

DEP SPECIFICATION

PREPARATION OF SAFEGUARDING MEMORANDA AND PROCESS SAFEGUARDING FLOW SCHEMES

DEP 01.00.02.12-Gen.

February 2011

(DEP Circular 15/12 has been incorporated)

ECCN EAR99

DESIGN AND ENGINEERING PRACTICE

DEM1



© 2011 Shell Group of companies

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, published or transmitted, in any form or by any means, without the prior written permission of the copyright owner or Shell Global Solutions International BV.

This document contains information that is classified as EAR99 and, as a consequence, can neither be exported nor re-exported to any country which is under an embargo of the U.S. government pursuant to Part 746 of the Export Administration Regulations (15 C.F.R. Parts 746) nor can be made available to any national of such country. In addition, the information in this document cannot be exported nor re-exported to an end-user or for an end-use that is prohibited by Part 744 of the Export Administration Regulations (15 C.F.R. Parts 744).

PREFACE

DEP (Design and Engineering Practice) publications reflect the views, at the time of publication, of Shell Global Solutions International B.V. (Shell GSI) and, in some cases, of other Shell Companies.

These views are based on the experience acquired during involvement with the design, construction, operation and maintenance of processing units and facilities. Where deemed appropriate DEPs are based on, or reference international, regional, national and industry standards.

The objective is to set the recommended standard for good design and engineering practice to be applied by Shell companies in oil and gas production, oil refining, gas handling, gasification, chemical processing, or any other such facility, and thereby to help achieve maximum technical and economic benefit from standardization.

The information set forth in these publications is provided to Shell companies for their consideration and decision to implement. This is of particular importance where DEPs may not cover every requirement or diversity of condition at each locality. The system of DEPs is expected to be sufficiently flexible to allow individual Operating Units to adapt the information set forth in DEPs to their own environment and requirements.

When Contractors or Manufacturers/Suppliers use DEPs, they shall be solely responsible for such use, including the quality of their work and the attainment of the required design and engineering standards. In particular, for those requirements not specifically covered, the Principal will typically expect them to follow those design and engineering practices that will achieve at least the same level of integrity as reflected in the DEPs. If in doubt, the Contractor or Manufacturer/Supplier shall, without detracting from his own responsibility, consult the Principal.

The right to obtain and to use DEPs is restricted, and is typically granted by Shell GSI (and in some cases by other Shell Companies) under a Service Agreement or a License Agreement. This right is granted primarily to Shell companies and other companies receiving technical advice and services from Shell GSI or another Shell Company. Consequently, three categories of users of DEPs can be distinguished:

- 1) Operating Units having a Service Agreement with Shell GSI or another Shell Company. The use of DEPs by these Operating Units is subject in all respects to the terms and conditions of the relevant Service Agreement.
- 2) Other parties who are authorised to use DEPs subject to appropriate contractual arrangements (whether as part of a Service Agreement or otherwise).
- 3) Contractors/subcontractors and Manufacturers/Suppliers under a contract with users referred to under 1) or 2) which requires that tenders for projects, materials supplied or - generally - work performed on behalf of the said users comply with the relevant standards.

Subject to any particular terms and conditions as may be set forth in specific agreements with users, Shell GSI disclaims any liability of whatsoever nature for any damage (including injury or death) suffered by any company or person whomsoever as a result of or in connection with the use, application or implementation of any DEP, combination of DEPs or any part thereof, even if it is wholly or partly caused by negligence on the part of Shell GSI or other Shell Company. The benefit of this disclaimer shall inure in all respects to Shell GSI and/or any Shell Company, or companies affiliated to these companies, that may issue DEPs or advise or require the use of DEPs.

Without prejudice to any specific terms in respect of confidentiality under relevant contractual arrangements, DEPs shall not, without the prior written consent of Shell GSI, be disclosed by users to any company or person whomsoever and the DEPs shall be used exclusively for the purpose for which they have been provided to the user. They shall be returned after use, including any copies which shall only be made by users with the express prior written consent of Shell GSI. The copyright of DEPs vests in Shell Group of companies. Users shall arrange for DEPs to be held in safe custody and Shell GSI may at any time require information satisfactory to them in order to ascertain how users implement this requirement.

All administrative queries should be directed to the DEP Administrator in Shell GSI.

