



NTNU – Trondheim
Norwegian University of
Science and Technology

RELIABILITY ASSESSMENT OF A SUBSEA HIPPS

Ellen Margrete Stølen

Subsea Technology

Submission date: February 2014

Supervisor: Marvin Rausand, IPK

Norwegian University of Science and Technology
Department of Production and Quality Engineering

Preface

This master thesis was written during the fall semester 2013 as a final contribution to my master's degree, at the Norwegian University of Science and Technology. The title of the thesis is *Reliability Assessment of a Subsea HIPPS* and is written with the guidance of my supervisor professor Marvin Rausand at the Department of Production and Quality Engineering.

The reader of this assumed to have some basic knowledge within the field of reliability and should be familiar with the textbook *System Reliability Theory: Models, Statistical Methods, and Applications* by Rausand and Høyland.

I would like to thank my supervisor, Marvin, for his help thought with this thesis. I will also thank Mary Ann Lundteigen for a helpful meeting and providing me with some additional documentation on HIPPS.

Trondheim, 04.02.2014

Ellen Margrete Stølen

Innhold

- Chapter 1 Introduction 4
 - 1.1 Background 4
 - 1.2 Objective 4
 - 1.4 Approach 5
 - 1.5 Structure of report 5
- Chapter 2 High Integrity Pressure Protection System..... 6
 - 2.1 HIPPS components..... 7
- Chapter 3 Reliability assessment of HIPPS 15 9
 - 3.1 IEC 61508 and 61511..... 9
 - 3.2 Requirements..... 10
 - 3.3 Function analysis..... 11
 - 3.4 Failure classification 11
 - 3.5 Proof testing of HIPPS 13
 - 3.6 Reliability block diagram 14
 - 3.6 Approximation formula..... 16
 - 3.7 Common Cause Failures 17
 - 3.8 PFD calculation with the IEC 6158 formula..... 19
- Chapter 4 Partial Stroke Testing 8 21
 - 4.1 Concept..... 21
 - 4.2 Coverage..... 22
- Chapter 5 Markov analysis 15..... 28
 - 5.1 Markov model 28
 - 5.2 Phased Markov 30
 - Repair strategy..... 33
 - All failures are repaired after testing..... 36
 - Only critical failures are repaired after testing..... 36

Imperfect repair model	37
5.3 HIPPS evaluation in GRIF workshop	37
SIL module	37
Markov Graphs module	39
Chapter 7 Available data	42
7.1 OREDA	43
7.2 PDS Data Handbook	43
Chapter 8 Discussions and concluding remarks	44
Concluding remarks	45
Referanser	46

Chapter 1 Introduction

1.1 Background

Safety instrumented systems are vital in the oil and gas industry. A SIS consists of input elements, a logic solver and final elements. A High Integrity Pressure Protection System is an example of such a system. HIPPS is installed to protect a platform from too high pressure by shutting off the source before exceeding the design pressure. Traditionally, subsea flowlines and infrastructure has been rated to contain the full shut-in pressure of the well. When installing a HIPPS on the manifold, the flowlines can be designed with a lower rating than the well shut-in pressure which gives a significant cost reduction. HIPPS will also allow for high pressure developments to be tied into an existing low pressure infrastructure.

The IEC 61508 and IEC 61511 are used in the oil and gas industry during all phases of the SIS lifecycle. As a measure of SIS reliability, both standards use safety integrity level. The standards lists several requirements for both hardware and software. Compliance to the SIL must be demonstrated by quantitative assessments including estimations to the SIS reliability. Several models for reliability assessments are demonstrated in IEC 61508.

A HIPPS is installed to perform a safety instrumented function (SIF) that is operated in low-demand mode and its availability must be quantified by using the average probability of failure on demand, PFD_{avg} .

1.2 Objective

The main objective of this thesis is to present and discuss analytical approaches that can be used to quantify the PFD_{avg} of a specific HIPPS implementation, and to study how the various input parameters influence the value of the PFD_{avg} .

1. Based on a literature survey, the candidate shall identify, compare, and discuss analytical approaches relevant to HIPPS reliability assessment
2. Describe and discuss relevant aspects of partial stroke testing (PST), with focus on factors that affect the coverage of the PST
3. Establish reliability models of a subsea HIPPS based on reliability block diagrams and use approximation formulas to determine the average PFD
4. Discuss the availability of data for the required input parameters to the model in point 3 and set up a reliability data dossier

5. Establish a reliability model for the HIPPS based on a phased Markov model and explain in detail the various elements in this model
6. Choose some relevant architectures for a HIPPS and carry out reliability analyses based on the phased Markov model in point 5
7. Identify and discuss challenges related to HIPPS reliability assessment, for which further research is needed

1.4 Approach

A great deal of work has gone into the gathering of information for this thesis. The main references in this thesis is IEC 61508 and *System Reliability Theory: Models, Statistical Methods, and Applications* by Rausand and Høyland [2004]. Other sources are found in search engines like OnePetro and ScienceDirect. Computer simulations are done in GRIF workshop, a program developed by Total.

1.5 Structure of report

A description of HIPPS is given in Chapter 2. IEC 61508 and IEC 61511 are introduced in Chapter 3. Different approaches to reliability assessment of HIPPS is described based on some of the models in the standards and models presented in the book *System Reliability Theory* by Rausand and Høyland [2004]. Chapter 4 address the concept of partial stroke testing and how to decide the coverage of such a test. Markov modeling is described in Chapter 5. A phased Markov model is described with the modelling of different repair strategies for the system. The repair strategies are simulated in GRIF workshop and presented. Chapter 6 is an overview of available data sources for quantification of reliability analysis. A discussion of uncertainties is presented in Chapter 7 followed by the conclusion in Chapter 8

Chapter 2 High Integrity Pressure Protection System

A safety instrumented system (SIS) is defined by IEC 61511 as an instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor(s), logic solver(s), and final elements. A High Pressure Protection System (HIPPS) is such a system and it has been used in the oil and gas industry for a long time. A basic HIPPS is illustrated in figure 1. Redundant 2oo3 voted pressure transmitters detects high pressure and gives a signal to the logic solver. The 2oo3 voting offers both a level of redundancy and fault tolerance. The logic solver then signals the solenoid valves to de-energize, causing the safety valves to close and act as barriers against the high pressure.

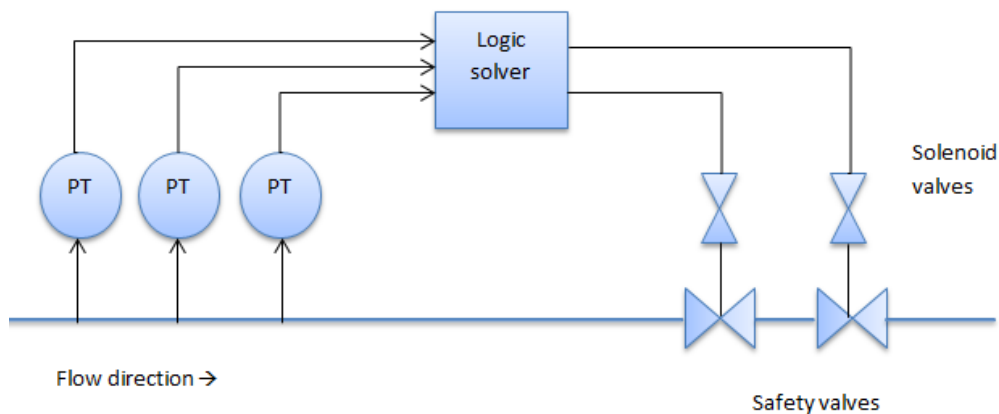


Figure 1 HIPPS schematic

HIPPS has traditionally been installed topside to protect lowrated process equipment from high pressures. The production pipelines then need to be rated for full shut-in pressure. For high pressure and deep sea reservoirs, this will cause high expenses and production from such a reservoir might be unprofitable. Installing a subsea HIPPS in the manifold will allow a lower pressure rating of the pipeline. The wall thickness may be reduced with as much as 30% [1] resulting in high economic benefits. As a rule of thumb it has been recommended to use subsea HIPPS for well pressures higher than 5000 psi and distances longer than 20 km [1] [2].

For reservoirs developed in waters too deep for a fixed platform, a floating vessel is used. These vessels move with the motion of the sea which requires the riser to be flexible. A flexible riser cannot be made to withstand high pressures. By installing a subsea HIPPS the

riser can have a lower pressure rating and production in deep water and high pressure reservoirs is possible.

New developments are often made in an area where production has started. A tie-back to the existing infrastructure is used in this case. The existing pipeline may have a lower pressure rating than the shut-in pressure in the new development. By installing a HIPPS, the tie-back is still possible and new material and laying operation costs are saved [1].

Statoil applied HIPPS to the over pressure protection system on the Kristin field. The shut-in wellhead pressure was 740 bar, while the flowlines and risers were designed for 330 bar. The HIPPS was therefore set to trip when detecting pressure of 280 bar or more [3]. Kristin was the first Statoil field to apply subsea HIPPS, and is therefore used as a reference when developing new fields.

2.1 HIPPS components

The pressure transmitters are installed to monitor the upstream pressure. The voting of the transmitters needs to be evaluated to meet the required SIL level. Kristin used four transmitters in a 2oo4 voting. This will allow the production to continue with one failed transmitter giving the voting 1oo3. If another transmitter fail, the HIPPS valves will close and the production is stopped. Locating two of the sensors upstream the valves and two between assures effective testing and reporting of valves. The sensors should be placed with a maximum distance from each other to minimize common cause failures [3], as shown in Figure 3.

The control unit receives signals from the pressure transmitters and compares them with pre-defined values. If the pressure inputs are higher than these values, the controller switches off the current to the solenoid and the barrier valve closes. At Kristin, the logic was delivered from Yokogawa and was certified for a SIL 3. It was placed on the Subsea Control Module (SCM) on the manifold [4]. Because of the placement, the logic could not be changed after installation. Status of the HIPPS and features for testing can be monitored topside through the subsea control system. Figure 2 illustrates the logic at Kristin. The analog inputs from the pressure transmitters are converted by AL-917 to logic pulse outputs which are sent to the voting logic. Logic from the voter is then converted by the Fail-safe output module (FO-526) to digital outputs which then signals Directional Control Valve (DCV).

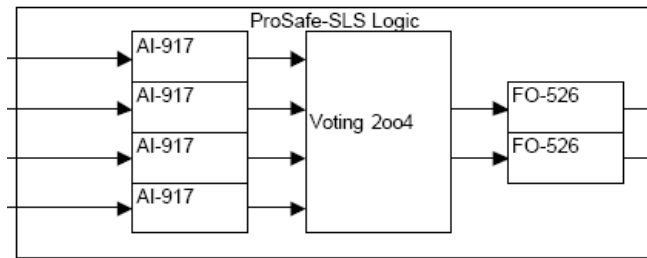


Figure 2 HIPPS logic at Kristin [3]

Barrier valves are the final elements of the HIPPS. They close and act as barriers to protect against over-pressure. The HIPPS valves have a fail-safe design, meaning that any loss of electric or hydraulic power will cause the valves to close. Two valves are installed in series with a 1oo2 voting to meet the requirements of IEC 61508. Valve closing time is important and needs to be decided to prevent pressure built up in the low rated zone.

