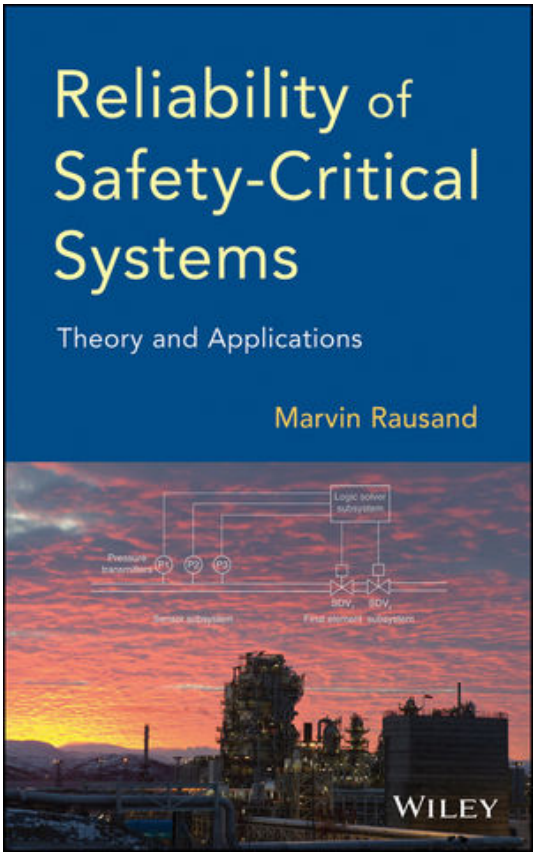
Solutions for problems in:



http://www.ntnu.edu/ross/books/sis

Marvin Rausand Mary Ann Lundteigen

(Version July 2017)

RAMS Group
Department of Production and Quality Engineering
Norwegian University of Science and Technology
Trondheim, Norway

Contents

Preface

This booklet contains solutions to a selection of problems in the problems booklet prepared as a supplement to *Reliability of Safety-Critical Systems*, Wiley, 2014. Solutions are still under development. Current revision is dated July 2017. An update may be expected once or twice per year.

Marvin Rausand
marvin.rausand@ntnu.no

Mary Ann Lundteigen
mary.a.lundteigen@ntnu.no

Chapter 1

Introduction

Problem 1. (Part of tutorial 1)

- A *safety-critical system* is a general term used to denote a system whose failure may result in harm to people, the environment, or material assets. Loss of material assets in this context is not primarily related to the costs and lost production, but rather to the negative impact on the society (such as loss of working place, loss of critical infrastructures, and so on). The system may be based on, or at least include some electrical, electronic, and/or programmable electronic (E/E/PE) technology, and in this case we may refer to the system as a E/E/PE safety-related system (or safety-instrumented system, as the term is used in the process industry).
- *Active safety barrier*: Safety barrier is a common term used to denote any system (technical, organizational, human) that can interact (prevent or mitigate) in the sequence of events that can lead to an accident. An active safety barrier is a safety barrier that needs to be activated in order to interact.
- *Functional safety* relates to the safety that is "taken care of" by the safety-critical system using E/E/PE technology. Functional safety is the part of the overall system safety that depends on the correct functioning of active control and safety systems. Functional safety relies on active barriers, while passive barriers are not part of functional safety.
- SIS is a term that has been introduced in the process industry (through ISA standards and IEC 61511), and denotes primarily "on demand" safety-critical systems that are realized using instrumented technology (but we also talk about high-demand and continuous demand SIS, even if they are more rare

in the process industry). Instrumented technology means instruments used for measurement and control such as sensors, logic solvers, and valves.

- A SIS can be classified as an active safety barrier, both when operating in the low and the high/continuous demand mode.
- Functional safety points to safety measures that relies on active safety barriers relates to the functional capabilities of the SIS, and in what whay the SIS is able to provide the necessary safety functions.

The terms are related by:

- SIS being an example of a safety-critical system that uses E/E/PE technology
- That SIS is an active safety barrier
- Functional safety applies to active safety barriers, like a SIS.

Problem 2. Solution not yet available here, but relevant information is found in the text book.

Problem 3.

Solution not yet available here, but relevant information is found in the text book.

Problem 4.

Solution not yet available here, but relevant information is found in the text book.

Problem 5.

(a) The main difference between the two modes of operation is how often the safety-critical systems (or here titled safety barriers) are demanded. The term "are demanded" means how often the event that requires a response by the safety-critical system occurs. A *low-demand* system is operated seldom, and seldom means here less often than once per year. A *high-demand* system is operated frequently or even continuously, and frequently means here more often

than once per year. The rationale behind using one year as the borderline is not clear or fully argued in IEC 61508 and related standards.

(b) Low-demand safety barriers may be the airbag system in an automobile or an emergency call center alarm (if available), while high-demand safety barriers are include the anti-lock braking systems and anti-spin systems in an automobile. Seat belts and the car frame are also safety barriers, but they do not employ E/E/PE technology and are not usually considered as either low-demand or high-demand. However, we may consider the seat belt as low-demand (since the event where it should lock is rather seldom, luckily), while the car frame is more difficult to place. However, if we look at the frames ability to withstand the dimensioning loads during a car crash, it should be low demand.

Problem 6.

(a) Fail-safe relates to a design property. A fail-safe valve is designed or installed such that it enters a state where the plant either maintains or enters a safe state upon loss of energy (electrical power, hydraulic pressure, or pneumatic pressure). What is safe state depends on the situation. Often, it means to close the valve so that the flow is stopped (so-called fail-safe close), however, in some cases the safe state is to open the valve to release the pressure (so-called fail-safe open).

(b) Examples of fail-safe implementation can be found at `https://en.wikipedia.org/wiki/Fail-safe`

(c) De-energize-to-trip means that the component activates when the energy supply is removed, while energize-to-trip components will activate when energy is applied. An energize-to-trip valve that is open during normal operation requires power to close. If the safe state is achieved when the valve closes, the valve is not a fail-safe valve. De-energize would therefore be a better principle to use for a shutdown valve.

(d) Difference between fail-safe passive, fail-safe active, and fail-safe operational are: Solution not yet available here, but relevant information is found in the text book.

(e) Choice of fail-safe design for:

- Fly-by-wire: Fail-safe operational. Many planes are today almost impossible to fly without automatic systems, so even-fail safe active could be an inadequate alternative.
- Red light: Fail-safe active. System enters a new state where all traffic is

stopped. Ensure that power is not removed to the circuit for red light.

- Shutdown valve: Fail-safe passive, where de-energize to trip (here: close) of valve.

Problem 7.

(a)

- Safe state is the state in which the equipment under control (EUC) is safe. This can mean that hazardous events that have arised within the EUC have been stopped (for example by a prompt shut down the process in an off-shore facility) or entered a new phase (for example cooling down, controlled run down of chemical process).

- Fail-safe is related to how the safety-critical system (SIF and/or single element) should behave in a situation where the safety-critical system has one or more faults in order to reach a safe state of the EUC. This cannot be in case of any faults, but special type of faults like power loss, sensor signal out of range, abnormal output signal (for example "frozen signal") from logic controller etc.

  It may be remarked that fail-safe is a design property (something we design into the system), but it cannot be done without knowing something about how the system is going to be used (what type of the EUC). For example, a valve designed as a fail-safe *close* valve should not be chosen if the safe state of the EUC is achieved if valve opens upon a fault condition.

- De-energize to trip describe how the safety function is achieved in response to a demand, and is a design property. As the term states, the safety function (here denoted trip, even if this is somewhat limiting word) by removing power. Such systems are powered during normal (non-demand) conditions, and removal of power is a "signal" about being in a demand situation. The secondary effect of this design principle is that any fault condition that relates to loss of power would also result in a safe state, assuming that the trip (or the carry out of safety function) results in a transition to the safe state.

- Energize to trip describes (as for de-energize to trip) how the safety function is achieved in response to a demand, and is a design property. Unlike de-energize to trip, the energize to trip system requires power in order to

carry out the safety function. A loss of power would not result in a safe state automatically, so we may claim that energize to trip is not a fail-safe system. There are two (among probably more) reasons why energize to trip systems are chosen:

- Energize to trip systems will under normal (non-demand) situation not require power. Power is first added to e.g. switch a solenoid valve to a new position or open or close a valve. Where power consumption is an issue (for example subsea) it is sometimes chosen.
- For some systems it may not be easy to identify in advance what is the safest action to do in case of a demand. Sometimes the safest thing is to wait and see, or in some cases close while in other situations open a valve. In this case it may be safer to add power when an action is needed, in order to avoid the situation where a loss of power could result in a pre-defined activation. One example of such a system is the blowout preventer (BOP) installed on the top of a well (or Xmas tree) during well drilling and intervention work. If an uncontrolled situation occurs in the well, it may be important not to activate the BOP immediately, but wait till tools or pipes inside well has been relocated or removed. If the BOP automatically activates (meaning shearing whatever is inside the BOP and blinds) upon an (accidental) loss of power, the situation may become more harmful than trying other measures like increasing weight of mud.

(b) A fail-safe valve will usually go automatically to the closed position upon loss of power (hydraulics, air/pneumatics) or electrical signal/power. In this case we refer to the valve as fail-safe close. However, if the safe state is that the valve opens in a demand situation (which could be in the case of a valve being used for pressurization), one could select a valve actuator which results in fail-safe open.

(c) This question was already addressed in (a). Please review the explanation given there.

Problem 8.

(a) The main characteristics of a generic standard (in this context) is that it is sector/application-independent, meaning that it may be applicable to any sector or application area. IEC 61508 also lists some additional purposes of the standard: To be a basis for development of sector and application specific standards, and to

be able to specify requirements that are flexible enough to apply to most E/E/PE technologies.

(b) A sector-specific standard is targeted to a specific sector. This means that the requirements are aligned with common practice within the sector and that sector-specific terms are used. Sometimes, the sector-specific standard may restrict its application to the most typical and desired way of designing and operating a safety-critical system, and make reference back to IEC 61508 when this is not the case.

(c) You may check if your Internet search included the standards listed in Section 1.3.2 of the textbook. The list includes IEC 61511 (process industry), IEC 62061 (machinery systems), IEC 62425, or EN50129 which is a more frequently used name for the same standard, (railway industry), IEC 61513 (nuclear industry), IEC 60601 (medical equipment) and ISO 26262 (automobile industry). You may to your internet seach also try to determine in what contexts the standards seem to appear (what companies are writing about them, in what services are they used).

(d) Rule-based requirements are often rather prescriptive, so that less freedom is available to suggest alternative implementations. Rule-based requirements often builds on best-practice engineering principles, and the rule based requirements represent a way to maintain /preserve good technical solutions. At the same time, the rule-based requirements may prevent the best solutions, if a system is installed under new operating environment or with new type of technology. One practical example here is that rule-based requirements for topside systems (e.g. allowed leakage rates of valves) may not apply (and in fact be cost driving) for subsea environment. Risk-based requirements are formulated on the basis of risk, meaning that high risk gives stricter requirements to safety-critical systems than low risk. Rule-based requirements seldom differentiate between high and low risk, and applies the same requirements in both cases. Risk-based requirements opens up for alternative technical solutions, as long as they can be demonstrated sufficiently reliable to control risk. This can both be positive (allowing adaption of new design principles) and negative (the new principles are not proven by field experience yet).

(e) Chapters 1 and 2 briefly mention life cycle phases. It is difficult to explain the content of the phases without reading IEC 61508-1, or IEC 61511 (for the process industry). You may put the emphasis on explaining:

- In which phase(s) are the functional safety requirements and the safety integrity level (SIL) requirements specified?

- Which phase(s) are handling the design and construction of a safety-critical system/SIS in accordance to these requirements?
- In which phase(s) is SIL verification carried out?
- Which phases and activities are needed to maintain the functional safety and safety integrity in the operational phase?

- It is reasonable to arrange the requirements according to the life-cycle approach, due to several reasons:
    - This gives a traceability from the definition of needs for protection and to the implementation and follow-up
    - It gives a logical structure in terms of sequence of activities
    - It gives the opportunity to define intermediate inputs and outputs to phases, to ensure ease the verification and validation at different points in time

  Note: Please add further explanations.

Problem 9.

(a) Examples of EUCs in a process facility are (assuming here an offshore platform): Wells including Xmas tree, pipeline, separation train (including one or more separators), compression train (or alternatively each unit separately, such as cooler, schrubber (vessel that removed water droplets), compressor).

(b) Multiple layer is about not placing "all the eggs in the same basket". Multiple layers (meaning multiple systems, including safety systems) can be tailor made to handle specific events: Process shutdown system (PSD) is tailor-made to act upon process upsets not managed by the control system. Emergency shutdown system is tailor-made to act upon more severe events, resulting from events that have not been properly managed by PSD (resulting in a overpressure and leakage), sudden events (pipe breakage due to corrosion), gas or fire detected automatically by fire and gas (F&G) detection system or by personnel at the plant etc. The level of severity calls for isolation of power to non-essential equipment to avoid escalation of the situation.

(c) Some examples of SISs were given in (b), PSD, ESD and F&G detection system. Other protection layers include control system (which is not a safety system in a process plant, but still a credible layer to manage hazards within the EUC).

(d) IEC 61508 must be used instead of IEC 61511 in the process industry in case of (i) need to qualify new elements and subsystems for use in safety-critical applications, and (ii) in the event where a SIL 4 requirement has been specified for a SIF. IEC 61511 is typically used to ensure safe integration of elements and subsystems already certified or with documented compliance to IEC 61508.

For this reason, manufacturers often apply IEC 61508, while end-users (who wants to integrated different products into a complete system) use IEC 61508.

Problem 10. Solution not yet available here, but relevant information is found in the text book.

Problem 11. Solution not yet available here, but relevant information is found in the text book.

Problem 12. Solution not yet available here, but relevant information is found in the text book.

Chapter 2

Concepts and requirements

Problem 1.

(a) The main attributes and interpretation of a SIF is described in Chapter 2.3 in the textbook. The main differences are:

- A SIS is the collection of hardware and software used to carry out one or (and more typically) several safety functions. The most practical way to define the bounardies of a SIS is to say that it contains all hardware and software connected to the logic solver, including sensors, final elements, human interface.
- A safety function carried out by a SIS is called safety *instrumented* function (SIF), since it is carried out by some instrumented technology (which may be used as an alternative term to denote electrical, electronic, programmable electronic (E/E/PE) technologies as well as hydraulics and pneumatics used to transmit signals or activated final elements).

(b) A SIS includes often many SIFs. Each SIF shall operate on specific demands, and often in different situations. It would therefore not be meaningful to e.g. sum up the reliability of all functions to get an overall reliability of somekind of superfunction of a SIS.

(c)

- Channel: A collection of a single or more elements which are all must operate in order to carry out a sub-function. A SIF is therefore not a channel, but each subsystem of a SIF can have one or more channels. A subsystem of pressure transmitters voted 1oo3 or 2oo3 both have three channels,

and each channel consists of a pressure transmitter. Each channel could be broken down to more elements, meaning that the pressure transmitter could have been spit into sensing line (if applicable), transmitter unit, and communication unit.

- Element is the smallest entity considered in a subsystem or system. What is the smallest depends on the purpose of the analysis. In the analysis of a SIS, we would normally consider a pressure transmitter, valve and logic solver as elements. However, in some situations it may be of interest to split e.g. valve into two elements: valve and actuator, or the logic solver into input card(s), central processing unit (CPU), and output card(s). It may be remarked that when a channel contains only one element, it does not matter whether we refer to them as channels or elements.
- Voted group is a way to characterize the arrangement of channels in a subsystem to carry out the safety function.
- Subsystem is a collection of one or more channels needed in order to carry out a subfunction in a SIF.

Problem 2. Solution not yet available here, but relevant information is found in the text book.

Problem 3. Solution not yet available here, but relevant information is found in the text book.

Problem 4. Solution not yet available here, but relevant information is found in the text book.

Problem 5. Solution not yet available here, but relevant information is found in the text book.

Problem 6. Solution not yet available here, but relevant information is found in the text book.

Problem 7. Solution not yet available here, but relevant information is found in the text book.

Problem 8. Solution not yet available here, but relevant information is found in the text book.

Problem 9.

(a) Safety integrity is *the probability that a SIS satisfactorily performs the specified SIFs under all stated conditions within a stated period of time* [IEC 61508]. From the definition it may be noted that it is a probabilistic statement about the functional capability of the SIS, and that there are specific conditions added (all stated conditions, within stated period of time). The safety integrity is therefore not something generic statement about performance, but linked to a particular condition and period.

(b) PFD_{avg} and PFH are the two reliability measures used. PFD_{avg} is a safety integrity measure for SISs operating in low demand mode (where the demand frequency is no higher than once a year). It measures the average probability (averaged over time) that the SIS is not able to perform the specified function due to dangerous failures. PFH is a safety integrity measure for SIS operating in high/continuous mode (where the demand frequency is higher than once a year). It measure the average frequency of dangerous failures per hour. Note that PFH (Probability of dangerous Failure per Hour) as a term has been kept from previous IEC 61508 version (1997), even if it denotes now an average failure frequency. The rational why PFH is a preferred measure against PFD_{avg} for SIS operating in high/continuous mode is that since the demand is so frequent, upon SIS failure (dangerously) the accident will most likely occur, i.e. too late to bring the EUC back to the safe state.

For a more specific description of the two measures, it is referred to Chapter 2.8 and chapter 7.5.

(c) IEC 61508 distinguishes between hardware safety integrity, software safety integrity, and systematic safety integrity. The standard requires quantitative measure for the hardware safety integrity through PFD/PFH together with architectural constraints (hardware fault tolerance and safe failure fraction). However, systematic failures, represented by software safety integrity and systematic safety integrity, are required to be addressed qualitatively through fulfilling the requirements set out by the standard. Hence, demonstrating the PFD_{avg} or PFH within the specified range of the SIL requirement, is just one out of several requirements that must be met. Each of these integrity measures represents a set of requirements that must be fulfilled in order to claim that a SIF meets a specified SIL requirement.

(d) There is no definite answer to explain why a four level classification scheme is

a suitable way of distinguishing different safety integrity levels. However, some issues of relevance to address are:

- It is meaningful to give both an upper constraint of how reliable we think that a SIF can be and lower constraint of how low the reliability of a SIF can be in order to use it for safety. So it makes sense to define a high and a low level.
- High level of safety integrity often means more complex safety-functions (such as e.g. more redundancy), or alternatively frequent testing. Using higher safety integrity level than necessary is therefore costly and not necessarily the safest approach. A risk analysis will define a level of safety integrity that is needed in light of other protection layers (SIS, other risk reducing measures) that are relevant for either preventing or mitigating the effects of an hazardous event.
- We may therefore conclude that more than two safety integrity levels are feasible, without having arguments to state that four is the best number.

(e) IEC 61511 gives several arguments why SIL 4 is not recommended, and it is recommended to visit IEC 61511, part 1, for this purpose:

- Such application should be rare, in light of common design principles such as layers of protection
- Systematic failures account for many SIS-related failures. It is doubted that it is possible to maintain a SIL 4 performance, even if "fault-free" at the start of life.
- IEC 61511 defines many specific and demanding requirements if a SIL 4 is defined for a SIF, despite it is being not recommended. It is also pointed back to IEC 61508: 11.5.2.2 in IEC 61511-1 says: "Components and subsystems selected for use as part of a safety instrumented system for SIL 4 applications shall be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate."

(f) A SIL requirement defines the required performance of the SIF, based on a risk analysis. SIL performance of a SIF is the "calculated" performance, meaning in this context:

- The demonstration that the target failure measure is within the specified SIL range for the SIF.

- That the architectural constraints are met.
- That requirements for avoidance and control with systematic failures are fulfilled (if the technology is not “proven”, and as such supported by evidence that also systematic failures are handled in a sufficient way)
- That requirements for application program development meet the requirements for software safety integrity at the level of the specified SIL.

Problem 10.

(a) Architectural constraints represent a set of requirements in the standard that restrict the freedom in how the system architecture may look like, in light of the SIL requirement. More specifically, it determines if you must include redundancy and with what voting, in light of the SIL requirement, maturity level/complexity of components, and the performance measure safe failure fraction (SFF). More information is found in Chapter 2.8.1 and chapter 7.

(b) One reason that has been mentioned is the need to have a balance between how much we can rely on probabilistic calculations and how much we should rely on “good engineering practice”. Applying the architectural constraints may, for a subsystem of a SIF, result in a need for a 1oo2 system (or 2oo3, rather than a single system even if the calculated PFD or PFH is within the range of the SIL requirement. The architectural constraints define a *minimum hardware fault tolerance*, meaning the minimum number of failures the system should tolerate without causing a SIF failure. A 1oo2 and a 2oo3 system has the same hardware fault tolerance.

(c) The information you need to determine the minimum HFT of a subsystem in a SIF is:

- SIL requirement of the SIF
- The safe failure fraction (SFF)
- The “complexity and novelty level” of the technology (as category A or B)

For example, SIL 4 cannot be claimed for a zero fault tolerance subsystem, no matter how low the PFD is, how high the SFF is and how "standard" the subsystem elements are. The maximum SIL that can be claimed with zero fault tolerance is SIL 3.

(d) The SFF may be interpreted as the probability that a failure does not impact the SIF, given that a failure has occurred. In this context, this means that

the failure is either safe (resulting in a safe state of the EUC) or dangerous detected (DD) meaning that it is immediately notified with an assumption of also immediate repair.

- As such, the SFF seems like a reasonable measure, and it may be reasonable that a high SFF require less hardware fault tolerance, for a given SIL requirement.
- A problem may be that a "push" for a high SFF may result in a high safe failure rate or high DD failure rate. This may impact the availability and nuisance for operators, which may also reduce the overall safety.
- The SFF is also a relative measure, and high failure rates and low failure rates may give the same SFF, as long as the fraction of S and DD to total failure rate is the same. See DOI:10.1016/j.ress.2008.06.003 for more information.

(e) It is first necessary to classify the pressure transmitters as type A or type B. Often, type B is selected due to the software included in the processing part of the sensor. It is also necessary to determine the SFF. You could for example visit exida webpages to look at some typical certificates for pressure transmitters or you can look at data sources where failure rates are provided, such as in the PDS data handbook from www.sintef.no/pds. With this information available, you can find the minimum hardware fault tolerance. To complete this example, you may want to just assume a SFF, for example 85%. For a type B subsystem with SIL 3 and SFF of 85%, the minimum HFT is 2.

Problem 11. Solution not yet available here, but relevant information is found in the text book.

Problem 12.

(a) Applicable methods are layers of protection analysis, (calibrated) risk graph, and minimum SIL-requirements. The latter method is not advocated in IEC 61508 or related standards, but is suggested in the Norsk Olje and Gass (NOG) Guideline 070. The guideline is available from http://www.norskoljeoggass.no/en/Publica/Guidelines/

(b) The description of the risk graph should include a presentation of the parameters C (consequence), F (probability of occurrence of hazardous event), P (probability of escaping, if the hazardous event occurs), W (demand rate/rate of

hazardous events) and entry points. The details of a risk graph can be seen from Fig. 2.1.

- Some pros:
  - Simple structure and easy to use, if calibrated
  - May be applicable in an early phase, to get a first indication of SIL requirement ("rough estimate")

  Some cons:
  - May be misused (non-calibrated risk graph used without further considerations)
  - Not so suitable when multiple protection layers available

In the response, you should elaborate somewhat further on the mentioned pros and cons

(c) The main attributes of a layers of protection analysis (LOPA) are:

- Applicable where multiple on-demand protection layers are used (rather than one) to reduce risk below the tolerable criteria
- Closely linked to the HAZOP, and should therefore be conducted after the HAZOP has been carried out
- Identifies available protection layers, and judge for each initiating cause whether or not the protection layer can be and how much it can be credited for risk reduction ("rules" are: (i) The initiating cause and the protection layer should be independent, so that the presence of an initiating cause does not impact the performance of the protection layer, (ii) The protection layers should be *relevant*, meaning that it is efficient (fast enough, is able to prevent or mitigate the effects of the initiating cause in question).
- Based on the intermediate event likelihood, determine if a new SIF is required in order to meet the tolerable risk criteria

Pros and cons:

- Pros:
  - Identifies the role of not one, but several protection layers in relation to specific initiating causes
  - Identifies assumptions made about applicable protection functions

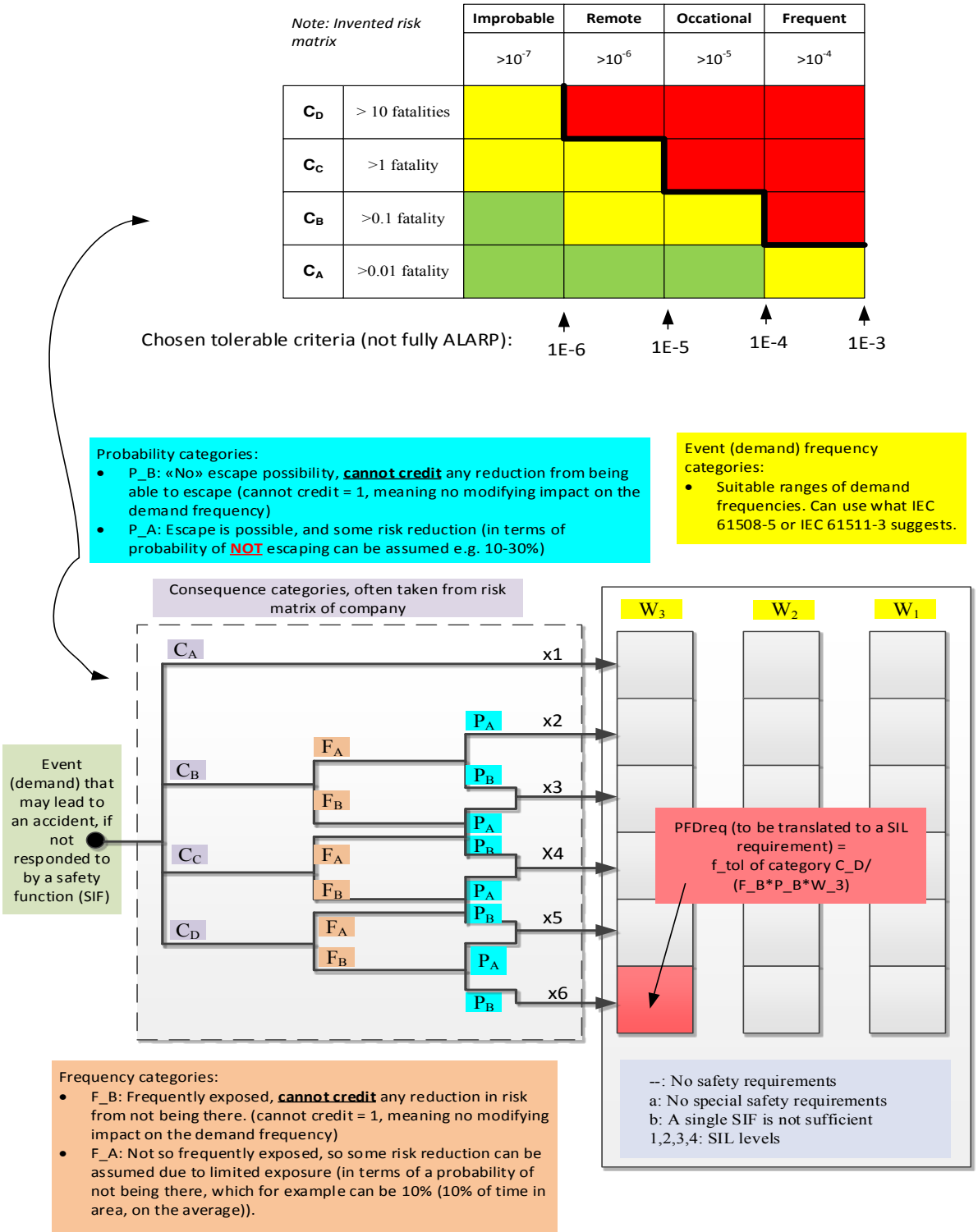


Figure 2.1: Details of a risk graph

Cons:

- Can give an impression of being very accurate (producing e.g. a PFD_{req} for a new SIF that is $xx.xxxx \cdot 10^{-x}$, but many assumptions have been made to come up with this number that may be more or less uncertain.
- Time consuming
- Requires a lot of details to be available about the process, type of events that can lead to accidents, and availability of protection layers.
- May encourage a split of necessary risk reduction to too many protection layers, some of which are safety-related and others that are not, and it may be challenging for the sharp end in operation (operators, maintenance personnel, engineers) to follow-up these and be able to respond as expected.

