Queen Mary
University of London

A Bayesian Network Approach for Product Safety Risk Management

Submitted in partial fulfilment of the requirements of the

Degree of Doctor of Philosophy

By

Joshua Levi Hunte

April 2023

Declaration

I, Joshua Levi Hunte, confirm that the research included within this thesis is my own work or that where it has been carried out in collaboration with, or supported by others, that this is duly acknowledged below and my contribution indicated. Previously published material is also acknowledged below.

I attest that I have exercised reasonable care to ensure that the work is original, and does not to the best of my knowledge break any UK law, infringe any third party's copyright or other Intellectual Property Right, or contain any confidential material.

I accept that the College has the right to use plagiarism detection software to check the electronic version of the thesis.

I confirm that this thesis has not been previously submitted for the award of a degree by this or any other university.

Joshua Levi Hunte
Date: 18th April 2023

Acknowledgements

I would like to express my sincere gratitude to God for guiding me throughout this research journey. Without His blessings and grace, I would not have been able to complete this thesis.

I would like to thank my partner Kaiser for her unwavering love, support and encouragement throughout this research journey. Her patience, understanding and sacrifice have made this thesis possible.

I would like to express my sincere gratitude to Professor Norman Fenton for his unwavering support, guidance, and mentorship throughout the course of this research. His invaluable feedback and comments have been instrumental in shaping this thesis and me as a researcher, and I will always be grateful to him.

I would also like to thank the other members of my thesis committee, Professor Martin Neil and Dr William Marsh, for their support, insightful comments, and suggestions during my thesis.

I would like to thank the UK Government Office for Product Safety and Standards (OPSS) for their assistance and support in various aspects of this research. Their support has been immensely helpful in achieving the objectives of this thesis.

I would also like to thank Dr Eric Maass, Dr Sarah Jenkins, Professor Magda Osman, Mr Bijan Elahi, Dr Christos Bechlivanidis and Dr Robert Lachlan, for their support, insightful comments, and suggestions during my thesis.

I would like to thank all the current and former researchers of the MInDS group, formerly the RIM group.

I would like to thank my family and friends for their support and encouragement during my thesis. Special thanks to my uncle Henry for his endless support, motivation and encouragement throughout this research journey.

Finally, I would like to dedicate this thesis to the memory of my beloved father, Philip. Although he is no longer with us, his unwavering support, encouragement and confidence have been instrumental to me throughout my life. His memory will continue to live on in my heart and in my work.

Abstract

A new method for safety risk management and assessment using Bayesian networks is proposed to resolve limitations of existing methods and to ensure that products and systems available on the market are acceptably safe for use. The method is applicable to a wide range of products and systems, ranging from consumer goods through to medical devices, and even complex systems such as aircraft.

While methods such as Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA) have been used quite effectively in safety assessment for certain classes of critical systems, they have several limitations which are addressed by the proposed Bayesian network (BN) method. In particular, the BN approach enables us to combine multiple sources of knowledge and data to provide quantified, auditable risk estimates at all stages of a product's life cycle, including especially when there are limited or no testing or operational safety data available. The BN approach also enables us to incorporate different perceptions of risk, including taking account of personal differences in the perceived benefits of the product under assessment.

The proposed BN approach provides a means for safety regulators, manufacturers, risk professionals, and even individuals to better assess safety and risk. It is powerful and flexible, can complement traditional safety and risk assessment methods, and is applicable to a far greater range of products and systems. The method can also be used to validate the results of traditional safety and risk assessment methods when relevant data become available. It is demonstrated and validated using case studies from consumer product safety risk assessment and medical device risk management.

Contents

Glossary of Abbreviations

AED	Automated External Defibrillator
AI	Artificial Intelligence
ASRM	Aviation System Risk Model
BN	Bayesian Network
BT	Bow-Tie Model
CPT	Conditional Probability Table
DAG	Directed Acyclic Graph
DFT	Dynamic Fault Tree
ET	Event Tree
ETA	Event Tree Analysis
EU	European Union
FAA	Federal Aviation Administration
FDA	Food and Drug Administration
FDD	Fault Detection Diagnosis
FMEA	Failure Mode and Effects Analysis
FT	Fault Tree
FTA	Fault Tree Analysis
IoT	Internet of Things
NASA	National Aeronautics and Space Administration
NPT	Node Probability Table
OOBN	Object-Oriented Bayesian Network
OPSS	The UK Government Office for Product Safety and Standards
ORR	Overall Residual Risk
PFD	Probability of Failure on Demand
PHA	Preliminary Hazard Analysis
RRP	Recommended Retail Price
SaMD	Software as a Medical Device
SPAD	Signal Passed at Danger
TTF	Time To Failure
WTP	Willingness To Pay

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Safety of Products and Systems

Every day we interact with many different products and systems to complete various tasks and activities. For instance, we use mobile phones for communication, washing machines for laundry, and airplanes for travelling for work or vacation. Despite the many benefits offered by products and systems, their use also poses a potential risk to our health and safety. For example, the devastating Grenfell Tower fire in the UK on 14 June 2017 was caused by a fridge freezer. In this disaster, 72 people died, and the UK public costs since the disaster have exceeded £500 million, including £221 million for rehousing survivors [1], [2]. Two Boeing 737 Max planes crashed due to flaws in the plane flight control system in 2018 and 2019, killing a total of 346 people [3]. Less well-known examples, but equally relevant to this thesis include the recall of more than 500,000 Whirlpool washing machines in the UK due to a fire risk in 2020 [4]. Since the consequences of risks associated with products and systems range from negligible injuries to fatal injuries or damage to property [2]–[6], it is mandatory that all of these kinds of products and systems are assessed to be acceptably safe before use.

To ensure our safety, manufacturers, safety and risk professionals and safety regulators (both national and independent bodies) perform safety risk management and assessment for products and systems at all stages of their life cycle, from concept to decommissioning and disposal. These assessments include identifying potential risks and associated injuries, their likelihoods and severities, and implementing appropriate risk control measures to reduce risk to acceptable levels. Hence, risk assessment is essential for informing safety and risk management decisions during production and post-production, ensuring that the products and systems we use or available on the market comply with safety standards (both mandatory and voluntary).

1.2 Risk Management for Product and System Safety

Many different standards and legislation address the safety and risk management of products and systems in different industries and jurisdictions [6]–[9]. For instance, ISO 14971 [7] is the main standard used for medical device risk management, and the

European Union (EU) Rapid Information System (RAPEX) Risk Assessment Guidelines [8] is the primary method or guidelines used to assess the safety and risk for a wide range of consumer products in the EU, including toys, household appliances and automobiles. In general, safety standards and legislation require that product manufacturers establish a method for risk management throughout the entire life cycle of the product (from concept to decommissioning and disposal). Risk management is the "systematic application of management policies, procedures and practices to the task of analysing, evaluating, controlling and monitoring risks" [10]. It is iterative and dynamic and should be tailored to the culture and needs of an organisation or industry. Figure 1 illustrates the generic risk management process provided by ISO 31000 [11], which is adapted and applied in many domains and industries, including product safety.

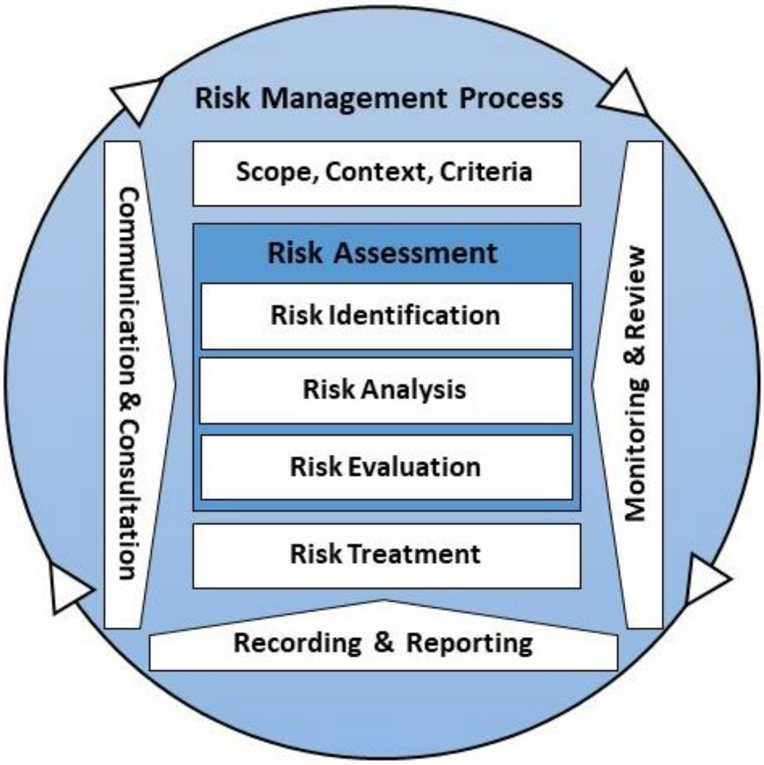


Figure 1 Risk Management Process

An essential part of the risk management process is risk assessment, which consists of three activities: risk identification, risk analysis, and risk evaluation. In product safety, risk identification involves identifying known and foreseeable hazards, hazardous situations, and related harms associated with the product or system. For example, given a domestic iron, a hazard is 'hot surface', a hazardous situation is 'user touches the hot surface', and the associated harm is 'burn'. Risk analysis involves estimating the risk associated with the hazard or hazardous situation. Risk is the combination of the probability of occurrence of harm P and the severity of that harm S, i.e., $Risk = P \times S$. The probability of occurrence of harm is the combination of the probability of a hazard or hazardous situation occurring P_1 and the probability that a hazard or hazardous situation causes harm P_2, i.e., $P = P_1 \times P_2$. For instance, given the domestic iron example, the risk depends on the probability of the burn and its severity. Finally, risk evaluation involves determining risk acceptability by comparing the estimated risk of the product or system with the criteria for risk acceptance. In situations where the risk is judged not acceptable, appropriate risk treatment or risk control measures are implemented to reduce risks to acceptable levels. Risk control measures for products and systems include inherently safe design and manufacture and information for safety.

1.3 Limitations of commonly used risk assessment and analysis techniques

There are many techniques and approaches used in the industry to assess and model the risks of products and systems, including the commonly used Failure Mode and Effects Analysis (FMEA) and static Fault Tree Analysis (FTA) (see Chapter 3). However, these traditional risk analysis techniques have the following limitations [6], [12]–[15], which can lead to inaccurate or ill-defined risk estimates when applied to products and systems:

1. ***Limited approach to handling uncertainty***: In situations where quantitative data are available for risk analysis, we find that most techniques and approaches use single-point values, e.g., 0.5, to describe the probability of events (hazards, failures, and hazardous situations) rather than probability distributions, e.g., Normal (0.5, 0.001). Hence, they cannot fully handle second-order uncertainty (i.e., the uncertainty in the probability values) during risk estimation. In addition, they are unable to provide a reasonable method for identifying and handling unidentified risks or hazards (i.e., unknown unknowns) for products and systems. Though Monte Carlo simulation (discussed in Chapter 3) may be used in conjunction with other risk analysis methods such as FTA [16] or as a standalone method to handle uncertainty, it is time-consuming and computationally expensive for complex systems.

2. ***Does not consider the causal nature of risk***: Many risk analysis techniques compute risk as the product of the probability of occurrence of harm P and the severity of the harm S, i.e., $Risk = P \times S$. However, this method of risk estimation does not consider the causal context in which the risk occurs. In the causal perspective, the risk depends on a set of events, including triggers (i.e., initiating events that cause the risk event), controls and mitigants (i.e., events that can stop the occurrence of the risk event or mitigate the consequence of the risk event) [13]. Moreover, since the assumptions that the risk is conditioned on may not be explicit or clearly defined, the values for P and S may be inaccurate and overly subjective. Finally, we find that 'risk register' approaches using the $P \times S$ metric, where P and S are measured on a scale of 1 to 5, where the resulting number represents the size of the risk, are generally insufficient for decision making.

3. ***Limited approach to computing risk for novel products with limited or no historical data*****:** Many risk analysis techniques are unable to provide reasonable risk estimates for novel products or products with limited or no available data since the probability of the occurrence of harm P may be unknown. Though the parts count technique (discussed in Chapter 3) may be used in conjunction with other methods or as a standalone method to estimate the risk of a novel system, it is time-consuming and expensive for complex systems. Furthermore, the parts count technique can give inaccurate results if the system is redundant [17].

4. ***Limited approach to handling multi-state variables***: Some risk analysis methods, such as FTA, can only support binary state variables (i.e., variables with only two states); hence they are not suitable for performing analysis for products and systems with multi-state variables (i.e., variables with three or more states).

5. ***Limited approach to handling sequence-dependent variables***: Some risk analysis methods, such as FMEA, cannot estimate the risk of products and systems where component failures and hazards are causally dependent. In these situations, extensions of FTA such as Dynamic Fault Tree and Beta

factors (discussed in Chapter 3) can be used in conjunction with other methods or as a standalone method to address this limitation, however these extensions require expert knowledge and are time-consuming and computationally expensive for complex systems.

6. ***Limited approach to updating risk estimates given new data (or evidence)***: For most risk analysis methods, revising the risk estimates for a product or system given new data (or evidence) entails repeating the risk analysis using the new data. For some methods, this approach to revising risk may be impractical since it is usually time-consuming and expensive.

7. ***Limited approach to combining subjective and objective evidence*****:** Most risk analysis methods cannot combine subjective (expert judgement) and objective evidence to estimate risk.

Although some extensions to the commonly used risk analysis methods, such as Dynamic Fault Trees (DFTs), have resolved some of these limitations, Bayesian networks (BNs) can resolve all of these limitations [13].

1.4 Research Hypotheses

Despite the many benefits of using BNs for safety risk management, such as handling uncertainty, their widespread acceptance and use as a standard systematic method for product safety risk management in industry may be restricted due to limited or no standard method or guidelines for building BNs for the many different product safety cases. For instance, some of the published BNs are presented with little information on how the BN was developed and why it is suitable for a specific application. In other cases, the BN development process may be ad hoc and presents little or no opportunity for repeatability and standardisation. Although there are some established automated, mapping, and knowledge representation methods [18]–[21] for defining BN structure and parameters, for many product safety cases, some of these methods may not be feasible due to adoption barriers e.g., lack of knowledge, and the complexity of the safety risk (i.e., it is dependent on the interaction between hard factors e.g., systems, and soft factors e.g., users). In these situations, the BN must be developed using expert knowledge and literature. However, the literature lacks a systematic, repeatable method or guidelines for developing BNs for product safety risk management using expert knowledge and literature. Therefore, the main objective of this thesis is to address this research gap. To achieve this objective, the following four hypotheses are argued in this thesis.

Hypothesis 1: It is possible to develop a generic method to build Bayesian networks for product safety risk management.

Hypothesis 2: It is possible to use Bayesian networks for safety risk management for many different types of products, including novel products or products with limited or no available data.

Hypothesis 3: It is possible to use Bayesian networks to model consumer risk perception and/or perform benefits-risk analysis for products.

Hypothesis 4: It is possible to deploy BNs for product safety risk management in production in a practical format for easy access and use by end users, including manufacturers, consumers and safety regulators.

Hypothesis 1 is explored by applying the idiom-based approach [19] for BN development to product safety risk management. The underlying concept of the idiom-based approach is that complex modelling problems can be broken down into smaller manageable chunks. This thesis presents novel idioms called *product safety idioms* which represent generic causal reasoning patterns that are common in product safety risk management. The aim of this work is to provide a standard, repeatable method or guidelines for developing BNs specifically for product safety risk management.

Hypotheses 2-4 are explored using two case studies. A case study on medical device risk management is used to investigate the application of BNs for managing the risk of medical devices. This case study provides a generic BN for medical device risk management that can assess the risk of many different types of medical devices during production and post-production, especially in situations where there is limited or no testing data available. The proposed BN also performs a benefit-risk analysis which is useful when the risk is judged not acceptable and additional risk control measures are not applicable. This case study is also used to demonstrate the deployment of BNs to end users using the Agena.ai cloud service. Therefore, this case study is a good example of how manufacturers can use BNs for product safety risk management in production.

The second case study on consumer product risk assessment is used to investigate the application of BNs for assessing the risk of consumer products as an alternative to the RAPEX risk assessment method [8] used by safety regulators in UK and EU. The proposed generic BN resolves the limitations of the RAPEX methodology and can assess the risk of many different types of consumer products, especially in situations where there is limited or no testing data available. The generic BN also models consumer risk perception and risk tolerability (acceptability). This case study includes empirical work examining the effect of risk communication on consumer risk perception done in collaboration with the UK Government Office for Product Safety and Standards (OPSS). Further collaboration was with the Royal Holloway University of London (RHUL). Since the proposed BN is tailored to the needs of safety regulators, this case study is a good example of how safety regulators can use BNs for product safety risk management in production. The case study results supported the development of the new product safety risk assessment method introduced by OPSS to replace the RAPEX methodology. It also informed and improved OPSS risk management decisions and strategies concerning non-compliant products by providing novel insights on consumer risk perception and how they are affected by risk communication.

The BNs presented in this thesis were developed using AgenaRisk Desktop and deployed in production using the Agena.ai cloud service [22].

1.5 Publications and Awards

The work in this thesis has led to the following list of publications and awards.

Publications

1. Hunte, J., Neil, M., & Fenton, N. E. (2021). A causal Bayesian network approach for consumer product safety and risk assessment: Research and Summary Report 2021/035. Office for Product Safety & Standards [23], https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1018546/bayesian-networks-research-summary-report.pdf

2. Hunte, J., Neil, M., & Fenton, N. E. (2022). A causal Bayesian network approach for consumer product safety and risk assessment [15]. Journal of Safety Research 80, pp 198-214, https://doi.org/10.1016/j.jsr.2021.12.003

3. Hunte, J., Neil, M., & Fenton, N. (2022). Product safety idioms: a method for building causal Bayesian networks for product safety and risk assessment [24]. arXiv preprint arXiv:2206.02144. https://arxiv.org/abs/2206.02144

4. Hunte, J., Neil, M., & Fenton, N. (2022). A hybrid Bayesian network for medical device risk assessment and management [25]. arXiv preprint arXiv:2209.03352. https://arxiv.org/abs/2209.03352, *Revision submitted to Reliability Engineering and System Safety Journal*

5. Hunte, J., Neil, M., Fenton, N. E., Osman, M., & Bechlivanidis, C., (2022). The effect of risk communication on consumers' risk perception, risk tolerance and utility of smart and non-smart home appliances, *Revision submitted to Safety Science Journal*

6. Hunte, J., Jenkins, S., Fenton, N. E. (2022). The effect of product compliance and credibility of the risk communicator on willingness to pay and risk perception of consumer products, *Research Report submitted to UK Government Office for Product Safety and Standards (OPSS)*

Other Related Publications

The terms, concepts, and principles presented in Chapter 2 contributed to the development of the UK Government Office for Product Safety and Standards (OPSS) risk lexicon [26].

Awards

The work presented in Publications 1, 2, 5, and 6 received funding from the UK Government Office for Product Safety and Standards (OPSS).

1.6 Thesis Structure

To investigate our hypotheses, this thesis is structured as follows.

Chapter 1 provides an overview of risk management for products and systems. It also summarises the limitations of commonly used risk assessment methods and defines the hypotheses examined in this thesis.

Chapter 2 provides the essential context required to understand the remainder of this thesis. We describe concepts, principles, and terms related to risk management, risk assessment, risk analysis and risk perception and their general application in the product safety industry. Since many risk management terms and concepts are application-specific (i.e., dependent on context, domain or industry), we define the risk management terms used in this thesis. The concepts and terms presented here were first presented in Publications 1-6.

Chapter 3 describes the commonly used risk analysis methods and techniques in the product safety industry. Risk analysis methods such as Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA) are reviewed.

Chapter 4 introduces Bayesian networks (BNs) and their underlying theory. This introduction is followed by a review of the approaches used to build BNs, and a review of the inferences and reasonings done using BNs. This background knowledge is necessary to understand the contributions made in the following chapters.

Chapter 5 provides a review of the BNs used in the safety domain. This background knowledge is necessary to understand the contributions made in Chapter 6 since none of the BNs reviewed provides a standard method for building BNs specifically for product safety risk management. However, each provides some insight into the use of BNs for the safety risk management of products and systems.

Chapter 6 presents a generic method for building BNs for product safety risk management. The proposed method is based on the idiom-based approach [19] for building BNs described in Chapter 4. This chapter supports Hypothesis 1 and was first presented in Publication 3.

The ideas explored in Chapter 6 are applied in Chapters 7 and 8, where two case studies are presented, which illustrate the new approach to building BNs for many different product safety cases.

Chapter 7 introduces the medical device risk management case study. This chapter describes the medical device risk management process as presented in ISO 14971:2019 [7] and its supporting documentation ISO/TR 24971:2020 [6]. We introduce a novel method for manufacturers to manage the risk of medical devices using hybrid BNs. The proposed hybrid BN resolves the limitations of traditional risk analysis methods discussed in Chapter 1 and provides a systematic method for medical device risk management, especially when there is little or no relevant testing or operational data available. It also performs a benefit-risk analysis of medical devices, which is useful for making risk management decisions such as product recall. The BN for medical device risk management was developed using the method proposed in Chapter 6. Therefore, this chapter supports Hypotheses 2 and 3 and was first presented in Publication 4.

Chapter 8 introduces the consumer product risk assessment case study. This chapter describes safety risk management for consumer products based on the RAPEX risk assessment guidelines [8]. We introduce a novel method for managing the risk of many different consumer products using hybrid BNs. The proposed BN for consumer product risk assessment developed using the method presented in Chapter 6 resolves the limitations of traditional risk assessment methods such as RAPEX and can provide reasonable risk estimates for products, especially when there is little or no relevant testing or operational data available. It also examines consumer risk perception of products and systems, useful for making risk management decisions such as product recall. This chapter supports Hypotheses 2 and 3 and was first presented in Publications 1 and 2.

Chapter 9 presents the results of empirical work that examines how risk perception of consumer products is affected by sources of risk communication. The principal merit of this work is to inform and validate the predictions of the consumer risk perception component of the BN presented in Chapter 8. This chapter supports Hypothesis 3 and was first presented in Publications 5 and 6.

Chapter 10 describes the process for deploying Bayesian networks in production. This is demonstrated by deploying the BN for medical device risk management (see Chapter 7) to end users as a web-based application using Agena.ai cloud service [22]. This chapter supports Hypothesis 4.

Chapter 11 revisits the research hypotheses of this thesis and summarises the related contributions. This chapter also discusses future directions of research.

Chapter 2 Risk Management Concepts and Terms

This chapter provides the essential context required to understand the remainder of the thesis. The concepts, principles, and terms relating to risk management, risk assessment, risk analysis, risk modelling, risk perception, safety management and their general application in the product safety industry are described. We defined the risk management terms and concepts used in this thesis since many risk management terms and concepts are application-specific (i.e., dependent on context, domain or industry). Most of the terms and concepts presented in this chapter have been presented as part of the following publications: Publication 1 [23], Publication 2 [15], Publication 3 [24], Publication 4 [25], Publication 5 and Publication 6.

2.1 Fundamental risk terms, concepts, and principles

In this section, we describe key risk concepts and terms used in this thesis.

2.1.1 Risk

In general, the term *risk* is often expressed in terms of a combination of the consequences of an event and the likelihood of occurrence of that event [27]. In this context, the consequences of an event will be something negative or an adverse effect. In product safety, risk is defined as “the combination of the probability of occurrence of harm (to the consumer) and the severity of that harm” [5], [7]. It is often expressed using the following equation:

Equation 1

$$Risk = P \times S$$

Where *P* refers to the probability of occurrence of harm and *S* refers to the severity of the harm.

Risk is estimated using subjective evidence (i.e., expert judgement), objective evidence (i.e., available quantitative data) or both subjective and objective evidence. Qualitative methods, such as matrices and quantitative methods, such as Fault Tree Analysis (FTA), discussed in Chapter 3, can be used to estimate risk. Hence, the magnitude or level of the risk can be expressed qualitatively using a ranked scale ranging from ‘low’ to ‘serious’ or quantitatively, such as ‘probability of injury per demand’ or in similar units considering the frequency of the risk event.

2.1.2 Causal Perspective of Risk

As mentioned in Section 1.3, traditional risk analysis techniques compute risk using Equation 1; however, this method of risk estimation does not consider the causal context in which risk occurs. In the causal perspective of risk, the *risk* is characterised by a causal chain of events, including the risk event itself, consequences (i.e., negative or adverse events caused by the risk event), triggers (i.e., events causing the risk event), controls (i.e., events that help avoid the risk event) and mitigating events (i.e., events that help avoid the negative consequence event) [13]. In the product safety context, we are interested in the causal view of risk since the level of risk for a product or system depends on a causal chain of events, including triggers, controls and mitigating events. An example of the causal view of risk applied in product safety is shown in Figure 2. Figure 2 shows a causal diagram that describes the sequence of events that leads to a patient being burnt by a defibrillator (in Chapter 4, probabilities are assigned to these events).

