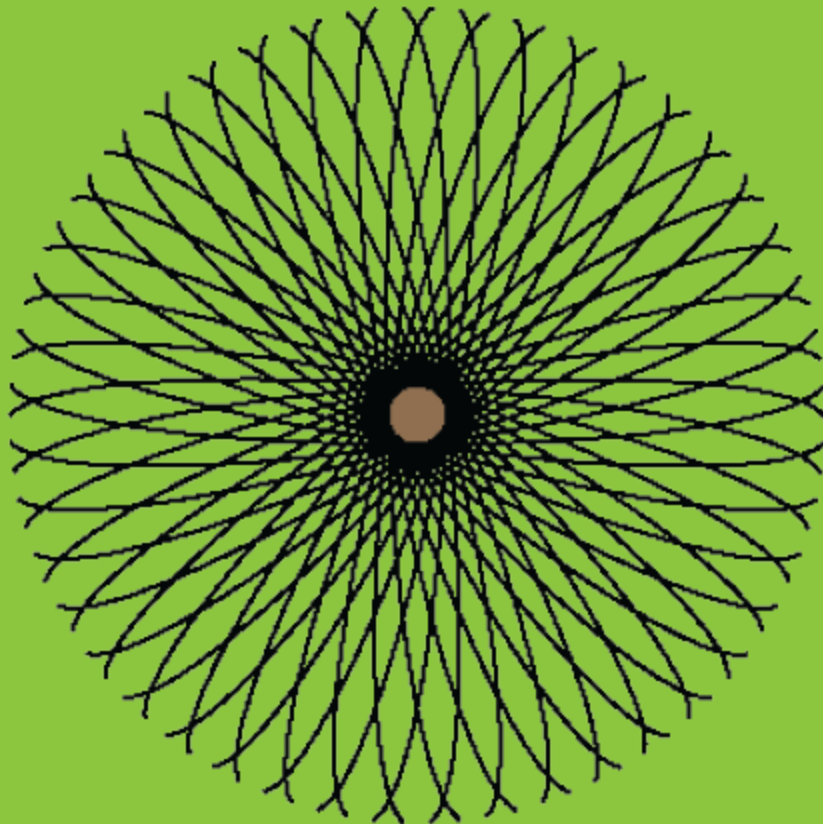


**Free electronic version
Selected pages only**

Reliability Data for
Safety Instrumented Systems

PDS DATA HANDBOOK 2010 EDITION



PREFACE

The present report is an update of the 2006 edition of the Reliability Data for Control and Safety Systems, PDS Data Handbook [12]. The handbook presents data in line with the latest available data sources as well as data for some new equipment.

The work has been carried out as part of the research project “Managing the integrity of safety instrumented systems”.¹

Trondheim, December 2009

Stein Hauge

PDS Forum Participants in the Project Period 2007 - 2009

Oil Companies/Operators

- A/S Norske Shell
- BP Norge AS
- ConocoPhillips Norge
- Eni Norge AS
- Norsk Hydro ASA
- StatoilHydro ASA (Statoil ASA from Nov. 1st 2009)
- Talisman Energy Norge
- Teekay Petrojarl ASA
- TOTAL E&P NORGE AS

Control and Safety System Vendors

- ABB AS
- FMC Kongsberg Subsea AS
- Honeywell AS
- Kongsberg Maritime AS
- Bjørge Safety Systems AS
- Siemens AS
- Simtronics ASA

Engineering Companies and Consultants

- Aker Kværner Engineering & Technology
- Det Norske Veritas AS
- Lilleaker Consulting AS
- NEMKO AS
- Safetec Nordic AS
- Scandpower AS

Governmental Bodies

- The Directorate for Civil Protection and Emergency Planning (Observer)
- The Norwegian Maritime Directorate (Observer)
- The Petroleum Safety Authority Norway (Observer)

¹ This user initiated research project has been sponsored by the Norwegian Research Council and the PDS forum participants. The project work has been carried out by SINTEF.

ABSTRACT

This report provides reliability data estimates for components of control and safety systems. Data dossiers for input devices (sensors, detectors, etc.), control logic (electronics) and final elements (valves, etc.) are presented, including some data for subsea equipment. Efforts have been made to document the presented data thoroughly, both in terms of applied data sources and underlying assumptions. The data are given on a format suitable for performing reliability analyses in line with the requirements in the IEC 61508 and IEC 61511 standards.

As compared to the former 2006 edition, the following main changes are included:

- A general review and update of the failure rates, coverage values, β -values and other relevant parameters;
- Some new equipment groups have been added;
- Data for control logic units have been updated and refined.

