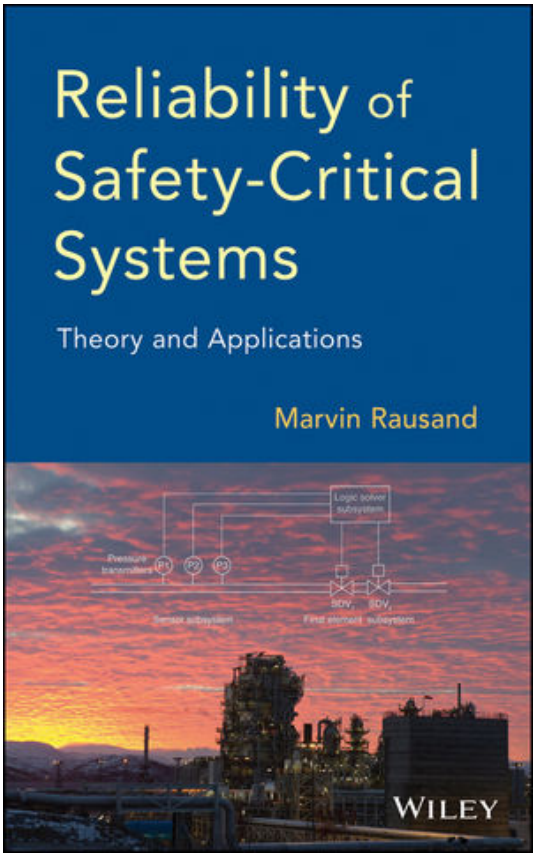
Problems for:



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

Marvin Rausand Mary Ann Lundteigen

(Revision: July 2017)

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

Contents

Preface

This booklet contains problems related to the book Reliability of Safety-Critical Systems, Wiley, 2014. Problems are presented for the first 12 of the 13 chapters of the book.

In most cases, the answers to the questions may be found by studying the book, but there are also a few cases where you have to obtain information from other sources. These sources are available on the Internet and you may need to make a search or visit a given Internet page.A solution booklet covering solution proposals for some of the problems, has also been prepared, and may be obtained on request.

This booklet is always under construction. If you have downloaded the file, please check that you have the most recent version (Version (given by month-year) appears on the front page). 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. Safety-critical systems and related concepts
Explain the following terms and how they are related to each other:

- Safety-critical system
- Active safety barrier
- Functional safety
- Safety-instrumented system (SIS)

Problem 2. Equipment under control (EUC)
A definition and analysis of the equipment under control (EUC) is the starting point for identifying needs for safety-critical systms.

(a) What do we mean by EUC?

(b) It is not always straight forward to define EUC, at least restrict the scope to *one* EUC. Why is this the case?

(c) What methods may be used to identify the need for safety-critical systems for an EUC?

Problem 3. Safety barriers
Safety barriers is a commonly used term in risk analysis.

(a) What do we mean by safety barriers, and to what extent does this concept overlap with the meaning of safety-critical systems?

(b) Why is it useful to classify safety barriers? Give some examples of such classification.

(c) What measures can be used to define the performance of a safety barrier?

Problem 4. Safety performance criteria and risk reduction

(a) The textbook suggest five safety performance criteria for safety barriers:

- Risk reduction
- Functionality/effectiveness
- Reliability/availability
- Response time
- Robustness

Explain what is meant by each of these, and why they are important characteristics of a safety-barrier.

(b) A safety barrier may be installed to either prevent hazardous events from occuring or to mitigate the consequences of hazardous events. Due to this, the textbook suggest two different ways to calculate the risk reduction for each of these. Explain these two approaches.

(c) How can you formuulate a reliability or availability requirement on the basis of required amout of risk reduction?

Problem 5. Safety barriers and mode of operation

(a) What are the main differences between safety barriers operating in *low-demand* mode compared to safety barriers operated in *high-demand* mode?

(b) List some automobile safety barriers that operate in low-demand mode and some that operate in high-demand mode.

Problem 6. Fail-safe design

Fail-safe is an important design principle for safety-critical systems.

(a) What do we mean by fail-safe, and in what way can fail-safe design be achieved?

(b) Give some examples for fail-safe design principle in relation to:

- Sensors
- Logic solver
- Final or actuating devices/elements

(c) What is the difference between de-energize to trip and energize-to trip, and which of these two principles would you select for a shutdown valve?

(d) What is the difference between fail-safe passive, fail-safe active, and fail-safe operational?

(e) Which of these fail-safe design principles should be selected to allow:

- Fly-by-wire (avionics)
- Ensure that red light is activated if if the interlock system detects a failure the green light has been set (railway)
- A shutdown valve closes automatically upon loss of signal to actuator (process industry)

Problem 7. Fail-safe design

(a) What do we mean by the following terms:

- Safe state
- Fail-safe
- De-energize to trip
- Energize to trip

(b) What characterizes a shutdown valve that is fail-safe?

(c) Would it be reasonable to select an energize to trip solution to operate this valve or a de-energize to trip?

Problem 8. Generic standard

IEC 61508 is a so-called generic standard for electrical, electronic, and programmable-electronic (E/E/PE) systems. Several sector-specific standards related to IEC 61508 have been published.

(a) What are the main characteristics of a *generic* standard?

(b) What do we mean by a sector-specific standard?

(c) IEC 61508 is often referred to as a to be a *risk-based* standard. What is meant by risk-based in this context, and what is the main implication of taking this approach?

(d) Some other sectors (like maritime sector) prefer rule-based standards for design of safety-critical systems. What can be arguments for and against rule-based and risk-based standards?

(e) IEC 61508 takes a life cycle approach in the structuring of requirements. Why is reasonable to address the whole life cycle of a system, and not only the design phases, in order to achieve functional safety?

Problem 9. Special considerations in process industry sector

(a) What are typical examples of EUC at a process plant?

(b) What may explain why the process industry relies on layers of protections, rather than a single layer?

(c) What are the SISs within the layers of protection model, and why is it important that each of them are independent? In some cases, it is still relevant to rely on IEC 61508 even if a sector-specific standard is available. This is the case for the IEC 61511, the standard that applies to the process industry sector.

- Give some examples when IEC 61508 must be used in stead of IEC 61511 when designing a new safety-critical system for a process plant
- Why can it be reasonable to refer to IEC 61508 as the manufacturer standard and IEC 61511 as the end-user or system integrator standard?

Problem 10. Special considerations for machinery

(a) What characterizes a SRECS for machinery (in comparison with e.g. a SIS for the process industry)?

(b) What is the EUC in relation to machinery?

(c) What standards are relevant for design of SRECSs?

Problem 11. Special considerations for railway industry standards

(a) What subsystems constitute a signaling system, and how are they related?

(b) Give some examples of safety functions associated with signaling systems?

(c) Give some examples of scenarios that must be treated by a signaling system in relation to a two-track station with single tracks to and from the station.

(d) What standards are applicable for the design of a signaling system?

(e) What do we mean by a safety case, and what is the difference between a generic product safety case, a generic application safety case and a specific application safety case?

Problem 12. Automotive

(a) Give some examples of safety-critical systems installed in a car?

(b) What would be examples of EUC in relation to a car?

(c) What are some of fundamental differences in designing safety-critical systems for cars and for a process plant? Hint: Accident severity, type of users, ability to separate systems.

(d) What is the sector specific implementation of IEC 61508 for automotive?

(e) If you where to compare the 6 parts of IEC 61508 and the 10 parts of the automotive standard: To what extent are the different parts of IEC 61508 covered by the automotive standard?

Chapter 2

Concepts and Requirements

Problem 1. SIS, SIF and other related terms
The textbook has adopted the terms SIS and SIF as generic terms for E/E/PE safety-related system and E/E/PE safety-related safety function.

(a) Explain the difference between safety instrumented system (SIS) and safety instrumented function (SIF).

(b) Why is it important to relate reliability assessment to individual functions, and not to the system as such?

(c) A SIF may be characterized by several attributes. Explain what we mean by by the following terms:

- Channel
- Element
- Voted group
- Subsystem

Problem 2. Redundancy
Redundancy is often introduced to enhance reliability of SIFs.

(a) What do we mean by the term *redundancy*?

(b) Give some arguments for and against the use of redundancy as a means to improve reliability.

(c) Give several examples of devices that are often made redundant in safety instrumented systems for the process industry.

(d) What are the differences between *active* and *passive* redundancy? Give some illustrative examples.

(e) What do we mean by *partly loaded* redundancy? Give some examples.

Problem 3. Redundancy and hardware fault tolerance
Redundancy level may be expressed by the hardware fault tolerance (HFT).

(a) What do we mean by HFT?

(b) What do we mean by the term "k-out-of-n ($k$oo$n$) voted system"? What is the corresponding HFT?

(c) Assume that you have four alternative votings to select among: 1oo4, 2oo4, 3oo4, or 4oo4. Which of these configurations would be best for safety (and explain why)?

(d) Subsystems with high HFT are often prone to spurious/unintended activations, resulting in unscheduled stops. Which configuration would you choose for a sensor subsystem if you would like to avoid unscheduled stops?

Problem 4. Hardware fault tolerance
Hardware fault tolerance is a concept that is closely related to redundancy and voting.

(a) What is meant by *hardware fault tolerance* (HFT) ?

(b) What is the hardware fault tolerance of a 2oo4 voted group?

(c) What is the hardware fault tolerance of a $k$oo$n$ voted group?

(d) Give examples of some voted groups with HFT $= 2$

Problem 5. Safe state
It is important to define and account for the safe state in the design of a SIS.

(a) What do we mean by the term *safe state*?

(b) In what kind of situations can it be difficult to define unique safe state?

Problem 6. Demands and demand rate

Demands and demand rate are two important issues to address during a risk assessment of the EUC.

(a) What do we mean by the term *demand*?

(b) Give several examples of typical demands within different application areas

(c) What do we mean by the term *demand rate*?

(d) Why is the demand rate of importance for the design of a SIF?

(e) The demand rate is $\lambda_{\mathrm{de}} = 5.2 \cdot 10^{-5}$ per hour. How many demands should we expect during a period of 20 years? What is the probability that we will have at least one demand during one year?

(f) Give examples of demands where the *demand duration* may be important.

Problem 7. Risk reduction and RRF
Risk-reduction factor, RRF, has been introduced in standards like IEC 61511.

(a) What is meant by the term *risk-reduction factor*, RRF?

(b) A SIF has risk-reduction factor, RRF $= 150$. What is the $\mathrm{PFD}_{\mathrm{avg}}$ of the SIF?

Problem 8. Safety barriers
Safety barriers are installed to either prevent hazardous events, or mitigate their consequences if they occur.

(a) What do we mean by the term *hazardous event*?

(b) What is the main difference between an *intermediate* barrier and an *ultimate* barrier?

(c) Describe possible effects of a hazardous event after a ultimate barrier failure. Give an example.

Problem 9. Safety integrity

Safety integrity and safety integrity level (SIL) are two key concepts in IEC 61508. In fact, some may refer to IEC 61508 as a SIL-standard.

(a) What do we mean by the term *safety integrity*?

(b) Which quantitative reliability measures are used for safety integrity? Give a brief explanation.

(c) IEC 61508 defines three categories of requirements that must be met in order to achieve a certain level of safety integrity. Explain the meaning of each category.

(d) The safety integrity requirements are given as four distinct safety integrity levels, SIL 1-4, where SIL 4 is the most strict requirement. What is, according to your opinion, the rationale for splitting the requirements into four levels (SILs)? Give a brief explanation.

(e) The process industry (see IEC 61511) does not recommend the use of SIL 4 requirements. Why may this be a reasonable position to take?

(f) What is the principal difference between a *SIL requirement* and the *achieved SIL* for a SIF?

Problem 10. Architectural constraints

Architectural constraints pose restrictions on the design of SIS.

