SINTEF Industrial Management
Safety and Reliability

Address: N-7034 Trondheim, NORWAY
Location: Strindveien 4
Telephone: +47 73 59 27 56
Fax: +47 73 59 28 96

Enterprise No.: NO 948 007 029 MVA

SINTEF REPORT

TITLE

Reliability Quantification of Computer-Based Safety Systems. An Introduction to PDS.

AUTHOR(S)

Geir Klingenberg Hansen and Ragnar Aarø

CLIENT(S)

Multiclient

REPORT NO.	CLASSIFICATION	CLIENTS REF.	
STF38 A97434	Unrestricted		
CLASS. THIS PAGE	ISBN	PROJECT NO.	NO. OF PAGES/APPENDICES
Unrestricted	82-14-00445-4	384120.10	24
ELECTRONIC FILE CODE		PROJECT MANAGER (NAME, SIGN.)	CHECKED BY (NAME, SIGN.)
s:\3840\pro\384120\10-top97\pds metodebeskrivelse.doc		Ragnar Aarø	Per R. Hokstad
FILE CODE	DATE	APPROVED BY (NAME, POSITION, SIGN.)	
384120.10	1997-12-19	Lars Bodsberg, Research Director	

ABSTRACT

The increased use of computer-based safety systems has resulted in a focus on the reliability of these systems. There is often a need to verify and improve the safety system design in order to reach the safety objectives stated.

PDS is a method used to quantify the reliability, the safety and the Life Cycle Cost (LCC) of computer-based safety systems and is thus a tool to achieve the above goals. This report gives an introduction to PDS without mathematical details, making it comprehensible to the non-expert. The method is illustrated using the dedicated computer program PDS-Tool. Also, the need for reliability analyses in general is discussed.

KEYWORDS	ENGLISH	NORWEGIAN
GROUP 1	Reliability	Pålitelighet
GROUP 2	Risk	Risiko
SELECTED BY AUTHOR	Reliability quantification	Kvantifisering av pålitelighet
	Computer-based safety systems	Datamaskinbaserte sikkerhetssystemer
	Safety	Sikkerhet

TABLE OF CONTENTS

1. INTRODUCTION

PDS[1] is a method used to quantify the reliability, the safety and the Life Cycle Cost (LCC) of computer-based safety systems. The method is widely used in the offshore industry, but is also applicable to other business sectors. The purpose of this document is to present the PDS method and its applications to a broad audience, in a way that makes it comprehensible to the non-expert. The report is aimed at management, designers and the technical personnel working with computer-based safety systems, as well as reliability engineers.

PDS was developed in the SINTEF project "Reliability and Availability of Computer-Based Process Safety Systems" and is more thoroughly described in [Aar89] and [Bod95]. The method has been developed in close co-operation with oil companies as well as vendors of control and safety systems. See also the web site http://www.sintef.no/sipaa/prosjekt/pds.html

The increased use of computer-based safety systems has resulted in an IEC standard addressing the safety aspects for all lifecycle activities of such systems [IEC95]. It should be noted that PDS is in line with the principles advocated in the IEC standard[2], and is a useful tool when implementing the principles of the IEC standard.

When designing computer-based safety systems there is a general conflict between *safety* (the need to ensure that the safety system will function at an emergency), and *production regularity* (avoiding the safety system to spuriously shut down the production). Today, most safety systems are designed in a fail-safe manner. This implies that the system should enter a safe state in the case of a failure of the computer-based safety system. By this design, safety is maintained while production regularity is impaired. When using PDS the reliability analyses will focus on both these aspects, and provide means for balancing a system configuration with respect to both safety and production regularity.

The report is organised as follows. Chapter 2 gives a discussion of safety and reliability in general and should be read by anyone with an interest in safety and reliability issues. It states some of the benefits of performing reliability analysis, and tries to give an answer to why PDS is a useful tool for this purpose. In Chapter 3, we describe the method in more detail. However, the discussion is on a high level, free from mathematical details. This makes the presentation understandable for non-experts of reliability theory and is aimed at those prepared for making reliability analysis. Finally, in Chapter 4, the method is illustrated by means of an example. The example is prepared and presented using the PDS-Tool, which is a computer program dedicated for performing analysis based on PDS.

An extension to PDS was developed in the SINTEF project "Control and Safety Systems Reliability", described in [Bod94]. This method takes into consideration the combined effect of the control system and the safety system, and is termed the **PDS-II method**. Both human as well as technical barriers of safety are considered in the PDS-II method.

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

[2] The IEC standard, IEC 61508, aims at so-called E/E/PES safety related systems (E/E/PES is an acronym for Electrical/Electronic/Programmable Electronic Systems). This is similar to computer-based safety systems, which are focussed by PDS.

2. THE NEED FOR RELIABILITY CONSIDERATIONS

2.1 Who needs Reliability Analysis of Computer-Based Safety Systems?

Microprocessors are increasingly replacing electromechanical relays in safety systems in the process industry. Computer-based fire and gas detection systems, process shutdown systems, and emergency shutdown systems are installed to prevent abnormal operating conditions from developing into an accident. Further, a major increase in the use of these kind of systems is anticipated also in other business sectors such as the public transport industry (air and rail) and the manufacturing industry. The background for this is that, according to several sources, there are significant benefits in terms of cost and manufacturing flexibility, while not jeopardising safety.

