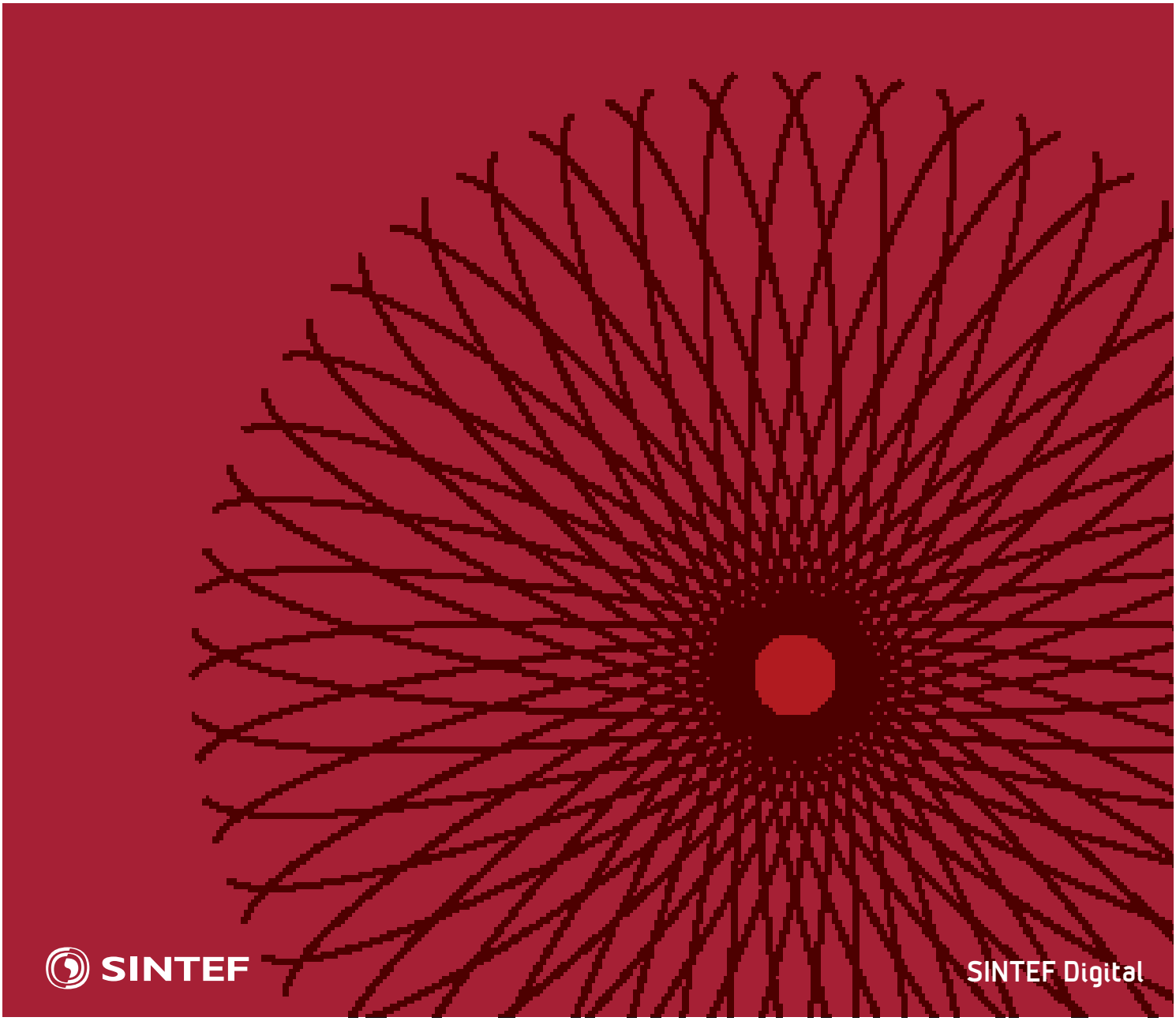
PDS DATA HANDBOOK – 2021 EDITION

Reliability Data for Safety Equipment



SINTEF

SINTEF Digital

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

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 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	DATE
FINAL	2021-05-30

AUTHORS
Maria Ottermo, Stein Hauge and Solfrid Håbrekke

CLIENT(S)	CLIENT'S REF.
Multiclient – PDS Forum	Mathilde Cot

PROJECT NO.	NUMBER OF PAGES:
60S051	214

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 (β 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

