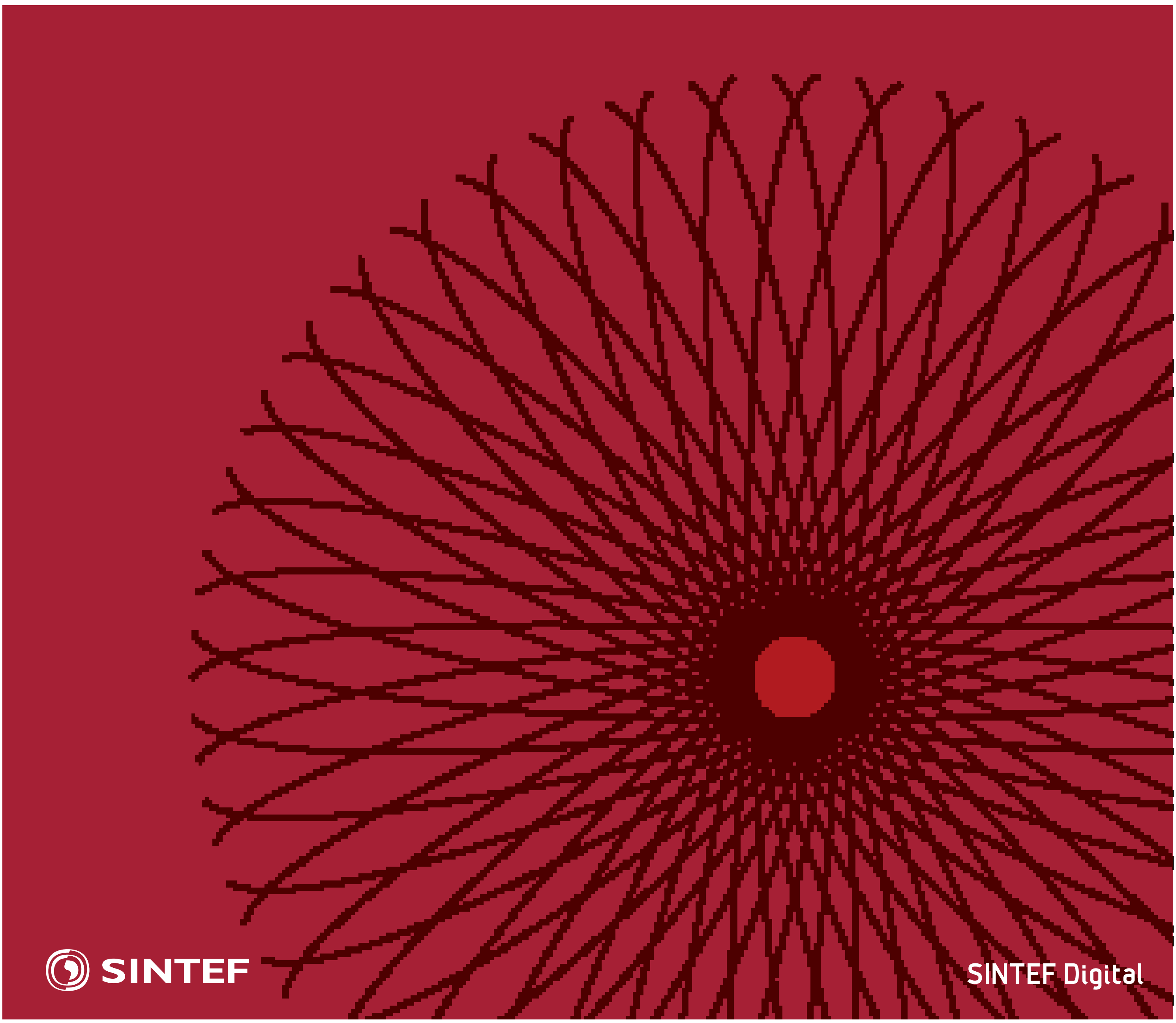
PDS DATA HANDBOOK – 2021 EDITION

# Reliability Data for Safety Equipment



SINTEF Digital

Maria Ottermo, Stein Hauge and Solfrid Håbrekke

# Reliability Data for Safety Equipment

PDS Data Handbook – 2021 Edition

www.sintef.no

Maria Ottermo, Stein Hauge and Solfrid Håbrekke
**Reliability Data for Safety Equipment**
PDS Data Handbook – 2021 Edition

Keywords:
Safety, Reliability Data, Safety Instrumented Systems (SIS), SIL calculations

ISBN 978-82-14-06468-1
SINTEF Report no. 2021:00370

printed by 07 Media AS
Content: 115 g G-print
Cover: 250 g Galerie Art Silk

© Copyright SINTEF 2021
The material in this publication is covered by the provisions of the Norwegian Copyright Act. Without any special agreement with SINTEF, any copying and making available of the material is only allowed to the extent that this is permitted by law or allowed through an agreement with Kopinor, the Reproduction Rights Organisation for Norway. Any use contrary to legislation or an agreement may lead to a liability for damages and confiscation, and may be punished by fines or imprisonment.

**SINTEF Digital**
Software Engineering, Safety and Security
Address:
NO-7465 Trondheim
Norway
Telephone: +47 40 00 51 00

www.sintef.no
www.sintef.no/digital
www.sintef.no/PDS
www.sintefbok.no

SINTEF
SINTEF Digital
**SINTEF Digital**
Address:
Postboks 4760 Torgarden
NO-7465 Trondheim
NORWAY
Switchboard: +47 40005100

info@sintef.no

Enterprise /VAT No:
NO 919 303 808 MVA

# Report

# Reliability Data for Safety Equipment

PDS Data Handbook – 2021 Edition

KEYWORDS:
Reliability data
Failure rates
Safety systems
SIL calculations

**VERSION**
FINAL

**DATE**
2021-05-30

**AUTHORS**
Maria Ottermo, Stein Hauge and Solfrid Håbrekke

**CLIENT(S)**
Multiclient – PDS Forum

**CLIENT'S REF.**
Mathilde Cot

**PROJECT NO.**
60S051

**NUMBER OF PAGES:**
216

ABSTRACT
This handbook provides reliability data based on field feedback for components of safety instrumented systems, subsea and drilling equipment, and selected non-instrumented safety critical equipment. Considerable effort has been made to ensure that the data are credible, traceable, documented and justified, in line with requirements in the IEC 61508 and IEC 61511 standards. Compared to the 2013 edition of the handbook, the main changes are:

- Greatly expanded data basis, including comprehensive and more recent operational experience.
- New equipment groups are added.
- For several sensors and final elements, the failure rates differentiate between relevant attributes such as dimension, measuring principle, process service, etc.
- Updated values for the common cause factor ($\beta$ factor), diagnostic coverage (DC) and random hardware fraction (RHF).
- Improved data traceability and a more detailed assessment of data uncertainty.