(d) Main difference is that IEC 61508 suggests a fully risk-based approach, whereas the NOG guideline bases minimum SIL requirements on the estimated performance of similar safety-functions, using collected field data for the industry (OREDA).

(e) The minimum SIL requirement for a particular SIF is deduced after having first calculated the PFD_{avg} for a similar SIF that has "proved" to give adequate performance. The proof is based on overall evaluation of this type of functions (based on operating experience, including review of reported failures for the components used for the functions). The calculated PFD_{avg} depends on (i) failure rates, which are mainly taken from OREDA data base (`www.oreda.com`, and (ii) a typical functional test interval for these type of functions. Of course, different operating companies may have different implementations of the functions, and different maintenance procedures, but they need to derive at a conclusion about what is most typical. Too conservative failure rates (and also very long test intervals) may give the odd effect that the PFD_{avg} becomes uncessarily high, and the SIL requirements may become too low (compared to the necessary risk reduction).

Problem 13. Solution not yet available here, but relevant information is found in the text book.

Problem 14. Solution not yet available here, but relevant information is found in the text book.

Cons.	$\mathbf{f}_{tol}$ (per year)	F	P	Entry point	$\mathbf{W}_3$	$\mathbf{W}_2$	$\mathbf{W}_1$	$\mathbf{W}_3$	$\mathbf{W}_2$	$\mathbf{W}_1$
C_A	1E-4	1	1	x1	E-4	1E-3	1E-2	SIL4	SIL3	SIL2
C_B	1E-5	0.1	0.3	x2	3.33E-4	3.33E-3	3.33E-2	SIL3	SIL2	SIL1
C_B	1E-5	0.1	1	x3	1E-4	1E-3	1E-2	SIL4	SIL3	SIL2
C_B	1E-5	1	0.3	x4	3.33E-5	3.33E-4	3.33E-3	SIL4	SIL3	SIL2
C_B	1E-5	1	1	x5	1E-5	1E-4	1E-3	b	SIL4	SIL3
C_C	1E-6	0.1	0.3	x6	3.33E-5	3.33E-4	3.33E-3	SIL4	SIL3	SIL2
C_C	1E-6	0.1	1	x7	1E-5	1E-4	1E-3	b	SIL4	SIL3
C_C	1E-6	1	0.3	x8	3.33E-6	3.33E-5	3.33E-4	b	SIL4	SIL3
C_C	1E-6	1	1	x9	1E-6	1E-5	1E-4	b	b	SIL4
C_D	1E-7	0.1	0.3	x10	3.33E-6	3.33E-5	3.33E-4	b	SIL4	SIL3
C_D	1E-7	0.1	1	x11	1E-6	1E-5	1E-4	b	b	SIL4
C_D	1E-7	1	0.3	x12	3.33E-7	3.33E-6	3.33E-5	b	b	SIL4
C_D	1E-7	1	1	x13	1E-7	1E-6	1E-5	b	b	b

Table 2.1: Calibrated SIL table

Problem 15. Solution not yet available here, but relevant information is found in the text book.

Problem 16. Solution not yet available here, but relevant information is found in the text book.

Problem 17.

(a) The rationales for the need to calibarate risk graph is discussed in the SIS textbook.

(b) The formula to find the required PFD (here denoted PFD_{req}) for each entry point j for the i^{th} consequence category (A, B, C or D) is:

$$\text{PFD}_{\text{req,jk}} = \frac{f_{tol,i}}{F_j \cdot P_j \cdot W_k} \tag{2.1}$$

where k is representing the demand categories 1,2 or 3.

For $\text{PFD}_{req} \leq 1E-5$, we assign a "b", and if $\text{PFD}_{req} \geq 1E-1$, we assign an "a". By doing so, the entry tables becomes as seen in Table 2.1.

Problem 18. Solution not yet available here, but relevant information is found

in the text book.

Problem 19.

(a) The given PFD_{avg} indicates a SIL 2 performance of the SIF.

(b) The given PFH indicates a SIL 2 also.

(c) If we know the PFD and the test frequency, it is possible to determine the DU failure rate used for the analysis using this formula:

$$\lambda_{DU} = \frac{\text{PFD}_{avg} \cdot 2}{\tau} = \frac{8.0 \cdot 10^{-4} \cdot 2}{2920 \text{ hours}} \approx 5.48 \cdot 10^{-7} \text{ per hour}$$

If we assume that the DU failure rate is applicable regardless of system being operated in the low-demand or high-demand mode, we could assume for a single system that PFH= $\lambda_{DU} \approx 5.48 \cdot 10^{-7}$ per hour.
This means that PFH is in the range of a SIL 2, while the PFD was in the range of SIL 3. This very simple example shows that SIL is not a design property of the system as such, but a property when design as well as mode of operation is taken into account.

(d) The target value is often set equal to the highest (upper) value of the target range of the SIL requirement. This is ok in theory, but considering the uncertainty associated with the calculation of PFD or PFH, it may be reasonable to select a lower value as the target value. Some companies have the policy to always choose the mid value of the target range. The most important thing is to be aware of the fact that PFD and PFH are not deterministic models, and give deterministic results. In one way or another, uncertainty should be addressed. Sensitivity analysis may be carried out to decide how the overall risk reduction is affected if the calculated reliability is higher than expected. If very sensitive to a specific SIF, it may be reasonable to select a lower target value for this one.

Problem 20. Solution not yet available here, but relevant information is found in the text book.

Problem 21.

(a) In case of a subsystem comprising identical items of type A and with SFF=92%, we allow single elements if the SIF has a SIL 3 requirement.

(b) In case of type B (and other assumptions as above), we need a HFT=1. This means that we could (typically) use configurations 1oo2 and 2oo3.

Problem 22. Solution not yet available here, but relevant information is found in the text book.

Chapter 3

Failures and Failure Analysis

Problem 1.
Solution not yet available here, but relevant information is found in the text book.

Problem 2.
Solution not yet available here, but relevant information is found in the text book.

Problem 3.
Solution not yet available here, but relevant information is found in the text book.

Problem 4.

(a) It is assumed that the pump is passive during normal operation, and shall start automatically or upon a manual request. The following failure modes are suggested:

- SU fault: Spurious start of fire water pump
- SD fault: Deviation in performance. Pump delivery slightly above the specified amount
- DD fault: Alarm on events or conditions that may result in fail to start up pump, such as low level alarm in diesel tank
- DU fault: Fail to start pump. Causes may be stuck contacts for start-up circuit, and perhaps manual valve in supply line to pump in closed position.

(b) A failure is said to be detected if it is revealed by automatic diagnostic testing in a short time after it occurs. Note that the time required to reveal the failure is important. (See Chapter 3.5.2)

(c) In this case, the pump is continuously running, and needs to stop upon the specified demand. In this case, a safe failure would be that the a spurious stop of the pump, while a dangerous failure would be to be unable to stop the pump.

(d) Measuring too low level would be dangerous if the level transmitter has a HH trip point. The actual level may lead to overflowing, without being detected. Measuring too high level would be dangerous if the level transmitter has a LL trip point. An unnoticed too low level may result in a gas blow-by from a separator into systems that are expecting liquids and not gases.

Problem 5.

(a) Random hardware failures/faults are explained in textbook, Chapter 3.5.4. It is specifically mentioned that a random hardware failure has three features:

- It applies to the hardware part of an item
- The failures occur random in time
- The probability distribution is used to express the effect of degradation on the time to failure, but may also be extended to include other failure causes.

A random hardware failure is therefore a physical failure, primarily caused by natural degradation.
It should be noted that a new recommended practise published by ISO on reliability analyses, ISO TR 12489, suggests the term “random failure” rather than “random hardware failure”. Their argument is that also some types of human errors are reoccuring, despite the effort made to avoid them. In this case, it is common to assume exponential distributed time to failure, as it is difficult to at least argue for degradations effects of human performance.

(b) The PDS method defines random hardware failures as hardware failures caused by aging. Human errors and excessive stresses are placed in the other failure category, i.e. systematic failures. Failure rates published by PDS (PDS data handbook) comprise random hardware failures as well as systematic failures. One reason or argument is that one of the main data sources used, the OREDA data, collects data for both failure categories, and the estimated failure rates in OREDA are not restricted to random hardware failures only.
See next question for systematic failure.

(c) Systematic failures are those failures that in theory is not reoccuring unless a specific condition apply. Guideline ISO TR 12489 defines a systematic fault as *failure that consistently occurs under particular conditions of handling, storage, or use*. Systematic failure is a category that covers software (software "bugs") and organizational and human errors, that eventually are manifested as a non-functional or damaged hardware.

Remark:The answer is not straightforward and there is no consensus about where excessive stress belongs to, either random hardware or systematic failure. In order to be a random hardware failure, the failure should occur (and reoccur) at random times, but this is not necesssarily the case. Excessive stresses are design issues and if items are designed (or corrected) to fit with the operating envelope, they can be avoided or eliminated. However, it is not straight forward to argue that excessive stress is a pure systematic failure because it is hard to differentiate aging and excessive stress due to their positive association (stress leads to wear, but what is wear beyond what is expected?). However, the fact that collected field date contains also failures due to excessive stress, it may be reasonable to belong them to random hardware failure.

Remark:It may be noted that a systematic failure is often a temporary loss of function. For example, a level transmitter that has been subject to wrong calibration is not damaged as such. After a re-calibration, the transmitter is functioning well again. A programming error in a software code does not cause any physical damage (at least in most cases), and the software (and associated hardware) will function correctly again once the programming error has been corrected. This is the reason why systematic faults are sometimes called non-physical fault or functional fault, even if these terms are not always valid.

(d) Yes, there are relationships between the two failure categories. In many cases, we may say that replicated systematic faults may be CCFs. The replication may be due to some coupling factors. If we extend the definition of random hardware failures to also include other failure causes than natural degradation, it is easier to understand why we treat CCFs as random hardware failures in our calculations, which is kind of contradictory in light of the faults being of a systematic nature.

(e) The classification of OREDA is discussed in the textbook, Chapter 3.5.9. It may be remarked that the category of critical failures may include safe as well as dangerous failures. For example, a premature closure and fail to close are both defined as critical failures in OREDA, but only the last one (fail to close) is dangerous if the valve is fail-safe closed.

Tag no	Proposed failure category	Remark
70-GD-01	DD	Alarm indicates detected by diagnostics
70-GD-008	NA	Test line is not used under demand, just for testing
70-GD-118	DU	Detected during PM/ regular test. Too low value means late detection
70-GD-004	DD	Alarm indicates detected by diagnostics
70-GD-001	DU	Detected during PM/regular test. Assumed to influence detection capability
70-GD-011	S	Alarm indicates detected by diagnostics. Assumed that dust is not critical to detection
70-GD-098	DD (or S)	Alarm indicates detected by diagnostics. This fault may be considered as systematic, as introducing better weather protection may fully remove recurrence of such faults
70-GD-026	S	Too high value is safe, as it would result in early (later than late) detection. However, the downside is chance of spurious activations, i.e. signal indicating that gas is present in the concentration corresponding to a dangerous situation while the gas concentration in reality is much lower.

Table 3.1: Proposed classification with remarks

Problem 6.

Solution not yet available here, but relevant information is found in the text book.

Problem 7.

(a) Classification may be as follows, see Table 3.1.

(b) Typical challenges are:

- You need to know quite a bit about the technology involved and its way of functioning, in this case the gas detection. As a reliability analyst, you may not have this knowledge. It is therefore important that you involve those disciplines that could supplement with the information needed for the classification: operators and or process engineers, personnel from the

automation discipline, personnel from mechanical department (in case of other technologies, like valves).

(c) Many of the faults seem to be of the type that is reoccurring. For example, dirty lenses may come from exposure from the environment, and will reoccur some time after last cleaning. In some cases, protection may be added, but this is not always possible. Placing the detector inside a box to avoid that it gets dirty could prevent it from being able to detect gas - at all or with delayed response.

Chapter 4

Testing and maintenance

Problem 1.

(a) Regular testing is more important for low-demand systems than for high-demand because:

- Faults that are introduced while there is no demand situation may remain undiscovered for a long time (i.e. till the next demand, which may be one or several years apart).
- It is also sufficient time to carry out repair of a failed item without having an unacceptable level of risk while the system is degraded or fully isolated while the repair is ongoing.
- In the high-demand mode, it is more likely that faults are discoved by a demand, and diagnostics and automatic response to fault conditions are therefore more critical design properties than for a low-demand system.

(b) It may be needed to introduce regular function testing of a high-demand system that has redundant channels, if the state of each channel is not reported during demand. For example, a 1oo2 system will always function as long as only one channel (of the two) is functioning. If we do not know the state of the other channel, we could think that everything is ok, but in reality the other channel has beed in the failed state for months and we are operating with a 1oo1 system instead of a 1oo2 system.

Problem 2.
Solution not yet available here, but relevant information is found in the text book.

Problem 3.

(a) Some differences between partial proof tests (using partial stroke testing of valves as exampole) and full proof tests, are:

- A partial proof test *may* be carried out without interfering with the operation of the EUC
- For the reason above, it is possible to carry out the partial test more often
- To ensure minor or no interference with the operaiton of the EUC, only some failure modes can be detected by the partial test

(b) Splitting a full proof test into several sub-tests may include testing of each sensor/detectors/transmitters (including calibration) as one type of test, testing of signaling from sensor to the logic solver as a second test, testing of output signals from logic solver to solenoid valve (without switching the solenoid valve) as a third test, and finally testing full closure of valves (including responsetime and leakage test) as a fourth test. The main reason is to cover the whole function, but at the same time avoid or reduce (to the extent possible) impact on operation of the EUC and coordinate resources efficiently. For example (in the latter case): It may be resource efficient to gather testing of all pressure transmitters at the process plant in a campaign like activity, and not limit testing of pressure transmitters to a specific SIF.

Problem 4.
Solution not yet available here, but relevant information is found in the text book.

Problem 5.
Solution not yet available here, but relevant information is found in the text book.

Problem 6.
Solution not yet available here, but relevant information is found in the text book.

Problem 7.
Solution not yet available here, but relevant information is found in the text book.

Problem 8.
Solution not yet available here, but relevant information is found in the text book.

Problem 9. Solution not yet available here, but relevant information is found in the text book.

Chapter 5

Reliability Quantification

Problem 1.
Solution not yet available here, but relevant information is found in the text book.

Problem 2.
Solution not yet available here, but relevant information is found in the text book.

Problem 3.
Solution not yet available here, but relevant information is found in the text book.

Problem 4.
Solution not yet available here, but relevant information is found in the text book.

Problem 5.
Solution not yet available here, but relevant information is found in the text book.

Problem 6.
Solution not yet available here, but relevant information is found in the text book.

Problem 7.

(a) The steady state equations for the Markov model of the 2oo3 voted system,

presented in Figure 5.18 in SIS textbook, are:

$$\begin{bmatrix} P_0 & P_1 & P_2 & P_3 \end{bmatrix} \begin{bmatrix} -3\lambda & 3\lambda & 0 & 0 \\ \mu_1 & -(\mu_1+2\lambda) & 2\lambda & 0 \\ \mu_2 & 0 & -(\mu_2+\lambda) & \lambda \\ \mu_3 & 0 & 0 & -\mu_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$$

and the fact that

$$P_0 + P_1 + P_2 + P_3 = 1$$

To reduce the calculation burden it is always wise to eliminate a column (equation) with the most number of non-zero transition rates, in this case the first column should be eliminated and the steady state equations will then be

$$\begin{aligned} &P_0 + P_1 + P_2 + P_3 = 1 \\ &3\lambda P_o - (\mu_1 + 2\lambda)P_1 = 0 \\ &2\lambda P_1 - (\mu_2 + \lambda)P_2 = 0 \\ &\lambda P_2 - \mu_3 P_3 = 0 \end{aligned}$$

Substitute (5) into (6)

$$\begin{aligned} &3\lambda(1 - P_1 - P_2 - P_3) - (\mu_1 + 2\lambda)P_1 = 0 \\ &3\lambda - 3\lambda P_1 - 3\lambda P_2 - 3\lambda P_3 - (\mu_1 + 2\lambda)P_1 = 0 \\ &3\lambda - (5\lambda + \mu_1)P_1 - 3\lambda P_2 - 3\lambda P_3 = 0 \end{aligned}$$

From (8),

$$P_2 = \frac{\mu_3}{\lambda} P_3$$

Substitute (10) into (7)

$$\begin{aligned} &2\lambda P_1 - (\mu_2 + \lambda)\frac{\mu_3}{\lambda} P_3 = 0 \\ \Rightarrow \quad &P_1 = \frac{(\mu_2 + \lambda)\mu_3}{2\lambda^2} P_3 \end{aligned}$$

Substitute (10) and (11) into (9)

$$\begin{aligned} 3\lambda - (5\lambda + \mu_1)\frac{(\mu_2 + \lambda)\mu_3}{2\lambda^2} P_3 - 3\lambda\frac{\mu_3}{\lambda} P_3 - 3\lambda P_3 = 0 \\ 3\lambda - (5\lambda + \mu_1)\frac{(\mu_2 + \lambda)\mu_3}{2\lambda^2} P_2 - 3\mu_3 P_3 - 3\lambda P_3 = 0 \\ 3\lambda = \left[\frac{(5\lambda + \mu_1)(\mu_2 + \lambda)\mu_3 + 6\mu_3\lambda^2 + 6\lambda^3}{2\lambda^2}\right] P_3 \end{aligned}$$

Rearranging the above equation gives what is stated in the book

$$P_3 = \frac{6\lambda^3}{6\lambda^3 + 11\lambda^2\mu_3 + 5\lambda\mu_2\mu_3 + \mu_1\mu_2\mu_3 + \lambda\mu_1\mu_3}$$

P_2 can easily be obtained by substituting (12) into (10)

$$\begin{aligned} P_2 &= \frac{\mu_3}{\lambda}\frac{6\lambda^3}{6\lambda^3 + 11\lambda^2\mu_3 + 5\lambda\mu_2\mu_3 + \mu_1\mu_2\mu_3 + \lambda\mu_1\mu_3} \\ &= \frac{6\lambda^2\mu_3}{6\lambda^3 + 11\lambda^2\mu_3 + 5\lambda\mu_2\mu_3 + \mu_1\mu_2\mu_3 + \lambda\mu_1\mu_3} \end{aligned}$$

Substitute (12) into (11)

$$\begin{aligned} P_1 &= \frac{(\mu_2 + \lambda)\mu_3}{2\lambda^2}\frac{6\lambda^3}{6\lambda^3 + 11\lambda^2\mu_3 + 5\lambda\mu_2\mu_3 + \mu_1\mu_2\mu_3 + \lambda\mu_1\mu_3} \\ &= \frac{3\lambda\mu_3(\mu_2 + \lambda)}{6\lambda^3 + 11\lambda^2\mu_3 + 5\lambda\mu_2\mu_3 + \mu_1\mu_2\mu_3 + \lambda\mu_1\mu_3} \end{aligned}$$

and finally P_0 can be calculated as follows:

$$\begin{aligned} P_0 &= 1 - (P_1 + P_2 + P_3) \\ &= 1 - \frac{3\lambda\mu_3(\mu_2 + \lambda) + 6\lambda^2\mu_3 + 6\lambda^3}{6\lambda^3 + 11\lambda^2\mu_3 + 5\lambda\mu_2\mu_3 + \mu_1\mu_2\mu_3 + \lambda\mu_1\mu_3} \\ &= \frac{-3\lambda\mu_3(\mu_2 + \lambda) + 5\lambda^2\mu_3 + 5\lambda\mu_2\mu_3 + \mu_1\mu_2\mu_3 + \lambda\mu_1\mu_3}{6\lambda^3 + 11\lambda^2\mu_3 + 5\lambda\mu_2\mu_3 + \mu_1\mu_2\mu_3 + \lambda\mu_1\mu_3} \\ &= \frac{\mu_3(2\lambda^2 + 2\lambda\mu_2 + \mu_1\mu_2 + \lambda\mu_1)}{6\lambda^3 + 11\lambda^2\mu_3 + 5\lambda\mu_2\mu_3 + \mu_1\mu_2\mu_3 + \lambda\mu_1\mu_3} \end{aligned}$$

The steady state equation for the 2oo3 architecture Markov model presented in *Figure 5.18* is

$$\begin{bmatrix} P_0 & P_1 & P_2 & P_3 \end{bmatrix} \begin{bmatrix} -(3\lambda_I + \lambda_C) & 3\lambda_I & 0 & \lambda_C \\ \mu_1 & -(\mu_1 + 2\lambda_I + \lambda_C) & 2\lambda_I & \lambda_C \\ \mu_2 & 0 & -(\mu_2 + \lambda) & \lambda \\ \mu_3 & 0 & 0 & -\mu_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$$

and

$$P_0 + P_1 + P_2 + P_3 = 1$$

Thus, by eliminating the first row we get

$$\begin{aligned} &P_0 + P_1 + P_2 + P_3 = 1 \\ &3\lambda_I P_0 - (\mu_1 + 2\lambda_I + \lambda_C)P_1 = 0 \\ &2\lambda_I P_1 - (\mu_2 + \lambda)P_2 = 0 \\ &\lambda_C P_0 + \lambda_C P_1 + \lambda P_2 - \mu_3 P_3 = 0 \end{aligned}$$

From (15)

$$P_1 = \frac{3\lambda_I}{\mu_1 + 2\lambda_I + \lambda_C} P_0$$

From (16)

$$\begin{aligned} P_2 &= \frac{2\lambda_I}{\mu_2 + \lambda} P_1 \\ &= \frac{6\lambda_I^2}{(\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C)} P_0 \end{aligned}$$

Thus From (14)

$$\begin{aligned} P_3 &= 1 - P_0 - P_1 - P_2 \\ &= 1 - P_0 - \frac{3\lambda_I}{\mu_1 + 2\lambda_I + \lambda_C} P_0 - \frac{6\lambda_I^2}{(\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C)} P_0 \\ &= 1 - \left[\frac{(\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C) + 3\lambda_I(\mu_2 + \lambda) + 6\lambda_I^2}{(\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C)} \right] P_0 \end{aligned}$$

From (17)

$$\begin{aligned} 0 &= \lambda_C P_0 + \frac{3\lambda_I \lambda_C}{\mu_1 + 2\lambda_I + \lambda_C} P_0 + \frac{6\lambda_I^2 \lambda}{(\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C)} P_0 - \mu_3 \\ &\quad + \mu_3 \left[\frac{(\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C) + 3\lambda_I(\mu_2 + \lambda) + 6\lambda_I^2}{(\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C)} \right] P_0 \end{aligned}$$

Therefore P_0 is

$$P_0 = \frac{\mu_3(\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C)}{\lambda_C(\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C) + 3\lambda_I\lambda_C(\mu_2 + \lambda) + 6\lambda_I^2\lambda + (\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C) + 3\lambda_I(\mu_2 + \lambda) + 6\lambda_I^2}$$

and P_1, P_2 and P_3 can be obtained by substituting P_0 into (18), (19) and (20) respectively:

$$P_1 = \frac{3\lambda_I\mu_3(\mu_2 + \lambda)}{\lambda_C(\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C) + 3\lambda_I\lambda_C(\mu_2 + \lambda) + 6\lambda_I^2\lambda + (\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C) + 3\lambda_I(\mu_2 + \lambda) + 6\lambda_I^2}$$

$$P_2 = \frac{6\lambda_I^2\mu_3}{\lambda_C(\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C) + 3\lambda_I\lambda_C(\mu_2 + \lambda) + 6\lambda_I^2\lambda + (\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C) + 3\lambda_I(\mu_2 + \lambda) + 6\lambda_I^2}$$

$$P_3 = 1 - \frac{\mu_3(\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C) + 3\mu_3\lambda_I(\mu_2 + \lambda) + 6\mu_3\lambda_I^2}{\lambda_C(\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C) + 3\lambda_I\lambda_C(\mu_2 + \lambda) + 6\lambda_I^2\lambda + (\mu_2 + \lambda)(\mu_1 + 2\lambda_I + \lambda_C) + 3\lambda_I(\mu_2 + \lambda) + 6\lambda_I^2}$$

The numerical results can be verified by substituting the transition rates in the formulas above.

