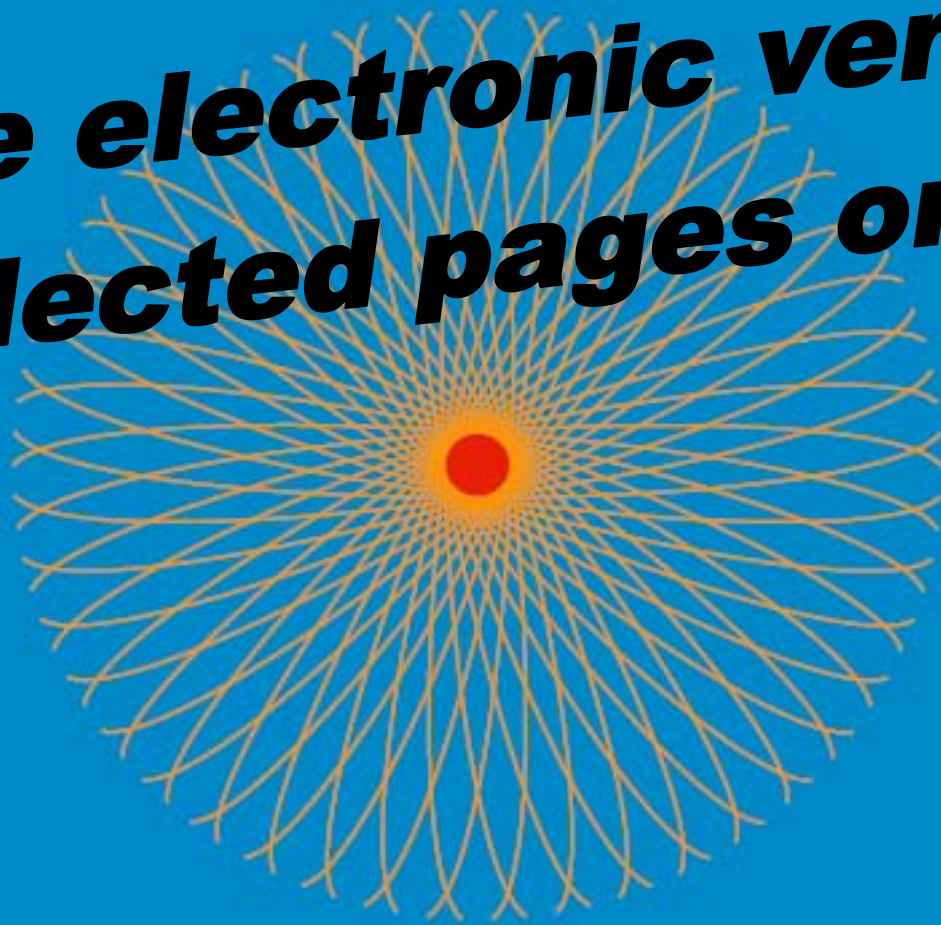


Reliability Data for Safety Instrumented Systems

PDS Data Handbook, 2006 Edition

***Free electronic version
Selected pages only***



SINTEF
April 2006

Selected pages from:

Reliability Data for Safety Instrumented Systems

PDS Data Handbook, 2006 Edition



SINTEF REPORT

SINTEF Technology and Society
Safety and Reliability

Address: NO-7465 Trondheim,
NORWAY
Location: S P Andersens veg 5
NO-7031 Trondheim
Telephone: +47 73 59 27 56
Fax: +47 73 59 28 96

Enterprise No.: NO 948 007 029 MVA

TITLE

Reliability Data for Safety Instrumented Systems

PDS Data Handbook, 2006 Edition

AUTHOR(S)

Stein Hauge, Helge Langseth and Tor Onshus

CLIENT(S)

Multiclient - PDS Forum

REPORT NO. STF50 A06030	CLASSIFICATION Unrestricted	CLIENTS REF.	
CLASS. THIS PAGE Unrestricted	ISBN 82-14-03898-7	PROJECT NO. 384630.40	NO. OF PAGES/APPENDICES 86 / 2
ELECTRONIC FILE CODE		PROJECT MANAGER (NAME, SIGN.) Stein Hauge	CHECKED BY (NAME, SIGN.) Knut Øien
FILE CODE	DATE 2006-04-03	APPROVED BY (NAME, POSITION, SIGN.) Lars Bodsberg, Research Director	

ABSTRACT

This report provides Reliability Data estimates for components of control and safety systems. Data dossiers for field devices (sensors, valves) and control logic (electronics) are presented, including data for subsea equipment. The dossiers are based on various sources, e.g., OREDA[®], and expert judgements. The level of detail of the data is adapted to the format required for reliability analyses and quantification of safety integrity levels (SIL) of safety instrumented systems.