TABLE OF CONTENTS

1.	INTRODUCTION	4
1.1	SCOPE.....	4
1.2	DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS	4
1.3	DEFINITIONS	4
1.4	ABBREVIATIONS	7
1.5	CROSS-REFERENCES	8
1.6	SUMMARY OF MAIN CHANGES.....	8
1.7	DUAL UNITS.....	9
1.8	COMMENTS ON THIS DEP	9
2.	GENERAL.....	10
2.1	OBJECTIVES.....	10
2.2	BASIS.....	10
2.3	REQUIREMENTS	11
3.	FORMAT OF THE SAFEGUARDING MEMORANDUM.....	12
3.1	SECTION 1 - INTRODUCTION	12
3.2	SECTION 2 - PREMISES	12
3.3	SECTION 3 - SAFEGUARDING ELEMENTS	13
3.4	SECTION 4 - INTERFACES BETWEEN SYSTEMS AND UNITS	17
3.5	SECTION 5 - MISCELLANEOUS	19
3.6	SECTION 6 - PROCESS SAFEGUARDING FLOW SCHEME (PSFS)	20
3.7	SECTION 7 - APPENDIX.....	22
4.	REFERENCES	23

APPENDICES

APPENDIX A	EXAMPLE - EQUIPMENT PROTECTION SUMMARY TABLE - SECTION 3.3.1.1.....	24
APPENDIX B	EXAMPLE - PUMP PRESSURE SUMMARY TABLE - SECTION 3.3.1.2.....	27
APPENDIX C	EXAMPLE - UNIT TURNDOWN LIMIT TABLE – SECTION 3.3.1.5	28
APPENDIX D	EXAMPLE - INSTRUMENTED PROTECTION FUNCTIONS TABLE – SECTION 3.3.1.6.....	29
APPENDIX E	EXAMPLES - REMOTE OPERATION VALVE TABLES – SECTION 3.3.2.1	30
APPENDIX F	EXAMPLE - CLASS 1 CHECK VALVE TABLE – SECTION 3.3.2.4.....	31
APPENDIX G	EXAMPLE - INTERFACES BETWEEN HIGH & LOW PRESSURES – SECTION 3.4.2.....	32
APPENDIX H	EXAMPLE - UNIT FLARE LOAD TABLE – SECTION 3.4.5	35

1. INTRODUCTION

1.1 SCOPE

This DEP specifies requirements and gives recommendations for preparation of the Safeguarding Memoranda (SGM) and Process Safeguarding Flow Schemes (PSFS) to be prepared for each new construction or major modification project.

The project manager is responsible for the delivery of a safeguarding memorandum as per this DEP.

The Principal is responsible for ensuring that the safeguarding of an existing unit is studied and developed before any modification is made to process conditions, equipment, piping or instrumentation.

The SGM and PSFS are required to be updated as an integral part of the plant change procedure.

Changes to the original design are recommended to be followed up by a re-assessment of the ultimate level of protection, including the re-sizing of the capacity determining components.

This DEP contains mandatory requirements to mitigate process safety risks in accordance with Design Engineering Manual DEM 1 – Application of Technical Standards.

This is a revision of the DEP of the same number dated January 2010 which has been fully revised; see (1.5) regarding the changes.

1.2 DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS

Unless otherwise authorised by Shell GSI, the distribution of this DEP is confined to Shell companies and, where necessary, to Contractors and Manufacturers/Suppliers nominated by them. Any authorized access to DEPs does not for that reason constitute an authorization to any documents, data or information to which the DEPs may refer.

This DEP is intended for use in facilities related to oil and gas production, gas handling, oil refining, chemical processing, gasification, distribution and supply/marketing. This DEP may also be applied in other similar facilities.

When DEPs are applied, a Management of Change (MOC) process should be implemented; this is of particular importance when existing facilities are to be modified.

If national and/or local regulations exist in which some of the requirements could be more stringent than in this DEP, the Contractor shall determine by careful scrutiny which of the requirements are the more stringent and which combination of requirements will be acceptable with regards to the safety, environmental, economic and legal aspects. In all cases the Contractor shall inform the Principal of any deviation from the requirements of this DEP which is considered to be necessary in order to comply with national and/or local regulations. The Principal may then negotiate with the Authorities concerned, the objective being to obtain agreement to follow this DEP as closely as possible.

1.3 DEFINITIONS

1.3.1 General definitions

The **Contractor** is the party that carries out all or part of the design, engineering, procurement, construction, commissioning or management of a project or operation of a facility. The Principal may undertake all or part of the duties of the Contractor.

The **Manufacturer/Supplier** is the party that manufactures or supplies equipment and services to perform the duties specified by the Contractor.

