

Reliability Prediction Method for Safety Instrumented Systems

PDS Method Handbook, 2006 Edition

***Free electronic version
Chapters 1 to 4 only***

SINTEF
April 2006

Chapters 1 to 4 from:

Reliability Prediction Method for Safety Instrumented Systems

PDS Method Handbook, 2006 Edition



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

SINTEF REPORT

TITLE

**Reliability Prediction Method for Safety Instrumented Systems
PDS Method Handbook, 2006 Edition**

AUTHOR(S)

Stein Hauge, Per Hokstad, Helge Langseth and Knut Øien

CLIENT(S)

Multiclient - PDS Forum

REPORT NO. STF50 A06031	CLASSIFICATION Unrestricted	CLIENTS REF.	
CLASS. THIS PAGE Unrestricted	ISBN 82-14-03899-5	PROJECT NO. 384630.40	NO. OF PAGES/APPENDICES 77 / 5
ELECTRONIC FILE CODE		PROJECT MANAGER (NAME, SIGN.) Stein Hauge <i>Stein Hauge</i>	CHECKED BY (NAME, SIGN.) Tor Onshus <i>Tor Onshus</i>
FILE CODE	DATE 2006-04-03	APPROVED BY (NAME, POSITION, SIGN.) Lars Bodsberg, Research Director <i>Lars Bodsberg</i>	

ABSTRACT

PDS is a method used to quantify the safety unavailability and loss of production for safety instrumented systems (SIS). The method accounts for all types of failure categories; technical, software, human, etc.

This report gives an updated version of the PDS method. Among new features of the updated PDS method handbook are:

- A somewhat revised failure classification scheme;
- A modified common cause failure (CCF) model;
- An updated approach on the modelling of systematic failures;
- Some new and revised terminology.

IEC 61508 has become the main standard for specification, design and operation of safety instrumented systems. The PDS method is in line with the main principles advocated in this standard, however presenting some alternative approaches, e.g. to the modelling of systematic failures.

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

PREFACE

The “PDS Forum” is a co-operation between oil companies, engineering companies, consultants, vendors and researchers, with a special interest in reliability of safety instrumented systems. A PDS method handbook was issued in 2003, where the notation and approach were brought in line with functional safety standards like IEC 61508 and IEC 61511.

This new and revised edition is mainly a result of the work carried out as part of the user initiated research project “User friendly analysis tool for safety instrumented systems”¹. This work has included an update of the model for common cause failures, revised modelling of systematic failures as well as an update of some definitions and terminology.

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 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	3
1 INTRODUCTION	7
1.1 Purpose of the Handbook	7
1.2 Organisation of the Handbook	7
2 THE NEED FOR RELIABILITY CALCULATIONS.....	9
2.1 Why do we Need Reliability Analysis of Safety Instrumented Systems?	9
2.2 Why PDS?.....	10
2.3 Applications of the PDS Method	10
3 PDS RELIABILITY PARAMETERS.....	11
3.1 Introduction	11
3.2 Failure Classification by Cause of Failure	11
3.3 Quantification of Systematic Failures	13
3.4 Testing and Failure Fetection.....	14
3.4.1 Automatic Self-test and Random Detection by Personnel.....	14
3.4.2 Functional Testing.....	14
3.5 Failure Classification Related to IEC 61508.....	15
3.6 Performance Measures for Loss of Safety	20
3.6.1 Contributions to Loss of Safety.....	20
3.6.2 Loss of Safety due to DU Failures - Probability of Failure on Demand (PFD).....	21
3.6.3 Loss of Safety due to (Systematic) Test Independent Failures - TIF.....	22
3.6.4 Loss of Safety due to Downtime Unavailability – DTU.....	22
3.6.5 Overall Measure for Loss of Safety – Critical Safety Unavailability (CSU).....	23
3.7 Loss of Production	24
4 MODELLING OF COMMON CAUSE FAILURES.....	25
NOTE! THE REMAINING PART OF THE HANDBOOK IS NOT INCLUDED IN THIS FREE ELECTRONIC VERSION	
5 PDS CALCULATION FORMULAS	29
5.1 Introduction	29
5.2 Limitations	29
5.3 Approximate Loss of Safety Formulas.....	29
5.3.1 PFD Formulas	30
5.3.2 TIF Formulas.....	31
5.3.3 Formulas for Downtime Unavailability (DTU)	32
5.4 Quantification of Spurious Trip Rate (STR).....	35
5.5 Application Specific Calculations.....	36
6 QUANTIFICATION EXAMPLE – USING THE FORMULAS.....	37
6.1 Case Description – HIPPS System.....	37
6.2 Reliability Input Data	37
6.3 Loss of Safety Assessment - CSU.....	38
6.4 Production Availability Assessment	40

7	REFERENCES	41
	APPENDIX A: Notation and Abbreviations	43
	APPENDIX B: Detailed Formulas for PFD	47
	B.1 The CCF Model and Configuration Factors, C_{M00N}	47
	B.2 Formulas for PFD and DTU_R	48
	APPENDIX C: Application Specific Calculations for λ_{DU-S} , β and P_{TIF}	51
	C.1 Application Specific λ_{DU-S}	51
	C.2 Application Specific β	56
	C.2.1 Active Protection against Common Cause Failures	56
	C.2.2 Indirect Measures Taken against Common Cause Failures	58
	C.3 Application Specific P_{TIF}	60
	APPENDIX D: Generalised Reliability Models for Dependent Failures	63
	D.1 Non-Identical Components in Parallel	63
	D.2 Multiple Voting Configurations	65
	APPENDIX E: Diagnostic Coverage and the 1oo2D Configuration	71
	E.1 Diagnostic Coverage	71
	E.2 PFD for Standard Configurations	73
	E.3 The 1oo2D Configuration	74

1 INTRODUCTION

1.1 Purpose of the Handbook

The PDS² method is used to quantify the reliability, the safety and the Life Cycle Cost (LCC) of computer-based safety systems. The method is widely used in the Norwegian offshore industry, but is also applicable to other business sectors.

The increased use of computer-based safety systems has resulted in functional safety standards like IEC 61508³ and IEC 61511⁴. IEC 61508 provides a basis for specification, design and operation of Safety Instrumented Systems (SIS) with emphasis on safety activities related to each lifecycle phase of the system. The PDS method is in line with the main principles advocated in this standard, and is a useful tool when implementing and verifying quantitative (SIL) requirements as described in IEC 61508. For some areas like failure classification, modelling of common cause failures and how to treat systematic failures, the PDS method, however, offers an approach somewhat different from IEC 61508.

This report provides an updated version of the PDS method. The objective has been to incorporate development work done in the PDS project during the last two years. New features of this 2006 Edition of the PDS Method Handbook include:

- A somewhat revised failure classification scheme, more closely related to IEC terms and classification;
- New terminology for splitting of dangerous undetected failures in order to indicate the distribution between random hardware failures and systematic failures;
- A new common cause failure model, including a method for application specific calculation;
- New terminology for classification of systematic failures and a more thorough discussion on how to approach systematic failures in the reliability modelling;
- A new method for calculating application specific contributions from systematic failures;
- The terminology and classification related to “known” and “unknown” PFD as well as “non critical safety unavailability” (NSU) have been somewhat altered.

The report is aimed at reliability and safety engineers, as well as management, designers and technical personnel working with safety instrumented systems.

1.2 Organisation of the Handbook

The report is organised as follows:

- Chapter 2 includes a general discussion on the need for reliability calculations, and why the PDS calculation method is recommended.
- Chapter 3 discusses the failure classification and the reliability parameters of the updated PDS method.
- Chapter 4 describes modelling of common cause failures.

² PDS is the Norwegian acronym for “reliability of computer-based safety systems”.

³ The IEC standard, IEC 61508, applies to so-called E/E/PES safety related systems (E/E/PES is an acronym for Electrical/Electronic/Programmable Electronic Systems), frequently referred to as safety instrumented systems (SIS).

