Maritime Accident and Incident Investigation

Alexander Arnfinn Olsen

Maritime Accident and Incident Investigation

Maritime Accident and Incident Investigation covers a wide range of topics relating to maritime-orientated organisational hazards and risks, as well as root cause analyses and techniques for analysing evidence. Its approach to maritime casualty and incident investigation caters to the unique needs of the maritime industry and covers the human element, machinery and engineering, and structural and security concerns.

The book is divided into four parts, which respectively introduce the concepts and theories of organisational risks and hazards; provide a framework structure for planning, initiating, performing, and closing out maritime casualty and incident investigations; provide an overview of the main forms of analyses; and offer a toolkit of forms and documents for preparing and carrying out incident investigations.

Features:

- Focuses on basic principles independent of particular software or protocols, allowing customisation to the reader's own management system, Health, Safety and Environment (HSE) programmes, or related initiatives
- Supports the reader in applying class-related activities such as the provisions of the International Safety Management (ISM) Code and the International Ship and Port Facility Security (ISPS) Code

The book is ideal for trainees, advanced students, and junior maritime professionals involved in the investigation of maritime accidents and incidents. Also available as online Support Material is a full MaRCIIF Toolkit, containing several resources, such as checklists, forms, and guidelines, useful in the execution of maritime incident investigations. Access the Support Material: www.routledge.com/9781032530239

Alexander Arnfinn Olsen is a Senior Consultant at RINA Consulting Defence UK. He is STCW II 1995 qualified and has also worked as a marine training designer, marine auditor, and fisheries observer. He is the author of *Introduction to Ship Operations and Onboard Safety*, *Core Concepts of Maritime Navigation*, *Introduction to Ship Engine Room Systems*, *Maritime Cargo Operations*, *Merchant Ship Types*, and *Firefighting and Fire Safety Systems on Ships* (with Routledge).

Maritime Accident and Incident Investigation

Alexander Arnfinn Olsen

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

Cover image: Shutterstock ©

First published 2023
by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
Names: Olsen, Alexander Arnfinn, author.
Title: Maritime accident and incident investigation / Alexander Arnfinn Olsen.
Description: Abingdon, Oxon; New York, NY : Routledge, 2024. |
Includes bibliographical references and index.
Identifiers: LCCN 2023005169 | ISBN 9781032530604 (hbk) |
ISBN 9781032530239 (pbk) | ISBN 9781003409977 (ebk)
Subjects: LCSH: Marine accidents—Investigation—Handbooks, manuals, etc. |
Marine accidents—Prevention—Handbooks, manuals, etc. | Merchant
marine—Safety measures—Handbooks, manuals, etc. | Shipping—Risk
management—Handbooks, manuals, etc.
Classification: LCC VK199 .O47 2024 | DDC 363.12/365—dc23/eng/20230530
LC record available at https://lccn.loc.gov/2023005169

ISBN: 978-1-032-53060-4 (hbk)
ISBN: 978-1-032-53023-9 (pbk)
ISBN: 978-1-003-40997-7 (ebk)

DOI: 10.1201/9781003409977

Typeset in Sabon
by codeMantra

Contents

List of Figures

List of Tables

Preface

Every year, the maritime industry experiences incidents that range from the minor and inconsequential to major newsworthy events. These incidents should be investigated since many Flag State Administration regulations require it; international agreements mandate it (such as the IMO ISM Code); and industry initiatives encourage it. Incident investigation is a process that is designed to help the shipping industry learn from past performance and develop strategies to improve safety on ships. This book is intended as support material for marine professionals tasked with conducting investigations under the IMO Casualty Investigation (CI) Code,[1] which came into force on 1 January 2010. The book is divided into two main components: the first examines the principles of hazard and risk analysis (HRA), and the second provides a framework through which investigators can conduct maritime casualty and incident investigations. The principle of investigating marine casualties has been included, for many years in international maritime conventions including UNCLOS,[2] SOLAS,[3] and MARPOL.[4] It should be noted, however, that the purpose of the various conventions differs. Whilst SOLAS does not provide for any sanctions that may result in court or disciplinary action, MARPOL (as implied in Article 4(2)) includes provisions that may have adverse outcomes for individuals who contravene MARPOL. The CI Code incorporates and builds on the best practices in safety investigation and seeks the promotion of cooperation and a common approach to marine casualty and marine incident investigation between Maritime States. Whilst the CI Code specifies a limited number of mandatory requirements, it also recognises the variations in international and national laws and includes many recommended practices as a result. The thrust of the CI Code is not one of prosecution or sanction, but rather, is focused on investigations that result in safety outcomes and which do not attribute blame or apportion liability. As such, safety investigations under the CI Code are primarily focused on understanding the underpinning causes and reasons why an unsafe action or condition led to the casualty and the environment – be it physical and or organisational – in which the casualty or incident occurred.

[1] International Convention for the Safety of Life at Sea (SOLAS) 08 amendment, Chapter XI-1, Regulation 6, additional requirements for the investigation of marine casualties and incidents.

[2] United Nations Conventions on the Law of the Sea (UNCLOS), Article 94(7), Duties of the Flag State.

[3] International Convention for the Safety of Life At Sea (SOLAS) 74, Chapter I, Regulation 21, Casualties.

[4] The International Convention for the Prevention of Pollution from Ships, Article 12, Casualties to ships.

ABOUT THIS BOOK

Throughout this book, we will refer to a process that we will call the *maritime casualty and incident investigation framework* or MarCIIF. MarCIIF is a process that provides an effective and efficient approach for investigating marine casualties and incidents of any magnitude. This process is the outcome of an evaluation of hazard and risk analyses, shipping industry best practices, and established maritime investigation techniques. The approach offered by this book to maritime casualty and incident investigation caters to the unique needs of the maritime industry and covers the human element, machinery and engineering, and structural as well as security concerns. In essence, the aim of the MarCIIF approach is to

- Provide the reader with a framework that will guide them in the conduct of root cause analyses and in so doing, assist in identifying, documenting, and trending the causes of maritime casualties, accidents, and near-misses.
- Provide the reader with background into the investigation of a variety of types (for example, groundings, collisions, and fires) and sizes of casualties and incidents (minor to major, including near-misses) related to their vessels and facilities (ashore and at sea).
- Allow the reader to analyse losses whether they are related to safety, the environment, human element concerns, security, reliability, quality, or business losses.
- Support the reader in applying class-related activities such as the provisions of the ISM Code and the ISPS Code.[5]
- Provide the reader with techniques that are sufficiently flexible to allow customisation to the reader's own management system, HSE programmes, or related initiatives.

Furthermore, this book has been developed to provide the reader with guidance for planning, conducting, and closing out maritime casualty and incident investigation activities, including

- An introduction to the core concepts of hazard and risk analysis.
- Incident investigation initiation techniques.
- Data gathering.
- Data analysis.
- Root cause determination.
- Development of generation recommendations.
- Reporting and trend identification of maritime casualty and incident investigation outcomes.

