SINTEF

STF38 A02420
Classification: Unrestricted

Chapters 1 to 4 from:

Reliability Prediction Method for Safety Instrumented Systems

PDS Method Handbook, 2003 Edition

SINTEF Industrial Management
Safety and Reliability
March 2003

SINTEF

SINTEF Industrial Management
Safety and Reliability

Address: N-7465 Trondheim, NORWAY
Location: S P Andersens veg 5
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, 2003 Edition

AUTHOR(S)

Per Hokstad and Kjell Corneliussen

CLIENT(S)

Multiclient - PDS Forum

REPORT NO.	CLASSIFICATION	CLIENTS REF.	
STF38 A02420	Unrestricted		
CLASS. THIS PAGE	ISBN	PROJECT NO.	NO. OF PAGES/APPENDICES
Unrestricted	82-14-02707-1	384269.61	77 / 6
ELECTRONIC FILE CODE		PROJECT MANAGER (NAME, SIGN.)	CHECKED BY (NAME, SIGN.)
T:384269-PDS/Reports/ PDS Method Handbook 2003 Edition.doc		Knut Øien	Knut Øien
FILE CODE	DATE	APPROVED BY (NAME, POSITION, SIGN.)	
	2003-03-10	Lars Bodsberg, Research Director	

ABSTRACT

PDS is a method used to quantify and balance the safety and production loss of computer-based safety systems. The method accounts for all types of failure categories; technical, software, human, etc.

This report gives a new updated version of the PDS method, including the mathematical details. It has, however, also been an objective to make it comprehensible to the non-expert.

The standard IEC 61508 provides useful information and guidance on safety requirements regarding the use of Safety Instrumented Systems (SIS). In the present report the notation of the old PDS method has been changed in order to be in line with the standard. The objective has been to “keep the best of the PDS method and at the same time to adapt the method to terms and requirements in IEC”. New features of this 2003 Edition of the PDS Method Handbook include:

- New PDS terms adapted to the notation used in IEC.
- A new failure classification based on the "old PDS" method, but adapted to IEC terms and classification.
- An improved common cause failure model, which is a generalisation of the beta-factor model suggested in IEC.

KEYWORDS	ENGLISH	NORWEGIAN
GROUP 1	Safety	Sikkerhet
GROUP 2	Risk	Risiko
SELECTED BY AUTHOR	Control and Safety Systems	Regulerings- og sikkerhetssystemer

PREFACE

The PDS Forum is a forum for oil companies, vendors and researchers with a special interest in reliability of computer based safety systems. A PDS method handbook was issued back in 1989. This new and completely revised edition is carried out as the main topic of the PDS Forum in 2002. The main objective has been to update the PDS method so that the notation and approach are in line with that of the standard IEC 61508. Further, the objective has been to include new material issued in various reports after 1989. Thus, the present report depends heavily on previous work, in particular carried out by Lars Bodsberg, Ragnar Aarø and Jørn Vatn.

The modifications of the PDS approach have also been the topic at various PDS Forum meetings, and a lot of useful input has been provided at these meetings. We also received very useful suggestions to the draft version of the present report, and in particular want to thank Stian Ruud and Gjermund Våge (both DNV) for their written comments.

Trondheim, 2003-03-10

Per Hokstad

PDS Forum Participants 2002:

Oil Companies
- BP Norge
- Norsk Hydro ASA
- PPCoN
- Shell
- Statoil
- TotalFinaElf Expl. Norge AS

Control and Safety System Vendors
- ABB
- FMC Kongsberg Subsea
- Honeywell
- Kongsberg Simrad
- SAAS ASA
- Siemens
- Simrad Optronics ASA

Engineering Companies and Consultants
- Det Norske Veritas
- Kværner Oil & Gas
- Safetec Nordic AS
- Scandpower

Table of Contents

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

1 INTRODUCTION

The PDS[1] 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 the standard IEC 61508. This standard addresses the safety aspects for all lifecycle activities of such systems. The PDS method is in line with the principles advocated in the standard[2], and is a useful tool when implementing the principles of the IEC standard. The standard IEC 61508 provides useful information and guidance regarding the use of safety instrumented systems. However, the proposed failure classification and the approach for loss of safety quantification could be improved. In particular the beta(β)-factor modelling chosen for common cause failures (CCF) is unsatisfactory.

The report gives an updated version of the PDS method. The objective has been to "keep the best of the old PDS method and at the same time to adapt the method to the terms and requirements in IEC". New features of this 2003 Edition of the PDS Method Handbook include:

- New PDS terms adapted to the notations used in IEC.
- A new failure classification based on the "old PDS" method, but adapted to IEC terms and classification.
- An improved common cause failure model, which is a generalisation of the beta-factor model suggested in IEC.

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

The report is organised as follows:

- Chapter 2 includes a general discussion on safety and reliability issues.
- Chapter 3 discusses the failure classification and the reliability parameters of the "New PDS" method.
- Chapter 4 describes the treatment of common cause failures.
- Chapter 5 presents the calculation formulas; so this is a main chapter. Some of the formulas given here are approximate.
- Chapter 6 presents a worked example of quantification.

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

Appendix D presents a new generalisation of the calculation method, e.g. to handle non-identical redundant components. Appendices E-F present methods for quantifying loss of safety due to "systematic failures" (cf. IEC 61508) for software and gas detectors, respectively. These results are not new, but are here updated according to the new notation. It may be a future task for the PDS Forum to provide a more unified approach for quantifying systematic failures.

The present report focuses on the safety and reliability aspects of the PDS method, and does not handle LCC; (see /15/ for some guidance on LCC calculations).

---

[1] PDS is the Norwegian acronym for "reliability of computer-based safety systems".

[2] 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), being similar to computer-based safety systems.

2 THE NEED FOR RELIABILITY CALCULATIONS

2.1 Who Needs 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 anticipated also in other business sectors such as the public transport industry (air and rail) and the manufacturing industry. The background for this is that there are benefits in terms of cost and manufacturing flexibility, without jeopardising safety (provided the design of the computer-based safety system is adequate).

