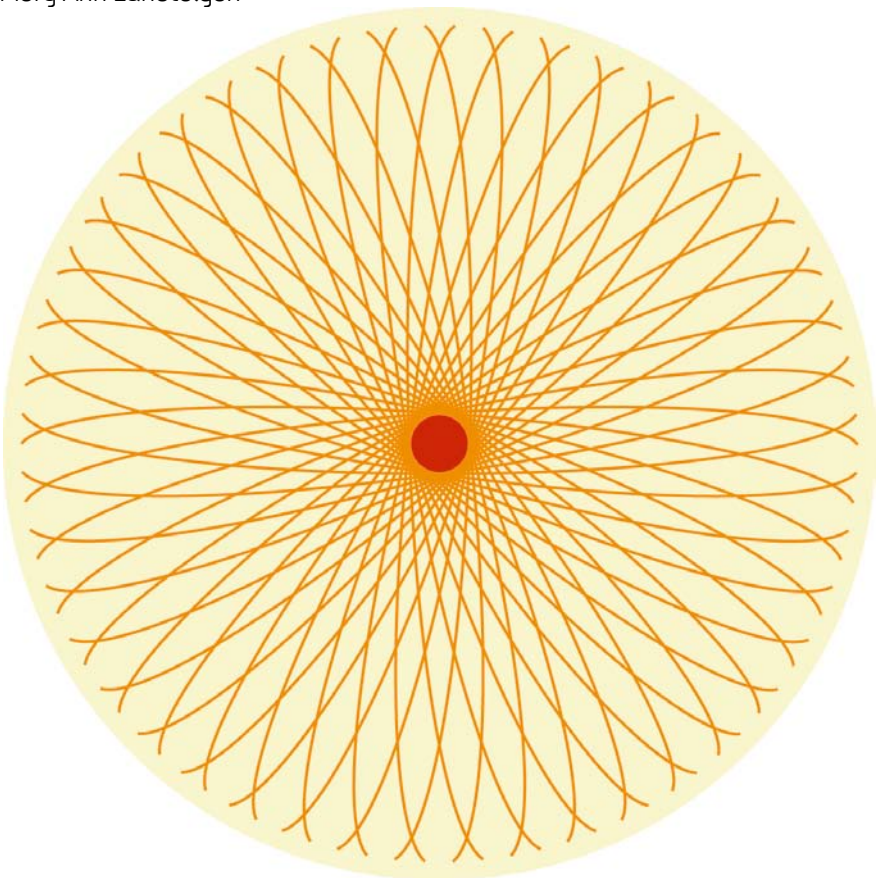
SINTEF

SINTEF A17956- Unrestricted

Report

Reliability Prediction Method for Safety Instrumented Systems – PDS Example collection, 2010 Edition

Author(s)
Stein Hauge
Solfrid Håbrekke
Mary Ann Lundteigen



SINTEF Technology and Society
Safety Research
2010-12-14

SINTEF Teknologi og samfunn
SINTEF Technology and Society

Address:
Postboks 4760 Sluppen
NO-7465 Trondheim
NORWAY

Telephone:+47 73593000
Telefax:+47 73592896

ts@sintef.no
www.sintef.no
Enterprise /VAT No:
NO 948007029 MVA

KEYWORDS:
Safety
Reliability calculations
Safety Instrumented Systems
IEC 61508

Report

Reliability Prediction Method for Safety Instrumented Systems – PDS Example collection, 2010 Edition

VERSION
1.0

DATE
2010-12-14

AUTHOR(S)
Stein Hauge
Solfrid Håbrekke
Mary Ann Lundteigen

CLIENT(S)
Multiclient – PDS forum

CLIENT'S REF.

PROJECT NO.
60S051

NUMBER OF PAGES/APPENDICES:
50/1

ABSTRACT
The PDS method is used to quantify the safety unavailability and loss of production for safety instrumented systems (SIS). This report presents a collection of worked examples, demonstrating how the PDS method can be applied to different cases and problems.

The example collection also serves as an indicated "best PDS practice" on how to perform reliability calculations for fairly complex systems.

PREPARED BY
Stein Hauge
SIGNATURE

CHECKED BY
Per Hokstad
SIGNATURE

APPROVED BY
Lars Bodsberg, Research Director
SIGNATURE

REPORT NO.	ISBN	CLASSIFICATION	CLASSIFICATION THIS PAGE
SINTEF A17956	978-82-14-05080-6	Unrestricted	Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
Version No. 1.0	2010-12-14	

SINTEF

Table of contents

Preface

The "PDS Forum" is a co-operation between oil companies, engineering companies, consultants, vendors and researchers, with a special interest in reliability of safety instrumented systems. The PDS method for reliability quantification and data handbooks were first issued in 1998, and later updated with new revisions in 2003, 2004, 2006 and in January 2010. In the latest revisions, the notations and approaches have gradually been brought in line with key standards on functional safety of safety instrumented systems, like IEC 61508 and IEC 61511. This new example collection is a result of work carried out in the user initiated research project "Managing the integrity of safety instrumented systems" as well as work done in the ongoing PDS-BIP; "Developing barriers and indicators to minimize environmental releases to sea". Both these projects have been sponsored by the Norwegian Research Council and the PDS participants. The work has mainly been carried out by SINTEF and may therefore not express the view of all the PDS participants.

PDS forum participants in 2010:

Oil Companies/Operators

- A/S Norske Shell
- BP Norge AS
- ConocoPhillips Norge
- Eni Norge AS
- GDF Suez E&P Norge AS
- Norsk Hydro ASA
- Statoil ASA
- Talisman Energy Norge
- Teekay Petrojarl ASA
- TOTAL E&P NORGE AS

Control and Safety System Vendors

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

Engineering Companies and Consultants

- Det Norske Veritas AS
- Lilleaker Consulting AS
- Safetec Nordic AS
- Scandpower AS

Governmental bodies

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

1 Introduction

1.1 Purpose of example collection

People working with reliability analysis often face a number of challenges such as which data to use, how to represent the technical system in a reliability model, and how to model dependencies between components. The purpose of this document is to discuss some of these modelling challenges and to present a collection of worked examples showing how the PDS method may be applied on some practical cases and problems.

Obviously, different practices will exist on how to quantify the reliability of a given technical system. Furthermore, the suitability of various methods will vary depending on the nature of the system to be considered and the results to be achieved. This document attempts to illustrate this versatility and gives some guidance on how to model different systems.

1.2 Content of the example collection

The following issues are discussed in this report:

- *Chapter 1* includes an introduction and a presentation of abbreviations, terms and definitions used in the report. Some specific abbreviations are only included in the example(s) where they are used.
- *Chapter 2* includes a discussion of some practical modelling challenges and special features to take into consideration when performing reliability analyses.
- *Chapter 3* contains four worked practical examples illustrating some of the modelling challenges discussed.
- *Appendix A* gives a brief listing of relevant formulas and parameters applied in the examples. Details are given in the PDS method- and data handbooks, ref. /1/ and /2/.

The worked examples in chapter 3 may be read independently of the discussions in chapter 2. However, chapter 2 gives some background information and motivation for the selected examples.

For the purpose of getting a better understanding of the examples and the applied formulas, the reader is encouraged to read the PDS method handbook prior to or in parallel with this example collection.

1.3 Terms and definitions

In this section, terms and definitions used in the report are listed and explained. For further details reference is made to /1/.

Table 1: Terms and definitions

Terms and definitions	
Random hardware failure	A failure caused by the natural degradation mechanisms when the component is assumed to be operated within the defined design envelope of the system.
Systematic failure	A failure that can be related to a particular cause (other than natural degradation) such as excessive stress, design related failures or a human error related failure introduced during operation or maintenance.
PFD	Probability of failure on demand. This is the measure for loss of safety caused by dangerous undetected failures detectable by functional testing.
PFH	Probability of failure per hour. This is the average frequency of failure per hour of a component or system.
P_{TIF}	Probability of a test independent failure. This is the measure for loss of safety caused by a failure not detectable by functional testing, but occurring upon a true demand.
CSU	Critical safety unavailability, $CSU = PFD + P_{TIF}$.
DTU	Downtime unavailability. This is the "known" downtime unavailability caused by by-pass during repair or functional testing. The downtime unavailability comprises two elements: • The unavailability related to repair of dangerous detected failures (with rate λ_{DD}). The average duration of this period is the mean time to restoration (MTTR); This downtime unavailability is also denoted DTU_R • The unavailability resulting from planned activities such as testing, maintenance and inspection (of average time *t*). This downtime unavailability is also denoted DTU_T.
CSU_{TOT}	The total critical safety unavailability including the "known" downtime unavailability: $CSU_{TOT} = PFD + P_{TIF} + DTU$.
MTTR	Mean time to restoration; i.e. time from failure is detected/revealed until function is restored, ("restoration period"). Note that this restoration period may depend on a number of factors. It can be different for *detected* and *undetected* failures: The *undetected* failures are revealed and handled by functional testing and could have shorter *MTTR* than the *detected* failures. The *MTTR* could also depend on configuration, operational philosophy and failure multiplicity.
STR	Spurious Trip Rate. Rate of spurious trip failures of the safety system, i.e. failures were the safety system is activated without a demand, when taking into consideration the voting configuration.
λ_{crit}	Rate of critical failures; i.e., failures that may cause loss of one of the two main functions of the component/system, i.e. the ability to maintain production when it is safe and to shut down when production is not safe. Critical failures include dangerous (D) failures which may cause loss of the ability to shut down production when required and safe (S) failures which may cause loss of the ability to maintain production when safe (i.e. spurious trip failures).
λ_D	Total rate of Dangerous failures, including detected as well as undetected failures. $\lambda_D = \lambda_{DU} + \lambda_{DD}$.

Terms and definitions	
λ_{DU}	Rate of Dangerous failures, *un*detected by automatic self-test or incidentally by personnel (i.e. revealed only by a functional test or upon a demand). The undetected Dangerous failures contribute to the *PFD* of the component/system; ("loss of safety").
λ_{DD}	Rate of Dangerous failures, detected by automatic self-test or (incidentally) by personnel.
λ_S	Rate of safe (spurious trip) failures, including both undetected as well as detected failures. $\lambda_S = \lambda_{SU} + \lambda_{SD}$.
λ_{SU}	Rate of safe (spurious trip) undetected failures, i.e. *un*detected by automatic self-test or incidentally by personnel and therefore results in a spurious trip of the component (and possibly of the system depending on system configuration).
λ_{SD}	Rate of safe (spurious trip) detected failures, i.e. detected by automatic self-test or personnel. Hence, an actual trip of the component is avoided.
λ_{NONC}	Rate of failures that are not critical (i.e. failures not affecting the two main functions of the component/system, see definition of λ_{crit} above).
λ	Total failure rate, $\lambda = \lambda_{crit} + \lambda_{NONC}$.
c	Coverage; percentage of failures detected either by the automatic self-test *or* by personnel (i.e. control room operator or maintenance personnel).
TC	Test Coverage; fraction of dangerous undetected failures revealed by functional test.
CCF	Common Cause Failure, i.e. failure of two or more (redundant) components of the same cause, occurring simultaneously or within a rather short time interval.
SFF	Safe Failure Fraction, i.e. the fraction of failures that are not critical with respect to safety unavailability of the safety function (in IEC 61508 defined as the ratio of safe failures plus dangerous detected failures to the total failure rate). In PDS defined as: $SFF = (1 - \lambda_{DU} / \lambda_{crit})$ x 100 %.
β	The fraction of failures of a single component that causes both components of a redundant pair to fail “simultaneously”. The β is application specific, and should therefore, preferably, reflect application specific conditions.
C_{MooN}	Modification factor for voting configurations other than 1oo2 in the β-factor model (e.g. 1oo3, 2oo3 and 2oo4 voting logics). MooN voting (with respect to safety) implies that at least M-out-of-N components must function for the safety function to work (on demand).
τ	Interval of functional test (time between functional tests of a component).

1.4 Abbreviations

Below is a list of abbreviations used throughout this report. Abbreviations that are used only once, e.g. for specific equipment, are introduced in the text and not mentioned here.

CCF	-	Common Cause Failure
CSU	-	Critical Safety Unavailability
DTU	-	Downtime Unavailability
DD	-	Dangerous Detected
DU	-	Dangerous Undetected
ESD	-	Emergency Shutdown Valve
FMECA	-	Failure Modes, Effects and Criticality Analysis
FMEDA	-	Failure Modes, Effects and Diagnostic Analysis
FTA	-	Fault Tree Analysis
HEP	-	Human Error Probability
HIPPS	-	High Integrity Pressure Protection System
I/O	-	Input/Output
OGP	-	International Association of Oil & Gas Producers
OREDA	-	Offshore Reliability Data
PLC	-	Programmable Logic Controller
PFD	-	Probability of Failure on Demand
PFH	-	Probability of Failure per Hour
PSD	-	Process Shut Down
PT	-	Pressure transmitter
RBD	-	Reliability Block Diagram
RNNP	-	Risk level in the petroleum activity[1]
SFF	-	Safe Failure Fraction
SIF	-	Safety Instrumented Function
SIL	-	Safety Integrity Level
SIS	-	Safety Instrumented System
TIF	-	Test Independent Failure
TC	-	Test Coverage

[1] Project on trends in the risk level for petroleum activity in Norway, see www.ptil.no/rnnp.

2 Modelling challenges

When performing reliability analyses of safety instrumented systems (SISs), the reliability analysts face several challenges:

- What input data to apply, for example failure rates?
- How to model common cause failures (CCF)?
- How to include the contribution from operator intervention and potential human errors?
- How to document the analysis, how to identify all relevant assumptions, and how to present the reliability results for the decision makers?
- How to model the contribution from non-perfect testing, for example from failures that are not covered by a functional test (the test independent failures)?

These topics are further discussed in the following sections.

Other challenges include:

- Getting hold of the information that is needed to fully understand and describe the system and how it is being operated.
- How to make proper assumptions and simplifications in relation to complex system structures?
- How to model SIS operating in the high-demand or continuous mode, and what input data to use for such analyses?

For SIS operating in the high-demand / continuous mode, a reference is made to chapter 6 in the PDS method handbook, and example 4 in this report.

2.1 Failure data – why and from where?

Identification of relevant failure data is an essential part of any quantitative reliability analysis. It is also one of the most challenging tasks and requires a reflection on e.g. the following questions:

- Are failure data available for the equipment under consideration?
- Are the available data relevant for the specific application, under the given operating and environmental conditions?
- Should manufacturer/ vendor supplied data be combined with experience data for a limited population or should generic data from larger (but not necessarily fully comparable) populations of components be applied?
- Are the assumptions underlying the given data known, such as e.g. system boundaries, what components that are included, type of failure modes covered, energised or de-energised to trip, etc.?
- Is there a maintenance strategy in place to support the assumption about the components being in their useful life period?
- What uncertainties are associated with the data, for example due to the quality of failure recording, the quality and coverage of functional tests, the number of operating hours (confidence intervals), and so on?

Often, there are no straight forward answers to these questions, and the situation may differ from case to case. Still, it is important that the reliability analyst gives a brief statement about relevance and uncertainty in input data, and for this purpose the above questions may be useful.

2.1.1 Failure data sources

Collection of high quality failure data is a very time consuming activity and the number of relevant data sources for SIS is therefore limited. Some examples of frequently used data sources for SIS are:

- OREDA handbooks and database, including data from offshore and onshore oil and gas installations (www.oreda.com)
- PDS data handbook, including data for SIS components used in the process industry (www.sintef.no/pds)
- RNNP reports, including barrier testing data from the Norwegian petroleum industry (www.ptil.no/risikonivaa-rnnp/category20.html)
- Exida Safety Equipment Reliability Handbooks including generic and brand specific component failure data (www.exida.com)
- T-book handbook including equipment data from the Swedish nuclear industry (T-Book, Version 5, Reliability Data of Components in Nordic Nuclear Power Plants. TUD-office and Pörn Consulting, 2000)
- FARADIP.THREE database including accumulated data from a number of industries (www.technis.org.uk).

Table 2 suggests a way to classify failure data according to how they have been collected.