When computer-based safety systems are used, e.g. replacing "conventional" safety devices, it is very important to verify that the safety requirements are fulfilled, and here PDS plays an important role, as discussed in the next section.

2.2 Benefits of Reliability Analysis

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

Some main applications of reliability analysis are:

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

Documenting safety, reliability, maintainability and/or production regularity is an important application of reliability analysis. Also, it is becoming increasingly more important to verify the quality of the products and systems in terms of its reliability attributes. Acceptance criteria are stated from customers and authorities, specifying requirements to safety, reliability, maintainability and/or production regularity. In the Norwegian petroleum industry the NORSOK standard *"Common Requirements, Safety and Automation Systems (SAS)"* [NOR94] is commonly in use, and in a study conducted by SINTEF [Lon96], the standards IEC61508 [IEC95] and EN 954 [EN97] have been identified as becoming especially important in the time ahead.

NORSOK is the Norwegian initiative to reduce development and operation cost for the offshore oil and gas industry, and has issued a number of technical standards. It should be noted that PDS is referred to as a recommended method to use for assessing the reliability of computer-based safety systems. See also the web site http://www.nts.no/norsok/

The IEC standard addresses the safety aspects of computer-based safety systems. With respect to PDS, it is important to be aware that PDS is fully in line with the principles advocated in the IEC standard.

However, the IEC standard does not prepare for the balancing between the loss of safety and the loss of production regularity, as is offered by PDS. It is anticipated that many end-users of safety-related systems as well as national authorities will refer to the upcoming IEC standard[3], and this will lead to an even increased focus on the safety and reliability aspects of computer-based safety systems.

The **IEC 61508 standard**, currently under preparation as a FDIS ("Final Draft International Standard"), is denoted "*Functional Safety; Safety-Related Systems* [IEC95]. The standard sets out a generic approach for all safety lifecycle activities for electrical/electronic/programmable electronic systems (E/E/PESs) that are used to perform safety functions.

Although most reliability analyses have been used to *gain confidence* in the system by assessing the reliability attributes, it is perhaps more interesting to use reliability analysis as a means to *achieve* reliability, e.g., by design optimisation.

It would be most efficient to employ these techniques in the design phase of the system, when less costly changes can be made, see Figure 1. Proper analytic tools available during the design process may ensure that an optimal system configuration is installed from the very beginning, thereby reducing significantly overall system cost. Investing in reliability analyses is profitable in the long run since the absence of equipment breakdown enhances safety, and at the same time frees the company from lost production costs and repair costs.

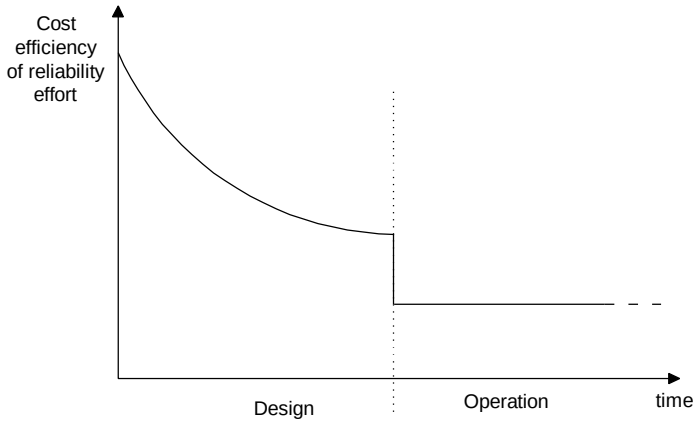

Figure 1: The cost efficiency of performing reliability analysis in different project phases.

The benefit of using reliability analysis is greater in the early stages of the project, since less costly changes can be made. Furthermore, reliable solutions can be identified, reducing greatly operational costs.

[3] Please note that the number of the standard recently have been changed from IEC 1508 to IEC 61508, and the name changed to "Functional safety of electrical/electronic/programmable electronic safety-related safety systems".

2.3 Why PDS?

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

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

- Common cause failures
- Automatic self-tests
- Test-independent failures (failures not revealed by functional testing)
- Complete systems including redundancies
- All failure categories/causes.

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

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

The main characteristics of PDS are summarised as follows:

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

- normal ageing
- human operator errors
- design errors
- environmental conditions

The failure taxonomy is customised to utilising input data from various data sources:

- corrective and preventive maintenance report systems
- data bases (OREDA)
- expert judgements

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

- dependent (common cause) failures
- the actual effect of all types of testing (automatic as well as manual)

In particular, the model distinguishes between the ways a system can fail (failure mode), such as fail-to-operate, spurious operation and non-critical.

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

The method is simple and structured:

- highlighting the important factors contributing to loss of safety and life cycle cost
- promoting transparency and communication

As stressed in IEC 61508, it is important to incorporate the whole computer based system when performing reliability analyses. This is a core issue in PDS; it is function-oriented, and the whole path from the sensors, via the control logic and to the actuators is taken into consideration when modelling the system.

2.4 Applications of PDS; some Examples

PDS has been applied in numerous projects and in many different contexts. The main concern, however, has been to computer-based safety systems in the offshore and onshore oil and gas industry. PDS has a.o. been utilised

- in a large number of third-party verifications of offshore safety systems.
- to consider the effects of integrating the process control, process shutdown and emergency shutdown systems.
- in a comparative reliability assessment of different control and safety systems for boiler applications.
- as a tool for specifying emergency shutdown (ESD) system requirements on offshore installations.
- to compare different voting configurations of gas detectors, including different combinations of high/low alarm limits, based on economic and safety assessments.
- to optimise the functional testing interval for offshore equipment, considering both safety and maintenance cost.
- in several HIPPS (High Integrity Pressure Protection System) studies.
- in the evaluation of a new detector design (with increased self test facilities).