Computer-based systems may contain hidden errors that may lead to potentially disastrous system failure, perhaps after many years of correct operation. Further, it is hardly possible to construct these systems completely fail-safe. It can not be claimed that all possible failure modes are identified, and thus it can not be assured that a fail-safe response is designed for all the failure modes.

If safety is addressed in the entire life cycle of the safety systems, significant commercial advantages and reduced commercial risks can be achieved: Some examples are:

- *Access to a larger market*. The operators will demand compliance with the standards and regulations that are emerging. Not addressing these issues is likely to reduce an organisation's potential market share. Even where standards are not mandatory and there is no regulation, those who build and operate systems to a recognised standard will have a benefit that should result in increased market share.
- *Reduced litigation risks*. Systems built and operated in line with recognised practice are less likely to face litigation should an accident occur. Furthermore any costs coming as a result of such litigation may be significantly mitigated.
- *Reduced direct losses*. System failure can have a direct effect on profitability. Appropriate attention to safety reduces the likelihood of failures and can minimise the consequences of failures.
- *Reduced bad publicity*. Safety related incidents usually lead to bad publicity.

It should be verified that the safety requirements of safety systems are fulfilled, and here the PDS method plays an important role.

2.2 Benefits of Reliability Analysis

The first step towards solving a problem is to fully understand its nature. If we don’t, we may draw erroneous conclusions. Reliability analysis may be used as a systematic tool for understanding the system from a safety and production regularity point of view, and thereby understanding how to improve it.

Some main applications of reliability analysis are:

- Reliability assessment: Verifying that the system fulfils its safety and reliability requirements.

- Design optimisation: Balancing the design to get an optimal solution with respect to safety, production regularity and LCC.
- Operation planning: To establish the optimal testing and maintenance strategy.
- Modification support: To verify that planned modifications are legal with respect to the safety and reliability requirements.

Documenting safety, reliability, maintainability and/or production regularity is an important application of reliability analysis. Also, it is becoming increasingly more important to verify the quality of the products and systems in terms of their reliability attributes. IEC 61508, (ref /1/) is an example of a standard stating requirements to Safety Instrumented Systems (SIS), and this standard is currently becoming the main standard within the SIS industry. The standard sets out a generic approach for all safety lifecycle activities for SIS. IEC 61508 is a generic standard common to several industries, and the process industry is currently developing their own sector specific standard for application of SIS, called the IEC 61511 (ref /2/). Both these standards present a unified approach to achieve a rational and consistent technical policy for all SIS systems. The Norwegian Oil Industry Association (OLF) has developed a guideline (OLF guideline no. 070) to support the use of IEC 61508/61511 (ref /3/). 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 regularity. 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 is perhaps 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 may be used as a tool for verifying that the desired safety and reliability is achieved.

2.3 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 input data used.

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

- Common cause failures
- Automatic self-tests
- Functional (manual) testing
- Systematic failures (not revealed by functional testing)

- Complete systems including redundancies and voting
- All failure categories/causes.

Most methods used today do not consider all of these aspects. It should be noted that the PDS method is by no means perfect, but to quote the famous statistician George E. P. Box; “All models are wrong, but some are useful!" It is our belief that the PDS method is useful, and that by applying it a large step is taken towards more realistic analyses and trustworthy results.

Although the 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, and to bridging the gap between reliability theory and application.

Main characteristics of the PDS method
The method gives an integrated approach to hardware, software and human factors. Thus, the model accounts for all failure causes:

- Normal ageing
- Stress and environmental conditions
- Human operator interaction errors
- Design errors.

The failure taxonomy is customised to utilising input data from various data sources, see /14/:

- Corrective and preventive maintenance report systems (e.g. SAP[3])
- Failure databases (e.g.OREDA[4])
- Expert judgements.

Furthermore, the model includes all failure types that may occur, and explicitly accounts for:

- Dependent (common cause) failures
- The actual effect of all types of testing (automatic as well as manual).

The main benefit of the PDS taxonomy compared to other taxonomies is the direct relationship between failure cause and the means used to improve safety system performance.

The method is simple and structured:

- Highlighting the important factors contributing to loss of safety and spurious trip failures
- Promoting transparency and communication.

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.

[3] *Systeme Anwendungen Produkte* in der Datenverarbeitung
[4] *Offsore REliability Data*

2.4 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 to computer-based safety systems in the offshore and onshore oil and gas industry. PDS has e.g. been utilised in:

- A large number of third-party reliability verifications of offshore 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, including different combinations of high/low alarm limits, based on economic and safety assessments.
- Optimisation of the functional testing interval for offshore equipment, considering both safety and maintenance cost.
- Several HIPPS (High Integrity Pressure Protection System) studies.
- The evaluation of a new detector design (with increased self test facilities).

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 new PDS terms will as far as possible comply with those used in IEC, so that the PDS method now 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* or *spurious trip*), 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 new and old 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 refined classification, as shown in Figure 1.

