DEP SPECIFICATION

HUMAN FACTORS ENGINEERING – DESIGN FOR PROCESS SAFETY CRITICAL TASKS

DEP 30.00.60.19-Gen.

February 2011

DESIGN AND ENGINEERING PRACTICE

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 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

APPENDICES

1.   INTRODUCTION

1.1   SCOPE

This new DEP specifies requirements and gives recommendations to ensure that Shell capital projects with significant risk to Asset Integrity and/or Process Safety (AIPS):

   a)   Take reasonable steps to identify and assess human tasks that are either relied on to ensure AIPS, or which could represent a significant risk to AIPS. These are referred to as "Process Safety Critical Tasks";

   b)   Are able to demonstrate that all reasonably practical engineering and design measures to ensure human reliability in these tasks have been considered and, where practical, applied.

This DEP applies to capital projects within the scope of the Opportunity Realisation Manual (ORM) that have risks in the red region of the Shell Risk Assessment Matrix (RAM).

It also applies on projects of lower capital value with risks in the red region of the RAM.

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 authorised 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 word **should** indicates a recommendation.

1.3.2   **Specific definitions**

Term	Meaning
DCS	Distributed Control System
SCADA	Supervisory Control and Data Acquisition
CWE	Common Work Environment
ESD	Emergency Shut-Down
AIPS	Asset Integrity/ Process Safety
AIPS Critical Error (ACE)	A human error which could be the initiating event in a hazardous scenario or which could occur in performing a Front Line Operational HSSE Critical Activity. Includes Threats or Escalation Factors arising from inadequate human performance. An ACE is defined at a lower level of task definition than an Initiating event or Front Line Operational HSSE Critical Activity.
AIPS Critical Task (ACT)	Tasks supporting Human Barriers or Front Line Operational HSSE Critical Activities. Includes human performance representing Barriers and Controls against Escalation Factors. ACTs should include a verb-noun pair ("do x to y") and are usually defined at a lower level of task definition than a HSSE Critical Activity.
Critical Task Inventory	A documented inventory of ACEs and ACTs identified by the project as requiring ALARP demonstration. The Inventory will exist in two versions: an initial release usually during DEFINE phase, and a final release during EXECUTE.
ALARP	As Low As Reasonably Practicable. As defined in HSSE CF Glossary - the point at which the cost (in time, money and effort) of further risk reduction is grossly disproportionate to the risk reduction achieved.
Asset Integrity	As defined in HSSE CF Glossary - the ability of an Asset to perform its required function effectively and efficiently whilst safeguarding life and the environment.
CTA	Critical Task Analysis
FEED	Front-End Engineering Design
HEMP	As defined in HSSE CF Glossary - a structured Risk analysis methodology that involves Hazard identification, Risk Assessment, selection of Controls and Recovery Measures, and comparison with tolerability and ALARP criteria.
HFE	Human Factors Engineering
HFE Co-ordinator	As defined in DEP 30.00.60.10-GEN. The project HFE Co-ordinator is an individual assigned responsibility within a project for management and organization of the project HFE activities, including coordination with the HFE Technical Authority, HFE Authorised Person and HFE Authorised SME, as appropriate. An HFE Co-ordinator shall have competence at least at HFE Knowledge level.
HFE Technical Authority	The individual assigned as Technical Authority for HFE on the project under the Shell Manual of Authorities or Discipline Control and Assurance Framework (DCAF).
Process Safety	As defined in HSSE CF Glossary - is the management of Hazards that can give rise to major accidents involving release of potentially dangerous materials, release of energy (such as fire or explosion) or both.

Process Safety Critical Tasks	Human tasks that are either relied on to ensure AIPS, or which could represent a significant risk to AIPS. The totality of ACTs and ACEs for an asset.