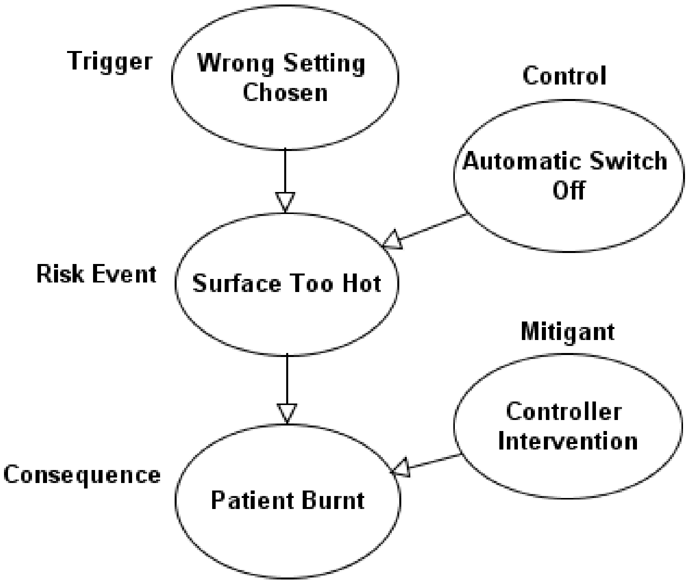


Figure 2 Causal view of risk in product safety – Defibrillator Example

The causal view of risk in product safety supports comprehensive and practical risk estimates since the uncertainty associated with the risk for a product or system is not a separate notion (as assumed in traditional risk analysis approaches). Every event associated with the risk has uncertainty expressed by the event’s probability distribution (this is covered in depth in Chapter 4). Also, since the risk problem is decomposed into a causal chain of events and the risk event is identified from a particular perspective, e.g., regulator, consumer or manufacturer, there is little ambiguity about the risk event, triggers, controls, mitigants and consequences. Therefore, factors affecting risk are easily identified and described. In Chapters 6, 7 and 8 we show how the causal perspective of risk is used to assess the risk of products and systems using Bayesian networks (BNs). The underlying theory of BNs is presented in Chapter 4.

2.2 Risk Assessment Terms and Concepts

In this section, we describe the key concepts and terms used for risk assessment and the intended use of these terms in this thesis.

2.2.1 Product and System

In this thesis, we use the terms *product* and *system* interchangeably. A *system* is defined as “a combination of interacting elements or components organised to achieve one or more stated purposes” [9]. Elements of a system include hardware, software, material, facilities, personnel, data and services. A *product* is “any artefact offered in a market to satisfy consumer needs”. Since the general definition of a system encompasses all products, then all products are systems, and a system can be described as a product or as the services it provides [24].

2.2.2 Defect, Fault and Failure

In this thesis, we define a *defect* as a generic term for a *fault*. We use the definitions for fault, error and failure associated with a system as defined by Laprie [28]. A *fault* “is a hypothesised cause of an *error*”. An *error* is “that part of the system state that can lead to subsequent failure”. A *failure* is an event that “occurs when the delivered service deviates from fulfilling the system function”. Please note that faults, errors and failures are recursive notions that depend on the perspective of the user or system [24]. For instance, given a system with an embedded software component, if the failure of the software does not result in system failure, it will be considered a fault from the overall system perspective. In Figure 3, we show the relationship between a fault, error and failure. According to Laprie [28], [29], the three main classes of faults that can affect a system leading to failure are *physical faults*, *design faults* and *interaction faults*.

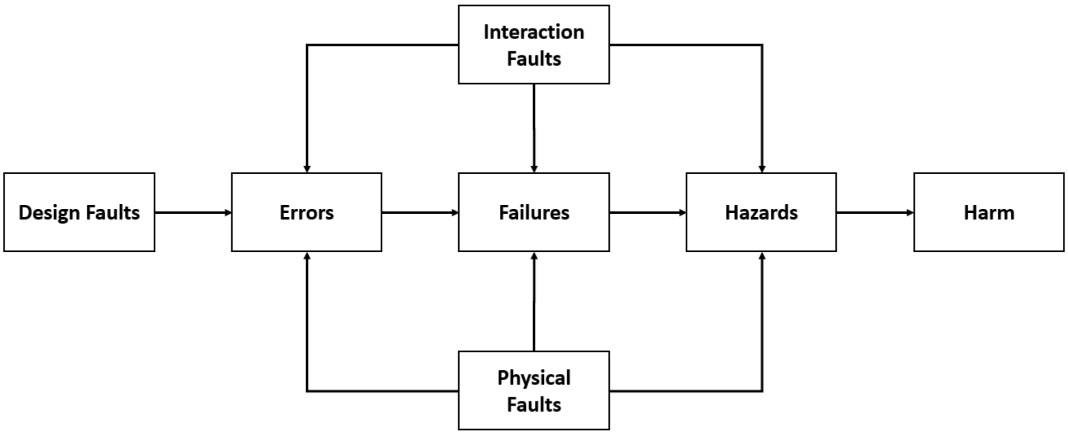


Figure 3 Relationship between system fault, error, failure and hazard

Physical faults are faults in the hardware of a system or faults that affect the hardware of a system [28], [29]. They are caused by physical deterioration of system hardware, interaction faults or physical interference by external events in the use environment. As illustrated in Figure 3, physical faults can cause an error, a failure in the absence of an error, and hazards in the absence of a failure.

Design faults are faults in the design of a system [28]. They are caused by interaction faults and development faults, e.g., errors in software code, incorrect or incomplete requirements. As illustrated in Figure 3, design faults can cause an error leading to failure and potential hazards.

Interaction faults are faults occurring during the use of a system [28], [29]. These are external faults since they are caused by elements in the use environment. For instance, most interaction faults are caused by some human action in the use environment, such as device misuse, and others are due to physical interference caused by external events in the use environment, e.g., weather conditions. As illustrated in Figure 3, interaction faults can cause an error, a failure in the absence of an error, and hazards in the absence of a failure.

2.2.3 Harm, Hazard and Hazardous Situation

In product safety, the term *harm* is defined as “injury or damage to the health of people or damage to the property or the environment” [7]. In some risk assessment methods, for example, RAPEX, the severity or level of the harm is usually defined using a four-point or five-point scale ranging from ‘negligible’ to ‘fatal’. The level of harm is dependent on factors such as the type of medical intervention required, or the economic costs associated with the harm. For instance, any harm resulting in injuries that cause minor discomfort is considered ‘negligible’, while harm resulting in death is considered ‘fatal’. As shown in Figure 3, harm is caused by a *hazard*.

A *hazard* is “a potential source of harm” [7], [8] usually caused by faults (i.e., physical, design and interaction) and failures (see Figure 3). According to the EU RAPEX guidelines, a *hazard* is “the intrinsic property of a product that may cause an injury to the consumer who uses the product”. In this thesis, both definitions of a hazard are considered when describing hazards associated with a system. A system can have one or more hazards that can cause harm. Where a system has several hazards, the risk associated with each hazard is assessed separately during the risk assessment. For instance, given a defibrillator with electrical and thermal hazards, the risk associated with each hazard is assessed to determine the overall risk of the product. Some risk assessment methods, such as RAPEX, usually chooses the highest level of risk estimated as the overall risk of the product [5].

Hazard identification is a key part of the risk management process, it entails identifying and documenting hazards associated with a system based on the intended use, foreseeable misuse and characteristics of the system. Any hazards for a system that are not identified during this phase would not be assessed, resulting in unknown harms and potential injuries to consumers. Risk analysis techniques such as Preliminary Hazard Analysis and Failure Mode and Effects Analysis (see Chapter 3) are used to identify hazards associated with a system. Other techniques for hazard identification include reviewing hazards reported in injury databases, publications, and scientific literature.

In this thesis, we used a combination of risk analysis methods, injury databases and scientific literature to identify hazards for our case study examples discussed in Chapters 7 and 8. Once the hazards of a system are identified, the *hazardous situation* is described. A *hazardous situation* is “any circumstance in which people, property or environment are exposed to one or more hazards” [7]. Hence a hazard can only cause harm if a hazardous situation occurs. Please note that some risk assessment and analysis methods may describe an *injury scenario* (i.e., steps leading to injuries) instead of a hazardous situation, given identified hazards. Therefore, in this thesis, we use the terms *injury scenario* and *hazardous situation* interchangeably.

2.2.4 Risk Criteria

This thesis also uses the term *risk criteria* when discussing risk management, especially risk evaluation. According to ISO Guide 73 [27], *risk criteria* are the "terms of reference against which significance of a risk is evaluated". It can include qualitative and quantitative requirements based on standards, policies and laws. The risk criteria are defined at the start of the risk management process and used during the risk evaluation phase to determine whether the risk is acceptable. In summary, the risk criteria determine whether the estimated risk for a system is acceptable or not and inform additional risk control measures.

2.2.5 Risk Control, Risk Treatment and Residual Risk

In this thesis, we use the terms *risk control* and *risk treatment* interchangeably. *Risk control* is any process, policy or action taken to reduce or eliminate a risk [27]. It can include removing the source of the risk and changing the likelihood of occurrence of harm. The risk remaining after risk treatment is called *residual risk.*

2.3 Risk Perception Terms and Concepts

In this section, we describe key terms and concepts for risk perception.

2.3.1 Risk Perception

According to ISO Guide 73 [27], *risk perception* is the "stakeholder's view on a risk". A *stakeholder* is "any person or organisation that can affect or be affected by a decision or activity". These include consumers, regulators and manufacturers.

In this thesis, we investigate consumer risk perception and how it is influenced by risk communication sources (see Chapter 9). We define *consumer risk perception* or *perceived risk* as consumers' subjective judgement of risk when purchasing or using a product or service [30], [31]. Previous research suggests that risk perception consists of two dimensions: *dread* and *unknown* [32]. *Dread risk* refers to the lay-person feelings about risks or hazards. It is defined in terms of the likelihood of consequence (harm) and its severity, lack of control and feelings of fear. *Unknown risk* refers to risks considered new, unobservable, unknown, and delayed in their manifestation and consequences.

2.3.2 Utility or Benefit

In this thesis, we use the terms *utility* and *benefit* interchangeably. *Utility* is the (perceived) *benefits* consumers receive from using a product. Since each consumer is unique, utility is personal and situational. For example, a consumer will assign utility to a product based on their personality, situation and experience [33]–[35]. In general, perceived benefit (or utility) has an inverse relationship with perceived risk [36]–[38]. For instance, Alhakami and Slovic [36] found that when people perceive an item as having high benefits, they perceive it as low risk (and vice versa).

2.3.3 Risk Tolerance (Acceptance)

In this thesis, we defined *risk tolerance (acceptance)* as the amount of (perceived) risk consumers are willing to accept or tolerate to obtain the benefits (value or utility) of a product [39]. It is influenced by individual characteristics, knowledge (or experience) of the product, risks, risk controls and benefits. For instance, some research suggests that risk tolerance is a personality trait [40]–[42]. For example, consumers with a high propensity to take risks are more tolerant of risks. On the other hand, other research suggests that risk tolerance is based on experience and knowledge [43]–[45]. For example, consumers that are more familiar with a particular product via experience or knowledge will be more tolerant of its risks.

2.3.4 Risk Communication

Risk communication is the exchange of information between different stakeholders about the risks associated with products [46]. The most common and familiar sources of risk communication are the government, manufacturers and the media [47]. Previous research shows that the risk communication source can affect risk perception. For example, if consumers perceive the risk communication source as reliable and trustworthy, e.g., the government, they will most likely adhere to the risk message. However, they may ignore or reject the risk message if they perceive the risk communication source as unreliable and untrustworthy, e.g., non-experts [48], [49].

These observations are essential when deciding on the best media for informing consumers about risk and will be covered in Chapter 9.

2.4 Chapter Summary

In this chapter, the concepts, terms and principles that underpin risk management and assessment in the product safety industry were defined. Definitions were provided for key terms that will be used throughout the thesis.

In the next chapter, we review the commonly used methods for risk analysis and assessment in the safety domain.

Chapter 3 Review of commonly used risk assessment and analysis techniques

This chapter describes commonly used techniques for risk analysis in the product safety domain. The following risk analysis techniques are discussed: Preliminary Hazard Analysis (PHA), Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Bow-tie models, Risk Matrices, Monte Carlo Simulation, Beta Factor Method and Parts Count Method. These techniques are complementary and can be used as required to facilitate a comprehensive risk analysis. This chapter is adapted from Publication 4 [19], previously published by Arxiv.org.

3.1 Preliminary Hazard Analysis

Preliminary Hazard Analysis (PHA) is an inductive analysis method that is performed early in the development of a product when there is little information about its design or operating procedures [6], [12]. It is used to identify hazards, hazardous situations and events that can cause harm for a product. Hazards and hazardous situations are identified by considering product characteristics such as the use environment and interfaces among system components. PHA is often done using brainstorming techniques and is a precursor to more elaborate risk analysis methods such as FTA. The PHA method includes the following steps:

1. Describe the product and scope of the analysis.
2. Identify applicable hazards and hazardous situations for the product.
3. Identify the probability of occurrence of harm *P*. Please note that since PHA is done early in the development process, there would be insufficient information about the product to estimate probabilities accurately. However, the reported injury information from previous similar products can be used to provide reasonable estimates for the probability of occurrence of harm *P*.
4. Identify the severity of the harm *S*.
5. Estimate the risk of the product, i.e., *P* × *S*, using a *risk matrix* (see Section 3.6).
6. Identify potential risk controls.

The results of a PHA may be presented in a tabular format, as shown in Table 1. A PHA is essential for informing risk management decisions such as risk controls.

Table 1 Example of preliminary hazard analysis for a defibrillator

Preliminary Hazard Analysis (PHA)							
Product: Defibrillator							
ID #	**Hazard**	**Harm**	**Potential Causes**	**Probability of harm (1-5)**	**Severity of harm (1-5)**	**Risk Score P × S**	**Risk controls**
1	Hot surface	The patient is burnt during use	Device malfunction	1	2	2	Automatic switch off

Several studies have used PHA to identify potential hazards and hazardous situations for systems [12], [50]–[53]. For instance, Zhang et al. [50] used a PHA to identify hazards and hazardous situations for an insulin infusion pump. Masci et al. [51] used a PHA to identify hazards for the number entry part of an infusion pump interface. Aloqaily [53] used it to identify hazards associated with pipelines. Elahi [12] used it to identify hazards and hazardous situations associated with medical devices.

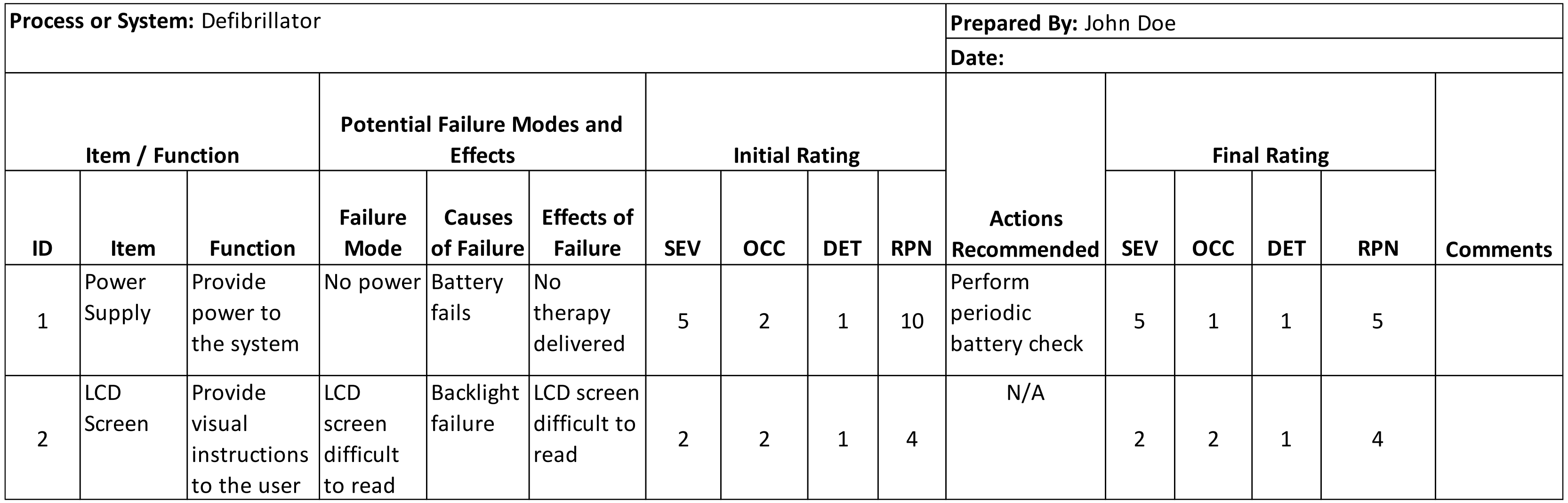
3.2 Failure Mode and Effects Analysis

Failure Mode and Effects Analysis (FMEA) is an inductive, bottom-up analysis method that explores the failure modes of a system and how each failure mode affects the system [54], [55]. The causes, consequences, risks, and risk controls for each failure mode are recorded in an FMEA worksheet. An example of an FMEA worksheet is shown in Figure 4. FMEA is useful for analysing systems containing many components, e.g., medical devices. However, since device components are analysed one at a time, FMEA is usually a time-consuming activity and is not suitable for analysing systems with common cause failures or systems with a high degree of redundancy. The FMEA method includes the following steps:

1. Describe the product and scope of the analysis.
2. Identify the failure modes of the system.
3. Identify the cause and effect of each failure mode.

4. For each failure mode, determine and assign ratings for the severity of the effect *S* (using a 5-point ranking scale ranging from negligible to fatal), the probability of occurrence *O* (using a 5-point ranking scale ranging from improbable to frequent), and the detectability *D* (using a 5-point ranking scale ranging from almost certain to undetectable).
5. For each failure mode, compute the Risk Priority Number (RPN) and estimate the risk. The RPN is the product of severity, occurrence and detection ratings, i.e., $S \times O \times D$, and it is used to determine the criticality ranking of the failure modes. Failure modes with a high RPN are the most critical for the system. The risk is computed using a *risk matrix* that combines severity and occurrence ratings (see Section 3.6).
6. Identify potential risk controls for each failure mode.

Additional information on performing an FMEA can be found in the standard IEC 60812:2018 [55]. Although several studies have used FMEA to assess failures of system components [12], [56]–[58], it can also be used to assess failures in the manufacturing process (process FMEA) and the use and misuse of a system (use FMEA). In the product safety domain, FMEA is used to identify failure modes of a system that can cause a hazard or hazardous situation. Since FMEA is usually performed during the design phase of a system, the results from the FMEA are useful for informing risk management decisions such as risk controls and providing the basis for further analysis methods such as FTA.



Process or System: Defibrillator										**Prepared By:** John Doe					
										Date:					
Item / Function			**Potential Failure Modes and Effects**			**Initial Rating**					**Final Rating**				
ID	**Item**	**Function**	**Failure Mode**	**Causes of Failure**	**Effects of Failure**	**SEV**	**OCC**	**DET**	**RPN**	**Actions Recommended**	**SEV**	**OCC**	**DET**	**RPN**	**Comments**
1	Power Supply	Provide power to the system	No power	Battery fails	No therapy delivered	5	2	1	10	Perform periodic battery check	5	1	1	5	
2	LCD Screen	Provide visual instructions to the user	LCD screen difficult to read	Backlight failure	LCD screen difficult to read	2	2	1	4	N/A	2	2	1	4	

Figure 4 Example of an FMEA worksheet

3.3 Fault Tree Analysis

A Fault Tree Analysis (FTA) is a deductive, top-down analysis method that is usually used in the safety domain to analyse hazards identified by other methods such as PHA [54], [59]. FTA starts with an assumed undesired consequence or event, e.g., harm, followed by the identification of its causes or contributing events. The assumed undesired event is called the *top event*, and the independent events contributing to the *top event* are called *basic events*. Hence, a *fault tree* (FT) can be described as a graphical representation of the (basic) events or contributing factors causing the top event. An example of a fault tree to determine the likelihood of an engine fire (adapted from [12]) is shown in Figure 5. In a fault tree (see Figure 5), the top event is connected to the basic events using logic gates such as OR and AND gates. The symbols for OR gates, AND gates, and top and basic events are shown in Figure 6. In this thesis, when discussing FTA, we are referring to static FTA unless specified otherwise.

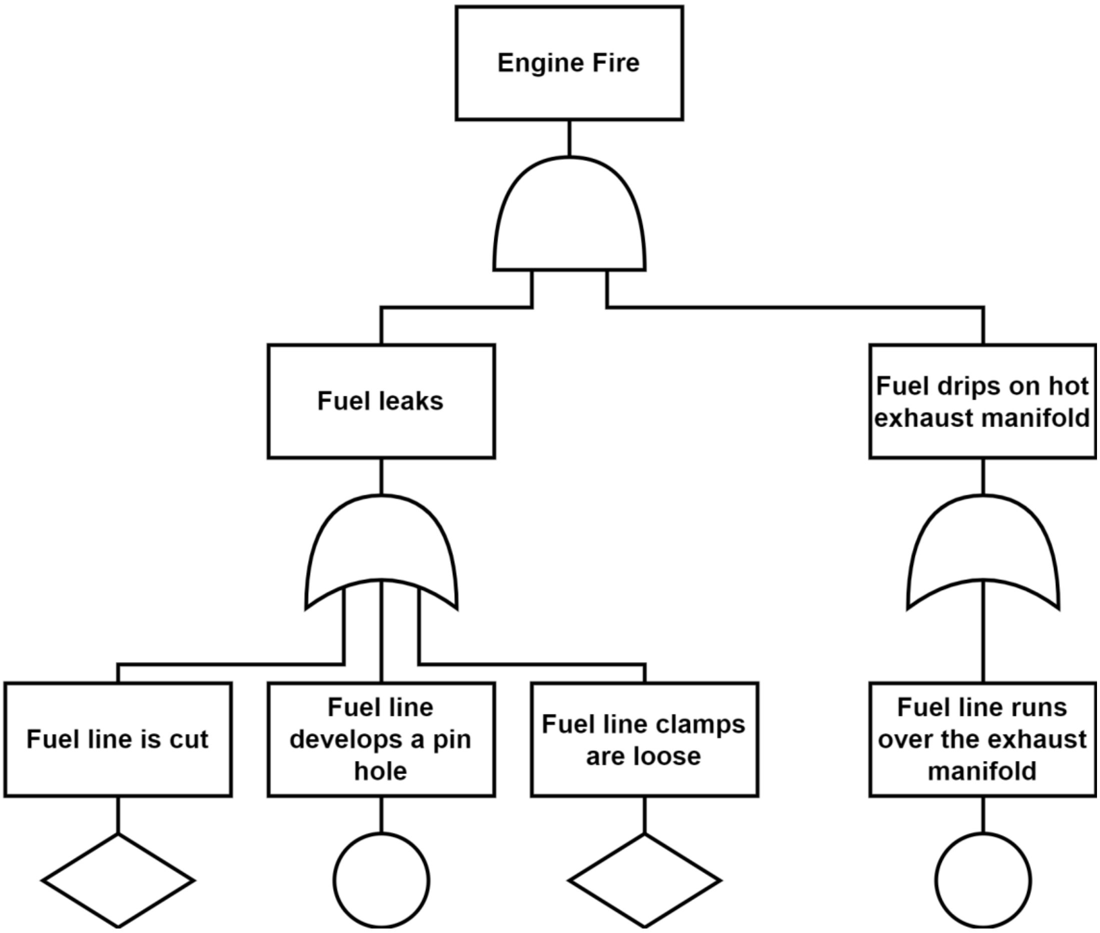
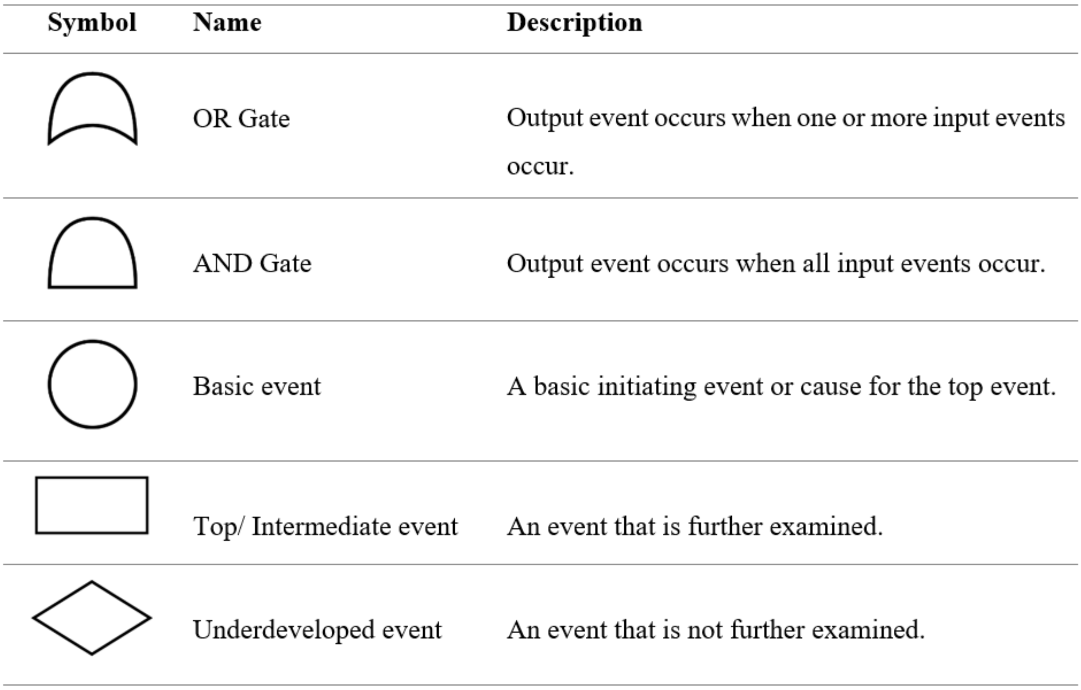

Engine Fire
Fuel leaks
Fuel drips on hot exhaust manifold
Fuel line is cut
Fuel line develops a pin hole
Fuel line clamps are loose
Fuel line runs over the exhaust manifold

Figure 5 Example of a fault tree for an engine fire



Symbol	Name	Description
	OR Gate	Output event occurs when one or more input events occur.
	AND Gate	Output event occurs when all input events occur.
○	Basic event	A basic initiating event or cause for the top event.
□	Top/ Intermediate event	An event that is further examined.
◇	Underdeveloped event	An event that is not further examined.