3. RELIABILITY QUANTIFICATION BY PDS

3.1 Introduction

This chapter presents the main features of PDS, and also discusses reliability performance measures of computer-based safety systems. Please note that the objective is *not* to give a full and detailed presentation of the method, but to give an introduction to the model taxonomy and the basic ideas. In Chapter 4, an example of a complete analysis using PDS (yet on a very simple system) is presented using the PDS-Tool.

The **PDS-Tool** is a Windows application developed by SINTEF, implementing the PDS method. It provides a user-friendly interface and gives significant gains in terms of man-hours required to carry out and document the reliability analyses. See also the web site http://www.sintef.no/sipaa/prosjekt/pds-tool.html

3.2 Reliability Performance Measures

The following performance measures are used:

A measure for quantifying *loss of safety* is the *Critical Safety Unavailability (CSU)*:

> *The probability that the safety system due to an unrevealed fault will fail to automatically carry out a successful safety action on the occurrence of a hazardous/accidental event*[4].

PDS distinguishes between the CSU and the Safety Unavailability (SU). The SU includes both critical and Non-Critical Unavailability (NCU) of the safety system where the NCU is due to situations where it is *known* that the safety system is unavailable (e.g., by maintenance or functional tests). However, the NCU is not considered in PDS since it is assumed that extra precautions are taken during known unavailability of the safety system. Please not that the IEC 61508 standard does not distinguishes between the CSU and the SU.

A reliability measure for quantifying *loss of production regularity* is the *Spurious Trip Rate (STR):*

> *The mean number of spurious activations of the safety system per time unit.*

In addition, a measure of the expected maintenance effort is also of interest for the LCC calculations. The rate of physical failures combined with the mean man-hours spent on corrective maintenance for each type of equipment (see also [Aar89]) gives the quantitative reliability measure for the total maintenance effort, as the *Mean Corrective Maintenance (MCM):*

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

[4]Please note that the CSU is a failure on-demand probability, and that this complies with for instance the notation in the draft IEC 61508, ref. [IEC95] (“*Probability of failure to perform its design function on demand”*). The term CSU is, however, used in this report, as it has already been established as a preferred term in the PDS method.

3.3 Failure Classification

An essential feature of PDS is the detailed failure classification scheme.

PDS considers Three Failure Modes:

- Fail To Operate (FTO)
  - Safety system/module does not operate on demand
    (e.g. sensor stuck upon demand)
- Spurious Operation (SO)
  - Safety system/module operates without demand
    (e.g. sensor provides signal without demand - 'false alarm')
- Non-Critical (NC)
  - Main functions not affected
    (e.g. sensor imperfection, which has no direct effect on control path)

The first two of these failure modes, Fail To Operate (FTO) and Spurious Operation (SO) are considered "critical". The SO failures are usually revealed instantly upon occurrence, whilst the FTO failures can be detected by automatic as well as manual (functional) testing.

Failure Classification by Cause of Failure
Figure 2 shows how failure causes are classified in PDS. This classification is applied both for FTO and SO failures.

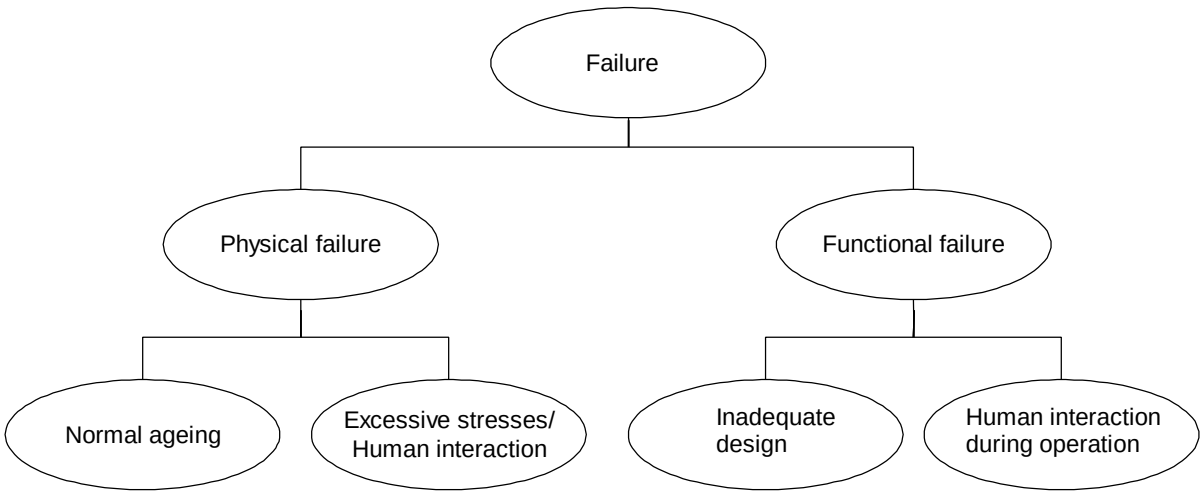

Figure 2: Failure classification.

