TEXTBOOK

Engineering Safety

From Fundamentals to Functional Safety

Dr. Ahsan Rahman

Engineering Excellence Series

TEXTBOOK

Engineering Safety

From Fundamentals to Functional Safety

Theory • Practice • Standards • Industrial Applications • Certification

Dr. Ahsan Rahman

Engineering Excellence Series • Book 2 of 2

AR Resources

AR Resources
© 2026 Dr. Ahsan Rahman

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means — including photocopying, recording, or other electronic or mechanical methods — without the prior written permission of the author, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.

No part of this work may be used to train, fine-tune, evaluate, or otherwise develop any machine-learning or artificial-intelligence model or system without the express written permission of the author.

This book is provided for educational and professional-development purposes. Safety practice is governed by law and by official standards that vary by jurisdiction and are periodically revised. While every effort has been made to ensure technical accuracy, the author and publisher assume no liability for errors, omissions, or for any outcome arising from the use of the methods, standards interpretations, or examples presented herein. Readers must always consult the current, official text of any standard or regulation, and qualified professional advice, before applying it in practice.

Author: Ahsan Rahman
Series: Engineering Excellence Series — Book 2: Engineering Safety
First edition • 2026 • ahsanrahman.com

To everyone who goes home safe at the end of a shift — and to the engineers who make sure they do.

Preface

Safety is the quiet promise an engineer makes to everyone their work touches: that the machine will not maim, the plant will not explode, the structure will not fall, and the worker will go home whole at the end of the day. It is the most human of engineering disciplines, because its measure is not profit or performance but harm avoided — the accidents that never happened, the injuries no one suffered, the lives that were never lost.

This is the second volume of the Engineering Excellence Series, the companion to Engineering Quality Assurance. The two books are deliberately built on the same foundations, because in real organisations quality and safety are managed by the same people, using the same disciplines: risk thinking, standards, root-cause analysis, audits, reliability, and a culture of prevention. Where the first book asks 'will it meet its requirements?', this one asks 'will it hurt anyone?' — and the methods for answering are remarkably alike.

The book is written for students meeting safety engineering formally for the first time, for practising engineers who carry safety responsibilities they were never explicitly taught, and for professionals preparing for safety certification who want the reasoning behind the regulations, not just the regulations. It moves from first principles — what a hazard is, how accidents happen — through management systems and human factors to the rigorous mathematics of functional safety, and on to the digital and process frontiers.

Every chapter follows the same rhythm as its companion: objectives, theory and the reasoning behind it, the international standards that govern practice, worked examples, a case study, and a generous bank of questions, laboratory activities, projects, and certification practice. Cross-references point to the quality volume wherever the two disciplines meet.

Safety, like quality, is a habit of mind before it is a procedure — a way of seeing the world that asks, before anything else, what could go wrong, and who could be hurt. I hope this book helps you build that habit, and keep people safe.

— Dr. Ahsan Rahman

How to Use This Book

The book is organised into six parts that move from first principles to specialised practice. You can read it cover to cover as a course, or enter at the part you need as a reference. Each chapter stands on its own while pointing to the chapters it depends on.

Recurring features

- Learning Objectives and Key Concepts open every chapter so you know the destination before you start.
- Standards boxes (teal, left-barred panels) summarise the relevant ISO, IEC, OSHA, HSE, and sector standards in plain language.
- Worked Examples and Numerical Problems turn theory into calculation — especially in the functional-safety chapters; do them with a pen.
- Case Studies show the method working — or, instructively, failing — in a real industrial setting.
- Review Questions are graded across four tiers: Recall, Application, Analysis, and Design.
- Certification Practice questions mirror NEBOSH, IOSH, and functional-safety (TUV) examination styles, with explained answers.
- A See also line at the end of each chapter links to the companion Engineering Quality Assurance volume.

A note on standards and law: clause numbers, legal duties, and requirements are summarised for learning and vary by jurisdiction. Before applying any standard or regulation professionally, obtain and read its current official text and seek qualified advice — in safety, the source always governs, and this book is a guide to understanding, not a substitute for it.

Contents

PART I

Foundations of Safety

What safety means, how accidents happen, and the language of hazard, risk, and control that underpins every method in this book.

PART I — FOUNDATIONS OF SAFETY

Chapter 1 — The Meaning and Evolution of Safety

Learning Objectives

Define safety in engineering terms and explain why absolute safety is unattainable.

Distinguish clearly between hazard, risk, and harm.

Trace the evolution of safety thinking through its successive ages.

Explain the moral, legal, and financial case for safety.

Describe why the true cost of an accident far exceeds its visible cost.

Relate safety to quality as two expressions of engineering integrity.

Key Concepts

- Safety as freedom from unacceptable risk; tolerable vs absolute safety.
- Hazard, risk, and harm — a property, a probability, and an outcome.
- The ages of safety: technical, systems, human factors, culture.
- The moral, legal, and financial case for safety.
- The accident cost iceberg; direct vs indirect costs.