Figure 6 Common symbols used in a fault tree

FTA can be used to perform quantitative and qualitative analyses. Quantitative analysis is done when the probabilities of the basic events are known. These probabilities are combined using probability rules based on the structure of the FT to determine the probabilities of occurrence for the top event. In situations where the probabilities of the basic events are unknown, qualitative analysis is done using descriptive probabilities of occurrence such as ‘frequent’ or ‘remote’. The primary output of an FTA is the identification of the set of basic events that can cause the top event to occur, referred to as a *cut set*. The smallest set of basic events that can cause the top event to occur is called a *minimal cut set*. Identifying the minimal cut set is important for informing appropriate risk controls. In summary, the FTA method includes the following steps:

1. Identify and define the system or system component and scope of the analysis.
2. Define the top event.
3. Identify basic and intermediate events.
4. Construct the FT: Link the top event to basic events using logic gates and intermediate events.
5. Perform the analysis:

  a. Identify the minimal cut set
  b. Calculate the probability of occurrence of the top event if quantitative data is available.

6. Estimate the risk using a *risk matrix* given the severity of the top event and the probability of occurrence of the top event (see Section 3.6).

Additional information on performing FTA can be found in the standard IEC 61025:2006 [59]. FTA has been used in many domains, including safety and reliability. In the safety domain, the top event is usually a hazard or hazardous situation; in the reliability domain, it is usually a failure. In the safety domain, FTA can be used to analyse the entire system or components of the system that may pose a risk to operational safety. This is useful since the interaction between the system components causing the top event can be incorporated into the analysis, unlike in an FMEA (see Section 3.2). Since FTA is a useful tool for assessing the safety of systems, it should be performed at all stages of the life cycle of a system. At each stage of the life cycle, the FT will increase understanding of existing and potential failures, hazards and hazardous situations of the system. It is important to note that FTA is not limited to a system or its components but is sufficiently flexible also to incorporate factors such as human errors when estimating the occurrence of the top event. This is essential since a hazardous situation can only occur when users are exposed to a hazard or interact with a system. However, estimating probabilities for human errors may be challenging since it is time-consuming and context-specific (i.e., requiring many observations for a particular system). Despite the popularity of FTA in the safety domain [60]–[64] and benefits such as informing and complementing other risk analysis methods such as FMEA and PHA, it is important to note the following limitations of the method:

1. *Limited approach to handling uncertainty*: In a FT, the probabilities for basic events are usually assigned using single-point values rather than probability distributions. As a result, uncertainty cannot be incorporated in the probabilities for basic events when estimating the probability of the top event.

2. *Limited approach to handling multi-state variables*: In a FT, events are usually binary state, e.g., *working* or *fail*; however, it is possible to have scenarios with events that are multi-state, e.g., *working*, *fail-open* or *fail-closed*. In these

situations, the multi-state events are represented using one or more events. For instance, given an event with three states, e.g., *working*, *fail-open* or *fail-closed*, in a FT, this will be represented as two independent binary events, e.g., *working/fail-open* and *working/fail-closed.* This approach to handling multi-state variables is usually time-consuming and expensive.

3. *Unable to model sequence-dependent failures*: In situations where component failures are dependent, a FT is not suitable for modelling these types of failures.

There are several extensions to the static FT that resolve the above mentioned limitations. For instance, dynamic fault trees (DFTs) [65] have been proposed to handle sequence-dependent failures, fuzzy fault trees [66] have been proposed to handle uncertainty in data and the beta factor method have been proposed to improve modelling of common cause failures [67], [68]. In this thesis, we propose that BNs can resolve all these limitations. We discuss BNs and their underlying theory in Chapter 4.

3.4 Event Tree Analysis

An Event Tree Analysis (ETA) is an inductive method of analysis that shows all potential outcomes or consequences of an initiating event [6], [54]. An event tree (ET) is a logic tree diagram used to analyse “the occurrence of accidents as consequences of hazard events in a system” [20] [13]. In general, systems usually have risk controls or mitigants to avoid or mitigate the consequences of potential initiating events. Hence the potential outcomes or consequences of an initiating event are affected by the success or failure of the risk control measures. An example of an ETA for an explosion (presented in [54]) is shown in Figure 7. In this example, given an explosion (initiating event), the probability of a fire occurring (outcome/consequence) depends on the operation or failure of the sprinkler and the alarm system.

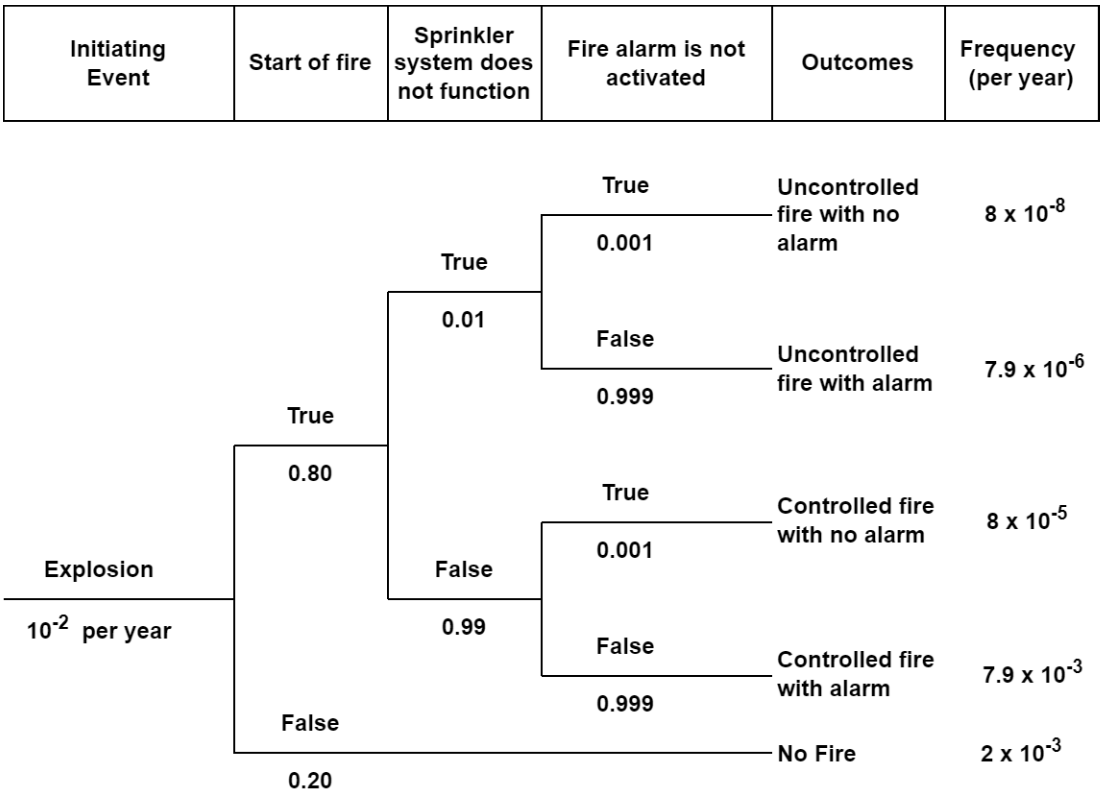


Figure 7 Example of an event tree for an explosion

In general, the outcome of events in the tree are assumed to be binary, e.g., true or false; however, some events may include multiple outcomes, e.g., true, false or open. ETA can be used to perform quantitative and qualitative analyses. Quantitative analysis is done when probabilities are assigned to events in the tree. For instance, as shown in Figure 7, the probability of "an uncontrolled fire with no alarm" is determined by multiplying the probability of the initiating event and the probabilities of all events in the sequence:

$$P = 0.01 \times 0.8 \ \times 0.01 \ \times 0.001$$

$$P = 8 \ \times 10^{-8}$$

In safety risk management, the initiating event is usually a hazard or hazardous situation. Therefore, the probability of occurrence of the consequence event e.g., injury, calculated using the event tree can then be combined with the severity of the consequence event to estimate the risk associated with the hazard, i.e., *Risk* = *P* × *S*. The severity of the event can be determined based on the economic cost or medical intervention required or any other suitable measure or method.

In summary, the ETA method includes the following steps:

1. Identify an initiating event (hazard or hazardous situation).
2. Identify intermediate events, safety measures, risk controls and mitigants.
3. Identify potential outcomes or consequences of the initiating event.
4. Construct the event tree.
5. Calculate the probabilities for each potential outcome or consequence if quantitative data is available.

Additional information on performing ETA can be found in the standard IEC 62502 [69]. A limitation of the ETA method is the inability to handle second-order uncertainty in the assigned probability values since single-point values are used rather than distributions. Risk assessors and manufacturers will find the ETA useful for estimating the probability of occurrence of harm associated with identified hazards. Also, ETA complements other risk analysis methods such as PHA and FTA and can be applied at different phases during the life cycle of a system.

3.5 Bow-tie Model

A bow-tie model is a graphical tool used to describe and analyse the causes of an event, e.g., hazard, its consequences and the safety barriers or controls required to prevent the event or mitigate its consequences [70], [71]. It is often considered to be a combination of a fault tree (FT) and an event tree (ET). However, the principal merit of the bow-tie model is identifying and describing the safety barriers or controls to prevent the event or mitigate its consequences. An example of a generic bow-tie model adapted from [71] is shown in Figure 8.

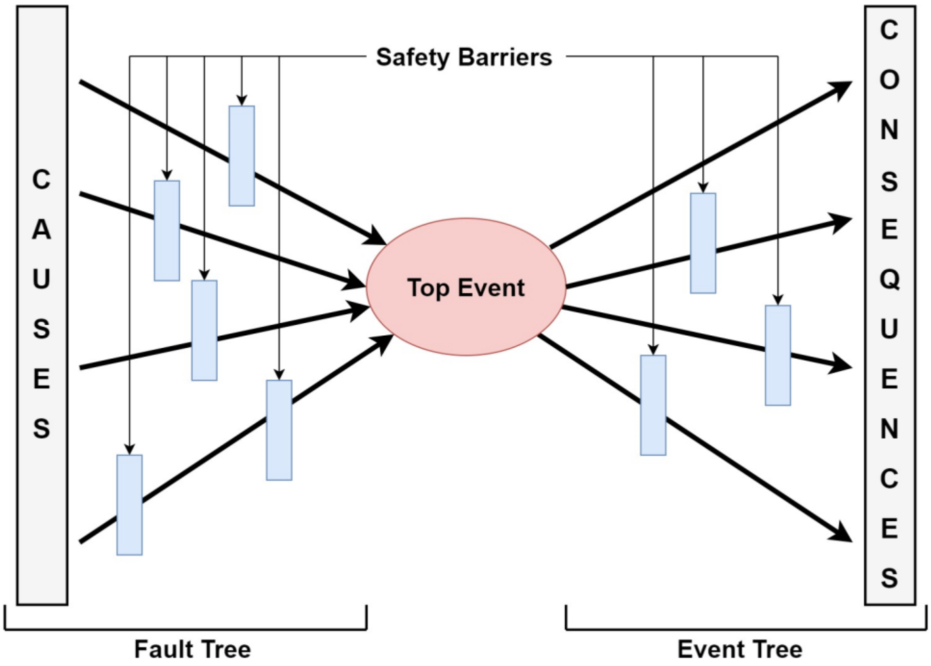


Figure 8 Generic Bow-tie Model

3.6 Risk Matrices

A risk matrix is a tool that is used to determine the level of risk associated with a particular hazard. It combines the probability of the harm occurring and the severity of the harm using a matrix or table to estimate the risk, i.e., $Risk = P \times S$. The estimated risk is usually classified qualitatively using a ranking scale such as ‘low’, ‘medium’ ‘high’, quantitatively using a number (obtained by multiplying the rankings for likelihood and the severity of the risk) or a combination of both. Risk matrices can be used in conjunction with other risk analysis methods, such as FTA, or independently using qualitative or quantitative data or both to estimate risk. An example of a risk matrix adapted from [6] is shown in Table 2, and the definitions of the severity levels and probability occurrence levels used in the risk matrix are shown in Table 3 and Table 4 respectively.

Table 2 Example of a risk matrix

		Severity Levels				
		Negligible (1)	**Minor (2)**	**Serious (3)**	**Critical (4)**	**Fatal (5)**
Likelihood / Probability Levels	**Frequent (5)**	5	10	15	20	25
	Probable (4)	4	8	12	16	20
	Occasional (3)	3	6	9	12	15
	Remote (2)	2	4	6	8	10
	Improbable (1)	1	2	3	4	5

Risk classification: Green = Low (1-8), Yellow = Medium (9-15), Red = High (16-25)

Table 3 Definition of severity levels for harm

Rank	**Terms**	**Description**
5	Fatal	Result in death
4	Critical	Result in irreversible injury
3	Major	Results in injury requiring medical intervention
2	Minor	Results in temporary injury
1	Negligible	Results in temporary discomfort

Table 4 Definition of probability levels for the occurrence of harm

Rank	**Terms**	**Probability range**
5	Frequent	$\geq 10^{-3}$
4	Probable	$<10^{-3}$ and $\geq 10^{-4}$
3	Occasional	$<10^{-4}$ and $\geq 10^{-5}$
2	Remote	$<10^{-5}$ and $\geq 10^{-6}$
1	Improbable	$<10^{-6}$

In summary, the risk matrix method includes the following steps:

1. Identify the hazard.
2. Assign the probability of occurrence of harm and severity of harm ratings.
3. Look up the risk matrix to determine the overall risk of the hazard.

The risk matrix method is used in several industries, including product safety. It offers advantages such as quick risk estimation of hazards; however, it does not consider the causal context in which hazards or risks occur. Hence, risk estimates may be overly subjective or ill-defined resulting in flawed risk estimates. For these reasons, risk matrices are usually used to quickly identify hazards posing the highest risks or in conjunction with other robust analysis methods such as FTA discussed previously.

3.7 Monte Carlo Simulation

The Monte Carlo simulation is a mathematical technique used to model the probability of potential outcomes of an uncertain event [72], [73]. It is used in several industries for risk assessment and making decisions under uncertainty. For instance, in reliability engineering, it is used to predict the failure rate of a system using available information such as historical testing and operational data.

Monte Carlo simulation consists of *input variables* (i.e., random variables that influence the results of the analysis), *output variables* (i.e., the results of the analysis) and the *mathematical model* (i.e., the mathematical function used to describe or simulate the relationship between the input and output variables). A schematic of Monte Carlo simulation is shown in Figure 9.

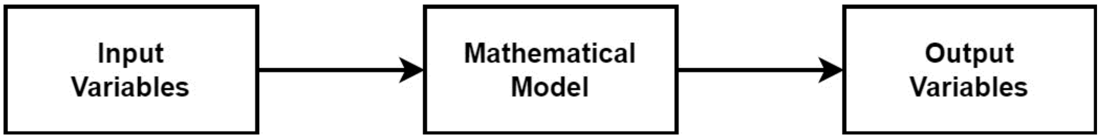


Figure 9 Schematic of Monte Carlo Simulation

In Monte Carlo simulation, the values of the variables are represented using probability distributions such as a Normal distribution; hence it is suitable for modelling uncertainty. In fact, Monte Carlo simulation is used in conjunction with other risk analysis methods, such as FTA [16] or as a standalone method to handle uncertainty. However, it is important to note that it is time-consuming and computationally expensive for complex systems.

3.8 Beta Factor Method

The Beta (β) factor method is used to model common cause failures of a system [67], [68]. A *common cause failure* is the failure of multiple components of a system due to a shared or common cause. The underlying assumption of the β-factor method is that the failure λ of a component is dependent on *independent failures* λ_1 (failures impacting only the component) and *common cause failures* λ_2 (failures impacting all components sharing the common cause) i.e., $\lambda = \lambda_1 + \lambda_2$.

The β-factor parameter is the probability that a failure of a component is due to common cause failures, i.e., $\beta = \frac{\lambda_2}{\lambda}$. Hence $\lambda_2 = \beta\lambda$ and $\lambda_1 = (1 - \beta)\lambda$.

When applied to FTA (see Section 3.3), the β-factor method allows the modelling of common cause failures within FTA. An example of a fault tree model with common cause failures is shown in Figure 10. In this example, we estimate the probability of a power failure for a system. We assume that the probability of failure for each power supply in the system is 0.001, and the β-factor is 0.1. Hence, using Boolean algebra, probability rules and the β-factor, the probability that the power supplies fail due to common cause failures is 0.0001 (i.e., 0.1 × 0.001), and the probability that the power supplies fail independently is 8.1E-7 (i.e., (0.9 × 0.001) × (0.9 × 0.001)). Hence the probability of a power failure for the system is 1.0081E-4 (i.e., 0.0001 + 8.1E-7).

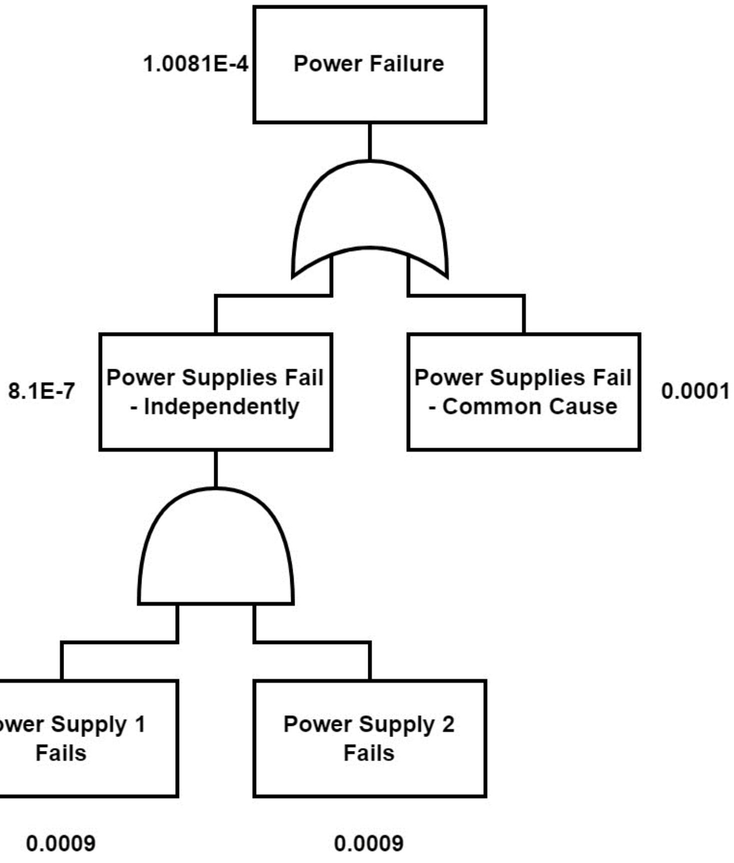


Figure 10 Fault Tree Analysis with CCF

3.9 Parts Count and Parts Stress Methods

The parts count method and the parts stress method defined in MIL-HDBK-217F [74] are used to estimate the reliability of systems. The parts count method is used to estimate the reliability of a system in the early design stage when insufficient information is available [74]. This method uses the generic failure rates of the parts given an operating or use environment. These failure rates are multiplied by a quality factor and summed up to estimate the failure rate of the system.

Though the parts count technique may be used in conjunction with other methods or as a standalone method to estimate the risk of a novel system, it is time-consuming and expensive for complex systems. Furthermore, the parts count technique can give inaccurate results if the system is redundant [17]. Other limitations of the method include limited approach to handling uncertainty.

The parts stress method is used to estimate the reliability of a system later in the development stage when sufficient operating information is available [74]. This method is more accurate than the parts count method since it incorporates operating stresses when estimating the failure rates of the parts. The failure rates are then summed to estimate the failure rate of the system. The accuracy of the failure rate estimates increases as more operating information becomes available.

3.10 Chapter Summary

In this chapter, we described the commonly used risk analysis methods and techniques in the product safety industry. We also discussed some of the limitations associated with these methods previously discussed in Section 1.3. In the next chapter, Bayesian Networks (BNs) are reviewed as a method for risk analysis and assessment which resolves the limitations associated with existing risk analysis methods.

Chapter 4 Bayesian Networks

In this chapter, Bayes' Theorem and Bayesian Networks (BNs) are introduced. Then, the concepts of conditional independence and types of reasoning done using BNs are presented. The material presented in this chapter is essential to understand the novel work presented in Chapter 6 and applied in Chapters 7 and 8. Some of the material presented in this chapter has previously been presented in the following publications: Publication 1 [23], Publication 2 [15], Publication 3 [24], Publication 4 [25], Publication 5 and Publication 6.

4.1 Conditional Probability and Bayes' Theorem

"The basic expressions in the Bayesian formalism are statements about conditional probabilities" [75]. Given two events, *A* and *B*, a *conditional probability* is the probability that event *A* occurs, given that event *B* has already occurred. This relationship between events *A* and *B* is expressed as *P(A|B)*, i.e., the probability of *A* given *B* or the probability of *A* in the context of event *B*.

If we assume that events *A* and *B* are independent ($A \perp B$), then our belief in event *A* is unchanged given event *B* (vice-versa for our belief in event B). This relationship is expressed as follows:

Equation 2:

$$P(A|B) = P\ (A)$$

$$P(B|A) = P\ (B)$$

If we assume the joint event (*A*, *B*), then the relationship between the joint event and conditional probabilities is expressed as follows:

Equation 3:

$$P(A, B) = P\ (A|B)P(B) = (B|A)\ P(A)$$

Equation 3 can be re-written as follows:

Equation 4:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

Equation 4 is called Bayes' Theorem, developed in the 1750s by Reverend Thomas Bayes [76], [77]. Bayes Theorem provides a formula for updating our prior belief about an event given new evidence. Our prior belief is called the *prior probability* (or prior), and our revised belief is called the *posterior probability* (or posterior). Bayes Theorem is essential since it expresses a probability (posterior probability) which people generally find difficult to evaluate in terms of probabilities that can be obtained directly from our experience, knowledge or observations [75]. For instance, in the safety domain, a manufacturer can estimate the probability of an injury given a hazard using injury reports but may find it difficult to estimate the probability of a type of hazard given a particular injury. The latter information is important since an injury can be caused by one or more different hazards, e.g., burns can be caused by hot surfaces or electric shock. Suppose that we assume for a domestic iron that the probability of burns (injury) is 0.75. The probability of a hot surface (hazard) is 1, and based on injury reports, the probability of a burn due to a hot surface and electric shock is 0.6 and 0.4, respectively. We can calculate the probability that the hazard is a 'hot surface' given the injury (burns) using Bayes' Theorem (see Equation 4) as follows:

$$P(Hot\ surface|Burns) = \frac{P(Burns|Hot\ surface)P(Hot\ surface)}{P(Burns)}$$

$$= \frac{0.6\ \times 1}{0.75} = 0.80$$

It is important to note that at the core of the Bayesian approach is the belief that all probabilities are conditional on a context *K,* where *K* is background knowledge and assumptions [13], [75]. Therefore, the probability assigned to an uncertain event *A* is always conditional on the context *K,* i.e., *P*(*A*|*K*). In practice, when we assign a probability to an (uncertain) event *A*, we often write *P*(*A*), excluding the symbol for *K*. This is appropriate when the context *K* does not change during a given analysis. In situations where the context *K* changes, we have to explicitly specify *K*. Hence Bayes Theorem can also be expressed as follows:

Equation 5:

$$P(A|B,K) = \frac{P(B|A,K)P(A|K)}{P(B|K)}$$

Where *K* is background knowledge or assumptions.