Table 2: Categories of failure data sources

Type of data	Description	Example of data sources
Generic data	Failure data based on a broad group of components without information on manufacturer, make, and component specifications. Such data can be based on recorded failures, from expert judgments, or from laboratory testing, /3/. The data can apply for one specific industry, such as e.g. OREDA and PDS for the oil and gas industry, or it may be collected from several industries such as e.g. FARADIP.THREE.	OREDA handbooks/database, PDS data handbook, FARADIP.THREE.
Operator/company specific data	Failure data based on operating experience from one operator/oil company from e.g. all company installations and/or their own interpretation of different data sources.	Company specific databases and documents.
Site/application specific data	Failure data based on failures recorded at a specific site or in relation to a specific application.	Manual logs, maintenance databases, automatic shutdown reports, SAP, Synergi, etc. Such data normally requires some manual processing and failure classification to enhance the usefulness.
Manufacturer provided data	Failure data for a particular product prepared by a particular manufacturer (or a consultant). Can be based on component FMECA/FMEDA studies, laboratory testing, and in some cases also field experience.	Vendor data reports, Exida handbooks.

Generic data are often (but not necessarily, see above table) based on operational experience from a number of installations and a number of comparable equipment types, such as e.g. flame detectors from different vendors. In such case the generic data reflect some kind of average expected field performance for the equipment type under consideration. As such, using generic data can often be considered a fairly robust approach in reliability quantification.

At early project stages generic data is often selected due to lack of detailed information. However, at later project stages one should, if possible, apply valid application or equipment specific data – if well documented and considered relevant.

Authorities require that the companies keep control of their safety barriers throughout the entire lifecycle of an installation. Consequently, it is mandatory for the operators to collect *site specific failure data* during maintenance and operation. During modification analyses such data are of particular relevance for the purpose of documenting the performance history of a given equipment type. However, since the statistical confidence in data from only one installation may often be poor, reliability analyses are seldom based on such data alone. However, for some equipment types where the number of installed units is high, e.g. fire and gas detectors, it may be relevant to apply site specific data only.

One often experiences that supplied *manufacturer data* are significantly "better" than comparable generic data (i.e. giving lower failure rates). This may have several reasons, such as varying equipment quality, failure modes included and the definition of equipment boundaries. Another important aspect, however, is that so called systematic failures, i.e. failures due to environmental stress, due to mal-operation, installation failures, maintenance errors, etc. have frequently been excluded from the manufacturer data. This is understandable since manufacturers do not want to include failures that can be attributed to factors external to the equipment itself. Another aspect is the fact that feedback from the operators using the equipment may be poor (especially beyond the warranty period) and in such cases it is difficult for the manufacturer to establish a good failure rate estimate.

Consequently, when applying manufacturer data that is significantly "better" than the corresponding generic data, it is important to give a brief rationale and documentation for the selected figures. Manufacturer data may be well suited for comparison of reliability performance provided that they are sufficiently documented, while generic data, possibly in combination with manufacturer data, may be best suited for compliance studies, i.e., verification that a SIF is able to provide the required risk reduction. This is further discussed in section 3.3 in the new PDS method handbook, /1/ and section 2.4.1 in the data handbook, /2/.

Figure 1 below illustrates in a simplified manner the compromise between the need for failure data and the relevance of the data. The broader the category of failure data becomes, the less representative the data can be for a particular component make. Data for emergency shutdown valves that have been collected at several installations, give a large population, but the population can have an inherent variability due to differing operating environment, valve types, etc. But when data on this valve is collected from one installation only, the data will be highly relevant, but the sample will be small.

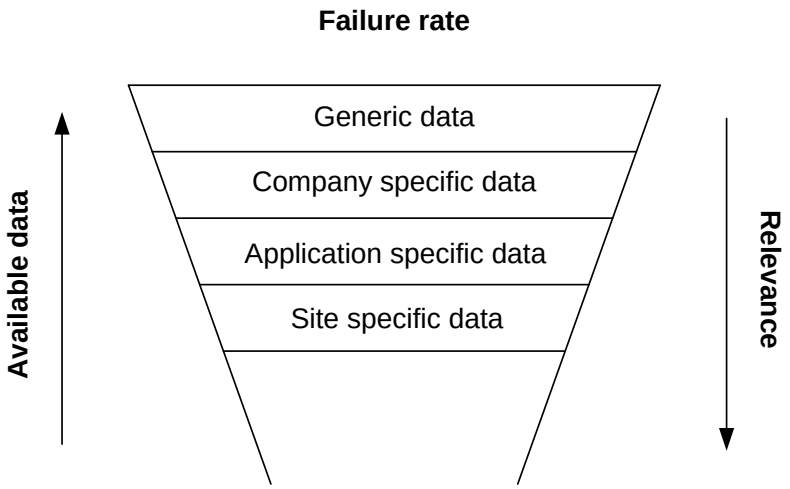


Figure 1: Classes of failure rate data and their availability and component relevance.

In general, selection of data in the design phase should always be supported by the underlying assumptions, the rationale for the selected source(s), and a discussion about the relevance of the applied data. Note that data used in predictive analyses (i.e. in the SIS design phase) must be verified throughout the operational phase, ref. /7/. This involves a regular review and classification of reported failures in order to verify that operational performance complies with assumptions made in the design phase.

2.1.2 Data uncertainty

The results from reliability analyses are highly influenced by the values assigned to parameters like failure rates and CCF parameters. The failure rate estimates can be uncertain for several reasons, in particular related to:

- Quality and coverage of failure reporting and registrations: Are all failures recorded and properly classified?
- Relevance: Are the data underlying the failure rate estimates relevant
  - for the given product in its specific operating environment?
  - in light of the type (and size of) equipment for which data have been collected.
- Statistical uncertainty: What is the number of installation years for which data have been collected, and have a sufficient number of failures been recorded to give reliable estimates?

As a consequence, it is frequently claimed that the uncertainty in the data often exceeds the uncertainty related to the reliability model itself.

It should be noted that some data sources, like OREDA, /11/, in addition to giving a best (mean) estimate for the failure rate, also provides confidence intervals and standard deviation figures. Data uncertainty is further discussed in section 3.4 in the PDS data handbook, /2/.

2.2 Modelling of common cause failures – a special case

SIS often introduces redundancy to increase the reliability and/or availability of a system. Unfortunately, the intended gain in system reliability can be considerably reduced due to common cause failures (CCF). The

modelling of such failures is therefore a vital part of any reliability analysis. See also chapter 4 of the PDS method handbook, /1/, on modelling of CCF.

The beta factor model for including CCF in reliability analysis has gained wide acceptance in the process industry. Several other methods have also been developed since the 1970s, for example the alpha factor model, the binomial failure rate model (the shock model) and the multiple Greek letter model. The main challenge with these models is lack of relevant data to support the model parameters.

There are two types of beta factor models: (1) The standard beta factor model and (2) the multiple beta factor model upon which the PDS method is based. In the standard beta factor model it is assumed that a certain fraction of the failure rate of a component (equal β) are due to some common cause(s), i.e. failures that will cause *all* the redundant components to fail simultaneously or within a limited time interval. The realism in this model is sometimes questioned since it does not account for the voting (MooN) of the system; i.e. this model gives the same rate of CCF for any configuration (like 1oo2, 1oo3 and 2oo3).

The PDS method is based on an extension of the beta factor model, called the multiple beta factor model. This model considers different multiplicities of failures and has introduced a configuration factor C_{MooN} that modifies the contribution of CCFs for different voting configurations. A further description of the PDS approach is found in the PDS method handbook, ref. /1/, and is not further elaborated here. However, there will be special cases where the model must be adapted, and below we consider one such special case, i.e. modelling of CCFs among non-identical components (or functions).

2.2.1 Why model CCF among different protection layers?

Often, multiple protection layers are implemented in order to reduce the risk to a sufficiently low level. In example 1 of chapter 3, both a PSD and a HIPPS function are implemented to protect against overpressure of downstream equipment, whereas in example 2 each run of a pressure letdown station is equipped with different types of valves to close in case of pressure build up.

Often, in traditional risk analysis these different protection layers are considered independent of each other, and typically, in an event tree analysis, the branch probabilities are simply multiplied together. This approach surely brings the calculated risk down to a low level, but is it correct? What if the two protection functions are tested at about the same time and what if they include similar components that are subject to the same common influences? As will be seen from example 1 and 2, CCF between non-identical components may in some cases actually be decisive for the resulting failure probability.

Note that the standard beta factor model and the PDS method generally apply for quantification of CCF of similar components. The approach for quantifying CCF between *non-identical components* must be considered separately for each case, in particular in cases where the failure rates differ considerably.

Below is proposed and discussed some alternatives for handling CCF quantification of components having different failure rates, beta values and/or test-intervals. The approach is applicable for modelling dependencies among redundant components in a particular SIF as well as for dependencies among components in different protection layers. It should be noted that there are no definite answers to what is best practice for such cases, since none of the methods to our knowledge have been calibrated against real life experience.

2.2.2 How to handle CCFs among components with different failure rates?

Consider two components A and B in a redundant configuration that have non-identical failure rates for dangerous undetected (DU) failures, i.e. $\lambda_{DU,A} \neq \lambda_{DU,B}$. To account for CCFs in this situation, we need to first select a "representative" failure rate for the two components. Here, we may choose between the following two approaches:

1. Using some representative average value, typically the geometric mean of the CCF failure rates of the two components.
2. Using the lowest failure rate of the two components.

In either cases, it is also necessary to introduce a $\beta_{A,B}$, and the selection of this factor is discussed in the next section.

For redundant components with non-identical failure rates using the *geometric mean* has often been the preferred method. This is an adequate approach if the failure rates are of the same magnitude. The use of a geometric mean is also discussed in /1/. The contribution of CCFs to the PFD is then for two components voted 1oo2 with the same test interval τ:

$$\mathrm{PFD}_{1oo2}^{(CCF)} \approx \beta_{A,B}\sqrt{\lambda_{DU,A} \cdot \lambda_{DU,B}} \cdot \tau / 2 .$$

There is no proper theoretical or practical foundation for using the geometric mean although the resulting common cause contribution obviously will depend heavily on this average, /3/. A problem with the above approach is that for components with very different failure rates, the "weighting" of the largest failure rate will become dominating, and in extreme cases the CCF contribution may exceed the likelihood of an independent failure of the most reliable component (i.e. introducing an additional component may give little, no or even a negative effect).

The second approach suggested when the failure rates have different order of magnitude is to use the *lowest* failure rate. Again, consider two components A and B voted 1oo2 with similar test interval. Let $\lambda_{DU,A} < \lambda_{DU,B}$. Then the contribution from CCF to the PFD becomes;

$$\mathrm{PFD}_{1oo2}^{(CCF)} \approx \beta_{A,B} \cdot \lambda_{DU,A} \cdot \tau / 2$$

The motivation for this approach will be to say that when having two (or more) redundant components in parallel, then the rate of common cause failures of the combined system will be governed by the best component. Assume that the components A and B have a basic probability of failure on demand of 1/50 and 1/1000 respectively. Since both components per definition shall fail in order for a common cause failure to occur, and since it is implicitly assumed that the *most reliable component will not fail more often than 1 in 1000 times* (independent failure or common cause), then the combined PFD will *at least* be as good as the best one, in this case 1/1000, multiplied with some suitable β-factor (ref. next section).

The minimum failure rate approach is not necessarily appropriate in situations with several components where the failure rates differ considerably. Take for example a system with three equally good components as opposed to a system with one very good component and two poor components (i.e. having a much higher failure rate). If these systems are voted 2oo3 (i.e. two components must function), it appears illogical to apply the same common cause failure rate for the two cases. However, this could be adjusted for when selecting the beta factor value.

2.2.3 How to select β-factors for non-identical components?

First, consider two redundant and identical components A and B. The beta factors related to component A and B are denoted β_A and β_B respectively, being equal for the case since the two components are identical:

$$\beta_A = \Pr(\text{B fails} \mid \text{A fails}) = \Pr(\text{A fails} \mid \text{B fails}) = \beta_B$$

Note that for identical components it makes sense to talk about the β-factor *for* a component. E.g. for a specific HIPPS valve A, an assumed β-factor of 0.03 means that once the valve has failed, there will be a probability of 3% that also the redundant HIPPS valve B fails due to a CCF.

Now consider that as part of reducing the vulnerability to common cause failures, *diversity* has been introduced. Components A and B are still redundant but they are no longer identical. However, they may still be exposed to common influences, for example from the operating environment, even if the degree of dependency will be less than for identical components. Consider e.g. a case where a level transmitter (LT) and a pressure transmitter (PT) are used to initiate a closure of a separator inlet valve in case of blocked outlet. The beta factor *between* the components, $\beta_{LT,PT}$ will be different and probably lower than the beta factors that are used *for* pressure transmitters (i.e. β_{PT}) and *for* level transmitters (i.e. β_{LT}), due to e.g. different measurement principles.

It is difficult to give general rules for how to select $\beta_{A,B}$, but the following two approaches have often been used in relation to the PDS method:

1. Let $\beta_{A,B}$ equal the lowest value of β_A and β_B, or select an even lower value than this in case of high degree of diversity or resistance to the same common causes/influences.
2. Select $\beta_{A,B}$ from expert judgements and failure cause analysis. For instance, where the minimum of two rather distinct failure rates are chosen, a beta value even higher than the highest beta value of the components may be appropriate.

If any prior knowledge concerning the possible causes of common cause failures and their individual contributions is available, it will generally be preferable to perform some kind of failure cause analysis.

2.2.4 How to select τ for components with non-identical test intervals?

For components having distinct test intervals, it becomes a question of which test interval to apply in the CCF quantification, e.g. when combining this with the geometric mean of the failure rates. Given the standard assumption that a functional test reveals 100% of the critical failures, this implies that also common cause failure modes are revealed during testing. Now, consider N redundant components, each having a test interval τ_i, (i=1, ..., N). For an arbitrarily chosen component we must then ask how long on average it is since last functional test? The test interval τ can then be seen as a random variable, having value τ_i with probability 1/N, (i=1, ..., N), and so the mean length (expected value) of the test interval for an arbitrarily chosen component equals $\bar{\tau}$. For the system with *N* redundant components, each with test interval τ_i, the average test interval becomes:

$$\bar{\tau} = \frac{1}{N}\sum_{i=1}^{N} \tau_i \ .$$

2.2.5 Some final remarks

The three previous subsections have presented some guidance on how to account for CCF among non-identical components, considering the failures rate, the β-values and the test interval separately. When having to select a representative value both for the failure rate, the β-factor and the test interval there are several alternatives.

One compromise which have been chosen in some of the examples in chapter 3, is to select the *geometric mean of the* λ_i's for the *i* redundant components, the minimum of the β_i's (or even lower depending on the degree of diversity between the components) and the arithmetic mean of the test intervals. Generally, for N different components voted MooN, the CCF contribution to the PFD then becomes:

$$PFD_{MooN}^{(CCF)} = C_{MooN} \cdot \beta_{\min} \cdot \sqrt[N]{\lambda_1 \cdot \lambda_2 \cdot \ldots \cdot \lambda_N} \cdot \bar{\tau} / 2 \, .$$

where $\beta_{\min} = \min_{i=1,2,\ldots,N} \{\lambda_i\}$. As mentioned above, this approach does not recognize that diversity could indicate an even lower contribution from CCF. If a high degree of diversity can be claimed, one may select an even lower beta from expert judgments. This is further discussed in the examples in chapter 3.

2.3 How to include human errors / human factors

Functional safety standards like IEC 61508 and IEC 61511 include a number of references to "human factors" and thereby recognise the need for considering the interaction between the operators and the SIS as part of a hazard and risk analysis. The standards are however, not very specific on this issue and leave it very much to the reader (and analyst) to figure out how to include human factors and whether quantification is necessary or not. The following rules of thumb are here suggested with respect to the need for quantification:

- The contribution from human errors is not included in the quantification of PFD (or PFH) if the SIF is activated automatically without any required operator intervention (e.g. a PSD function activated automatically upon high temperature). Obviously, failure rates are influenced by "human factor issues" due to e.g. maintenance interaction, but these factors are assumed to be reflected in the applied component failure rates (given that generic or operator specific data are applied).
- The contribution from human errors should be considered included in the quantification of PFD (or PFH) also for a fully automatic SIF, if the function is frequently inhibited or bypassed during special operational modes. An example can be a low pressure alarm (PALL) function on the inlet piping that frequently needs to be inhibited during start-up. For such functions, the possibility of them being inhibited during a demand should be quantified if the likelihood of such an event is considered to affect the PFD value.
- The contribution from human errors should be included in the quantification of PFD (or PFH) if a person/operator is an active element in the execution of the SIF. For example, an operator may be expected to initiate a valve closure (shutdown) or valve opening (blow down) upon an alarm from the SIS.

