Solutions to Risk Assessment: Theory, Methods, and Applications, 2nd ed.

Wiley, Hoboken NJ, 2020

Stein Haugen and Marvin Rausand

Version 1.0

Contents

Preface

All problems in Chapter 1 are open-ended with no specific solution and proposed solutions are therefore not provided. Further, there are no problems in Chapter 20 and solutions are obviously not provided.

Many problems do not have a single, correct solution, but we still provide a called "model solutions," to illustrate how this could be done. In those cases, we have tried to state that in the beginning of the proposed solutions.

The set of solutions has not been through the same rigorous checking of language, formatting, etc as the book and there may therefore be smaller or larger mistakes. It is also likely that some of the problems may be interpreted in different ways and thus also that very different solutions may be the result. We can only apologize for this, but would very much welcome any feedback on points that can be improved.

Please send comments and suggestions to Stein Haugen.

Chapter 1

Introduction

Solutions to the problems in Chapter 1 are not provided.

Chapter 2

The Words of Risk Analysis

Problem 2.1
The main difference lies in the fact that hazards are associated with random events that are not planned while threats are associated with deliberate events where a threat agent intends a specific negative outcome to occur.

The definitions are as follows (although they do no necessarily bring out the main difference clearly):

> *Hazard*: A source or condition that alone or in combination with other factors can cause harm.
>
> *Threat*: A generic category of an action or event that has the potential to cause damage to an asset.

Problem 2.2
Probability can be defined in many different ways but for this purpose we can say that probability is a number describing how likely it is that a certain event will occur (within a given time period or in a given situation). Frequency on the other hand is an expression of the number of times we expect a certain event to occur within a given time period. In short, probability is an expression of "how likely" while frequency is "how often". Both are used in risk analysis and for this purpose it is particularly important to remember that probability is a number in the range $[0, 1]$ while frequency is in the range $[0, \infty\rangle$. Probabilities are often also expressed as percentages, e.g. 1% probability of occurrence of an accident, while frequency is associated with a time interval, e.g. 5 accidents per year. Note that when the frequency becomes small (which is often the case in risk analysis), the frequency and the probability will approach each other in value.

Problem 2.3
In Table 2.1, the suggested rephrasing is shown after the sentence from Table 2.1 in the book. It is underlined that this is based on the definitions that we apply in this book. These are primarily developed for risk analysis purposes

and may therefore not be appropriate in other contexts. The purpose here is to illustrate that the definitions that we apply deviate from everyday language.

As can be seen, probability (or likelihood/frequency) can be used in many of the cases. In some cases, other interpretations are also possible.

Problem 2.4
No solution provided.

Problem 2.5
The following are some of the failure modes that can be identified:

- Door cannot be opened
- Door opens unintentionally
- Door cannot be closed
- Door cannot be locked
- Door cannot be unlocked
- Door locks unintentionally
- Door unlocks unintentionally
- Door can be opened only partially
- Door can be closed only partially
- Window cannot be opened
- Window cannot be closed
- Window can be opened only partially
- Window can be closed only partially
- Door falls off

Observe that the failure modes are different in different operational modes of the door. Item 1 and 2 are only relevant when the door is closed, item is relevant only when the door is open and so on.

Problem 2.6
Three examples of scenarios are described (many others can of course be envisaged):

1. A pedestrian steps into the road
2. You apply the brakes but are not able to stop the bicycle in time

Table 2.1: Rephrased statements (Problem 2.3)