(a) Explain briefly what is meant by *architectural constraints* in IEC 61508.

(b) Why do you think these constraints have been introduced?

(c) The architectural constraints lead to a statement about the minimum required hardware fault tolerance (HFT) of a subsystem. Explain what input information or data you need to derive the minimum HFT a subsystem.

(d) The safe failure fraction (SFF), which is one type of information needed to find the minimum HFT, is heavily disputed. Give some arguments for and against the use of this parameter as an ability to act safely in response to failures.

(e) Explain how you can find the minimum HFT for a subsystem of pressure transmitters that has been assigned a SIL 3. Write down the assumptions you make and the result you get.

Problem 11. Systematic safety integrity

For channels that are not proven in use, it is necessary to also demonstrate compliance with the requirements for *systematic safety integrity*. Systematic safety integrity is mainly met by following certain qualitative requirements. Some of the requirements are SIL independent (meaning that they apply to all SILs), whereas others are SIL dependent. The SIL dependent requirements are listed in separate tables in IEC 61508- 2 and 3.

(a) Give some rationales to why systematic safety integrity is a meaningful concept (in view of what is covered and not covered by hardware safety integrity)

(b) Why can it be argued that software safety integrity is a subset of systematic safety integrity?

(c) Explain the difference between a highly recommended (HR) requirement and a recommended (R) requirement.

(d) Why are some requirements classified as not recommended (NR)?

(e) Go through tables B.1 and B.2 in IEC 61508-2 (with the support from IEC 61508-7) and discuss how easy it is to apply these requirements.

Problem 12. SIL allocation

SIL allocation is the process of defining SIL requirements for individual safety instrumented functions (SIFs), based on the overall need for risk reduction as defined by the risk acceptance criteria.

(a) Mention some methods/approaches that can be used to allocate SILs to SIFs.

(b) Give a brief description of the *risk graph* method and discuss pros and cons related to this method

(c) Give a brief description of the LOPA method and give some pros and cons related to this method.

(d) What are the main differences between the IEC 61508 and the NOG Guideline 70 with respect to principles for determining the required SIL? Mention and discuss some pros and cons for the NOG guideline 070 approach compared to the IEC approach. Hint: To solve this problem it may be feasible to read selected sections of Norsk Olje og Gass (NOG) guideline 070, which can be found at `www.norskoljeoggass.no/no/Publikasjoner` (select "Retningslinjer" on this page). You may read sections 7.2 (Approach), 7.6 (Minimum SIL requirements), and e.g. Appendix A.3.3 for an practical example).

(e) The SIL requirements derived at in Appendix A in NOG guideline 070, and presented in table 7.2, are highly influenced by the choice of failure rates used for the underlying calculations. Discuss some effects on the SIL requirement setting from using overly conservative ("too high") failure rates versus using overly optimistic ("too low") failure rates.

Problem 13. SIL versus PFD and PFH

A SIL requirement gives the target range of the $\mathrm{PFD}_{\mathrm{avg}}$ and PFH for a safety instrumented function (SIF). The target value selected within the range defines

what is sometimes referred to as the SIL budget for the function, from end to end.

(a) The SIL budget may be distributed down to individual subsystems of the SIF. What could be possible strategies to distribute this SIL budget (i.e., what could be possible ways to define how much each subsystem can "consume" of the total SIL budget)?

(b) Consider a SIF that must fulfill SIL 3. Assume that the subsystem of final elements is allowed to consume 70% of the *maximum* allowed PFD_{avg} for the SIF. What is the PFD_{avg} requirement for this subsystem?

Problem 14. Safety requirements specification
Safety requirements specification, SRS, is a key document for the design of a safety instrumented system (SIS).

(a) Describe briefly the main contents of an SRS and at what phase(s) in the safety lifecycle it is developed.

(b) The SRS should include information about *functional safety requirements* and *safety integrity requirements*. Explain these two terms.

(c) A proposed structure of an SRS is presented in NOG guideline 070. Here, it is suggested that the SRS is developed in three revisions. What could be the rationales for developing the SRS in stages, and not in one single step.

Problem 15. Safety analysis report (SAR)
A *safety analysis report* (SAR) is a document type introduced in the NOG guideline 070. The SAR is therefore not a well known concept outside Norway, but with the new revision of IEC 61508 (that came in 2010) a similar document was introduced; the *safety manual* in IEC 61508 (see appendix D in IEC 61508-2).

(a) What is the main purpose of a SAR (or alternatively, a safety manual) and by whom is the document developed?

(b) What type of information does the SAR (or alternatively, the safety manual) provide?

(c) In what way does this type of document relate to the SRS?

Problem 16. Functional safety assessment (FSA)
A functional safety assessment (FSA) is a key activity within what we define as management of functional safety.

(a) Explain the main objectives of a *functional safety assessment* (FSA).

(b) IEC 61508-1 gives requirements to the level of independence for those carrying out an FSA. Explain briefly how this level of independence is defined, and describe the factors contributing to a high level of independence.

(c) Assume that you would like to carry out an FSA just after the SIL allocation process has been completed (the design of the SIFs has not yet started). Assume further that at least one SIF of the SIFs within the scope of the FSA has been assigned a SIL 3 requirement. You suggest that an independent group in your company, for example from an office within your company that is situated in another city. Would this be an acceptable approach? Hint: The SIL 3 requirement is not part of your decision here, but still it may indicate the severity level of consequences if a SIF with a SIL 3 requirement fails to perform its functions.

(d) Assume now that your project has proceeded and that you are close to finalizing the detail design phase. You decide to carry out an FSA before the construction starts, so ensure that no major issues are overlooked. This time you suggest using an external consultant company to carry out the FSA who has not been involved in any previous phases of the project. Is this a feasible approach according to IEC 61508? Explain.

(e) Assume now instead that this external company was involved in the development of the SRS. Would you still think it was feasible to use this company to carry out the FSA? Explain.

Problem 17. Risk graph
A risk graph may require calibration.

(a) Why is a calibration required?

(b) Assume that the a specific EUC design has been studied, and that it has been found that reasonable estimates for F_A and P_A are 0.1 and 0.3 respectively (P_B and P_B are equal to 1). Calibrate the risk graph considering the following critera: The tolerable frequencies for consequence A, B, C and D are 1E-4, 1E-5, 1E-6 and 1E-7 per year respectively. W_1, W_2, and W_3. W_3 corresponds to demands less than once per year, W_2 to demands less than once every 10 years, and W_1 to demands less than once every 100 years.

Problem 18. Minimum SIL requirements
Read paragraph A.3.1 "Process segregation through PSD" in NOG 070 (accessed from `https:/www.norskoljeoggass.no/en/Publica/Guidelines/`). The

section argues why a minimum SIL 2 requirement can be set for this function. The arguments are based on calculated values of PFD_{avg} and some expert judgment, but do not check the architectural constraints.

(a) Check if the SIL2 requirement is met when the architectural constraints are taken into account

(b) Architectural constraints are introduced to compensate for *uncertainty* in reliability calculations. However, there may be uncertainty associated with the assumptions and calculations made to determine the minimum HFT. Discuss main uncertainties that are made to find the architectural constraints.

Problem 19. Reading SIL table

SIL tables give a relationship between the selected reliability measure and the achievable SIL.

(a) A SIF has $\text{PFD}_{\text{avg}} = 5 \cdot 10^{-3}$. Which SIL can the SIF fulfill?

(b) A SIF has $\text{PFH} = 4 \cdot 10^{-7}$ per hour. Which SIL can the SIF fulfill?

(c) When the demand rate is close to once per year, we may, according to IEC 61508, use either PFH or PFD_{avg} as reliability measure. A careful analysis has shown that PFD of a single system is $\text{PFD}_{\text{avg}} = 8.0 \cdot 10^{-4}$ such that the SIL 3 requirement is fulfilled. It has been assumed that the system is tested four times every year (1 year =8760 hours). Is it possible to say if the same system would also meet SIL 3 in the high demand mode, and how would you do this evaluation?

(d) The SIL table can also be used the opposite way. If a SIL requirement has been stated, it outlines the required PFD_{avg} or PFH *range*. Assume that you would like to select *one* value as a PFD_{avg} or PFH target value (so that you have one specific value to compare with the calculated PFD_{avg} or PFH for a SIF). Discuss where in the range you would select the target value (upper, lower, or in the middle)?

Problem 20. Precisions in the use of terms

(a) Is it correct to say that a SIS has SIL 3? (explain your position)

(b) Is it correct to say that a subsystem fulfills SIL 2, given that the architectural constraints for SIL 2 are met? (explain your position)

(c) Will a SIF with a PFD_{avg} between 10^{-4} and 10^{-3} automatically fulfill the SIL

3 requirements? Explain.

Problem 21. Architctural constraints
Assume that a SIL 3 requirement has been specified for a SIF, and that one of the subsystems is a voted group of identical component, each with a SFF = 92%:

(a) What is the minimum HFT for this subsystem, considering the SIL 3 requirement and that the components are of type A?

(b) Why is it reasonable that the minimum HFT increases if the components are reclassified as type B?

Problem 22. Architectural constraints

Assume that a subsystem comprises two non-identical components, where component 1 has a SFF = 75% and component 2 has a SFF = 95%. Assume that one component is type A (component 1) and one is type B (component B). What is the SIL achieved for this architecture?

Chapter 3

Failures and Failure Analysis

Problem 1. Failure, fault, and error
Explain, discuss and compare the following terms

(a) Failure

(b) Fault

(c) Error

(d) What are the differences between the three concepts?

(e) A valve is not able to close as designed, is this a failure or a fault?

Problem 2. Failure modes
Failure analysis usually includes the identification of failure modes.

(a) What do we mean by the term *failure mode*?

(b) List and explain briefly the main failure modes of a water pump

(c) OREDA data handbooks (`www.oreda.org` distinguish between *critical failures*, *degraded failures*, and *incipient failures*. Classify the failure modes you identified into these categories, and give a brief explanation to why a failure mode is assigned to this category. Make sure that at all failure mode categories include at least two failure modes.

Problem 3. Other failure terms
Explain the following terms and give examples:

(a) Failure cause

(b) Failure mechanism

(c) Failure effect

(d) What are the main differences between a failure mode and a failure effect?

Problem 4. Failure classification in IEC 61508
IEC 61508 classifies failure modes into the following categories: Dangerous detected (DD), dangerous undetected (DU), safe detected (SD) and safe undetected (SU). A category called no part/no effect failures are also suggested in the standard.

(a) Assume that a water pump is used as a fire pump. The pump is normally passive and started on demand in case of a fire. Suggest at least one failure mode in each of the categories: DD, DU, SD and SU. List your assumptions.

(b) What does it mean that a dangerous (or safe) failure is detected (DD or SD), i.e. what requirements apply for a failure to be defined as detected? Explain

(c) Assume now that the pump instead is used for boosting fluid pressure in a pipeline, and that the pump must close in case of a downstream restriction to avoid over-pressurization of pipeline. How would this change in functionality affect your classification? Explain.

(d) It is not always straight forward to judge if a failure is safe or dangerous. Consider the two cases: It is found during a proof test that a level transmitter (with low low set-point) indicates a too high level (compared to real level). On the same vessel, another level transmitter (with high high set-point) is also indicating too high level. How would you classify these two failures (too high level) for these two cases. Explain.

Problem 5. Failiure classification in IEC 61508

Failures may be classified according to their causes. IEC 61508 distinguishes between a *random hardware failure* and a *systematic failure*, and the two failures are treated quite differently in the design of a safety instrumented system (SIS).

(a) Explain what we mean by a random hardware failure and argue why it is a *physical* failure

(b) Random hardware failures are given different definitions in this book and by the PDS method. Discuss these definitions and present your own view on this concept.

(c) What is a *systematic* failure/fault? Give some examples.