Given the wide-reaching breadth of this approach, this book has been purposefully divided into parts. The first part concentrates on introducing the concepts and theories of organisational risks and hazards and how these impact on organisational performance and safety. The second part provides a framework structure for planning, initiating, performing, and closing out maritime casualty and incident investigations

[5] The ISPS Code entered into force under SOLAS chapter XI-2, on 1 July 2004.

in accordance with MarCIIF; Part 3 provides the reader with an overview of the three main forms of analyses (MarCIIF, fault tree analysis, and causal factor charting); and Part 4 contains tools and templates that the reader may find useful when preparing for and carrying out incident investigations.

Alexander Arnfinn Olsen
Southampton, January 2023

Author's note

As there are various commercial off-the-shelf (COTS) software packages that provide incident root cause analysis, this book has taken a deliberately generic approach which will apply to any number of proprietary COTS products. The reader may therefore find some dissimilarities between the examples provided herein and what they may view when accessing root cause analysis software. In any case, the principles are the same and should be applied irrespective of the COTS software used.

Acknowledgements

I would like to acknowledge and thank my editor, Tony Moore and Aimee Wragg, and the production team at Code Mantra, with particular thanks to SM Amudhapriya for their support and guidance in writing this book. I would also like to thank Oessur J. Hilduberg, Head of the Danish Maritime Accident Investigation Board for permission to reproduce the accident investigation report into the unfortunate incident onboard the *Hendrika Jacoba*. Finally, I would like to extend my warmest thanks and gratitude to my wife, Fidaa, who has always kept my morale high even when the going gets tough. To you all, my gratitude and my thanks.

Abbreviations and acronyms

°C	Degrees Centigrade
°F	Degrees Fahrenheit
AB	Able Seaman
ABS	American Bureau of Shipping (US)
ACA	Apparent Cause Analysis
AIAG	Automotive Industry Action Group (US)
ALARP	As Low As Reasonably Practicable
ARPA	Automatic Radar Plotting Aid
ATSB	Australian Transport Safety Bureau (AUS)
AUS	Australia
BAE	**BAE Systems**
BBRM	Behaviour-Based Resource Management
BV	Bureau Veritas (FRA)
CA	Criticality Analysis
CAR	Corrective Action Request
CAV	Connected and automated vehicles
CCTV	Closed circuit television
CD	Compact Disk
CENELEC	*French:* Comité Européen de Normalisation Électrotechnique *English:* European Committee for Electrotechnical Standardisation
COC	Chain of Custody
COLREG	Convention on the International Regulations for Preventing Collisions at Sea 1972
COSHH	Control of Substances Hazardous to Health Regulations 2002
COTS	Commercial off-the-shelf
DE	*German:* Deutschland *English:* Germany
Def Stan	Defence Standard
DG	Diesel Generator
DIAB	Danish Maritime Accident Investigation Board
DNV	Det Norske Veritas (NOR)
DOD	Department of Defence (US)
DPA	Designated Person Ashore
DRACAS	Data Reporting Analysis and Corrective Action System
DSE	Display Screen Equipment

DTI	Department of Trade and Industry (UK)
DTSB	Dutch Transport Safety Board (NL)
EEZ	Exclusive economic zone
E/E/PE	Electrical/Electronic/Programmable Electronic
EOL	End-of-life
EOW	Engineer of the Watch (Engineering)
ETA	Event Tree Analysis
EUC	Equipment Under Consideration
EUR	Euro (€)
FHA	Failure Hazard Analysis
FMD	Failure Mode Distribution
FMEA	Failure Modes, Effects Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
FRA	France
FRACAS	Failure Reporting, Analysis, and Corrective Action System
FSHA	Functional Systems Hazard Analysis
FTA	Fault Tree Analysis
GAMAB	*French:* Globalement au moins aussi bon *English:* Globally at least as good
GAME	*French:* Globalement au moins equivalent English*:* Globally at least as good
GBP	British Pound Sterling (£)
GL	Germanischer Lloyd (DE)
GMDSS	Global Maritime Distress and Safety System
GPS	Global Positioning System
HASAWA	Health and Safety at Work etc. Act 1974 (UK)
HAZOP	Hazards and Operability Analysis
HEART	Human Error Assessment and Reduction Techniques
HERP	Human Error Rate Prediction
HRA	Hazard and Risk Analysis
HSE	Health, Safety and Environment (UK)
HUD	Head Up Display
HVAC	Heating, Ventilation and Air Conditioning
ICI	Imperial Chemical Industries (1926–2008)
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ILO	International Labour Organisation
IMO	International Maritime Organisation
ION	Item-of-Note
ISM	International Safety Management Code
ISO	International Organisation for Standardisation
ISPS	International Ship and Port Facility Security Code
ISS	International Space Station
IT	*Italian:* Italia *English:* Italy
JPN	*Japanese:* Nippon *English:* Japan

JSA	Job Safety Analysis
km	Kilometres
KOR	*Korean:* Hanguk *English:* South Korea
KR	Korean Register (KOR)
LOLER	Lifting Operations and Lifting Equipment Regulations 1998 (UK)
LNG	**Liquid natural gas**
LR	Lloyds Register (UK)
LTA	Loss Time Accident
MAIB	Marine Accident Investigation Branch (UK)
MarCIIF	Maritime Casualty and Incident Investigation Framework
MARPOL	International Convention for the Prevention of Pollution from Ships, 1973/78
MCA	Maritime and Coastguard Agency (UK)
MEM	*German:* Minimale endogene Mortalität *English:* Minimum Endogenous Mortality
Mi	Miles
MIL-STD	Military Standard (US)
MOCA	Management of Change Assessment
MOD	Ministry of Defence (UK)
MOTU	Maritime Operational Training Unit
MS	Management System
N	*Norwegian:* Norge *English:* Norway
NASA	National Aeronautics and Space Administration (US)
NATO	North Atlantic Treaty Organisation
Navtex	Navigational Telex
NDT	Non-Destructive Testing
NK	Nippon Kaiji Kyokai (JPN)
NL	*Dutch:* Nederland *English:* The Netherlands (Holland)
NTM	Notice-to-Mariner
NTSB	National Transportation Safety Board (US)
OBO	Oil Bulk Ore (carrier)
OCIMF	Oil Companies International Marine Forum
OCM	Oil Content Meter
OHHA	Occupational Health Hazard Analysis
OHSAS	Occupational Health and Safety Assessment Series
OOW	Officer of the Watch (Deck)
OS	Ordinary Seaman
OSHA	Operating and Support Analysis
pf	Probability of failure
PFD_{avg}	Probability of Failure on Demand
PHA	Preliminary Hazard Analysis
PPE	Personal Protective Equipment
p_s	Probability of success
PSC	Project Safety Committee