Table of Contents

PREFACE	3
ABSTRACT	4
1 INTRODUCTION	9
1.1 Objective and Scope	9
1.2 Benefits of Reliability Analysis – the PDS Method	9
1.3 The IEC 61508 and 61511 Standards	10
1.4 Organisation of Data Handbook	10
1.5 Abbreviations	10
2 RELIABILITY CONCEPTS	13
2.1 The Concept of Failure	13
2.2 Failure Rate and Failure Probability	13
2.2.1 Failure Rate Notation	13
2.2.2 Decomposition of Failure Rate	14
2.3 Reliability Measures and Notation	15
2.4 Reliability Parameters	16
2.4.1 Rate of Dangerous Undetected Failures	16
2.4.2 The Coverage Factor, c	17
2.4.3 Beta-factors and C_{MooN}	17
2.4.4 Safe Failure Fraction, SFF	18
2.5 Main Data Sources	18
2.6 Using the Data in This Handbook	19
3 RELIABILITY DATA SUMMARY	21
3.1 Topside Equipment	21
3.2 Subsea Equipment	27
3.3 Comments to the PDS Data	28
3.3.1 Probability of Test Independent Failures (P_{TIF})	28
3.3.2 Coverage	29
3.3.3 Fraction of Random Hardware Failures (r)	30
3.4 Reliability Data Uncertainties – Upper 70% Values	32
3.4.1 Data Uncertainties	32
3.4.2 Upper 70% Values	33
3.5 What is “Sufficient Operational Experience“? – Proven in Use	34
4 MAIN FEATURES OF THE PDS METHOD	37
4.1 Main Characteristics of PDS	37
4.2 Failure Causes and Failure Modes	37
4.3 Reliability Performance Measures	39
4.3.1 Contributions to Loss of Safety	40
4.3.2 Loss of Safety due to DU Failures - Probability of Failure on Demand (PFD)	40
4.3.3 Loss of Safety due to Test Independent Failures (P_{TIF})	40
4.3.4 Loss of Safety due to Downtime Unavailability – DTU	41
4.3.5 Overall Measure for Loss of Safety– Critical Safety Unavailability	41
5 DATA DOSSIERS	43
5.1 Input Devices	44
5.1.1 Pressure Switch	44
5.1.2 Proximity Switch (Inductive)	46

5.1.3	Pressure Transmitter	47
5.1.4	Level (Displacement) Transmitter	49
5.1.5	Temperature Transmitter	51
5.1.6	Flow Transmitter	53
5.1.7	Catalytic Gas Detector	55
5.1.8	IR Point Gas Detector	57
5.1.9	IR Line Gas Detector	60
5.1.10	Smoke Detector	62
5.1.11	Heat Detector	64
5.1.12	Flame Detector	66
5.1.13	H ₂ S Detector	69
5.1.14	ESD Push Button	71
5.2	Control Logic Units	73
5.2.1	Standard Industrial PLC	74
5.2.2	Programmable Safety System	80
5.2.3	Hardwired Safety System	86
5.3	Final Elements	89
5.3.1	ESV/XV	89
5.3.2	ESV, X-mas Tree	93
5.3.3	Blowdown Valve	96
5.3.4	Pilot/Solenoid Valve	98
5.3.5	Process Control Valve	101
5.3.6	Pressure Relief Valve	104
5.3.7	Deluge Valve	106
5.3.8	Fire Damper	107
5.3.9	Circuit Breaker	109
5.3.10	Relay	110
5.3.11	Downhole Safety Valve – DHSV	111
5.4	Subsea Equipment	112
6	REFERENCES	117

List of Tables

Table 1	Decomposition of critical failure rate, λ_{crit}	15
Table 2	Performance measures and reliability parameters	15
Table 3	Failure rates, coverages and SFF for input devices	21
Table 4	Failure rates, coverages and SFF for control logic units	22
Table 5	Failure rates, coverages and SFF for final elements	23
Table 6	P_{TIF} for various components	24
Table 7	β -factors for various components	25
Table 8	Numerical values for configuration factors, C_{MooN}	26
Table 9	Failure rates for subsea equipment - input devices, control system units and output devices.....	27
Table 10	Estimated upper 70% confidence values for topside equipment.....	33
Table 11	Discussion of proposed subsea data	112

List of Figures

Figure 1	Decomposition of critical failure rate, λ_{crit}	15
Figure 2	Illustration of failure rate with confidence level of 70%	32
Figure 3	Failure classification by cause of failure.....	38
Figure 4	Contributions to critical safety unavailability (CSU).....	42

1 INTRODUCTION

Safety standards like IEC 61508, [1] and IEC 61511, [2], require quantification of failure probability for operation of safety systems. Such quantification may be part of design optimization or verification that the design is according to stated performance requirements.

The use of relevant failure data is an essential part of any quantitative reliability analysis. It is also one of the most challenging parts and raises a number of questions concerning the availability and relevance of the data, the assumptions underlying the data and what uncertainties are related to the data.

In this handbook recommended data for reliability quantification of Safety Instrumented Systems (SIS) are presented. Efforts have been made to document the presented data thoroughly, both in terms of applied data sources and underlying assumptions.

Various data sources have been applied when preparing this handbook, the most important source being the OREDA database and handbooks (ref. section 2.5).

1.1 Objective and Scope

When performing reliability quantification, the analyst will need information on a number of parameters related to the equipment under consideration. This includes basic failure rates, distribution of critical failure modes, diagnostic coverage factors and common cause factors. In this handbook best estimates for these reliability parameters are presented for selected equipment. The data are given on a format suitable for performing analyses in line with the requirements in the IEC 61508/61511 standards and the PDS method, [10].

As compared to the former 2006 edition, [12], the following main changes are included:

- A general update / review of the failure rates, coverage values, β -values and other relevant parameters;
- Some new equipment groups have been added;
- Data for control logic units have been updated and refined.

1.2 Benefits of Reliability Analysis – the PDS Method

Instrumented safety systems such as emergency shutdown systems, fire and gas systems and process shutdown systems, are installed to prevent abnormal operating conditions from developing into an accident. High reliability of such systems is therefore paramount with respect to safe - as well as commercial - operation.