Hence, human errors should be considered in the reliability calculations if human tasks are likely to have a direct influence on the performance of the SIF.

The probability of a human error is often represented by the so called human error probability (HEP). Data and methods for arriving at human error probabilities is not discussed in this example collection, but a possible starting point for further reading may be ref. /4/.

2.4 Proper documentation of underlying assumptions

Many reliability analysts may have experienced a situation somewhat similar to this: *Some years after a reliability analysis was performed, there is a request for an update or a comparable analysis. The previous report is recovered, and within short time the following questions are raised: why are the results as they are, what assumptions are they based on, and where do the (extremely good) failure rates come from?*

Thorough documentation of the results and especially of all the underlying assumptions and prerequisites is therefore an important part of any reliability analysis. This may be related to overall issues such as:

- What technical, operational and analytical assumptions the result are based on and the consequences of these assumptions.
- Measures and activities that need to be implemented and followed up in design and operation and which are vital to achieve the required performance of the SIS.

For the reliability modelling, assumptions that are important to highlight are for example:

- Where the reliability input data is taken from (what sources), and to what extent the data has been adjusted to account for a particular application.
- What assumptions that have been made for the data concerning diagnostic coverage, critical failure modes, safe state, and so on, which are normally not presented (or presented in the same way) in many data sources. In particular it is important to document and substantiate failure rates that are significantly better than average generic data.
- What assumptions that have been made in relation to functional testing and maintenance, including required intervals and specific methods and/or tools to be applied.
- What assumptions that have been made regarding operating environment.
- What assumptions and analyses that have been made in relation to reducing CCFs, e.g. diversity or staggered testing.
- All relevant assumptions related to procedures for inhibits and overrides, degraded operation, maximum repair times (if any), and assumptions concerning set points and required human interaction.
- What assumptions that need to be validated during operation and how often such validation needs to be performed.

All assumptions and prerequisites should be clearly stated in order to provide a good foundation for evaluating the validity of the results, or for future use of the analysis, e.g. during a modification analysis.

It may often be useful to distinguish between general assumptions and case/project specific assumptions and/or distinguish between analytical assumptions and assumptions related to design and operation.

It may also be useful to categorize the assumptions according to whether they contribute to data uncertainty or model uncertainty, ref. discussion in section 2.4 in the PDS method handbook, /1/.

2.5 The use of P_{TIF} vs. reduced test coverage

The PDS method has introduced the P_{TIF} to account for the probability that certain failures are not identified during functional testing. As such the P_{TIF} acknowledges that most tests are not 100% perfect and that the SIS, for this reason, may not be able to function shortly after a test. When for example a blowout preventer (BOP) is tested, the cutting function of the shear ram is not actually tested.

When the P_{TIF} is added to the PFD, we get the critical safety unavailability (CSU), which for a single system is given by:

$$CSU = PFD + P_{TIF} \approx \lambda_{DU} \cdot \tau/2 + P_{TIF}$$

IEC 61508 also considers non-perfect testing in part 6, section B.3.2.5 (*Effects of non-perfect proof test*) of the final draft version of the 2.0 edition of the standard, /5/. Here, a *test coverage* (TC) factor is introduced, which is defined as the fraction of DU failures that are revealed by the functional test. The residual fraction (1-TC) of failures remains un-revealed until a more thorough proof test is performed (not always possible) or till the next real demand.

For a system comprising a single component that is tested with interval τ and completely proof tested with an interval τ_c, the PFD may be estimated as:

$$PFD = TC \cdot \left(\frac{\lambda_{DU} \cdot \tau}{2} \right) + (1 - TC) \cdot \left(\frac{\lambda_{DU} \cdot \tau_c}{2} \right)$$

There are pros and cons of either approach for modelling incomplete testing. The main difference is that P_{TIF} represents a contribution from un-revealed failures being independent of time, while the corresponding contribution increases with time when the latter test coverage approach is used. More important than discussing what method to select, is perhaps to recognize and take into consideration the potential effect of non-perfect test conditions.

3 Example collection

3.1 Introduction – structure of cases

This chapter includes 4 worked examples, illustrating the use of the PDS method on selected practical cases. The cases are based on projects in which SINTEF has been involved and illustrate some of the modelling challenges discussed in the previous chapter.

All the examples have a similar structure:

i. *System description*; i.e. a description of the case study including the technical systems and operational features involved. It also includes a brief description of modelling challenges particular for that example.

ii. *Assumptions and limitations*; i.e. a description of the assumptions and prerequisites underlying the modelling case, also giving an outline of limitations and simplifications.

iii. *Reliability modelling*; i.e. a description and illustration of how the case has been modelled, including particular modelling challenges.

iv. *Reliability data*; i.e. a listing of the reliability data and test intervals applied for the case and a discussion of particular challenges related to the selection of data.

v. *Reliability calculations*; i.e. presenting a detailed quantification of the system reliability according to the reliability modelling.

vi. *Discussion of result*; i.e. a presentation and discussion of the results from the reliability modelling.

The examples include the following systems:

Example 1: A pressure protection system comprising a HIPPS function and a PSD protection function. This example illustrates how the PFD is calculated with non-identical components in the parallel branches of reliability block diagrams (RBDs).

Example 2: A multiple pipe run system (a pressure letdown station) with individual overpressure protection of each run where a given number of the runs must shut down in order to avoid critical overpressure. This example illustrates CCF modelling as well as modelling of a relatively complex system structure.

Example 3: A part of an ESD function for a workover control system (WOCS) used during well intervention. This example illustrates the significance of P_{TIF} for components with rather short test intervals, as well as the challenges related to failure data selection.

Example 4: A railway signalling system operating in the high-demand mode. The example illustrates how the probability of failure per hour (PFH) is calculated with the new formulas for continuous operated systems in the PDS method handbook, /1/.

3.2 Example 1 – Modelling of a pressure protection system (HIPPS + PSD)

3.2.1 System description

A pressure protection system comprises two separate SIFs; i.e. a PSD function and a HIPPS function. The system is illustrated in Figure 2 below; Instead of installing a conventional pressure protection solution with a PSD valve and a process safety valve (PSV), the PSD valve is combined with an instrumented barrier, the so-called HIPPS. These two systems shall protect the downstream equipment (having a lower design pressure) from overpressure.

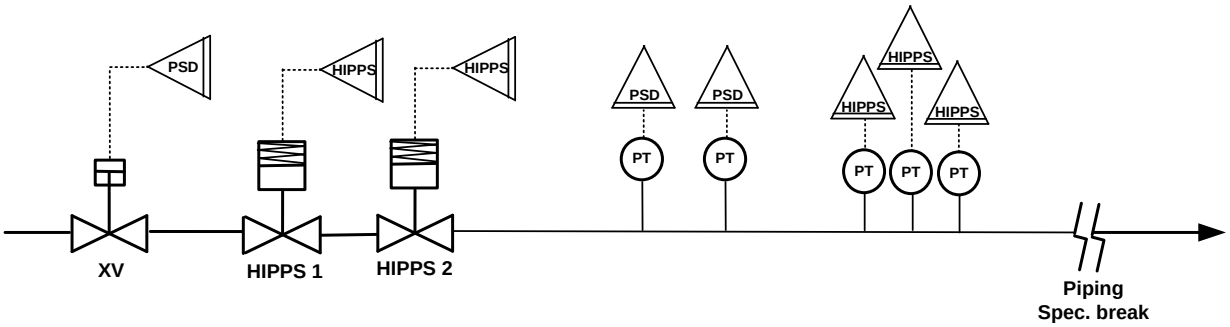


Figure 2: Pressure protection system for a piping spec. break concept

Figure 3 and Figure 4 give a somewhat more detailed description of the two protection functions.

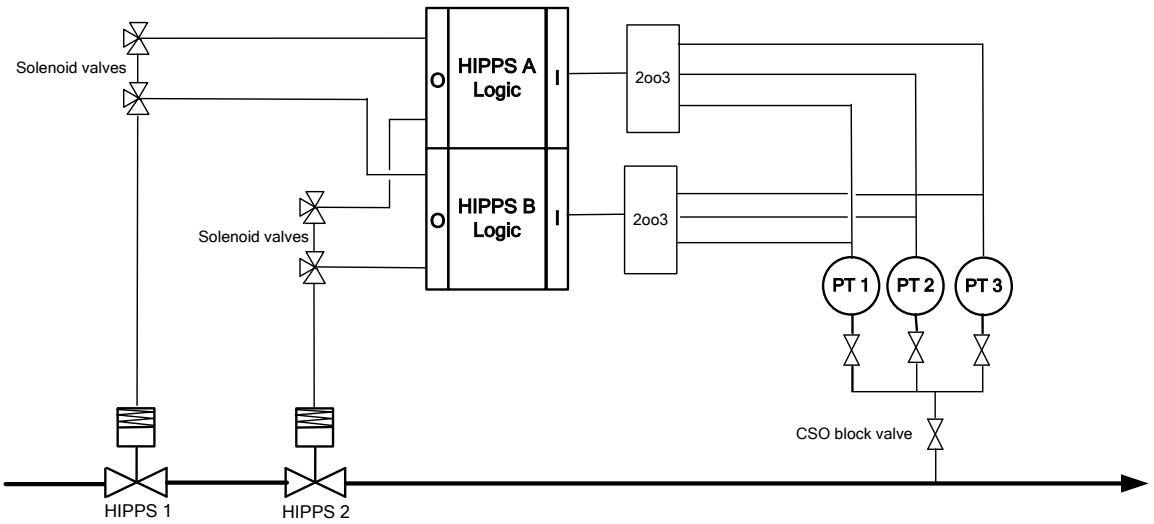


Figure 3: Schematic of HIPPS function

The HIPPS has a 2oo3 voted system for the pressure transmitters (PTs), a redundant hardwired HIPPS logic, and two HIPPS valves voted 1oo2. Each valve is equipped with two solenoid/pilot valves so that each logic unit can close down both HIPPS valves. The PTs are installed on a common connection point with a locked open (car seal open - CSO) block valve towards the process piping.

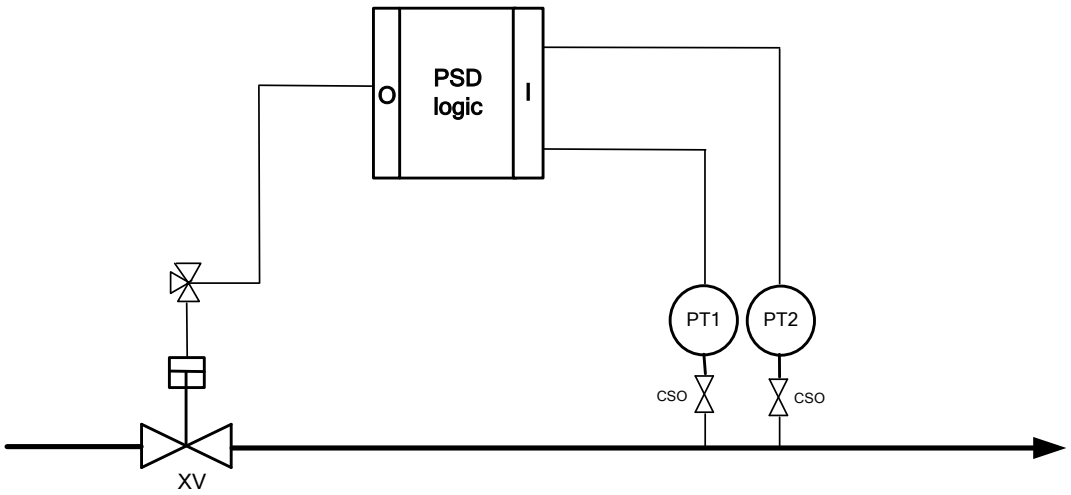


Figure 4: Schematic of PDS function

The PSD function here comprises a single programmable safety system with analogue input, CPU and digital output, as well as redundant PTs which upon activation (both) shuts down the XV (i.e. a 1oo2 voting on the PTs).

Abbreviations

The following *equipment related abbreviations* are used only in this example:

CSO	-	Car Seal Open
PSV	-	Process Safety Valve
PT	-	Pressure transmitter
XV	-	Shutdown valve

3.2.2 Assumptions and limitations

Relevant assumptions and limitations are listed in Table 3 and Table 4 below.

Table 3: Analytical assumptions for example 1

No.	Description of assumption / limitation
1	For calculating the PFD figures the formulas in Table A.1 in Appendix A of this example collection have been applied. These formulas are based on the assumptions and limitations listed in section 5.2 in the method handbook, /1/, and will not be repeated here.
2	The β-factor between the HIPPS and the PSD logic is assumed to be low due to diverse technology, i.e. hardwired HIPPS logic versus programmable PSD logic. In ref. /2/ the β-factor for HIPPS logic and PSD logic is assumed to be 0.03 and 0.05 respectively. The β-factor between the HIPPS and the PSD logic must be assumed to be significantly lower than this and here a β-factor of 0.01 has been applied.
3	The β-factor *between* different types of valves, i.e. HIPPS valves and PSD valve (XV) is assumed to be somewhat lower than the β-factor for the valves themselves due to different make and different actuator strength. However, the degree of diversity between the valves is not comparable to the case above with hardwired versus programmable logic. In ref. /2/ the β-factor for shutdown valves is assumed to be 0.03, and for the β-factor *between* the HIPPS valves and the PSD valve a slightly lower value of 0.02 has here been applied.

No.	Description of assumption / limitation
4	A β-factor of 0.04 is assumed for the transmitter in the PSD function based on PDS data. For the transmitters in the HIPPS function we assume a β-factor of 0.10 due to the common connection point (ref. system description). For the combined HIPPS and PSD function, a common β-factor for all transmitters, β^*, is assumed to be 0.06 which is the geometric mean of the beta factors for the transmitters in the PSD and HIPPS function, respectively: $\beta^* = \sqrt{0.04 \cdot 0.10} = 0.06$.
5	Since the main purpose of this example is to illustrate modelling of a system with several protection functions, the P_{TIF} has *not* been included in the calculations for this example. This is in line with IEC 61508/61511 where only the PFD is estimated, but may give non-conservative results. Note that example 3 (section 3.4) shows a case with reduced test coverage and the use of P_{TIF}.

Table 4: Assumptions related to design and operation for example 1

No.	Description of assumption / limitation
6	A functional test interval of 3 months (2190 hours) is assumed for all the HIPPS components.
7	The PSD function is assumed tested once every year.
8	Upon a downstream blockage, it is assumed that the PSD function is able to respond fast enough to prevent any critical overpressures. The HIPPS is expected to respond if the PSD function fails.
9	No degraded operation is assumed in this example. Upon failure or testing of any component, the system will be shut down. Hence no DTU (Downtime unavailability) contributions are assumed.
10	No inhibition or override of the PSD or HIPPS function is assumed to take place during normal operation.

3.2.3 Reliability modelling

It is suggested to first study the PSD and HIPPS functions separately. Each RBD is split into three main parts: sensors, logic solvers, and actuating devices. A second step is to develop a RBD that includes both functions (Figure 7). Here, the PSD and the HIPPS functions are placed in parallel branches since it is sufficient that either the PSD or the HIPPS function is able to stop flow in order to avoid overpressure. The contributions from CCFs are included as additional (shaded) elements in the RBDs.

