SINTEF A11612 – Unrestricted

REPORT

Use of the PDS Method for Railway Applications

Per Hokstad, Solfrid Håbrekke, Mary Ann Lundteigen (NTNU), Tor Onshus

SINTEF Technology and Society
Safety Research

June 2009

www.sintef.no

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 03 00
Fax: +47 73 59 28 96

Enterprise No.: NO 948 007 029 MVA

SINTEF REPORT

TITLE

Use of the PDS Method for Railway Applications

AUTHOR(S)

Per Hokstad, Solfrid Håbrekke, Mary Ann Lundteigen (NTNU), Tor Onshus

CLIENT(S)

Jernbaneverket

REPORT NO. SINTEF A11612	CLASSIFICATION Unrestricted	CLIENTS REF. Trond Daling	
CLASS. THIS PAGE Unrestricted	ISBN 978-82-14-04810-0	PROJECT NO. 60S022	NO. OF PAGES/APPENDICES 30/2
ELECTRONIC FILE CODE SluttRapport_JBV_PDS_2009.doc		PROJECT MANAGER (NAME, SIGN.) Per Hokstad Per Hokstad	CHECKED BY (NAME, SIGN.) Sture Holmstrøm S. Holmstrøm
FILE CODE	DATE 2009-06-03	APPROVED BY (NAME, POSITION, SIGN.) Lars Bodsberg, Research Director Lars Bodsberg	

ABSTRACT

This report demonstrates the applicability and usefulness of the PDS method for analysis of railway signalling systems, and suggests in particular how to account for the contribution from:

- Common cause failures,
- Self-testing and functional testing.

The report also explains how the PDS method relates to concepts and definitions that are used in IEC 61508, also taking into account the new committee draft released 2008-10-31.

KEYWORDS	ENGLISH	NORWEGIAN
GROUP 1	Safety	Sikkerhet
GROUP 2	Railway	Jernbane
SELECTED BY AUTHOR	Safety system	Sikkerhetssystem
	Quantification	Kvantifisering

TABLE OF CONTENTS

Executive summary

The PDS method provides quantification of loss of safety for safety systems; it builds on traditional theory for reliability modelling, and the following comments apply:

- *Common cause failures (CCF):* The PDS method does not, as many other modelling approaches, apply the beta factor model. In addition to the beta factor model, the PDS method applies a configuration factor (C_{MooN}), to distinguish between the effect of various voting configurations (M-out-of-N MooN). It is noted that IEC 61508 in its new committee draft has suggested a similar set of correction factors.

- *Failure classification:* The PDS method essentially uses the current IEC 61508 approach to failure classification, splitting failures into random hardware failures and systematic failures. There is one exception: In PDS a fraction of the failures are classified as non-critical (affecting no major function) and is taken out of calculations. This approach has been adopted in the new committee draft of IEC 61508.

- *Degraded operation:* The PDS method also suggests formulas for handling degraded operation. However, this is not seen to be particularly relevant for railway applications.

- *High vs. low demand mode*: Traditionally, the PDS method has focused on "low demand mode", that is quantifying safety in terms of *PFD* (probability of failure on demand). However, the present report discusses the difference between this measure and the measure suggested by IEC 61508 for high demand mode, i.e. *PFH* (probability of failure per hour). The presentation of the present report then focuses on *PFH*.

The main objectives of the report are

1. To demonstrate the applicability and usefulness of the PDS method for analysis of railway signaling systems

2. To explain how the PDS method relates to definitions and approaches that are used in (particular the new committee draft of) IEC 61508.

There are found some discrepancies in the quantification formulas of the present report (i.e. PDS) and the committee draft of IEC 61508. However, these discrepancies essentially relate to the contributions from independent failures, which in practical (railway) applications are completely dominated by the contributions from CCF.

Regarding DD (Dangerous Detected) failures it is in PDS pointed out that whether DD failures should be included or not in the quantifications, will depend on the design and operational philosophy of the signalling system. The DD failures should not be included if the system (automatically) goes to a safe state on detection of a dangerous failure, and so for railway applications it is assumed most relevant not to include DD failures. However, the PDS method as such allows for both options, (based on a discussion of the most appropriate modelling of the design and operational philosophy for the signalling system under investigation).

Therefore, the suggested calculation formulas in the current IEC draft, /2/, apply for a specific set of assumptions only, (and are not in particular adapted to railway applications). For most

configurations /2/ suggests to include contributions from DD failures. However, this seems to be handled somewhat inconsistently, as for a single system, the DD failures are not included.

The CCF modelling and failure detection modelling, which are the main elements of the PDS method are seen as rather similar to the new suggested IEC approach. This is in particular the case, as the IEC committee draft also presents a CCF method (as an alternative to the beta factor modelling), which is completely analogous to the PDS approach.

A numerical example is carried out to illustrate the method. This indicates that the CCF represent the most significant contribution to *PFH*. Further, if DD failures are included as a contribution to CCF, this could actually dominate. Thus, it is an important task to agree whether these failures are actually relevant for a specific application.

The uncertainty related to any quantification of this type is stressed; so that the result must in no way be considered as exact figures. However, the structured process of carrying out such quantification can in itself be very useful, as it obviously can point out weak parts/components, and provide comparison of different configurations.

Alternative quantification methods to the PDS method are shortly reviewed The PDS approach is based on the use of Reliability Block Diagram (RBD). Since the railway industry often uses fault trees as basis for reliability analysis, it should be noted that a RBD can always be transferred into a fault tree and vice versa. When the reliability model is established, the two approaches give the same result.

1 Introduction

The PDS method, /3/, /4/, is a method used to quantify the safety unavailability for safety instrumented systems. It has achieved a broad use, in particular in Norwegian offshore industry, see the OLF guideline, /5/. However, it has also been applied in other industry sectors, like e.g. for railway safety systems. It should be noted that the PDS method is not static; it is continuously being developed, and a series of the PDS Method Handbook has been issued. There will appear a new edition in 2009, /20/.

The PDS method is adapted (but not identical) to the calculation methods that are presented in part 6 of the IEC 61508 standard, /1/, and is even closer to the new draft version, /2/. The main objectives of this report are to demonstrate how the PDS method is applied to analysis of railway signaling systems, and to explain how the PDS method relates to definitions and approaches suggested in IEC 61508.

As this report indicates, it is not straightforward to develop a model that reflects failure detection of railway signaling system. The approach presented in this report may therefore be used as basis for further discussion and investigation by reliability analysts and researchers. However, it should be noted that these challenges are overall rather than unique for the PDS method.

Structure of the report
Chapter 2 discusses the application of the PDS quantification method for safety instrumented systems operating in the "high demand mode", and formulas for the use with railway signalling systems are presented. Comparison with the formulas presented in the new committee draft of IEC 61508 are given. The application of the formulas is illustrated by a practical example.

Chapter 3 describes alternative quantification methods, and relates these to the PDS method. Overall methods like FTA and Markov are discussed. And also alternatives to the PDS CCF modelling are reviewed; e.g. the beta-factor model and the Binomial Failure Rate (BFR) model; (both discussed in /2/).

Chapter 4 summarizes the main findings, in particular comparing the assumptions and formulas of the PDS method with those given in the committee draft of IEC 61508.

Appendix A includes a more thorough discussion of required data, in particular for the modelling of common cause failures, and Appendix B provides a list of the most important abbreviations.

2 The PDS method for safety quantification

The PDS method, as it is described in /3/, has so far been mainly used to quantify the reliability of safety instrumented systems working in *the low demand mode*. This means that most formulas and examples in /3/ are directed to such systems. A frequently used reliability measure for such systems is the (average) probability of failure on demand (PFD).

Safety functions performed by railway signaling systems can be classified as operating in the high demand mode. In this case, the reliability measure is the frequency of dangerous failures per hour, or alternatively the probability of having a dangerous failure per hour (PFH), rather than the PFD. So far, in /3/ does not give much guidance on how to calculate the PFH; however, the associated formulas may be deduced from basic reliability modeling and key principles in /3/, for example related to failure classification and common cause failure modeling.

This chapter outlines the differences in reliability calculations for high demand (continuous) mode vs. low demand mode. In the remaining part of the report we restrict to discuss high demand mode, being particularly relevant for railway applications. This chapter then describes various aspects of the PDS method:

- failure classification
- failure detection
- CCF modelling

The assumptions of the PDS method are also summarised, and a numerical calculation example is given.

2.1 Use of low demand vs. high demand mode

2.1.1 Definitions of low and high demand mode

The IEC 61508 standard, /1/ makes a distinction between so called low demand systems and high demand systems. This split and the associated definitions given in IEC 61508-4, sect. 3.5.12, have caused a great deal of confusion and discussions and is one of the aspects that has been subject to discussions in the ongoing update of the IEC 61058 standard (ref. /2/).

Roughly speaking, the two modes of operation can (at least in a historic perspective) be though of as:

- A low demand safety system operates only upon a demand, can often be seen as an add-on to the basic control system, and shall only be called upon when something goes wrong or starts to go wrong

- A high demand mode system may be a system that experiences frequent demands or more or less operates continuously. If operating continuously it can be seen more as a control system which shall prevent the process or equipment it controls from exceeding certain bounds.

For both modes, dangerous (D) failures are "dormant", and thus the D failures are not detected without performing a test or a demand occurs. IEC 61508, /1/ has defined the split between these two operating modes by saying that systems where the frequency of demands exceed one per year or greater than twice the proof test interval shall be defined as continuous mode systems. This split is however somewhat unmotivated and leaves an impression of two different types of systems that shall be treated completely different when calculating the safety level. This is not necessarily the case, and one of the topics that the IEC 61058 update committee has discussed is whether the two separate tables for low demand versus high demand systems could be merged into one common table, (however not the case in the current CDV version, /2/). Further, as seen in the preceding section, the calculation formulas for the two operating modes are essentially equivalent.

2.1.2 Quantification formulas for independent failures

In this section, we illustrate the argument by considering independent failures only. The formulas that are derived here are based on traditional reliability analysis, and are not specific for the PDS method.