The **Principal** is the party that initiates the project and ultimately pays for it. The Principal may also include an agent or consultant authorised to act for, and on behalf of, the Principal.

The word **shall** indicates a requirement.

The capitalised term **SHALL [PS]** indicates a process safety requirement.

The word **should** indicates a recommendation.

1.3.2 Specific definitions

The following definitions shall apply in the context of Safeguarding Memoranda (SGM) and Process Safeguarding Flow Schemes (PSFS).

Term	Definition
Administrative Controls	Operational and maintenance procedures that, along with proper training and/or supportive measures, ensure that personnel actions do not compromise overpressure protection.
Capacity determining components	Elements that when (fully) open or removed can lead to relief flows. Typically referred to if the “Element related relief load” would lead to or contribute more than 25% of the maximum defined relief load.
Car Seal	Band or wire that has to be broken in order to change the valve position. Car seals installed on a valve inhibit unauthorized valve operation. A valve can be Car Seal Open (CSO) or Car Seal Closed (CSC). Structured procedures and highly discipline organization to ensure proper operation of these valves.
Interlock System	Mechanism which allows operation of the two or more valves only when a proper key is inserted in a specified order to ensure the correct sequence of opening and closing the valves.
Class I Check Valves	Check valves that are inspected to assure reliable operation. Refer to DEP 80.45.10.11-Gen. for more guidance on Class 1 Check valves
Process Engineering Flow Sheet	A drawing depicting equipment configuration, control instrumentation, interconnecting piping and certain mechanical details for a portion of a process or utility system. Also known as a Piping and Instrumentation Diagram (P&ID) Engineering Flow Diagram (EFD), and Utility Flow Diagram (UFD).
Final Elements	See Ultimate Safeguards. Note that final elements are also used related to the acting element in IPFs (see below).
Hazard	a physical situation potentially entailing human injury, loss of equipment or production, or environmental pollution
Instrumented Protective Function (IPF)	A function comprising one or more sensors, a Logic Solver and one or more Final Elements whose purpose is to prevent or mitigate hazardous situations and that have SIL 1, SIL 2, SIL 3 or SIL 4. An IPF is intended to achieve or maintain a safe state for the process, in respect of a specific hazardous event. In IEC 61508 and IEC 61511 an IPF is referred to as a Safety Instrumented Function (SIF)
Instrumented Protective System (IPS)	The electromechanical, electronic and/or programmable electronic Logic Solver component of the Instrumented Protective Function, complete with input and output equipment. In IEC 61508 and IEC 61511 an IPS is referred to as a ‘Logic Solver’.

Term	Definition
Limiting Elements	Devices or systems that are intended to limit the quantity/ effect of a loss of containment e.g. RO, control valve CV.
Locked Valve	Chain padlock and/ or key lock system installed around a valve that has to be broken in order to change the valve position. Locks installed on a valve inhibit unauthorized valve operation. A valve can be Locked Open (LO) or Locked Closed (LC). Structured procedures and highly discipline organization are required to ensure proper operation of these valves.
Management of Change (MOC)	The scope of MOC Standard (ST) covers changes that affect health, safety and environmental (HSE) performance, product quality (PQ), and reliability.
Mitigating systems	Systems or elements that function as barriers specifically included in the design to prevent process conditions or scenarios that would lead to activation of ultimate safeguards; and limit the consequences of an uncontrolled loss of containment. Examples: IPFs to prevent relief and/or impact on health, assets and environment; class I check valves, ROVs, emergency depressuring systems, etc.
Pressure System Safety Study (PSSS)	Structured examination of each pressure system for all potential overpressure and under pressure scenarios
Pressure System	Equipment and attached piping that are pressure protected by a common relief device(s). The boundaries of a pressure system are defined by system components that can affect mass/energy flows into or out of the system (e.g., control valves, operating valves, check valves, pumps, etc.). Generally, only those system components immediately upstream and downstream of the system equipment/piping are considered when establishing system boundaries
Process Safety Assessment	A structured procedure whereby hazards associated with a process are identified and evaluated (i.e. PHA, HAZOP, desk safety review, technical safety review, PSA, etc)
Project manager	The Project manager is the person representing the project organisation who is responsible for the project development and execution.
Penultimate safeguards	A penultimate safeguard is a formerly used term for mitigating systems that provided penultimate level of protection against uncontrolled loss of containment, mostly IPFs.
Safeguarding	Protection against uncontrolled loss of containment.