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). 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.). 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
λ_{crit}	Rate of critical failures. 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).
λ_{D}	Rate of dangerous failures, including both undetected and detected failures. $\lambda_{\text{D}} = \lambda_{\text{DU}} + \lambda_{\text{DD}}$ (see below).
λ_{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 (λ_{DU}), originating from random hardware failures.
λ_{DD}	Rate of dangerous detected failures, i.e., dangerous failures detected upon occurrence by e.g. self-diagnostics.
λ_{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 $= 1 - (\lambda_{\mathrm{DU}}/\lambda_{\mathrm{crit}}) \cdot 100\%$.
β	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; $\mathrm{DC} = (\lambda_{\mathrm{DD}}/\lambda_{\mathrm{D}}) \cdot 100\%$. 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. Note that the PFD is the average probability of failure on demand over a period of time, i.e., $\mathrm{PFD}_{\mathrm{avg}}$ as denoted in IEC 61508. However, due to simplicity $\mathrm{PFD}_{\mathrm{avg}}$ is denoted as PFD in the PDS handbooks.
τ	Interval of proof test (time between proof tests of a component).

2.3 Failure Classification Schemes

2.3.1 Failure Classification by Mode

In line with IEC 61508/615111, the PDS method considers both critical and non-critical failure modes. Dangerous, safe and non-critical failure modes are given the following interpretations – on a component level:

- **Dangerous (D):** The component does not operate upon a demand, e.g., sensor stuck upon demand or valve does not close on demand. The Dangerous failures are, depending on how they are revealed, further split into:
  - **Dangerous Undetected (DU):** Dangerous failures not detected automatically upon occurrence, i.e., revealed only by a functional test, or upon a planned or unplanned demand.
  - **Dangerous Detected (DD):** Dangerous failures detected automatically upon occurrence, e.g., by self-diagnostics or sensor comparison.

- **Safe (S):** Safe failures either cause a spurious operation of the equipment and/or maintain the equipment in a safe state. The safe failures are not dangerous with respect to the safety function of

the equipment itself but are often critical for production. Safe failures can be further split into safe detected (SD) and safe undetected (SU) failures (not further pursued in this handbook).

- **Non-critical (NONC):** The main function(s) of the component are still intact, but performance may be reduced. Non-critical failures will cover all failures that are not dangerous (safety critical) nor safe/spurious (production critical). They may be further split into:
  - **Degraded failures:** Failures where the ability of the equipment to carry out the required safety function (or maintain production) has not ceased but is *reduced*, and which over time may develop into a dangerous (or a safe) failure.
  - **No effect failure:** Failures that have no direct effect on the equipment safety (or production) function.

The Dangerous and Safe failures are considered *critical* in the sense that they may affect either of the two main functions of the component, i.e., (1) the ability to shut down on demand or (2) the ability to maintain production when safe. The safe failures are often revealed instantly upon occurrence. The dangerous failures are detected by built in self-diagnostic or sensor comparison (dangerous detected) or are "dormant" and can only be detected upon testing or a true demand (dangerous undetected).

It should also be noted that a given failure may be classified as either dangerous or safe depending on the intended application. E.g., loss of hydraulic supply to a valve actuator operating on-demand will be dangerous in an energise-to-trip application and safe in a de-energise-to-trip application. Hence, when performing reliability calculations, the assumptions underlying the applied failure data as well as the context in which the data shall be used must be carefully considered. Definitions of dangerous failure are included in the data dossiers in Chapter 4.

2.3.2 Failure Classification by Cause

Failures can be categorised according to failure cause and the IEC standards differentiate between *random hardware failure* and *systematic failure*. PDS uses the same classification and suggests a somewhat more detailed breakdown, as indicated in Figure 2.1.

