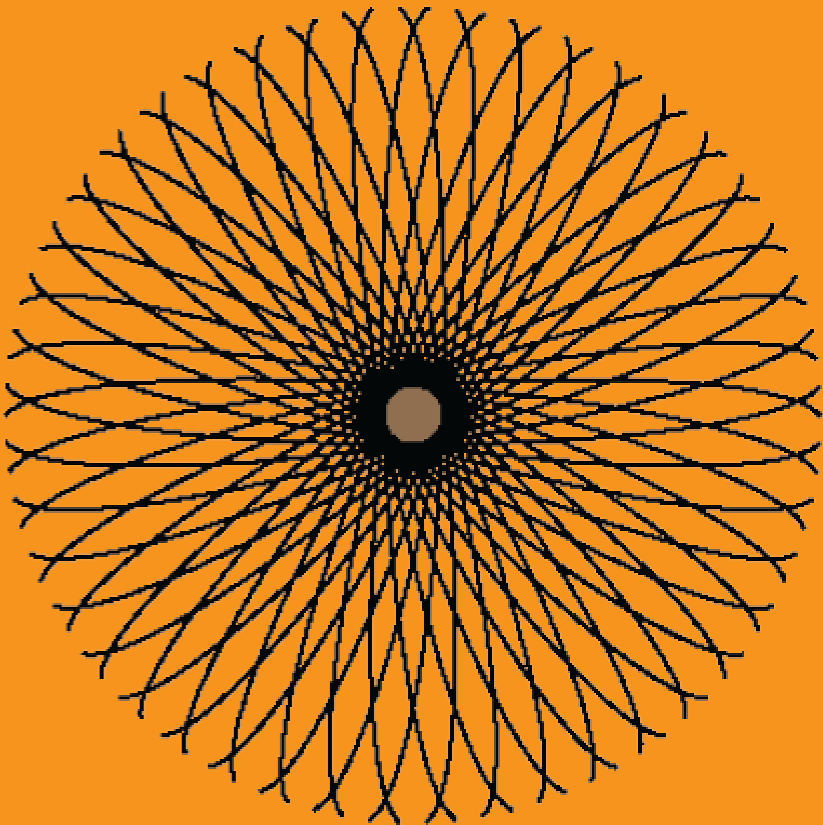
SINTEF

Reliability Prediction Method for Safety Instrumented Systems

PDS METHOD HANDBOOK 2010 EDITION



SINTEF REPORT

SINTEF

SINTEF Technology and Society
Safety Research

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 Prediction Method for Safety Instrumented Systems

PDS Method Handbook, 2010 Edition

AUTHOR(S)

Stein Hauge, Mary Ann Lundteigen, Per Hokstad and
Solfrid Håbrekke

CLIENT(S)

Multiclient - PDS Forum

REPORT NO. SINTEF A13503	CLASSIFICATION Unrestricted	CLIENTS REF.	
CLASS. THIS PAGE Unrestricted	ISBN 978-82-14-04850-6	PROJECT NO. 504091.18	NO. OF PAGES/APPENDICES 97 / 6
ELECTRONIC FILE CODE		PROJECT MANAGER (NAME, SIGN.) Stein Hauge	CHECKED BY (NAME, SIGN.) Tor Onshus
FILE CODE	DATE 2009-12-18	APPROVED BY (NAME, POSITION, SIGN.) Lars Bodsberg, Research Director	

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 presents an updated version of the PDS method. Among new features are:

- A general review and update of the methodology and the formulas, including a more in depth discussion of the assumptions underlying the formulas;
- An update of the model for common cause failures (CCF) in multiple redundant systems;
- A discussion on the use of the method for continuously (high demand mode) operating systems;
- Some new and revised terminology.

IEC 61508 and IEC 61511 have become important standards for specification, design and operation of safety instrumented systems in the process industry. The PDS method is in line with the main principles advocated in these standards, focusing on the quantitative aspects of the standards.

KEYWORDS	ENGLISH	NORWEGIAN
GROUP 1	Safety	Sikkerhet
GROUP 2	Reliability	Pålitelighet
SELECTED BY AUTHOR	Safety Instrumented Systems (SIS)	Instrumenterte sikkerhetssystemer
	Safety Integrity Level (SIL)	SIL
	IEC 61508 and IEC 61511	IEC 61508 og IEC 61511

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. PDS method and data handbooks were issued in 1998, 2003, 2004 and 2006, and the notation and approach have gradually been brought in line with functional safety standards like IEC 61508 and IEC 61511. This new and revised edition of the method handbook is mainly a result of the work carried out as part of the user initiated research project "Managing the integrity of safety instrumented systems"[1].

Trondheim, December 2009

Stein Hauge

PDS Forum Participants in the project period 2007 - 2009

Oil Companies/Operators

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

Control and Safety System Vendors

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

Engineering Companies and Consultants

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

Governmental bodies

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

[1] This project has been sponsored by the Norwegian Research Council and the PDS participants. The work has mainly been carried out by SINTEF.

Table of Contents

1 INTRODUCTION

1.1 Purpose of the Handbook

The PDS[2] method is used to quantify the safety unavailability and loss of production for safety instrumented systems (SIS). The method has been widely used in the Norwegian petroleum 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 61508, /1/ and IEC 61511, /2/. IEC 61508 provides a basis for specification, design and operation of SIS with emphasis on safety activities in each lifecycle phase of the system. The PDS method is in line with the main principles advocated in the IEC standards, and together with the PDS data handbook, it offers an effective and practical approach towards implementing the quantitative aspects of the standards. To overcome some of the weaknesses in the IEC standards, the PDS method uses a slightly different interpretation of failure classification, and suggests an alternative approach to modelling of common cause failures and how to incorporate systematic failures.