PSSR	Pressure Systems Safety Regulations 2000 (UK)
PUWER	Provision and Use of Work Equipment Regulations 1998 (UK)
QC	Queen's Counsel (alt. KC – King's Counsel) (UK)
RAF	Royal Air Force (UK)
RAMS	Reliability, Availability, Maintainability, and Safety
RCA	Root Cause Analysis
RCM	Reliability-Centred Maintenance
RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013
RINA	Registro Italiano Navale (IT)
RMS	Royal Mail Ship
RORO	Roll On Roll Off
RPN	Region Proposal Network
RSSB	Rail Safety and Standards Board (UK)
SAE	Society of Aeronautical Engineers (UK)
SCP	Supplementary Conditioning Pack
SEMP	Systems Engineering Management Plan
SFARP	So Far As Is Reasonably Practicable
SFPS	Single Failure Points
SHA	Systems Hazard Analysis
SHERPA	Systematic Human Error Reduction and Process Analysis
SI	Statutory Instrument (UK)
SIL	Safety Integrity Level
SMS (1)	Safety Management System
SMS (2)	Ship Management System
SOLAS	International Convention for the Safety of Life at Sea 1974
SPAC	Standards, Policies, or Administrative Controls
SPAR(H)	Systematic Human Error Reduction and Process Analysis (Human Reliability Analysis)
SQE	Safety, Quality, and Environment
SSOW	Safe Systems of Work
STCW	International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers 1978
SWIFT	Structured What If Techniques
THERP	Technique for Human Error Rate Prediction
TMSA	Tanker Management and Self-Assessment
UK	United Kingdom
US NRC	United States Nuclear Regulatory Commission (US)
US	United States
USCG	United States Coast Guard (US)
USD	United States Dollar ($)
VDA	German Association of the Automotive Industry (DE)
WAH	Working at Height Regulations 2005 (UK)
WIA	What-If Analysis
ZHA	Zonal Hazard Analysis

Part I

Introducing hazards and risks

Chapter 1

Core concepts and themes of hazard and risk analysis

In this first chapter, we will begin by looking at some of the core concepts and themes maritime casualty and incident investigators encountered during the investigation process. It is important to understand the core concepts and themes of hazard and risk as they will have a direct bearing on how you plan, prepare, and carry out your investigation. They will also influence how you interpret the root causes of the incident when concluding the investigation. To that end, we will begin by examining organisational safety management. Moreover, the principles of hazard analysis and risk management are widely applied within many organisations to minimise the risk of incidents from occurring in the first place, and where the risk cannot be removed, to mitigate the impact of those risks. If this all seems a bit complicated, worry not as we will examine each of these themes throughout this book. Before we go on, it is perhaps worth explaining what we mean by organisation… when we refer to an organisation, we can refer to an entire company, a single operational entity such as a ship, a component of that entity such as the navigational bridge or engine room, or a subcomponent such as a set of actions (procedures). Given hazard and risk forms an entire subdomain of organisational safety, we will limit our attention to four key concepts, which are as follows:

- Casualties, accidents, and incidents.
- Hazards.
- Risks.
- Safety.

DEFINING KEY TERMS

Casualties, accidents, and incidents. The Health and Safety Executive (HSE), which is an independent authority of the UK Government, uses the term "adverse event" to describe what we will refer to as an "accident" or "incident". The HSE describes an incident as "a near miss or undesired circumstance", whereas an accident is defined as an "event that results in injury or ill health". Many types of accidents and incidents are indicative of weak safety management procedures and processes within an organisation, which are collectively called the Safety Management System. Not every organisational

DOI: 10.1201/9781003409977-2

approach to safety management is done in the same way. Different organisations use different words and terminologies to refer to the same thing. For example, the International Electrotechnical Commission (IEC), in their standard IEC 61508, refers to "hazardous events" instead of "accidents". The US Department of Defence (DOD), in Military Standard 882 (MIL-STD-882), refers instead to "mishaps". To complicate matters further, those organisations that do use the term "accident" frequently apply different definitions altogether. To simplify matters, throughout this book, we will use the HSE definition of an accident, which is "an event or situation in which people are injured".[1]

1. **Hazards.** In the previous section, we across the terms "hazard" and "hazardous event". These are important terms and are, in fact, central to understanding the principles of organisational safety management and implementing safe systems of work (SSOW). As we saw with "accidents", there is no universally accepted definition of "hazard", though for our purposes we can turn to IEC 61508, which defines a hazard as a "potential source of harm". In this sense, harm means any form of injury or ill health to a person or people. If harm is any form of injury or ill health caused to a person, and an accident is an event that leads to injury or ill health, we can say that a hazard is in effect a potential source of an accident. The problem with this definition is that it is too broad. This is because (a) we cannot be certain whether the potential source of an accident (the hazard) will occur and (b) we cannot be certain we can pinpoint the exact cause of the accident. To simplify things, we can think of an organisation or process as a *system*. Some systems contain hundreds, and even thousands, of hazards. Some hazards are seemingly innocuous, such as standing on a stool. Other hazards have the potential to cause life-changing injuries or organisational damage (for example, the sinking of the Italian cruise ship, *Costa Concordia*, in 2012[2]). What is important to recognise is that one or more small hazards have

[1] HSE, 2004. *Investigating accidents and incidents: A workbook for employers, unions, safety representatives and safety professionals*. https://www.hse.gov.uk/pubns/hsg245.pdf

[2] On 13 January 2012, the Costa Cruises vessel *Costa Concordia* (Figures 1.1 and 1.2) was on the last leg of a cruise around the Mediterranean Sea when she deviated from her planned route at Isola del Giglio, Tuscany. The ship was steered closer to the island and struck a rock formation on the sea floor. This caused the ship to list and then capsize, landing unevenly on an underwater ledge. Although a six-hour rescue effort brought most of the passengers ashore, 34 people died: 27 passengers, 5 crew, and later, 2 members of the salvage team. An investigation focused on shortcomings in the procedures followed by *Costa Concordia*'s crew and the actions of her captain, Francesco Schettino, who left the ship prematurely. He left about 300 passengers onboard the sinking vessel, most of whom were rescued by helicopter or motorboats in the area. Schettino was found guilty of manslaughter and sentenced to 16 years in prison. Despite receiving its own share of criticism, Costa Cruises and its parent company, Carnival Corporation, did not face criminal charges. *Costa Concordia* was declared a "constructive total loss" by the cruise line's insurer, and her salvage was "one of the biggest maritime salvage operations". On 16 September 2013, the parbuckle salvage of the ship began, and by the early hours of 17 September, the ship was set upright on her underwater cradle. In July 2014, the ship was refloated using sponsons (floatation tanks) welded to her sides and was towed 200 mi (320 km) to her home port of Genoa for scrapping, which was completed in July 2017. The total cost of the disaster, including victims' compensation, refloating, towing, and scrapping costs, is estimated at USD 2 billion, more than three times the USD 612 million construction cost of the ship. Costa Cruises offered compensation to passengers (to a limit of Euros 11,000; GBP 9,468; USD 11,448 per person) to pay for all damages, including the value of the cruise; one-third of the survivors accepted the offer.

the potential to lead to larger complex hazards. It is almost impossible for complex organisations such as shipping companies and airlines to identify every single hazard within their processes. To get around this, we can refer instead to "system-level hazards".