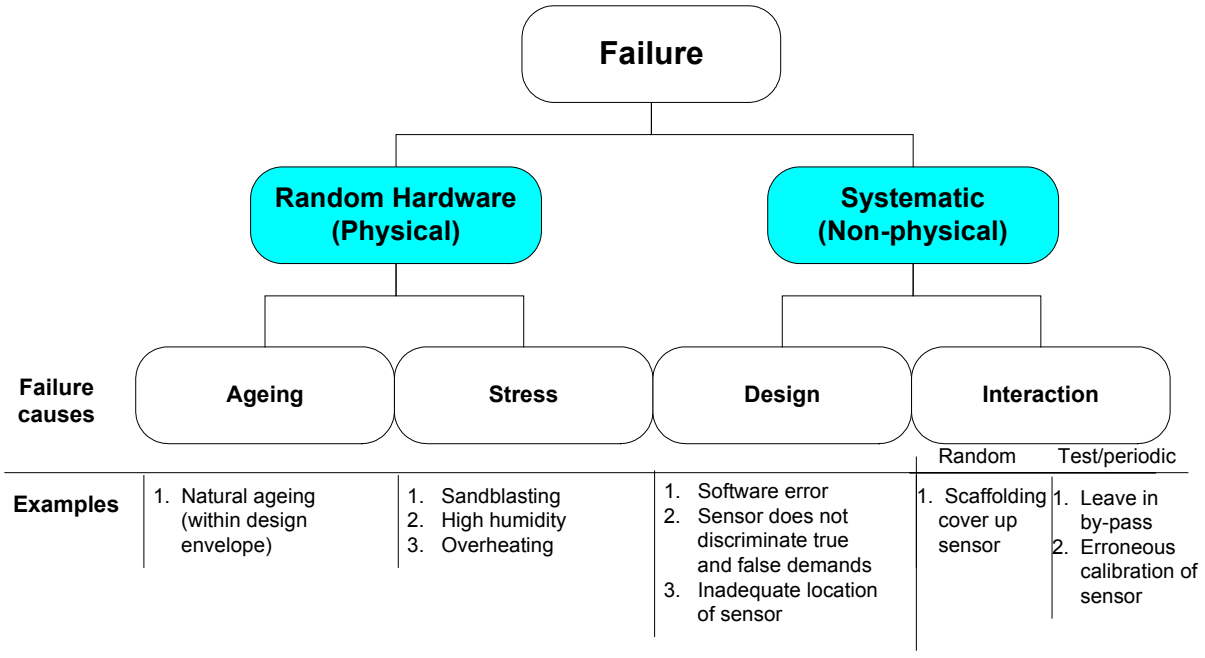

Figure 1 Failure classification by cause of failure.

As seen from Figure 1 the PDS method applies the following failure categories (causes):

- ***Random hardware failures*** are ***physical failures,*** were the delivered service deviates from the specified service due to physical degradation of the module. Random hardware failures are further split into:
  - ***Ageing*** failures, which are failures occurring under conditions within the design envelope of a module.
  - ***Stress*** failures, which occur when excessive stresses are placed on the module. The excessive stresses may be caused either by external causes or by human errors during operation. An example is damage to gas detectors due to inadequate protection during sand blasting.

- ***Systematic failures*** are ***non-physical failures***, where the delivered service deviates from the specified service *without* any physical degradation of the module. The failure can only be eliminated by a modification either of e.g. design or manufacturing process, the operating procedures or documentation. Thus, modifications rather than repairs are required in order to remove these failures. The systematic failures are further split into:
  - ***Design*** failures, which are initiated during engineering and construction and may be latent from the first day of operation. Examples are software failures, sensors do not discriminate between true and false demands, and erroneous location of e.g. fire/gas detectors.
  - ***Interaction*** failures, which are initiated by human errors during operation or maintenance/testing. Examples are loops left in the override position after completion of maintenance, and erroneous calibration of sensors during testing. Scaffolding that cover up a sensor making it impossible to detect an actual demand is another example of an interaction failure.

As a general rule it can be said that *stress*, *interaction* and *design* failures are *dependent* failures (give rise to common cause failures), while the *ageing* failures can be denoted *independent* failures.

In order to avoid a too complex classification, some of the above statements may be somewhat approximate. Not every failure may fit perfectly into the above scheme.

In the PDS method quantitative measures for loss of safety are provided for both random hardware failures and systematic failures. The IEC standard, however, suggests that only the contribution of random hardware failures should be quantified.

The PDS method has a strict focus on the *entire* safety function, and intend 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. "scaffolding cover up sensor"), rather than the safety system itself. However, it is part of the "PDS philosophy" to include such events.

3.3 Testing

The PDS method takes into account the effect of two types of testing:

- Automatic self-tests
- Functional testing.

These tests are essentially designed to detect random hardware failures. The model will account for the fact that no test is perfect.

Functional testing
Functional testing is performed manually at defined time intervals, typically 3, 6 or 12 months intervals. The functional test may *not* be perfect due to:

- **Design** failures (present from day 1 of operation) not being detected by functional testing, e.g.:
  - software errors
  - lack of discrimination (sensors)
  - inadequate location (of sensor).

- **Interaction** failures occurring during functional testing, e.g.:
  - maintenance crew forgets to test specific sensor
  - test performed erroneously (e.g. wrong calibration or component being damaged)
  - maintenance personnel forgets to reset by-pass of component.

It may also be other shortcomings in the functional testing; e.g. the test demand is not identical to a true demand, and thus some part of the function is not tested.

Automatic self-test
Modules often have built-in *automatic self-test* to detect random hardware 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* random hardware failures are detected automatically. A *fault coverage factor (Diagnostic coverage, DC)* is introduced to quantify the efficiency of the self-test. This factor equals the fraction of failures being detected by the automatic 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).

"Random" detection by personnel
In addition, an operator or maintenance crew may detect failures in between tests. For instance, the panel operator may detect a transmitter that is “stuck”. He may also detect a sensor left in by-pass (systematic failure). The PDS method also aims at incorporating this effect, and defines a coverage factor reflecting detection both by automatic self-test and operator.

Further, a spurious trip failure of a (redundant) detector, giving a pre-alarm, can allow the operator to prevent an automatic activation (trip) to occur, if specified in the operational philosophy; (one should obviously be careful when allowing such a practice). Such failures would then be part of "detected" (and not "undetected") failures.

3.4 Classification of Random Hardware Failures by Failure Mode

The IEC standard splits all random hardware failures into:
- Dangerous Undetected (DU) failures
- Dangerous Detected (DD) failures
- Safe Undetected (SU) failures
- Safe Detected (SD) failures.