In addition, failure rates, equipment boundaries, failure definitions and other relevant information have been updated or included.

**PREPARED BY**
Maria Ottermo, Stein Hauge and Solfrid Håbrekke

**CHECKED BY**
Tor Onshus

**APPROVED BY**
Lars Bodsberg, Project Director

MANAGEMENT SYSTEM CERTIFICATION
DNV·GL
ISO 9001 = ISO 14001
OHSAS 18001

| REPORT NO. | ISBN | CLASSIFICATION | CLASSIFICATION THIS PAGE |
|---|---|---|---|
| 2021:00370 | 978-82-14-06468-1 | Unrestricted | Unrestricted |

# Table of contents

# PREFACE

SINTEF is proud to present this new 2021 edition of the PDS[1] data handbook. As compared to the 2013 edition of the PDS data handbook [1], the historical data basis has been greatly expanded and the detailing and assessment of the data have been significantly improved. The data have been subject to extensive quality assurance, where equipment experts and operational personnel have gone through and classified some thirty thousand maintenance notifications and work orders manually. As to our knowledge, this represents one of the broadest and best documented data bases for safety equipment, worldwide.

The work has been carried out as part of the research project "Automized process for follow-up of safety instrumented systems" (APOS) and has been funded by SINTEF, the Research Council of Norway, the APOS project members and the PDS forum participants. We would like to thank everyone who has provided us with quality assured reliability data, comments, and valuable input to this PDS data handbook.

Trondheim, May 2021

**PDS Forum Participants as per 2021**

**Petroleum Companies / Operators:**
- AkerBP
- Altera Infrastructure
- ConocoPhillips Norge
- Equinor
- Gassco
- Lundin Energy
- Neptune Energy
- Norske Shell
- OKEA
- Repsol Norge
- Vår Energi

**Control and Safety System Vendors:**
- ABB
- Emerson
- Honeywell
- Kongsberg Maritime
- Optronics Technology
- Origo Solutions
- Siemens Energy

**Engineering Companies and Consultants:**
- Aibel
- Aker Solutions
- DNV Norge
- ORS Consulting
- Proactima
- Rosenberg WorleyParsons
- Safetec Nordic
- TechnipFMC
- Vysus Group

**Governmental Bodies (Observers):**
- Norwegian Maritime Directorate
- Petroleum Safety Authority Norway

[1] PDS is a Norwegian acronym for reliability of Safety Instrumented Systems. See also www.sintef.no/pds.

# 1 INTRODUCTION

## 1.1 Objective and Scope

The use of realistic failure data is an essential part of any quantitative reliability analysis. It is also one of the most challenging parts and raises several questions concerning the suitability of the data, the assumptions underlying the data and the uncertainties related to the data.

This handbook provides reliability data for safety equipment, including components of safety instrumented systems, subsea and drilling equipment and selected non-instrumented safety critical equipment such as valves, fire-fighting equipment, fire and gas dampers, fire doors, etc. Efforts have been made to document the presented data thoroughly, both in terms of applied data sources, underlying assumptions, and uncertainties in terms of confidence limits.

Compared to the 2013 version, the main changes and improvements are:

- Greatly expanded data basis, including comprehensive and more recent operational experience.
- New equipment groups have been added, and more detailed failure rates, differentiating on attributes such as dimension, measuring principle, medium, etc., are given for selected sensors and final elements.
- Updated common cause factors (β values) based on an extensive field study of some 12.000 maintenance notifications, as described in [3].
- Updated values for diagnostic coverage (DC) and random hardware fraction (RHF) based on operational experience, vendor certificates and discussions with equipment experts.
- Improved data traceability and a more detailed assessment of failure rate uncertainty.

In addition, failure rates, equipment boundaries including a definition of dangerous (or safety critical) failure, and other relevant information and parameters have been reviewed and updated for all components.

This data handbook may also be used in conjunction with the PDS method handbook [2][2], which describes a practical approach for calculating the reliability of safety systems.

## 1.2 The IEC 61508 and 61511 Standards

The IEC 61508 and IEC 61511 standards, [4] and [5], present requirements to SIS for all relevant lifecycle phases, and have become leading standards for SIS specification, design, implementation, and operation. IEC 61508 is a generic standard common to several industries, whereas IEC 61511 has been developed especially for the process industry. The Norwegian Oil and Gas Association (NOROG) has also developed a guideline to support the use of IEC 61508 / 61511 in the Norwegian Petroleum Industry [6].

A fundamental concept in both IEC 61508 and IEC 61511 is the notion of risk reduction; the higher the risk reduction is required, the higher the SIL. It is therefore important to apply *realistic* failure data in the design calculations, since too optimistic failure rates may suggest a higher risk reduction than what is obtainable in operation. In other words, the predicted risk reduction, calculated for a safety function in the design phase, should to the degree possible reflect the actual risk reduction that is experienced in the operational phase, see also [6].

This is also emphasized in the second edition of IEC 61511-1 (sub clause 11.9.3) [4] which states that the applied reliability data shall be *credible, traceable, documented and justified* and shall be based on field feedback from similar devices used in a similar operating environment. It is therefore recommended [6] to use data based on actual historic field experience when performing reliability calculations.

[2] The PDS method handbook is currently under revision. A new version is planned to be issued early 2022.

The reliability data in this PDS handbook represent collected experience from operation of safety equipment, mainly in the Norwegian oil and gas industry. As such, the PDS data and associated method are in line with the main principles advocated in the IEC standards, and the data presented in this handbook are on a format suitable for performing reliability calculations in line with the IEC standards.

## 1.3 Data Sources

The most important data source for this handbook is extensive operational experience gathered from Norwegian offshore (and some onshore) oil and gas facilities during the last 10–15 years. Data from 54 different facilities and seven different operators, are represented. In fact, the total accumulated experience sums up to more than 3 billion operational hours for topside equipment and more than 750 million operational hours for subsea and well completion equipment. Note that these data have been subject to extensive quality assurance through the fact that equipment experts and operational personnel have gone through and classified thousands of maintenance notifications and work orders manually. As to our knowledge, this represents one of the broadest and best documented data bases for safety equipment, worldwide.

Other data sources applied include: OREDA reliability data handbooks, subsea BOP data from Exprosoft, RNNP, manufacturer data and certificates, in addition to various data studies and expert judgements. Each of the data sources applied in this handbook are briefly discussed in Table 1.1.