1.1 What Is Safety?

Ask most people what safety means and they will say ‘freedom from danger’ or ‘the absence of accidents.’ Both are intuitive and both are wrong in a way that matters to an engineer, because they imply that safety is an absolute state that can be fully achieved. It cannot. Every worthwhile activity carries some risk; crossing a road, flying a plane, and running a chemical plant can all be made safer, but none can be made perfectly safe. The working definition used throughout this book is therefore more careful: safety is freedom from unacceptable risk of harm. The crucial word is unacceptable — safety is not the elimination of all risk but the reduction of risk to a level society, the law, and reasonable judgement consider tolerable.

This reframing has profound consequences. It means safety is not a yes/no property but a matter of degree, to be measured, managed, and continually improved — exactly the engineering posture this book develops. It means every safety decision is, at bottom, a judgement about how much risk is acceptable and at what cost, a judgement that must be made honestly and transparently rather than hidden behind the comfortable fiction that something is simply ‘safe.’ And it means safety, like quality, is built in by deliberate design and management, not bolted on or hoped for.

1.2 Hazard, Risk, and Harm

The single most important distinction in all of safety — and the one most often blurred in everyday speech — is between hazard, risk, and harm. Confusing them leads directly to bad decisions, so they must be kept sharply separate.

Figure 1.1 Hazard is a property, risk is a probability, and harm is an outcome.

A hazard is anything with the potential to cause harm — a moving blade, a live conductor, a toxic chemical, a height, a flammable vapour. It is a property of the thing, present whether or not anyone is near it. Risk is the likelihood that the hazard actually causes harm, combined with how severe that harm would be — risk = likelihood × severity. A hazard with no exposure carries little risk; the same hazard with frequent exposure and no controls carries high risk. Harm is the actual outcome — the injury, ill-health, or damage — that occurs when the risk is realised. The whole of safety engineering can be read as the work of breaking the chain between hazard and harm: ideally by removing the hazard altogether, and where that is impossible, by reducing the risk until the chain rarely, if ever, completes.

1.3 The Evolution of Safety

Safety thinking did not arrive fully formed; it evolved through successive ages, each responding to the limits of the last, and each adding a layer that we still use today.

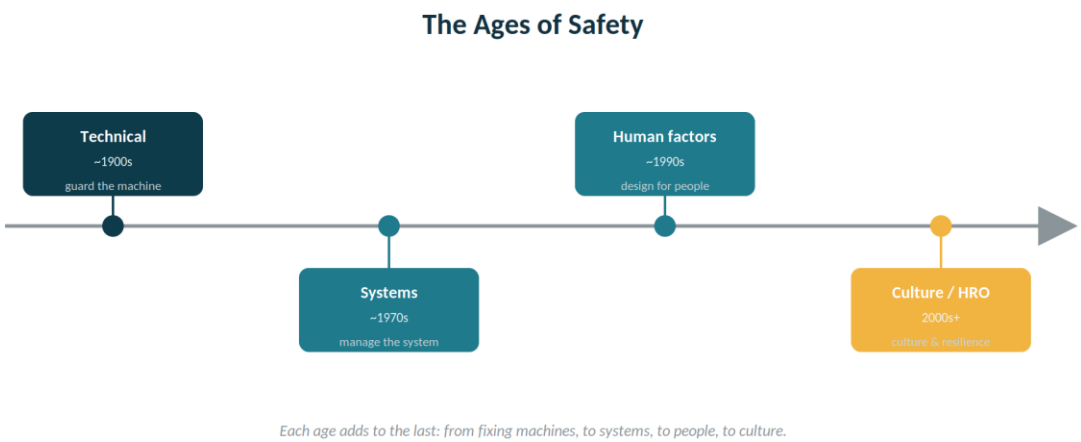

Figure 1.2 Safety thinking evolved through successive, cumulative ages.

The technical age, born in the early industrial era, saw accidents as engineering failures to be fixed with engineering: guard the machine, fence the pit, strengthen the boiler. The systems age, emerging through the twentieth century, recognised that accidents flowed from management and organisational systems, not just faulty parts, and gave us safety management. The human-factors age understood that people are not infinitely reliable components and that work must be designed around human capabilities and limitations rather than blaming the worker. And the culture age, dominant today, holds that beyond systems and ergonomics lies something deeper — the shared attitudes, values, and habits of an organisation, its safety culture, and its capacity to remain resilient in the face of the unexpected, as the high-reliability organisations of Chapter 2 do. Each age did not replace the last but built upon it; modern safety practice uses all four lenses at once.

1.4 The Cost of Getting It Wrong

Why invest in safety? The case rests on three pillars. The moral case is the simplest and the strongest: people should not be injured or killed by the work that sustains them, and an engineer who can prevent harm has a duty to do so. The legal case, developed in Chapter 4, makes that duty enforceable — employers and engineers carry legal obligations whose breach brings prosecution, fines, and imprisonment. The financial case is the one most often underestimated, because the true cost of an accident is largely hidden.

Figure 1.3 The visible direct costs of an accident are a fraction of the hidden indirect costs.

The direct costs of an accident — medical treatment, compensation, immediate repairs — are visible above the waterline, but they are the small, exposed tip of a much larger mass. Below the surface lie the indirect costs: lost production while a line is stopped, the time of everyone drawn into investigation and administration, recruiting and retraining replacements, damaged equipment, legal fees and rising insurance premiums, regulatory penalties, and the slow corrosion of morale and reputation. These hidden costs typically dwarf the visible ones, often by a factor of several to one. The lesson is decisive: prevention is almost always far cheaper than the accident it averts, and an organisation that judges safety spending against only the visible costs will systematically under-invest in it.

