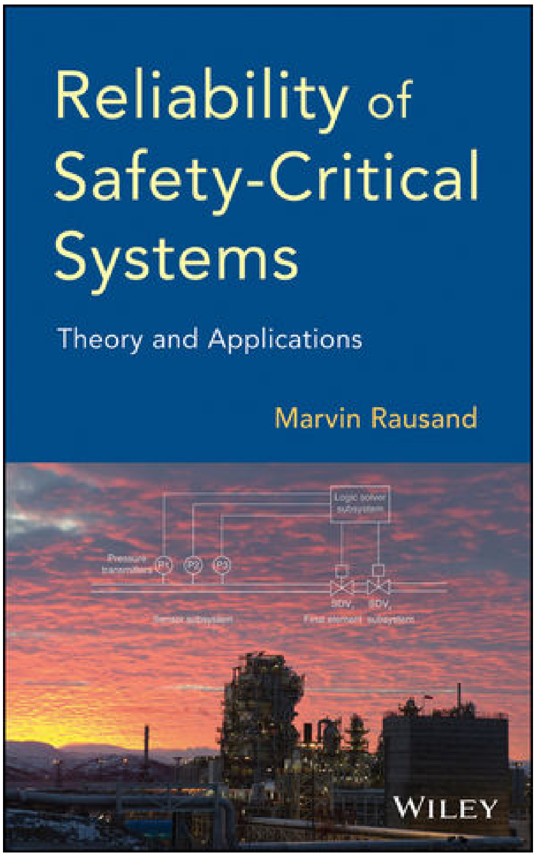
Problems for:



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

Marvin Rausand Mary Ann Lundteigen

(Version 0.001)

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 each of the 14 chapters of the book. In addition, we have included problems that cover topics from several chapters in Chapter 15.

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.

Solutions to the problems are currently not available but we hope to find time to provide solutions a bit later.

This booklet is always under construction. If you have downloaded the file, please check that you have the most recent version (Version number appears on the front page).

Marvin Rausand	Mary Ann Lundteigen
`marvin.rausand@ntnu.no`	`mary.a.lundteigen@ntnu.no`

Chapter 1

Introduction

Problem 1.

(a) Define and interpret the following terms:

- Safety-critical system
- Safety-related system
- Functional safety

(b) Explain how a safety instrumented system (SIS) is related to these three specific terms.

Problem 2. 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) Based on an Internet search, list sector-specific standards to IEC 61508

Problem 3. IEC 61508 is applicable in some situations, even in the presence of a sector-specific standard. Describe the relationship between IEC 61508 and the sector-specific standards. You may use the process sector standard IEC 61511 as an example.

Problem 4. IEC 61508 is said 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?

Problem 5. IEC 61508 takes a lifecycle approach in the structuring of requirements. List the main phases suggested in the standard and discuss why it may be reasonable to define requirements for the whole life cycle of a system.

Problem 6. What is the main difference between safety-instrumented systems (SISs) as the term is defined in IEC 61511 and conventional safety devices such as pressure safety valve?

Problem 7. Safety barrier is an important term and concept within the discipline of risk assessments, and is closely linked (but not limited to) to terms already introduced such as safety-critical system, safety-related system, and safety instrumented system.

(a) Explain what we mean by the term *safety barrier*

(b) List safety barriers in (or related to) an automobile

(c) What is the main difference between a *proactive* and a *reactive* safety barrier?

(d) Classify the automobile safety barriers as proactive and reactive and explain why each safety barrier is proactive or reactive

(e) Describe the main difference between an *active* and a *passive* safety barrier. Classify the automobile safety barriers as active versus passive.

Problem 8. 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 9. Fail-safe principles

(a) Explain what we mean when we say that a valve is *fail-safe*.

(b) Describe the main differences between the design principles *energize-to-trip* and *de-energize-to-trip*.

(c) Are any of the automobile safety barriers designed according to the de-energize-to-trip principle? Explain and give example(s).

Problem 10. Safety-instrumented systems in the process industry

(a) Give several examples of safety-instrumented systems that are typically used in a process plant.

