Effect of Safe Failures on the Reliability of Safety Instrumented Systems

Master Thesis by Einar Munkeby

Department of Production and Quality Engineering, Norwegian University of Science and Technology, 7491 Trondheim, Norway
E-mail: munkeby@stud.ntnu.no

June 9, 2008
Preface

This report is written in relation to a master thesis carried out in the 10th semester spring 2008, at the Norwegian University of Science and Technology. The title of the master thesis is *Effect of safe failures on the reliability of safety instrumented systems* and is written in cooperation with the Department of Production and Quality Engineering.

The reader is assumed to have basic knowledge within the field safety and reliability and preferably be familiar with the textbook *System Reliability Theory: Models, Statistical Methods and Applications*, (Rausand and Høyland, 2004).

Professor Marvin Rausand, at the Department of Production and Quality Engineering, has been the supervisor. For his weekly follow up as well as enlightening discussions, he deserves great thanks. His guidance and enthusiasm has made this work educational and inspiring. In addition, PhD student Mary Ann Lundteigen at NTNU and Thor Kjetil Hallan at Aker Solutions also deserve acknowledgment, for their supportive attitude and constructive comments.
4 Presentation of the article Effect of Safe Failures on Safety-Related Risk Assessment

4.1 Hazardous event rate .............................................. 17
4.2 Complete spurious trip system .................................. 18
4.3 Interpretation of model ............................................. 18
4.4 Evaluation of model ................................................ 21

5 Evaluation and modeling of potential effects 23

5.1 General for all models of the 1oo1 system ....................... 23
5.2 Effect of restoration times ......................................... 24
5.3 Safe failures as a means to remove dangerous undetected faults .. 30
5.4 Safe failures as an assurance of functionality .................... 33

6 Accurate modeling of HIPPS 37

6.1 Dangerous failure modes for a HIPPS ............................ 37
6.2 Detailed state transition diagram ................................. 38
6.3 Numerical results .................................................. 39

7 Modeling of a 1oo2 system 42

7.1 Assumptions for models of 1oo2 system ......................... 42
7.2 Potential states .................................................... 43
7.3 State transition diagrams ......................................... 45
7.4 Numerical results .................................................. 49

8 Conclusions and recommendations for further work 52

8.1 Conclusion ........................................................ 52
8.2 Recommendations for further work ............................. 54

A M-files i

A.1 M-files for 1oo1 models .......................................... ii
   A.1.1 M-file for effect of restoration times ......................... ii
   A.1.2 M-file for safe failures as a means to remove DU faults .... iv
   A.1.3 M-file for safe failures as an assurance of functionality ... vi
   A.1.4 M-file for detailed model of HIPPS ............................ viii
A.2 M-files for 1oo2 system .......................................... x
   A.2.1 M-file for availability analysis ................................. x
   A.2.2 M-file for safe failures as a means to reveal DU faults, with various dangerous failure rates ......................... xii
   A.2.3 M-file for safe failures as a means to reveal DU faults, with various beta factors ................................. xiv
List of Tables

2.1 Safety integrity levels for safety functions operating on demand (IEC 61508-1, Table 2) ................................................. 7
2.2 Hardware safety integrity: architectural constraints on type A safety-related subsystems (IEC 61508-2 table 2) ......................... 8
2.3 Hardware safety integrity: architectural constraints on type B safety-related subsystems (IEC 61508-2 table 3) ........................ 8
3.1 PFD obtained from classical probability calculations .......................... 16
5.1 Potential states for a 1oo1 subsystem ........................................ 23
6.1 Dominant dangerous failure modes for the final element on a HIPPS 37
7.1 Potential states for a 1oo2 subsystem ........................................ 44
### List of Figures

2.1 Safety instrumented system .............................................. 4

3.1 Schematic representation of a HIPPS ................................. 12
3.2 Interpretation of failure and restoration times in different contexts  
(adapted from IEC 61165 Figure 3) ..................................... 13
3.3 MTTRD as it is interpreted in this thesis. .............................. 15
3.4 Reliability block diagram for a 1oo1 configuration. ............... 15
3.5 Reliability block diagram for a 1oo2 configuration. ............... 16

4.1 Non-repeatable incident model (Sato and Yoshimura, 2007, Figure  
1b). ...................................................................................... 18
4.2 State transition model for a complete spurious trip system (Sato  
and Yoshimura, 2007, Figure 3) .......................................... 19

5.1 Potential effects on the PFD depending on the restoration procedure. 25
5.2 State transition diagram when potential dangerous failures are not  
detected before restoration. ............................................... 26
5.3 State transition diagram, when potential dangerous failures cannot  
evolve during safe state/ are always detected before restoration. ..... 27
5.4 Reduced state transition diagram, when potential dangerous failures  
cannot evolve during safe state/ are always detected before  
restoration. ........................................................................... 28
5.5 Dangerous steady state probability when as good as new assump-  
tion is assumed. ................................................................. 29
5.6 State transition diagram when a safe failure is a means to reveal/  
eliminate DU faults. .......................................................... 31
5.7 State transition diagram when a safe failure is a means to reveal/  
eliminate DU faults without effect from safe steady state. .......... 31
5.8 PFD when considering safe failures as a means to reveal/ eliminate  
DU faults. ........................................................................... 31
5.9 A safe failure gives assurance of functionality at time t ............ 33
5.10 State transition diagram when the expected unknown safety un-  
availability can be reduced by a safe failure prior to a DU failure in  
the same test interval. ......................................................... 35
5.11 Reduced state transition diagram when the expected unknown safety unavailability can be reduced by a safe failure prior to a DU failure in the same test interval. 35
5.12 PFD when safe failures give assurance of functionality. 36

6.1 Detailed state transition diagram for a 1oo1 HIPPS 38
6.2 PFD based on detailed state transition diagram for different values of $\lambda_D$. 40
6.3 Percentage effect on the PFD based on detailed state transition diagram, for different values of $\lambda_D$. 41

7.1 State transition diagram to evaluate production unavailability. 47
7.2 State transition diagram for a 1oo2 system, when a safe failure is is seen as a means to reveal/eliminate DU faults. 48
7.3 PFD for a 1oo2 system when safe failures are seen as means to reveal DU faults with $\beta = 0.02$. 49
7.4 Effect of safe failures when safe failures are seen as means to reveal DU faults with $\beta = 0.02$. 50
7.5 PFD for 1oo2 configuration for various beta factors with dangerous failure rate $10^{-6}$. 50
7.6 Effect of safe failures for a 1oo2 configuration for various beta factors with dangerous failure rate $10^{-6}$. 51
**Abbreviations**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCF</td>
<td>Common Cause failures</td>
</tr>
<tr>
<td>EUC</td>
<td>Equipment Under Control</td>
</tr>
<tr>
<td>FSC</td>
<td>Fail Safe Close valve</td>
</tr>
<tr>
<td>HFT</td>
<td>Hardware Fault Tolerance</td>
</tr>
<tr>
<td>HIPPS</td>
<td>High Integrity Pressure Protection System</td>
</tr>
<tr>
<td>DU</td>
<td>Dangerous Undetected</td>
</tr>
<tr>
<td>DD</td>
<td>Dangerous Detected</td>
</tr>
<tr>
<td>koon</td>
<td>k-out-of-n structure</td>
</tr>
<tr>
<td>MTTR\text{D}</td>
<td>Mean Time To Restore Dangerous failures</td>
</tr>
<tr>
<td>MTTR\text{S}</td>
<td>Mean Time To Restore Safe failures</td>
</tr>
<tr>
<td>OREDA</td>
<td>Offshore Reliability Data</td>
</tr>
<tr>
<td>PFD</td>
<td>Probability of Failure on Demand</td>
</tr>
<tr>
<td>SFF</td>
<td>Safe Failure Fraction</td>
</tr>
<tr>
<td>SIF</td>
<td>safety Instrumented Function</td>
</tr>
<tr>
<td>SIS</td>
<td>Safety Instrumented System</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>ST</td>
<td>Spurious Trip.</td>
</tr>
</tbody>
</table>
IEC 61508 is a standard for safety instrumented systems (SIS). In this standard, the probability of failure on demand (PFD) and the safe failure fraction (SFF) are decisive measures.

Reliability engineers discuss the influence of safe failures on the SIS availability. The SFF is a requirement concerning the minimum ratio of failures in a SIS, that can be classified as safe or detected. Since a minimum fraction of safe failures is required, the safe failures must be assumed to have a positive effect on the availability of a SIS. Some claim that the SFF requirement should be excluded, since the negative effects of safe failures may be more important than the positive effects. These negative effects of safe failures are thoroughly covered, while limited literature exists on the positive effects. The question is what the intent of the SFF really is. In other words, what positive impact may safe failures have on the availability of a SIS.

This thesis attempts to address all potential positive effects of safe failures. The PFD is a recognized measure for the safety unavailability. The safe failures are therefore incorporated into the PFD calculations. Markov models are applied for this purpose. To evaluate the realism of the effects, a production shutdown system is analyzed. Conclusions are drawn, based on the numerical results.

I. Yoshimura and Y. Sato have recently submitted for publication a paper called Effect of safe failures on safety-related risk assessment. They propose a Markov model to quantify the effect of safe failures. The adequacy and realism of the model is discussed.

Two distinct properties of a safe failure are relevant in relation to the PFD; the time needed to restore the system after a safe failure and the frequency of safe failures.

The former is not relevant for a production shutdown system. A demand cannot occur while the production is shut down and the restoration time of safe failures should therefore not be included in the PFD calculations. It does not affect the capability of the SIS to respond upon demand. For some applications, however, a long restoration time may affect the PFD negatively.

PFD calculations are done under the assumption that the safety unavailability caused by dangerous undetected failures is unaffected by other operating disturbances. Dangerous undetected faults are assumed to only be detected by
function tests or upon demand. Safe failures represent a third alternative to detect dangerous undetected faults. Safe failures may affect the unknown safety unavailability caused by dangerous undetected failures.

The effect of safe failures is only relevant when a safe failure occurs in the same test interval as a dangerous undetected failure. It is therefore concluded that safe failures only can be seen to have an effect, when the dangerous failure rate is high. On the contrary, the safe failure rate must be impractically high, before an effect is noticeable.

In addition, for the safe failures to have the intended effect, the following must be fulfilled:

- Upon detection of a safe failure, perfect repair can be assumed, i.e. either replacement of component or all dangerous faults revealed and removed before restoration.

- The safe failure must be detected and result in instant repair activities.

It seems that the SFF requirement is implemented to compensate for inaccuracies in the PFD calculations, when the dangerous failure rate is high. The numerical results do, however, show that other parameters have a more significant effect on the safety unavailability than safe failures. For a 1oo2 system, common cause failures affect the PFD more than a high safe failure rate.

It is not reasonable to change the design to make it in accordance with the calculated PFD. The PFD calculations should rather be accommodated to better reflect the designed system. The Markov models and interpretations presented in this thesis can be applied for this purpose.

Since safe failures often have negative effects as well, the SFF cannot remain a requirement to SISs. If a high safe failure rate is inevitable, one could use the positive effects of safe failures to justify a long test interval. This would not be better than frequent function tests and a low safe failure rate.

The effect of safe failures is mainly due to an increased probability of revealing dangerous undetected faults. An alternative requirement opposed to the SFF should be developed. The alternative requirement should allow other means of detection, such as by the operator, partial stroke testing, etc.
Chapter 1

Introduction

1.1 Background

The probability of failure on demand (PFD) and the safe failure fraction (SFF) are decisive measures for the reliability of a safety instrumented system (SIS).

The influence of safe failures on the SIS availability has been strongly discussed by reliability engineers, but a firm conclusion has yet not been drawn. Two Japanese researchers, I. Yoshimura and Y. Sato have recently submitted for publication a paper called Effect of safe failures on safety-related risk assessment, where Markov models are applied to quantify the effect of safe failures.

Sato and Yoshimura (2007) state that there is a logical conflict between the PFD requirement and the SFF, as the safe failures are ignored in the PFD calculations while taken into account through the architectural constrains. It is recognized that the safe failures have an effect on the SIS, while still being excluded from the numerical analysis. Sato and Yoshimura (2007) conclude that by including the safe failures in the numerical calculations, the SFF requirement may be neglected. The assumptions and the system modeled seems, however, rather artificial. Due to an introduction of additional variables, the numerical results become rather challenging to interpret.

1.2 Objectives

The main objective of this thesis is to evaluate the effect of safe failures on the availability of a SIS. This thesis is based on the following work tasks:

1. A literature survey on the relationship between safe failures and SIS reliability.

2. Become familiar with the paper by Yoshimura and Sato along with a discussion on the realism of their approach.
3. Identify potential effects of safe failures on SIS reliability and discuss their applicability and limitations.

4. Extend the approach in para. 2 to a more complex and realistic system.

5. Input realistic parameters into the model and discuss the results.

1.3 Limitations and constraints

A great deal of literature pinpoints the potential negative effects of safe failures, while there is little on the positive effects. In agreement with the supervisor of this master thesis, the scope of work has been limited to only examine the positive effects of safe failures that directly influence the safety integrity. This way, a more firm understanding of the reasoning behind the SFF requirement is obtained. Indirect effects, such as an increasing dangerous failure rate as a result of wear on the equipment or inducement of systematic failures as a result of for example human errors during restoration, are not considered in this thesis.

To keep the analysis clear, mainly the subsystem final element of a SIS is treated. This does not compromise the result, as the objective of the thesis mainly is to determine whether safe failures have a positive effect on the safety integrity.

1.4 Methodology

The SFF requirement and how it should be interpreted, is discussed frequently by reliability engineers. This literature is used to generate ideas on how safe failures may affect the availability of SISs. Little literature quantitatively address the effect of safe failures on SISs. There is however a great deal of literature on application of Markov models for determination of SILs. These are used to obtain an overview on how safe failures are treated in reliability models.

Sato and Yoshimura (2007) address the effect of safe failures through use of Markov models. As it seems to be the only present literature on quantification of the positive effect of safe failures, it forms the basis for this thesis. The adequacy and realism of the model presented is evaluated. The model is further extended, to take into account other effects of safe failures.