2. **System-level hazards.** A system-level hazard is a hazard that occurs on the boundary of the system in question. This may involve the failure of a system-level function, or the failure of an entire system level, either of which will have an interaction with the outside world leading to an "external event". Imagine we have a railway and along that railway are a series of complex signals, junctions, and crossings. What would happen if a resistor in one of those signals failed? It might cause a red light to turn green. A train passing that signal will think it is safe to proceed when in fact there may be an obstruction on the line a mile or so around a corner. The consequences of that simple failure could be devastating. In this scenario, the resistor is a hazard, but its failure was the primary cause of the second hazard, which is the red light turning green. In essence, we have two separate hazards which, when combined, create a system-level hazard. It is useful to focus on system-level hazards for two reasons: (a) doing so provides a relatively tidy way of determining the chances of a hazard occurring and the likelihood that hazard(s) will evolve into an accident; and (b) by doing so, it makes it easier to manage the overall number of hazards an organisation face. This is because the previously non-system-level hazards are now considered the causes of system-level hazards (Figures 1.1 and 1.2).

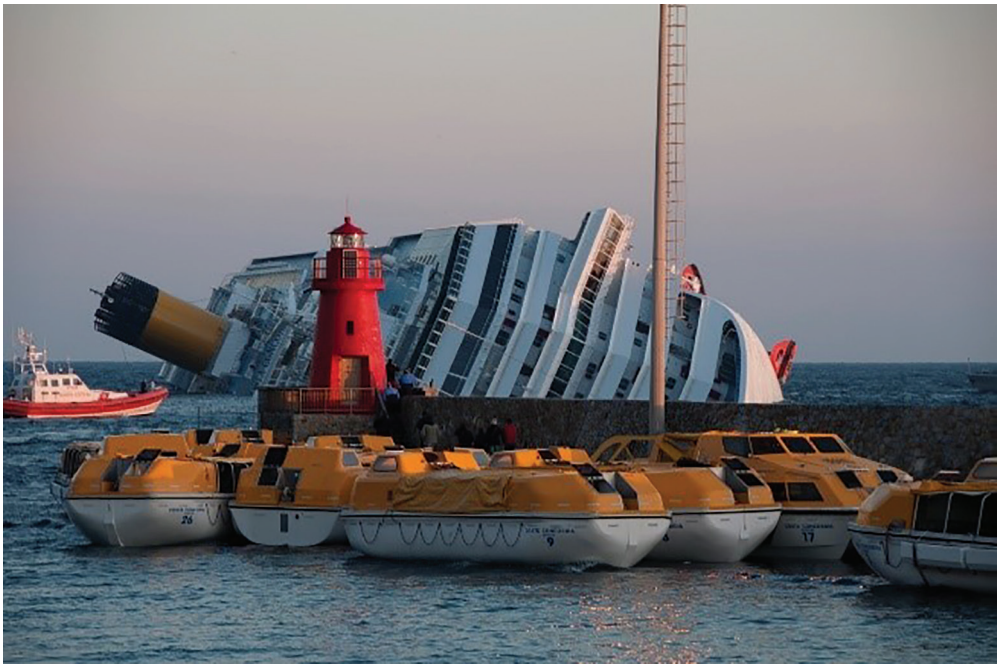

Figure 1.1 Costa Concordia.

Figure 1.2 Costa Concordia.

3. **Risk and risk management.** Risk can be defined in many ways, though the crucial components of defining risk are the frequency or probability of occurrence and the consequences of occurrence. In other words, we can describe risk as a combination of the probability of an accident occurring and the severity of the accident should it occur. Importantly, risk is an increasing value. This means the greater the probability or severity of the accident, the greater the risk. In terms of system-related risk, we refer to the combination of the risks associated with the accidents that the system can cause. Again, the risk is an increasing value. Finally, it is sometimes useful to discuss the risk of a hazard. This is defined as the combination of the probability of the hazard occurring, the probability of accidents resulting from the hazard, and the severity of those accidents. As we said previously, it is almost impossible for organisations to remove all hazards and risks from their systems and processes, irrespective of their severity or probability. For this reason, we turn to another concept called "tolerable risk" or "acceptable risk". In this sense, where the risk cannot be removed entirely, it is reduced to a level that is acceptable within a given context. What this means is the probability and severity of a hazard is reduced to such a level that the likelihood and consequences are tolerable or acceptable. This is the key objective of risk management. Unfortunately, determining what level of risk is tolerable or acceptable is highly subjective and depends on many interfacing factors.
4. **Risk and safety.** Safety and risk are often interchangeable terms. For instance, if we reduce the risk of something, we make it safer. If we increase the risk of something, we make it less safe. Safety is, therefore, the absence of unacceptable risk.

When we talk about safe systems, we mean the risk associated with the system is acceptable. To put this into context, we can turn to *Heinrich's Triangle* (Figure 1.3). Heinrich's Triangle is a visual representation of the increasing level of risk associated with a given process – in this instance, flying an aircraft. At the bottom of the triangle, we can see there were 1,000 unreported unsafe acts. An unsafe act may be as simple as leaving a toolbox unlocked and unattended in the workshop. Above that, we can see there were ~300 hazardous conditions. A hazardous condition is a situation that could have caused an incident but did not. This might include an aircraft engineer taking a spanner from the unlocked toolbox and leaving it on top of an aircraft tug. Second from the top of the triangle, we can see there were ~30 incidents. An incident is the same as a near miss, or an event that could have caused injury or ill health. Using our example, the spanner may have been knocked off the tug and left lying on the runway. At the top of the triangle, there is one aircraft accident. Although the number of occurrences has reduced as we move up the triangle, the severity and consequences of the hazards have increased quite dramatically. It is entirely feasible for the spanner that was left lying on the runway to get sucked up into an aircraft's engine causing it to crash. What seemed like an innocuous failure in safety protocol (i.e., not locking the toolbox) has resulted in a potentially devastating accident.

5. **Cause and consequence.** A cause is a potential event that may precipitate the occurrence of a hazard. Each cause has a probability attached to it. If we consider a fire, all fires need four elements: oxygen, heat, fuel, and a chain reaction. This is commonly referred to as the fire tetrahedron. If a piece of electrical equipment malfunctions, causing a spark, this can ignite any flammable or combustible