Reliability analysis represents a systematic tool for evaluating the performance of safety instrumented systems (SIS) from a safety and production availability point of view. Some main applications of reliability analysis are:

- Reliability assessment and follow-up; verifying that the system fulfils its safety and reliability requirements;
- Design optimisation; balancing the design to get an optimal solution with respect to safety, production availability and lifecycle cost;
- Operation planning; establishing the optimal testing and maintenance strategy;

- Modification support; verifying that planned modifications are in line with the safety and reliability requirements.

The PDS method has been developed in order to enable the reliability engineer and non-experts to perform such reliability considerations in various phases of a project. The main features of the PDS method are discussed in chapter 4.

1.3 The IEC 61508 and 61511 Standards

The IEC 61508 and IEC 61511 standards, [1] and [2], present requirements to safety instrumented systems (SIS) for all the 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. These standards present a unified approach to achieve a rational and consistent technical policy for all SIS systems. The Norwegian Oil Industry Association (OLF) has developed a guideline to support the use of IEC 61508/61511, [19].

The PDS method is in line with the main principles advocated in the IEC standards, and is a useful tool when implementing and verifying quantitative (SIL) requirements as described in the IEC standards.

1.4 Organisation of Data Handbook

In chapter 2 important reliability aspects are discussed and definitions of the applied notations are given.

The recommended reliability data estimates are summarised in chapter 3 of this report. A split has been made between input devices, logic solvers and final elements.

Chapter 4 gives a brief summary of the main characteristics of the PDS method. The failure classification for safety instrumented systems is presented together with the main reliability performance measures used in PDS.

In chapter 5 the detailed data dossiers providing the basis for the recommended reliability data are given. As for previous editions of the handbook, some data are scarcely available in the data sources, and it is necessary to, partly or fully, rely on expert judgements.

1.5 Abbreviations

CCF	-	Common cause failure
CSU	-	Critical safety unavailability
DTU	-	Downtime unavailability
FMECA	-	Failure modes, effects, and criticality analysis
FMEDA	-	Failure modes, effects, and diagnostic analysis
IEC	-	International Electro technical Commission
JIP	-	Joint industry project
MTTR	-	Mean time to restoration
NDE	-	Normally de-energised
NE	-	Normally energised
OLF	-	The Norwegian oil industry association

OREDA	-	Offshore reliability data
PDS	-	Norwegian acronym for “reliability of computer based safety systems”
PFD	-	Probability of failure on demand
RNNP	-	<i>Project</i> : Risk level in Norwegian petroleum production www.ptil.no
SIL	-	Safety integrity level
SIS	-	Safety instrumented system
SFF	-	Safe failure fraction
STR	-	Spurious trip rate
TIF	-	Test independent failure

Additional abbreviations (equipment related)

AI	-	Analogue input
BDV	-	Blowdown valve
CPU	-	Central Processing Unit
DO	-	Digital output
ESV	-	Emergency shutdown valve
DHSV	-	Downhole safety valve
XV	-	Production shutdown valve

2 RELIABILITY CONCEPTS

In this chapter some selected concepts related to reliability analysis and reliability data are discussed. For a more detailed discussion reference is made to the updated PDS method handbook, ref. [10].

2.1 The Concept of Failure

A failure is in IEC 61508-4 defined as the *termination of the ability of a functional unit to perform a required function*. The two main functions of a safety system are [10]; the ability to shut down or go to a predefined safe state when production is not safe and the ability to maintain production when it is safe. Hence, a failure may have two facets; (1) loss of the ability to shut down or go to a safe state when required or (2) loss of the ability to maintain production.

From a safety point of view, the first category will be the more critical and such failures are defined as dangerous failures (D), i.e. they have the potential to result in loss of the ability to shut down or go to a safe state when required.

Loss of the ability to maintain production is normally not so critical to safety and such failures have therefore in PDS traditionally been denoted spurious trip (ST) failures whereas IEC 61508 categorise such failures as ‘safe’ (S). In the forthcoming update of the IEC 61508 standard the definition of safe failures is more in line with the PDS interpretation. Therefore PDS have in this updated version also applied the notation ‘S’ (instead of ‘ST’ failures).

It should 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 applying the failure data, the assumptions underlying the data as well as the context in which the data shall be used must be carefully considered.

2.2 Failure Rate and Failure Probability

The failure rate (numbers of failures per time unit) for a component is essential for the reliability calculations. In section 2.2.1, definitions and notation related to the failure rate are given, whereas in section 2.2.2 the decomposition of this failure rate into its various elements is further discussed.

2.2.1 Failure Rate Notation

λ_{crit} = Rate of critical failures; i.e., failures that may cause loss of one of the two main functions of the component/system (see above).