(b) *System MTTF (Figure 5.18 in SIS textbook):* State 2 and 3 are defined as absorbing states where the system stays in failed state forever in the Markov process, i.e. $\mu_2 = \mu_3 = 0$. Thus, the Laplace transform of the state transition equation with the reduced transition rate matrix is:

$$\begin{bmatrix} P_0^*(s) & P_1^*(s) \end{bmatrix} \begin{bmatrix} -3\lambda & 3\lambda \\ \mu_1 & -(\mu_1 + 2\lambda) \end{bmatrix} = \begin{bmatrix} sP_0^*(s) - P_0(0), & sP_1^*(s) - P_1(0) \end{bmatrix} = \begin{bmatrix} sP_0^*(s) - 1, & sP_1^*(s) \end{bmatrix}$$

Where $P_i^*(s)$ is the Laplace transform of $P_i(t)$, and $sP_i^*(s) - P_i^*(0)$ is the time derivative of $P_i(t)$. Moreover, $P_i^*(0)$ is zero except the state where the system starts out, in this case state 1.
For $s = 0$, we have

$$\begin{aligned} -3\lambda P_0^*(0) + \mu_1 P_1^*(0) &= -1 \\ 3\lambda P_0^*(0) - (\mu_1 + 2\lambda) P_1^*(0) &= 0 \end{aligned}$$

Add the above two:

$$\begin{aligned} & \mu_1 P_1^*(0) - (\mu_1 + 2\lambda) P_1^*(0) = -1 \\ \Rightarrow \quad & P_1^*(0) = \frac{1}{2\lambda} \end{aligned}$$

and

$$P_0^*(0) = \frac{\mu_1 + 2\lambda}{6\lambda^2}$$

Therefore

$$\begin{aligned} \text{MTTF} &= P_0^*(0) + P_1^*(0) \\ &= \frac{\mu_1 + 5\lambda}{6\lambda^2} \end{aligned}$$

System MTTF (Figure 5.18 in SIS textbook) Here also state 2 and 3 defined as absorbing states and so the Laplace transform of the state transition equation with the reduced transition rate matrix is:

$$\begin{bmatrix} P_0^*(s) & P_1^*(s) \end{bmatrix} \begin{bmatrix} -(3\lambda_I + \lambda_C) & 3\lambda_I \\ \mu_1 & -(\mu_1 + 2\lambda_I + \lambda_C) \end{bmatrix} = \begin{bmatrix} sP_0^*(s) - 1, & sP_1^*(s) \end{bmatrix}$$

With $s = 0$, we have

$$\begin{aligned} -(3\lambda_I + \lambda_C) P_0^*(0) + \mu_1 P_1^*(0) &= -1 \\ 3\lambda_I P_0^*(0) - (\mu_1 + 2\lambda_I + \lambda_C) P_1^*(0) &= 0 \end{aligned}$$

Add the above two equations,

$$\begin{aligned} 1 &= (2\lambda_I + \lambda_C)P_1^*(0) + \lambda_C P_0^*(0) \\ P_1^*(0) &= \frac{1 - \lambda_C P_0^*(0)}{2\lambda_I + \lambda_C} \end{aligned}$$

Substitute this into one of the state equations

$$\begin{aligned} &-(3\lambda_I + \lambda_C)P_0^*(0) + \mu_1 \frac{1 - \lambda_C P_0^*(0)}{2\lambda_I + \lambda_C} = -1 \\ &(3\lambda_I + \lambda_C)(2\lambda_I + \lambda_C)P_0^*(0) + \mu_1 \lambda_C P_0^*(0) = 2\lambda_I + \lambda_C + \mu_1 \\ &P_0^*(0) = \frac{2\lambda_I + \lambda_C + \mu_1}{(3\lambda_I + \lambda_C)(2\lambda_I + \lambda_C) + \mu_1 \lambda_C} \\ &P_0^*(0) = \frac{2\lambda_I + \lambda_C + \mu_1}{6\lambda_I^2 + 5\lambda_I \lambda_C + \lambda_C \mu_1 + \lambda_C^2} \end{aligned}$$

Substitute $P_0^*(0)$ into (21)

$$\begin{aligned} P_1^*(0) &= \frac{1}{2\lambda_I + \lambda_C} - \lambda_C \left(\frac{2\lambda_I + \lambda_C + \mu_1}{6\lambda_I^2 + 5\lambda_I \lambda_C + \lambda_C \mu_1 + \lambda_C^2} \right) \left(\frac{1}{2\lambda_I + \lambda_C} \right) \\ &= \frac{6\lambda_I^2 + 5\lambda_I \lambda_C + \lambda_C \mu_1 + \lambda_C^2 - 2\lambda_C \lambda_I - \lambda_C^2 - \lambda_C \mu_1}{\left(6\lambda_I^2 + 5\lambda_I \lambda_C + \lambda_C \mu_1 + \lambda_C^2\right)(2\lambda_I + \lambda_C)} \\ &= \frac{3\lambda_I (2\lambda_I + \lambda_C)}{\left(6\lambda_I^2 + 5\lambda_I \lambda_C + \lambda_C \mu_1 + \lambda_C^2\right)(2\lambda_I + \lambda_C)} \\ &= \frac{3\lambda_I}{6\lambda_I^2 + 5\lambda_I \lambda_C + \lambda_C \mu_1 + \lambda_C^2} \end{aligned}$$

Therefore

$$\begin{aligned} \text{MTTF} &= P_0^*(0) + P_1^*(0) \\ &= \frac{5\lambda_I + \lambda_C + \mu_1}{6\lambda_I^2 + 5\lambda_I \lambda_C + \lambda_C \mu_1 + \lambda_C^2} \end{aligned}$$

MAPLE can also be used to solve the equation (the code is slightly differently composed than what was done in problem 8, but this is just an example of an alternative way to do the programming):

```
restart; with(LinearAlgebra) :

a01 := 4·(1 − beta)·lambda[DU];
a02 := 0;
a03 := 0;
a04 := beta·lambda[DU];
a00 := −(a01 + a02 + a03 + a04);

a10 := 1/(tau/2 + MRT);
a12 := 3·(1 − beta)·lambda[DU];
a13 := 0;
a14 := beta·lambda[DU];
a11 := −(a10 + a12 + a13 + a14);

a20 := 1/(tau/3 + MRT);
a21 := 0;
a23 := 2·(1 − beta)·lambda[DU];
a24 := beta·lambda[DU];
a22 := −(a20 + a21 + a23 + a24);

a30 := 1/(tau/4 + MRT);
a31 := 0;
a32 := 0;
a34 := lambda[DU];
a33 := −(a30 + a31 + a32 + a34);

a40 := 1/(tau/2 + MRT);
a41 := 0;
a42 := 0;
a43 := 0;
a44 := −(a40 + a41 + a42 + a43);

A := Matrix([[a00, a01, a02, a03, a04], [a10, a11, a12, a13,
    a14], [a20, a21, a22, a23, a24], [a30, a31, a32, a33, a34],
    [a40, a41, a42, a43, a44]]);

A[1..5, 1] := Matrix([[1], [1], [1], [1], [1]]);
A;
AT := Transpose(A);
B := Vector[row]([1, 0, 0, 0, 0]);
BT := Transpose(B);
P := LinearSolve(AT, BT) :
    # Colon instead of semi-colon hides the symbolic expression
PFD[avg, tot] := P[4] + P[5] :

#Table 7.2 data
```



```
lambda[DU] := 1E−6;
lambda[DD] := 6E−6;
tau := 8760;
beta := 0.10;
beta[D] := 0.05;
MRT := 10;
MTTR := 8;
```

Chapter 6

Reliability Data Sources

Problem 1. Solution not yet available here, but relevant information is found in the text book.

Problem 2. Using manufacturer data in reliability assessments in a design phase (compared to using generic data):

- some pros
  - Compared to generic data sources, the data provided by the manufacturer is specific to the specific equipment under consideration.
  - The data is based on good knowledge about the equipment (the physics of the equipment), and thus the qualitative description of failures is likely better.
- some cons
  - Different definition of failures, and different taxonomy
  - The failure rate is likely to be optimistic due to
    - Involvement of a business mindset
    - Unable to keep track of the equipment in the field
  - Manufacturers consider failures which they are accountable for, which excludes some failures that are due to human errors and excessive exposures during operation and maintenance.

Problem 3.
Solution not yet available here, but relevant information is found in the text book.

Problem 4.
Solution not yet available here, but relevant information is found in the text book.

Problem 5.

(a) Plant specific failure rate λ_P can be determine by adjusting the industry average failure rate λ_B using k influencing factors as

$$\lambda_P = \lambda_B \prod_{i=1}^{k} \omega_i \sigma_{c,i}$$

Where ω_i and $\sigma_{c,i}$ are the weight and score of the i^{th} influencing factor

- Weights measure the importance of the influencing factor for the failure rate. Some influencing factors have high impact (positively or negatively) to the failure rate than others.
- Scores measure how "good" (or "bad") the plant is compared to the average in the industry.

(b) The plant specific failure rate λ_P can be calculated as follows:

$$\begin{aligned} \lambda_P &= \lambda_B \prod_{i=1}^{k} \omega_i \sigma_{c,i} \\ &= 1.90E-06 \cdot (0.1 \cdot 1.0)(0.2 \cdot 1.5)(0.2 \cdot 0.9)(0.2 \cdot 1.2)(0.3 \cdot 1.2) \\ &= 2.24E-06 \text{ per hour} \end{aligned}$$

(c) The method in MIL-HDBK-217(F) uses a more sophisticated approach of incorporating influence factors than the method suggested by Brissaud et al.(2010). The method in MIL-HDBK-217(F) uses the proportional hazard model where influencing factors are the covariants. Therefore, the coefficient of each covariant measures its effect and importance to the industry average failure rate. Note that the weight of the influencing factors is determined by using the model (the "π-factors", which you will se if you google the handbook), as opposed to the Brissaud et al.(2010) approach in which the weights are determined by expert judgment.

Problem 6.
Solution not yet available here, but relevant information is found in the text book.

Chapter 7

Demand Mode and Performance Measures

Problem 1.
Solution not yet available here, but relevant information is found in the text book.

Problem 2.

(a) Two SIFs are involved in this situation: (i) Start firepumps upon detected fire and (ii) Continue supplying water during X hours. For (i), we can consider demand (fire) as a shock (fire was not here -> now the fire occured and we must start the fire pumps), while for (ii) the demand (fire) is continuously present and fire pumps, pipes and water supply must resist damage from fire during this period. Adequate risk reduction is not achieved if either of these two SIFs occur.

(b) The answer to this question is found in the textbook, chapter 2.

Problem 3.

(a) The safe failure fraction (SFF) is a measure calculated on the basis of the following failure rates: DU, DD, and S (considering the contribution from spurious failures only in the S category). The measure expresses the fraction of failure rates that is "safe" compared to the total failure rate, taking both S and DD failures into account as "safe" under the condition that DD failures are repaired within short time, or results in an automatic transition to a safe state.

(b) Yes. The SFF will most likely be differnet, as the what is regarded as safe and dangerous failures would be different. SFF is therefore a measure that MUST be

seen in relation to how the equipment is going to be used.

(c) SFF is a relative measure, meaning that it is the relative relationship between "safe" and total faliure rates that matters. This relationship may give high SFF with both low and high failure ratres, as long as the fraction of "safe" is much larger than the total failure rate.

(d) Some possible options for you as a designer:

- Introduce new diagnostic functions to detect dangerous failure modes. You may need to balance this effort with the new complexity added to the equipment.
- If the added complexity means that your equipment is reclassified from type A to type B, it may be that your equipment cannot longer operate as e.g. single in a SIL 3 function.
- You can re-design the equipment so that failures that used to be dangerous become safe. For example more fail-safe capability. However, as a designer you may need to consider the possible negative impact of spurious activations.
- You can investigate means to reduce the rate of occurence of DU failure modes.

Chapter 8

Average Probability of Failure on Demand

Problem 1.

- Failure modes are often classified as either safe (S) or dangerous (D). The two categories of failure modes are defined and explained in the book. It is further of interest to classify dangerous failures into dangerous *detected* (DD) or dangerous *undetected* (DU). These are further explained in the book. It is the DU failure modes that are the most important when calculating the PFD_{avg}. It should be noted, however, that some formulas for PFD_{avg} also include the contribution from DD failure modes, but their effects are usually negligible compared to the effect of DU failure modes.

- It may be remarked IEC 61508 restricts the calculation to the contribution from random *hardware* failures) that are included, while systematic failures (which may also be classified as DU, DD etc) are excluded as they do not follow any failure distribution. ISO TR 12489 suggests that random hardware failures may be supplemented by other random events, like some types of human errors. In this case, the term used is random failure rate, and not random *hardware* failure rate.

Problem 2.

(a) Formulas for the PFD_{avg} of a subsystem:

- The exact formula for PFD_{avg} is $1 - \frac{1}{\tau}\int_0^\tau R_S(t)dt$, where $R_S(t)$ is the survival function of the system.

– The survival function of a 1oo3 voted group of independent and identical channels is:

$$R_{\mathrm{S}} = 3e^{-\lambda_{DU}t} - 3e^{-2\lambda_{\mathrm{DU}}t} + 2e^{-3\lambda_{\mathrm{DU}}t}$$

Remark: Formulas can be obtained by using MAPLE or by hand calculation.

– The resulting $\mathrm{PFD}_{\mathrm{avg}}$ function becomes:

$$\mathrm{PFD}_{\mathrm{avg,exact}} = 1 + \frac{1}{6} \cdot \frac{2e^{-3\lambda_{DU}\tau} - 9e^{-2\lambda_{\mathrm{DU}}\tau} - 6\lambda_{\mathrm{DU}}\tau + 18e^{-\lambda_{\mathrm{DU}}\tau} - 6e^{-\lambda_{\mathrm{DU}}\tau} - 11}{\lambda_{\mathrm{DU}}\tau}$$

– For comparison, the approximation formula is (see text book):

$$\mathrm{PFD}_{\mathrm{avg,approx}} = \frac{(\lambda_{\mathrm{DU}}\tau)^3}{4}$$

(b) The calculated result using $\lambda_{\mathrm{DU}} = 1.9 \cdot 10^{-7}$ per hour and $\tau = 8760$ hours becomes:

$$\begin{aligned} \mathrm{PFD}_{\mathrm{avg,exact}} &\approx 1.102 \cdot 10^{-6} \\ \mathrm{PFD}_{\mathrm{avg,approx}} &\approx 1.153 \cdot 10^{-6} \end{aligned}$$

The $\mathrm{PFD}_{\mathrm{avg}}$ obtained by the approximation formula is seen to be slightly conservative, which is a desired property of an approximation formula.

Problem 3.

– The three typical subsystems of a SIF, the sensor (S) subsystem, the logic solver (LS) subsystem, and the final elements (FE) subsystem, are usually configured as a *series structure*. A dangerous SIF failure is an event where at least one of the three subsystems fail, hence a series structure.

– A suitable approach to calculate system failure is the upper bound approximation, where the average $\mathrm{PFD}_{\mathrm{avg}}$ is:

$$\mathrm{PFD}_{\mathrm{avg}} = 1 - \prod_{i \in [S,LS,FE]} \mathrm{PFD}_i$$

– For small values of PFD_i it is possible to verify that the same result is obtained by adding the PFD_i's of each subsystem. Example: Assume that

- $\mathrm{PFD}_{\mathrm{S}} = 2.5 * 10^{-3}$ for the sensor subsystem

- $\text{PFD}_{\text{LS}} = 2.2 * 10^{-4}$ for the logic solver subsystem
- $\text{PFD}_{\text{FE}} = 5.3 * 10^{-2}$ for the final elements subsystem

Then the PFD using upper bound approximation becomes:

$$\text{PFD}_{\text{avg}} = 1 - \prod_{i \in [S,LS,FE]} (1 - \text{PFD}_i) = 4.55 * 10^{-2}$$

while the PFD_{avg} by adding the PFD_i's becomes:

$$\text{PFD}_{\text{avg}} \approx \text{PFD}_{\text{S}} + \text{PFD}_{\text{LS}} + \text{PFD}_{\text{FE}} = 4.57 * 10^{-2}$$

As seen, the difference in result is negligible.

Problem 4.
Solution not yet available here, but relevant information is found in the text book.

Problem 5.
Solution not yet available here, but relevant information is found in the text book.

Problem 6.
Solution not yet available here, but relevant information is found in the text book.

Problem 7.
Solution not yet available here, but relevant information is found in the text book.

Problem 8.
Solution not yet available here, but relevant information is found in the text book.

Problem 9.
Solution not yet available here, but relevant information is found in the text book.

Problem 10.
Solution not yet available here, but relevant information is found in the text book.

Problem 11. Input data from Table 7.2 from the text book (all are in hour): $\lambda_{\text{DU}} = 1 \cdot 10^{-6}, \lambda_{\text{DD}} = 6 \cdot 10^{-6}, \tau = 8760, \beta = 0.1, \beta_{\text{D}} = 0.05$, MRT=10 and MTTR=8. Further $\lambda_D = \beta\lambda_{\text{DU}} + \beta_{\text{D}}\lambda_{\text{DD}} = 6.6 \cdot 10^{-6}$

(a)

$$\text{PFD}_{\text{avg}} = ((1-\beta)\lambda_{DU}\tau)^3 + \frac{\beta\lambda_{DU}\tau}{2} \approx 4.38 \cdot 10^{-4}$$

(b) The IEC 61508 formula for 2oo4 (based on equation 8.48 in the corrected version of the text book) is

$$\text{PFD}_{\text{avg}} = 24\lambda_D^3 \prod_{i=1}^{3}\left[\frac{\lambda_{\text{DU}}}{\lambda_{\text{D}}}\left(\frac{\tau}{i} + \text{MRT}\right) + \frac{\lambda_{\text{DD}}}{\lambda_{\text{D}}}\text{MTTR}\right] + \beta\lambda_{\text{DU}}(\frac{\tau}{2} + \text{MRT}) + \beta_{\text{D}}\lambda_{\text{DD}}\text{MTTR}$$

and based on the above input date, the average PFD will be $4.42 \cdot 10^{-4}$.

(c) A fault tree of a 2oo4 architecture gives four minimal cut sets with order three. Thus, the average probability of failure of a cut set with a correction factor (which is 4) is

$$q = 4 \cdot \left((1-\beta)\lambda_{\text{DU}}\left(\frac{\tau}{2} + \text{MRT}\right)\right)^3$$

Thus,

$$\text{PFD}_{\text{avg}} = 1 - (1-q)^4 + \frac{\beta\lambda_{\text{DU}}\tau}{2}$$

Substituting the input data gives an average PFD of $4.39{\cdot}10^{-4}$.

(d) Figure 8.1 shows the state transition diagram for a 2oo4 architecture. Since failures are undetected the repair rate is the inverse of the expected downtime. The assumption is that there is no constraint on the number of repair crew (or the repair time is the same regardless of the number of components found faulty during the test). The corresponding transition matrix is

$$\mathbb{A} = \begin{pmatrix} -4(1-\beta)\lambda_{\text{DU}} - \beta\lambda_{\text{DU}} & 4(1-\beta)\lambda_{\text{DU}} & 0 & 0 & \beta\lambda_{\text{DU}} \\ \frac{1}{\tau/2+\text{MRT}} & -\frac{1}{\tau/2+\text{MRT}} - 3(1-\beta)\lambda_{\text{DU}} - \beta\lambda_{\text{DU}} & 3(1-\beta)\lambda_{\text{DU}} & 0 & \beta\lambda_{\text{DU}} \\ \frac{1}{\tau/3+\text{MRT}} & 0 & -\frac{1}{\tau/3+\text{MRT}} - 2(1-\beta)\lambda_{\text{DU}} - \beta\lambda_{\text{DU}} & 2(1-\beta)\lambda_{\text{DU}} & \beta\lambda_{\text{DU}} \\ \frac{1}{\tau/4+\text{MRT}} & 0 & 0 & -\frac{1}{\tau/4+\text{MRT}} - \lambda_{\text{DU}} & \lambda_{\text{DU}} \\ \frac{1}{\tau/2+\text{MRT}} & 0 & 0 & 0 & -\frac{1}{\tau/2+\text{MRT}} \end{pmatrix}$$

Thus, the state equations are

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} P_0 & P_1 & P_2 & P_3 & P_4 \end{pmatrix} \cdot \mathbb{A} \tag{8.1}$$

and

$$P_0 + P_1 + P_2 + P_3 + P_4 = 1 \tag{8.2}$$

One of the state equations from eq. (8.1) must be eliminated to obtain a unique solution (here the first column is eliminated). Further, for bravery purpose each

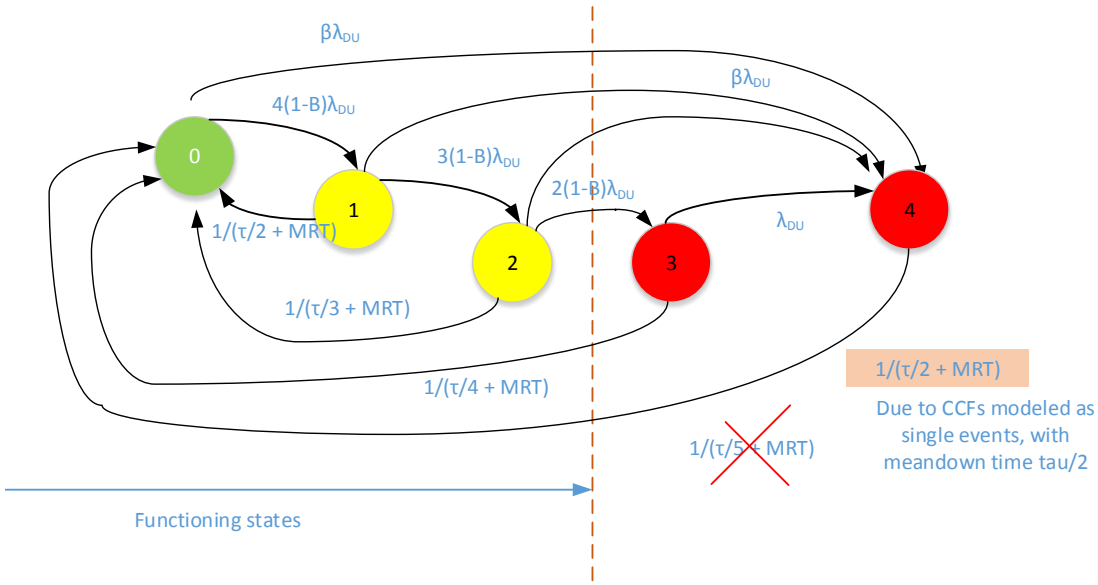


Figure 8.1: Markov model for a 2oo4

transition rates are represented by a single letter. Thus the combined state equations of eq. (8.1) and (8.2) is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} P_0 & P_1 & P_2 & P_3 & P_4 \end{pmatrix} \cdot \begin{pmatrix} 1 & a_0 & 0 & 0 & d_0 \\ 1 & a_1 & b_1 & 0 & d_1 \\ 1 & 0 & b_2 & c_2 & d_2 \\ 1 & 0 & 0 & c_3 & d_3 \\ 1 & 0 & 0 & 0 & d_4 \end{pmatrix}$$

We have

$$P_0 + P_1 + P_2 + P_3 + P_4 = 1 \tag{8.3}$$

$$a_0 P_0 + a_1 P_1 = 0 \Longrightarrow P_0 = -\frac{a_1}{a_0} P_1 \tag{8.4}$$

$$b_1 P_1 + b_2 P_2 = 0 \Longrightarrow P_2 = -\frac{b_1}{b_2} P_1 \tag{8.5}$$

$$c_2 P_2 + a_3 P_3 = 0 \Longrightarrow P_3 = -\frac{c_2}{c_3} P_2 = \frac{c_2 b_1}{c_3 b_2} P_1 \tag{8.6}$$

$$d_0 P_0 + d_1 P_1 + d_2 P_2 + d_3 P_3 + d_4 P_4 = 0 \tag{8.7}$$

Eq. (8.3) and (8.7) can be rewritten as

$$\left(-\frac{a_1}{a_0}+1-\frac{b_1}{b_2}+\frac{c_2 b_1}{c_3 b_2}\right)P_1+P_4=1$$
$$\left(-d_0\frac{a_1}{a_0}+d_1-d_2\frac{b_1}{b_2}+d_3\frac{c_2 b_1}{c_3 b_2}\right)P_1+d_4 P_4=0$$

Thus,

$$\begin{aligned} P_1 &= \frac{d_4}{d_4\left(-\frac{a_1}{a_0}+1-\frac{b_1}{b_2}+\frac{c_2 b_1}{c_3 b_2}\right)-\left(-d_0\frac{a_1}{a_0}+d_1-d_2\frac{b_1}{b_2}+d_3\frac{c_2 b_1}{c_3 b_2}\right)} \\ P_4 &= 1-\left(-\frac{a_1}{a_0}+1-\frac{b_1}{b_2}+\frac{c_2 b_1}{c_3 b_2}\right)P_1 \end{aligned}$$

Substituting the input data in the equations above gives $P_0 = 9.84 \cdot 10^{-1}, P_1 = 1.54 \cdot 10^{-2}, P_2 = 1.21 \cdot 10^{-4}, P_3 = 4.78 \cdot 10^{-7}, P_4 = 4.39 \cdot 10^{-4}$. Therefore, $\text{PFD}_{\text{avg}} = P_3 + P_4 = 4.39 \cdot 10^{-4}$.

As can be observed all methods provide very similar results. Two reasons can be mentioned: first is the dominance of the CCF (and the fact that CCF modeling is the same across methods) and second is the negligibility of the restoration time of DD failures compared to the test interval. Significant difference among the methods may be expected if this were not the case.