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 years. New features of this 2010 Edition of the PDS Method Handbook include:

- A general review and update of the methodology and the formulas, including a more in depth discussion of the assumptions underlying the formulas;
- An update of the model for common cause failures (CCF) in multiple redundant systems;
- A discussion on the use of the method for continuously (high demand mode) operating systems;
- Some new and revised terminology.

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.
- In chapter 4 the modelling of common cause failures is discussed.
- Chapter 5 presents calculation formulas for low demand mode systems.
- Chapter 6 presents calculation formulas for continuously operating (high demand mode) systems
- Chapter 7 presents a worked example of quantification.

Appendix A presents a complete list of notation and abbreviations used in the report. Also, a comparison between the IEC and the PDS notation is given. In Appendix B the modelling of

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

common cause failures is discussed in some more detail and in Appendix C slightly more detailed formulas than those given in chapter 5 are presented.

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

Appendix F discusses the treatment of diagnostic coverage and the 1oo2D 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 explicitly, (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?

There is an increasing reliance on safety instrumented systems (SIS) to achieve satisfactory risk levels in the process industry. Also, in other business sectors such as the public transport industry (air and rail) and the manufacturing industry, there is a major increase in the use of computer based safety systems.

Fire and gas detection systems, process shutdown systems and emergency shutdown systems are examples of SIS used to prevent abnormal operating conditions from developing into an accident. Such systems are thus installed to reduce the process risk associated with health and safety effects, environmental impacts, loss of property, and business interruption costs, /5/. In the PDS method failure of such systems is referred to as "loss of safety".

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 SIS are satisfied, and that the risk reduction actually obtained from the SIS is in line with what is required. Here, the PDS method plays an important role in predicting the risk reduction obtained from the safety instrumented functions (SIF) that are performed by the SIS.

IEC 61508 and IEC 61511 have become the main standards for design, construction, and operation of SIS in the process industry. The Norwegian Oil Industry Association (OLF) has developed a guideline (OLF guideline no. 070) to support the implementation of the two IEC standards. In the regulations from the Norwegian Petroleum Safety Authorities (PSA), /4/, specific references are given to the IEC standards and the OLF guideline. IEC 61508 allows using different approaches for quantifying loss of safety. In the OLF guideline, it is recommended to use the PDS method for this purpose.

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 for barrier control is stressed in the PSA regulations (ref. /4/). Further, both the IEC standards and the PSA regulations focus on the entire life cycle of the safety systems. In the PDS project, guidelines for follow-up of SIS in the operating phase have been developed (downloadable from the web) and procedures for updating failure rates and test intervals in the operating phase have been suggested, ref. /7/ and /8/.

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

Attempts have been made to keep the PDS method and associated formulas as simple and intuitive as possible without losing required accuracy. 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.

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.

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.
- 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 High Integrity Pressure Protection System (HIPPS) reliability studies, for onshore, offshore and subsea applications.
- In a number of SIL verification studies and preparation of Safety Analysis Reports (SAR).
- In reliability analyses of railway signalling systems (i.e. typical high demand systems).

2.4 Uncertainty in Reliability Analysis

It is important to realize that quantification of loss of safety is associated with uncertainty. This means that the results that we obtain from such analyses are not *the* true value, but rather a basis for comparing the reliability of different system designs and for trending reliability performance in the operational phase. An important objective of quantitative (and qualitative) reliability analyses is to increase the awareness among system designers, operators, and maintenance personnel on how the system may fail and what the main contributors to such failures are.

We may relate the uncertainty to:

- The model: To what extent is the model able to capture the most important phenomena of the system, including its operating conditions?
  In practice, we often need to balance the two conflicting interests:
    - The model should be sufficiently simple to be handled by available mathematical and statistical methods, and
    - The model should be sufficiently realistic such that the results are of practical relevance.

- Data used in the analysis: To what extent are the data relevant and able to capture the future performance?
    - The use of reliability data are usually based on some assumed statistical model. E.g. the standard assumption of a constant failure rate may be a simplification for some equipment types.
    - Historical performance is not the same as future performance, even for the same component. The historical performance is often based on various samples with various operating conditions and in some cases different properties (such as size, design principle and so on).
    - Data may be incomplete due to few samples, lack of censoring, and not including all type of failures, for example software related failures.
    - There is also uncertainty related to data collection, failure reporting, classification and interpretation of data

Sensitivity analyses may be performed to investigate how changes in the model and the assumed data can influence the estimated loss of safety. The use of sensitivity analyses is common practise in sectors like the nuclear industry and the aerospace industry, but has so far been given limited attention in the process industry.

3 IMPORTANT RELIABILITY CONCEPTS

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 explain the relation between the PDS and the IEC 61508 approach for quantification of loss of safety.

IEC 61508 and IEC 61511 distinguish between four levels of risk reduction, called safety integrity levels (SIL). To each SIL, the IEC standards assign a target range for loss of safety. To measure loss of safety, the standards use Probability of Failure on Demand (PFD) for low demand SIS and Probability of Failure per Hour (PFH) for high demand/continuous operating SIS. This chapter describes some of the main concepts and principles underlying the formulas for PFD and PFH, and outlines the differences between the PDS approach and the approaches in IEC 61508 and IEC 61511.

3.2 Failure Classification by Cause of Failure

Failures can be categorised according to failure cause and the IEC standards differentiate between *random hardware failure* and *systematic failures*. PDS uses the same classification, but gives a more detailed breakdown of the systematic failures, as indicated in Figure 1.