(d) Would you classify an excessive stress failure as random or systematic, and why?

(e) Are there any relationships between common-cause failures and systematic failures? Give some illustrative examples.

(f) How are failures/faults classified in the OREDA project (and data handbooks)?

Problem 6. FMECA and FMEDA

Failure mode, effects and criticality analysis (FMECA) is a widely used method for identifying and classifying failures of a system and its components.

(a) Why is it possible to argue that FMECA may be used to achieve reliability growth in a design process?

(b) A similar approach, the failure modes, effects, and diagnostics analysis (FMEDA), is often used to document compliance to the IEC 61508. In fact, an FMEDA is often included in an equipment safety manual or safety analysis report (SAR). What is the main difference between an FMECA and an FMEDA?

(c) Assume that you would like to use an FMEDA to determine DU, DD, SU and SD failure rates. Assume further that the component in question constitutes some parts with high level of redundancy (on the control side) and other parts that has only single elements. One such example could be a blow out preventer (BOP) used to shut in the well in case of a well kick or rig problem. A BOP manufacturer may want to provide failure rates for the BOP as such, since the BOP from their perspective is a single unit of delivery. Discuss some challenges in applying FMEDA in this case. Would you argue that it is reasonable to calculate DU, DD, SD and SU failure rates for the BOP as such?

Problem 7. Failure classification

Assume that you are part of a team reviewing failures reported for safety-critical items. The failures found in relation to point gas detectors are described in the table below. Detection method means how the failure was discovered. Detection method PM means that the failure was found during regular preventive maintenance, such as function testing. Alarm means that the failure was announced by an alarm from the self-diagnostic system of the component, or the fire and gas central.

Hint: If you are not familiar with point gas detectors, you may do a search on the internet to find some useful sources. Here is one example accessed in July 2017: `https://www.gmiuk.com/wp-content/uploads/2014/09/GD10P_Operator_Manual.pdf`

Table 3.1: Failure description for gas (point) detector

Tag no	**Short text**	**Comments**	**Detection method**	**Cat.**
70-GD-001	Gas detection comes in with fault	May be due to snow	Alarm	
70-GD-008	Need to flush test line	Dirty test line	PM	
70-GD-118	Unstable measurement	Indicated too low value	PM	
70-GD-004	Defect detector	Unknown cause	Alarm	
70-GD-001	Change of filter	Decayed filter	PM	
70-GD-011	Dirty lens	Dusty lens. Needs cleaning	Alarm	
70-GD-098	Gas detector fails when rainy weather	Need better weather protection/cover	Alarm	
70-GD-026	Gas detector showing too high value	Zero point adjusted and span calibrated	PM	

(a) Classify failures using failure categories DU, DD, S, NA (NA means here Not Applicable, due to not being a failure at all or the equipment being in a degraded, but still functioning state).

(b) Discuss some of the challenges you face when you do the classification. What would you do to clarify missing information?

(c) What types of failures seem to be of a type that is reoccurring. How easy is it to avoid such failures in operation?

Chapter 4

Testing and Maintenance

Problem 1. Importance of regular testing
Testing is of particular importance for safety instrumented functions (SIFs) that are operating in the (low) demand mode.

(a) Why is regular testing more important (on a general basis) for low demand SIFs than high demand SIFs?

(b) In what situations may it also be reasonable to argue for testing of high demand SIFs?

Problem 2. Proof testing
IEC 61508 uses the term *proof testing*.

(a) What are the main differences between the more general term *function test* and a *proof test* as it is defined in IEC 61508 and in the book? Illustrate your answer by an example.

(b) A proof test should ideally be performed under realistic demand conditions. Discuss why this is difficult to achieve (and in some cases not wanted) for (1) a SIF that includes pressure transmitters, (2) a SIF that include gas detectors, (3) a SIF that releases CO_2 into an local equipment room, and (4) a SIF that shears a pipe (such as closure of blow out preventer shear ram).

(c) At what stage in the life cycle of a SIS should considerations to proof testing be introduced? Explain.

(d) The need to carry out proof testing may have design implications. It may, for example, be necessary to add new components (e.g., to to allow confirmation of test) and new logic (for inhibiting input signals, overriding output signals,

forcing input/output signals). Discuss the possible implications that these design measures may have on the reliability in light of random hardware failures and systematic failures.

Problem 3. Partial testing
The term partial testing is often used, but sometimes with different meaning.

(a) One example of a partial proof test is partial stroke testing. With basis in this particular type of test: What are the main differences between a *full proof test* and a *partial proof test*? Give examples.

(b) A partial proof test may also be used to characterize a proof test that has been split into sub-proof tests, so that the sum of the sub-proof tests covers the scope of the full proof test. This is, however, not most common interpretation, and sub-tests could maybe be a a more suitable term. Discuss some of the differences between this way of defining a partial proof test (in the meaning of sub-tests) and way it was defined in bullet a, including the implication on test coverage.

Problem 4. Partial versus imperfect test
Partial proof test and imperfect (or non-perfect) proof test are two terms that may be used with similar meaning. In the book, however, a small distinction has been made between the two. With basis in this distinction, what are the main differences between a *partial proof test* and an *imperfect proof test*?

Problem 5. Partial proof test coverage
Proof test coverage is an important concept in relation to partial proof testing.

(a) How can we define proof test coverage?

(b) What do we mean when we say that the *proof test coverage* is 95%?

Problem 6. Classification of tests
In what categories would you be able to place a diagnostic test among the following test strategies:

- Partial test
- Full test
- Manual test
- Automatic test

– Imperfect test

– Online test

– Offline test

Include a brief explanation of your choice(s).

Problem 7. Spurious activations as tests
False or unintended activations (also referred to as spurious activations) may result in a full or partial activation of the SIF.

(a) Why can it be of useful to credit spurious activations as tests?

(b) What would be some of the differences between a regular proof test (or function test) and a spurious activation?

Problem 8. Staggered testing
There are different strategies for*how* proof tests are carried out. Explain briefly each of these approaches, and give some pros and cons for each of these strategies:

– Staggered testing

– Sequential testing

– Simultaneous testing

Problem 9. Introducing human errors during testing
The main purpose of a proof test is to *reveal* failures. However, failures may also be introduced during a proof test.

(a) Give examples of failures that may be introduced during a proof test. Hint: You may consider reading the Health and Safety Executive (HSE) guideline *Principles for proof-testing of safety instrumented systems in the chemical industry*, which is referenced in the book.

(b) Would you define such failures as systematic failures or the random hardware failure category. Explain.

(c) To what extent would it be reasonable to include such failures in the total failure rate, and what could be possible challenges? For example, the occurrence rate of systematic failures would be highly dependent on how frequent proof tests are carried out. Discuss, but it is not necessary to make any calculations.

Chapter 5

Reliability Quantification

Problem 1. RBDs

Consider the system represented by the reliability block diagram in Figure 5.1.

(a) Carry out the following:

- Explain what we mean by the concept *minimal cut set* in a reliability block diagram (RBD).
- Find the minimal cut sets of the system in Figure 5.1.
- Explain what we mean by saying that a cut set is of *order* 2.

(b) Find the structure function of the system in Figure 5.1.

Assume that the components of the system are independent with the following function probabilities (reliabilities):
$p_1 = 0.90,\ p_2 = 0.95,\ p_3 = 0.85,\ p_4 = 0.90,\ p_5 = 0.80.$

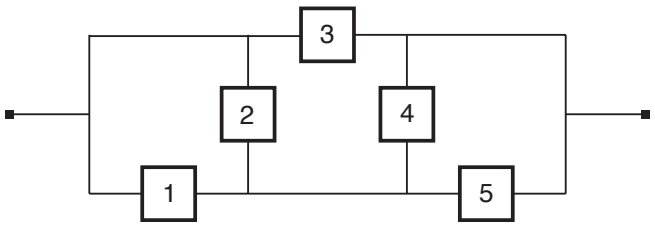


Figure 5.1: System to analyze

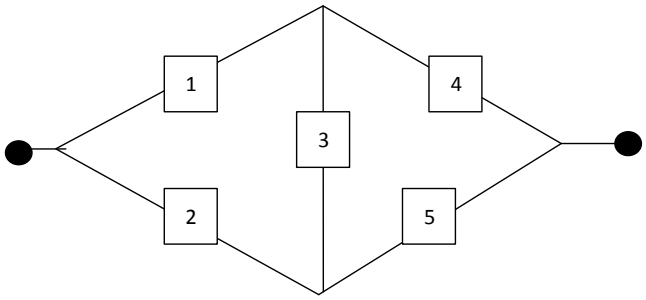


Figure 5.2: System to analyze

(c) Find the system reliability p_S.

Problem 2. RBDs
A system has two minimal cut sets: $C_1 = \{1, 2, 3\}$ and $C_2 = \{1, 3, 4, 5\}$.

(a) Carry out the following:

- Draw the corresponding reliability block diagram.
- Redraw the reliability block diagram (RBD) to obtain an as simple layout as possible.
- Find the minimal path sets of the system.

(b) Carry out the following:

- Establish the structure function for the system.
- Which component do you consider to be the most important in this system (justify your answer).

Problem 3. RBDs

Consider the system described by the reliability block diagram in Figure 5.2. The six components are assumed to be independent with reliabilities: $p_1 = 0.90$, $p_2 = 0.95$, $p_3 = 0.85$, $p_4 = 0.80$, $p_5 = 0.95$, and $p_6 = 0.85$.

(a) Carry out the following:

- Identify the minimal cut sets of the system

– Explain, with words, what a minimal cut set is

– Establish the structure function for the system

– Determine the reliability p_S of the system

(b) Determine Birnbaum's measure of reliability importance, $I^{\mathrm{B}}(i)$, for component $i = 4$. What does this number tell? Give a brief explanation.

Problem 4. Survivability using Weibull distribution
The time to failure of a pump is assumed to be Weibull distributed with scale parameter $\lambda = 2.7 \cdot 10^{-4}$ per hour and shape parameter $\alpha = 2.2$.

(a) Write the expression for the failure rate function of the pump and make a sketch of this function.

(b) Find the mean time to failure (MTTF) of the pump.

(c) Find the probability that the pump survives 1 500 hours in operation. Assume then that the pump has survived $t_1 = 1\,500$ hours, and find the probability that it will survive another 1 500 hours. Comment the result.

Problem 5. Case study: Production system
A production system has two identical channels and is running 24 hours a day all days. Each channel can have 3 different states, representing 100%, 50%, and 0% capacity, respectively. The failure rate of a channel operating with 100% capacity is assumed to be constant, $\lambda_1 00 = 2.4\dot{1}0^{-4}$ hours^{-1}. When a failure occurs, the capacity will go to 50% with probability 60% and to 0% capacity with probability 40%. When a channel is operated with 50% capacity, it may fail (and go to 0% capacity) with constant failure rate $\lambda_1 00 = 1.8\dot{1}0^{-3}$ hours^{-1}. The system is further exposed to external shocks that will take down the system irrespective of the state it is in. The rate of these shocks is $\lambda_1 00 = 5\dot{1}0^{-6}$ hours^{-1}. (A shock will take down all channels at the same time)

The two channels are assumed to operate and fail independent of each other. When both channels have capacity of 50% or less, the whole system is closed down, and it is not started up again until both channels have been repaired. When a channel enters 50% capacity, a repair action is "planned" and then carried out. The planning time includes bringing in spare parts and repair teams. The planning time is 30 hours in which case the channel continues to operate with 50% capacity. The active repair time is so short that it can be neglected. When a channel enters 0% capacity (and the other channel is operating with 100% capacity), the planning time is compressed to 20 hours and the active repair time is still negligible. After

a system stop, the mean time to bring the system back to operation is 48 hours, irrespective of state of the system when it entered the idle state.