**Table 1.1: Discussion of applied data sources**

| Data source | Description | Relevance of data in present handbook |
|---|---|---|
| Operational review data | Experience data from operational reviews on Norwegian offshore and onshore facilities. Equipment experts from the operator, often together with personnel from a consultant (SINTEF or other), have assessed failures (notifications and work orders) registered in maintenance databases and have classified each failure (typically into categories DU, DD, S, non-critical). | The operational reviews represent the most important data source in this handbook, particularly due to the thorough failure classification, extensive population, and the fact that the data have been collected recently, i.e., during the last 10–15 years. The operational reviews are the main data source for topside equipment, and an important data source for subsea and well completion equipment. |
| WellMaster RMS, [13] | WellMaster RMS (Reliability Management System) is a world leading well and subsea equipment reliability database and analysis solution for oil and gas operators. It is utilized through the full well life cycle, from designing better wells and selecting better equipment, to risk assessment, well integrity analysis, and remaining life assessments. | WellMaster data is the main data source for several subsea and well completion equipment groups, including both topside and subsea located wells. As for the data from operational reviews, the WellMaster data have been subject to extensive quality assurance and failure classification. |
| Subsea BOP data, [14] | From 1983 to 2019, SINTEF and Exprosoft have documented results from several detailed reliability studies of subsea blowout preventer (BOP) systems. A total of nearly 1000 wells have been reviewed with respect to subsea BOP reliability. | The latest study *Subsea BOP Reliability, Testing, and Well Kicks* [15] was completed in October 2019. This study was based on experience from well operations in Norwegian waters in the period 2016–2018. Most wells were drilled in water depths less than 500 meters. |

| **Data source** | **Description** | **Relevance of data in present handbook** |
|---|---|---|
| | | The study *Reliability of Deepwater Subsea BOP Systems and Well Kicks* [16] was completed in 2012. The study was based on wells drilled in water-depths deeper than 600m in the period 2007 – 2010 in US GoM OCS (Outer Continental Shelf).<br><br>These two studies, in addition to [17], [18] and Exprosoft expert judgements have been used as basis for the subsea BOP failure rates. |
| Expert judgements | Discussions and meetings with experts (operators and manufacturers) provide essential input to this handbook. This includes numerous virtual and physical meetings, PDS workshops, as well as extensive mail and telephone correspondence. | Expert judgements have been important to enable data differentiation and to establish diagnostic coverage and proof test coverage values. Expert judgements have been particularly important to establish data for control logic since limited operational data have been available. |
| OREDA reliability data handbooks, [19] | OREDA is a project organisation whose main purpose is to collect and exchange reliability data among the participating companies, see www.oreda.com. The OREDA handbooks contain failure data (failure mode and failure severity) for a broad group of components within oil and gas production. | OREDA has been applied as a data source for some subsea equipment groups, and as part of the input to estimate the distribution between dangerous and safe failures and RHF values. |
| Manufacturer data / equipment certificates | Failure data, e.g., in the form of equipment certificates or assessment reports, prepared for specific products. The data can be based on component FMECA/FMEDA studies, laboratory testing, and in some cases also field experience. | Manufacturer data have been particularly relevant for equipment with limited operational experience, such as control logic. Furthermore, equipment certificates[3] have provided valuable input to diagnostic coverage values. |
| RNNP, [20] | Failure data from the RNNP project for selected safety critical equipment. The RNNP data comprise a high number of facilities on the Norwegian Continental Shelf. The RNNP data also include *all* components within the specified equipment groups, giving a very high overall operational time. RNNP data contain results from the period 2003–2018. | RNNP data mainly include results from functional testing, implying that failures detected otherwise are normally not included. Therefore, the failure rates may be optimistic for equipment groups where failures are also detected between tests (e.g., for valves, fire doors, etc.).<br><br>RNNP only includes selected equipment, and the degree of detailing is limited (e.g., all gas detectors are grouped together, and test intervals are not explicitly stated). Therefore, RNNP data have been applied as a data source only for selected equipment groups such as e.g., deluge valves and downhole safety valves. |

[3] See e.g., www.exida.com

## 1.4 Organisation of the Data Handbook

In chapter 2, important reliability concepts are discussed and defined. Failure classification for safety equipment is presented together with the main reliability performance measures used in the IEC standards and in PDS.

The reliability data are summarised in chapter 3. A split has been made between topside equipment, subsea and downhole well completion equipment, and drilling equipment. Chapter 3 also includes main considerations and assumptions behind the given parameter values.

In chapter 4 all the detailed data dossiers with data sources and failure rate assessments are presented, including an explanation of the various data dossier fields.

Finally, a list of references, i.e., reports, standards, guidelines, and other relevant data sources and documents, is included.

## 1.5 List of abbreviations

**General terms**

| | | |
|---|---|---|
| CCF | - | Common cause failure |
| CSU | - | Critical safety unavailability |
| D | - | Dangerous |
| DC | - | Diagnostic coverage |
| DD | - | Dangerous detected |
| DU | - | Dangerous undetected |
| ESD | - | Emergency shutdown |
| FMECA | - | Failure modes, effects, and criticality analysis |
| FMEDA | - | Failure modes, effects, and diagnostic analysis |
| F&G | - | Fire and gas |
| FTA | - | Fault tree analysis |
| HC | - | Hydrocarbon |
| HMI | - | Human machine interface |
| IEC | - | International electro-technical commission |
| IR | - | Infrared |
| ISO | - | International organization for standardization |
| mA | - | Milliampere |
| MoC | - | Management of change |
| MooN | - | $M$-out-of-$N$ |
| MTTF | - | Mean time to failure |
| MTTR | - | Mean time to restoration |
| MUX | - | Multiplex |
| NA | - | Not applicable |
| NDE | - | Normally de-energised |
| NE | - | Normally energised |
| NOG/NOROG | - | Norwegian oil and gas association |
| OREDA | - | Offshore reliability data |
| PA | - | Public address |
| PDS | - | Norwegian acronym for “reliability of computer-based safety systems” |
| PFD | - | Probability of failure on demand |
| PFH | - | Probability of failure per hour (or average frequency of failure per hour) |
| PSD | - | Process shutdown |
| PST | - | Partial stroke test |
| PTC | - | Proof test coverage |

| | | |
|---|---|---|
| RBD | - | Reliability block diagram |
| RH | - | Random hardware |
| RHF | - | Random hardware fraction |
| RNNP | - | Project on risk level in the Norwegian petroleum production |
| S | - | Safe |
| SFF | - | Safe failure fraction |
| SIF | - | Safety instrumented function |
| SIL | - | Safety integrity level |
| SIS | - | Safety instrumented system |
| SOLAS | - | Safety of life at sea |
| TIF | - | Test independent failure |
| UV | - | Ultraviolet |