The draft IEC 61508 standard, /2/ suggests two slightly different ways to measure the safety level for low demand and high demand mode of operation:

- For the "*low demand*" mode we measure safety as:
  PFD = Probability of failure on demand.
  PFD is the (average) probability that a safety system is operational (does not have a dangerous failure) upon a demand. If MDT(τ) is the mean down time over a period [0, τ], then we also have $PFD = MDT(\tau)/\tau$, (see Section B.2.2 of /2/).
- For the "*high demand*" mode we can measure safety as (see Section B.2.3.1 of /2/):
  PFH = Probability of Failure per Hour; being a rate of failures.
  If w(t) is the unconditional failure intensity at time *t,* then average PFH over an interval [0, τ], equals $PFH(\tau) = \int_0^\tau w(t)dt \,/\, \tau$, (being the average rate of failures over the interval).

The formulas for these two "modes" are completely analogous, and we shall see that there is a close relation between the two. Consider as an example a single component with rate of dangerous (D) failures, λ_D. As usual we apply the exponential failure model with constant failure rate. Then for this single component, (cf. /6/)

- $PFH = \lambda_D$ (high demand mode, single comp.)
- $PFD = 1 - [1\text{-exp}(-\lambda_D\, \tau)] \,/\, (\lambda_D\, \tau) \approx \lambda_D \cdot \tau/2$ (low demand mode, single comp.)[1]

Hence in order to obtain the PFD, we just multiply the rate PFH with the average period (τ /2) that the component will be unavailable due to a D failure.

To take a more general example, consider a 1ooN configuration[2] of N identical components, which are failing *independently,* i.e. not considering Common Cause failures, (CCF). Then it is easily shown that

$$w(t) = N\cdot[1\text{-}exp(-\lambda_D\, t)]^{N-1}\cdot\lambda_D\, exp(-\lambda_D\, t)\,, \qquad \text{(1ooN voting)}$$

which says that N-1 failures have occurred prior to time *t* and the last component fails at time *t*. Further, from this expression for *w(t)* it is easily derived that the average rate over [0, τ] equals

$$PFH_{1ooN} = [1\text{-exp}(-\lambda_D\, \tau)]^N/\, \tau \approx (\lambda_D\, \tau\,)^N/\, \tau, \qquad \text{(1ooN; independent failures only)}$$

[1] We use the standard approximation 1-exp(-λ_D τ) ≈ λ_D τ, (valid for small λ_D τ).

[2] With respect to safety, meaning that at least 1 out of N components must function to avoid system failure.

The relation between w(t) and PFH is illustrated in Figure 1. Here τ is taken as the period of functional testing, and so it is assumed that w(t) is "restarted" immediately after a test, and for a 1ooN voting with N>1 this means w(t)=0 at the beginning of each test interval.

We can actually give a simple interpretation of the above formula for PFH_{1ooN}. The term $[1-\exp(-\lambda_D\,\tau)]^N \approx (\lambda_D\,\tau)^N$ is the probability that all N units (components) fail within the same interval of length τ, resulting in a system failure. So PFH_{1ooN} equals the probability of system failure during the interval (of length τ), divided by the length of this interval.

Note that by a 1ooN (1-out-of-N) voting configuration we here mean that at least 1 out of the N components must function in order for the system to function; so it fails when all N components fail.

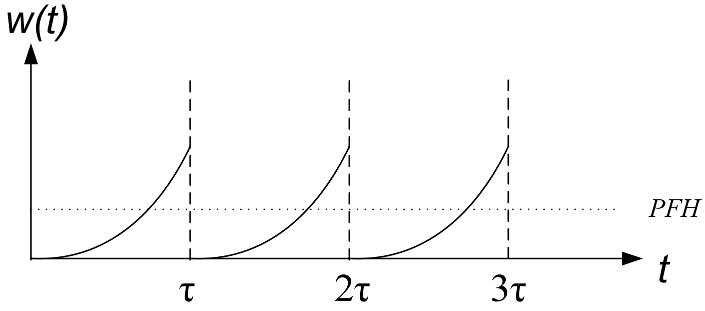

Figure 1: w(t) and PFH (N>1)

The analogous standard approximation for PFD due to independent failures in a 1ooN system equals (e.g. see Table 10.1 in /3/):

$$PFD_{1ooN} \approx (\lambda_D\,\tau)^N / (N+1), \qquad \text{(1ooN; independent failures only)}$$

Here 1/(N+1) is the average fraction of the interval τ that all N components are failed, (and thus system having a dangerous failure).

Note that PFD_{1ooN} and PFH_{1ooN} are very similar and are just two different ways to express safety. In the above example of a 1ooN voting we have [3]:

$$PFD_{1ooN} = PFH_{1ooN} \cdot \tau \,/\, (N+1)$$

Such a relation is also more generally valid, and we can easily transform the formula for the failure *probability, PFD* to a *rate* of failures, *PFH* and *vice versa*. We also note that none of these measures are restricted to be used for low demand or high demand mode only. However, there is a difference in interpretation: *PFD* is the relative time that the system is unavailable; *PFH* expresses the rate at which failures occur (irrespective of duration of the unavailability). For high reliability systems (with repair times being very short compared to *MTTF* [4]), it could seem rather arbitrary which measure is chosen. However, in our opinion *PFH* has a weakness compared to *PFD*. Using *PFH* as a measure for loss of safety it does not matter whether the failure exists in the system just for a few seconds or for days (or even weeks); it is just counted as a failure. But if a system failure is detected almost instantly, we suggest that it should not be "given the same weight" as if it remains undetected for a long period. *PFD,* however, will account for this difference in criticality.

[3] Here the factor τ/(N+1) is interpreted as the average duration of the unavailability period after a failure has occurred.

[4] Mean Time To Failure.

The description of the PDS method, /3/, focuses on the measure *PFD,* suggested by IEC 61508 for low demand mode. However, in spite of the above mentioned weakness, the present report focuses on *PFH*, since IEC 61508 suggests this for high demand mode, (which is the relevant mode for railway).

2.2 Failure classification

The failure classification of PDS mainly follows the failure classification of IEC 61508. Both approaches classify failures according to their causes and according to their effects, see Figure 2. IEC 61508 distinguish between:

- *Random hardware failures*, which are aging failures, i.e., failures that are due to natural (and foreseen) stresses. The time to failure may be modeled by a probability distribution function.

- *Systematic failures*, which are due to inadequate design, manufacturing, installation, or operation and maintenance. The time to failure may not be predicted in the same way as random hardware failures. In PDS the systematic failures are further split into(Figure 2):
  - *Software failures* e.g. due to inadequate specification or programming error.
  - *Design failures,* whose causes may be traced back to the design phase, e.g. inadequate specification,
  - Installation failures, which could be caused by wrong installation of valve or incorrect sensor location.
  - Excessive stress failures caused by stresses outside the design envelope, i.e., excessive vibration, too high temperature, unforeseen corrosive medium and so on.
  - Operational failures whose causes are associated with inadequate interaction during operation and maintenance. Examples include leaving a valve in wrong position, making a calibration error, or leaving a detector in bypass mode

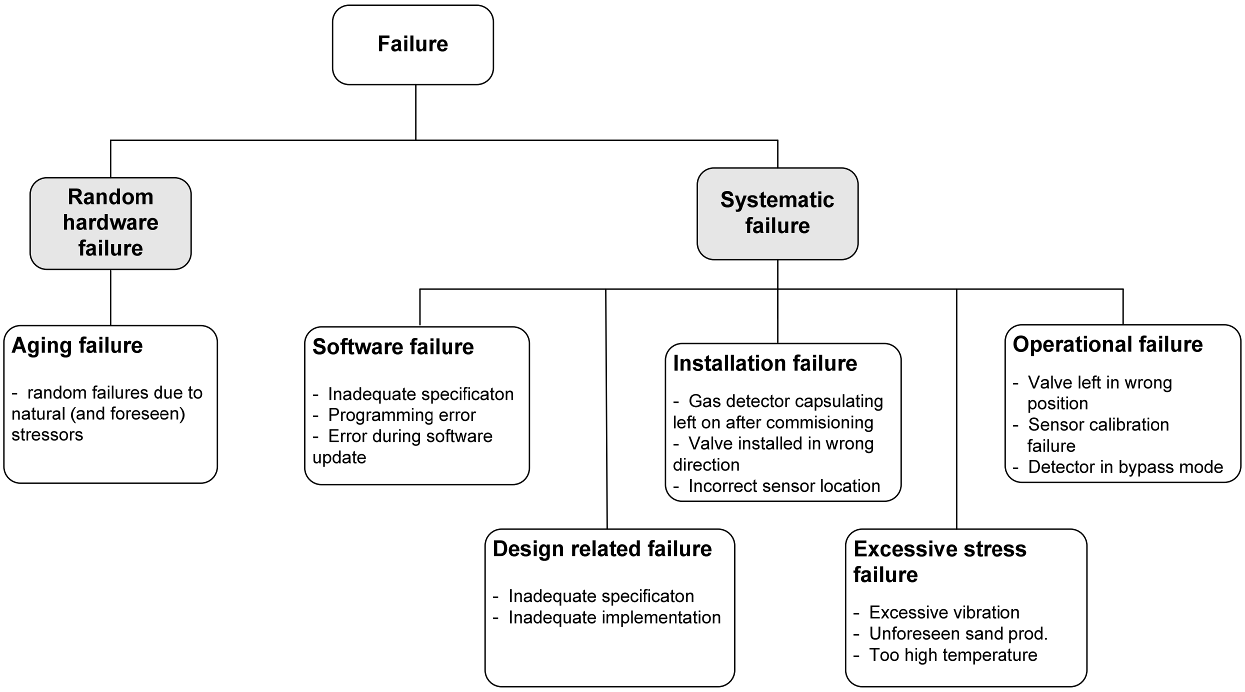
Failure
Random hardware failure
Systematic failure
Aging failure
- random failures due to natural (and foreseen) stressors
Software failure
- Inadequate specificaton
- Programming error
- Error during software update
Installation failure
- Gas detector capsulating left on after commisioning
- Valve installed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

Figure 2. Failure classification, (from /20/).