As a result of development work done in the PDS project during the last two years, the PDS method and related taxonomy have been updated. This report provides input data in line with the updated PDS method. The following main updates have been included in the present handbook:

- General update of models and taxonomy described in this data handbook;
- New values for the updated common beta (β) factor have been given (to replace the former β and β_{SF});
- New and updated values for test independent systematic failures (P_{TIF}) are given, especially relevant for fire and gas detectors;
- For dangerous undetected failures, estimates for the fraction of random hardware- and systematic failures have been given;
- A general update of some of the failure rates and coverage values;

KEYWORDS	ENGLISH	NORWEGIAN
GROUP 1	Safety	Sikkerhet
GROUP 2	Data	Data
SELECTED BY AUTHOR	Safety Instrumented Systems (SIS)	Instrumenterte sikkerhetssystemer
	Safety Integrity Level (SIL)	SIL
	IEC 61508	IEC 61508

PREFACE, 2006 EDITION

The present report is an update of the 2004 Edition of the Reliability Data for Control and Safety Systems, [16]. The update has been carried out as part of the research project “User friendly analysis tool for instrumented safety systems”.¹ The main objective of this new and updated PDS data handbook has been to present input data in line with the revised models and taxonomy.

As part of this research project, the PDS method has been further developed updating the taxonomy and some of the models. The details on this work are presented in the new PDS method handbook, ref. [20].

Trondheim, April 2006

Stein Hauge

PDS Forum Participants in 2006

Oil Companies/Operators

- A/S Norske Shell
- BP Norge AS
- Eni Norge AS
- Norsk Hydro ASA
- PGS Production AS
- ConocoPhillips Norge
- Statoil ASA
- TOTAL E&P NORGE AS

Control and Safety System Vendors

- ABB AS
- FMC Kongsberg Subsea AS
- Honeywell AS
- Invensys Systems Norge AS
- Kongsberg Maritime AS
- Saas System as
- Siemens AS
- Simrad Optronics ASA

Engineering Companies and Consultants

- Aker Kværner Engineering & Technology
- Det Norske Veritas AS
- Nemko AS
- Safetec Nordic AS
- Scandpower Risk Management AS

Governmental bodies

- Petroleum Safety Authority Norway (observer)
- Directorate for Civil Protection and Emergency Planning (observer)

¹ This user initiated research project has been sponsored by the Norwegian Research Council and the PDS participants. The work has mainly been carried out by SINTEF. Some results from the project may not express the view of all the PDS participants.

Table of Contents

PREFACE, 2006 EDITION	3
1 INTRODUCTION	7
1.1 Objective and Content	7
1.2 Benefits of Reliability Analysis – the PDS Method	7
1.3 The IEC 61508 Standard	8
1.4 Abbreviations Used in the Report	8
2 RELIABILITY DATA SUMMARY	9
2.1 Parameter Definitions	9
2.1.1 Failure Rate Notation	9
2.1.2 Decomposition of Failure Rate	10
2.1.3 Coverage, c	11
2.1.4 Beta-factors and C_{Moon}	12
2.1.5 Reliability Measures and further Notation	12
2.2 PDS Input Data – Topside Equipment	14
2.3 PDS Input Data for Subsea Equipment	20
2.4 Comments on the PDS Input Data	21
2.4.1 Probability of Test Independent Failures (P_{TIF})	21
2.4.2 Coverage Values	22
2.4.3 Values for r ($\lambda_{\text{DU-RH}} / \lambda_{\text{DU}}$)	23
3 MAIN FEATURES OF THE PDS METHOD	27
3.1 Main Characteristics of PDS	27
3.2 Failure Classification and Failure Modes	27
3.3 Reliability Performance Measures	29
3.3.1 Contributions to Loss of Safety	29
3.3.2 Loss of Safety due to DU Failures - Probability of Failure on Demand (PFD)	30
3.3.3 Loss of Safety due to Systematic Test Independent Failures (P_{TIF})	30
3.3.4 Loss of Safety due to Downtime Unavailability – DTU	31
3.3.5 Overall Measure for Loss of Safety– Critical Safety Unavailability	31
3.4 Worked Quantification Example	32
3.4.1 Example Case: HIPPS System	32
3.4.2 Reliability Input Data	33
3.4.3 Loss of Safety Assessment - CSU	33
4 DATA DOSSIERS	35
4.1 Input Devices	36
4.1.1 Pressure Switch, Conventional	36
4.1.2 Pressure Transmitter, Conventional	38