**Technical (equipment related) terms**

| | | |
|---|---|---|
| AI | - | Analogue input |
| AMV | - | Annulus master valve |
| ASV | - | Annulus safety valve |
| BPCS | - | Basic process control system |
| BOP | - | Blowout preventer |
| CAP | - | Critical action panel |
| CCR | - | Central control room |
| CIESDV | - | Chemical injection emergency shutdown valve |
| CIV | - | Chemical injection valve |
| CLU | - | Control logic unit |
| CPU | - | Central processing unit |
| DCP | - | Driller's control panel |
| DHSV | - | Downhole safety valve |
| DO | - | Digital output |
| ESV | - | Emergency shutdown valve |
| FOV | - | Fast opening valve |
| GLESDV | - | Gas lift emergency shutdown valve |
| GLV | - | Gas lift valve |
| HART | - | Highway addressable remote transducer (protocol) |
| HASCV | - | Hydraulically actuated safety check valve |
| HIPPS | - | High integrity pressure protection system |
| HXT | - | Horizontal X-mas tree |
| LMRP | - | Lower marine riser package |
| MCS | - | Master control station |
| MIV | - | Methanol injection valve |
| PLC | - | Programmable logic controller |
| PMV | - | Production master valve |
| PPS | - | Pressure protection system |
| PSS | - | Programmable safety system |
| PSV | - | Pressure relief valve |
| PWV | - | Production wing valve |
| QSV | - | Quick closing shut-off valve |
| SAS | - | Safety and automation system |
| SCM | - | Subsea control module |
| SEM | - | Subsea electronic module |
| SPM | - | Side-pocket mandrel |
| SSIV | - | Subsea isolation valve |
| TCP | - | Toolpusher's control panel |
| TRCIV | - | Tubing retrievable chemical injection valve |

| | | |
|---|---|---|
| TRSCSSV | - | Tubing retrievable surface-controlled subsurface valve |
| TRSCASSV | - | Tubing retrievable surface-controlled annulus subsurface valve (also abbr. ASV) |
| UPS | - | Uninterruptable power supply |
| WRCIV | - | Wire retrievable chemical injection valve |
| WRSCSSV | - | Wireline retrievable surface-controlled subsurface valve |
| XT | - | X-mas tree |
| XOV | - | Crossover valve |
| XV | - | Production shutdown valve |

**Failure mode abbreviations**

| | | |
|---|---|---|
| AIR | - | Abnormal instrument reading |
| BRD | - | Breakdown |
| DOP | - | Delayed operation |
| ELP | - | External leakage process medium |
| ELU | - | External leakage utility medium |
| ERO | - | Erratic output |
| FTC | - | Fail to close on demand |
| FTF | - | Fail to function on demand |
| FTO | - | Fail to open on demand |
| FTR | - | Fail to regulate |
| FTS | - | Fail to start on demand |
| HIO | - | High output |
| INL | - | Internal leakage utility medium |
| LAP | - | Leakage across packer |
| LCP | - | Leakage in closed position |
| LOO | - | Low output |
| NONC | - | Non-critical |
| NOO | - | No output |
| PLU | - | Plugged/choked |
| PRD | - | Premature disconnect |
| SPO | - | Spurious operation |
| STP | - | Fail to stop on demand |
| UST | - | Spurious stop (unexpected stop) |

# 2 RELIABILITY CONCEPTS – THE PDS METHOD

The PDS method has been developed to enable safety and reliability engineers to perform reliability calculations in various phases of a project. This chapter presents some main characteristics of the PDS method, the failure classification scheme, and reliability performance measures. Please note that the objective is *not* to give a full and detailed presentation of the method, but to introduce the model taxonomy and some basic ideas. For a more comprehensive description of the PDS method and the detailed formulas, see the PDS method handbook, [2].

## 2.1 The PDS Method

For estimating SIS reliability, different calculation approaches can be applied, including analytical formulas, Boolean approaches like reliability block diagrams (RBD) and fault tree analysis (FTA), Markov modelling and Petri Nets (see IEC 61508-6, Annex B). The IEC standards do not mandate one specific approach or a set of formulas but leave it to the user to choose the most appropriate approach for quantifying the reliability of a given system or function.

The PDS method includes a set of analytical formulas and concepts to quantify loss of safety [2], and together with the PDS data, it offers an effective and practical approach towards implementing the quantitative aspects of the IEC standards. In the following sections some main characteristics of the PDS method are briefly introduced, including important notation and classification schemes.

## 2.2 Notation and Definitions

Table 2.1 presents some main parameters and performance measures used in the PDS method and in this data handbook.

**Table 2.1 Performance measures and reliability parameters**

| Term | Description |
|---|---|
| $\lambda_{\text{crit}}$ | Rate of critical failures.<br><br>Critical failures include dangerous (D) failures which may cause loss of the ability to shut down production (or go to a safe state) when required, plus safe (S) failures which may cause loss of the ability to maintain production when safe (e.g., spurious trip failures). Hence: $\lambda_{\text{crit}} = \lambda_{\text{D}} + \lambda_{\text{S}}$ (see below). |
| $\lambda_{\text{D}}$ | Rate of dangerous failures, including both undetected and detected failures. $\lambda_{\text{D}} = \lambda_{\text{DU}} + \lambda_{\text{DD}}$ (see below). |
| $\lambda_{\text{DU}}$ | Rate of dangerous undetected (DU) failures, i.e., dangerous failures undetected by automatic self-test (only revealed by a functional test or upon a planned or unplanned demand). |
| $\lambda_{\text{DU-RH}}$ | The rate of dangerous undetected failures ($\lambda_{\text{DU}}$), originating from random hardware failures. |
| $\lambda_{\text{DD}}$ | Rate of dangerous detected failures, i.e., dangerous failures detected upon occurrence by e.g. self-diagnostics. |
| $\lambda_{\text{S}}$ | Rate of safe failures, i.e., failures that either cause a spurious operation of the equipment and/or maintain the equipment in a safe state. |