(b) For some of the safety-instrumented systems from item (a), list typical input elements and typical final elements. Provide brief descriptions.

Chapter 2

Concepts and Requirements

Problem 1. Define the following terms, and discuss any relationships between them:

(a) Safety instrumented function (SIF)

(b) Safety instrumented system (SIS)

(c) Safety integrity level (SIL)

(d) Average probability of failure on demand (PFD_{avg})

Problem 2. A SIS may be split into three subsystems: sensors or input elements, logic solver, and final (or actuating) elements. In this problem, we assume that the system includes: Pressure transmitter, a programmable logic controller (PLC), a solenoid operated hydraulic valve and a shutdown valve (including hydraulic operated actuator).

(a) Describe the main functionality of these devices

(b) Describe how these devices are interconnected, using e.g., a simple functional block diagram

Problem 3. A safety instrumented system (SIS) is installed to protect an *equipment under control* (EUC). Give examples of possible EUC in relation to:

(a) Medical treatment

(b) Robotizised manufacturing

(c) Oil and gas production wells

(d) Container lifting operations

(e) Railway transportation

(f) Car driving
List your assumptions for each item.

Problem 4. Define and explain the main terms used to describe a SIS and the relationships between the various terms.

(a) Subsystem

(b) Voted group

(c) Safety loop

(d) Channel

(e) Element

(f) Barrier

Problem 5. Redundancy is often introduced in the design of SIS.

(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 6. Redundancy may be realized in different ways. *How* it is realized may be expressed by its voting.

(a) What do we mean by k-out-of-n ($k$oo$n$) voting? Give some examples.

(b) How would you interpret the number $n - k$?

(c) Fault tolerance may be defined as the number of faults tolerated without affecting the execution of a SIF. If you have four independent and identical channels, these may be configured as 1oo4, 2oo4, 3oo4, or 4oo4. Which of these configurations has the highest fault tolerance and which has the lowest fault tolerance?

(d) Subsystems with high fault tolerance are often prone to spurious/unintended activations. Which configuration would you choose for a sensor subsystem if you would like to balance fault tolerance and resistance against spurious/false activation? Explain why.

Problem 7. Voting of sensors is often set up in the logic solver, meaning that it is the logic solver that compares sensor readings and decides if k-out-of-n ($k$oo$n$) readings have exceeded a predefined setpoint. This approach is often not applicable for final elements. Explain the phyiscal meaning of two valves being voted 1-out-of-2 (1oo2) and 2-out-of-2 (2oo2). Hint: Draw a pipeline system and place the valves according to how they are voted in order to fulfill the function "stop flow".

Problem 8. Hardware fault tolerance is a conept 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 9. 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) Give examples of safe states in some application areas

(c) Are there any applications where a safe state does not exist? Explain.

Problem 10. 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 11. 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 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 principle difference between a SIL requirement and the SIL performance that is estimated for a SIF?

Problem 12. 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 leads 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 13. Read paragraph A.3.1 "Process segregation through PSD" in NOG 070 (accessed from `http://www.norskoljeoggass.no/en/Publica/`). 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 14. 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 15. Average probability of failure on demand, PFD_{avg}

(a) Explain (with words) what we mean by PFD_{avg}

(b) In which cases is PFD_{avg} the recommended reliability measure in IEC 61508, and give some arguments why this may be a reasonable reliability measure in this case?

(c) A subsystem has $\text{PFD}_{\text{avg}} = 5.0 \cdot 10^{-3}$. If the subsystem should be in continuous operation, how many hours per year will the subsystem be in a dangerous fault state (on the average)?

(d) A subsystem is in a dangerous fault state on the average 13 hours per year. What is the PFD_{avg} of the subsystem?

(e) What might the rationale be, according to your opinion, for using the average PFD instead of the time-dependent PFD (i.e., $\text{PFD}(t)$) as reliability measure? Give some pros and cons.

Problem 16. Average frequency of dangerous failures per hour, PFH, is an alternative to using PFD_{avg}, in the high demand or continuous mode of operation.

(a) Explain(with words) what we mean by PFH?