Here the *safe* (S) failures (i.e. SU and SD) apparently include also *noncritical* failures, i.e. those failures that do not affect any of the two main functions of the module/system[5]. As a consequence, it is from this classification not possible to derive the rate of spurious trips, which is an integrated part of the PDS approach.

Therefore, the PDS method uses a slightly different notation (see Figure 2). The main difference is that in PDS the *safe* failures are split into *noncritical* failures (as defined above) and *spurious trip* failures (i.e. failures were the safety system is activated without a demand). For convenience we assume that all noncritical failures belong to the SU category (and thus none to the category SD).

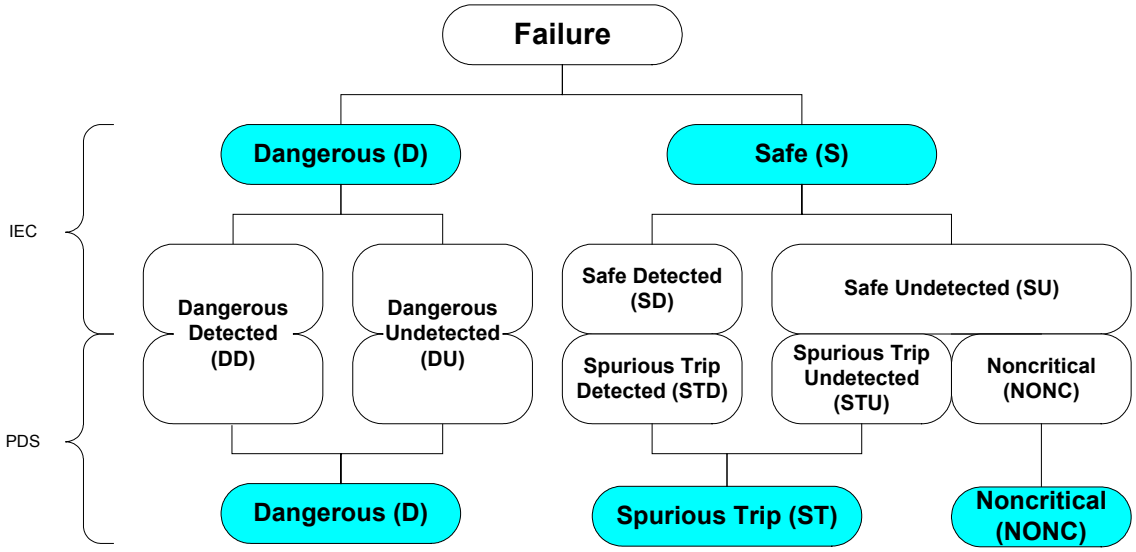

Figure 2 Failure mode classification – component level.

Hence, the PDS method considers three failure modes, dangerous, spurious trip and noncritical:

- ***Dangerous (D).*** The module does not operate on demand (e.g. sensor stuck upon demand). The Dangerous failures are further split into
  - ***Dangerous Undetected (DU).*** Dangerous failures not detected by automatic self-tests (i.e. revealed by a functional test or by demands).
  - ***Dangerous Detected (DD).*** Dangerous failures detected by automatic self-test.

- ***Spurious Trip (ST).*** The module operates without demand (e.g. sensor provides 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.
  - ***Spurious Trip Detected (STD)*** Spurious trip failures detected by automatic self-test, (depending on configuration, the detection of failure could prevent an actual spurious trip of the system).

- ***Noncritical (NONC).*** Main functions are not affected, (e.g. sensor imperfection, which has no direct effect on control path).

[5] The two main functions are the ability to maintain production when it is safe and to shut down when production is unsafe.

The first two of these failure modes, Dangerous (D) and Spurious Trip (ST) 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 a true demand.

Observe that IEC make no explicit distinction between critical and noncritical failures. However, the following interpretation applies. The safe detected (SD) in the IEC notation is identical to spurious trip detected (STD) in PDS. Further, safe undetected (SU) in IEC is here interpreted as the sum of spurious trip undetected (STU) and noncritical (NONC) used in the PDS method.

In PDS there is a focus on the critical failures, i.e. failures contributing either to loss of safety or spurious trips. So the discussion is complicated by IEC apparently defining safe failures to include also noncritical; (also the definition of "noncritical" may be less explicit, and it may not be completely clear what type of deviations to include in this concept).

Based on this classification we split the total rate of random hardware failures, λ, into the following elements:

- λ_{DD} = Rate of DD failures (same as in IEC)
- λ_{DU} = Rate of DU failures (same as in IEC)
- λ_{STD} = Rate of STD failures (= λ_{SD} in IEC)
- λ_{STU} = Rate of STU failures
- λ_{NONC}= Rate of NONC failures

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

Note that it must be further specified what to mean with *detected failure*. In the definitions given above, we adopted the IEC definition "detected by automatic self-test". This could be the main interpretation, at least when we consider random hardware failures for the logic.

However, for some modules (sensor, actuator) it may also be relevant to account for "random detection by personnel" (control room operator or maintenance crew). *If this is the case it should obviously be explicitly stated.*

As illustrated in Figure 3, we also introduce:

- $\boldsymbol{\lambda_{undet}} = \lambda_{DU} + \lambda_{STU}$ is the rate of critical failures that are undetected by automatic self-test (or by personnel in between functional tests)
- $\boldsymbol{\lambda_{det}} = \lambda_{DD} + \lambda_{STD}$ is the rate of critical failures that are detected by automatic self-test (or by personnel, independent of functional testing).
- $\boldsymbol{\lambda_{crit}} = \lambda_{undet} + \lambda_{det}$ is the rate of critical failures; i.e. failures that will cause either trip (ST) or unavailability of safety functions (D); (unless failure is detected and is prevented from causing such failure). Thus, we may also write $\boldsymbol{\lambda_{crit}} = \lambda_{ST} + \lambda_{D}$

Also, $\lambda = \lambda_{crit} + \lambda_{NONC.}$ Further, Table 1 shows how λ_{crit} is split into its various elements.