Original statement	Rephrased	Comment
Ford recalls electric car power cables due to fire risk.	...due to probability of fire.	Risk may also be used.
Is financial turmoil in Turkey and other emerging economies at risk of spreading?	Is there a probability that financial turmoil in Turkey....	The consequence is that financial turmoil will spread.
Are there any other legal risks?		Risk is appropriate.
Investors are willing to take on a high risk.		Risk is appropriate.
Bridge designer warned of risk of corrosion.	...warned of probability of corrosion.	
Saturday features more widespread rain risk.	...widespread probability of rain.	
Multi-gene test may find risk for heart disease.	...may find probability of heart disease.	Heart disease is the consequence.
We could put at risk our food and water supplies.		Risk may be used, although it depends on the context.
This political risk was described in an intriguing analysis.		Risk is appropriate.
Because of the risk of theft.	Because of the probability of theft.	
Reindeer at risk of starvation after summer drought.	Reindeer have a probability of starvation...	The consequence is starvation and possibly death.
Coalition at risk as talks on refugee policy falter.	Probability that coalition may fail after talks...	
Seven ways to minimize the risk of having a stroke.	...minimize the probability of having a stroke.	
Company to close 42 stores, putting 1,500 jobs at risk.	...stores, with 1500 jobs probably lost.	
Death is a risk the drivers willingly take and their loved ones accept.	Death is a consequence the drivers...	
You are putting lives at risk over Brexit.	There is a probability that Brexit can cause loss of lives.	
This carries an accident risk of “Chernobyl proportions”.		Risk may be appropriate although "Chernobyl proportions" most likely refers to the consequences.
£80bn investment plan at risk.	There is a probability that the £80bn investment plan fails.	

3. You steer away from the pedestrian off the road
4. You hit a tree
5. You are thrown off the bike
6. You break an arm in the fall

In this case, the hazard is the high speed of the bicycle. This is kinetic energy that if not controlled can cause injury. The enabling event in this case is that the pedestrian steps into the road. This can probably also be regarded as the initiating event.

1. A car approaches the crossing from another direction
2. You apply the brakes but are not able to stop the bicycle in time
3. You are unable to steer away and hit the car
4. You are thrown off the bike and onto the car
5. You slide off the car and onto the ground
6. You are seriously injured by the impact

This is also quite similar to the previous scenario, except that it is the approaching car that is the enabling event/initiating event.

1. Your speed increases towards the crossing
2. You hit a slippery spot in the road
3. You lose control over your bicycle
4. You are thrown off the bicycle at high speed
5. You hit the ground and are seriously injured

In this case, the slippery spot in the road can be regarded as an enabling condition. The initiating event is perhaps less obvious in this case, but it could be either that you hit the slippery spot or that you lose control over your bicycle.

Problem 2.7

1. A possible accident scenario is as follows:
   (a) The captain of a ship is planning a voyage and fails to identify an obstruction in the planning process
   (b) The ship sets sail from port

(c) During the voyage, the person on the bridge of the ship falls asleep

(d) The ship hits an obstruction

(e) The ship starts sinking

(f) The crew abandons ship

(g) All crew drowns

2. The definitions are as follows:

   Initiating event: An identified event that represents the beginning of an accident scenario

   Hazardous event: An event that has the potential to cause harm.
   Both terms are primarily analytical terms that are difficult to define precisely. For risk analysis purposes, it would probably be reasonable to start with item 3 as the initiating event. This is when something abnormal arises and when corrective actions need to be taken to normalize the situation. Hazardous event could be item 4. However, in both cases, the choice would also depend on the objectives and scope of the analysis that is performed and it may be argued that other events can be chosen.

Problem 2.8

1. Reference accident scenario is an accident scenario considered to be representative of a set of scenarios and to be likely to occur. The main purpose of defining these is to simplify the analysis and avoid having to analyze every conceivable scenario. These scenarios are selected for detail analysis in order to save time and resources for risk analysis. Worst-case accident scenario is, on the other hand, an accident scenario with the highest possible consequence regardless of likelihood. In some cases, it is very important to look into these worst scenarios even if the likelihood is extremely small. Worst credible accident scenario is a accident scenario which has plausible likelihood with highest-consequence.

2. Defining reference accident scenarios is a balance between limiting the number of scenarios to save time in the analysis versus defining a sufficient number of scenarios to make the analysis sufficiently detailed. This can be challenging. Further, when defining worst credible scenarios we need to consider what is meant by “plausible likelihood”. Some guidance is given, but this may still be contentious.

Problem 2.9

Robustness is a static concept that is basically synonymous with damage tolerance. A concrete wall can robust against impact and fire. Vulnerability (as it is

defined in this book) is associated with security and is defined as "A weakness of an asset or control that can be exploited by one or more threat actors." This can be e.g. inadequate access limitations to confidential information. Vulnerability is often also used in a wider sense, meaning more or less the opposite of robustness, i.e. a system that is not robust is vulnerable.

Problem 2.10
Risk as defined in this book: The combined answer to the three questions: (1) What can go wrong? (2) What is the likelihood of that happening? and (3) What are the consequences?