Equation 3 computes the joint probability distribution for two events; however, in practice, we may need to compute the joint probability distribution for three or more events. In these situations, Equation 3 can be extended as required using the *chain rule* formula [75]. For instance, given a set of n events, $E_1, ...E_n$, the joint probability distribution is computed as the product of n conditional probabilities:

Equation 6:

$$P(E_1 \ldots . E_n) = P\ (E_n\ |E_{n-1,} \ldots . E_1) \ldots . P(E_2|E_1)P(E_1)$$

Finally, Bayes' Theorem is easy to compute when a problem consists of one or a few variables. However, for complex problems with a large number of variables, computing the joint probability distributions and posterior probabilities becomes a complex and time-consuming task. In these situations, we recommend using Bayesian networks (BNs) since it efficiently computes Bayes' Theorem and the joint probability distribution for a large number of variables. In the following section, we discuss BNs and their features.

4.2 Bayesian Networks

A *Bayesian network* (BN) (also known as a *Bayesian belief network* (BBN) or *causal Bayesian network* (CBN)) is a directed acyclic graph (DAG) that encodes the joint probability distribution for a large set of random variables. It consists of qualitative and quantitative components [13], [75], [76], [78]–[81]. The qualitative component of the BN is a DAG with nodes representing a set of random variables and directed edges (arcs) representing the causal relationship or dependencies between the connected variables (nodes). For instance, given two variables X_1 and X_2, a directed edge from X_1 to X_2 ($X_1 \rightarrow\ X_2$) indicates that X_1 causally influences X_2 or X_2 is dependent on X_1; thus, X_1 is called the parent of X_2 and X_2 is called the child of X_1.

The quantitative component of the BN consists of node probability tables (NPTs), also called conditional probability tables (CPTs). NPTs specify the strength of the relationship or conditional dependency between the connected variables by defining the conditional probability distribution for each variable given its parents. For instance, given set $X\ =\ \{X_1, \ldots X_n\}$ of random variables, the NPT for each variable X_i given its parents $PA\ (X_i)$ can be represented as $P\ (X_i|\ PA\ (X_i))$. Any variable X_i

without parents is called a root node, and its NPT is its prior or marginal probability distribution, i.e., $P(X_i)$.

The conditional independence assumptions for the variables in the BN, represented by the directed edges and NPTs, facilitate decomposition of the underlying joint probability distribution as a product of conditional probability distributions. Hence, the joint probability distribution for set $X \ = \{X_1, \dots X_n\}$ of random variables for any BN can be computed as follows (using the chain rule formula [75]):

Equation 7:

$$P\ (X_1, \dots X_n) = \prod_{i=1}^{n} P(X_i \mid PA\ (X_i))$$

Equation 7 is useful since it reduces the complexity of inferences performed in a BN [82].

NPTs in a BN can also be defined using other methods instead of manually specifying the conditional probabilities. For instance, NPTs for discrete variables can be defined using comparative expressions such as IF statements. The NPTs for continuous or numeric variables can be defined using mathematical functions such as A = B + C and statistical distributions such as an Exponential distribution [13]. Some of these methods are illustrated in Table 5.

Bayesian networks consisting of discrete and continuous variables are called *hybrid* Bayesian networks [13] [79]. An example of a hybrid BN is shown in Figure 11. In this example, the probability of a patient being burnt by a defibrillator due to its surface being too hot is estimated. The graphical structure of this BN was previously presented in Chapter 2 (see Figure 2); in this section, we assign probabilities to the variables. In Figure 11, the probability that the patient is burnt depends on the probability of the node ‘Surface Too Hot’ and the probability of the node ‘Controller Intervention’. The probability of the node ‘Surface Too Hot’ depends on the probability of the node ‘Wrong Setting Chosen’ and the probability of the node ‘Automatic Switch-Off’. In this example, the probability that the patient is burnt is 0.0016 if we assume that the mean probability of the node ‘Surface Too Hot’ is 0.004, the mean probability of the node ‘Wrong Setting Chosen’ is 0.1, the probability of the node ‘Automatic Switch Off’ is 0.80 and the probability of the node ‘Controller Intervention’ is 0.30. The NPTs for the variables in the BN are shown in Table 5. Ultimately, this simple example demonstrates the flexibility and power of using hybrid BNs to model complex problems involving discrete and continuous variables, such as risks associated with products.

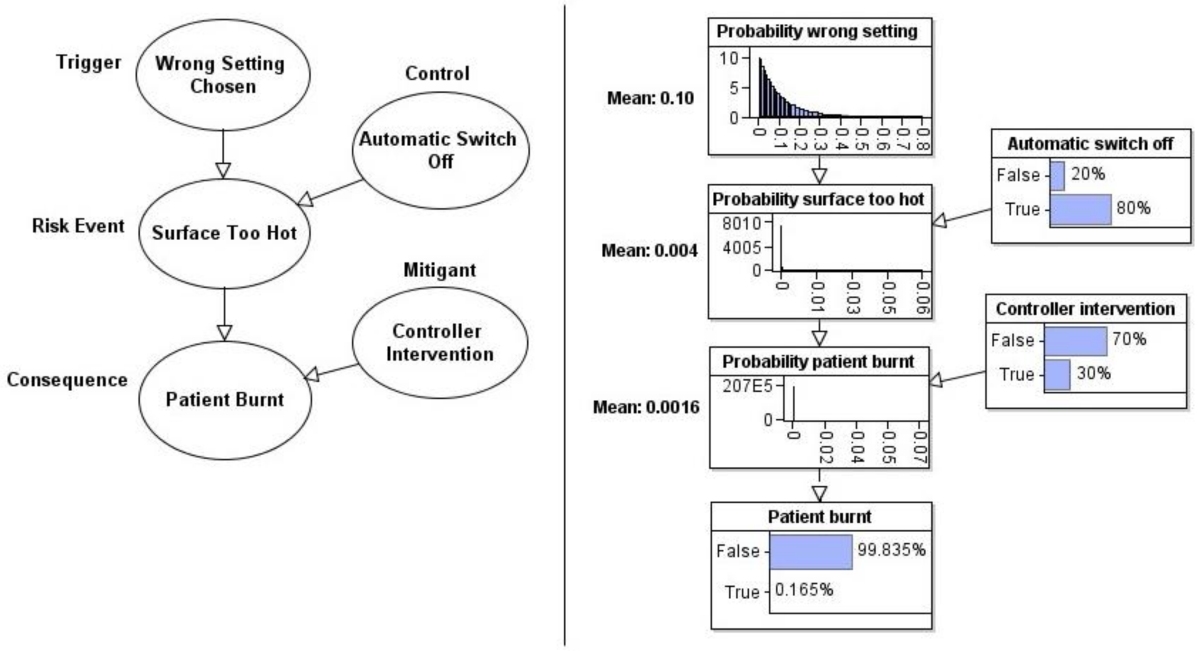


Figure 11 Hybrid BN – Defibrillator Example

Table 5 NPT for nodes in the hybrid BN - Defibrillator Example

Node Name	**NPT**
Wrong Setting Chosen	Exponential (10)
Automatic Switch Off	False: 0.2, True: 0.8
Controller Intervention	False: 0.7, True: 0.3
Surface Too Hot	Partitioned expression (False: 0.2 × wrong_setting, True: wrong_setting × 0.001)
Patient Burnt	Partitioned expression (False: Triangle (0.2 × hot_surface, hot_surface, 0.5 × hot_surface), True: 1.0E-4 × hot_surface)

For additional information on the theory of BNs, see [13], [75], [76], [78]–[81]. In the following section, we discuss the process and methods used to build BNs.

4.3 Building Complex Bayesian Networks

The process of building a Bayesian network consists of two main activities:

1. *Determine the structure of the BN*: The first part of this phase entails identifying the set of variables relevant to the problem and specifying their states. The last part of this phase entails building the DAG. This can be done by linking relevant variables using directed edges based on the causal (cause-effect) relationships among the variables [81].

2. *Specify the parameters (or NPT) of the BN variables*: Once the structure of the BN is defined, the next step is to specify the parameters (or NPT) for the variables. The parameters (or NPTs) describe the strength of the relationship or conditional dependency between the variables in the structure.

The BN structure and parameters can be learnt from data (data-driven approach), elicited knowledge from domain experts (knowledge-based approach) or a hybrid approach that combines both methods. In practice, most BNs are built using the knowledge-based approach due to potential issues with automated learning from data, such as requiring a large amount of data and poor data quality [83]. For this reason, several knowledge engineering approaches have been proposed to facilitate the easy development of BNs using expert knowledge. In the following section, we review these knowledge engineering approaches. Automated methods for learning BN structure and parameters using data such as score-based algorithms and maximum likelihood expectation are briefly discussed.

4.3.1 Knowledge Engineering Methods: BN Structure

Several knowledge engineering approaches have been proposed for developing Bayesian networks (BNs) [19], [84]–[87]. For instance, Laskey and Mahoney [84], [85] proposed a method for specifying knowledge in larger semantically meaningful units or modules called *network fragments*. A network fragment is a set of related random variables together with knowledge about their probabilistic relationships. Network fragments should be practical, explainable and adhere to the semantics and syntax of BNs. Koller and Pfeffer [86] proposed the object-oriented Bayesian networks (OOBNs) approach. In this approach, network fragments are called *classes* and variables, and instantiated fragments are called *objects*. Helsper & Van der Gaag [87] proposed using ontologies to develop BNs. An ontology is an explicit specification of the elicited domain knowledge, including meta-level and background knowledge. The information contained in the ontology is then used to develop the required BN structure [87].

Neil et al. [19] proposed using idioms to develop large complex BNs. *Idioms* are small BN structures or fragments that represent generic types of uncertain reasoning. Using this approach, researchers have developed idioms specifically for legal and medical domains [88], [89]. For instance, Lagnado et al. [89] proposed idioms for legal BN development and Kyrimi et al. [88] proposed idioms for medical BN development.

In this thesis, we used the idiom-based approach to develop idioms specifically for building BNs for product safety risk management called *product safety idioms* (see Chapter 6). The proposed product safety idioms are sufficiently generic that they can be applied to many different product safety cases. In the following section, we review the idiom-based approach proposed by Neil et al. [19].

4.3.1.1 Idiom-based Approach

Neil et al. [13], [19] proposed the following four idioms as part of the idiom-based approach for building BNs:

1. *Cause-consequence idiom:* This idiom models the causal relationship between causes and consequences. It uses chronological order where the cause always precedes the consequence, or the consequence always follow the cause. For example, as shown in Figure 12, Rain causes Flooding.

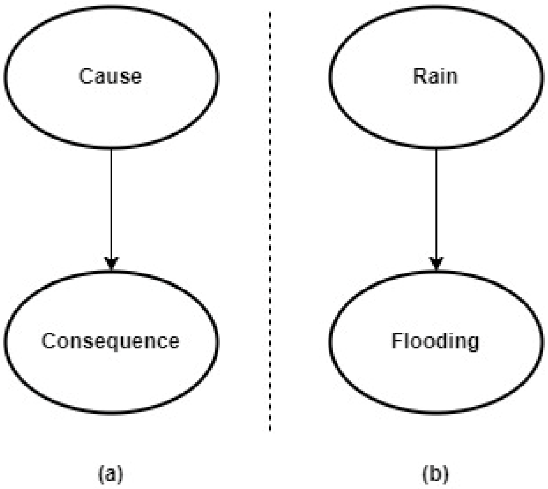


Figure 12 Cause-consequence idiom (a) with instantiation (b)

2. *Risk/Opportunity event idiom:* This idiom is an instance of the cause-consequence idiom that models a risk/opportunity event. Its structure includes a cause (trigger), risk/opportunity event, consequence, control and mitigant. For example, consider the risk of a car crash shown in Figure 13. In this example, driving fast (cause) can cause a crash (risk event), resulting in injury (consequence). However, speed bumps (control) help avoid the crash, and the seat belt (mitigant) helps avoid injury if there is a crash.

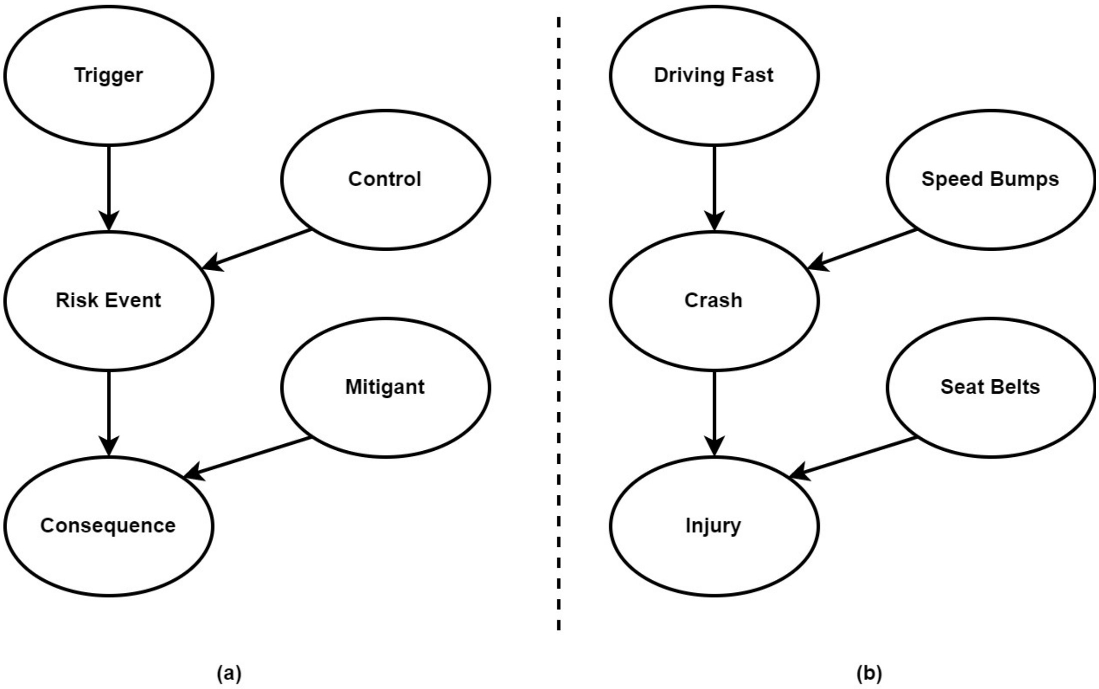


Figure 13 Risk event idiom (a) with instantiation (b)

3. *Measurement idiom:* This idiom models the uncertainty concerning the measurement of a variable. It assumes – as is generally the case – that the actual value of the variable is not directly observed but is rather assessed by a 'measured' value. The extent to which the measured value 'matches' the actual value is determined by the accuracy of the measurement instrument used to measure the variable. For example, as shown in Figure 14, we generally cannot observe the 'true' number of product defects. Instead, we use a measured value, namely the number of product defects found in testing. The extent to which this accurately captures the true number of defects depends on the accuracy of testing. If testing is extensive, we might expect to find most or even all defects, and so the number found would be a very accurate 'measure' of the true number of defects. However, if we did very little testing, then the number found would not be an accurate measure of the true number of defects.

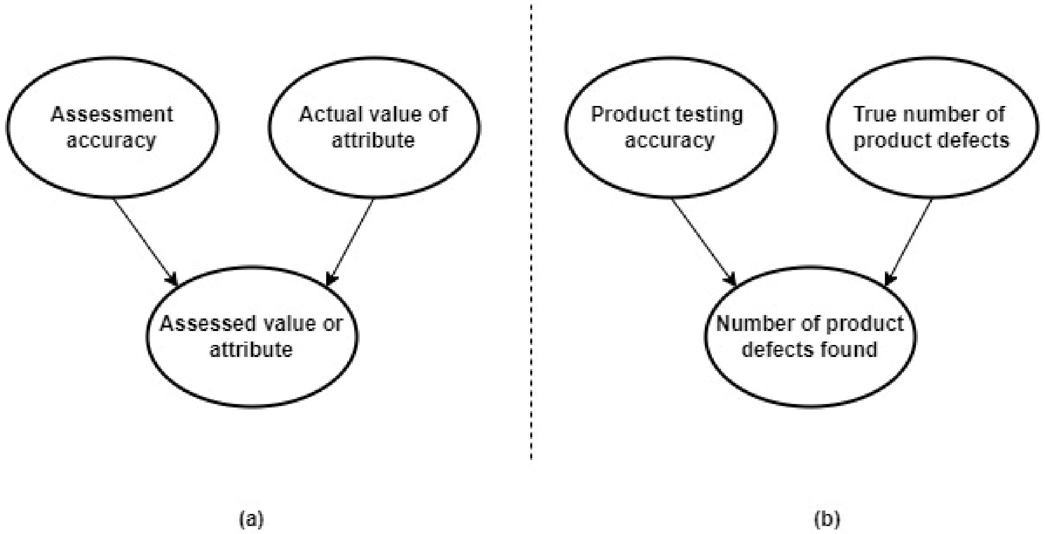

Assessment accuracy
Actual value of attribute
Assessed value or attribute
Product testing accuracy
True number of product defects
Number of product defects found
(a)
(b)

Figure 14 Measurement idiom (a) with instantiation (b)

4. *Definitional/synthesis idiom:* This idiom (see Figure 15) models the combination of nodes into one synthetic node. This is done in one of the following ways:
   a. *Definitional relationship between variables:* This entails defining the synthetic node in terms of its parents.
   b. *Hierarchical definitions:* This entails combining nodes into definitional idioms and linking them together to establish a hierarchical structure.

c. *Combining parent nodes to reduce the size of child nodes NPTs:* This entails combining parent nodes into synthetic nodes to reduce the number of parents and the NPT parameters of child nodes.

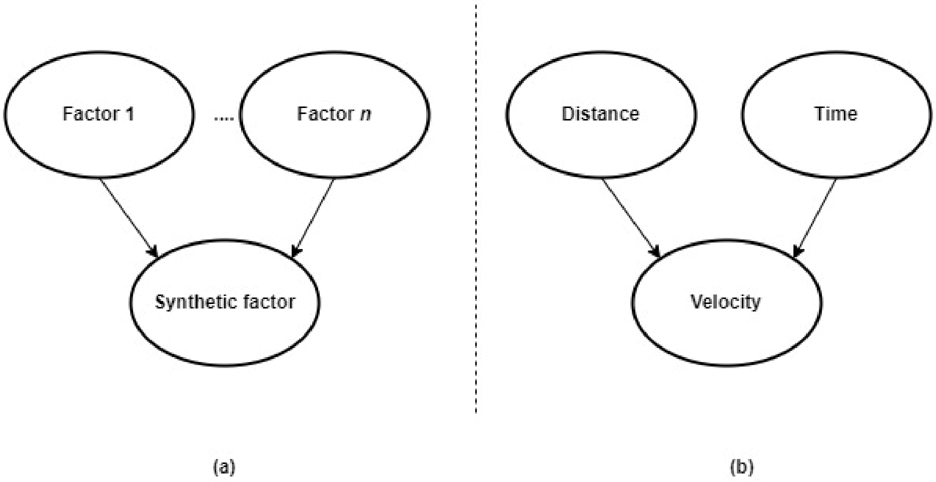


Figure 15 Definitional idiom (a) with instantiation (b)

5. *Induction idiom:* This idiom models statistical induction to learn an unknown or partially known parameter about some population of interest from data. The idiom structure is shown in Figure 16. The induction idiom is the general model for any type of statistical inference done using a BN.

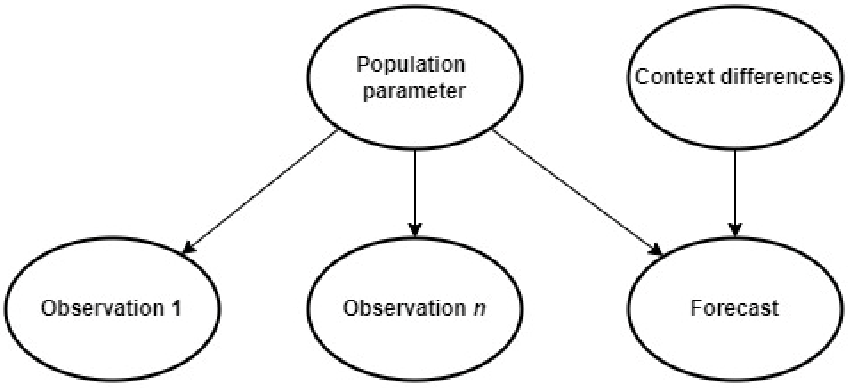


Figure 16 Induction idiom

The idiom-based approach is useful since it allows modellers to organise variables into meaningful BN fragments that can be combined into larger BNs. Also, it can be applied to many different problems.

Experts also use automated methods to learn the BN structure. The two main algorithms for learning BN structures are *constraint-based* and *score-based*. *Constraint-based* algorithms learn the structure of the BN by identifying causal relationships or dependencies among variables using *conditional independence tests* and linking variables with dependencies [90]–[92]. *Score-based* algorithms apply general optimisation techniques to learn the BN structure. It involves identifying candidate structures and assigning them a *network score* based on their goodness of fit; the structure with the highest score is selected [92]–[94].

4.3.2 Knowledge Engineering Methods: BN Parameters

There are several methods proposed to ease the burden and reduce the time taken to populate NPTs for variables in a BN [13]. Comparative expressions such as IF statements and logic functions such as OR, AND, and NoisyOR can be used to populate the NPTs for discrete variables. For instance, given three binary variables *A, B,* and *C,* if *C* is true when *A* or *B* is true, then the NPT for variable *C* can be easily populated using the following expression:

$$\text{IF (A == "True" || B == "True", "True", "False")}$$

Where || represents OR.

Ranked nodes have been proposed to represent variables with states measurable on a subjective ranked scale like {“low”, “medium”, “high”}. A ranked node assumes that the states of a variable are mapped to an underlying numerical scale interval [0,1]. For this reason, the NPTs of these nodes can be defined using statistical distributions, specifically a TNormal distribution. Ranked nodes are useful for defining the NPTs for nodes with parents. In these situations, the NPT of the child node is defined simply as a TNormal distribution with mean μ (weighted average of its parents) and variance σ^2. Other methods for defining NPTs include using mathematical expressions such as $X = Y + Z$ and statistical distributions such as Normal distribution [13], [95].

Experts also use automated methods such as *maximum likelihood estimation* and *expectation maximisation* algorithms to learn parameters. *Maximum likelihood estimation* is a method of inferring or estimating the parameters of a probability distribution using observed data [13], [96]. It entails maximising the likelihood function to determine the parameters that best describe the observed data. *Expectation maximisation* is a method for performing maximum likelihood estimation using incomplete data or data with latent variables [13], [96].

It is important to note that applying the above methods accurately to different risk problems requires the modeller to understand the subject matter sufficiently. However, due to many different risk problems, modellers often require input from domain experts. Several processes have been proposed to elicit knowledge from experts. These processes include determining what information to elicit, designing the process for elicitation and performing the elicitation [13], [97]–[99].

The proposed methods for populating BN parameters discussed in this section have been used in this thesis to define the NPTs for the BNs presented in the case studies.

4.3.3 Conditional Independence in Bayesian Networks

Building any BN requires understanding the three types of dependency connections (*d-connections*). D-connections encode assumptions about conditional independence (see Equation 2 and Equation 7) among variables based on *d-separation* (a criterion for deciding whether two variables in a BN are independent given a third variable). The underlying assumption for conditional independence in a BN is that each variable is conditionally independent of its non-descendants, given its parents. The three types of d-connections are shown in Figure 17 and described using variables *X, Y* and *Z* [13], [75], [76]:

1. *Serial d-connection*: In this structure (Figure 17a), information from X is transmitted to Y via Z. As a result, Z is called the *mediator* that transfers the effect of X to Y. Information is only transmitted from X to Y via Z when Z is unknown. When Z is known, X has no effect on Y since Z blocks any information about X from Y. For this reason, X and Y are conditionally independent (or d-separated) given Z, i.e., $(X \perp Y) \mid Z = z$.

2. *Diverging d-connection*: In this structure (Figure 17b), information is transmitted from Z to X and Y, respectively. Information is only transmitted from X to Y via Z when Z is unknown. When Z is known, then X has no effect on Y since Z blocks any information about X from Y. For this reason, X and Y are conditionally independent (or d-separated) given Z, i.e., $(X \perp Y) \mid Z = z$.

3. *Converging d-connection*: In this structure (Figure 17c), information is transmitted to Z from both X and Y, respectively. Information is only

transmitted from *X* to *Y* via *Z* when *Z* is known. When *Z* is unknown, *X* and *Y* are considered independent (or d-separated), i.e., $(X \perp Y) \mid Z$, and no information is transmitted between them. For this reason, *X* and *Y* are conditionally dependent given *Z*.