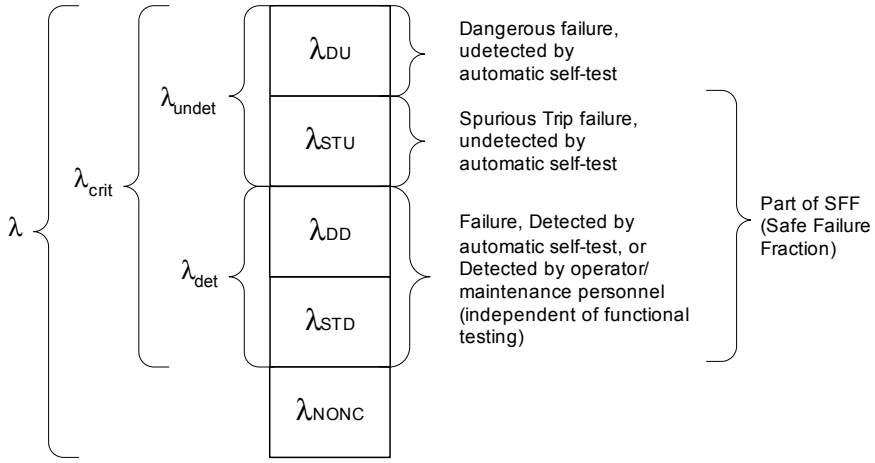

Figure 3 Total rate of random hardware failures, λ, split into various elements.

Table 1 The 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}

Coverage factors
IEC 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 also refer 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-s, and it is necessary to introduce a notation to distinguish between these. So in PDS we use:

- $DC_D = \lambda_{DD}/\lambda_{D}$ = Diagnostic coverage for dangerous (D) failures;
- $DC_{ST} = \lambda_{STD}/\lambda_{ST}$ = Diagnostic coverage for spurious trip (ST) failures, (applies in PDS only);
- $DC_S = \lambda_{SD}/\lambda_{S}$ = Diagnostic coverage for safe (S) failures;
- $DC = \lambda_{det}/\lambda_{crit}$ = Diagnostic coverage for critical failures, (applies in PDS only).

So also in the PDS method we apply the term "*diagnostic coverage*" to describe the fractions of random hardware failures that are detected in automatic self-tests. We consider DC_S to be rather irrelevant, and focus on DC_D and $DC_{ST.}$ (Observe that $DC_S = \lambda_{STD}/(\lambda_{ST}+\lambda_{NONC}) < DC_{ST}$, and further, $DC_S = DC_{ST}$ if $\lambda_{NONC} = 0$.)

As stated above, for some modules and failure modes it may be decided that "detection" shall also include "random detection by personnel" (i.e. control room operator or maintenance personnel). Then we shall refer to the corresponding fraction of detected failures as the "*coverage*". Thus, an "overall" coverage related to critical failures would be defined as

- c = λ_{det} / λ_{crit} = Fraction of critical failures detected by automatic self tests *or* by personnel.

Thus, we include as part of the *coverage, c,* any failure that in some way is detected in between functional tests.

Finally, observe that IEC also introduces SFF = Safe Failure Fraction. In PDS we use the interpretation:

- SFF = 1 - λ_{DU} / λ_{crit}; or rather in per cent: SFF = (1 - λ_{DU} / λ_{crit}) x 100%.

Strictly speaking, IEC applies the definition SFF = 1 - λ_{DU} / λ; but then we should note that the IEC standard does not discuss the potential difference between λ and λ_{crit}.

Summary of differences in IEC and PDS notation
To highlight and summarise the slight differences in the IEC and PDS notation related to failure classification, the following should be noted:

- In PDS the total random hardware 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 *noncritical* (NONC) failures.
- *Detected* (D) failures will also in PDS mean failure detected by automatic self-test, *unless otherwise explicitly stated.*
- *Diagnostic coverage* (DC) always refers to detection by automatic self-test only, (both IEC and PDS).
- *Coverage* (c) refers to any detection in between functional tests (either by automatic self-test or by personnel).
- In PDS the safe failure fraction is defined as SFF = 1 - $\lambda_{DU}/\lambda_{crit}$.
- The PDS method does not explicitly distinguish between β and β_D (=beta for detected failures). The most relevant β should always be used, but the notation β_D is not used in PDS. Unfortunately, the term β_D could also be (miss)interpreted as β for dangerous failures.
- The PDS method introduces separate betas for random hardware failure (β) and for systematic failures (β_{SF}).

Note that the last two bullets refer to the modelling of dependent failures (cf. chapters 4 and 5).

3.5 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, (the probability of not to function 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. The various measures and the relation between these will be discussed below.

3.5.1 Contributions to Loss of Safety

First consider the following potential contributions to loss of safety (safety unavailability) of a safety system (cf. Figure 1):

1) *Unavailability due to random hardware failures,* split into (cf. Figure 2):
   a) The "unknown" unavailability due to DU random hardware failures (of rate λ_{DU}). The average period of unavailability due to such a failures is $\tau/2$ (where τ = period of functional testing). In this period the failure has not been detected, and it is *not known* that the component is unavailable.
   b) The "known" unavailability due to dangerous (D) random hardware failures. The average period of unavailability due to these events equals to the mean restoration time, MTTR, i.e. 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.
   c) The "known" (or "planned") unavailability due to the inhibition time during inspection/functional testing.

2) *Unavailability due to systematic failures.* Also this unavailability is caused by "dormant" (dangerous and undetected failures). Note that all unavailability due to systematic failures is considered to be "unknown".

Observe that the contributions to loss of safety of categories 1b) and 1c) will depend on the operating philosophy, i.e. whether any action is taken when a failure is detected/revealed. This provides a good reason to treat these contributions separately and not together with 1a). Often both the contributions 1b) and 1c) are very small compared to the contribution of 1a). 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 1c) is the least critical, as this represents a truly planned unavailability of the safety system.