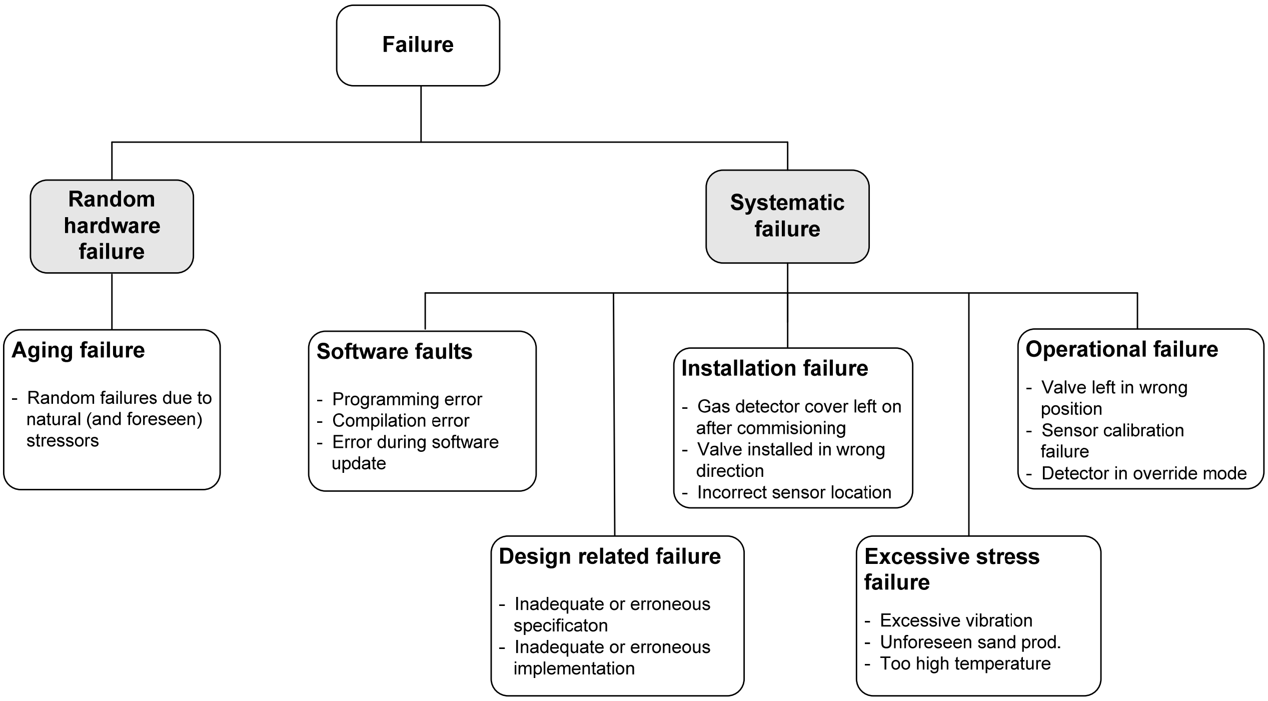

Failure
Random hardware failure
Systematic failure
Aging failure
- Random failures due to natural (and foreseen) stressors
Software faults
- Programming error
- Compilation error
- Error during software update
Installation failure
- Gas detector cover left on after commisioning
- Valve installed in wrong direction
- Incorrect sensor location
Operational failure
- Valve left in wrong position
- Sensor calibration failure
- Detector in override mode
Design related failure
- Inadequate or erroneous specificaton
- Inadequate or erroneous implementation
Excessive stress failure
- Excessive vibration
- Unforeseen sand prod.
- Too high temperature

Figure 1 Possible 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 in PDS defined as failures that can be related to a particular cause other than natural degradation and foreseen stressors. Systematic failures are due to errors made during specification, design, operation and maintenance phases of the lifecycle. Such failures can therefore normally be eliminated by a modification, either of the design or manufacturing process, the testing and operating procedures, the training of personnel or changes to documentation.

There are several possible schemes for classifying systematic failures. Here, a further split into five categories has been suggested:

- ***Software*** faults may be due to programming errors, compilation errors, inadequate testing, unforeseen application conditions, change of system parameters, etc. Such faults are present from the point where the incorrect code is developed until the fault is detected either through testing or through improper operation of the safety function. Software faults can also be introduced during modification to existing process facilities, e.g. inadequate update of the application software to reflect the revised shutdown sequences or erroneous setting of a high alarm outside its operational limits.
- ***Design related*** failures, are failures (other than software faults) introduced during the design phase of the equipment. It may be a failure arising from incorrect, incomplete or ambiguous system or software specification, a failure in the manufacturing process and/or in the quality assurance of the component. Examples are a valve failing to close due to insufficient actuator force or a sensor failing to discriminate between true and false demands.
- ***Installation*** failures are failures introduced during the last phases prior to operation, i.e. during installation or commissioning. If detected, such failures are typically removed during the first months of operation and such failures are therefore often excluded from data bases. These failures may however remain inherent in the system for a long period and can materialise during an actual demand. Examples are erroneous location of e.g. fire/gas detectors, a valve installed in the wrong direction or a sensor that has been erroneously calibrated during commissioning.
- ***Excessive stress*** failures occur when stresses *beyond* the design specification 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.
- ***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 so that the instrument does not sense the medium.

As a general rule, systematic 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. Similarly it may be argued that there is overlap between some of the failure categories. However, for the purpose of illustrating that SIS failures may have a variety of causes without introducing a too complex classification scheme, the above categories are considered sufficiently detailed.

Random hardware failures are sometimes referred to as *physical failures* whereas systematic failures are referred to as *non-physical 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 relay which due to wear out is not able to change position.

A non-physical 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 correct to state that all systematic failures are non-physical failures.