Since assumptions made are highly dependent on the application of the SIS, a case is selected. Markov models with relevant assumptions are derived and justified through use of the case. Relevant data are used to numerically indicate the effect of safe failures. Conclusions are drawn, based on argumentation and the numerical results.
1.5 Structure of the report

A general introduction to SISs is presented in Chapter 2. Potential effects of safe failures are presented in Chapter 3. A discussion on how different interpretations of quantitative assessment may result in different results is further given. In Chapter 4, the article Effect of safe failures on safety-related risk assessment (Sato and Yoshimura, 2007) is presented. An interpretation of the Markov model presented in this article and its adequacy is further given. In Chapter 5, each potential effect of safe failures is treated one by one, along with an evaluation on how to correctly incorporate them into Markov models. The effects that are concluded to influence the safety integrity, are further included in a detailed model for a 1oo1 system in Chapter 6. In Chapter 7, a 1oo2 system is treated. Conclusions and recommendations for further work is provided in Chapter 8.
Chapter 2

Safety Instrumented Systems & IEC requirements

2.1 Safety instrumented systems

A Safety Instrumented System (SIS) may be defined as an independent protection layer that is installed to mitigate the risk associated with the operation of a specified hazardous system, which is referred to as the equipment under control (EUC). OLF-070 defines EUC as a piece of equipment, machinery, part of an offshore installation, or even the entire installation. The EUC is the unit protected against going into a dangerous state, by the SIS.

The SIS performs specified functions to achieve or maintain a safe state of the process when deviations are detected. The safe state is a state of the process operation where the hazardous event cannot occur. The functions are called safety instrumented functions (SIF) and may, for example, be fire detection, gas detection, electric isolation, start and stop of fire pumps, active fire fighting, active smoke control, process protection or isolation of wells and riser, (OLF-070).

As shown in Figure 1, a SIS comprises detectors, logic solvers and final elements. In this figure the final element is illustrated as a valve.

![Diagram of SIS](image)

**Figure 2.1: Safety instrumented system**

The operation of a SIS requires a series of equipment to function properly. First, the sensors must be capable of detecting deviations. Second, the logic
solver must receive the sensor input signal, perform preprogrammed actions and give output to the final element. The logic solver output results in the final element taking action on the process to bring it to a safe state. If the SIS fails to do so, it is called failed to function.

A SIS may activate when no demand mode is present. This is called spurious trip (ST). In case the SIF is to shut down production, spurious trips will cause down time and production losses. Whether spurious trips also have an effect on the safety integrity is treated in detail in this thesis.

SISs may be divided into SISs with a high or with a low demand mode of operation. High demand mode of operation is when process demands occur frequently and the SIS is operated almost continuously. Low demand mode of operation means more seldom need and is in a passive state for long periods of time. Low demand mode is defined by IEC 61508 as less than once annually and no greater than twice the function test frequency.

2.2 IEC 61508

To provide guidance on development of SISs, the International Electrotechnical commission (IEC) has issued the standard IEC 61508 Functional safety of electrical/ electronic/ programmable electronic safety related systems. The IEC 61508 standard is a standard for SISs for all industries. This standard provides a framework for design and implementation of safety related systems based on electrical, electronic and/or programmable electronic technology. IEC 61508 is written generic and enables future development of more application specific standards. An example of such is IEC 61511 for the process industry. What differs the IEC 61508 standard from previous standards is the focus on quantitative safety analysis and safety life cycle.

2.3 Failure mode classification

IEC 61508 classifies failure modes into two main categories. A dangerous failure is a failure which has the potential to put the SIS in a hazardous or fail-to-function state. The standard further defines a safe failure as a failure which does not have the potential to put the SIS in a hazardous or fail-to-function state. The latter definition is a bit vague. CCPS (2007) specifies by defining a safe failure as a failure affecting equipment within a system, which causes, or places the equipment in a condition where it can potentially cause, the process to achieve or maintain a safe state. This definition is applied in this thesis as well. The safe failures considered can lead to a spurious activation of the SIF.

Dangerous failures are referred to as detected or undetected. Low demand of operation SISs may be passive systems until a process demand occurs in the EUC. The SIS may fail in the passive position and the failure may remain undetected until the SIS is required to operate on demand or function tested. These
failures are defined as *dangerous undetected* (DU) failures. Diagnostic self testing may reveal some of the failures. The dangerous failures are then defined as *dangerous detected* (DD) failures.

Safe failures may also be denoted detected and undetected, (Hauge et al., 2006a). The interpretation is that a safe failure may be detected before activation of the SIF and thereby can be avoided, before the process is brought to safe state. In this thesis, all safe failures are assumed to result in activation of the SIF.

### 2.4 Requirements and constrains

For safety instrumented systems a compound requirement called *Safety Integrity Level* (SIL) applies. Safety integrity is defined by IEC 61508 as the probability of a safety related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.

Four SILs are defined. The highest and most strict is SIL 4. For safety functions implemented through SIS technology, IEC 61508 states three main parameters that all have to be fulfilled in order to achieve a given SIL:

- Quantitative requirements,
- Architectural constrains,
- Requirements concerning techniques and measures for avoidance and control of systematic failures.

#### 2.4.1 Quantitative requirements

The quantitative requirement for low demand mode of operation SISs is expressed as the *Probability of Failure on Demand* (PFD).

The PFD may be expressed as the average safety unavailability $A(t)$ in a test interval $\tau$, (Rausand and Høyland, 2004).

$$\frac{1}{\tau} \int_0^\tau A(t)dt$$

(2.1)

In Equation (2.1), $A(t)$ is the probability that a DU failure has occurred at, or before, time $t$ within a test interval. In addition, to be in compliance with IEC 61508, also the unavailability due to restoration time should be included. MTTR$_D \times \lambda_D$ must then be added to the equation. Whether to include the latter is discussed further in Chapter 3.

The PFD requirement applies for the whole SIS. The PFD for the SIS can be approximated by summarizing the PFD for the sensors, logic solvers and final elements as indicated in Equation (2.2). If support systems are needed, they should be included in the subsystem they support. If for example a valve needs power to close, the power supply increases the unavailability of the valve, and should count as a part of the final element.
As shown in Equation (2.2) the PFD can be calculated independently for each subsystem. In this thesis the PFD for a final element is treated. For a subsystem with another configuration than 1oo1, the PFD is a combination of individual failures and common cause failures (CCF). In equation (2.3), \( i \) means sensors, logic solvers or final elements.

\[
PFD_i = PFD_{CC,i} + PFD_{independent,i}
\]

Table 2.1 presents the maximum PFD values a low demand SIS can have, to obtain a given SIL.

<table>
<thead>
<tr>
<th>Safety integrity level</th>
<th>Probability of failure on demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>( \geq 10^{-5} ) to ( &lt;10^{-4} )</td>
</tr>
<tr>
<td>3</td>
<td>( \geq 10^{-4} ) to ( &lt;10^{-3} )</td>
</tr>
<tr>
<td>2</td>
<td>( \geq 10^{-3} ) to ( &lt;10^{-2} )</td>
</tr>
<tr>
<td>1</td>
<td>( \geq 10^{-2} ) to ( &lt;10^{-1} )</td>
</tr>
</tbody>
</table>

### 2.4.2 Architectural constrains

A second requirement that must be fulfilled for a SIS to obtain a given SIL is the architectural constrains. Architectural constraints on hardware safety integrity are given in terms of three parameters; the **hardware fault tolerance** (HFT) of the subsystem, the **safe failure fraction** (SFF) and whether the subsystem is of type A or B.

SFF is the fraction of failures which can be considered safe because they are either detected or are classified as safe failures. Equation (2.4) may be used to calculate the SFF:

\[
SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_{total}}
\]

If the SFF is low, more strict requirements to the HFT apply. The HFT states the minimum number of faulty components that must be present in a subsystem to cause loss of safety function. For a koon structure, a subsystem that is functioning only if at least k out of n components are functioning, the HFT is k subtracted from n. For a SIS to achieve a given SIL, all subsystems in a single channel system must fulfill the criteria.
A subsystem may be of type A or type B. Table 2.2 and 2.3 shows the architectural constrains for type A and type B subsystems respectively. In accordance with IEC 61508, the items below summarize the criteria to for a subsystem to be of type A. If not all three criteria are fulfilled, the subsystem is of type B.

- All possible failure modes can be determined for all constituent components,
- Behavior of subsystem under fault conditions can be determined,
- There is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met.

<table>
<thead>
<tr>
<th>Safe failure fraction (%)</th>
<th>Hardware fault tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;60</td>
<td>SIL 1, SIL 2, SIL 3</td>
</tr>
<tr>
<td>60-90</td>
<td>SIL 2, SIL 3, SIL 4</td>
</tr>
<tr>
<td>90-99</td>
<td>SIL 3, SIL 4, SIL 4</td>
</tr>
<tr>
<td>&gt;99</td>
<td>SIL 3, SIL 4, SIL 4</td>
</tr>
</tbody>
</table>

Reliability engineers discuss the adequacy of this requirement. This is elaborated further in Chapter 3.

**2.4.3 Avoidance and control of systematic failures**

A third requirement is concerned with techniques and measures for avoidance and control of systematic failures. IEC 61508 distinguishes between random hardware failures and systematic failures. Random hardware failures are defined as failures, occurring at a random time, which result from one or more of
the possible degradation mechanisms in the hardware. A systematic failure is a failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or the manufacturing process, operational procedures, documentation or other relevant factors. IEC 61508 states that systematic failures must be handled qualitatively through certain techniques and measures. OLF-070 recommend the PDS method in favor of the calculation method described in IEC 61508, since the PDS method quantifies both safety unavailability caused by systematic failures and random hardware failure by using generic data from the PDS Data Handbook, (Hauge et al., 2006b). It is beyond the scope of this thesis to go into details about treatment of systematic failures. Only random hardware failures are considered in this thesis.
Chapter 3

Basis for the analyses

3.1 Interpretation of the SFF requirement

The SFF is discussed frequently by reliability engineers. It seems the basis for the discussion is a general confusion regarding the purpose of the SFF requirement. Lundteigen and Rausand (2006) state that the intent of the SFF may be to achieve safe design by reducing the DU failure rate by increasing the DD or safe failure rate. Sato and Yoshimura (2007) support this interpretation and state that a flaw with the SFF requirement is that the designer may add extraneous components or utilize components with poor quality, to increase the SFF. To avoid this loophole, Sato and Yoshimura (2007) suggest that there should be requirements to the total failure rate.

This interpretation does not entirely justify the SFF requirement, as the SFF is a supplement to the PFD requirement. If the PFD is within the stated requirements, there is no need to decrease the DU failure rate. In this thesis, the DU failure rate is therefore assumed unaffected by the SFF.

One question often brought up is what to consider as safe failures in relation to SFF. Grebe and Goble (2007) state that failure modes on parts or failure modes that affect a sub function not needed for successful completion of the SIF, should not be included in the SFF. An example of the latter is a function implemented to ease the communication with the operator. If the communication fails, the SIF is not necessarily affected. In this thesis, only safe failures that may result in a spurious trip, are considered relevant in relation to the SFF. Since all subsystems treated in this thesis are of 1ooN configuration, all safe failures result in activation of the SIF, i.e. a spurious trip. All DD failures, regardless of whether they result in a spurious trip or not, are however considered safe in relation to the SFF. This is done to be able to focus on the effect of safe failures only.

Lundteigen and Rausand (2008a), Lundteigen and Rausand (2006) and Signoret (2007) discuss the potential negative effects of safe failures and questions the adequacy of the SFF requirement. Langeron et al. (2007) perform a quantitative assessment of the effect of safe failures on SISs. The basis for the analysis
is that while the process is in safe state, either a dangerous failure cannot occur, occur with the same rate as during functioning state or occur with a higher rate than during functioning state. It is concluded that only the latter affects the PFD considerable, i.e. the PFD is increased as a result of safe failures. Also here, it is concluded that the SFF is not a reasonable requirement to achieve safe design.

This literature illustrates that the SFF requirement, as a generic requirement for all applications of SISs can be questioned. A quantitative assessment of the positive effects of safe failures is required. Only then, a firm conclusion can be drawn on whether the SFF requirement is viable or not. The positive effects are therefore treated in this thesis. Only one article obtained, Sato and Yoshimura (2007), treat quantitative assessment of the positive effects of safe failures. This article is therefore treated in Chapter 4.

### 3.2 Potential effects of safe failures

The potential effects of safe failures on the safety integrity are identified to be:

1. A safe failure may bring the process from dangerous state to safe state, (Sato and Yoshimura, 2007). If the detectors are in dangerous state, a safe failure resulting in a spurious trip in the final element brings the process to safe state.

2. An increased probability of being in safe state reduces the frequency of going to dangerous state, (Langeron et al., 2007). A closed shutdown valve (safe state), most likely stays in closed position even if a dangerous failure occurs.

3. A safe failure can be seen as a function test and reveal/ remove DU faults. If a safe failure activates the SIF but a DU fault inhibits the process from achieving safe state, the DU fault may be revealed. Alternatively, if parts are replaced as a result of the safe failure, the new item is without DU faults.

4. A safe failure may give assurance that the subsystem functions properly. After a spurious trip, the functionality is verified and it is known that certain DU faults are not present.

5. Safe failures result in more frequent operation of the SIS and may result in wear on the SIS and thereby increase the dangerous failure rate, (Lundteigen and Rausand, 2008a).

6. Safe failures may induce systematic failures due to, e.g., human errors during restoration, (Lundteigen and Rausand, 2008a).