1.4 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 (3).
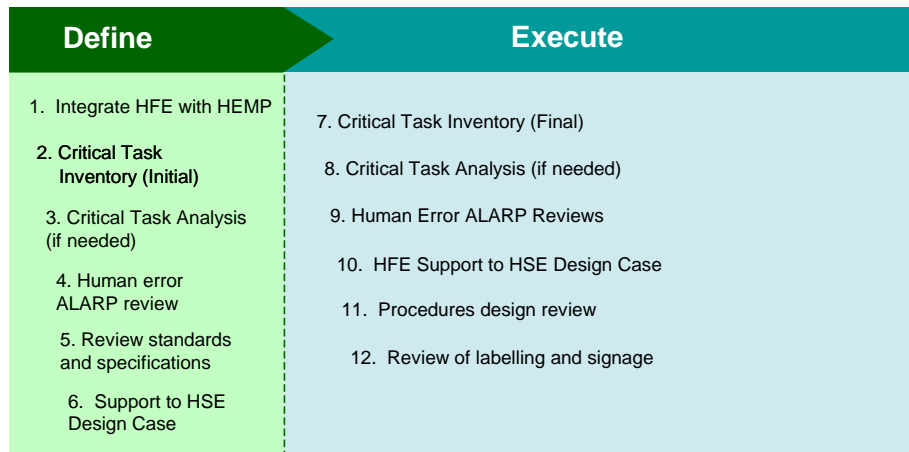
1.5 COMMENTS ON THIS DEP

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://sww.shell.com/standards and on the main page of the DEPs DVD-ROM.

2 PROCESS DESCRIPTION

2.1 GENERAL

Figure 1 summarizes the activities involved in applying this DEP.

Define	Execute
1. Integrate HFE with HEMP	7. Critical Task Inventory (Final)
2. Critical Task Inventory (Initial)	8. Critical Task Analysis (if needed)
3. Critical Task Analysis (if needed)	9. Human Error ALARP Reviews
4. Human error ALARP review	10. HFE Support to HSE Design Case
5. Review standards and specifications	11. Procedures design review
6. Support to HSE Design Case	12. Review of labelling and signage

Figure 1 – Summary of Activities

2.2 ACTIVITIES TO BE CONDUCTED DURING DEFINE PHASE

2.2.1 General

Six activities shall be completed during the projects' DEFINE phase:

- Integrate HFE activity with the HEMP team;
- Prepare Critical Task Inventory (Initial);
- (If necessary) Conduct Critical Task Analysis;
- Conduct initial Human Error ALARP Review;
- Review Standards and Specifications;
- Support to ALARP Justification.

2.2.2 Integrate HFE with HEMP

A meeting shall be held to ensure that all areas of the project which may identify or make judgments about potential for human errors are aware of the requirement to comply with this DEP, and of the role and purpose of the Critical Task Inventory.

The meeting shall confirm any specific requirements for Human Factors content in the HSE Design Case (or other safety case material) as required by national legislation.

The meeting shall also identify any need for HFE awareness training for those involved in HEMP activities.

2.2.3 Critical Task Inventory (Initial)

An inventory of operations and maintenance tasks considered to be essential in ensuring process safety or asset integrity shall be produced by the project, and used as input to the design during DEFINE and EXECUTE phases. The Inventory shall be initiated during DEFINE, and shall be updated throughout DEFINE and EXECUTE phases.

Appendix A illustrates the format the Inventory might take, including examples of how it can be completed.

The inventory shall include the following two types of tasks (see Glossary for definitions):

- AIPS Critical Tasks (ACTs);
- AIPS Critical Errors (ACEs).

Classifying ACTs and ACEs

Tasks included in the Critical Task Inventory shall be classified as one or more of the following:

Field	tasks performed in a field setting.
IT HMI	tasks involving extracting information from, or interaction with a DCS, SCADA, CWE or other IT-based system
Alarm	tasks involving response to alarms (including DCS, Fire and Gas or ESD alarms).
Organisational	tasks that rely on procedures, operator training or experience, or organizational arrangements (such as Supervision or the use of Permits to Work) as controls against Escalation Factors.