(b) In which cases is PFH the recommended reliability measure in IEC 61508, and give some arguments why this reliability measure is a better choice than the PFD_{avg} in this particular case.?

(c) In which cases do *you* consider PFH to be a more suitable reliability measure than PFD_{avg}?

(d) Assume that $\text{PFH} = 2 \cdot 10^{-6}$ per hour and that the demand rate is $\lambda_{\text{de}} = 2 \cdot 10^{-4}$ per hour. What does this tell about the safety of the system?

Problem 17. 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 PFD_{avg} of the SIF?

Problem 18. 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 19. 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 $\text{PFD}_{\text{avg}} = 9.9 \cdot 10^{-4}$ such that the SIL 3 requirement is fulfilled. Which conditions must be fulfilled to also fulfill the SIL 3 requirement when using PFH as reliability measure?
Hint: Because PFD_{avg} can be interpreted as the mean dangerous downtime per time unit, it can be calculated as the average frequency of dangerous failures (i.e., PFH) times the mean downtime associated with each dangerous failure.

(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). What issues do you see when you want to pick such a target value?

Problem 20. It is important with precision in the application of terminology.

(a) Is it correct to say they a SIS has SIL 3? (explain why)

(b) Is it correct to say that a subsystem fulfills SIL 2? (explain your rationales)

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

Problem 21. The identification of safety instrumented functions normally starts with a hazard and risk assessment.

(a) What do we mean by the term *hazard*? List some typical hazards related to an EUC in the process industry.

(b) What is the difference between a hazard and an hazardous (or undesired) event?

(c) Mention some methods that can be used to identify hazards and undesired events.

(d) What are the main steps of a risk analysis, and at what step is the reliability targets for safety instrumented functions (SIFs) formulated?

(e) What is a *risk metric*? Give examples of some risk metrics and discuss the transition from such metrics to reliability metrics for SIFs (PFD_{avg} or PFH).

(f) What do we mean by *tolerable* risk?

(g) Explain briefly the main elements of the ALARP principle. Discuss how the ALARP principle may affect the choice of SIL requirements.

Problem 22. 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.

(e) The SIL requirements in NOG guideline 070 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 23. A SIL requirement gives the target range of the PFD_{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 24. Safety requirement 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 25. 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 26. 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.

Chapter 3

Failures and Failure Analysis

Problem 1. 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 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 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. 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. 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. 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) Systematic faults are sometimes called *nonphysical* faults? What is meant by this?

(e) Describe the main differences between random hardware failures and systematic failures/faults.

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

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

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

Problem 6. 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?

Chapter 4

Testing and Maintenance

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

(a) Why is 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. 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. 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 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. 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. Diagnostic coverage (DC) is an important attribute of electrical/ electronic/ programmable electronic (E/E/PE) technology.

(a) What do we mean by *diagnostic coverage* (DC)?

(b) Why is it fair to say that DC is (usually) not applicable with non-E/E/PE technology, such as e.g., valves.

(c) What is the difference between DC and proof test coverage? (for example: Under what conditions would a detected dangerous failure be attributed to DC rather than proof test coverage, and vis versa)?

(d) The IEC 61508 standard (and IEC 61511) give requirements on how to act upon failures that are detected by diagnostics. Give some examples of such requirements.

(e) Tests may be manual, automatic or semi-automatic. In what category would you place failures detected by diagnostics?

(f) Test may be also carried out online or offline. In what category would you place failures detected by diagnostics.

Problem 7. It may be argued that real or false/spurious demands can be treated as a test.

(a) Under what conditions may it be argued that a demand can be credited as a full proof test?

(b) Under what conditions may it be argued that a demand is a partial proof test (in the meaning of covering only a part of the safety instrumented function)

Problem 8. There are different strategies for*how* proof tests are carried out.

(a) Staggered testing is sometimes introduced to enhance reliability. Why can it be argued that staggered testing improves reliability of a safety instrumented function?

(b) Sequential testing is perhaps the most commonly used approach for carrying out proof testing. Why do you think this is the case?

(c) Simultaneous testing is often not preferred, sometimes with the argument of being an unsafe way of carrying out the test and other times with the argument of requiring two long downtime (depending on whether inputs or or outputs are tested separately). Why do you think these arguments are used?