⁴ The process industry has developed its own sector specific application of IEC 61508, i.e. IEC 61511.

- Chapter 5 presents the calculation formulas and is therefore a main chapter.
- Chapter 6 presents a worked example of quantification.

Appendix A gives a full list of the notation, and Appendix B presents somewhat more detailed formulas than those given in Chapter 5.

In Appendix C application specific methods for calculating different PDS parameters are presented, whereas in Appendix D generalised reliability models for dependent failures are given.

Appendix E discusses the treatment of diagnostic coverage and the 1002D configuration.

The present report focuses on the safety and reliability aspects of the PDS method, including performance measures for loss of safety and for production availability. It does not consider maintenance performance and LCC, (see e.g. /12/ for some guidance on lifecycle cost calculations).

2 THE NEED FOR RELIABILITY CALCULATIONS

2.1 Why do we Need Reliability Analysis of Safety Instrumented Systems?

Microprocessors are increasingly replacing electromechanical relays in safety systems in the process industry. Computer-based fire and gas detection systems, process shutdown systems, and emergency shutdown systems are installed to prevent abnormal operating conditions from developing into an accident. Further, a major increase in the use of this kind of systems is seen also in other business sectors such as the public transport industry (air and rail) and the manufacturing industry.

At the same time, functional safety standards like IEC 61508, (ref /1/) are gradually replacing more “prescriptive” standards. This means that the design can be tailor-made for each particular application, given that a set of performance measures have acceptable values. An example may be the “spec-break” concept applied for long offshore pipelines. Whereas the entire pipeline traditionally used to be designed for full shut in pressure, this concept introduces a lower design pressure for the downstream part of the pipeline. In case of blocked pipeline outlet, an instrumented safety system shall shut down the inlet side of the pipeline in order to prevent overpressure in the downstream part of the line. Obviously, such solutions are often beneficial in terms of cost, but reliable operation of the instrumented safety system becomes crucial since a failure to shut in the pipeline may lead to disastrous consequences.

Addressing safety and reliability in all relevant phases of the safety system life cycle, therefore becomes paramount both with respect to safe as well as commercial operation. It must be verified that all safety requirements for the safety instrumented system are satisfied, and here the PDS method plays an important role.

IEC 61508, which has become a main standard within the SIS industry, is an example of a standard stating requirements to Safety Instrumented Systems (SIS). The Norwegian Oil Industry Association (OLF) has developed a guideline (OLF guideline no. 070) to support the use of IEC 61508 (and IEC 61511). In the new regulations from the Norwegian Petroleum Directorate (NPD) (ref /4/) specific references are given to the IEC standards and the OLF guideline. PDS is fully in line with the principles advocated in the IEC standard. The OLF Guideline recommends using the PDS method when quantifying loss of safety.

The IEC standard focuses on safety unavailability, although when designing safety shutdown systems there is generally a conflict between safety and production availability. The PDS method treats both these aspects of safety systems.

Although most reliability analyses have been used to *gain confidence* in the system by assessing the reliability attributes, it may be even more interesting to use reliability analysis as a means to *achieve* reliability, e.g., by design optimisation. It would usually be efficient to employ these techniques in the design phase of the system, when less costly changes can be made. Proper analytic tools available during the design process may ensure that an optimal system configuration is installed from the very beginning, thereby reducing overall system cost.

The operational phase has been given more attention in recent years, and the need of barrier control is stressed in the new NPD regulations (ref /4/). Further, both the IEC standard and the new requirements from NPD focus on the entire life cycle of the safety functions/systems. Also in the operational phase the PDS method can be used as a tool for verifying that the desired safety and reliability is achieved.

2.2 Why PDS?

Uncritical use of quantitative analyses may weaken the confidence in the value of performing reliability analyses, as extremely ‘good’, but highly unrealistic figures can be obtained, depending on the assumptions and the input data used.

The PDS method is considered to be realistic as it accounts for all major factors affecting reliability during system operation, such as:

- All failure categories/causes
- Common cause failures
- Automatic self-tests
- Functional (manual) testing
- Systematic failures
- Complete safety function
- Redundancies and voting logic

As stressed in IEC 61508, it is important to be function oriented, and take into account the performance of the total signal path from the sensors via the control logic and to the actuators. This is a core issue in PDS.

Although the PDS model is considered realistic, it is still relatively simple. The method is primarily a tool for non-experts in reliability, and should thus contribute to enhance the use of reliability analysis in the engineering disciplines, thereby bridging the gap between reliability theory and application.

2.3 Applications of the PDS Method

The PDS method has been applied in numerous projects and in many different contexts. The main application, however, has been related to computer-based safety systems in the offshore and onshore oil and gas industry. The PDS method has e.g. been utilised in:

- A large number of third-party reliability verifications of offshore and onshore safety systems.
- Projects that consider the effects of integrating the process control, process shutdown and emergency shutdown systems.
- Comparative reliability assessments of different control and safety systems for boiler applications.
- A study for specifying emergency shutdown (ESD) system requirements on offshore installations.
- Studies to compare different voting configurations of gas detectors, and to evaluate new detector design.
- Optimisation of the functional testing interval for offshore equipment, considering both safety and maintenance cost.
- A large number of HIPPS (High Integrity Pressure Protection System) related studies, for onshore, offshore and subsea applications.
- The development of the OLF 070 guideline, ref. /3/.

3 PDS RELIABILITY PARAMETERS

3.1 Introduction

This chapter presents the failure classification and the reliability parameters used in the PDS method. The objective is to give an introduction to the model taxonomy and to show the relation between the PDS and the IEC approach for quantification of loss of safety. The PDS terms will as far as possible comply with those used in IEC, so that the PDS method can easily be used for verification of SIL (Safety Integrity Level), without confusion of terms. However, we will in PDS introduce some additional terms based on a more detailed failure classification than used in the IEC approach. Failures are classified both according to cause of failure, failure mode (dangerous, spurious trip or non-critical), and whether or not failures are detected in tests.

There exist various performance measures for loss of safety. The IEC standard introduces PFD (Probability of Failure on Demand) to measure the loss of safety due to hardware failures. The PDS method introduces performance measures to account also for systematic failures. This chapter presents the various measures for loss of safety used in PDS and IEC. The complete relation between the terms used in the PDS method and the corresponding IEC terms is presented in Appendix A.

3.2 Failure Classification by Cause of Failure

Failures can be categorised according to failure cause. IEC splits the failures into *random hardware* and *systematic* failures. The PDS method will adopt this classification, but also utilises a more detailed classification, as shown in Figure 1.

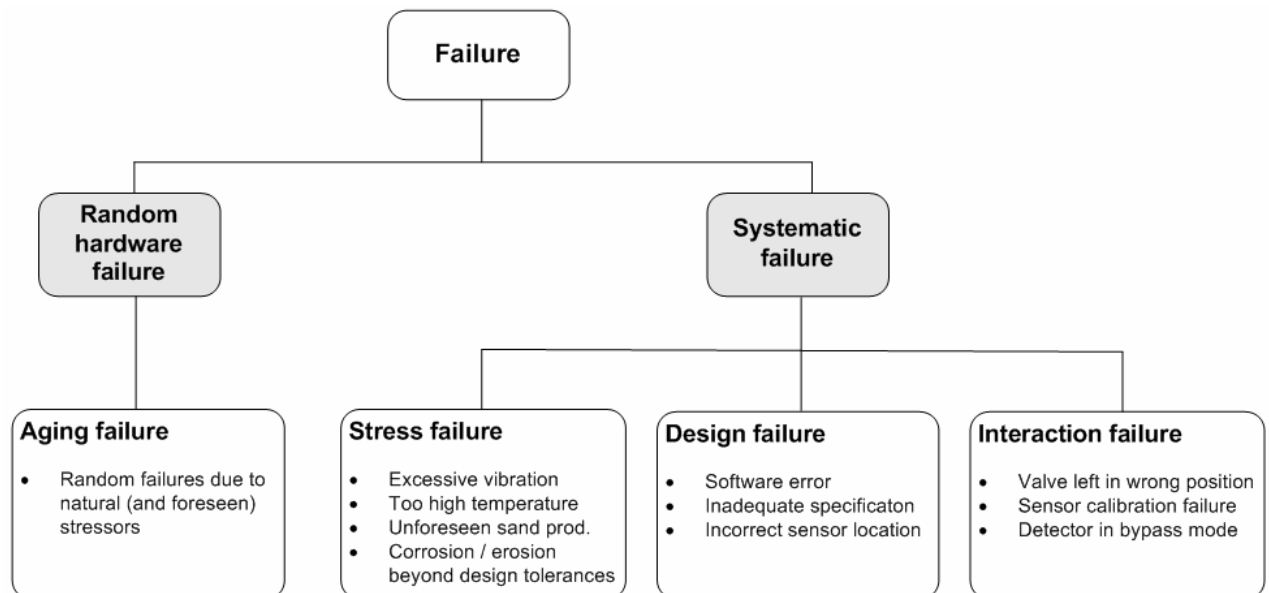


Figure 1 Failure classification by cause of failure.