IEC 61508 requires that random hardware failures are included in the quantification of reliability, and that systematic failures, including software failures, should be handled (i.e., avoided, revealed, and corrected) by procedures. Here, the PDS method takes a slightly different approach, by introducing a probability of having test independent failures (P_{TIF}). This is further commented in Section 2.3.2.

Comment: Excluding the contribution from systematic failures is an obvious deficiency of the quantification. Without the systematic failures, we can expect that the predicted reliability (based on the data for random hardware failures) may deviate from the actual or experienced reliability, (based on the actual number of experienced failures).

Similar to IEC 61508, the PDS method distinguishes between different failure effects. IEC 61508 classifies failures (or failure modes) as either:

- Dangerous (D): A failure that has the potential to put the safety-related system in a hazardous or fail-to-function state.
- Safe (S): A failure that does not have the potential to put the safety-related system in a hazardous or fail-to-function state.

Both safe and dangerous failures are further split into detected and undetected failures, i.e.

- DU = Dangerous Undetected
- DD = Dangerous Detected
- SU = Safe Undetected
- SD = Safe Detected

An undetected failure is a failure that is hidden (or dormant) until there is a real demand or a functional test, whereas a detected failure is revealed prior to this point, by self-testing (diagnostics).

Both DU and DD failures contribute to the unreliability of the safety instrumented function: In particular, the DU failures to the unknown unreliability, and the DD failures to the known unreliability when operating in degraded mode. It is often assumed that a DD failure is repaired within short time (a few hours), and if we use *PFD* as a measure for loss of safety, this means that the contribution from DD failures, compared to the contribution from DU failures, is negligible.

When we use PFH as a measure for loss of safety it could be a more difficult question to what extent DD failures shall be included in the quantification. In our opinion the new committee draft of the IEC 61508 standard is somewhat inconsistent at this point; see below.

Safe failures include spurious operation failures, i.e. failures that lead to the execution of a safety function of a component (e.g., red light signal) without the presence of a demand. It is sometimes debated whether or not such transitions are safe, as they may cause unnecessary stress on components, on the operators (e.g., train drivers), and added risk during the restoration of the process.

Safe failures also include various types of failures that do not have any effect on the safety instrumented system. In the PDS method, such failures are classified as non-critical failures, a concept that seems to have been adopted in the new committee draft of the IEC 61508 standard.

The discussion of the present report focuses on DU and DD failures.

2.3 Failure detection and the effect on safety

The dangerous failures of safety systems are "dormant", i.e. there are detected either by some kind of testing or by demands. Mainly, we have three methods for failure detection:

- Automatic self test (diagnostic testing) at period, τ_1
- Functional testing, at period, τ
- Demands

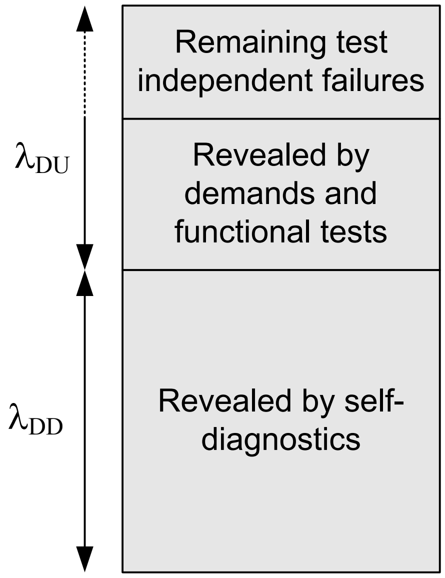
Remaining test independent failures
Revealed by demands and functional tests
Revealed by self-diagnostics
λ_{DU}
λ_{DD}

Figure 3. Failure detection and the classification of rate of dangerous failures, $\boldsymbol{\lambda_D = \lambda_{DU}+\lambda_{DD}}$

All three types of tests contribute to the detection of dangerous failures in the way that is illustrated in Figure 3. For simplicity we assume that essentially the same failures are detected by functional tests and demands. Observe that, in principle the PDS method opens for the possibility that some DU failures are neither detected by demands or functional tests. Most other approaches assume that the coverage of these tests are 100%.

2.3.1 Automatic self test

The PLC components are subject to automatic self test with diagnostic coverage, DC. Then we split λ_D into

$$\lambda_D = \lambda_{DU} + \lambda_{DD}, \quad \text{where } DC = \lambda_{DD} / \lambda_D.$$

Here, we distinguish between the rate of DU (dangerous undetected) failures, λ_{DU}, and the rate of DD (dangerous detected) failures, λ_{DD}.

For a 1ooN system without CCF (common cause failures) the contribution to *PFH* from failures detected by automatic self test, i.e. DD failures, equals $(\lambda_{DD}\,\tau_1)^N / \tau_1$. In many applications the period of diagnostic testing, τ_1 is very short, (i.e. essentially continuous testing), and this contribution to *PFH* is negligible, (for N>1). However, (unless τ_1 is *very* low), this should be checked by calculation; further see Section 2.4, below.

It is worth noting that the DC of a single component may be improved when it is inserted in a redundant system subject to comparison between redundant branches.

2.3.2 Functional testing

Functional testing aims to test all components involved in the execution of a safety instrumented function, for example to secure a rail section. Presently, the PDS method relates functional testing to the manual testing on an offshore installation, performed with an interval equal to e.g., $\tau = 6$ months. This testing principle is different from what is used for railway signaling systems.

For railway signaling systems, the functional tests must be performed more often to achieve a sufficient level of safety. For this reason, all objects involved in securing a rail section are tested as part of a train passing request. A functional test, simulating a train passing request. is performed automatically for objects that have not been activated by a train passing during a period of for instance 24 hours. Thus, for railway signaling systems, $\tau = 24$ hours may be considered as a (typical) functional test interval.

The functional testing (as demands) is often assumed to be “perfect”, (i.e. detecting 100% of the failures). However, the PDS method also allows for a non-perfect functional testing by adding the contribution P_{TIF}[5] to PFD; which is the probability that the system will not function on a demand occurring immediately after a functional test has taken place. This failure probability could be caused by systematic failures (software; inadequate testing) or by failure of maintenance personnel to carry out testing/maintenance correctly.

Example (“test independent failure”): Consider the testing of gas detectors at an oil and gas installation. Such detectors are often tested with test gas rather than hydrocarbon gases (to avoid the risk of ignition), often through a hose going into the detector chamber rather directly exposure at the detector head. In this case, the test is not able to reveal wrong location of the detector and if the detector head is covered with dust or dirt.

Further analysis may be required if “test independent failures” is an issue also for railway signaling systems. In the present report we will not proceed on this question, but point out the possibility of the PDS method to model functional testing to be imperfect.

Now assuming the coverage of functional testing to be 100%, the contribution from DU failures to *PFH* for a 1ooN voting (without CCFs), approximately equals $(\lambda_{DU}\,\tau)^N / \tau$.

We note that an additional test interval, in addition to the interval of automatic selftest and the interval of functional test can easily be included in the modeling. There could for instance be a third test with test interval 1 year. This could be modeled in exactly the same way as the two test introduced above. For each test the following should be documented as a basis for the modelling:

- Which functions, objects and components are tested?
- How often are they tested?
- What types of failures are detected by the test; (what is the coverage)?

2.3.3 Demands (train passings) serving as testing

It is not so common to model demands as a means for failure detection. However, in offshore applications of PDS demands have in some cases been considered as “functional tests”, thus in reality reducing the period of functional testing.

[5] TIF = Test Independent Failures; (Failures not detected in functional tests).

In railway applications, we should also consider demands (train passings) as additional tests particularly since each train passing request and rail section securing involve a continuous confirmation of correct operation of the components.

Assume that, on the average, there are k train passings affecting a certain object in a secured rail section in between each functional testing. This means that the average time between "tests" can be seen as τ/(k+1). However, the additional "tests" are occurring more randomly, and will not have the same efficiency as if they very evenly spread (with identically same interval). In practice, it is as an approximation suggested to include demands into the automatic self-test term, by replacing τ with 2 τ/(k+1) in the formula for *PFH;* (if this modeling is adopted we of course have k>0, and if k =1 this conservative suggestion actually gives no credit for the train passing).

2.4 Total quantification result for independent failures (1ooN voting)

From the previous section, the overall result for a 1ooN voting, considering the effect of independent failures only, now equals

$$PFH_{1ooN} \approx (\lambda_{DU}\tau)^N / \tau + (\lambda_{DD}\,\tau_1)^N / \tau_1 \qquad \text{[for 1ooN voting, without CCF]} \qquad (1)$$

Here τ can be modified according to the number of train passings affecting a specific safety function, (Section 2.3.3), and so the contribution from demands is included in the first term. Note that possible failures that are not detected in functional testing (or train passing) are not included in the above formula, cf. Section 2.3.2.

Relevance of MTTR
Note that in the above equation (1), there is no term for repair/restoration time, (e.g. MTTR = total time elapsing from a component failure is detected, until it is again fully operative). This is the case since *PFH* is a measure of frequency of failures (and not unavailability), and since it is here assumed that "degraded operation" does not apply for railway operation.

Accounting for DD failures in the calculations
The second term of (1) with the contribution from DD failures can often be ignored. In general this will depend on the "operational philosophy", as discussed for PFD in /3/. However, when loss of safety is measured by *PFH*, we simply take a numerical check to compare the order of magnitude of the "DU term" and the "DD term". The DD term is insignificant if the period of automatic self test (incl. train passings) is very short compared to τ, and we do not have $\lambda_{DD} >> \lambda_{DU}$; (i.e. if $\lambda_{DD}\,\tau_1 << \lambda_{DU}\,\tau$).

Note: If we take a look at the above formula (1) for the case *N*=1, we get $PFH_{1oo1} = \lambda_{DU} + \lambda_{DD}$ (independent of any test period!). So here the above argument related to the length of τ_1 does not apply. However, for a single system IEC 61508 requires that a safe state should be achieved by detection of a dangerous failure, and therefore gives $PFH = \lambda_{DU}$ for 1oo1, (see Section B.3.3.2.1 of /2/). As we comment below, it is unclear why this argument to remove the DD term apparently applies only for the 1oo1 voting.