7. Safe failures may result in an increased overall risk associated with the EUC, since a spurious trip can be an initiating event for another hazard scenario, (Grebe and Goble, 2007), (Signoret, 2007).
Statement 1 is discussed in Chapter 4 through the study by Sato and Yoshimura (2007). Statement 2, 3 and 4 are discussed in Chapter 5. How to incorporate them into Markov transition diagrams is further evaluated for a 1oo1 subsystem. Based on the arguments given in Chapter 4 and 5, a detailed model of a final element with 1oo1 configuration for a High Integrity Pressure Protection System (HIPPS) is presented in Chapter 6. A 1oo2 configuration is modeled in Chapter 7. Statement 5, 6 and 7 are considered to be beyond the scope of this thesis. Negative effects of safe failures are well covered by Langeron et al. (2007), Lundteigen and Rausand (2008a), Lundteigen and Rausand (2006) and Signoret (2007).

3.3 HIPPS

The case selected for this thesis is a HIPPS. A HIPPS is a SIS installed in a pipeline to a production system and protects against overpressure by quickly isolating the source causing the overpressure. If deviations are detected, a Fail Safe Close (FSC) valve is intended to close. Figure 3.1 presents a schematic of a HIPPS. As indicated with the dashed line, only the final element is treated.

![Figure 3.1: Schematic representation of a HIPPS](image)

The reliability data for a HIPPS valve including actuator and solenoid valve are derived from Hauge et al. (2006b). Hauge et al. (2006b) assumes no diagnostic self testing for the final elements but states that dangerous failures may be detected by other measures than upon demand and during function tests. The coverage factor $C_D$ for dangerous failures is therefore set to 0.28. It is not stated whether the detection is due to partial stroke testing performed periodically, instant detection upon occurrence or by other means. In this thesis, the mean time to isolate the EUC after occurrence of a DD failure is set to 8 hours. A DD failure is assumed not to result in a spurious activation of the SIF. $C_D$ equals the minimum SFF, when the safe failure rate is assumed zero. Instead of applying a constant safe failure rate, different values are applied to examine their effect.
The safe failure rate is calculated from the SFF with the dangerous failure rates set constant. Applying the SFF is done to keep the amount of new parameters to a minimum. It does also ease the possibility to examine the adequacy of this measure, as it is applied in IEC 61508. The dangerous failure rate is downsized from $4.0 \times 10^{-6}$ to $10^{-6}$, to avoid a too high safe failure rate when the SFF is higher than 90%. The test interval is assumed 12 months (8760 hours) and the beta factor is 0.02 for the 1oo2 subsystem.

### 3.4 PFD calculations by Markov models

Different interpretations of what PFD is, seems to be the crucial point of the discussion on how it should be calculated, (Bukowski et al., 2002), (Langeron et al., 2008), (Bukowski, 2005). Whether to take the effect of safe steady state probability into account, depends on the interpretation of what PFD is. Neither IEC 61508 nor ANSI/ISA 84.01 give a thorough definition of PFD. If the definition is the classical probability equation, Equation (2.1), the Markov model would have to be adjusted to give the same result. Bukowski (2005) discusses how the Markov model should be modified to provide the same result as using classical probability calculations. The model presented excludes safe failures to obtain the same numerical result. By following this path, the PFD may be used as an indicator of the reliability based on the same assumptions as the classical probability calculations. The advantages that lie within Markov modeling, are then not taken advantage of.

To obtain correct results, the main challenge is to define what is really to be measured. IEC 61165 outlines some interpretations on what to include in a Markov model, in different contexts.

![Figure 3.2: Interpretation of failure and restoration times in different contexts (adapted from IEC 61165 Figure 3)](image)

The timeline in Figure 3.2 illustrates that from detection of a dangerous fault, some time elapses until the EUC is isolated. The SIS is then repaired or replaced before it is restored back into operation. When analyzing a SIS, one may focus the analysis on the whole time line, the time the EUC is in operation and may experience a demand or on the time the SIS is assumed to operate without fail-
ures. These interpretations are, in Figure 3.2, denoted availability, safety and reliability respectively.

Evaluating a SIS based on the availability gives the most realistic result regarding steady state probabilities. This model aids decision makers select the SIS that best balances safety, cost, repair frequencies, uptime etc. However, when the EUC is isolated, there are no demands and one can question if the PFD can be claimed to be defined for this time interval at all. Bukowski (2001a) comes to a similar conclusion, when analyzing the MTTF_D.

PFD is a measure of the SIS’ capability to function as a barrier during operation. The PFD is the average probability that the SIF fails to activate upon a demand, which means that continuous exposure of the EUC is a prerequisite. Safe state should not be included when analyzing a production shutdown system.

One should exclude the time interval the EUC is isolated, to only consider the SIS when it is needed to protect the EUC. This is denoted as the safety interpretation in Figure 3.2. This interpretation is applied in IEC 61508 and IEC 61511.

In many applications, temporary compensating measures are introduced once a failure is detected. One can therefore assume that DU failures often create a higher risk than DD failures. Hauge et al. (2006a) therefore recommends to separate between known and unknown safety unavailability.

The interpretation denoted reliability in Figure 3.2 considers the probability that the SIS fails during operation and does not consider the duration of the known safety unavailability. This interpretation is applied in OLF-070. It should be noted that if there is continuous diagnostic surveillance and the EUC can be isolated instantaneously, the safety interpretation and the reliability interpretation are the same. In applications where the demand cannot be terminated, i.e. the EUC cannot be isolated, the safety interpretation and availability interpretation are also the same. The question regarding what interpretation to pursue, is in other words dependent on the application of the SIS.

When a failure is detected, time is often needed to introduce the risk reducing measures or isolate the EUC. In this thesis, MTTR_S for safe failures is different in nature from the MTTR_D for dangerous failures. The process is assumed to be in safe state during MTTR_S of safe failures and does therefore not pose an added risk.
3.5 Classical probability calculations

Reliability block diagrams are often applied to determine the PFD for a SIS. Equation (3.1) presented previously may be applied to determine the PFD.

\[ PFD = 1 - \frac{1}{\tau} \int_{0}^{\tau} R_{DU}(t) \, dt + \lambda_{DD} \, MTTR_{D} \]  

(3.1)

The first term is the unknown safety unavailability and the second term is the known safety unavailability. Note that MTTR\(_{D}\) due to DU failures is assumed not to contribute to safety unavailability, as the process is in function test mode. In this mode it is assumed that the EUC is isolated and therefore do not contribute to an increased safety unavailability. For SISs where the function test is performed on-line, the known safety unavailability is \(\lambda_{D} \, MTTR_{D}\), (Zhang et al., 2002).

For a 1oo1 subsystem, the PFD can be calculated based on the reliability block diagram in Figure 3.4.

\[ PFD = 1 - \frac{1}{\tau} \int_{0}^{\tau} e^{-\lambda_{DU}t} \, dt + \lambda_{DD} \, MTTR_{D} \]  

(3.2)

For a 1oo2 subsystem, the PFD can be calculated based on the reliability block diagram in Figure 3.5.

The contribution from individual failures to the PFD becomes

\[ PFD_{\text{individual}} = 1 - \frac{1}{\tau} \int_{0}^{\tau} 2e^{-(1-\beta)\lambda_{DU}t} - e^{-(1-\beta)2\lambda_{DU}t} \, dt \]  

(3.3)

The effect from two individual DD failures is considered negligible and the known safety unavailability due to individual DD failures is therefore excluded from this equation.
The contribution from common cause failures to the PFD becomes

$$\text{PFD}_{CC} = 1 - \frac{1}{\tau} \int_{0}^{\tau} e^{-\beta \lambda_{DU} t} dt + \beta \lambda_{DD} \text{MTTR}_D$$  \hspace{1cm} (3.4)

The numerical results, when assuming MTTR\(_D = 8, \lambda_D = 10^{-6}, C_D = 0.28\) and \(\beta = 0.02\), are presented in Table 3.1.

<table>
<thead>
<tr>
<th>Safety unavailability</th>
<th>PFD (1001)</th>
<th>PFD (1002)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>0.003147</td>
<td>7.57 (10^{-5})</td>
</tr>
<tr>
<td>Known</td>
<td>2.24 (10^{-6})</td>
<td>4.48 (10^{-8})</td>
</tr>
<tr>
<td>Total</td>
<td>0.003149</td>
<td>7.58 (10^{-5})</td>
</tr>
</tbody>
</table>
Chapter 4

Presentation of the article Effect of Safe Failures on Safety-Related Risk Assessment

4.1 Hazardous event rate

Sato and Yoshimura (2007) propose to calculate the average hazardous event rate, instead of applying PFD and SFF, to evaluate the safety integrity. Hazardous event, in this context, is the event the SIF is designed to mitigate the effects of or prevent from occurring. The frequency of a hazardous event is calculated by the joint probability of a dangerous failure and a process demand. According to Sato and Yoshimura (2007), the hazardous event may occur either by a demand when the SIF is unable to function or by a dangerous failure during demand. A simplified illustration is shown in Figure 4.1.

In Figure 4.1, $\lambda_M$ denotes the demand rate, i.e. the frequency a demand occurs per time unit. $\lambda_D$ is the dangerous failure rate. $\mu_M$ reflects the duration of a demand and $\mu_D$ is the restoration rate of dangerous failures.

The sequence with a dangerous failure followed by a demand is the most intuitive assumption, when calculating the PFD. The frequency of a hazardous event is then calculated by multiplying the PFD with the demand rate. The sequence with a demand followed by a dangerous failure may at first sight seem rare. However, if the EUC is in demand state in a deterministic time interval, failures can occur also in this time interval. Safe state is defined by IEC 61508 as a state of the EUC when the safety is achieved. It is further noted that for some situations a safe state exists only so long as the EUC is continuously controlled. Such continuous control may be for a short or an indefinite period of time. By including the demand state, Sato and Yoshimura (2007) takes this scenario into account. It is assumed that the SIF is activated once a demand occurs, i.e. demand state is safe state. An Example of this sequence is an AntiBlockierSystem (ABS) for car breaks. The ABS may be activated on demand but if the system fails
before the car is stopped and the friction is still too low, a hazardous event (the wheels slip) occurs.

The hazardous event rate is the frequency of hazardous events per unit time, (Sato and Yoshimura, 2007). Considering both sequences, one may express the hazardous-event rate, $\omega$, by

$$\omega = \lambda_M \Pr(\text{SIS in a dangerous state}) + \lambda_D \Pr(\text{demand state})$$

4.2 Complete spurious trip system

Sato and Yoshimura (2007) assume a Complete Spurious trip system, which means that the system always can go from dangerous to safe state, if a safe failure occurs. If the detectors are in dangerous fault state, a spurious trip in the final element brings the system to safe state.

A complete model of a 1oo1 system is presented in Figure 4.2.

4.3 Interpretation of model

To understand the model, all the states and transitions must be defined. An interpretation of the transitions and states is given below.

1. State A is the initial state where the SIF is available. From state A the process can:
   - fail DD and go to state K with rate $\lambda_{DD}$
Figure 4.2: State transition model for a complete spurious trip system (Sato and Yoshimura, 2007, Figure 3)

- fail DU and go to state C with rate $\lambda_{DU}$
- fail safe and go to state B with rate $\lambda_S$
- activate SIF on demand and go to state D with demand rate $\lambda_M$

2. State B is safe fault state. The SIF has not yet been activated. The process is brought to state B when a safe failure occurs in initial state. From state B the process can:

- go to safe state with rate $\mu_{SD}$. $1/\mu_{SD}$ is the time it takes to complete the SIF and bring the system to safe state.

3. State C is DU fault state. The SIF is unavailable. The process is brought to state C when a DU failure occurs in initial state. In state C the system can:

- go to initial state A with restoration rate $2/\tau$. $\tau/2$ is the average unknown safety unavailability, (shown in Chapter 5).
• go to hazardous event state E with demand rate $\lambda_M$.
• fail safe and go to state F with rate $\lambda_S$

4. State D is demand state. The SIF is activated in state D. The process is brought to state D when a demand occurs in initial state and thereby the SIF is successfully activated. From state D the system can:

• go back to initial state with rate $\mu_M$. $1/\mu_M$ is the duration of the demand and the time it takes to deactivate the SIF.
• fail DU or DD, causing the SIF to expire, and go to state E.
• fail safe and be brought to state H.

5. State E is the hazardous event state. The process is brought to state E when the SIF is unavailable and a demand is present. From state E the process can:

• be restored back to initial state with rate $m$.

6. State F is dangerous and safe fault state. The SIF has not yet been activated. The process is brought to state F when a safe failure occurs while the SIS is in dangerous fault state. From state F the process can:

• go to safe state S with rate $\mu_{SD}$. $1/\mu_{SD}$ is the time the SIF needs to put the system in safe state.

7. State H is safe fault state. The process is brought to state H when the SIS fails safe during operation of SIF. From state H the system can:

• go to state S with rate $\mu_{SD}$. $1/\mu_{SD}$ is the time the SIF needs to put the system in safe state.

8. State K is DD fault state. The SIF is unavailable. The process is brought to state K when a DD failure occurs in initial state. From state K the process can:

• go to initial state A with restoration rate $\mu_{DD}$. $1/\mu_{DD}$ is the time from failure to diagnostic detection and restoration is completed.
• go to hazardous event state E with demand rate $\lambda_M$
• fail safe and go to state F with rate $\lambda_S$

9. State S is safe state with a safe fault. The safe state is locked in and the process cannot be brought to another state without active intervention. From state S the process can:

• go to initial state A with reset rate $\mu_S$. This includes replacement or repair of all dangerous and safe faults that may be present in the SIS.
4.4 Evaluation of model

It is assumed that $\mu_{SD} \to \infty$, which means that the time from activation to completion of the SIF is insignificant. The states F, B, H, and S are then instantaneous states. State B, F, H, and S could have been merged to one state, i.e., safe fault state. Since it is assumed that $\mu_{SD} \to \infty$, it is not of importance but one could question the transition from state D to H. The SIF is already activated in state D and the time to obtain safe state is likely less than from for example initial state to safe state. To be consistent, the transition should have gone directly from state D to state S with rate $\lambda_S$.

The result based on the model in Figure 4.2 is optimistic regarding the effect of safe failures in three ways:

1. Complete spurious trip assumption is not entirely realistic,
2. It is assumed that all DU faults are revealed by a spurious trip and restoration always is back to initial state,
3. A SIS is often programmed to go to safe state when a DD failure is detected.