The following failure categories (causes) are defined:

Random hardware failures are failures resulting from the natural degradation mechanisms of the component. For these failures it is assumed that the operating conditions are within the design envelope of the system.

Systematic failures are failures that can be related to a particular cause other than natural degradation (aging). The failure can normally be eliminated by a modification, either of e.g. the design or manufacturing process, the operating procedures or documentation. The systematic failures are further split into three categories according to their cause.

- **Stress** failures occur when excessive stresses, i.e. stresses beyond the design envelope, are placed upon the component. The excessive stresses may be caused either by external causes or by internal influences from the medium. Examples may be damage to process sensors as a result of excessive vibration or valve failure caused by unforeseen sand production.
- **Design** failures, broadly speaking are introduced during phases prior to operation. It may be a failure in the system specification itself, a manufacturing fault or a failure introduced during installation. Examples are valve failure due to insufficient actuator force, sensors failing to discriminate between true and false demands, and erroneous location of e.g. fire/gas detectors.
- **Interaction** (or operational) failures are initiated by human errors during operation or maintenance/testing. Examples are loops left in the override position after completion of maintenance or a process sensor isolation valve left in closed position. Another example can be during a modification, e.g. installation of a new process module, where the logic is not sufficiently updated to include all required equipment in the shutdown sequence.

As a general rule, systematic failures, i.e. *stress*, *interaction* and *design* failures, can give rise to failure of multiple components, i.e. common cause failures. Random hardware failures, on the other hand, can be denoted *independent* failures and are assumed not to result in common cause failures.

It should be noted that some failures may not fit perfectly into the above scheme. E.g., it may sometimes be difficult to discriminate between an aging failure and a stress failure. However, in order to avoid a too complex classification, the above scheme is considered sufficiently detailed for most purposes.

As seen from Figure 1 and the above definitions, the PDS failure classification has been somewhat altered as compared to the previous version of the handbook. The stress failure category has been classified as a type of systematic failures. This has been done to comply with definitions given by IEC⁵, but also since stress failures have the typical features of a systematic failure: the failure can only be eliminated by removing the excessive stresses put upon the component or by modifying the component itself.

Random hardware failures are sometimes referred to as *physical failures* whereas systematic failures are referred to as *non-physical* or *functional failures*. A physical failure occurs when a component has degraded to a point of failure where it is not able to operate and thus needs to be changed or repaired. An example can be a limit switch which due to wear out is not able to change position.

⁵ Ref. IEC 61508-4, section 3.6 for definitions of *Random hardware failure* and *Systematic failure*.

A non-physical or functional failure on the other hand, occurs when the component is still able to operate but does not perform its specified function. An example is a pressure transmitter that is not functioning because the sensing line is plugged. It should, however, be noted that systematic failures caused by excessive stresses may result in a physical failure of the component. E.g. unforeseen vibration of a pump can cause a physical failure of a flow transmitter located on the connected piping. Hence, given the classification scheme in figure 1, it is not always correct to state that all systematic failures are non-physical failures.

The PDS method has a strict focus on the *entire* safety function, and intends to account for *all* failures that could compromise this function (i.e. result in "loss of function"). Some of these failures are related to the interface/environment (e.g. "overheating in the safety cabinet"), rather than the safety system itself. However, it is part of the "PDS philosophy" to include such events.

3.3 Quantification of Systematic Failures

In the PDS method quantitative measures for loss of safety are provided for both random hardware failures as well as systematic failures. This approach differs from the IEC 61508 standard, which explicitly states that only the contribution from random hardware failures shall be quantified. It should, however, be noted that IEC implicitly quantifies part of the systematic failures through the proposed method for quantifying hardware related common cause failures (ref. IEC 61508-6, Annex D).

The approach chosen by IEC is understandable as failure rates for systematic failures are often hard to predict and will depend on each particular application. On the other hand there are several reasons why we should attempt to quantify the contribution from systematic failures:

- When performing reliability calculations our main interest will often be to estimate how the component/system will actually perform in the field (as opposed to in a "laboratory-like" environment). Similarly, when using our failure estimates in Quantitative Risk Analysis (QRA), it is important to use realistic failure rates in order to reflect the actual risk related to the operation;
- Failure rates as given in e.g. /15/, /16/ and /17/, are often based on historic (operational) data and therefore implicitly include (at least some) systematic failures;
- Often, systematic failures may be the dominant contributor towards the overall failure probability (further discussed in /17/). This is e.g. seen by the major discrepancies between certificate/manufacturer data (which often accounts for only random hardware failures) and actual field performance data (which will include also systematic failures). Consequently, it can be argued that it is somewhat illogical only to include part of the failure rate in the reliability calculations;
- When introducing measures to prevent systematic failures, these measures should (ideally) be reflected in the quantitative failure rate estimate.

Therefore, in the PDS method we have chosen to provide models and data for quantification of both random hardware failures as well as systematic failures. In this edition of the handbook, modelling of systematic failures has been somewhat revised. The systematic failures comprise two main categories:

- Systematic failures detectable during testing. Examples may be a detector left in bypass mode at the last test, or a valve that will not close due to hydrate formation;
- Systematic failures not detected during testing but occurring upon a true demand. One example is a software error introduced during update of the program logic. Another

example can be an internal leakage through a valve which is not detected during regular stroke testing.

The actual modelling of these failure types is further discussed in following sections.

3.4 Testing and Failure Fetection

The PDS method takes into account the following two main types of testing and subsequent failure detection:

- Failure detection by automatic self-tests
- Failure detection by functional testing (manual testing)

In addition to failures revealed by self-test or functional testing, the PDS model will also take into consideration the fact that some failures may be revealed incidentally by operators or maintenance personnel. E.g., when performing maintenance on a process segment, the operator may find out that a valve will not close. Such random failure detection by personnel will be treated in conjunction with automatic self-test (even though it may be seen as a distinct third way of detecting failures).

3.4.1 Automatic Self-test and Random Detection by Personnel

Modules often have built-in *automatic (diagnostic) self-test* to detect failures. Further, upon discrepancy between redundant modules in the safety system, the system may determine which of the modules have failed. This is considered part of the self-test. But it is never the case that *all* failures are detected automatically. 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; (i.e. the effect depends on the voting logic and whether degraded operation takes place when a failure is detected).

In addition to the automatic 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*⁶; *c* reflecting detection *both* by automatic self-test and by operator.

Furthermore, potential spurious trip failures may also be revealed prior to an actual trip. E.g. if the operator notices that a pressure transmitter is “drifting”, he may deactivate the transmitter in order to prevent a shutdown (one obviously needs to be careful when allowing such a practice).

