

DEP SPECIFICATION

SAFETY INSTRUMENTED SYSTEMS

DEP 32.80.10.10-Gen.

February 2017

ECCN EAR99

DESIGN AND ENGINEERING PRACTICE



© 2017 Shell Group of companies

All rights reserved. No part of this document 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. Part 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. Part 744).

This document has been supplied under license by Shell to:
UOP Honeywell ted.fuger@honeywell.com 19/01/2018 03:12:37

AVA Documents
Document Sharing Hub

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 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	CROSS-REFERENCES	9
1.5	SUMMARY OF MAIN CHANGES.....	9
1.6	COMMENTS ON THIS DEP	10
1.7	DUAL UNITS.....	10
1.8	NON NORMATIVE TEXT (COMMENTARY).....	10
2.	COMPLIANCE WITH INTERNATIONAL STANDARDS	11
3.	MANAGEMENT OF FUNCTIONAL SAFETY	11
3.1	GENERAL.....	11
3.2	ORGANISATION AND RESOURCES.....	11
4.	RISK ANALYSIS AND ALLOCATION OF PROTECTION LAYERS	12
4.1	GENERAL.....	12
4.2	ALLOCATION OF SAFETY FUNCTIONS TO PROTECTION LAYERS.....	12
5.	SIS SAFETY REQUIREMENTS SPECIFICATION (SRS).....	16
6.	SIS DESIGN AND ENGINEERING	17
6.1	GENERAL.....	17
6.2	QUANTIFICATION OF RANDOM FAILURE	17
6.3	IMPLEMENTATION OF SIFS.....	17
6.4	MAINTENANCE OVERRIDES	22
7.	SIS APPLICATION PROGRAM DEVELOPMENT	23
7.1	GENERAL.....	23
7.2	OPERATOR INTERFACE	24
7.3	ALARM SIGNAL HANDLING.....	24
7.4	RESETTING	24
7.5	SIS DATA CAPTURE	25
8.	FACTORY ACCEPTANCE TEST (FAT).....	25
9.	SIS INSTALLATION AND COMMISSIONING.....	25
10.	SIS SAFETY VALIDATION.....	25
11.	SIS OPERATION AND MAINTENANCE	26
12.	SIS MODIFICATION.....	26
13.	SIS DECOMMISSIONING	27
14.	INFORMATION AND DOCUMENTATION REQUIREMENTS	27
15.	SYSTEM SPECIFIC REQUIREMENTS	27
15.1	AUTOMATED SEQUENCED DEPRESSURING SYSTEM.....	27
15.2	BURNER MANAGEMENT SYSTEMS (BMS)	28
15.3	HIGH INTEGRITY PRESSURE PROTECTION SYSTEM (HIPPS).....	28
16.	REFERENCES	29

1. INTRODUCTION

1.1 SCOPE

This DEP specifies requirements and gives recommendations for designing new safety instrumented systems (SIS) and functions (SIFs) and for confirming the suitability of existing SIS and SIFs.

This DEP covers SIS and SIF Life Cycle management as it pertains to projects. It does not cover all the aspects of operation and maintenance of SIS and SIFs, just requirements and deliverables related to projects.

This DEP is intended for use for both new projects and amendments to existing installations.

This DEP applies to all automated SIFs greater than or equal to SIL 1.

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 February 2014; 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 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 shall 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.

The word **may** indicates a permitted option.

1.3.2 Specific definitions

The definitions used in this DEP are aligned with IEC 61511-1. In some cases, a fuller explanation can be found by referencing IEC 61511-1 clause 3.

Term	Definition
ALARP	As Low As Reasonably Practicable, The point at which the cost (in time, money and effort) of further risk reduction is grossly disproportionate to the risk reduction achieved.
Architecture	Specific configuration of hardware and software components in a system
Automatic MOS	An automatic MOS automatically overrides the SIS input upon a detected fault of the sensor loop.
Availability	Fraction of time that a system or plant is able to perform its designated service.
Average probability of dangerous failure on demand (PFDavg)	Mean unavailability (see IEC 60050-191) of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system
Common Mode Failure	Concurrent failures of different devices characterized by the same failure mode (i.e., identical faults).
Dangerous Failure	Failure which impedes or disables a given safety action.
Dangerous fault tolerant	The property that enables a system to continue operating properly in the event of a dangerous fault of one of its components (e.g., 1oo2)
Demand	An event which requires a SIF to take action to prevent a Hazardous Situation.
Diagnostics	Frequent (in relation to the process safety time) automatic test to reveal faults (ref. IEC 61511)
Diagnostic Coverage	Fraction of dangerous failure rates detected by diagnostics. Diagnostics coverage does not include any faults detected by proof tests (ref. IEC 61511)
Fail Safe	A concept that defines the failure direction of a component or system as a result of specific malfunctions. That failure direction is towards a safer or less hazardous condition.
Failure (also fault)	Loss of ability to perform as required.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults.