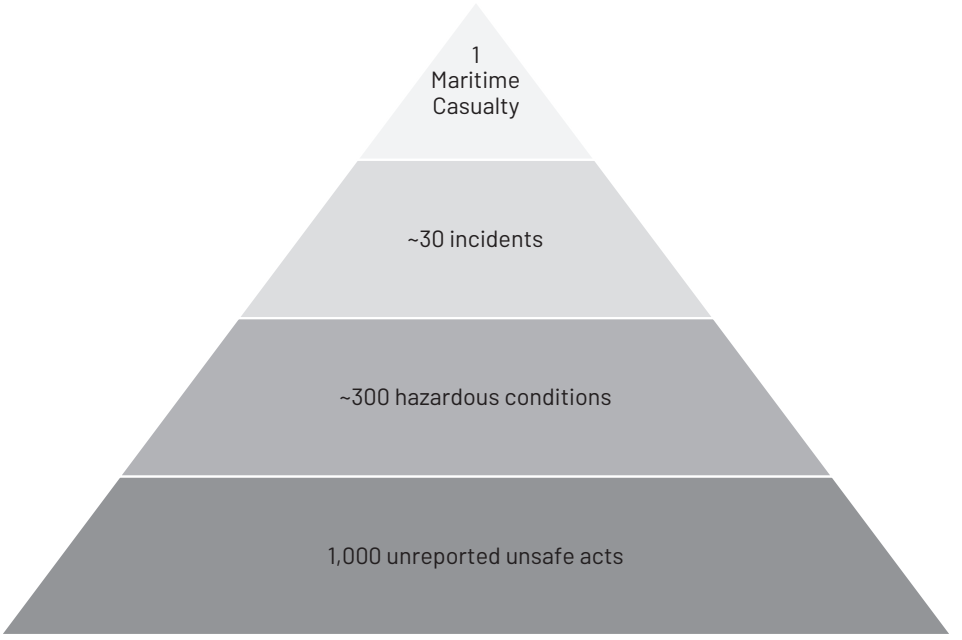

Figure 1.3 Heinrich's triangle.

items around it causing an electrical fire. We know the direct cause of the fire is the spark, but what caused the spark in the first place? Obviously, the electrical equipment malfunctioned, but we need to know what the initial cause was that led to the spark. In this instance, we are returning to the discussion of hazards. One small hazard (the initial malfunction) caused a larger hazard (the spark), which caused a system-level hazard (the fire).

6. **Controls and mitigations.** We have now covered some of the core themes and concepts associated with organisational safety management, which leads us to the last two concepts we need to discuss: controls and mitigations. In essence, a control is a measure – be it physical or procedural – that will reduce either the probability of a cause or the probability that the cause will result in a hazard occurring. For example, by double skinning fuel pipes, we can reduce the probability that the fuel pipe will leak, or double hulling a ship, we can reduce the probability of the ship sinking if one of the two hulls is pierced. Mitigation is a form of control that limits the effects once a hazard has occurred. For example, a fire extinguisher will not prevent a fire from happening, but it will help prevent the spread of the fire when used. Alternatively, wearing a seatbelt will not stop a person from having a car accident, but it will help limit the extent of their injuries.

SWISS CHEESE MODEL

The Swiss cheese model (Figure 1.4) is an organisational model developed by Professor James Reason and Dante Orlandella at the University of Manchester, England.

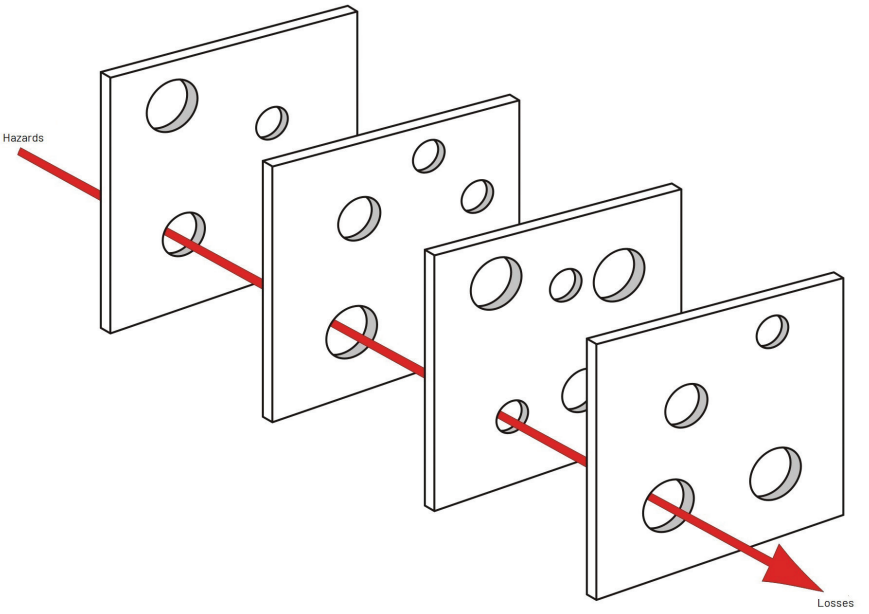

Figure 1.4 Swiss cheese model.

The model is used to analyse the causes of systematic failures or accidents. It is commonly used in the fields of aviation, engineering, and healthcare. The model describes accident causation as a series of events, which must occur in a specific order and manner for the accident to happen. This is analogous to a series of unique slices of Swiss cheese all lined up in order. Each hole in each slice of cheese represents an opportunity for a failure to happen, and each slice represents one level in the system. A hole may allow a problem to pass through one layer, but in the next slice the holes are positioned differently. This provides an opportunity to prevent the problem from passing through to the next layer. If, however, more than one slice is aligned, then the problem can freely pass from one layer of the system to the next.

SUMMARY

In this chapter, we have been introduced to some of the basic concepts and terms used in organisational safety management. To recap on what we have covered so far:

- Safe is the absence of unacceptable risk, though we must appreciate there is an element of risk in everything we do.
- Hazards, incidents, and accidents are different things.
- A hazard must have the potential to result in an accident.
- A cause must have the potential to contribute to a hazard.
- A control must have a limiting effect on the risk, hazard, incident, or accident.
- Hazards are central to system safety.
- System boundary is an important element in defining hazards and mitigating risks.
- It is useful to distinguish between system-level hazards and causes.
- Risk is a combination of the likelihood and consequences of a hazard turning into an accident.

In Chapter 2, we will turn out attention to the importance of risk in organisational safety management.

Chapter 2

Importance of risk in organisational safety management

For most people, the idea of risk is an abstract concept. As individuals we generally know what we are prepared to do, and how far we are prepared to go, to achieve our personal aims and objectives. As humans, we are quite good at recognising our own limitations. For organisations, however, recognising risk is an entirely different proposition. The way we view a risk to ourselves is very different to how we perceive risks to our organisations. In this chapter, we will begin by reminding ourselves what a risk is and how the risks are defined at an organisational level. We will also briefly examine the historical and legal background to risk management, the perception of risk tolerability, public perceptions of risk, and the dangers of failing to take risks seriously. It is also worth reminding ourselves that when we refer to an organisation, we may refer to the company as a whole or a single operational component such as a single ship in the fleet. There are many different definitions of the word "risk", but they all tend to involve at least one of the following two components:

1. The likelihood of something unpleasant happening.
2. Consequences of something happening.

For our purposes, we can safely assume risk consists of both components, although we need not be prescriptive in how each concept is defined, except to say that increasing likelihood or severer consequences imply a greater level of risk. In terms of applying this definition of risk to an accident, we can say risk is "a combination of the likelihood of the accident occurring, and the severity of the accident". In relation to the risk of a system, we can refer instead to "a combination of the risks associated with the accidents that the system can cause". To apply these definitions, we use what is called a "risk matrix". Given that it is not possible to eliminate risk entirely from organisational systems, the question arises as to what is a tolerable risk? One possible answer to this question is any risk is acceptable so long as the benefit is greater than the consequence of failure. In theory, this sounds perfectly reasonable. The consequence of failing to achieve the objective is off set by the potential benefit of achieving the objective, so long, of course, as the probability of failure is within a reasonable tolerance. As you might be starting to realise, this answer is not as simple or as straightforward as it initially seems. In practice, it is often far harder to rationalise the decisions we make about risk. If we consider the sinking of the *MS Herald of Free Enterprise* in 1987

DOI: 10.1201/9781003409977-3

Figure 2.1 MS Herald of Free Enterprise after salvage.