Critical failures include dangerous (D) failures which may cause loss of the ability to shut down production when required and safe (S) failures which may cause loss of the ability to maintain production when safe (i.e. spurious trip failures). Hence:

$$\lambda_{crit} = \lambda_D + \lambda_S \text{ (see below)}$$

λ_D = Rate of dangerous (D) failures, including both undetected as well as detected failures. $\lambda_D = \lambda_{DU} + \lambda_{DD}$ (see below)

- λ_{DU} = Rate of dangerous undetected failures, i.e. failures undetected both by automatic self-test or personnel
- λ_{DD} = Rate of dangerous detected failures, i.e. failures detected by automatic self-test or personnel
- λ_S = Rate of safe (spurious trip) failures, including both undetected as well as detected failures. $\lambda_S = \lambda_{SU} + \lambda_{SD}$ (see below)
- λ_{SU} = Rate of safe (spurious trip) undetected failures, i.e. undetected both by automatic self-test and personnel
- λ_{SD} = Rate of safe (spurious trip) detected failures, i.e. detected by automatic self-test or personnel
- λ_{undet} = Rate of (critical) failures that are undetected both by automatic self-test and by personnel (i.e., detected in functional testing only). $\lambda_{undet} = \lambda_{DU} + \lambda_{SU}$
- λ_{det} = Rate of (critical) failures that are detected by automatic self-test or personnel (independent of functional testing). $\lambda_{det} = \lambda_{DD} + \lambda_{SD}$
- c = Coverage: percentage of critical failures detected *either* by the automatic self-test *or* (incidentally) by personnel observation
- c_D = Coverage of dangerous failures. $c_D = (\lambda_{DD} / \lambda_D) \cdot 100\%$
Note that λ_{DU} then can be calculated as: $\lambda_{DU} = \lambda_D \cdot (1 - c_D/100\%)$
- c_S = Coverage of safe (spurious trip) failures. $c_S = (\lambda_{SD} / \lambda_S) \cdot 100\%$
Note that λ_{SU} then can be calculated as: $\lambda_{SU} = \lambda_S \cdot (1 - c_S/100\%)$
- r = Fraction of dangerous undetected (DU) failures originating from random hardware failures ($1-r$ will then be the fraction originating from systematic failures)
- SFF = Safe failure fraction = $(1 - \lambda_{DU} / \lambda_{crit}) \cdot 100 \%$
- β = The fraction of failures of a single component that causes both components of a redundant pair to fail “simultaneously”
- C_{MooN} = Modification factor for voting configurations other than 1oo2 in the beta-factor model (e.g. 1oo3, 2oo3 and 2oo4 voting logics)

2.2.2 Decomposition of Failure Rate

Some important relationships between different fractions of the critical failure rate are illustrated in Table 1 and Figure 1.

Table 1 Decomposition of critical failure rate, λ_{crit}

	Spurious trip failures	Dangerous failures	Sum
Undetected	λ_{SU}	λ_{DU}	λ_{undet}
Detected	λ_{SD}	λ_{DD}	λ_{det}
Sum	λ_S	λ_D	λ_{crit}

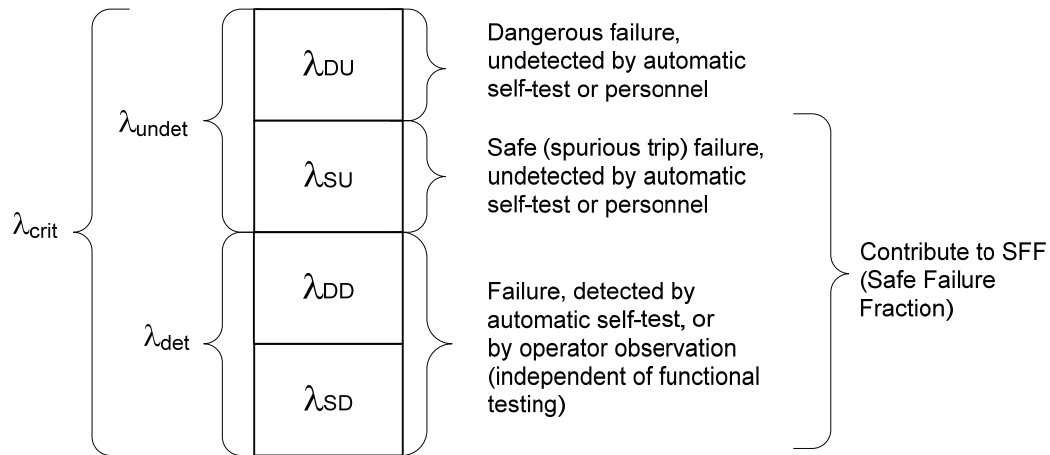


Figure 1 Decomposition of critical failure rate, λ_{crit}

2.3 Reliability Measures and Notation

Table 2 lists some performance measures for safety and reliability, and some other main parameters in the PDS method. A more complete description is found in the updated PDS Method Handbook, 2010 Edition, [10].

Table 2 Performance measures and reliability parameters

Term	Description
PFD	Probability of failure on demand. This is the measure for loss of safety caused by dangerous undetected failures, see section 4.3.
P_{TIF}	Probability of a test independent failure. This is the measure for loss of safety caused by a failure not detectable by functional testing, but occurring upon a true demand (see section 4.3).
CSU	Critical safety unavailability, $CSU = PFD + P_{TIF}$

Term	Description
MTTR	Mean time to restoration. Time from failure is detected/revealed until function is restored, ("restoration period"). Note that this restoration period may depend on a number of factors. It can be different for <i>detected</i> and <i>undetected</i> failures: The <i>undetected</i> failures are revealed and handled by functional testing and could have shorter <i>MTTR</i> than the <i>detected</i> failures. The <i>MTTR</i> could also depend on configuration, operational philosophy and failure multiplicity.
STR	Spurious trip rate. Rate of spurious trips of the safety system (or set of redundant components), taking into consideration the voting configuration.
τ	Interval of functional test (time between functional tests of a component)

2.4 Reliability Parameters

In this section some of the reliability parameters defined above is further discussed.