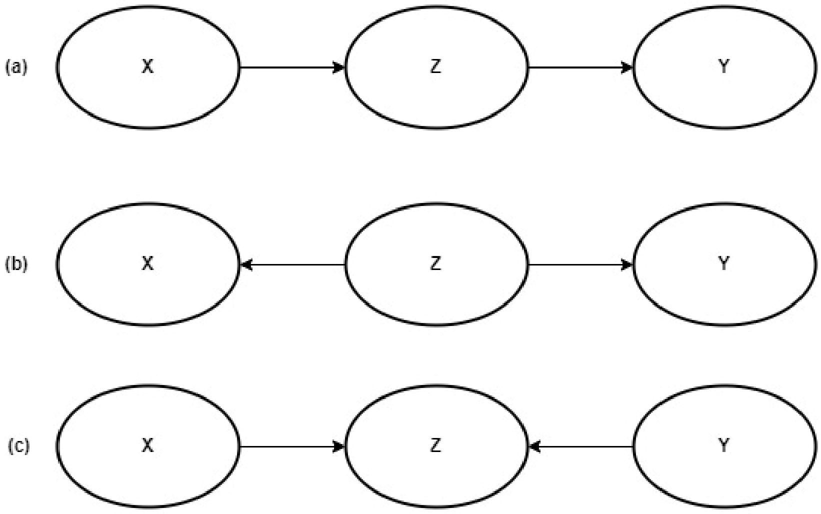


Figure 17 Types of d-connections (a) Serial (b) Diverging (c) Converging

4.4 Inference in Bayesian Networks

Since performing Bayes' Theorem computations in large BNs can be challenging, several inference algorithms have been proposed to perform computations efficiently [13], [75], [100]–[102]. The most popular inference algorithm used in BNs is the *junction tree* algorithm [13], [100], [102]. This algorithm transforms a Bayesian network into a tree structure with clusters (groups consisting of one or more variables) known as a *junction tree*. In a junction tree (see Figure 18), the clusters (represented by nodes) are connected via edges (represented by lines) and separators (represented by square nodes). The separators must be a common subset of the nodes in the clusters they link. Computations are done locally on parts of the tree and propagated to other parts of the tree structure as 'messages' (known as *message passing*). This allows the BN to provide global answers based on local computations.

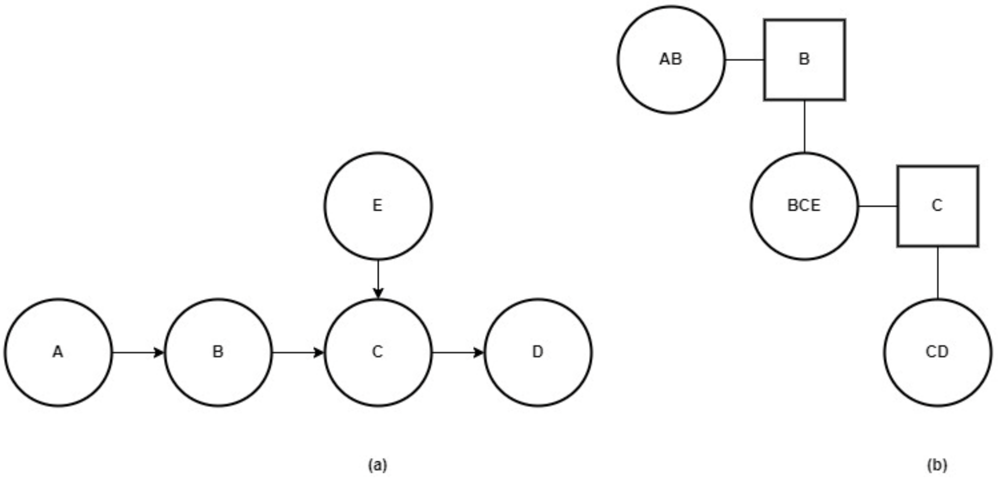


Figure 18 (a) A BN and (b) associated junction tree

Another useful algorithm supporting inference in BNs, especially hybrid BNs, is *dynamic discretization* [13], [103], [104]. *Discretization* is the process of transforming a continuous variable into a discrete variable. In the past, BN methods and tools used *static discretization* (i.e., discretization done using a predefined interval) to handle continuous variables. However, this approach has several limitations, including loss of accuracy, slow execution and high memory demands [13], [103], [104]. These limitations are resolved using *dynamic discretization* (i.e., discretization based on the distribution of the data).

The *dynamic discretization* algorithm proposed by Marquez et al. [104], [105] based on work by Kozlov and Koller [106] entails "a process of dynamic discretization of the domain of all continuous variables in the BN and using entropy error as the basis for approximation". It improves the accuracy of inference in hybrid BNs and has fewer memory demands than static discretization. In this thesis, the dynamic discretization and junction tree algorithms are used for inference in the hybrid BNs discussed in the case studies. Both algorithms are implemented using AgenaRisk Desktop software [22].

4.5 Reasoning with Bayesian Networks

In this section, we describe the three types of reasoning done using BNs, i.e., observation, intervention and counterfactual. These types of reasoning vary in terms of the queries they can answer and are organised into a three-level causal hierarchy called the *ladder of causation*. The ladder of causation shown in Table 6, proposed by Pearl [76], provides a framework to understand the different levels of reasoning and how they relate to each other. The three levels correspond to the complexity of the causal queries ranging from observation (Level 1) to counterfactual (Level 3). The underlying concept of the ladder of causation is that queries at level *n* can only be answered if the information at level *n-1* is available.

Table 6 Pearl's Ladder of Causation

Level	**Reasoning**	**Activity**	**Questions**
1	Observation or Association	Seeing, Observing	What if I see? How would seeing X change my belief in Y?
2	Intervention	Doing, Intervening	What if I do? What would Y be if I do X?
3	Counterfactual	Imagining, Retrospective	What if I had done? Was it X that caused Y?

In the following sections, we illustrate the three types of reasoning using the Garden BN shown in Figure 19 adapted from [75]. The Garden BN describes the relationships between the variables season, rain, sprinkler and garden wet using the following assumptions:

1. P(Rain season) = P (Dry season) = 0.5
2. P(Sprinkler = On | Rain season) = 0.20
3. P(Rain = Yes | Rain Season) = 0.80
4. P(Garden wet = Yes | Sprinkler = On, Rain = Yes) = 0.99
5. P(Garden wet = Yes | Sprinkler = On, Rain = No) = 0.9
6. P(Garden wet = Yes | Rain = Yes, Sprinkler = Off) = 0.9
7. P(Garden wet = Yes | Sprinkler = Off, Rain = No) = 0.01

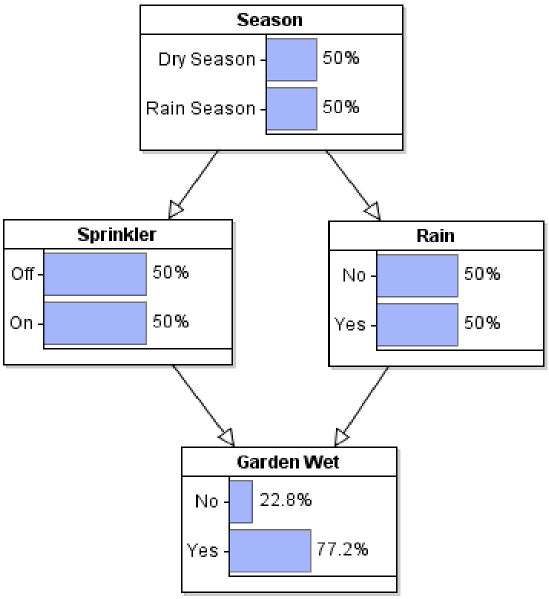


Figure 19 Garden BN with marginal probabilities

4.5.1 Observation Reasoning

The first level of the ladder of causation entails making predictions or inferences using passive observations. Observation or association reasoning is based on statistical relationships informed by the data [75], [76], [107]. For instance, as shown in Figure 20, observing that the sprinkler is on, we can infer that it is most likely the dry season. This type of association can be informed directly from the data without any information on the causal relationship among the variables. In fact, we are simply computing the probability of the dry season given that the sprinkler is “On”, i.e., $\mathrm{P}\,(\text{Dry season} \mid \text{Sprinkler} = \text{On})$. Hence methods such as regression, machine learning and conditional probabilities are examples of observation reasoning since they measure the degree of associations between variables [76].

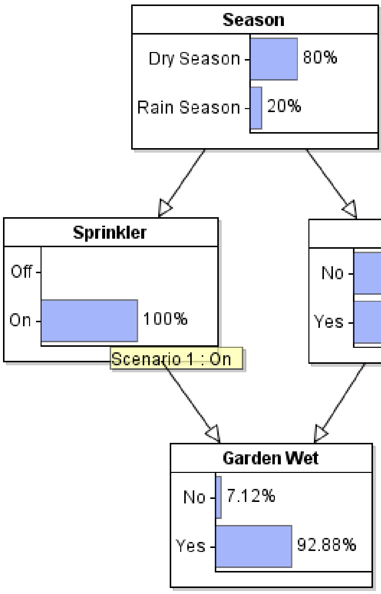


Figure 20 Garden BN after observing the sprinkler is on

In a BN, we can perform two types of reasoning using observations, i.e., diagnostic (backward) reasoning and predictive (forward) reasoning.

1. *Diagnostic reasoning*: This type of reasoning entails discovering the cause of an observation. For instance, observing the sprinkler is "On", we can infer that it is most likely the dry season, as shown in Figure 20. In Figure 20, when we observe that the sprinkler is "On", the probability of dry season increases to 0.8 (the prior was 0.5, as shown in Figure 19). There is a special type of diagnostic inference known as *explaining away* [13], [75], [108]. Explaining away can be done when a child variable has at least two independent parent variables. If the child variable is observed, then the likelihood of the parent variables increases. However, suppose only one of the parent variables occurs. In that case, it becomes the most likely explanation of the child variable, hence explaining away the other possible causes—the likelihood of the other parent variables decreases. For instance, if sprinkler and rain were independent variables, if we observe that the sprinkler is "On", we can infer it is the most likely cause of the garden being wet.

2. *Predictive reasoning*: This type of reasoning entails discovering the effect of an observation. For instance, observing that the sprinkler is "On", we can infer that the garden is most likely wet, as shown in Figure 20. In Figure 20, when

we observe that the sprinkler is “On”, the probability that the garden is wet increases to 0.93 (the prior was 0.77, as shown in Figure 19).

4.5.2 Intervention Reasoning

The second level of the ladder of causation entails predicting the effects of interventions [75], [76], [107]. Intervention reasoning differs from observation reasoning since it evaluates the effects of an intended action, whereas observation reasoning observes the effect of an action. The former is done by intervening on a variable (see Figure 21), and the latter is done by conditioning on a variable (see Figure 20). Intervening on a variable entails fixing its value by making the variable independent of its causes via graph surgery, i.e., removing all arcs entering the intervened variable. For instance, as shown in Figure 21, the intervened variable sprinkler is made independent of the variable season by removing the arcs from season to sprinkler. The do operator proposed by Pearl [75] is used in probability expressions to specify intervention reasoning. For instance, the probability that the garden is wet after seeing the sprinkler “On” is expressed as $\mathrm{P(Garden\ wet\ |\ Sprinkler\ =\ On)}$ whereas the probability that the garden is wet after turning on the sprinkler (i.e., performing an action) is expressed as $\mathrm{P(Garden\ wet\ |\ do\ (Sprinkler\ =\ On))}$.

Contrary to observation reasoning, intervention reasoning depends on the causal relationship among the variables. Without knowledge of causal relationships, the data used in observation reasoning cannot be used to answer intervention queries [76]. Also, intervention reasoning does not support diagnostic reasoning since the intervened variable is made independent of its causes.

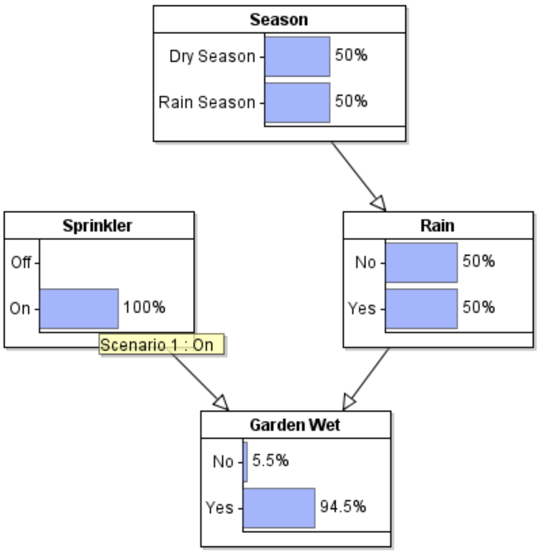


Figure 21 Garden BN after turning the sprinkler on

4.5.3 Counterfactual Reasoning

The third level of the ladder of causation entails imagining what would have happened if the observed events were different. Counterfactual reasoning is essential since "it allows us to learn from history and the experience of others" [75], [76], [107]. For instance, determining why some risk controls are effective on some systems can inform better risk controls for other systems.

Counterfactual reasoning combines observation and intervention reasoning; hence, it is at the top of the ladder of causation. It is implemented in BNs using the twin network method proposed by Balke and Pearl [109]. The twin network method uses two identical networks, one network represents the real world, and the other represents the counterfactual world. The two networks are connected by shared background variables u. The real world is modelled using observations, and the counterfactual world is modelled using interventions. The background variables are essential in the network since they share information learnt from the real world with the counterfactual world. As a result, predictions using the counterfactual world are performed under the same conditions as the real world, allowing us to compare the outcomes of both worlds accurately. Pearl suggests the following three steps for computing counterfactuals which are encoded in the twin network model [75], [76]:

1. ***Abduction***: Use the evidence e in the real world to update the information of the background variables, i.e., $P\ (u \mid e)$

2. ***Action***: Apply the *do*-operator to modify the model based on the counterfactual assumptions made.
3. ***Prediction***: Make predictions using the modified model and revised background information.

For example, suppose we observe that the sprinkler is on, and the garden is wet. In this case, we might wonder whether the garden would be wet if the sprinkler is off. We can answer this counterfactual question using the BN shown in Figure 22. In the real world, we enter our observations, and the BN uses this information to update the information about the *season* (background variable), which is shared with the counterfactual world. In the counterfactual world, we intervene on the sprinkler setting its value to "Off" to compute whether the garden will be wet. According to the BN shown in Figure 22, there is a 30% chance that the garden will be wet if the sprinkler is off.

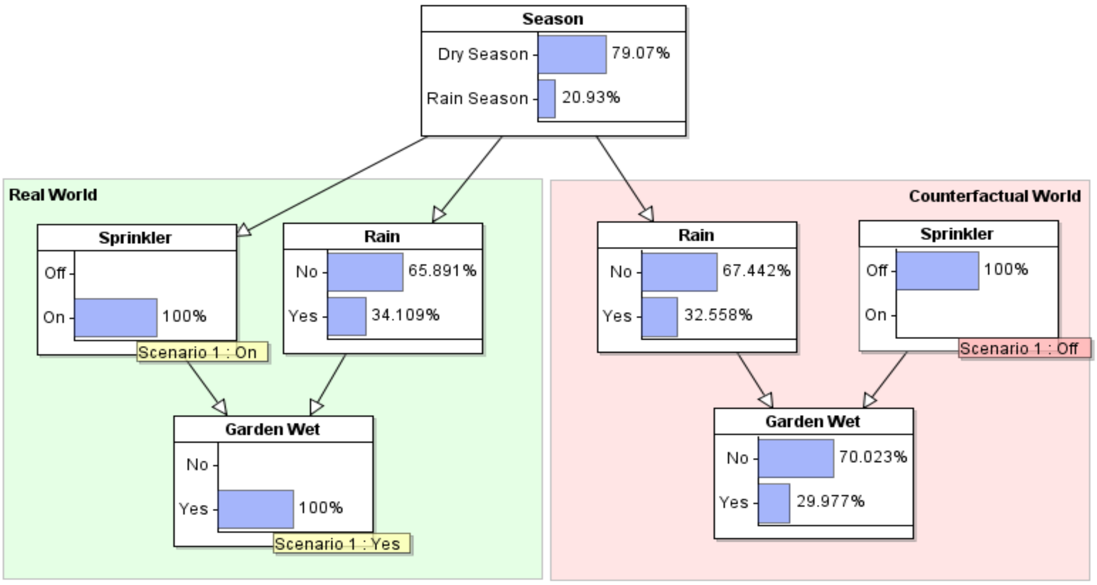


Figure 22 Garden BN counterfactual reasoning

4.6 Chapter Summary

In this chapter, we introduced Bayesian networks. We described the methods used to build complex BNs and to perform inferences in BNs. Finally, we described the types of reasoning done using BNs. In the next chapter, we review the use of BNs in the safety domain.

Chapter 5 Review of the use of Bayesian Networks in the Safety Domain

In this chapter, a review of the use of BNs in the safety domain is presented. We review their applications in two areas relevant to the work presented in this thesis:

1. Safety, reliability and risk assessments
2. Model-to-model transformation/mapping approaches

The material presented in this chapter informs the BN development method presented in Chapter 6 and applied in Chapters 7 and 8.

5.1 Safety, Reliability and Risk Assessments

Safety-critical systems are used in many products and industries, such as maritime, railway and aviation industries. Despite the benefits these systems offer, they pose a serious risk to our health and safety when they fail. As a result, during production and post-production, the safety, reliability, and risk of these systems must be continuously assessed and judged acceptable by manufacturers and safety regulators. Commonly used approaches for assessing the safety, reliability, and risk of systems include Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA) and Bow-tie models (see Chapter 3 for a review of these risk analysis methods). However, these approaches have several limitations, such as the inability to handle multi-state variables, uncertainties in system behaviour and failure data, and dependencies among system components (as discussed in Chapter 1). These limitations are resolved using Bayesian networks. BNs are suitable for this task since they are a robust, rigorous, normative method for modelling uncertainty and causality. They have been used in several industries to assess the safety, reliability, and risk of systems [110], [111]. A review of their applications in energy, defence, railway, aviation, maritime, medical, software and product safety industries relevant to the work described in this thesis is undertaken.

5.1.1 Energy Industry

Lee et al. [112] used BNs for the probabilistic risk assessment of nuclear waste disposal. They noted that for events in a controlled environment such as a nuclear power station, risk could be easily assessed using traditional risk analysis methods since relevant data is available. However, traditional risk analysis methods are not applicable to rare events such as nuclear waste disposal, whose data is limited and often uncertain. Therefore, the authors proposed using BNs to assess the risk associated with nuclear waste disposal. Since Bayesian networks are a rigorous normative method for modelling uncertainty and causality, it is clear why the authors used this approach for assessing the risk associated with nuclear waste disposal. This research demonstrates the use of BNs for performing risk assessment with uncertain data, which is relevant to the work done in this thesis.

Wu et al. [113] used BNs for fault detection and diagnosis (FDD) in nuclear power plants. Their experiments show that BNs can perform FDD with incomplete data and multi-sensor information at a nuclear power plant. Ur et al. [114] used BNs for reliability analysis of nuclear instrumentation and control systems. Chojnacki and Audouin [115] developed an expert system based on BNs for fire safety analysis in the nuclear area.

Bayesian networks have also been used for the reliability assessment of power systems. Yu et al. [116] used BNs for the reliability assessment of power systems. They conclude that BNs enhance reliability assessment since they can compute posterior probabilities, handle uncertainty and manage dependency among relevant variables. Daemi et al. [117] developed a BN for the reliability assessment of composite power systems. The authors used the BN to perform probabilistic assessments, such as the criticality ranking of system components. Other applications and review of BNs for the reliability and risk assessment of power systems include Yongli et al.[118], Jie et al. [119], Weber et al. [110], Kabir et al. [111] and Sykora et al. [120].

5.1.2 Defence Industry

Neil et al. [121] used BNs to predict the reliability of military vehicles. They noted that the reliability of military vehicles is dependent on both objective and subjective information. Objective information includes statistical data such as failure rate obtained from trials and use. Subjective information includes information about the manufacturer’s reputation, design and process information. However, traditional methods used for reliability evaluations of military vehicles cannot incorporate subjective information; hence the authors proposed using BNs. The authors noted that BNs could improve reliability predictions of military vehicles since it can be done earlier in the life cycle using design and process information.

In their proposed method, historical data about similar systems are used to learn the failure rate distribution of the system. The failure rate distribution is then revised using operational data obtained from tests and design and process information. An example of a BN used to estimate the quality of the design process and revise the reliability estimation of a military vehicle is shown in Figure 23.

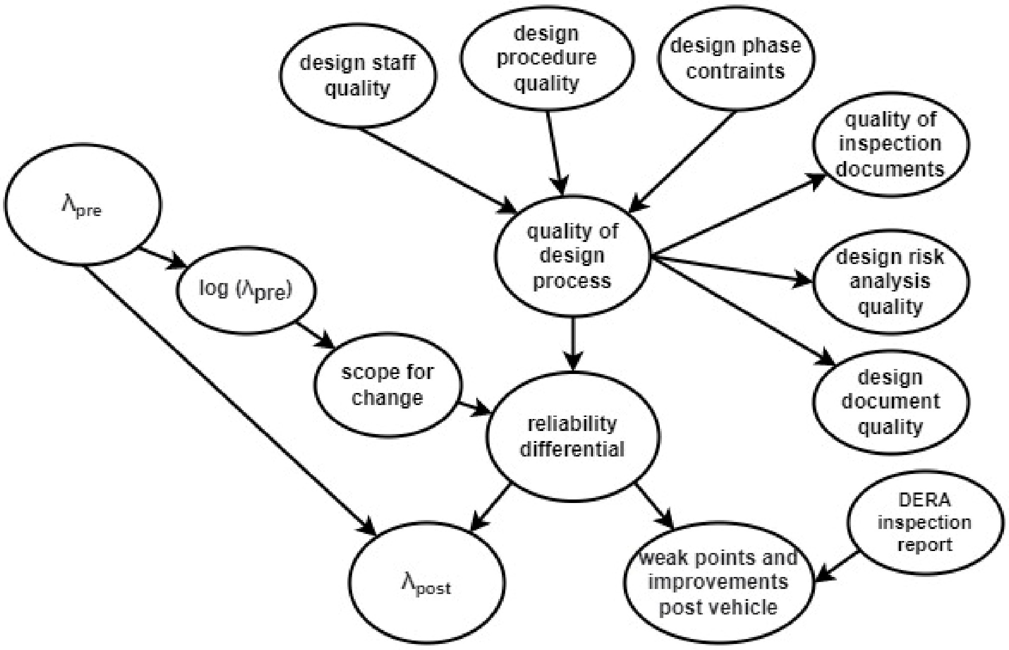


Figure 23 Example of BN used to predict the design process quality and revise the failure rate of military vehicles

In this BN example, the quality of the design process is dependent on measurable factors and indicators such as design staff quality and design document quality. Once the quality of the design process is determined, it is then used to revise the prior failure rate distribution λ_{pre}. The revised failure rate distribution is λ_{post}. One key finding of this work is the use of historical data from similar systems, manufacturer's reputation, and design and process information to estimate the reliability of military vehicles. This is very valuable and is applicable to the work presented in this thesis.

Banghart et al. [122] used BNs to assess the risk of an EA-6B aircraft. Their research concluded that BNs are suitable for assessing the risk of potential degraders to readiness, such as high failure systems and excessive repair times. Crispim et al. [123]

used BNs to assess the risk associated with military shipbuilding projects. They concluded that BNs are suitable for this task since they can assess risk with limited data, especially in the early stages of the project, handle the interdependencies among risk events and simulate the effect of risk mitigation methods. Other applications and review of BNs for reliability and risk assessment in the defence industry include Weber et al. [110], Kabir et al. [111] and Hudson et al. [124].

5.1.3 Railway Industry

Marsh and Bearfield [125] used BNs to model accident causation in the UK railway industry. They noted that events such as Signals Passed at Danger (SPADs), usually attributed to human error, have other causes, such as organisational factors. However, traditional risk analysis methods such as event trees do not include organisational factors as part of the sequence of events leading to the accident (since they influence accidents indirectly). As a result, the scope of the accident investigation is limited. Given the limitations of traditional risk analysis methods, the authors proposed using BNs to model operational accidents. Figure 24 shows an example of a proposed BN model incorporating organisational factors to estimate the risk levels of SPAD accidents. In this BN example, the event nodes are shaded, and the factors that influence the event nodes and the occurrence of the SPAD scenario are unshaded.

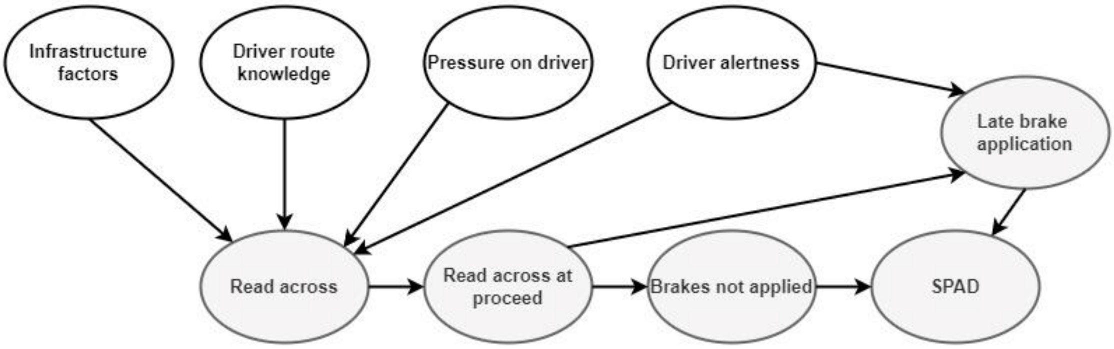


Figure 24 BN for SPAD Scenario: Read Across an Adjacent Signal

The key aspect of the work that is applicable to the work described in this thesis is the use of organisational factors to produce more reliable risk estimates.