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

Problem 10. 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.

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

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

(a)

- Explain what we mean by the concept *minimal cut set* in a reliability block diagram.
- 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):
$p_1 = 0.90$, $p_2 = 0.95$, $p_3 = 0.85$, $p_4 = 0.90$, $p_5 = 0.80$.

(c) Find the system reliability p_S.

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

(a)

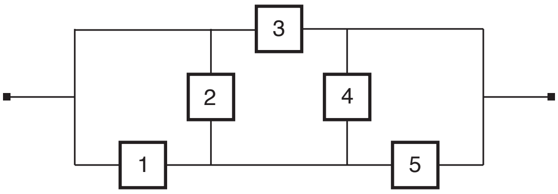


Figure 5.1: Reliability block diagram, Problem 1.

Six components with bridge

Figure 5.2: Reliability block diagram, Problem 3.

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

(b)

- 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. 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) System reliability:

- 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. 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.

Table 5.1: Failure rates for Problem 6.

Symbol	Failure rate (per hour)
LT	$6.0 \cdot 10^{-4}$
LIC	$5.0 \cdot 10^{-5}$
LICV	$3.0 \cdot 10^{-3}$
SV	$2.3 \cdot 10^{-3}$
PCV	$5.0 \cdot 10^{-3}$
LE	$5.0 \cdot 10^{-4}$
PC	$3.5 \cdot 10^{-5}$
V-1	$5.0 \cdot 10^{-3}$

Problem 5. System reliability book problem 3.13 (page 145)
Additional questions

(a) Find all minimal cut sets of the reliability block diagram and construct a corresponding fault tree with the minimal cut sets.

(b) Give a brief explanation of the basic events in the constructed fault tree in connection to the blocks in the reliability block diagram.

Problem 6. System reliability book problem 3.3 (page 141)
Additional questions

(a) Reconstruct the fault tree and the reliability block diagram based on the minimal cut sets you identified.

(b) Identify the EUC, SIS and demand for the system.
Given the probability of failure of each components in Table 5.1

(c) Calculate the Birnbaum's measure of important for SV and PC. What does the result tell us about these two components?

(d) Calculate the Fussell-Vesely's measure of important for LE and PC, what does the result tell us about these two components?

Problem 7. 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, $\lambda_100 = 2.4\dot{1}0^{-4}$ 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 $\lambda_100 = 1.8\dot{1}0^{-3}$ 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 8. A gas detector is assumed to have constant failure rate $\lambda_{\text{DU}} = 1.6 \cdot 10^{-6}$ 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 $\lambda_{\text{S}} = 2.1 \cdot 10^{-6}$ 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.

Knockout drum with high level protection

Figure 5.3: Knockout drum with high level protection.

- 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.

- 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.

- 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 9. Consider a system for high level protection of a knockout drum installed topside on an offshore oil and gas facility. The purpose of the knockout drum is to extract any liquid and as such prevent liquid carry-over to flare. A simple sketch of the system is shown in 5.3.

The knockout drum is equipped with on level transmitter that sends a 4-20mA signal to a logic solver. The value of the mA signal corresponds to a certain drum level, and the level transmitter is assumed to have been calibrated correctly. The logic solver compares the mA reading with a set point (also in mA), and sends a close signal to two identical shutdown valves, one in each of two incoming flare lines. In addition, a liquid outlet valve is forced open, to ensure that liquid in knockout drum is sent back to one of the production separators.It assumed that this safety instrumented functions, constituting the level transmitter, the logic solver and the three valves, is tested once every year to reveal any dangerous undetected (DU) failures. The repair time must be considered and is referred to as the mean time to repair (MTTR). It is expected that the situations where a response by the SIF is rare, an much less than once per year.

(a) We first limit the study to the two shutdown valves that receives a close signal. Build operational failure models for the two valves of with Markov and Petri net methods respectively.