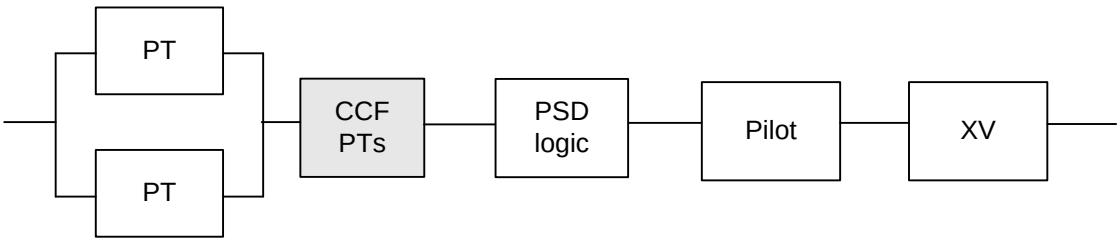


Figure 5: RBD for the PSD function

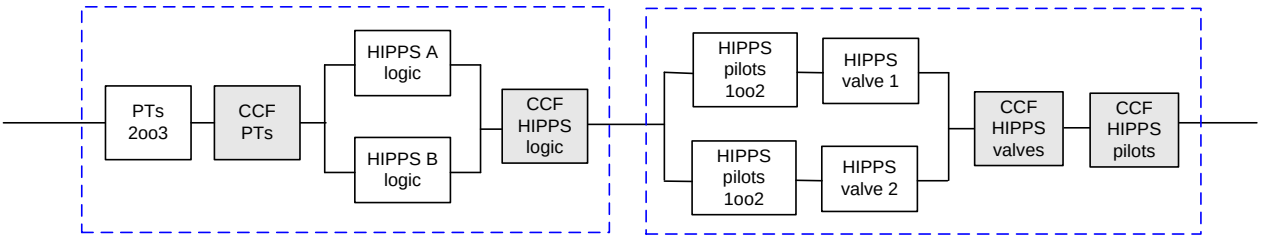


Figure 6a: RBD for the HIPPS function (sensors and logic to the left and final elements to the right in the RBD)

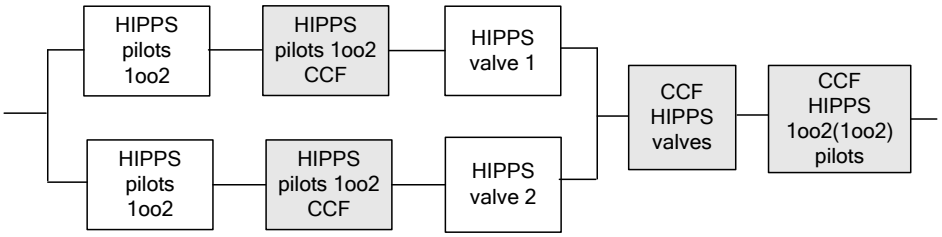


Figure 6b: Slightly restructured RBD for the HIPPS valves and pilots

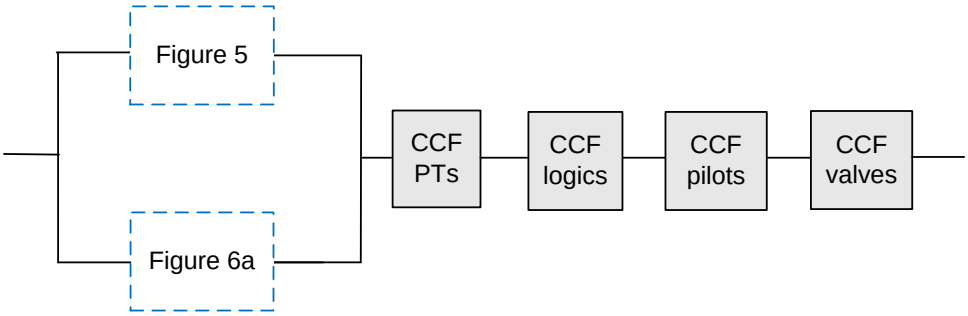


Figure 7: RBD for the combined HIPPS (upper branch) and PSD function (lower branch)

3.2.4 Reliability data

The reliability data utilized in this example are listed in Table 5.

Table 5: Reliability data for the HIPPS and PSD system

Component	λ_{DU} *(per hour)*	β	Comments and reference
Pressure transmitter (PT)	$0.3 \cdot 10^{-6}$	0.04	Failure rate: Ref. /2/. Assuming coverage of 60% for dangerous failures for pressure transmitters. β-factors: β = 0.04 is assumed for the PSD transmitters, ref. /2/. For the HIPPS transmitters a β = 0.10 is applied due to the common connection point leading to possibility of plugging of sensor line (the PSD transmitters are assumed to have different connection points). For the combined PSD and HIPPS function the geometric mean of the two beta factors 0.04 and 0.10 have been used, which gives a common beta factor of 0.06. Note that in order to ensure robustness, the minimum β has not been chosen since the PTs are assumed to be of the same type and the impulse lines located relatively close.
		0.10	
		0.06	
Trip amplifier / analogue input (HIPPS)	$0.04 \cdot 10^{-6}$	0.03	Ref. /2/. Data for hardwired safety system.
Hardwired HIPPS logic	$0.03 \cdot 10^{-6}$		
Digital output (HIPPS)	$0.03 \cdot 10^{-6}$		
Analogue input, AI (PSD)	$0.16 \cdot 10^{-6}$	NA	Ref. /2/. Assuming single safety PLC.
CPU (PSD)	$0.48 \cdot 10^{-6}$		
Digital output, DO (PSD)	$0.16 \cdot 10^{-6}$		
Pilot valve	$0.8 \cdot 10^{-6}$	0.10	Assumed a β of 0.10 for pilots on same valve and 0.03 for pilots on different valves, ref. /2/
		0.03	
Shutdown valve (HIPPS, XV)	$2.1 \cdot 10^{-6}$	0.03	Ref. /2/. Assuming the same failure rate for the HIPPS valves as for a standard shutdown valve (ESV/XV).

3.2.5 Reliability calculations

The RBDs in Figure 5 - 7 are used as basis for establishing formulas for calculating the PFD.

PSD function

For small PFD values, an adequate approximation of the total PFD is achieved by adding the PFD of each subsystem. With basis in Appendix A, Table A.1, we may set up the following formulas:

$$\mathrm{PFD}_{\mathrm{PSD}} = \mathrm{PFD}_{\mathrm{PT}}^{(\mathrm{ind})} + \mathrm{PFD}_{\mathrm{PT}}^{(\mathrm{CCF})} + \mathrm{PFD}_{\mathrm{logic}} + \mathrm{PFD}_{\mathrm{pilot}} + \mathrm{PFD}_{\mathrm{valve}} =$$

$$(\lambda_{\mathrm{DU,PT}} \cdot \tau)^2 / 3 + \beta \cdot \lambda_{\mathrm{DU,PT}} \cdot \frac{\tau}{2} + (\lambda_{\mathrm{DU,AI}} + \lambda_{\mathrm{DU,CPU}} + \lambda_{\mathrm{DU,DO}}) \cdot \frac{\tau}{2} + \lambda_{\mathrm{DU,pilot}} \cdot \frac{\tau}{2} + \lambda_{\mathrm{DU,valve}} \cdot \frac{\tau}{2} =$$

$$\left(0.3 \cdot 10^{-6} \cdot 8760\right)^2 / 3 + 0.04 \cdot 0.3 \cdot 10^{-6} \cdot \frac{8760}{2} + 0.8 \cdot 10^{-6} \cdot \frac{8760}{2} + 0.8 \cdot 10^{-6} \cdot \frac{8760}{2} + 2.1 \cdot 10^{-6} \cdot \frac{8760}{2} =$$

$$2.3 \cdot 10^{-6} + 5.3 \cdot 10^{-5} + 3.50 \cdot 10^{-3} + 3.50 \cdot 10^{-3} + 9.20 \cdot 10^{-3} = \underline{1.6 \cdot 10^{-2}}$$

Remarks:
The single elements in the RBD, i.e. the logic solver, solenoid/pilot valve, and the XV valve, are the main contributors to the total PFD. The pressure transmitters have minor contribution due to the redundancy, and for the transmitters the PFD is mainly influenced by the CCFs.

HIPPS function
The HIPPS function becomes more complicated than the PSD function, as is seen from the RBD in Figure 6a. As will be further discussed, it is the HIPPS solenoids/pilots and valves that give some calculation challenges. As a first step, we exclude these components and first calculate the PFD for the transmitters and HIPPS logic (within the leftmost dotted rectangle in Figure 6a), which is rather straight forward. Again, the formulas are based on table A.1:

$$\mathrm{PFD}_{\mathrm{HIPPS\,PTs}+\mathit{HIPPS}\,1oo2\,\mathrm{logic}} = \mathrm{PFD}^{(\mathrm{ind})}_{2oo3\mathrm{PTs}} + \mathrm{PFD}^{(\mathrm{CCF})}_{2oo3\mathrm{PTs}} + \mathrm{PFD}^{(\mathrm{ind})}_{1oo2\mathrm{logic}} + \mathrm{PFD}^{(\mathrm{CCF})}_{1oo2\mathrm{logic}} =$$

$$(\lambda_{\mathrm{DU,\,PT}}\cdot\tau)^2 + C_{2oo3}\cdot\beta_{\mathrm{PT}}\cdot\lambda_{\mathrm{DU,PT}}\cdot\frac{\tau}{2} + ((\lambda_{\mathrm{DU,\,AI}} + \lambda_{\mathrm{DU,\,logic}} + \lambda_{\mathrm{DU,\,DO}})\cdot\tau)^2/3$$

$$+\beta_{\mathrm{logic}}\cdot(\lambda_{\mathrm{DU,AI}} + \lambda_{\mathrm{DU,\,logic}} + \lambda_{\mathrm{DU,\,DO}})\cdot\frac{\tau}{2} =$$

$$\left(0.3\cdot10^{-6}\cdot2190\right)^2 + 2.0\cdot0.10\cdot0.3\cdot10^{-6}\cdot\frac{2190}{2} + \left(0.1\cdot10^{-6}\cdot2190\right)^2/3 + 0.03\cdot0.1\cdot10^{-6}\cdot\frac{2190}{2} =$$

$$4.3\cdot10^{-7} + 6.6\cdot10^{-5} + 1.6\cdot10^{-8} + 3.3\cdot10^{-6} = \underline{6.9\cdot10^{-5}}$$

Remarks:
The PFD of the HIPPS transmitters and logics is mainly influenced by CCFs, and from the above expression it is seen that the transmitters have the highest contribution.

Calculating the PFD for the HIPPS pilots and valves, requires a slightly restructuring of the rightmost dotted rectangle of the RBD in Figure 6a, as shown in Figure 6b.

Observe that a simultaneous failure of both pilots for HIPPS valve 1 in combination with a failure of HIPPS valve 2, (and vice versa) lead to a system failure. Therefore, a separate element, representing CCF of two pilot valves on the same HIPPS valve, has been added in each branch of the RBD. The remaining contributions from CCFs are modelled as separate elements in series to the parallel branches: First, the CCF of the HIPPS valves, and second, the contribution from CCF that may affect *all* four pilot valves.

We start off by calculating the PFD for the two parallel branches in Figure 6b (i.e. independent failure of both HIPPS valves). First we have to make some remarks concerning the calculations:

- We first calculate the PFD of each branch, which will comprise the sum of three PFD terms: independent failure of two pilots, CCF of two pilots and failure of one HIPPS valve.
- By simply multiplying the total PFD of each branch together we will obtain a non-conservative estimate, since the failure probability is actually increasing with time and the HIPPS components are assumed tested simultaneously.
- As discussed in Appendix A, a correction factor therefore has to be applied when multiplying the PFDs. Since the two parallel branches represent a 1oo2 voting, we will here (for simplicity) apply a correction factor of 4/3, which actually applies for a 1oo2 redundant structure of two components.

Hence, we get the following equation for the PFD of the parallel branches in Figure 6b:

$$\mathrm{PFD}_{\mathrm{pilots+valves}}^{(\mathrm{ind})} = \frac{4}{3}\cdot\left[\mathrm{PFD}_{\mathrm{1oo2\,pilots}}^{(\mathrm{ind})} + \mathrm{PFD}_{\mathrm{1oo2\,pilot}}^{(\mathrm{CCF})} + \mathrm{PFD}_{\mathrm{HIPPS\,valve}}\right]^2 =$$

$$\frac{4}{3}\cdot\left[\left(\lambda_{\mathrm{DU,\,pilot}}\cdot\tau\right)^2/3 + \beta_{\mathrm{pilot}}\cdot\lambda_{\mathrm{DU,\,pilot}}\cdot\frac{\tau}{2} + \lambda_{\mathrm{DU,\,valve}}\cdot\frac{\tau}{2}\right]^2 =$$

$$\frac{4}{3}\cdot\left[\left(0.8\cdot10^{-6}\cdot2190\right)^2/3 + 0.1\cdot0.8\cdot10^{-6}\cdot\frac{2190}{2} + 2.1\cdot10^{-6}\cdot\frac{2190}{2}\right]^2 =$$

$$\frac{4}{3}\cdot\left[1.0\cdot10^{-6} + 8.8\cdot10^{-5} + 2.30\cdot10^{-3}\right]^2 = 7.6\cdot10^{-6}$$

For the remaining elements of the RBD in Figure 6b, we first consider the CCF for the HIPPS valves:

$$\mathrm{PFD}_{\mathrm{HIPPS\,valves}}^{(\mathrm{CCF})} = \beta_{\mathrm{valve}}\cdot\lambda_{\mathrm{DU,\,valve}}\cdot\frac{\tau}{2} = 0.03\cdot2.1\cdot10^{-6}\cdot\frac{2190}{2} = 6.9\cdot10^{-5}$$

The PFD for the last element of the RBD, i.e. the CCF affecting all four pilot valves, is calculated with basis in the method in Appendix E.2 in the PDS method handbook, /1/. For the calculation, the components are treated as a 1oo2x1oo2 configuration, with an "inner voting" and an "outer voting". Here, the beta factor for the inner voting (β_{inner}) will be the assumed beta for the pilots on the same HIPPS, i.e. 0.10, and the beta of the outer voting (β_{outer}) will be the assumed beta for pilots on different valves, i.e. 0.03.

As further described in section E.2 in /1/, the CCF contribution can then be estimated using the following formula:

$$\mathrm{PFD}_{\mathrm{1oo2x1oo2\ pilots}}^{(\mathrm{CCF})} = 0.30\cdot\beta_{mean}\cdot PFD_0\,.$$

Here, β_{mean} is the combined (mean) beta factor for the inner and outer voting and:$\mathrm{PFD}_0 \approx \lambda_{\mathrm{DU}}\cdot\tau/2$. Following section E.2 in /1/ and taking the arithmetic mean of the two beta factors, we then have:

$$\mathrm{PFD}_{\mathrm{1oo2\ x\ 1oo2\ pilots}}^{(\mathrm{CCF})} = 0.30\cdot\beta_{\mathrm{mean}}\cdot\lambda_{\mathrm{DU,\,pilot}}\cdot\frac{\tau}{2} = 0.30\cdot0.065\cdot0.8\cdot10^{-6}\cdot\frac{2190}{2} = 1.7\cdot10^{-5}\,.$$

Now, the total contribution from the right part of the RBD in Figure 6a becomes:

$$\mathrm{PFD}_{\mathrm{pilots+valves}} = \mathrm{PFD}_{\mathrm{pilots+valves}}^{\mathrm{ind}} + \mathrm{PFD}_{\mathrm{pilots+valves}}^{(\mathrm{CCF})} = 7.6\cdot10^{-6} + (6.9+1.7)\cdot10^{-5} = 9.4\cdot10^{-5},$$

i.e. the total estimated PFD for the HIPPS function becomes:

$$\mathrm{PFD}_{\mathrm{HIPPS}} = \mathrm{PFD}_{\mathrm{PTs+logics}} + \mathrm{PFD}_{\mathrm{pilots+valves}} = 6.9\cdot10^{-5} + 9.4\cdot10^{-5} = \underline{1.6\cdot10^{-4}}\,.$$

Combined HIPPS and PSD function

For the combined pressure protection function including both the HIPPS function and the PSD function (See RBD in Figure 7) the main challenge is the calculation of the CCFs between non-identical components from the PSD and the HIPPS function respectively (ref. discussion in section 2.2). In this case we have to deal with both non-identical failure rates and different test intervals in addition to beta factors between non-identical components. Here we have chosen to use geometric means for the failure rates and arithmetic mean

for the test intervals (ref. section 2.2.5) whereas the β-factors between non-identical components have been assessed based on expert judgements (see Table 3). Further discussion of the topic is included in section 3.2.6.