Prioritising ACTs and ACEs

Tasks identified as potential ACEs/ACTs shall be scored using the screening method on Table B.1 in Appendix B. Those with scores of 8 or more are considered to be AIPS Critical, either ACTs or ACEs. Tasks scoring less than 8 on this screening should be marked as being 'non-critical'. Non-critical tasks require no further analysis[1].

2.2.4 Critical Task Analysis

A Critical Task Analysis (CTA) should be conducted for any tasks included in the Critical Task Inventory considered to require a more detailed analysis.

The method to be used shall be approved by the project HFE Technical Authority 2, (or alternately, an Authorized HFE SME for the region where the project is based).

2.2.5 Human error ALARP Review (Initial)

Tasks and potential errors identified in the Critical Task Inventory shall be subject to review to:

- confirm the assessment of the critical nature of each task (ACTs and ACEs); and

- assess the extent to which design or engineering decisions have reduced the risk to a level that may be shown to be ALARP.

The output shall be a record of the current ALARP judgement for those tasks included in the Critical Task Inventory, and an action plan to ensure any work needed to further reduce the risk, or to be able to support the ALARP judgement, is included in the HEMP (or HFE) plan for EXECUTE phase.

2.2.6 Review DEFINE Phase Deliverables

Deliverables from the DEFINE phase shall be reviewed to ensure they capture all of the requirements identified in the Critical Task Inventory and Human Error ALARP review.

---

[1] Note that this screening means that potential human errors that affect production - such as leading to product contamination – or with the potential for injury or exposure to health hazards, but are not specifically AIPS related will not be included in the Critical Task Inventory.

2.2.7   **Support to ALARP Justification**

Relevant considerations of the potential for human failure shall be captured in the developing ALARP justification. This shall ensure that evidence or action taken to ensure the risks have been reduced to ALARP is documented and traceable.

2.3   ACTIVITIES TO BE CONDUCTED DURING EXECUTE PHASE

2.3.1   **General**

The following activities shall be conducted in EXECUTE phase:

- Critical Task Inventory (Final);
- Critical Task Analysis (if needed);
- Human error ALARP review;
- Support to Final ALARP Justification;
- Conduct a HFE review of procedures;
- Conduct an HFE review of labeling and signage;
- Pre-commissioning human error ALARP review.

2.3.2   **Critical Task Inventory (Final)**

The Critical Task Inventory shall be maintained and further developed during EXECUTE phase. Potential new ACTs and ACEs – identified from bow-tie analysis or other studies – shall be included in the inventory. Tasks shall be categorized by type, and classified as AIPS critical or non-critical (see 2.2.3).   Additional detail shall be added to existing inventory items as it becomes available.

2.3.3   **Critical Task Analysis**

If required, additional Critical Task Analyses shall be performed, see (2.2.4).

2.3.4   **Human error ALARP review**

Human error ALARP reviews shall be completed for all tasks included in the Critical Task Inventory which are either new additions or where there has been significant change in the task or design since DEFINE phase, see (2.2.5).

2.3.5   **Support to Final ALARP Justification**

Relevant considerations of the potential for human failure should be captured in the developing ALARP Justification, either directly, or as a reference to the results of the Human Error ALARP reviews. This shall ensure that evidence or action taken to ensure the risks have been reduced to ALARP is documented and traceable.

2.3.6   **HFE Review of Procedures**

A review shall be organized in which all procedures and supporting work instructions intended to support activities included in the Critical Task Inventory are subject to a systematic review. This review shall be conducted before the Procedures are issued for use.

2.3.7   **Review of labelling and signage**

An HFE review shall be held of the draft design of all labels and signage supporting performance of critical tasks. The review shall ensure that labels and signs have been developed in accordance with, and comply with, agreed standards.

Unless an alternative industry standard has been specified, the review shall be based on ENG0073SP.

The review shall cover both:

1. The proposed design of all labels and signage (including size, shape, wording, use of graphics, colours and fonts);

2. The proposed location of labels and signs on the facility.

The review shall be timed such that it is possible to make changes both to the proposed design, and positioning.