The complete spurious trip assumption is as stated by Sato and Yoshimura (2007) not entirely correct. Some dangerous failures may inhibit the completion of a SIF. The process is then not brought to safe state by the safe failure. If the SIF is not completed, the safe failure may not be revealed and thereby have no effect. This is elaborated further in 5.3.

$\mu_S$ is the reset rate of the SIS from safe state. Since the SIS is assumed to always be restored to initial state A, all dangerous failures must be assumed removed while in safe state. This is relevant if either the subsystem is replaced after every safe failure or if all dangerous failure modes are revealed by the spurious trip or during safe state. If dangerous faults are not revealed before restoration, the process is brought back to dangerous state. Whether the assumption is correct depends on the failure modes and the restoration procedure. The effect of eliminating dangerous failures by safe failures, can therefore not be claimed generic for all SISs. This is elaborated further in Section 5.2.

SISs are often programmed to activate the SIF if a DD failure occurs. A DD failure would then behave as a spurious trip, (Lundteigen and Rausand, 2008b), (Guo and Yang, 2007). If the DD failure itself does not inhibit the completion of the SIF, the transition from state DD to safe state would be close to $\mu_{SD}$ and not $\lambda_S$. Note that this explains the SFF requirement, where DD failures and safe failures are assumed to have an equal positive effect on the safety integrity.

To exclude the contribution from the increased steady state probability of being in safe or hazardous event state, the calendar time hazardous event rate, $\omega_{ct}$, is divided with the time the EUC is not in operation as shown in Equation (4.2). State B, F, E, H, and S are then assumed instantaneous states. The resulting $\omega$ then reflects the average hazardous event rate per unit EUC operating time at
time $t$. The result is then consistent with the safety interpretation discussed in Chapter 3.

$$\omega = \frac{\omega_{cl}}{1 - (P_B + P_E + P_F + P_H + P_S)}$$ \hspace{1cm} (4.2)

According to Sato and Yoshimura (2007), the effect of safe failures is negligible except for low demand systems with a demand duration higher than 10% of the test interval. The dominant sequences are either a demand followed by a dangerous failure or a DU failure followed by a demand, as indicated in the simplified model in Figure 4.1.

The effect of safe failures is high when the demand duration is long. When the system is in demand state, it can either go to hazardous event state or to safe state. If the safe failure rate is higher than the dangerous failure rate, the frequency of going from demand state to safe state is higher than the frequency of going from demand state to hazardous event state. The long demand duration is then cut off by a safe failure. However, if the DD failure rate is high, a higher hazardous event rate is obtained. The latter indicates that an increased DD failure rate, i.e. increased SFF, does not necessarily improve the safety integrity.

The effect of safe failures is also high if the demand rate is low. This conclusion can be drawn by considering the sequence where a dangerous undetected failure is followed by either a demand or a safe failure. The frequency of reaching hazardous event state from DU state is affected by the demand rate compared to the safe failure rate.

The introduction of the demand rate as well as the demand state makes the evaluation of the numerical results more challenging. Sato and Yoshimura (2007) conclude that, for a low demand system, safe failures have little effect when the demand duration is shorter than 10% of the test interval. In this thesis, a low demand system with demand duration assumed close to zero, i.e. $\mu_M \to \infty$ is treated. The component treated, a FSC valve, is designed to be locked in safe state after completion of the SIF. Once the valve is closed, the demand may be seen as eliminated. Demand state D and the demand rate is excluded from the analysis which eases the interpretation of the numerical results obtained. It is shown that safe failures still have an effect on the safety integrity, however depending on the underlying assumptions and the dangerous failure rate.
Chapter 5

Evaluation and modeling of potential effects

5.1 General for all models of the 1oo1 system

In this chapter, the potential positive effects, listed as item 2, 3 and 4 in Chapter 3, are treated one by one. For all the models, the potential states listed in Table 5.1 are defined for the 1oo1 subsystem.

Table 5.1: Potential states for a 1oo1 subsystem

<table>
<thead>
<tr>
<th>State</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>OK</td>
</tr>
<tr>
<td>2</td>
<td>S</td>
</tr>
<tr>
<td>1</td>
<td>DD</td>
</tr>
<tr>
<td>0</td>
<td>DU</td>
</tr>
</tbody>
</table>

The following assumptions apply for all 1oo1 models:

1. The subsystem is considered as one component.
2. Several failures are restored simultaneously and restoration of one fault does not require more time than two faults.
3. After a function test, the component is as good as new.
4. DD failures result in perfect repair.
5. All failure rates are constant, i.e. exponential distribution is assumed.
6. All restoration rates are constant, i.e. exponential distribution is assumed by applying mean restoration time. This approximation is adequate when calculating steady state probabilities, (Bukowski, 2006).
7. The duration of a demand is assumed negligible.

8. The probability that a component may have two or more dangerous faults simultaneously is negligible, compared to the probability of a single fault.

### 5.2 Effect of restoration times

*An increased probability of being in safe state reduces the frequency of going to dangerous state.*

Several studies Bukowski and Goble (1995), Rouvroye (2001), Langeron et al. (2007) include the safe state when applying Markov models to calculate the PFD. MTTR\textsubscript{s} may then affect the result. The effect of this interpretation is determined in this section.

It may seem trivial to implement safe state into a state transition diagram. However, when doing so, one must be clear on what assumptions that lie behind the modeling. Sato and Yoshimura (2007) assume that the SIS cannot fail dangerously, while the process is in safe state. However, even the process is in safe state, the failure mechanisms are not paused. As stated in IEC 61508 regarding random hardware failures, there are many degradation mechanisms occurring at different rates in different components and, since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of equipment comprising of many components occur at predictable rates but unpredictable (i.e. random) times.

Even though the failure rate is assumed constant, many of the failure mechanisms evolve gradually such as corrosion and fatigue. Often the failure mechanisms are not induced by the SIS operation in itself but by micro stresses such as cyclic pressure, temperature or vibrations in static position, (O’Brien, 2007). If the SIS is not removed from its environment, it is still affected by these mechanisms. A SIS that has been in safe state for an extended period has gone through almost the same stresses as if it had been in operating state.

The failure rate must therefore be based on the calendar time and not the EUC operating time. The SIS cannot fail dangerously in safe state but degradations induced while in safe state may become dangerous failures when the EUC is restored back into operation. Such a failure is denoted potential dangerous failure in this thesis.

Sato and Yoshimura (2007) assume that the SIS is as good as new after each safe failure. This does however depend on the failure mode and the restoration procedure. Mainly there are two distinct options, (Bukowski and Goble, 1994):

1. The system is as good as new after restoration from a safe failure
   
   • Component is replaced after safe failures
   • A safe failure can only lead to a spurious trip if it is not in dangerous fault state and the SIS cannot fail while in safe state

24
2. The SIS is not as good as new after restoration from safe fault state

- Repair activities are limited to only treat the safe fault. No monitoring activities are performed and potential DU failures induced while in safe state remain undetected.

The cumulative PFD distributions for the two extremes are illustrated in Figure 5.1. The PFD distribution denoted restore is the one normally assumed, when applying classical probability calculations. The assumption then follows item 2 and a spurious trip can be assumed negligible. The distribution denoted replace illustrates the potential effect of a safe failure.

Figure 5.1: Potential effects on the PFD depending on the restoration procedure.

Only the effect of being in safe state is modeled in this section. Depending on the assumptions made, the effect can differ. Considering Figure 5.1, the condition of the system can be unchanged during safe state, i.e. all failures are repaired before restoration. Otherwise potential dangerous failures may occur during safe state and put a system that is functioning at the time of the safe failure, into potential dangerous state before it is restored. For both assumptions treated below, it is assumed that a safe failure only can result in safe state when the system is in initial state.

**No repair assumption**

This assumption is relevant when the SIS is not restored back to initial state after a safe failure. No replacements or repairs are performed. If the process is restored back to operation without maintenance activities beyond the repair of the safe failure, a safe failure does not affect the safety integrity. As illustrated with dashed lines in Figure 5.1, the probability that the system is in DU fault state increases also when the system is in safe state. The operator obtains no indication on whether the system is functioning or not.

A transition from safe state to safe state with a potential DU fault is added in Figure 5.2 with rate $\lambda_{DU}$. When the system is assumed restored back to initial
state, in reality there exists a potential dangerous failure, which brings the system to DU state once it is put back into operation. DD failures occurring during MTTR\textsubscript{S} are however assumed to be repaired before restoration. They have no effect on the safety integrity, as the system already is in safe state. This is shown in Figure 5.2.

![State transition diagram](image)

**Figure 5.2**: State transition diagram when potential dangerous failures are not detected before restoration.

A similar scenario is discussed by Langeron et al. (2007), where the dangerous failure rate from safe state to dangerous fault state can either be lower, equal or higher than the transitions from initial state. Langeron et al. (2007) conclude that the effect of safe steady state is only significant, when the dangerous failure rate is higher during safe state. The effect of safe failures on the PFD is then negative.

**As good as new assumption**

If the safe faulty component is replaced or a complete maintenance bringing the system back to initial state can be assumed, the state transition diagram in Figure 5.3 can be applied. The longer duration of MTTR\textsubscript{S}, the less probability of a hazardous event during the test interval can be expected. The states denoted **safe state PDU** and **safe state PDD** are safe states with potential dangerous failures induced while in safe state. These are revealed before restoration and the system is restored back to initial state. For this model to be correct, a safe failure with the following restoration procedure must give the same assurance as a function test. This is the same assumption as Sato and Yoshimura (2007) make, to evaluate the effect of safe failures.

As illustrated in the state transition diagram in Figure 5.3, all failures induced while in safe state are detected and repaired. Since the restoration rates are as-
Figure 5.3: State transition diagram, when potential dangerous failures cannot evolve during safe state/ are always detected before restoration.

sumed the same for multiple repairs, the state transition diagram in Figure 5.3 can be simplified to the state transition diagram in Figure 5.4.

The states and transitions for the state transition diagram in Figure 5.4 are as follows:

1. In initial state, state 3, the SIF is available. From initial state the process can go to
   - DU fault state with transition rate $\lambda_{DU}$
   - DD fault state with transition rate $\lambda_{DD}$
   - Safe state with transition rate $\lambda_{S}$

2. In safe state, state 2, the production is shut down and the demand is eliminated. From safe state the process can go to
   - Initial state with rate $\mu_{S} = \frac{1}{MTTR_{S}}$.

3. In DD fault state, the SIF is unavailable. From DD fault state the process can go to
   - Initial state with transition rate $\mu_{DD} = \frac{1}{MTTR_{D}}$.

4. In DU fault state, the SIF is unavailable. From DU fault state the process can go to
   - Initial state with transition rate $\mu_{DU1oo1} = \frac{2}{7}$, (See below).
Equation (5.1) provides the average unknown safety unavailability in a test interval for a 1oo1 system, given the system has a DU fault at time $\tau$. For more details reference is made to Rausand and Høyland (2004), Chapter 10.

$$E(D|X(\tau) = 0) = \frac{E(D)}{F(\tau)} = \frac{\int_0^\tau F(t)dt}{F(\tau)} \approx \frac{\tau}{2} \tag{5.1}$$

This approximation is applicable when $\lambda_{DU}\tau < 0.1$. As outlined below in this chapter, an additional prerequisite is that the DU faults cannot be revealed by other means than function tests. The restoration rate from DU fault state becomes $DU1001 = 2/\tau$. As for the classical probability calculations, it is assumed that the EUC is isolated during the function test mode.

To obtain a complete production unavailability analysis, the contribution from MTTR$_D$ resulting from DU failures could have been included in this context. The transition $\mu_{DD}$ from DD fault state could further have been directed to an additional state representing the time the system is isolated after a dangerous failure. A complete representation of the production availability is then obtained. This is avoided in this context, to only examine the effect of safe failures.

The transition matrix derived from the model in Figure 5.4 becomes

$$A_\lambda = \begin{pmatrix} -\mu_{DU1001} & 0 & 0 & \mu_{DU1001} \\ 0 & -\mu_{DD} & 0 & \mu_{DD} \\ 0 & 0 & -\mu_S & \mu_S \\ \lambda_{DU} & \lambda_{DD} & \lambda_S & -\left(\lambda_{DU} + \lambda_{DD} + \lambda_S\right) \end{pmatrix}$$
The plot in Figure 5.5 is calculated based on the as good as new assumption. The plot shows that the DU and DD steady state probabilities are reduced, when the safe steady state probability is increased. This is a direct result of the reduced steady state probability of initial state, hence the reduced probability of a transition from initial steady state to DU or DD state.

![Dangerous steady state probability](image)

**Figure 5.5:** Dangerous steady state probability when as good as new assumption is assumed.

The effect is little as long as \( \lambda S \text{MTTR}_S \ll \tau \). Considering the plot in Figure 5.5, the effect is small, even when \( \text{MTTR}_S = 168 \text{ hours} \). However, when \( \lambda S \text{MTTR}_S \) is large, an optimistic result regarding the safety integrity is obtained.

These models are important for decision makers to select the SIS that best balances safety, cost, repair frequencies, uptime etc. Further would these models be useful to evaluate maintenance procedures. However, the result when including safe state, does not pinpoint the capability of a shutdown system to respond on demand. When evaluating a shutdown system from a safety point of view, the safe steady state should be excluded, as stated in Chapter 3.

It should be noted that the restoration of safe failures, for some applications, may be similar to the restoration of a DD failure. Considering a smoke detector that fails safe. The SIS may then have to be shut off, without the possibility to also isolate the EUC. Until the SIS is restored back into functioning state, the EUC is not protected. This would result in reduced safety availability due to safe failures.
5.3 Safe failures as a means to remove dangerous undetected faults

A safe failure can be seen as a function test and reveal/remove dangerous undetected faults.