- Regarding the Markov approach: Use three system states; two valves are available (no DU failures), one valve is available, while the other has a DU failure, and both valves have a DU failure. Include the transition rates, and show how the test interval and the MTTR are treated in the transitions.
- Regarding the Petri net: Build the model using the following places: piW (place for valve i working), i=1,2 and piF (place for valve i failed), i= 1,2 p_{SW} (place for system working) and p_{SF} (place for system failed).

(b) Transitions with test interval included violates the Markov properties, but it may be shown that the error made is negligible. Why are the Markov properties violated? subprob.

(c) What states would be used as basis for calculating the unavailability (for Markov and for Petri net model) (just explain, it is not necessary to include any equations).

Chapter 6

Reliability Data Sources

Problem 1. 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. What are the pros and cons of using manufacturer provided data?

Problem 3. How can reliability data be provided by using FMEDA? Give a brief explanation.

Problem 4. ISO 13849-1 suggests that dangerous failure rates are calculated based on the following formula for mean time to failure ofa dangerous failure (MTTF$_\mathrm{d}$:

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

where n_op is the mean number of annular operation of the component and B_10d is the mean number of cycles till 10% of the components fail dangerously. 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

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

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. 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 this model with the model in MIL-HDBK-217(F).

Chapter 7

Demand Modes and Performance Measures

Problem 1. IEC 61508, the generic standard for design and operation of safety instrumented systems (SIS) distinguish between three modes of operation: low demand mode, high demand mode, and continuous demand mode.

(a) In which mode of operation would you place the following systems? Explain your position in each case.

- A railway signaling system controlling the lights at a train station
- An air bag release function (automotive)
- A system monitoring the state of a respirator (medical devices)
- The anti-brake system (automotive)
- A door sensor in relation to a fence surrounding a number of robots (no human intervention required on daily basis)
- A fire detection system in a building
- A house security system

Problem 2. Some safety systems may experience prolonged demand duration (e.g., the fire pumps need to function for a couple of hours to put out a fire).

(a) How would a prolonged demand duration influence the reliability (or risk reduction) of a safety instrumented system?

(b) Is this influence reflected in the current SIS reliability metrics?

(c) How would you suggest to include the prolonged demand duration in SIS reliability analysis?

Problem 3. 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?

Problem 4. 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: What is the practical interpretation that$PFH \leq PFD_{avg}\lambda_{de}$, where λ_{de} is the demand frequency.

Problem 5. The safe failure fraction (SFF) is a disputed reliability parameter.

(a) Define the SFF

(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. Explain the classification of failure modes used in reliability analysis of SIFs. Which failure mode(s) and corresponding failure rate(s) are the most important ones for calculating the PFD_{avg}? Comment on any differences you find in the literature, for example, between the PDS method and IEC 61508.

Problem 2. 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 3. ThePFD_{avg} of a subsystem can be calculated using exact formula or approximation formula (using Taylor series expanstion). Consider a subsystem of identical components that are voted 1oo3 with failure rate $\lambda_{\text{DU}} = 1.9 \cdot 10^{-7}$ per hour. Do not consider common cause failures (CCFs).

(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 4. 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 $\lambda_{\text{DU}} = 7 \cdot 10^{-7}$ 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 PFD_{avg} for the voted group
- Explain verbally what PFD_{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.
- 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.

(c) How many test intervals may pass before the subsystem is found in a failed state considering the situation with and without considering CCFs of the 2oo4 subsyste)? Does the result seem reasonable?

(d) What is the mean time to the a failed state of the subsystem considering the two cases in 4(c)?

Problem 5. 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. Please record any extra assumptions you have to make to answer the questions below.

(a)

- 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.

- 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.

- 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 $\beta = 0.08$.

- 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.

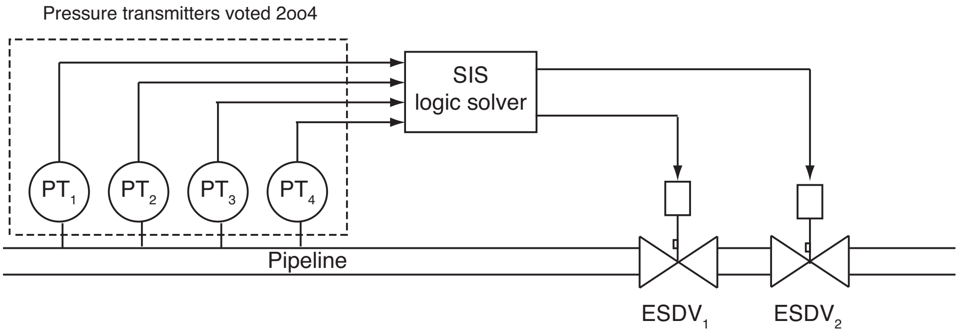


Figure 8.1: Safety instrumented system (SIS).