| Term | Description |
|---|---|
| SFF | Safe failure fraction. $SFF = 1 - (\lambda_{DU}/\lambda_{crit}) \cdot 100\%$. |
| $\beta$ | The fraction of failures of a single component that result in simultaneous failure of both components of a redundant pair, due to a common failure cause. |
| $C_{MooN}$ | Modification factor for redundant configurations other than 1oo2 in the beta-factor model (e.g., 1oo3, 2oo3 and 2oo4 configurations). |
| RHF | Random hardware fraction, i.e., the fraction of DU failures originating from random hardware failures ($1 - RHF$ will be the fraction originating from systematic failures). |
| DC | Diagnostic coverage, i.e., the fraction of dangerous failures detected by automatic diagnostic tests (i.e., internal self-diagnostic built into the equipment plus external diagnostic facilities). This fraction is computed using the rate of dangerous detected failures divided by the total rate of dangerous failures; $DC = (\lambda_{DD}/\lambda_{D}) \cdot 100\%$.<br><br>Note that the interval between automatic diagnostic tests, is often referred to as *diagnostic test interval*. |
| PTC | Proof test coverage, i.e., the fraction of DU failures detected during functional proof testing. |
| PFD | The probability of failure of a system or component to perform its specified safety function upon a demand.<br><br>Note that the PFD is the average probability of failure on demand over a period of time, i.e., $PFD_{avg}$ as denoted in IEC 61508. However, due to simplicity $PFD_{avg}$ is denoted as PFD in the PDS handbooks. |
| $\tau$ | Interval of proof test (time between proof tests of a component). |

**Apart from the following five example pages in Chapter 4 Data Dossier, the remaining part of the handbook is not included in this free copy.**

# 4 DATA DOSSIERS

This chapter presents the detailed data dossiers for the various safety related components. The dossiers are input to the tables in chapter 3 that summarise the PDS data.

The data provide SINTEF's best estimates of equipment failure rates based on the data sources discussed in section 1.3 and specified in the data dossiers. Also, uncertainty estimates (confidence intervals) have been provided whenever feasible. An explanation of the content of each data dossier field is given in section 4.1. Sections 4.2–4.4 contain data dossiers for topside input devices, logic, and final elements, respectively. Data dossiers for subsea and downhole well completion equipment are included in section 4.5 and 4.6 respectively, whereas section 4.7 includes data dossiers for subsea drilling BOPs.

## 4.1 Explanation of data dossier fields

The main fields of the data dossiers are described in the following.

**Module**

The module indicates whether the device is (cf. IEC 61508/IEC 61511, [4] and [5]):

- an input element (e.g., a sensor that monitors a process parameter or a push button).
- a control logic unit (logic solver that decides it if is necessary to act upon monitored signal).
- a final element (actuating element).

**Equipment group and component**

In the report “Standardised failure reporting and classification of SIS failures in the petroleum industry" [11], a three-level hierarchy of equipment has been suggested:

- The main level, L1 (main equipment groups), includes equipment that shares a common main functionality. Examples of such functionality are e.g., to detect a process upset, to detect hydrocarbons or a fire, to stop the process flow or to facilitate evacuation.
- The second level, L2 (safety critical elements), represents the *most important* characteristics of the L1 equipment groups. As compared to the L1 group, these elements will often have a further specified (sub)functionality, e.g., to detect $H_2S$ gas, to detect smoke or to shut in and isolate the riser, and some additional design characteristics, e.g., a diesel engine or an electric engine.
- The third level, L3 (equipment attributes), is represented by a common set of *attributes* with a foreseen potential to impact the performance and reliability of the equipment within an L2 group. For example, among topside ESV/XVs, there can be ball valves, globe valves, and gate valves handling fluids of different types, and there are gas detectors located in air intakes versus gas detectors located in open process areas.

Each equipment group in the second row of the data dossier corresponds to a L1 equipment group while component corresponds to a safety critical element on the L2 level described above, e.g., a line HC gas detector or a PSD valve. In addition, the component, may in some cases be further detailed in terms of relevant L3 attributes.

**Component boundaries / Failure definition**

This field provides additional information about the boundaries of the specified component, e.g., whether the actuator of the main valve is included or if local electronics and process connections are part of a transmitter. A reference to the comparable equipment class in ISO 14224 [12] is also given.

When relevant, additional assumptions concerning safe state, fail safe design, self-test ability, loop monitoring, NE/NDE design, etc. are also given. Hence, when using the data for reliability calculations, it is important to consider the relevance of these assumptions for each specific application.

Also (except for drilling equipment), a definition of dangerous (or safety critical) failure for the component under consideration is given. This definition will in some cases depend on the specific application and must therefore be considered as typical rather than unique.

**SINTEF's Best Estimates – Failure rates (per $10^6$ hours)**
Provides SINTEF's best estimates for $\lambda_{DU}$, $\lambda_D$, $\lambda_S$ and $\lambda_{crit}$ (see section 2.2) for the specified component under consideration.

**SINTEF's Best Estimates – Coverage/Others**
Provides SINTEF's best estimates for the diagnostic coverage DC for dangerous failures, as well as suggested $\beta$ factor for the specified component under consideration. For a further discussion $\beta$ and DC values, reference is made to section 3.4 and 3.5, respectively.

**SINTEF's Best Estimates – Failure mode distribution**
Provides SINTEF's best estimate for the failure mode distribution wherever this has been available for the specified component.

**$\lambda_{DU}$ (per $10^6$ h) Uncertainty and Population Details**
Provides further details for the specified part of the component population (e.g., all IR gas detectors from operational reviews, or a further extract of the population such as "all valve sizes > 3""). The details include:

| | |
|---|---|
| $\lambda_{DU}$ | The average rate of dangerous undetected failures for the specified population |
| $\lambda_{DU}^{70\%}$ | The upper 70% confidence limit of the dangerous undetected failure rate |
| $\lambda_{DU}^{5\text{-}95\%}$ | The 90% confidence interval for the dangerous undetected failure rate |
| $DU_{obs}$ | The observed number of dangerous undetected failures for the specified component population. |
| $DU_{calc}$ | The number of DU failures used in the estimation of the average $\lambda_{DU}$ failure rate (when lower than $DU_{obs}$ this is typically due to some facilities being given a reduced weight due to uncertainties related to number of actual DU failures). The reasoning will normally be further explained in the failure rate assessment and/or the failure rate references fields |
| T | The accumulated observation period (operational time) for the specified component population, i.e., the operating time multiplied with the number of components in the population. |
| Observation period | The period (years) during which the failure history for the specified population has been registered. |
| Population size | The number of components (tags / functional locations) in the specified population. |
| Number of facilities | The number of facilities (and number of operators) represented in the specified population. |

**Failure rate assessment**
Provides a discussion and elaboration of the suggested failure rates, such as comparison with previous editions of the handbook, weight of different data sources, whether the equipment is new to this edition of the handbook, basis for data differentiation, explanation of equipment details, as well as other relevant assumptions underlying the failure rates.