3.4.2 Functional Testing

Functional testing is performed manually at predefined time intervals, typically 3, 6, 12 or 24 months intervals. However, the testing can be imperfect and/or the test conditions may deviate

⁶ In previous editions of the PDS handbook, the fault coverage factor, taking into consideration automatic (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 one common coverage factor *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.

from the true demand conditions, leaving some parts of the function untested. Consequently, some systematic failures are not revealed until an actual demand occurs. Figure 2 exemplifies this somewhat further.

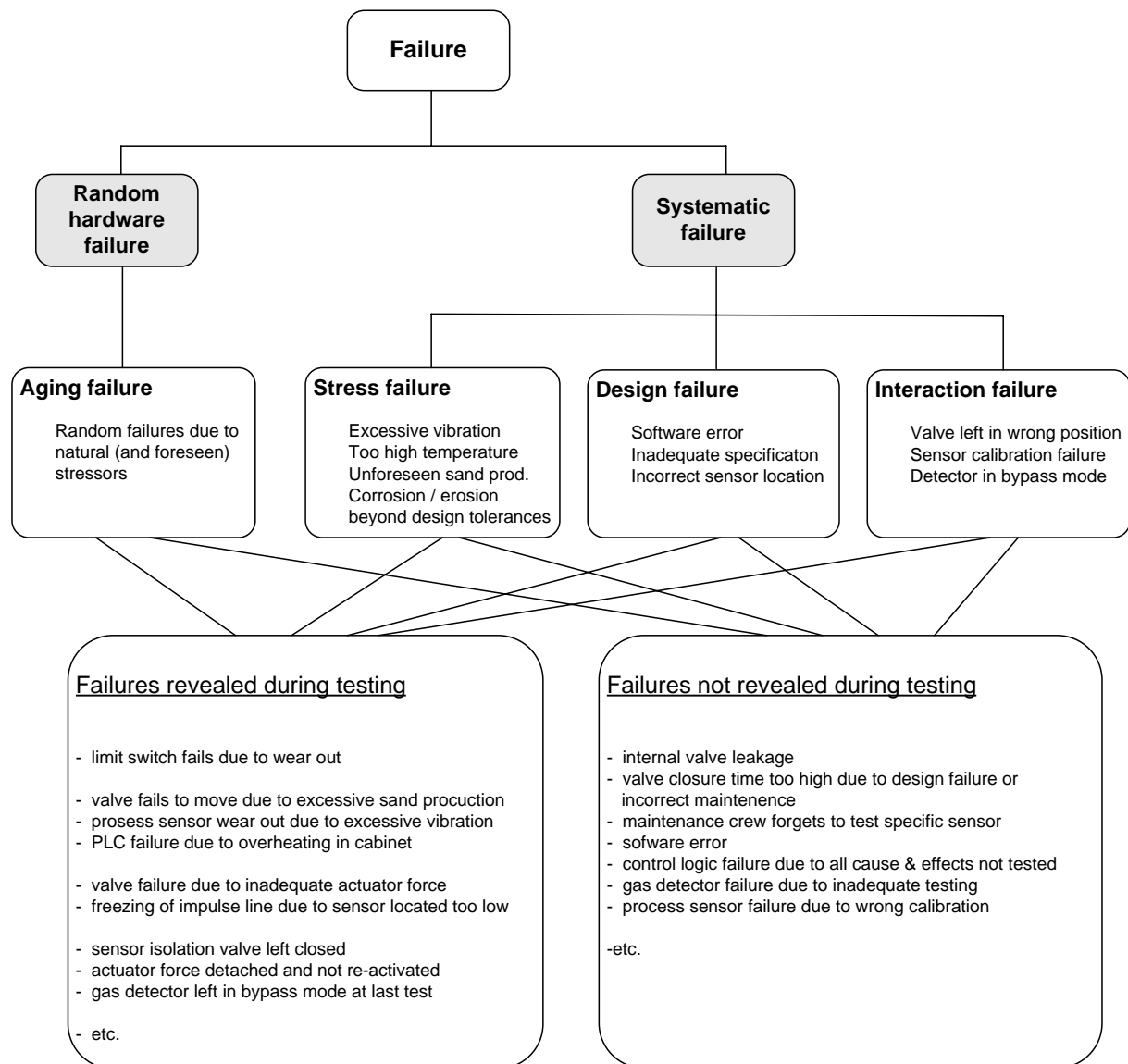


Figure 2 Failure classification and testing

3.5 Failure Classification Related to IEC 61508

In this section we will discuss the failure classification proposed in IEC 61508 and clarify some differences between the IEC and the PDS notation.

The IEC 61508 standard splits all (random hardware) failures into:

- Dangerous Undetected (DU) failures
- Dangerous Detected (DD) failures
- Safe Undetected (SU) failures
- Safe Detected (SD) failures.

A similar failure classification is made also in PDS, but is not limited to random hardware failures only. All failures that can be detected by either functional testing, automatic self-test or incidentally by an operator, are split into these categories. A comparison of the IEC and PDS failure classification is illustrated in Figure 3.

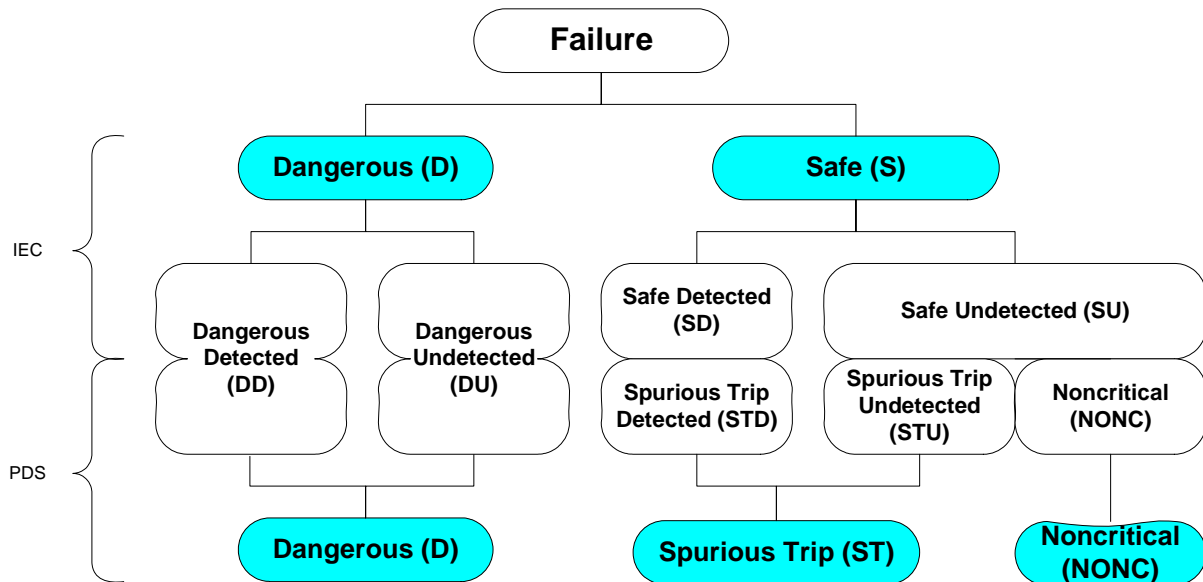


Figure 3 Failure mode classification – component level.

From the IEC standard it is somewhat unclear what is actually included in the safe (S) failures (i.e. SU and SD)⁷. One possible interpretation, reflected in Figure 3, is that IEC includes both critical as well as non-critical failures (i.e. those failures that do not affect any of the two main functions of the module/system⁸). In the PDS method we have therefore chosen to use a slightly different notation for safe failures; i.e. these failures are split into spurious trip failures (i.e. failures where the safety system is activated without a demand) and non-critical failures (which do not affect the main functions of the system). For convenience we classify all non-critical failures as safe undetected failures (i.e. in the SU category).

Hence, the PDS method considers three failure modes; dangerous, spurious trip and non-critical failures.