Below, we first introduce the loss of safety measures for random hardware failures, then for systematic failures, and finally the overall measure is given.

3.5.2 Loss of Safety due to Random Hardware Failures - Probability of Failure on Demand (PFD)

IEC uses the term

PFD = Probability of Failure on Demand

to quantify loss of safety due to random hardware failures. According to the formulas for PFD given in IEC, it is obvious that this parameter includes the contribution from both categories 1a) and 1b), see discussion in Section 3.5.1 above. In PDS it is argued that these two contributions should be shown separately:

- $\boldsymbol{PFD_{UK}}$ represents the unknown (UK) part of the safety unavailability (i.e. category 1a). It quantifies the loss of safety due to dangerous undetected failures (with rate λ_{DU}), *during the period when it is not known that the function is unavailable.* The average duration of this period is $\tau/2$, where τ = test period.

- $\boldsymbol{PFD_K}$ represents the known (K) part of the safety unavailability (Category 1b). It quantifies the loss of safety due to dangerous failures (with rate λ_D), *during the period when it is known that the function is unavailable.* The average duration of this period is the mean repair time, MTTR (or *restoration period*; i.e. time from failure is detected until safety function is restored).

Thus, $PFD = PFD_{UK} + PFD_K$.

3.5.3 Loss of Safety due to Systematic Failures – Probability of Systematic Failures (PSF)

It is an essential and rather unique feature of the PDS approach that it accounts also for systematic failures (category 2 above) when safety unavailability is quantified. This is done through the introduction of the unavailability measure:

PSF = *The Probability that a Systematic Failure causes the safety function to be unavailable*[6]*. Thus, it is the probability that the module/system will fail to carry out its intended function due to a systematic failure.*

This PSF is rather close to *the probability that a component that has just been functionally tested will fail on demand*. That is, the functional testing will not reveal and prevent many systematic failures to occur if there should be an actual demand. So for example, a PSF of 0.05, means that there is (approximately) a probability of 5% for a dangerous failure to occur on demand, even if a manual testing has just been carried out. The probability, PSF, may be an important contributor to the overall loss of safety, and the effect of this term is further elaborated in Appendices E and F.

As explained in Section 3.2, a systematic failure may be caused either by a design error or an interaction error. The interaction errors can be classified either as occurring at a "random" instant of time, or during functional testing (with interval τ). Thus, we may consider three main contributions to PSF:

- **Design Failure unavailability - PSF_{DF}**
  There is a possibility that a failure are caused by errors during engineering and construction (and may be latent from the first day of operation). Examples of design failures are software errors, lack of discrimination of sensors, and erroneous location of e.g. fire/gas detectors. In PDS this contribution to loss of safety is denoted PSF_{DF}, and is defined as the *probability that a component will fail to carry out its intended function by a true demand, due to design errors.* (Note that the design errors are *not* detected during manual testing.)

- **Random Interaction unavailability - PSF_{RI}**
  There is also a possibility that the component will not function due to some random human interaction. For instance, safety system is by-passed for some reason, or scaffolding has been set up to perform some maintenance work on a structure close to a gas detector, so that the detector would not detect a possible gas leak. This contribution to loss of safety is accounted for by the probability PSF_{RI}, defined as the *probability that a component will fail to carry out its intended function by a true demand, due to random interaction/tasks performed on (or affecting the function of) the actual SIS*. (Some of these failures may be detected by the next manual test, or earlier.)

- **Test Interaction unavailability - PSF_{TI}**
  When performing the functional test there is a possibility that a failure will be generated, e.g. because the component has been left in bypass or the sensor are covered up, or another failure has been introduced during testing/maintenance. The PDS method takes this into account by the probability PSF_{TI}, defined as the *probability that a component will fail to carry out its intended function by a true demand, due to interaction/tasks performed during testing*. (These failures are usually detected by the next manual test, or earlier.)

Thus, $PSF = PSF_{DF} + PSF_{RI} + PSF_{TI}$

[6] This has been denoted the probability of a Test Independent Failure (TIF) in earlier versions of PDS

Note that if an imperfect testing *principle* is adopted for the functional testing, this will lead to an increase of the PSF 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. Furthermore, use of a *dedicated* test gas is a contribution to the uncertainty, as testing with *process* gas has not been done. So, firstly, the possibility that specific failures (e.g. blockage of port) are *not* revealed during functional testing will lead to a higher PSF_{DF}. Secondly, the lack of "realistic" testing (e.g. detector discrimination), increases the possibility of design errors being present, and will also contribute to a higher PSF_{DF}.

Note that all systematic failures (and therefore PSF) relate to Dangerous failures. Thus, all Safe failures are classified as random hardware failures.

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

As the IEC standard suggests quantifying the contribution to loss of safety due to random hardware failures, the PDS method also include the contribution from systematic failures (see Section 3.5.3). The PDS method uses the measure Critical Safety Unavailability (CSU) to quantify total loss of safety:

CSU = *The probability that the module/safety system (either due to a random hardware or a systematic failure) will fail to automatically carry out a successful safety action on the occurrence of a hazardous/accidental event.*

Thus, we have the relation:

$$CSU = PFD + PSF$$

where still

$$PFD = PFD_K + PFD_{UK}$$

$$PSF = PSF_{DF} + PSF_{RI} + PSF_{TI}$$

To complete the discussion on safety unavailability, we should finally introduce the measure for loss of safety related to category 1c) of Section 3.5.1. Let

NSU = Noncritical safety unavailability of the module/safety system. This is the unavailability caused by functional tests, and equals the probability that it is known (actually planned) that the safety system is unavailable due to functional testing.

Neither in IEC nor PDS the term NSU will enter the standard formulas for quantification of loss of safety. In PDS it is assumed that extra precautions are taken during known unavailability of the safety system, and so this contribution to loss of safety is much less critical than the other contributions. However, a separate formula will be given to demonstrate also the magnitude of this term. Note that an overall, total safety unavailability could be defined as CSU + NSU. All potential contributions to such overall safety unavailability are presented in Figure 4. Please note that the IEC 61508 standard only discusses the term PFD.