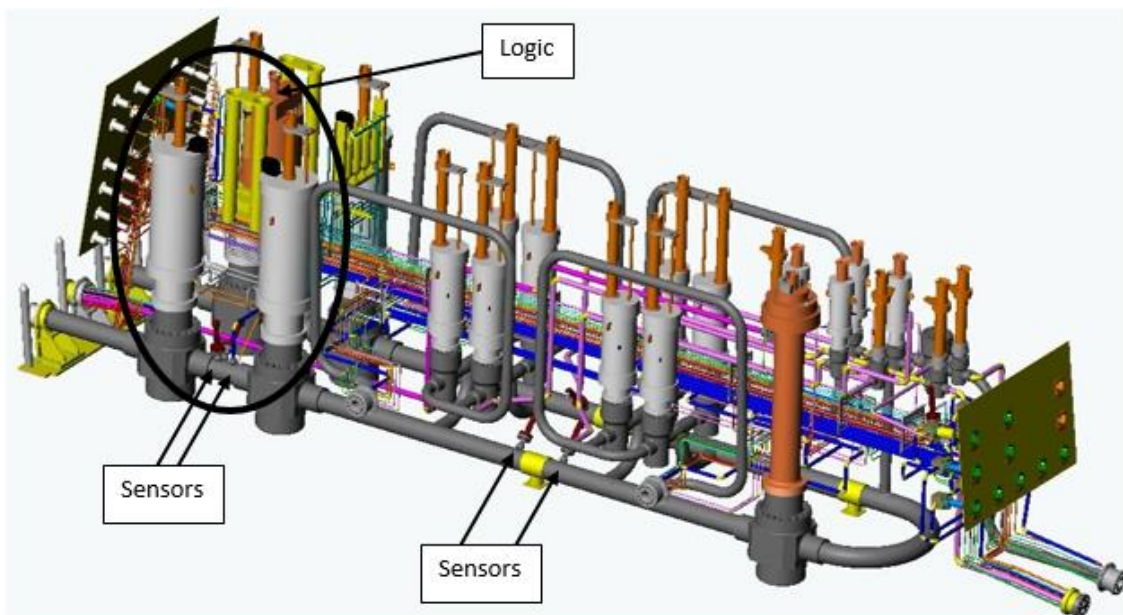


Figure 3 HIPPS placed on manifold at Kristin [3]

Figure 3 shows the placement of the different channels of the subsea HIPPS at Kristin.

Chapter 3 Reliability assessment of HIPPS 15

3.1 IEC 61508 and 61511

IEC 61508 is a standard written by the International Electrotechnical Commission and is titled: *Functional safety of electrical/electronic/programmable electronic safety-related systems*. The standard gives requirements for design, installation operation and maintenance of a safety instrumented system. The overall safety lifecycle model is the framework for the standard, and it is organized into seven parts.

Part 1: General requirements

Part 2: Requirements for E/E/PE safety-related systems

Part 3: Software requirements

Part 4: Definitions and abbreviations

Part 5: Examples of methods for the determination of safety integrity levels

Part 6: Guidelines to the application of IEC 61508-2 and IEC 61508-3

Part 7: Overview of measures and techniques

Parts 1-3 contain standard requirements which should be followed by the industry, while parts 4-7 provide guidelines and examples on how to apply the standard. IEC 61508 concerns all E/E/PE safety-related systems, and is the basis for several standards written for specific industries such as the oil and gas industry.

IEC 61511 is written for the process sector and is based on IEC 61508. The requirements made in IEC 61508 is followed, but modified to suit practical situations, concepts and terms in the process industry. The standard has 3 parts

Part 1: Framework, definitions, system, hardware and software requirements

Part 2: Guidelines in the application of IEC 61511-1

Part 3: Guidance for the determination of the required safety integrity levels

The concept of safety integrity is very important in IEC 61508 and is defined as the probability of an E/E/PE safety-related system satisfactory performing the specified safety

functions under all the stated conditions within a stated period. It is classified into four Safety Integrity Levels (SIL), where level 4 has the highest level of integrity and level 1 has the lowest. The SIL is determined by the average probability of failure on demand (PFD) for safety functions in a low demand mode of operation, and by the probability of dangerous failure per hour (PFH) for safety functions in high demand/continuous mode. Low demand mode means that the SIS demand is less than once per year, while high demand/continuous mode is when the demand is greater than once per year.

Safety Integrity Level (SIL)	Low Demand Mode (PFD)	High demand/continuous mode (PFH)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

Table 1

The Norwegian Oil Association had developed a guideline called OLF 070 with a purpose to adapt and simplify the applications of IEC 61508 and IEC 61511 for use in the Norwegian petroleum industry.

API RP 170 *Recommended Practice for Subsea High Integrity Pressure Protection System (HIPPS)* specifies the requirements for SIS made in IEC 61508 and IEC 61511 to address the specific needs for subsea production. It covers requirements for the HIPPS sensors, logic shutdown valves and ancillary devices including testing, communications and monitoring systems.

3.2 Requirements

Adequate response rate to protect against an over-pressure hazard: The response time is the time it takes for the HIPPS to shut in the well after a high pressure is detected [2]. A “fast acting” system has a reaction time of less than two seconds, while the response time of a “slow acting” system may be greater than 10 seconds. The system response time is dependent on the type of production fluid, pressure ratings and length of flowline and the trip pressure of the HIPPS [5].

Failsafe design principle: The system should go into a safe state upon any failure that impairs its safety state [6]. The HIPPS valve will close immediately at any loss of electrical or hydraulic power.

High reliability of safety function to comply with appropriate SIL requirements: The SIL may be pre-selected or calculated based on risk thresholds, initiating frequencies, and other layers

of protection to determine the required SIL of the HIPPS [7]. Typically, a HIPPS is required to meet SIL3.

Testable: The HIPPS must be periodically function tested to ensure that it meets the safety integrity requirements. Short test intervals will improve the systems PFD, but is very costly and therefore typically every 12 months. A test scheme needs to be made to meet the SIL 3 requirement.

3.3 Function analysis

In order to understand potential failures of a system it is important to have a good understanding of the various functions of each functional block. The various functions of a HIPPS are shown in the function tree in Figure 4. The function tree is constructed by asking how the HIPPS function is accomplished.

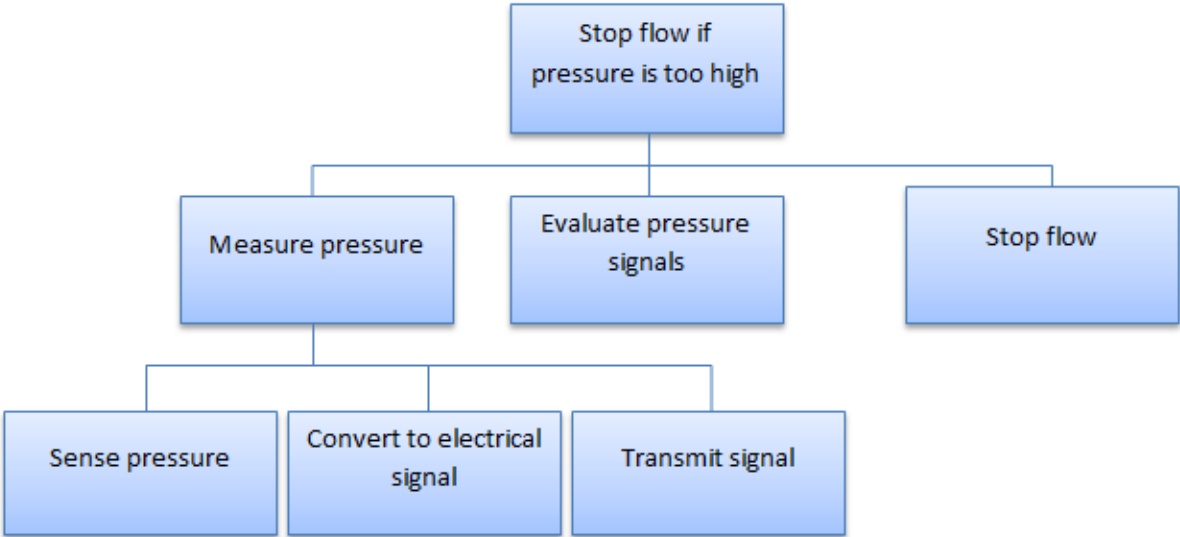


Figure 4 Function tree for a HIPPS

For this system function to be accomplished the pressure has to be measured, pressure must be evaluated and flow must be stopped. In order to do this this the pressure must be sensed and converted to a electrical signal. The signal must also be transmitted for evaluation.

3.4 Failure classification

IEC 61508 defines failure as *termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required*. It categorize failures according to cause as random hardware failure and systematic failure. The standard defines these failure mode classifications as:

Random hardware failure – failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware. Split into ageing failures and stress related failures.

Systematic failure – failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors. It is further split into design failures and interaction failures.

Further, failure mode classification is also made in IEC 61508 as illustrated in Figure 5.

Dangerous (D) is when the SIS is not able to perform its safety related function upon demand. This may be split into Dangerous Undetected (DU) and Dangerous Detected (DD) failures. DU failures are revealed only by proof testing or when a demand occurs, while DD failures are detected immediately after they occur or by diagnostic testing and actions to repair may be taken. Safe failure (S) is if the SIS has a failure which is not considered dangerous to the system function, like a spurious trip. They are also divided into Safe Undetected (SU) and Safe Detected (SD).

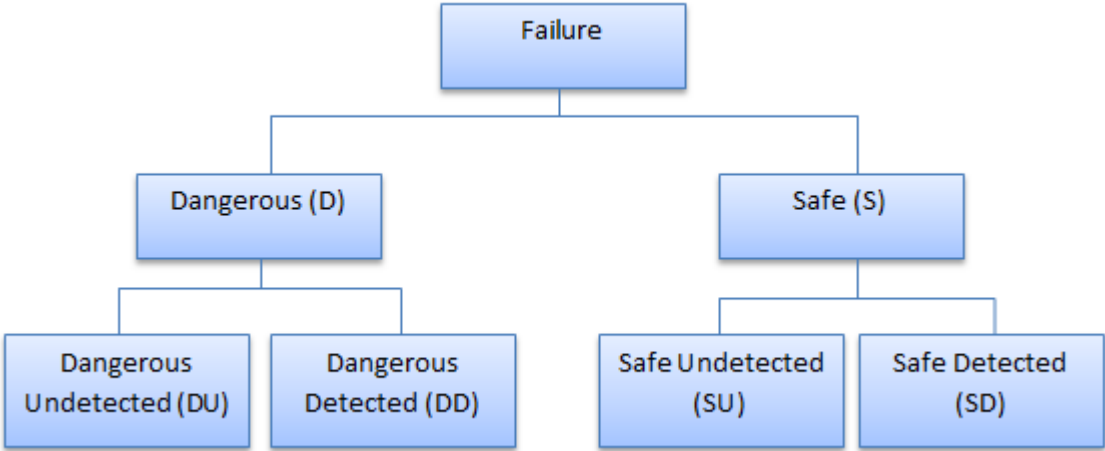


Figure 5 failure mode classification

The main failure modes for the HIPPS are:

Failure to close (FTC): Considered the most severe type of failure. This can be caused by a broken spring, blockage in the return line for the hydraulic fluid, too high friction between the stem and the stem seal, too high friction between the gate and the seats or by sand, debris or hydrates in the valve cavity [8]. This failure mode is only detected upon demand or by proof testing of the valve and is therefore a DU-failure.

Leakage in closed position (LCP) is often caused by corrosion and/or erosion on the gate or the seal, but may also be caused by misalignment between the gate and the seal [8]. This can only be detected by closing the valve completely, causing a stop in production.

Spurious trip (ST) is when the valve closes without a real demand from the logic unit. This can be caused by a failure in the hydraulic system or a leakage in the supply line from the control system [8]. This is considered a safe detected failure.

Fail to open (FTO) only occurs after a test or a demand and it is detected immediately by the maintenance team.. This is considered a safe failure and can be caused by leakage in control line, too high friction between the gate and the stem seats, too high friction between the stem seal and the stem or hydrates in the valve cavity [8].