1.5 Safety and Quality: Two Faces of Integrity

This book's companion volume treats quality; this one treats safety; and it is worth stating at the outset why they belong together. Both are about making engineering deliver what it should reliably and predictably — quality that the product meets its requirements, safety that it does not harm. Both depend on the same disciplines: understanding requirements, assessing risk, controlling variation and failure, investigating causes, and improving continuously. The risk matrix of quality Chapter 19 is the risk matrix of safety; the root-cause analysis of quality Chapter 15 is the incident investigation of safety Chapter 8; the FMEA and fault trees of quality Chapter 16 are the functional-safety tools of safety Chapters 15–18. They are two faces of a single engineering integrity — the determination to know what could go wrong and to prevent it — which is why the practitioner who masters one is already most of the way to the other.

1.6 Multi-disciplinary Applications and a Case Study

Safety is universal across engineering. Civil engineering manages structural and construction safety; chemical and process engineering manage major-hazard and process safety (Chapter 19);

electrical engineering manages shock and arc-flash (Chapter 13); mechanical engineering manages machinery safety (Chapter 11); and software and systems engineering increasingly manage functional and cyber safety (Chapters 15–21). Each field has its own hazards and standards, but all share the same foundational logic of hazard, risk, control, and harm-avoidance that this chapter establishes.

Case Study 1.1 — The hazard that was never a risk — until it was

A maintenance platform on a production line had an unguarded edge two metres above the floor — a fall hazard that had existed, unremarked, for years. Because access was rare and the regular technicians knew to keep clear, the risk had stayed low and the hazard was tolerated; nothing had ever happened, which was quietly taken as proof that nothing would.

Then the line's output doubled, maintenance frequency rose sharply, and a new contractor unfamiliar with the platform was sent up at night. The hazard had not changed at all — but the exposure had, and with it the risk. The contractor fell and was seriously injured. The subsequent investigation found a hazard known to everyone and assessed by no one.

The lesson is section 1.2 made painfully concrete. The hazard (the unguarded edge) had been constant; the risk (likelihood × severity) had risen with exposure while no one re-examined it. 'Nothing has happened yet' is not a risk assessment, and a hazard tolerated because exposure is low must be re-evaluated the moment exposure changes.

1.7 Best Practices, Common Mistakes, and Troubleshooting

Best Practices

- Treat safety as the management of risk to a tolerable level, not the pursuit of an impossible zero.
- Keep hazard, risk, and harm distinct in every analysis and conversation.
- Re-assess risk whenever exposure, frequency, or people change — a constant hazard can become a new risk.
- Make the financial case using total cost, including the hidden indirect costs, not just the visible ones.

Common Mistakes

- Treating 'nothing has happened yet' as evidence that a hazard is safe.
- Confusing a hazard (a property) with a risk (a probability) and so mis-prioritising.
- Judging safety investment against only the visible direct costs of accidents.
- Assuming safety is an absolute state rather than a level of risk to be managed.

Troubleshooting

Symptom	Likely root cause	First action
A long-tolerated hazard causes	Exposure changed, risk not re-	Re-assess risk on any change (1.2,

Symptom	Likely root cause	First action
harm	assessed	1.6)
Safety seen as a cost, not an investment	Only direct costs counted	Quantify total cost incl. indirect (1.4)
'We have always done it this way'	Risk normalised by long habit	Re-examine the hazard with fresh eyes

Frequently Asked Questions

Q: Is anything ever completely safe? **A:** No. Safety is freedom from unacceptable risk, not the absence of all risk. Every activity carries some hazard; the engineer's task is to reduce risk to a level that is tolerable in law and in reasonable judgement.

Q: What is the difference between a hazard and a risk? **A:** A hazard is something with the potential to cause harm — a property of the thing. A risk is the likelihood that the hazard actually causes harm, combined with the severity. The same hazard can carry high or low risk depending on exposure and controls.

Q: Why is the cost of an accident usually underestimated? **A:** Because only the direct costs (medical, compensation, repairs) are visible. The indirect costs — lost production, investigation, retraining, reputation — are hidden below the surface and typically far larger.

Chapter Summary

Safety in engineering is freedom from unacceptable risk of harm — not the impossible elimination of all risk, but its reduction to a tolerable level, which makes safety a matter of degree to be measured, managed, and improved. The foundational distinction is between hazard (a potential to cause harm, a property), risk (the likelihood and severity of that harm, a probability), and harm (the actual outcome), and safety engineering is the work of breaking the chain between hazard and harm. Safety thinking evolved through cumulative ages — technical, systems, human factors, and culture — all of which the modern practitioner uses together. The case for safety rests on moral duty, legal obligation, and a financial reality in which the hidden indirect costs of an accident dwarf the visible direct ones, so prevention is almost always cheaper than the accident it averts. Safety and quality are two faces of the same engineering integrity, sharing the same risk-based, prevention-focused disciplines.