Problem 12.
No solution prepared.

Problem 13.
No solution prepared.

Problem 14.

(a) The approximation formula for a 2oo4 voted system may be used here.

$$\text{PFD}_{\text{avg}} = (\lambda_{DU}\tau)^3 \approx 2.31 \cdot 10^{-4}$$

Two interpretations of PFD_{avg} are commonly used (and they are both important depending on the application):

- The PFD_{avg} is the average probability that the SIF fails to perform in response to a demand in a test interval. If the test interval is kept unchanged, it may be assumed that the average probability of failure applies at any point in time.

- PFD_{avg} is the mean fractional downtime (in a test interval) where the SIF is unavailable (meaning not able to respond if a demand occurs).

(b)

- The PFD_{avg} for the 2oo4 voted group with CCF can be calculated as

$$\text{PFD}_{\text{avg}} = ((1-\beta)\lambda_{DU}\tau)^3 + \frac{\beta\lambda_{DU}\tau}{2} \approx 3.23 \cdot 10^{-3}$$

- The approximation formula for a 2oo3 is.

$$PFD_{avg,approx} = ((1-\beta)\lambda_{DU}\tau)^2 + \frac{\beta\lambda_{DU}\tau}{2} \approx 6.11 \cdot 10^{-3}$$

  The 2oo4 voting group is about 90% safer than the 2oo3 voting group, however, if considering the range of a SIL requirement, they would both be within the range of a SIL 2 (assuming that no other contributions to the total PFD of the SIF).

- The following points are among the relevant points that need to be considered:

  - At first glance, it may seem reasonable to suggest the 2oo4 system with the lowest PFD. However, introducing four sensors means that the system complexity increases (installation wise), and the forth sensor means additional testing compared to the 2oo3 system. When we know that many dangerous failures are introduced during a test (e.g., wrong calibration, lack of proper re-installation after test and so on), it may be questioned if the 2oo4 system is so much safer.
  - A 2oo3 system tolerates only one DU failure, while the 2oo4 tolerates two DU failures. This means that the 2oo4 is more fault tolerant. The reliability of the 2oo3 may be enhanced by introducing an alarm on deviating readings from the three sensors (making it less likely that two or more dangerous failures are left unattended).
  - Both configurations have the same level of defense against spurious failures (meaning that two spurious signals are needed in order to have false/unintended activation of the SIF). Yet, the 2oo4 voting group is highly susceptible than the 2oo3 (i.e. 3 possibilities in 2oo3 versus 6 possibilities in 2oo4).

(c)

- The beta factor model splits the failure rate of a component into two parts, one independent failure rate and one dependent (or CCF) failure rate with the fraction β

  $$\lambda = \lambda^{(i)} + \lambda^{(c)}$$

  where

  $$\beta = \frac{\lambda^{(c)}}{\lambda}$$

  If we set up the equation for conditional probability, we get:

  $$\begin{aligned} \Pr(\text{CCF}|\text{a failure}) &= \frac{\Pr(\text{CCF and failure})}{\Pr(\text{a failure})} \\ &= \frac{1 - e^{-\beta\lambda t}}{1 - e^{-\lambda t}} \\ &\approx \frac{\beta\lambda t}{\lambda t} = \beta \end{aligned}$$

- The following points are relevant to mention:
  - The beta factor model may be considered as a lethal shock model, where an exposure (a common cause) results in the simultaneous failure of all affected components. The realism in this model is influenced by how likely it is that the components in question will face this type of exposure, at all, or if such exposure will dominate compared to other exposures.
  - The beta factor covers a number of different common causes of failure. As such, we may find that it is too conservative to assume that the SIF fails in the presence of any such event.
  - If a set of redundant components are exposed to high temperature, we may assume that they will degrade over time and the failures may occur at very different points in time. In this case, we may find the beta factor model to be too conservative since sufficient time may be available to correct the failure before the next one appears.
  - If the same components are exposed to an electrical shock or a replicated calibration error, this may result in immediate failure, and the beta factor may be a suitable representation of the phenomena of CCFs.
- As seen in Fig. 10.1, the curve is linear as the contribution from CCF is dominating, i.e. PFD_{avg} is related almost linearly to β with slop $\lambda_{DU}\tau/2$.

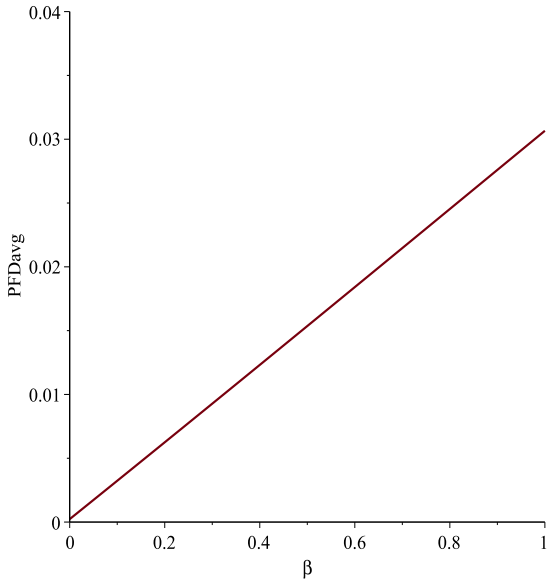


Figure 8.2: Sketch of PFD_{avg} as a function of β.

(d) Let C_i denote an event that a component survives a test interval τ. This means that $\Pr(C_i) = Pr(T > \tau) = R(\tau)$. These events (for i=1....) are independent with the same probability of occurring p (with $p = R(\tau)$). The number of test intervals (called Z here) passing until the component fails the first time has a geometric distribution with point probability:

$$\Pr(Z = z) = Pr(C_1 \cap C_2 \cap \ldots \cap C_z \cap \bar{C}_{z+1}) = p^z(1-p)$$

for $z = 0, 1, \ldots$ Note that $\bar{C}_{z+1}$ denote the event where the component fails in the $z+1$ interval. The mean number of test intervals becomes:

$$E(Z) = \sum_{z=0}^{\infty} z \cdot Pr(Z = z) = \frac{p}{1-p} = \frac{R(\tau)}{1-R(\tau)} \tag{8.8}$$

The survival function for a 2oo4 configuration without considering CCFs is:

$$R_{S,2oo4,I} = 6e^{-2\lambda_{DU}t} - 8e^{-3\lambda_{DU}t} + 3e^{-4\lambda_{DU}t}$$

This equation may be simplified with taylor expansion (second order). The survival function for a 2oo4 configuration when CCFs are included is:

$$R_{S,2oo4,CCF} = 6e^{-(2-\beta)\lambda_{DU}t} - 8e^{-(3-2\beta)\lambda_{DU}t} + 3e^{-(4-3\beta)\lambda_{DU}t}$$

The simplification with taylor expansion is shown here (but only with first order, which is possible here).

$$\begin{aligned} R_{S,2oo4,CCF} &\approx 6(1-(2-\beta)\lambda_{DU}t) - 8(1-(3-2\beta)\lambda_{DU}t) + 3(1-(4-3\beta)\lambda_{DU}t) \\ &= (6-8+3) - (-12+24-12)\lambda_{DU}t + (-6-16+9)\beta\lambda_{DU}t \\ &= 1 - 13\beta\lambda_{DU}t \end{aligned}$$

By inserting $\lambda_{DU} = 7.0 \cdot 10^{-6}$ (failures/hour) and $\tau = 8760$ hours into the above equations and using equation (8.8), we get E(Z) = 1243 intervals for when CCFs are not considered and 148 intervals when CCFs are considered. The result can also be found by using Maple, see code in Fig. 8.3.

Remark:The impact of CCFs is as expected significant for the results. But is the realism in the result questionable? How likely is it that failures being part of a CCF would occur within the same test interval? Is the beta factor model overly conservative? No definite answer is formulated here, but these are questions that may be relevant to address when looking into the details of CCF models.

(e) When $E(Z)$ is known, it is possible to calculate the time from the component is put into operation till the first failure, here called mean time to failure (TTF):

$$E(TTF_S) = \tau E(Z) + (\tau - E(D_1|X_S(\tau) = 0)) \tag{8.9}$$

where D_1 is the downtime and $X(\tau) = 0$ is the state where the system has failed. By using double expectations, it may be shown that:

$$E(D_1) = E(D_1|X_S(\tau) = 0) \cdot \Pr(T < \tau) = E(D_1|X_S(\tau) = 0) \cdot F(\tau)$$

By also knowing that $E(D_1) = \int_0^\tau F(t)dt$, we get the result that:

$$E(D_1|X_S(\tau) = 0) = \frac{1}{F(\tau)} \int_0^\tau F(t)dt = \frac{1}{F(\tau)}\tau - \frac{1}{F(\tau)} \int_0^\tau R(t)dt \tag{8.10}$$

By inserting (8.10) into (8.9) while knowing that $E(Z) = \frac{R(\tau)}{F(\tau)}$, we find that

$$E(TTF_S) = \frac{1}{1-R(\tau)} \int_0^\tau R(t)dt$$

We illustrate how the integral part with CCF can be calculated as follows, respectively. For the independent part (excluding CCFs) it is not shown, but instead programmed using Maple®:

$$\begin{aligned} \int_0^\tau R(t)dt &\approx \int_0^\tau (1 - 13\beta\lambda_{DU}tdt \\ &= \tau - \frac{13}{2}\beta\lambda_{DU}\tau^2 \end{aligned}$$

```
restart; #CCFs are not included!
R[s, "2oo4"I] := 6/exp(lambda[DU]·tau)^2
    - 8/exp(lambda[DU]·tau)^3 + 3/exp(lambda[DU]·tau)^4;
lambda[DU] := 7·10^-6;
tau := 8760;
R[s, "2oo4"] := eval(R[s, "2oo4"]);
EZ[I] := R[s, "2oo4"I]/(1 - R[s, "2oo4"I]);
convert(EZ[I], float, 5);
```

```
restart; #CCFs are included
R[s, "2oo4"CCF] := 6·exp(beta·lambda[DU]·tau)/exp(lambda[DU]·tau)^2
    - 8·exp(beta·lambda[DU]·tau)^2/exp(lambda[DU]·tau)^3
    + 3·exp(beta·lambda[DU]·tau)^3/exp(lambda[DU]·tau)^4;
lambda[DU] := 7·10^-6;
tau := 8760;
beta := 0.10;
R[s, "2oo4"] := eval(R[s, "2oo4"]);
EZ[CCF] := R[s, "2oo4"CCF]/(1 - R[s, "2oo4"CCF]);
convert(EZ[CCF], float, 5);
```

Figure 8.3: Maple code to find the mean number of test intervals passing before first system failure

```
restart;
restart; #CCFs are not included! ;
lambda[DU] := 7·10^-6;
tau := 8760;
R[s, "2oo4"I] := 6/exp(lambda[DU]·t)^2
    - 8/exp(lambda[DU]·t)^3 + 3/exp(lambda[DU]·t)^4;
R[integr, I] := int(R[s, "2oo4"I], t = 0 ..tau);
R[s, "2oo4"I] := eval(R[s, "2oo4"I], t = tau);
#R[s, integr, I] := eval(R[integr, I]);
ETTF := 1/(1 - R[s, "2oo4"I]) · R[integr, I];
hours := convert(ETTF, float, 5);
years := hours/8760;
```

```
restart;
restart; #CCFs are included! ;
lambda[DU] := 7·10^-6;
tau := 8760;
beta := 0.10;
R[s, "2oo4"CCF] := 6·exp(beta·lambda[DU]·tau)/exp(lambda[DU]·tau)^2
    - 8·exp(beta·lambda[DU]·tau)^2/exp(lambda[DU]·tau)^3
    + 3·exp(beta·lambda[DU]·tau)^3/exp(lambda[DU]·tau)^4;
R[integr, CCF] := int(R[s, "2oo4"CCF], t = 0 ..tau);
R[s, "2oo4"CCF] := eval(R[s, "2oo4"CCF], t = tau);
ETTF[CCF] := 1/(1 - R[s, "2oo4"CCF]) · R[integr, CCF];
hours[CCF] := convert(ETTF[CCF], float, 5);
years[CCF] := hours[CCF]/8760;
```

Figure 8.4: Total time passing until first failure occur of system

By inserting $\lambda_{DU} = 7.0 \cdot 10^{-6}$ (failures/hour) and $\tau = 8760$ hours into the the above equations, we get $E(TTF_S)$ equal to $1.095 \cdot 10^7$ hours (which is 1250 years when CCFs are not considered and $1.299 \cdot 10^6$ hours when the contribution from CCFs are included (corresponding to approximately 148 years). See Fig. 8.4 for using Maple to calculate the result.

Problem 15.

(a)

- The probability that component survives a failure mode (denoted event E) is assuming exponentially distributed time to failure is:

$$\Pr(E) = \Pr(T > t) = e^{-\lambda_{DU} t}$$

  If we assume that more than one failure mode(each failure mode assigned a failure rate $\lambda_i, i = 1, 2...$ could occur and that these are independent, we get:

$$\Pr(E_1 \cap E_2 \cap ...) = \Pr(E_1) \cdot \Pr(E_2)... = e^{-(\lambda_1 + \lambda_2..)t}$$

  This means that the probability of surviving six months (4320 hours) is:

$$Pr(T > 6 \cdot 4320) = e^{-(2.4 \cdot 10^{-6} + 3.5 \cdot 10^{-6})4320} \approx 0.975$$

- The MTTF is defined as:

$$MTTF = \int_0^\infty R(t)dt$$

  where R(t) was given in task (a). The result becomes:

$$MTTF = \int_0^\infty e^{-(\lambda_{DU} + \lambda_{SU})t} dt = \frac{1}{\lambda_{DU} + \lambda_{SU}} \approx 1.695 \cdot 10^5 \text{hours}$$

- If the failure modes are to be considered independent, the *failure causes* must be independent. A dangerous failure mode of a gas detector could be that it has been located in the wrong position or that the detector has been calibrated wrongly so that the sensitivity is too low. The latter failure cause "calibration error" could in principle resulted in too high sensitivity also, if the calibration procedure is not fully understood by the technician. As such, one may question if the failure modes are truely independent in all respect.

  (b)

- The PFD_{avg} is (when inserting $\tau = 6$ months (4320 hours) and $\lambda_{DU} = 2.4 \cdot 10^{-6}$ failures per hour):

$$\text{PFD}_{avg} \approx \frac{\lambda_{DU}\tau}{2} = 5.18 \cdot 10^{-3}$$

- The average PFD has two interpretations: (i) it denotes the average unavailability of a safety function (or component) in a test interval due to the presence of DU failures. (ii) it denotes the average/mean probability that a safety function (or component) fail to perform its intended function(s), if a demand occurs. It may be remarked for (i) that if the test interval is not changed over a time period, the average unavailability is the same over the whole period.

- The number of hours in a year (8760 hours) being unprotected (called t_up here) is calculated as:

$$t_{up} = PFD_{avg} \cdot 8760 \text{ hours} \approx 45.4 \text{ hours}$$

(c)

- The survial functions may be set up with basis in the structure function. The alternative used here is to consider the subsystem as a binominal situation where:
  - Four components operate independently of each othe
  - A demand occurs, and each component gets the opportunity to respond (in total 4 trials, one for each component)
  - The probability is the same for all trials, and given by the survial function of a single component ($p(t) = R_s(t) = e^{-\lambda_{DU}t}$

  The system survives if the number 3 or all 4 components are able to perform their intended functions. This gives:

$$\begin{aligned} R_s(t) &= \sum_{i=3}^{4} \binom{n}{i} (e^{-\lambda_{DU}t})^i (1 - e^{-\lambda_{DU}t})^{4-i} \\ &= 4e^{-3\lambda_{DU}t} - 3e^{-4\lambda_{DU}t} \end{aligned}$$

  This can be found by hand or by using Maple®.

– The PFD_{avg} may be calculated as:

$$\begin{aligned} PFD_{avg} &= 1 - \frac{1}{\tau}\int_0^{\tau} R_s(t)dt \\ &= 1 - \frac{1}{12}\frac{9e^{-4\lambda_{DU}t} - 16e^{-3\lambda_{DU}t} + 7}{\lambda_{DU}\tau} \end{aligned}$$

This can be found by hand (for the patent ones) or by using Maple®. Inserting $\tau = 6$ months (4320 hours) and $\lambda_{DU} = 2.4 \cdot 10^{-6}$, we get:

$$PFD_{avg} \approx 2.11 \cdot 10^{-4}$$

For comparison you may use the approximation formula for a 3oo4 system directly, and in this case you will find that $\text{PFD}_{\text{avg}} \approx 2.15 \cdot 10^{-4}$ (which is a slightly higher value, and therefore conservative).

Remark:It is ok to just solve this question by using approximation formula.

(d)

– The β may have two interpretations: (i) it denotes the fraction of all the failures (in total or for a particular failure mode) of a component in a redundant configuration that are CCFs, and (ii) the conditional probability that a failure of a component in a redundant configuration is a CCF.

– In this case, it would be possible to calculate the PFD_{avg} using approximation formulas, when the CCF is modelled as a virtual block in the reliability block diagram. It should be remarked that we split the failure rate into two parts: the independent part with failure rate $(1-\beta)\lambda_{DU}$ and the CCF part with failure rate $\beta\lambda_{DU}$. The formula would then be:

$$PFD_{avg} = 2((1-\beta)\lambda_{DU})\tau)^2 + \frac{\beta\lambda_{DU}\tau}{2}$$

Inserting $\tau = 6$ months (4320 hours) and $\lambda_{DU} = 2.4 \cdot 10^{-6}$, we get $\text{PFD}_{\text{avg}} \approx 5.97 \cdot 10^{-4}$. The more cumbersome approach would be to determine the exact formula for PFD_{avg}. For the those who would like to use Maple®or similar, may want to verify the following result:

$$\begin{aligned} PFD_{avg} &= 1 - \frac{1}{\lambda_{DU}(2\beta-3)(3\beta-4)\tau}\Big[12\beta e^{(2\beta-3)\lambda_{DU}\tau} \\ &- 6\beta e^{(3\beta-4)\lambda_{DU}\tau} \\ &- 16e^{(2\beta-3)\lambda_{DU}\tau} + 9e^{(3\beta-4)\lambda_{DU}\tau} - 6\beta + 7\Big] \end{aligned}$$

By inserting the same values of the paramters, we get $\text{PFD}_{\text{avg}} \approx 5.93 \cdot 10^{-4}$.

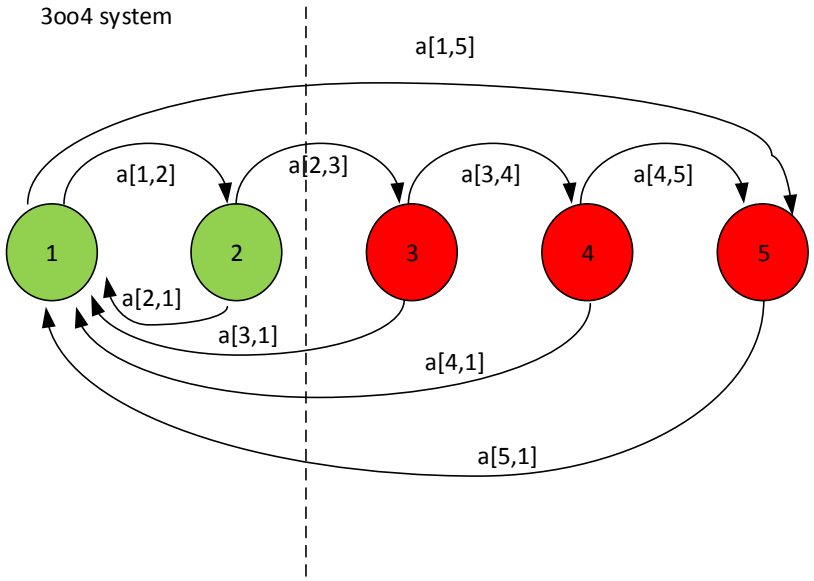


Figure 8.5: Markov state model for a 3oo4 system

- Here, Chapter 10 in textbook may be visited. Key words to include in the discussion are:
  - Simpllicity of the model
  - Degree of being a realistic
  - Possibility to be supported by data
  - Degree of being accepted by the realibility analysts community

(e) The 3oo4 system is sketched in Fig. **??**, and the transition rates are provided in the table below.

The failure states are state 3, 4 and 5, and the average PFD can be found by adding the steady state probabilities of these states. MAPLE®has been used to solve for these probabilities. The result became $5.82 \cdot 10^{-4}$, which is slightly lower than the PFD calculated with basis in the approximation formulas.

Remark:: In this problem, we have set one month equal to 720 hours. However, an alternative can also be to set it equal to 730 hours. Note the transition rate from state 5 to state 1, where the mean downtime for CCFs have been chosen. An alternative could be to add a new state 6 to treat the CCFs, but it has been

Transition rate	Explanation
$a[1,2] = 4 \cdot (1-\beta)\lambda_{DU}$	
$a[2,3] = 3 \cdot (1-\beta)\lambda_{DU}$	
$a[3,4] = 2 \cdot (1-\beta)\lambda_{DU}$	
$a[4,5] = \lambda_{DU}$	
$a[1,5] = \beta\lambda_{DU}$	
$a[5,1] = \mu_4 = \frac{1}{\mathrm{MDT_4}}$	$\mathrm{MDT_4} \approx \frac{\tau}{2}$
$a[4,1] = \mu_3 = \frac{1}{\mathrm{MDT_3}}$	$\mathrm{MDT_3} \approx \frac{\tau}{4}$
$a[3,1] = \mu_2 = \frac{1}{\mathrm{MDT_2}}$	$\mathrm{MDT_2} \approx \frac{\tau}{3}$
$a[2,1] = \mu_1 = \frac{1}{\mathrm{MDT_1}}$	$\mathrm{MDT_1} \approx \frac{\tau}{2}$

checked that the result is not much affected from the simplification made in this solution.

Problem 16.

(a) *IEC 61508 formulas:* These formulas are explained in chapter 8 of the text book. The needed formulas are as follows:

$$\begin{aligned}
\mathrm{PFD_{avg}} &= 2 \cdot ((1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_{\mathrm{D}}) \cdot \lambda_{\mathrm{DD}})^2 t_{\mathrm{GE}} t_{\mathrm{CE}} \\
&+ \beta\lambda_{\mathrm{D}} t_{\mathrm{CE1}} + \beta_{\mathrm{d}}\lambda_{\mathrm{D}} t_{\mathrm{CE2}}
\end{aligned}$$

where:

$$\begin{aligned}
t_{\mathrm{CE}} &= \frac{\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}(\frac{\tau}{2} + \mathrm{MRT}) + \frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}}\mathrm{MTTR} \\
t_{\mathrm{GE}} &= \frac{\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}(\frac{\tau}{3} + \mathrm{MRT}) + \frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}}\mathrm{MTTR} \\
t_{\mathrm{CE1}} &= \frac{\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}(\frac{\tau}{2} + \mathrm{MRT}) \\
t_{\mathrm{CE2}} &= \frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}}\mathrm{MTTR}
\end{aligned}$$

All notations are as used in the text book. One small distinction from the text book is, however, the use of independent failure rates ($\lambda^{()}_{\mathrm{DU}}$, $\lambda^{()}_{\mathrm{DD}}$, and $\lambda^{()}_{\mathrm{D}}$) in $\mathrm{t_{CE}}$ and $\mathrm{t_{GE}}$ rather than the total failure rates.
By inserting the failure rates, and assuming that $\beta = \beta_{\mathrm{d}}$ and MTR=MTTR, the $\mathrm{PFD_{avg}}$ becomes $1.14 \cdot 10^{-2}$.

PDS-formulas: The PDS approach is to treat the unavailability due to DU failures, referred to as $\mathrm{PFD_{avg}}$, and other type of downtime, referred to as downtime

unavailability (DTU) due to repair of dangerous failures (DTU_R) and DTU due to the test itself (DTU_T). All these contributions are added in what is referred to as the critical safety unavailability (CSU):

$$\begin{aligned} PFD_{\text{avg}} &= \frac{(\lambda_{\text{DU}}\tau)^2}{3} + \frac{\beta\lambda_{\text{DU}}\tau}{2} \\ DTU_{\text{R}} &= 2\lambda_{\text{D}} \cdot MTTR \cdot \lambda_{\text{DU}} \cdot \tau/2 \text{ (Note 1)} \\ DTU_{\text{T}} &= MRT \cdot \lambda_{\text{DU}} \text{ (Note 2)} \\ CSU &= PFD_{\text{avg}} + DTU_{\text{R}} + DTU_{\text{T}} \end{aligned}$$

Note 1: The underlying assumption is that the system is degraded to 1oo1 in the presence of a repair, and the unavailability is influenced by the probability of having one additional failure while repairing the first failure.
Note 2: The underlying assumption is that one component is tested at a time.

By inserting the failure rates, and assuming that $\beta = \beta_{\text{d}}$ and MTR=MTTR, the PFD_{avg} becomes $1.26 \cdot 10^{-2}$ (insignificantly higher result than what the IEC 61508 formulas gave).

Markov: The markov transition diagram is shown in Fig 8.6. Observe that effort is made to reduce the number of states in order to make it tractable. The corresponding transition matrix is

$$\mathbf{A} = \begin{pmatrix} -2(1-\beta)\lambda_{\text{DU}} - 2(1-\beta)\lambda_{\text{DD}} - \beta\lambda_{\text{DU}} & 2(1-\beta)\lambda_{\text{DU}} & 2(1-\beta)\lambda_{\text{DD}} & \beta\lambda_{\text{DU}} \\ \left(\frac{\tau}{2} + \text{MRT})\right)^{-1} & -\left(\frac{\tau}{2} + \text{MRT})\right)^{-1} - \lambda_{\text{D}} & 0 & \lambda_{\text{D}} \\ (\text{MTTR})^{-1} & 0 & -(\text{MTTR})^{-1} - \lambda_{\text{D}} & \lambda_{\text{D}} \\ \left(\frac{\lambda_{\text{DU}}}{\lambda_{\text{D}}}(\frac{\tau}{3} + \text{MRT}) + \frac{\lambda_{\text{DD}}}{\lambda_{\text{D}}}\text{MTTR}\right)^{-1} & 0 & 0 & -\left(\frac{\lambda_{\text{DU}}}{\lambda_{\text{D}}}(\frac{\tau}{3} + \text{MRT}) + \frac{\lambda_{\text{DD}}}{\lambda_{\text{D}}}\text{MTTR}\right)^{-1} \end{pmatrix}$$

Thus, the state equations are

$$\begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} P_1 & P_2 & P_3 & P_4 \end{pmatrix} \cdot \mathbb{A} \tag{8.11}$$

and

$$P_1 + P_2 + P_3 + P_4 = 1 \tag{8.12}$$

Remark:: It would also be ok to split state 4 into two states, one for two DU failures and one for two DD failures.