Other definitions mentioned in the book:

(a) Effect of uncertainty on objectives

(b) The possibility that human actions or events lead to consequences that harm aspects of things that human beings value

(c) Situation or event where something of human value (including humans themselves) has been put at stake and where the outcome is uncertain

(d) Uncertainty about and severity of the consequences (or outcomes) of an activity with respect to something that humans value

(e) The probability that a particular adverse event occurs during a stated period of time, or results from a particular challenge

(f) Risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organization's objectives

The definition provided in this book is very useful for the performance of risk analysis and it also needs to be seen in this context. This does not necessarily mean that the definition is equally useful for other purposes and in other contexts. This may also explain some of the differences compared to the other definitions mentioned.

- The most striking difference is perhaps that all the other definitions (except e)) use uncertainty instead of probability/likelihood.
- a) and f) talk about effect on "objectives" rather than "consequences" (definition b), c) and d) all use something that we value (assets)). Objectives can be regarded as a wider term than just "protecting something that we value."
- Definition e) is in reality limited to only probability of an adverse event occurring, without considering the extent of consequences of the event. This is a significant difference compared to the other definitions.

Problem 2.11
No solution provided.

Problem 2.12

- *Hazardous event:* An event that has the potential to cause harm.
- *Incident:* A sudden, unwanted, and unplanned event or event sequence that could reasonably have been expected to result in harm to one or more assets, but actually did not.

The main difference between these two lies is the fact that a hazardous event can cause harm, whereas an incident did not. First, this means that hazardous events are related to the future while incidents are related to the past. Secondly, hazardous events can cause harm, i.e. they do not necessarily lead to harm but can do so. Incidents can then be regarded as one group of possible outcomes of a hazardous event, namely the outcomes that cause no harm.

If we illustrate this with an example, we can say that fire in a tumble drier is a hazardous event. This may cause harm, but if it is extinguished quickly enough, no (significant) harm is done. If this is the case, we can say that the fire was an incident. However, if the fire develops unchecked, serious harm may occur and then it would not be an incident.

Problem 2.13
First, we repeat the definitions of the three terms:

- *Failure:* The termination of the ability of an item to perform as required.
- *Failure mode:* The manner in which a failure occurs, independent of the cause of the failure.
- *Failure mechanism:* Physical, chemical, or other process that leads to failure.

Table 2.2 provides examples, but is not a complete set of failures, failure modes and failure mechanisms.

Problem 2.14
The bow-tie in Figure 2.1 is one possible way of drawing this and it is not complete. Barriers illustrated in the bow-tie:

B1: Speed limits

B2: Pre-warning of obstruction

B3: Driving carefully

B4: Cleaning up spill quickly

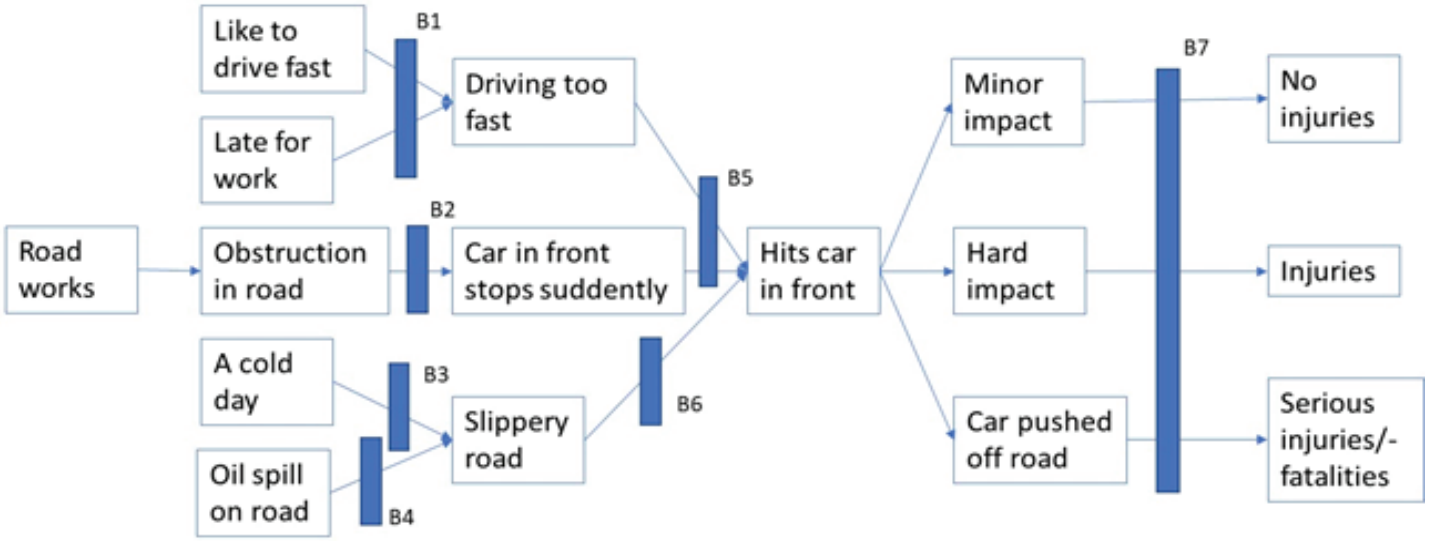

Figure 2.1: Bow-tie for Problem 2.14

Table 2.2: Failure, failure mode and failure mechanism (Problem 2.13)

Failure	Failure mode	Failure mechanism
Brakes fail to stop the bicycle	Handle breaks	Corrosion
		Fatigue
		Overload
	Wire fails	Corrosion
		Fatigue
		Overload
		Wire stuck
	Wire slack	Wire has stretched over time
		Wire has slipped from fastenings at ends
	Brake pads fail to stop the wheel	Brake pads worn down
		Brake pads slippery due to oil etc.

B5: ABS brakes

B6: Anti-skid system

B7: Seat belt

Other barriers are also relevant to include, but are not illustrated.

Problem 2.15
The bow-tie in Figure 2.2 is one possible way of drawing this and it is not complete. Barriers illustrated in the bow-tie:

B1: Inspection of electrical system

B2: Fire/smoke detectors

B3: Sprinkler system

B4: Emergency escape routes

B5: Automatic power cut to stove on overheating

Other barriers are also relevant to include, but are not illustrated.

Problem 2.16
The definitions are as follows:

- Definition 2.31 *Safety*: A state where the risk has been reduced to a level that is as low as reasonably practicable (ALARP) and where the remaining risk is generally accepted.