In line with the IEC standards, the PDS method has a strict focus on the *entire* safety function and therefore intends to account for *all* failures that could compromise this function. Some of these failures may be related to the interface/environment such as e.g. “vibration of pump causing a nearby transmitter to fail”. However, it is part of the PDS philosophy to include or at least to consider the possibility of having such events since they may contribute towards the unavailability of the safety system.

3.3 Quantification of Systematic Failures

Following the introduction of IEC 61508 and the accompanying SIL verification process, it has become an increasing problem that exaggerated performance claims are made by equipment manufacturers, (see e.g. /9/). Predictive analyses based on seemingly perfect operating conditions often claim failure rates a magnitude or more below what has historically been observed during operation. There may be several causes for such exaggerated claims of performance, including imprecise definition of equipment- and analysis boundaries, incorrect failure classification or too optimistic predictions of the diagnostic coverage factor, /9/. Another important reason seems to be that figures from such predictive analyses frequently exclude any possible contributions from systematic failures, e.g. failures that in one way or another can be attributed to operation rather than the equipment itself. From a manufacturers point of view this is understandable – why include failures that are not “his responsibility”? On the other hand the SIS is installed for the purpose of providing a further specified risk reduction and unrealistic failure rates can result in far too optimistic predictions.

An important idea behind the PDS method is that the *predicted risk reduction,* calculated for a safety instrumented function (SIF) in the design phase, should reflect the *actual risk reduction* that may be experienced in the operational phase. In the PDS method we have therefore argued that both the contribution from random hardware failures as well as systematic failures should, to the degree possible, be quantified. This approach differs from the IEC 61508 standard, saying that only the contribution from random hardware failures shall be quantified and that reduction and avoidance of systematic failures shall be treated qualitatively. It should, however, be noted that IEC 61508 actually quantifies part of the systematic failures through the proposed method for quantifying hardware related common cause failures (ref. IEC 61508-6, Annex D). The IEC standard also repeatedly states that the contribution from human errors should be included, although not explicitly saying how this shall be done.

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 good reasons why we should attempt to quantify the contribution from systematic failures:

- We want our risk reduction predictions to be as realistic as possible;
- Systematic failures can be the dominant contributor towards the overall failure probability (ref. failure data dossiers in /16/);

- Failure rates as given in e.g. /15/ and /16/ are often based on historic (operational) data and therefore implicitly include (at least some) systematic failures;
- When introducing measures to prevent systematic failures, these measures should (ideally) be credited in the applied failure rate estimate.

Therefore, in the PDS method we have proposed models and data for quantification of both random hardware failures as well as systematic failures. In PDS the systematic failures have been classified in two main categories:

1. Systematic failures *detectable during testing*. Examples may be a detector left in override mode at the last test, or a valve that will not close due to hydrate formation;

2. Systematic failures *not detected during testing* but occurring upon a true demand. One example may be a software error introduced during update of the program logic. Another example can be a valve that closes during regular testing but due to insufficient actuator force does not close upon a process demand situation (with high process pressure).

3.4 Testing and Failure Detection

Testing and subsequent failure detection is vital in order to reveal and remove hidden failures in the safety system. Mainly, we have three possibilities for failure detection:

- Failure detection by automatic self-tests (including operator observation)
- Failure detection by functional testing (i.e. manual testing)
- Failure detection upon process demands / shutdowns

3.4.1 Automatic Self-tests

Modules often have built-in *automatic (diagnostic) self-test* to detect failures. Typical failure modes that can be detected by diagnostics are signal loss, drifted analogue signal / signal out of range or final element in wrong position, /5/. 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 *diagnostic (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 what action is taken when the equipment fault is detected. In particular it is important to consider whether the fault initiates an automatic shutdown action or alternatively only generates a system alarm which requires an active operator response.

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 has frozen or a detector 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 allows for incorporating this effect into the diagnostic coverage factor. Typically, manual fault detection through operator observation will be relevant for field equipment whereas for control logic units, self-test will be the dominant contributor towards the diagnostic coverage. The possibility of detection by operator observation needs to be considered for each specific application; e.g. on a low- or unmanned (or subsea) installation such failure detection will obviously be more limited.

3.4.2 Functional Testing

Functional testing is performed manually at predefined time intervals and aims at testing the components involved in the execution of a safety instrumented function. In reliability analyses it is often assumed that functional testing is “perfect” in the sense that it replicates a true demand and thereby detects 100% of the failures. However, in reality the testing may be imperfect and/or the test conditions may deviate from the true demand conditions, leaving some parts of the function untested. In PDS this can be catered for by adding the probability of so called test independent failures to the PFD. This is further discussed in section 3.6.3.

Equipment may also be subject to so called partial testing, in which case a further defined fraction of the critical failure modes are subject to testing. Partial stroke testing of valves is the most known example where part of the valve functionality is tested but not the full stroke. Typically, for such a partial test, the test coverage must be estimated and applied in the reliability calculations.

3.4.3 Process Demands Serving as Testing

Generally, it has not been standard practice in reliability analyses to model demands as a means for failure detection. One obvious reason for this being that a *real* demand on the safety function can not be predicted and detection of a failure at this point will anyhow be too late!

There will however be several planned (and unplanned) shutdown events where data related to SIS performance can be recorded - either manually or automatically in the plant information management system. Such information may typically include a listing of activated equipment, result of activation and possible failure modes including response/travel times. Hence, it may be possible to utilise this shutdown information for testing purposes, thereby potentially reducing the need for manual testing.

Utilising shutdown reports as a means of testing should however be done with great care. It is paramount that the data recorded during the shutdown provides the equivalent information as obtained during a functional test. Further, it is important to identify which functions or parts of functions that are *not* activated during the shutdown and therefore need to be tested separately.