This review shall use the Critical Task Inventory as a guide: i.e. it shall explicitly review signs and labelling associated with tasks identified in the inventory.

2.3.8 Pre Start-Up human error ALARP review

As part of pre-start-up audit, a review shall be conducted of either a sample, or all human barriers included in the final Critical Task Inventory. The decision on which tasks to review shall be made in consultation with the project HFE Technical Authority (level 2).

This review shall assess the extent to which engineering, design or other controls identified in the inventory have been implemented in the facility, as constructed or actions been taken in planning for training or other organizational arrangements.

The review should include an on-site walk-through of each task included in the inventory.

2.4 KEY ROLES AND COMPETENCY REQUIREMENTS

The key roles and competencies involved in implementing this DEP are:

- The project HFE Co-coordinator shall organize and manage implementation of the activities required by this DEP;

- The project HFE Technical Authority shall be consulted for approval of methods to be used, and results developed;

- The project HSE Manager should be familiar with the contents of this DEP;

- An HFE Specialist may be required to conduct Critical Task Analysis;

- Operations and Maintenance representatives must be involved and consulted throughout the process.

Competence requirements for these roles are as defined in DEP 30.00.60.10-GEN.

2.4.1 Responsibilities

Table 1 defines the responsibilities within the project team for performing the tasks defined in this DEP. The table shows which roles are expected to lead, support and approve each of the activities.

If the event of any conflict between the responsibilities defined in Table 1 and the HSSE CF or DCAF, those documents take precedence over Table 1.

Table 1: Project responsibility matrix

	HFE Technical Authority	HFE Co-ordinator	HSE Manager	HFE Specialist	Operations and Maintenance
DEFINE					
Integrate HFE with HEMP	APP	EXE	CON		
Critical Task Inventory (Initial)	CHK	EXE	APP	CON	CON
Critical Task Analysis (if needed)	APP	CON	CON	EXE	CON
Human Error ALARP Review	APP	EXE	CHK	CON	CON
Review standards and	CHK	EXE	APP	CON	CON

specifications					
Support to HSE Design Case	CHK	CON	APP	EXE	
EXECUTE					
Critical Task Inventory (Final)	CHK	CON	APP	EXE	CON
Critical Task Analysis (if needed)	APP	CON	CON	EXE	CON
Human Error ALARP Reviews	APP	EXE	CHK	CON	CON
Support to HSE Design Case	CHK	EXE	APP		
HFE Review of Procedures	CHK	CON	CON	EXE	CON
HFE signage and labelling design review	CHK	CON	CON	EXE	CON
Pre-commissioning human error ALARP review	APP		CON	EXE	CON

Key:

EXE = Execute

CON = Consult

CHK = Check and verify results

APP = Approve

3 REFERENCES

In this DEP reference is made to the following publications:

NOTES: 1. Unless specifically designated by date, the latest issue of each publication shall be used together with any amendments/supplements/revisions thereof.

2. The DEPs and most referenced external standards are available to Shell users on the SWW (Shell Wide Web) at address http://sww.shell.com/standards.

SHELL STANDARDS

Human Factors Engineering in Projects'	DEP 30.00.60.10-Gen
Human Factors Engineering – Human Machine Interface Design for Situation Awareness	DEP 30.00.60.16-Gen
SEPCO HFE Specification for Labelling of Facilities, Equipment and Piping.	ENG0073SP
Opportunity Realisation Manual	http://sww.shell.com/control_framework/orm/

APPENDIX A   **CRITICAL TASK INVENTORY**

This appendix provides an example format of a Critical Task Inventory (Sections 2.2.3 and 2.3.2).