NOTE! APART FROM SOME EXAMPLE PAGES FROM CHAPTER 4 (DATA DOSSIERS), THE REMAINING PART OF THE HANDBOOK IS NOT INCLUDED IN THIS FREE ELECTRONIC VERSION

4.1.3	Level (Displacement) Transmitter, Conventional.....	40
4.1.4	Temperature Transmitter, Conventional	42
4.1.5	Flow Transmitter, Conventional	44
4.1.6	Catalytic Gas Detector, Conventional	46
4.1.7	IR Point Gas Detector, Conventional.....	48
4.1.8	IR Line Gas Detector, Conventional.....	50
4.1.9	Smoke Detector, Conventional	52
4.1.10	Heat Detector, Conventional	54
4.1.11	Flame detector, Conventional	56
4.1.12	ESD Push Button.....	58
4.2	Control Logic Units.....	59
4.2.1	Safety system – single system.....	59
4.3	Final Elements.....	62
4.3.1	ESV/XV	62
4.3.2	ESV, X-mas Tree	66
4.3.3	Pilot/Solenoid Valve	68
4.3.4	Process Control Valve.....	70
4.3.5	Pressure Relief Valve.....	73
4.3.6	Blowdown Valve incl. Actuator (ex. Pilot).....	75
4.3.7	Down Hole Safety Valve – DHSV.....	76
4.3.8	Circuit Breaker	77
4.3.9	Relay	78
4.4	Subsea Equipment.....	79
5	REFERENCES	82
	APPENDIX A: IEC vs. PDS Notation.....	84
	APPENDIX B: TYPICAL CONTRIBUTIONS TO CSU	85

List of Tables

Table 1	Decomposition of the critical failure rate, λ_{crit}	10
Table 2	Performance measures and reliability parameters.....	13
Table 3	Failure rates, coverages and SFF for input devices.....	14
Table 4	Failure rates, coverages and SFF for control logic units.....	16
Table 5	Failure rates, coverages and SFF for final elements	16
Table 6	P_{TIF} estimates for various components	17
Table 7	Average proportion of dangerous undetected random hardware failures (r factor)	18
Table 8	β -factors for various components.....	19
Table 9	Numerical values for configuration factors, C_{Moon}	19
Table 10	Failure rates for subsea equipment - input devices, control system units and output devices	20
Table 11	Reliability data for HIPPS components.....	33
Table 12	Summary of PFD, P_{TIF} , and CSU for the worked example	34
Table 13	Discussion of proposed subsea data	79

List of Figures

Figure 1	Decomposition of the critical failure rate, λ_{crit}	10
Figure 2	Failure classification by cause of failure.....	28
Figure 3	Contributions to critical safety unavailability (CSU).	32
Figure 4	HIPPS protecting a vessel.....	32
Figure 5	Simplified RBD for loss of safety.....	33
Figure 6	Component CSUs with λ_{DU-RH} , λ_{DU-S} and P_{TIF} contributions	85

1 INTRODUCTION

1.1 Objective and Content

SINTEF has developed a reliability quantification method for analysing the safety and reliability of control and safety systems on process installations such as offshore installations and onshore processing plants (ref. [20]). This report presents a set of recommended generic input data to these analyses, and is an update of the data found in the '04 edition of the PDS Reliability data handbook, [16].