Problem 6. Consider the SIS in Figure 8.1. The system is a 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 proof-testing. The whole system is proof-tested at the same time at regular intervals – with test interval $\tau = 1$ year.

(a)

- 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)

- Find the mean time to a DU-failure of a specified valve
- Find 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)

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

- Find 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)

- Find 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)

- Find the $\mathrm{PFD}_{\mathrm{avg}}$ of the system.
- Find 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 7. 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.

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

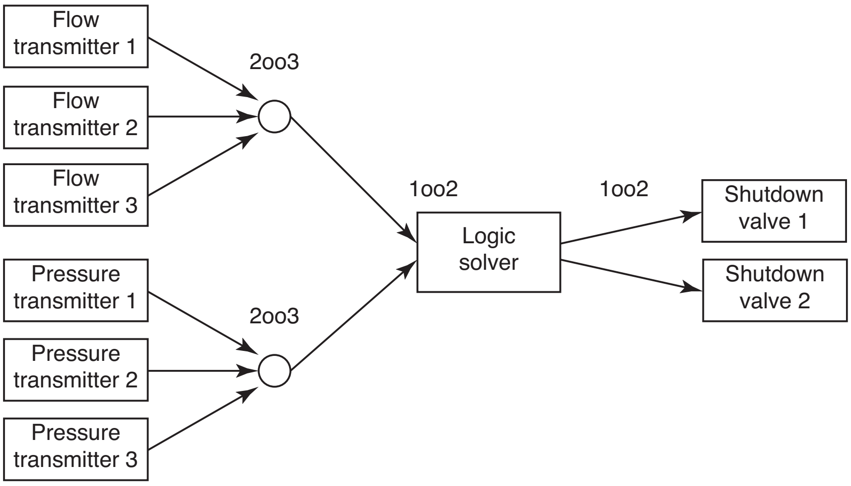


Figure 8.2: Safety instrumented system (SIS).

Table 8.1: Failure rates for the SIS components in Figure 8.2.

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

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

The logic solver is not able to perform any diagnostic testing, and all the components of the SIS will therefore have only 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 8.1.

(c) Find the probability of failure on demand (PFD) for a single component of each type (approximation formulas may be used).

(d) 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.

(e) Use the *upper bound approximation formula* to find the PFD of the system. All steps in the calculation shall be shown.

(f) 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.

(g) 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 $\beta_{\text{DU,FT}} = 0.10$, and the the pressure transmitters are exposed to CCF-DUs that can be modeled by a beta-factor with $\beta_{\text{DU,PT}} = 0.08$. 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 $\beta_{\text{DU,V}} = 0.20$.

(h) Find the PFD of the whole system when you assume that the main modules of the system are independent.

(i) Explain (briefly) what we mean by this PFD.

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.

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

(k) 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 $\beta_{\text{S,FT}} = 0.12$ for the flow transmitters, while the corresponding β-factor is $\beta_{\text{S,PT}} = 0.15$. The two shutdown valves are assumed to be independent with respect to S-failures.

(l) 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?

The flow transmitters and pressure transmitters cost 3000 and 3500 NOK each. There are options of embedding diagnostics in the transmitters with an additional cost of 2000 NOK. The transmitter with diagnostic, upon detection of dangerous failures, will send analog outputs to a predefined out of range analog current. Since the diagnostic testings are preformed rather frequent (e.g., every second), the dangerous failures are detected immediately. The diagnostics can detect 90 %

of the dangerous failures, so the DU failure rate becomes 10 % of what it is without diagnostics.