One often assumes that a DU fault can be revealed by either a function test or upon a demand. A spurious trip may be a third alternative. This section evaluates the effect safe failures may have on detection/elimination of DU faults. The scenario is relevant when a safe failure occurs while the system is in DU state. This deviates slightly from the assumptions made by Sato and Yoshimura (2007), since the system is not brought directly to safe state. Two options are possible:

1. The faulty component is replaced after a safe failure.
2. The DU fault is revealed by the safe failure.

Item 1 is relevant if parts are replaced as a result of a safe failure. Any DU fault on the safe faulty part is then removed as well. An example can be a downhole safety valve. A spurious trip is assumed to wear the system considerably and as a result the SIS replaced after a certain number of spurious trips. Item 2 is relevant if a safe failure reveals DU faults. Regarding the HIPPS, an example is if the hydraulic pressure decreases as a result of utility leakage (safe failure) and the valve position indicator communicates that the valve is still in open position. The DU failure mode Fail To Close is then revealed by a safe failure. The safe failure will not bring the system to safe state, since the DU fault inhibits the completion of the SIF. Isolation of the EUC is required after detection. It should be noted that a prerequisite is that the safe failure is detected, despite that the process is not brought to safe state.

The event can be modeled as shown in Figure 5.6. To be consistent with the safety interpretation, the time it takes to isolate the system, MTTR_D, is included by bringing the transition from DU state to DD state. The transition rate is denoted \( ST \) and not \( \lambda_S \). This is done to outline that only the safe failures that are detectable, despite that the SIF is not completed, are relevant. A spurious trip from the logic solver or detector subsystems is most likely detected. Hydraulic leakage may however remain undetected. \( ST \) rate may, in other words, both be higher and lower than the safe failure rate for the subsystem final element, depending on the SIS. This is then not completely consistent with IEC 61508, as only safe failures on the relevant subsystem is to be included in the SFF.

To exclude the contribution from being in safe state, the safe state is assumed an instantaneous state, i.e. \( \mu_S \rightarrow \infty \). The state transition diagram can then be simplified to the model in Figure 5.7.

The transition matrix becomes
Figure 5.6: State transition diagram when a safe failure is a means to reveal/eliminate DU faults.

Figure 5.7: State transition diagram when a safe failure is a means to reveal/eliminate DU faults without effect from safe steady state.

\[
A = \begin{pmatrix}
-(\frac{2}{T} + ST) & ST & \frac{2}{T} \\
0 & -\mu_{DD} & \mu_{DD} \\
\lambda_{DU} & \lambda_{DD} & -(\lambda_{DU} + \lambda_{DD})
\end{pmatrix}
\]

In Figure 5.8, the PFD is plotted vs the SFF. As can be seen decreases the PFD when the safe failure rate increases. The justification of the SFF in this context can be that a high safe failure rate results in a higher rate of leaving, than entering the DU state. The relationship between the duration of the function test interval and the safe failure rate is however more decisive than the relationship between the dangerous failure rate and the safe failure rate. In IEC 61508, these three variables are interconnected. The combination of the dangerous failure rate and the test interval are examined through the PFD calculations. The safe failure rate is then linked to these two variables through the SFF.

It should be noted that there is a possibility that safe failures reveal faults that are not revealed by function tests. Hauge et al. (2006a) introduce the term \textit{test independent failures}, which are systematic failures that are only revealed...
Figure 5.8: PFD when considering safe failures as a means to reveal/ eliminate DU faults.

upon a true demand. Spurious trips may have a more random behavior, varying from time to time, in contrast to the function tests which often are performed in accordance with a procedure. This may be seen as an additional positive effect of safe failures.
5.4 Safe failures as an assurance of functionality

A safe failure gives assurance that the system functions properly.

This postulate may be seen as a direct translation of the SFF, i.e. the probability of a DD or safe failure before a DU failure. Equation (5.2) derives the SFF by calculating the probability of a safe failure before a DU failure.

\[
\Pr(T_S < T_{DU}) = \int_0^\infty f_s(t) \times \Pr(T_{DU} > t|T_S = t)dt
\]

\[
= \int_0^\infty \lambda_S e^{-\lambda_S t} \times e^{-\lambda_{DU} t} dt = \frac{\lambda_S}{\lambda_S + \lambda_{DU}}
\]

Here, \(T_S \) and \(T_{DU} \) are the times of safe and DU failure occurrences, respectively. \(f_s(t) \) is the probability that the system fails safe at time \(t \). \(\Pr(T_{DU} > t|T_S = t) \) is the probability that the system does not fail DU at or before time \(t \), given that the system fails safe at time \(t \). Note that if the effect of DD failures also had been taken into account, this approximation would be equal to the equation for SFF, given in Equation (2.4).

The statement examined in this section is that if a safe failure occurs in a test interval, the functionality is verified as shown in Figure 5.9. Alternatively is the SIS replaced after a safe failure, as a result of the additional stress on the SIS, caused by the operation of the SIF. This results in an assurance that the system functions at time \(t \). The effect of a safe failure before a DU failure is relevant if the system can be assumed as good as new after restoration.

![Figure 5.9: A safe failure gives assurance of functionality at time t](image)

If a safe failure occurs, the functionality of the system is verified, denoted \(X(t) = 1 \) in Figure 5.9. If the system then is found in DU state at time \(\tau \), \((X(\tau) = 0)\), the expected unknown safety unavailability is half the remaining of the test interval, for a 1oo1 system. Considering Figure 5.9, the expected DU down time is \(T2/2\).

Below, the expected unknown safety unavailability, given a safe failure before a dangerous failure in the same test interval, is estimated. \(\tilde{F}_{DU}(t) \) is the probability that one safe failure occurs before a DU failure within the same test interval. The downtime due to MTTRs is excluded from the estimation, to obtain a conservative result.

\[
\tilde{F}_{DU}(t) = \int_0^t f_s(u) \times \Pr(T_{DU} \leq t|0 < u < T_{DU} \leq \tau)du
\]
The first term is the probability of a safe failure at time \( u \). The second term is the probability that a DU failure occurs at or before time \( t \), given that the sequence of failures is a safe failure before a dangerous failure within the same test interval. By integrating, all values of \( u \) is considered. This may be expressed as

\[
\tilde{F}_{DU}(t) = \int_0^t \frac{P(0 < u < T_{DU} < t)}{P(0 < u < T_{DU} < \tau)} f_s(u) \, du
\]

The expected unknown safety unavailability, may be calculated based on the survival function \( \tilde{R}_{DU}(t) \) derived from \( \tilde{F}_{DU}(t) \)

\[
E(D) = \tau - \int_0^\tau \tilde{R}_{DU}(t) \, dt
\]

The average DU downtime, given the system has failed safe and the system is found in DU fault state at time \( \tau \), is then

\[
E(D|SF \cap X(\tau) = 0) = \frac{E(D)}{\tilde{F}_{DU}(\tau)} \approx \frac{\tau}{4}
\]

Since only the possibility of one safe failure is treated, exact calculations show that when the safe failure rate increases, the unknown safety unavailability increases. When the expected number of safe failures is less than once per test interval, \( \tau/4 \) is a good approximation. Further must \( \lambda_{DU} \tau < 0.1 \).

The state transition diagram is illustrated in Figure 5.10. The DU state has been split into two states, (Bukowski, 2006). If no safe failures have occurred previously in the same test interval, the normal restoration rate, \( \mu_{DU|SF} = 2/\tau \) applies. Otherwise is the restoration rate \( \mu_{DU|SF} = 4/\tau \). \( R_S(\tau) \) is here the probability that no safe failures occurs in a test interval. \( F_S(\tau) \) is the probability that at least one safe failure occurs in a test interval.

With safe state as an instantaneous state, \( \mu_S \to \infty \), the safe state can be excluded from the model. Further based on Bukowski (2006), the DU states may be merged by applying the average expected restoration rate. The transition diagram in Figure 5.10 can then be reduced to the transition diagram in Figure 5.11. The restoration rate from DU state then becomes

\[
\mu_{DU} \approx \frac{1}{\tilde{F}_S(\tau)\frac{1}{4} + R_S(\tau)\frac{\tau}{4}}
\]

The transition matrix becomes

\[
A = \begin{pmatrix}
-\mu_{DU} & 0 & \mu_{DU} \\
0 & -\mu_{DD} & \mu_{DD} \\
\lambda_{DU} & \lambda_{DD} & -(\lambda_{DD} + \lambda_{DU})
\end{pmatrix}
\]
Figure 5.10: State transition diagram when the expected unknown safety unavailability can be reduced by a safe failure prior to a DU failure in the same test interval.

The plot in Figure 5.12 shows that the PFD decreases, if assurance of functionality is obtained frequently. Also for this postulate, the effect of safe failures is caused by a reduced expected unknown safety unavailability. The effect of safe failures reflects the frequency of a safe and a DU failure in the same test interval.

A limitation of the presented model is that the possibility of multiple DU failures within a test interval must be assumed negligible. If several DU failures are likely to occur in the same test interval, it affects the unknown safety unavailability negatively. For the numerical result to be approximately correct, the DU failure rate must be low, i.e. $\lambda_{DU} \tau < 0.1$. This prerequisite may explain the intent of the SFF requirement. Whether classical probability calculations or

Figure 5.11: Reduced state transition diagram when the expected unknown safety unavailability can be reduced by a safe failure prior to a DU failure in the same test interval.
Figure 5.12: PFD when safe failures give assurance of functionality.

Markov models are applied, a system is assumed to either be functioning or not functioning. In reality, a number of possibilities exist. The effect of multiple DU failures within a test interval is not treated in this thesis. However, if two DU faults are found by function testing, the expected unknown safety unavailability is likely longer than $\tau/2$. In other words, if the SFF is low, the PFD is not conservative. If the SFF is 50%, the probability of a safe failure and a DU failure is the same as the probability of two DU failures occurring in the same test interval. Their effect work against each other. If the SFF is high, the PFD can be claimed conservative.

One may still question if it is correct to manipulate the design to improve the accuracy of the PFD. Taking the negative effects into account, the safety integrity is not necessarily improved by these modifications. Further, since the minimum PFD allowed is 0.1, $\lambda_{DU}\tau < 0.1$ is always fulfilled for a 1oo1 system.
Chapter 6

Accurate modeling of HIPPS

6.1 Dangerous failure modes for a HIPPS

To summarize the findings in the previous chapter, a detailed model of a 1001 HIPPS FSC valve is presented in this section. Based on arguments presented in Chapter 3, the restoration times of safe failures are not considered. The possibility of bringing the process from DU state to safe or DD state is considered. Further is the effect of assurance of functionality considered. The objective is to outline the realism of the presented postulates. Since a safe failure may have different effect on different dangerous failure modes, the DU state must be broken down into DU failure modes.

The dangerous failure modes assumed dominant for the HIPPS with percentage k, are given in Table 6.1. The percentage k is estimated based on failure mode rates in OREDA (2002) and Hauge et al. (2006b). The coverage factor for the dangerous failures is higher for the solenoid valve and in reality are therefore the failure modes FTC and DOP more affected by the coverage factor. Since the properties of the coverage factor for dangerous failures are not explained by OREDA (2002) in detail, it is assumed that it affects the listed failure modes equally.

Table 6.1: Dominant dangerous failure modes for the final element on a HIPPS

<table>
<thead>
<tr>
<th>Failure mode</th>
<th>k%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail to close (FTC)</td>
<td>35</td>
</tr>
<tr>
<td>Delayed operation (DOP)</td>
<td>20</td>
</tr>
<tr>
<td>External leakage of process medium (ELP)</td>
<td>35</td>
</tr>
<tr>
<td>Valve leakage in closed position (LCP)</td>
<td>10</td>
</tr>
</tbody>
</table>
6.2 Detailed state transition diagram

Figure 6.1 illustrates a detailed state transition diagram for the final element on a HIPPS.

The state transition diagram takes into account the effect of reducing the unknown safety unavailability. The DU state has been split into three states, to treat each failure mode separately. FTC and ELC are assumed to have the same properties, regarding detection by safe failures.

The transition from state 1 to state 3 is based on the assumption that safe failures may reveal/eliminate DU faults. The failure modes FTC and ELP are detected when the valve is intended to go to safe state. Since the SIS is unable to bring the process to safe state with these DU faults present, the dangerous faults are only detected, i.e. the transition is brought to DD state.

The transition from state 2 to state 4 is based on the assumption that safe state is obtained, despite a DU fault in the system. Although the system is in DU state DOP, safe state is obtainable. The additional time due to DOP is assumed negligible. DOP can be assured by a spurious trip from the sub systems logic solver or detectors. Hydraulic leakage would not likely reveal DOP; hence does it depend on the safe failure mode. This is not considered in the numerical calculations, as the safe failure rate is varying.
Leakage testing would in most cases require additional preparations such as pipe drainage. LCP is therefore assumed unaffected by safe failures. LCP can only be detected upon function tests.

If a safe failure has occurred prior to a DU failure in the same test interval, the expected unknown safety unavailability is $\tau/4$ as estimated in Section 5.4. The same failure modes that are revealed by safe failures, i.e. DOP, FTC and ELP, are also affected by the assurance of functionality.

The restoration rate for these failure modes is $\mu_{DU|S}$. The restoration rate from LCP is $\mu_{DU}$, the restoration rate normally assumed.