Glossary

Safety — Freedom from unacceptable risk of harm.

Hazard — Anything with the potential to cause harm — a property of the thing.

Risk — The likelihood that a hazard causes harm, combined with its severity.

Harm — The actual injury, ill-health, or damage that occurs.

Tolerable risk — A level of risk accepted as reasonable in law and judgement.

Indirect costs — The hidden costs of an accident — lost production, investigation, reputation — beyond the direct ones.

References and Suggested Reading

1. HSE, Reducing Risks, Protecting People (R2P2). UK Health and Safety Executive.
2. Hollnagel, E. Safety-I and Safety-II: The Past and Future of Safety Management. Ashgate.
3. Heinrich, H. W. Industrial Accident Prevention. McGraw-Hill.
4. ISO 45001:2018, Occupational health and safety management systems.
5. Hopkins, A. Safety, Culture and Risk. CCH.
6. ILO, Safety and Health at Work (International Labour Organization resources).

Review Questions — Chapter 1

Recall

1. Define safety in engineering terms.
2. Distinguish hazard, risk, and harm in one sentence each.
3. Name the four ages of safety.

Application

1. For a kitchen knife, identify the hazard, describe a low-risk and a high-risk scenario, and the potential harm.
2. List three indirect costs that would follow a forklift collision in a warehouse.
3. Explain how the same machine hazard could carry different risks on two different shifts.

Analysis

1. Explain why ‘nothing has happened yet’ is not a valid risk assessment, using Case Study 1.1.
2. Argue why judging safety spending against only visible costs leads to under-investment.

Design

1. Design a simple one-page hazard-and-risk register format that keeps hazard, risk, and control distinct.
2. Design a brief argument to persuade a sceptical manager of the financial case for a guarding upgrade.

Multiple-Choice Questions

1. Safety is best defined as: (A) The absence of all risk (B) Freedom from unacceptable risk (C) Zero accidents forever (D) Following all rules ✓ **Answer: B.** *Safety is freedom from unacceptable risk, not the impossible elimination of all risk.*

2. A live electrical conductor is an example of a: (A) Risk (B) Harm (C) Hazard (D) Control ✓ **Answer: C.** *It has the potential to cause harm — a hazard.*

3. Risk is best expressed as: (A) Severity only (B) Likelihood only (C) Likelihood × severity (D) Cost × time ✓ **Answer: C.** *Risk combines how likely harm is with how severe it would be.*

4. The hidden costs of an accident are called: (A) Direct costs (B) Indirect costs (C) Fixed costs (D) Capital costs ✓ **Answer: B.** *Indirect costs — lost production, investigation, reputation — lie below the waterline.*

Short and Long Questions

Short Questions

1. Why can no activity be made perfectly safe?
2. Why must risk be re-assessed when exposure changes?
3. Why is prevention usually cheaper than the accident it averts?

Long Questions

1. Explain the distinction between hazard, risk, and harm and why confusing them leads to poor decisions.
2. Trace the evolution of safety through its four ages and explain how each still informs practice.

Problems, Labs, and Projects

Structured Problems

1. For five everyday items, tabulate the hazard, a risk scenario, and the potential harm.
2. Estimate the total cost of a minor lost-time injury, separating direct and indirect costs.
3. Classify a list of statements as describing a hazard, a risk, or harm.

Practical Assignment

Walk through a familiar space (a kitchen, workshop, or office) and produce a short hazard list, assigning each a rough risk level and noting how exposure affects it.

Laboratory Activity

Lab 1 — Hazard spotting. In a supervised workshop or lab, identify ten hazards, classify the risk of each as low/medium/high with justification, and propose how exposure changes would alter the risk. Deliverable: a completed hazard-and-risk table.

Mini-Project

Build a one-page ‘cost of an accident’ calculator that separates direct and indirect costs and shows the hidden-cost multiplier, to support the financial case for prevention.

Capstone Project Idea

Choose a real or hypothetical workplace as your running project for this book. In this chapter, establish its context: the activities, the people exposed, and an initial register of its principal hazards, to be developed in every later chapter.

Interview and Certification Practice

Interview Questions

- How would you explain the difference between hazard and risk to a new worker?
- Why is 'zero risk' an unrealistic safety goal, and what is the realistic one?
- How would you make the business case for a safety investment?
- How are safety and quality related in an engineering organisation?

Certification Practice (NEBOSH / IOSH style)

1. A hazard is best described as: (A) The chance of harm (B) Something with potential to cause harm (C) An injury (D) A safety rule ✓ **B.** *A hazard is a potential to cause harm.*

2. Risk is a function of likelihood and: (A) Cost (B) Severity (C) Time (D) Distance ✓ **B.** *Risk = likelihood × severity.*

3. The largest share of accident cost is usually: (A) Direct/visible (B) Indirect/hidden (C) Insurance only (D) Medical only ✓ **B.** *Indirect costs typically far exceed the visible direct costs.*

See also — companion volume

Engineering Quality Assurance, Chapter 1 (The Meaning and Evolution of Quality) is this chapter's twin: quality and safety both evolved from after-the-fact inspection toward designed-in prevention, and both rest on the same insight that the property you want — conformance or harm-avoidance — must be built in, not hoped for. The risk thinking introduced here is developed quantitatively in that volume's Chapter 19.