- **Dangerous (D).** The module does not operate upon a demand (e.g. sensor stuck upon demand or valve does not close on demand). The Dangerous failures are further split into:
 - **Dangerous Undetected (DU).** Dangerous failures not detected by automatic self-test or incidentally by personnel (i.e. revealed only by a functional test or upon a demand);
 - **Dangerous Detected (DD).** Dangerous failures detected by automatic self-test or incidentally by personnel.
- **Spurious Trip (ST).** The module operates without any demand (e.g. sensor provides a shut down signal without a true demand - 'false alarm'). These are further split into:
 - **Spurious Trip Undetected (STU)** Spurious trip failures not detected by automatic self-test or incidentally by personnel;

⁷ In IEC 61508 a safe failure is defined as a “failure which does not have the potential to put the safety-related system in a hazardous or fail-to-function state”.

⁸ The two main functions are the ability to maintain production when it is safe and to shut down when production is not safe.

- **Spurious Trip Detected (STD)** Spurious trip failures detected by automatic self-test or incidentally by personnel⁹.
- **Non-critical (NONC)**. The main functions of the module are not affected. Examples may be sensor imperfection or a minor leakage of hydraulic oil for a valve, which has no immediate impact on the specified safety function.

The Dangerous and Spurious Trip failures are considered "critical", as they affect basic/main functions ("ability to shut down on demand" and "ability to maintain production when safe"). The ST failures are usually revealed instantly upon occurrence, whilst the D failures are "dormant" and can be detected by testing or upon a true demand.

As discussed above, the IEC standards make no explicit distinction between critical and non-critical failures. However, the following interpretation applies (ref. Figure 3); the safe detected (SD) in the IEC notation is identical to spurious trip detected (STD) in PDS. Further, safe undetected (SU) in IEC is in PDS interpreted as the sum of spurious trip undetected (STU) and non-critical (NONC).

Based on the classification discussed above, the failure rate λ , is split into the following elements:

- λ_{DD} = Rate of dangerous detected failures (as in IEC)
- λ_{DU} = Rate of dangerous undetected failures (as in IEC)
- λ_{STD} = Rate of spurious trip detected failures (= λ_{SD} in IEC)
- λ_{STU} = Rate of spurious trip undetected failures (part of λ_{SU} in IEC)
- λ_{NONC} = Rate of non-critical failures (part of λ_{SU} in IEC)

The λ_{SU} in the IEC notation equals the sum of the last two terms, i.e. $\lambda_{SU} = \lambda_{STU} + \lambda_{NONC}$. Hence, there is an implicit assumption that all the non-critical failures are undetected by automatic self-test. Further, if we can assume $\lambda_{NONC} = 0$, then $\lambda_{SU} = \lambda_{STU}$.

We also introduce:

- $\lambda_{undet} = \lambda_{DU} + \lambda_{STU}$, which is the rate of critical failures that are undetected by automatic self-test (or by personnel in between functional tests);
- $\lambda_{det} = \lambda_{DD} + \lambda_{STD}$, which is the rate of critical failures that are detected by automatic self-test (or incidentally by personnel, independent of functional testing).
- $\lambda_{crit} = \lambda_D + \lambda_{ST}$, which is the rate of critical failures; i.e. failures which unless detected, will cause either dangerous (D) or spurious trip (ST) unavailability of safety functions.

In addition we have the total failure rate $\lambda = \lambda_{crit} + \lambda_{NONC}$. Table 1 and Figure 4 further illustrate how λ_{crit} and λ can be split into their various elements.

⁹ Depending on configuration, the detection of a failure could prevent an actual trip of the system, ref Appendix E.

Table 1 Rate of critical failures, λ_{crit} , split into various elements.

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

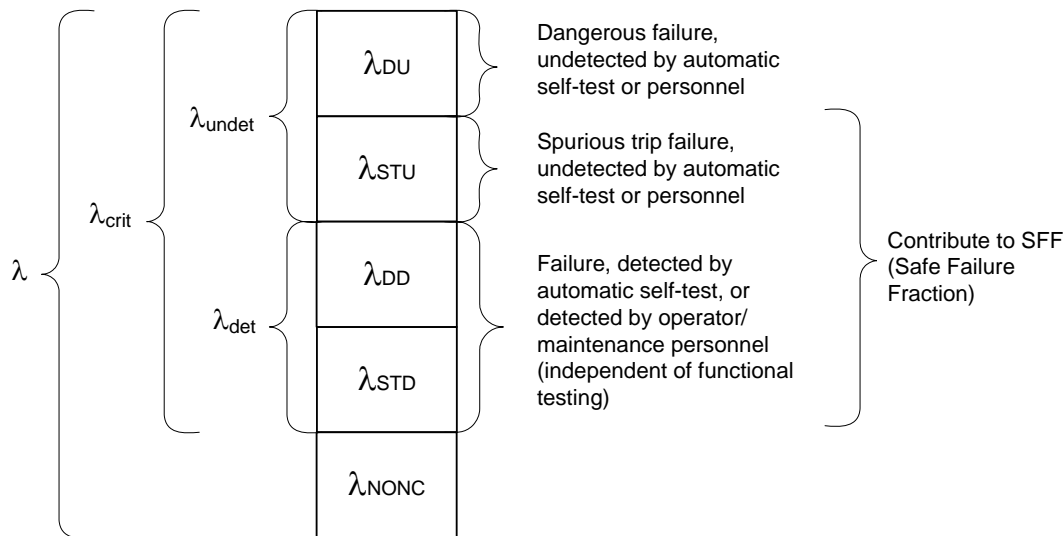


Figure 4 Failure rate, λ , split into various elements.

Dangerous Undetected Failures - λ_{DU}

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, as discussed in section 3.2, when going through historic failure data, it can be seen that many of the reported failures are systematic ones. 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 to open due to excessive internal erosion or corrosion.

Hence, when considering the failure rates (λ_{DU}) presented in many data handbooks such as /15/, /16/ and /17/, these data may include both random hardware failures as well as systematic failures. As a result, systematic failures are implicitly included in the reliability calculations. On the other hand, 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. This can be explained by the fact that such failure data often result from FMECA type of analyses where failures that in some sense can be related to errors in design or operation of the equipment are not included.

Consequently, it is relevant to think of λ_{DU} as comprising two elements; λ_{DU-RH} which is the rate of DU random hardware failures (i.e. the strict IEC definition of λ_{DU}), and λ_{DU-S} , being the rate of DU systematic failures, detectable by functional testing. Hence, $\lambda_{DU} = \lambda_{DU-RH} + \lambda_{DU-S}$. What is obtained by making such a split?

- As discussed above, the difference between generic data found in handbooks and vendor/certificate data, can often be explained by the fact that (experienced) λ_{DU} rates includes both random hardware- as well as systematic failures;
- The importance of systematic failures is more explicitly shown since λ_{DU-S} often will make up a considerable part of the total λ_{DU} ;
- Similarly, the fact that many systematic failures can be revealed during functional testing is also illustrated by making this split;
- When we shall quantify the effect of implementing measures against systematic failures, we need to consider the value of λ_{DU-S} (together with the effectiveness of functional tests against systematic failures, see section 3.6.3 and Appendix C).

Note that the splitting of λ_{DU} will *not* be a necessity in order to perform the standard reliability calculations. This is further discussed when the calculation formulas are presented in the next sections. One should, however, bear in mind that when we want to predict the actual performance of the equipment in the field, we should always include the systematic failure part of the λ_{DU} (i.e. the λ_{DU-S}). Furthermore, when application specific calculations are performed (ref. Appendix C), splitting of the failure rate, λ_{DU} , will be required.

Coverage Factors and Safe Failure Fraction

IEC 61508 introduces the *diagnostic* coverage (DC) as:

- $DC = \lambda_{DD}/\lambda_D =$ Fractional decrease in the probability of dangerous hardware failures resulting from the operation of automatic *diagnostic* tests

In addition, the standard refers to the term "safe diagnostic coverage", to represent the fractional decrease of *safe* hardware failure, and similarly refer to the coverage of both safe and dangerous hardware failures. Thus, there are various DC factors, and it is necessary to introduce a notation to distinguish between these.