As seen from Figure 2, there are two main categories of failures:

- ***Physical failures***, the delivered service deviates from the specified service due to physical degradation of the safety system/module. Any failure that requires some kind of repair may be denoted physical failure.
- ***Functional failures***, the delivered service deviate from the specified service although there is no physical degradation of the safety system/module. Modifications rather than repairs are required in order to remove these failures.

The ***physical failures*** are further split as described below:

- A physical failure due to ***normal ageing*** occurs under conditions within the design envelope of a module.
- A physical failure due to ***stress/human interaction*** occurs when excessive stresses are placed on the module. The excessive stresses may be caused either by external causes or by human errors during operation. An example is damage to gas detectors due to inadequate protection during sand blasting.

The ***functional failures*** are further split as described below:

- Functional failure due to ***design*** is initiated during engineering and construction (and may be latent from the first day of operation). Examples of ***functional design failures*** are software failures, lack of selectivity of sensors, and erroneous location of e.g. fire/gas detectors.
- Functional failure due to ***human interaction*** is initiated by human errors during operation. Examples of functional failures caused by ***human interaction*** are loops left in the override position after completion of maintenance, and erroneous calibration of sensors.

3.4 Testing

PDS takes into account the effect of two types of testing of the system: Automatic self-tests and functional testing. Both types of tests are ideally designed to be *perfect*, i.e., they aims at detecting *all* failures of the system. In practice, however, the tests are *not* perfect, and PDS takes this into account as described below.

Failures Detectable/Undetectable by Automatic Self-Test

For systems with *automatic self-test,* PDS will, as stated above, take into account that some failures are not detected automatically. Upon discrepancy between modules in the safety system, it may also be determined which of the modules have failed. The actual effect of a detected failure depends on the operating philosophy of the system. A *fault coverage factor* is given to quantify the efficiency of automatic self-tests. The fault coverage factor equals the fraction of failures being detected by the automatic self-test.

Functional Testing

The functional test may *not* be perfect due to:

- Design errors (present from day 1 of operation), e.g.
  - software errors
  - lack of discrimination (sensors)
  - wrong location
  - shortcomings in the functional testing (the test demand is not identical to a true demand and some part of the function is not tested)
- Human errors during functional testing, e.g.
  - maintenance crew forgets to test specific sensor
  - test performed erroneously (e.g. wrong calibration or component is damaged)
  - maintenance personnel forgets to reset by-pass of component

It is an essential and rather unique feature of PDS that it accounts also for such failures. This is done through the introduction of the *TIF* probability.

Test-Independent Failures - *TIF*

The *TIF* probability is defined as the *probability that a component that has just been tested (by a manual/functional test) will fail to carry out its intended function by a true demand*. For example, a *TIF*-probability of 0.05, means that there is a probability of 5% of an on demand failure (irrespective of the interval of manual testing).

The **PDS Forum** is a forum of oil companies, vendors and researchers with a special interest in reliability issues relating to computer based safety systems. The main activity of the PDS Forum will in 1998 be collection of more data for the PDS method, especially data relating to the TIF probability. See also the web site http://www.sintef.no/sipaa/prosjekt/pds-forum.html

Test-independent failures will include failures caused by for example improper location or inadequate design (software error or inadequate detection principle). An imperfect functional testing procedure will also contribute. Finally, the possibility that the maintenance crew performs an erroneous functional test (which is usually not detected before the next test) also contributes to the *TIF* probability.

3.5 Dependent Failures

When quantifying the reliability of systems employing redundancy, e.g., duplicated or triplicated systems, it is essential to distinguish between *independent* and *dependent* failures. Normal ageing failures (ref. Figure 2) are *independent* failures. However, both physical failures due to excessive stresses/human interaction and all functional failures are by nature *dependent* (common cause) failures. Dependent failures can lead to simultaneous failure of more than one module in the safety system, and thus reduce the advantage of redundancy.

In PDS dependent failures are accounted for by introducing a *multiplicity distribution*. The multiplicity distribution specifies the probability that - given that a failure has occurred - exactly k of the n redundant modules fail. Here, k equals 1,2, ... , n. The probability of k modules failing simultaneously is denoted p_k.

As an example, consider the multiplicity distribution for a redundant set of two modules, see Figure 3. Here $p_1 = 0.90$ and $p_2 = 0.10$. This means that - given that a failure has occurred - the probability that just one module has failed equals 0.90, and the probability that both modules have failed is 0.10.

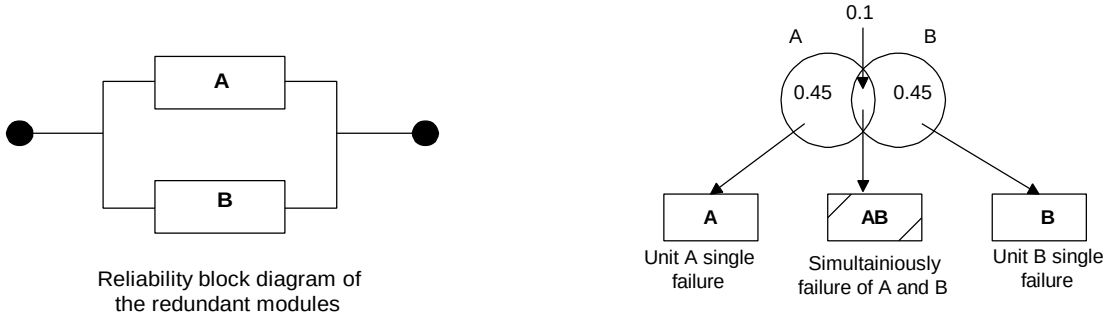

Figure 3: Example of multiplicity distribution for duplicated components.