Complementing their previous work in the railway industry, Marsh and Bearfield [20] proposed a systematic method of translating event trees into BNs described in Section 5.2.2. In [63] the authors also translated fault trees to BNs based on the work by

Bobbio et al. [18] described in Section 5.2.1. The resulting BN was used to model the risk at different locations on a railway network for derailment accidents.

One key finding of the work is that event and fault trees can be easily translated to BNs to produce more accurate risk estimates. Though translating event and fault trees to BNs for risk analysis is not the focus of this thesis, the work provides useful insights on integrating and extending traditional methods using BNs. Other applications and review of BNs for risk assessment in the railway industry include Castillo et al. [126], Leśniak et al. [127], Kabir et al. [111] and Huang et al. [128].

5.1.4 Aviation Industry

In the early 2000s, the Federal Aviation Administration (FAA), National Aeronautics and Space Administration (NASA) and Luxhoj and Coit [129] adopted BNs as the basis for their aviation system risk model (ASRM). ASRM uses BN modelling to identify and understand the causal relationships among the factors that cause aviation accidents and to assess the risk of new aviation safety products and system failures [129][130]. For instance, Luxhoj and Coit [129] used the ASRM method to model aircraft accidents. The authors developed BNs using case studies and expert knowledge. For example, relevant variables and their causal interactions were identified using expert knowledge and case study data such as accident reports. Conditional probability tables (CPTs) were defined using available data and expert knowledge. Expert knowledge was essential for BN development since aviation accidents are rare events. The authors' study results indicate that BNs are a suitable method for probability risk modelling of aviation accidents. A key aspect of the work related to the work described in this thesis is identifying relevant variables and their causal interactions using expert knowledge and data such as accident reports.

Neil et al. [131] used BNs to model an air traffic control environment to estimate safety and operational risks. The authors used a barrier model describing the sequence of events that led to an aircraft collision to identify the relevant variables and causal interactions for the BN. Once all relevant variables were identified, the authors used the idiom-based approach to build the BN. This approach entails organising variables into small BN fragments and connecting these fragments to build the BN (see Section 4.3.1.1). Their results show that BNs can be used to model safety and operational risks.

A key aspect of the work related to the work described in this thesis is organising relevant variables into small BN fragments to build BNs.

Washington et al. [132] used BNs for system safety assessment of remote pilot aircraft systems. The authors' interest in using BNs stems from the ability of BNs to handle uncertainties in the system safety assessment process. Their results show that BNs can be used for safety assessments of novel or complex systems with uncertainty in system behaviour or available data.

Other applications of BNs for safety and risk assessment in the aviation industry include Shih et al. [133], Zhang et al. [134], Wang et al. [135], Chen and Huang [136], and Ale et al. [137].

5.1.5 Maritime Industry

Hanninen and Kujala [138] and Fan et al. [139] used BNs to investigate the impact of human factors on the risk of ship collisions. Their research shows that BNs can inform appropriate risk mitigation measures, as they provide valuable information on factors that contribute to ship collisions. Trucco et al. [140] used BNs to assess the risk of the maritime transport system taking into account human and organisational factors. Montewka et al. [141] also used a BN to assess the risk of maritime transportation systems.

Zhang et al. [142] used a BN and a formal safety assessment to assess the navigational risk of the Yangtze River. In their proposed BN shown in Figure 25, they combined the consequence of the accident and the probability of the accident to estimate the navigational risk. They concluded that using BNs allowed them to identify the factors that have the largest influence on navigational risk.

A key aspect of the work discussed in this section relevant to the work described in this thesis is incorporating organisational and human factors in risk estimation. Other applications and review of BNs in the maritime industry include Weber et al. [110] and Kabir et al. [111].

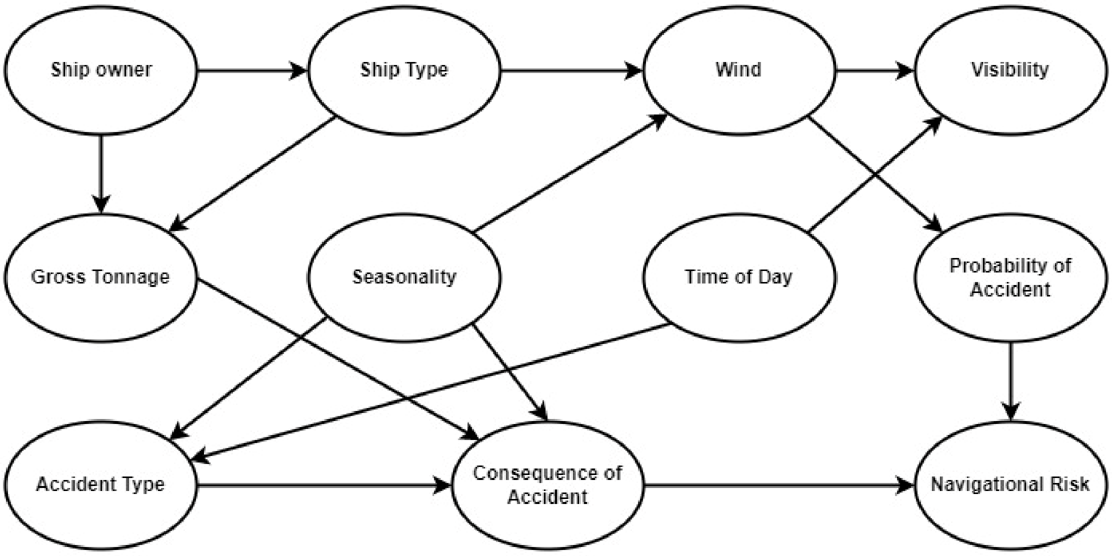


Figure 25 Navigational Risk BN

5.1.6 Medical Industry

This section is adapted from Publication 4 [25], previously published by Arxiv.org.

Haddad et al. [143] developed a BN to predict fatigue fracture of a cardiac lead. They validated the results of the BN by comparing it to the field performance data for cardiac leads available on the market. Medina et al. [144] developed a BN to identify the critical factors that affect the decision time for the Food and Drug Administration (FDA) to approve a medical device for market release. Zhang et al. [145] developed a BN to detect faults associated with medical body sensors network that collects and uses physiological signs for patient health monitoring. Rieger et al. [146] proposed a Bayesian risk identification model (BRIM) to predict and reduce use error risk during the development of medical devices. Li et al. [147] used a dynamic BN to assess the risk of device failures and human errors in healthcare. Other applications and review of BNs in the medical industry include Kabir et al. [111], Kyrimi et al. [148], Lucas et al. [149] and McLachlan et al. [150].

A key aspect of the research discussed in this section relevant to the work in this thesis is the use of BNs to assess the risk of failures and injuries associated with medical devices. However, all the proposed BNs are tailored and are not generalisable. Hence, a generic BN for medical device risk assessment is needed to assess the risk of different types of medical devices. In Chapter 7, we present a generic BN for medical device risk management.

5.1.7 Software Industry

Fenton et al. [151]–[154] used BNs to predict defects and estimate the reliability of complex software systems. For instance, they created the AID tool (powered by BNs) to predict software defects in consumer products for Philips. The authors built software reliability models using object-oriented Bayesian networks (OOBNs), empirical data and expert knowledge. The OOBNs approach [155] entails creating predefined BN fragments called *classes* and using instances of these *classes* called *risk objects* to build the BN. The authors created *classes* for activities done during each life cycle phase. For instance, the Rework class shown in Figure 26 was created to model rework activities. Instances of the different classes were then linked to create a full lifecycle BN model.

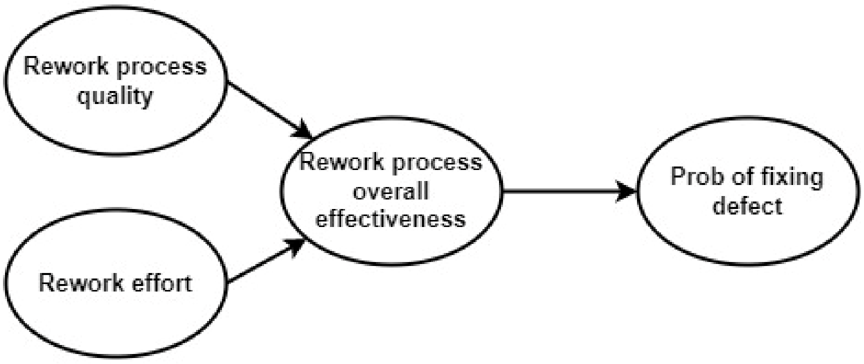


Figure 26 Rework BN Fragment

Other applications and review of BNs in the software industry include Weber et al. [110], Kabir et al. [111], Helminen et al.[156], [157], Bai [158] and Roshandel et al. [159]. For instance, Bai [158] used BNs to predict software reliability with an operational profile. Roshandel et al. [159] used BNs to predict software reliability at the architectural level.

5.1.8 Product Safety Industry

This section is adapted from Publication 2 [15], previously published by the Journal of Safety Research.

Suh [160] developed a product risk assessment system using a BN to assess product risk based on injury information from the Korea Consumer Agency. They evaluated 33 children’s products and compared the results with RAPEX. Berchialla et al. [161] used a BN to estimate the risk of ingestion, inhalation, and insertion of consumer products in children aged 0–14. Their proposed BN, shown in Figure 27, was used to identify potential injury scenarios that can lead to hospitalisation. The BN structure was learnt using the K2 algorithm with data from 672 cases and validated using 10-fold cross-validation. Their results show that the removal technique for ingested foreign bodies had the greatest impact on the risk of hospitalisation. Also, the risk of hospitalisation is reduced with adult supervision. The authors noted that BNs are suitable for quantitative risk assessment since the causal relationships among the variables are explicit. Also, the ability to perform diagnostic and predictive reasoning in BNs allows factors affecting the risk of hospitalisation to be easily identified.

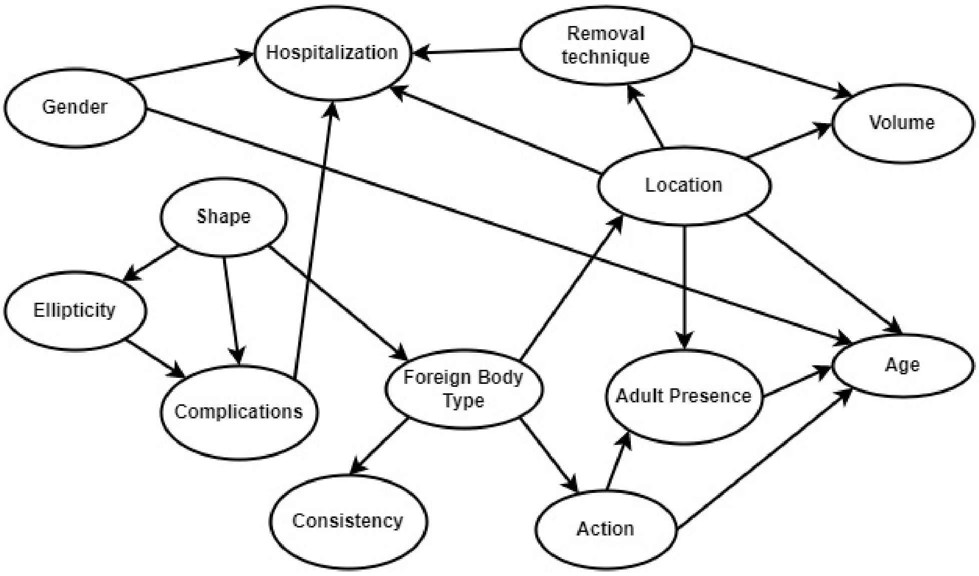


Figure 27 BN for quantitative risk assessment of foreign body injuries in children

Berchialla et al. [162] also compared the BN approach to other quantitative risk assessment methods, such as neural networks, classification trees, and logistic models. Their results indicate that BNs are the best method for assessing safety risk because they are easier to interpret and provide accurate predictions.

A key observation of the work reviewed in this section relevant to the work in this thesis is the limited use of BNs for product safety risk assessment. This may be due to the lack of a systematic approach for building BNs for different product safety cases. For instance, the process used for building the two published BNs in this domain is ad hoc and presents little or no opportunity for repeatability and standardisation. Berchialla et al. [161] used automated techniques to learn BN structure and parameters, and Suh [160] did not provide any details on how the structure of the BN was determined. For many product safety cases, automated learning may not be feasible or practical, and the structure and parameters must be elicited from experts and literature. Also, Berchialla et al. [161] BN cannot be used to assess the risk of a wide range of consumer products since its structure and parameters are not applicable. Though Suh [160] used a BN to assess the risk of different children's products, it is unclear if this BN is generalizable since the authors did not provide a causal diagram that explicitly describes the structure of the BN. For this reason, a generic BN is needed for product safety risk assessment and a standard method for building such a BN that is applicable to a wide range of products and safety cases. In Chapter 6, we present a generic method for building BNs for product safety risk management and in Chapter 8 we present a generic BN for consumer product risk assessment.

An overview of BN applications in the safety domain is shown in Table 7.

Table 7 Overview of BN applications in the safety domain

Industries	**Contributions**
Energy	Lee et al. [112], Wu et al. [113], Ur et al. [114], Chojnacki and Audouin [115], Yu et al. [116], Daemi et al. [117], Yongli et al.[118], Jie et al. [119], Sykora et al. [120], Weber et al. [110], Kabir et al. [111]
Defence	Neil et al. [121], Banghart et al. [122], Crispim et al. [123], Weber et al. [110], Kabir et al. [111], Hudson et al., [124]
Railway	Marsh and Bearfield [20], [63], [125] Castillo et al. [126], Leśniak et al. [127], Huang et al. [128], Kabir et al. [111]
Aviation	Netjasov et al. [130], Luxhoj and Coit [129], Neil et al. [131], Washington et al. [132], Chen and Huang [136], Ale et al. [137], Shih et al. [133], Zhang et al. [134] Wang et al. [135]
Maritime	Hanninen and Kujala [138], Fan et al. [139], Trucco et al. [140], Montewka et al. [141], Zhang et al. [142], Weber et al. [110], Kabir et al. [111]
Medical	Haddad et al. [143], Medina et al. [144], Zhang et al. [145], Rieger et al. [146], Li et al. [147], Kyrimi et al. [148], Lucas et al. [149], McLachlan et al. [150], Kabir et al. [111]
Software	Fenton et al. [151]–[154], Bai [158], Roshandel et al. [159] Weber et al. [110], Kabir et al. [111], Helminen et al.[156], [157]
Product Safety	Suh [160], Berchialla et al. [161], Berchialla et al. [162]

5.2 Model-to-model Transformation / Mapping Approaches

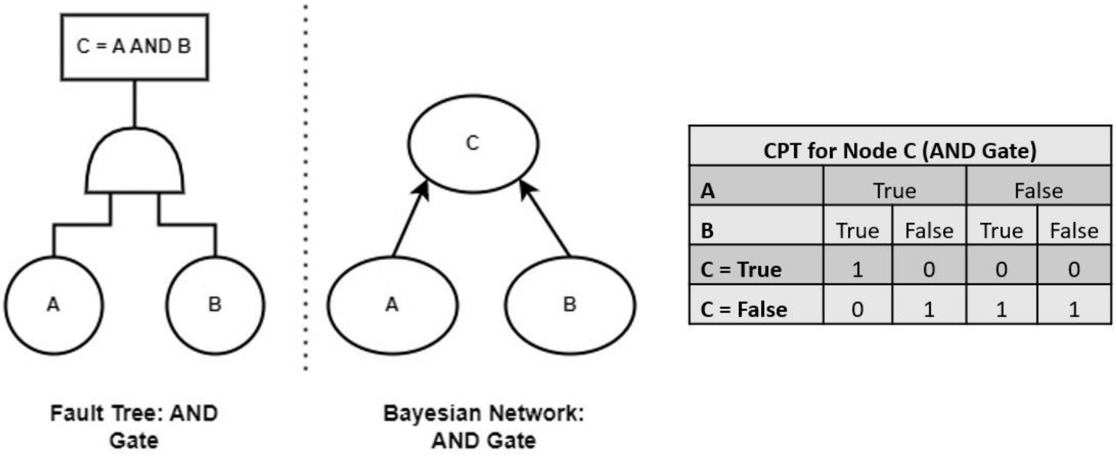
BNs have been used extensively as a model-to-model transformation/mapping approach in the safety domain. Several mapping approaches have been proposed to extend the functionality of commonly used risk analysis tools such as fault trees. In the following subsections, we review these approaches since they complement the work described in this thesis.

5.2.1 Translating Fault Trees into BNs

Fault Trees (FTs) (see Section 3.3) have been used extensively in the safety domain for modelling the reliability of systems [64]. However, despite their widespread use, they have limitations, such as handling multi-state variables (see Section 1.3). Given the limitations of FTs, Bobbio et al. [18] proposed a pioneering method for translating any fault tree into a BN. The authors noted that BNs resolve the limitations associated with FTs and extend their functionality by handling multi-state variables, sequence-dependent failures and common cause failures. The proposed method for translating FTs to BNs consists of the following steps:

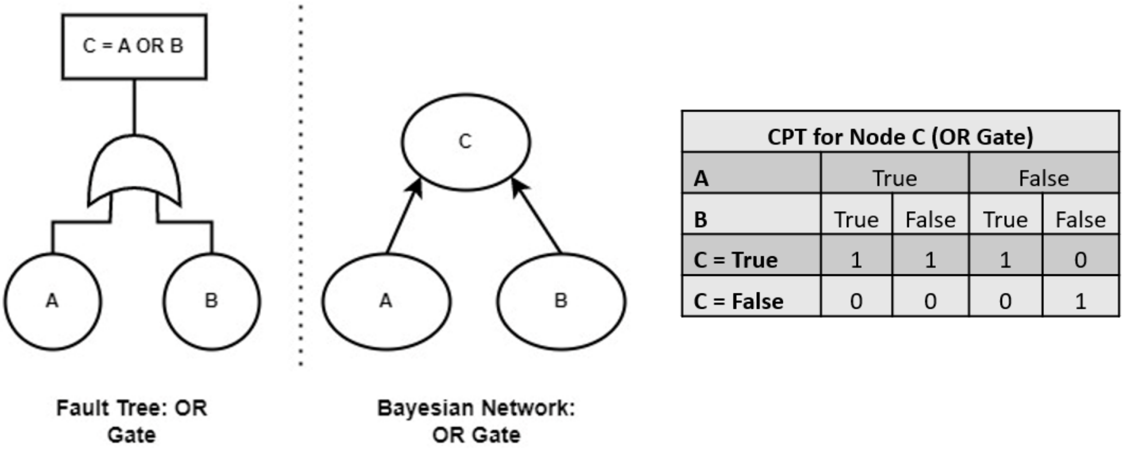
1. Create a root node in the BN for each basic event in the FT.
2. Assign the probabilities of the basic events in the FT to the equivalent root nodes in the BN.
3. For each logic gate in the FT, create a logic gate node in the BN.
4. Connect the logic gate nodes in the BN as they are connected in the FT.
5. Assign the equivalent conditional probabilities of the logic gates in FT to the logic gate nodes in BN.

Figure 28 and Figure 29 show the proposed method applied to fault trees AND and OR gates, respectively.



CPT for Node C (AND Gate)				
A	True		False	
B	True	False	True	False
C = True	1	0	0	0
C = False	0	1	1	1

Figure 28 Fault Tree AND Gate and BN Equivalent



CPT for Node C (OR Gate)				
A	True		False	
B	True	False	True	False
C = True	1	1	1	0
C = False	0	0	0	1

Figure 29 Fault Tree OR Gate and BN Equivalent

This research shows the ease with which fault trees can be translated into BNs. It also illustrates how BNs can be used to complement and extend the functionality of commonly used risk analysis methods. Other research illustrating the conversion of FT to BNs includes Abimola et al. [163] Castillo et al. [164] and Mahadevan et al. [165].

5.2.2 Translating Event Trees into BNs

In the safety domain, event trees (ET) (see Section 3.4) are used to analyse the sequence of events that can lead to accidents in a system [13], [20]. However, ET cannot explicitly represent the state of the system and its environment and how these affect the sequence of events [20]. Also, ET cannot model events that are not dependent on the hazard but influenced by other factors [13]. Given these limitations, Bearfield and Marsh [20] proposed using BNs to extend the functionality of ET. They proposed a pioneering method to translate any ET to a BN. Their model to model transformation approach is described using a generic BN representation of an event tree shown in Figure 30, accompanied by rules for linking event nodes to event nodes and event nodes to the consequence node.

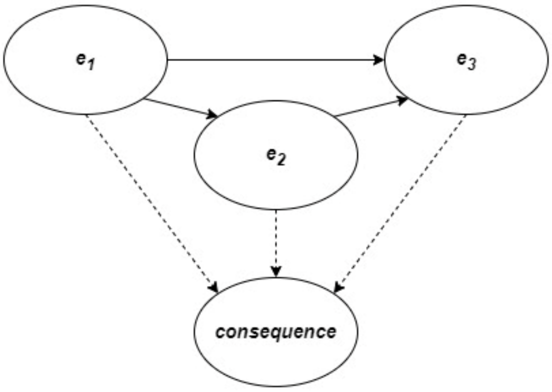


Figure 30 Generic BN representation of an event tree

In Figure 30, nodes e_1, e_2, and e_3 represent the events. Events are connected to the consequence node using *consequence arcs* (represented by the dotted lines). Events are connected to other events using causal arcs (represented by the solid lines). The number of nodes used in the BN is dependent on the number of events in the ET. The following rules are used for linking event nodes to event nodes and event nodes to a consequence node:

1. An event node is connected to the consequence node only if the event node influences the probabilities of the states of the consequence node. For example, in the event tree *A* shown in Figure 31, the consequences *C1* and *C2* are determined by the combination of events e_1 and e_2 that have occurred; hence in the equivalent BN shown in Figure 32, these event nodes are the parents of the consequence node.

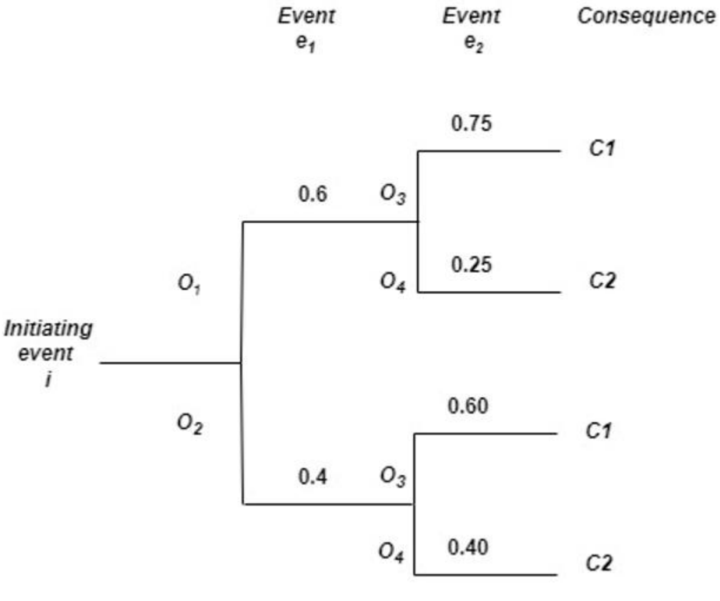
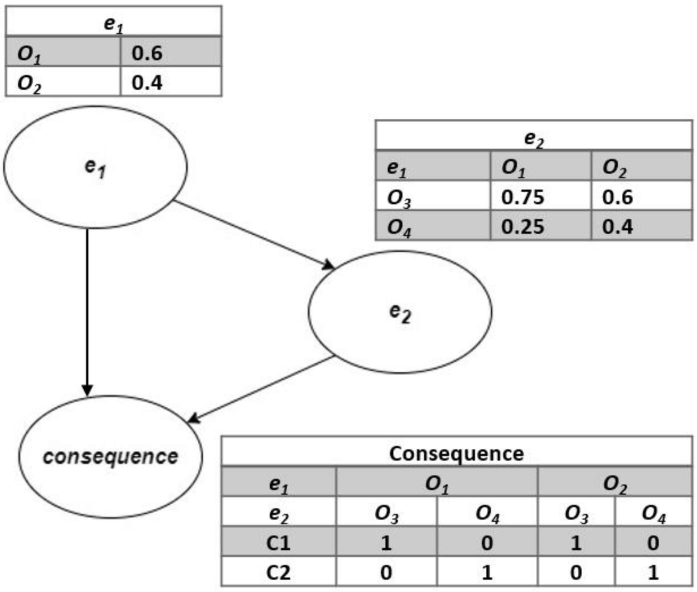


Figure 31 Event Tree A



e_1	
O_1	0.6
O_2	0.4

e_2		
e_1	O_1	O_2
O_3	0.75	0.6
O_4	0.25	0.4

Consequence				
e_1	O_1		O_2	
e_2	O_3	O_4	O_3	O_4
C1	1	0	1	0
C2	0	1	0	1

Figure 32 BN equivalent for Event Tree A

2. An event node *B* is connected to a previous event node *A* only if event node *B* is conditionally dependent on event node *A*. For example, in the event tree *B* shown in Figure 33, the outcome of event e_2 is not dependent on event e_1; hence the two events are conditionally independent. In the equivalent BN shown in Figure 34, there is no arc linking event e_1 and event e_2.