3.5 Proof testing of HIPPS

In order to maintain the required SIL of a system, it is important to perform tests that verify the functionality of the system. If testing is not performed, a fault may not be discovered until a demand occur and the unsafe event the system was designed to prevent will occur. IEC 61508 stresses the importance of testing both during the design and operational phase. Testing during operation is especially important in the beginning of new projects in order get more knowledge and documentation of systems.

Proof testing is defined by IEC 61508 *as periodic test performed to detect hidden failures in a safety-related system so that is necessary, a repair can restore to an “as new” condition or as close as practical to this condition.* Because proof testing often requires production shutdown different online test measures may be taken. Diagnostic testing may be performed by the logic of the system. The logic sends frequent signals to actuators and detectors and compare their response with predefined values.

Partial stroke testing is also a form of online testing. Partial closure is not performed as frequently as diagnostic testing and is usually performed manually. It is therefore not considered a diagnostic test. This type of testing will only reveal if the valve is stuck, leaving it somewhere between a full function test and diagnostic testing. Partial stroke testing is described in detail in Chapter 4.

The test strategy at Kristin involves a full function test once a year and partial valve testing and sensor verification six times a year [3]. Function test is initiated with flow in the system

by isolating two of the pressure transmitters. The logic will initiate shutdown of valves when it stops receiving from two of the transmitters. The two remaining sensors monitor the pressure. Pressure and valve position is monitored and logged in the control room to verify that the valves are closing as intended.

The next step is to verify that the sensors trip the logic at the set pressure. This is done by relieving pressure in manifold and between the HIPPS valves before resetting the system. HIPPS valve opens after system reset and the pressure in the manifold is increased to more than the trip pressure by injection. All signals should trip and close the open valve.

Finally the valves are tested for leakage. This is done by lowering the pressure between the valves. Once the pressure is stable, the pressure is increased and the flow line pressure is monitored. Decrease in pressure indicate a leakage in the upstream valve, while increase indicate leakage in the downstream valve [4].

The partial valve operation is performed by sending a signal from the control room to the HIPPS. HIPPS test logic initiates valve closure and valves start to close. After a defined time, test logic initiates valve open and valves go back to fully open. The HIPPS test logic reports valves position/time to control room where the operator verifies that the valves are not stuck in open position [3].

Sensor verification is done to control that all HIPPS sensors measure the same value. This is done by changing the choke position to increase/decrease pressure and verifying that all sensors measure the same pressure variation.

3.6 Reliability block diagram

A Reliability Block Diagram (RBD) is a graphical illustration of a system which shows the logical connections of functioning item that are needed to fulfill a specific function. Each component in the system is represented by a block. The way these blocks are connected describes the functionality of the system. An RBD for a simple HIPPS is shown in Figure 6 with a 2oo3 voting of the PTs, one logic solver and a 1oo2 voting of the safety valves.

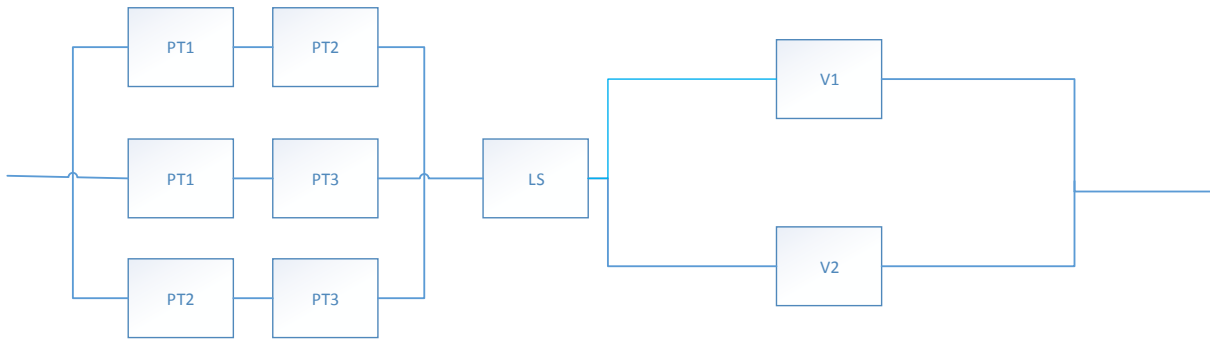


Figure 6 Reliability block diagram

The system is functioning if there is a connection between the starting point and the end point.

The standard IEC 61078 *Analysis techniques for dependability – reliability block diagram and Boolean methods* defines the system reliability as:

$$R_S(t) = \exp\left(-\int_0^t \lambda(u) du\right)$$

Where $\lambda(u)$ is the system failure rate at time $t=u$

For a system with a series structure, all components need to function for the system to function. The system reliability is found by multiplying the reliabilities of all the blocks in the system.

$$R_S = \prod_{i=1}^n R_i$$

If the system has a parallel structure, the system is functioning if at least one of the components are functioning and the system reliability is found by

$$R_S = 1 - \prod_{i=1}^n (1 - R_i)$$

For a system with a *koon* structure with identical components, the general formula is

$$R_S = \sum_{r=0}^{n-k} \binom{n}{r} \cdot R^{n-r} \cdot (1 - R)^r$$

For the RBD in Figure 6 we consider the pressure transmitters, the logic solver and the valves as three subsystems in series. This results in a system reliability of

$$R_S = (3 \cdot R_{PT}^2 - 2 \cdot R_{PT}^3) \cdot R_{LS} \cdot (2 \cdot R_V - R_V^2)$$

3.6 Approximation formula

To assess the SIL of the HIPPS the PFD may be decided on the basis of approximation formulas. The RBD is divided into sub-systems and the PFD for each sub-system is calculated. There are some limitations when using approximation formulas based on the assumptions that need to be taken. The assumptions are listed:

- All failure rates are constant with respect to time
- Components are identical with the same failure rate
- PFD is calculated as average value
- Component is considered “as good as new” after a repair or a test
- The contribution of unavailability due to repair and testing of component is not included
- The system is brought to a safe state upon detection of a dangerous failure
- The PFD of the system is obtained by summing the sub-systems PFD because the values are assumed to be small, rather than more accurate formulas
- Only function test is performed
- All hidden failures are revealed by function testing

Based on the general approximation formula for a k -out-of- n ($koon$) system derived in Rausand and Høyland [2004], the PFD for each sub-system is calculated.

$$PFD = \frac{1}{\tau} \int_0^{\tau} \binom{n}{n-k+1} \cdot (\lambda_{DU}t)^{n-k+1} dt = \binom{n}{n-k+1} \frac{(\lambda_{DU}\tau)^{n-k+1}}{n-k+2}$$

Some of the most common approximation formulas are shown in Table 1.

K\N	1	2	3	4
1	$\frac{\lambda_{DU}\tau}{2}$	$\frac{(\lambda_{DU}\tau)^2}{3}$	$\frac{(\lambda_{DU}\tau)^3}{4}$	$\frac{(\lambda_{DU}\tau)^4}{5}$
2	-	$\lambda_{DU}\tau$	$(\lambda_{DU}\tau)^2$	$(\lambda_{DU}\tau)^3$
3	-	-	$\frac{3\lambda_{DU}\tau}{2}$	$2(\lambda_{DU}\tau)^2$
4	-	-	-	$2\lambda_{DU}\tau$

Table 1 Approximation formulas for some of the most common koon systems

The HIPPS has three sub-systems, the 2oo3 pressure transmitters, the logic solver and the 1oo2 safety valves.

$$PFD_{PT} = (\lambda_{DU,PT}\tau)^2$$

$$PFD_{LS} = \frac{\lambda_{DU,LS}\tau}{2}$$

$$PFD_V = \frac{(\lambda_{DU,V}\tau)^2}{3}$$

The failure rates are found in Table 2. An appropriate test interval for the system is one year, 8760 hours. The PFD for the system is then $5,93 \cdot 10^{-4}$.

.Component	Failure rates (per 10 ⁶ hour)				β
	λ_D	λ_S	λ_{DU}	λ_{SU}	
Pressure transmitter	1,5	0,5	0,5	0,4	6%
Trip amplifier/Analog input	0,04	0,4	0,04	0,4	3%
Logic Solver	0,03	0,3	0,03	0,3	
Digital output	0,04	0,4	0,04	0,4	
HIPPS valve	2,7	3,3	1,9	3,0	5%

Table 2 Reliability data adapted from the PDS handbook [9]

3.7 Common Cause Failures

Because of the high level of redundancy, the system may be influenced by Common Cause Failures (CCF). A CCF is defined by NUREG/CR 6268 as a dependent failure in which two or more component fault state exists simultaneously, or within a short time interval, and are a direct result of a shared cause [8]. Such a failure may be caused by design or material deficiency, error during installation or maintenance, or by environmental conditions. The CCF are included as a separate block to the redundant sub-systems in the RBD as shown in Figure 7.

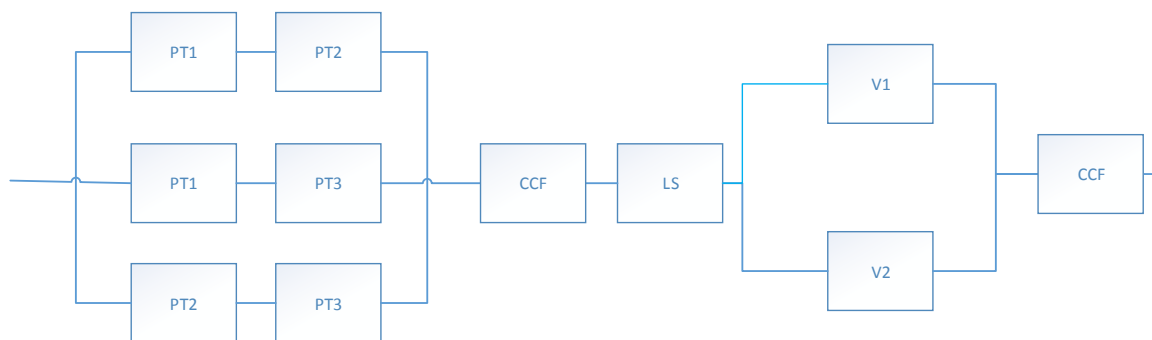


Figure 7 RBD including CCF

IEC 61508 recommends the beta factor model. The beta factor, β , is the probability of a failure being caused by a CCF. The beta factor is decided based on a set of 40 specific questions which are answered on a scale of 0, 1, 2, 5 or 10. The scores are compared to predefined values in IEC 61508 and an estimated beta factor is defined. The questions address:

1. Degree of physical separation/segregation
2. Diversity/redundancy
3. Complexity/maturity of design/experience
4. Use of assessment/analyses and feedback data
5. Procedures/human interface
6. Competence/training/safety culture
7. Environmental control
8. Environmental testing

The total failure rate is divided into individual failure rate and common cause failure rate. The beta factor is the probability that a failure is a CCF, and the remaining probability ($1 - \beta$) involve only the remaining failures. The individual and CCF failure rates are therefore:

$$\lambda = \lambda_I + \lambda_C$$

$$\lambda_C = \beta\lambda$$

$$\lambda_I = (1 - \beta)\lambda$$

Hence:

$$\beta = \frac{\lambda_C}{\lambda_I + \lambda_C} = \frac{\lambda_C}{\lambda}$$

The beta factor model suggested in IEC 61508 does not consider the voting of a system. It only accounts for the probability that all components fail upon a CCF, which may not always be the case. SINTEF has developed an extended version of the beta factor model called the PDS method. This method introduces a modification factor, C_{koon} , that distinguishes between the voting of the system. Some values of C_{koon} is shown in Table 3

k/n	2	3	4	5	6
1	1	0.5	0.3	0.2	0.15
2	-	2	1.1	0.8	0.6
3	-	-	2.8	1.6	1.2
4	-	-	-	3.6	1.9
5	-	-	-	-	4.5

Table 3 PDS model C factor [9]

The total average PFD for the system is

$$\begin{aligned}
 PFD_{avg} &= PFD_{PT,2003}^{ind} + PFD_{PT,2003}^{CCF} + PFD_{LS} + PFD_{V,1002}^{ind} + PFD_{V,1002}^{CCF} \\
 &= ((1 - \beta_{PT})\lambda_{DU,PT} \cdot \tau)^2 + \frac{C_{2003}\beta_{PT}\lambda_{DU,PT} \cdot \tau}{2} + \frac{\lambda_{DU,LS} \cdot \tau}{2} + \frac{((1 - \beta_V)\lambda_{DU,V} \cdot \tau)^2}{3} \\
 &\quad + \frac{\beta_V\lambda_{DU,V} \cdot \tau}{2}
 \end{aligned}$$

$$PFD = 1,261 \cdot 10^{-3}$$

3.8 PFD calculation with the IEC 6158 formula

IEC 61508-6 provides some simplified formulas for determining the PFD of a SIS. Formulas for systems of 1oo1, 1oo2, 2oo2, 1oo3 and 2oo3 voting are described, but no general formula is provided. The assumptions are similar to the once made for the approximation formulas and are listed below.