The various contributions to CSU related to the failure classification are presented in Figure 5. So this figure (contrary to Figure 1) illustrates the classification of Dangerous failures only.

A graphical illustration of the contribution of systematic failures (PSF) and random hardware failures (PFD) to the Critical Safety Unavailability (*CSU*) is illustrated in Figure 6.

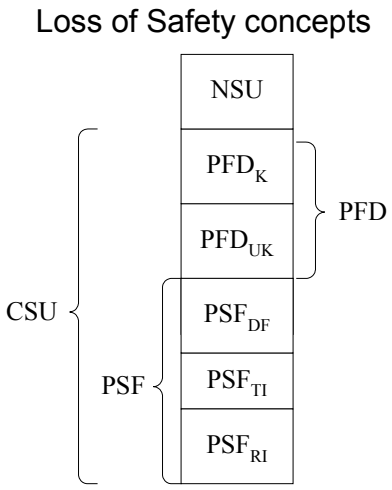

Figure 4 *Relation between loss of safety measures used in PDS.*

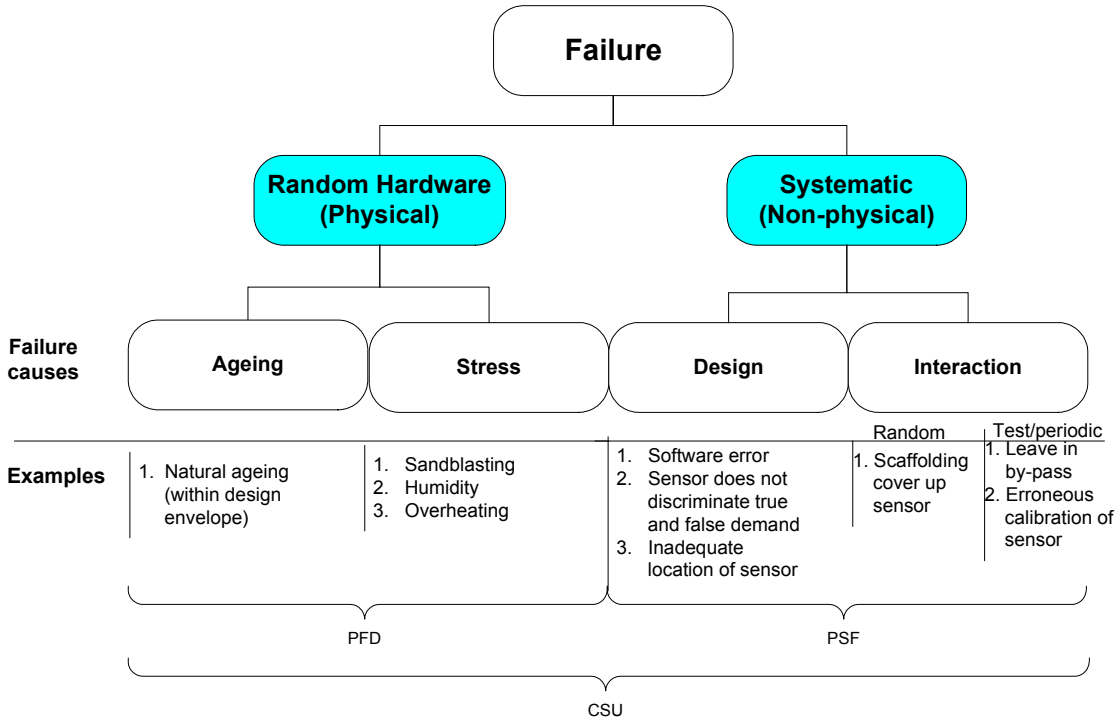

Figure 5 *Loss of safety concepts and failure classification.*

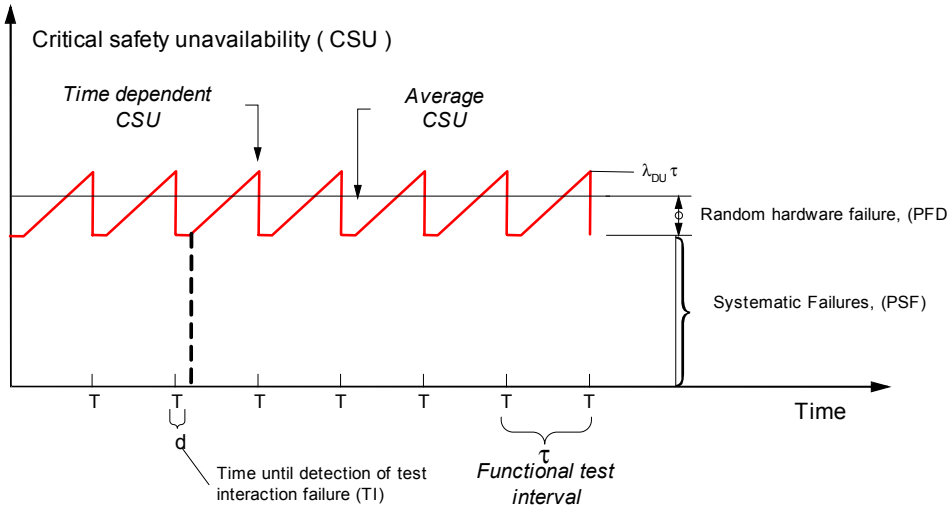

Figure 6 Contributions to Critical Safety Unavailability, CSU.

3.6 Loss of Production Regularity and Maintenance

Note that all measures for loss of production and maintenance efforts considered in this section restrict to include random hardware failures (and no potential systematic failures).