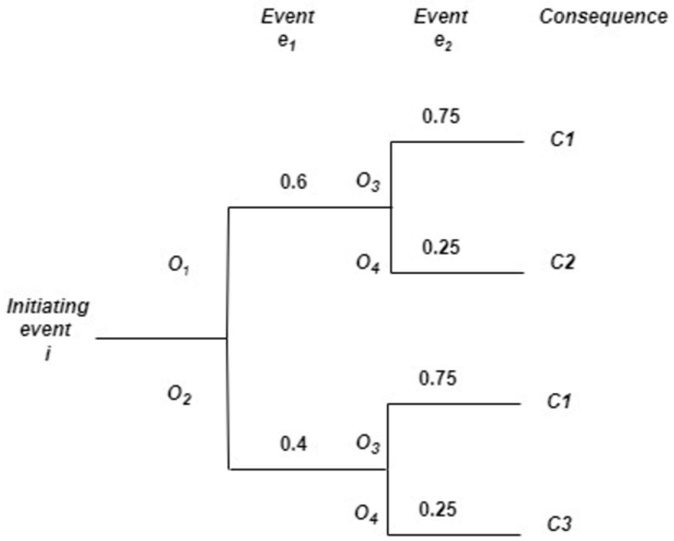
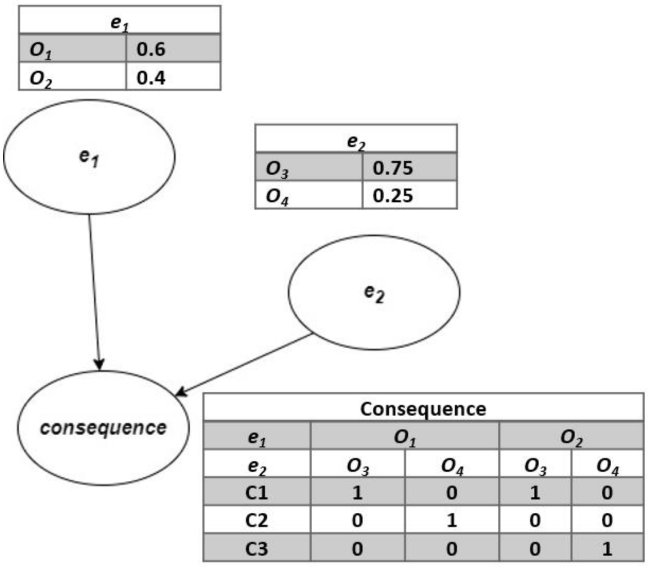


Figure 33 Event Tree B



e_1	
O_1	0.6
O_2	0.4

e_2	
O_3	0.75
O_4	0.25

Consequence				
e_1	O_1		O_2	
e_2	O_3	O_4	O_3	O_4
C1	1	0	1	0
C2	0	1	0	0
C3	0	0	0	1

Figure 34 BN equivalent for Event Tree B

Using a train derailment case study, the authors translate event trees used to analyse the consequences of a derailment into BNs. The BNs were used to calculate accident probabilities in different scenarios. This research shows the ease with which event trees can be translated into BNs. Similar to Bobbio et al. [18] work discussed in the previous section, it shows how BNs can be used to complement and extend the functionality of commonly used risk analysis methods.

5.2.3 Translating Bow-tie Models into BNs

Khakzad et al. [166] translate a bow-tie (BT) model into a BN for the safety analysis of process systems. Since a bow-tie model composes a fault tree and an event tree, the authors used the methods proposed by Bobbio et al. [18] and Bearfield and Marsh [20] to translate the fault tree and event tree components, respectively, to a BN. They tested these approaches by translating a simple bow-tie model for a gasoline release accident shown in Figure 35a into a BN model shown in Figure 35b. Given the results of their experiment, they proposed an algorithm for mapping BT into BN, summarised in Figure 36. The authors then applied their proposed algorithm to a vapour ignition case study for verification. Their results indicate that a BT model can easily be translated to a BN for safety analysis.

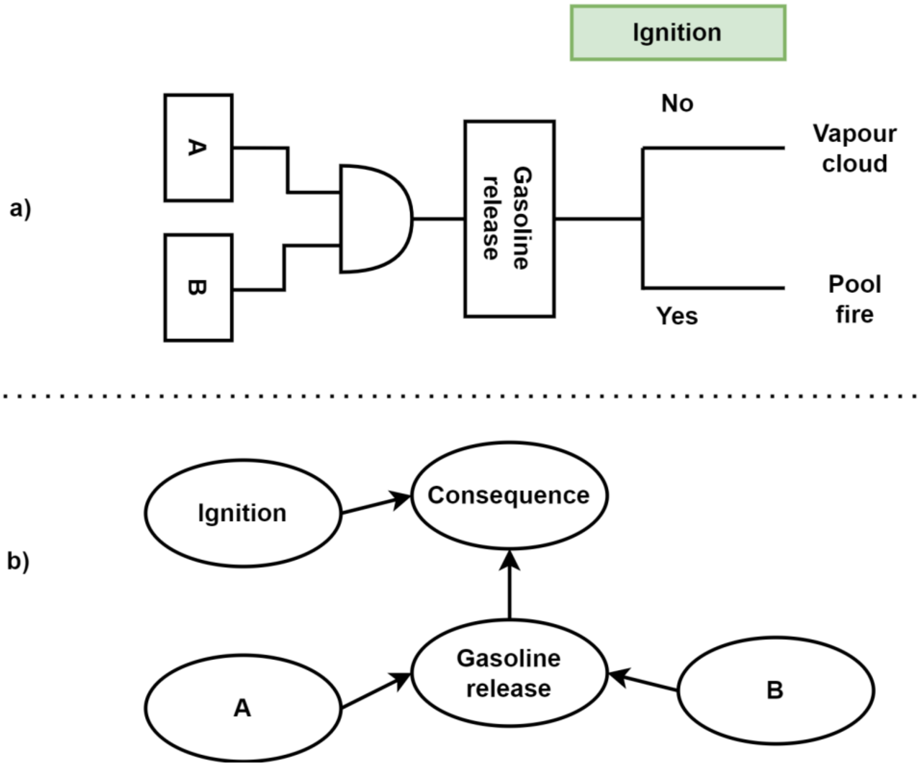


Figure 35(a) Bow-tie model example (b) BN Equivalent

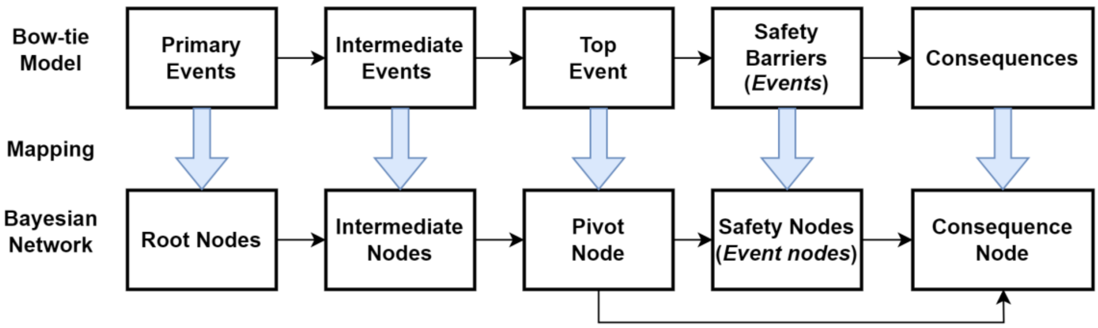


Figure 36 Bow-tie to BN mapping algorithm

An overview of BN mapping approaches in the safety domain is shown in Table 8.

Table 8 Overview of BN mapping approaches

Models	**BN Mapping Contributions**
Fault Tree	Bobbio et al. [18], Abimola et al. [163] Castillo et al. [164] and Mahadevan et al. [165]
Event Tree	Marsh and Bearfield [20]
Bow-tie	Khakzad et al. [166]

5.3 Promoting the use of BNs in the Product Safety domain

The literature review provides evidence that BNs are used to model many complex problems in the safety domain. However, despite their widespread use in this domain, their application in the product safety domain is limited (see Table 7). Their limited use may be due to the lack of explicit principled guidelines for building BNs for the many different product safety cases. For instance, the process used for building the two published BNs in this domain is ad hoc and presents little or no opportunity for repeatability and standardisation. Berchialla et al. [161] used automated techniques to learn BN structure and parameters, and Suh [160] did not provide any details on how the structure of the BN was determined. For many product safety cases, automated learning may not be feasible or practical, and the structure and parameters must be elicited from experts and literature. Although there are some established mapping and knowledge representation methods [18]–[20] to define BN structure and parameters, for many product safety cases, these methods may not be feasible since the safety risk is based on the interaction of hard factors (e.g., systems) and soft factors (e.g., users). In these situations, the BN must be developed using expert knowledge and literature. However, the literature lacks a systematic, repeatable method or guidelines for developing BNs for product safety risk management using expert knowledge and literature. This problem is tackled in the next chapter using the idiom-based approach proposed by Neil et al. [19].

Other challenges to the widespread use of BNs in the product safety domain include:

1. The lack of significant competence and understanding in Bayesian networks: Developing, validating, and using BNs can be challenging for non-experts.

2. The need for BN models to be able to stand up to scrutiny, such as civil or legal challenges in a post-accident scenario: To stand up to scrutiny, a BN model should be robust, transparent, based on accurate and reliable data, validated, and comply with relevant standards and laws.

3. Encouraging the use of the BNs, given that, unlike traditional methods, Bayesian approaches may not be explicitly referenced in safety risk and reliability standards.

4. Lack of methods for easy deployment to end users (discussed in Chapter 10).

5.4 Chapter Summary

In this chapter, the application of BNs in the safety domain is reviewed. The literature review revealed that despite the widespread use of BNs in the safety domain, their application is limited in the product safety area. Their limited use in this area may be due to several factors including the lack of explicit principled guidelines for modelling different product safety cases. Although there are some established methods for defining BN structure and parameters, some of these methods may not be feasible for many product safety cases, and the BN must be developed using expert knowledge and literature. Therefore, a systematic method or principled guidelines are needed to develop BNs specifically for the product safety domain.

In the next chapter, we present a novel approach for developing BNs for many different product safety cases based on causal idioms. We believe that these special types of idioms, called *product safety idioms,* can help promote the use of BNs in the product safety domain by simplifying the knowledge elicitation task. They also complement existing methods of BN development described in previous research.

Chapter 6 An idiom-based approach for Product Safety Risk Management

In this chapter, the *product safety idioms* for building product safety BNs are presented. These novel idioms are illustrated using product safety case examples. Hence this chapter supports Hypothesis 1 (it is possible to develop a generic method to build BNs for product safety risk management).

In Section 6.1, an overview of the product safety idioms is presented. In Section 6.2, idioms for risk analysis are presented, and idioms for risk evaluation are presented in Section 6.3. In Section 6.4, the process for building BNs using the idioms is described and in Section 6.5 the benefits of the idioms are discussed. The proposed idioms are applied and validated in the case study examples presented in Chapters 7 and 8. The material presented in this chapter has previously been presented in Publication 3 [24] published by Arxiv.org.

6.1 Product Safety Idioms Overview

In the safety risk domain, people make risk management decisions based on complex interrelated factors such as users, processes, and systems. The literature review (see Chapter 5) provides evidence that the application of BNs to safety risk management is not novel, but there is limited or no principled guidelines for developing BNs for product safety risk management using expert knowledge and literature.

A BN for product safety risk management should include all relevant variables affecting risk and follow the logical causal process of how systems lead to hazards and harm. When building BNs using knowledge elicitation techniques, the risk modeller recognises and uses logical causal patterns to connect elicited variables. Idioms represent generic logical causal patterns of uncertain reasoning that can be combined and reused to model complex problems [19], [88]. Since idioms follow the human reasoning process, they are the basis of our proposed method to build BNs for product safety risk management.

The underlying assumption of the idiom-based approach is that large complex problems can be decomposed into smaller manageable components or modules called *idioms*. Though Neil et al. [19] generic idioms (discussed in Section 4.3.1.1) are applicable in many domains, including safety, this chapter proposes new types of idioms called *product safety idioms*, specifically for building product safety BNs. These idioms are tailored to the requirements of the different phases of the risk assessment process, specifically risk analysis and risk evaluation. They are based on the logical causal relationship among the relevant variables used to estimate and evaluate risks associated with products (systems), such as hazards, injuries, risk controls, manufacturer's reputation and use information.

We believe that the product safety idioms can help promote the use of BNs in the product safety domain by simplifying the knowledge elicitation task. They provide a library of BN patterns for product safety risk management. The risk modeller maps elicited knowledge to suitable idioms to build practical BNs. While the proposed idioms are sufficiently generic to be applied to a wide range of product safety cases, they are not prescriptive or complete and should be considered as a guide for developing suitable idioms for product safety risk management using data and knowledge.

In this chapter, we base our discussion on the product safety idioms using two real-life product examples: a hammer (Brand: Chetak Tools, Model: 1402CKA01) [167] and a car engine (Brand: Ferrari, Model: F142, F149) [168]. These products were previously identified by national safety regulators in the EU as posing a risk of injury to users and were reported to Safety Gate. Safety Gate [169] is a system used to share information about dangerous non-food products among the national safety regulators in the EU. The real-life product examples and related injury scenarios are as follows:

1. **Hammer** (Brand: Chetak Tools, Model: 1402CKA01) [167]: "The hammer head has been made from unsuitable material, and the metal parts may detach and injure the person using the hammer or people nearby. The product does not comply with relevant European standard EN10083."

2. **Car Engine** (Brand: Ferrari, Model: F142, F149) [168]: "A possible crack in the crankshaft may lead to engine failure and might cause the engine to seize, which may lead to a road accident."

For additional information about the product examples, please see the risk reports in Appendix A. It is important to note that testing and injury information, such as the number of failures, are not included in the safety reports; thus, the product safety idioms are illustrated using hypothetical data.

There are no product safety idioms associated with the risk/hazard identification phase of the risk assessment process. The risk identification phase entails identifying the system, risks, hazards, hazardous situations and associated harm. Hence the information presented for the product safety examples is documented in the risk identification phase. This information is then used to identify variables that affect risk. The identified variables are then organised into idioms for risk analysis and evaluation.

6.2 Product Safety Idioms for Risk Analysis

The second stage of the risk assessment process is risk analysis (see Figure 1). Traditionally, given the information presented in the injury scenario during the risk/hazard identification stage for a particular system, the risk is computed as $P \times S$, where P is the probability of injury and S is the severity of the injury. However, this method of estimating risk has several limitations discussed in Section 1.3, which are resolved using BNs. In this section, we show how the information gathered during the risk/hazard identification stage can be organised into novel idioms to estimate the overall risk of a system. Estimating the risk of a system includes considering factors such as reliability, rework and reported injuries; hence the proposed idioms are classified based on their scope as follows:

1. *Reliability*: These idioms model the reliability of a system in terms of failure rate (i.e., probability of failure on demand and time to failure) using data collected during testing or operational field use.
2. *Rework or Maintenance*: These idioms model the probability of repairing identified faults of a system.
3. *Requirement*: These idioms predict whether the system complies with defined operational and safety requirements.
4. *Quality*: These idioms estimate the quality of a particular entity or process, such as manufacturing process quality, that may affect the overall reliability of a system.

5. *Failure, Hazard and Injury Occurrence*: These idioms model hazard or failure occurrence and related injuries for a system given relevant factors such as device use.

6. *Risk:* These idioms estimate the overall risk of a system.

6.2.1 Reliability Idioms

Assessing the reliability of a system is essential for estimating risk and informing risk control measures since failures and hazards pose a potential risk to our health and safety. The two primary reliability metrics for systems are the *probability of failure on demand* (PFD) and *time to failure* (TTF) [54]. The probability of failure on demand (PFD) relates to the reliability associated with a finite set of uses of the system. For instance, if the system is a car, we might be interested in the probability of failure for a given journey. In contrast, time to failure (TTF) relates to the reliability associated with a system operating in continuous time. For instance, for a car, we may also be interested in the number of miles it could drive before a failure occurs. For complex systems such as an aircraft, it is inevitable that we will need to consider both TTF and PFD measures to determine its overall reliability because some of its sub-systems, like the engine, require the TTF measure while others, like the landing gear system, require the PFD measure.

In Subsection 6.2.1.1, we describe idioms for modelling PFD, and in Subsection 6.2.1.2, we describe idioms for modelling TTF.

6.2.1.1 Idioms for Modelling Probability of Failure on Demand (PFD)

There are three idioms in this category:

1. Hazard or failure per demand idiom (generic)
2. Hazard or failure per demand with limited data idiom
3. Probability of an event with uncertain accuracy idiom

Please note that the proposed idioms for handling limited data and uncertain accuracy are situational; model experts may develop other idioms based on the type of censored data.

Hazard or Failure per Demand Idiom (Generic)

Once hazards and failures are identified during the risk/hazard identification stage, product testing (physical or simulation) is done to quantify and learn the ‘true’ reliability or safety of the product. During product testing, the product is used many times, and each observed failure or hazard is recorded, respectively. In this thesis, we define a *demand* as a measure of usage; for example, a washing machine is typically used on average 270 times per household per year in the UK. Some products, such as certain medical devices, e.g., syringes, are intended to be only used once, i.e., single-use devices. Given sufficient failure data for a system collected during testing (or operational use), we can learn an estimate of the ‘true’ probability of hazard or failure per demand as a probability distribution. The more demands we observe, the smaller the variance (uncertainty) we have about this distribution.

The generic *hazard or failure per demand idiom* (see Figure 37) models the probability distribution of the hazard or failure per demand based on the number of hazards or failures observed during a set of demands (trials). This idiom uses a Binomial distribution for the number of observed hazards or failures since each demand can be considered a Bernoulli trial, with either success or failure as a result (see Table 9). In situations where there are no prior data for the ‘probability of the hazard or failure per demand’ node, we use an ‘ignorant’ uniform prior. For instance, assuming a uniform prior for the hammer example (see Section 6.1), if we observe the hammer head detaching (hazard) 10 times in 1000 demands during testing, we can use the idiom to estimate the reliability of the hammer as a probability distribution. In Figure 38, the idiom estimates that the mean probability of the hammer head detaching per demand is 0.01 with a variance of 1.11E-5.

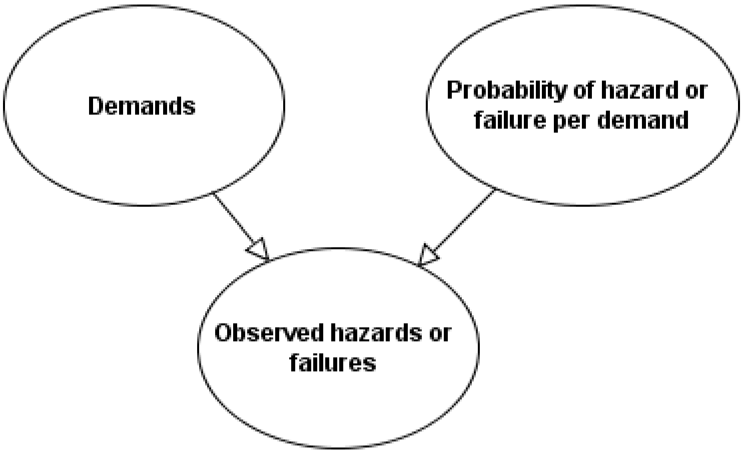

Demands
Probability of hazard or failure per demand
Observed hazards or failures

Figure 37 Hazard or failure per demand idiom (generic)

Table 9 NPTs for nodes in the Hazard or failure per demand idiom

Node Name	NPT
Observed hazards or failures	Binomial (*n*, *p*), where *n* = demands and *p* = probability of hazard or failure per demand
Demands	Uniform (0, 1E9)
Probability of hazard or failure per demand	Uniform (0,1)

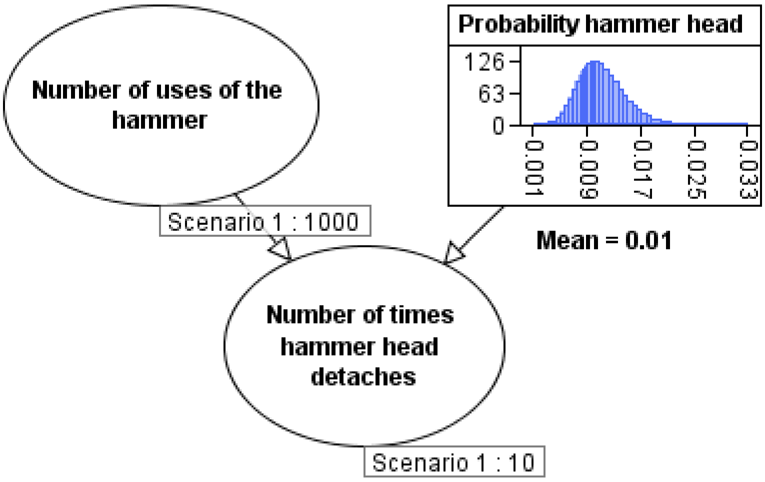


Figure 38 Hazard or failure per demand idiom instance

Hazard or Failure per Demand with Limited Data Idiom

For some systems, it will neither be feasible nor possible to obtain sufficient data from testing to estimate their ‘true’ reliability. In these situations, the hazard or failure per demand idiom can be extended to incorporate testing data from previous similar systems (if available) to estimate the ‘true’ reliability or safety of the system.

The *hazard or failure per demand with limited data idiom* is shown in Figure 39, and instances are shown in Figure 40 and Figure 41, respectively. This idiom consists of two components: the first component models the PFD of the current system, and the second component models the PFD of the previous system. The results of both components are combined using a weighted formula shown in Equation 8 to determine the overall PFD for the current system:

Equation 8:

$$\theta_{Current\ system\ overall} = r \times \theta_{Previous\ system} + (1 - r) \times \theta_{Current\ system}$$

Where $\theta_{Previous\ system}$ represents the PFD learned from the previous system, $\theta_{Current\ system}$ represents the PFD learned from the current system, $\theta_{Current\ system\ overall}$ represents overall PFD for the current system, and r is a probability that represents the relative weight given to PFD from the previous system versus the current system.

Imagine that no testing data is available for the current system. In that case, the idiom can estimate the reliability using only testing data from a previous similar system, as shown in Figure 40. In this example, the idiom estimates the reliability of the hammer (mean PFD is 0.125 with a variance of 8.7E-5) using testing data from a previous similar hammer (200 failures in 2000 demands); hence $r = 1\ or\ 100\%$. Also in this example, we assume there were “minor differences” between the hammers and their testing. In situations with limited testing data for the hammer, as shown in Figure 41, the idiom can combine limited testing data for the hammer (0 hazards or failures in 500 demands in this example) with testing data from the previous similar hammer to provide a reasonable estimate for the PFD of the hammer. In this example, we assume that we rely on 70% of the previous similar hammer data to estimate the overall PFD of the hammer. The idiom estimates that the mean probability of hammer head detaching (hazard) per demand is 0.09 with a variance of 8.7E-5. Please note that the

NPT values for the node ‘PFD adjusted for similarity’ (see Table 10) can be adapted given the product.