PART I — FOUNDATIONS OF SAFETY

Chapter 2 — Accident Causation and Safety Philosophies

Learning Objectives

Explain why models of accident causation matter for prevention.

Interpret Heinrich's safety triangle and the value of near-miss reporting.

Describe the domino model of sequential causation and its limits.

Explain Reason's Swiss Cheese model of latent and active failures.

Outline modern systems thinking, high-reliability organisations, and Safety-II.

Choose an appropriate causation lens for analysing and preventing accidents.

Key Concepts

- Accident causation models; why they shape prevention.
- Heinrich's triangle; the ratio of near-misses to serious harm.
- The domino model; sequential, linear causation.
- Reason's Swiss Cheese model; latent vs active failures; defence in depth.
- Systems thinking, high-reliability organisations (HRO), and Safety-II.

2.1 Why Models of Causation Matter

How you think accidents happen determines how you try to prevent them. If you believe accidents are caused by careless workers, you will respond with discipline and posters; if you believe they emerge from flawed systems, you will redesign the work; if you believe they result from the alignment of many small failures, you will build layered defences. A model of accident causation is therefore not an academic abstraction but the hidden logic behind every safety programme, and choosing a good model is the difference between blaming people and actually preventing harm. This chapter traces the major models in the order they emerged, because each corrected a limitation in the last, and together they form the modern safety practitioner's mental toolkit.

2.2 Heinrich's Triangle

In the 1930s Herbert Heinrich, studying thousands of industrial accidents, observed a consistent numerical relationship between outcomes of differing severity, captured in what is now called the safety triangle or accident pyramid.

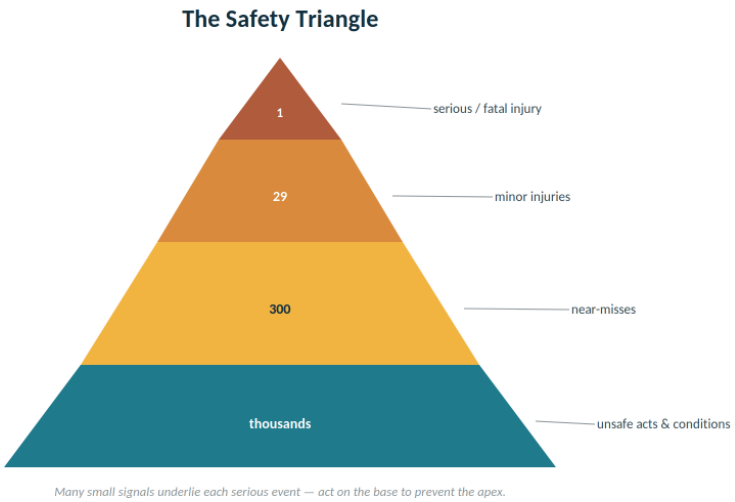

Figure 2.1 The safety triangle: many minor events underlie each serious one.

The triangle holds that for every serious or fatal injury there are many more minor injuries, many more near-misses, and a vast base of unsafe acts and conditions — in Heinrich's original ratio, roughly 1 : 29 : 300, with thousands of unsafe acts beneath. The exact numbers are less important than the principle, which is profound and remains central to modern safety: serious harm sits atop a broad base of smaller signals, and those signals are warnings. The practical consequence is the discipline of near-miss reporting — treating the near-misses and unsafe conditions at the base as free lessons, investigated and acted upon before they climb the triangle to become a serious injury. An organisation that ignores its near-misses is, in effect, waiting for the apex. The triangle has been criticised for implying that reducing minor injuries automatically reduces fatalities — the causes can differ — but its core insight, that you should act on weak signals at the base, is sound and enduring.

2.3 The Domino Model

Heinrich also gave safety its first causation model: the domino theory, which pictured an accident as the last in a falling line of dominoes.

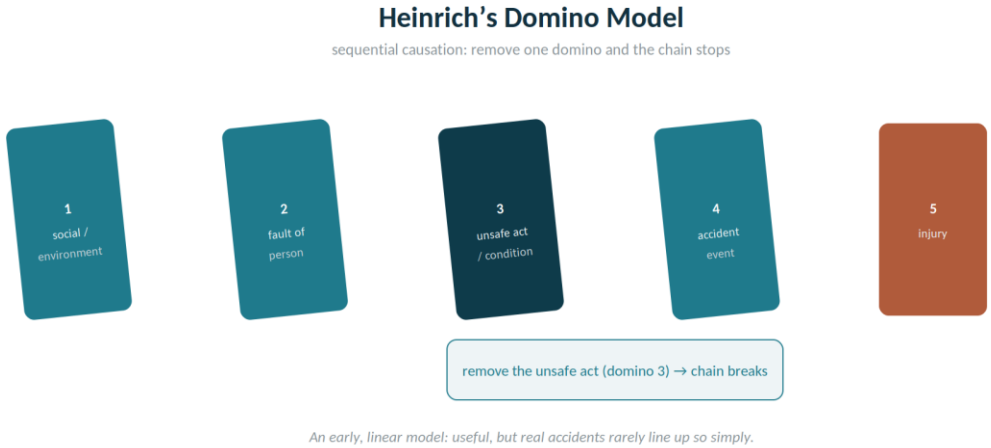

Figure 2.2 The domino model: accidents as a sequence of falling causes.