(m) When the transmitters are equipped with diagnostics, calculate the PFD of the flow transmitters group and pressure transmitters group with IEC 61508 formula and the PDS formula. Explain briefly what are the sources of the difference from the two sets of formulas. (use the same CCF rate as in question g)

(n) One consultant suggest to consider the following options, please give your opinion with regard to reliability, spurious trips and cost
1) 2oo3 flow transmitters and 2oo3 pressure transmitters, both without diagnostics
2) 2oo2 flow transmitters and 2oo2 pressure transmitters, both with diagnostics
3) 2oo3 flow transmitters without diagnostics and 2oo2 pressure transmitters with diagnostics
4) 2oo2 flow transmitters with diagnostics and 2oo3 pressure transmitters without diagnostics

Improving the reliability (unavailability) of the valve group can significantly reduce the overall PFD. One consultant suggests to use stagger testing to the valves to achieve a lower PFD. She suggests to keep the proof test interval of the valves, but the test of one valve is done at month 3, 9, 15,.... and the other valve is tested at month 6, 12,18....

(o) Please calculate the PFD of the valve group when stagger testing is applied.

Another consultant prefers to use partial stroke testing (PST) to achieve a lower PFD. With the PST technology she suggested, the PST can achieve a 60% coverage.

(p) Please calculate the PFD of the valve group when PST is conducted every month.

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

Problem 8. Two identical fire pumps are installed with a 1oo2 configuration as part of a fire fighting system. The relevant data are given in Table **??**

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

(a) Please calculate the PFD of the pumps with IEC 61508 formula, PDS formula, Markov model and Petri net.

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 frequency of having a critical event? (Several approaches may be used to calculate the frequency, please use as many approaches as possible and cross check on the results.)

Problem 9. Explain and discuss briefly the following terms used by the PDS method

(a) Critical safety unavailability (CSU)

(b) Downtime unavailability (DTU)

(c) Probability of test-independent failure (p_{TIF}

Chapter 9

Average Frequency of Dangerous Failures

Problem 1. 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. In the offshore oil and gas installations, there are several PSD systems that are demanded more often than once per year (up to once per month). According to IEC 61508, the PFH of these PSD systems should be calculated. The system shown in Fig. 9.1 is installed in a gas platform. 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 **??**

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

(a) Please established a reliability block diagram for this system.

(b) Calculate the PFH for the PSD systems using IEC 61508 formula and the formula presented in the book. And explain briefly what PFH means.

(c) Establish a Markov diagram for the final element subsystems and calculate the PFH.

A high pressure pipeline protection system (HIPPS) is installed to prevent accident when the PSD fails on demand as shown in Fig. 9.2. When a demand occurs, the PSD reacts first, if PSD fails to respond, the demand will be carried on to the HIPPS, and we have a demand for the HIPPS function, otherwise, we do not have a demand on HIPPS.

(d) Assume that the PSD is demanded 2 times per year, what is the demand frequency for HIPPS? What if the PSD is demanded 10 times per year and once every five years? Compare and reflect on the results?

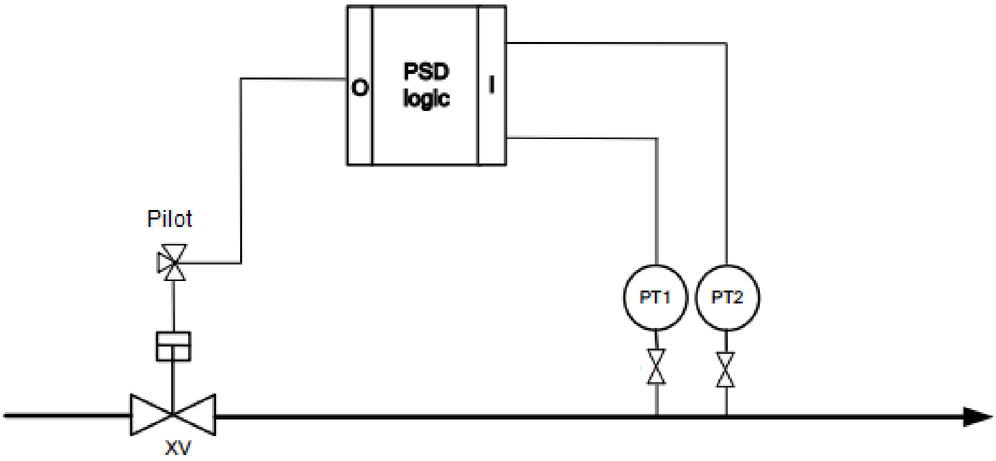


Figure 9.1: Process shutdown (PSD) system.