When considering the two redundant branches to the left in the RBD in Figure 7 we can estimate that the contribution from independent failure of the HIPPS and the PSD function will be in the same *order of magnitude* as the product of the PFDs for the two functions. Consequently the contribution from independent failure of HIPPS and PSD will be *in the order of* $1.6 \cdot 10^{-2} \cdot 1.6 \cdot 10^{-4} \approx 2.5 \cdot 10^{-6}$. Following the discussion given above, where the independent PFD contribution from two parallel branches (for the pilots and valves of the HIPPS function) was quantified, this expression could also be multiplied with the factor 4/3.

Next the contribution from the CCFs between HIPPS and PSD is estimated. A possible approach for doing this is described below, given the following assumptions:

- There are 5 PTs. The PSD function is available as long as one of its two PTs is functioning, whereas the HIPPS function will be available with two PTs functioning. Consequently, overpressure protection is *always* available if two (or more) PTs are functioning and *sometimes* available with only on PT functioning. It may therefore be argued that a weighted average of C_{1oo5} and C_{2oo5} could be applied. However, we will here conservatively consider this as a 2oo5 configuration and will apply $C_{2oo5} = 0.7$.

- Three out of five transmitters with a test interval of 2190 hours (HIPPS function) and two out of five transmitters with a test interval of 8760 hours (PSD function) results in an average test interval for the transmitters of $3/5 \cdot 2190 + 2/5 \cdot 8760 = 4818$ hours.

- $\beta = 0.06$ is assumed for the transmitters (see Table 3 and Table 5).

- The HIPPS logic is redundant (1oo2) and the PSD logic is single. Hence, this can be considered a 1oo3 voting configuration since it is sufficient that one of the logic units work. Due to diversity between the HIPPS and the PSD we will as discussed in section 3.2.2 apply a $\beta = 0.01$. Two logic units with a test interval of 2190 hours and one logic unit with a test interval of 8760 hours yield an average test interval of $2/3 \cdot 2190 + 1/3 \cdot 8760 = 4380$ hours.

- There are 5 solenoid/pilot valves; two on each of the two HIPPS valves and one on the PSD valve. Since the pilots on each HIPPS valve are voted 1oo2, it is actually sufficient that either of the pilots function. Hence, the pilots can be considered a 1oo5 configuration and we can apply $C_{1oo5} = 0.21$. Due to diversity we will apply $\beta = 0.03$ for the pilots (see Table 5). With four pilots being tested every 2190 hours and one pilot being tested every 8760 hours, the average test interval becomes: $4/5 \cdot 2190 + 1/5 \cdot 8760 = 3504$ hours.

- There are two redundant HIPPS valve and a single PSD valve. Hence, this can be considered a 1oo3 voting configuration since it is sufficient that one of the valves close. Due to diversity between the HIPPS valves and the PSD valve we will as discussed in section 3.2.2 apply $\beta = 0.02$. Two valves with a test interval of 2190 hours and one valve with a test interval of 8760 hours give an average test interval of 4380 hours (as for the logics).

Based on these assumptions, the PFD may be approximated as:

$$\mathrm{PFD}_{\mathrm{PSD+HIPPS}}^{\mathrm{CCF}} = \mathrm{PFD}_{\mathrm{PTs}}^{(\mathrm{CCF})} + \mathrm{PFD}_{\mathrm{logics}}^{(\mathrm{CCF})} + \mathrm{PFD}_{\mathrm{pilots}}^{(\mathrm{CCF})} + \mathrm{PFD}_{\mathrm{valves}}^{(\mathrm{CCF})} =$$

$$C_{2oo5} \cdot \beta_{\mathrm{PT}}^{*} \cdot 0.3 \cdot 10^{-6} \cdot \bar{\tau}_{\mathrm{PT}} / 2 + C_{1oo3} \cdot \beta_{\mathrm{mixed\,logics}} \cdot \sqrt[3]{1.0 \cdot 10^{-6} \cdot \left(0.1 \cdot 10^{-6}\right)^2} \cdot \bar{\tau}_{\mathrm{logics}} / 2$$

$$+ C_{1oo5} \cdot \beta_{\mathrm{mixed\,pilots}} \cdot 0.8 \cdot 10^{-6} \cdot \bar{\tau}_{\mathrm{pilots}} / 2 + C_{1oo3} \cdot \beta_{\mathrm{mixed\,valves}} \cdot 2.1 \cdot 10^{-6} \cdot \bar{\tau}_{\mathrm{valves}} / 2 =$$

$$0.7 \cdot 0.06 \cdot 0.3 \cdot 10^{-6} \cdot 4818 / 2 + 0.5 \cdot 0.01 \cdot 2.2 \cdot 10^{-7} \cdot 4380 / 2$$

$$+ 0.21 \cdot 0.03 \cdot 0.8 \cdot 10^{-6} \cdot 3504 / 2 + 0.5 \cdot 0.02 \cdot 2.1 \cdot 10^{-6} \cdot 4380 / 2 =$$

$$3.04 \cdot 10^{-5} + 2.4 \cdot 10^{-6} + 8.8 \cdot 10^{-6} + 4.60 \cdot 10^{-5} = \underline{8.8 \cdot 10^{-5}}$$

3.2.6 Summary and discussion of results

The below table summarizes the results from the reliability calculations in this example.

Table 6: Summary of results for example 1

Function	Estimated PFD
PSD function	$1.63 \cdot 10^{-2}$
HIPPS function	$1.6 \cdot 10^{-4}$
Combined HIPPS and PSD function	$9.1 \cdot 10^{-5}$

It may be noted that the PFD for the HIPPS function alone and PFD of the combined HIPPS and PSD function are approximately of the same magnitude (just a 45% reduction in PFD from having added the PSD to the HIPPS function). Intuitively, we may have expected a higher reduction in the PFD from adding the PSD. The main explanation is the use of similar components in the two functions; if a CCF exist among similar components in one function, it is likely that also other similar components are affected. Or said in another way; when having a system with extensive redundancy, the (calculated) effect of adding even more redundancy is limited due to the way that CCF failures are being modelled.

Note that if we simply multiply the PFD of the PSD function with the PFD of the HIPPS function, assuming the two functions to be totally independent, which is often done in e.g. event tree analysis and in LOPA (layer of protection analysis), we obtain a total PFD in the order of $3.0 \cdot 10^{-6}$. This a factor 30 lower than the above calculated PFD for the combined HIPPS and PSD function, showing the importance of considering potential common cause failures between (non-identical and identical) components in different functions.

We have in this example chosen to use RBDs to model the PSD, the HIPPS and the combined PSD + HIPPS function. Alternatively a fault tree could have been constructed, in which case the minimal cut sets could have been identified, using the approach in e.g., /9/. Applying this approach, may lead to slightly different results due to some of the assumptions and simplifications that we made for the formulas that were deduced from the RBDs. However, also in the fault tree we would have to deal with common cause failures among identical and non-identical components and therefore the same elements (i.e. CCFs) would still dominate the contribution to the total PFD.

3.3 Example 2 – Shutdown of multiple pipe runs

3.3.1 System description

A high pressure rich gas pipeline is arriving at an onshore processing plant for further processing into dry gas. In order to reduce the pressure prior to processing, the gas is routed through a pressure letdown station. The pressure letdown station comprises four pipe runs. Each run is equipped with a quick shut-off valve (QSV) and a control valve (CV) that shall close on high pressure. A conventional PSV station is installed downstream of the letdown station, which is able to handle full flow through *one* fully open pipe run at the worst possible pressure difference. Hence, in order to prevent overpressure upon a downstream blockage, at least three of the four pipe runs must close. The challenges in calculating the reliability for such a system is mainly related to modelling of system complexity and modelling of CCFs between multiple components.

The letdown station is illustrated in Figure 8.

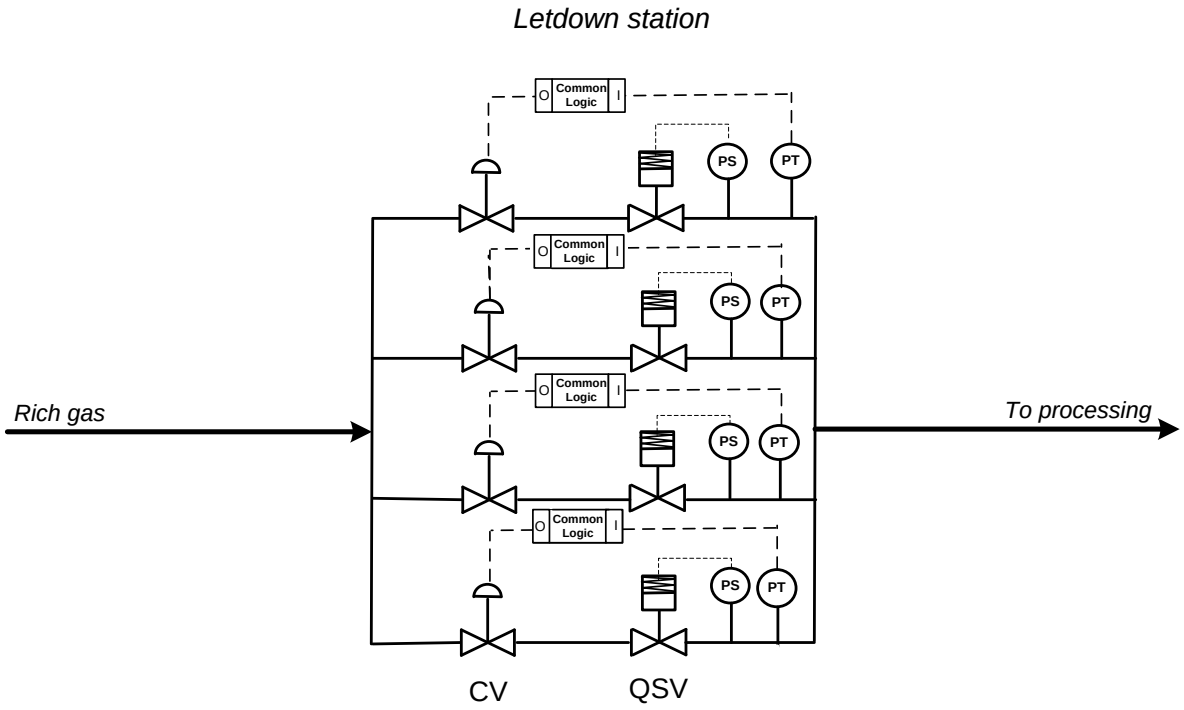


Figure 8: System description of the 3oo4 letdown station with CV and QSV on each run

Each of the four parallel runs consists of one CV equipped with a "HIPPS function". The (common) single hardwired "HIPPS logic" will respond by closing the CV when the pressure reading from the PT exceeds a certain limit. Each run is also equipped with a QSV which is automatically closed when the pressure switch (PS) is activated.

Abbreviations

The following *equipment related abbreviations* are used only in this example:

CV	-	Control valve
PS	-	Pressure switch
QSV	-	Quick shut-off valve

3.3.2 Assumptions and limitations

Limitations and assumptions concerning the system and the reliability modelling are summed up in Table 7 and Table 8.

Table 7: Analytical assumptions for example 2

No.	Description of assumption
1	The PFDs are calculated using the formulas in Table A.1 in Appendix A. These formulas are based on the assumptions and limitations listed in section 5.2 in the method handbook, /1/, and will not be repeated here.
2	The possibility of two or more runs failing *independently* of each other (within the same test interval) will require independent failure of at least three components and can therefore be disregarded due to very low probabilities.
3	The CV and the associated solenoid valve have an assumed total failure rate of $4 \cdot 10^{-6}$ per hour, based on Table 9 on page 32.
4	Since the analogue pressure transmitter signal is not continuously monitored, a coverage c_D of only 50% has been assumed for the PT, giving a λ_{DU} of $0.4 \cdot 10^{-6}$ per hour (as compared to $0.3 \cdot 10^{-6}$ per hour in /2/).
5	The QSV and the associated pilot valve have an assumed total failure rate of $2.9 \cdot 10^{-6}$ per hour based on data in Table 9 on page 32.
6	A β-factor for common cause failures *between* CV and QSV must be estimated. In ref. /2/ the β-factor for shutdown valves and control valves is assumed to be 0.03. A CV and a QSV may be considered as relatively diverse technology. The β-factor *between* the CV and the QSV may therefore be assumed to take a low value, and in this example it has been set to 0.01. Also PTs and PSs may be considered as diverse technology. In ref. /2/ the β-factor for PTs and PSs is assumed to be 0.04 and 0.05, respectively. With diversity, β = 0.02 for CCF *between* PT and PS has been applied.
7	Since the main purpose of this example is to illustrate modelling of a relatively complex system with extensive degree of redundancy, the P_{TIF} has *not* been included in the calculations for this example. Note that example 3 (section 3.4) shows a case with reduced test coverage and the use of P_{TIF}.

Table 8: Assumptions related to design and operation for example 2

No.	Description of assumption
8	It is implicitly assumed that both the CVs and the QSVs have sufficiently short response times to prevent any high pressure situations arising. Further, it is assumed that the downstream PSV has sufficient capacity to cater for any internal leakages through the valves in closed position.
9	All components (CVs, QSVs, PTs and PSs) are assumed fully tested every 3rd month, i.e. a test interval of 2190 hours.
10	In order to avoid overpressure it is under all conditions sufficient that three of the four runs close. In order to close one run it is sufficient that at least one valve on the run closes.
11	All the QSVs and the CVs are equipped with single solenoid valves.

No.	Description of assumption
12	No degraded operation is assumed in this example. Upon failure or testing of any component, the complete letdown system will be shut down. Hence no DTU (Downtime unavailability) contributions are assumed.
14	No inhibition or override of the transmitters or logic activating the QSVs or the CVs is assumed to take place during normal operation.

3.3.3 Reliability modelling

There are several alternative approaches for estimating the PFD for the high pressure protection in relation to the letdown station. In this example, the PFD is estimated based on the possible *combinations of success scenarios*, i.e., by considering ways to maintain overpressure protection in the presence of combinations of failures related to the QSVs, the CVs, the PSs, the PTs and logic.

The letdown station provides successful overpressure protection as long as three out of four runs are closing upon demand. This means that the overpressure protection in relation to the letdown station tolerates one, but not two or more pipe run failures. To obtain shutdown of a given run it is sufficient that either the CV or the QSV (or both) on the run closes.

Since the PT, the PS, the QSV, the logic, and the CV from a reliability modelling perspective are single elements within each run, we are mainly concerned with CCFs among components in *different* runs. The modelling is not straight forward, but a possible approach is explained below.

3.3.4 Reliability data

The reliability data for this example are listed in Table 9 below. The data applied are obtained from the new PDS data handbook, ref. /2/.

Table 9: Reliability data for example 2

Component	λ_{DU} *(per hour)*	β	Comments and reference
Pressure switch (PS)	$2.0 \cdot 10^{-6}$	0.05	Ref. /2/.
Pressure transmitter (PT)	$0.4 \cdot 10^{-6}$	0.04	Ref. /2/. Since the analogue PT signal is not continuously monitored, a coverage c_D of only 50% has been assumed for the PT, giving a slightly higher λ_{DU} as compared to /2/.
Hardwired safety system, incl. trip amplifier / analogue input and digital output	$0.1 \cdot 10^{-6}$	0.03	Ref. /2/.
Pilot/solenoid valve	$0.8 \cdot 10^{-6}$	0.03	Ref. /2/. Beta value for solenoids on different valves.
Control valve (CV)	$3.5 \cdot 10^{-6}$	0.03	Control valve applied for shutdown service only, ref. /2/.
Quick shut-off valve (QSV)	$2.1 \cdot 10^{-6}$	0.03	Assumed same failure rate as for conventional shutdown valves (ESV/XV), ref. /2/.

3.3.5 Reliability calculations

There are several combinations of "simultaneous" component failures (i.e., failures occurring within the test interval) that may lead to system failure; i.e. two (or more) runs failing. Translated to a RBD, which is success oriented, we need to identify all the combinations of valves or sensors functioning that will lead to successful performance of the system. If any of these success combinations occur, the system provides successful overpressure protection.