3.5 Failure Mode Classification and Taxonomy

In this section we will discuss the failure mode classification proposed in IEC 61508 and clarify some minor 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 automatic self-test, incidentally by personnel, during functional testing or upon a process demand, are split into these categories. A comparison of the IEC and PDS failure classification is illustrated in Figure 2.

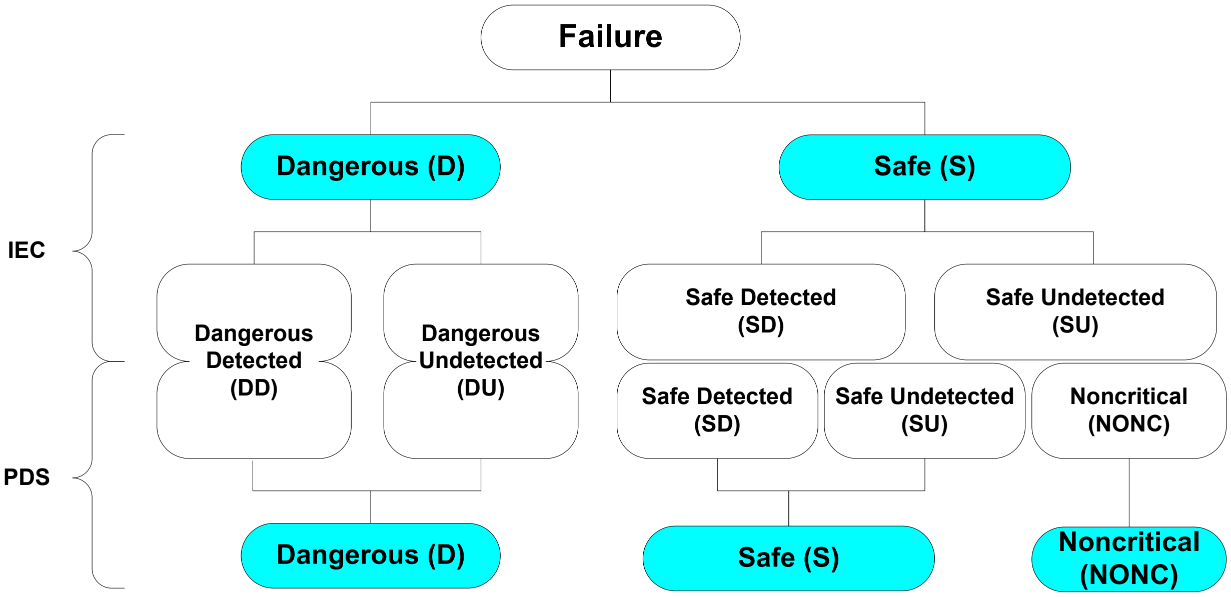


Figure 2 Failure mode classification – component level.

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”. Hence, this may be interpreted as including both spurious trip failures as well as non-critical failures (i.e. failures that do not affect any of the two main functions of the module/system[3]). In the PDS method we have therefore chosen to use a slightly different definition of safe failures; Safe failures are defined as failures *with a potential* to cause a spurious trip (i.e. failures were the safety system is activated without a demand). All other failures are defined as non-critical (NONC), i.e. they will not affect the main functions of the system.

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

- ***Dangerous (D).*** The component does not operate upon a demand (e.g. sensor stuck upon demand or valve does not close on demand). The Dangerous failures are 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.

- ***Safe (S).*** The component may operate without any demand (e.g. sensor provides a shut down signal without a true demand - 'false alarm'). The safe failures are further split into:
  - ***Safe Undetected (SU)*** The failures is not detected by automatic self-test or incidentally by personnel and therefore results in a spurious trip of the component[4];
  - ***Safe Detected (SD)*** The potential spurious trip failure is detected by automatic self-test or incidentally by personnel. Hence, an actual trip of the component is avoided.

- ***Non-critical (NONC).*** The main functions of the component are not affected. Examples may be sensor imperfection or a minor leakage of hydraulic oil from an actuator, which has no immediate impact on the specified safety function.

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

[4] Depending on system configuration a spurious trip of the system may be avoided; e.g. by using a 2oo2 voting.

The Dangerous and Safe (spurious trip) failures are considered "critical" in the sense that they affect either of the two main functions, i.e. the ability to shut down on demand or the ability to maintain production when safe. The Safe failures are usually revealed instantly upon occurrence, whilst the Dangerous failures are "dormant" and can be detected by testing or upon a true demand.

Note that although a safe failure typically results in the system going to its predefined safe state such failures are by no means without consequences. There may be associated production losses, environmental emissions caused by flaring and also the required process start-up with all of its potential hazards.

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

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

- λ_{DD} = Rate of dangerous detected failures
- λ_{DU} = Rate of dangerous undetected failures
- λ_{SD} = Rate of safe (spurious trip) detected failures
- λ_{SU} = Rate of safe (spurious trip) undetected failures
- λ_{NONC} = Rate of non-critical failures (not explicitly defined in IEC)

We also introduce:

- $\boldsymbol{\lambda_{undet}} = \lambda_{DU} + \lambda_{SU}$, which is the rate of critical failures that are undetected by automatic self-test (or by personnel in between functional tests);
- $\boldsymbol{\lambda_{det}} = \lambda_{DD} + \lambda_{SD}$, which is the rate of critical failures that are detected by automatic self-test (or incidentally by personnel, independent of functional testing).
- $\boldsymbol{\lambda_{crit}} = \lambda_D + \lambda_S$, which is the rate of critical failures; i.e. failures which unless detected can cause a failure on demand or a spurious trip of the safety function.

In addition we have the total failure rate $\lambda = \lambda_{crit} + \lambda_{NONC.}$ Table 1 and Figure 3 further illustrate how λ_{crit} and λ can be split into their various elements.