- $\mu_{DU|S} = \frac{1}{T_S(t_\frac{1}{4}) + T_S(t_\frac{1}{2})}$
- $\mu_{DU} = \frac{2}{T}$

Since the restoration from safe state is assumed instantaneous, the numerical calculations is manipulated by excluding state 4. The transition with rate $ST$ from state 2, failure mode DOP, to state 4 is then assumed directly back to initial state. The transition matrix becomes

$$A = \begin{pmatrix}
-\mu_{DU} & 0 & 0 & 0 & \mu_{DU} \\
0 & -(\mu_{DU|S} + ST) & 0 & ST & \mu_{DU|S} \\
0 & 0 & -(\mu_{DU|S} + ST) & 0 & ST + \mu_{DU|S} \\
0 & 0 & 0 & -\mu_{DD} & \mu_{DD} \\
\lambda_{DU,LCP} & \lambda_{DU,FTC,ELP} & \lambda_{DU,DOP} & \lambda_{DD} & -(\lambda_{DU} + \lambda_{DD})
\end{pmatrix}$$

### 6.3 Numerical results

Figure 6.2 shows plots of PFDs, for various dangerous failure rates. Safe failures may reduce the PFD considerable, however depending on the dangerous failure rate. To illustrate the effect of the safe failures more clearly, Equation (6.1) calculates the percentage reduction.

$$\text{Effect} = \frac{\text{PFD}_{\lambda_S=0} - \text{PFD}_{\lambda_S}}{\text{PFD}_{\lambda_S=0}}$$  \hspace{1cm} (6.1)

Based on Equation (6.1), the effect on the PFD for different values of $\lambda_D$ is plotted against the SFF in Figure 6.3.

As illustrated in Figure 6.3, the PFD is reduced when including the effect of safe failures. The reduction does however become insignificant, when the dangerous failure rate is low. When the dangerous failure rate is as low as $10^{-7}$, the effect is only 5%. This is due to the decreasing frequency of a DU failure and a safe failure occurring in the same test interval.

Based on the plot in Figure 6.3, the effect is only considerable for high dangerous failure rates. When the DU failure rate is $10^{-6}$ and the SFF is 99%, the
Figure 6.2: PFD based on detailed state transition diagram for different values of $\lambda_D$.

The reduction effect equals a reduction of almost 35%. The corresponding safe failure rate is then $7 \cdot 10^{-5}$. If the restoration time after a safe failure is considerable, this is impracticable with regards to production downtime.
Figure 6.3: Percentage effect on the PFD based on detailed state transition diagram, for different values of $\lambda_D$. 

![Diagram showing the percentage effect on the PFD for different values of $\lambda_D$.]
Chapter 7

Modeling of a 1oo2 system

7.1 Assumptions for models of 1oo2 system

In this section an extended model for a 1oo2 system is presented. Only the effect of revealing/eliminating DU faults is considered. The effect of assurance of functionality is not treated in this chapter. For the 1oo1 system, it was shown that the unknown safety unavailability, given a safe failure prior to a DU failure in the same test interval, may be approximated to $\tau/4$. A similar approximation is impracticable for a 1oo2 system. The number of failure sequences are considerable. Further is the approximation more dependent on the input variables. The unknown safety unavailability must be estimated for each combination of dangerous failure rate and SFF. Due to the complex integrals involved, a powerful computer would be required for this purpose.

For the 1oo2 system, common cause (CC) failures occur when both components fail due to a shared cause. IEC 61508 recommends that dangerous CC failures are modeled by a beta-factor model. In part 6 of the standard, a procedure is provided to estimate an application specific beta factor. In this thesis, it is relevant to both consider dangerous and safe CC failures. The procedure presented in the standard is according to Lundteigen and Rausand (2008b) not suitable for estimation of the beta-factor for safe CC failures. However, many of the same factors do apply, such as separated location and similarity in design. The same beta factor is applied for both safe and dangerous failures.

The same assumptions as for the 1oo1 system apply. In addition are the following assumptions made:

1. A CC failure cannot result in different fault categories. A CC failure results in either two safe failures, DD failures or DU failures.

2. It is assumed that each fault has a dedicated repair team. When several repairs are needed, the state transition is directly to OK state. The repair rate is then not increased with respect to the number of faults, (Bukowski and Goble, 1994). This means that:
• Several DU faults are repaired simultaneously.
• Several DD faults are repaired simultaneously
• Several safe faults are repaired simultaneously
• Safe and DD faults are repaired with duration MTTRₕ

3. The DU-DD state cannot go directly back to state OK. The probability of being in state DU-DD at time \( nt \) is assumed negligible.

4. The restoration of one faulty component does not affect the state of the other component.

5. Both components are function tested at the same time.

6. If one component is unavailable due to a dangerous fault, the system is run as a 1oo1 system.

7. The same beta factor is applied for DD, DU and safe failures.

7.2 Potential states

State 10, OK state, is initial state where both components are available. States 6, 7, 8 and 9 are defined as safe states. State 4 and 5 are reduced reliability states, i.e. run as 1oo1 system, but do not inhibit the SIF from activating on demand. In state 0, 1, 2 and 3 the SIF is unavailable, i.e. the system has failed dangerously.

The DU-DU fault state has been split into two states. This is done because the restoration rate due to a CC DU failure is \( \mu_{DU1oo1} = 2/\tau \), as estimated previously for the 1oo1 system. The restoration rate from two independent failures, \( \mu_{DU1oo2} \), may be estimated by applying Equation 7.1, (Rausand and Høyland, 2004).

\[
E(D|X(\tau) = 0) = \frac{E(D)}{F(\tau)} = \frac{\int_0^\tau F(t)dt}{F(\tau)} \approx \frac{\tau}{3} \quad (7.1)
\]
Table 7.1: Potential states for a 1oo2 subsystem

<table>
<thead>
<tr>
<th>State</th>
<th>Component 1</th>
<th>Component 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>9</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>8</td>
<td>OK</td>
<td>S</td>
</tr>
<tr>
<td></td>
<td>S</td>
<td>OK</td>
</tr>
<tr>
<td>7</td>
<td>S</td>
<td>DU</td>
</tr>
<tr>
<td></td>
<td>DU</td>
<td>S</td>
</tr>
<tr>
<td>6</td>
<td>DD</td>
<td>S</td>
</tr>
<tr>
<td></td>
<td>S</td>
<td>DD</td>
</tr>
<tr>
<td>5</td>
<td>DD</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>OK</td>
<td>DD</td>
</tr>
<tr>
<td>4</td>
<td>DU</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>OK</td>
<td>DU</td>
</tr>
<tr>
<td>3</td>
<td>DD</td>
<td>DD</td>
</tr>
<tr>
<td>2</td>
<td>DD</td>
<td>DU</td>
</tr>
<tr>
<td></td>
<td>DU</td>
<td>DD</td>
</tr>
<tr>
<td>1</td>
<td>DU</td>
<td>DU</td>
</tr>
<tr>
<td>0</td>
<td>DUCC</td>
<td>DUCC</td>
</tr>
</tbody>
</table>
7.3 State transition diagrams

Figure 7.1 shows a state transition diagram for a 1oo2 system focusing on the production availability.

In Figure 7.2, the effect of revealing/eliminating DU faults by safe failures is evaluated for 1oo2 subsystem. To stay consistent with the argumentation presented previously, the safe states are excluded.

The states and transitions are as follows:

1. State 6 is initial state. Both components are available. From state 6 the process can go to
   - state 0 with rate $\beta \lambda_{DU}$
   - state 3 with rate $\beta \lambda_{DD}$
   - state 4 with rate $2(1 - \beta)\lambda_{DU}$
   - state 5 with rate $2(1 - \beta)\lambda_{DD}$

2. State 5 comprises one DD faulty component. The system is run as a 1oo1 system. From state 5 the process can
   - be restored to initial state 6 with restoration rate $\mu_{DD}$.
   - fail safe and be restored to initial state 6 with rate $\lambda_{S}$ (since the $\mu_{S} \rightarrow \infty$, the transition is directly to initial state, and not by safe state)
   - fail DD and go to state 3 with rate $\lambda_{DD}$
   - fail DU and go to state 2 with rate $\lambda_{DU}$

3. State 4 comprises one DU faulty component. The system is run as a 1oo1 system. From state 4 the process can
   - be restored back to initial state with rate $\mu_{DU\text{1001}} = 2/\tau$
   - fail DU and go to state 1 with rate $\lambda_{DU}$
   - fail DD and go to state 2 with rate $\lambda_{DD}$
   - fail safe (DU faulty component) and go to state 5 with rate $ST = \lambda_{S}$

4. State 3 comprises two DD faulty components. The SIF is unavailable. From state 3 the process can
   - go to initial state with rate $\mu_{DD}$

5. State 2 comprises one DD and one DU faulty component. The SIF is unavailable. From state 2 the process can
   - be restored to state 4 with rate $\mu_{DD}$.
   - fail safe (DU faulty component) and go to state 3 with rate $ST = \lambda_{S}$
6. State 1 comprises two DU faulty components caused by individual failures. The SIF is unavailable. From state 1 the process can

- be restored to state 6 with restoration rate $\mu_{DU1oo2} = 3/\tau$.
- a CC safe failure reveals both DU faults and brings the system to state 3 with rate $STCC = \beta\lambda_S$
- one safe failure reveals one of the DU faults and brings the system to state 2 with rate $2ST = 2(1 - \beta)\lambda_S$

7. State 0 comprises two DU faulty components caused by CC failure. The SIF is unavailable. From state 1 the process can

- be restored to state 6 with restoration rate $\mu_{DU1oo1} = 2/\tau$.
- a CC safe failure reveals both DU faults and brings the system to state 3 with rate $STCC = \beta\lambda_S$
- one safe failure reveals one of the DU faults and brings the system to state 2 with rate $2ST = 2(1 - \beta)\lambda_S$

Note that when a system is in 2DU state, only a safe CC failure can bring it directly back to initial state. Independent safe failures occurring while the system is in 2DU state, only reveal the DU fault in the relevant component.

The transition matrix becomes

$$A = \begin{pmatrix}
-a_{00} & 0 & 2ST & STCC & 0 & 0 & \mu_{DU} \\
0 & -a_{11} & 2ST & STCC & 0 & 0 & \mu_{DU1oo2} \\
0 & 0 & -(\mu_{DD} + ST) & ST & \mu_{DD} & 0 & 0 \\
0 & 0 & 0 & -\mu_{DD} & 0 & 0 & \mu_{DD} \\
0 & \lambda_{DU} & \lambda_{DD} & 0 & -a_{44} & ST & \mu_{DU1oo1} \\
0 & 0 & \lambda_{DU} & \lambda_{DD} & 0 & -a_{55} & \mu_{DD} + \lambda_S \\
CC_{DU} & 0 & 0 & CC_{DD} & 2\lambda_{DU} & 2\lambda_{DD} & -a_{66}
\end{pmatrix}$$

where

- $a_{00} = \mu_{DU} + STCC + 2ST$
- $a_{11} = \mu_{DU1oo2} + 2ST + STCC$
- $a_{44} = \lambda_{DU} + \mu_{DU1oo1} + ST + \lambda_{DD}$
- $a_{55} = \mu_{DD} + \lambda_S + \lambda_{DD} + \lambda_{DU}$
- $a_{66} = CC_{DD} + CC_{DU} + 2\lambda_{DD} + 2\lambda_{DU}$
Figure 7.1: State transition diagram to evaluate production unavailability.
Figure 7.2: State transition diagram for a 1oo2 system, when a safe failure is is seen as a means to reveal/ eliminate DU faults.
7.4 Numerical results

The plot in Figure 7.3 shows the PFD for different values of $\lambda_D$, when the beta factor is set to 0.02. The same input variables are applied to calculate the percentage effect on the PFD in Figure 7.4. Since the model in Chapter 6 is based on different assumptions, one cannot compare the results one to one. However, it seems that the percentage effect for both configurations, is highly dependent on the dangerous failure rate. The effect when the dangerous failure rate is low, is insignificant.

![Figure 7.3: PFD for a 1oo2 system when safe failures are seen as means to reveal DU faults with $\beta = 0.02$.](image)

In Figure 7.5, different beta factors have been applied with $\lambda_D = 10^{-6}$. The percentage effect, shown in Figure 7.6, is highest for low beta factors. There is no overlap between any of the PFDs, which means that the applied beta factors affect the PFD more than the safe failures. Accurate estimation of the beta factor may be seen as more important than implementation of the safe failures, when calculating the PFD for a redundant subsystem.
Figure 7.4: Effect of safe failures when safe failures are seen as means to reveal DU faults with $\beta = 0.02$.

Figure 7.5: PFD for 1oo2 configuration for various beta factors with dangerous failure rate $10^{-6}$. 
Figure 7.6: Effect of safe failures for a 1oo2 configuration for various beta factors with dangerous failure rate $10^{-6}$.
Chapter 8

Conclusions and recommendations for further work

8.1 Conclusion

A literature survey on the relationship between safe failures and SIS reliability has been carried out. Reliability engineers discuss whether SFF is an adequate measure in relation to the safety integrity. The negative effects of safe failures are thoroughly covered, while limited literature exists on the positive effects. A quantitative assessment of the potential positive effects of safe failures is needed and has therefore been conducted.

Sato and Yoshimura (2007) address one of the potential positive effects of safe failures. The realism of their approach has been examined and the presented model has been concluded reasonable.

In addition to the effect treated by Sato and Yoshimura (2007), other potential effects of safe failures on SIS reliability have been identified. The potential effects have been incorporated into Markov models for a 1oo1 system. An evaluation of the applicability and limitations of the models has further been conducted. To obtain numerical results and to be able to evaluate the realism of the effects, a HIPPS has been selected as a case study. Finally, incorporation of the effects of safe failures has been discussed for a 1oo2 system. Conclusions have been drawn, based on the numerical results.

The potential positive effects of safe failures are due to the restoration time of safe failures and the frequency of safe failures.

For a HIPPS, a long restoration time after a safe failure, results in a reduced frequency of hazardous events based on calendar time. It is, however, not adequate when analyzing the safety integrity of a shutdown system, to take into account the time spent in safe state. It does not affect the capability of the system to respond upon demand. For other applications, however, the restoration
time may affect the safety integrity negatively.

Safe failures can be seen as a third alternative to detect dangerous undetected faults, in addition to function tests and upon demands. This is concluded to be the intent of the SFF requirement.

For the safe failures to have the intended effect, the following assumptions are prerequisites:

- Upon detection of a safe failure, perfect repair can be assumed, i.e. either replacement of component or all dangerous faults revealed and removed before restoration.

- The safe failure must be detected and instantly result in repair activities.

The SFF requirement is most likely meant to compensate for inaccuracies in the PFD calculations. Whether classical probability calculations or Markov models are applied, it is assumed that a component only can be in one fault state. In reality, for mechanical components, numerous of faults may be present at the same time. An accurate model would require a large number of states.