Record any additional assumptions you have to make to answer the questions below.

(a) Define the relevant system states. Use as few states as possible.

(b) Draw the corresponding state transition diagram (Markov diagram).

(c) Establish the transition rate matrix A for the production system.

(d) Establish the Markov steady-state equations on matrix form.

(e) Explain (briefly) what we mean by the concept steady-state probability in this case.

(f) Find the steady-state probability of the production system.

(g) Establish the Petri net model for this system.

(h) Identify markings with 100%, 50%, and 0% capacity respectively.

(i) Compare the pros and cons of using Markov method and Petri net for this particular problem and in general.

Problem 6. Case study: Gas detection system

A gas detector is assumed to have constant failure rate $\lambda_{\mathrm{DU}} = 1.6 \cdot 10^{-6}$ per hour with respect to the DU failure mode "gas detector does not raise alarm when gas is present." Assume that the failure rate with respect to the failure mode "false alarm" is $\lambda_{\mathrm{S}} = 2.1 \cdot 10^{-6}$ per hour. Further, assume that the two failure modes are independent. Record any extra assumptions you have to make to answer the questions below.

(a)

- Find the probability that the gas detector will survive 6 months without any of the two failure modes.
- Find the mean time to failure, MTTF, of the gas detector (with respect to all (both) failures).
- Explain (briefly) why the assumption of independent failure modes may be dubious in this case.

(b) Assume that one of the two failure modes has occurred. Carry out the following:

– What is the probability that this failure is a DU failure?

– Explain (briefly) how you determine this probability (or, develop the formula).

(c) Assume that the production of the gas detectors is subject to variations. When we buy a gas detector, it will have a constant DU failure rate λ_{DU}, but the failure rate may vary from detector to detector. The variation may be described by a gamma distribution with probability density function

$$f_\Lambda(\lambda_{\mathrm{DU}}) = \frac{\beta^\alpha}{\Gamma(\alpha)}\lambda_{\mathrm{DU}}^{\alpha-1}e^{-\beta\lambda_{\mathrm{DU}}} \quad \text{for } \lambda_{\mathrm{DU}} > 0 \tag{5.1}$$

The mean value of this distribution is α/β and the variance is α/β^2. Based on earlier experience, we assume that the mean value of the failure rate λ_{DU} is $1.6 \cdot 10^{-6}$ påer hour, and that the standard deviation is $0.5 \cdot 10^{-6}$ per hour. Carry out the following:

– Determine the values of α and β.

– Assume that we choose a gas detector at random from the production and find the survivor function $R_{\mathrm{DU}}(t)$ for this detector with respect to the DU failure mode.

– Determine the corresponding failure rate function $z_{\mathrm{DU}}(t)$ for the gas detector and make a sketch of the function. Discuss the result.

Problem 7. Case study: 2oo3 system

Consider the 2oo3 system that is modeled in figure 5.18 and 5.19 in the text book.

(a) Verify the formulas and the numerical results of example 5.23 (which does not include CCFs) and example 5.24 which does include CCFs.

(b) Determine the MTTF for both cases and compare the results.

Chapter 6

Reliability Data Sources

Problem 1. Reliability data types and sources
Reliability assessments require access to applicable data to support the models.

(a) Give some examples of reliability data sources that may be applicable?

(b) Discuss some of the differences between generic and application-specific data

(c) Give also some examples of standards that may be used to derive application-specific data.

Problem 2. Reliability data types and sources (Part of tutorial 2)
What are the pros and cons of using manufacturer provided data in reliability assessments at at design stage?

Problem 3. Reliability data types and sources
How can failure rates of a device be determined using FMEDA? Give a brief explanation.

Problem 4. Reliability data for Machinery
ISO 13849-1 suggests that dangerous failure rates are calculated based on the following formula for mean time to failure ofa dangerous failure ($\mathrm{MTTF_d}$):

$$MTTF_d = \frac{B_{10d}}{0.1 \cdot n_{op}}$$

where n_{op} is the mean number of annular operation of the component and $B_{10\mathrm{d}}$ is the mean number of cycles till 10% of the components fail dangerously.

Table 6.1: Influencing factors

Influencing factor	Weight	Score
Working principle	0.1	1.0
Location	0.2	1.5
Frequency of use	0.2	0.9
Environmental exposure	0.2	1.2
Frequency and quality of maintenance	0.3	1.2

The latter parameter is determined by the manufacturer based on relevant product standards for test methods (see ISO 13489 for relevant references).

(a) Give some arguments why it is reasonable to let the MTTF (and thereby the failure rate) be influenced by the number of cycles/operations per year, rather than being constant as we often assume for components that are part of safety instrumented functions (SIF) being operated on demand.

(b) The PDS data handbook (2013 edition) suggests a failure rate $\lambda_{\mathrm{D}} = 0.2 \cdot 10^{-6}$ failures per hour for relays. In ISO 13849-1 suggests that relays (with maximum load) has a $\mathrm{B}_{10d} = 400000$. How many mean annual operations would this failure rate correspond to?

(c) ISO 13849-1 also suggests B_{10d} for small load. In this case $\mathrm{B}_{10d} = 20000000$. How many annular operations does this B_{10d} correspond to? Discuss the results with respect to applicability for operation in the low demand mode.

Problem 5. Transfer of historical data for new applications (Part of tutorial 2)

A generic failure rate, as it is given in e.g. the PDS data handbook, may not necessarily capture plant-specific conditions. Brissaud et. al (2010) has suggested an approach where the generic failure rate may be adjusted, see chapter 6.5.2 in text book. Assume that an analysis has been carried out and that the following weight has been assigned for the most important influencing factors, see Table 6.1:

(a) Explain the meaning of weight and score in this model.

(b) Assume that you are considering a shutdown valve. Calculate the plant specific dangerous undetected (DU) failure rate λ_P if the generic DU failure rate, $\lambda_B = 1.9 \cdot 10^{-6}$ failures per hour.

(c) Compare the approach (at a high level) of this model with the approach used

in MIL-HDBK-217F. What are some of the differences?

Problem 6. Data dossier

(a) What do we mean by a (reliability) data dossier and what type of information is provided here?

(b) Study one specific reliability data dossier, for example the sample pages provided for the PDS data handbook at `http://www.sintef.no/projectweb/pds-main-page/pds-handbooks/pds-data-handbook/`. Explain in more detail the information provided and why this information is important in relation to a reliability assessment.

Chapter 7

Demand Modes and Performance Measures

Problem 1. PFD versus PFH

Probability of failure on demand (PFD) and average frequency of a dangerous failure per hour (PFH) are two suggested failure measures in IEC 61508.

(a) Define PFD and PFH and discuss some of the differences between the two measures.

(b) The textbook also introduces the term "Hazardous event frequency" (HEF) and relates this term to PFD and PFH. Based on these relationships: Why is it reasonable to claim that $HEF \leq PFH$ for a SIF that operates in the high-demand mode and in the low demand mode that $HEF = PFD_{avg}\lambda_{de}$, where λ_{de} is the demand frequency?

Problem 2. Demand duration and PFD

A fire extinguishing system must both start on demand (a fire) and continue distributing water as long as required to stop fire and cool down equipment. In some cases, it is specified in design for how many hours the fire extinguishing system must continue to run, once started.

(a) Why is it important to include demand duration when assessing the reliability of a SIF in this case?

(b) How would you suggest to include the prolonged demand duration in the analysis of hazardous event frequency (HEF)?

Problem 3. Safe failure fraction (SFF)
The safe failure fraction (SFF) is a disputed reliability parameter.

(a) Explain briefly what the SFF is and what it is used for

(b) Assume that you want to purchase a valve. Would the SFF be different if the valve is to be used to open on demand or close on demand? Explain your position.

(c) A SFF=99% may be obtained for a component with high dangerous failure rates as well as for low dangerous failure rates. Why is it so? Under what conditions would this statement apply?

(d) Assume that you have designed a component and that you have determined the SFF to be 72%. However, you would like to initiate a reliability improvement program to increase the SFF to 95%. What could you do and what would be the consequences (pros/cons) of your approach?

Chapter 8

Average Probability of Failure on Demand

Problem 1. Failure categories to include in assessment
Which failure mode(s) and corresponding failure rate(s) are the most important ones for calculating the PFD_{avg}, and why? (using failure classification in IEC 61508 as basis)

Problem 2. Using Taylor expansion
The PFD_{avg} of a subsystem can be calculated using exact formula or approximation formula (using Taylor series expanstion). Consider a subsystem of independent and identical channels that are voted 1oo3 with failure rate $\lambda_{\text{DU}} = 1.9 \cdot 10^{-7}$ per hour. The system is proof-tested with test interval $\tau = 8760$ hours.

(a) Set up the formulas for PFD_{avg} using (i) exact formula and (ii) approximation formula (it is not necessary to develop (ii), just set it up)

(b) Calculate the PFD_{avg} for (i) and (ii) and compare the results. Which one is the most conservative one?

Problem 3. Total PFD
The overall PFD_{avg} is normally calculated by adding the average PFD for each subsystem of the SIF. Why are we allowed to do this (with negligible inaccuracy), and in what situations should we use the exact formulas?

Problem 4. Underlying assumptions

(a) What are the underlying assuptions for using the *average* value of PFD as a reliability measure?

(b) The PFD is the (average) probability of failure *on demand*. But demand rate is not a parameter of the formula for $\mathrm{PFD}_{\mathrm{avg}}$. Why do you think *on demand* has been added to the term?

(c) Mean fractional downtime (MFDT) is another term used with the same meaning as PFD. Why may it be argued that MFDT is a better (or more prescriptive) term than PFD?

Problem 5. Selection of Methods
The $\mathrm{PFD}_{\mathrm{avg}}$ may be calculated by using one of the folloiwng methods:

- Simplified formulas (as described in the textbook)
- Simplified formulas in IEC 61508, part 6
- Fault tree analysis
- Markov analysis
- Petri nets
- Monte Carlo simulation

Mention some pros and cons related to each of these methods. Suggest some criteria that would be useful when selecting which method to use.

Problem 6. Simplified formulas in the textbook
The textbook has introduced a set of simplified formulas for PFD.

(a) It is often reasonable to regard the unknown downtime due to DU failures as the main contributors. What is meant by unknown downtime, and why is this contribution often dominating compared to other contributions?

(b) In some cases, it may also be reasonable to add contribution from known downtime due to DU failures. What is mean by known downtime in this case, and what are some of the challenges involved in setting up the formula for this contribution?

(c) There are situations where also DD failures can influence the PFD. Give some examples of such situations. Would you regard this contribution as a known downtime or unknown downtime (and why)?

(d) Indicate how you may include the contribution from DD failures for a single element and a subsystem comprising two elements voted 1oo2.

Problem 7. Fault tree analysis
Fault tree analysis is a widely used approach for reliability analysis, and many companies use their own or purchased fault tree analysis software.

(a) Many software programs may underestimate PFD. Why is this the case?

(b) What could be an alternative way to determine the PFD using conservative approximations, if you had the possibility to list all the minimal cutsets?

Problem 8. Markov analysis
Markov analysis can be a useful alternative to calculate PFD.

(a) It is possible to use Markov to derive analytical expressions for PFD, in situations where it is not so easy to set up the formulas directly from reliability block diagrams. In what situations could this apply?

(b) The long term PFD requires that we introduce a non-Markovian transition in the Markov model. Why is this the case?

(c) For those that would like to investigate on topics beyond the scope of the textbook: Multiphase Markov has been introduced as an alternative to solve the problem with the non-Markovian transition. The approach is explained in e.g. IEC 61508, part 6, and in ISO TR 12489. Give a brief explanation of this approach, using a simple system (e.g. single) as an example.