Comparison with the most recent formulas in IEC 61508, /2/, (independent failures).
Section B.3.3.2 (Informative) of the committee draft, /2/ gives formulas for *PFH* for standard configurations, like 1oo2, 2oo3 etc. We presently restrict to consider independent failures, and these IEC formulas deviate from the above formula (1), except for the case N=1, as discussed in the *Note* above.

- The IEC standard uses (1-β) λ_{DU} where PDS suggests to simply use λ_{DU}. This is a conservative approximation often applied in PDS. However, this is not essential, and the factor (1-β) could of course be introduced also in the PDS quantifications, (and often is).

- Further, the IEC formulas actually includes MTTR (through the term t_{CE}), which is not included in the above PDS formula for *PFH*. As stated above, from our understanding of railway operation, MTTR terms should not be included in *PFH*, as there is no degraded operation of the safety system during repair of a single critical component. Thus, MTTR contributes to system unavailability but not frequency of dangerous system failures.

- Actually, the contribution from independent failures in the suggested quantification formulas of Annex B in /2/, also in other respects differs from the very simple expression given in the above equation (1). However, the exact derivation of the formulas in /2/ is not given, and is not pursued in the present report; cf. discussion in /19/.

In conclusion, the PDS formula with respect to independent failures deviates from the formulas presented in /2/. The discrepancies will, however, in most practical applications have no actual effect on the total result, as the contributions from CCF will dominate in the quantifications.

2.5 CCF modeling

In safety critical systems we often introduce redundancy to increase the availability of the system. However, the common cause failures (CCFs) may cause two or more redundant units to fail "simultaneously" and thus reduce the effect of redundancy. For redundant systems, the loss of reliability and safety is often dominated by the occurrence of CCFs, and these failures therefore need to be taken proper care of in the reliability models.

2.5.1 Some basic definitions

For the further discussion it may be useful to repeat some of the definitions on dependent failures and common cause failures. Somewhat pragmatically we suggest the following definitions:

- *Independence* between two components (or systems) A and B: Given the information that unit A has failed this will not change our prediction of when unit B will fail, and vice versa:

- *Dependence* between two components (or systems) A and B: Given the information that unit A has just failed; this will change our prediction of when unit B will fail.

- *CCF*: Failure of two or more (redundant) components of the same cause, occurring simultaneously or within a rather short time interval.

- *β-factor*: The fraction of common cause failures among all failures of a component, /6/.

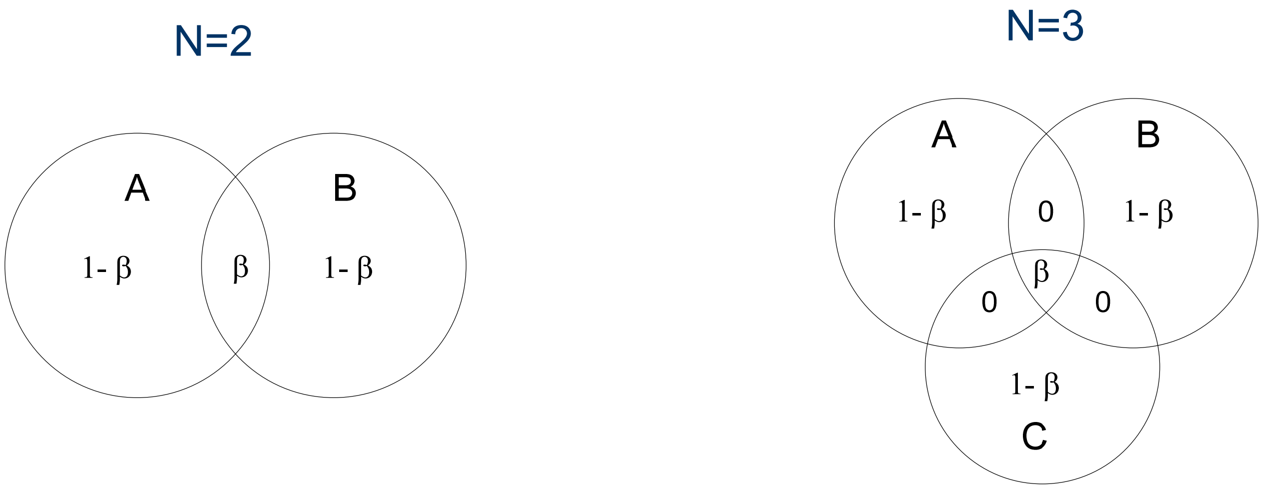

Figure 4. Illustration of the beta factor model for N=2 and N=3 identical components.

Hence, in the so-called beta factor model, a fraction, β of the component failure rate λ is introduced, resulting in all redundant components to fail, see Figure 4 (for N=2 and N=3). That is, the rate of all N (similar) components failing due to a CCF equals:

$$PFH_{sys} = \beta \cdot \lambda \quad (N>1)$$

This model is simple and easy to understand but has some obvious weaknesses:

- It will not allow a "double" CCF to occur in a triplicated system, and so on.
- Thus it will not distinguish between configurations like 1oo2, 1oo3 and 2oo3: all three configurations will have the same rate of CCF, which is rather unrealistic.
- It will also be problematic to estimate β from actual data, as there can actually occur double failures in a triplicated system (N=3), and so on.

So the beta factor model is OK for N=2 components in parallel, but will not provide a proper ranking of the various voting logics, (which of course is an essential feature of the safety modeling!)

2.5.2 The PDS model for CCF

From the beginning of CCF modelling in the 1970-s, the modelling has focused on the so-called beta factor (β-factor) due to its simplicity as discussed above. The β-factor model is also the model suggested in the present revision of the IEC 61508 standard, /1/.

As an attempt to improve the β-factor model and make it more realistic for systems with higher degree of redundancy, SINTEF has developed a modification of the model, as described in the PDS method handbook, ref. /3/.

One difference between the PDS approach and the current IEC 61508 approach is the use of the so called C_{MooN} (configuration) factors. This is a correction factor that reflects the fact that when going from a simple redundant 1oo2 system to another voting configuration, e.g. 1oo4 or 1oo5, this needs to be reflected in the applied common cause failure rate. In other words, an important reason for including the C_{MooN} factors is that credit shall be given when increasing the redundancy from two to more components, (and result should also depend on the voting of these redundant components).

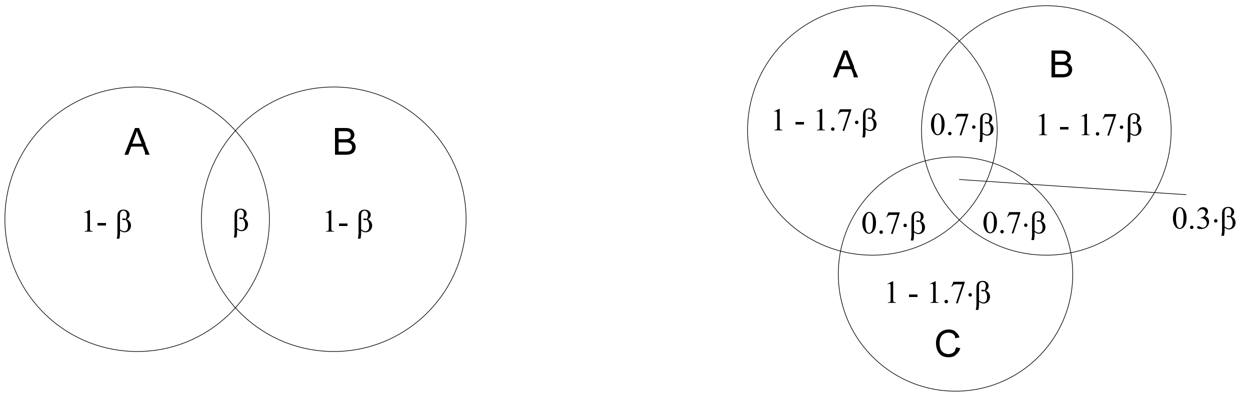

Figure 5. **PDS model for CCF, (N=2 and N=3)**

In the CCF model of PDS, β represents the fraction of CCF between any two redundant components (see Figure 5). When going from a 1oo2 to a 1oo3 voting, three components instead of two components must fail to get a system failure. This, as illustrated in Figure 5, three components voted 1oo3 has a smaller probability than two components failing (1oo2). Formally, in the PDS model the rate of system CCF for a MooN configuration of N identical components with rate λ equals:

$$PFH_{MooN} = C_{MooN} \cdot \beta \cdot \lambda, \quad \text{for M<N,} \quad \text{[for MooN voting M<N; CCF only]}$$

Suggested values for some configuration factors, C_{MooN}, are given in /3/:

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

When having systems (like e.g. the ABB Merkur system), where we have up to five redundant protection layers, the IEC 61508 standard *does not* provide an answer on which formulas to apply. It does not make sense to apply the beta factor model directly for a 1oo5 (or 1oo4) voting as this would lead to the same result as a 1oo2 voting. This obvious deficiency of the standard beta factor model has been recognized by the IEC 61508 working committee, and the new committee draft /2/ includes C_{MooN} factors, however, with slightly different values than in the PDS method. These values are further commented in Appendix A, and in the forthcoming version of the PDS method handbook, /20/, the C_{MooN} factors will also be modified.

2.6 Total quantification formulas for CCF

In PDS the CCF contribution from a MooN voting (accounting for both DU and DD failures) now equals:

$$\mathrm{PFH}^{(\mathrm{CCF})}_{\mathrm{MooN}} \approx \mathrm{C}_{\mathrm{MooN}}(\beta \cdot \lambda_{\mathrm{DU}} + \beta_{\mathrm{D}} \cdot \lambda_{\mathrm{DD}}) \qquad \text{[for MooN voting, M<N; CCF only]} \tag{2}$$

where β and β_D is the beta factor for DU failures and DD failures, respectively. In PDS it is common *not* to distinguish between β and β_D, but of course the method allows for this, (if it is found relevant to include the DD term).