2.4.1 Rate of Dangerous Undetected Failures

As discussed in section 2.2.2, the critical failure rate, λ_{crit} are split into dangerous and safe failures, (i.e. $\lambda_{crit} = \lambda_D + \lambda_S$) which are further split into detected and undetected failures. When performing safety unavailability calculations, the rate of dangerous undetected failures, λ_{DU} , is of special importance, since this parameter - together with the test interval - to a large degree governs the prediction of how often a safety function is likely to fail on demand.

Equipment specific failure data reports prepared by manufacturers (or others) often provide λ_{DU} estimates being an order of magnitude (or even more) lower than those reported in generic data handbooks. There may be several causes for such exaggerated claims of performance, including imprecise definition of equipment- and analysis boundaries, incorrect failure classification or too optimistic predictions of the diagnostic coverage factor (see e.g. [20]).

When studying the background data for generic failure rates (λ_{DU}) presented in data sources such as OREDA and RNNP, it is found that these data will include *both* random hardware failures as well as systematic failures. Examples of the latter include incorrect parameter settings for a pressure transmitter, an erroneous output from the control logic due to a failure during software modification, or a PSV which fails due to excessive internal erosion or corrosion. These are all failures that are detectable during functional testing and therefore illustrate the fact that systematic failures may well be part of the λ_{DU} for generic data.

Since failure rates provided by manufacturers frequently tend to exclude all types of failures related to installation, commissioning or operation of the equipment (i.e. systematic type of failures), a mismatch between manufacturer data and generic data appears. Our question then becomes - since systematic failures inevitably will occur - why not include these failures in predictive reliability analyses?

In order to elucidate the fact that the failure rate will comprise random hardware failures as well as systematic failures, the parameter r has therefore been defined as the fraction of dangerous undetected failures originating from random hardware failures. Rough estimates of the r factor are given in the detailed data sheets in chapter 5. For a more thorough discussion and arguments concerning the r factor, reference is made to [10].

2.4.2 The Coverage Factor, c

Modules often have built-in *automatic self-test*, i.e. on-line diagnostic testing to detect failures prior to an actual demand². The fraction of failures being detected by the automatic self-test is called the *fault coverage* and quantifies the effect of the self-test. Note that the actual effect on system performance from a failure that is detected by the automatic self-test will depend on system configuration and operating philosophy. In particular it should be considered whether the detected failure is configured to only raise an alarm or alternatively bring the system to a safe state. It is often seen that failures classified as dangerous detected only raise an alarm and in such case it must be ensured that the failure initiates an immediate response in the form of a repair and/or introduction of risk reducing measures.

In addition to the diagnostic self-test, an operator or maintenance crew may detect dangerous failures incidentally in between tests. For instance, the panel operator may detect a transmitter that is “stuck” or a sensor that has been left in by-pass. Similarly, when a process segment is isolated for maintenance, the operator may detect that one of the valves will not close. The PDS method also aims at incorporating this effect, and defines the *total coverage factor*; c reflecting detection *both* by automatic self-test and by operator. Further, the coverage factor for dangerous failures is denoted c_D whereas the coverage factor for safe failures is denoted c_S .

Critical failures that are not detected by automatic self-testing or by observation are assumed either to be detectable by functional (proof) testing³ or they are so called test independent failures (TIF) that are not detected during a functional test but appear upon a true demand (see section 2.3 and chapter 4 for further description).

It should be noted that the term “*detected safe failure*” (of rate λ_S), is interpreted as a failure which is detected such that a spurious trip is *actually avoided*. Hence, a spurious closure of a valve which is detected by, e.g., flow metering downstream the valve, can not be categorised as a detected safe failure. On the other hand, drifting of a pressure transmitter which is detected by the operator, such that a shutdown is avoided, will typically be a detected safe failure.

2.4.3 Beta-factors and C_{MooN}

When quantifying the reliability of systems employing redundancy, e.g., duplicated or triplicated systems, it is essential to distinguish between *independent* and *dependent* failures. Random hardware failures due to natural stressors are assumed to be *independent* failures. However, all systematic failures, e.g. failures due to excessive stresses, design related failures and maintenance errors are by nature *dependent* (common cause) failures. Dependent failures can lead to simultaneous failure of more than one (redundant) component in the safety system, and thus reduce the advantage of redundancy.

Traditionally, the dependent or common cause failures have been accounted for by the β -factor approach. The problem with this approach has been that for any M -out-of- N (MooN) voting ($M < N$) the rate of dependent failures is the same, and thus the approach does not distinguish between e.g. a 1oo2 and a 2oo3 voting. The PDS method extends the β -factor model, and distinguishes between the voting logics by introducing β -factors which depend on the voting configuration; i.e. $\beta(MooN) = \beta \cdot C_{MooN}$. Here, C_{MooN} is a modification factor depending on the voting configuration, MooN.

² Also refer to IEC 61508-4, section 3.8.6 and 3.8.7

³ See also IEC 61508-4, section 3.8.5.

Standard (average) values for the β -factor are given in Table 7. Note that when performing reliability calculations, application specific β -factors should preferably be obtained, e.g. by using the checklists provided in IEC 61508-6, or by using the simplified method as described in Appendix D of the PDS method handbook, [10].

