purpose.

Performance standards (PS) include all the controls that are needed to verify SCE integrity together with the minimum performance that should be maintained for each control point. It is important to note that the requirements set in PS may not coincide with original design specifications of the equipment. PS should rather correspond to operational needs. Typical example is the output of a firepump that should satisfy the actual firewater worst case demand, which could be lower than the OEM specified max output.

Performance Standards should cover at least three main areas of control:

1. **Functionality** – What to control to ensure the equipment fulfils its functions

Example: for an ESD Valve - pressure containment, mechanical activation, system activation (control loop), closure time

2. **Availability, reliability** – At what frequency should it be controlled and maintained to meet performance/integrity minimum requirements

Example for an ESD Valve: testing frequency for partial and full stroke, instrument loop testing, based on SIL assessments

3. **Survivability** – Does the equipment need to keep its functions during an incident and how to maintain this capacity

Example for an ESD Valve: fail safe philosophy, fire proofing