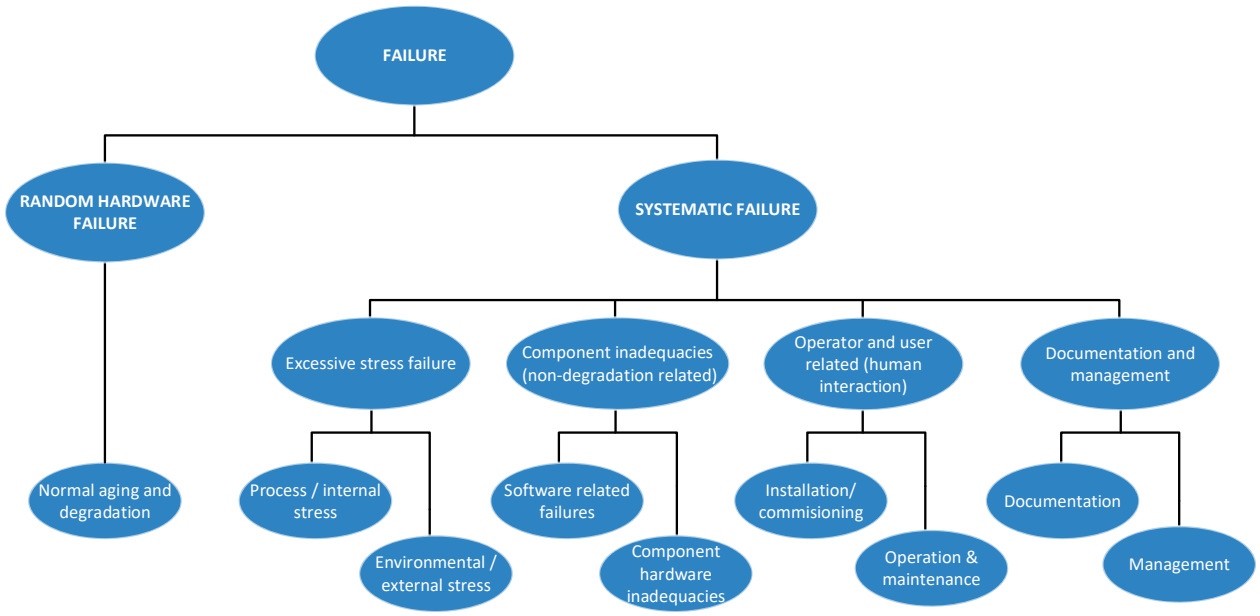


Figure 2.1 Possible failure classification by cause of failure

Random hardware failures are failures occurring at a random time during operation, resulting from one or more degradation mechanisms. It is here assumed that the operating conditions are within the design envelope of the system.

Systematic failures are in PDS defined as failures that can be related to a specific cause other than natural degradation. Systematic failures are due to errors made during specification, design, operation and maintenance phases of the lifecycle. Such failures can therefore normally be eliminated by a modification, either of the design or manufacturing process, the testing and operating procedures, the training of personnel or changes to procedures and/or work practices.

The failure rates presented in this handbook are based on operational experience, and do not distinguish explicitly between failure causes. However, some values for the relative distributions between random hardware failures and systematic failures are suggested (RHF, see section 2.4.4 and section 3.7). For further discussion of suggested taxonomies for failure modes, detection methods, failure causes and equipment classification, reference is made to the APOS project [11].

2.4 Reliability Parameters

2.4.1 The Beta (β) factor and C_{MooN}

When quantifying the reliability of systems with redundancy / voted systems, e.g., duplicated, or triplicated systems, it is essential to distinguish between *independent* and *dependent* failures. Random hardware failures due to natural stressors are often assumed to be *independent* failures. However, all systematic failures, e.g., hardware inadequacies and maintenance errors, are *dependent* failures and can lead to simultaneous failure of more than one (redundant) component in the safety system, reducing the advantage of redundancy.

Dependent or common cause failures are often accounted for by the β factor approach. The PDS method presents a β factor model that distinguishes between different types of redundancies by introducing β factors which depend on the configuration, i.e., $\beta(MooN) = \beta \cdot C_{MooN}$. Here, C_{MooN} is a modification factor depending on the configuration, $MooN$. A similar concept is described in IEC 61508-6 (Table D.5).

Values for C_{MooN} are given in Table 3. For a more complete description of the extended β factor approach and the reasoning behind the C_{MooN} values, see the 2013 PDS method handbook [2]. SINTEF's suggested values for the β factor for different equipment types are given in section 3.4.