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

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

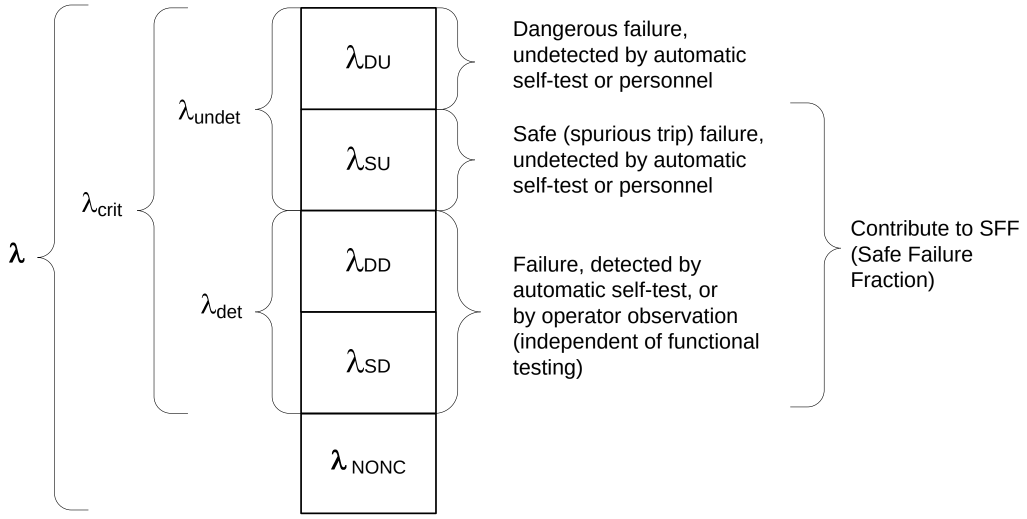

λ
λcrit
λundet
λdet
λDU
λSU
λDD
λSD
λ NONC
Dangerous failure, undetected by automatic self-test or personnel
Safe (spurious trip) failure, undetected by automatic self-test or personnel
Failure, detected by automatic self-test, or by operator observation (independent of functional testing)
Contribute to SFF (Safe Failure Fraction)

Figure 3 Failure rate λ split into various elements

3.5.1 Dangerous Undetected Failures - λ_{DU}

As discussed above, the critical failure rate, λ_{crit} is split into dangerous and safe failures which are further split into detected and undetected failures. When performing safety unavailability calculations, the rate of dangerous undetected failures, λ_{DU}, is of special importance, since this parameter - together with the functional test interval - to a large degree governs the prediction of how often a safety function is likely to fail on demand. As discussed in section 3.2 and 3.3, this λ_{DU} will include both random hardware failures as well as systematic failures.

Consequently, it is relevant to think of λ_{DU} as comprising two elements; $\lambda_{DU\text{-}RH}$ which is the rate of DU random hardware failures (i.e. the strict IEC 61508 definition of λ_{DU}), and $\lambda_{DU\text{-}SYST}$, being the rate of DU systematic failures, *detectable by functional testing*. Hence we can write; $\lambda_{DU} = \lambda_{DU\text{-}RH} + \lambda_{DU\text{-}SYST}$. Further, in PDS the parameter *r* is defined as being the fraction of λ_{DU} originating from random hardware failures, i.e. $r = \lambda_{DU\text{-}RH} / \lambda_{DU}$. Then, *1-r* will be the fraction of λ_{DU} originating from systematic failures, i.e. $1\text{-}\ r = \lambda_{DU\text{-}SYST} / \lambda_{DU}$.

Note that splitting λ_{DU} is *not* necessary when performing standard reliability calculations. This is further discussed when the calculation formulas are presented in the next sections. However, when application specific calculations are performed (ref. Appendix D), it is required to have an estimate of the fractional split between random hardware failures and systematic failures making up the total λ_{DU}.

3.5.2 Coverage Factors and Safe Failure Fraction

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

- DC = λ_{DD}/λ_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 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 will for some equipment and some installations where detected failures can be rectified quickly, be relevant also to include random observation (by 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 safe (spurious trip) failures as:

- $c_D = \lambda_{DD} / \lambda_D =$ Fraction of dangerous failures detected by automatic self tests *or* by personnel
- $c_S = \lambda_{SD} / \lambda_S =$ Fraction of safe (spurious trip) failures detected by automatic self tests *or* by personnel

Thus, as part of the *coverage* we include any failure that in some way is detected in between functional tests. It should be noted that the possibility of detecting dangerous failures will differ for different types of equipment. For control logic, failures will mainly be detected through diagnostic self-test. For valves with little or no diagnostic coverage some failures may be detected by personnel observation, whereas for process transmitters and detectors failures may typically be detected both by automatic self test and by casual observation.

Concerning the coverage factor for safe failures, c_S, the physical interpretation of this parameter seem to vary among users of the IEC standards. In PDS a safe detected (SD) failure is interpreted as a failure which is detected prior to a spurious trip, whereas a safe undetected failure actually causes a component trip (but a system trip may be avoided due to the configuration of the system, e.g. 2oo2 voting).

Finally, observe that IEC also introduces the safe failure fraction (SFF) in relation to the requirements for hardware fault tolerance. 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:

- $\text{SFF} = 1 - (\lambda_{DU} / \lambda_{crit})$; or rather in percent: $\text{SFF} = [1 - (\lambda_{DU} / \lambda_{crit})] \times 100\%$

This interpretation differs slightly from the definition given in the first edition of IEC 61508, /1/, where the $\text{SFF} = 1 - (\lambda_{DU} / \lambda)$, the reason being that IEC does not distinguish the potential difference between λ and λ_{crit} (ref. discussion above). In the committee draft for the second edition of IEC 61508, it is suggested to exclude the “no part/no effect” failures from the total failure rate when calculating the SFF, which corresponds well with the approach already used in the PDS method.