The objective of the present data handbook has been to update the required input data according to the revised models and taxonomy presented in the latest PDS method handbook, ref. [20]. The following main changes are included in this version of the data handbook (as compared to the 2004 edition, [16]):

- New values for the updated (common) beta (β) factor has been given based on a weighted average of the former β and β_{SF} ;
- New and updated values for test independent systematic failures (P_{TIF}) are given, especially relevant for fire and gas detectors
- For dangerous undetected failures, estimates for the fraction of random hardware- and systematic failures have been given
- A general update of some of the failure rates and coverage values based on input data from sources such as:
 - The OREDA[®] phase IV (1993-1996) and phase V (1997-2000) databases;²
 - Discussions and interviews with experts;
 - Recent data from the RNNS (Norwegian: “Risikonivået på Norsk Sokkel”) project on safety critical equipment;

The recommended reliability data estimates are summarised in Chapter 2. In the same Chapter, the precise definitions of the applied notations are given. Chapter 3 gives a brief description 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 4 the 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.

A more comprehensive description of the PDS method is given in the SINTEF report [20].

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.

² OREDA[®] is a project organisation whose main purpose is to collect and exchange reliability data among the participating companies (i.e. BP, Eni, ExxonMobil, Hydro, ConocoPhillips, Shell, Statoil, Total and Gassco). Thanks to the OREDA project for providing access to OREDA data. For more information about OREDA, feedback concerning data and contact person, see <http://www.oreda.com>.

Reliability analysis represents a systematic tool for understanding 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 is more thoroughly discussed in Chapter 3.

1.3 The IEC 61508 Standard

The IEC 61508 standard, [6], presents requirements to safety instrumented systems (SIS) for all the relevant lifecycle phases, and has been given extensive attention within the SIS industry. IEC 61508 is a generic standard common to several industries. The process industry has also developed their own sector specific standard for application of SIS, IEC 61511, [10]. 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, [7].

The PDS method is in line with the main principles advocated in IEC 61508, and is a useful tool when implementing and verifying quantitative (SIL) requirements as described in the IEC standards. Appendix A presents a comparison of the PDS notations and the IEC 61508 notation.

1.4 Abbreviations Used in the Report

BIP	-	User Initiated Project (Norwegian: Brukerinitiert prosjekt)
CCF	-	Common Cause Failure
CSU	-	Critical Safety Unavailability
DTU	-	Downtime Unavailability
IEC	-	International Electrotechnical Commission
MTTR	-	Mean Time to Restoration
NDE	-	Normally De-Energised
NE	-	Normally Energised
OLF	-	The Norwegian Oil Industry Association
OREDA [®]	-	Offshore Reliability Data
PDS-BIP	-	Acronym for the user initiated PDS project “User friendly analysis tool for instrumented safety systems”
PFD	-	Probability of Failure on Demand
RNNS	-	<i>Norwegian</i> : Risikonivået på Norsk Sokkel
SIL	-	Safety Integrity Level
SIS	-	Safety Instrumented System
SFF	-	Safe Failure Fraction
STR	-	Spurious Trip Rate
TIF	-	Test Independent Failure

2 RELIABILITY DATA SUMMARY

First in Section 2.1 we define the main parameters and introduce the notation. A summary of the "generic" input data to PDS analyses is presented in Section 2.2.

2.1 Parameter Definitions

The failure rate (numbers of failures per time unit) for a component is essential for the reliability calculations. First in Section 2.1.1, definitions and notation related to the failure rate are given, together with the decomposition of this failure rate into its various elements. Next, some aspects of the notation (coverage, beta-factor) are elaborated, and finally the main measures for safety and reliability are presented.