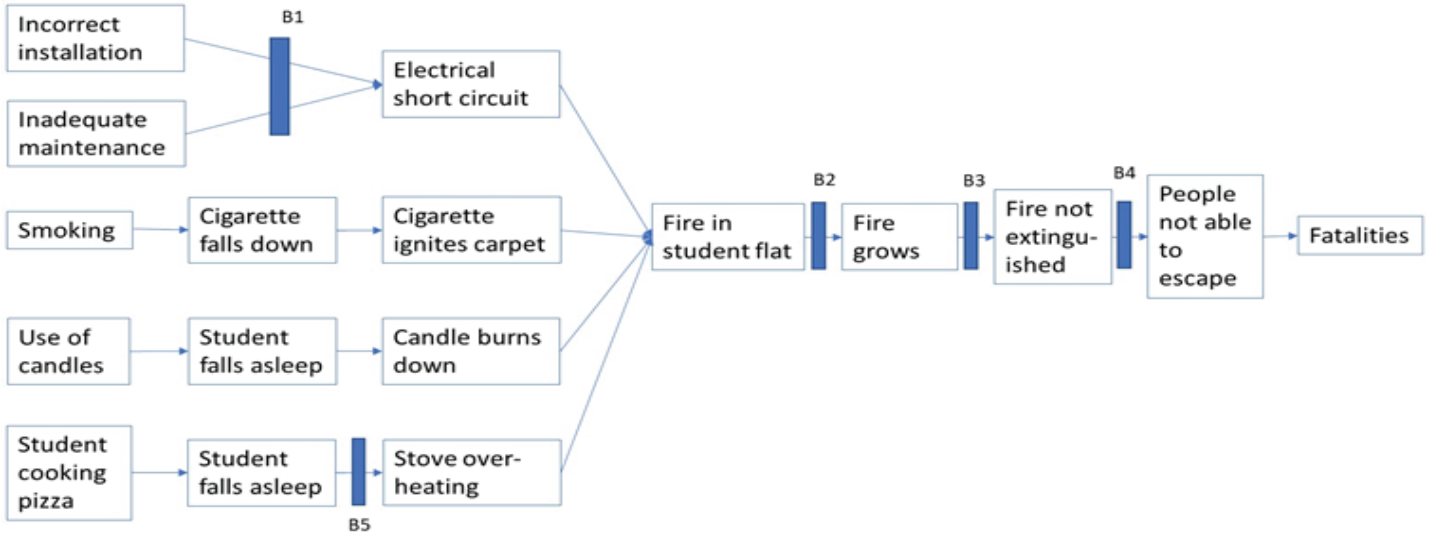

Figure 2.2: Bow-tie for Problem 2.15

- Definition 2.33 *Security*: Freedom from, or resilience against, harm committed by hostile threat actors.

The definitions are quite different in that safety is defined as a state where the risk is below a certain level that is generally accepted, while security is freedom from harm caused by a specific source, implicitly saying that only in situations where no harm can occur do we have a state of security. This is a situation that is highly unlikely to achieve and thus not very practical. An alternative definition could be something more similar to the definition of safety:

- *Security*: A state where the risk associated with harm committed by hostile threat actors is reduced to a level as low as reasonably practicable (ALARP) and where the remaining risk is generally accepted.

Chapter 3

The Main Elements of Risk Assessment

Problem 3.1
A risk analysis is "A systematic study to identify and describe what can go wrong and what the causes, the likelihoods, and the consequences might be." On the other hand, risk assessment is "The process of planning, preparing, performing, and reporting a risk analysis, and evaluating the results against risk acceptance criteria." Risk assessment is thus a wider process than risk analysis, and risk analysis is an element in risk assessment.

Problem 3.2
The risk assessment process consists of six steps, with the following main objectives/activities in each step:

1. Plan the risk assessment – Planning, clarifying decision and decision criteria, define outputs, objectives and scope, establish study team and project plan, identify and provide background information.

2. Define the study – Define and delimit the study object, provide documentation, familiarize, select method and data and identify relevant assets.

3. Identify hazards and initiating events – Identify and describe generic and specific hazards and events, identify causes of events and determine frequencies/probabilities.

4. Develop accident scenarios and describe consequences – Identify barriers and other factors, describe representative scenarios, end events and consequences, determine frequencies of end events and quantify consequences.

5. Determine and assess the risk – Summarize results, assess uncertainty, evaluate risk, identify risk reduction measures and determine their effect and cost.

6. Risk presentation – Prepare report and present the results.

Problem 3.3
The following are some examples of what needs to be considered when we define the study object (without necessarily specifying what should be part of the study object and not):

- First, we include not only the railway line as such but also trains running on the railway line. The study object is thus the railway line and all trains running on the line.
- Traffic crossing the line (cars, pedestrians, other) also must be included, but only to the extent that they influence the system or is influenced by the system (e.g. the train hitting a car crossing the line).
- We need to define if external services such as external power supply (electrical power), communication signals, water, etc. should be included or not. We may choose to say that only disturbances to the external services are considered to the extent that they have an effect on the study object. We do not go into details on the causes of such disturbances.
- The physical limits of the system need to be decided. How far away from the railway line should the limit be placed? If there are fences, this may be a suitable way of limiting the system. If not, we should consider how far away from the railway line effects of events can be experienced (e.g. can a train derail and slide down a steep slope?). Physical limits for stations also need to be considered. Is it only the platforms that are included? Buildings on the platforms? Access ways to stations?
- We need to decide if only normal operation should be covered by the risk analysis or if more unusual situations like maintenance work, modifications to the infrastructure or other activities should be considered.

Problem 3.4
The following are some examples of the three types of events:

- Generic events: Collision between trains, Collision with cars crossing the line, Derailing, Fire on train, etc…
- Specific events: Collision with private car crossing the line on crossing no X, Collision with private car crossing line on crossing Y, Collision with small truck crossing line on crossing no X, etc…
- Representative events: Collision with private cars crossing the line, Collision with small truck crossing the line, Collision with large truck crossing the line, etc…

The specific events can typically be grouped into a set og representative events and these can in many cases be grouped together into generic events.