Term	Definition
Ultimate Safeguards	Devices or systems that prevent uncontrolled loss of containment. Ultimate Safeguards are considered "the last line of defence" and can be divided in the following three groups • Design: Equipment design pressure (or vacuum) that contain the pressure that results during the process deviation. • Mechanical: Hardware, such as relief devices, restriction orifices, that prevent or mitigate the process upset which could otherwise lead to an uncontrolled loss of containment. • Instrumentation: High integrity or "protective" instrument systems that prevents the process deviation which could otherwise lead to uncontrolled loss of containment; e.g. TZA protection against runaway reactions or over-firing.
Uncontrolled loss of containment	Occurs when process variables (usually pressure or temperature) exceed limits to such an extent that process equipment fails to contain the process materials. Uncontrolled loss of containment may be due to ruptures, failures of seals, gaskets, welds, etc.

1.4 ABBREVIATIONS

CSO	Car Seal Open
CSC	Car Seal Closed
DCAF	Discipline Controls and Assurance Framework
DSR	Desk Safety Review
CSO	Car Seal Open
CSC	Car Seal Closed
DCAF	Discipline Controls and Assurance Framework
DSR	Desk Safety Review
EDP	Emergency Depressuring (system)
EFD	Engineering Flow Diagram, also known as PEFS or P&IDs
ESD	Emergency Shutdown (system)
FZA	Flow emergency / safety function with alarm
IPF	Instrumented protective function
HAZOP	Hazard and Operability study
LO	Locked Open

LC	Locked Closed
LZA	Level emergency / safety function with alarm
MAWP	Maximum allowable working pressure
MOC	Management of Change
NRV	Non-return valve
PEFS	Process Engineering Flow Schemes also known as P&IDs
PFD	Process Flow Diagrams
PFS	Process Flow Schemes
PHA	Process Hazard Analysis
P&ID	Process and Instrumentation Diagrams also known as PEFs
PSA	Process Safety Assessment (includes HAZOPs, DSR, PHA, TSR, RHA, etc)
PSFS	Process Safeguarding Flow Scheme (= PSFD)
PSFD	Process Safeguarding Flow Diagram (= PSFS)
PSSS	Pressure System Safety Study
PZA	Pressure emergency / safety function with alarm
RHA	Reactive Hazard Analysis
ROV	Remotely Operated Valves
SGM	Safeguarding Memorandum
SIF	Safety Instrumented Function (equal to IPF)
TERV	Thermal Expansion Relief Valve
TSO	Tight shut-off
TSR	Technical safety Review
TZA	Temperature emergency / safety function with alarm

1.5 CROSS-REFERENCES

Where cross-references to other parts of this DEP are made, the referenced section number is shown in brackets. Other documents referenced by this DEP are listed in (4).

1.6 SUMMARY OF MAIN CHANGES

This DEP is a revision of the DEP of the same number dated January 2010. This DEP has been fully revised and based on a merger of DEP and 1-GS-5.

1.7 DUAL UNITS

**Amended per
Circular 15/12**

Dual units have been incorporated throughout this DEP.

This DEP contains both the International System (SI) units, as well as the corresponding US Customary (USC) units, which are given following the SI units in brackets. When agreed by the Principal, the indicated USC values/units may be used.

1.8 COMMENTS ON THIS DEP

Comments on this DEP may be sent to the Administrator at standards@shell.com, using the DEP Feedback Form. The DEP Feedback Form can be found on the main page of "DEPs on the Web", available through the Global Technical Standards web portal <http://www.shell.com/standards> and on the main page of the DEPs DVD-ROM.

2. GENERAL

2.1 OBJECTIVES

The Safeguarding Memorandum (SGM), of which the Process Safeguarding Flow Scheme (PSFS) is an integral part of identification and summarization of protective devices (ultimate safeguards) which are installed as the ultimate level of protection against uncontrolled loss of containment of toxic and/or flammable materials.

A SGM is intended to demonstrate that process safety measures have been identified and are implemented. It also explains the basis for their design and other critical equipment associated with their design. The Safeguarding memorandum serves as a vehicle to describe the identified and implemented process safety measures during the design and engineering stage of a project. During the operational lifetime, modifications that are planned shall be verified against the existing measures and avoid defeating its original purpose. As a result, it is a valuable tool in the original design phase and during the Management of Change (MOC) process.