2.1.1 Failure Rate Notation

- λ_{crit} = Rate of critical failures; i.e., failures that will cause loss of one of the two main functions of the component/system:
- 1) shut down when the production is unsafe, i.e., dangerous (D) failure;
 - 2) maintain production when it is safe; i.e., spurious trip (ST) failure.
- $\lambda_{crit} = \lambda_D + \lambda_{ST}$ (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 and personnel, (control room operator or maintenance personnel). $\lambda_{DU} = \lambda_{DU-RH} + \lambda_{DU-S}$ (see below). λ_{DU} contributes to the Probability of Failure on Demand (PFD) of the component/system ("*loss of safety*")
- λ_{DD} = Rate of dangerous detected failures, i.e. failures detected by automatic self-test or personnel
- λ_{DU-RH} Rate of dangerous undetected random hardware failures, i.e. the part of λ_{DU} originating from random hardware failures (i.e. equals the λ_{DU} as defined in IEC 61508)
- λ_{DU-S} Rate of dangerous undetected systematic failures, i.e. the part of λ_{DU} originating from systematic failures
- r The fraction of λ_{DU} originating from random hardware failures, $r = \lambda_{DU-RH} / \lambda_{DU}$. $1-r$ will be the fraction of λ_{DU} originating from systematic failures, i.e. $1-r = \lambda_{DU-S} / \lambda_{DU}$
- λ_{ST} = Rate of spurious trip failures, including both undetected as well as detected failures. $\lambda_{ST} = \lambda_{STU} + \lambda_{STD}$ (see below)
- λ_{STU} = Rate of spurious trip undetected failures, i.e. undetected both by automatic self-test and personnel
- λ_{STD} = Rate of 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). $\lambda_{undet} = \lambda_{DU} + \lambda_{STU}$
- λ_{det} = Rate of (critical) failures that are detected by automatic self-test or personnel (independent of functional testing). $\lambda_{det} = \lambda_{DD} + \lambda_{STD}$
- c = Coverage: percentage of critical failures detected *either* by the automatic self-test *or* (incidentally) by operational personnel
- c_D = Coverage of dangerous failures. $c_D = (\lambda_{DD} / \lambda_D) \times 100 \%$
- c_{ST} = Coverage of spurious trip failures. $c_{ST} = (\lambda_{STD} / \lambda_{ST}) \times 100 \%$
- SFF = Safe failure fraction = $(1 - \lambda_{DU} / \lambda_{crit}) \times 100 \%$
- β = The fraction of failures of a single component that causes both components of a redundant pair to fail “simultaneously”. The β is application specific, and should therefore, preferably, reflect application specific conditions
- C_{MooN} = Modification factor for voting configuration different from 1oo2 in the beta-factor model. Applies, e.g., for 1oo3, 2oo3 and 2oo4 voting logics.

2.1.2 Decomposition of Failure Rate

Important relationships between different fractions of the critical failure rates are illustrated in Table 1 and in Figure 1.

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

	Spurious trip failures	Dangerous failures	Sum
Undetected	λ_{STU}	λ_{DU}	λ_{undet}
Detected	λ_{STD}	λ_{DD}	λ_{det}
Sum	λ_{ST}	λ_D	λ_{crit}

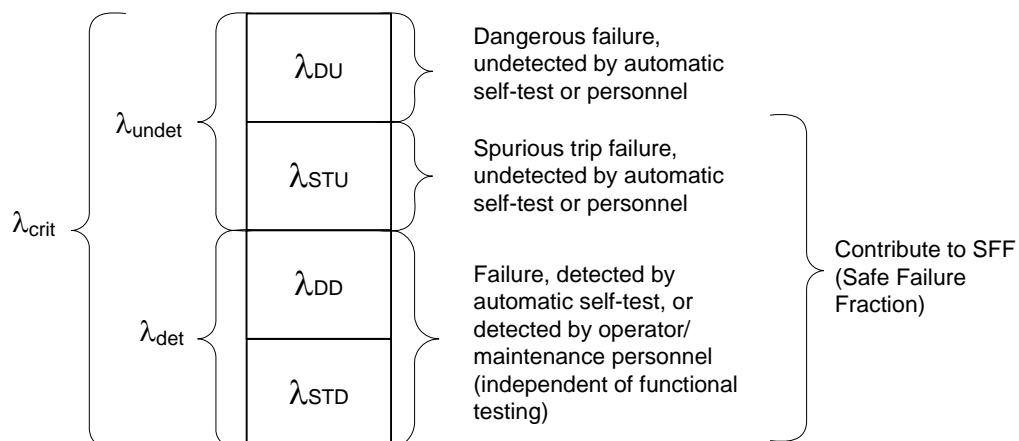


Figure 1 Decomposition of the critical failure rate, λ_{crit}

When performing safety unavailability calculations, the rate of dangerous undetected failures, λ_{DU} , is essential, since this parameter (together with the test interval) predicts how often a safety function is likely to fail on demand. According to IEC 61508 the λ_{DU} rate will include random hardware failures only. However, when considering generic failure rates (λ_{DU}) presented in many data handbooks such as [16], [18] and [21]; these data will include *both* random hardware failures as well as systematic failures. Examples include incorrect parameter settings for a pressure transmitter, an ESV which does not close since the control logic has not been updated after a 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.