Problem 9. IEC 61508 formulas
IEC 61508 formulas introduce parameters like:

- Channel-equivalent mean downtime (t_{CE})
- Group-equivalent mean downtime (t_{GE})
- Dangerous group frequency (DGF)
- Beta factors (β and β_D)

(a) Explain briefly each of these parameters

(b) Explain their application for a single element and a subsystem of two identical elements voted 1oo2

(c) Comment the principle difference between β and β_D.

Problem 10. PDS method
The PDS method has been widely adopted in the Norwegian process industry, see `www.sintef.no/pds`

(a) Explain and discuss briefly the following terms used by the PDS method:

- Critical safety unavailability (CSU)
- Downtime unavailability (DTU)
- Probability of test-independent failure (p_{TIF})

(b) What is terms are included in PFD, and what is included in CSU?

(c) Based on the previous question: What is the main difference between CSU and PFD?

Problem 11. Comparing results of using different methods (Part of tutorial 3)
Determine the PFD_{avg} of a 2oo4 system using the following methods and the data provided in Table 7.2 in textbook:

(a) Simplified formulas, assuming DU failures only

(b) IEC 61508 formulas, including both DU and DD failures

(c) Fault tree analysis, including DU failures only

(d) Markov methods, including DU failures only

Compare and discuss the differences in the results. Note that CCFs should be included.

Problem 12. Petri Net
Consider a system of one component that may fail due to DU failure. The component is subject to regular tests.

(a) Set up the Petri Net model for the single component, that allow markings for functioning state, failed (due to DU) state and repair (state)

(b) Suggest how the regular tests may be added to this model, and include this approach into the Petri Net model.

(c) Indicate what place would be of interest for the quantification of PFDavg.

(d) Assume that the DU failure rate of the component is $\lambda_{DU} = 1 \cdot 10^{-6}$ per hour, that the mean time to repair (MTR) is 8 hours, and that the test is carried out every year (1 year is 8760 hours). Calculate the PFDavg using GRIF (google "GRIF workshop", trial version).

Problem 13. Petri Net
Consider a system of two components that may fail due to DU failures. The components are subject to regular tests.

(a) Explain the meaning of the following three types of proof tests: simultaneous tests, sequential tests, and staggered tests.

(b) Set up the Petri Net model for the situation with sequential testing

(c) Suggest in this model how you may change the model to include staggered testing

(d) Assume that the DU failure rate of the components is $\lambda_{DU} = 1 \cdot 10^{-6}$ per hour, that the mean time to repair (MTR) is 8 hours, and that the test is carried out every year (1 year is 8760 hours). For the option of staggered testing, we assume a staggered time of 3 months. Calculate the PFDavg using GRIF (google "GRIF workshop", trial version) for the two options. Compare the results.

Problem 14. Case study: Smoke detector system
A 2oo4 voted group of smoke detectors are installed in a production room. The voted group shall give a shutdown signal when at least two of the four detectors are activated. Assume that each of the smoke detectors has a constant failure rate $\lambda_{\mathrm{DU}} = 7 \cdot 10^{-6}$ per hour, with respect to the DU failure mode "unable to provide signal when sufficient amount of smoke is present."

The four detectors are tested and, if necessary, repaired once per year. It is assumed that the test and the repair times are negligible. Record possible extra assumptions you have to make to solve the following problems.

(a) Assume that the smoke detectors are independent.

- Determine the $\mathrm{PFD}_{\mathrm{avg}}$ for the voted group
- Explain verbally what $\mathrm{PFD}_{\mathrm{avg}}$ expresses

(b) Now, assume that the four detectors are not independent, but that 10% of all DU failures of a detector are common cause failures (CCFs), and assume that CCFs can be modeled by a beta-factor model with $\beta = 0.10$.

– Determine the PFD_{avg} of the 2oo4 voted group

– How much safer is a 2oo4 voted group compared with a 2oo3 voted group when $\beta = 0.10$?

– Would you recommend that a 2oo3 voted group is installed instead of a 2oo4 voted group? Justify your recommendation.

(c) Common cause failures (CCFs) represent a main contributor to PFD.

- Explain briefly why the parameter β can be interpreted as the conditional probability of multiple failures when a detector fails.
- Discus, briefly, the realism of the beta-factor model.
- Draw a sketch of the PFD_{avg} as a function of β, for $0 \leq \beta \leq 1$, and comment on the shape of the function.

(d) How many test intervals may pass before the subsystem is found in a failed state considering the situation with and without CCFs? Does the result seem reasonable?

(e) What is the mean time to the a failed state of the subsystem considering the two cases in 14(d)?

Problem 15. Case study: Gas detection system
A gas detector has constant failure rate $\lambda_{\text{DU}} = 2.4 \cdot 10^{-6}$ per hour with respect to the DU failure mode "gas detector does not raise alarm when gas is present." Assume that the failure rate with respect to the SU failure mode "false alarm" is $\lambda_{\text{SU}} = 3.5 \cdot 10^{-6}$ per hour. Further, assume that the two failure modes occur independent of each other. Record any extra assumptions you have to make to answer the questions below.

(a) Carry out the following:

– Find the probability that the gas detector survives 6 months (in continuous operation) without any of the two failure modes.

– Find the mean time to failure, MTTF, of the gas detector (with respect to all (both) failures).

– Explain briefly why the assumption about independent failure modes may be a bit doubtful in this case.

(b) The gas detector is therefore proof-tested after regular intervals of length $\tau = 6$ months. The time required to test and repair a failed detector is so short that it may be neglected. After a test/repair, the gas detector is assumed to be as-good-as-new. Carry out the following:

- Determine the PFD_{avg} for the gas detector.
- Briefly explain (with words) the meaning of the PFD_{avg}.
- How many hours per year are we not "protected" by the gas detector – when we assume that the gas detector should always be functioning?

(c) Assume now that we have four gas detectors of the same type. The four detectors are connected to a logic solver with a 3-out-of-4 (3oo4) logic. The gas detectors are tested at the same time every six months. Otherwise the same assumptions as in point (c) apply. The logic solver is assumed to be so reliable that its failure rate may be set to zero. In this question we assume that the four detectors are independent. Carry out the following:

- Find the survivor function for the 3oo4 voted group.
- Find the PFD_{avg} for the 3oo4 voted group.

(d) Now, assume that the gas detectors are exposed to common cause failures that can be modeled by a beta-factor model with $\beta = 0.08$. Carry out the following:

- Explain (briefly) what the parameter β tells us in the beta-factor model.
- Find the PFD_{avg} of the 3oo4 voted group in this case. Specify the proportion of the PFD_{avg} that is caused by independent failures and the proportion caused by common-cause failures.
- List the main strengths and weaknesses of the beta-factor model.

(e) Establish a Markov diagram for the 3oo4 system (with common-cause failures). Define the states required, the relevant transitions between these states, and include the transition rates. You may assume that no repair actions are carried out. Explain briefly how this model can be used to determine the PFD_{avg} of the system.

Problem 16. Case study: Fire pump system
Two identical fire pumps are installed with a 1oo2 configuration as part of a fire fighting system. The relevant data are given in Table 8.1

Table 8.1: Reliability data

Components	Value
DU-failure rate	$3.0 \cdot 10^{-5}$ per hour
DD-failure rate	$5.0 \cdot 10^{-5}$ per hour
Test interval	6 months
Mean repair time (DD and DU)	8 hours
β_{DD} and β_{DU}	0.1

Remember to list any additional assumptions you have to make to answer the questions below.

(a) Calculate the PFD of the pumps with IEC 61508 formula, PDS formula, and Markov model.

In a fire situation, the pumps need to run for a period of time to successfully put out the fire. If the pumps stop in this period, the fire fighting is not successful. This period of time is not accounted for in PFD calculation. During fire fighting, the pumps are normally under much higher stress than when they are idle, so the failure rate is higher. If the pumps need to run for 8 hours to put out a fire and a running pump is 10 times as likely to failure as an idle pump.

(b) What is the probability of an unsuccessful fire fighting when we know that the pump group has started?

(c) An unsuccessful fire fighting is a critical event, assume that fires break out once every second year, what is the average frequency of critical events? Discuss, and preferably show, how this measure may be calculated using e.g., an analytical approach and Markov.

Problem 17. Case study: Overpressure protection system

Consider the safety-critical system in Figure 8.1. The system is an overpressure protection system for an oil/gas pipeline. Four identical pressure transmitters are installed in the pipeline. When two of the four pressure transmitters signal high pressure, the logic solver sends signal to both shutdown valves, ESDV_1 and ESDV_2, to close. The pressure transmitters are therefore configured as a 2oo4 voted group with respect to the system's main safety function. The two valves are identical. They are kept open in normal operation and should shut the flow in the pipeline when high pressure is "detected" by the pressure transmitters. The system is a passive safety system and critical failures are only detected during

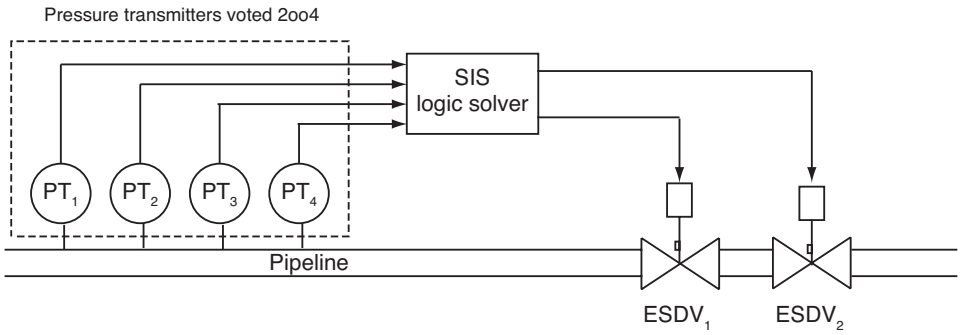


Figure 8.1: Safety instrumented system (SIS).

proof-testing. The whole system is proof-tested at the same time at regular intervals – with test interval $\tau = 1$ year.

(a) Carry out the following:

- Establish a reliability block diagram of the whole system with respect to the system's main function as a safety barrier.
- List the minimal cut sets of the system.

The two valves, ESDV_1 and ESDV_2, have two main failure modes: dangerous undetected (DU) failures and safe (S) failures. The failure rate with respect to DU failures is $\lambda_{\text{DU,V}} = 2.5 \cdot 10^{-6}$ per hour, and the failure rate with respect to S failures is $\lambda_{\text{S,V}} = 3.0 \cdot 10^{-6}$per hour. To act as a safety barrier, it is sufficient that one of the valves is functioning.

(b) Carry out the following:

- Find the mean time to a DU-failure for one of the valves
- Determine the probability that both valves survive a test interval without any failures.
- Consider one single valve, and find the probability that an S failure occurs before a DU failure.

A pressure transmitter is has failure rate $\lambda_{\text{DU,PT}} = 3.0 \cdot 10^{-7}$ per hour with respect to DU failures and failure rate $\lambda_{\text{S,PT}} = 5.0 \cdot 10^{-6}$ per hour with respect to S failures.

(c) Carry out the following:

- Explain (briefly) what we mean by a DU failure and an S failure for a pressure transmitter.

– Calculate the probability that the 2oo4 voted group of pressure transmitters survives a test interval (1 year) without any DU failures – when you assume that all items are independent.

– Calculate the PFD_{avg} for the 2oo4 voted group (when you assume that the pressure transmitters are independent – and when you assume that the time required to test and repair the transmitters is negligible).

– List and explain the assumptions you make in order to calculate PFD_{avg}.

The logic solver (LS) has failure rate $\lambda_{\text{DU,LS}} = 7.0 \cdot 10^{-7}$ per hour with respect to DU failures and failure rate $\lambda_{\text{S,LS}} = 1.0 \cdot 10^{-6}$ per hour with respect to S failures.

(d) Carry out the following:

– Calculate the PFD_{avg} of the whole system when you assume that all the items are independent.