**Failure rate references**
Provides a more detailed specification of the different data sources. For each source this includes the (dangerous undetected) failure rate, the associated source or facility (anonymized), the number of DU

failures from that source ($DU_{obs}$), as well as T, the observation period, and the population size (see above) for that specific source/facility.

## 4.4 Topside Final Elements

### 4.4.1 Topside ESV and XV

| | | | | | |
|---|---|---|---|---|---|
| Module: | Final Elements | | | **PDS Reliability Data Dossier** | |
| Equipment Group: | Topside Shutdown and Isolation Valves | | | | |
| Component: | Topside ESV and XV | | | | |
| *Component Boundaries / Failure Definition* | | | | | |
| Includes the main valve (ESV or XV) and the actuator (both gate, ball and some butterfly valves). Not including solenoid/pilot valve (differs from ISO 14224 where pilot and solenoid are included in the equipment class = Valves). Valve/actuator assumed to be spring return to closed position. Full stroke with tight shut off.<br><br>Dangerous failure typically defined as "*the valve does not close upon signal or within specified time (if response time requirement given), or has a higher internal leakage rate in closed position than the specified acceptance criterion (if given)* ". | | | | | |
| *SINTEF's Best Estimates* | | | | | |
| **Failure rates (per $10^6$ h)** | | **Coverage/Other** | | **Failure mode distribution** | |
| $\lambda_{DU}$ = | 2.3 | DC = | 0.05 | FTC: | 45 % |
| $\lambda_D$ = | 2.5 | β = | 0.08 | DOP: | 40 % |
| $\lambda_S$ = | 2.0 | | | LCP: | 15 % |
| $\lambda_{crit}$ = | 4.5 | | | | |
| *$\lambda_{DU}$ (per $10^6$ h) Uncertainty and Population Details* | | | | | |
| **All operational review data** | | | | | |
| $\lambda_{DU}$ = | 2.3 | $DU_{obs}$ = | 248 | Observation period: | 2006 – 2019 |
| $\lambda_{DU}^{70\%}$ = | 2.4 | $DU_{calc}$ = | 215 | Population size: | 1846 |
| $\lambda_{DU}^{5\text{-}95\%}$ = | [ 2.1, 2.6 ] | T = | $9.2 \cdot 10^7$ h | No. of facilities: | 10 (5 operators) |
| **Application:** ESD and combined ESD/PSD service | | | | | |
| $\lambda_{DU}$ = | 2.3 | $DU_{obs}$ = | 112 | Observation period: | 2006 – 2019 |
| $\lambda_{DU}^{70\%}$ = | 2.6 | $DU_{calc}$ = | 93 | Population size: | 837 |
| $\lambda_{DU}^{5\text{-}95\%}$ = | [ 1.9, 2.8 ] | T = | $4.0 \cdot 10^7$ h | No. of facilities: | 10 (5 operators) |
| **Application:** PSD service | | | | | |
| $\lambda_{DU}$ = | 2.3 | $DU_{obs}$ = | 136 | Observation period: | 2006 – 2019 |
| $\lambda_{DU}^{70\%}$ = | 2.5 | $DU_{calc}$ = | 122 | Population size: | 1009 |
| $\lambda_{DU}^{5\text{-}95\%}$ = | [ 2, 2.7 ] | T = | $5.2 \cdot 10^7$ h | No. of facilities: | 8 (3 operators) |
| **Size:** Small (0-1 inch) | | | | | |
| $\lambda_{DU}$ = | 1.3 | $DU_{obs}$ = | 6 | Observation period: | 2006 – 2019 |
| $\lambda_{DU}^{70\%}$ = | 1.7 | $DU_{calc}$ = | 6 | Population size: | 97 |
| $\lambda_{DU}^{5\text{-}95\%}$ = | [ 0.6, 2.6 ] | T = | $4.6 \cdot 10^6$ h | No. of facilities: | 5 (2 operators) |
| **Size:** Medium (1-3 inches) | | | | | |
| $\lambda_{DU}$ = | 1.7 | $DU_{obs}$ = | 47 | Observation period: | 2006 – 2019 |
| $\lambda_{DU}^{70\%}$ = | 1.9 | $DU_{calc}$ = | 39 | Population size: | 407 |
| $\lambda_{DU}^{5\text{-}95\%}$ = | [ 1.3, 2.2 ] | T = | $2.3 \cdot 10^7$ h | No. of facilities: | 5 (2 operators) |

| Module: | Final Elements | | **PDS Reliability Data Dossier** |
|---|---|---|---|
| Equipment Group: | Topside Shutdown and Isolation Valves | | |
| Component: | Topside ESV and XV | | |

*$\lambda_{DU}$ (per $10^6$ h) Uncertainty and Population Details*

**Size:** Large (3-18 inches)

| | | | | | |
|---|---|---|---|---|---|
| $\lambda_{DU}$ = | 3.0 | $DU_{obs}$ = | 85 | Observation period: | 2006 – 2019 |
| $\lambda_{DU}^{70\%}$ = | 3.2 | $DU_{calc}$ = | 69 | Population size: | 443 |
| $\lambda_{DU}^{5-95\%}$ = | [ 2.4, 3.7 ] | T = | $2.3 \cdot 10^7$ h | No. of facilities: | 5 (2 operators) |

**Size:** Extra Large (>18 inches)

| | | | | | |
|---|---|---|---|---|---|
| $\lambda_{DU}$ = | 7.0 | $DU_{obs}$ = | 34 | Observation period: | 2006 – 2019 |
| $\lambda_{DU}^{70\%}$ = | 7.9 | $DU_{calc}$ = | 30 | Population size: | 77 |
| $\lambda_{DU}^{5-95\%}$ = | [ 5.1, 10 ] | T = | $4.2 \cdot 10^6$ h | No. of facilities: | 5 (2 operators) |

**Design:** Ball

| | | | | | |
|---|---|---|---|---|---|
| $\lambda_{DU}$ = | 2.1 | $DU_{obs}$ = | 137 | Observation period: | 2006 – 2019 |
| $\lambda_{DU}^{70\%}$ = | 2.2 | $DU_{calc}$ = | 116 | Population size: | 1025 |
| $\lambda_{DU}^{5-95\%}$ = | [ 1.8, 2.4 ] | T = | $5.5 \cdot 10^7$ h | No. of facilities: | 7 (4 operators) |

**Design:** Gate

| | | | | | |
|---|---|---|---|---|---|
| $\lambda_{DU}$ = | 3.3 | $DU_{obs}$ = | 54 | Observation period: | 2006 – 2019 |
| $\lambda_{DU}^{70\%}$ = | 3.6 | $DU_{calc}$ = | 47 | Population size: | 300 |
| $\lambda_{DU}^{5-95\%}$ = | [ 2.6, 4.2 ] | T = | $1.4 \cdot 10^7$ h | No. of facilities: | 6 (3 operators) |