IEC focus on loss of safety only. However, there is also a possibility that the safety systems can shut down the process when there is no actual demand. 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 regularity is the *Spurious Trip Rate*:

STR = *The mean number of spurious activations of the safety system per time unit (due to random hardware failures)*

In addition, measures of the expected maintenance effort are also of interest for LCC calculations[7]. The rate of hardware failures combined with the mean man-hours spent on corrective maintenance for each type of equipment gives the quantitative reliability measure for the total corrective maintenance effort, as the *Mean Corrective Maintenance*:

MCM = *The mean number of man-hours spent on corrective maintenance per unit time.*

The rate of tests combined with the mean man-hours spent on tests for each type of equipment gives the quantitative reliability measure for the total preventive maintenance effort, as the *Mean Preventive Maintenance*:

MPM = *The mean number of man-hours spent on preventive maintenance per unit time.*

In all these three measures the time unit is usually either *per year* or *per 10^6 hrs*.

[7] LCC calculations are not included in this report. Please refer to /15/.

4 MODEL FOR COMMON CAUSE FAILURES

When quantifying the reliability of redundant systems, e.g., duplicated or triplicated systems, it is essential to distinguish between *independent* and *dependent* failures. Random hardware failures due to ageing (ref Figure 1) are *independent* failures. However, both random hardware failures due to excessive stresses and all systematic (non-physical failures) are by nature *dependent* failures (or common cause failures, CCF). Such failures can lead to simultaneous failure of more than one module in the safety system, and thus reduce the advantage of redundancy.

Beta (β)-factor model
The traditional way of accounting for common cause failures (CCF) has been the beta-factor approach. The problem with this approach is that for any M-out-of N (MooN) voting[8], (M<N), the rate of dependent failures is the same. If λ is the components failure rate, the MooN system has failure rate $\beta \cdot \lambda$. So this approach does not distinguish between different voting logics, and the same result is obtained e.g. for 1oo2, 1oo3 and 2oo3 voted systems. The reason why it still can make sense to apply this model is that the sensible reliability engineer can come around this problem by using different β-s; e.g. using β=1% for 1oo3, β=5% for 1oo2 and β=10% for 2oo3.

The approach suggested in the IEC standards (IEC 61508-6, App. D), 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 is not considered satisfactory in the PDS approach.

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

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

where C_{MooN} is a modification factor for various voting configurations, and β is the beta-factor obtained for 1oo2 voting when the IEC approach is applied.

The suggested coefficient C_{MooN} for some typical voting configurations is given in Table 2 below. The values are chosen to get "multiplicity distributions" being in agreement with the "old PDS" method; (for instance for N=3 the "multiplicity distribution" gives the probability of a single, double and triple failure; given that at least one of the three components have failed). There is of course no definite choice of these values of Table 2. Nevertheless they are expected to be far more realistic than the standard beta-factor modelling. Observe that C_{1oo2} =1, thus, for the 1oo2-voting we use the specified β-value without any modification.

One main advantage of this approach is that the β is maintained as an essential parameter. However, its interpretation is now entirely related to a duplicated system. Further, note that the effect of voting is introduced as a *separate* factor, independent of β, which makes this very simple to use in practice.

[8] 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 Modification factor for β, according to voting of channels.

Voting	1oo2	1oo3	2oo3	1oo4	2oo4	3oo4
C_{MooN}	1.0	0.3	2.4	0.15	0.8	4.0

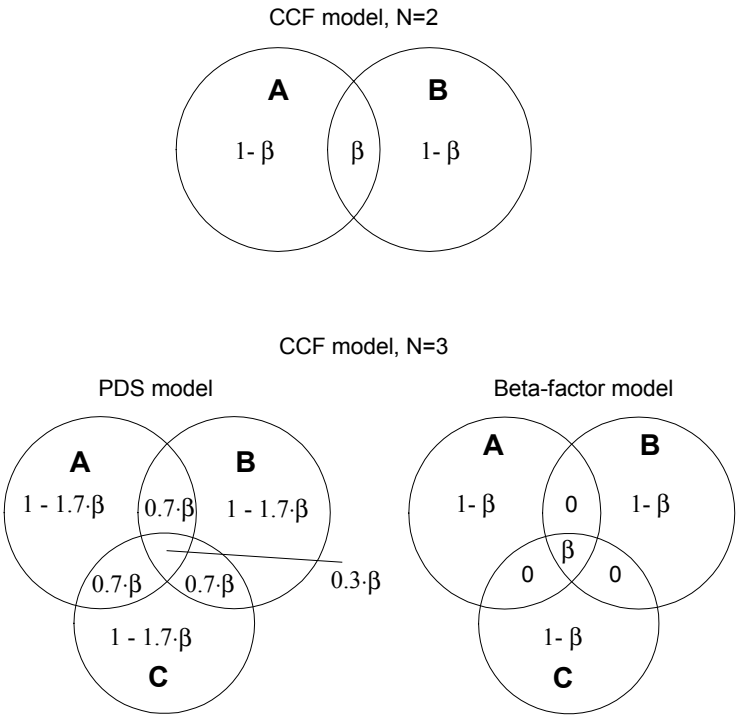

Figure 7 Illustration of CCF models for N=2 and N=3.

The difference between the IEC and PDS approach is also illustrated in Figure 7. A circle (say A) represents the event that component A has failed. For a duplicated set of redundant components A and B (N=2), the two approaches are identical. Thus, β represents the fraction of A-failure that also affects B, so that A and B fail simultaneously.

However, for a triplicated 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, also C will fail in 30% of the cases. It is of course somewhat arbitrary to postulate that this percentage equals 30%, but this is considered far more realistic than to assume the percentage to be 100%. The percentage 30% will result in a multiplicity distribution similar to that used in the "old PDS" method.

Application specific β

IEC adopts a method to calculate an application specific ("plant specific") β. This is considered a good principle, and is adopted also in PDS, see /9/, even if a simplified approach might be considered. When the PDS method is used, the β corresponding to a 1oo2 voting should be derived.

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