Note that in PDS the DD term is usually not included, cf. discussion in Section 2.4. But there should be a thorough discussion (based on design and operational philosophy), whether or not to include DD terms. However, it is our opinion that the IEC draft, /2/, is inconsistent at this point. Since it does not include the DD term for 1oo1 voting, (see above), it is found strange that it includes $\beta_D\lambda_{DD}$ in the suggested formulas for a MooN voting when N>1.

2.7 Reliability Block Diagram and overall quantification formulas

The first step of a reliability analysis is to develop a thorough description of the system supported by an architectural model and/or functional block diagram. This information is used to construct a reliability model, where the purpose is to model events and components that contribute to system success, alternative system failure.

A reliability block diagram (RBD) is a success-oriented network describing a specified system function and can be applied as an alternative to a fault tree. RBD shows the logical connections of (functioning) components needed to fulfil the system function.

The way *n* components are interconnected to fulfil a specified system function may be illustrated by a reliability block diagram as illustrated in Figure 6. Each of the components is illustrated by a block in the diagram. When we have connection between the end points *a* and *b*, we say that the specified system function is achieved.

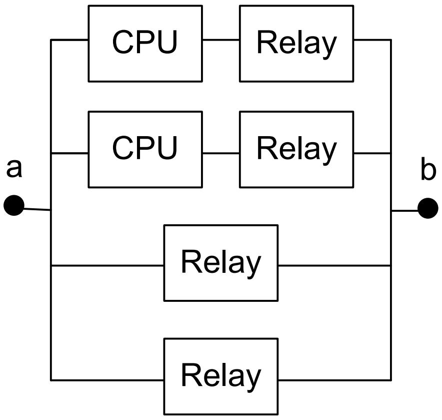

Figure 6: Example of RBD

Two important structures of a reliability block diagram are a series structure and a parallel structure. These are illustrated in Figure 7 below. A system that is functioning if and only if all of its *N* components are functioning is called a *series structure or N-out-of-N, (NooN);* see left part of Figure 7). A *parallel structure or 1-out-of-N (1ooN) structure* (right in Figure 7) is a system that is functioning if at least 1 out of the *N* components is functioning. In general a MooN structure is functioning if at least *M* of its *N* components is functioning. Often, we can simplify the RBD to approximate it with a series structure of *MooN* structures; That is, inputs have one voting configuration, CPUs another, etc., and we can obtain the total loss of safety by *adding* the contributions of these. For *MooN* votings where *M<N*, the independent failure contribution is often negligible compared to the CCF contribution, but this must be verified.

Analysis of RBD is presented e.g. /6/. A detailed description of RBD is to find in the standard, IEC61078 (2006).

Note that a RBD can always be transferred to fault tree and vice versa. When the model is established, the two approaches give the same result. However, when constructing a fault tree, we focus on how a function may fail rather than how the function may be achieved. This failure oriented approach is therefore considered more comprehensive and complete than RBD, features that are appreciated for safety instrumented systems with complex interactions. The construction of a fault tree could be a supplement to the PDS approach, see Section 3.1.1.

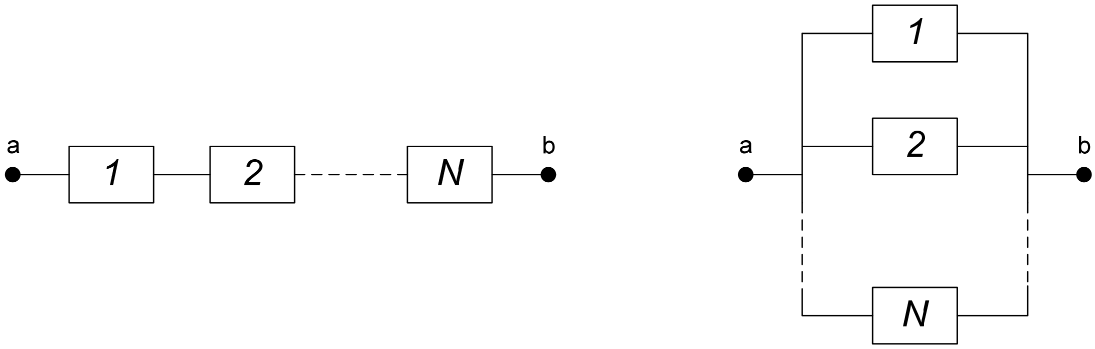

Figure 7. The RBD of a series structure, NooN, (left), and parallel structure, 1ooN, (right).

Now we summarise main PDS formulas for quantification of loss of safety by *PFH*. We split the contributions to the system *PFH* in the contribution from CCF and independent failures (ind.) as follows

$$PFH_{sys} = PFH^{(ind)} + PFH^{(CCF)} \tag{3}$$

Accounting both for DU failures and DD failures, the approximate contribution from *independent failures* of a MooN voting equals, (cf. equation (1) for the case M=1)[6],

$$\mathrm{PFH}_{\mathrm{MooN}}^{(\mathrm{ind})} \approx \frac{N!}{(N-M+1)!\cdot(M-1)!}\cdot\left[(\lambda_{\mathrm{DU}}\cdot\tau)^{N-M+1}/\tau + (\lambda_{\mathrm{DD}}\cdot\tau_1)^{N-M+1}/\tau_1\right] \tag{4}$$

where τ is the functional test interval, and τ_1 is the self-test interval. (The analogous formula for *PFD* is given in /3/.)

The CCF contribution from a MooN voting(M<N) was given in eq. (2) above:

$$\mathrm{PFH}_{\mathrm{MooN}}^{(\mathrm{CCF})} \approx \mathrm{C}_{\mathrm{MooN}}(\beta\cdot\lambda_{\mathrm{DU}} + \beta_{\mathrm{D}}\cdot\lambda_{\mathrm{DD}})$$

As discussed above, in PDS it is often found to be an appropriate approximation to exclude the DD terms, and in that case we get:

$$\mathrm{PFH}_{\mathrm{MooN}}^{(\mathrm{ind})} \approx \binom{N}{M-1}\cdot(\lambda_{DU}\cdot\tau)^{N-M+1}\frac{1}{\tau} \qquad \text{(DU terms only)} \tag{5}$$

$$\mathrm{PFH}_{\mathrm{MooN}}^{(\mathrm{CCF})} \approx C_{\mathrm{MooN}}\cdot\beta\cdot\lambda_{\mathrm{DU}} \qquad \text{(DU terms only)} \tag{6}$$

[6] Note that we often write $\frac{N!}{(N-M+1)!\cdot(M-1)!} = \binom{N}{M-1}$

2.8 Summary of assumptions

Some important general assumptions and limitations of the PDS method are given below (analogue to assumptions are made in the IEC standard):

- Exponential failure model, i.e. all failure rates are constant with respect to time. [standard assumption]
- A component is considered “as good as new” after a repair or a functional test (period τ). [standard assumption]
- System in a safe state during repair.
- For CCF, the DC is interpreted as the fraction of D failures detected before any train is operated by the system, (this DC could be lower than DC for independent failures). This will imply that DD will not contribute to system rate of D failures.
- The PFH of the function (safety system) is obtained by summing the PFH of each (series of / set of) redundant modules(s). That is we assume that PFH_A and PFH_B are small enough to let: $1\text{-}(1\text{-}PFH_A) \cdot (1\text{-}PFH_B) \approx PFH_A\text{+}PFH_B$
- The term $\lambda_{DU} \cdot \tau$ should be small enough to allow $e^{-\lambda DU \cdot \tau} \approx 1 - \lambda_{DU} \cdot \tau$, i.e. $\lambda_{DU} \cdot \tau \leq 0.2$

In addition assumptions and limitations concerning each analysis must be evaluated; e.g. regarding testing, data uncertainty and system modelling.

2.9 Numerical example

This section gives an example of the application of the PDS quantification method for the system illustrated by the RBD of Figure 6. The figure illustrates an example system, the RBD showing four parallel branches. The “Relay” is common for all branches (similar components in parallel) and must be considered as a CCF contribution. In addition, for the upper two branches the CPU is common, where also a CCF contribution must be considered. Including these CCF contributions as blocks in the RBD, we get the RBD shown in Figure 8.

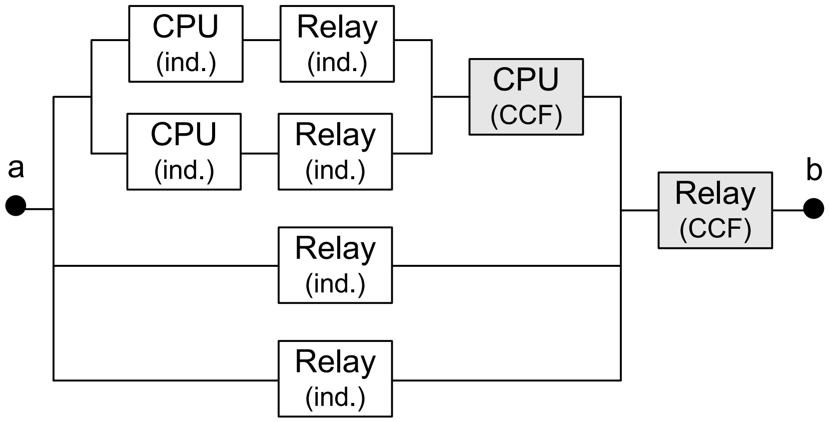

Figure 8: RBD of numerical example

The total rate of system failures can be written (eq. (3))

$$PFH_{sys} = PFH^{(ind)} + PFH^{(CCF)}$$

It should be noted that the CCF contribution for this system is the CCF of the four relays. The CCF of the CPUs becomes a part of the independent *PFH*, as if such a CCF occurs the system is still functioning.