(Figure 2.1), for example, there was always an inherent risk that the ferry might sink. The probability of the ferry sinking was considered relatively low, but the consequences were devastatingly high. For the passengers on board the ferry, the consequences of the ship sinking were offset by the low probability. Unfortunately, in this instance, the *MS Herald of Free Enterprise* did sink (due to human error). And so, it falls to safety professionals and experts to try to determine what level of risk is tolerable, whilst always remaining cognisant of public perception and opinion.

There are very few hard rules regarding the tolerability of risk. There is also little official guidance although standards such as IEC 61508 and the UK Ministry of Defence (MOD) Safety Management Requirements for Defence Systems Part 1: Requirements (Def Stan 00-56) go some way to addressing this problem. Often, it is up to the operators, developers, and vendors of safety-related systems to make decisions, cast judgements, and devise protocols for determining the tolerability of risk, and in so doing, justifying those risks to sectorial regulators, the public, and when necessary, the law courts. To make matters more complicated, the tolerability of risk varies considerably across domestic, national, and international borders, between industries, and even within different sectors of the same industry. When determining the tolerability of risk, it is important to consider the following factors:

1. The absolute upper limit. Often, there is an absolute upper limit to the tolerability of risk. This, however, only tells us that risks are intolerable at and above this limit. It does not tell us what is tolerable or acceptable beneath this limit.
2. A comparison of new risks against existing risks. Sometimes, new risks may be considered tolerable if it can be shown not to significantly increase the overall risk or is deemed to be at or lower than the risk to be replaced.

Table 2.1 Example risk matrix

	Consequence			
Frequency	*Catastrophic*	*Critical*	*Marginal*	*Negligible*
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV

3. The degree of control that casualties or victims have over the risk.
4. The benefits to be accrued in accepting the risk.
5. The practicality or cost associated with reducing the risk.

This last factor – the practicality or cost associated with reducing the risk – raises an interesting question, which is: how much is worth paying to save a single human life? It is an unpleasant question, and surely anyone should be forgiven for saying the only answer is "whatever it takes". Unfortunately, however, it is almost impossible to eliminate risk completely. Every human activity involves and requires some element of risk, whether it be flying in an aeroplane, crossing the road, or standing on a ladder. In our everyday lives, we trade the benefits of the risk against the probability and consequences of the risk. For some industries, such as the maritime industry, the risks are inherently high, but it would be impractically expensive to reduce every risk associated with shipping to a level that is below our every average day. Therefore, to make a judgement about the practicality of reducing risks, it is often necessary to place a value on human life or at least on the practicality of saving a human life. Such costs should be constantly reviewed in accordance with public perception and changes to the legal framework. By current standards in the UK, the typical minimum value placed on a single human life is GBP 1.8 million (USD 2,174,202; Euros 2,088,558) (November 2022). This excludes any additional compensation for injuries such as loss of sight or limbs and loss of earnings. Determining tolerability of risk is a complex and emotive issue and is never easy. Fortunately, there is a method that can be used to visualise the consequences of a risk against the probability or frequency of the risk turning into an accident. This method is the risk matrix, which uses a table (shown in Table 2.1) consisting of five levels of risk. The highest level of risk (I) is categorised as catastrophic and frequent, whereas the lowest category of risk (IV) is improbable with negligible consequences. As we can clearly see from the matrix, the level of risk is the delta between the likelihood of the risk occurring and the related consequence.

In the next section of this chapter, we will look at perceptions of risk from an organisational perspective.

PERCEPTIONS OF RISK

It is critical for organisations to never underestimate the importance and influence of public perception to risk. Today, the public are more conscious of risk than at any time in history. Social media and 24-hour news broadcasting have made people increasingly aware of the world around them and of the risks and hazards they face every

day. Unfortunately, media influence has also led people to react in less rational ways. It is often argued that collectively we are getting worse at dealing with risk, and we are spending too much time and resources wrapping ourselves up in "cotton-wool" to protect ourselves against trivial risks whilst simultaneously ignoring the larger risks. In truth, dealing with risk with any level of confidence is impossible as each new technology that evolves creates new risks. For example, although vehicle safety standards have improved in leaps and bounds over the past few decades, meaning modern vehicles are lighter and larger than ever before, this has led in part to the introduction of ancillary technologies such as satellite navigation systems, integrated media systems, and so forth. Despite modern vehicles being more structurally protected from the *effects* of accidents, the growth of in vehicle technology has increased the *probability* of accidents as drivers are more easily distracted. From the public's perspective, the convenience of having integrated vehicle technology, combined with the improvement of vehicle safety, outweighs the consequences of being involved in a potentially lethal accident.

In essence, there are many factors that influence the public's perception of risk, and ultimately, their willingness to accept risk. This means people are more likely to accept risks where they

- Understand the technologies and dangers involved.
- Recognise the dangers are distributed equitably between individuals.
- Recognise individuals voluntarily take on risk.
- Believe they can control their exposure to risk.
- The consequences of any accident are immediate.

Now we have considered risk from an organisational and individual perspective, we can consider the law's point of view towards managing risk. As you might expect, the legal framework around risk management is quite complex. To summarise it, there are four key considerations that organisations must factor in relation to managing risk from a legal perspective: ethical considerations, societal considerations, commercial considerations, and legal considerations.

1. **Ethical considerations.** In the UK, employers have a duty of care towards their workforce. In return, workers are expected to take a commercial interest in the wellbeing of the organisation. This means working in a safe and considerate manner with due regard to health and safety, the provision and use of personal protective equipment, and protecting the organisation – insofar as is reasonably possible – from accidents occurring.
2. **Societal considerations.** Organisations have a legal duty to limit the impact of their operations, as well as their products and services, on society. This means being considerate to local communities and the environment (e.g., by not discharging waste at sea).
3. **Commercial considerations.** Organisations have a legal responsibility to limit their exposure to the possibility of financial loss due to failure of their products and services, decreasing value of their reputation and marques, and exposure to litigation from customers, regulators, and other third parties.
4. **Legal considerations.** Lastly, organisations have legal responsibilities such as the health, safety, and welfare of their employees, customers, and members of the public.

Figure 2.2 Piper Alpha disaster.