Equipment specific failure data reports prepared by manufacturers (or others) often provide failure rates which may be an order of magnitude (or more) lower than those reported in generic data handbooks. One explanation of this can be fact that such failure data often result from FMECA³/FMEDA type of analyses, and often exclude all type of failures that in some sense can be related to errors in design or operation of the equipment (i.e. systematic failures).

It is therefore relevant to think of λ_{DU} as comprising two elements; λ_{DU-RH} which is the rate of dangerous undetected random hardware failures detectable by functional testing (i.e. the strict IEC definition of λ_{DU}), and λ_{DU-S} , being the rate of dangerous undetected systematic failures, also detectable by functional testing. Hence, $\lambda_{DU} = \lambda_{DU-RH} + \lambda_{DU-S}$. Furthermore, the parameter r is defined as the fraction of dangerous undetected failures originating from random hardware failures. Hence; $r = \lambda_{DU-RH}/\lambda_{DU}$ (and $1 - r = \lambda_{DU-S}/\lambda_{DU}$).

It should be pointed out that splitting of the λ_{DU} will *not* be necessary in order to perform the standard reliability calculations. One should, however, bear in mind that when we want to predict the actual performance of the equipment in the field, inclusion of the systematic failure part of λ_{DU} (i.e. the λ_{DU-S}) is essential. For a more thorough discussion and arguments for making this split, reference is made to the new updated method handbook, [20].

2.1.3 Coverage, c

Modules often have built-in *automatic self-test*, i.e. on-line diagnostic testing to detect failures prior to an actual demand⁴. The fraction of failures being detected by the automatic self-test is called the *fault coverage* and quantifies the effect of the self-test⁵. 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; (i.e. the effect depends on the voting logic and whether degraded operation takes place when a failure is detected).

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

³ E.g. refer to IEC 60812; “Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)”, ed. 2.0, January 2006

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

⁵ In previous editions of the PDS handbook, the fault coverage factor, taking into consideration diagnostic self-test only, was denoted DC , whereas the total coverage including also random detection by personnel was denoted c . In this new edition of the handbook only the coverage c is defined. For field equipment this factor will include both detection methods, whereas for control logic units, self-test will be the dominant contributor towards the coverage.

also aims at incorporating this effect, and defines the *total coverage factor*; c reflecting detection *both* by automatic self-test and by operator.

Critical failures that are not detected by automatic self-testing or (incidentally) by personnel are assumed to be detectable by functional (proof) testing⁶ 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 2.1.5 and Chapter 3 for further description).

It should be noted that the term “*detected spurious trip failure*” (of rate λ_{STD}), is interpreted as a failure which is detected such that the 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 spurious trip 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 spurious trip failure.

2.1.4 Beta-factors and C_{MooN}

When quantifying the reliability of systems employing redundancy, e.g., duplicated or triplicate 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, i.e. failures due to excessive stresses, design related failures and human interaction/operational failures, 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 do 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, $MooN$.

Standard (average) values for the β -factor are given in Table 8. These values deviate somewhat from previous β values, as the former β and β_{SF} have been combined into one common beta value. 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 C of the PDS method handbook, [20].

Values for C_{MooN} are given in Table 9. For a more complete description of the extended β -factor approach of PDS, see [20].

2.1.5 Reliability Measures and further 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 PDS Method Handbook, 2006 Edition, [20].

⁶ See also IEC 61508-4, section 3.8.5.

Observe that the probability of test independent systematic failures (P_{TIF}) has been reintroduced in PDS. Section 3.3 goes into more detail about safety/reliability measures, including the P_{TIF} .