Values for C_{Moon} are given in Table 8. For a more complete description of the extended β -factor approach of PDS, see [10].

2.4.4 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 failure; i.e. $SFF = (\lambda_{DD} + \lambda_S) / (\lambda_D + \lambda_S)$. The objective of including this measure (and the associated hardware fault tolerance; HFT) was to prevent manufacturers from claiming excessive SILs based solely on PFD calculations. However, experience has shown that failure modes that actually do not influence the main functions of the SIS (ref. section 2.1) are frequently included in the safe failure rate so as to artificially increase the SFF, [20].

It is therefore important to point out that when estimating the SFF, only failures with a potential to actually cause a spurious trip of the component should be included among the safe failures. Non-critical failures, such as a minor external leakage of hydraulic oil from a valve actuator, should not be included.

The SFF figures presented in this handbook are based on reported failure mode distributions in OREDA as well as some additional expert judgements. Higher (or lower) SFFs than given in the tables may apply for specific equipment types and this should in such case be well documented, e.g. by FMEDA type of analyses.

2.5 Main Data Sources

The most important data source when preparing this handbook has been the OREDA database and handbooks. OREDA is a project organisation whose main purpose is to collect and exchange reliability data among the participating companies (i.e. BP, ENI, ExxonMobil, ConocoPhillips, Shell, Statoil, TOTAL and Gassco). A special thanks to the OREDA Joint Industry Project (JIP) for providing access to an agreed set of the OREDA JIP data. For more information about the OREDA project, any feedback to OREDA JIP concerning the data or name of contact persons, reference is made to <http://www.oreda.com>. Equipment for which reliability data are missing or additional data desirable should be reported to the OREDA project manager or one of the participating OREDA companies, as this will provide valuable input to future OREDA data collection plans.

Other important data sources have been;

- Recent data from the RNNP (Norwegian: “Risikonivået i Norsk Petroleumsindustri”) project on safety critical equipment;
- Failure data and failure mode distributions from safety system manufacturers;
- Experience data from operational reviews on Norwegian offshore and onshore installations;
- Other commercially published data handbooks such as Exida, [15] and the T-book, [16];
- Discussions and interviews with experts.

A complete list of data sources and references is given in chapter 6.

2.6 Using the Data in This Handbook

The data in this handbook provide best (average) estimates of equipment failure rates based on experience gathered mainly throughout the petroleum industry.

The recommended data is based on a number of assumptions concerning safe state, fail safe design, self-test ability, loop monitoring, NE/NDE design, etc. These assumptions are, for each piece of equipment, described in the detailed data sheets in chapter 5. Hence, when using the data for reliability calculations, it is important to consider the relevance of these assumptions for each specific application.

NOTE! APART FROM SOME EXAMPLE PAGES FROM CHAPTER 3 (RELIABILITY DATA SUMMARY), CHAPTER 5 (DATA DOSSIERS) AND CHAPTER 6 (REFERENCES), THE REMAINING PART OF THE HANDBOOK IS NOT INCLUDED IN THIS FREE ELECTRONIC VERSION.

THE FOLLOWING PAGES FROM CHAPTER 5 ARE INCLUDED BELOW:

- Page 43: "5 DATA DOSSIERS", introduction
- Page 62: "5.1.10 Smoke Detector"

3 RELIABILITY DATA SUMMARY

3.1 Topside Equipment

The tables 3 to 8 summarise the input data to be used in reliability analyses. The definitions of the column headings relate to the parameter definitions given in section 2.2 and 2.3. Some additional comments on the values for P_{TIF} , coverage and r , are given in section 3.3.

Observe that λ_D (third column of tables 3 to 5), together with $\lambda_{crit} = \lambda_D + \lambda_S$, will provide the λ_S . The rates of *undetected failures* λ_{DU} and λ_{SU} follow from the given coverage values, c_D and c_S . I.e. $\lambda_{DU} = \lambda_D \cdot (1 - c_D / 100\%)$ and $\lambda_{SU} = \lambda_S \cdot (1 - c_S / 100\%)$. The safe failure fraction, SFF, can be calculated by $SFF = ((\lambda_{crit} - \lambda_{DU}) / \lambda_{crit}) \cdot 100\%$.

Data dossiers with comprehensive information for each component are given in chapter 5 as referred to in tables 3 to 5.

Table 3 Failure rates, coverages and SFF for input devices

Input Devices								
Component	$\lambda_{crit}^{1)}$	$\lambda_D^{1)}$	c_D	c_S	$\lambda_{DU}^{1)}$	$\lambda_{SU}^{1)}$	SFF	Ref.
Pressure switch	3.4	2.3	15 %	10 %	2.0	1.0	41 %	Sect. 5.1.1
Proximity switch, inductive	5.7	3.5	15 %	10 %	3.0	2.0	47 %	Sect. 5.1.2
Pressure transmitter	1.3	0.8	60 %	30 %	0.3	0.4	77 %	Sect. 5.1.3
Level (displacement) transmitter	3.0	1.4	60 %	30 %	0.6	1.1	80 %	Sect. 5.1.4

Rest of table not shown in this free copy.

¹⁾ All failure rates given per 10^6 hours

5 DATA DOSSIERS

The following pages present the data dossiers of the control and safety system components. The dossiers are input to the tables in chapter 3 that summarise the generic input data to PDS analyses. Note that the generic data, by nature represent a wide variation of equipment populations and as such should be considered on individual grounds when using the data for a specific application.