Also a SGM provides an additional level of technical assurance that the original design of process unit safeguards was done correctly. The development of the Process Safeguarding Flow Scheme (PSFS) and the discussion of "Interfaces with Other Systems" are intended to ensure that the "big picture" or systems view is examined. The review of each overpressure scenario allows for rapid logic checking, and the examination of the "Equipment Protection Summary" provides a cross check to ensure each piece of equipment is appropriately protected.

For each unit of a project, a standalone SGM SHALL [PS] be developed in the course of the design and ultimately included in the Technical HSE Deliverables as defined in the Discipline Controls and Assurance Framework (DCAF). Additional copies for information may be provided to the Operators and or incorporated in the Operating Manual, as they provide a useful and important safety and training aid for operating personnel as well as contributing generally towards plant safety.

2.2 BASIS

The SGM and PSFS should be prepared from the Process Engineering Flow Schemes (PEFS) also known as Process and Instrumentation Diagrams (P&IDs), under the general guidance and responsibility of the Project Manager or the MOC Process Owner.

The SGM and PSFS shall be the result of a thorough investigation of the process design. During this investigation, all overpressure events that could result in uncontrolled loss of containment shall be identified and adequate safeguarding and protection measures shall be decided upon – protection measures such as pressure relief devices, remotely operated valves (ROVs) and Emergency depressuring valves.

The details of the instrumented protective functions (IPFs) are typically described by the process control engineer in the Control and Safeguarding Narratives document and Cause and Effect charts and are not required to be included in the SGM. However, if the site does not have an adequate control and instrumentation narrative and system in place, then the Control and Safeguarding Narratives SHALL [PS] be included in the SGM.

Sections (3) of this DEP provide the guidelines for what information should be extracted from the PEFS. The guidelines shall be followed unless there are overriding reasons for deviating from them. If deviations from these guidelines are applied, the underlying principles behind these deviations shall be recorded in a form and inserted in the Appendix of the Safeguarding Memorandum as per section (3.7) and in the Project documentation delivered to the site at the end of a project as per section (3.3.1.3.5) for critical re-examination later.

2.3 REQUIREMENTS

A SGM SHALL [PS] be developed and/or modified whenever designing or constructing new assets, process units/areas (i.e. process units, storage tank farms, utility systems) or making permanent modifications to existing assets. Accordingly, for existing process units, any changes to a unit, green field, brown field, capital or expense projects will require a review and modification of the SGM, as part of the MOC.

The scope of the SGM is limited to the equipment under the asset owner responsibility.

The scope of a SGM shall cover the entire process unit, not just the new or modified portion.

Changes to the original design should be followed up by a re-assessment of the ultimate level of protection, including the re-sizing of the capacity determining components.

The SGM and PSFS shall be updated as an integral part of the plant change procedure.

3. FORMAT OF THE SAFEGUARDING MEMORANDUM

The SGM shall be based on the following structure:

Section 1	1.0 Introduction
Section 2	2.0 Premises
Section 3	3.0 Safeguarding Elements
Section 4	4.0 Interfaces with other units
Section 5	5.0 Miscellaneous
Section 6	6.0 Process Safeguarding Flow Scheme
Section 7	7.0 Appendix

3.1 SECTION 1 - INTRODUCTION

This section shall be used to introduce the subject and specify any deviations as referred to in this DEP.

3.2 SECTION 2 - PREMISES

Section 2 shall contain the following information:

1. Description of the process unit for which the SGM is prepared. The description should contain a general description on the process with feed streams, processing of products with description of process parameters relevant to understand the process, risks, and information that is relevant for process safety understanding. Also include operational modes that are different from the normal operational mode and may have impact on the relief valve sizing and relief flow (example is regeneration mode at different temperature and composition).

A simplified block diagram with narrative description of the process. Note that this should be a one or two page high level schematic of process.

2. The SGM process design basis:

- Operating Modes:

Describe the operating modes, such as normal operation and regeneration that are used as the design basis for the safeguarding.

- Unit Throughput Limits:

Taking credit for the normal flow that is leaving a pressure system is allowed in accordance with ISO 23251 and DEP 80.45.10.11-Gen. when calculating relief loads. Such credits, however, shall be based on the minimum turndown operating limit for the equipment/process unit. Normally for operability reasons the minimum turndown should be specified in the design premise.

Rationale: If a system outflow credit was taken for pressure relief load determination at the specified minimum turndown, then the unit turndown may be controlled by the relief system design. Any turndown limitations caused by the relief system must be consistent with the design premises for operability.