**Design:** Butterfly

| | | | | | |
|---|---|---|---|---|---|
| $\lambda_{DU}$ = | 3.1 | $DU_{obs}$ = | 13 | Observation period: | 2006 – 2019 |
| $\lambda_{DU}^{70\%}$ = | 3.7 | $DU_{calc}$ = | 12 | Population size: | 88 |
| $\lambda_{DU}^{5-95\%}$ = | [ 1.7, 4.9 ] | T = | $4.0 \cdot 10^6$ h | No. of facilities: | 7 (4 operators) |

*Failure Rate Assessment*

Data given for ESD and PSD valves (i.e., ESVs and XVs respectively). The population size and the number of observed DU failures have increased significantly as compared to the 2013 edition of the data handbook [1]. As a result, the overall suggested $\lambda_{DU}$ has also slightly increased (i.e., from 1.9 to 2.4 per $10^6$ hours). Note that in the previous edition of the handbook, the dangerous failure rate was based on operational review data from two facilities in addition to OREDA [19], whereas in this edition, operational review data from several additional facilities are included. This being the direct explanation for the increased failure rate.

$DU_{obs}$ specifies the number of observed DU failures. Some facilities (one onshore plant and one floating installation) have a disproportional number of observed DU failures (and these facilities are identified as "outliers"), typically due to a specific repeating systematic cause and / or other uncertainties related to the failure classification (i.e., generally less confidence in the data). These facilities (and associated DU failures) have therefore been weighted down (here to 25%) in order to reduce their contribution to the suggested $\lambda_{DU}$ (number of DU failures resulting from the weighting denoted as $DU_{calc}$).

| Module: Final Elements | PDS Reliability Data Dossier |
|---|---|
| Equipment Group: Topside Shutdown and Isolation Valves | |
| Component: Topside ESV and XV | |

*Failure Rate Assessment*

The suggested failure mode distribution (for dangerous failures) is based on internal and external studies of experienced failures (see e.g., [3], [19] and [22]). All ESD valves are assumed to have a tight shut off criterion. Hence, LCP (leakage in closed position) applies for all these valves. For XV valves with no tight shut off requirement, the contribution from or fraction of the failure rate resulting from LCP, may be disregarded.

Based on the data from the entire population of ESV/XV valves, we see that the failure rate generally increases with valve size and varies between design (ball, gate and butterfly valves). However, the uncertainty bounds are relatively large and partly overlapping, and only some 55% and 75% of the valves have been registered with valve size and design, respectively. Furthermore, we observe a varying failure rate depending on type of medium, but in a rather "inconsistent" matter. Here, many of the individual populations are small, and the classification applied for medium, e.g., for gas (where a difference between e.g., wet import gas and dry export gas is expected), and for HC liquid, is too coarse. For the purpose of differentiating between $\lambda_{DU}$ failure rates for ESVs/XVs, we therefore suggest to apply the below table (based on observed failure rates and expert judgments). Note that the mid row (normal HC service) represents the average of the collected data which is mainly represented by normal HC process service. Mild service here represents e.g., fuel gas, clean utility mediums, air/nitrogen, etc., whereas examples of dirty/severe service can be corrosive and erosive liquids and vapours, streams containing $H_2S$, high temperature crude, etc. Failure rates are given per $10^6$ hours.

| Service / medium | Ball valves | | Gate valves | |
|---|---|---|---|---|
| | ≤ 3" | > 3" | ≤ 3" | > 3" |
| Clean service | 1.2 | 1.6 | 1.7 | 2.2 |
| Normal HC service | 2 | 2.6 | 2.8 | 3.7 |
| Dirty/severe service | 4 | 5.2 | 5.6 | 7.4 |

Similar differentiation could also be done for ESVs and XVs separately, but as seen from the population details, the observed differences between valves in combined ESD/PDS service and valves in PSD service are very small, hence separate data dossiers are not presented for these two categories. Separate data dossier sheets have, however, been presented for ball and gate valves.

*Failure Rate References*

| Failure rates (per $10^6$ h) | Source | $DU_{obs}$ | T | Observation period | Population size |
|---|---|---|---|---|---|
| $\lambda_{DU}$ = 1.1 | Facility A | 21 | $2.0 \cdot 10^7$ h | 2006 – 2018 | 179 |
| *Comment:* | | | | | |
| $\lambda_{DU}$ = 5.2 | Facility B | 23 | $4.4 \cdot 10^6$ h | 2010 – 2013 | 171 |
| *Comment:* | | | | | |
| $\lambda_{DU}$ = 2.8 | Facility C | 18 | $6.5 \cdot 10^6$ h | 2010 – 2012 | 246 |
| *Comment:* | | | | | |
| $\lambda_{DU}$ = 4.9 | Facility D | 15 | $3.0 \cdot 10^6$ h | 2010 – 2013 | 87 |
| *Comment: 61 ESVs (15 DUs), 26 XVs.* | | | | | |

| Module: | Final Elements | | | | **PDS Reliability Data Dossier** |
|---|---|---|---|---|---|
| Equipment Group: | Topside Shutdown and Isolation Valves | | | | |
| Component: | Topside ESV and XV | | | | |
| *Failure Rate References* | | | | | |
| **Failure rates (per $10^6$ h)** | **Source** | **$DU_{obs}$** | **T** | **Observation period** | **Population size** |
| $\lambda_{DU}$ = 2.4 | Facility E | 1 | $4.2 \cdot 10^5$ h | 2010 – 2013 | 12 |
| *Comment: Four ESVs (1 DU), eight XVs.* | | | | | |
| $\lambda_{DU}$ = 3.7 | Facility O | 44 | $1.2 \cdot 10^7$ h | 2009 – 2012 | 272 |
| *Comment: Number of dangerous undetected failures has been given reduced weight (0.25) to reflect uncertainties with the underlying data material.* | | | | | |
| $\lambda_{DU}$ = 1.2 | Facility R | 8 | $6.5 \cdot 10^6$ h | 2016 – 2019 | 184 |
| *Comment:* | | | | | |
| $\lambda_{DU}$ = 1.7 | Facility S | 24 | $1.4 \cdot 10^7$ h | 2012 – 2018 | 225 |
| *Comment:* | | | | | |
| $\lambda_{DU}$ = 6.9 | Facility T | 8 | $1.2 \cdot 10^6$ h | 2016 – 2017 | 114 |
| *Comment:* | | | | | |
| $\lambda_{DU}$ = 3.4 | Facility U | 86 | $2.5 \cdot 10^7$ h | 2010 – 2019 | 356 |
| *Comment: Note that the number of components varies within the given time period, but the failure rate has been calculated from the total aggregated operational time.* | | | | | |
| $\lambda_{DU}$ = 1.9 | PDS 2013 [1] | | | | |
| *Comment: Data mainly based on two operational reviews and old OREDA data (1997 – 2003)* | | | | | |

## References

[1] Håbrekke, S., and Hauge, S., Reliability Data for Safety Instrumented Systems, PDS Data Handbook, 2013 ed., SINTEF, SINTEF A24443, ISBN 978-82-14-05600-6, 2013.