In the IEC definition (of DC) given above, the coverage only includes failures "detected by automatic self-test". As discussed in Section 3.4, it is relevant also to include "random detection by personnel" (control room operator, field operator or maintenance crew). Therefore, in PDS we will refer to the fraction of detected failures as simply the (overall) *coverage*, c , defined for dangerous and spurious trip failures as:

- $c_D = \lambda_{DD} / \lambda_D =$ Fraction of dangerous failures detected by automatic self tests *or* by personnel
- $c_{ST} = \lambda_{STD} / \lambda_{ST} =$ Fraction of spurious trip failures detected by automatic self tests *or* by personnel

Thus, as part of the *coverage*, c , we include any failure that in some way is detected in between functional tests. It should be noted that the rate of dangerous detected failures λ_{DD} will differ for different type of equipment. For control logic, failures will mainly be detected through diagnostic self-test. For valves and sensors some additional failures will also be detected incidentally by personnel.

Finally, observe that IEC also introduces the safe failure fraction (SFF). This is the fraction of failures that are not critical with respect to safety unavailability of the safety function (in IEC 61508 defined as the ratio of safe failures plus dangerous detected failures to the total failure rate). In PDS we use the following interpretation:

- $SFF = 1 - (\lambda_{DU} / \lambda_{crit})$; or rather in per cent: $SFF = (1 - (\lambda_{DU} / \lambda_{crit})) \times 100\%$.

Note that IEC 61508 applies the definition $SFF = 1 - (\lambda_{DU} / \lambda)$, the reason being that IEC does not discuss the potential difference between λ and λ_{crit} (ref. discussion above).

Summary of Differences between IEC and PDS Notation

To highlight and summarise the differences between the IEC and PDS notation related to failure classification, the following should be noted:

- PDS recognises that data for the failure rate λ given in different generic data sources often include systematic failures revealed in e.g. functional tests, in addition to the random hardware failures. In particular, we split λ_{DU} into the rate of random hardware failure (λ_{DU-RH}) and the rate of systematic failures (λ_{DU-S}).
- In PDS the total failure rate, λ , is split into λ_{crit} and λ_{NONC} .
- Safe (S) failures in IEC are in PDS split into spurious trip (ST) failures and non-critical (NONC) failures.
- IEC defines the *diagnostic* coverage, DC, which only includes self-tests. In PDS we rather use the coverage, c, which refers to any detection in between functional tests (*either* by automatic self-test *or* incidentally by personnel).
- In PDS the safe failure fraction is defined as $SFF = 1 - \lambda_{DU} / \lambda_{crit}$.

3.6 Performance Measures for Loss of Safety

This section presents the various measures for loss of safety used in PDS. All these reflect *safety unavailability* of the function, i.e. the probability of a failure on demand. The measure for loss of safety used in IEC is denoted PFD (Probability of Failure on Demand), and this is also one of the measures adopted in the PDS method.

3.6.1 Contributions to Loss of Safety

The potential contributors to loss of safety (safety unavailability) can be split into the following categories:

- 1) *Unavailability due to dangerous undetected (DU) failures.* For a single component, these failures occur with a rate λ_{DU} . The average period of unavailability due to such a failure is $\tau/2$ (where τ = period of functional testing), since the failure can have occurred anywhere inside the test interval. In this period the failure has not been detected, and it is *not known* that the component is unavailable. The unavailability may therefore be referred to as “unknown”. This unavailability may be thought of as comprising two elements:
 - a) The unavailability due to dangerous undetected random hardware failures (of rate λ_{DU-RH}). I.e. random hardware failures introduced some time after the last functional test (which is either revealed during a demand or during the next functional test).
 - b) The unavailability due to dangerous undetected systematic failures (of rate λ_{DU-S}). I.e. systematic failures introduced some time after the last functional test (which is either revealed during a demand or during the next functional test).
- 2) *Unavailability due to systematic failures* which are *not* revealed even during the functional testing. Hence, this unavailability is caused by “unknown” (“dormant”), dangerous and undetected failures which are detected only during a true demand. These systematic failures

are denoted *Test Independent Failures* (TIF), as they are not detected through the functional test (nor by automatic self-test or incidentally by personnel).

- 3) *Unavailability due to known or planned downtime*. This is the unavailability or downtime caused by components which are either known to have failed or are taken out for testing/maintenance. This unavailability may also be split in two main contributors:
 - a) The "known" unavailability due to dangerous (D) failures where the failed component must be repaired. The average period of unavailability due to these events equals the mean restoration time, MTTR, i.e. the time elapsing from the failure is detected until the situation is restored. In this period it is *known* that the component has failed and is unavailable.
 - b) The "planned" (and known) unavailability due to the downtime/inhibition time during functional testing and/or preventive maintenance.

It should be noted that the actual contribution to loss of safety from failures in category 3) will depend heavily on the operating philosophy, on the configuration of the process plant as well as the configuration of the SIS itself. Sometimes, temporary compensating measures will be introduced while a component is down for maintenance or repair. Other times, when the component is considered too critical to continue production (e.g. a critical shutdown valve in a 1 x 100% configuration), the production may simply be shut down during the restoration and testing period. Hence, the downtime unavailability should be treated separately and not together with category 1) and 2). Furthermore, often both the contributions 3a) and 3b) are small compared to the contribution from failures in category 1). That is, usually $MTTR \ll \tau$. This is, however, not always the case; e.g. for subsea equipment in offshore production, the MTTR could be rather long. Category 3b) can often be considered the least critical, as this represents a truly planned unavailability of the safety system and since testing and maintenance is often performed during planned shutdown periods.

Below, we discuss separately the loss of safety measures for the three failure categories, and finally an overall measure for loss of safety is given.

3.6.2 Loss of Safety due to DU Failures - Probability of Failure on Demand (PFD)

In order to quantify the loss of safety due to random hardware failures, IEC uses the term:

$$PFD = \text{Probability of Failure on Demand}$$

According to the formulas given in IEC, it appears that the PFD includes the failure contributions from category 1a) as well as from 3a). However, as argued above, it is natural to consider the known downtime unavailability separately. Therefore, in the updated PDS method, when we refer to the PFD, this includes only the unknown (category 1) DU failures (which in the previous PDS report was denoted PFD_{UK}). Hence, the PFD quantifies the loss of safety due to dangerous undetected failures (with rate λ_{DU}), *during the period when it is unknown that the function is unavailable*. The average duration of this period is $\tau/2$, where τ = test period. If the downtime unavailability (i.e. category 3 above) is added, this is explicitly stated.

IEC 61508 further states that only the effect of random hardware failures shall be quantified. However, as discussed in section 3.3, the standard recommends a quantification of PFD which includes a contribution from common cause failures, and these are obviously systematic failures. It seems somewhat illogical to account for systematic failures for redundant systems, but not for single systems. Therefore, in PDS, the PFD consists of two elements also for single systems; i.e.

the unavailability due to random hardware failures (of rate λ_{DU-RH}) and the unavailability due to systematic failures detectable by functional testing (of rate λ_{DU-S}). Consequently, for a single unit:

$$PFD \approx \lambda_{DU} \tau/2 = \lambda_{DU-RH} \tau/2 + \lambda_{DU-S} \tau/2$$

Note that when we perform standard reliability calculations, it will for most purposes be unnecessary to split the rate of DU failures, and so the $\lambda_{DU} \tau/2$ formula can be applied directly.