– List the assumptions you make to calculate this PFD, and explain (briefly) what we mean by this PFD.

When a (single) signal about high pressure from a pressure transmitter is received by the logic solver, the control room is alarmed and a repair-man is sent to check and fix the problem. When the signal is "false" (safe), the repair-man needs around 2 hours to repair the problem.

(e) Carry out the following:

– Calculate the total frequency of S failures from the SIS (that give production shutdown).

– How many production shutdowns caused by S failures from the SIS must we expect during a period of 10 years?

Assume now that the pressure transmitters are not independent, but that they are exposed to common-cause failures that can be modeled by a beta-factor model. Assume that the β-factor with respect to DU-failures is $\beta_{\text{DU,PT}} = 0.10$ while the β-factor with respect to S-failures is $\beta_{\text{S,PT}} = 0.25$. The two shutdown valves and the logic solver are still assumed to be independent.

(f) Carry out the following:

– Calculate the PFD_{avg} of the system.

– Calculate the frequency of shutdowns caused by S failures in the SIS.

– How many production shutdowns caused by S failures from the SIS must we now expect during a period of 10 years?

Problem 18. Case study: Overpressure protection system at a chemical plant In a chemical process plant, several compounds are mixed in a chemical reactor. Here, we consider the pipeline where one of these compounds is fed into the reactor. If too much of this compound enters into the reactor, the mixture will come out of balance and the pressure in the reactor will increase. This is a very critical event and is controlled by the safety instrumented system (SIS) illustrated in Figure8.2. Three flow transmitters are installed in the pipeline. When at least two of the three flow transmitters detect and alarm "high flow", a signal is sent to the main logic solver that will transmit a signal to close the two shutdown valves in the pipeline. In addition, three pressure transmitters are installed in the reactor. When at least two of the three pressure transmitters detect and alarm "high pressure", a signal enters the main logic solver that will transmit a signal to close the two shutdown valves in the pipeline – and stop the flow of the compound into the reactor.

Any unplanned shutdown of the reactor, may also lead to dangerous situations, and spurious shutdowns (i.e., caused by false alarms) should therefore be avoided.

The three flow transmitters are of the same type and are, as illustrated in Figure 8.2, configured as a 2-out-of-3 (2oo3) system. In the same way, the three pressure transmitters are of the same type and also configured as a 2oo3 system. The logic solver transmits a shutdown signal to the valves if it receives a signal from either the flow transmitters or the pressure transmitters. The main logic solver is therefore a 1-out-of-2 (1oo2) configuration. It is sufficient that one of the two shutdown valves (of the same type) is able to close to stop the flow of the compound into the reactor. The shutdown valves are therefore a 1oo2 system. The 2oo3 votings for the flow and pressure transmitters are physically modules of the logic solver, even if they are drawn as separate entities in Figure 8.2.

The two shutdown valves are kept open in normal operation and should shut the flow in the pipeline when high flow or high pressure is "detected" by the transmitters. The system is a passive safety system and critical failures are only detected during proof testing (also called function testing). The whole system is proof tested at the same time at regular intervals – with test interval $\tau = 6$ months.

Record any additional assumptions you have to make to answer the questions below.

Remark:Some of these questions require that also chapters 9-12 have been covered.

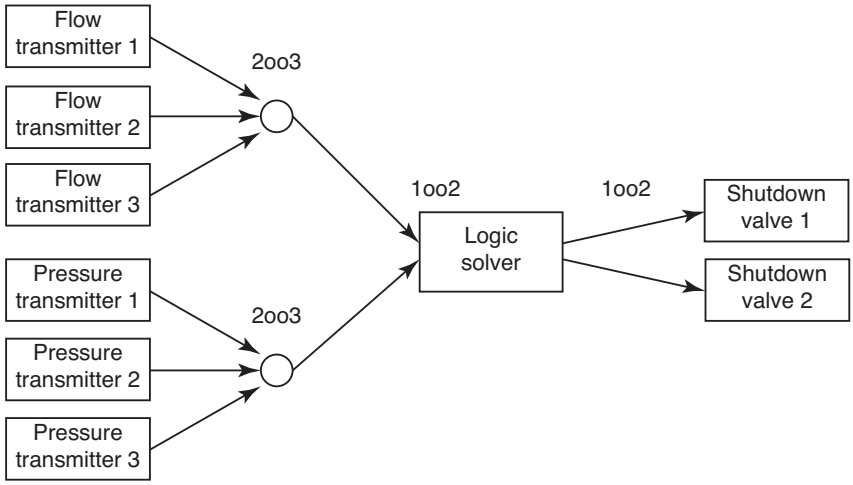


Figure 8.2: Safety instrumented system (SIS).

(a) Set up a reliability block diagram of the whole system with respect to the system's main function as a safety barrier.

(b) Explain briefly why a 2oo3 configuration of transmitters may have been chosen for this particular SIS.

For the following analyses, we consider two failure modes dangerous undetected (DU) failures and safe (S) failures. The times required for periodic proof testing and the possible repair after a failure has been detected are first considered to be negligible.

The failure rates for the various components are listed in Table 8.2.

Table 8.2: Failure rates for the SIS components in Figure 8.2.

Component	DU-failure rate (hours^{-1})	Safe failure rate (hours^{-1})
Flow transmitter	$\lambda_{\mathrm{DU,FT}} = 6.0 \cdot 10^{-7}$	$\lambda_{\mathrm{S,FT}} = 1.1 \cdot 10^{-6}$
Pressure transmitter	$\lambda_{\mathrm{DU,PT}} = 3.0 \cdot 10^{-7}$	$\lambda_{\mathrm{S,PT}} = 4.5 \cdot 10^{-7}$
Logic solver	$\lambda_{\mathrm{DU,LS}} = 1.0 \cdot 10^{-8}$	$\lambda_{\mathrm{S,LS}} = 5.0 \cdot 10^{-8}$
Shutdown valve	$\lambda_{\mathrm{DU,V}} = 2.1 \cdot 10^{-6}$	$\lambda_{\mathrm{S,V}} = 2.3 \cdot 10^{-6}$

(c) Find the probability that the whole system survives a test interval without any failures at all.

It is first assumed that all components are independent.

A consultant claims that the PFD of the system can be determined by the upper bound approximation formula.

(d) Use fault tree analysis along with the upper bound approximation formula to find the PFD of the system.

(e) Discuss (briefly) the accuracy of the result you obtain.

Another consultant claims that it would be better to first find the PFD of each of the 2oo3 transmitter subsystems by using approximation formulas and then combine these to find the system PFD.

(f) Perform this calculation. Which of the two approaches would you prefer? Will the last approach give a more correct result?

The flow transmitters are exposed to common-cause DU-failures (CCF-DUs) that can be modeled by a beta-factor model with $\beta_{\mathrm{DU,FT}} = 0.10$, and the the pressure transmitters are exposed to CCF-DUs that can be modeled by a beta-factor with $\beta_{\mathrm{DU,PT}} = 0.08$. The flow transmitter subsystem and the pressure transmitter subsystem are assumed to be independent. The two shutdown valves are assumed to be exposed to CCF-DUs that can be modeled by a beta-factor model with $\beta_{\mathrm{DU,V}} = 0.20$.

(g) Find the PFD of the whole system when you assume that the main modules of the system are independent.
Hint: We may assume no dependency between flow transmitters and pressure transmitters.

When a (single) signal about high pressure from a transmitter is received by the logic solver, the control room is alarmed and a repair-man is sent to check and fix the problem. When the signal is "false" (safe), the repair-man needs around 1 hour to repair the problem.

(h) Find the total frequency of S-failures from the SIS-system (that give production shutdown) when you assume that all safe failures are independent.

(i) How many production shutdowns caused by S-failures from the SIS must we expect during a period of 10 years?

Assume now that the transmitters are not independent, but that they are exposed to common cause failures that can be modeled by a beta-factor model. Assume that the beta-factor with respect to safe (S) failures is $\beta_{\mathrm{S,FT}} = 0.12$ for the flow transmitters, while the corresponding β-factor is $\beta_{\mathrm{S,PT}} = 0.15$. The two shutdown valves are assumed to be independent with respect to S-failures.

(j) Find the frequency of shutdowns caused by S-failures in the SIS-system. How many production shutdowns caused by S-failures from the SIS must we now expect during a period of 10 years?

Improving the reliability (unavailability) of the valve group can significantly reduce the overall PFD. One consultant suggests to introduce stagger testing for the valves as a means to reduce the PFD. It is proposed to maintain the 6 montly test interval, but always carry out the test of one valve 3 months later than the other valve.

(k) Calculate the PFD of the valve group when stagger testing is applied.

Another consultant suggests using partial stroke testing (PST) of the valves instead of staggered testing. A 60% coverage for the partial stroke test is assumed for each valve.

(l) Calculate the PFD of the valve group when PST is conducted every month.

(m) Discuss briefly the pros and cons of stagger testing and partial stroke testing, and tell us which testing technique you prefer.

Chapter 9

Average Frequency of Dangerous Failures

Problem 1. Meaning of PFH

(a) PFH is introduced as a reliability measure for safety-critical systems operating in the high-demand and continuous mode. Why is this measure a reasonable choice for this mode of operation?

(b) PFH is a frequency measure, but the abbreviation means *probability* of having a dangerous failure per hour. Why is the probability per hour introduced (what is the underlying assumptions)? Hint: Review the assumptions when setting up the formula where $PFH \approx \frac{F(T)}{T}$

(c) The formula above applies only when T is not too long. Why is this the case?

(d) PFH may be regarded as the rate of occurrence of failures (ROCOF) with respect to dangerous failures. What do we mean by ROCOF?

Problem 2. Simplified formulas for PFH as defined in textbook

(a) Demonstrate how PFH formulas are set up in the textbook for a single element and for a subsystem of two elements voted 1oo2. Explain briefly how DU failures and DD failures, including CCFs, are incorporated into the formula.

(b) Under what assumptions can we disregard the contributions from DD failures?

Problem 3. Simplified formulas for PFH in IEC 61508, part 6

(a) PFH is the dangerous group frequency (DGF) already introduced in rela-

Table 9.1: Failure rates for the PSD system components in Figure 9.1.

Component	DU-failure rate (hours^{-1})	β
Pressure transmitter (PT)	$\lambda_{\mathrm{DU,PT}} = 3.0 \cdot 10^{-7}$	5%
Logic solver (LS)	$\lambda_{\mathrm{DU,LS}} = 1.0 \cdot 10^{-7}$	
Shutdown valve (XV)	$\lambda_{\mathrm{DU,V}} = 2.1 \cdot 10^{-6}$	10%

tion to PFD formulas. What is the main difference between DGF in the high-demand/continuous demand mode and the low-demand mode? Include one example.

(b) Under what assumptions can we disregard the contributions from DD failures?

(c) Explain how to set up the formula for a single element and for a subsystem of two elements voted 1oo2. Explain briefly how DU failures and DD failures, including CCFs, are incorporated into the formula.

Problem 4. Determine PFH from Fault tree analysis

(a) How may the PFH be calculated using fault tree analysis?

(b) PFH may also be calculated on the basis of the Birnbaum measure. Briefly explain this approach, and indicate any advantages of using this approach.

Problem 5. Case study: Process shutdown system (Part of tutorial 4)

Most systems in the process industry are designed such that the demand for a process shutdown is rather infrequent (<<once per year), therefore most process shut down (PSD) systems are operated in the low demand mode and their reliability are quantified by PFD. Due to more extensive use of automatic trips, one may find that PSD systems on oil and gas installations offshore are demanded more often than once per year (up to once per month). In such a situation, it may be reasonable to calculate the PFH rather than the PFDavg.