3.6 Reliability Parameter Definitions of PDS

The following parameters are used in PDS (please also refer to Figure 4):

λ_{crit} = Total critical failure rate of the component. Rate of failures that will cause either trip or unavailability of safety function (unless detected and prevented from causing such failure).

λ_{det} = Rate of critical failures that are detected by automatic self-test or by control room monitoring. The effect of these failures on the Spurious Trip Rate *(STR*) depends on the operational philosophy of the system.

c = λ_{det} / λ_{crit} = Coverage of the automatic self-test and/or of the control room operator.

λ^{SO} = Total rate of Spurious Operation (SO) failures, including both detectable as well as undetectable failures.

λ^{SO}_{Undet} = Rate of SO failures, *un*detectable by automatic self-test. The rate of Spurious Operation (*SO*) failures of a component contributes to the *STR* of the system (*"production regularity"*)[5].

λ^{FTO} = Total rate of Fail-To-Operate (*FTO*) failures, including both detectable as well as undetectable failures.

λ^{FTO}_{Undet} = Rate of Fail-To-Operate (*FTO*) failures, *un*detectable by automatic self-test. The undetetcted *FTO* failures contribute to the Critical Safety Unavailability (*CSU*) of the component/system (*"loss of safety"*).

TIF = The probability of Test Independent Failures. The probability that a component that has just been functionally tested will fail on demand (applies for FTO failures only).

Observe that $\lambda_{crit} = \lambda_{det} + \lambda^{SO}_{Undet} + \lambda^{FTO}_{Undet}$.

An essential element is to clarify precisely which failures contribute to *TIF* and λ_{crit}, respectively. Figure 4 is an aid to clarify this. In particular the following is stressed concerning the interpretation of these concepts as used in the present report.

If an imperfect testing *principle* is adopted for the functional testing, this will increase the *TIF* probability. For instance, if a gas detector is tested by introducing a dedicated test gas to the housing via a special port, the test will not reveal a blockage of the main ports. Furthermore, use of a *dedicated* test gas is a contribution to the uncertainty, as testing with *process* gas has not been done.

The contribution of the *TIF* probability and λ^{FTO}_{Undet} to the Critical Safety Unavailability (*CSU*) is illustrated in Figure 5. The two main contributions to *TIF* are also indicated in the figure.

[5] Note that in the case of a *single* module, both detectable and undetectable failures of that module may contribute to the system STR, depending on the operating philosophy.

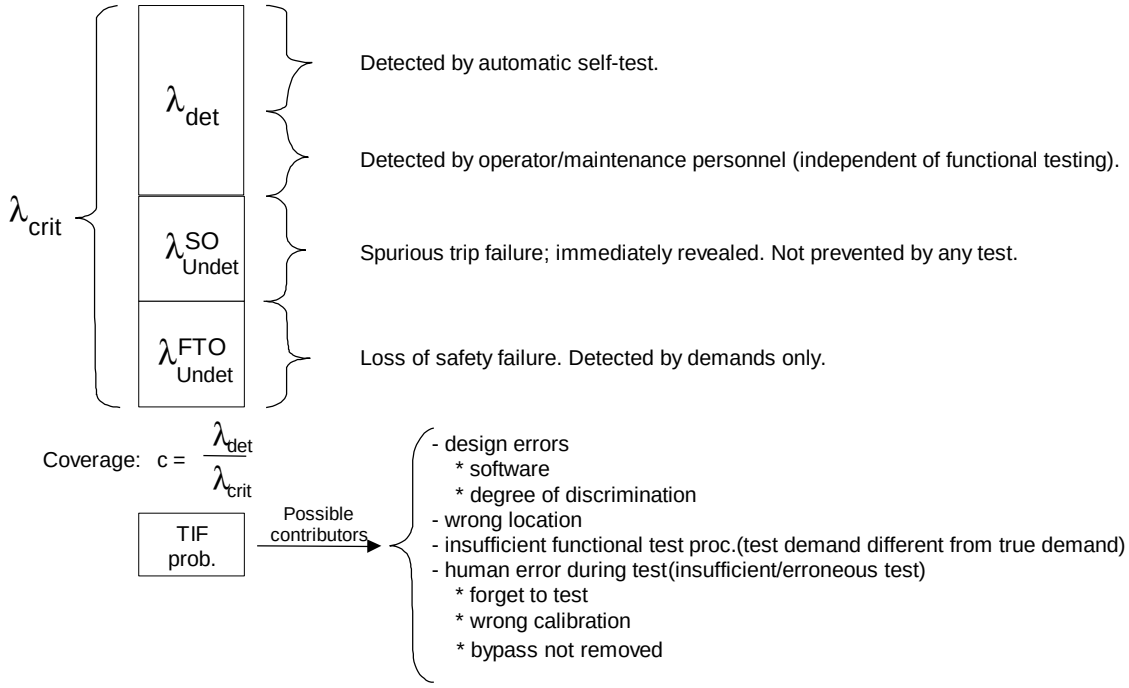

Figure 4: Interpretation of reliability parameters.