A safe failure in the same test interval as a dangerous failure, reduces the unknown safety unavailability. The actual PFD is then lower than the calculated PFD. Several dangerous undetected failures in the same test interval, on the other hand, increases the unknown safety unavailability. A high SFF results, in other words, in a conservative PFD. The inaccuracy is, however, in most cases negligible.

The effect of safe failures on the PFD, is dependent on the dangerous failure rate. When the dangerous failure rate is of an order of magnitude less than $10^{-7}\text{hours}^{-1}$, the effect of safe failures is negligible even with a SFF as high as 99%. When the dangerous failure rate is higher than $10^{-6}\text{hours}^{-1}$, the effect may be significant. However, before the effect is noticeable, the corresponding safe failure rate must be impractically high. If the restoration time after safe failures is long, the effect on the production availability is considerable.

It seems unreasonable to state requirements to the design, to make it in accordance with the calculated PFD. The PFD calculations should rather be accommodated to better reflect the designed system. In any case, other parameters have a more significant effect than safe failures. Numerical results in this thesis, have shown that for a 1oo2 system, common cause failures and the accuracy of the beta factor has more potential to affect the PFD than safe failures.

Since safe failures often have negative effects as well, the SFF cannot remain a requirement to SISs. If a high safe failure rate is inevitable, one could use the positive effects of safe failures to justify a long test interval. The Markov models and interpretations presented in this thesis, can be applied for numerical justification.
8.2 Recommendations for further work

The presented Markov models are only applicable for applications with a low frequency of dangerous failures. Markov models should be developed for redundant systems where the assumption \( \lambda_D \tau < 0.1 \) is not fulfilled. The models should be applied to evaluate whether several dangerous undetected failures, in the same test interval, actually affect the PFD considerable.

The effect of safe failures is mainly due to an increased probability of revealing dangerous undetected faults, through other measures than the ones accounted for in the PFD calculations. An alternative requirement to the SFF should be developed. The alternative requirement should allow other means of detection, such as; by the operator, partial stroke testing, etc. This requirement should be seen in relation to the calculated PFD and not as an independent requirement.
Bibliography


Appendix A

M-files
A.1 M-files for 1oo1 models

A.1.1 M-file for effect of restoration times

```matlab
%Input data
format long
tau=8760;
undetected =tau/2;
MTTR=8;
DU=1/(MTTR+undetected);%restoration rate for individual DU failures
muDD=1/MTTR;

Cd=0.28; %diagnostic coverage
lamD=1e-6 %total dangerous failure rate
lamDU=lamD*(1-Cd); %DU failure rate
lamDD=lamD*Cd; %DD failure rate

mttrsafe=[8 168 730 2190]; %Variable durations of restoration of safe fault
SFF=[Cd:0.01:0.99]; %SFF between Cd and 0.99

%Matrices to store steady state probabilities
safestate=ones(length(mttrsafe),length(SFF));
PFD=ones(length(mttrsafe),length(SFF));
availability=ones(length(mttrsafe),length(SFF));
OK=ones(length(mttrsafe),length(SFF));

for r=1:4
    muSO=1/mttrsafe(r) % safe restoration rate
    l=1:length(SFF); %matrix to store safe failure rates
    states=ones(length(SFF),4);
    for i=1:length(SFF)
        SFFi=SFF(i);
        lamSO=((lamDU+lamDD)*SFFi-lamDD)/(1-SFFi);
        l(i)=lamSO; %stores the safe failure rate values in l matrix
    end
    A=[-DU 0 0 DU;
       0 -muDD 0 muDD;
       0 0 -muSO muSO;
       lamDU lamDD lamSO -(lamDU+lamDD +lamSO)];
    A(:,4)=ones;
    dP=zeros(1,4);
    dP(1,4)=1;
    Po=dP*inv(A);
    CHECK=sum(Po);
    states(i,1:4)=Po;
end
```

%temporary stores the values from the above calculations
safestate_2=safestate(1:length(SFF),3);
PFD_state01=states(1:length(SFF),1)+states(1:length(SFF),2)
```
stores the values in a permanent matrix for all MTTRs
safestate(r,:) = safestate_2;
PUU(:,1,:) = PUU_state1;
availability(r,:) = availability_state3;
end
and repeats for next MTTR value

end/repeats for next MTTR value

Calculates the percentage effect
DR1 = (1:length(SFF));
DR2 = (1:length(SFF));
DR3 = (1:length(SFF));
DR4 = (1:length(SFF));
for k = 1:length(SFF)
    DR1(k) = (PFD(1,1) - PFD(1,k)) / PFD(1,1);
    DR2(k) = (PFD(2,1) - PFD(2,k)) / PFD(2,1);
    DR3(k) = (PFD(3,1) - PFD(3,k)) / PFD(3,1);
    DR4(k) = (PFD(4,1) - PFD(4,k)) / PFD(4,1);
end

plots the probabilities for each state against the SFF

dangerous steady state probability
plot(SFF,PFD(:,1,:),SFF,PFD(:,2,:),SFF,PFD(:,3,:),SFF,PFD(:,4,:));
xlabel('SFF','dangerous steady state probability');
format long
title('###');
legend('MTTRS=8 hours','MTTRS=168 hours','MTTRS=730 hours');

Safe steady state probability
semilogy(SFF,safestate_2,'k')
xlabel('SFF');
ylabel('Safe state');

Availability steady state probability
plot(SFF,availability(:,1,:))
xlabel('SFF');
ylabel('Production availability');
A.1.2 M-file for safe failures as a means to remove DU faults

0001 % Failure rates from PDS table 11: Reliability data for HIPPS components
0002 format long
0003 tau=8760;
0004 undetected =tau/2;
0005 MTTR=8;
0006 DU=1/(undetected); % Restoration rate for individual DU failures
0007 muDD=1/MTTR; % DU restoration rate
0008 muSO=1/MTTR; % Safe restoration rate
0009
0010 Cd=0.28; % Diagnostic coverage
0011 lamD=1.0e-6; % Total dangerous failure rate
0012 lamDU=(1-Cd)*lamD; % DU failure rate
0013 lamDD=Cd*lamD; % DD failure rate

0014 % Safe failure fraction from Cd (only DD failures) to 0.99
0015 SFF=[Cd:0.01:0.99];
0016 l=1:length(SFF);
0017
0018 % Produces a matrix to store the steady state probabilities
0019 % for all the SFF values.
0020 states2=ones(length(SFF),3);
0021
0022 % i is here the number of values of SFF. Do the following i times.
0023 for i=1:length(SFF);
0024 % Sets SFF value from SFF matrix
0025 SFFi=SFF(i);
0026 % Calculate safe failure rate from SFF
0027 lamSO=((lamDU+lamDD)*SFFi-lamDD)/(1-SFFi);
0028 % Store all lamSO
0029 l(i)=lamSO;
0030 % Assumes that all safe failures cause detection of DU failures
0031 STdetect=lamSO;
0032
0033 % Transition matrix
0034 As=[-(DU+STdetect) STdetect DU;
0035 0 -muDD muDD;
0036 lamDU lamDD -(lamDU+lamDD)];
0037 As(:,3)=ones;
0038
0039 dPtau=zeros(1,3);
0040 % Sum of Po(t)+...Pi(t)=1
0041 dPtau(1,3)=1;
0042 % Calculates the steady state probabilities
0043 Potau=dPtau*inv(As);
0044 % Verifies that sum=1
0045 CHECK=sum(Potau);
0046 % Stores all values
0047 states2(i,1:3)=Potau;
0048 end % repeat for next value of lamSO/end
0049
0050 % Stores the steady state probabilities in matrices
0051 Production_availabilityS=states2(1:length(SFF),3);
0052 PFD_state0S=states2(1:length(SFF),1)+states2(1:length(SFF),2);
0053
0054 DR1=(1:length(SFF));
0055 for k=1:length(SFF)
0056 DR1(k)=(PFD_state0S(1)-PFD_state0S(k))/(PFD_state0S(k));
0057 end
0058
0059 % Plots steady state probabilities vs SFF
0060 subplot(2,2,1)
0061 plot(SFF,PFD_state0S,'k')
0062 xlabel('SFF')
0063 ylabel('PFD')
0064 subplot(2,2,2)
0065 plot(SFF,DR1,'k')
0066 xlabel('SFF')
0067 ylabel('Effect (%)')

iv
A.1.3 M-file for safe failures as an assurance of functionality

```matlab
%Input data
format long
tau=8760;
MTTR=8;
muDD=1/MTTR;

Cd=0.28; %diagnostic coverage
lamD=1.0e-6 %total dangerous failure rate
lamDU=lamD*(1-Cd); %DU failure rate
lamDD=lamD*Cd; %DD failure rate

% Safe failure fraction from Cd (only DD failures) to 0.99
SFF=[Cd:0.01:0.99];

%Produces a matrix to store the steady state probabilities
l=1:length(SFF);
states=ones(length(SFF),3);

% Do the following 'i' times.
for i=1:length(SFF);

% Set SFF value 'i'
SFFi=SFF(i);

% input value for SFF to calculate safe failure rate
lamS=((lamDU+lamDD)*SFFi-lamDD)/(1-SFFi);

%store safe failure rate in matrix l
l(i)=lamS;

%Survival probability at time tau
R=exp(-lamS*tau)
%Probability of failure before time tau
F=1-R

%Mean unknown unavailability, taking into account the
%the probability of a safe failure previously in the
%same test interval
undetected = (R*tau/2)+(F*tau/4);

DU=1/undetected

A=[-DU 0 DU;
0 -muDD muDD;
lamDU lamDD -(lamDU+lamDD)];

%sum of Po(t)+....Pi(t)=1
A(:,3)=ones;

dP=zeros(1,3);
dP(1,3)=1;

%calculate steady state probability
Po=dP*inv(A);

CHECK=sum(Po)

%store steady state probabilities
Production_availability=states(1:length(SFF),3);
PFD_state0=states(1:length(SFF),1)+states(1:length(SFF),2)

DR1=(1:length(SFF));
for k=1:length(SFF)
    DR1(k)=(PFD_state0S(1)-PFD_state0S(k))/PFD_state0S(k);
end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

---

vi
plots the steady state probabilities vs SFF

plot(SFF,PFD_state0,'k')
xlabel('SFF')
ylabel('PFD')

plot(SFF,DR1,'k')
xlabel('SFF')
ylabel('Effect (%)')

plot(SFF,Production_availability,'k*')
xlabel('SFF')
ylabel('safe production')

vii
A.1.4 M-file for detailed model of HIPPS

```matlab
% Input data
format long
tau=8760;
undetected = tau/2;
MU = MTTR;
muDD = 1/MTTR;

Cd=0.28; % diagnostic coverage

LCP=0.10; % percentage LCP of DU failure rate
DOP=0.20; % percentage DOP of DU failure rate
FTC=0.35; % percentage FTC of DU failure rate
ELP=0.35; % percentage ELP of DU failure rate

% Safe failure fraction from Cd (only DD failures) to 0.99
SFF=[Cd:0.01:0.99];
lammD=[1e-6 5e-7 1e-7 5e-8 1e-8]; % total dangerous failure rate

for r=1:5
    lamD=lammD(r);
    lamDU=(1-Cd)*lamD; % DU failure rate
    lamDD=Cd*lamD; % DD failure rate
end

l=1:length(SFF);
states=ones(length(SFF),6);

% Do the following i times.
for i=1:length(SFF);
    SFFi=SFF(i);
    lamS=(((lamDU+lamDD)*SFFi)-lamDD)/(1-SFFi);
    l(i)=lamS;
end

R=exp(-lamS*tau); % probability of failure before time tau
F=1-R;

undetected2=(R*tau/2)+(F*tau/4);
DUS=1/undetected2;

A=[-DU 0 0 0 0 DU;
     0 -(DUS+lamS) 0 0 0 -(DUS+lamS);
     0 0 -(lamS+DUS) 0 lamS DUS;
     0 0 0 -(lamS+DUS) lamS DUS;
     0 0 0 0 -muDD muDD;
     lamDU*LCP lamDU*DOP lamDU*FTC lamDU*ELP lamDD -(lamDU+lamDD)];

% sum of Po(t)+....Pi(t)=1
A(:,6)=ones;

dP=zeros(1,6);
dP(1,6)=1;
Po=dP*inv(A);

CHECK=sum(Po);
```

viii
states(1,1:6)=Po;
end
availability=states(1:length(SFF),6);
PFD_state=states(1:length(SFF),1)+states(1:length(SFF),2)+states(1:length(SFF),3)+states(1:length(SFF),4)+states(1:length(SFF),5);

%stores the values in a permanent matrix for all MTTRs
PFD(r,:)=PFD_state;
%availability(r,:)=availability1;
end %ends/repeats for next MTTR value

%Calculates the percentage effect
DR1=((1:length(SFF)));
DR2=((1:length(SFF)));
DR3=((1:length(SFF)));
DR4=((1:length(SFF)));
DR5=((1:length(SFF)));
for k=1:length(SFF)
    DR1(k)=(PFD(1,1)-PFD(1,k))/PFD(1,1);
    DR2(k)=(PFD(2,1)-PFD(2,k))/PFD(2,1);
    DR3(k)=(PFD(3,1)-PFD(3,k))/PFD(3,1);
    DR4(k)=(PFD(4,1)-PFD(4,k))/PFD(4,1);
    DR5(k)=(PFD(5,1)-PFD(5,k))/PFD(5,1);
end

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%plots the probabilities
plot(SFF,DR1,'k.-',SFF,DR2,'k',SFF,DR3,'k:',SFF,DR4,'k--')
xlabel('SFF')
ylabel('Effect (%)')
legend('lambda_D=1e-6','lambda_D=5e-7','lambda_D=1e-7','lambda_D=5e-8')