There is a plethora of laws, regulations, statutory instruments, and guidelines relating to the organisational management of risk. Together, these form the legal framework, which governs the ways organisations plan, mitigate, manage, and respond to risks. In the UK, the number one piece of legislation that all safety professionals must be cognisant of is the Health and Safety at Work etc. Act, 1974 (HASAWA). The HASAWA was passed by Parliament into law in 1974 following the publication of the Robens Report in 1972, which recommended the formation of the Health and Safety Commission (formed in 1974 and dissolved in 2008), and the Health and Safety Executive (formed in 1975). The HASAWA places a general duty on all employers to safeguard the health and safety of their workers whilst in their employ, and sometimes even after their employment has ended. The HASAWA also places a legal duty on people who are not employees of the organisation, such as contractors, customers, and members of the public visiting the premises of the organisation; it places duties on the design, manufacture, import, and export, and supply of articles and materials relating to the business of the organisation. The HASAWA also places a legal duty on the workers and employees themselves. These duties may be absolute, practicable, or reasonably practicable. Up until the mid-1980s, health and safety regulation was largely prescriptive. This meant that the regulations themselves determined what was and what was not considered safe from a health and safety perspective. In 1987, following the *Piper Alpha* disaster (Figure 2.2), a new approach to health and safety was implemented in the UK following the publishing of the Cullen Report. Lord William Cullen was tasked by the government to chair the official Public Inquiry into the *Piper Alpha* disaster, which involved a fire on a North Sea oil rig some 120 miles (190 km) north-east of Aberdeen, Scotland. The incident claimed the lives of 167 men, with 30 declared missing, and over GBP 1.7 billion in property and environmental damage. The ensuing Cullen Report, which ended the official enquiry in 1990, was published in two parts: the first part concerned the causes of the *Piper Alpha* disaster, and the second part made recommendations for fundamental changes to the UK's health and safety regime.

SUMMARY

In the second part of this chapter, we have been introduced to the concept of risk, why organisations care about risk, and the legal framework around risk management. In summary, organisations have a legal duty to protect their workers, customers, and the public from any hazards and risks arising from the organisation's operations and products. These duties are broadly defined as ethical, societal,

commercial, and legal. Identifying risks and determining what is a tolerable risk is a difficult and sensitive, but necessary undertaking for safety professionals. In the next chapter, we will turn our attention towards the product life cycle and the safety life cycle and how these interact and influence an organisation's approach to safety management.

Chapter 3

Safety planning

To be able to investigate maritime accidents and incidents, we must first have a thorough understanding of why accidents and incidents occur in the first place. We know from the previous two chapters that safety is a legal obligation that is placed on every organisation. An accident or incident is the consequence of failing to comply with that legal duty. To ensure failures like this do not happen, organisations are required to carry out detailed safety planning in relation to their scope of operations. The planning of safety-related activities that should be carried out during the development of safety-related systems is a critical activity. Yet, frequently, insufficient effort and resources are spent on ensuring robust safety plans are developed, followed, and where appropriate, modified in accordance with emerging organisational needs. The safety plan should provide an initial indication of how the safety of the system is to be assured, what safety target(s) have been identified, how they will be met, and provide an outline of the strategy to be employed through which safety system objectives will be achieved and demonstrated. Like the term organisation, when we refer to the system, we may refer to an individual component (such as radar), a microsystem such as a navigational watch or cargo loading operation, or a macrosystem, such as bridge or engine room operations or even the whole vessel. The first step in safety planning is to carry out a preliminary hazard analysis. This is a process of identifying and qualifying potential hazards within the system.

PRELIMINARY HAZARD ANALYSIS

Preliminary hazard analysis combines two key activities: initial hazard identification and initial risk assessment. The objective of the preliminary hazard analysis is to determine the safety targets for the system and the extent of risk reduction required to be implemented by the system. It is a process that is widely used to determine all requirements (i.e., safety functions and safety integrity levels). We start by dividing the hazards, accidents, and the acceptable level of risk associated with each. We then identify the measures (safety requirements) to mitigate the risks that were identified. This process requires a significant volume of work to be carried out to be effective and should never be seen or treated merely as a "bolt on" activity. To carry out preliminary hazard analysis effectively, there are five key stages, which are outlined below:

DOI: 10.1201/9781003409977-4

1. **Requirements specification.** Although an integral stage in the system life cycle, IEC 61508 considers requirements specification to be a standalone activity, which falls outside the scope of the safety life cycle.
2. **Design.** At the design stage, it is important to begin to allocate safety functions. This means, for example, signposting safety functions in hardware or software.
3. **Systems hazard analysis.** At this point in the safety life cycle, we are effectively carrying out a risk assessment, but in greater and deeper detail. As we now know the design and function of the system, we can begin to estimate how the system might fail and how likely these failures are to occur. We use the same techniques as the preliminary hazard analysis, but remember the objectives are different. Here, we want to confirm that the design meets the target level or risk.
4. **Safety validation.** For safety validation, we carry out extra testing to confirm the safety requirements of the system have been met. As we may not be able to achieve a desirable level of certainty, it may be necessary to perform additional analysis and systems modelling.
5. **Safety case report.** The safety case report is the document that summarises and pulls together all the safety activities undertaken as part of the safety life cycle. It is used to convince Regulatory Authorities that the system is safe for operation.

VERIFICATION AND VALIDATION

Verification and validation are a combined process, which crosses both safety and conventional development activities, and it is critical that verification and validation activities are carried out for safety-related systems. Despite its importance, there is often confusion around what verification and validation entails – even amongst published standards and guidelines. To provide some clarity on this issue, we may refer to IEC 61508, which provides the following guidance:

1. **Verification.** IEC 61508 defines verification as a top-down and bottom-up "V" process at each stage, where processes and procedures are appropriate and adhered to, by competent personnel, at each stage in the system development, and each safety specification complies with previous safety specifications, and there is justification for the adequacy of the tools, methods, and techniques used throughout the system life cycle.
2. **Validation.** IEC 61508 defines validation as crossing the "V", which involves simulation, analysis, testing, commissioning, product testing, and integration testing, that implements the requirements, whereby verification and validation overlaps both the safety and development life cycles. It is important to define the strategy for achieving safety and to ensure that the verification and validation activities are sufficient to satisfy that strategy as well as demonstrate that the requirements (functional, safety, performance, and non-functional requirements) have been implemented.

SAFETY PLANNING

Commonly used safety standards such as Def Stan 00-56 and IEC 61058 propose similar overall approaches to demonstrating safety. At the core of the process is the hazard

analysis and risk assessment. Once these have been developed, appropriate measures can be incorporated into the system design. The design should be appropriately controlled, with adequate verification and validation carried out. All phases of the system life cycle should be addressed from initial concept to end-of-life (EOL).[1] In this chapter, we will concentrate on the requirements for the plans for the management of functional safety, but also touch on the remaining aspects of planning. This will focus on the system life cycle proposed in IEC 61508. There are three parts to IEC 61508: (1) System Safety Standard (IEC 61508 Part 1), (2) Hardware Safety Standard (IEC 61508 Part 2), and (3) Software Safety Standard (IEC 61508 Part 3). Safety planning is an important process as it

- Helps to define safety objectives and targets.
- Helps define the activities needed for achieving safety (i.e., for each phase of the life cycle).
- Helps develop an understanding of the main difficulties associated with achieving the objectives.
- Helps develop a plan for overcoming the difficulties associated with achieving the objectives.