Coverage

The coverage is the fraction of the critical failures which is detected by the automatic self-test *or* by an operator. Thus, we include as part of the coverage any failure that in some way is detected in between functional tests. An analog sensor (e.g. transmitter) that is "stuck" will have a critical failure, but this failure is assumed to be detected by the panel operator and thus contribute to l_{det}. Any trip failure of a detector, giving a pre-alarm, which in principle allows the operator to prevent an automatic activation (trip) to occur is also part of l_{det}, and contributes to the coverage, *c*. In short, we include in l_{det} failures for which a trip *could* be prevented by specifying so in the operation philosophy. This means that *both* l_{det} and $l^{\text{SO}}_{\text{Undet}}$ can contribute to the spurious trip rate.

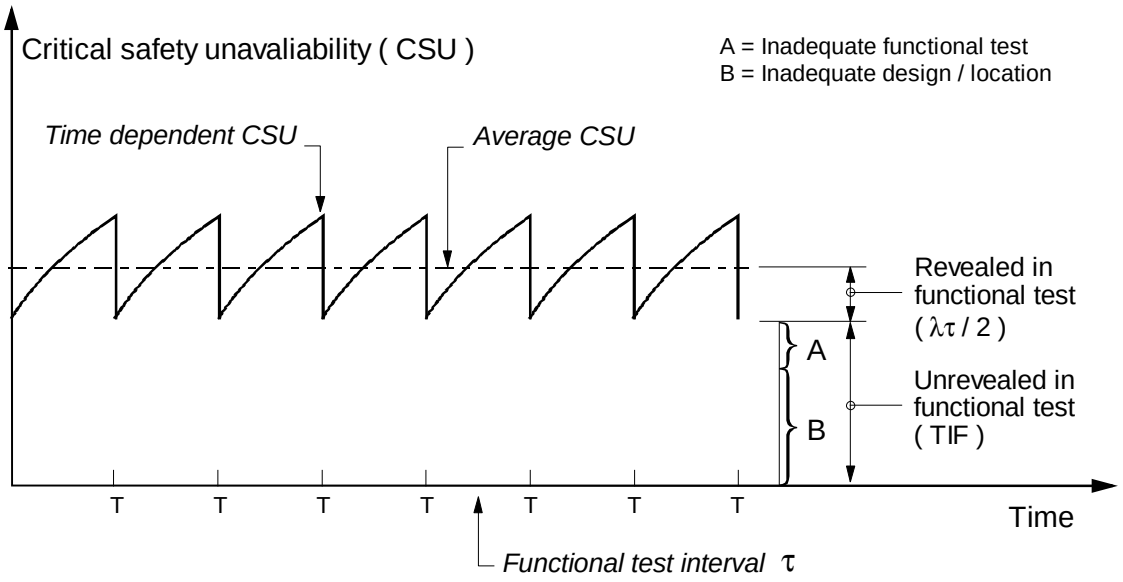

Figure 5: Contributions to the on demand failure probability, CSU.

3.7 Limitations

The main assumptions and limitations of PDS are given below. In addition to the general assumptions, a set of assumptions is needed to perform approximate calculations (to save time and effort). The PDS-Tool uses these approximate calculations.

General assumptions:

- All failure rates are constant with respect to time.
- A component is as good as new when repaired or tested.
- The CSU of the system is obtained by summing the CSU of each (set of) redundant module(s).

Assumptions for approximate calculations:

- The repair time and the self-test period are small compared to the interval between functional testing.
- All failure rates are less than 10^{-2} per hour.
- At least 10% of all failures in a redundant system are multiple failures causing two or more identical modules to fail at the same time.

Not considered:

- Non-critical unavailability of the computer-based safety system due to repair or functional testing of system modules (e.g. sensors inhibited) is not considered when quantifying loss of safety. It is assumed that the safety is maintained in other ways (e.g. by personnel located in the area given the task to activate proper shutdown command manually).
- Deliberate trip events due to maintenance/test activities are not considered.

4. A WORKED EXAMPLE

To illustrate PDS, a worked example is presented. The gas part of a fire and gas safety system is evaluated with respect to safety (CSU), production regularity (STR) and expected maintenance efforts (MCM). The PDS-tool is used for the calculations.

4.1 System Description

As a basis, a single fire area and one well on an offshore platform is considered. The fire and gas (F&G) system consists of twelve gas detectors, a F&G Node and two Emergency Shutdown Valves (ESV). The purpose of the F&G system is to shut down the production in the case of a fire or a gas leakage, and it is connected to the emergency shutdown system. A principal circuit diagram of the example system is shown in Figure 6. The twelve gas detectors are connected in a loop. A shutdown is initiated if at least two of the twelve detectors sense gas. In this case the F&G node closes both ESV A and ESV B. However, the valves are redundant, i.e., only one valve need to operate properly to carry out a successful shutdown.

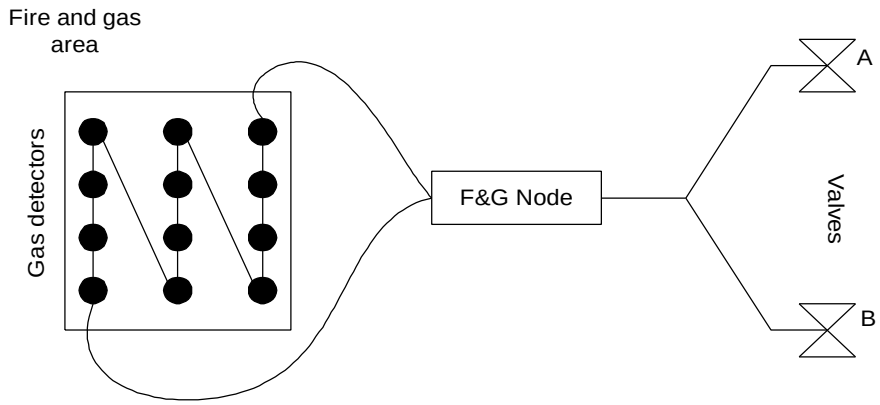

Figure 6: Example system.