3.6.3 Loss of Safety due to (Systematic) Test Independent Failures - TIF

It is an essential and rather unique feature of the PDS approach that it accounts also for systematic failures. As discussed above, systematic failures can be either detectable by functional testing (i.e. category 1b above) or they are detected only during an actual demand (i.e. category 2 above). The latter category is here referred to as test independent failures (TIF). The following unavailability measure is introduced¹⁰:

$$P_{TIF} = \textit{The Probability that the module/system will fail to carry out its intended function due to a (latent) systematic failure not detectable by functional testing (therefore the name "test independent failure")}$$

It should be noted that if an imperfect testing *principle* is adopted for the functional testing, this will lead to an increase of the TIF probability. For instance, if a gas detector is tested by introducing a dedicated test gas to the housing via a special port, the test will not reveal a blockage of the main ports. Also, use of a *dedicated* test gas is a contribution to the uncertainty, as testing with *process* gas has not been done. Another example is the use of partial stroke testing for valves. When replacing a full stroke test, the P_{TIF} is likely to increase because the valve is not fully proof tested during a partial stroke test.

3.6.4 Loss of Safety due to Downtime Unavailability – DTU

This represents the *downtime* part of the safety unavailability as described in categories 3a) and 3b) above and has previously been denoted PFD_K and NSU respectively. In order to avoid having two different PFD measures as well as the NSU (non-critical safety unavailability), we rather introduce the measure DTU (downtime unavailability). The DTU comprises two elements:

- DTU_R ; i.e. downtime unavailability due to repair of dangerous failures of rate λ_D , resulting in a period when it is known that the function is unavailable (i.e. category 3a above, corresponding to the previous PFD_K). The average duration of this period is the mean restoration time (MTTR); i.e. the time from the failure is detected until the safety function is restored;
- DTU_T ; i.e. planned downtime (or inhibition time) resulting from activities such as testing, maintenance and inspection (i.e. category 3b above, corresponding to the previous NSU).

¹⁰ In the previous PDS method handbook, /6/, we applied the term PSF (probability of systematic failure) which was split in three contributors; PSF_{DF} , PSF_{RI} and PSF_{TI} (i.e. design failure-, random interaction- and test interaction unavailability, respectively). In order to simplify the modelling, we will rather consider the systematic failure as comprising two elements, those detectable by functional testing (of rate λ_{DU-S}) and those undetectable by functional testing (with probability P_{TIF}).

Depending on the operational philosophy and the configuration of the process plant and the SIS, it must be decided whether it is relevant to include (part of) the DTU in the overall measure for loss of safety. This is further discussed in Chapter 5.

3.6.5 Overall Measure for Loss of Safety – Critical Safety Unavailability (CSU)

In PDS we use the measure Critical Safety Unavailability (CSU) to quantify the total loss of safety:

CSU = The probability that the module/safety system will fail to automatically carry out a successful safety action on the occurrence of a hazardous/accidental event, (and it is not known that the safety system is unavailable).

Thus, we have the relation:

$$CSU = PFD + P_{TIF}$$

If we want to include also the “known” downtime unavailability, the formula becomes:

$$CSU_{TOT} = PFD + P_{TIF} + DTU$$

As discussed above, IEC quantifies only the downtime unavailability which is due to component restoration time resulting from a dangerous failure (i.e. only the DTU_R). No separate formula for quantification of unavailability caused by component downtime during testing and inspection is given in IEC (i.e. for the DTU_T). In PDS it is assumed that extra precautions are taken during known unavailability of the safety system, and the downtime contribution to loss of safety therefore needs separate consideration. However, for the sake of completeness, formulas are given also for downtime unavailability (ref. section 5.3.3).

The potential contributions to the overall safety unavailability are presented in Figure 5.

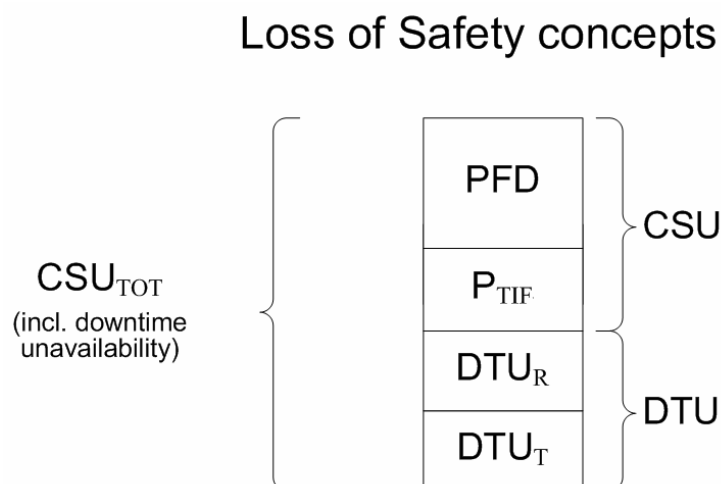


Figure 5 Loss of safety measures used in PDS

A graphical illustration of the contribution from dangerous undetected failures (PFD) and test independent failures (TIF) to the critical safety unavailability (CSU) is illustrated in Figure 6.

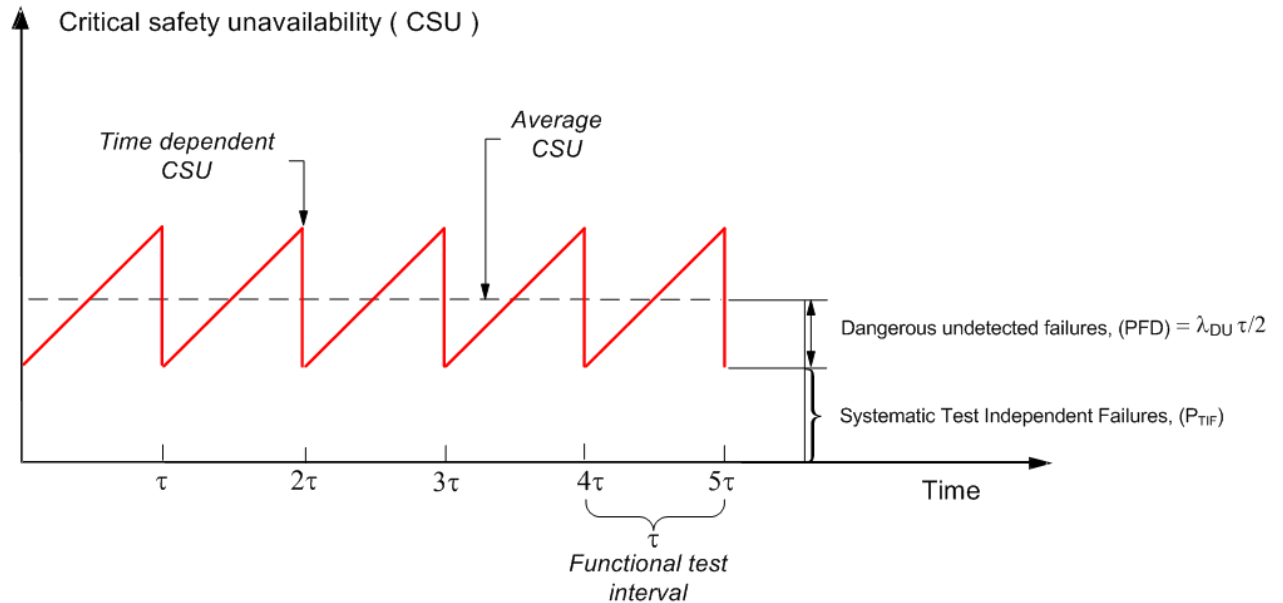


Figure 6 Contributions to critical safety unavailability (CSU)

3.7 Loss of Production

The IEC standards focus on loss of safety. However, there is also a possibility that the safety systems can cause a shut down of the process when there is no actual demand. Examples may be a gas detector giving an alarm when there is no gas in the area, or a level transmitter indicating high level when the level is actually within normal. Such failures are called spurious trip failures, (or safe failures in IEC). It is important to balance the loss of safety against the rate of spurious trips (loss of production). In the PDS method the measure for quantifying loss of production is the *spurious trip rate*:

$$\text{STR} = \text{the mean number of spurious activations of the safety system per time unit}$$

For this measure, the applied time unit is usually *per year* or *per 10⁶ hrs.*

In addition there may be loss of production due to repair of dangerous (and safe) failures and also during testing. Whether this contributes to the downtime unavailability (DTU - which is safety related) or to loss of production, will depend upon the operational philosophy during repair and testing. This is further discussed in Section 5.3.3.