[2] Hauge, S., Kråkenes, T., Hokstad, P., Håbrekke, S., and Jin, H., Reliability Prediction Method for Safety Instrumented Systems – PDS Method Handbook, 2013 Edition. SINTEF report A24442, ISBN 978-82-536-1333-8, 2013.

[3] Hauge, S., Hoem, Å., Hokstad, P., Håbrekke, S., and Lundteigen M.A., Common Cause Failures in Safety Instrumented Systems, SINTEF A26922, ISBN 978-82-14-05953-3, 2015.

[4] IEC 61508 Standard. "Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety related systems", part 1-7, Edition 2.0, 2010.

[5] IEC 61511 Standard. "Functional safety - safety instrumented systems for the process industry sector", part 1 – 3, Edition 2, 2016.

[6] Norwegian Oil and Gas (NOROG), Guideline 070: "Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Recommended SIL requirements)". Norwegian Oil and Gas Association, rev. 04, 2020.

[7] Flexible proof testing of field devices in safety instrumented systems, NAMUR worksheet NA 106, 2018-09-06.

[8] Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design. 3rd Edition. ISO Standard 13849–1. 2015.

[9] The Meaning of Diagnostic Test Interval and its Impact on the Performance of Safety Instrumented Functions, Exida White paper, W.M. Goble and J.V. Bukowski, July 2017.

[10] Partial Stroke Testing of Automated Valves, ISA-TR96.05.01-2017.

[11] Hauge, S., Håbrekke, S., and Lundteigen, M. A., Standardised failure reporting and classification of SIS failures in the petroleum industry, SINTEF report no 2019:01303, rev. 03.

[12] ISO 14224. Petroleum, petrochemical and natural gas industries – Collection and exchange of reliability and maintenance data for equipment. Edition 3, 2016.

[13] Jenssen, H.P., ExproSoft Memo: "Reliability data from WellMaster RMS as input to revised SINTEF PDS Handbook", Version 02 (restricted), Date: 18.02.2020.

[14] Holand, P., Exprosoft Memo, "Subsea BOP data", Version 02, February 2020.

[15] Holand, P.: "Subsea BOP Reliability, Testing, and Well Kicks", Exprosoft report ES20150201/01, Trondheim 2019 (Open)

[16] Holand, P. & Awan, H.: "Reliability of Deepwater Subsea BOP Systems and Well Kicks"ExproSoft Report ES 201252/02, Trondheim Norway, 2012 (Unrestricted version).

[17] Holand, P.: "Reliability of Subsea BOP Systems for Deepwater Application, Phase II DW"Sintef Report STF38 A99426 Trondheim Norway, 1999 (Unrestricted version).

[18] Holand, P., Reliability of Subsea BOP Systems for Deepwater Application, Sintef Report STF38 F97417, Trondheim, Norway, 1997.

[19] OREDA participants, OREDA; Offshore Reliability Data Handbook, Volume 1 - topside data and Volume 2 – subsea data. 6th edition, 2015.

[20] Norwegian Petroleum Safety Authorities, Risikonivået i Norsk Petroleumsindustri (RNNP). Reported safety barrier data from 2003 – 2020.

[21] EXIDA, Safety Equipment Reliability Handbook, 3rd edition, Volume 1–3, exida.com, 2015.

[22] Håbrekke, S., Hauge S., Hoem Å., Lundteigen M.L., and Xie L., Modified generic failure rates for safety instrumented systems based on operational experience from the oil and gas industry, Esrel 2017.

[23] Håbrekke, S., Hauge S., Xie L., and Lundteigen M.L., Failure rates of safety critical equipment based on inventory attributes, Esrel 2018.

[24] API 521, Pressure-relieving and Depressuring Systems, 6th Edition, January 2014.

[25] STATOIL 2016, "SIS Reliability data from operation". Restricted and anonymised version of Safetec report provided to SINTEF for internal APOS/PDS project use.

[26] Hauge, S., and Onshus, T., Reliability Data for Safety Instrumented Systems, PDS Data Handbook, 2010 Edition. SINTEF report A13502. ISBN 978-82-14-04849-0.

[27] Centre for Chemical Process Safety (CCPS): Guidelines for safe automation of chemical processes, Wiley, second edition, 2017

[28] Béla G. Lipták (Editor): Instrument Engineers Handbook – Process Control and Optimisation, fourth edition, Taylor & Francis, 2006.

[29] Håbrekke, S., Hauge S., and Lundteigen M.L., Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase. SINTEF report 2020:00014, Rev. 02, 2021.

[30] ISO TR 12489. Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems. Edition 1, 2013.

[31] HSE. Offshore Technology Report: Reliability study into subsea isolation systems. OTH 94 445. Published 1996. ISBN 0-7176-1110-8.

[32] HSE. Offshore Technology Report: Extension of the subsea isolation systems reliability database. OTH 96 502. Published 1997. ISBN 0-7176-1301-1.

# Reliability Data for Safety Equipment

## PDS DATA HANDBOOK – 2021 EDITION

SINTEF is proud to present this new 2021 edition of the PDS data handbook. As compared to the 2013 edition, the historical data basis has been greatly expanded and the detailing and assessment of the data have been significantly improved. SINTEF has also developed a reliability prediction method (PDS Method Handbook), describing a practical approach for reliability and availability quantification. The PDS handbooks can be used to calculate safety integrity levels (SIL) in line with the IEC 61508 and IEC 61511 standards. The PDS handbooks are updated through the PDS Forum (see http://www.sintef.no/PDS).

**The SINTEF Group** is the largest independent research organisation in Scandinavia. SINTEF's goal is to contribute to wealth creation and to the sound and sustainable development of society. We generate new knowledge and solutions for our customers, based on research and development in technology, the natural sciences, medicine and the social sciences.

**SINTEF Digital**, Department of Software Engineering, Safety and Security performs contract research and development within the safety, reliability, maintenance and quality disciplines.

9 788214 064681