Assumptions:

- All failure rates are assumed constant
- Components are statistically independent
- Function test coverage is 100%
- PFD is an average value
- All components in an architecture have the same failure rate and diagnostic coverage
- Overall failure rate of a channel subsystem is the sum of dangerous undetected failures and safe failures for the channel, which is considered to be equal

- The function test is at least one order of magnitude greater than the mean repair time (MRT)
- For each subsystem there is a function test interval and MRT
- Test times are neglected
- Expected interval of demand is greater than the test interval
- $\lambda_{DU} \cdot \tau$ is small enough to allow $e^{-\lambda_{DU} \cdot \tau} \approx 1 - \lambda_{DU} \cdot \tau$

Channel equivalent mean downtime (MTTR – mean time to restoration)

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{\tau}{2} + MRT \right) + \frac{\lambda_{DU}}{\lambda_D} \cdot MTTR$$

System equivalent downtime

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{\tau}{3} + MRT \right) + \frac{\lambda_{DU}}{\lambda_D} \cdot MTTR$$

PFD for a single system

$$PFD = (\lambda_{DU} + \lambda_{DD})t_{CE} = \lambda_D \cdot t_{CE} = \lambda_{DU} \left(\frac{\tau}{2} + MRT \right) + \lambda_{DD} \cdot MTTR$$

For a 1oo2 system

$$PFD_{1oo2} = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} \left(\frac{\tau}{2} + MRT \right)$$

The RBD for a 2oo3 system can be drawn as three 1oo2 architectures in series. The system will fail if one of the 1oo2 structures fail. The PFD for 2oo3 is therefore three times the PFD of a 1oo2 system

$$PFD_{2oo3} = 6((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} \left(\frac{\tau}{2} + MRT \right)$$

Chapter 4 Partial Stroke Testing 8

4.1 Concept

The most common and dangerous failure mode of a shutdown valve is failure to close. The only way to detect such a failure is by moving the valve. A Partial Stroke Test (PST) will reveal failure of this sort without interfering with the production. By introducing partial stroke testing the function test interval can be longer and the downtime is reduced.

One basic way of implementing PST is by integrating it in the SIS. All hardware and software necessary is implemented in the logic solver of the SIS. A signal is manually given to the logic solver from a control panel controlled by an operator. The logic solver then deactivates the outputs for a short period of time. This causes the solenoid to depressurize the safety valve and the valve will start closing into a fail-safe position [10]. When the valve starts to move the logic solvers outputs are re-energized and the valve returns to fully open position. The results are then recorded and monitored by the operator. In such a system all components from the logic output card to the safety valve are tested.

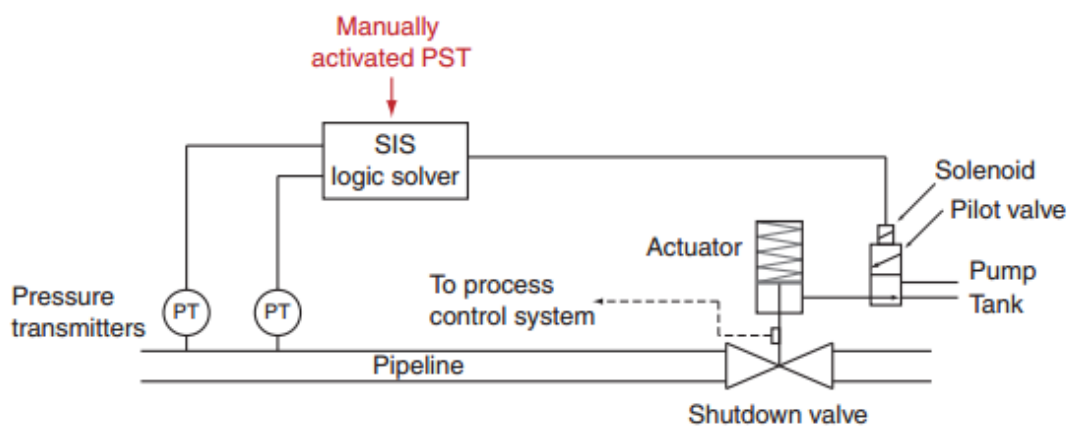


Figure 8 PST integrated in SIS [11]

Another way of implementing a PST is by a separate package supplied by the vendor. The test sequence is the same as the above, but hardware and software is implemented in a separate system. This system may automatically perform the test at set intervals, but can also be performed manually. In this way the operator can control the test time and results fault like

delay reaction and delayed movement are revealed. This gives a more detailed analysis of the safety valve, but the other components are not tested like in the integrated PST test.

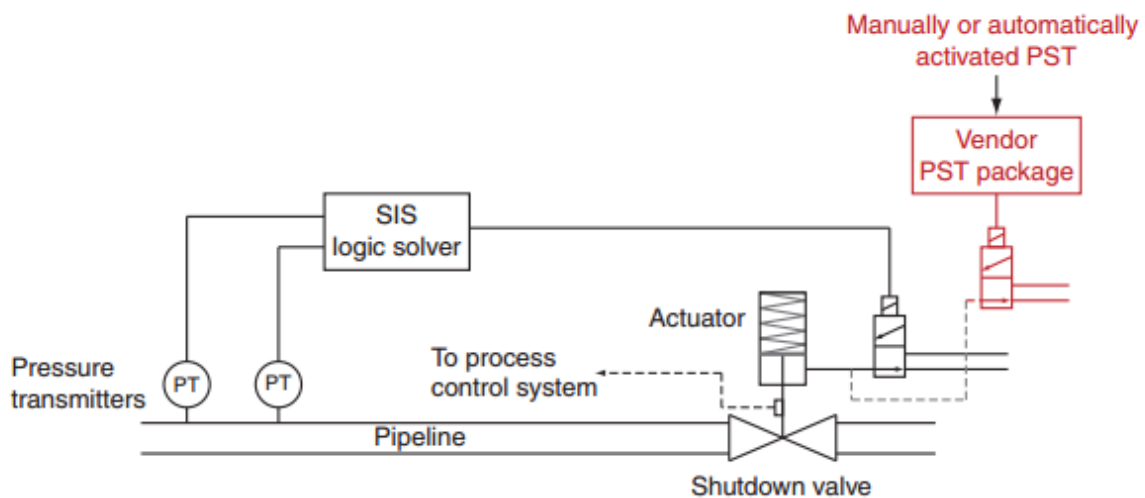


Figure 9 Separate vendor package to perform PST [11]

Implementing PST as a supplement to the function test can be done for two reasons; either to improve the systems PDF or to extend the time interval between function testing. By introducing PST without changing the test interval, the probability of failure on demand is reduced resulting in a higher SIL.. The additional PST will also reduce the probability of sticking seals due to a more frequent operation of the valve. There are some additional advantages when PST is implemented to extend the function test interval. Because the valve is less frequently brought to a closed position, the wear of the valve seat area is reduced and operational disturbance is reduced [10].

There are still some disadvantages when implementing PST. When adding software and hardware to the SIS, the system becomes more complex. The probability of spurious trips increase since the valve may continue to fail safe position instead of returning to open position after a test. An increase in valve wear may also occur due to more frequent operation.

4.2 Coverage

Testing of SIS functions are done by diagnostic self-testing and function testing. Diagnostic self-testing is when the logic solver is programmed to send signals to detectors and actuating systems to compare the response with predefined values in the logic solver [8]. Diagnostic self-testing only reveals some of the failure modes, DD failures. It is therefore necessary to

perform a function test of the system. The function test reveals DU failures and verifies that the system is still able to perform the required functions. Partial stroke testing can partially replace the need for a full function test and covers failure modes not discovered by the diagnostic self-test. Figure 10 illustrates how the dangerous failure rate can be divided into three failure rates depending on the different detection methods.

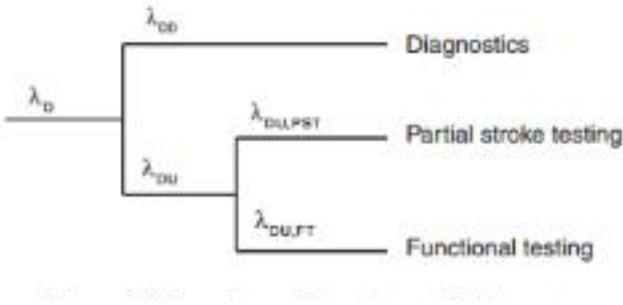


Figure 10 Relationship between failure rates [10]

Because the PST falls between the two test methods, it is necessary to distinguish between PST coverage and diagnostic coverage. IEC 61508 defines diagnostic coverage as *the fraction of dangerous failures that are detected by diagnostic among all failures*.

$$\theta_{DC} = \frac{\lambda_{DD}}{\lambda_D}$$

Since the PST reveal some of the failures not covered by diagnostics testing, the PST coverage is defined as the fraction of dangerous undetected failures revealed by PST among all dangerous undetected failures.

$$\theta_{PST} = \frac{\lambda_{DU,PST}}{\lambda_{DU}}$$

It can be discussed if the failures detected by PST should be classified as dangerous undetected or dangerous detected failures. This does not have any effect on the PFD calculations.

The PST coverage may from its definition be expressed as:

$$\theta_{PST} = Pr(\text{Detected DU failure} | \text{DU failure is present})$$

The value of the coverage should be based on plant specific conditions, such as valve type, functional requirements, and operational and environmental conditions [11]. The average PFD for the shutdown valve is then the sum of average PFD for function testing, diagnostic testing and the PST. Because diagnostics are usually performed at very short intervals, its contribution to the PFD can be neglected. It is also assumed that the component is as good as new after a test or repair is performed. The PFD is therefore expressed by

$$PFD \approx PFD_{FT} + PFD_{PST} \approx (1 - \theta_{PST}) \cdot \frac{\lambda_{DU}\tau_{FT}}{2} + \theta_{PST} \frac{\lambda_{DU}\tau_{PST}}{2}$$

$$PFD_{without\ PST} = 8.322 \cdot 10^{-3}$$

$$PFD_{with\ PST} = 5.825 \cdot 10^{-3}$$

Figure 11 is a graphical illustration of the contribution of PST for a HIPPS valve. The test interval for PST is every other month, while the full function test is performed once a year. The PST coverage is set to be 60% of all DU failures. The contributions from FT and PST are the blue and red graphs. Together they form the green graph representing the equation above. The purple graph shows the PFD without considering PST.