Table 2.2: Numerical values for configuration factor, C_{MooN}

$M \setminus N$	$N = 2$	$N = 3$	$N = 4$	$N = 5$	$N = 6$
$M = 1$	$C_{1oo2} = 1.0$	$C_{1oo3} = 0.5$	$C_{1oo4} = 0.3$	$C_{1oo5} = 0.2$	$C_{1oo6} = 0.15$
$M = 2$	-	$C_{2oo3} = 2.0$	$C_{2oo4} = 1.1$	$C_{2oo5} = 0.8$	$C_{2oo6} = 0.6$
$M = 3$	-	-	$C_{3oo4} = 2.8$	$C_{3oo5} = 1.6$	$C_{3oo6} = 1.2$
$M = 4$	-	-	-	$C_{4oo5} = 3.6$	$C_{4oo6} = 1.9$
$M = 5$	-	-	-	-	$C_{5oo6} = 4.5$

2.4.2 Safe Failure Fraction (SFF)

The Safe Failure Fraction as described in IEC 61508 is given by the ratio between dangerous detected failures plus safe failures and the total rate of critical failures, i.e., SFF $= (\lambda_{DD} + \lambda_S)/(\lambda_D + \lambda_S)$. The SFF can also be estimated as:

- SFF $= 1 - (\lambda_{DU}/\lambda_{crit})$; or rather in percentage: SFF $= [1 - (\lambda_{DU}/\lambda_{crit})] \cdot 100\%$.

The SFF values presented in this handbook are based on reported failure mode distributions in operational reviews, as well as additional expert judgements by SINTEF and industry in workshops. Higher (or lower) SFFs than indicated in the tables will apply for specific equipment types, but should be documented, e.g., by FMEDA type of analyses.

2.4.3 Diagnostic coverage (DC) and proof test coverage (PTC)

There are two main test methods available to detect dangerous SIS failures:

- Automatic on-line diagnostic testing.
- Manual proof testing, including activation of the SIS component.

To perform PFD quantification, the effectiveness of these two methods needs to be known.

- The effectiveness of the automatic diagnostic test is defined by the diagnostic coverage (DC). A distinction is often made between internal self-diagnostic built into the equipment and external diagnostic facilities implemented by the user (e.g., comparison of different instrument readings). Both properties are however captured by the DC. See section 3.5.

- The effectiveness of manual proof testing is defined by the proof test coverage (PTC). Based on the extent and quality of the proof test, such as a complete functional test versus a partial test, the PTC will vary since a varying number of failure modes (and associated failure causes) can be revealed.

Both the DC and PTC will affect the system availability, but they differ slightly in terms of their mathematical treatment in the PFD calculations:

- DC defines the fraction of dangerous failures that are revealed by diagnostic on-line tests and is mathematically expressed as: DC $= (\lambda_{DD}/\lambda_D) \cdot 100\%$. Since $\lambda_{DU} + \lambda_{DD} = \lambda_D$, diagnostic coverage can also be expressed as: DC $= (1 - \lambda_{DU}/\lambda_D) \cdot 100\%$. The assumed value of DC will therefore affect the rate of DU failures (λ_{DU}) used in the PFD calculations.

- The PTC defines the fraction of DU failures that is revealed during a proof test. This implies that the rate of DU failures (λ_{DU}) *itself* is not directly affected. However, when the PTC is less than 100%, the PFD is affected since some DU failures are not revealed upon test but remain dormant until a test that completely restores the component's functionality (PTC = 100%) has been performed. This contributes to an increasing average PFD as illustrated in Figure 2.2. Here an *incomplete* test (with PTC less than 100%) is performed with interval τ and this test reveals a certain fraction of the DU failures. At time T a *complete* functional test that also reveals the residual DU failures, is performed, and the system is assumed restored back to its original state.