In this model, five factors fall in sequence — the social environment and ancestry, the fault of the person, an unsafe act or condition, the accident, and finally the injury — each toppling the next. Its enduring contribution is the idea that an accident is the end of a causal chain, not a random bolt from the blue, and crucially that removing any single domino stops the sequence: take away the unsafe act or condition and the accident never reaches the injury. This was a powerful step toward prevention. Its limitation, recognised later, is that it is linear and simplistic: real accidents rarely arise from a single neat chain, but from many interacting causes, and the model's focus on the 'fault of the person' encouraged blaming the worker rather than examining the system — the very trap Chapter 9 warns against.

2.4 Reason's Swiss Cheese Model

The dominant modern model, proposed by James Reason, replaces the single chain with layered defences and explains why well-defended systems still suffer accidents.

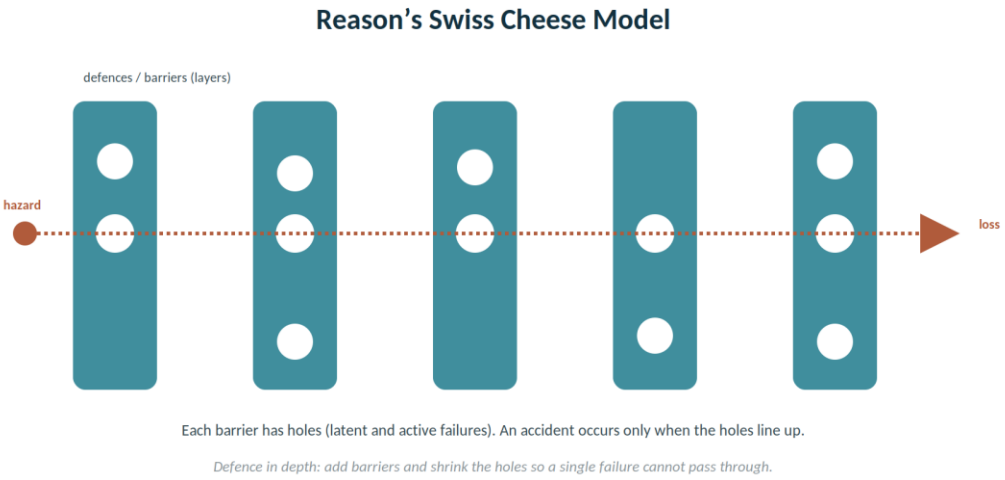

Figure 2.3 The Swiss Cheese model: an accident occurs only when holes in successive defences line up.

Picture an organisation's defences against a hazard as a series of barriers — procedures, training, guards, alarms, supervision — each drawn as a slice of Swiss cheese. No barrier is perfect; each has holes, which are its weaknesses and failures. The holes are of two kinds. Active failures are the unsafe acts of people at the sharp end — the slip, the lapse, the violation — whose effect is immediate. Latent failures are the hidden weaknesses built into the system long before — a poor design, an under-resourced team, a flawed procedure, a production-before-safety culture — that lie dormant until they combine with an active failure. An accident happens only when, on a particular occasion, the holes in every barrier momentarily line up, letting the hazard pass through all the defences to cause harm. The model's power is twofold: it explains why accidents in well-defended systems are rare but never impossible, and it directs prevention not at blaming the person whose active failure was the last hole, but at finding and closing the

latent failures — the holes that were waiting. This is the principle of defence in depth: provide multiple, independent barriers and keep shrinking their holes, so that no single failure can ever pass through alone.

2.5 Modern Thinking: Systems, HRO, and Safety-II

Safety thinking has continued to evolve beyond even the Swiss Cheese model. Systems thinking holds that in complex, tightly coupled operations, accidents can emerge from the interactions between parts that are each working as designed — no single broken component, but a dangerous combination — requiring analysis of the whole system rather than its pieces. High-reliability organisations (HROs) — such as aircraft carriers, air-traffic control, and nuclear operations — are studied because they achieve extraordinary safety in hazardous conditions through a distinctive culture: preoccupation with failure, reluctance to simplify, sensitivity to operations, commitment to resilience, and deference to expertise over rank. And Safety-II reframes the goal itself: instead of only studying the rare times things go wrong (Safety-I), it studies the many times things go right, asking how people's everyday adaptations and expertise create safety, and how to strengthen them. These modern lenses do not discard Heinrich or Reason; they extend them, shifting attention from components to systems, from blame to learning, and from counting failures to building resilience.

Standards & Method Spotlight — causation and learning

Reason's Swiss Cheese model underpins most modern incident-investigation methods (Chapter 8).

HRO principles (Weick & Sutcliffe) inform high-hazard industry safety culture (Chapter 9).

Safety-II / Resilience Engineering (Hollnagel) reframes safety as the presence of success.

Near-miss reporting systems operationalise the base of the safety triangle.