Successful overpressure protection is achieved when at least three of the runs close. As seen in Figure 8 and from assumption no. 8 in Table 8, it is sufficient that one of the two valves on a run close in order for the run to close. In total there are four runs and 8 valves (2 valves on each run) that are supposed to close upon a high pressure situation. Examples of successful and unsuccessful combinations with three valves, four valves or five valves closing are illustrated in Figure 9.

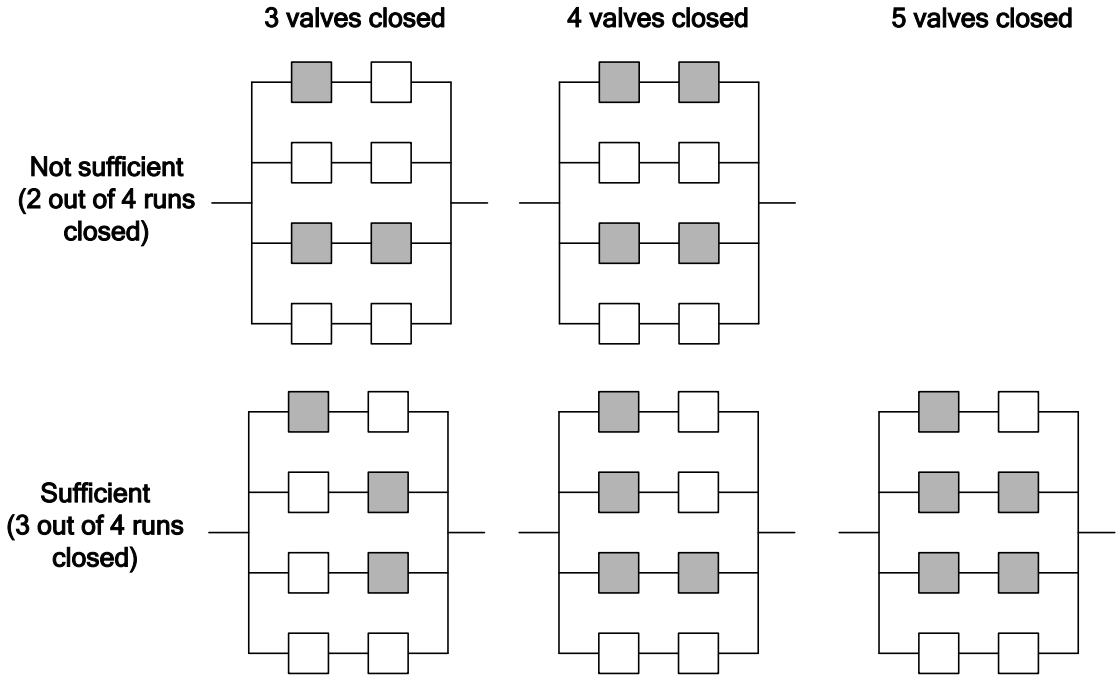


Figure 9: Examples of combinations of closing 3 valves, 4 valves and 5 valves. Grey illustrates closed valve, blank illustrates open valve.

A system with MooN voting will function if at least M out of N components functions (in this case close) on demand. Or said in another way the system can tolerate N-M failures, but not more. This means that the system *fails* if N-M+1 or more components *fail to close*. Thus, the factor C_{MooN} refers to a system that fails by failure of N-M+1 components or more; which means that at most M-1 are functioning/closing. So for instance, C_{4oo8} refers to a system that fails by failure of 8-4+1=5 or more components, (i.e. when at most 3 are functioning).

In our example, we see that sufficient overpressure protection is always achieved when 5 or more valves close (cf. Figure 9); so in this case the probability for three or more runs closing equals 1. And when just 2 valves close, the probability of three runs closing of course equals 0. But when either 3 or 4 valves close (i.e. 5 or 4 valves fail), sufficient overpressure protection is achieved only for *some* valve combinations (cf. Figure 9), i.e. the probability of three or more runs closing is then smaller than 1.

Since the factor C_{MooN} corresponds to a system that fails if M-1 or less components are functioning, it follows that $C^*_{MooN} = C_{(M+1)ooN} - C_{MooN}$ corresponds to functioning of exactly M components, (i.e. failure of exactly N-M components).

The PFD expression for the CCF contribution from the valves then becomes:

$$\mathrm{PFD}_{\mathrm{valves}}^{\mathrm{CCF}} = \left[C^*_{3oo8} \cdot \Pr(\geq 3 \text{ runs close} \mid 3 \text{ valves close}) + C^*_{4oo8} \cdot \Pr(\geq 3 \text{ runs close} \mid 4 \text{ valves close}) + C_{5oo8}\right] \cdot \beta_{\mathrm{valves}} \cdot \lambda_{DU}^{valves} \cdot \tau / 2$$

The factor that corresponds to failure of exactly 4 out of 8 components equals:

$$C^*_{4oo8} = C_{5oo8} - C_{4oo8} = 2.1 - 1.1 = 1.0$$

Similarly the factor that corresponds to failures of exactly 3 out of 8 components equals:

$$C^*_{3oo8} = C_{4oo8} - C_{3oo8} = 1.1 - 0.6 = 0.5$$

The applied C_{MooN} factors can be found in Table A.3 in Appendix A. For a general discussion of the C_{MooN} factors, reference is made to Appendix B of the PDS method handbook /1/.

In order to find the probabilities in the above PFD expression we use combinatorics, and the expressions for each of the probabilities for overpressure protection are derived below.

Pr(≥ 3 runs close | 4 valves close): There are in total 70 combinations with four out of eight valves being closed[2], but not all of them lead to successful overpressure protection. The overpressure protection *fails* if the four valves being closed are located in exactly two out of the four runs and where both the valves on the two runs close. This may occur in:

$$\binom{4}{2} \cdot \binom{2}{2} \cdot \binom{2}{2} = 6 \cdot 1 \cdot 1 = 6 \text{ combinations (out of the 70).}$$

Here the first factor refers to the closure of two runs (6 possible combinations) and the second and third factor refers to closure of both valves on each of the two runs (1 combination on each run). Thus, a successful overprotection when 4 valves are closed can be achieved in 70 – 6 = 64 out of 70 combinations, and hence

Pr(≥ 3 runs close | 4 valves close) = 64/70 = 0.9.

Pr(≥ 3 runs close | 3 valves close): There are in total 56 combinations with three out of eight valves can close[3]. The only way of achieving successful overpressure protection is when one valve close on three separate runs, for which there are

[2] The number of ways to combine 4 out of 8 valves, can be calculated using the formula: $\binom{8}{4} = \frac{8!}{(8-4)!\cdot 4!} = \frac{8!}{4!\cdot 4!} = 70$

[3] The number of ways to combine 3 out of 8 valves, can be calculated using the formula: $\binom{8}{3} = \frac{8!}{(8-3)!\cdot 3!} = \frac{8!}{5!\cdot 3!} = 56$

$$\binom{4}{3}\cdot\binom{2}{1}\cdot\binom{2}{1}\cdot\binom{2}{1} = 4\cdot 2\cdot 2\cdot 2 = 32 \text{ combinations (out of the 56).}$$

Hence,

$$\Pr(\geq 3 \text{ runs close} \mid 3 \text{ valves close}) = 32/56 = 0.6.$$

Further, when estimating the CCF contribution we will apply the geometric mean of the failure rates of the QSV and CV including the solenoids, which equals:

$$\lambda_{\mathrm{DU}}^{\mathrm{valves}} = \sqrt{\lambda_{\mathrm{DU,QSV}} \cdot \lambda_{\mathrm{DU,CV}}} = \sqrt{2.9\cdot 10^{-6}\cdot 4.3\cdot 10^{-6}} = 3.5\cdot 10^{-6}.$$

Finally, the β-factor between CV and QSV is assumed to be 0.01 (see assumptions). Then we can quantify the CCF contribution of the valves:

$$\begin{aligned}
&\mathrm{PFD}_{\mathrm{valves}}^{\mathrm{CCF}} \\
&= \left[C_{3\mathrm{oo}8}^{*}\cdot \Pr(\geq 3 \text{ runs close} \mid 3 \text{ valves close}) + C_{4\mathrm{oo}8}^{*}\cdot \Pr(\geq 3 \text{ runs close} \mid 4 \text{ valves close}) + C_{5\mathrm{oo}8}\cdot 1\right]\cdot \beta_{\mathrm{valves}}\cdot \lambda_{\mathrm{DU}}^{\mathrm{valves}}\cdot \tau/2 \\
&= (0.5\cdot 0.6 + 1.0\cdot 0.9 + 2.1)\cdot 0.01\cdot 3.5\cdot 10^{-6}\cdot 2190/2 = 3.3\cdot 0.01\cdot 3.5\cdot 10^{-6}\cdot 2190/2 = 1.3\cdot 10^{-4}
\end{aligned}$$

As for the valves, there are one PS and one PT on each run giving a total of eight components. Thus, the similar approach as derived for the valves also applies for the PS and PT for the CCF contribution quantification. Applying a β-factor between the PS and PT of 0.02 (see assumptions) we get the following CCF contribution:

$$\begin{aligned}
&\mathrm{PFD}_{\mathrm{valves}}^{\mathrm{CCF}} \\
&= \left[C_{3\mathrm{oo}8}^{*}\cdot \Pr(\geq 3 \text{ runs close} \mid 3 \text{ PS/PT close}) + C_{4\mathrm{oo}8}^{*}\cdot \Pr(\geq 3 \text{ runs close} \mid 4 \text{ PS/PT close}) + C_{5\mathrm{oo}8}\cdot 1\right]\beta_{\mathrm{PS/PT}}\cdot \lambda_{\mathrm{DU}}^{\mathrm{PS/PT}}\cdot \tau/2 \\
&= 3.3\cdot 0.02\cdot \sqrt{\lambda_{\mathrm{PS}}\cdot \lambda_{\mathrm{PT}}}\cdot 2190/2 = 3.3\cdot 0.02\cdot \sqrt{2.0\cdot 10^{-6}\cdot 0.4\cdot 10^{-6}}\, 2190/2 = 3.3\cdot 0.02\cdot 0.9\cdot 10^{-6}\cdot 2190/2 = 6.5\cdot 10^{-5}
\end{aligned}$$

The entire CCF contribution towards the unavailability of the letdown station can then be estimated by the following formula:

$$\mathrm{PFD}_{3\mathrm{oo}4\,\mathrm{runs}}^{\mathrm{CCF}} = \mathrm{PFD}_{\mathrm{PSs\text{-}PTs}}^{\mathrm{CCF}} + \mathrm{PFD}_{\mathrm{QSVs\text{-}CVs}}^{\mathrm{CCF}} = 1.3\cdot 10^{-4} + 6.5\cdot 10^{-5} = \underline{2.0\cdot 10^{-4}}$$

Remarks:

Note that we in the above calculations have only considered CCF between QSVs and CVs and between PTs and PSs. The reasoning behind this is as follows: Remember that in order to get a system failure we need simultaneous failure of both a QSV and a CV on two or more runs. Clearly, a CCF of several identical components will be more likely than a failure of say a PT and a PS. However, since diverse components on each run must fail, a CCF of e.g. all the PTs or all the CVs will in addition require *other* components to fail. We are then facing several independent failures, the contribution from which is considered negligible in this example.

3.3.6 Discussion of results

For systems like the one considered here, where a high number of components have to fail in order to get a system failure, we see that modelling of common cause failures between multiple components becomes essential for the results obtained. This is generally a major challenge in reliability calculations due to the fact that there are little or no field data available on common cause failures of multiple components.

We have performed the reliability calculations of the shutdown system based on an approach where a weighted C-factor has been estimated and applied to calculate the CCF contribution from failures between non-identical multiple components. An alternative approach to this could have been to model explicitly the causes that may result in failure of all the components involved in a system failure. This will require (1) finding the relevant causes, (2) using expert judgements to determine the frequency of occurrence of these causes, and (3) use expert judgements to estimate how often the occurring causes result in failure of all components. Since experience data on the two latter issues will hardly be available, this approach will be difficult, but given the right experts, may result in additional qualitative insight. Another alternative is by simulation. However, such complex problems will probably require extensive programming since there may not be tailor made software systems for such complex systems. In addition, also simulation will require estimates for the various CCF rates.
Again, the geometric mean of failure rates in combination with suggested beta values (smaller than the beta values for identical components), are used throughout the calculations. As discussed in section 2.2 this seems to lead to a reasonable result when the PFDs are of comparable magnitude.

Similar as for example 1, it is the contribution from CCFs among non-identical components (CVs and QSVs, and PTs and PSs) that dominate the PFD. Given that we had only considered CCFs among identical components, i.e. among PTs, among PSs, among CVs and among QSVs, the resulting PFD would as discussed above, have become significantly lower. Hence, again the example illustrates the importance of including potential common cause failures also between non-identical components when modelling multi-layer protection systems.

3.4 Example 3 – Analysis of workover control system

3.4.1 System description

A workover control system (WOCS) is primarily used during well maintenance, workover operations or interventions. There are several types of WOCSs, and several arrangements of equipment (e.g. valves) mounted onto the X-mas tree. The WOCS and its valve arrangements depend on (among others) the type of X-mas tree, i.e. horizontal or vertical, and the type of well intervention, e.g. riser-less, use of a completion/workover (C/WO) riser system, use of C/WO riser system in combination with drilling BOP and marine riser.

A workover operation is a typical “batch process” which takes place for a shorter period of time. The WOCS is tested prior to launching and if the operation lasts for more than 14 days, the WOCS is retrieved and re-tested. The equipment used is often moved from installation to installation.

The WOCS usually comprises:

- Hydraulic power unit (HPU) package/section, incl. e.g. hydraulic supply and instrumentation

- Control package/section, incl. e.g. instrumentation, PLC, control panels, emergency power unit (EPU) and uninterrupted power supply (UPS)
- Umbilicals
- WOCS controls and riser packages (comprising several valves and shear ram).

Three safety functions are normally implemented through the WOCS: an ESD function, an emergency quick disconnect (EQD) function and a PSD function. The ESD and EQD functions include activating a pushbutton and closing the production line (i.e. the vertical line / annulus line), the injection line and the kill line (horizontal lines from the production). The (vertical) production line is closed by one or more shear rams or one or more production isolation valves (PIVs).

The ESD and EQD functions implemented into the WOCS is an interesting case due to several reasons:

- There are limited failure data available in regular offshore data sources for many of the involved components, in particular the subsea components.
- The WOCS and riser package are not in continuous use. The WOCS is always tested prior to use resulting in very short test intervals. Also the shear ram is only partially tested since the cutting function is not fully verified during testing. Hence, this raises questions related to modelling of reduced test coverage and/or the inclusion of P_{TIF} (probability of test independent failures) in the calculations.

There are also other issues related to analysing WOCS' that could be discussed, such as complex systems and combination of topside and subsea equipment, manual valves, etc., leading to modelling challenges, in particular related to CCFs. However, since CCF modelling has been extensively covered in the two previous examples, we here discuss the challenges related to limited failure data, short test intervals and P_{TIF}.

In this example we consider the ESD function and its relevant sub-functions as illustrated in the RBD in Figure 10. ESD activation can be either electric, pneumatic or both, and includes pushbuttons, PLC, power supply, signals and topside solenoids/valves. The umbilicals contain hydraulic supply and return lines and electrical signal lines. The ESD function includes valves and final elements, such as chemical injection valves, shear ram and PIV. In addition, for the final elements to close, it is a prerequisite that return lines/systems (if relevant) for return of hydraulic fluids are opening/functioning. Thus, a WOCS and the corresponding ESD function are rather complex.

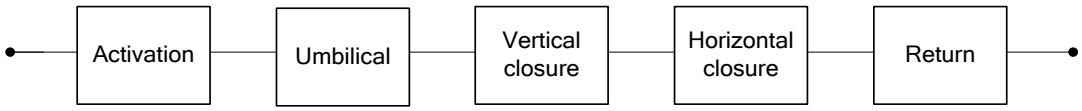


Figure 10: RBD of sub-functions in an ESD/EQD of a WOCS

Abbreviations

The following *equipment related abbreviations* are used only in this example:

BOP	-	Blowout preventer
DHSV	-	Downhole safety valve
EQD	-	Emergency quick disconnect
EPU	-	Emergency power unit
HPU	-	Hydraulic power unit

PIV	-	Production isolation valve
PLC	-	Programmable logic solver
UPS	-	Uninterrupted power supply
WOCS	-	Workover control system
WCP	-	Well control package

3.4.2 Assumptions and limitations

Limitations and assumptions concerning the reliability modelling and the system are summed up in Table 10 and Table 11 respectively.