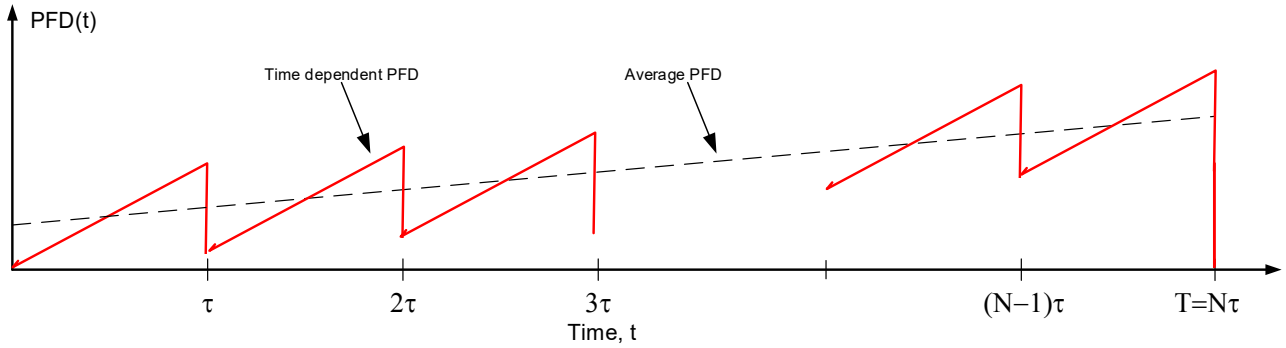


Figure 2.2 Time dependent PFD with PTC < 100%

Mathematically, the above implies that the rate of dangerous undetected failures can now be split into:

1. Failures *detected* during normal proof testing: with rate $\text{PTC} \cdot \lambda_{\text{DU}}$ and proof test interval τ, and
2. Failures *not detected* during normal proof testing: with rate $(1 - \text{PTC}) \cdot \lambda_{\text{DU}}$ and "test interval" T.

For a 1oo1 configuration the PFD is then given as:

$$\text{PFD}_{1\text{oo}1} \approx \text{PTC} \cdot \left(\lambda_{\text{DU}} \cdot \frac{\tau}{2}\right) + (1 - \text{PTC}) \cdot \left(\lambda_{\text{DU}} \cdot \frac{T}{2}\right).$$

For a more detailed discussion, reference is made to the PDS method handbook [2].

Proof tests as diagnostic tests – partial stroke testing
Note that *in theory*, any proof test can be turned into a diagnostic test, but it requires that the frequency of this automated or on-line (i.e., during operation) proof test is sufficiently high. In [7] it is suggested that the frequency of the automated test should *at least be a factor 100 of the demand rate of the associated SIS*. This factor is also discussed in IEC 61508-2 [4] (section 7.4.4.1) for high demand systems, as well as in an EXIDA white paper [9]. Note that for low demand systems, the diagnostic test frequency is normally only minutes or seconds (or even microseconds), i.e., a factor by far exceeding 100 times the demand rate.

The latter implies that partial stroke testing of valves can normally *not* be accounted for as a diagnostic test due to too infrequent execution. Rather, a partial stroke test should be counted as a proof test with reduced test coverage as discussed above. See also section 3.6.3 for further discussion of test coverage for partial stroke testing.

2.4.4 Random Hardware Failure fraction (RHF)

Failure rates based on analyses and/or provided by manufacturers often tend to exclude systematic failures related to installation, commissioning, or operation of the equipment. A mismatch between manufacturer / certificate data and operational data is therefore often observed. However, since systematic failures inevitably will occur, why not include these failures in predictive reliability analyses (see also discussion in section 1.2)?

The approach taken in this handbook is to present reliability data based on historically observed and further classified failures. As a result, both random hardware failures and systematic failures will be included in the presented failure rates. To reflect this, the parameter RHF has been defined as the fraction of dangerous undetected failures (λ_{DU}) originating from random hardware failures ($\lambda_{\text{DU-RH}}$), i.e., $\text{RHF} = \lambda_{\text{DU-RH}}/\lambda_{\text{DU}}$ (i.e., $1 - \text{RHF}$ becomes the fraction of systematic failures). Indicative values of the RHF factor, based on observed failure causes, are given in section 3.7, but will obviously depend heavily on facility specific conditions.

3 RELIABILITY DATA SUMMARY

This chapter gives a summary of SINTEF's best estimates for failure rates, DCs and SFFs (see section 2.2. for definitions), for topside, subsea, downhole well completion, and drilling equipment, respectively. For each component, a reference to the detailed data dossier in Chapter 4 is given. The notion (D) is used to indicate that the data dossier presents more detailed/differentiated component failure rates for selected component characteristics and attributes such as measuring principle, dimension, design, etc.

Values for $\lambda_{DU}^{70\%}$, i.e., the upper 70% confidence limits of the dangerous undetected failure rates, are included to indicate uncertainty in the failure rate estimate (see also section 3.8). Note that in cases where there is a small difference between λ_{DU} and $\lambda_{DU}^{70\%}$ (due to very large component populations), the failure rates are, instead of one decimal, given with two decimal places. Similarly, round-off errors can in some cases result in small differences between λ_{crit} and $\lambda_S + \lambda_D$.