3.5.3 Summary of Differences between IEC and PDS Notation

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

- The definition of Safe (S) failures given in the present version of IEC 61508 is somewhat unclear. Therefore in PDS, failures that are not dangerous or can not cause a spurious trip has been explicitly defined as non-critical (NONC) failures (i.e. not to be included in the safe failures)
- As a result the total failure rate, λ, is split into λ_{crit} and λ_{NONC}
- In order to avoid that non-critical failures are included as part of the safe failure fraction, PDS defines this term as: $\text{SFF} = 1 - \lambda_{DU}/\lambda_{crit}$
- In PDS it is recognised that the equipment failure rate in addition to random hardware failures will include also systematic failures that can be revealed through functional testing. To

illustrate this, the λ_{DU} can be split into the rate of random hardware failure (λ_{DU-RH}) and the rate of systematic failure ($\lambda_{DU-SYST}$).

- 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 observation).

3.6 Performance Measures for Loss of Safety – low demand systems

The measures for loss of safety used in IEC are the average PFD (Probability of Failure on Demand) for low demand systems and PFH (Probability of Failure per Hour) for high demand systems. 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. Probability of failure per hour (PFH) is discussed separately in chapter 6.

3.6.1 Contributions to Loss of Safety

The potential contributors to loss of safety (safety unavailability) have in PDS been split into three main categories:

- *PFD*: Unavailability due to dangerous undetected (DU) failures.
- P_{TIF}: Unavailability due to TIF failures (test independent failures)
- *DTU*: Unavailability due to known or planned downtime

1) *Unavailability due to dangerous undetected (DU) failures*, i.e. unavailability caused by dangerous failures that are *detectable* only during functional testing *or* upon a demand (not revealed by automatic self-test). This unavailability, which is often referred to as “unknown” may be thought of as comprising two elements:
   a) The unavailability due to dangerous undetected random hardware failures (occurring with rate λ_{DU-RH}).
   b) The unavailability due to dangerous undetected systematic failures (occurring with rate $\lambda_{DU-SYST}$).

2) *Unavailability due to test independent failures,* i.e. unavailability caused by hidden dangerous failures that are *not* revealed during functional testing but only upon a true demand. These failures are denoted *Test Independent Failures* (TIF), as they are not detected through the functional test or by automatic self-test, only during a real demand.

3) *Unavailability due to known or planned downtime.* This unavailability is caused by components either taken out for repair or for testing/maintenance. The downtime unavailability can 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 time to restoration, MTTR, i.e. the time elapsing from the failure is detected until the situation is restored.
   b) The *planned* (and known) unavailability due to the downtime/inhibition time during functional testing and/or preventive maintenance.

Figure 4 attempts to illustrate the three categories of contributors to loss of safety.

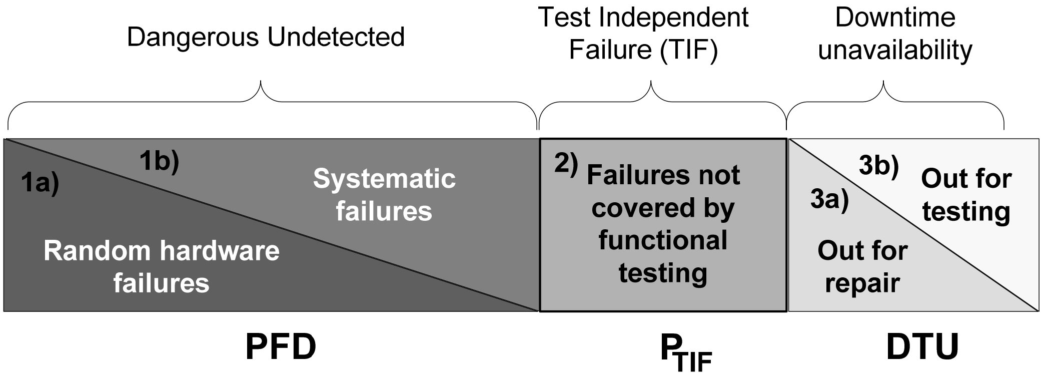


Figure 4 Loss of safety contributors in PDS

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. Often, 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 single 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 << τ. 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 Probability of Failure on Demand (PFD)

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

PFD = (Average) Probability of Failure on Demand

The PFD is therefore the average probability that the SIS is *unable* to perform its safety function upon a demand.

According to the formulas given in IEC 61508, 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 give the *known* downtime unavailability a separate notation. Therefore, in the PDS method 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 $\tau/2$ for a single component. If the downtime unavailability (i.e. category 3 above) is added, this is explicitly stated.

3.6.3 Test Independent Failures - TIF

As discussed in section 3.4.2, it is often assumed in reliability analyses that functional testing is "perfect" and as such detects 100% of the failures. In true life this is not necessarily the case; the test conditions may differ from the real demand conditions, and some dangerous failures can therefore remain in the SIS after the functional test. In PDS this is catered for by adding the probability of so called test independent failures (TIF) to the PFD.

P_{TIF} = *The Probability that the component/system will fail to carry out its intended function due to a (latent) 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. Another example is that a pressure transmitter is tested by applying a test pressure directly to the diaphragm, rather than by raising the pressure in the pipeline or vessel in which the pressure transmitter is installed.

Test independent failures will often be systematic by nature, e.g. a programming error in the application software that is not revealed since all Cause & Effects are not tested. Some test independent failure may however be classified as random hardware failures, e.g. wear and tear of a valve stem causing internal leakage that is not revealed during regular stroke testing.