%plot(SFF,states(1,:),'k.-',SFF,states(2,:),'k',SFF,states(3,:),'k:',SFF,states(4,:),'k--')
xlabel('SFF')
ylabel('PFD')
legend('lambda_D=1e-6','lambda_D=5e-7','lambda_D=1e-7','lambda_D=5e-8')
A.2 M-files for 1oo2 system

A.2.1 M-file for availability analysis

```matlab
% Failure rates from PDS table 11 for HIPPS components.
format long % gives out exact numbers

tau=8760; % test interval
undetected1oo1 =tau/2; % unavailability caused by DU common cause
undetected1oo2 =tau/3; % unavailability caused by individual DU failures

MTTR=8; % MTTR for all repair actions

% restoration rate for individual DU failures
muDU1oo2=1/(undetected1oo2);

% restoration rate for CC DU failures
muDU1oo1=1/(undetected1oo1);

muDD=1/MTTR; % restoration rate for DD failures
muDD2=muDD; % restoration of two DD
muSO=1/MTTR; % restoration rate for CC failures
muSO2=muSO; % restoration of two SO
muDDSO=muSO; % restoration of SO and DD

Cd=0.28; % diagnostic coverage of dangerous failures
C=0.2; % diagnostic coverage of safe failures

lamD=1e-6; % dangerous failure rate set constant

lambdaDD=lamD*Cd; % DD failure rate
lambdaDU=lamD-lambdaDD; % DU failure rate

% B=0.02; % Dangerous beta factor for a 1002 HIPPS system

SFF=[Cd:0.01:0.99]; % Safe failure fraction from Cd (only DD failures) to 0.99

safestate=ones(4,length(SFF)); % restoration rate for DD failures

PFD=ones(4,length(SFF)); % availability

availability=ones(4,length(SFF)); % availability

Bsafe=[0 0.02 0.1 0.2];

for beta=1:4
    B=Bsafe(beta)
    lamDU=(1-B)*lambdaDU; % DU failure rate with Beta factor
    lamDD=(1-B)*lambdaDD; % DD failure rate with Beta factor

    CCDD=B*lambdaDD; % common cause DD failure rate
    CCDU=B*lambdaDU; % common cause DU failure rate

    states=ones(length(SFF),11);

    for i=1:length(SFF)
        lamSOt=(lamD*SFF(i)-lambdaDD)/(1-SFF(i));
        lamSO=(1-B)*lamSOt;
        CCSO=B*lamSOt;

        safe(i)=lamSOt;

    end

    A=[-muDU1oo1 0 0 0 0 0 0 0 0 0 muDU1oo1;
        0 -muDU1oo2 0 0 0 0 0 0 0 0 muDU1oo2;
        0 0 -muDD 0 0 0 0 0 0 0 muDD;
        0 0 0 0 -muSO 0 0 0 0 0 muSO;
        0 0 0 0 0 -muDD 0 0 0 0 muDD;
        0 0 0 0 0 0 -muSO 0 0 0 0 muSO;
        0 0 0 0 0 0 0 -muDD 0 0 0 0 muDD;
        0 0 0 0 0 0 0 0 -muSO 0 0 0 0 muSO;
        0 0 0 0 0 0 0 0 0 -muDD 0 0 0 0 muDD;
        0 0 0 0 0 0 0 0 0 0 -muSO 0 0 0 0 muSO];

    % Column 11 is replaced with ones to obtain a unique solution by using Po+P1+...=1
    A(:,end)=ones(1,1);
end
```

x
0081 df=zeros(1,length(A)); %generates a 1x10 matrix with zeroes
0082
0083 for Pi=...Pi=1 the 8th zero is replaced with one.
0084 df(1:length(A))=1;
0085
0086 Pi=inv(A); %Solve the steady state equation
0087 %stores the probabilities for each value of SFF in the states matrix.
0088 states(i,1:11)=Pi;
0089 end
0090
0091 %plots the probabilities for each state against the SFF
0092 safestate_state6789=states(1:length(SFF),7)+states(1:length(SFF),8)+states(1:length(SFF),9)+states(1:length(SFF),10);
0093 PFD_state0123=states(1:length(SFF),1)+states(1:length(SFF),2)+states(1:length(SFF),3)+states(1:length(SFF),4);
0094 Production_availability=states(1:length(SFF),11)+states(1:length(SFF),5)+states(1:length(SFF),6);
0095 CHECK=safestate_state6789+PFD_state0123+Production_availability;
0096
0097 safestate(beta,:)=safestate_state6789;
0098 PFD(beta,:)=PFD_state0123;
0099 availability(beta,:)=Production_availability;
0100 end
0101
0102 %subplot(2,2,1)
0103 plot(SFF,PFD(1,:),'k--',SFF,PFD(2,:),'k',SFF,PFD(3,:),'k:',SFF,PFD(4,:),'k.-')
0104 xlabel('SFF')
0105 ylabel('PFD')
0106 legend('B=0','B=0.02','B=0.1','B=0.2')
0107 title('1oo2')
0108
0109 %subplot(2,2,2)
0110 plot(SFF,DR1,'k--',SFF,DR2,'k',SFF,DR3,'k:',SFF,DR4,'k.-')
0111 xlabel('SFF')
0112 ylabel('Diffrence')
0113
0114 subplot(2,2,3)
0115 plot(SFF,availability(1,:),'k',SFF,availability(2,:),'k--',SFF,availability(3,:),'k:',SFF,availability(4,:),'k.-')
0116 xlabel('SFF')
0117 ylabel('Availability')
A.2.2 M-file for safe failures as a means to reveal DU faults, with various dangerous failure rates

Failure rates from PDS table II for HIPPS components.

format long % gives out exact numbers

tau=8760; % test interval

undetected1oo1 = tau/2; % unavailability caused by DU common cause

undetected1oo2 = tau/3; % unavailability caused by individual DU failures

MTTR=8; % MTTR for all repair actions

restoration rate for individual DU failures

muDU1oo2 = 1/(undetected1oo2);

restoration rate for CC DU failures

muDU1oo1 = 1/(undetected1oo1);

MuDD = 1/MTTR; % restoration rate for DD failures

muDD2 = muDD; % restoration of two DD

muSO = 1/MTTR; % restoration rate for CC failures

muSO2 = muSO; % restoration of two SO

muDDSO = muSO; % restoration of SO and DD

Cd = 0.28; % coverage of dangerous failures

Cs = 0; % coverage of safe failures

B = 0.02; % Beta factor

SFF = [Cd:0.01:0.99]; % Safe failure fraction from Cd (only DD failures) to 0.99

% matrices to store steady state probabilities

PFD = ones(4, length(SFF));

availability = ones(4, length(SFF));

% dangerous failure rates

lammmD = [1e-6 5e-7 1e-7 5e-8 1e-8];

for r = 1:5
    lamD = lammmD(r); % apply rth dangerous failure rate
    lambdaDD = lamD * Cd; % DD failure rate
    lambdaDU = lamD - lambdaDD; % DU failure rate
    lamDU = (1 - B) * lambdaDU; % DU failure rate with Beta factor
    lamDD = (1 - B) * lambdaDD; % DD failure rate with Beta factor

    CCDD = B * lambdaDD; % Common cause DD failure rate
    CCDU = B * lambdaDU; % Common cause DU failure rate

    safe = ones(length(SFF), 1); % store safe failure rates

    states2 = ones(length(SFF), 7);

    for i = 1:length(SFF)
        SFFi = SFF(i); % Use ith SFF value from SFF matrix

        lamSOt = (lamD * SFFi - lambdaDD) / (1 - SFFi);
        lamSO = (1 - B) * lamSOt; % individual failure rate spurious operation
        CCSO = B * lamSOt;
        safe(i) = lamSOt;

        STdetect = lamSO; % ST Detection rate of DU failure
        STdetect1 = lamSOt;
        STdetectCC = CCSO;

    end

    USD = lamSOt; % DU failure rate with Beta factor

end

xii
Column 6 is replaced with ones to obtain a unique solution by using Po+P1+...=1.

\( Ax(:, \text{length}(Ax)) = \text{ones} \); \( dP = \text{zeros}(1, \text{length}(Ax)) \); % generates a 1x0 matrix with ones.

\( P_F = \text{pinv}(Ax); \) \( \% \) solves the steady state equation.

\( \% \) stores the probabilities for each value of SFF in the states2 matrix.

\( \% \) replaces ones with probabilities.

end

\% stores values in matrix

\% stores values in matrix

\% stores values in matrix

\% stores values in matrix

end

\% stores values in matrix

\% stores values in matrix

\% stores values in matrix

end

end

% Calculates the percentage effect

\( \text{DR1} = (\text{PFD}(1,1) - \text{PFD}(1,k))/\text{PFD}(1,1); \)

\( \text{DR2} = (\text{PFD}(2,1) - \text{PFD}(2,k))/\text{PFD}(2,1); \)

\( \text{DR3} = (\text{PFD}(3,1) - \text{PFD}(3,k))/\text{PFD}(3,1); \)

\( \text{DR4} = (\text{PFD}(4,1) - \text{PFD}(4,k))/\text{PFD}(4,1); \)

end

end

end

end

end

end

% plot(x, y)
% xlabel('x-axis label')
% ylabel('y-axis label')
% title('Plot Title')
% legend('Legend Entry 1', 'Legend Entry 2')
A.2.3 M-file for safe failures as a means to reveal DU faults, with various beta factors

0001 %Failure rates from PDS table 11 for HIPPS components.
0002
0003 format long %gives out exact numbers
0004 tau=8760; % test interval
0005 undetected1oo1 =tau/2; % unavailability caused by DU common cause
0006 undetected1oo2 =tau/3; % unavailability caused by individual DU failures
0007 MTTR=8; %MTTR for all repair actions
0008 % restoration rate for individual DU failures
0009 muDU1oo2=1/(undetected1oo2);
0010 % restoration rate for CC DU failures
0011 muDU1oo1=1/(undetected1oo1);
0012 muDD=1/MTTR; % restoration rate for DD failures
0013 muDD2=muDD; % restoration of two DD
0014 muSO=1/MTTR; % restoration rate for CC failures
0015 muSO2=muSO; % restoration of two SO
0016 muDDSO=muSO; % restoration of SO and DD
0017 Cd=0.28; % diagnostic coverage of dangerous failures
0018 Cs=0; % diagnostic coverage of safe failures
0019
0020 lamn=s-6; % dangerous failure rate set constant
0021 lambn=s-6; % DU failure rate
0022 lambn=s-6; % DU failure rate
0023
0024 SFF=[Cd:0.01:0.99]; % Safe failure fraction from Cd (only DD failures) to 0.99
0025
0026 % matrices to store steady state probabilities
0027 safestate=ones(4,length(SFF));
0028 PFD=ones(4,length(SFF));
0029 availability=ones(4,length(SFF));
0030
0031 % i is here the number of values of SFF. Do the following i times.
0032 for i=1:length(SFF)
0033 SFFi=SFF(i); % Set SFF value from SFF matrix
0034
0035 lamSOt=(lamD*SFFi-lambdaDD)/(1-SFFi);
0036 lamSO=(1-B)*lamSOt; % individual failure rate spurious operation
0037 CCSO=B*lamSOt;
0038 safe(i)=lamSOt;
0039 fi=1; % coverage of DU failures detected when a ST
0040 STdetect=lamSO; % ST Detection rate of DU failure
0041 STdetect1=lamSOt;
0042 STdetectCC=CCSO;
0043
0044 As=[-(muDU1oo1+STdetectCC+2*STdetect) 0 2*STdetect STdetectCC 0 0 muDU1oo1;
0045 0 -(muDU1oo2+2*STdetect+STdetectCC) 2*STdetect STdetectCC 0 0 muDU1oo2;
0046 0 0 -(muDD+STdetect1) STdetect1 muDD 0 0;
0047 0 lamDU 0 0 -(lamDU+muDU1oo1+lamDD+lamDDt) STdetect1 muDD;
0048 CCDU 0 CCDU 0 lamDD 0 -(CCDU+lamDD+lamDDt+lamDD)
0049];
0050 As(:,length(As))=ones; % Column 7 is replaced with ones to obtain a unique solution by using Po+P1+...=1
0051 dP=zeros(1,length(As)); % generates a 1x10 matrix with zeroes
0052 dP(1,length(As))=1; % for i=1:length(SFF),1;
0053
0054 D=As+B;
0055 f1(i); % coverage of DU failures detected when a ST
0056 SDetect=s-6; % ST Detection rate of DU failure
0057 SDetectt=s-6; % ST Detection rate of DU failure
0058 SDetecttt=s-6; % ST Detection rate of DU failure
0059
0060
0061
0062
0063
Pi_s = dP * inv(As); %Solves the steady state equation
stores the probabilities for each value of SFF in the states2 matrix.
states2(i,1:7) = Pi_s;
%replaces ones with probabilities
end

PFD_state0123 = states2(1:length(SFF), 1) + states2(1:length(SFF), 2) + states2(1:length(SFF), 3) + states2(1:length(SFF), 4);
Production_availability = states2(1:length(SFF), 6) + states2(1:length(SFF), 5) + states2(1:length(SFF), 7);
CHECK = PFD_state0123 + Production_availability;

PFD(beta,: ) = PFD_state0123;
availability(beta,:), Production_availability;
end

%Calculates the percentage effect
DR1 = (1:length(SFF));
DR2 = (1:length(SFF));
DR3 = (1:length(SFF));
DR4 = (1:length(SFF));

for k = 1:length(SFF)
DR1(k) = (PFD(1,1) - PFD(1,k)) / PFD(1,1);
DR2(k) = (PFD(2,1) - PFD(2,k)) / PFD(2,1);
DR3(k) = (PFD(3,1) - PFD(3,k)) / PFD(3,1);
DR4(k) = (PFD(4,1) - PFD(4,k)) / PFD(4,1);
end

plot(SFF, PFD(2,:),'k--', SFF, PFD(1,:),'k.-', SFF, PFD(3,:),'k:', SFF, PFD(4,:),'k--')
xlabel('SFF')
ylabel('PFD')
legend('B=0','B=0.02','B=0.1','B=0.2')