Suggested β values are presented in section 3.4 and some background information on the values for diagnostic coverage are given in section 3.5. Also, other aspects such as PTC values, failure causes, RHF values and data uncertainties are discussed.

3.1 Topside Equipment

Table 3.1 – Table 3.4 summarise SINTEF's best estimates for input data to reliability analyses of topside equipment.

3.1.1 Input devices

Table 3.1 – Table 3.3 summarise failure rates, diagnostic coverage (DC) and safe failure fraction (SFF) for transmitters and switches, detectors, and pushbuttons.

Table 3.1: Failure rates (per 10^6 hour), DC and SFF – Transmitters and switches

Component	λ_{crit}	λ_S	λ_D	λ_{DU}	$\lambda_{DU}^{70\%}$	DC	SFF	Section
Position (proximity or limit) switch	1.9	0.7	1.2	1.1	1.3	5%	41%	4.2.1
Aspirator system including flow switch (excl. detector)	4.6	1.9	2.6	2.5	3.0	5%	46%	4.2.2
Pressure transmitter	1.95	0.58	1.36	0.48	0.52	65%	75%	4.2.3 (D)
Level transmitter	10	4.2	6.3	1.9 [1)]	2.5	70%	82%	4.2.4 (D)
Temperature transmitter	0.7	0.3	0.4	0.1	0.2	70%	82%	4.2.5 (D)
Flow transmitter	6.6	2.7	4.0	1.4	1.8	65%	79%	4.2.6 (D)

[1)] See section 4.2.4 for a more thorough discussion of how failure rates vary with complexity of application.

Rest of table not shown in this free copy

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 λ_{DU}, λ_D, λ_S and λ_{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 β factor for the specified component under consideration. For a further discussion β 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.

λ_{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:

λ_{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 λ_{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.

4.2.4 Level Transmitter

Module:	Input Devices	**PDS Reliability Data Dossier**
Equipment Group:	Process Transmitters	
Component:	Level Transmitter	

Component Boundaries / Failure Definition

The level transmitter includes the sensing element, local electronics and the process isolation valves/process connections. Corresponds to ISO 14224 equipment class = Input devices.
Dangerous failure typically defined as: *"transmitter does not provide correct signal/alarm when the process parameter falls outside the setpoint limit(s)", (i.e., no/frozen signal, or signal read value deviates more than e.g., 5% from true process conditions, criticality depending on LL and/or HH application).*

SINTEF's Best Estimates

Failure rates (per 10^6 h)		**Coverage/Other**	
λ_{DU} =	1.9	DC =	0.70
λ_D =	6.3	β =	0.10
λ_S =	4.2		
λ_{crit} =	10		

λ_{DU} (per 10^6 h) Uncertainty and Population Details

All operational review data

λ_{DU} =	1.9	DU_{obs} =	57	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%}$ =	2.0	DU_{calc} =	57	Population size:	542
$\lambda_{DU}^{5\text{-}95\%}$ = [	1.5, 2.4]	T =	$3.0 \cdot 10^7$ h	No. of facilities:	9 (5 operators)

Measuring principle: Displacer

λ_{DU} =	0.7	DU_{obs} =	3	Observation period:	2006 – 2018
$\lambda_{DU}^{70\%}$ =	1.1	DU_{calc} =	3	Population size:	74
$\lambda_{DU}^{5\text{-}95\%}$ = [	0.2, 1.9]	T =	$4.2 \cdot 10^6$ h	No. of facilities:	3 (1 operator)

Measuring principle: Differential pressure

λ_{DU} =	3.2	DU_{obs} =	22	Observation period:	2006 – 2019
$\lambda_{DU}^{70\%}$ =	3.7	DU_{calc} =	22	Population size:	198
$\lambda_{DU}^{5\text{-}95\%}$ = [	2.2, 4.6]	T =	$6.9 \cdot 10^6$ h	No. of facilities:	4 (2 operators)

Measuring principle: Free space radar

λ_{DU} =	2.7	DU_{obs} =	6	Observation period:	2006 – 2018
$\lambda_{DU}^{70\%}$ =	3.7	DU_{calc} =	6	Population size:	40
$\lambda_{DU}^{5\text{-}95\%}$ = [	1.2, 5.4]	T =	$2.2 \cdot 10^6$ h	No. of facilities:	6 (2 operators)