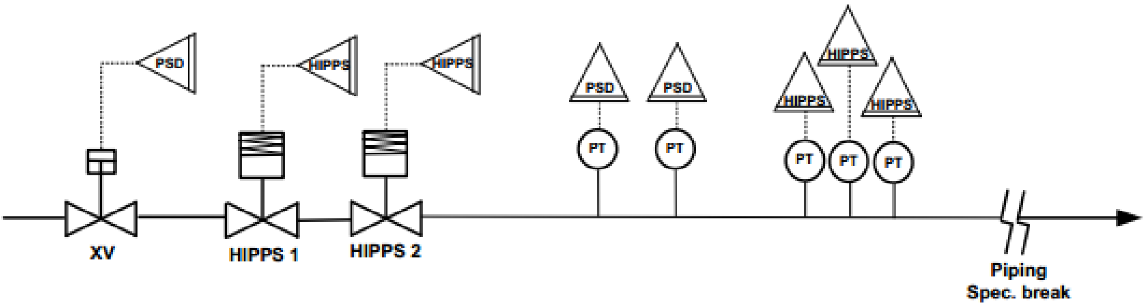


Figure 9.2: Pressure protection systems for a pipeline section.

(e) Is PFH an appropriate reliability measure for this PSD?

Chapter 10

Common-Cause Failures

Problem 1. Consider the standard beta-factor model. The estimated fraction, β, of CCFs is considered to be too high in a special application and efforts are made to reduce β. If we are able to reduce β by 20%, what is the effect on the independent failure rate of the channel? What does this result tell about the beta-factor model?

Problem 2. Describe and discuss the main differences between the beta-factor model and the C-factor model.

Problem 3. Consider a 2oo3 voted group of identical channels. Let $\lambda_{\text{DU}}^{(i)}$ 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: $\lambda_{\text{DU}}^{(i)} = 1.5 \cdot 10^{-6}$ 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 $p = 0$. 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 PFD_{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 $p \to 1$?

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 $\beta = 0.10$.

(e) Determine the PFD_{avg} of the 2oo4 voted group

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

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

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

(i) Discus, briefly, the realism of the beta-factor model.

(j) 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.

Chapter 11

Imperfect Proof-Testing

Problem 1. Partial stroke testing may be used to supplement proof testing.

(a) Explain the two main rationales for introducing partial stroke testing

(b) Explain the meaning of partial stroke testing coverage

(c) Explain the method in the article by Lundteigen and Rausand on partial stroke testing (2008)[1]

(d) Assume that you come up with a PST reliability of 95% (by using the checklist). Calculate the PST coverage, using the revealability factors in table 3 and the weights in table 4 (in the article).

(e) Calculate the PFD for a 1oo2 voted group of valves with and without using partial stroke testing.

- PST coverage (use the one you calculated above)
- Failure rate $\lambda_{\mathrm{DU}} = 2.0 \cdot 10^{-6}$ failures/hour
- Proof test interval $\tau_{\mathrm{FT}} = 12$ months
- Test interval of partial stroke test τ_{PST} =2 months

Compare the results. Will the change in the PFD also change the SIL (if we exclude other SIL-related requirements).

[1] Lundteigen, M. A. and M. Rausand (2008): Partial stroke testing of pricess shutdown valves: how to determine the test coverage. *Journal of Loss Prevention in the Process Industries*, 21: 1208-1217.

Chapter 12

Spurious Activation

Problem 1.

Chapter 13

Uncertainty Assessment

Problem 1.

Chapter 14

Closure

Problem 1.

Chapter 15

Combined Problems

The problems in this chapter covers topics from several chapters of the book.

Problem 1.