Term	Definition
Final Element	Part of the BPCS or SIS that implements the physical action necessary to achieve or maintain a safe state. (ref. IEC 61511)
Logic Solver	Part of either a BPCS or SIS that performs one or more logic function(s) For example: electrical systems, electronic systems, programmable electronic (PE) systems, pneumatic systems, hydraulic systems.
Mitigation	Action that reduces the consequence(s) of a hazardous event.
Necessary risk reduction	Risk reduction to be achieved by the SIS or other protection layers to ensure that tolerable risk is not exceeded.
Negative MOS	MOS that forces the bypassed input to the trip condition
Permissive	The result of a check on whether or not a combination of conditions is healthy, to allow the Logic Solver to proceed with the next step in a sequence.
Prior use	Documented assessment by a user that a device is suitable for use in a SIS and can meet the required functional and safety integrity requirements, based on previous operating experience in similar environments. (ref. IEC 61511)
Proof Test	Periodic test performed to detect dangerous hidden faults in a SIS so that, if necessary, a repair can restore the system to an as-new condition or as close as practical to this condition.
Regression Testing	In the context of a SIS application program modification; this entails re-testing some or all of the application program parts that are unchanged by the modification to verify that it still functions as desired and to establish that new faults have not inadvertently been introduced into previously healthy parts of the program.
Risk	Combination of the probability of occurrence of harm and the severity of that harm (ref. IEC 61511)
Safe Failure	Failure which favours a given safety action.
Safe fault tolerant	The property that enables a system to continue operating properly in the event of a safe fault of one of its components (e.g., 2oo2)
Safety instrumented function (SIF)	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. A SIF is intended to achieve or maintain a safe state for the process, in respect of a specific hazardous event. A SIF is designed to achieve a required SIL which is determined in relationship with the other protection layers participating in the reduction of the same risk. Previously referred to as an Instrumented Protective Function (IPF).

Term	Definition
Safety Instrumented System (SIS)	Instrumented system used to implement one or more SIFs. (Ref. IEC 61511) A SIS is composed of any combination of sensors, logic solvers, and final elements. It also includes communication and ancillary equipment (e.g., cables, tubing, power supply, impulse lines, heat tracing). A SIS can include software. A SIS can include human action as part of a SIF (see ISA TR84.00.04:2015, Part 1).
Safety Integrity Level (SIL)	Discrete level (one out of four) allocated to the SIF for specifying the safety integrity requirements to be achieved by the SIS. SIL 4 has the highest level of safety integrity; SIL 1 has the lowest.
Safety Requirements Specification (SRS)	Specification containing the functional requirements for the SIFs and their associated safety integrity levels.
Sensor	Part of the BPCS or SIS that measures or detects the process condition. For example, transmitters, transducers, process switches and position switches
SIF Group	A group of SIFs dedicated to a specific piece of equipment (e.g., a compressor, a furnace); a functional grouping of interlocks. Previously referred to as UZ Group.
SIF Process Safety Time	Time period between exceeding the SIF trip setting and occurrence of the hazardous event if the SIF is not performed.
Tolerable risk	Level of risk which is accepted in a given context based on the current values of society. Source: ISO/IEC Guide 51:2014, 3.15
Trip	A SIF action to bring the process to a safe state.

1.3.3 Abbreviations

Term	Definition
AFD	Approved For Design
ALARP	As Low As Reasonably Practicable
BPCS	Basic Process Control System
CEM	Cause and Effect Matrix
CPU	Central Processing Unit
DCS	Distributed Control System
DTT	De-energise to trip

Term	Definition
DTTM	DCS trip to manual
ESD	Emergency Shutdown
ETT	Energise to Trip
EWS	Engineering Workstation
FE	Final Element
FGS	Fire gas and smoke detection and protection system
FMEA	Failure Mode and Effects Analysis
FSA	Functional Safety Assessment
FSP	Functional Safety Plan
H&RA	Hazard and Risk Analysis process (term used in IEC 61511-1 and interchangeably with HEMP at Shell)
H&S	Health and Safety
HAZID	Hazard Identification Study
HAZOP	Hazards and Operability Study
HEMP	Hazards and Effects Management Process
HIPPS	High Integrity Pressure Protection System
HSE	Health, Safety & Environment
HSSE	Health, Safety, Security and Environment
I/O	Input/Output
IEC	International Electrotechnical Commission
LCP	Local Control Panel
LOPA	Layer of Protection Analysis
MAIP	Maximum Allowable Incidental Pressure
MOC	Management of Change
MOS	Maintenance Override Switch
MVC	Measurement, Validation and Comparison
OOS	Operational Override Switch
P&ID	Piping and Instrumentation Diagram

Term	Definition
PAS	Process Automation System (consisting of BPCS, SIS and FGS)
PEFS	Process Engineering Flow Scheme
PFDavg	Average probability of dangerous failure on demand
QRA	Quantitative Risk Assessment
SER	Sequence of Events Recorder
SFF	Safe-Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SME	Subject Matter Expert
SRS	Safety Requirements Specification
TÜV	Technischer Überwachungsverein (German body, translates to Technical Inspection Agency). Throughout this DEP, reference to TÜV means either TÜV Bayern or TÜV Rheinland.
UCP	Unit Control Panel
1oo2	1 out of 2 voting (Fail Dangerous Tolerant)
2oo2	2 out of 2 voting (Fail Spurious Tolerant)
2oo3	2 out of 3 voting (Fail Dangerous and Spurious Tolerant)

1.4 CROSS-REFERENCES

Where cross-references to other parts of this DEP are made, the referenced section or clause number is shown in brackets (). Other documents referenced by this DEP are listed in (16).

1.5 SUMMARY OF MAIN CHANGES

This DEP is full a revision of the DEP of the same number dated February 2014. The following are the main, non-editorial changes.

Section/Clause	Change
All	Aligned with IEC 61511-1 Edition 2, February 2016.
All	Extensive rewrite to remove duplication and overlap with IEC 61511-1 and re-focus on essential additions to IEC 61511-1 only.