2.6 Multi-disciplinary Applications and a Case Study

These models are applied across every high-hazard field. Aviation built its remarkable safety record on Swiss-Cheese thinking and just-culture reporting; healthcare adopted the same models to attack medical error; the nuclear and offshore industries are studied as high-reliability organisations; and process-safety investigations (Chapter 19) routinely map latent and active failures onto layered defences. The vocabulary differs, but the underlying logic — accidents as the alignment of many failures across imperfect barriers — is shared.

Case Study 2.1 — The holes that lined up

A worker was injured when a machine restarted unexpectedly during a clearing task. The immediate, tempting conclusion was operator error: the worker had reached in without isolating the machine — an active failure. A blame-based response would have stopped there, with retraining and a warning.

A Swiss-Cheese investigation looked instead for the holes behind the hole. It found a string of latent failures lined up behind the worker's act: the isolation procedure was ambiguous and rarely enforced; the guard interlock had been bypassed months earlier to speed up clearing and never restored; production pressure made stopping the line strongly discouraged; and supervision was stretched thin on the night shift. The worker's active failure was simply the last hole; behind it sat four latent failures that management had built and tolerated.

The lesson is section 2.4 in action. Blaming the worker would have left every latent hole open for the next person. Real prevention came from closing them — restoring the interlock, clarifying and enforcing isolation, and relieving the production pressure — which is exactly where the Swiss-Cheese model directs attention, and why it has displaced the blame-the-person logic of the early domino era.

2.7 Best Practices, Common Mistakes, and Troubleshooting

Best Practices

- Treat near-misses and unsafe conditions as free warnings and investigate them before they escalate.
- Look behind every active failure for the latent failures that allowed it.
- Build defence in depth — multiple independent barriers — and keep shrinking their holes.
- Adopt a just culture that learns from error rather than punishing the last person in the chain.

Common Mistakes

- Stopping the investigation at the worker's active failure and missing the latent ones.
- Assuming that reducing minor injuries automatically reduces fatalities (different causes).
- Relying on a single barrier instead of layered, independent defences.
- Ignoring near-misses because 'no one got hurt.'

Troubleshooting

Symptom	Likely root cause	First action
Same type of accident keeps recurring	Latent failures never addressed	Investigate behind the active failure (2.4, Ch 8)
Blame culture, hidden near-misses	People fear reporting	Build a just culture; protect reporters (Ch 9)
A single failure caused a serious event	No defence in depth	Add independent barriers; shrink holes

Frequently Asked Questions

Q: What is the difference between an active and a latent failure? **A:** An active failure is an unsafe act with immediate effect at the sharp end (a slip, lapse, or violation). A latent

failure is a hidden system weakness — a poor procedure, design, or culture — that lies dormant until it combines with an active failure to cause harm.

Q: Is Heinrich's 1:29:300 ratio exact? **A:** No — the specific numbers are not a law of nature and vary by industry. The enduring value is the principle: serious harm sits atop many smaller signals, so acting on near-misses prevents the rare apex event.

Q: Why is the Swiss Cheese model better than the domino model? **A:** Because real accidents rarely arise from a single neat chain. The Swiss Cheese model captures multiple imperfect barriers and the latent failures behind the obvious active one, directing prevention at the system rather than at blaming the last person.

Chapter Summary

How we believe accidents happen shapes how we try to prevent them, so models of causation are the hidden logic behind every safety programme. Heinrich's triangle shows serious harm sitting atop a broad base of minor injuries, near-misses, and unsafe acts, making near-miss reporting a way to act on weak signals before they reach the apex. His domino model framed accidents as a sequence of causes in which removing one link stops the chain, but its linear, person-focused view was too simple. Reason's Swiss Cheese model — now dominant — pictures layered defences each with holes, where active failures at the sharp end combine with hidden latent failures, and an accident occurs only when the holes line up; it directs prevention at closing latent failures and building defence in depth rather than blaming the last person. Modern systems thinking, high-reliability organisations, and Safety-II extend this further, shifting from components to systems, from blame to learning, and from counting failures to building resilience.

Glossary

Accident causation model — A theory of how accidents happen that shapes how they are prevented.

Safety triangle — Heinrich's ratio of serious to minor to near-miss events — act on the base.

Domino model — Early linear model of accidents as a sequence of falling causes.

Active failure — An unsafe act with immediate effect at the sharp end.

Latent failure — A hidden system weakness that lies dormant until it combines with an active failure.

Defence in depth — Multiple independent barriers so no single failure causes harm.

References and Suggested Reading

1. Reason, J. Human Error. Cambridge University Press.
2. Reason, J. Managing the Risks of Organizational Accidents. Ashgate.
3. Heinrich, H. W. Industrial Accident Prevention. McGraw-Hill.
4. Weick, K. E. & Sutcliffe, K. M. Managing the Unexpected (HRO). Wiley.
5. Hollnagel, E. Safety-I and Safety-II. Ashgate.

6. Dekker, S. The Field Guide to Understanding 'Human Error'. Ashgate.

Review Questions — Chapter 2

Recall

1. What does Heinrich's triangle represent?
2. Name the five dominoes in Heinrich's sequence.
3. Distinguish active from latent failures.