Table A.1: Example format for a Critical Task Inventory

Task Description	Score and Criticality[2]	Type[3]	Source	Systems affected	Equipment affected	Performance Shaping Factors[4]	Design Requirement	Design Controls	Validation
Operator error in identifying which well to isolate. (ACE)	8 Critical	Field	HFE Analysis	Well Cellar	Christmas Tree	Task will be performed in SCBA and winter gear. Time limits for work in SCBA demands very efficient working.	Job Aids must be easy to carry, manipulate and read in SCBA. Christmas Tree signage and tags must be easy to identify and read in SCBA.	Specify design requirements for visibility, legibility and manipulation of Job Aids and signage for SCBA work	Design review of proposed format for Job Aids to be carried to-site. Usability trial of legibility of job aids and signage in SCBA. Pre-commissioning review of location and appearance of signage relative to operator routes.
Operator action on indication of pressure excursion. (ACT)	15 Critical	IT/ HMI	Generic onshore bow-tie for loss of containment	DCS Alarm system	DCS Workstation and Human Machine Interface	Control room manning at lower end of preferred. High potential workload on panel operator.	Treat task as HMI critical (as defined in DEP 30.00.60.16-GEN).	Ensure compliance with DEP 30.00.60.16-GEN in HMI design.	As per DEP 30.00.60.16-GEN. • HMI design reviews. • HMI usability testing.

---

[2] From Appendix B

[3] Four types as defined in section 3.2.3:   1. Field, 2. IT/HMI, 3. Alarm 4. Organisational

[4] Performance Shaping Factors: These should be factors specific to the project or operational context that could make the task more demanding than in other operations with similar process or equipment, but a different operational context.

APPENDIX B: SCREENING FOR TASK CRITICALITY

This appendix provides a procedure for screening tasks identified as potential candidates for inclusion in the Critical Task Inventory (See section 2.2.3).

All ACTs and ACEs identified from generic bow-ties are considered to be critical, and should be included in the Inventory without an assessment needing to be made.

Tasks proposed as potential ACTs or ACEs shall be scored based on the screening questions shown on Table B.1.

For each question on the table, a score of 0 to 3 is possible. A score of 0 means that the task does not involve any of the characteristics covered by the question. A score between 1 and 3 indicates an increasing risk potential (3 being the highest) because of the nature of the task.

The sum of the scores for a task gives a rating between 0 and 15. A score of 8 or higher indicates a process safety critical task, and should be logged in the Critical Task Inventory.

Table B.1: Potential ACT/ ACE Screening Questions

Diagnostic	Definition	Rating Guide and Score		
		Low (1)	*Medium (2)*	*High (3)*
Is the ACE or ACT included on a bow-tie?		Scores 15		
1. How hazardous is the system involved?	Task involves interaction with systems involving intrinsically hazardous substances or conditions	Small amount* of low hazard substance / condition	Large amount of low hazard or small amount of a high hazard	High amount of a high hazard / condition
2. To what extent are ignition sources introduced into the task when it is performed?	Task uses or may produce heat, sparks or flames	Static spark or low current electrical supply	High current electrical supply, sparks from grinding	Flames for welding or cutting, internal combustion engines
3. To what extent does the task involve change to isolations or the operating configuration?	Task involves valve movements, temporary connections, opening flanges, changing isolation or change to process flows.	Simple change, to valve or equipment status. No effect on isolation.	Complex changes to single equipment (valves or isolation element), or making a single temporary connections	Significant change to isolations or status of process units, or making multiple temporary connections.
4. To what extent could incorrect performance of the task result in release of a hazardous substance / escalate an event?	Incorrect task performance could result in release of hydrocarbons or escalation of the event. Opportunity for recovery is reduced.	Minor release/ escalation of event with opportunity for recovery.	Release/ escalation of event.	Major release/ escalation of event, recovery options limited.
5. To what extent does the task involve defeating or overriding isolation or protection devices?	Task requires bypass or override of indications, alarms or trips	Disabling gauges, meters or electronic displays	Disabling alarms.	Overriding trip systems, isolating safety valves, inserting or removing blinds, etc.

* - Note: Reference should be made to the relevant MSDS when assessing a chemical substance