Problem 3.5
Some possible causes are:

- Failure of track due to flooding
- Landslide on top of track
- Track failing due to landslide under track
- Track failure due to fatigue
- Objects on track
- Snow/ice on track
- Failure of wheel on train
- Too high speed

Other causes may also be relevant.

When defining representative events, a primary concern is whether the consequences are different depending on the cause. In this cause, the consequences may be different id the cause is a landslide on top of the track compared to e.g. track failure due to fatigue because hitting a landslide may cause a very quick stop. It may also be relevant to distinguish between natural causes and technical causes, mainly because the risk reduction measures that can be introduced to mitigate the causes are very different. As always, this is however a balancing of details in modelling vs work required to do the analysis.

Problem 3.6
To answer this, we need to understand the different groups, what knowledge they have and what their interests/motivations are. The following is proposed:

- Company management: Will have some, but fairly limited knowledge of risk assessment. Are responsible for the safety of the passengers and the ships and need to make decisions about whether risk is acceptable or not and what to do if risk needs to be reduced. Results describing the risk level and comparisons with requirements from authorities and other companies and activities are relevant to present. Effects of implementing risk reduction measures are also relevant. Details of methodology, data used etc are most likely not relevant, but key assumptions and limitations in the analysis are important and in particular how these may affect the results.

- Safety department: This group is likely to be familiar with risk assessment, how results can be presented and limitations in analyses. Are responsible for implementing decisions about risk made by company management. For this group, it is more relevant to show details of methodology and data, to provide assurance that the analysis is sound. Key assumptions and limitations and the reasoning behind the assumptions are relevant and also results in detail.

- Passengers: Are unlikely to have much knowledge about risk analysis. Are primarily interested in being reassured that it is safe to use the ferries. Details of methodology, data, limitations etc are of very little relevance. Expressions of risk such are FAR-values, IR-values etc are also not relevant. Focus should instead be on comparison with other, known activities, and also on what measures are in place to reduce risk.

Problem 3.7

It is not straightforward to give a simple answer to this question. On the one hand it can be argued that a risk analysis consists of models and data and as long as the models and the data are documented properly it is possible to reproduce this. On the other hand, it can be argued that a lot of work is done before the models and the data are established and this is not necessarily reproducible. First, hazards are identified and described as representative scenarios. This depends very much on the knowledge and experience of the analysts involved. Secondly, data often have to be adjusted to be fit for the purpose in a specific analysis. This often also requires judgment from the analyst. It is unlikely that two different analysts would arrive at the same results. Studies have also confirmed that this is the case.

What this highlights is the importance of documenting not only the models and data used, but also the judgment that is used to establish this. If this is known and applied by other analysts, it is more likely that the same results can be reached, although the documentation clearly is a challenge.

Chapter 4

Study Object and Limitations

Problem 4.1
A black box analysis is an analysis where we give input to the analysis and we receive outputs, but we do not know exactly what is going on inside the analysis. With a definition like this, what is a black box is dependent on the user of the analysis model. For any man-made system, there must be someone who understand the inner workings of the system to be able to design and build it.

For people with no experience or knowledge of risk analysis, a quantitative risk analysis would be an example of a black box analysis. Other examples (for most of us) would be many electronic systems, e.g. a computer, a radio or a navigation system in a car.

Problem 4.2
This depends on how we set the boundaries for the system. The coffee maker will not work without a human operating it and if we consider operation, this becomes a sociotechnical system, where the person operating the system is the non-technical part. On the other hand, we may also choose to look only at the coffee maker as a stand alone product, not considering how it is operated. It would then be regarded as a technical system.

Problem 4.3
As mentioned in the solution of Problem 4.2, this depends on how we define the boundaries of the system, but if we assume that we always take into account the operation of the system, there are fewer examples of purely technical systems. The best examples are various autonomous systems that operate entirely on their own without human intervention. This may be e.g. self-driving cars. On a smaller scale, it can also be argued that various driver assistance systems in cars (like lane-assist systems, adaptive cruise controls, ABS-braking systems) are purely technical systems. On the other hand, if we widen the scope of the analysis to include maintenance activities, humans are normally involved making it into a sociotechnical system.