When we estimate $PFH^{(ind)}$ we will first estimate the independent failure of the two upper branches (branches 1 and 2) with one CPU and one relay each. Then the CCF of the CPUs is added, giving a joint figure for the upper two branches. Finally, this figure is multiplied by the PFH for the two lower branches (branches 3 and 4), i.e.

$$\mathrm{PFH}^{(\mathrm{ind})} = \mathrm{PFH}_{\mathrm{branches\,1\,and\,2}} \cdot \mathrm{PFH}_{\mathrm{branch\,3}} \cdot \mathrm{PFH}_{\mathrm{branch\,4}}$$

This gives the following expression for the system PFH:

$$\mathrm{PFH} = \left[\left(\mathrm{PFH}^{(\mathrm{ind})}_{\mathrm{DU,CPU}} \cdot \tau + \mathrm{PFH}^{(\mathrm{ind})}_{\mathrm{DU,Relay}} \cdot \tau\right)^2 / \tau + \mathrm{PFH}^{(\mathrm{CCF})}_{\mathrm{DU,CPU}}\right] \cdot \left[\mathrm{PFH}^{(\mathrm{ind})}_{\mathrm{DU,Relay}} \cdot \tau\right]^2 / \tau + \mathrm{PFH}^{(\mathrm{CCF})}_{\mathrm{DU,Relay}} \qquad (7)$$

Detailed calculations are given below. In the first simplified example only DU failures are considered, i.e. DD failures are neglected, (and the formulas (5) and (6) are used).

Calculation 1: Excluding DD failures, using PDS formulas.
The input data used in this example case is listed in the table below:

Component	**τ**	**λ_{DU}**	**β**
CPU	24 *h*	$0.1 \cdot 10^{-6}$ h^{-1}	0.05
Relay	24 *h*	$0.2 \cdot 10^{-6}$ h^{-1}	0.02

The C_{MooN} factors used in the estimation are the suggested factors from the PDS handbook, i.e. C_{1oo2} equals 1 and C_{1oo4} equals 0.15. Further, we do not account for train passing between each test interval, (i.e. k=0 , ref. section 2.3.3).

The independent failures of one CPU and one Relay respectively are, using the formula (5):

$$\mathrm{PFH}^{(\mathrm{ind})}_{\mathrm{DU,CPU}} = \lambda_{DU,CPU} = 0.1 \cdot 10^{-6} h^{-1}$$

and

$$\mathrm{PFH}^{(\mathrm{ind})}_{\mathrm{DU,Relay}} = \lambda_{DU,\mathrm{Re}lay} = 0.2 \cdot 10^{-6} h^{-1}$$

The common cause failure of the two CPUs is, using (6):

$$\mathrm{PFH}^{(\mathrm{CCF})}_{\mathrm{DU,CPU}} = C_{1oo2} \cdot \beta_{\mathrm{CPU}} \cdot \lambda_{\mathrm{DU,CPU}} = 1 \cdot 0.05 \cdot 0.1 \cdot 10^{-6} h^{-1} = 5.0 \cdot 10^{-9} h^{-1}$$

And the common cause failure of the four relays is:

$$\mathrm{PFH}^{(\mathrm{CCF})}_{\mathrm{DU,Relay}} = C_{1oo4} \cdot \beta_{\mathrm{Relay}} \cdot \lambda_{\mathrm{DU,Relay}} = 0.15 \cdot 0.02 \cdot 0.2 \cdot 10^{-6} h^{-1} = 6 \cdot 10^{-10} h^{-1}$$

Thus, the estimate for the system PFH is as follows, putting the above estimates into (7):

$$\mathrm{PFH} = \left[\left(\mathrm{PFH}^{(\mathrm{ind})}_{\mathrm{DU,CPU}} + \mathrm{PFH}^{(\mathrm{ind})}_{\mathrm{DU,Relay}}\right)^2 + \mathrm{PFH}^{(\mathrm{CCF})}_{\mathrm{DU,CPU}}\right] \cdot \left[\mathrm{PFH}^{(\mathrm{ind})}_{\mathrm{DU,Relay}}\right]^2 + \mathrm{PFH}^{(\mathrm{CCF})}_{\mathrm{DU,Relay}} =$$

$$\left[\left(0.1 \cdot 10^{-6} h^{-1} \cdot 24h + 0.2 \cdot 10^{-6} h^{-1} \cdot 24h\right)^2 / 24h + 5.0 \cdot 10^{-9} h^{-1}\right] \cdot \left[0.2 \cdot 10^{-6} h^{-1} \cdot 24h\right]^2 / 24h + 6 \cdot 10^{-10} h^{-1}$$

$$= \underline{6 \cdot 10^{-10} h^{-1}}$$

From the calculations we see that the contribution from independent failures (including the CCF of the CPUs) is negligible compared to the contribution form the CCF of the four relays. As discussed above it is often found that contribution from CCF dominates over independent failures, especially for configurations with more than two redundant branches.
Given the assumptions in section 2.8, the estimated PFH for the example system is $6 \cdot 10^{-10}$ per hour, i.e. approximately one system failure per 20 000 year.

Note that this figure just gives the contribution from DU failures, as DD failures have been ignored in the calculations.

Sensitivities of calculation 1
As a sensitivity we could also apply the C_{MooN} values suggested in the IEC 61508 draft version (i.e. table D.5 in part 6, ref. /2/). For $C_{1\mathrm{oo}4}$, the new draft standard suggests 0.2 (instead of 0.15 as used in PDS). This will increase the results above with a factor of 4/3.

Further, we could also account for train passings as tests; assuming k>0. However, as the independent failures are completely dominated by CCF, there is no need to perform this additional calculation, (which would reduce the contribution from independent failures even more.

Calculation 2: Including DD failures, using PDS formulas.
Now, we estimate the *PFH* value including DD failures, assuming the following data, (τ, λ_{DU} and β as above):

Component	τ	τ_1	λ_D	**DC**	λ_{DD}	λ_{DU}	β_D	β
CPU	24 *h*	0.1 *h*	$1.0 \cdot 10^{-6}$ h^{-1}	90 %	$0.9 \cdot 10^{-6}$ h^{-1}	$0.1 \cdot 10^{-6}$ h^{-1}	0.01	0.05
Relay	24 *h*	0.1 *h*	$1.3 \cdot 10^{-6}$ h^{-1}	85 %	$1.1 \cdot 10^{-6}$ h^{-1}	$0.2 \cdot 10^{-6}$ h^{-1}	0.01	0.02

Detailed calculations are not shown for independent failures her, but as in the above calculations, the independent contribution becomes negligible compared to the CCF contribution from the relays.

The common cause failure of the four relays using (2) now becomes:

$$\mathrm{PFH}^{(\mathrm{CCF})}_{\mathrm{D,Relay}} =$$
$$C_{1\mathrm{oo}4} \cdot (\beta_{\mathrm{Relay}} \cdot \lambda_{\mathrm{DU,Relay}} + \beta_{\mathrm{D,\,Relay}} \cdot \lambda_{\mathrm{DD,Relay}}) =$$
$$0.15 \cdot (0.02 \cdot 0.2 \cdot 10^{-6} h^{-1} + 0.01 \cdot 1.1 \cdot 10^{-6} h^{-1}) = 0.15 \cdot (0.4 \cdot 10^{-8} h^{-1} + 1.1 \cdot 10^{-8} h^{-1}) =$$
$$0.15 \cdot (1.5 \cdot 10^{-8} h^{-1}) = 0.2 \cdot 10^{-8} h^{-1}$$

We see that in this case when we have chosen to include the DD failures, these will dominate. In fact the DD contribution makes 73 % of the total PFH figure for the system.

To illustrate the calculation of an independent PFH, we have calculated the contribution from a 1oo2 voting of CPUs:

$$\mathrm{PFH}^{(\mathrm{ind})}_{1\mathrm{oo}2,\,\mathrm{CPU}} \approx \frac{2!}{(2-1+1)!{\cdot}(1-1)!}\cdot\left[(\lambda_{\mathrm{DU,\,CPU}}\cdot\tau)^{N-M+1}/\,\tau+(\lambda_{\mathrm{DD,\,CPU}}\cdot\tau_1)^{N-M+1}/\,\tau_1\right]=$$

$$(0.1\cdot 10^{-6}\cdot 24h^{-1})^2\,/\,24h+(0.9\cdot 10^{-6}\,h^{-1}\cdot 0.1h)^2\,/\,0.1h=2.4\cdot 10^{-13}+8.1\cdot 10^{-14}\;=3.2\cdot 10^{-13}$$

which is smaller than the CCF contribution to the overall PFH with a factor about 10^{-5}. Furthermore, since the RBD regarding independent failures actually has 3 (4) branches in parallel, (cf. Figure 8), the contribution of independent failures to the overall PFH is even much less than this result for the 1oo2 voting.

These two calculations illustrate that the discussion whether or not to include DD failures is indeed important. However, this discussion is not about making a choice between PDS and IEC approaches, but about clarifying the design and operational philosophy of the system, (cf. discussion of /2/ regarding 1oo1 referred above).

Finally, consider the result that would be obtained, using suggested formulas in the IEC draft /2/.

Calculation 3: using IEC formulas.
The IEC draft, /2/ gives no formulas for 1oo4, which is most relevant in the present example. However, from the formulas given for 1oo2 and 1oo3, it is clear that the CCF contribution will equal, (here in PDS notation)[7]:

$$\mathrm{PFH}^{(\mathrm{CCF})}_{1\mathrm{oo}4} \approx \mathrm{C}_{1\mathrm{oo}4}(\beta\cdot\lambda_{\mathrm{DU}}+\beta_{\mathrm{D}}\cdot\lambda_{\mathrm{DD}})$$

This is identical to the general PDS formula, and in particular to the formula used for Calculation 2 above. However, /2/ provides no discussion on whether the DD term shall be included, and also suggests another value for $C_{1\mathrm{oo}4}$. The “C-factor” given in /2/ equals $C_{1\mathrm{oo}4} = 0.3$, as compared to $C_{1\mathrm{oo}4} = 0.15$ used in the above PDS quantifications[8]; (cf. Appendix A of the present report).

Regarding the contribution from independent failures, /2/ gives rather complex formulas, cf. discussion in Section 2.4 above, and it is not clear which is the exact formula that IEC would suggest for a more complex configuration like the one illustrated in Figure 8. However, it is clear that also in the IEC approach the contribution to PFH from independent failures will be completely dominated by the CCF contribution, (cf. numerical illustration in Calculation 2 above).