4 MODELLING OF COMMON CAUSE FAILURES

When we quantify the reliability of redundant safety systems, it is essential to distinguish between *independent* and *dependent* failures. Random hardware failures caused by natural stressors (ref. Figure 1) are *independent* failures, i.e. a failure of one component/module is not assumed to influence the failure frequency of other identical modules in the safety system. However, all systematic failures, including stress failures, design related failures and interaction failures are by nature potentially *dependent* failures. Such failures can lead to simultaneous failure of more than one module in the safety system (i.e. a common cause failure, CCF), and will therefore reduce the effect of redundancy.

Beta (β)-factor Model

The traditional way of accounting for common cause failures (CCF) has been the beta-factor approach. One problem with this approach is that for any M-out-of N (MooN) voting¹¹, ($M < N$), the rate of dependent failures is the same. If λ is the component failure rate, the MooN voted system has a common cause failure contribution equal to $\beta \cdot \lambda$. Hence, this approach does not distinguish between different voting logics, and the same result is obtained e.g. for 1oo2, 1oo3 and 2oo3 voted systems. A possible solution is to use different β factors for each voting; e.g. using $\beta=1\%$ for 1oo3, $\beta=5\%$ for 1oo2 and $\beta=10\%$ for 2oo3. This is the approach suggested in the IEC standards (IEC 61508-6, App. D), which introduces an "application specific" β , which to some extent depends on the voting logic, MooN. However, the rate of system CCFs does only to a slight degree depend on the system configuration. For instance, this approach does not distinguish between voting logics like 1oo2 and 2oo3. This may not be sufficiently detailed for all applications, e.g. if the purpose is to compare two different voting logics.

PDS Extension of the Beta-factor Model - C_{MooN}

Due to the limitations in the IEC approach for modelling of common cause failures, the PDS method will provide an extension of the beta-factor model. In PDS the beta-factor explicitly depends on the configuration, and the beta-factor of a MooN voting logic is expressed as:

$$\beta(\text{MooN}) = \beta \cdot C_{\text{MooN}}, (M < N),$$

Here, C_{MooN} is a modification factor for various voting configurations, and β is the beta-factor which applies for a 1oo2 voting. This means that if each of the N modules has a failure rate λ , then the MooN configuration will have a system failure rate due to CCF that equals $C_{\text{MooN}} \cdot \beta \cdot \lambda$.

By using the suggested model, the parameter β is maintained as an essential parameter whose interpretation is now entirely related to a duplicated system. Further, note that the effect of voting is introduced as a *separate* factor, C_{MooN} , independent of β . This makes the model easy to use in practice.

Suggested values of C_{MooN} for some typical voting configurations are given in Table 2.

¹¹ A MooN voting means that at least M of the N redundant modules have to give a shutdown signal for a shutdown to be activated.

Table 2 CCF configuration factor, C_{MooN} , for different voting logics

$N \setminus M$	$M = 1$	$M = 2$	$M = 3$	$M = 4$	$M = 5$
$N = 2$	$C_{1002} = 1.0$	-	-	-	-
$N = 3$	$C_{1003} = 0.30$	$C_{2003} = 2.4$	-	-	-
$N = 4$	$C_{1004} = 0.15$	$C_{2004} = 0.75$	$C_{3004} = 4.0$	-	-
$N = 5$	$C_{1005} = 0.08$	$C_{2005} = 0.45$	$C_{3005} = 1.2$	$C_{4005} = 6.0$	-
$N = 6$	$C_{1006} = 0.04$	$C_{2006} = 0.26$	$C_{3006} = 0.8$	$C_{4006} = 1.6$	$C_{5006} = 8.1$

There is of course no definite choice of these values of Table 2. Nevertheless they are, for most applications, expected to be more realistic than the standard beta-factor modelling. Observe that $C_{1002} = 1$, thus, for the 1002-voting we use the specified β -value without any modification.

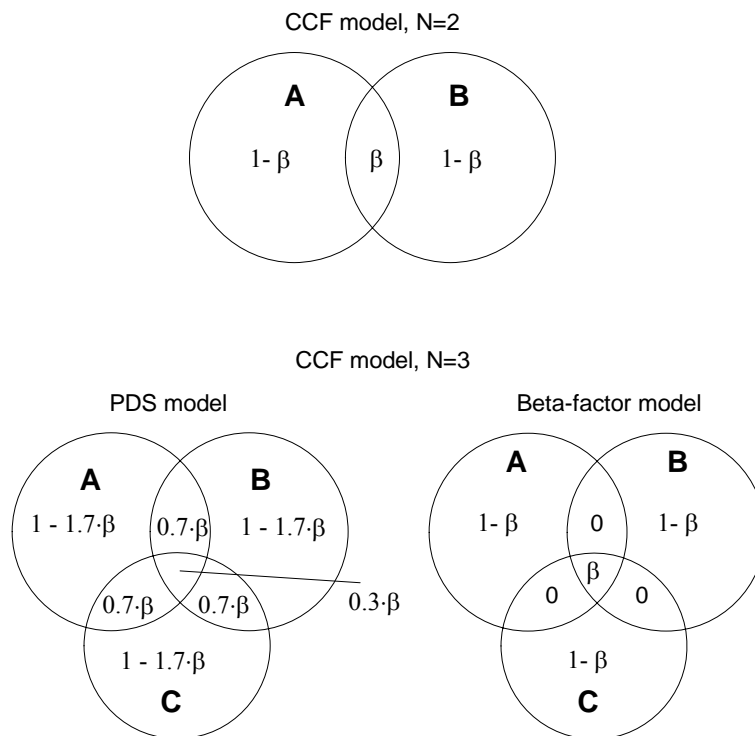


Figure 7 Illustration of the CCF model for $N=2$ and $N=3$

The difference between the IEC and the PDS approach is further illustrated in Figure 7. A circle (say A) represents the event: “component A has failed”. For a duplicated set of redundant components A and B ($N=2$), the IEC and PDS approaches are identical; Here, β represents the fraction of failures affecting both A and B, so that they fail simultaneously.

For a triplicate set of components ($N=3$), the standard beta-factor model assumes that whenever there is a failure affecting two components (say A and B) the third component (C) will also fail.

Thus, it will never happen that just two of the three components fail due to a CCF. The PDS model, however, specifies that if A and B have failed due to a CCF, C may also fail (but only in 30% of the cases). It is of course somewhat arbitrary to postulate that this fraction equals 30%, but it is, however, considered more realistic than assuming the percentage to be 100¹².

Application Specific β Models

IEC adopts a method to calculate an application or plant specific beta. This is considered a good principle and has also been adopted in the PDS method. However, the suggested IEC checklists are extensive and the questions are general for all equipment types. As part of the PDS project, a simplified application (and equipment) specific approach has therefore been developed. A further description of this new approach to determine an application specific β is given in Appendix C, section C.2.

Summary of Differences between the IEC and PDS Approach for CCF Modelling

To highlight and summarise the differences between the IEC and PDS approach for modelling of common cause failures, the following should be noted:

- In order to reflect the effect of voting, the PDS model introduces the configuration factor C_{MooN} , i.e. $\beta(MooN) = \beta \cdot C_{MooN}$;
- In PDS, a simplified approach has been developed in order to determine application specific β values (ref. Appendix C, section C.2);
- In this edition of the PDS method handbook, β and (the former) β_{SF} have been combined into one common β in order to simplify the common cause model;
- The PDS method does not distinguish between β and β_D (=beta for detected failures in IEC). The most relevant β should always be used, but the notation β_D is not used in PDS.

¹² The 30% figure and the rest of the figures in Table 2, will result in a multiplicity distribution similar to that used in the "old PDS" method. Obviously, the "true" values of C_{MooN} could be higher or lower depending on the application. Hence, the C_{MooN} values should ideally be application specific. This is, however, a potential future development of the model.

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