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 3.3.
P_{TIF}	Probability of a test independent failure. This is the measure for loss of safety caused by a systematic failure not detectable by functional testing, but occurring upon a true demand (see Section 3.3).
CSU	Critical safety unavailability, $CSU = PFD + P_{TIF}$
DTU	Downtime unavailability. This is the “known” downtime unavailability caused by by-pass during repair or functional testing. The downtime unavailability comprises two elements: <ul style="list-style-type: none"> • The unavailability related to repair of dangerous detected failures (with rate λ_{DD}). The average duration of this period is the mean time to restoration (MTTR); This downtime unavailability is also denoted DTU_R • The unavailability resulting from planned activities such as testing, maintenance and inspection (of average time t). This downtime unavailability is also denoted DTU_T
CSU_{TOT}	The total critical safety unavailability including the “known” downtime unavailability: $CSU_{TOT} = PFD + P_{TIF} + DTU$
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)
t	Length of by-pass period during functional testing

2.2 PDS Input Data – Topside Equipment

The Tables 3 to 9 summarise the reliability input data to PDS analyses. The definitions of the column headings relate to the parameter definitions given in Section 2.1. Some additional comments on the values for P_{TIF} , coverage and r , are given in Section 2.4.

The input data are mainly based on the 2004 Edition of “Reliability Data for Control and Safety Systems” [16] and the update work performed as part of the PDS-BIP. The β -factors in Table 8 have been updated based on the fact that the former β and β_{SF} have been combined into one common factor.

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

Data dossiers with comprehensive information for each component are given in Chapter 4 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_{ST}	$\lambda_{DU}^{1)}$	$\lambda_{STU}^{1)}$	SFF	Ref.
Pressure Switch, Conventional	3.4	2.3	30 %	10 %	1.6	1.0	52 %	Sect. 4.1.1
Pressure Transmitter	1.3	0.8	60 %	50 %	0.3	0.3	76 %	Sect. 4.1.2
Level (displace) Transmitter	3.0	1.4	60 %	50 %	0.6	0.8	81 %	Sect. 4.1.3
Temperature Transmitter	1.8	0.7	60 %	50 %	0.3	0.6	84 %	Sect. 4.1.4
Flow Transmitter	3.7	1.5	60 %	50 %	0.6	1.1	84 %	Sect. 4.1.5
Gas detector, catalytic	5.0	3.5	50 %	40 %	1.8	0.9	65 %	Sect. 4.1.6
Gas detector IR point	4.0	3.3	80 %	70 %	0.7	0.2	84 %	Sect. 4.1.7
Gas detector IR line	5.3	3.3	80 %	70 %	0.7	0.6	88 %	Sect. 4.1.8
Smoke detector	3.7	1.3	40 %	40 %	0.8	1.4	81 %	Sect. 4.1.9
Heat detector	2.5	1.0	40 %	40 %	0.6	0.9	76 %	Sect. 4.1.10
Flame detector	6.8	3.0	70 %	60 %	0.9	1.5	86 %	Sect. 4.1.11
ESD Push button	0.9	0.5	20 %	10 %	0.4	0.4	56 %	Sect. 4.1.12

1) All failure rates are given per 10^6 hours

NOTE! APART FROM SOME EXAMPLE PAGES FROM CHAPTER 4 (DATA DOSSIERS), THE REMAINING PART OF THE HANDBOOK IS NOT INCLUDED IN THIS FREE ELECTRONIC VERSION.

THE FOLLOWING PAGES FROM CHAPTER 4 ARE INCLUDED BELOW:

- Page 33: “4 DATA DOSSIERS”, introduction
- Page 60-61: “4.3 Final Elements – 4.3.1 ESV/XV”

4 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 2 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, [5], [15] and [16], and are updated according to the work done in the PDS-BIP.

Adapting the definitions used in OREDA[®], several severity class types are referred to in the data dossiers. The definitions of the various types are, [18]:

- *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 which 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 which, 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 spurious trip failures (i.e. $\lambda_{crit} = \lambda_D + \lambda_{ST}$). 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