The maple code for implementation (when not having split into two states) is shown below. The results using Maple becomes $\text{PFD}_{\text{avg}} = P_4 = 1.20 \cdot 10^{-2}$ which is slightly higher than the result using approximation formulas. (This may be due to having merged two states (2DU) and 2 DD) into one (2 DU or 2 DD).

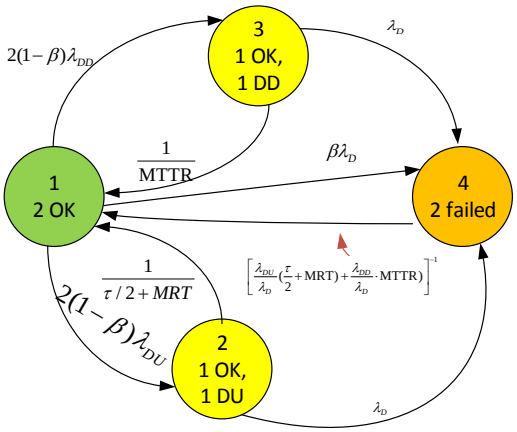


Figure 8.6: Markov model for the 1oo2 fire pump system

(b) We assume now that one pump alone can provide enough water supply (thereby a 1oo2 system). What we then want to calculate here is the probability that both fire pumps fail during the 8 hours required running time, using a DU failure rate that is 10 times higher than in standby/passive mode of operation. The probability that at least one pump survives a specified time, here set to 8 hours:

$$\Pr(T < 8 \text{ hours}) \quad \approx \quad (1 - 2e^{-10\lambda_D \cdot 8}) + 2e^{-(2-\beta)10\lambda_D \cdot 8})$$

Inserting values given, gives $\Pr(T < 8 \text{ hours}) \approx 6.72 \cdot 10^{-4}$.

(c) We here denote the frequency of fires (demands) as λ_d and the frequency of critical events as *HEF*. A critical event occurs if there is a fire and the fire pumps do not start *or* they start, but do not provide the specified amount of water during the prescribed 8 hours. From this rationale, the the frequency of critical events may be found as follows:

$$\text{HEF} \approx \lambda_d(\text{PFD}_{\text{avg}} + \Pr(T < 8))$$

where PFD_{avg} was calculated in task (a) (result using IEC 61508 formula has been used here) and $\Pr(T < 8)$, and $\lambda_d \approx 5.7 \cdot 10^{-5}$ per hour. This gives (we here se-

```
> restart;
  with(linalg) :
  size := 4; #Number of states
  A := array(sparse, 1 ..size, 1 ..size); #Transition matrix
  e := array(sparse, 1 ..size);

  #Definition of input data;
  lambda[DU] := 3.0·10^-5;
  lambda[DD] := 5.0·10^-5;
  lambda[D] := lambda[DU] + lambda[DD];
  tau := 6·730;
  MRT := 8;
  MTTR := 8;
  beta := 0.10;

  # Entering non-zero transitions (except diagonal values and zeros)
  mu[DU] := (lambda[DU]/lambda[D] · (tau/2 + MRT))^-1;
  mu[DD] := (lambda[DD]/lambda[D] · MTTR)^-1;
  mu[DUDD] := (lambda[DU]/lambda[D] · (tau/3 + MRT) + lambda[DD]/lambda[D] · MTTR)^-1;

  A[1, 2] := 2·(1 − beta)·lambda[DU];
  A[1, 3] := 2·(1 − beta)·lambda[DD];
  A[1, 4] := beta·lambda[D];
  A[2, 1] := mu[DU];
  A[2, 4] := lambda[D];
  A[3, 1] := mu[DD];
  A[3, 4] := lambda[D];
  A[4, 1] := mu[DUDD];
  # Remark: =0's do not need to be defined


  #Filling in the diagonal values:
  for i to size do
  s := 0 :
  for j to size do
  s := s + A[i, j]
  od;
  A[i, i] := −s
  od;

  #Preparing for using linsolve to find steady state
  Atran := transpose(A);
  for i to size do Atran[size, i] := 1 od;
  e[size] := 1;
  p := linsolve(Atran, e);
```

Figure 8.7: Maple code for solving for PFD

lected result using IEC 61508 formula) $\text{PFD}_{\text{avg}} = 6.89 \cdot 10^{-7}$ per hour.

We can also calculate the HEF by using Markov. The extended Markov transition diagram is shown in Fig 8.8. The HEF frequency is found by

$$\text{HEF} = P_4(\infty) \cdot \lambda_d + P_5(\infty) \cdot 10 \cdot \lambda_D + P_6(\infty) \cdot \beta \cdot 10\lambda_D$$

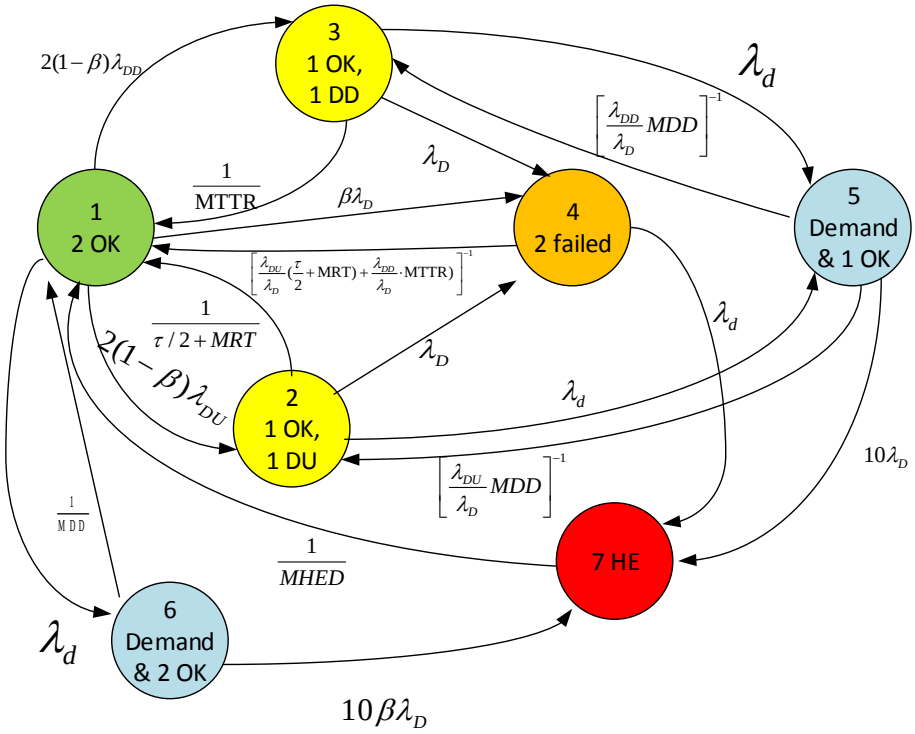


Figure 8.8: Markov model for the 1oo2 fire pump system to compute HEF

The following notations have been used:

- MDD: Mean demand duration, set equal to 8 hours
- MHED: Mean hazardous event duration (set equal to three months, but this contribution is nevertheless negligible)
- λ_d: Demand rate (per hour)

The HEF calculated on the basis of Markov has here been done using Maple (see fig.8.9).

```
restart;
with(linalg) :
size := 7; #Number of states
A := array(sparse, 1 ..size, 1 ..size); #Transition matrix
e := array(sparse, 1 ..size);

#Definition of input data:
lambda[DU] := 3.0·10^-5;
lambda[DD] := 5.0·10^-5;
lambda[D] := lambda[DU] + lambda[DD];
tau := 6·730;
MRT := 8;
MTTR := 8;
beta := 0.10;
MDD := 8; #hours
MHED := 3·730; #3 months
lambda[d] := 1/(2·8760);

# Entering non-zero transitions (except diagonal values
    and zeros)
mu[DU] := ((tau/2 + MRT))^-1;
mu[DD] := (MTTR)^-1;
mu[DUDD] := (lambda[DU]/lambda[D]·(tau/2 + MRT)
    + lambda[DD]/lambda[D]·MTTR)^-1;

A[1, 2] := 2·(1 − beta)·lambda[DU];
A[1, 3] := 2·(1 − beta)·lambda[DD];
A[1, 4] := beta·lambda[D];
A[1, 5] := 0;
A[1, 6] := lambda[d];
A[1, 7] := 0;
A[2, 1] := mu[DU];
A[2, 4] := lambda[D];
A[2, 5] := lambda[d];
A[2, 6] := 0;
A[2, 7] := 0;
A[3, 1] := mu[DD];
A[3, 4] := lambda[D];
A[3, 5] := lambda[d];
A[3, 6] := 0;
A[3, 7] := 0;
A[4, 1] := mu[DUDD];
A[4, 5] := 0;
A[4, 6] := 0;
A[4, 7] := lambda[d];
A[5, 2] := (lambda[DU]/lambda[D]·MDD)^-1;

A[5, 3] := (lambda[DD]/lambda[D]·MDD)^-1;
    #Should be a equivalent downtime, but I did not correction
A[5, 7] := 10·lambda[D];
A[6, 1] := 1/MDD;
A[6, 7] := beta·10·lambda[D];
A[7, 1] := 1/MHED;
# Remark: =0's do not need to be defined


#Filling in the diagonal values:
for i to size do
s := 0 :
for j to size do
s := s + A[i, j]
od;
A[i, i] := −s
od;

#Preparing for using linsolve to find steady state
Atran := transpose(A);
 for i to size do Atran[size, i] := 1 od;
 e[size] := 1;
 p := linsolve(Atran, e);

HEF := p[4]·lambda[d] + p[6]·beta·10·lambda[D] + p[5]·10
    ·lambda[D]
```

Figure 8.9: Maple code for the 1oo2 fire pump system to compute HE

The resulting HEF is $\approx 6.8 \cdot 10^{-7}$ per hour. The analytical approach resulted in HEF equal to $\approx 6.9 \cdot 10^{-7}$ per hour. The two approaches give therefore about the same result.

Remark:It may be remarked that the mean equivalent downtime used to determine the transition rate from state 4 to state 1 is based on a single failure event (CCF event) and not two independent failures. State 4 could have been split into two separate states, to treat both type of transitions.

Problem 17.

(a)

- The reliability block diagram becomes (see Fig. 8.10)
- The minimal cut sets are:
  $\{PT_1, P_T2, PT_3\}, \{PT_1, PT_2, PT_4\}, \{PT_1, PT_3, PT_4\}, \{PT_2, PT_3, PT_4\}, \{LS\}, \{ESDV_1, ESDV_2\}$

(b)

- The MTTF of a single component is the reciprocal of the failure rate. If we want to find the MTTF_{DU}, we get:
  $$MTTF_{DU} = \frac{1}{\lambda_{DU}} = 4.00 \cdot 10^5 \text{hours} \approx 45.7 \text{years}$$
- The probability that both valves survive a test interval is:
  $$\Pr(T > 8760) = e^{-2 \cdot 2.5 \cdot 10^{-6} \cdot 8760} \approx 0.957$$
- The probability that an S failure occurs before DU failure is solved by considering conditional probabilities: Consider two events A and B. Then:
  $$\Pr(A|B) = \frac{\Pr(B)}{\Pr(A \bigcap B)}$$
  If event A is that an S failure occurs, and B is the event where a failure (S or DU) occurs, we get:
  $$\begin{aligned} \Pr(\text{S|DU or S is present }) &= \frac{1 - e^{-\lambda_S t}}{1 - e^{-(\lambda_{DU} + \lambda_S)t}} \\ &\approx \frac{\lambda_S t}{(\lambda_{DU} + \lambda_S)t} \\ &= \frac{\lambda_S}{\lambda_{DU} + \lambda_S} \end{aligned}$$

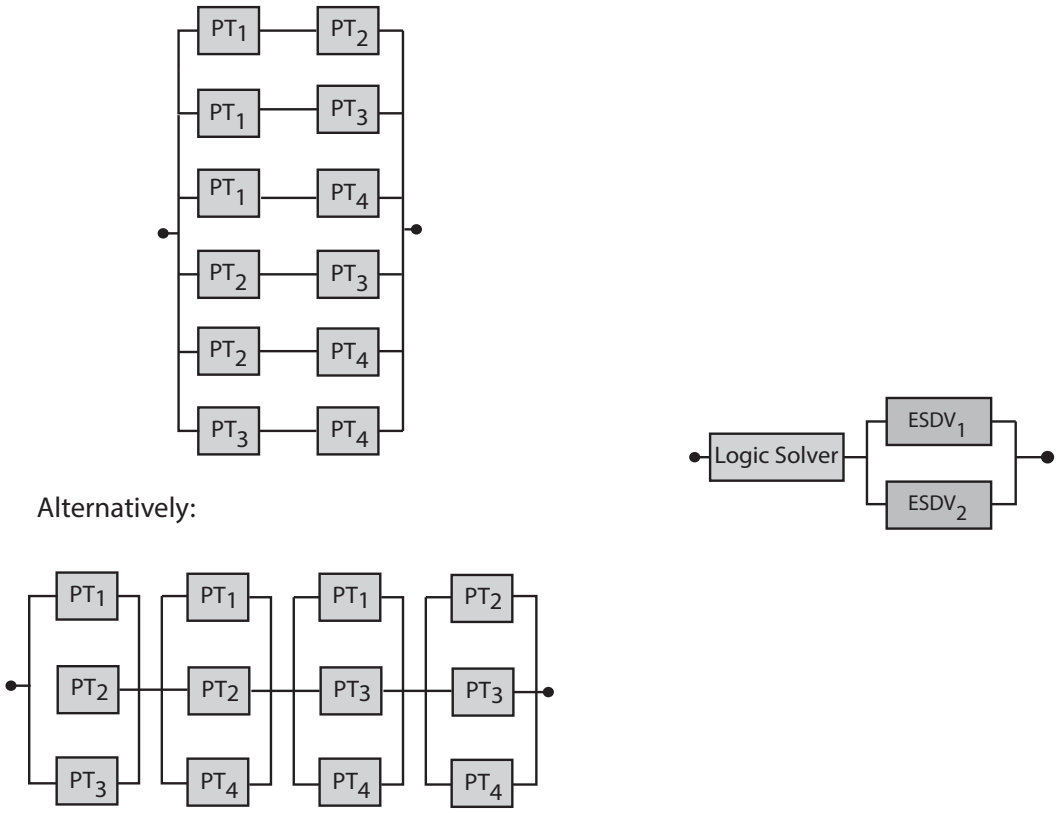


Figure 8.10: Reliablity block diagram for SIS (two alternatives for PTs)

By inserting the failure rates we get 0.55, i.e. it is 55% probability that a S failure occurs before a DU failure.

(c)

- A pressure transmitter normally send a 4-20mA signal corresponding to a pressure within the range of the transmitter readings. Zero pressure would normally correspond 4 mA and 20mA to the maximum readable value in the range of the transmitter (it should be noted that some setup are made inverse, so that zero pressure corresponds to 20mA). The comparison with a set point is then made in the logic solver, along with the voting setup of the transmitter system. If the transmitter is used to detect a HIGH pressure, we may define a DU failure as:
  - Transmitter sends a too low value (mA) compared to the pipeline pressure

  It should be noted that no signal from the detector or a signal outside the range (<4mA or >20mA) would be a dangerous failure, but it is detected by the diagnostic checks in the logic solver. Using digital communication for the pressure transmitters (instead of analogue) would place many of the diagnostic functions (e.g. out of range) in the pressure transmitter itself. A DU failure would still be a too low value transmitted, but the underlying causes of this DU failure would be more complex than for the analogue set up.
  A Safe failure (considering analogue transmission) and high pressure set-point, may be:
  - Transmitter sends a too high value (mA) compared to the pipeline pressure
- A 2oo4 system will survive if two components survive, three components survive and four components survive the time interval mentioned. By considering the binominal situation, we get:

$$\begin{aligned} \Pr(T > t) &= R_s(t) = \sum_{i=2}^{4} \binom{n}{i} (e^{-\lambda_{PT} t})^i (1 - e^{-\lambda_{PT} t})^{4-i} \\ &= 6e^{-2\lambda_{PT} t} - 8e^{-3\lambda_{PT} t} + 3e^{-4\lambda_{PT} t} \end{aligned}$$

  with $\lambda_{PT} = \lambda_{PT,DU} + \lambda_{PT,S}$. By inserting the failure rates and time period of interest, we find that the probability is 0.999.

– We may use the approximation formula directly for a 2oo4 voted group $\text{PFD}_{\text{avg,approx}} = (\lambda_{DU}\tau)^3$. The exact analytical formula can be obtained by first finding the survival function and then integrating for an average. The survival function was already found in equation (8.13) (but remember to replace the failure rate in this formula with the DU failure rate). The exact formula for PFDavg is (using here Maple®):

$$PFD_{avg,exact} = 1 + \frac{1}{12\lambda_{PT,DU}\tau}\left[9e^{-4\lambda_{PT,DU}\tau} - 32e^{-4\lambda_{PT,DU}\tau} + 36e^{-2\lambda_{PT,DU}\tau}\right]$$

By inserting the failure rates and test interval, we get $\text{PFD}_{\text{avg,approx}} = 1.81 \cdot 10^{-8}$ and $\text{PFD}_{\text{avg,exact}} = 1.73 \cdot 10^{-8}$.

– The following assumptions apply when calculating PFD_{avg}:

  – The main contributor to unavailability is DU failures (some formulas also include DD failures, but its contribution is often negligible)
  – The components are subject to regular testing (often denoted by test interval τ)
  – During the test, *all* failures are revealed
  – The system is restored to "an as good as new condition" after the test
  – No *new* failures are introduced during the test
  – $\lambda_{DU}\tau < 0.01$ (assumption apply when using the analytical approximation formulas

(d)

– The PFD_{avg} of the system (or more precisely, the function) is equal to the sum of the PFD_{avg} of the individual subsystems (provided that PFD_{avg} is small). The formulas and the results are presented in Table 8.1. Note that a test interval of 1 year (8760 hours) has been used :

Table 8.1: PFD of system.

Subsystem	Formula	Faiure rate (per hour)	result
Pressure transmitters (2oo4)	$(\lambda_{PT,DU}\tau)^3$	$\lambda_{PT,DU} = 3.0 \cdot 10^{-6}$	$1.81 \cdot 10^{-8}$
Logic solver (1oo1)	$\frac{\lambda_{LS,DU}\tau}{2}$	$\lambda_{LS,DU} = 7.0 \cdot 10^{-7}$	$3.07 \cdot 10^{-3}$
Valves (1oo2)	$\frac{(\lambda_{ESDV,DU}\tau)^2}{3}$	$\lambda_{ESDV,DU} = 2.5 \cdot 10^{-6}$	$1.60 \cdot 10^{-4}$
		Total:	$3.23 \cdot 10^{-3}$

- The following assumptions apply when calculating PFD_{avg} of the system:
  - On the subsystem level, the same assumptions as in problem (c) apply.
  - The PFD_{avg} of each subsystem is small ($\approx< 0.01$) so that the PFD_{avg}'s may be added (the correct approach would have been to calculate the $PFD_{\text{avg,syst}} = 1 - (1 - PFD_{\text{avg,PTs}})(1 - PFD_{\text{avg,LS}})(1 - PFD_{\text{avg,ESDVs}})$.

(e)

- It is here assumed that we are only considering the contribution from the subsystem of the pressure transmitters. In this case, a spurious trip of the SIS occurs if two or more spurious signals are received by the logic solver. The approximation formula for this situation is (see Chapter 12 in textbook):

$$STR_{SIS} = 4\lambda_{S,PT}(1 - e^{-3\cdot\lambda_{S,PT}MTTR_S}) \approx 12\lambda_{S,PT}^2 MTTR$$

  where $MTTR_S$ is the repair time (2 hours). Inserting the failure rate gives $\text{STR}_{\text{SIS}} = 2.0 \cdot 10^{-10}$ failures/hour.

- The number of S failures (n) during a 10 year period, caused by the pressure transmitters, is:

$$n = 10 \cdot 8760 \cdot STR_{SIS} \approx 0.0000175$$

  which means that 1-2 spurious trips are expected once every 1 million years (which is what we may define as rare). No spurious trip should therefore occur during the 10 year period

(f)

- The PFD_{avg} of the system (or more precisely, the function) is equal to the sum of the PFD_{avg} of the individual subsystems (provided that PFD_{avg} is small). The formulas and the results are presented in Table 8.2. Note that a test interval of 1 year (8760 hours) and $\beta_{PT} = 0.25$. Note that the result does not change so much in this case, as the most dominant contributor is the single component, the logic solver.

- It is here assumed that we are only considering the contribution from the subsystem of the pressure transmitters. In this case, contribution from CCFs will dominate. The analytical formula for this situation is:

$$STR_{SIS} = 12\lambda_{S,PT}^2 MTTR + \beta\lambda_{S,PT}$$

  where $MTTR_S$ is the repair time (2 hours). Inserting the failure rate and $\beta = 0.25$ gives $\text{STR}_{\text{SIS}} = 1.25 \cdot 10^{-6}$ failures/hour.

Table 8.2: PFD of system.

Subsystem	Formula	Faiure rate (per hour)	result
Pressure transmitters (2oo4)	$\frac{\beta\lambda_{DU,PT}\tau}{2}$	$\lambda_{PT,DU} = 3.0 \cdot 10^{-7}$	$1.31 \cdot 10^{-4}$
Logic solver (1oo1)	$\frac{\lambda_{LS,DU}\tau}{2}$	$\lambda_{LS,DU} = 7.0 \cdot 10^{-7}$	$3.07 \cdot 10^{-3}$
Valves (1oo2)	$\frac{(\lambda_{ESDV,DU}\tau)^2}{3}$	$\lambda_{ESDV,DU} = 2.5 \cdot 10^{-6}$	$1.60 \cdot 10^{-4}$
		Total:	$3.36 \cdot 10^{-3}$

- The number of failures in a 10 year period is $\mathrm{STR}_{\mathrm{SIS}} \approx 0.1$. This means that one spurious trip is expected every 100 years.
- Do you think this is a realistic result? Can you think why the experienced number of spurious trips may be higher? Anyway, $x$oo$N$ systems with k$\geq$ 2 have good protection against spurious activations.

Problem 18.

(a) The reliability block diagram is shown in Fig. 8.11. Note that "FT" means flow transmitter, "PT" means pressure transmitter, and "SHDV" means shutdown valve.

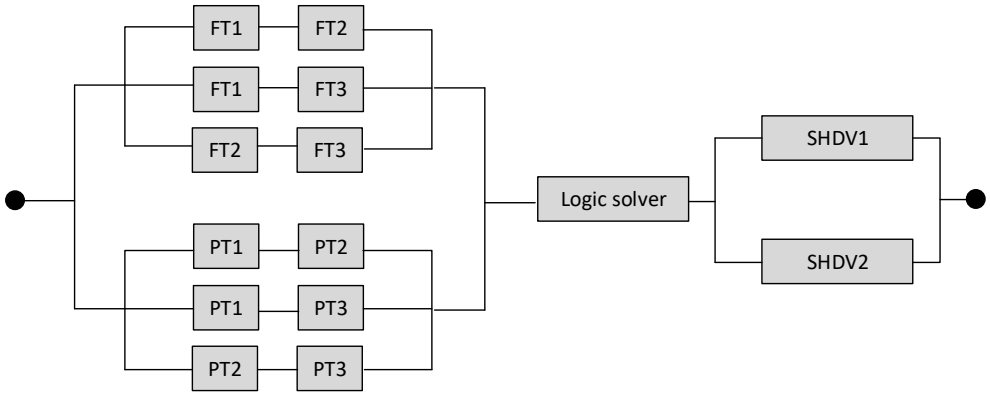


Figure 8.11: Reliability block diagram for SIS

Remark:. The sensor system may seem unnecessary complex, and it may be reasonable to ask why the system designer would come up with this solution. One

possible explanation may be that both pressure *and* flow sensors are needed in order to achieve reliable detection (one of these principles are not alone sufficient to detect in all modes of operation). Second, the system designer or owner may find that the negative effects of spurious activation of the system is so severe, that it is worthwhile the high number of sensors, despite the added complexity, installation costs and operation/maintenance costs.

(b) Chemical processes are often complex, and unnecessary disruptions may lead to long production stops, and in some cases, complex start-ups (process wise, and possibly also safety wise). It is therefore reasonable to assume that 2oo3 has been chosen to have an adequate level of safety as well as a good protection against spurious (unintended) activations of the SIS.

Example from: [1]: "Our decision of 6 February 2014 was founded on the fact that persons staying and sleeping in the accommodation camp would be exposed to higher risk during periods when the facility had not been fully depressurised and shut down. Experience also shows that the risk of leaks and injury at the facility is higher during shutdown and startup than during stable operations," said PSA in a release.

(c) "Any" failure means that both DU and S failures must be considered. Any failure also means that we do not need to consider the system voting,but just treat all items as a serial structure of 3xFTs, 3xPTs, 1xLSs, and 2xVs (any S or DU failure will then be contribute). This means that:

$$\begin{aligned} \lambda_{\text{DU,tot}} &= 3 \cdot \lambda_{DU,FT} + 3 \cdot \lambda_{DU,PT} + 1 \cdot \lambda_{DU,LS} + 2 \cdot \lambda_{DU,V} \\ \lambda_{\text{S,tot}} &= 3 \cdot \lambda_{S,FT} + 3 \cdot \lambda_{S,PT} + 1 \cdot \lambda_{S,LS} + 2 \cdot \lambda_{S,V} \\ Pr(T > 6 \text{ months}) &= e^{-(\lambda_{\text{DU,tot}} + \lambda_{\text{S,tot}}) \cdot 6 \cdot 720} \end{aligned}$$

By inserting the failure rates, the probability of having a failure during the test interval becomes 0.93. This is perhaps not a very impressive result, however, we must remember that the effect of a single failure is limited: A single failure leads only to system failure if it is dangerous and involves the logic solver.