The data dossiers are based on the data dossiers in previous editions of the handbook, [12], [13], [14], and have been updated according to the work done in the PDS-BIP and the new data available.

Adapting the definitions used in OREDA, several severity class types are referred to in the data dossiers. The definitions of the various types are, [3]:

- *Critical failure*: A failure which causes immediate and complete loss of a system's capability of providing its output.
- *Degraded failure*: A failure which is not critical, but it prevents the system from providing its output within specifications. Such a failure would usually, but not necessarily, be gradual or partial, and may develop into a critical failure in time.
- *Incipient failure*: A failure which does not immediately cause loss of the system's capability of providing its output, but if not attended to, could result in a critical or degraded failure in the near future.
- *Unknown*: Failure severity was not recorded or could not be deduced.

Note that only the *critical failures* are included as a basis for the failure rate estimates (i.e. the λ_{crit}). From the description of the failure mode, the critical failures are further split into dangerous and safe failures (i.e. $\lambda_{crit} = \lambda_D + \lambda_S$). E.g. for shutdown valves a “fail to close on demand” failure will be classified as dangerous whereas a “spurious operation” failure will be classified as a safe (spurious trip) failure.

The following failure modes are referred in the data dossier tables:

DOP	-	Delayed operation
EXL	-	External leakage
FTC	-	Fail to close on demand
FTO	-	Fail to open on demand
FTR	-	Fail to regulate
INL	-	Internal leakage
LCP	-	Leakage in closed position
LOO	-	Low output
NOO	-	No output
PLU	-	Plugged/choked
SHH	-	Spurious high level alarm
SLL	-	Spurious low level alarm
SPO	-	Spurious operation
STD	-	Structural deficiency
VLO	-	Very low output

5.1.10 Smoke Detector

Module: Input Devices Component: Smoke Detector		PDS Reliability Data Dossier
Description / equipment boundaries The detector includes the sensor and local electronics such as the address-/interface unit.	Date of Revision 2009-12-18	
	Remarks Fire central not included	
Recommended Values for Calculation		
<i>Total rate</i>	<i>Coverage</i>	<i>Undetected rate</i>
$\lambda_D = 1.2$ per 10^6 hrs	$c_D = 0.40$	$\lambda_{DU} = 0.7$ per 10^6 hrs
$\lambda_S = 2.0$ per 10^6 hrs	$c_S = 0.30$	$\lambda_{SU} = 1.4$ per 10^6 hrs
$\lambda_{crit} = 3.2$ per 10^6 hrs	$P_{TIF} = 1 \cdot 10^{-3}$	
	$r = 0.4$	
Assessment		
<p>The failure rate estimate is an update of the 2006 figure which was primarily based on OREDA phase III as well as some phase V data. The rate of DU failures is estimated still assuming coverage of 40 % (observed in OREDA incomplete and complete phase III were 29% and 50%, respectively). The rate of dangerous and safe failures has been slightly decreased based on observations from failure reviews and later OREDA phases. For safe failures 30 % coverage - mainly based on OREDA phase III observations as well as expert judgement - has been assumed. It should be noted that for some type of smoke detectors with more extensive self test, the coverage may be significantly higher. This must be assessed for each specific detector type.</p> <p>The P_{TIF} is based on expert judgements and is based on the assumption that the detectors are exposed. The estimated r value is based on observed failure causes for critical detector failures (40% “expected wear and tear” and 60% “maintenance errors”). A summary of some of the main arguments is provided in section 3.3.</p>		
Failure Rate Reference		
<i>Overall failure rate (per 10^6 hrs)</i>	<i>Failure mode distribution</i>	<i>Data source/comment</i>
$\lambda_{crit} = 3.7$	$\lambda_D = 1.3$ per 10^6 hrs $\lambda_{DU} = 0.8$ per 10^6 hrs $\lambda_{STU} = 1.4$ per 10^6 hrs $P_{TIF} = 10^{-3}$	Recommended values for calculation in 2006-edition, [12] Assumed $c_D = 40\%$
$\lambda_{crit} = 3.7$	$\lambda_D = 1.3$ per 10^6 hrs $\lambda_{DU} = 0.8$ per 10^6 hrs $\lambda_{STU} = 1.2$ per 10^6 hrs $P_{TIF} = 10^{-3} - 0.05$ ¹⁾	Recommended values for calculation in 2004- and 2003-edition, [13], [14] Assumed $c_D = 40\%$ ¹⁾ The range represents different types of fires (smoke/flame)