Measuring principle: Nuclear

λ_{DU} =	4.1	DU_{obs} =	4	Observation period:	2010 – 2018
$\lambda_{DU}^{70\%}$ =	6.1	DU_{calc} =	4	Population size:	24
$\lambda_{DU}^{5\text{-}95\%}$ = [	1.4, 9.4]	T =	$1.0 \cdot 10^6$ h	No. of facilities:	4 (2 operators)

Failure Rate Assessment

Note that the average observed λ_{DU} failure rate is more than doubled compared to the previous 2013 edition [1] of the handbook. This is mainly explained by more operational data and the fact that level measuring is difficult and therefore associated with both practical and methodical challenges, especially related to the complexity of the specific application (with associated systematic failures).

Module:	Input Devices	**PDS Reliability Data Dossier**
Equipment Group:	Process Transmitters	
Component:	Level Transmitter	

Failure Rate Assessment

Selection of appropriate measuring principle for the specific process/application is essential. It has for example been observed that liquid density variations combined with relatively narrow measuring ranges, are causing problems for transmitters that rely on calibration against an assumed average density. The observed failure rates for different measuring principles are comparable, with exception of displacer, which is lower (and nuclear which is somewhat higher). Displacer transmitters are often used in relatively simple storage tank applications, where e.g., interface and foaming issues are less relevant. The high failure rate of nuclear level transmitters may be related to challenging applications. Note that the failure rate uncertainty is large for these nuclear transmitters due to very limited operational experience. Also note that the measuring principle is known only for some 40% of the total population.
A somewhat higher DC (increased from 60% to 70%) has been assumed for level transmitters (see discussion in section 3.5.2) whereas the distribution between safe failures and dangerous failures is assumed approximately the same as in the 2013 edition. As a result, λ_{crit} has increased as compared to the 2013 edition [1]. See also additional comments under each data source below.

Failure Rate References

Failure rates (per 10^6 h)	**Source**		**DU_{obs}**	**T**	**Observation period**	**Population size**
λ_{DU} = 1.1	Facility	A	7	6.7 ·10^6 h	2006 – 2018	64
Comment: 22 tags displacer (0 DU), 14 tags differential pressure (1 DU (3 CCFs removed)), 11 tags free space radar (3 DUs), eight tags nuclear (1 DU), nine tags other measuring principle (2 DUs). Note that for the eight nuclear tags, data before 2016 are not included. These transmitters had calibration issues and were replaced with a new generation in 2015.						
λ_{DU} = 5.3	Facility	B	5	9.5 ·10^5 h	2010 – 2013	36
Comment: 27 tags differential pressure (3 DUs), three tags free space radar (0 DU), six tags nuclear (2 DUs).						
λ_{DU} = 2.0	Facility	C	5	2.5 ·10^6 h	2010 – 2012	95
Comment: 20 tags displacer (1 DU), 61 tags differential pressure (4 DUs), six tags free space radar (0 DU), eight tags other measuring principle (0 DU).						
λ_{DU} = 4.1	Facility	D	4	1.0 ·10^6 h	2010 – 2013	28
Comment: Three tags nuclar (0 DU), 25 tags differential pressure (4 DUs).						
λ_{DU} = 3.6	Facility	O	12	3.3 ·10^6 h	2009 – 2012	94
Comment: 32 tags displacer (2 DUs (7 CCFs/repeating failures removed)), 20 tags free space radar (3 DUs), 28 tags differential pressure (7 DUs), 14 tags other measuring principle.						
λ_{DU} = 2.3	Facility	R	3	1.3 ·10^6 h	2016 – 2019	50
Comment: 43 differential pressure (3 DUs), seven tags other measuring principle (0 DU).						
λ_{DU} = 2.3	Facility	S	1	4.3 ·10^5 h	2010 – 2018	7
Comment: All nuclear (gamma) transmitters.						
λ_{DU} = 7.2	Facility	T	2	2.8 ·10^5 h	2016 – 2017	27
Comment:						
λ_{DU} = 1.3	Facility	U	18	1.4 ·10^7 h	2008 – 2019	141
Comment: Data from onshore plant.						
λ_{DU} = 1.0	PDS 2013 [1]					
Comment:						

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