(d) The upper bound approximation may be used to calculate the probability of failure of a system (or system function) in cases where the same component may be part of more than one minimal cut set. In this particular case, it may be shown

[1] `http://www.offshoreenergytoday.com/psa-statoil-exposes-workers-to-risk-at-melkoya/`

that:

$$Q_0(t) \approx 1 - \prod_{j=1}^{k}(1 - \breve{Q}_j(t))$$

where $Q_0(t)$ is the probability of failure of the system, and $\breve{Q}_0(t)$ is the failure probability of a minimal cut set. The same formula may be used with PFD_{avg} for all series elements (i.e. the merging of minimal cut sets structures), meaning that $Q_0(t)$ can be replaced by PFD_{avg} (of the system function) and $\breve{Q}_j(t)$ may be replaced by the $\text{PFD}_{\text{avg,j}}$, where j corresponds to the three subsystems: sensors, logic solver and valves. The minimal cut sets have been identified using Cara FaulTree, and the result is listed in Table 8.3.

Table 8.3: Minimal cut sets of system

$\{FT1, FT2, PT1, PT2\}$
$\{FT1, FT2, PT1, PT3\}$
$\{FT1, FT2, PT2, PT3\}$
$\{FT1, FT3, PT1, PT2\}$
$\{FT1, FT3, PT1, PT3\}$
$\{FT1, FT3, PT2, PT3\}$
$\{FT2, FT3, PT1, PT2\}$
$\{FT2, FT3, PT1, PT3\}$
$\{FT2, FT3, PT2, PT3\}$
$\{LS\}$
$\{V_1, V_2\}$

The $\breve{Q}_j(t)$ of a minimal cut set of order n, consisting of different components is calculated as:

$$\breve{Q}_j(t) = \frac{\prod_{i=1}^{n} \lambda_{DU,i}\tau^n}{n+1}$$

where n is the order of the minimal cut set. This means that

$$\begin{aligned}
\text{PFD}_{avg,syst} &= 1 - (1 - \text{PFD}_{avg,Sensor})^9(1 - \text{PFD}_{avg,LS})(1 - \text{PFD}_{avg,V}) \\
\text{PFD}_{avg,Sensor} &= \frac{\lambda_{DU,FT}^2 \lambda_{DU,PT}^2 \tau^4}{5} \\
\text{PFD}_{avg,LS} &= \frac{\lambda_{DU,LS}\tau}{2} \\
\text{PFD}_{avg,V} &= \frac{(\lambda_{DU,V}\tau)^2}{3}
\end{aligned}$$

Inserting the failure rates and the test interval, gives $\text{PFD}_{\text{avg,sys}} \approx 5.01 \cdot 10^{-5}$.

(e) The upper bound approximation, as applied here, will give a conservative result, i.e., it is the maximum value that the PFD_{avg} may take, and the explanation is follow:

- The system function will fail if all the events in one of the minimal cut set occurs. In a situation where the same component appears in more than one minimal cut set, we get what is sometimes referred to as a positive dependency.
- It may be shown that this results in a PFD_{avg} that is higher than the exact value. As such, it may be argued that the upper bound approximation is conservative. A more thorough discussion of this topic is found in the textbook "System Reliability Theory" (Rausand and Høyland, 2004), Chapters 4.4 and 6.5 .

(f) Many software programs for fault tree analysis use this approach. Even with the upper bound approximation being used, the average probability of the system may become too low compared to the exact value. The main reason is that the PFDavg calculated for each minimal cutset is underestimated, as the average of a product is higher than the product of averages (according to the "Schwartz's inequality"). We may demonstrate this in the following:

The PFD_{avg} of the sensor systems calculated on the basis of the respective PFDs:

$$\text{PFD}^{*}_{avg,Sensor} = (\lambda_{DU,FT}\tau)^2 \cdot (\lambda_{DU,PT}\tau)^2 = \lambda^2_{DU,FT}\lambda^2_{DU,PT}\tau^4 = 1.19 \cdot 10^{-11}$$

Using the PFDs of the minimal cut sets from eq. (8.13) the upper bound approximation for the sensor subsystem is

$$\text{PFD}_{avg,Sensor} = 1 - \left(1 - \frac{\lambda^2_{DU,FT}\lambda^2_{DU,PT}\tau^4}{5}\right)^9 \approx 9\frac{\lambda^2_{DU,FT}\lambda^2_{DU,PT}\tau^4}{5} = 2.15 \cdot 10^{-11}$$

The discussion about conservativeness on such small numbers may be somewhat "theoretical", but may be more important if considering other type of configurations. Obviously, this change in calculation principle for the sensors would not at all have an impact on the overall PFD of the system, as the contribution to PFDavg from these are much lower than the contribution from the logic solver and the valves.

(g) For the modeling part, the following additional assumptions are made:

- The upper bound approximation formula may be simplified, by adding the PFD's instead of using $1 - \prod_{i=1}^{m}(1 - PFD_i)$, where m is the number of minimal cut sets and PFD_i is the average PFD for each minimal cut set.

- The independent contribution from pressure transmitters and flow transmitters on the PFD is negligible (for those who want to include the independent part: The most simple approach is to add the independent part to the CCF for both subsystems, and otherwise follow the same approach when multiplying the PFD of these subsystems together).
- The new virtual elements for CCFs in the reliability block diagram (not drawn here) for the flow transmitter and pressure transmitter systems will be voted in a 1oo2 configuration. The PFD of this configuration is calculated by first multiplying the PFD for the two CCF events and then multiplying this result with a correction factor of 4/3 (which would compensate for the Schwartz's inequality in a 1oo2 system).

This means that the following formulas may be used ("I" denoted independent part):

$$
\begin{aligned}
\mathrm{PFD}_{\mathrm{CCF,FT}} &= \frac{\beta_{\mathrm{FT}}\lambda_{\mathrm{DU,FT}}\tau}{2} \\
\mathrm{PFD}_{\mathrm{CCF,PT}} &= \frac{\beta_{\mathrm{PT}}\lambda_{\mathrm{DU,PT}}\tau}{2} \\
\mathrm{PFD}_{\mathrm{CCF,Sensors}} &= \frac{4}{3} \cdot PFD_{\mathrm{CCF,FT}} \cdot \mathrm{PFD}_{\mathrm{CCF,PT}} \\
\mathrm{PFD}_{\mathrm{LS}} &= \frac{\lambda_{\mathrm{DU,LS}}\tau}{2} \\
\mathrm{PFD}_{\mathrm{I,V}} &= \frac{((1-\beta_{\mathrm{V}})\lambda_{\mathrm{DU,V}}\tau)^2}{3} \\
\mathrm{PFD}_{\mathrm{CCF,V}} &= \frac{\beta_{\mathrm{V}}\lambda_{\mathrm{DU,V}}\tau}{2} \\
\mathrm{PFD}_{\mathrm{avg,syst}} &\approx \mathrm{PFD}_{\mathrm{CCF,Sensors}} + \mathrm{PFD}_{\mathrm{LS}} + \mathrm{PFD}_{\mathrm{I,PT}} + \mathrm{PFD}_{\mathrm{CCF,V}}
\end{aligned}
$$

By inserting the failure rates, test interval and values of CCFs, we get $9.60 \cdot 10^{-4}$. As expected, the PFD is higher when the contribution from CCFs are included.

(h) Assumptions:

- Any of the three (pressure or flow) transmitters may raise a spurious signal, however, the logic solver will only initiate a closure of the valves (and thereby result in a spurious trip) in case of (at least) two spurious signals (from either of the pressure or flow transmitter system) are raised at the same time.
- A single spurious closure of the valve or spurious activation of the logic solver will lead to spurious trip

The equations for the spurious trip rates (STR) per category of components are (all results are per hour):

$$\begin{aligned}
STR_{\text{FT}} &= 3\lambda_{\text{S,FT}} \cdot (1 - e^{-2\lambda_{\text{S,FT}}t}) \approx 6\lambda_{\text{S,FT}}^2 t = 7.26 \cdot 10^{-12} \\
STR_{\text{PT}} &= 3\lambda_{\text{S,PT}} \cdot (1 - e^{-2\lambda_{\text{S,PT}}t}) \approx 6\lambda_{\text{S,PT}}^2 t = 1.22 \cdot 10^{-12} \\
STR_{\text{LS}} &= \lambda_{\text{S,LS}} = 5.0 \cdot 10^{-8} \\
STR_{\text{V}} &= 2\lambda_{\text{S,V}} = 4.6 \cdot 10^{-6} \\
STR_{\text{SIS}} &= 7.26 \cdot 10^{-12} + 1.22 \cdot 10^{-12} + 5.0 \cdot 10^{-8} + 4.6 \cdot 10^{-6} = 4.65 \cdot 10^{-6}
\end{aligned}$$

We can see that the result is dominated entirely by the contribution from the two shutdown valves.

(i) Over a period of 10 years, this will correspond to $10 \cdot 8760\text{hours} \cdot 4.65 \cdot 10^{-6}\text{per hour} \approx 0.41$. In other words, a failure is expected about once every 20 years.

(j) In this case, it is only the calculation of the $\text{STR}_{\text{S,FT}}$ and $\text{STR}_{\text{S,PT}}$ that need to be updated, as the other components remain independent. The beta factor model assumes that a CCF_S (to denote that this type of CCF is different than CCFs with respect to DU and DD failures) is the event results in all redundant components raising an S-failure at the same time. The new updated calculation of STR for the sensor system becomes:

$$\begin{aligned}
STR_{\text{FT}} &= 6\lambda_{\text{S,FT}}^2 t + \beta_{\text{S,FT}}\lambda_{\text{S,FT}} \\
STR_{\text{PT}} &= 6\lambda_{\text{S,PT}}^2 t + \beta_{\text{S,FT}}\lambda_{\text{S,PT}}
\end{aligned}$$

The new (updated result) becomes $4.87 \cdot 10^{-6}$ trips per hour. Over a period of 10 years, this will correspond to $10 \cdot 8760$ hours $\cdot 4.87 \cdot 10^{-6}$ per hour ≈ 0.43 — more or less the same result has calculated earlier.By comparing with the previous result, we may conclude that the CCFs for the sensor system do not have much effect on the STR, as the contribution from shutdown valves is still dominating. So, it may be important to direct the attention to measures that can avoid spurious trips of these valves.

(k) The starting point can be either one of the two scenarios:

- The the first valve is carried out at time 0, and first test of the second valve carried out after three months. he PFD_{avg} (and the PFD for each valve) based on this assumption is shown to the left of Fig. 8.12. However, as can

be seen the PFD_{avg} in the first test interval (0 to t_o=3 months) is different from the other test intervals. One may then use arithmetic or geometric average to find the overall PFD_{avg}, but perhaps this is unnecessary work compared to using the second alternative.

- We assume that the first valve started its operation $\tau - t_o$ time before time 0. It is obvious that this is unrealistic to assume an item starts operation before time 0 but it simplifies the calculation and provides a slightly conservative, if not almost the same, result. The PFD_{avg} based on this assumption is shown to the right of Fig. 8.12.

In either cases, the test interval for each of the valves remain as 6 months.

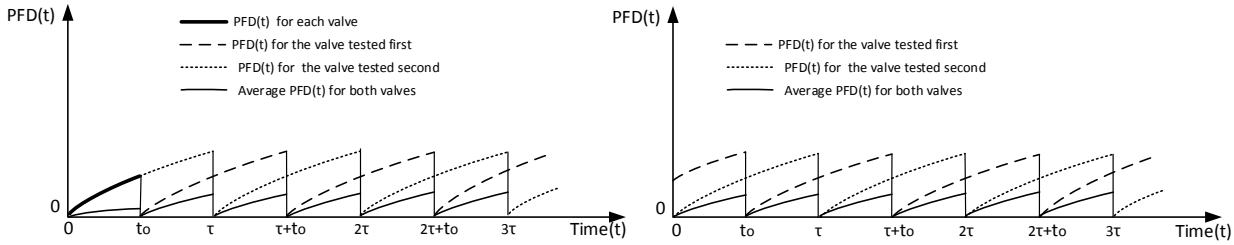


Figure 8.12: Stagger testing

For the calculation, we choose the second scenario. We then have:

$$\begin{aligned} q_{1,\text{V}} &= 1 - e^{-\lambda_{\text{DU,V}} \cdot t} \text{ for } 0 \le t \le \tau \\ q_{2\text{a,V}} &= 1 - e^{-\lambda_{\text{DU,V}} \cdot (t+\tau-t_0)} \text{ for } 0 \le t \le t_0 \\ q_{2\text{b,V}} &= 1 - e^{-\lambda_{\text{DU,V}} \cdot (t-t_0)} \text{ for } t_0 \le t \le \tau \end{aligned}$$

The failure probability distribution function for the valve subsystem becomes:

$$q_s(t) = \begin{cases} q_{1,\text{V}} \cdot q_{2\text{a,V}} & \text{for } 0 < t \le t_0 \\ q_{1,\text{V}} \cdot q_{2\text{b,V}} & \text{for } t_0 < t \le \tau \end{cases}$$

Hence

$$\begin{aligned}
\mathrm{PFD}_{\mathrm{avg}} &= \frac{1}{\tau}\int_0^{\tau} q_s(t)dt \\
&= \frac{1}{\tau}\left[\int_0^{t_0} q_{1,\mathrm{V}} \cdot q_{2a,\mathrm{V}}dt + \int_{t_0}^{\tau} q_{1,\mathrm{V}} \cdot q_{2b,\mathrm{V}}dt\right] \\
&\approx \frac{1}{\tau}\left[\int_0^{t_0} (\lambda_{\mathrm{DU,V}} \cdot t)(\lambda_{\mathrm{DU,V}} \cdot (t+\tau-t_0))dt + \int_{t_0}^{\tau} (\lambda_{\mathrm{DU,V}} \cdot t)(\lambda_{\mathrm{DU,V}} \cdot (t-t_0))dt\right] \\
&= \frac{\lambda_{\mathrm{DU,V}}^2}{\tau}\left[\int_0^{t_0} t^2 + \tau t - tt_0 dt + \int_{t_0}^{\tau} t^2 - tt_0 dt\right] \\
&= \frac{\lambda_{\mathrm{DU,V}}^2}{6}(3t_0^2 - 3\tau t_0 + 2\tau^2)
\end{aligned}$$

- The PFD using $\lambda_{\mathrm{DU,V}} = 2.1 \cdot 10^{-6}$ failures/hour, $\tau = 4380$ hours (6 months) and $t_0 = 2190$ hours (3 months) is $1.76 \cdot 10^{-5}$.
- Simultaneous testing resulted in $9.38 \cdot 10^{-4}$ when CCFs were considered, and $2.82 \cdot 10^{-5}$ when CCFs were excluded. In either case, we find that staggered testing gives a lower value for PFDavg.
- It may be noted that we assume no impact of CCFs for staggered testing. But is this a reasonable assumption? Testing valves at different points in time will reduce the likelihood of introducing CCFs during the testing activity itself. If a CCF is introduced, it will be revealed earlier (not necessarily as a CCF, but as a single failure of one of the valves. In practice, we may expect that a dangerous fault revealed during a regular test will also trigger a test of the other valve. In light of the added complexity to manage staggered testing, it is tempting to propose that this testing strategy is more of a theoretical interest than of practical use.

(l) As can be seen from Figure 8.13 the RBD of the valve subsystem can be drawn using virtual components. Thus the associated PFD can be calculated as follows:

$$\mathrm{PFD}_{\mathrm{avg}} = \frac{1}{\tau}\sum_{i=1}^{i=12}\int_{730\cdot(i-1)}^{730\cdot i}\left[1 - R^r(t - 730\cdot(i-1)) \cdot R^{nr}(t)\right]^2 dt$$

where $R^r(t) = \mathrm{e}^{-0.6\lambda_{DU,V}t}$, $R^{nr}(t) = \mathrm{e}^{-0.4\lambda_{DU,V}t}$ and the upper limit of the summation is the proof test interval divide by PST interval (8760/730=12).

This problem was solved using Maple®, but matlab or any other suitable software may also be used.

Table 8.4: Maple code.

Code text
restart;
with(plots);
tau[PST] := 730;
N := 6; #Number of partial test in a functional test interval
tau[FT] := 730*N;
lambda[DU, V] := $2.1*10^{-6}$;
#DU failure rate valve PSTcov := .60; #Partial test coverage
lambda[DU, VPST] := PSTcov*lambda[DU, V]; #DU failure rate revealed by partial stroke testing
lambda[DU, VFT] := (1-PSTcov)*lambda[DU, V];# Remaining DU failure rate
PFDa[avg] := 0;#Initialization
PFD := Array(1..N);#Define space for temporary results
qsplot := Array(1 .. N); #Define space for temporary resultsl
for m to N do
t[start] := (m-1)*tau[PST]; #Move from one partial test interval to the next
t[stopp] := m*tau[PST]; # As above
#Failure function for two parallel components with partial and full test:
qs1 := $(1-\exp(-\text{lambda[DU, VFT]}*t)*\exp(-\text{lambda[DU, VPST]}*(t-t[\text{start}])))^2$;
qsplot[m] := plot(qs1, t = t[start] .. t[stopp], style = line);#Plot unavailability PST interval
PFD[m] := (int(qs1, t = t[start] .. t[stopp]))/tau[FT];# Storing the PFDavg each PST interval
PFDa[avg] := PFDa[avg]+PFD(m); #Accumulating the result
end do;
qsplotref := plot($(1-\exp(-\text{lambda[DU, V]}*t))^2$,
t = 0 .. tau[FT], style = line, color = "blue"); #Plot for unavailability (no partial test)
display(qsplotref, qsplot[1], qsplot[2], qsplot[3], qsplot[4], qsplot[5], qsplot[6],
labels = ["Hours", "Unavailability"], labeldirections = [horizontal, vertical]);#Show plot

- The code used to generate the results is included in Table 8.4. Note that the programming may be done in different ways.
- The unavailability as a function of time is shown in Fig. 8.14. Red line is used for the result when the effects of partial stroke testing are included, and the blue line shows the result when only full functional test is considered.
- The result of PFD_{avg} becomes $6.56 \cdot 10^{-6}$.
- We may conclude that PST may be an efficient way to reduce the PFDavg, as long as there are no other negative impacts of doing partial tests (for example increased wear for the valves).

(m) Some issues that may be considered in this type of discussion are:

- Partial proof testing gives a more significant reduction in PFD than by staggered testing (in this particular set up).

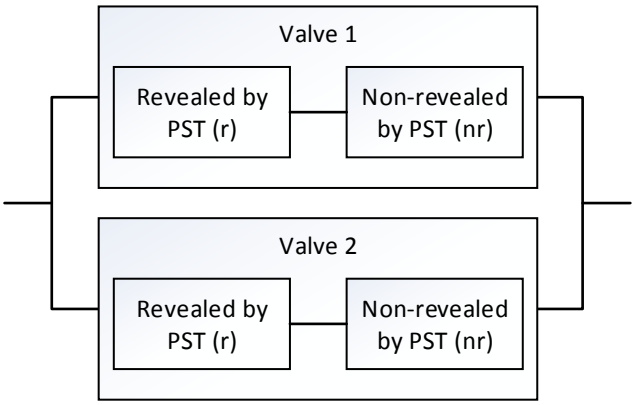


Figure 8.13: PST

- Partial stroke testing requires more frequent testing, automated means of testing should be installed to avoid an increase in costs from the additional tests.
- Partial stroke testing may result in earlier detection of some failure modes for all redundant components.
- Staggered testing may also lead to earlier detection of failures, if a failure revealed in a staggered test triggers a check for the same type of failure in the other redundant components. This additional testing is not scheduled in as part of the staggered test.
- Staggered testing reduces the dependency between tests carried out for redundant components (with respect to time of test and involved personnel)
- Staggered testing is not partial test, in the meaning that only some failure modes are revealed. A staggered test is a full functional test, but for a selection of redundant components.

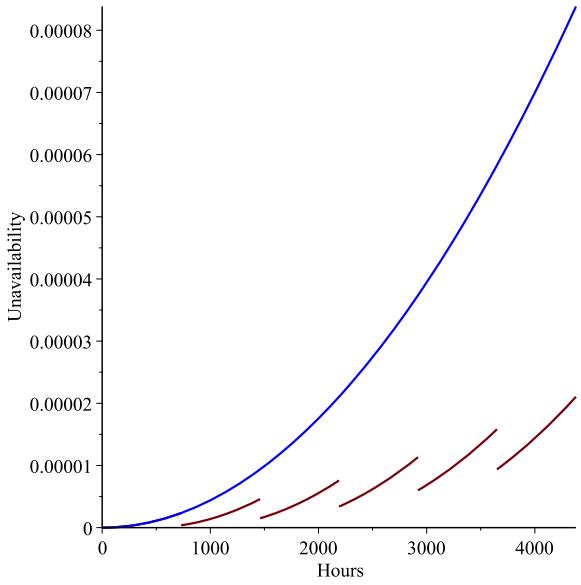


Figure 8.14: Unavailability with (red line) and without (blue line) partial stroke testing

Chapter 9

Probability of dangerous failure per hour

Problem 1.
Solution not yet available here, but relevant information is found in the text book.

Problem 2.

(a) The set up of PFH formulas is shown in chapter 9. Some key points to note are:

- It is assumed for high-demand systems that the system is broght to a safe state upon $k - n + 1$ or more DD failures . This means that no contribution from DD failures is added for PFH formulas, and that the last fault for independent failures is a DU and not either DU or DD failure.
- PFH is a dangerous group failure frequency similar to what we need to determine when we set up formula for PFDavg, but the formula is a bit modified to account for the point above.

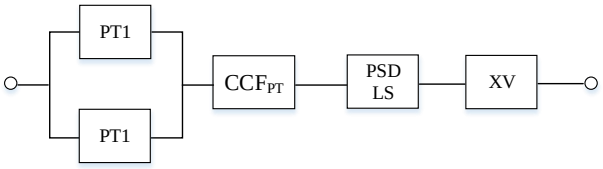
(b) We can disregard DD failures when it can be assumed that the transition is to a safe state within the process safety time (or time required in order to avoid that the fault is present when the next demand occurs).

Problem 3.
Solution not yet available here, but relevant information is found in the text book.

Problem 4.
Solution not yet available here, but relevant information is found in the text book.

Problem 5.

(a) The reliability block diagram considers the three subsystem, where structure for a 1oo2 system of pressure transmitters, a 1oo1 structure of logic solver, and a 1oo1 structure of valves are included. CCF elements may be added for the pressure transmitters.



(b) This problem can be solved by inserting data into formula (9.33) in textbook for each of the subsystems, but with CCFs included. The formula becomes:

$$\text{PFH}(0,\tau) = (1-\beta_{\text{PT}})^2\,\lambda_{\text{DU,PT}}^2\tau + \beta_{\text{PT}}\lambda_{\text{DU,PT}} + \lambda_{\text{DU, LS}} + \lambda_{\text{DU,V}}$$

Inserting data gives $PFH(0,\tau) = 2.22 \cdot 10^{-6}$ failures per hour, which would indicate a SIL 1 performance.The same formula will be established with IEC 61508 formula (equation 9.50 in the text book), when only DU failures are considered and MRT=0.

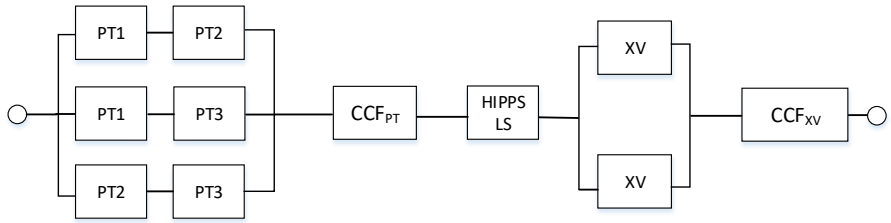
(c) This topic is discussed in Chapter 9.11 in the textbook. It is difficult to provide a clear recommendation to the question, but some arguments that are relevant to consider are:

- Considering HEF with PFDavg vs PFH: In high-demand mode it is assumed that PFH $\approx$ PFH, while in low-demand mode it is assumed that HEF$\approx$ PFD$_{avg} \cdot + \lambda_{de}$ (assuming short demand duation). With only a few demands per year, it is not so likely to be in a situation where the SIS is in a failed state at the same time as there is a demand, so it is of interest to investigate the second option, using PFDavg.
  - PFDavg: Using the test interval that has been proposed, we get PFD$_{\text{avg}} = 9.7 \cdot 10^{-3}$, If we say that the demand frequency is twice per year, the HEF would be 2.2E-6 per year
  - PFH: HEF$\approx$ PFH, which is 2.22E-6 per year.

  - We may conclude on the basis of the results above, we can conclude that for twice per year, and test interval of 1 year, it does not really matter which approach we choose.

- SIL level: With the PFH calculated in (a), we find that the SIF is at a SIL 1 level. When we calculate the PFDavg, we find that the SIF is at a SIL 2 level (we have not considered other factors like architectural constraints here). It is a bit strange that a SIF can achieve two different levels, when built just the same way for high- and low-demand. From a SIL perspective, we can claim that test interval may be used to enhance SIL level (as the test interval has a much higher effect on PFDavg than on PFDavg). This is way one should be a bit sceptical when a high SIL is claimed not because the components are reliable, but the test interval is short.

(d) The reliability block diagram should include all three subsystems, represented by a 2oo3 structure for pressure transmitters, 1oo1 structure for logic solver and 1oo2 structure for valves.