Application

1. For a workplace slip injury, sketch a Swiss-Cheese diagram naming two barriers and the holes in each.
2. Explain how a near-miss reporting scheme operationalises the base of the safety triangle.
3. Identify one active and two latent failures in a described accident.

Analysis

1. Explain why the domino model's focus on the 'fault of the person' is a weakness.
2. Using Case Study 2.1, explain how blaming the worker would have left the system unsafe.

Design

1. Design a near-miss reporting form that encourages honest reporting and captures latent causes.
2. Design a defence-in-depth scheme for a specified hazard, naming at least three independent barriers.

Multiple-Choice Questions

1. The Swiss Cheese model represents accidents as occurring when: (A) A worker is careless (B) Holes in successive defences align (C) A single domino falls (D) Costs exceed budget ✓ **Answer: B.** *An accident passes only when holes in all barriers line up.*

2. A bypassed guard interlock left unrepaired for months is a: (A) Active failure (B) Latent failure (C) Near-miss (D) Control ✓ **Answer: B.** *It is a hidden, dormant system weakness — a latent failure.*

3. The base of Heinrich's triangle consists of: (A) Fatalities (B) Serious injuries (C) Near-misses and unsafe acts (D) Insurance claims ✓ **Answer: C.** *Unsafe acts and near-misses form the broad base.*

4. High-reliability organisations are characterised by: (A) Complacency (B) Preoccupation with failure (C) Blame culture (D) Minimal training ✓ **Answer: B.** *HROs are preoccupied with failure and committed to resilience.*

Short and Long Questions

Short Questions

1. Why does the choice of causation model affect how accidents are prevented?
2. Why should near-misses be investigated even though no one was hurt?
3. What is defence in depth?

Long Questions

1. Compare the domino and Swiss Cheese models, explaining what each captures and where each falls short.
2. Explain latent and active failures using the Swiss Cheese model and show how they direct prevention.

Problems, Labs, and Projects

Structured Problems

1. Given a described accident, classify each contributing factor as an active or latent failure.
2. For a given hazard, list four barriers and a plausible hole in each.
3. Map a near-miss onto the safety triangle and explain what acting on it would prevent.

Practical Assignment

Take a real or reported accident and analyse it with the Swiss Cheese model: identify the active failure, at least three latent failures, and the barriers whose holes aligned.

Laboratory Activity

Lab 2 — Causation analysis. For a simulated incident scenario, the team builds both a domino chain and a Swiss-Cheese diagram, then compares what each reveals and which better directs prevention. Deliverable: both diagrams and a short comparison.

Mini-Project

Design a just-culture near-miss reporting scheme for an organisation: the form, the no-blame protections, and how reports would be triaged and acted upon to close latent failures.

Capstone Project Idea

For your running workplace project, take one credible accident scenario and analyse it with the Swiss Cheese model, identifying the latent failures already present in the workplace and the barriers needed to close them.

Interview and Certification Practice

Interview Questions

- Explain the Swiss Cheese model to someone who has never heard of it.
- Why is blaming the worker usually the wrong response to an accident?
- How would you use near-miss data to prevent serious injuries?
- What can ordinary industry learn from high-reliability organisations?

Certification Practice (NEBOSH / functional-safety style)

1. A latent failure is best described as: (A) An immediate unsafe act (B) A dormant system weakness (C) A near-miss (D) A type of guard ✓ **B.** *A latent failure is a hidden weakness awaiting an active failure.*

2. The principle of providing multiple independent barriers is: (A) Single-point control (B) Defence in depth (C) Blame culture (D) Cost control ✓ **B.** *Defence in depth uses layered, independent barriers.*

3. Acting on the base of Heinrich's triangle means: (A) Investigating only fatalities (B) Acting on near-misses and unsafe acts (C) Ignoring minor events (D) Counting claims ✓ **B.** *The base is the near-misses and unsafe acts to act upon.*

See also — companion volume

Engineering Quality Assurance, Chapter 2 (Quality Philosophies and the Gurus) is the parallel chapter: just as safety's thinkers moved from blaming workers to fixing systems, quality's pioneers — Deming above all — argued that most failures are system failures, not worker failures. The Swiss Cheese model's latent failures are the safety face of Deming's common-cause variation.

END OF FREE PREVIEW

Continue reading — Chapters 3 to 20

Engineering Safety • Engineering Excellence Series, Book 2

You have just finished Chapters 1 and 2. The complete book carries you through the remaining eighteen chapters — hazard, risk and the hierarchy of controls, the legal and standards landscape, ISO 45001, risk-assessment techniques, permits and safe systems of work, incident investigation and safety audits, human factors and safety culture, machine, electrical, fire and explosion hazards, functional safety and IEC 61508, safety integrity levels, safety instrumented systems, machinery functional safety, process safety and major-hazard management — with worked examples, industrial case studies, four-tier review questions, and certification practice throughout.

Full book (189 pages, 20 chapters) — US$50

Email Dr. Ahsan Rahman to purchase. He will share payment details and send the complete PDF to you personally.

ahsan.rahman@gmail.com • ahsanrahman.com

Series bundle: Book 1 (Engineering Quality Assurance) + Book 2 (Engineering Safety) — US$95.