Consider a PSD function that shall close one shutdown valve (XV) upon pipeline pressure above specified setpoint, as shown in Fig. 9.1. The pressure transmitters are voted 1oo2. All the components are proof tested at the same time with an interval of 12 months. The failure data of the components are given in Table 9.1, and for simplicity we include the contribution from DU failures only.

(a) Set up a reliability block diagram for the PSD function.

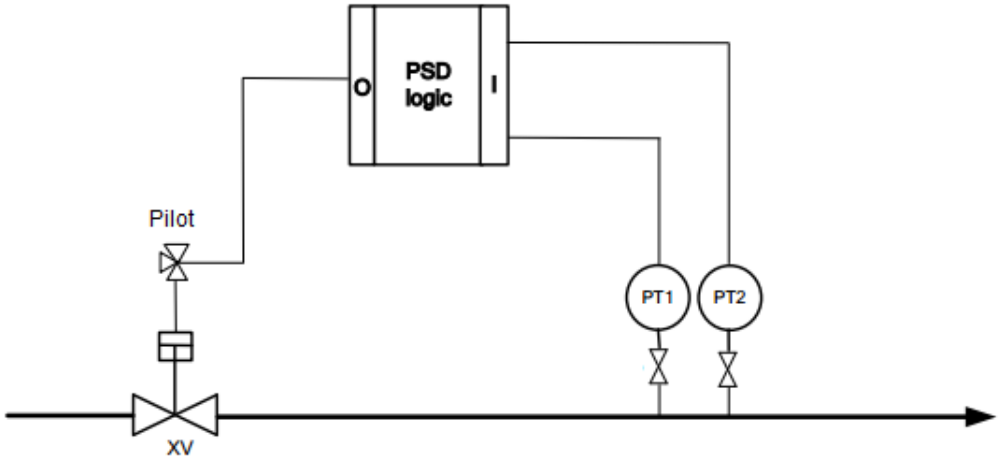


Figure 9.1: Process shutdown (PSD) function

(b) Calculate the PFH using what is referred to as simplified formula presented in the SIS book and the IEC 61508 formulas. Since no information is provided about DD failures, we ommit these failures from the calculations.

(c) Assume that demands occur with some months between (but still more often than once per year, on the average). Is it reasonable to also use PFDavg for this function, despite being in the high demand mode?

A high pressure pipeline protection system (HIPPS) is installed as a secondary protection of the pipeline, as shown in Fig. 9.2. The HIPPS has a logic solver that is separated from the PSD system, and dedicated pressure transmitters and shutdown valves. The setpoints of the HIPPS pressure transmitters (voted 2oo3) are set slightly higher than for the PSD function.When a demand occurs, the PSD function shall respond first, and a HIPPS response is required only in the situation where the PSD function fails.

We assume for simplicity that different types of pressure transmitters and valves are selected for the HIPPS and the PSD system, so that dependency between the PSD system and the HIPPS system can be disregarded.

(d) Set up a reliability block diagram for the HIPPS function.

(e) Assume that the PSD function is demanded on the average 2 times per year. What is the average demand rate for the HIPPS system? (hint: You may want to calculate the PFDavg for the PSD function in this case, to find the probability of being down in the test interval).

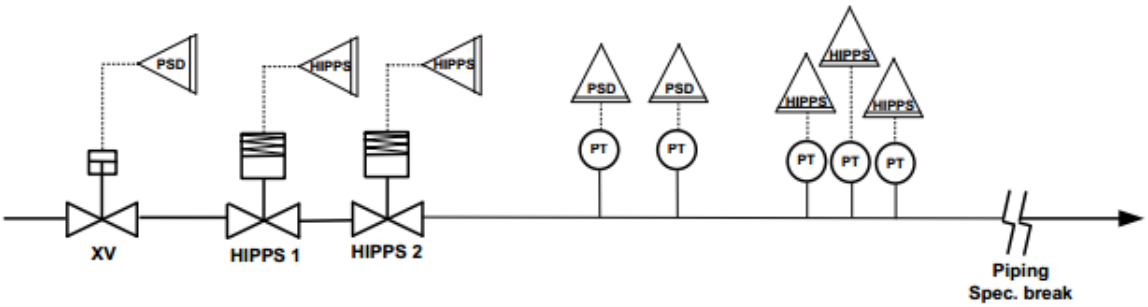


Figure 9.2: Pressure protection systems for a pipeline section.

(f) Calculate the PFD for the HIPPS systems using simplified formulas and IEC 61508 formula and the formula presented in the book. Since no information is provided about DD failures, we ommit these failures from the calculations.

(g) Assume that a tolerable frequency of overpressuring the pipeline is $1 \cdot 10^{-5}$ per year. Will the PSD system and the HIPPS system provide the necessary risk reduction? What could you do if they don't?

Problem 6. Determine PFH from Markov model (Part of tutorial 4)

Consider the Markov model in Figure 9.5 in textbook, and also shown in Figure 9.3.

The states are shown in Table 6:

State	State description
0	Both channels are functioning (OK)
1	One channel has a DD-fault, one is OK
2	One channel has a DU-fault, one is OK
3	Both channels have DD-faults
4	Both channels have DU-faults
5	One channel has a DD-fault and the other a DU-fault
6	The EUC is brought to a safe state (upon double DD fault)

(a) Add the transitions needed to prepare the model for calculating steady-state

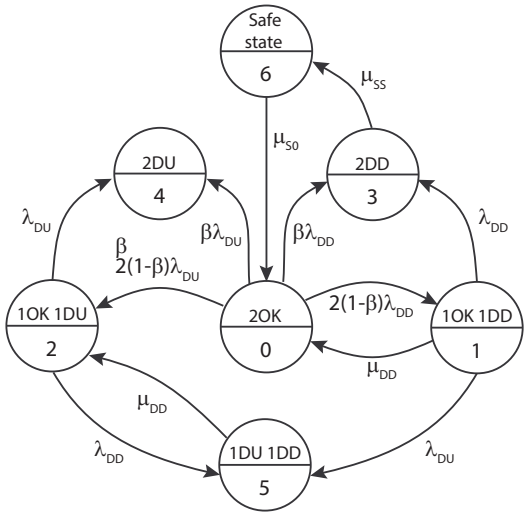


Figure 9.3: Markov model for a 1oo2 system exposed to DU and DD failures

solution for PFH. Explain the meaning of each added transition.

(b) Set up the equation for PFH (as a function of the steady state probabilities)

(c) Insert data from table 7.2 in SIS book, and calculate the average PFH in a test interval.

Chapter 10

Common-Cause Failures

Problem 1. CCF definition and interpretation

(a) Elaborate on the meaning of a CCF, using e.g. the definition in the text book as basis.

(b) What is a root cause and a coupling factor, and why are these two terms useful when explaining why CCFs occur?

(c) It is possible to argue that a CCF is sometimes a systematic (multiplicity of) failure and sometimes a random failure? Why is this the case?

Problem 2. Properties of beta factor model
The standard beta-factor model is often a preferred way to include CCFs, due to its simplicity. However, the model has some non-realistic properties:

(a) Comment on the effect on the independent failure rate when introducing measures to reduce the value of β. Why is this effect questionable?

(b) A 1oo3 voted system and 2oo3 voted system would obtain approximately the same value for PFD, assuming identical components and CCFs. Why is this the case, and what is the realism in having this effect on the PFD? In what situations would the effect be realistic scenario, and in what situations would it be less realistic?

Problem 3. C-factor model

(a) Describe and discuss the main differences between the beta-factor model and the C-factor model.

(b) In some cases, it may be argued that the C-factor model is more realistic than the beta-factor model. Why is this the case?

Problem 4. Extensions of beta factor model

(a) Describe and discuss the main differences between the beta-factor model and the PDS model.

(b) Study the C_{MooN} formula and verify some of the values in the table for C_{MooN} presented in the PDS method

Problem 5. Effects of CCFs
Consider 1oo3 and 2oo3 architectures and reflect on how vulnerable of CCFs with respect to dangerous failures and spurious (unintended) activations.

Problem 6. Determining the value of beta
Checklists are sometimes used to determine the value of the beta factor.

(a) Explain the approach advocated in IEC 61508-6 for determining beta

(b) Compare this approach with the approach by Humphrey that is included in the textbook. Which one do you think is better, and why?

Problem 7. Other CCF models

Consider a 2oo3 architecture may fail due to independent failures, external non-lethal shocks, and external lethal shocks.

Parameter	description	Value
$\lambda^{(I)}$	Internal (independent) failures	$2 \cdot 10^{-5}$
$\lambda^{(L)}$	External lethal shocks (causing *all* components to fail)	$1 \cdot 10^{-6}$
$\lambda^{(S)}$	External non-lethal shocks causing x components to fail	$1 \cdot 10^{-5}$
P	The probability that a component fails given the shock	0.25
τ	Test interval	3730

For the non-lethal shocks: Assume that X, the number of component failures given a shock, is distributed binomial with parameter (n, P), where n is the number of components failing and P is the probability that a component fails given the shock respectively.

(a) Explain how you will calculate the PFD_{avg} (set up the formula).

(b) Make a reflection on the way CCFs are included here versus in the standard beta factor model and the PDS CCF model.

Problem 8. Case study: Gas detector system
Consider a voted group of four identical detectors. The DU-failure rate of a detector is $\lambda_{\mathrm{DU}} = 2.5 \cdot 10^{-6}$ per hour. The four detectors are tested and, if necessary, repaired once per year. It is assumed that the test and the repair times are negligible. Record possible extra assumptions you have to make to solve the following problems. Assume that the four detectors are not independent, but that 10% of all DU-failures of a detector are common cause failures (CCFs), and assume that CCFs can be modeled by a beta-factor model with $\beta = 0.10$.

(a) Determine the $\mathrm{PFD}_{\mathrm{avg}}$ of the 2oo4 voted group

(b) How much safer is a 2oo4 voted group compared with a 2oo3 voted group when $\beta = 0.10$?

(c) Would you recommend that a 2oo3 voted group is installed instead of a 2oo4 voted group? Justify your recommendation.

(d) Explain briefly why the parameter β can be interpreted as the conditional probability of multiple failures when a detector fails.

(e) Discuss, briefly, the realism of the beta-factor model.

Problem 9. Case study: Use of different CCF models
Consider a 2oo3 voted group of identical channels. Let $\lambda_{\mathrm{DU}}^{(i)}$ be the rate of channel DU-failures caused purely by natural aging. These failures are assumed to be independent. A consultant claims that the causes of the natural aging failures can be considered as internal shock processes within the channels, and these processes are independent between the channels. Let ρ be the rate of external shocks that might cause a DU-failure of a cannel. If such a shock occurs, assume that there is a probability p that each channel will get a DU-failure. Assume that given a shock, the channels fail independent of each other, hence the number of channels failing is binomial distributed with parameters $n = 3$ and p. The following parameter values are assumed: $\lambda_{\mathrm{DU}}^{(i)} = 1.5 \cdot 10^{-6}$ per hour, $\rho = 10^{-7}$ per hour, and $p = 0.5$.

(a) Compare the model described above with (i) the PDS model, and (ii) the standard beta-factor model when $p = 1$. Describe similarities and differences.

(b) Determine the total DU-failure rate of a single channel in this model. Further, determine the total rate of single DU-failures, double DU-failures and triple DU-failures for the three channels (when both natural aging and external shock failures

are considered).

(c) Establish a Markov model for possible transitions within one test period, and find the $\mathrm{PFD}_{\mathrm{avg}}$ when the test interval τ is 6 months.

Hint: After a DU-failure, there will be only two channels left, and n in the binomial distribution is reduced to two.

(d) When using the beta-factor model, the effect adding more redundancy is very small. What would we gain by introducing four channels, and vote them 2oo4, when using the above shock model? (You may use approximation formulas). Discuss what will be the result when $p \to 1$?