The PFD is improved when PST is implemented because a portion of the undetected failures are detected and repaired within a shorter test interval than by function testing.

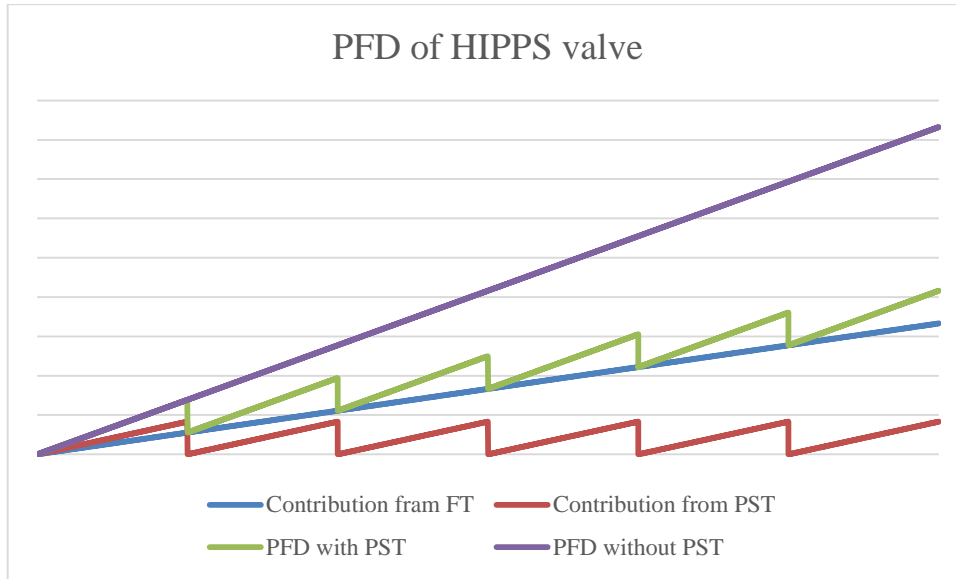


Figure 11 PFD of a HIPPS valve with and without PST

A new approach on how to determine the PST coverage is suggested in an article written by Lundteigen and Rausand [2008] that suggest how all factors can be taken into account. It is assumed that PST coverage is a property of individual SIS components rather than a group of components and should therefore be written

$$\theta_{PST} = \frac{\Pr(\text{Detected DU failure by PST} \cap \text{DU failure is present})}{\Pr(\text{DU failure is present})}$$

The different failure modes needs to be considered, such examples are failure to close, leakage in closed position, delayed operation and so on. The different failure modes are noted FM_1, FM_2, \dots, FM_i and it is assumed that only one failure mode is present at the time. The equation can then be written as

$$\theta_{PST} \approx \sum_{i=1}^n \frac{\Pr(\text{Detect } FM_i | FM_i \text{ is present}) \cdot \Pr(FM_i \text{ is present})}{\Pr(\text{DU failure is present})}$$

This equation consider the PST coverage of the DU failure mode FM_i and the fraction of FM_i failures among all DU failures for $I = 1, 2, \dots, n$. We define these to variables as

$$\theta_{FM,i} = Pr(\text{Detect } FM_i | FM_i \text{ is present})$$

$$w_i = \frac{Pr(FM_i \text{ is present})}{Pr(DU \text{ failure is present})}$$

The PST coverage can therefore be expressed as

$$\theta_{PST} = \sum_{i=1}^n \theta_{FM,i} \cdot w_i$$

The procedure of determining the PST coverage comprises six steps who are built on techniques like FMEA (Failure Mode and Effect Analysis) and checklists. Both techniques are well known and recognized techniques in the oil and gas industry. FMEA is used to gain extensive knowledge of the system behavior upon failure, while the checklists are used to give credit to desired behavior.

Step 1: Get familiar with the PST and its implementation

- Which SIS components that are operated during a PST
- The functional safety requirements of the SIS components, like valve closing time and maximum allowed leakage in closed position
- How PST is initiated and controlled by dedicated hardware and software
- The PST interface to the SIS and other systems, like the process control system
- The operational and environmental conditions under which the SIF operates, including fluid characteristics, temperature and pressure

Step 2: Analyze the PST hardware and software

Suggests an FMEA style analysis to identify and analyze potential PST hardware and software failures and the effect these failures may have on the PST execution and the SIS. The FMEA should include a description of the components related failure modes and effects. This analysis will also give important insight to constrains and potential secondary effects of implementing PST.

Step 3: Determine the PST reliability

The PST hardware and software ability to provide reliable and useful test results calculated by the use of a checklist. A set of questions give credit to the preferred system behavior. Each question is weighted according to importance. The questions reflecting requirements made by

SIS related standards such as IEC 61508 are considered mandatory and are weighted 10. Questions addressing behavior recognized by guidelines and several authors are considered highly recommended and are weighted 5. Other issues that may have an effect on the PST reliability are weighted 1.

Each question is answered yes or no. The reliability of the PST is scaled from 0.5 to 1. The corresponding credit to PST reliability for each of the questions are calculated by

$$\text{Credit when "yes"} = \frac{\text{Weight of question}}{\text{Sum of all weights}} \cdot 1.0$$

$$\text{Credit when "no"} = \frac{\text{Weight of question}}{\text{Sum of all weights}} \cdot 0.5$$

A check list starting point is given in Lundteigen and Rausand [2008].

Step 4: Determine the revealability (per failure mode)

Deciding whether or not the failure mode may be revealed by the PST. A failure mode may also only be revealed for a portion of the failures in each failure mode. A failure mode that is fully observable is given the revealability factor 100% and when not observable at all, 0%. A failure mode may also be revealable with a certain probability, which is used as the revealability factor.

Step 5: Determine the failure mode weight

The weight of failure mode is the fraction the specific failure mode among all failures, shown previously with the equation for w_i . The failure mode weight is determined by expert judgment or by analysis of historical data.

Step 6: Determine the PST coverage

The previous steps have provided the data necessary to determine the PSD coverage by the equation $\theta_{PST} = \sum_{i=1}^n \theta_{FM,i} \cdot w_i$.

Chapter 5 Markov analysis 15

5.1 Markov model

The previous methods described are static and only takes into consideration if the system is a functioning or failed state. A system may be functioning at a degraded state and this is not shown in a RBD analysis. This makes it difficult to accurately model system behavior and maintenance strategies. A Markov analysis takes into account all states of a system, the transition between the states and the rate at which the transitions may occur. A Markov process is a stochastic process where the future state only depends on the present, and not the past. This is called the Markov property and is shown mathematically for a stochastic process $\{X(t), t \geq 0\}$ as

$$\Pr(X(t+s) = j | X(t) = i, X(u) = i, X(u) = x(u), 0 \leq u < s) = \Pr(X(t+s) = j | X(s) = i)$$

Where the state of the process at time s is $X(s) = i$. In addition, the probability of a transition from state i to j does not depend on global time, but on the time interval available for the transition.

$$\Pr(X(t+s) = j | X(s) = i) = \Pr(X(t) = j | X(0) = i)$$

A process with this property is known as a process with stationary or homogeneous transition probabilities.

A Markov model consists of a number of possible states, transition between states and transition rates. The possible states of the system need to be listed and named. For a system with n components, with the states functioning and failed, there are 2^n states. The collection of all states is denoted S and is to be $\{1, 2, 3, \dots, r\}$.

To describe a Markov process, consider a system of two parallel components. Both components can be either functioning or failed. This gives four different states that are listed as in Table 4. For a system of n components with either failed or functioning states, there is a total of 2^n states.

State	Component 1	Component 2
3	Functioning	Functioning
2	Functioning	Failed
1	Failed	Functioning
0	Failed	Failed

Table 4 State transitions

If both components are functioning at time t , the system is in state 3. If component 2 fails, the system will have a transition to state 2. When in state 2, component 1 may also fail, sending the system to state 0. Transitions from failed to functioning are also considered, if the system is in state 1 and component 1 is repaired the system has a transition to state 3. All states and transitions are illustrated in a state transition diagram, also called Markov diagram, as shown in Figure 12.

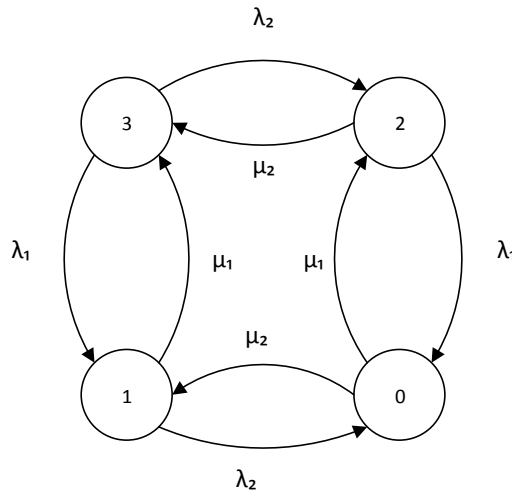


Figure 12 State transition diagram

All the different states are represented by circles and the possible transitions are shown by arcs connecting the states.

The transition probabilities for the process

$$P_{ij}(t) = \Pr(X(t) = j | X(0) = i)$$

for all $i, j \in \chi$ is arranged as a matrix

$$\mathbb{P}(t) = \begin{bmatrix} P_{00}(t) & P_{01}(t) & \cdots & P_{0r}(t) \\ P_{10}(t) & P_{11}(t) & \cdots & P_{1r}(t) \\ \vdots & \vdots & \ddots & \vdots \\ P_{r0}(t) & P_{r1}(t) & \cdots & P_{rr}(t) \end{bmatrix}$$

The transition rates are also included in the Markov diagram as failure rates and repair rates. The diagram can be used to form a *transition rate matrix*, \mathbb{A} . Where the rate at when in state i the process makes a transition to state j , a_{ij} .

$$\mathbb{A} = \begin{bmatrix} a_{00} & a_{01} & \cdots & a_{0r} \\ a_{10} & a_{11} & \cdots & a_{1r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r0} & a_{r1} & \cdots & a_{rr} \end{bmatrix}$$

The entries of row i are transition rates out of state i when j is not i , and the entries of column i is the transition rates into state i for $j \neq i$. The diagonal entries of the matrix are made up so that each row i is equal to 0. The transition matrix for the example of a 1oo2 system is then:

$$\mathbb{A} = \begin{bmatrix} -(\mu_1 + \mu_2) & \mu_2 & \mu_1 & 0 \\ \lambda_2 & -(\lambda_2 + \mu_1) & 0 & \mu_1 \\ \lambda_1 & 0 & -(\lambda_1 + \mu_1) & \mu_2 \\ 0 & \lambda_1 & \lambda_2 & -(\lambda_1 + \lambda_2) \end{bmatrix}$$

The system unavailability is decided based on the probability of the system being in a failed state at time t . If the state of the system is known at time 0, the performance probability of the system can be predicted, called state equations. The vector $P(t)=[P_0(t),P_1(t),\dots,Pr(t)]$ is the distribution of the Markov process at time t when the state is known at time 0. By adding the initial state with the transition matrix the state equations are obtained.

$$P(t) \cdot \mathbb{A} = \dot{P}(t)$$

To determine the PFD of a system we look at the unavailability of the system. In this example that is the case when the system is in state 0 where both components are failed and the intended safety function cannot be carried out if a demand occurs. To generalize this we call all functioning states B, and all failed states F. The PFD for the test interval n is obtained by

$$PFD(n) = \frac{1}{\tau} \int_{(n-1)\tau}^{n\tau} \Pr(X(t) \in F) dt$$

5.2 Phased Markov

For periodically tested SIS in low demand mode, repairs are only initiated when tests are performed. IEC 61508 suggests a multiphased Markovian approach to model such systems. A periodically tested component may have three states: working, DU failure, or under repair. In addition to the continuous time Markov model between test times, two discrete Markov

chains are used to include the state of the component immediately before and after testing. This may be used to consider imperfect repairs and maintenance [12]. IEC 61508 illustrates this as shown in Figure 13.