(e) The demand rate for the HIPPS should be $\lambda_{de,HIPPS} = 2 \cdot PFD_{avg} \approx 1.94 \cdot 10^{-2}$ per 8760 hours $\approx$ 2.2E-6 per hour, or once every 51-52 years. We could also have used PFH as demand rate for the HIPPS . As we showed in point c), it would not matter in this case as the HEF is nore or less the same.

(f) We first need to calculate the PFD_{avg} for the HIPPS system. Only the simplified formula is shown in this solution.

$$\begin{aligned} \text{PFD}_{\text{avg}} &= (1-\beta_{\text{PT}})^2 \lambda_{\text{DU,PT}}^2 \tau^2 + \frac{\beta_{\text{PT}} \lambda_{\text{DU,PT}} \tau}{2} \\ &+ \frac{\lambda_{\text{DU,LS}} \tau}{2} + \frac{(1-\beta_{\text{V}})^2 \lambda_{\text{DU,V}}^2 \tau^2}{3} + \frac{\beta_{\text{V}} \lambda_{\text{DU,V}} \tau}{2} \end{aligned}$$

When inserting the failure rates, we get $\text{PFD}_{\text{avg}} = 1.52 \cdot 10^{-3}$.

(g) The residual risk may be found by calculating $2 \cdot \text{PFD}_{\text{PSD}} \cdot \text{PFD}_{\text{HIPPS}}$. The PFD_{avg} of the PSD system was found to be $9.7 \cdot 10^{-3}$. This gives:

$$f_{\text{res}} = 2 \cdot 9.7 \cdot 10^{-3} \cdot 1.52 \cdot 10^{-3} = 2.95 \cdot 10^{-5} \text{ per year}$$

This is higher than the risk acceptance criteria ($1 \cdot 10^{-5}$ per year), and it is necessary to make some reliability improvements.

Some possible reliability enhancing measures could be to:

- Implement some changes in the control system, for example interlocks, so that operator errors (e.g. mal operaiton of a valve which may give a sudden pressure rise) to reduce demand rate. Alternatively, improve operating procedures and simulator training so that operators are more familiar with events that can lead to demands on PSD and HIPPS.
- Improve the reliability of the PSD system, by adding an additional valve, since the single valve consumes about 95% of the system PFD PFDavg. This may not be desired due to the high costs of adding more valves, both with respect to purchasing, installation costs, and costs due to future maintenance and testing.
- Improve the reliability of the HIPPS system, by changing the voting from 2oo3 to 1oo3. This may not be desired as the latter would give more spurious trips. An alternative would be to introduce one more pressure transmitter, and vote them 2oo4. Adding more transmitters is also introducing more possible leakage points (as they need to intersect hydrocarbon systems). The effect of adding more pressure transmitters is however limited. A last alternative could be to add one more valve, however, the effect on PFDavg is not very large. Instead, it will result in less availability of production as one additional valve must be tested on regular intervals.
- Reduce the test interval for PDS and/or HIPPS. This may not be desired, due to the implications on production while carrying out the function tests.
- Introduce partial stroke testing. This could have a positive effect on the PFDavg for both HIPPs and PSD.
- This list was not exhaustive, and you may propose other alternatives if you can.

Problem 6.

(a) Three additional transitions are needed, they are:

$$\begin{aligned} \text{Transition } 2{->}0 &: \mu_{\text{DU}} \\ \text{Transition } 4{->}0 &: \mu_{\text{2DU}} \\ \text{Transition } 5{->}0 &: \mu_{\text{DU}} \end{aligned}$$

where μ_{DU} is $1/(\tau/2 + \text{MRT})$ and μ_{2DU} is equal to μ_{DU} with CCFs (but would have been $1/(\tau/3 + \text{MRT})$ if no CCFs where included in the model for DU failures). It may be a better alternative to split state 4, but this is not shown here.

(b) PFH will be as indicated in example 9.12, but with time dependent probabilities. This means that:

$$\text{PFH}(0,\tau) = P_0 \cdot \beta\lambda_{\text{DU}} + P_1 \cdot \lambda_{\text{DU}} + P_2(\lambda_{\text{DU}} + \lambda_{\text{DD}})$$

(c) Using MAPLE, $\text{PFH}(0,\tau) = 1.077 \cdot 10^{-7}$ (SIF failures per hour). This would correspond to a SIL 2 performance. (havn't double-checked the maple code yet)

Chapter 10

Common cause failure

Problem 1.
No solution prepared here yet. Explanation can be found in textbook.

Problem 2.

(a) The standard β-factor model splits the failure rate (λ), for a channel, into independent failures each with failure rate $(1-\beta)\lambda$ and a CCF with rate $(\beta\lambda)$. Reducing the CCF rate by 20% means, therefore, increasing each independent failure by 20%. This is not reasonable since there is no way that a CCF reduction measure will increase the rate of independent failures. Thus, the model should be used carefully.

(b) No solution prepared here yet. Explanation can be found in textbook.

Problem 3.

(a) The only difference is that the C-factor model, unlike standard β-factor model, keeps the independent failures unmodified, and thus the total failure rate can be written as $\lambda = \lambda^i + \lambda^i = \lambda^i + \beta\lambda$.

(b) No solution prepared here yet.

Problem 4.

(a) The standard β-factor model assumes that, given common cause failure, all

components in a channel will fail with probability β. This means that the number of components in parallel and the voting are not taken into account. The PDS model, however, takes into account the voting (and also the number of components) of the architecture. The proof for the C_{MooN} can be seen in Appendix B of the PDS handbook.

(b) No solution prepared here yet. Explanation can be found in textbook.

Problem 5.
It appears that CCF is the dominating factor both in PFD and STR calculations. The PDS method provides the C_{MooN} values of 0.5 and 2 for the 1oo3 and 2oo3 architectures respectively. The same value will also be applied to quantify the STR of the 2oo3 architecture (note that the C_{MooN} value varies for PFD and STR calculation of the same architecture). A 2oo3 architecture is the most preferable architectures over 1oo3 in situations where spurious activation is strictly undesired, despite it is less reliable than 1oo3. Given the dominance of CCF, the PDS CCF model significantly discourage a 2oo3 architecture, i.e. the PFD_{avg} is almost four times higher.

Problem 6.

(a) No solution prepared yet, but the explanation is found in the textbook with support of appendix D in IEC 61508, part 6.

(b) No solution prepared yet. Explanation can be found in textbook.

Problem 7.

(a) Assume that the three event that lead to system failure, namely due to independent failures, lethal shocks and non-lethal shocks, are independent.

$$\begin{aligned}
\text{PFD}_{\text{avg}} &= \text{PFD}^{\text{I}}_{\text{avg}} + \text{PFD}^{\text{L}}_{\text{avg}} + \text{PFD}^{\text{S}}_{\text{avg}} \\
&= (\lambda^{\text{I}}\tau)^2 + \frac{\lambda^{\text{L}}\tau}{2} + \frac{\left(\lambda^{\text{S}}\left(\Pr(X=2) + \Pr(X=3)\right)\right)\tau}{2} \\
&= (\lambda^{\text{I}}\tau)^2 + \frac{\lambda^{\text{L}}\tau}{2} + \frac{\lambda^{\text{S}}\tau}{2}\left(3 \cdot P^2(1-P)^1 + 1 \cdot p^3 \cdot (1-p)^0\right) \\
&= 1.03 \cdot 10^{-2}
\end{aligned}$$

(b) The main distinction of this CCF modeling from standard $\beta-$ factor model is that it considers both the lethal and non-lethal mechanisms of CCF. This ap-

proach makes it identical to the PDS CCF model. The PDS CCF model is developed such that the traditional beta-factor estimate (i.e. β_{1oo2}) can be used to estimate the CCF factor for any other architectures. However, since in this example failure rate data is available, if the PDS CCF method were to applied, the analysis would be the same as in (a).

Problem 8.
Applying the β-factor model with $\beta = 0.1$, each detector has an independent DU failure rate of $\lambda_{DU}^{(I)} = 0.9 \cdot 2.5 \cdot 10^{-6} = 2.25 \cdot 10^{-6}$ and a common cause failure rate of $\lambda_{DU}^{(C)} = 0.1 \cdot 2.5 \cdot 10^{-6} = 2.5 \cdot 10^{-7}$. Assume that all the detectors are tested (each year, $\tau = 8760$ hours) at the same time and the test reveals all DU failures. Further, after test (and repair) it is assumed that each detector is put into operation in an *as good as new* state.

(a) The PFD_{avg} for the 2oo4 voted group with CCF can be calculated as

$$PFD_{avg} = (\lambda_{DU}^{(I)}\tau)^3 + \frac{\lambda_{DU}^{(C)}\tau}{2} = 1.10 \cdot 10^{-3}$$

(b) The PFD_{avg} for a 2oo3 voted group for the same detectors is

$$PFD_{avg} = (\lambda_{DU}^{(I)}\tau)^2 + \frac{\lambda_{DU}^{(C)}\tau}{2} = 1.48 \cdot 10^{-3}$$

The 2oo4 voting group is about 35% safer than the 2oo3 voting group, however, if considering the range of a SIL requirement, they would both be within the range of a SIL 2 (assuming that no other contributions to the total PFD of the SIF).

(c) The following points are among the relevant points that need to be considered:

- At first glance, it may seem reasonable to suggest the 2oo4 system with the lowest PFD. However, introducing four detectors means that the system complexity increases (installation wise), and the forth detector means additional testing compared to the 2oo3 system. When we know that many dangerous failures are introduced during a test (e.g., wrong calibration, lack of proper re-installation after test and so on), it may be questioned if the 2oo4 system is so much safer.
- A 2oo3 system tolerates only one DU failure, while the 2oo4 tolerates two DU failures. This means that the 2oo4 is more fault tolerant. The reliability of the 2oo3 may be enhanced by introducing an alarm on deviating

readings from the three detectors (making it less likely that two or more dangerous failures are left unattended).

- Both configurations have the same level of defense against spurious failures (meaning that two spurious signals are needed in order to have false/unintended activation of the SIF). Yet, the 2oo4 voting group is highly susceptible than the 2oo3 (i.e. 3 possibilities in 2oo3 versus 6 possibilities in 2oo4).

(d) The beta factor model splits the failure rate of a component into two parts, one independent failure rate and one dependent (or CCF) failure rate with the fraction β

$$\lambda = \lambda^{(I)} + \lambda^{(C)}$$

where

$$\beta = \frac{\lambda^{(C)}}{\lambda}$$

If we set up the equation for conditional probability, we get:

$$\begin{aligned} \Pr(\text{CCF}|\text{a failure}) &= \frac{\Pr(\text{CCF and failure})}{\Pr(\text{a failure})} \\ &= \frac{1 - e^{-\beta\lambda t}}{1 - e^{-\lambda t}} \\ &\approx \frac{\beta\lambda t}{\lambda t} = \beta \end{aligned}$$

(e) The following points are relevant to mention:

- The beta factor model may be considered as a lethal shock model, where an exposure (a common cause) results in the simultaneous failure of all affected components. The realism in this model is influenced by how likely it is that the components in question will face this type of exposure, at all, or if such exposure will dominate compared to other exposures.

- The beta factor covers a number of different common causes of failure. As such, we may find that it is too conservative to assume that the SIF fails in the presence of any such event.

- If a set of redundant components are exposed to high temperature, we may assume that they will degrade over time and the failures may occur at very different points in time. In this case, we may find the beta factor model to be too conservative since sufficient time may be available to correct the failure before the next one appears.

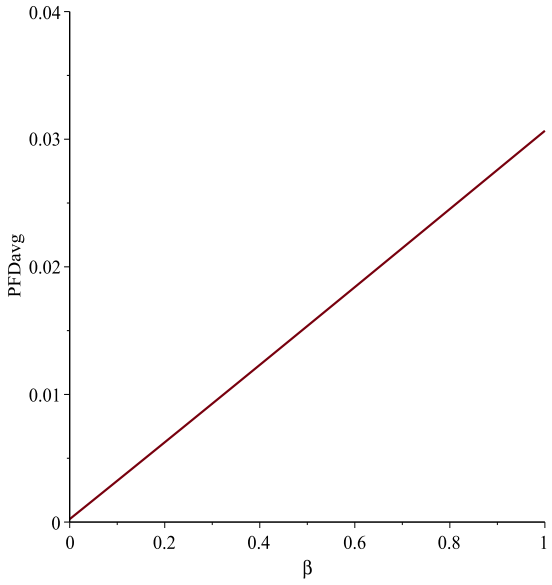


Figure 10.1: Sketch of PFD_{avg} as a function of β.

- If the same components are exposed to an electrical shock or a replicated calibration error, this may result in immediate failure, and the beta factor may be a suitable representation of the phenomena of CCFs.

(f) As seen in Fig. 10.1, the curve is linear as the contribution from CCF is dominating, i.e. PFD_{avg} is related almost linearly to β with slop $\lambda_{DU}\tau/2$.

Problem 9.

(a) The following differences with the PDS Method (Multiple beta factor model) can be mentioned:

- The PDS Method applies a multiplier, β with voting correction factor C_{koon} that gives $C_{koon}\beta$, which accounts the impact of CCF leading a $koon$ system to fail. Thus

$$\text{PFD}_{\text{DU}}^{\text{CCF}} = C_{koon}\beta\frac{\lambda_{DU}\tau}{2} \tag{10.1}$$

  Where β is the probability that a 1oo2 voting fails given a CCF. This model takes into account both "lethal shock" with probability q and "non-lethal shock" with probability $1-q$, that is embedded in the derivation of the value of C_{koon}. It is thus, unlike the model in the question, the PDS Method

makes it easer for users by proposing a numerical value for C_{koon}. However, the rational (mathematical approach) behind the derivation of C-factor is similar to the model in the question.

- The PDS method applies a conditional probability to calculate the effect of the "non-lethal" part in the C_{koon}. I.e, given the failure of k specific components, the failure of another specified component is calculated and used in the estimation of the C_{koon}. The model in the question, however, assumes components are statistically independent, i.e., the probability for a channel to fail due to external shock is p regardless of the status of the remaining channels.

Difference with the standard β-factor model: Unlike the model in the question (and the PDS Method model), the standard β-factor model assumes that given common cause failure, all components in a channel will fail with probability β. This means that the number of components in parallel and the voting are not taken into account.

(b) As described in the question, let X-be a random variable measuring the number of channels fail due to external shock, which is binomial distributed with parameter n and p, i.e, $X \sim \text{bin}(n, p)$.

Total DU failure rate for one, two and three channels are calculated, respectively, below:

$$\lambda_{\text{DU},1} = 3\lambda_{\text{DU}}^{\text{i}} + \rho \cdot \Pr(x = 1, n = 3) = 3 \cdot 1.5 \cdot 10^{-6} + 10^{-7} \cdot \binom{3}{1} \cdot 0.5^1 \cdot (1 - 0.5)^{3-1} = 4.54 \cdot 10^{-6}$$

$$\lambda_{\text{DU},2} = \rho \cdot \Pr(x = 2, n = 3) = 1.5 \cdot 10^{-6} + 10^{-7} \cdot \binom{3}{2} \cdot 0.5^2 \cdot (1 - 0.5)^{3-2} = 3.75 \cdot 10^{-8}$$

$$\lambda_{\text{DU},3} = \rho \cdot \Pr(x = 3, n = 3) = 1.5 \cdot 10^{-6} + 10^{-7} \cdot \binom{3}{3} \cdot 0.5^3 \cdot (1 - 0.5)^{3-3} = 1.25 \cdot 10^{-8}$$

Note that $\lambda_{\text{DU},2}$ and $\lambda_{\text{DU},3}$ may not be fully correct as they are not accounting for the independent failures. To accommodate such failure, let P_1 and P_2 be the probability that the 2oo3 system is in a state where one and two channels are failed respectively. Thus, the modified total failure rates will be

$$\lambda_{\text{DU},2}^{*} = P_1[2\lambda_{\text{DU}}^{\text{i}} + \rho \cdot \Pr(x = 1, n = 2)] + \rho \cdot \Pr(x = 2, n = 3)$$
$$\lambda_{\text{DU},3}^{*} = P_2[\lambda_{\text{DU}}^{\text{i}} + \rho \cdot \Pr(x = 1, n = 1)] + \rho \cdot \Pr(x = 3, n = 3)$$

(c) The Markov state transition diagram is shown in Fig. 10.2. It is assumed that a repair action restores the system in an "as good as new" state. The test and

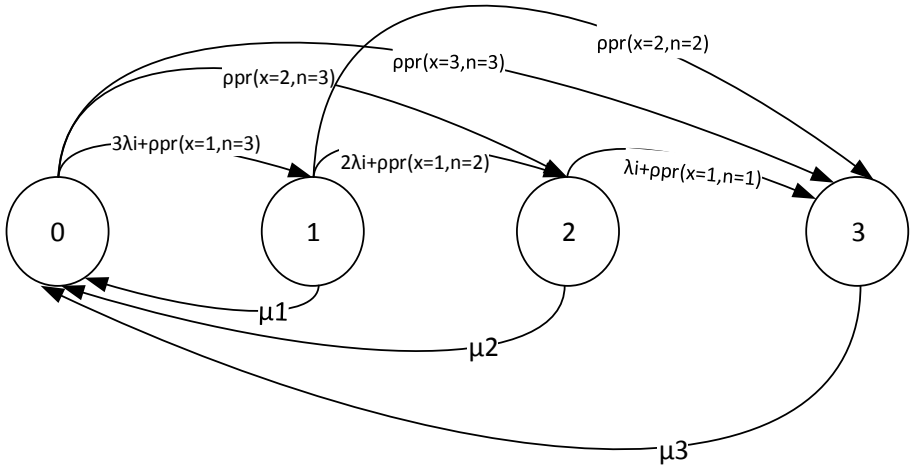


Figure 10.2: Safety instrumented system (SIS).

rapair times are assumed to be negligible. The repair rate is the inverse of the expected downtime given DU failure, i.e., $\mu = 1/(\tau/2)$. (for brevety purpose λ_i is used instead of λ^i_{DU}). The transition matrix ($\mathbb{A}$) is

$$\begin{bmatrix} -(3\lambda_I + \rho\sum_{i=1}^{3} Pr(x=i,n=3)) & 3\lambda_I + \rho Pr(x=1,n=3) & \rho Pr(x=2,n=3) & \rho Pr(x=3,n=3) \\ \mu_1 & -(\mu_1 + 2\lambda_I + \rho\sum_{i=1}^{2} Pr(x=i,n=2)) & 2\lambda_I + \rho Pr(x=1,n=2) & \rho Pr(x=2,n=2) \\ \mu_2 & 0 & -(\mu_2 + \lambda_I + \rho Pr(x=1,n=1)) & \lambda_I + \rho Pr(x=1,n=1) \\ \mu_3 & 0 & 0 & -\mu_3 \end{bmatrix}$$

Thus, the state equations are

$$\begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} P_0 & P_1 & P_2 & P_3 \end{pmatrix} \cdot \mathbb{A} \tag{10.2}$$

and

$$P_0 + P_1 + P_2 + P_3 = 1 \tag{10.3}$$

One of the state equations from eq. (10.2) must be eliminated to obtain a unique solution (here the last column is eliminated). Further, for brevity purpose each transition rates are represented by a single letter. Thus the combined state

equations of eq. (10.2) and (10.3) is

$$\begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} P_0 & P_1 & P_2 & P_3 \end{pmatrix} \cdot \begin{pmatrix} a_0 & b_0 & c_0 & 1 \\ a_1 & b_1 & c_1 & 1 \\ a_2 & 0 & c_2 & 1 \\ a_3 & 0 & 0 & 1 \end{pmatrix} \tag{10.4}$$

We have

$$a_0P_0 + a_1P_1 + a_2P_2 + a_3P_3 = 0 \tag{10.5}$$

$$b_0P_0 + b_1P_1 = 0 \Longrightarrow P_1 = -\frac{b_0}{b_1}P_0 \tag{10.6}$$

$$c_0P_0 + c_1P_1 + c_2P_2 = 0 \Longrightarrow P_2 = -\frac{1}{c_2}\left(c_0 - \frac{c_1b_0}{b_1}\right)P_0 \tag{10.7}$$

$$P_0 + P_1 + P_2 + P_3 = 1 \tag{10.8}$$

Eq. (10.5) and (10.8) can be rewritten as

$$\left(a_0 - \frac{a_1b_0}{b_1} - \frac{a_2c_0}{c_2} + \frac{a_2c_1b_0}{c_2b_1}\right)P_0 + a_3P_3 = 0 \tag{10.9}$$

$$\left(1 - \frac{b_0}{b_1} - \frac{a_2c_0}{c_2} + \frac{a_2c_1b_0}{c_2b_1}\right)P_0 + P_3 = 1 \tag{10.10}$$

Thus,

$$P_0 = \frac{a_3}{a_3\left(1 - \frac{b_0}{b_1} - \frac{a_2c_0}{c_2} + \frac{a_2c_1b_0}{c_2b_1}\right) - \left(a_0 - \frac{a_1b_0}{b_1} - \frac{a_2c_0}{c_2} + \frac{a_2c_1b_0}{c_2b_1}\right)} \tag{10.11}$$

$$P_3 = 1 - \left(1 - \frac{b_0}{b_1} - \frac{a_2c_0}{c_2} + \frac{a_2c_1b_0}{c_2b_1}\right)P_0 \tag{10.12}$$

Substituting the input data in the equations above gives $P_0 = 9.90 \cdot 10^{-1}, P_1 = 9.77 \cdot 10^{-3}, P_2 = 1.46 \cdot 10^{-4}, P_3 = 2.82 \cdot 10^{-5}$. Therefore, $\text{PFD}_{\text{avg}} = P_2 + P_3 = 1.74 \cdot 10^{-4}$.

(d) Here we compare the two architectures quantitatively (using PFD_{avg}) based on the model described in the question.

$$\begin{aligned} \text{PFD}_{\text{avg}}^{\text{2oo3}} &= (\lambda_{\text{DU}}^i\tau)^2 + \frac{\rho Pr(x=2,n=3)\tau}{2} + \frac{\rho Pr(x=3,n=3)\tau}{2} \\ &= (\lambda_{\text{DU}}^i\tau)^2 + \frac{\rho\left(3p^2 - 2p^3\right)\tau}{2} = 1.53 \cdot 10^{-4} \end{aligned}$$

$$\begin{aligned} \mathrm{PFD}_{\mathrm{avg}}^{2oo4} &= (\lambda_{\mathrm{DU}}^{i}\tau)^3 + \frac{\rho Pr(x=3,n=4)\tau}{2} + \frac{\rho Pr(x=4,n=4)\tau}{2} \\ &= (\lambda_{\mathrm{DU}}^{i}\tau)^3 + \frac{\rho\left(4p^3 - 3p^4\right)}{2} = 6.87 \cdot 10^{-5} \end{aligned}$$

The 2oo4 is about 123% safer than the 2oo3. As $p \longrightarrow 1$, the CCF modeling will be the same as the standard beta factor model. Thus, the difference between these votings will only be resulted from independent failures, which again will not be significant as in most cases CCF is the dominating factor. With the data provided, given $p = 1$, 2oo4 is only about 20% safer than 2oo3.

Chapter 11

Imperfect testing

Problem 1.
Solution not yet available here, but relevant information is found in the text book.

Problem 2.

(a) Partial stroke testing (PST) may be a desired option because it may lead to less production downtime from testing. More specifically, PST can be used to reveal certain types of DU failures without requiring a full stroke of the valve(s). In general, PST is introduced for one of the following purposes:

- To enhance safety. In this case, full stroke testing interval is not changed, due to the introduction of PST. The effect is not less production downtime, but improved safety.
- To reduce costs. In this case, PST is introduced to allow a longer interval between full stroke testing. The effect is less production downtime due to maintenance and testing, and thereby also reduced costs for these activities.

(b) Two options for PST were introduced:

- Option 1: PST initiated via the logic solver (using separate testing logic, including timer)
- Option 2: Manufacturer package, installed into the hydraulic supply line to the shutdown valve

Some of the pros and cons of the two options suggested for partial stroke testing are shown in Table 11.1:

Table 11.1: Pros and cons of option 1 and option 2

Option	Pros	Cons
1	Cheaper solution. Only some added software in the logic solver. No new equipment or new hardware failure modes	New failure modes of software introduced (e.g., timer error) Difficult to verify where the failure is, if the valve fails to move (do not know if it is solenoid failure or valve failure)
	A larger part of the safety function is covered in the test. The solenoid valve is for example fully tested (it switches completely) as part of the test.	
2	Test arrangement is fully independent of other equipment in SIF Test does not introduce additional complexity (in terms of software) in logic solver	May introduce new failure modes with new hardware More maintenance due to more hardware. May not be so feasible considering the system to be subsea.
	Some more diagnostic features may be available to detect early valve degradation (e.g., due to changed stroke profile)	Solenoid valve not covered by the test.

(c) Failure modes that can be revealed by PST are:

- Fail to close (FTC): More precisely, it is possible to detect that the valve fails to start closing, but in principle we cannot detect that the valve continues fully to the closed position. For this reason, we should not assume that the coverage factor for this specific failure mode is less 100%, but it is reasonable to assume that it is high (e.g. 90%).
- Delayed operation (DOP): Delayed operation means that the valve uses too long closing time, given that it has started to close. Delay can be that the valve sticks, so that it takes a few seconds before it starts to move, or it can mean that the valve just travels with a slower speed over the whole closing period. The PST coverage factor for this failure mode should be lower than what we assumed for FTC, as we do not monitor the whole travel period. One could expect +/-50% , depending on the valve type in question.

Not possible to reveal by partial stroke testing are:

- Leakage in closed position (LCP): Leakage normally requires a leakage test to be carried out, and even a full stroke test cannot reveal all LCP failures. It is often reasonable to assume 0% PST coverage for this failure mode.
- Premature closure (PC): Premature closure is the same as untimely/spurious activation of the valve. Such failures cannot be revealed in advance neither by a full stroke test or a partial test.
- Leakage to environment (LTE): Leakage to environment is usually a type of failure that is detected by other means than regular tests. Subsea for example, one may expect to have special sensors to detect hydrocarbon leakage (so called "leakage detection system"). On a topside facility, where people are present, the leakage would be revealed by operators being in the area (noticing the oil spill or noise) or by gas detectors.
- Fail to open (FTO): Normally, we assume that failure mode (assuming that we are considering a shutdown valve) is only found when the valve is to be re-opened after being fully closed. As such, the failure mode is not covered by a partial test, but it would be found in relation to a full stroke test. A remark: If the valve for some reason fails to return to its initial position (open) after a PST we could define this a s a FTO. However, it would require some more investigation about what are the causes of fail to open. It could be for example sticked seats after having been fully closed. If the valve is sticking in relation to a partial test, it would be reasonable to assume it is detected already while the valve is trying to move towards closed position.