Chapter 11

Imperfect Proof-Testing

Problem 1. Importance of partial and imperfect testing

(a) What is the difference between partial and imperfect testing?

(b) The effect on reliability may be positive if introducing partial testing. Why is this the case?

(c) What is the meaning of partial and imperfect test coverage, and what would influence the value that this coverage factor takes in each case?

(d) The effect of introducing partial stroke testing for shutdown valves may be used enhance reliability or to reduce operating costs. Explain how you would apply partial stroke testing for achieving each of these two purposes (you may use a single element as basis for the explanation)

(e) The effect on reliability may be underestimated if *not* including the effect of imperfect testing. Why is this the case?

(f) Partial testing and imperfect testing is mainly an issue with safety-critical systems operating in the low-demand mode. Why is this the case? Can you foresee situations where it would be reasonable to also include the contribution for safety-critical systems operating in the high-demand and continuous demand mode?

(g) The approach to model perfect and imperfect testing into the formula for PFD is the same. Explain the main principles for how this can be done.

Problem 2. Different PST implementations

Partial stroke testing of a valve is a partial proof test designed to operate the

valve partially at regular intervals. This means that the valve is moved e.g. 20% of its full stroke, before returned to its initial (open) position. Since the partial operation does not cause any significant disturbances in the process, it is possible to carry out this type of testing more often than a full proof test. Partial stroke testing of HIPPS valves was introduced for the HIPPS system subsea at the Kristin field (see the case study for more details).

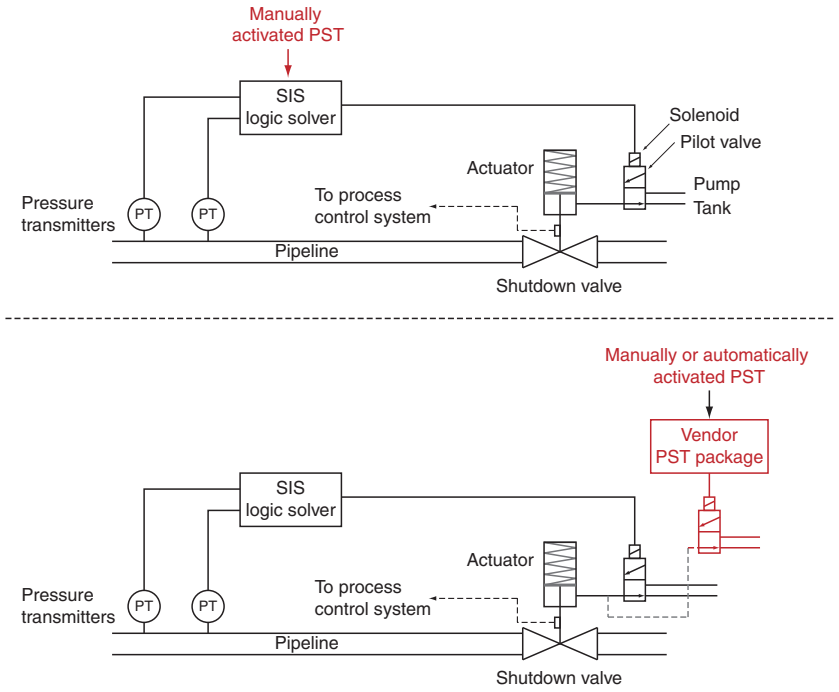


Figure 11.1: Two alternative implementations of PST

One out of possible implementations may be selected, see Fig. 11.1:

1. PST activated via SIS/HIPPS logic solver: A timer starts to count when the power is removed to the solenoid, and which repower the solenoid when the timer has reached its setting.

2. PST activated via vendor/manufacturer "package" for partial stroke testing: Separate PST circuit is directly interacting in the hydraulic supply to the valve.

(a) Why do you think partial stroke testing may be a desired option?

(b) What are the pros and cons of each of these options?

Failure mode	Revaled by PST?
Fail to close (FTC)	
Delayed operation (DOP)	
Leakage in closed position (LCP)	
Premature closure (PC)	
Fail to open (FTO)	
Leakage to environment (LTE)	

Figure 11.2: Failure modes of a shutdown valve

Table 11.1: Data for shutdown valve

Failure mode	DU	%Revaled by PST	Importance/weight
FTC	x	100%	30%
DOP	x	20%	30%
LCP	x	0%	15%
PC		NA	10%
FTO		NA	10%
LTE		NA	5%

(c) Assume that the following failure modes are applicable for the valve, see Figure 11.2. Which ones of these may be revealed by partial stroke testing?

Problem 3. Determine PST coverage

Assume that you have been given the following data for a shutdown valve, and you are asked to use this as input for determining the partial stroke test coverage.

(a) What do we mean by partial stroke test coverage, and what are the factors influencing its value?

(b) What is the partial stroke test coverage, Θ_{PST}, using the data in Table 11.1?

(c) Assume that the DU failure rate is $8 \cdot 10^{-6}$ failures per hour. What is the DU failure rate revealed by full proof test, $\lambda_{DU,FT}$, and what is the DU failure rate,$\lambda_{DU,PST}$, revealed by partial stroke testing?

Problem 4. Assume now that you have calculated the PST coverage factor and

the DU failure rates from from Problems 3(b) and 3(c) .

(a) Calculate the effects of introducing partial stroke testing compared to not using partial stroke testing (give also the percentage reduction). You may assume that the partial stroke testing is carried out every month (every 730 hours), and the full proof test every year (8760 hours).

Problem 5. We often say that partial stroke testing can be used for either improving safety or reducing costs.

(a) How would you explain this statement with basis in the formula for PFD_{avg}?

Assume now that the PFD requirement (and thereby the SIL requirement) was developed under the assumption that the HIPPS function is subject to *full* proof test every 6 months, and no PST implemented (you may now calculate the PFD_{avg} using this assumption). Consider the simplified HIPPS architecture with 1oo2 voted pressure transmitter, a single logic solver, a single solenenoid valve, and a single shutdown valve. The DU failure rate of the pressure transmitters is $5 \cdot 10^{-6}$ per hour, the DU failure rate of the logic solver $1 \cdot 10^{-7}$ per hour, and the DU failure rate of the solenoid valve is $4 \cdot 10^{-6}$ per hour. The beta factor for the pressure transmitters is assumed 5%.

(b) Consider the two alternative implementations of PST introduced in Problem 2. How would you calculate the PFD_{avg} for these two SIFs, when including the effects of PST. You may use the PST coverage factor for the valve as calculated in Problem 3(b) for both options, but you may want to make other assumptions about the PST coverage factor of the solenoid valve.

(c) How much can you extent the full proof test, when PST is added (consider e.g., option 1), without comprimising the required PFD_{avg}? Would you recommend this new interval? We assume that PST is carried out every month.

(d) Assume now that you consider two valves voted 1oo2 (rather than one valve voted 1oo1). How would you calculate the PFD_{avg} in this case (consider the valves only, and not the rest of the SIF).

Chapter 12

Spurious Activation

Problem 1. Meaning of spurious activation

(a) What is the meaning of spurious activations, and why is this type of activation of relevance to consider for a safety-critical system?

(b) It is sometimes suggested to distinguish between the following three types of spurious activations:

- Spurious operation
- Spurious trip
- Spurious shutdown

What is the difference between these terms, and why may it be important to distinguish them?

(c) What do we mean by the spurious trip rate (STR), and what failure rates may be included in the calculation of this measure?

(d) Give one example for how the STR formula is set up for a subsystem comprising three elements, voted e.g. 1oo3. Explain in each case, the different types of contributions.

(e) Assume that you have identified value for β for e.g. pressure transmitters. Would you use this value for safe as well as for dangerous failures? Why or why not?

Problem 2. Case study: High integrity pressure protection system (HIPPS)

Consider a HIPPS system comprising four pressure transmitters voted 2oo4, one logic solver, and two shutdown valves voted 1oo2 located subsea.

(a) Consider the pressure transmitters and discuss the interpretation of the terms spurious operation, spurious trip, and spurious shutdown in relation to these.

(b) It is suggested that both DD and spurious operation (SO)/safe failures may result in spurious trips. Why do you think that DD failures are considered?

(c) What is the hardware fault tolerance (HFT) of the 2oo4 system with respect to spurious trips (hint: A 2oo4 system means that 2-out-of-4 elements must carry out the function in order for the SIF to be carried out. In relation to spurious trips, the function is "to avoid spurious trips", so the question should be: How many spurious operation failures are tolerated without getting a spurious trip of the SIF?) What is the HFT for a general $k$oo$n$ system with respect to spurious trips.

(d) Common cause failures may also be an issue with spurious trips, and we may introduce β_S for this purpose (considering just only spurious operation failures). Why is it reasonable to assume that β_S may be different from β (for DU failures) and β_D (for DD failures). Give some examples, using either pressure transmitters or shutdown valves as examples.

Assume that SO failure rates for pressure transmitters, logic solver, valves are $1 \cdot 10^{-6}$, $1 \cdot 10^{-7}$ and $1 \cdot 10^{-5}$ respectively. β_S is set to 5% for all components. Assume further that the downtime of a channel after an SO failure is 6 hours. For the missing ones use input data from table 7.2 in textbook.

(e) Calculate the total spurious trip rate for the HIPP system, by consider SO and DD failures only, but exclude the contribution from false demands. Indicate the percentage contribution from the independent part and the CCF part for each subsystem.

(f) Calculate the probability of having exactly 1 (spurious) failures during a period of 5 years?

(g) How many spurious trips due to spurious operation of the valves will you, on the average, experience in a period of 5 years, if $\lambda_{\mathrm{SO}} = 1 \cdot 10^{-5}$? Would you find this result satisfactory? If you don't, what could you recommend to the engineering department? Some control question to base your discussions:

- Would a change in test interval matters?
- Would a more reliable valve type help?

- Would you recommend that a 2oo2 configuration was chosen instead, to reduce the contribution from spurious trips?

Problem 3. Case study: Shutdown valves
Assume that a SIF includes two shutdown valves, voted 1oo2. The two valves are of identical type with failure rate $\lambda_{DU} = 1.9 \cdot 10^{-6}$ failures per hour. The safe (spurious) failure rate for this type of valve is $\lambda_{DU} = 2.3 \cdot 10^{-6}$ failures per hourThe valves are tested every year (one year corresponds to 8760 hours). The demand rate is assumed to be 0.1 per year.

(a) What is the probability that the subsystem of two valves survives the proof test interval without any DU failure?

(b) Assume that a DU failure has been found in one of the proof tests. What is the probability that no demand will occur while this DU failure is present?

(c) How many tests will be carried out before one of the valves has a spurious failure?

(d) What is the probability that exactly one spurious trip failure is experienced for the two valves in a period of 50 years?

(e) What is the probability that one or more spurious trips have been experienced for the two valves in the 50 years period?

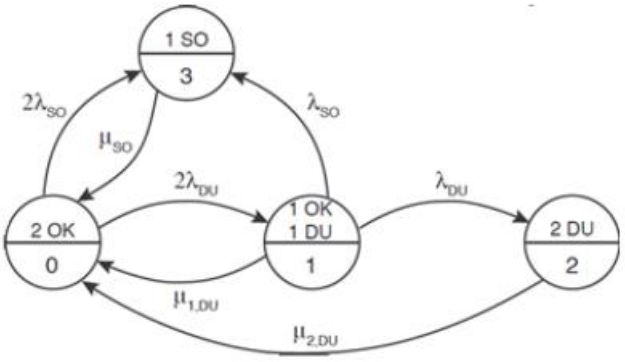


Figure 12.1: Markov model considering spurious trips

Problem 4. Using Markov to calculate STR

Calculate the STR for the Markov transition diagram shown in Figure 12.1. Use input data from table 7.2 in the textbook for the ones not given in problem 1.

Chapter 13

Uncertainty Assessment

Nothing yet.