Module: Input Devices Component: Smoke Detector		PDS Reliability Data Dossier
0.0	D: 0.0 ST:0.0 <i>Observed:</i> $c_D = N/A$ $c_{ST} = N/A$	OREDA phase V database [6] Data relevant for smoke/combustion detectors . <i>Filter:</i> Inv. Equipment class = Fire & Gas Detectors AND Inv. Design Class = Smoke/Combustion AND Inv. Phase = 5 AND Fail. Severity Class = Critical No. of inventories = 103 No. of critical D failures = 0 No. of critical ST failures = 0 Surveillance Time (hours) = 3 238 320
3.7	D: 1.0 SPO: 2.7 <i>Observed:</i> $c_D = 29\%$ (Calculated including detectors having some kind of self-test arrangement only)	OREDA phase III database, [8]. Data relevant for smoke/combustion detectors. Both <i>conventional</i> (65 %) and <i>addressable</i> (35 %) detectors are included. 56 % have automatic loop test, 35 % have a combination of loop and built-in self-test, the residual (9 %) have no self-test feature. No. of inventories = 1 897 Total no. of failures = 218 Cal. time = 50 374 800 hrs <i>Note! Only failures classified as "critical" are included in the failure rate estimates.</i>
	$\lambda_{DU} = 0.3$ per 10^6 hrs	Data from <i>review of safety critical failures on Norwegian onshore plant</i> . Data applicable for optical smoke detectors No. of inventories = 807 detectors (460 early warning) No. of critical DU failures = 2 ¹⁾ Cal. time = 7 069 320 hrs ²⁾ ¹⁾ The failure review focused on DU failures, but classification of other failure modes was also performed. No DD or safe failures registered. ²⁾ One year of operation
	$\lambda_{DU} = 0.6$ per 10^6 hrs	Data from <i>review of safety critical failures on Norwegian semi-submersible platform</i> . Data applicable for optical smoke detectors No. of inventories = 788 detectors No. of critical DU failures = 8 ¹⁾ Cal. time = 13 805 760 hrs ²⁾ ¹⁾ The failure review focused on DU failures. In addition 10 DD and 14 safe failures were also registered ²⁾ Two years of operation
	$\lambda_{DU} = 1.65$ per 10^6 hrs $\lambda_{SU} = 3.85$ per 10^6 hrs SFF = 70 %	Exida [15]: Generic smoke (ionization) detector

6 REFERENCES

- [1] IEC 61508 Standard. “Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety related systems”, part 1-7, Edition 1.0 (various dates).
- [2] IEC 61511 Standard. “Functional safety - safety instrumented systems for the process industry sector”, part 1-3. 2003
- [3] OREDA participants, OREDA; Offshore Reliability Data Handbook, Volume 1 - topside data and Volume 2 – subsea data. 5th edition, 2009.
- [4] OREDA participants, OREDA phases VI and VII, Computerised database on topside equipment, (data collected during the period 2000-2003).
- [5] OREDA participants, OREDA Handbook; Offshore Reliability Data Handbook, 4th edition, 2002.
- [6] OREDA participants, OREDA phases IV and V, Computerised database on topside equipment, (data collected during the period 1993-2000).
- [7] OREDA Participants, OREDA Handbook; Offshore Reliability Data Handbook, 3rd edition, 1997.
- [8] OREDA participants, OREDA phase III, Computerised database on topside equipment, (data collected during the period 1990-1992).
- [9] Norwegian Petroleum Safety Authorities, Risikonivået i Norsk Petroleumsindustri (RNNP). Reported safety barrier data from 2003 - 2008.
- [10] Hauge, S., Lundteigen, M.A., Hokstad, P., and Håbrekke, S., Reliability Prediction Method for Safety Instrumented Systems – PDS Method Handbook, 2010 Edition. SINTEF report A13503
- [11] Hauge, S., Hokstad, P., Langseth, H. and Øien K., Reliability Prediction Method for Safety Instrumented Systems – PDS Method Handbook, 2006 Edition. SINTEF report STF50 A06031
- [12] Hauge, S., Langseth, H. and Onshus T., Reliability Data for Safety Instrumented Systems – PDS Data Handbook, 2006 Edition. SINTEF report STF50 A06030
- [13] Hauge, S. and Hokstad, P., Reliability Data for Safety Instrumented Systems, PDS Data Handbook, 2004 Edition. SINTEF report STF38 A04423
- [14] Albrechtsen, E. and Hokstad, P., Reliability Data for Safety Instrumented Systems, PDS Data Handbook, 2003 Edition. SINTEF report STF38 A02421.
- [15] EXIDA, Safety Equipment Reliability Handbook, 3rd edition, Volume 1 – 3, exida.com, 2007
- [16] T-Book, Version 5, Reliability Data of Components in Nordic Nuclear Power Plants. TUD-office and Pörn Consulting, 2000.
- [17] Lunde, M., Ytelsesvurdering av sikkerhetsventiler (evaluation of pressure safety valve performance), NTNU, november 2004

- [18] Grammeltvedt, J.A., Oseberg C – Gjennomgang av erfaringsdata for brann- og gassdetektorer på Oseberg C. Forslag til testintervaller for detektorene. Report from Norsk Hydro, Forskningscenteret Porsgrunn (in Norwegian), 1994.
- [19] OLF Guideline 070: “Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry”. The Norwegian Oil Industry Association, rev. 02, 2004.
- [20] Angela Summers (2008). IEC Product Approval – Veering Off Course. Article posted 11.06.08 in www.controlglobal.com
- [21] Centre for Chemical Process Safety (CCPS): Guidelines for safe and reliable instrumented protective systems, Wiley, 2007
- [22] Béla G. Lipták (Editor): Instrument Engineers Handbook – Process Control and Optimisation, fourth edition, Taylor & Francis, 2006
- [23] Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase. SINTEF report A8788, Rev. 01, 01.12.2008 (Web: http://www.sintef.no/project/PDS/Reports/PDS%20Report-SIS_follow_up_guideline_final_v01.pdf)
- [24] Hauge, S., Lundteigen M.A and Rausand M., Updating failure rates and test intervals in the operational phase: A practical implementation of IEC 61508 and IEC 61511, ESREL September 2009, Prague, Czech Republic