Table 10: Analytical assumptions for example 3

No.	Description of assumption
1	For the shear ram, a P_{TIF} value is added, ref. discussion below and reliability data in section 3.4.4. The P_{TIF} represents the probability of a failure to occur that may only be detected during a real demand.
2	The example operates with a test coverage that is assumed to be 75% for the bi-weekly testing. A full certification testing is assumed performed annually, i.e. after 8760 hours calendar time.

Table 11: Assumptions related to design and operation for example 3

No.	Description of assumption
3	The system under consideration in this example is restricted to one shear ram as a final element only, i.e. other components that must function in order for the shear ram to function, such as solenoid valves, control valves, needle valves, accumulators, etc., are (for simplicity) not considered in this example.
4	The system is tested prior to each workover operation, resulting in very short test intervals as compared to what is common for offshore on demand SIS. It is also assumed that if the system is in use for 14 days it will be tested again. Thus, assumed functional test interval for the shear ram is here set to 14 days $\approx$ 340 hours, which corresponds to the maximum time between testing of the WOCS.
5	It is assumed that the safety functions and the shear ram operate on demand (i.e. a low demand system), as the frequency of ESD demands is low and the time between demands is significantly longer than the time between functional tests.
6	No degraded operation is assumed in this example. Upon failure of any component the WOCS will be retrieved immediately. Hence no DTU (Downtime unavailability) contributions are assumed.
7	The function of the shear ram will be to cut and seal properly on a demand.

3.4.3 Reliability modelling

The following issues are discussed concerning the reliability modelling:

- Using P_{TIF} when modelling systems with short test intervals where the functional testing is assumed not to be 100% complete.
- How should failure rates be determined?

Failure rates are discussed in section 3.4.4 and P_{TIF} is discussed below:

Why should P_{TIF} be taken into account?
With bi-weekly testing, the test interval becomes rather short as compared to "traditional" SIFs. The resulting PFD will be correspondingly low, even with failure rates that are significantly higher than what we normally consider for safety related components. This can be seen from the simplified PFD formula for a single component (also see discussion in Table A.1):

$$\text{PFD} \approx \lambda_{DU} \cdot \tau/2$$

E.g. even with a high failure rate λ_{DU} of $1{\cdot}10^{-5}$ per hour and a test interval of 14 days (340 hours) the estimated PFD becomes 1.710^{-3} which may be low when comparing to test data from RNNP for blowout preventers (ref. /10/).

Consequently, only calculating the PFD can be non-conservative and including the probability of experiencing additional test independent failures then becomes important. It is therefore necessary to carefully investigate if some DU failures may remain unrevealed after the test, or if DU failures may be introduced during the test due to some human error. In such cases P_{TIF} should be included in the reliability calculations. In our example, the bi-weekly functional testing of a shear ram will deviate from the real demand conditions and some of the failures may therefore not be revealed until a real demand occurs. E.g. the test will not confirm that the shear ram is able to cut and keep tight. To account for such potential undetected failures, we will therefore include the additional P_{TIF} for the shear ram, i.e. the probability of a test independent failure occurring upon a demand.

An alternative approach to account for unrevealed failures, is to introduce a test coverage for the bi-weekly test, c_{FT}, i.e. the fraction of dangerous undetected failures assumed revealed during a functional test. It is then assumed that the DU failures that are not detected during the bi-weekly test are revealed during a re-certification. Let τ be the assumed functional test interval (bi-weekly in this example), and let $\tau_{Certification}$ be the (operational) time between certifications where the remaining failures are assumed revealed. Assuming that a re-certification takes place regularly, the PFD then becomes:

$$PFD = c_{FT} \cdot \lambda_{DU} \frac{\tau}{2} + (1 - c_{FT}) \lambda_{DU} \frac{\tau_{Certification}}{2}$$

This approach is also exemplified below for this WOCS example.

3.4.4 Reliability data

In cases like workover control systems, where limited component field data has been collected, determination of parameters will be a big challenge. In lack of reliability data, we may consider one or more of the following approaches:

- Compare with data for similar/comparable components. Note that the influence from the current operating and environmental conditions versus what may be expected for the reference component should be considered. Also the influence from possible different design principles, e.g., failsafe versus non-failsafe design, should be considered. E.g. it might be necessary to include an accumulator in order to consider the shear ram as fail safe.
- Ask users or other personnel working with drilling/well intervention components for expert information and experiences. "How often does the component fail? Has the component ever failed?"
- Use of "best" available data, however such data may be outdated.

For the failure rate of the shear ram, the "best" publicly available data found are from the '92 edition of the OREDA handbook, i.e. data which is at least 20 years old. In order to obtain the λ_{DU} some additional assumptions as described in Table 12 have been made. Note that with the resulting assumed failure rate for a shear ram and a test interval of 14 days this correspond to a PFD of approximately 0.005.

For deciding the P_{TIF} – value we may first compare with the P_{TIF} for a topside ESV, which is a component with available P_{TIF} value, and also having characteristics being somewhat similar to a shear ram. For an ESV with standard testing a P_{TIF} of 10^{-4} has been assumed in /1/. In the previous 2006 version of the PDS handbook[4], a P_{TIF} of 10^{-3} was assumed for valves which were subject to partial stroke testing. Partial stroke testing is comparable to shear ram testing in the sense that neither of the tests completely confirms the safety function. A partial stroke test does not fully close the valve whereas a shear ram test does not confirm its capability of cutting and keeping tight. However, since cutting and tight closing of a shear ram is a more complex operation than closing a valve, we will here assume a somewhat higher P_{TIF} of $3 \cdot 10^{-3}$ for the shear ram.

Table 12: Reliability data for example 3

Component	λ_{DU} *(per hour)*	**P_{TIF}**	**Comments and reference**
Shear ram	$3 \cdot 10^{-5}$	$3 \cdot 10^{-3}$	Failure rate from the OREDA handbook (1992 edition). The critical failure mode significant internal leakage gives a total number of critical failures[5] of 4 during an operational time of $1.1 \cdot 10^5$ hours. Further, it is assumed that 80 % of these failures are related to the final elements of the shear ram. Then the estimated failure rate becomes: $4 \cdot 0.8 / 1.1 \cdot 10^5$ hours $\approx 3 \cdot 10^{-5}$ per hour No in-depth analyses have been identified that studies the shear ram failure modes and the behaviour under failure conditions. Systematic collection of failure data for different types of shear rams also seems to be lacking.

3.4.5 Reliability calculations

In this section, the reliability calculations for the shear ram are presented. The total CSU for the shear ram as final element is:

[4] The 2010 version of the data handbook considers for ESVs a P_{TIF} value that applies for a standard/average functional test only.

[5] The other critical failure mode where failures are registered is significant external leakage, which is not considered as a safety critical failure mode.

$$CSU = PFD + P_{TIF} = \lambda_{DU} \cdot \tau / 2 + P_{TIF} = 3 \cdot 10^{-5} \cdot 340/2 + 10^{-3} = 5.1 \cdot 10^{-3} + 3 \cdot 10^{-3} = 8.1 \cdot 10^{-3}$$

We may compare this result with the alternative approach of assuming reduced test coverage. We then have to make some assumptions. Say that the test coverage of the bi-weekly testing is 75 % and that a full certification testing is performed annually. In such case the PFD can be estimated as:

$$PFD = c_{FT} \cdot \lambda_{DU} \frac{\tau}{2} + (1 - c_{FT}) \lambda_{DU} \frac{\tau_{Certification}}{2} = 0.75 \cdot 3 \cdot 10^{-5} \cdot 340/2 + 0.25 \cdot 3 \cdot 10^{-5} \cdot 8760/2 =$$
$$3.8 \cdot 10^{-3} + 3.29 \cdot 10^{-2} = 3.7 \cdot 10^{-2}$$

We see that the results from the two approaches differ by a factor between four and five.

In a recent safety analysis report (SAR) for a new subsea field, a failure rate for a shear ram of $\lambda_{DU} = 5.2 \cdot 10^{-6}$ per hour was assumed, i.e. a factor six times better than the one based on OREDA 92. Let us now repeat the above calculations but with the lower failure rate. Using the PDS approach with P_{TIF} we get:

$$CSU = PFD + P_{TIF} = \lambda_{DU} \cdot \tau / 2 + P_{TIF} = 5.2 \cdot 10^{-6} \cdot 340/2 + 10^{-3} = 8.8 \cdot 10^{-4} + 3 \cdot 10^{-3} = 3.9 \cdot 10^{-3}$$

When using the reduced test coverage formula we get:

$$PFD = c_{FT} \cdot \lambda_{DU} \frac{\tau}{2} + (1 - c_{FT}) \lambda_{DU} \frac{\tau_{Certification}}{2} = 0.75 \cdot 5.2 \cdot 10^{-6} \cdot 340/2 + 0.25 \cdot 5.2 \cdot 10^{-6} \cdot 8760/2$$
$$= 6.6 \cdot 10^{-4} + 5.69 \cdot 10^{-3} = 6.4 \cdot 10^{-3}$$

We now see that the results from the two approaches differ by a factor of less than two.

3.4.6 Discussion of results

From the above calculation we see that for the shear ram the estimated contribution from P_{TIF} is some 37% of the total CSU when using the OREDA 92' data. In this case a quite high λ_{DU} failure rate for the shear ram has been assumed. When using the failure rate from the SAR, and the same assumed P_{TIF}, the total CSU is reduced by approximately 50% whereas the relative P_{TIF} contribution increases to more than 75%.

When applying the alternative approach of reduced test coverage, the resulting failure probabilities become higher. This is mainly due to the high failure rates combined with the relatively low test coverage assumed (75 %) and the subsequent fact that 25 % of the failures are tested for only once a year.

Hence, this example illustrates some major challenges that may face the reliability analyst, i.e.

- How to model systems with short test intervals where the functional testing is assumed not to be 100% complete
- What failure data to apply when the historic information is sparse and/or outdated?

Often in situations like this, where no standard answer is available, it may be useful to ask oneself some "control questions". E.g. knowing that the cutting and sealing function of the shear ram is not tested during

regular functional testing of the WOCS, one may ask the following question: “Do we believe that the shear ram is significantly better than a standard ESV (which has an average PFD of approximately 0.01) or is it comparable, or maybe even less reliable? We see that by choosing a dangerous undetected failure rate of either $5.2 \cdot 10^{-6}$ per hour or $3 \cdot 10^{-5}$ per hour the PFD contribution differs by a factor of approximately six.
Note that we in this example consider only the closure of the production line. In order to achieve a sufficient closure during a workover operation also the injection line and kill line must close. Besides, we have only considered one final element, namely the shear ram, neglecting all other components that must function sufficiently for the shear ram to operate, e.g. push buttons, PLC, solenoid valves, accumulator and needle valves. Generally, reliability quantification of WOCS is a complex matter where many components have to function to achieve shutdown. This often also includes modelling the hydraulic return lines and accounting for valves in the return lines in the quantification. Another issue when analysing WOCS is the PLC configuration and its associated failure rate. For many WOCS’ the PLC implements both process control and safety functions, and in such cases one should be careful if applying a lower failure rate for the WOCS PLC than for a standard industrial PLC.

3.5 Example 4 – Analysis of a continuously operating safety system

3.5.1 System description

Railway signalling is a SIS that is used to control railway traffic, including the setting of light signals and correct position of rail switches. The system does, unlike most SIS in the oil and gas industry, operate in the continuous or high demand mode.

This example illustrates the PDS-method used with a simplified version of a continuously operating railway signalling system. Different from the previous examples, we now deal with a safety system that must function not only on (rare) demands, but more or less continuously. A brief introduction to continuously operating systems is given in chapter 6 in the PDS-method handbook, ref. /1/. The main topic of this example is reliability calculations of both independent failures and CCFs for continuously operating systems.

The railway signalling system is to set a green (go) light only when all the underlying conditions for a train to enter a new rail section have been fulfilled. An important safety function is to prevent that a green light signal is set in the presence of a DU or DD failure.

A railway signalling system is complex, in terms of redundancy and read-back of signals to confirm correct operation. The system illustrated in this example has two PLCs (each comprising a CPU and an I/O card), and both of them must “agree on” setting a signal for free run (“green light”). If there are any contradictions between the two CPUs, the system will go to a fail-safe state and no green light signal is set; i.e., we have a 1oo2 voting between the two CPUs with respect to isolating the power to the green light signal. As an additional safety barrier, two watchdog (WD) functions (each with a separate relay) have been added, each of them being able to achieve a safe state in case a failure in both PLCs. The two WDs monitor the communication between the CPU and the I/O modules, and will detect certain types of CPU failures.

Abbreviations
The following *equipment related abbreviations* are used only in this example:

CPU	-	Central Processing Unit
HW	-	Hardware
I/O	-	Input/Output
SW	-	Software

WD - Watch-Dog

3.5.2 Assumptions and limitations

Limitations and assumptions concerning the reliability modelling and the system are summed up in Table 13.

Table 13: Assumptions for example 4

No.	Description of assumption
1	All failure rates are considered constant with respect to time. In reality, the failure rates may increase, especially when the functional test interval increases. See also section 6.2.1 of the PDS method handbook, /1/, for basic assumptions concerning reliability modelling of continuously operating systems.
2	The C_{MooN} factors applied in the calculations are the suggested factors from the PDS handbook, i.e. C_{1oo2} equals 1 and C_{1oo4} equals 0.15.
3	The present example considers failure contribution from DU failures only. See discussion in section 3.5.3.
4	The β-factor between CPUs and WD is assumed very low due to assumed diversity, here set to 0.01.
5	System downtime due to repair or testing has not been considered in this example. However, note that this should always be included if the system is allowed to operate in degraded mode while failed component(s) are being repaired or being tested.
6	Offshore (on demand) safety systems are often subject to manual testing typically performed every 3rd, 6th, 12th or every 24th months. For railway signalling systems it is assumed that more frequent testing is performed for components that have not been operated during a train passing, typically once every 24 hours, /8/. This is usually a fully automated test. In the calculations, it is therefore assumed that a functional test is not performed less seldom than every 24th hour, i.e. $\tau = 24\ h$. For simplicity, 100% test coverage is here assumed. However, this assumption should also be re-evaluated in each practical case.

3.5.3 Reliability modelling

A simplified RBD of the signalling system is shown in Figure 11. As shown, there are two channels available to isolate the power to the green light signal, each of them with its own redundancy: Channel 1 comprising redundant CPUs and channel 2 comprising redundant WDs.

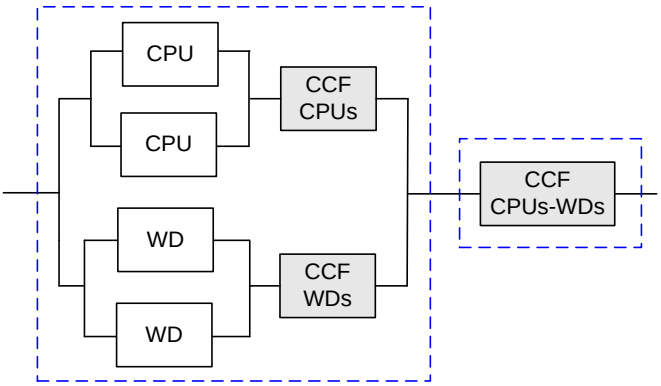


Figure 11: Simplified RBD of the safety function in this example

As this example illustrates below, is not straight forward to calculate the PFH for this RBD, but the following approach is suggested:

We first split the RBD into two parts, an independent part and a CCF part, as illustrated in Figure 11, so that the PFH of the system is:

$$\mathrm{PFH}_{\mathrm{sys}} = \mathrm{PFH}^{(\mathrm{ind}^*)} + \mathrm{PFH}^{(\mathrm{CCF})}$$

The $\mathrm{PFH}^{(\mathrm{ind}^*)}$ accounts for the PFH of the CPUs (including CCF between the two CPUs) *and* the WDs (including CCF between the two WDs).