Problem 3.

(a) By partial test coverage (factor) we mean the probability that a DU failure is revealed by a partial stroke test, given that a failure has occurred, or alternatively, the fraction of DU failures that are revealed by partial stroke testing.

It may be noted that the partial test coverage is influenced by two main factors:

- The ability of a partial stroke test to reveal a certain *type* of DU failure mode (a term we could have referred to as revealability of this failure mode by PST)
- The importance/weight of the DU failure mode among all DU failure modes.

Table 11.2: Data for shutdown valve

Failure mode	DU	%Revealability (by PST)	Weight (all failures)	Weight (DU only)	PST (per failure mode)
FTC	x	100%	30%	40%	0.4
DOP	x	20%	30%	40%	0.08
LCP	x	0%	15%	20%	0
PC		NA	10%	NA	NA
FTO		NA	10%	NA	NA
LTE		NA	5%	NA	NA
SUM:					0.48

The first factor (ability to reveal DU failures during partial stroke test) is a function of several sub-factors:

- What is the functional requirement associated with the valves: Is for example a maximum leakage specified for the valve in closed position. If it is not, this failure mode would not account to the contribution of DU failures.
- PST technology or implementation: We already discussed two different types of implementations of partial stroke testing. Different set up can have different monitoring possibilities, and cover different number of SIF components.

The second factor (weight) is a function of sub-factors such as:

- Type of valve: Different types of valves have different proneness to certain failure modes.
- Operational conditions and environment: The type of medium for which the valve is exposed (three phase flow with sand, sulfur etc), pure gas, oil, produced water, ...) can impact on which failure modes being experienced. Also ambient temperature can have an influence, as well as how often the valve is operated.

(b) The partial stroke test coverage for DU failures becomes 48% as shown in Table 11.2. The underlying assumptions is that the % for each failure mode used to determine PST coverage is calculated on the basis of DU failure modes, and not all failure modes (based on definition of PST coverage). It is here assumed that the three DU failure modes are FTC, DOP, and LCP. In total they account for

75% of the total failure rate. Example: If DU failures acount for 30% of the total failure rate, it would account for 30% of the 75% of DU failure modes, i.e. 40%.

(c) With DU failure rate equal to $8 \cdot 10^{-6}$ failures per hour, we find that $\lambda_{DU,FT} \approx 4.16 \cdot 10^{-6}$ per hour and $\lambda_{DU,PST} \approx 3.84 \cdot 10^{-6}$ per hour.

Problem 4.

(a) $\text{PFD}_{\text{avg,w/PST}}$ is compared to $\text{PFD}_{\text{avg,FTonly}}$ in Table 11.3. In this case, we consider only the valve. We have defined $\Theta_{PST,V}$ as the partial test coverage of the valve, while the test interval (τ) of partial stroke testing is given the notation "PST" for partial stroke testing and "FT" for full stroke testing.

This corresponds in a reduction of 44%, found by:

$$\text{Reduction (\%)} = \frac{\text{PFD}_{\text{avg,FT}} - \text{PFD}_{\text{avg,PST}}}{\text{PFD}_{\text{avg,FT}}}$$

Table 11.3: Formulas for PFDavg

Description	$\text{PFD}_{avg,FTonly}$	$\text{PFD}_{avg,w/PST}$
Formula	$\frac{\lambda_{DU,V}\tau_{FT}}{2}$	$\frac{\Theta_{PST,V}\lambda_{DU,V}\tau_{PST}}{2} + \frac{(1-\Theta_{PST,V})\lambda_{DU,V}\tau_{FT}}{2}$
Calculated value	$3.50 \cdot 10^{-2}$	$1.96 \cdot 10^{-2}$

Problem 5.

(a) PST as a measure to improve safety or reduce costs:

- Improving safety: The PFD_{avg} is reduced when we introduce partial stroke testing at regular intervals more often than full stroke tests. As such, we may say that partial stroke testing leads to increased safety.
- Reducing costs: We may allow less frequent full stroke testing without a reduction in PFD by introducing partial stroke testing. This approach would result in less downtime from testing, and as such a means to reduce costs.

(b) We may use the following approach to calculate the PFD_{avg} of the HIPPS function. We consider both options 1 and 2, assuming the following:

- The transmitters and the logic solver are assumed not affected by the PST (even for option 1, since we assume a separate testing logic being used). For these, we get:
  - Option 1 as well as for option 2:

$$\text{PFD}_{\text{avg,PTsLS}}^{(1\&2)} = \frac{((1-\beta_{\text{PT}})\lambda_{\text{DU,PT}}\tau_{\text{FT}})^2}{3} + \frac{\beta_{\text{PT}}\lambda_{\text{DU,PT}}\tau_{\text{FT}}}{2} + \frac{\lambda_{\text{DU,LS}}\tau_{\text{FT}}}{2}$$

- The PST coverage for the shutdown valve, $\Theta_{PST,V}$, is assumed to apply to both option 1 and 2 (even if we may argue differently). This means that we get: We have
  - Option 1 as well as for option 2:

$$\text{PFD}_{\text{avg,V}}^{(1\&2)} = \frac{\Theta_{\text{PST,V}} \cdot \lambda_{\text{DU,V}}\tau_{\text{PST}}}{2} + \frac{(1-\Theta_{\text{PST,V}})\lambda_{\text{DU,V}}\tau_{\text{FT}}}{2}$$

    Note that we have included common cause failures for the pressure transmitters.

- The PST coverage for the solenoid valve, $\Theta_{PST,SV}$, may be assumed to be 100% for option 1 (it is fully switched as part of the partial test) and 0% for option 2 (since the solenoid valve is not operated at all during this option). This means that the contribution to PFD from the solenoid valves are:
  - Option 1:

$$\text{PFD}_{\text{avg,SV}}^{(1)} = \frac{100\% \cdot \lambda_{\text{DU,SV}}\tau_{\text{PST}}}{2} + \frac{(100\% - 100\%)\lambda_{\text{DU,SV}}\tau_{\text{FT}}}{2} = \frac{\lambda_{\text{DU,SV}}\tau_{\text{PST}}}{2}$$

  - Option 2:

$$\text{PFD}_{\text{avg,SV}}^{(2)} = \frac{0\% \cdot \lambda_{\text{DU,SV}}\tau_{\text{PST,SV}}}{2} + \frac{(100\% - 0\%)\lambda_{\text{DU,SV}}\tau_{\text{FT}}}{2} = \frac{\lambda_{\text{DU,SV}}\tau_{\text{FT}}}{2}$$

With $\lambda_{\text{DU,PT}} = 5 \cdot 10^{-6}$ per hour, $\lambda_{\text{DU,LS}} = 1 \cdot 10^{-7}$, $\lambda_{\text{DU,SV}} = 4 \cdot 10^{-6}$, $\lambda_{\text{DU,V}} = 8 \cdot 10^{-6}$, $\beta_{\text{PT}} = 5\%$, and $\Theta_{\text{PST,V}} = 48\%$, we get for option 1, $\text{PFD}_{\text{avg}}^{(1)} = 2.05 \cdot 10^{-2}$ and with option 2, $\text{PFD}_{\text{avg}}^{(2)} = 2.20 \cdot 10^{-2}$.

(c) We now assume that we initially had found that the $\text{PFD}_{\text{avg,FTonly}}$ assuming full stroke testing would meet the reliability target, however, operations complaint about the frequent testing and would like you to extend the intervals between full stroke testing by introducing PST. In this case, we assume option 1, with $\Theta_{\text{PST,SV}} = 1$ and $\Theta_{\text{PST,V}}$ as calculated earlier.

The extension in the regular intervals of full stroke testing may be calculated as follows.:

- We want to achieve that $\text{PFD}_{\text{avg,FTonly}}$ remains equal to $\text{PFD}_{\text{avg,w/PST}}$, when we extend the interval of full proof testing to a new value $\tau_{\text{FT}}^{\text{NEW}}$.
- First, we may note that we can disregard the contribution from the transmitters and the logic solver, as its contribution would be the same with and without partial stroke testing.

We may start first by calculating $\text{PFD}_{\text{avg,FTonly}}$:

$$\text{PFD}_{\text{avg,FTonly}} = \frac{\lambda_{\text{DU,SV}}\tau_{\text{FT}}}{2} + \frac{\lambda_{\text{DU,V}}\tau_{\text{FT}}}{2}$$

Inserting $\lambda_{\text{DU,SV}} = 4 \cdot 10^{-6}$ per hour, $\lambda_{\text{DU,V}} = 8 \cdot 10^{-6}$ hours, $\tau_{\text{FT}} = 8760$ hours gives $\text{PFD}_{\text{avg,FTonly}} = 2.20 \cdot 10^{-2}$.

We now have to ensure that:

$$PFD_{avg,FTonly} = \frac{\lambda_{DU,SV}\tau_{PST}}{2} + \frac{\Theta_{PST}\lambda_{DU,V}\tau_{PST}}{2} + \frac{(1-\Theta_{PST})\lambda_{DU,V}\tau_{FT}^{NEW}}{2}$$

If we solve for τ_{FT}^{NEW}, we get:

$$\tau_{FT,new} = \frac{2PFD_{avg,FTonly} - \Theta_{PST}\lambda_{DU,V}\tau_{PST} - \lambda_{DU,SV}\tau_{PST}}{(1-\Theta_{PST})\lambda_{DU,V}}$$

The new $\tau_{FT,new}$ becomes $\approx$ 11258 hours, or 1.3 years with PFD = $5.26 \cdot 10^{-2}$, i got 2.73 :) .

(d) A 1oo2 voted introduces some new challenges. We now limit ourselves to consider the valves, and not the solenoid valves or the rest of the components. In this case we have two channels voted 1oo2, each with a valve. The valve in each channel may be split into two subparts, one represented by the $\Theta_{PST,V}\lambda_{DU,V}$ whose failures are revealed at intervals of τ_{PST}, and another represented by $(1 - \Theta_{PST,V})\lambda_{DU,V}$ whose failures are revealed at intervals of τ_{FT}. This is illustrated in Fig. 11.1.

The following alternatives would apply to quantifying the effect of partial stroke testing, with a 1oo2 voted group of valves:

- Alternative 1: Consider the contribution from CCFs only. In this case we are back to a series structure., and would get:

$$PFD_{avg,V}^{(1)} \approx \frac{\beta_V\Theta_{PST,V} \cdot \lambda_{DU,V}\tau_{PST}}{2} + \frac{\beta_V(1-\Theta_{PST,V})\lambda_{DU,V}\tau_{FT}}{2}$$

- Alternative 2: Define the minimal cut sets based on how the failures are revealed. We would get *four* minimal cuts representing the independent part and *two* minimal cut sets for the CCF part, for each we may calculate the $\text{PFD}_{avg}^{(2,i)}$, $i = 1..6$. The total PFD_{avg} would be the sum of these.

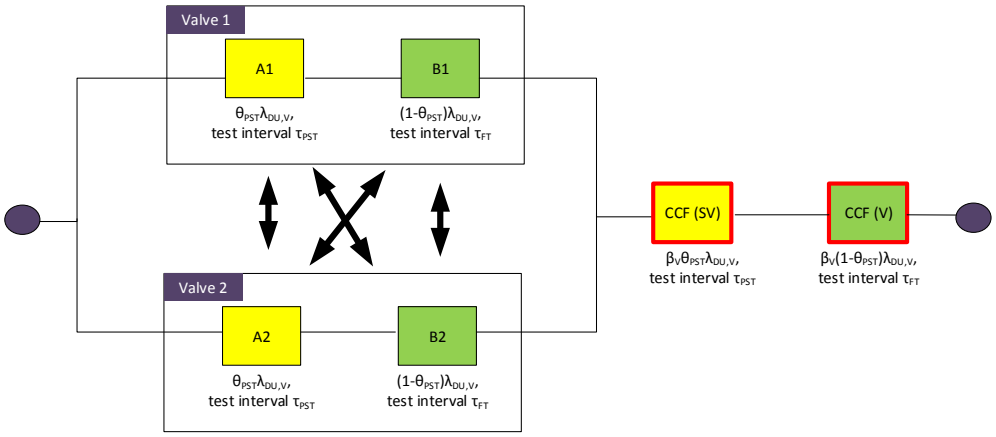


Figure 11.1: Two alternative implementations of PST

Table 11.4: PFD_{avg} for 1oo2 voted valves with PST

Option	PFD_{avg}	Result
Option 1:	$PFD^{(1)}_{avg,V}$	$5.26 \cdot 10^{-4}$
Option 2:	$PFD^{(2)}_{avg,V}$	$6.64 \cdot 10^{-4}$
Option 3:	$PFD^{(3)}_{avg,V}$	$6.39 \cdot 10^{-4}$

– $\mathbf{MCS}_1 = \{A1, A2\}$:

$$PFD^{(2,1)}_{avg,V} = \frac{((1-\beta_V)\Theta_{PST,V}\lambda_{DU,V}\tau_{PST})^2}{3}$$

– $\mathbf{MCS}_2 = \{B1, B2\}$:

$$PFD^{(2,2)}_{avg,V} = \frac{((1-\beta_V)(1-\Theta_{PST,V})\lambda_{DU,V}\tau_{FT})^2}{3}$$

– $\mathbf{MCS}_2 = \{A1, B2\}$:

$$PFD^{(2,3)}_{avg,V} = \frac{((1-\beta_V)\Theta_{PST,V}\lambda_{DU,V}\tau_{PST})}{2} \cdot \frac{((1-\beta_V)(1-\Theta_{PST,V})\lambda_{DU,V}\tau_{FT})}{2}$$

– $\mathbf{MCS}_2 = \{A2, B1\}$:

$$PFD^{(2,4)}_{avg,V} = \frac{((1-\beta_V)(1-\Theta_{PST,V})\lambda_{DU,V}\tau_{FT})}{2} \cdot \frac{((1-\beta_V)\Theta_{PST,V}\lambda_{DU,V}\tau_{PST})}{2}$$

– **MCS**$_{5\&6}$ = $\{CCF(SV)\}$ **and** $\{CCF(SV)\}$:
Here $\text{PFD}_{avg,V}^{(2,5\&6)}$ corresponds to $PFD_{avg,V}^{(1)}$.

The total $\text{PFD}_{avg}^{(2)}$ becomes:

$$PFD_{avg,V}^{(2)} = PFD_{avg,V}^{(2,1)} + PFD_{avg,V}^{(2,2)} + PFD_{avg,V}^{(2,3)} + PFD_{avg,V}^{(2,4)} + PFD_{avg,V}^{(2,5\&6)}$$

- An option 3 would be to sum the PFD_{avg} for mcs_1, mcs_2, and $\text{mcs}_{5\&6}$.

The results are presented in Tab. 11.4.

We may conclude that option 3 is an ok approximation, whereas option 1 may be too optimistic. It may be remarked that option 2 is somewhat pragmatic, when it comes to the treatment of the cross terms.

Chapter 12

Spurious activation

Problem 1. Solution not yet available here, but relevant information is found in the text book.

Problem 2.

(a) A spurious operation signal is coming from individual pressure transmitters, while a spurious trip of the SIF will occur if the number of spurious operation failures is equal to or larger than k. An example of a spurious operation failure of a pressure transmitter with a high trip point would be that it reads a too high pressure compared to the real pressure (for some reasons, for example a calibration error), and as such will exceed the trip point when the actual pressure is lower.

Whether a spurious shutdown occurs or not depends on what final elements being included. In case of valves, they will most likely stop the production, so in this case we may say that a spurious trip also results in a spurious shutdown of the plant. If the pressure transmitters instead had been just raising an alarm to the operators about confirmed high pressure, the result would not necessarily be a spurious shutdown. In this case, the operators may decide to take other actions.

(b) If $n-k+1 = 3$ or more DD failures are reported for the pressure transmitters we know for sure that the SIF is unavailable as long as the repair has not been carried out. A pressure increase in the pipeline or vessel above trip point would in this situation *not* result in a response by the SIF. In this case it may be reasonable to consider that the logic solver initiates a shutdown in the presence of n-k+1 or more DD failures. It may be considered too risky to continue operating with an unavailable SIF. We may therefore argue that it is reasonable to include DD-failures in the calculation of the STR, as DD failures may be one possible cause

for why the SIF is activated without the presence of a real demand.

An example of a DD failure of a pressure transmitter would be that the signal is below 4mA or above 20 mA, meaning outside the normal reading 4-20mA.

(c) The $\mathrm{HFT_S}$ with respect to spurious trips is 1. This means that no spurious trip will occur in the presence of one SO failure, at the most. $\mathrm{HFT_S}$ for a $k$oo$n$ system would be $k-1$.

(d) It may be reasonable to assume that β_S and β_D (and also β for DU failures) are different, as there are different failure causes of spurious operations than for dangerous failures. One example is a valve. A spurious closure of valve may be caused by a leakage of hydraulic fluids from the actuator, while a stuck valve may be caused by corrosion or debris on the valve actuator.

(e) We can use the most simplified equations presented in Chapter 11 in the text book, i.e. STR for $k$oo$n$

$$\begin{aligned}\mathrm{STR} &\approx n\binom{n-1}{k-1}\left[(1-\beta_\mathrm{SO})\lambda_\mathrm{SO}\right]^k \mathrm{MTTR}_\mathrm{SO}^{k-1} + \beta_\mathrm{SO}\lambda_\mathrm{SO} \\ &+ n\binom{n-1}{n-k}\left[(1-\beta_\mathrm{D})\lambda_\mathrm{DD}\right]^{n-k+1} \mathrm{MTTR}_\mathrm{DD}^{k-1} + \beta_\mathrm{DD}\lambda_\mathrm{DD}\end{aligned}$$

SO failure rates for pressure transmitter, logic solver and valves are $1\cdot10^{-6}$, $1\cdot10^{-7}$ and $1\cdot10^{-5}$ respectively. Further, $\lambda_\mathrm{SO}=6$ and $\beta_\mathrm{D}=5\%$. The necessary additional input data from Table 7.2 are $\lambda_\mathrm{DD}=6\cdot10^{-6}$, $\beta_\mathrm{D}=5\%$ and $\lambda_\mathrm{DD}=8$.

STRs for pressure transmitters (2oo4), logic solver (1oo1) and valves (1oo2) are calculated as follows:

$$\begin{aligned}\mathrm{STR_{PT}} &= 6.50\cdot10^{-11}+5.00\cdot10^{-8}+1.78\cdot10^{-14}+3.00\cdot10^{-7}=3.50\cdot10^{-7}\\ \mathrm{STR_{LS}} &= 1.00\cdot10^{-7}+0+6.00\cdot10^{-6}+0=6.10\cdot10^{-6}\\ \mathrm{STR_V} &= 2.00\cdot10^{-5}+0+6.50\cdot10^{-11}+3.00\cdot10^{-7}=2.03\cdot10^{-5}\\ \Rightarrow\quad & \mathrm{STR_{tot}}=\mathrm{STR_{PT}}+\mathrm{STR_{LS}}+\mathrm{STR_V}=2.68\cdot10^{-5}\end{aligned}$$

It is evident from the above result that CCF is the dominating factor with close to 100 % coverage, so considering only CCFs in STR calculations provides very similar result with the one with independent failures.

(f) Assume that STR of the HIPP system occurs according to a homologous Poisson process, with constant rate $\mathrm{STR_{tot}}$ in the operation time t. Hence, the probability of getting x failures in the time interval t is

$$P(N(t)=x)=\frac{(\mathrm{STR_{tot}}t)^x\,\mathrm{e}^{-\mathrm{STR_{tot}}t}}{x!}$$

Thus the probability of having 1 failure during a period of 5 years (43800 hours) can be calculated as

$$P(N(43800) = 1) = \frac{\left(2.68 \cdot 10^{-5} \cdot 43800\right)^1 e^{-2.68 \cdot 10^{-5} \cdot 43800}}{1!} = 0.363$$

(g) On the average $(2 \cdot 1 \cdot 10^{-5} \cdot 5 \cdot 8760)$ 0.88 SO failures is expected every 5 years. It is perhaps difficult to judge if it is satisfactory. If you were designing a subsea system, it would be problematic if several systems have this number of failures. With 5 systems of the same "quality" you would need to plan for an intervention almost each year. So, isolated for the function it may look ok, but perhaps not if considering several systems.

Assuming that you would suggest means to reduce vulnerability to spurious trips, you may consider the following issues:

- Would a change in test interval matters? No. The test interval is not a parameter that influences the STR. However, you could recommend that the maintenance procedure or inspection procedure look for early signs of degradations that eventually may develop into a spurious trip.
- Would a more reliable valve type help? Depends on what we mean by more reliable. The balancing of SFF with HFT and SIL requirement may force us to choose a valve which is more likely to enter a safe state than a dangerous state. The SFF is a relative measure and does not consider the absolute values of the failure rates. However, it may be reasonable to recommend an as low as DU and S failure rate as possible.
- Would you recommend that a 2oo2 configuration was chosen instead, to reduce the contribution from spurious trips? No, this would most likely violate your attempt to meet the SIL requirement. Other options like 2oo3 and 2oo4 do not apply to valves, due to installation costs, maintenance costs, and added complexity and in some cases weight.

Problem 3. Solution not yet available here, but relevant information is found in the text book.

Problem 4. The Markov transition diagram is shown in Fig 12.1. Observe that effort is made to reduce the number of states in order to make it tractable. The

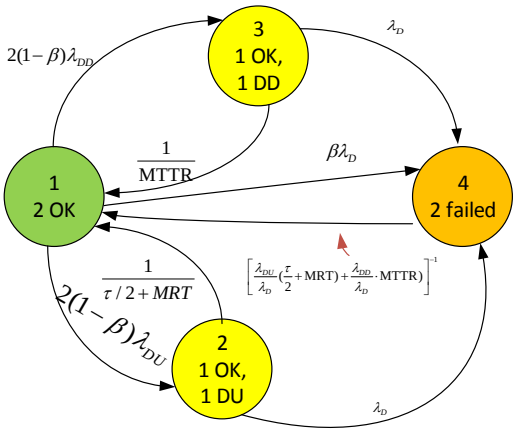


Figure 12.1: Markov model for the 1oo2 fire pump system

corresponding transition matrix is

$$\mathbb{A} = \begin{pmatrix} -2(\lambda_{\mathrm{DU}} + \lambda_{\mathrm{SO}}) & 2\lambda_{\mathrm{DU}} & 0 & 2\lambda_{\mathrm{SO}} \\ \mu_{1,\mathrm{DU}} & -(\mu_{1,\mathrm{DU}} + \lambda_{\mathrm{DU}} + \lambda_{\mathrm{SO}}) & \lambda_{\mathrm{DU}} & \lambda_{\mathrm{SO}} \\ \mu_{2,\mathrm{DU}} & 0 & -\mu_{2,\mathrm{DU}} & 0 \\ \mu_{\mathrm{SO}} & 0 & 0 & -\mu_{\mathrm{SO}} \end{pmatrix} \tag{12.1}$$

Thus, the state equations are

$$\begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} P_0 & P_1 & P_2 & P_3 \end{pmatrix} \cdot \mathbb{A} \tag{12.2}$$

and

$$P_0 + P_1 + P_2 + P_3 = 1 \tag{12.3}$$

One of the state equations from eq. (12.2) must be eliminated to obtain a unique solution (here the first column is eliminated). Further, for bravery purpose each transition rates are represented by a single letter. Thus the combined state equations of eq. (12.2) and (12.3) is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} P_0 & P_1 & P_2 & P_3 \end{pmatrix} \cdot \begin{pmatrix} 1 & a_0 & 0 & c_0 \\ 1 & a_1 & b_1 & c_1 \\ 1 & 0 & b_2 & 0 \\ 1 & 0 & 0 & c_3 \end{pmatrix} \tag{12.4}$$

We have

$$P_0 + P_1 + P_2 + P_3 = 1 \tag{12.5}$$

$$a_0 P_0 + a_1 P_1 = 0 \Longrightarrow P_1 = -\frac{a_0}{a_1} P_0 \tag{12.6}$$

$$b_1 P_1 + b_2 P_2 = 0 \Longrightarrow P_2 = -\frac{b_1}{b_2} P_1 = \frac{a_0 b_1}{a_1 b_2} P_0 \tag{12.7}$$

$$c_0 P_0 + c_1 P_1 + c_3 P_3 = 0 \tag{12.8}$$

Eq. (12.5) and (12.8) can be rewritten as

$$\left(1 - \frac{a_0}{a_1} + \frac{a_0 b_1}{a_1 b_2}\right) P_0 + P_3 = 1 \tag{12.9}$$

$$\left(c_0 - c_1 \frac{a_0}{a_1}\right) P_0 + c_3 P_3 = 0 \tag{12.10}$$

Thus,

$$P_0 = \frac{c_3}{c_3 \left(1 - \frac{a_0}{a_1} + \frac{a_0 b_1}{a_1 b_2}\right) - \left(c_0 - c_1 \frac{a_0}{a_1}\right)} \tag{12.11}$$

$$P_3 = 1 - \left(1 - \frac{a_0}{a_1} + \frac{a_0 b_1}{a_1 b_2}\right) P_0 \tag{12.12}$$

Substituting the input data in the equations above gives $P_0 = 9.91 \cdot 10^{-1}$, $P_1 = 8.62 \cdot 10^{-3}$, $P_2 = 5.46 \cdot 10^{-6}$, $P_3 = 1.19 \cdot 10^{-5}$. Therefore, STR $= \mu_{SO} P_3 = 2\lambda_{SO} P_0 + \lambda_{SO} P_1 = 1.99 \cdot 10^{-6}$.

Chapter 13

Uncertainty

Problem 1. Nothing yet.