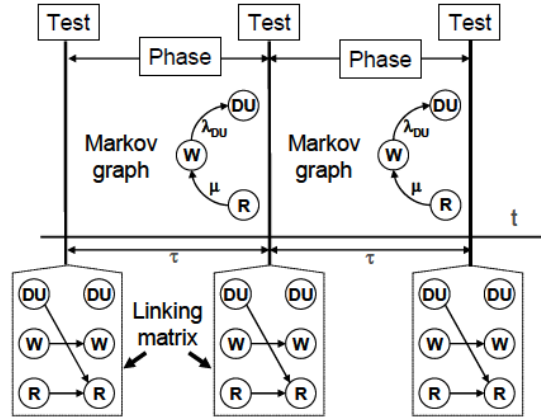


Figure 13 Multiphased Markov model as illustrated in IEC 61508 [13]

The process $\{X(t)\}$ behaves like a homogenous Markov process with transition matrix, \mathbb{A} , as long as time runs inside test intervals $((n - 1)\tau \leq t < n\tau, \text{ for } n = 1, 2..)$. Let $P_{jk}(t) = \Pr(X(t) = k | X(0) = j)$ denote the transition probabilities for $j, k \in S$.

The different states before and after each test is represented by linking matrixes. Let Y_n be the state of the component immediately before a test. Y_n is defined for $n=1,2,\dots$ as

$$Y_n = X(\pi\tau-) \equiv \lim_{t \rightarrow \pi\tau^-} X(t)$$

After a test, repair actions may be taken which will take the component to another state, Z_n , according to a transition matrix $R = (R_{jk})$, where

$$P(Z_n = k | Y_n = j) = R_{jk}; j, k \in S$$

Figure 14 illustrates where on the time line we have Y_n and Z_n .

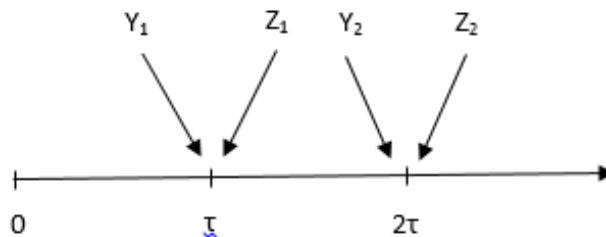


Figure 14 Definition of Y and Z

Distribution of the state of the safety system at time $t=0$, $Z_0 = X(t)$ is denoted $\rho = [\rho_0, \rho_1, \dots, \rho_r]$, where ρ_i is the probability the system is in state i right after a test and the sum of all ρ is equal to 1.

$$\begin{aligned} \Pr(Y_1 = k) &= \Pr(X(\tau -) = k) \\ &= \sum_{j=0}^r \Pr(X(\tau -) = k | X(0) = j) \cdot \Pr(X(0) = j) \\ &= \sum_{j=0}^r \rho_j \cdot P_{jk}(\tau) = [\boldsymbol{\rho} \cdot \mathbb{P}(\tau)]_k \end{aligned}$$

Now, for test intervals equal or greater than 1. Just after a test interval state of the system is Z_n . Assuming that the Markov process is independent of previous transitions.

$$\begin{aligned} \Pr(Y_{n+1} = k | Y_n = j) &= \sum_{i=0}^r \Pr(Y_{n+1} = k | Z_n = i, Y_n = j) \cdot \Pr(Z_n = i | Y_n = j) \\ &= \sum_{i=0}^r P_{ik}(\tau) R_{ji} = [\mathbb{R} \cdot \mathbb{P}(\tau)]_{jk} \end{aligned}$$

The discrete Markov chain of Y_n has the transition matrix

$$\mathbb{Q} = \mathbb{R} \cdot \mathbb{P}(\tau)$$

In the same way

$$\begin{aligned} \Pr(Z_{n+1} = k | Z_n = j) &= \sum_{i=0}^r \Pr(Z_{n+1} = k | Y_{n+1} = i, Z_n = j) \cdot \Pr(Y_{n+1} = i | Z_n = j) \\ &= \sum_{i=0}^r P_{ji}(\tau) \cdot R_{ik} = [\mathbb{P}(\tau) \cdot \mathbb{R}]_{jk} \end{aligned}$$

And the transition matrix is

$$\mathbb{T} = \mathbb{P}(\tau) \cdot \mathbb{R}$$

Let $\boldsymbol{\pi} = [\pi_0, \pi_1, \dots, \pi_r]$ be the stationary distribution of the Markov chain Y_1, Y_2, \dots . $\boldsymbol{\pi}$ is the unique probability vector satisfying the equation

$$\boldsymbol{\pi} \cdot \mathbb{Q} \equiv \boldsymbol{\pi} \cdot \mathbb{R} \cdot \mathbb{P}(\tau) = \boldsymbol{\pi}$$

When F is the set of states in S representing DU failure, then the long run expectation of the system being in an F state immediately before a test is defined by $\pi_F = \sum_{i \in F} \pi_i$. The mean time to critical failure can then be expressed by

$$MTBF_{DU} = \frac{\tau}{\pi_F}$$

And the average DU failure rate is

$$\lambda_{DU} = \frac{1}{MTBF_{DU}} = \frac{\pi_F}{\tau}$$

In the same way for the Markov chain Z_1, Z_2, \dots we let $\boldsymbol{\gamma} = [\gamma_0, \gamma_1, \dots, \gamma_r]$, where $\boldsymbol{\gamma}$ is the unique probability vector satisfying

$$\boldsymbol{\gamma} \cdot \mathbb{T} \equiv \boldsymbol{\gamma} \cdot \mathbb{P}(\tau) \cdot \mathbb{R} = \boldsymbol{\gamma}$$

The average probability of failure on demand in interval n may be expressed by

$$PFD(n) = \frac{1}{\tau} \int_{(n-1)\tau}^{n\tau} \Pr(X(t) \in F) dt = \frac{1}{\tau} \int_0^\tau \sum_{j=0}^r \sum_{k \in F} P_{jk}(t) \cdot \Pr(Z_n = j) dt$$

Letting n go to infinity, $\Pr(Z_n = j)$ is replaced by the long-term proportion of times the system is in state i just after a test /repair, γ_i . Given that the system is in state j at the beginning of the test interval, the long-term average PFD is then

$$PFD = \lim_{n \rightarrow \infty} PFD(n) = \frac{1}{\tau} \int_0^\tau \sum_{j=0}^r \sum_{k \in F} P_{jk}(t) \cdot \gamma_j dt = \sum_{j=0}^r \gamma_j Q_j$$

Where

$$Q_j = \frac{1}{\tau} \int_0^\tau \sum_{k \in F} P_{jk}(t) dt$$

Repair strategy

The repair matrix, \mathbb{R} , is decided based on what repair strategy is adopted for the specific system. Some repair strategies may be:

- All failures are repaired after each test interval. The system will always be in fully functioning state after testing.
- Only critical failures are repaired after testing. The system may have faults, but is still functioning with degraded failure after testing.
- Imperfect repairs. There is a probability that the failure may not be fully repaired after repair actions are taken.

To demonstrate the different repair strategies and example taken from Lindqvist and Amundrustad [1998] is described in the following.

Consider a single component that is as good as new in state 3. From state 3 the component may fail suddenly due to a hazardous event. The component may also suffer from failure due to degradation, which means that the component may still be functioning but at a degraded state. From the degraded state we may also have dangerous failure due to degradation. We then have the following states:

State	Description	Transitions to
3	As good as new	2 and 1
2	Degradation	1 and 0
1	Failure due to sudden hazardous event	-
0	Failure caused by degradation	-

Table 5 Description of states and transitions

The transitions are shown in the state transition diagram in Figure 15 where λ_s is the rates of failure caused by a sudden event. The rate of degradation failure is λ_d and the rate for a degraded failure to become critical is λ_{dc} .

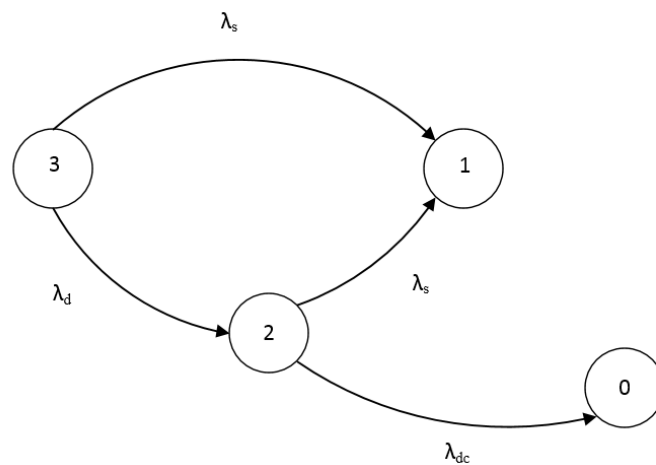


Figure 15 State transition diagram for one component with degraded and sudden failure.

From the state transition diagram we get the transition rate matrix

$$\mathbb{A} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \lambda_{dc} & \lambda_s & -(\lambda_{dc} + \lambda_s) & 0 \\ 0 & \lambda_s & \lambda_d & -(\lambda_s + \lambda_d) \end{bmatrix}$$

No repairs are performed between test intervals. The failed states 1 and 0 are therefore absorbed states, meaning once entered it is never left. We also assume that the system is in state 3 at time 0. By solving the forward Kolmogorov equations $P(t) \cdot \mathbb{A} = \dot{P}(t)$ to find the distribution $\mathbb{P}(t)$

$$\cdot \mathbb{P} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ P_{20}(t) & P_{21}(t) & P_{22}(t) & 0 \\ P_{30}(t) & P_{31}(t) & P_{23}(t) & P_{33}(t) \end{bmatrix}$$

Where the entries are

$$P_{22}(t) = e^{-(\lambda_s + \lambda_{dc})t}$$

$$P_{33}(t) = e^{-(\lambda_s + \lambda_d)t}$$

$$P_{20}(t) = \frac{\lambda_{dc}}{\lambda_s + \lambda_{dc}} (1 - e^{-(\lambda_s + \lambda_{dc})t})$$

$$P_{21}(t) = \frac{\lambda_s}{\lambda_s + \lambda_{dc}} (1 - e^{-(\lambda_s + \lambda_{dc})t})$$

$$P_{30}(t) = \frac{\lambda_d \lambda_{dc}}{(\lambda_d + \lambda_s)(\lambda_s + \lambda_{dc})} + \frac{\lambda_d \lambda_{dc}}{(\lambda_d - \lambda_{dc})(\lambda_d + \lambda_s)} e^{-(\lambda_s + \lambda_d)t} \\ + \frac{\lambda_d \lambda_{dc}}{(\lambda_{dc} - \lambda_d)(\lambda_{dc} + \lambda_s)} e^{-(\lambda_s + \lambda_{dc})t}$$

$$P_{31}(t) = \frac{\lambda_s(\lambda_d + \lambda_s + \lambda_{dc})}{(\lambda_d + \lambda_s)(\lambda_s + \lambda_{dc})} + \frac{\lambda_s \lambda_{dc}}{(\lambda_d - \lambda_{dc})(\lambda_d + \lambda_s)} e^{-(\lambda_s + \lambda_d)t} \\ + \frac{\lambda_s \lambda_{dc}}{(\lambda_{dc} - \lambda_d)(\lambda_{dc} + \lambda_s)} e^{-(\lambda_s + \lambda_{dc})t}$$

$$P_{32}(t) = \frac{\lambda_d}{\lambda_d - \lambda_{dc}} (e^{-(\lambda_s + \lambda_{dc})t} - e^{-(\lambda_s + \lambda_d)t})$$

All failures are repaired after testing

With this repair model, the system will always be in state 3 after a test. The repair matrix will therefore be

$$\mathbb{R} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

In this case it is easy to find the PFD. All test intervals have the same stochastic properties and the PFD is therefore given by

$$PFD = \frac{1}{\tau} \int_0^{\tau} (P_{31}(t) + P_{30}(t)) dt$$

Which follows the general model which was explained previously in this chapter.