Thus, the conclusion is that the IEC formulas will give essentially the same formula as PDS, when DD failures are included. However, the suggested input values can differ. If we apply the same τ, $\lambda_{\mathrm{DU},}$ λ_{DD} , *β and* β_{D} as in Calculation 2 above, the IEC calculation will give the numerical result

PFH = 0.4 10^{-8} h^{-1}

i.e. twice the result of Calculation 2. The reason is that the value of the “C-factor” here is twice the value of the suggested C-factor in the current PDS method handbook, /3/. If the standard beta factor model is applied, we get PFH =1.5 10^{-8} h^{-1}.

[7] If the standard beta factor model is applied, we insert $C_{1\mathrm{oo}4} = 1$.

[8] The forthcoming update of the PDS Method Handbook, /20/, will suggest $C_{1\mathrm{oo}4} = 0.3$ as the “generic value”.

2.10 Uncertainty in safety quantification

It is important to realize that safety quantification is associated with uncertainty. This means that the results that we obtain from such analyses are not *the* true value, but rather an indication and a basis for comparing the reliability of different system designs. One of the most important objectives of quantitative (and qualitative) analyses is to increase the awareness among system designers, operators, and maintenance personnel to 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?
  - Reliability data are usually expressed by statistical models, and a failure rate gives not the exact time between failures, but the *mean* time between failures. Even with a mean time between failures of 100 years, the next failure may occur tomorrow.
  - Historical performance is not the same as future performance, even for the same component. The historical performance is often based in 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.

Regarding data, there may in particular be considerable uncertainty about the values of model parameters like the β-factor and the C_{MooN} factors:

- In the new CDV draft version of IEC 61508, /2/, C_{MooN} values for modifying the β-factor for different MooN voting configurations are proposed (ref. new part 6 – table D.5). This approach is fully in line with the PDS approach, even if the modification factors suggested in the standard deviates somewhat from the values suggested in PDS. The main point is that the CCF model provides a ranking of the various configurations with respect to safety (and the ranking in /2/ is very similar to that of PDS).

- It is correct, as is with the new proposed values in IEC 61508 (part 6 – table D.5), that the C_{MooN} factors have not been validated by field experience but are based on expert judgements. However, as is clearly seen (in /3/ and the above Table from /2/) several of the C-factors are > 1, so the approach as such is neither conservative nor non-conservative, it is just considered somewhat more realistic (as confirmed by data) than the model suggested in the present version of IEC 61508. See Appendix A for further discussion.

An obvious limitation in the quantification approach suggested by IEC 61508 is the exclusion of application software failures and other *systematic failures* from the analysis as application software can be the main contributor to unreliability.

The technology development has made it possible to replace traditional hardware implemented functions with software implemented functions. As the contribution from software failures is excluded from the quantification, we may expect that it will become easier and easier to fulfill the quantitative SIL 4 requirement, alternatively another specified target for tolerable hazard rate. This is an area that may need more attention in the future.

3 Alternative quantification methods

In this chapter we review some alternatives to the PDS quantification approach. We mainly restrict to discuss models suggested in the Draft IEC standard, /2/). We start with commenting on the overall reliability modelling, and further discuss various options for the CCF modelling.

3.1 Overall modeling approaches

There are a couple of alternatives to the RBD modeling approach being used in PDS. Below we shortly discuss the use of Fault Tree Analysis (FTA) and Markov analysis. However, note that the degree of approximations in the modeling and the modeling of CCF and failure detection have a much greater impact on the quantification result than the choice between RBD, FT and Markov analyses.

3.1.1 FTA vs. RBD

When establishing a reliability/safety model of a technical system, fault trees (FT) and reliability block diagrams (RBD) are two well proven and frequently used techniques, e.g. see /6/. Both are Boolean models, and Appendix B of /2/ describes these methods and gives examples of how they are used. As pointed out there (e.g. Appendix B.4.4.1), RBD and FT represent exactly the same things, and the calculations may be handled exactly in the same way. A RBD may be given an equivalent representation as a FT, and a FT may be converted to a RBD. A common advantage of the two approaches is that they split the graphical representation (RBD or FT) from the calculations. Actually RBD is often mainly seen as a method of representation than as an analysis method.

Roughly speaking a reliability block diagram approach is often chosen when the system structure is fairly simple and/or the number of components is limited. However, the FT constitutes a top down method, helping the analyst to develop the reliability model step by step from the unwanted “top” event. So if the system structure is very complex one might find it advantageous to use a FT to model it. There are also software available, which find cut sets and carry out the safety calculations of a FT.

However, software to carry out the PDS safety quantifications of a given RBD, is now being developed in the PDS project, (and there also exist an old version of such a program).

In summary, for users who prefer to use FT as a graphical representation and calculations, this can very well be combined with use of the PDS-method, as long as the calculations are based on the modeling presented in Chapter 2.

3.1.2 Markov analysis

The Markovian approach is another old and well-proven reliability technique, e.g. see Appendix B.5.2 of /2/ and /6/. It is a time dependent approach, i.e. giving state probabilities depending on time. For a safety system we should then derive the time dependent solution for the interval τ, And then calculate the average over the interval. This can be quite a complex approach, unless the system is very simple. Thus, for safety systems we see the Markov approach mainly as a means to carry out rather detailed analyses for relatively simple systems, and do not see Markov analysis as a general alternative to FT or RBD. Markov analysis, using asymptotic probabilities (which are much easier to derive), could be seen as an alternative. However, for safety systems this represents an approximation, which validity must be verified.

3.2 Alternative CCF models

A number of CCF models exists. The simplest and perhaps most commonly used, the beta factor model, was also discussed in Chapter 2. Another relatively simple model is the Binomial Failure rate (BFR) model. Finally we refer to the class of completely general CCF models, which the CCF model of PDS belongs to. Also note that various aspects of CCF modeling of safety instrumented systems offshore are discussed in /18/.

3.2.1 Beta Factor model

Due to its simplicity, the beta factor model is often applied in actual reliability and safety (risk) analyses. However, it assumes that all redundant channels fail when there is a CCF. This could give quite sensible results for a small (2-3) number of "channels" (redundant components), or if the β-value is allowed to change with the configuration. However, if β is identical for all configurations it is commonly accepted that this model is too simplistic to give a good comparison of various design options.

3.2.2 Binomial Failure Rate BFR model

Models, like the Binomial Failure rate (BFR) model, have a limited number of parameters to fit a multiplicity distribution of CCF. This model assumes that a redundant set of *N* components are subject to shocks at rate *v*. At each shock the number of components failing, X, has a binomial distribution with parameters *N* and *p*; that is the probability that X = x equals

$$p_x = \binom{N}{x} p^x (1-p)^{N-x}; \;\; x = 0,1,2,....,N$$

To specify this CCF distribution we must estimate both *v,* and *p*; whilst *N* is known. Estimation of the shock rate, *v* is not straightforward, as this model allows it to be shocks both with 0 and 1 component failing. This is a somewhat unpleasant feature of the model. If *p* = 1 all *N* components fail and we have a beta factor model.

A generalization of the model has been suggested, where there are two types of shocks, one rate *v* as above and another rate v_L, which is "lethal", i.e. causing all *N* components to fail. This idea of introducing a "lethal shock rate" could be relevant, not the least for large *N*. Also the PDS method could easily be modified to account for these types of shocks, (in addition to the standard CCF model).

3.2.3 General CCF models and the need of data

A number of models have been defined and used to allow for several "failure multiplicities" when there is a CCF (similar to the BFR model). Several models are referred in /4/; more information is given for instance in /7/, /8/, /9/, /10/ and /11/. Some models are completely general; that is there can be an "arbitrary" probability that x out of N components fail in a CCF, (x= 2, … , N). Examples are the alpha factor model, Greek letter model, Basic Parameter (BP) model, (see above references), and it is rather a matter of convenience which of these models (parameterizations) to choose.

The CCF model of PDS, e.g. see /2/, /11/, /12/ and /14/, belongs to this type of general models. One advantage of this PDS model is that it is a very direct generalization of the commonly used beta factor model. One could say that for a MooN configuration we have a beta factor that is modified by a configuration factor (C_{MooN}), i.e.: $\beta_{MooN} = C_{MooN} \cdot \beta$. And even if we just apply *generic* C-values, we could estimate an application specific β (cf. the IEC 61508 approach), and thus get more sensible results from the quantifications.

4 Summary and conclusions

The application of the PDS quantification approach for railway applications is discussed, and it is concluded that it is very suitable also for railway applications.

It is true that in the past the PDS approach has essentially been applied to quantify PFD rather than PFH. However, it is seen that there is a close relation between PFD and PFH, and the same modelling used for PFD can also be applied for PFH.

It is not found any convincing argument why PFD shall necessarily apply to so-called low demand mode and PFH necessarily to high demand mode. In principle, both PFD and PFH could be applied to both low and high demand mode.

It is seen as a weakness of the safety measure, PFH, that it does not distinguish between failures that are detected almost immediately, and failures that are detected after very long time of operation. The PFH just counts the number of failures, and whether the failure is detected "immediately" (e.g. after a fraction of a second) or after 6 months makes no difference: a failure in the system has occurred. In this respect, the measure, PFD is better, as it describes the relative time the safety system is unavailable.

There are a couple of discrepancies in the PDS formulas and the formulas of the IEC 61508 committee draft. The most notable is the handling of the DD failures. It is pointed out that inclusion of DD failures must be based on a discussion of design and operational philosophy of the system; i.e. is the DD system immediately brought to a safe state upon detection of a DD failure?

The IEC committee draft suggests not to include DD failures for a 1oo1 voting configuration, but to include them for CCF of redundant systems. This is seen as inconsistent. The present report suggests that for railway applications DD failures should usually not be included; but the PDS method as such allows both options.

In general the PDS formula for the quantifying the contribution of independent failures to PFH is much simpler than the corresponding formulas of the IEC committee draft, and the exact argument for the formulas given in this draft is not known. However, this discrepancy will in most practical applications have no significance, since the quantifications are complete dominated by the CCF.

Some further comparisons between the IEC 61508 and PDS approaches are given in the table below.