4.3 Final Elements

4.3.1 ESV/XV

Module: Final Elements Component: ESV/XV		PDS Reliability Data Dossier	
Description Main valve including actuator. Valve de-energised to close. <i>Not</i> including pilot valve	Date of Revision 2006-01-27		
	Remarks ESV/XV incl. actuator (ex. pilot)		
Recommended Values for Calculation			
<i>Total rate</i>	<i>Coverage</i>	<i>Undetected rate</i>	
$\lambda_D = 2.7 \text{ per } 10^6 \text{ hrs}$	$c_D = 0.25$	$\lambda_{DU} = 2.0 \text{ per } 10^6 \text{ hrs}$	
$\lambda_{ST} = 2.7 \text{ per } 10^6 \text{ hrs}$	$c_{ST} = 0$	$\lambda_{STU} = 2.7 \text{ per } 10^6 \text{ hrs}$	
$\lambda_{crit} = 5.4 \text{ per } 10^6 \text{ hrs}$	$P_{TIF} = 1 \cdot 10^{-5}$ (extended functional testing) $= 1 \cdot 10^{-4}$ (standard functional testing) $= 1 \cdot 10^{-3}$ (incomplete test/partial stroke)		
	$r = 0.5$		
Assessment			
<p>The failure estimate is an update of the previous estimate in the 2003 handbook [15]. Data from OREDA 2002 [18] and input from operators indicate that the previous failure rate estimate for valves was too optimistic. Furthermore, part (i.e. approx. 50%) of the failure rate reported under the sub-unit "control and monitoring" has now been included as part of the valve itself (as opposed to previously when this was all included under the pilot valve – the failure rate for pilot valve has been reduced correspondingly). This has resulted in a higher proportion of safe failures as compared to the previous estimate. It is assumed that the shutdown valves are de-energised to close.</p> <p>Data from RNNS for the period 2003-2004 for riser ESVs has been reviewed. Assuming annual testing, a $\lambda_{DU} = 3.5 \cdot 10^{-6}$ results (incl. pilot valve). This is somewhat higher than the data given in this handbook ($\lambda_{DU} = 2.9 \cdot 10^{-6}$ for complete ESV including pilot valve).</p> <p>The coverage factor for D failures have been set to 25%, due to registered detection methods in OREDA IV (i.e. failures detected by other means than "on demand" and during testing contribute towards the coverage factor).</p> <p>The P_{TIF} values are estimated based on expert judgements. The size of the P_{TIF} will vary depending on the completeness of the functional testing. Here, three (rough) alternatives are indicated, where for the smallest P_{TIF} (<i>extended functional test</i>) it is assumed that the test also includes a complete tightness test.</p> <p>The estimated r is based on reported failure causes in OREDA as well as expert judgements. A summary of some of the main arguments is provided in Section 2.4.</p>			

Module: Final Elements Component: ESV/XV		PDS Reliability Data Dossier
Failure Rate References		
<i>Overall failure rate (per 10⁶ hrs)</i>	<i>Failure mode distribution</i>	<i>Data source/comment</i>
$\lambda_{crit} = 5.4$	$\lambda_D = 2.7$ per 10 ⁶ hrs $\lambda_{DU} = 2.0$ per 10 ⁶ hrs $\lambda_{STU} = 2.7$ per 10 ⁶ hrs $P_{TIF} = 10^{-6} - 10^{-5}$ ¹⁾	Recommended values for calculation in 2004-edition [16] Assumed $c_D = 25\%$ ¹⁾ For complete and incomplete functional testing respectively.
$\lambda_{crit} = 1.6$ $\lambda_D / \lambda_{ST} = 4.3$	$\lambda_{DU} = 1.3$ per 10 ⁶ hrs $\lambda_{STU} = 0.3$ per 10 ⁶ hrs $P_{TIF} = 10^{-6} - 10^{-5}$ ¹⁾	Previously recommended values for calculation in 2003-edition [15] ¹⁾ For complete and incomplete functional testing respectively.
14.4	D: 14.4 ST: 0.0 <i>Observed:</i> $c_D = N/A$ ¹⁾ $c_{ST} = N/A$ ¹⁾ <i>Detection method unknown</i>	OREDA phase V database [9] Data relevant for process ESD/PSD valves, excluding the pilot and control & monitoring. <i>Filter:</i> Inv. Equipment class = VALVES AND (Inv. System = Gas export OR Inv. System = Gas processing OR Inv. System = Oil export OR Inv. System = Oil processing OR Inv. System = Emergency shutdown) AND Inv. OREDA Phase = 5 AND Inv. Att. Application = ESD/PSD AND (Fail. Item Failed <> Pilot valve AND Fail. Subunit Failed <> Control & Monitoring) AND Fail. Severity Class = Critical No. of inventories = 8 No. of critical D failures = 2 No. of critical ST failures = 0 Surveillance Time (hours) = 140 160

**NOTE! THE REMAINING PART OF THE HANDBOOK IS NOT INCLUDED IN THIS
FREE ELECTRONIC VERSION**