Only critical failures are repaired after testing

If the system is in a degraded state, but no critical failure (state 2 in this example), then no repair actions are taken. Then the repair matrix will be

$$\mathbb{R} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Where r_{22} is set to 1 and $r_{23} = 0$ leaving the system in state 2 after repair. We may also consider a more general model where degraded failures are repaired with the probability of $r-1$ and is not repaired with the probability r , where $0 \leq r \leq 1$. Making r the determining parameter for the repair strategy. The repair matrix will then be

$$\mathbb{R} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & r & 1-r \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

To find the PFD we must compute the matrix $\mathbb{T} = \mathbb{P}(\tau) \cdot \mathbb{R}$ and solve the stationary distribution γ . It is obvious that $\gamma_0 = \gamma_1 = 0$ because of the perfect repair. We then get

$$\gamma_3 = \frac{1 + rP_{32}(\tau) - rP_{22}(\tau)}{1 - rP_{22}(\tau)}$$

$$\gamma_2 = \frac{1 + rP_{32}(\tau) - rP_{22}(\tau)}{rP_{32}(\tau)}$$

$$Q_3 = \frac{1}{\tau} \int_0^{\tau} P_{31}(t) + P_{30}(t) dt$$

$$Q_2 = \frac{1}{\tau} \int_0^{\tau} P_{21}(t) + P_{20}(t) dt$$

Now we can solve for the PFD by using $\sum_{j=0}^r \gamma_j Q_j$

$$PFD(r, \tau) = \gamma_3 Q_3 + \gamma_2 Q_2$$

Imperfect repair model

In the previous models we have considered perfect repair of DU failures. Realistically the repair action may repair some of the failure, but the system may not be in perfect condition after repair. The test may also create new failures leaving the system in worse state than before entering the test. The principle is the same as above with a probability r that the failure is not repaired and a probability of $(1-r)$ that the failure is repaired. The repair matrix will then be

$$\mathbb{R} = \begin{bmatrix} r_0 & 0 & 0 & 1 - r_0 \\ 0 & r_1 & 0 & 1 - r_1 \\ 0 & 0 & r_2 & 1 - r_2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

5.3 HIPPS evaluation in GRIF workshop

SIL module

The SIL module of GRIF is used to calculate the PFD of a SIS. The interface splits the screen into two, the left side is for entering parameters and configuration of the system architecture and the right side shows the graphical result of the computations.

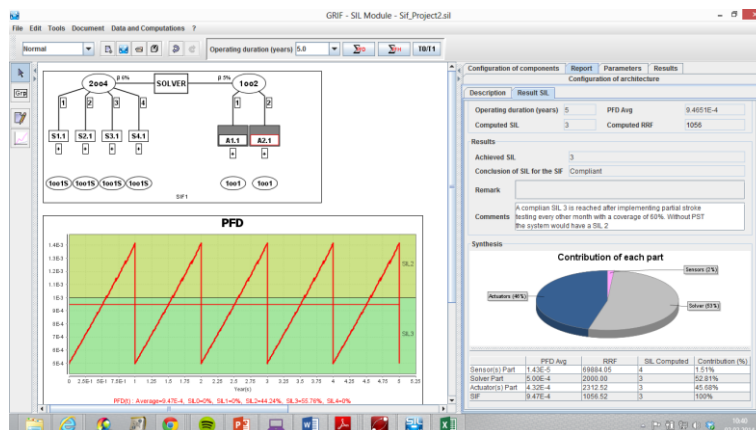


Figure 16 SIL module interface

The same architecture as used in Kristin and the parameters from Table 2 are used to simulate the effect of partial stroke testing on the HIPPS PFD. From the results shown in Figure 17 and

Figure 18 we can see that without PST the required SIL 3 was not reached, by when PST was implemented the system was improved just enough to reach SIL 3.

To be able to get a significant enough change in the PFD a PST coverage of as much as 75% was needed. This is not a realistic value and from this model it cannot be concluded that the PST has any significant influence on the HIPPS.

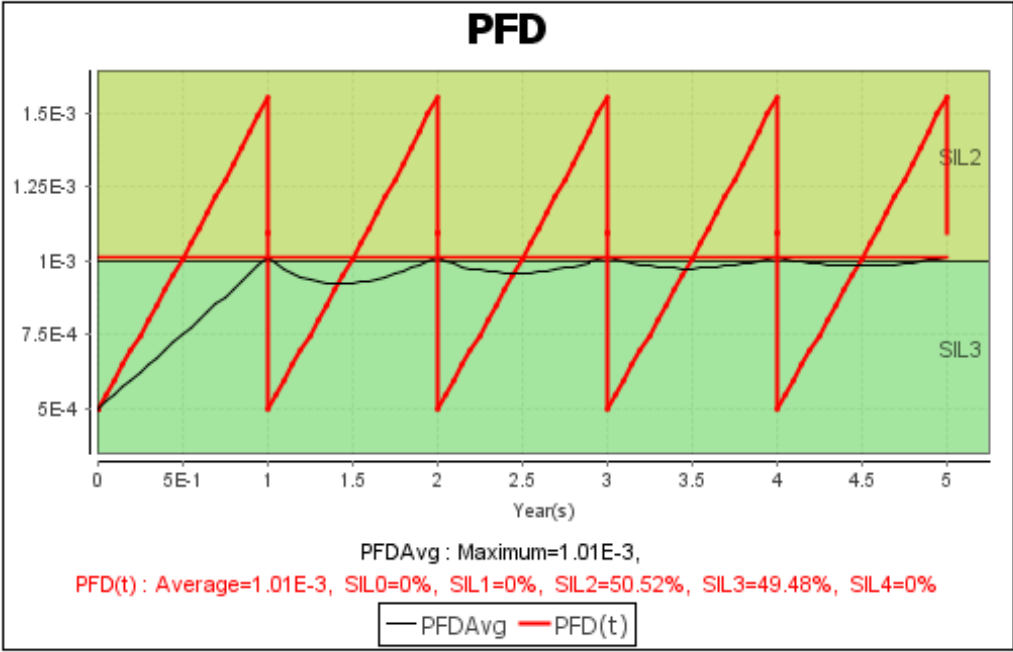


Figure 17 PFD without partial stroke testing

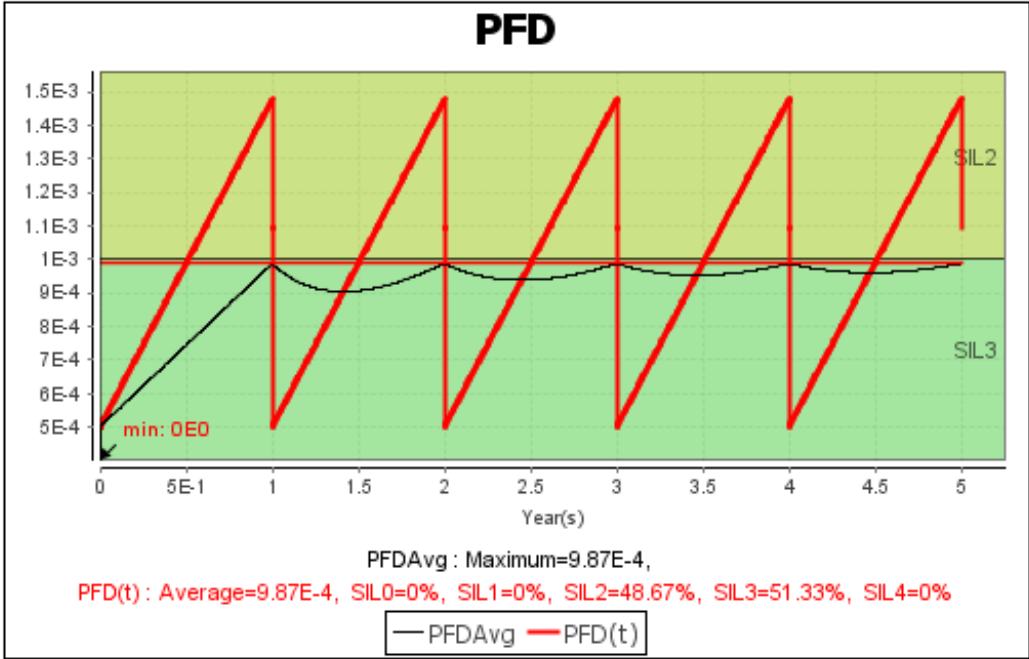


Figure 18 PFD with partial stroke testing

Markov Graphs module

The GRIF workshop also has a module for Markov graph. In this module different repair strategies can be modelled by chaining matrixes. During the simulation process some problems occurred and graphs with the results would not appear on the screen the way they should. The results are therefore not included in this report, but the principle is explained.

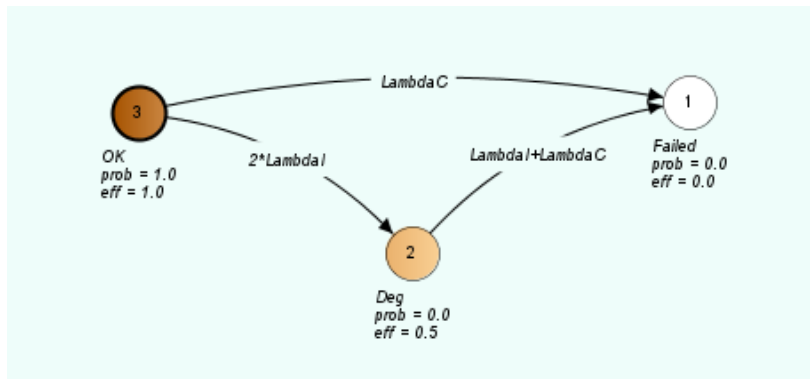


Figure 19 State transition diagram

The state transition diagram for the 1oo2 voted HIPPS valves are shown in Figure 19. The system starts in state 3 where both components are fully functioning. If one component fails the system will be in state 2. The system is still functioning, but in a degraded state. In state 1 the system both the components are failed and the system will not be able to perform its intended function.

The repair strategies are introduced by chaining matrices that work as transition matrices from one phase to the next. In repair strategy 1 all failures are repaired perfectly, bringing the system to state 3 after each test interval. The chaining for this repair strategy is shown in Figure 20, where the system all states to state 3 with the probability of 1.