Topic	Approach in IEC 61508	Comparison with the PDS method
Failure classification	• Classification of failure causes into random hardware failures and systematic failures • Classification of failure effects into safe and dangerous failures • Further classification of failure effects into detected and undetected failures	• Same approach as in IEC 61508, except that a certain fraction of safe failures are defined as non-critical • New committee draft of IEC 61508 has adopted a similar approach
Basic formulas for probability of dangerous failure per hour, PFH, (high demand systems)	• RBD used as basis and formulas are illustrated for some configurations • CCF are modeled with the standard beta factor model, but the new committee draft suggests correction factors as an alternative approach. • The approach for including dangerous detected (DD) failures and repair time (MTTR) is not well defined and is questioned in this report.	• The PDS method uses RBD, but does not currently describe formulas for PFH. • The PDS method for PFH in the present report has been deduced, based on the principles of the PDS approach for failure detection, the PDS method for modeling CCF (with correction factors), the IEC 61508 interpretation of PFH in the new committee draft, and traditional reliability theory. • The PDS method for PFH make other assumptions about the inclusion of dangerous detected failures and repair times, which are believed to be better founded than formulas given in IEC 61508.
Reliability data	• Provides approach to estimate betas. • The Committee draft includes suggested values for configuration factors	• Standard beta values suggested, but IEC approach can also be applied (for beta of 1oo2 configuration) • Currently, there are some differences in the configuration factors suggested in the committee draft of IEC 61508 and the PDS method, due to different underlying assumptions and expert judgments.
Handling of systematic failures (including application software failures)	• IEC 61508 does not recommend to include the contribution from systematic failures and software failures	• The PDS method suggests using reliability data that reflects ``real'' performance. This means that historical data should be preferred over theoretical estimates which are often restricted to random hardware failures. • A contribution from test independent failures is sometimes added, if test conditions are different from demand conditions, (incomplete test).

References

/1/ IEC 61508: Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety related systems, part 1-7, Edition 1.0 (various dates).

/2/ IEC 61508. Committee Draft for Vote (CDV), 31-10-2008.

/3/ Reliability Prediction Method for Safety Instrumented Systems – PDS Method Handbook, 2006 Edition, SINTEF Report STF50 A06031.

/4/ Reliability Data for Safety Instrumented Systems – PDS Data Handbook, 2003 Edition, SINTEF Report STF38 A02421.

/5/ OLF Guidelines no. 070. Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry, OLF Rev. 02, 29-10-2004.

/6/ Rausand and Høyland, *System Reliability Theory, Models, Statistical Methods and Applications.* 2004.

/7/ Guidelines on Modelling Common-Cause Failures in Probabilistic Risk assessment. NUREG/CR-5485. INEEL/EXT-97-01327. Prepared for US Nuclear Regulatory Commission by Mosleh, Rasmuson, Marshall. Idaho National Eng. and Env. Laboratory. University of Maryland. 1998.

/8/ Apostolakis and Moieni, *The Foundations of Models of Dependencies in Probabilistic Safety Assessment.* Rel. Eng. 18, 177-195. 1987.

/9/ Fleming, Mosleh and Deremer, *A systematic procedure for the incorporation of common cause events into risk and reliability models*. Nuclear Engineering and Design 93, 245-273. 1986.

/10/ Mosleh, *Common Cause Failures: An Analysis Methodology and Examples.* Reliab. Engineering and system Safety, 34, 249-292. 1991.

/11/ Hokstad and Rausand, *Common Cause Failure Modelling: Status and Trends*, pp 621-640. In *Handbook of Performability Engineering*. Ed.: Krishna B. Misra. Springer 2008.

/12/ Hokstad, *A Generalisation of the Beta Factor Model*. Probabilistic Safety Assessment and Management Eds.: C. Spitzer, U. Schmocker & V.N. Dang, Springer 2004. Proceedings from PSAM7-ESREL ‘04.

/13/ Hokstad & Corneliussen, *Loss of safety assessment and the IEC 61508 standard*. Reliability Engineering and System Safety, **83** 111-120. 2004.

/14/ Hokstad, Maria & Tomis, *Estimation of Common Cause Factors from Systems with Different Numbers of Channels.* IEEE Transactions on Reliability, Vol. 55, No. 1, pp 18-25. March 2006.

/15/ SKI Technical report NR 91:6. CCF analysis of high redundancy systems, safety/relief valve data analysis and reference BWR application. Stockholm 1992.

/16/ Hauge, Hokstad, Herrera, Onshus. *The Impact of CCF in Safety Systems* SINTEF report F04410, 2004, (restricted).

/17/ Vaurio, *Consistent mapping of common cause failure rates and alpha factors.* Reliability Engineering and System Safety, **92** : 628-645. 2007.

/18/ Lundteigen, *Safety instrumented systems in the oil and gas industry: Concepts and methods for safety and reliability assessments in design and operation*. PhD thesis. Norwegian university of Science and Technology (ISBN 978-82-471-1385-1). 2009.

/19/ Hokstad, *Probability of Failure on Demand (PFD) –the formulas of IEC 61508 with focus on the 1oo2D voting*. Advances in Safety and Reliability. Ed.: K. Kolowrocki. Balkema 2005, pp865-871. Proceedings from ESREL '05.

/20/ Reliability Prediction Method for Safety Instrumented Systems – PDS Method Handbook, 2009 Edition, SINTEF Report. In preparation.

Appendix A: Data

Providing realistic input data is essential for achieving reliable results. The PDS Data Handbook provides generic parameter values for relevant offshore safety equipment, to be used as a rough estimation of safety. However, system specific data should be provided (failure rate, DC, etc.)

Regarding beta values, the approach suggested for parameter estimation could apply also using the PDS method

Regarding the configuration factors, C_{MooN}, the PDS method also suggests some standard values (based on experience, expert judgments and literature studies).

Table D5 of the Draft IEC standard, /2/, suggests similar following modifications of β, (numbers in parentheses are the numbers suggested in PDS, /3/, /4/):

Table A1. Modification factors (C_{MooN}) of β suggested in the IEC Draft standard /2/, (with PDS values in parenthesis).

MooN		N			
		2	3	4	5
M	1	β (β)	$0,5\cdot\beta$ ($0,3\cdot\beta$)	$0,3\cdot\beta$ ($0,15\cdot\beta$)	$0,2\cdot\beta$ ($0,08\cdot\beta$)
	2	-	$1,5\cdot\beta$ ($2,4\cdot\beta$)	$0,6\cdot\beta$ ($0,75\cdot\beta$)	$0,4\cdot\beta$ ($0,45\cdot\beta$)
	3	-	-	$1,75\cdot\beta$ ($4,0\cdot\beta$)	$0,8\cdot\beta$ ($1,2\cdot\beta$)
	4	-	-	-	$1.0\cdot\beta$ ($6,0\cdot\beta$)

It is observed that /4/ and /2/ essentially give the same ranking of the configurations, and for line 1 we see that the PDS values for N=3-5 is quite systematically 50% of the values in /2/. We have been informed (ref Ken Simpson) that the values in /2/ are obtained from a combination of data and expert judgments, (as PDS values are). However, we consider these differences of estimates to be within the uncertainty of these values, (as this uncertainty at present is considerable), but our judgment is that both these sets of estimates are far more credible than using the value β for *all* configurations (beta factor model). In a forthcoming version of PDS handbook the C_{MooN} values will be very close to that of the IEC committee draft.

There are also other sources for data on C_{MooN}. SKI (Statens Kärnkraft Inspektion / Swedish Nuclear Power Inspectorate) has through several reports investigated CCF. In particular, from /15/ configuration factors can be derived for CCF data on EPV (Electromagnetic pilot valve) and MNV (Main Valve). The results are summarized in the table below (also referred in /16/):

Table A2. Estimated C_{MooN} values for some configurations (votings).

	Voting					
Source	1oo2	1oo3	2oo3	1oo4	2oo4	3oo4
SKI: EPV	1,0	0,4	2,3	0,2	1,0	3,0
SKI:MNV	1,0	0,5	2,0	0,4	1,0	2,5
PDS	1,0	0,3	2,4	0,15	0,75	4,0

Again we find a reasonable agreement with PDS values. However the PDS value for 1oo4 (and 1oo5?) seems to be smaller than those reported in other sources by a factor approximately 2.

A number of other sources discuss and estimate multiplicity distributions for CCF. Most of these use other models (see Appendix 3.2.3), but it is possible to transform their results to the PDS CCF model. Of these other sources we mention a few:

- /7/, see their Table 5-11 giving suggested generic α-factors of the alpha factor model,
- /8/, see their Tables 2 and 3,
- /9/, see their Table 6,
- /17/, giving a number of estimates for α–factors (for N = 2, 3, 4, 5, 6) in the alpha factor model; (from NUREG/CR-6497).

Appendix B: Abbreviations

Below is a list of abbreviations used in this report.

BFR	-	Binomial Failure Rate
BP	-	Basic Parameter
CCF	-	Common Cause Failures
CDV	-	Committee Draft Vote
CPU	-	Central Processing Unit
D	-	Dangerous
DD	-	Dangerous Detected
DU	-	Dangerous Undetected
EPV	-	Electromagnetic Pilot Valve
FTA	-	Fault Tree Analysis
IEC	-	International Electrotechnical Commission
MDT	-	Mean Down Time
MooN	-	M-out-of-N
MTTR	-	Mean Time To Restore
MNV	-	Main Valve
PDS	-	Reliability of computer-based safety systems, (Norwegian: Pålitelighet for datamaskinbaserte sikkerhetssystemer)
PLC	-	Programmable Logic Controller
PFD	-	Probability of Failure on Demand
PFH	-	Probability of Failure per Hour
RBD	-	Reliability Block Diagram
SKI	-	Statens Kärnkraft Inspektion

Trondheim
Address: NO-7465 Trondheim, Norway
Telefon: +47 73 59 30 00
Telefax: +47 73 59 33 50

Oslo
Address: P.O. Box 124, Blindern, NO-0314 Oslo, Norway
Telefon: +47 22 06 73 00
Telefax: +47 22 06 73 50