The contribution from such non-perfect testing may be included in the TIF, or as is often done for e.g. partial stroke testing; reducing the functional test coverage from 100% to a lower value.

3.6.4 Downtime Unavailability – DTU

This represents the *downtime* part of the safety unavailability as described in categories 3a) and 3b) above. 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). The average duration of this period is the mean time to restoration (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 and planned maintenance (i.e. category 3b above).

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 only the DTU_R, only the DTU_T or the entire $DTU = DTU_R + DTU_T$ in the overall measure for loss of safety. This is further discussed in chapter 5.

3.6.5 Critical Safety Unavailability (CSU)

In PDS the measure Critical Safety Unavailability (CSU) is used to quantify the loss of safety:

CSU = *the probability that the component/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 61508 quantifies only the downtime unavailability which is due to component restoration time resulting from a dangerous failure (i.e. the DTU_R). No separate formula for quantification of unavailability caused by component downtime during testing and inspection is given in IEC 61508 (i.e. 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 is therefore treated separately.

The relationship between the different loss of safety measures used in PDS is presented in Figure 5.

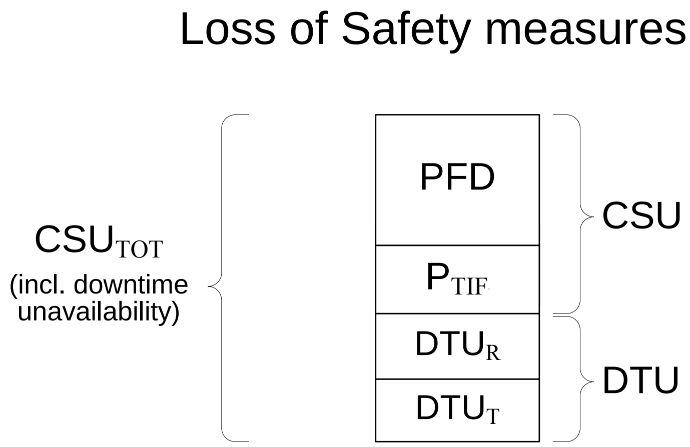


Figure 5 Loss of safety measures used in PDS

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. The figure applies for a single component and illustrates the variation in failure probability during the test period.

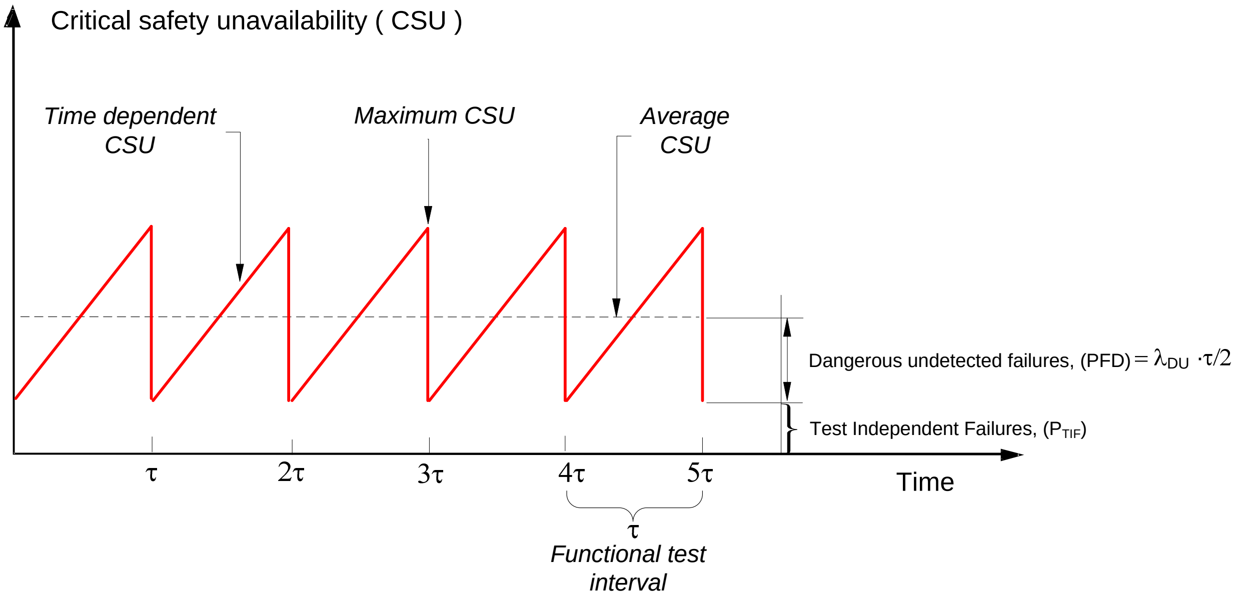


Figure 6 Contributions to critical safety unavailability (CSU)

Observe that the CSU is at its maximum right before a functional test and at its minimum right after a test. However, when we calculate the CSU and the PFD we actually calculate the average value as illustrated in the figure. As a consequence it may occur that the average CSU will fulfil a given PFD criteria although the CSU at its maximum may exceed the specified criteria.

3.7 Loss of Production

The IEC 61508 and related 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 (spurious trip). Examples may be a gas detector giving an alarm when there is no gas in the area, or a level transmitter giving a high alarm although the level is actually within normal. As discussed in previous sections such failures are classified as safe failures and depending on system configuration and whether the failures are detected or not, they may cause a spurious trip and resulting system downtime. Since loss of production and subsequent start-up situations are unwanted events, 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*:

STR = *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* 10^6 *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 on the operational philosophy during repair and testing. This is further discussed in section 5.3.4.