Chaining matrix		
Before chaining	After chaining	Probability
1	3	1
2	3	1
3	3	1

Figure 20 Repair Strategy 1

The unavailability of the system is shown graphically in Figure 21

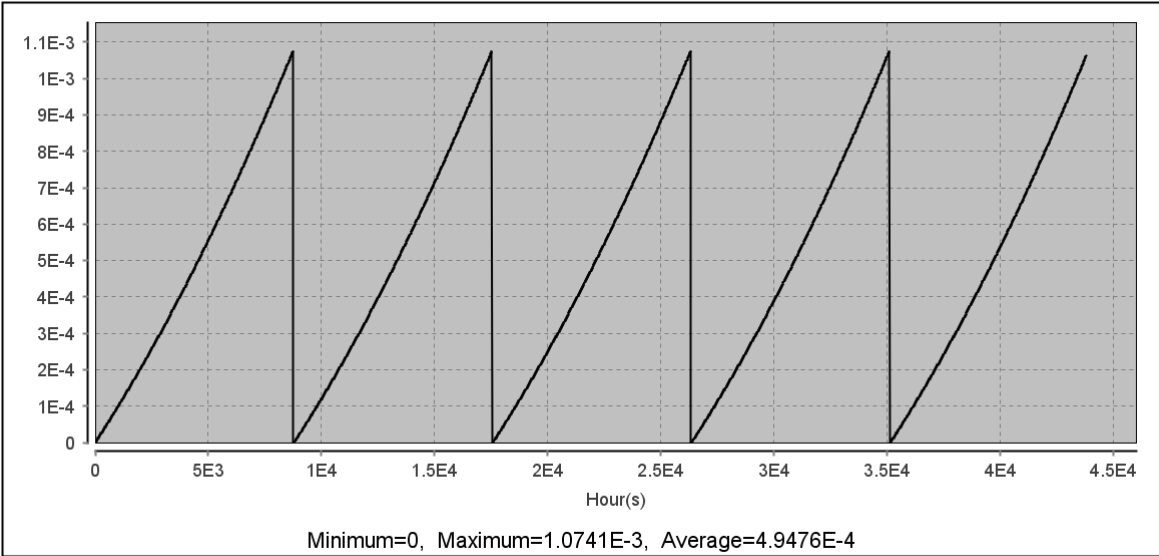


Figure 21 Unavailability with repair strategy 1

In repair strategy 2 only critical failure is repaired. If the system is in state 1 at the end of phase i , it will be in state 3 at the beginning of state $i+1$. And if the system is in state 2 no repairs are done and the system will continue to be in the degraded state.

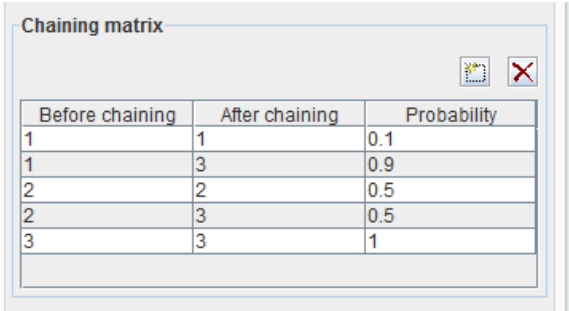
Chaining matrix

Before chaining	After chaining	Probability
1	3	1
2	2	1
3	3	1

Figure 22 Repair strategy 2

Repair strategy 3 is shown in Figure 23. If the system at the end of phase i is:

- In state 1, the probability of being in state 1 at the beginning of phase $i+1$ is 0,1;
- In state 1, the probability of being in state 3 at the beginning of phase $i+1$ is 0,9;
- In state 2, the probability of being in state 2 at the beginning of phase $i+1$ is 0,5;
- In state 2, the probability of being in state 3 at the beginning of phase $i+1$ is 0,5;
- In state 3, the probability of being in state 3 at the beginning of phase $i+1$ is 1;



Before chaining	After chaining	Probability
1	1	0.1
1	3	0.9
2	2	0.5
2	3	0.5
3	3	1

Figure 23 Repair strategy 3

Chapter 7 Available data

Relevant data is essential when conducting a quantitative reliability analysis. There are several existing data sources and it is important that the best available parameters are used in such an analysis. To decide whether or not the data is relevant, there are several things to consider:

- Does the data apply the specific application of the equipment considered (operating and environmental conditions)?
- Which is most relevant data source for the specific equipment?
- Are there any assumptions to the data sources that needs to be taken into account?
- How does the data support the maintenance strategy?
- What uncertainties are associated with the data?

In the industry there is rarely two cases that are the same. It is therefore difficult to evaluate the accuracy of data sources. It is therefore important to mention the uncertainty of the input data in a reliability analyses.

We may categorize failure rate sources into generic data, operator/company specific data, site/application specific data and manufacturer provided data. The PDS Handbook describe these types of data as

Generic data: Failure data based on a broad group of components without information on manufacturer, make and component specifications. Such data can be based on recorded failures, from expert judgments, or from laboratory testing. The OREDA handbooks and PDS data handbook are examples of generic data sources.

Operator/company specific data: Failure data based on operating experience from one operator/oil company e.g. all company installations and/or their own interpretation of different data sources.

Site/application specific data: Failure data based on failures recorded at a specific site or in relation to a specific application.

Manufacturer provided data: Failure data for a particular product prepared by a particular manufacturer (or a consultant). Can be based on component FMEA/FMEDA studies, laboratory testing, and in some cases also field experience.

Figure 24 illustrates the availability and relevance of the different data sources.

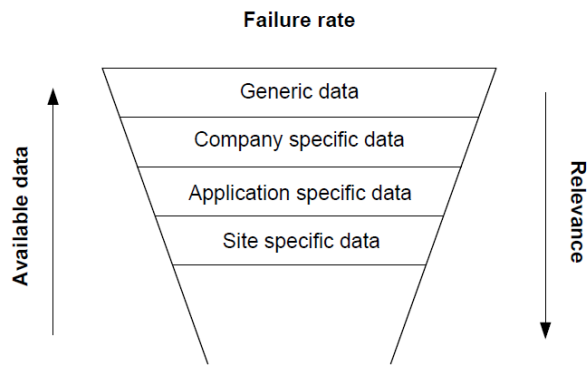


Figure 24 Availability and relevance of the different data sources [14]

7.1 OREDA

OREDA is a project sponsored by several companies in the oil and gas industry operating worldwide. The main purpose of the OREDA project is to exchange and collect reliability data from the participants and act as a forum to co-ordinate the reliability data collection. The OREDA database contains reliability and maintenance data for exploration and production equipment from a variety of geographic areas, installations, equipment types and operation conditions. Primarily the data is for offshore subsea and topside equipment, but there are also some available data for onshore equipment [15].

In OREDA, failure modes are classified critical, degraded or incipient [8]

- *Critical*: “A failure that causes immediate and complete loss of a system’s capability of providing its output”
- *Degraded*: “A failure that is not critical, but that prevents the system from providing its output within specifications. Such a failure would usually, but not necessarily, be gradual or partial, and may develop into a critical failure in time.”
- *Incipient*: “A failure that does not immediately cause loss of a system’s capability of providing its output, but which, if not attended to, could result in a critical or degraded failure”

Because the failure data is mainly collected from maintenance record, both component specific failures and common cause failures are included. This also implies that failures such as spurious trips are not included, because such failures may not require any maintenance [8].

7.2 PDS Data Handbook

The PDS Data Handbook is developed by SINTEF and contains data dossier for several different components. The data is based on OREDA, but some adjustments to the figures are made based on expert judgments.

Chapter 8 Discussions and concluding remarks

A reliability assessment is built on a number of assumptions about the system and the conditions it is operated in. If these assumptions and uncertainties about them are not well documented, the result of the assessment may be misinterpreted and a SIS design that is not suited for the purpose may be put to use.

The PFD is influenced by the three factors: modeling, data and calculations. The uncertainty of the PFD depends on how these factors reflects the main purpose of the SIS being analyzed [16].

The first step when developing a model is the construction of a functional model, then one or more reliability models are developed. The modeling uncertainties may stem from the choice and the understanding of the model. The degree of knowledge of the model may be expressed by answering questions like:

- Does the model reflect the main properties of the study
- Are the objectives of the model fully understood?
- Are all the relevant assumptions considered?
- Are the limitations of the model understood?
- Does the analyst understand the computational capacities and requirements?
- Are the input data requirements fully understood?

Parameter uncertainty may be influenced by the quality of the data collected, the amount of collected data, estimation procedures and expert judgment [17]. The technology in the oil and gas industry is always under development and systems are rarely used with the same conditions and requirements twice. The available data may therefore be outdated and irrelevant when assessing the reliability model. To decide whether or not the parameters are relevant it may be useful to ask if decisions would be made different if the parameters were different. Or if additional data collections and research would lead to a different decision.

The PFD can be calculated by exact mathematical methods or by approximation formulas. The two approaches only give small differences in the results and the uncertainties regarding calculations is considered the least important contributor to the uncertainty [16].

A sensitivity analysis may be used to improve the interpretation of the results. The sensitivity analysis is conducted by changing one uncertain parameter at the time and studying what effect this has on the output [17].

Concluding remarks

There are several methods for determining the reliability of a SIS. The assumptions and limitations for the different methods must be understood for the results to be of any value. The HIPPS has been assessed by Reliability block diagram, approximation formulas and Markov modeling.

The Reliability Block Diagram is easy to use and gives a logical presentation of the system. By using the approximation formulas fairly accurate results are obtained taking into account test intervals, test coverage and common cause failures.

The concept of Partial Stroke Testing is of high relevance when assessing a system such as HIPPS. In chapter 4 the PST showed a positive effect on the PFD of the valve. In the calculations made in chapter 5 the effect from the PST did not give the same results. The calculations were made for the whole system and the reason for the small effect of the PST may be that the contributions to the PFD from the pressure transmitters were greater than the contribution from the safety valves.

Referanser

- [1] B. H. Jacob G.Hoseth, "Optimizing Pressure in Subsea Pipelines with HIPPS," *ABB review*, no. 2, pp. 28-35, 2000.
- [2] B. L. T. O. R. Aarø, "Subsea HIPPS Design Procedure," in *Offshore Technology Conference* , Houston , 1995.
- [3] L. B. H. S. Roald Sirevaag, Writer, *Experience with HTHP Subsea HIPPS on Kristin*. [Performance]. Statoil, 2006.
- [4] R. S. H. S. Lars Bak, "HIPPS protects subsea production in HP/HT conditions," *Offshore magazine*, no. 1, 2007.
- [5] P. T. R. S. G. Gail, "Reliability if Subsea Control Systems: HIPPS a Case Study," *SCADA*, pp. 55-70, 2002.
- [6] E. W. Jacob G. Hoseth, "Implementation Options for the Subsea High Integrity Pipeline Protection System (HIPPS) Solution," in *Offshore Technology Conference*, Houston, 1997.
- [7] API RP 170, "Recomended Practice for Subsea High Integrity Pressure Protection System (HIPPS)," American Petroleum Institute, 2009.
- [8] A. H. Marvin Rausand, *System Reliability Theory: Models, Statistical Methods and Applications*, Secon Edition, Hoboken, NJ: Wiley, 2004.
- [9] Sintef, *Reliability Prediction Method for Safety Instrumented Systems - PDS Method Handbook*, Trondheim, Norway : SINTEF, 2013.
- [10] M. R. M. A. Lundteigen, "The effect of partial stroke testing on the reliability of safety valves," *Department of Production and Quality Engineering, NTNU*, 2007.

- [11] M. R. M. A. Lundteigen, "Partial stroke testing of process shutdown valves: How to determine the test coverage," *Journal of Loss Prevention in the Process Industries* , pp. 579-588, 23 April 2008.
- [12] OLF, "070 Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry," The Norwegian Oil Industry Association, 2004.
- [13] IEC 61511, "Functional safety - safety instrumented systems for the process industry," International Electrotechnical Commission, Geneva, 2004.
- [14] IEC 61508, "Functional Safety of electrical/electronic/programable electronic safety-related systems," International Electrothechnical Commission, Geneva, 2010.
- [15] R. A. B. L. T. Onhus, "HIPPS Applications and Acceptance Criteria," in *Offshore Technology Conference*, Houston, 1995.