Furthermore, two scenarios are considered;

- a small gas leakage, in which case on the average only three of the twelve gas detectors are located within the gas cloud. This implies that the actual voting configuration is in this case 2 out-of 3.
- large gas leakage, in which case on the average four of the twelve gas detectors are located within the gas cloud. This implies that the actual voting configuration is in this case 2 out-of 4.

The first scenario is considered the most common, and is given a weight 0.8, that is, 80% of all gas leakages are considered small. Large gas leakages are thus given a weight 0.2, see also [Bod94].

4.2 Input Data

The input data used in the calculations are extracted from the standard SINTEF PDS data. Table 1 below show the data needed for our calculations.

> The **standard SINTEF PDS data** was collected as a part of the SINTEF project "Reliability Data for Control and Safety Systems" [Hok95], for both field devices and control logic, and is included as a database in the PDS-Tool.

The total failure rate of FTO failures is given as l^{FTO}, and includes both detectable and undetectable failures. The effect of the automatic self-test, i.e. the coverage c is given as the proportion of all failures that are detected by the self-test or the operator. The rate of the remaining failures, l^{FTO}_{Undet}, is the one used to quantify the loss of safety. As we can see, the emergency shutdown valves are not equipped with self-test functions.

The failure rates of SO failures have the same interpretation as the FTO failures regarding coverage and undetected failures.

While the failure rates and the coverage are estimated from observed failure data, the TIF probabilities are based on expert judgements [Hok95].

For simplicity, a functional test interval of three months is assumed for all the gas detectors, the F&G node and the shutdown valves.

Table 1: Failure data of the example system.

Component	Fail to operate			Spurious operation			TIF
	l^{FTO}	Coverage	l^{FTO}_{Undet}	l^{SO}	Coverage	l^{SO}_{Undet}	
Gas Detector	$3\cdot10^{-6}$	50%	$1.5\cdot10^{-6}$	$2\cdot10^{-6}$	50%	$1\cdot10^{-6}$	$3\cdot10^{-4}$
F&G Node	$2\cdot10^{-5}$	90%	$2\cdot10^{-6}$	$6\cdot10^{-5}$	90%	$6\cdot10^{-6}$	$1\cdot10^{-4}$
ESV	$3\cdot10^{-6}$	0%	$3\cdot10^{-6}$	$5\cdot10^{-7}$	0%	$3\cdot10^{-6}$	$5\cdot10^{-5}$

4.3 Safety Assessment

In this case the undesired event is "*failure of the fire and gas system to close at least one of the valves in the case of a gas leakage in the fire area*".

The system consists of three modules; the gas detectors, the F&G node and the valves. The gas detectors are of the catalytic type.

In Figure 7 the reliability block diagram of the example system is shown. Details concerning the construction of this diagram may be found in [Aar89].

The PDS-Tool gives us the CSU of the small gas leakage scenario, using the input data of Section 4.2 and the reliability block diagram of Figure 7, as $CSU_S = 3.6\cdot10^{-3}$ (the scenario CSU is just the sum of the modules CSUs). The calculation of the CSU for the large gas leakage scenario is similar, but now we are using a 2 out-of 4 instead of a 2 out-of 3 configuration for the gas

detectors. This gives a $CSU_L = 4.0 \cdot 10^{-3}$. The general CSU is thus weighted to be CSU = $0.8 \times 3.6 \cdot 10^{-3} + 0.2 \times 4.0 \cdot 10^{-3} = 3.7 \cdot 10^{-3}$.

If we assume that the frequency of gas leakages (small or large) is once every two years, the frequency of undetected gas leakages due to an unavailable safety system is $3.7 \cdot 10^{-3} \times 0.5 = 1.85 \cdot 10^{-3}$ per year. The mean time to an undetected gas leakage due to an unavailable safety system is thus $1/1.85 \cdot 10^{-3} = 541$ years.

Even though the ESVs have a larger rate of undetectable FTO failures than the F&G node, the main contribution to the loss of safety comes from the F&G node, as seen from Figure 7. This is due to the fact that the valves employ redundancy whereas the F&G node is a single system.

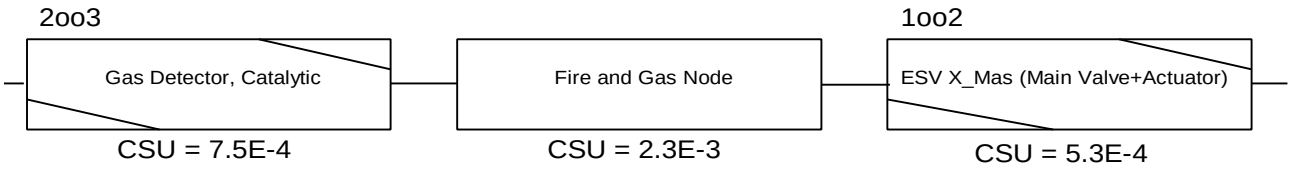

Figure 7: Reliability block diagram of the example system, small gas leakage scenario.