Table A.2 in Appendix A gives simplified PFH formulas for systems of identical components. These formulas may therefore be used to calculate the PFH for each of the two channels. To calculate the $\mathrm{PFH}^{(\mathrm{ind}^*)}$, we need to consider the probability that one of the channels has already failed in the interval between two functional tests when the other channel fails. The mean downtime when we know that a component has failed is $\tau/2$. A system failure may occur if the other channel fails in this time interval:

$$\mathrm{PFH}^{(\mathrm{ind}^*)} \approx \mathrm{PFH}_{\mathrm{CPU}} \cdot \frac{\tau}{2} \cdot \mathrm{PFH}_{\mathrm{WD}} + \mathrm{PFH}_{WD} \cdot \frac{\tau}{2} \cdot \mathrm{PFH}_{\mathrm{CPU}} = \mathrm{PFH}_{\mathrm{CPU}} \cdot \mathrm{PFH}_{\mathrm{WD}} \cdot \tau$$
$$= \left((\lambda_{\mathrm{DU,\,CPU}} \cdot \tau)^2 / \tau + C_{1oo2} \cdot \beta_{\mathrm{CPU}} \cdot \lambda_{\mathrm{DU,\,CPU}} \right) \cdot \left((\lambda^2_{\mathrm{DU,\,WD}} \cdot \tau)^2 / \tau + C_{1oo2} \cdot \beta_{\mathrm{WD}} \cdot \lambda_{\mathrm{DU,\,WD}} \right) \cdot \tau$$

$\mathrm{PFH}^{(\mathrm{CCF})}$ is the probability that the CPUs and the WDs (including relays) fail due to a shared cause. For simplicity, we may assume that the system is a parallel system voted 1oo4, where the system fails if all four components fail.

Two parameter need to be determined to calculate the $\mathrm{PFH}^{(\mathrm{CCF})}$: The common beta factor for the WDs and the CPUs and a "shared" failure rate. In this example the following approach is proposed:

- Selection of common beta factor: The common beta for the four components will be influenced by the degree of similarity and the vulnerability to the same shared cause of failure. In this example, we may consider the CPUs and WDs to be diverse technologies, but being located in the same environment and therefore exposed to the same stressors, such as e.g., electro-magnetic interference. The common beta factor for CPUs and WDs may be calculated in two ways: Selecting the lowest (or an even lower) value of the betas for the CPUs and the WDs, or by using the geometric mean of the two betas. Here, the latter alternative has been suggested

- Selection of failure rate: Two similar alternatives are available for the selection of a shared failure rate: Selecting the lowest failure rate of CPU and WD or calculating the geometric mean of the two rates. The latter alternative has been selected:

This gives:

$$\text{PFH}^{(\text{CCF})} = C_{1oo4} \cdot \beta_{\text{CPU, WD}} \cdot \sqrt{\lambda_{\text{DU, CPU}} \cdot \lambda_{\text{DU, WD}}}$$

.

Detailed calculations are given in section 3.5.5.

3.5.4 Reliability data

The reliability data used in this example is listed in Table 14 below. Note that the failure rates are generic process industry data and not railway specific data.

Table 14: Reliability data for example 5

Component	τ	λ_{DU} (per hour)	β	Comments and reference
CPU	24 *h*	$0.1 \cdot 10^{-6}$	0.03	Assumed similar failure rates and beta value as PDS data for a hardwired safety system, ref. /2/. I/O modules are included in the failure rate.
WD	24 *h*	$0.4 \cdot 10^{-6}$	0.03	As the WD function considered her includes a relay, the failure rate is simply assumed to be twice the PDS failure rate for a relay. The beta value is assumed similar as for a relay, ref. /2/.

As indicated in Table 14, we have used generic process industry data even if the application is railway signalling system. It may be argued that this is reasonable since WDs and CPUs are located in-house and in a controlled environment, but this assumption may not apply to other types of components.

In the calculation of PFH, we have omitted the contribution from DD failures. The main rationale is that railway signalling systems automatically go to a safe state upon detection of dangerous failures, i.e., giving setting of red (stop) light signal. Time elapsing from the test until train passing is also so short that the possibility of train passing with a DD failure can be neglected. The contribution from DD failures would need to be added in applications where this assumption is not valid. In high demand/continuous mode of operation, it is not always reasonable to assume that repair of DD failures may be completed before the next demand. In this case, it may be necessary to reclassify the failures as DU as long as there is no automatic transition to the safe state.

3.5.5 Reliability calculations

Applying the PFH expressions given in section 3.5.3 above, the "independent" contribution becomes:

$$\begin{aligned}
&\text{PFH}^{(\text{ind})} = \text{PFH}_{\text{CPU}} \cdot \text{PFH}_{\text{WD}} \cdot \tau \\
&= \left((\lambda_{\text{DU, CPU}} \cdot \tau)^2 / \tau + C_{1oo2} \cdot \beta_{\text{CPU}} \cdot \lambda_{\text{DU, CPU}}\right) \cdot \left((\lambda^2_{\text{DU, WD}} \cdot \tau)^2 / \tau + C_{1oo2} \cdot \beta_{\text{WD}} \cdot \lambda_{\text{DU, WD}}\right) \cdot \tau \\
&= \left((0.1 \cdot 10^{-6} \cdot 24)^2 / 24 + 1 \cdot 0.03 \cdot 0.1 \cdot 10^{-6}\right) \cdot \left((0.4 \cdot 10^{-6} \cdot 24)^2 / 24 + 1 \cdot 0.03 \cdot 0.4 \cdot 10^{-6}\right) \cdot 24 \\
&= \left(2.4 \cdot 10^{-13} + 0.3 \cdot 10^{-8}\right) \cdot \left((3.8 \cdot 10^{-12} + 1.2 \cdot 10^{-8}\right) \cdot 24 = 9.6 \cdot 10^{-16} h^{-1}.
\end{aligned}$$

The CCF contribution of CPUs and WDs becomes:

$$\mathrm{PFH}^{(\mathrm{CCF})} = C_{1oo4} \cdot \beta_{\mathrm{CPU,\,WD}} \cdot \sqrt{\lambda_{\mathrm{DU,\,CPU}} \cdot \lambda_{\mathrm{DU,\,WD}}} = 0.15 \cdot 0.01 \cdot \sqrt{0.1 \cdot 10^{-6} \cdot 0.4 \cdot 10^{-6}} = 0.15 \cdot 0.01 \cdot 0.2 \cdot 10^{-6}$$
$$= 3 \cdot 10^{-10}\, h^{-1}$$

From the above expressions we see that the contribution from independent failures between the CPUs and the WDs is negligible compared to the CCF contribution, even with the high degree of diversity.

The estimate for the system PFH is then:

$$\mathrm{PFH} = 3 \cdot 10^{-10}\, h^{-1}$$

A PFH of $3 10^{-10}$ per hour corresponds approximately to one system failure due to DU failures per 380 000 year. This is very safe from a safety point of view, but it may be questioned if also the regularity (or availability) of the system is adequate, an issue that has not been studied in this example.

3.5.6 Discussion of result

The purpose of this example is to illustrate the use of the PDS-method for a high demand system and, with this as basis, highlight some of the differences and similarities between reliability quantification for systems operating in the high and low demand mode.

Since this example is based on a railway signalling system, it is relevant to question the use of process industry reliability data. Having made the assumption about similar and controlled environment, it has been argued that the same data can be used. However, a more fundamental question to discuss is the use of data that has been collected for low demand systems in the analysis of high demand systems. Components that are operated in the high demand mode are exposed to more wear and stresses from the frequent operations than in the low demand mode. ISO 13849, which applies to machinery systems, has suggested a method for estimating the failure rate based on the annual number of operations (or cycles). Unfortunately, this method relies heavily on stress testing performed by the manufacturer and is not easy to adapt with current approaches to data collection.

We have also discussed whether or not to include DD failures in the quantification of PFH. In this example it is argued that the contribution from DD failures may be neglected as long as the system (which is to be protected) automatically enters a safe state in response to detection of a DD failure. Furthermore it is important to consider the frequency of self testing. If the time between self testing is significantly shorter than the time between demands, it may be reasonable to assume that the DD failures may be revealed and corrected within short time compared to the time between demands or between regular functional tests. In this case, the contribution from DD failures may be neglected based on the same reasoning as for low demand systems.

4 REFERENCES

/1/ Hauge, S., Lundteigen, M.A., Hokstad, P., and Håbrekke, S., Reliability Prediction Method for Safety Instrumented Systems – PDS Method Handbook, 2010 Edition. SINTEF report A13503, January 2010

/2/ Hauge S. and Onshus T., Reliability Data for Safety Instrumented Systems – PDS Data Handbook, 2010 Edition. SINTEF report STF50 A13502, January 2010

/3/ System Reliability Theory, Models, Statistical Methods and Applications. M. Rausand and A. Høyland, 2004

/4/ B. Kirwan, A Guide to Practical Human Reliability Assessment, Taylor & Francis, 1994.

/5/ IEC 61508 Standard. Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety related systems, part 1-7, Edition 2.0, final draft, 2009

/6/ Functional Safety. A Straightforward Guide to Applying IEC 61508 and Related Standards. D.J. Smith & K. G.L. Simpson

/7/ Hauge, S. and Lundteigen, M.A., Guidelines for Follow-up of Safety Instrumented Systems (SIS) in the operating phase. SINTEF report A8788, Rev. 01, 01.12.2008 (Web: http://www.sintef.no/project/PDS/Reports/PDS%20Report-SIS_follow_up_guideline_final_v01.pdf)

/8/ Hokstad, P., Håbrekke, S., Lundteigen, M.A. and Onshus, T., Use of the PDS Method for Railway Applications. SINTEF report A11612, June 2009.

/9/ Lundteigen, M. A., Rausand, M., Reliability assessment of safety instrumented systems in the oil and gas industry: A practical approach and a case study, International Journal of Reliability, Quality and Safety Engineering (IJRQSE), Volume 16, issue 2, April 2009

/10/ PSA Norway, Trends in Risk Level in the Petroleum Activity, summary report 2009 (Web: http://www.ptil.no/getfile.php/PDF/RNNP%202009/Trends%20in%20risk%20levels%20-%20Summary%20Report%202009.pdf)

/11/ OREDA 2009, Offshore Reliability Data, 5th Edition, Volume 1 – Topside Equipment and Volume 2 – Subsea Equipment, Prepared by: SINTEF, 2009

A PDS formulas

This appendix includes some of the formulas and parameters that are used in this report. For more details, reference is made to the PDS method handbook, ref. /1/.

A.1 PFD formulas

Table A.1 summarizes PFD formulas for some frequently occurring voting configurations.

Table A.1 Summary of simplified formulas for PFD (ref. Table 3 in /1/)

Voting	PFD calculation formulas		
	Common cause contribution		**Contribution from independent failures**
1oo1	-		$\lambda_{DU} \cdot \tau /2$
1oo2	$\beta \cdot \lambda_{DU} \cdot \tau /2$	+	$[\lambda_{DU} \cdot \tau]^2/3$
2oo2	-		$2 \cdot \lambda_{DU} \cdot \tau /2$
1oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$	+	$[\lambda_{DU} \cdot \tau]^3/4$
2oo3	$C_{2oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$	+	$[\lambda_{DU} \cdot \tau]^2$
3oo3	-		$3 \cdot \lambda_{DU} \cdot \tau /2$
1ooN; N = 2, 3,…	$C_{1ooN} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$	+	$\frac{1}{N+1} \cdot (\lambda_{DU} \cdot \tau)^N$
MooN, M<N; N = 2, 3,..	$C_{MooN} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$	+	$\frac{N!}{(N-M+2)! \cdot (M-1)!} \cdot (\lambda_{DU} \cdot \tau)^{N-M+1}$
NooN; N = 1, 2, 3, …	-		$N \cdot \lambda_{DU} \cdot \tau /2$

The above formulas for PFD have been derived after having integrated the failure rate function for the voted configuration over the test interval. The reader should be aware that some software tools first calculate the PFD at the component level, before the PFD is calculated for the voted configuration. This gives a non-conservative solution due to the Schwartz inequality. Considering a 1oo2 voted configuration, the first approach gives

$$[\lambda_{DU} \cdot \tau]^2/3$$

whereas the second gives

$[\lambda_{DU} \cdot \tau]/2 \cdot [\lambda_{DU} \cdot \tau]/2 = [\lambda_{DU} \cdot \tau]^2/4$.

It has been shown by /9/ that the correction factor for a 1ooN system is $2^N/N+1$. For a 1oo2 system, the correction factor is 4/3.

It can be tedious to determine the failure function for more complex 1oo2 configurations, such as for redundant configurations that comprise different type of components. For simplicity, the non-conservative approach is first used to calculate the PFD, by simply multiplying the PFD of each, branch in a 1ooN configuration. As a second step, it is suggested to reduce the non-conservative error, by using the same correction factor as mentioned above. This approach implies that 1oo2 configuration with two non-identical components becomes:

$$PFD_{1oo2}^{ind} = \frac{4}{3} \cdot PFD_{1,\,1oo1}^{ind} \cdot PFD_{2,1oo1}^{ind} \cdot$$

A.2 PFH formulas

Table A.2 summarizes PFH formulas for some frequently occurring voting configurations.

Table A.2 Summary of simplified formulas for PFH (ref. Table 9 in /1/)

Voting	**PFH calculation formulas**		
	Common cause contribution		**Contribution from independent failures**
1oo1	-		λ_{DU}
1oo2	$\beta \cdot \lambda_{DU}$	+	$[\lambda_{DU} \cdot \tau]^2/\tau$
2oo2	-		$2 \cdot \lambda_{DU}$
1oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{DU}$	+	$[\lambda_{DU} \cdot \tau\,]^3/\tau$
2oo3	$C_{2oo3} \cdot \beta \cdot \lambda_{DU}$	+	$3 \cdot [\lambda_{DU} \cdot \tau\,]^2/\tau$
3oo3	-		$3 \cdot \lambda_{DU}$
MooN, M<N; N = 2, 3, ...	$C_{MooN} \cdot \beta \cdot \lambda_{DU}$	+	$\frac{N!}{(N-M+1)!(M-1)!} \cdot \left[(\lambda_{DU} \cdot \tau)^{N-M+1}/\tau\right]$
NooN; N = 1, 2, 3, …	-		$N \cdot \lambda_{DU}$

A.3 C_{MooN} factors

The C_{MooN} factors applied in the above formulas are given in table A.3. As compared to Table 2 in /1/, Table A.3 have been extended with N=7 and N=8.

Table A.3 C_{MooN} factors for different voting logics (ref. Table 2 in /1/)

M \ N	N = 2	N = 3	N = 4	N = 5	N = 6	N = 7	N = 8
M = 1	$C_{1oo2} = 1.0$	$C_{1oo3} = 0.5$	$C_{1oo4} = 0.3$	$C_{1oo5} = 0.21$	$C_{1oo6} = 0.17$	$C_{1oo7} = 0.15$	$C_{1oo8} = 0.15$
M = 2	-	$C_{2oo3} = 2.0$	$C_{2oo4} = 1.1$	$C_{2oo5} = 0.7$	$C_{2oo6} = 0.4$	$C_{2oo7} = 0.27$	$C_{2oo8} = 0.15$
M = 3	-	-	$C_{3oo4} = 2.9$	$C_{3oo5} = 1.8$	$C_{3oo6} = 1.1$	$C_{3oo7} = 0.8$	$C_{3oo8} = 0.6$
M = 4	-	-	-	$C_{4oo5} = 3.7$	$C_{4oo6} = 2.4$	$C_{4oo7} = 1.6$	$C_{4oo8} = 1.1$
M = 5	-	-	-	-	$C_{5oo6} = 4.3$	$C_{5oo7} = 3.0$	$C_{5oo8} = 2.1$
M = 6	-	-	-	-	-	$C_{6oo7} = 4.8$	$C_{6oo8} = 3.5$
M = 7	-	-	-	-	-	-	$C_{7oo8} = 5.3$

Technology for a better society

www.sintef.no