Often, regulatory bodies expect to see evidence of appropriate safety planning and the development of strategies for providing safety assurance. This evidence is typically compiled in a safety plan. Central to the safety plan is the safety case, which consists of three arguments: risk-based, confidence-based, and compliance-based arguments (see Table 3.1).

There are several activities covered by the safety plan. These activities fall into three broad categories:

- **Management.** These cover the safety organisation, responsibilities, and personnel.
- **Technical.** These cover safety activities and the safety life cycle.
- **Control.** This covers the control of safety information and checking compliance and adherence to the safety plan.

Table 3.1 Summary of safety case composition

Risk-based argument	*Confidence argument*	*Compliance argument*
Results of: • Hazards analysis • Trials and testing • Loss modelling • Probability calculations	How do you do: • Hazards analysis • Trials and testing • Loss modelling • Probability calculations • Meet standards • SQEP • Manage risk • Through life maintenance	Compliance with: • Appropriate standards and regulations • Approved processes

SQEP: Suitably qualified and experienced personnel

[1] By system life cycle, we are referring to the start and end of the system process. For watchkeeping, this will begin at the point the Officer/Engineer of the Watch (OOW/EOW) enters the bridge and will end when the OOW/EOW signs off the ship's log at the end of their watch.

Management activities include deriving safety policy and safety strategy and ensuring that all parties involved in the system development process are aware of this policy and strategy. Further management activities include determining the competencies required for carrying out each task and allocating appropriate personnel to be responsible for each activity. Technical activities cover all safety-related activities within the scope of the safety life cycle. For each activity, the objective, inputs, and outputs should be clearly defined. Standards vary in their approach to documentation requirements. Some standards specify the individual documents to be produced, whereas others (including IEC 61508) describe the material which should be documented without specifying how the material should be presented. Effective safety planning should cover both items, in the sense that the main safety documents to be produced should be described, along with some indication of the document's contents. In some cases, additional safety procedures for the control of the project may need to be further defined. For instance, procedures for managing a hazard log and for controlling the treatment of hazardous or potentially hazardous incidents will be needed in the event they do not already exist.

ALLOCATION OF RESOURCES

The safety life cycle can be thought of as covering three distinct phases:

- **Phase 1: Definition.** Phase 1 covered the stages from concept to safety requirements allocation.
- **Phase 2: Design and development.** Phase 2 covers the stages from overall operation and maintenance planning to demonstration of risk level acceptability.
- **Phase 3: Operation, maintenance, and EOL.** Phase 3 covers the stages from installation and commissioning to EOL.

Typically, responsibility for safety will involve different parties at each of the different phases. The end user of the system will need to be involved during all three phases. If significant elements of the system design and development are to be subcontracted, then the subcontractors will need to be made aware of the responsibilities they are required to fulfil. Involvement of a separate maintainer in Phase 3 (a common occurrence) will produce a similar need for responsibility awareness with a separate organisation. Usually, this situation will lead to the generation of several safety plans. Each organisation will need a plan defining how its individual safety activities will be fulfilled. Taken as a whole, the safety plans should cover all activities and describe how separate organisations will interact to ensure that the safety responsibility is not falling in between organisational gaps.

SAFETY PLAN

When preparing the safety plan, a summary should be produced to include a detailed commentary on the methods and techniques to be adopted throughout the system development life cycle, including an evaluation of qualitative versus quantitative methods. It should also cover any relevant competency criteria, the standards to be followed, and

Table 3.2 Detailed safety plan structure

• Introduction	• Safety criteria
• Aim	• Tolerability criteria
• History of the system	• Safety requirements
• Description of the system	• Applicable standards
• Plan scope and objectives	• Standards and procedures
• Environment	• Technical plan
• System safety organisation	• Initial safety meeting
• Organisational structure	• Corporate safety culture
• Safety team objectives	• Change management
• Safety team responsibilities	• Management of trials
• Project safety team	• Incident reporting
• Engineer	• Hazard identification
• Membership	• Hazard tracking system overview
• Meetings	• Risk estimation and sentencing
• Audit plan	• Risk reduction process
• Audit process	• Verification of risk reduction
• Review process	• Safety case strategy
• Recordkeeping	• Safety assessment strategy

an indication of any risk classification scheme to be adopted (together with a definition of acceptable level of risk). Once the summary has been produced and signed off, the safety plan can be developed. As we have already seen, different standards set out what they consider appropriate in terms of document contents and style. To provide some context, we will use the example provided by the UK Rail Safety and Standards Board (RSSB) Engineering Safety Management (the Yellow Book). The Yellow Book proposes the following structure:

- Safety Management Activities.
- Safety Controls.
- Safety Documentation.
- Safety Engineering.
- Validation and Verification of External Items.

A detailed list of the safety plan contents may include any or all the following items (Table 3.2):

To be effective, it is critical that design and safety professionals are engaged and involved from the start of the process, through each phase and stage, right up to EOL.

SUMMARY

In this chapter, we have been introduced to the system development life cycle and the safety life cycle. We have seen the extraordinary amount of work that is needed to produce a well-thought-out safety plan. We have also begun to recognise the importance of engaging stakeholders from the beginning, and right up to the end of the system or product lifespan. In the next chapter, we will turn our attention towards preliminary hazard analysis.

Chapter 4

Preliminary hazard identification and analysis

In the previous chapter, we started to examine the role and function of preliminary hazard analysis and the process of developing the safety plan. In this chapter, we will take that examination further by looking more closely at preliminary hazard identification and analysis as a function of safety planning. To begin with, we will start by looking at preliminary hazard identification.

PRELIMINARY HAZARD IDENTIFICATION

Preliminary hazard identification and analysis, often shortened to preliminary hazard analysis, is a critical activity that is carried out early in the system life cycle. It usually takes place before any detailed design or system development begins. There are three primary objectives for preliminary hazard identification:

1. The identification of accidents and hazards associated with the system.
2. Analysis (often quantitative) of the ways in which accidents may develop from hazards.
3. Determination of system safety requirements (safety functions and associated SIL).

The word *preliminary* is important in this context as it not only denotes the usual place of preliminary hazard analysis within a system safety lifecycle, but also acts as an indication that the results of the analysis are often incomplete or approximate, and therefore subject to later refinement. For instance, preliminary hazard analysis tends to only identify a subset of system hazards, more of which will become apparent as the system life cycle develops. Preliminary hazard analysis can be split into two activities: (1) hazard and accident identification (objective 1 above) and (2) hazard and accident analysis (objective 2 above). That said, there is usually a large degree of overlap in the techniques used for carrying out the two activities. This means it is not uncommon for both activities to be performed simultaneously. For our purposes, however, we will examine both activities separately. The objective of the preliminary hazard and accident identification activity ("preliminary hazard identification") is to consider

DOI: 10.1201/9781003409977-5