4.4 Production Regularity Assessment

The spurious trip event for this example system is "*the production is unintentionally shut down due to spurious operation of the fire and gas system*".

An extract of the PDS-Tool printout is given in Table 2. In the table the number of components, the voting configuration, the coverage and the total SO failure rate of a *single* component is given. The "Coverage" and the "Component STR" columns are taken from Table 1. The right-most column of Table 2 is the STR of each module, calculated from the failure data of Table 2 and a reliability block diagram similar to that of Figure 7.

The spurious trip rate of this example system is STR = $72 \cdot 10^{-6}$ failures per hour. Multiplied by 8760 hours, this gives us an expected number of spurious trip events of 0.7 per year.

From the table below we see that the F&G node gives by far the largest contribution to the spurious trip events.

Table 2: Data used and results from the loss of production regularity calculation.

Component	Number of Components	Voting	Component STR [hr^{-1}]	Coverage	Module STR [hr^{-1}]
Gas Detector	12	2oo12	$2 \cdot 10^{-6}$	50%	$11 \cdot 10^{-6}$
F&G Node	1	1oo1	$60 \cdot 10^{-6}$	90%	$60 \cdot 10^{-6}$
ESV	2	1oo2	$0.5 \cdot 10^{-6}$	0%	$0.92 \cdot 10^{-6}$
Total STR					**72×10^{-6}**

4.5 Assessment of Corrective Maintenance

When performing the corrective maintenance calculations, the rate of physical failures is used. This is the total rate of physical failures of a component, including all failure modes, detectable as well as undetectable. These failure rates are not shown in Table 1. However, Table 3 below gives an extract from the PDS-Tool printout, with the third column containing the physical failure rates. The column named "Lambda Physical" is the rate of the components physical failures and the column named "Rate of failed components" is simply lambda physical times the number of components.

It should be stressed that preventive maintenance is not included in the calculations. Furthermore, there is no standard SINTEF PDS data on the man-hours spent per *repair*. In the example, these figures are chosen more or less arbitrarily, as an example.

Using the PDS-Tool, we find the resulting estimated total man-hours spent on repair per year to be 7.1 man-hours.

Once again it is the F&G node that causes most problems. The analyses of the example system show that the F&G node is the reliability bottleneck of the system. To enhance the safety of the system, an additional node may be introduced, giving a 1 out-of 2 system for the F&G node. However, this will increase the SO failure rate, giving a higher number of spurious trip events and an increased maintenance activity. Thus, it might be the best solution to reduce the failure rate of the single F&G node, either by replacing it with a different, more reliable type, improving the existing node through re-design.

Table 3: Data used and results from the maintenance calculations.

Component	Number of Components	Individual component failure rate (Lambda Physical)	Rate of failed components	Man-hours per repair	Man-hours per year
Gas Detector	12	5.0E-6	60.0E-6	2.0	1.1
F&G Node	1	80.0E-6	80.0E-6	6.0	4.2
ESV	2	2.6E-6	5.2E-6	4.0	1.8
Total					**7.1**

5. REFERENCES

[NOR94] *Common Requirements, SAFETY AND AUTOMATION SYSTEMS (SAS),* Norsok Standard, 1-CR-002, Rev. 1, December 1994. Distributed by NORSOK Standards Information Centre, OLF, P.O.Box 547, N-4001 Stavanger.

[Aar89] R. Aarø, L. Bodsberg and P. Hokstad, *Reliability Prediction Handbook. Computer Based Process Safety Systems.* SINTEF Report STF75 A89023, 1989.

[Bod95] L. Bodsberg and P. Hokstad, *A System Approach to Reliability and Life-Cycle-Cost for Process Safety Systems.* IEEE Transactions on Reliability, Vol. 44, Number 2, 1995.

[Bod94] L. Bodsberg, P. Hokstad, H. Berstad, B. Myrland and T. Onshus, *Reliability Quantification of Control and Safety Systems. The PDS-II Method,* SINTEF Report STF75 A93064.

[EN97] *Draft EN 954 - Safety of Machinery – safety related parts of control systems*, 1997

[Hok95] P. Hokstad, R. Aarø, *Reliability Data for Control and Safety Systems.* SINTEF Report STF75 F94056.

[IEC95] Draft IEC 61508 - *Functional Safety: Safety Related Systems*, International Electrotechnical Commission, 1995.

[Lon96] S. Lone, T. Onshus, R. Aarø, H. Rustad, S. Holmstrøm and K. Corneliussen, *Teknologiutvikling innen sikkerhetssystemer*, SINTEF Report STF72 A96324, 1996 (in Norwegian).

LIST OF ABBREVIATIONS

CSU	Critical Safety Unavailability
ESD	Emergency ShutDown
ESV	Emergency Shutdown Valve
FTO	Fail To Operate
HIPPS	High Integrity Pressure Protection System
LCC	Life Cycle Cost
MCM	Mean Corrective Maintenance
NC	Non-Critical
NCU	Non-Critical safety Unavailability
OREDA	Offshore REliability DAta
PDS	Norwegian acronyms for the reliability of computer-based safety systems
SO	Spurious Operation
STR	Spurious Trip Rate
SU	Safety Unavailability
TIF	Test-Independent Failures