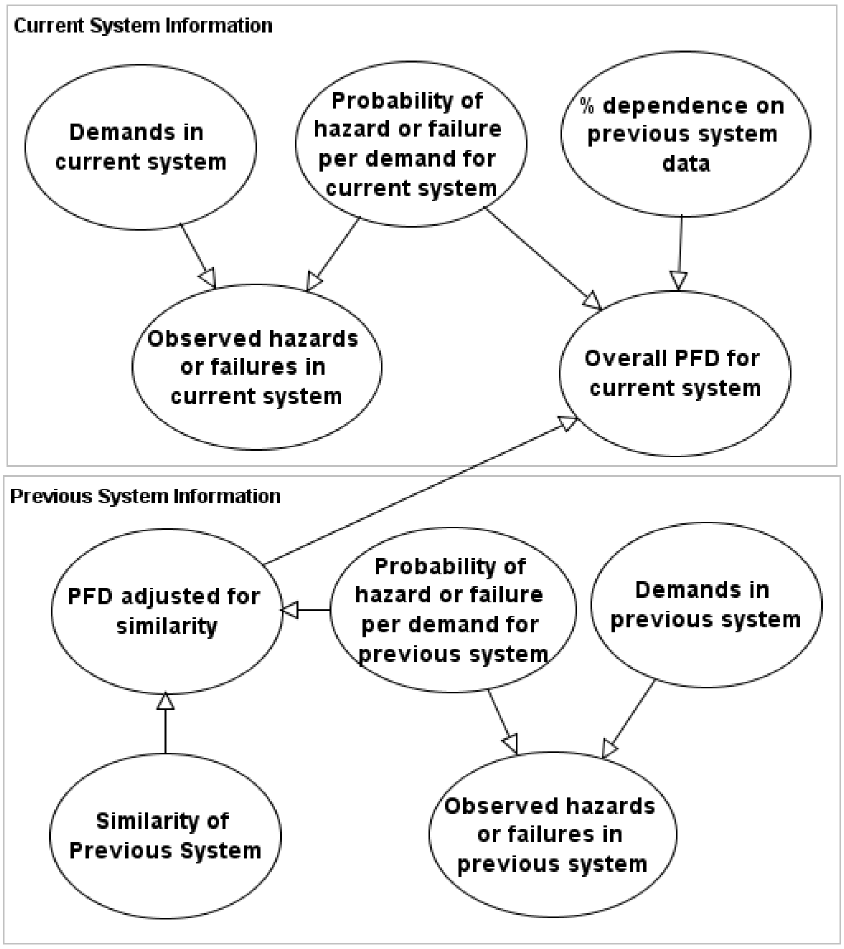

Current System Information
Demands in current system
Probability of hazard or failure per demand for current system
% dependence on previous system data
Observed hazards or failures in current system
Overall PFD for current system
Previous System Information
PFD adjusted for similarity
Probability of hazard or failure per demand for previous system
Demands in previous system
Similarity of Previous System
Observed hazards or failures in previous system

Figure 39 Hazard or failure per demand with limited data idiom

Table 10 NPT for the node *PFD adjusted for similarity*

Parent (Similarity of previous system) states	**Probability of hazard per demand**
Similar	Normal (*pfd*, 1E-4), where *pfd* = probability of hazard per demand for the previous system
Minor differences	Normal (*pfd* × 1.25, 1E-4)
Major differences	Normal (*pfd* × 2, 1E-4)

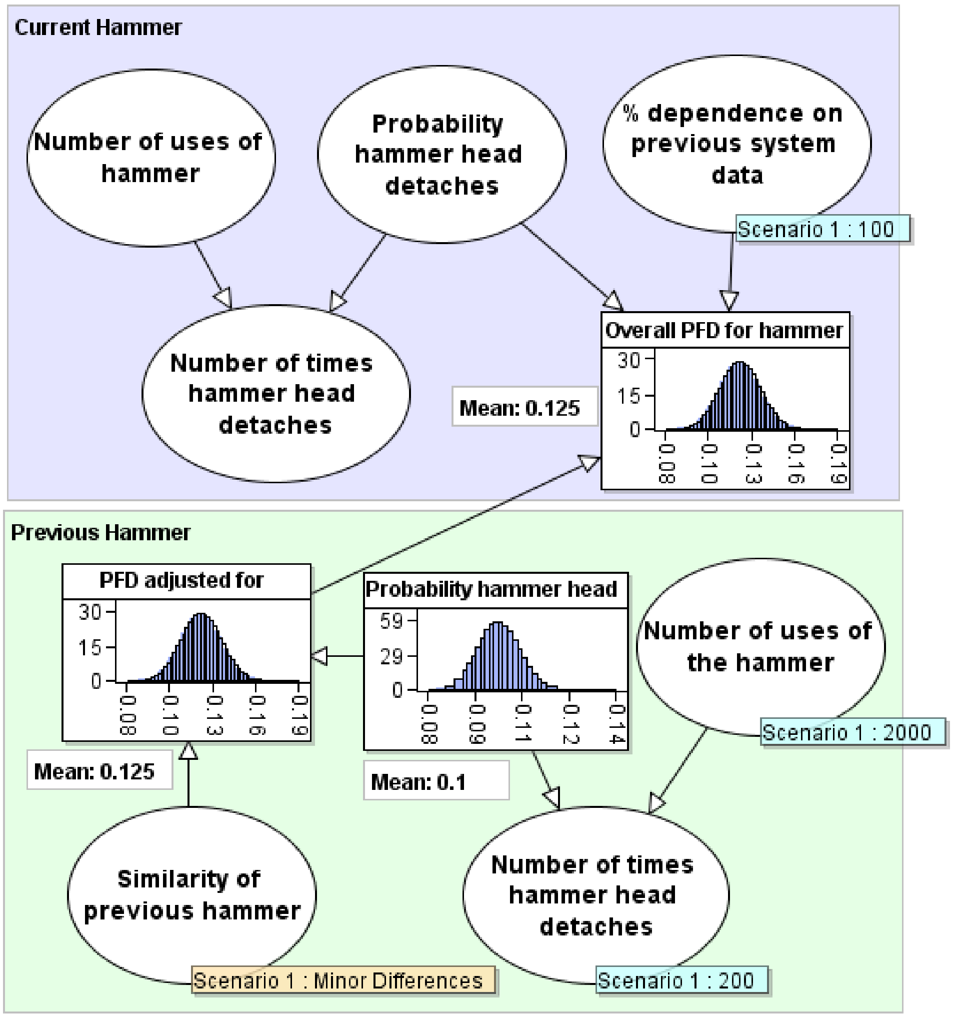


Figure 40 Hazard or failure per demand with limited data idiom instance 1

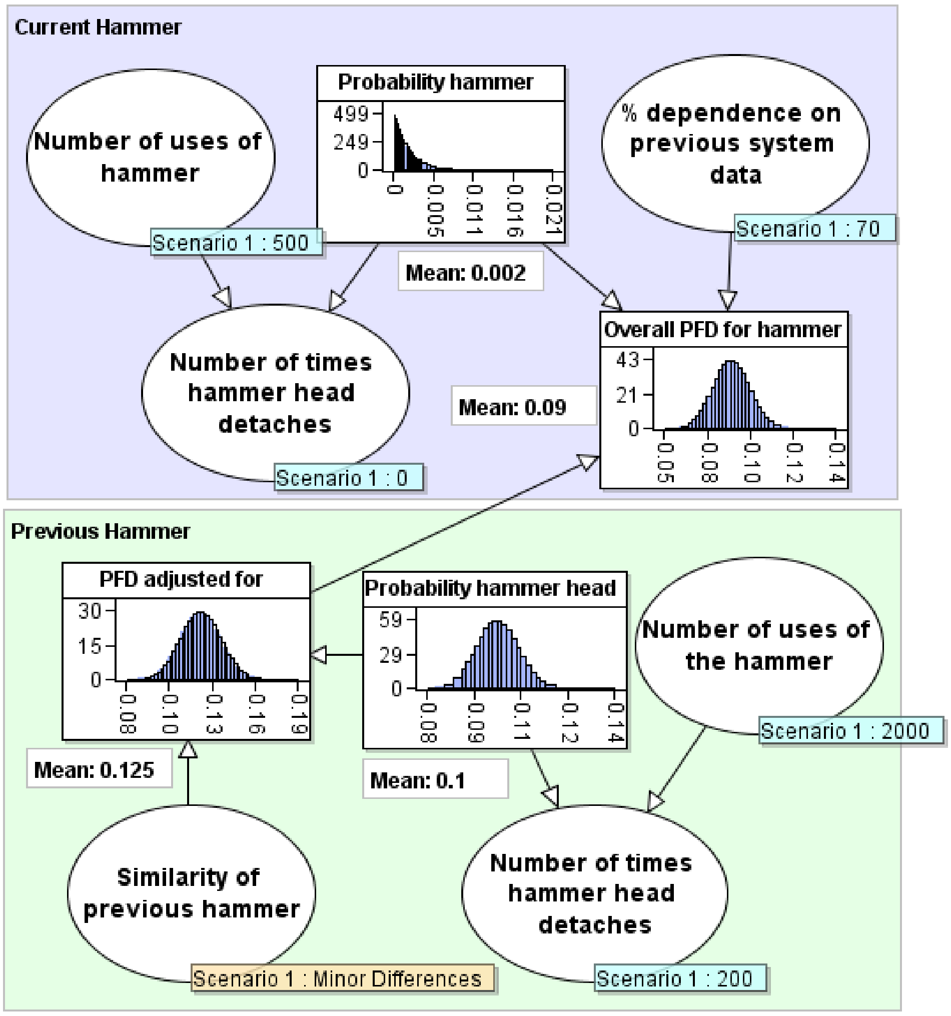


Figure 41 Hazard or failure per demand with limited data idiom instance 2

Probability of an Event with Uncertain Accuracy Idiom

For some products, there may be some uncertainty concerning the number of observed hazards or failures and, subsequently, their ‘true’ reliability or safety. In these situations, we need to consider the accuracy of the number of observed hazards or failures and the true number of observed hazards or failures, given our knowledge about the former, when estimating the ‘true’ reliability of the product.

The *probability of an event with uncertain accuracy idiom* shown in Figure 42 models the uncertainty concerning the number of observed events, e.g., hazards, failures or injuries for a specified number of demands (trials). The NPT values for the node ‘Number of observed events’ (see Table 11) can easily be adapted given the product. In Figure 43, for the hammer example (see Section 6.1), suppose we assume that the number of times we observe the hammer head detaching (100 in 1000 demands in this example) is underestimated; then the true number of times the hammer head detaches will be greater than our observations (in this example the true number of times the hammer head detaches is greater than 100, with a mean count of 125). Please note that this idiom can also be adapted to model the uncertainty concerning the number of trials or demands.

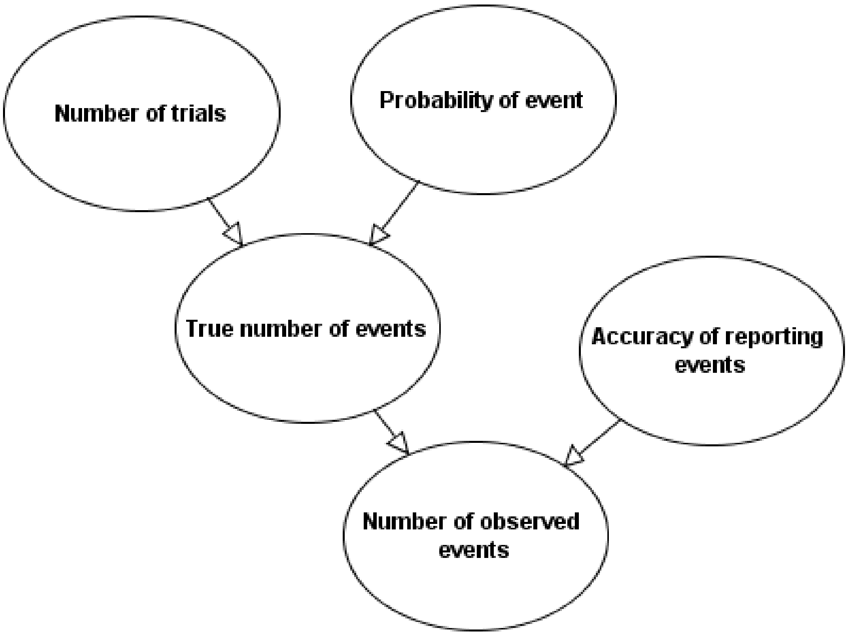


Figure 42 Probability of an event with uncertain accuracy idiom

Table 11 NPT for the node *Number of observed events*

Parent (Accuracy of reporting events) states	**Probability of hazard per demand**
Overestimated	Normal (*tne* × 1.2, 1E-4 × *tne*), where *tne* = true number of events
Accurate	Arithmetic(*tne)*
Underestimated	Normal (max (0, *tne* × 0.8), 1E-4 × *tne*)

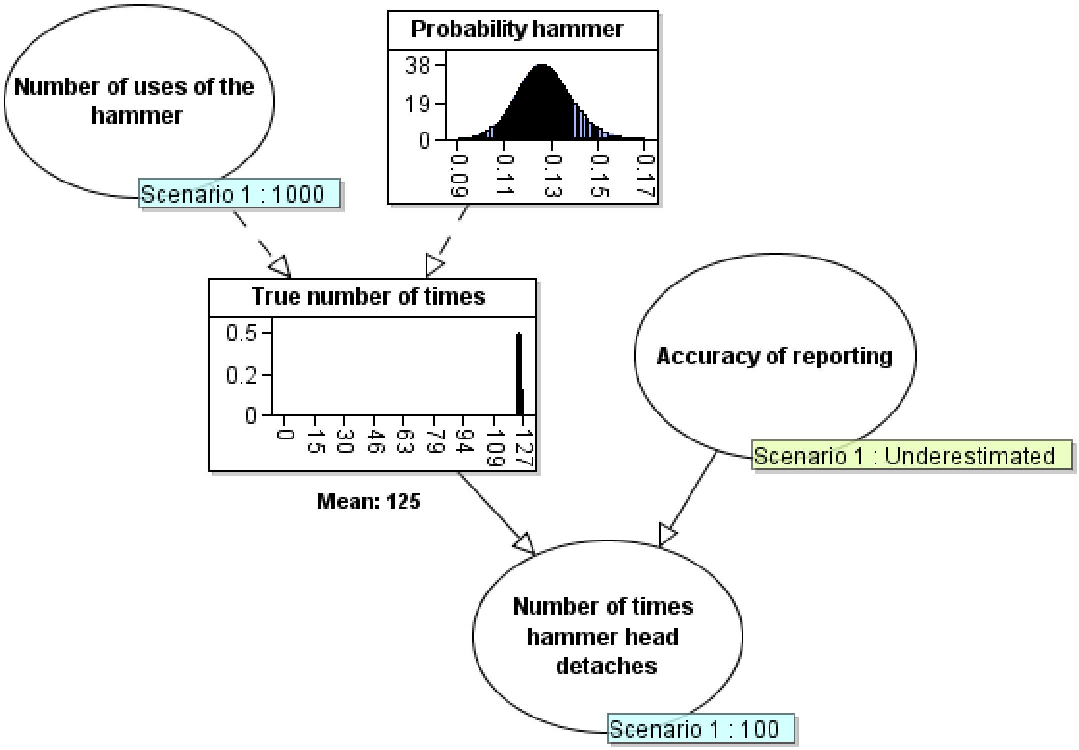


Figure 43 Probability of an event with uncertain accuracy idiom instance

6.2.1.2 Idioms for Modelling Time to Failure (TTF)

There are three idioms in this category:

1. Time to failure (or hazard) idiom (generic)
2. Time to failure (or hazard) idiom with summary statistics
3. Probability of failure within a specified time idiom

Time to Failure (or Hazard) Idiom (Generic)

For some products, we are interested in the reliability associated with the product operating in continuous time. In these situations, we can estimate the mean time to (next) failure by learning the time to failure (TTF) distribution of the product using failure data from testing or operational field use. The mean time to (next) failure is the summary statistic of the time to failure (TTF) distribution. The failure data will be a unit of time, such as hours, and may come from previous similar products. However, please note that model experts may develop other TTF idioms to estimate reliability given available TTF data and other related issues such as censoring.

The *time to failure idiom* shown in Figure 44 estimates the mean time to (next) failure for a product when there is a small number *n* of observed failure times. This idiom has *n* observed failure time nodes, which are used to estimate the failure rate of the product. The ‘Observed failure time’ and ‘Time to next failure’ nodes are (normally) defined as an Exponential distribution with the rate parameter as the value of the ‘Assessed failure rate’ node. Other distributions, such as Weibull and Gamma, can be used to define the nodes since the failure rate for many products is not usually constant but increases with time due to system use. However, please note that for the TTF idioms discussed in this chapter, we assume neither system improvement nor degradation; hence, the time to (next) failure is constant. Imagine that we observe failure times of 80, 90, 110 and 120 for the car engine example described in Section 6.1. As shown in Figure 45, the TTF idiom estimates that the mean time to (next) failure for the car engine is 100, and the failure rate is 0.01, given the observed failure times.

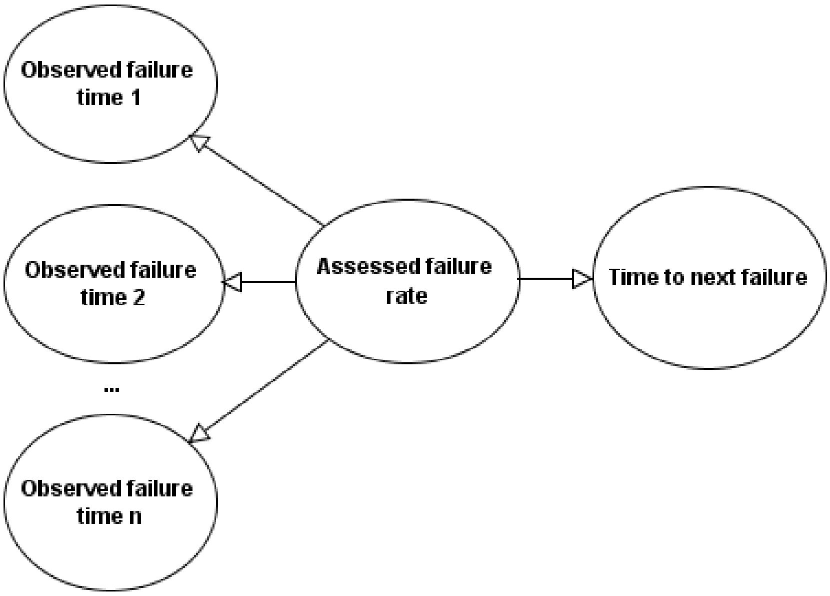


Figure 44 Time to failure (or hazard) idiom

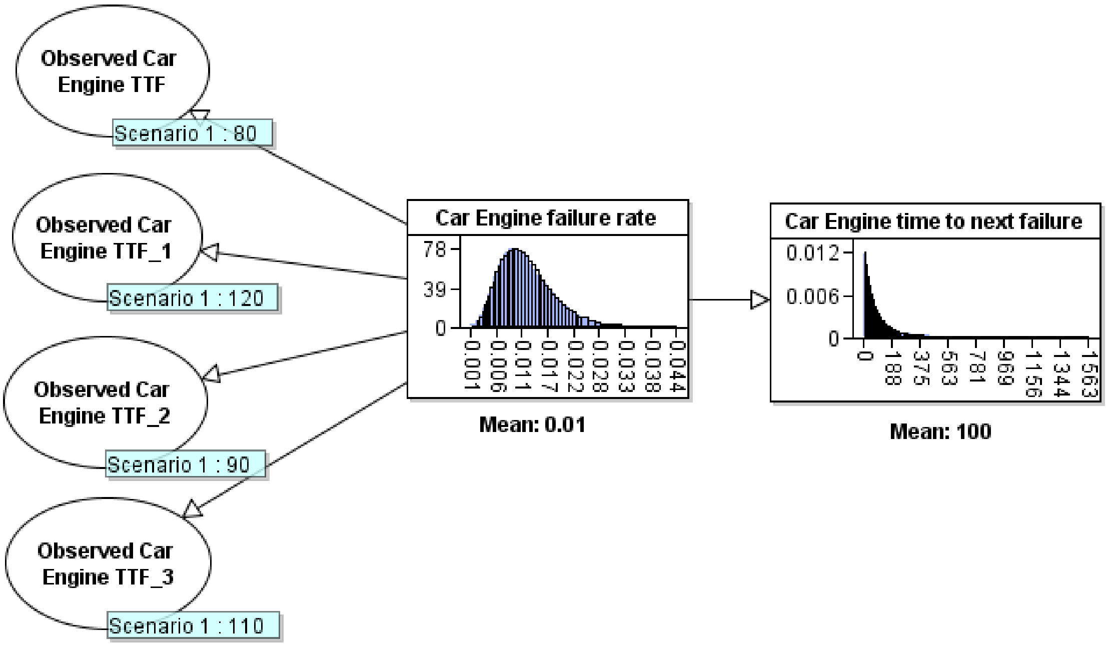


Figure 45 Time to failure (or hazard) idiom instance

Time to Failure (or Hazard) Idiom with Summary Statistics

For some products, there may be a large number of observed failure times. In these situations, it is more convenient to summarise the observed failure times in terms of their mean μ and variance σ^2 and use these as parameters to determine the rate value (i.e., $\frac{1}{Observed\ failure\ time}$) of an Exponential distribution. However, please note that this approach for handling a large number of observed failure times is situational, and the results are less accurate than using the generic TTF idiom; model experts may develop other TTF idioms to estimate reliability given available TTF data and other related issues such as censoring.

The *time to failure idiom with summary statistics* is shown in Figure 46, and an instance is shown in Figure 47. In Figure 47, for the car engine example, imagine that the mean μ observed failure time for the engine is 100 and the variance σ^2 is 250; the TTF idiom estimates that the mean time to (next) failure for the car engine is 100.

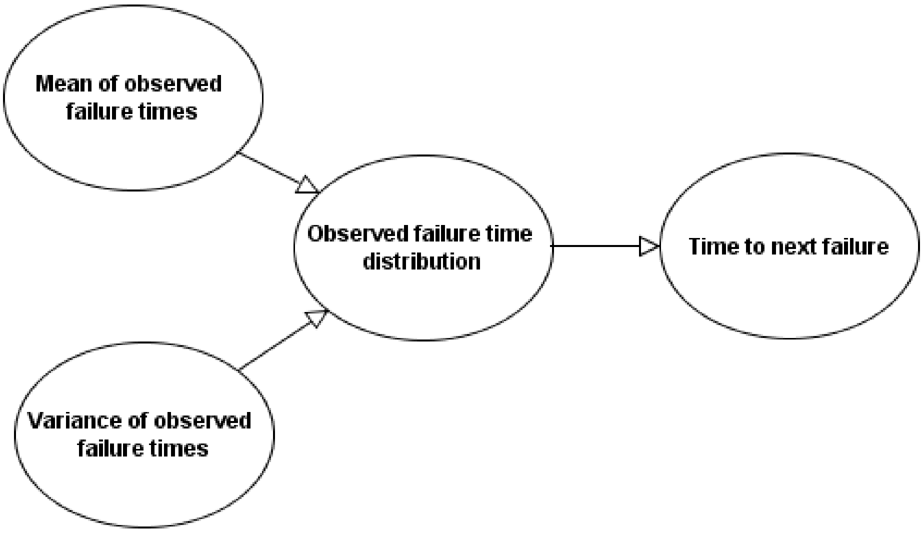

Mean of observed failure times
Observed failure time distribution
Time to next failure
Variance of observed failure times

Figure 46 Time to failure (or hazard) idiom with summary statistics

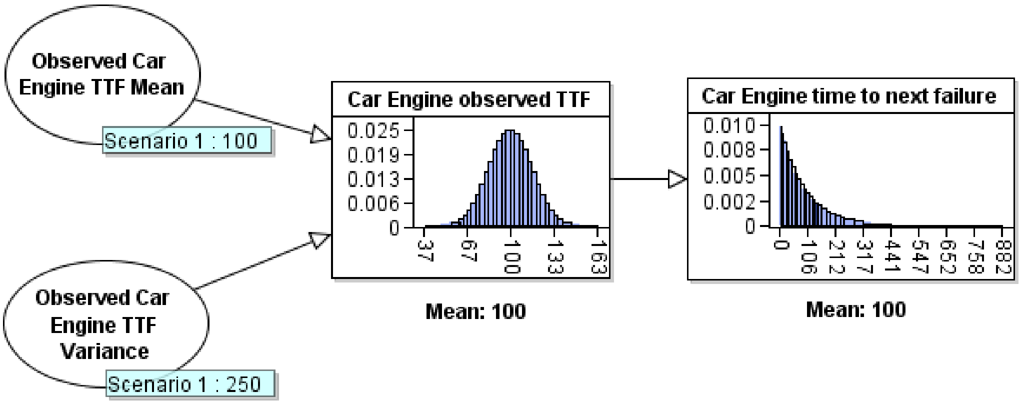


Figure 47 Time to failure (or hazard) idiom with summary statistics instance

Probability of Failure within a Specified Time Idiom

For some products, we are interested in the reliability of the product operating within a specified time t. In these situations, we can estimate the probability of failure (or hazard) for a product within a specified time $P(Failure \mid t)$ by computing the probability that the TTF distribution T is less than or equal to the specified time t, i.e., $P(Failure \mid t) = P(T \leq t)$.

The *probability of failure within a specified time idiom* shown in Figure 48 uses a discrete node called 'Assessed probability of failure' to compute $P(T \leq t)$. The TTF distribution T will be derived from the previous TTF idioms. An instance of this idiom is shown in Figure 49. In Figure 49, for the car engine example, imagine that the car is used continuously for 10 hours, e.g., a road trip; the idiom estimates the probability that the engine will fail is 0.1 or 10% given that the estimated mean time to next failure is 100.

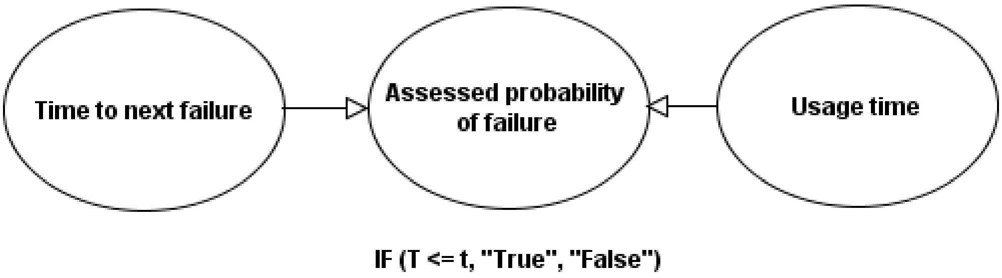


Figure 48 Probability of failure within specified time idiom

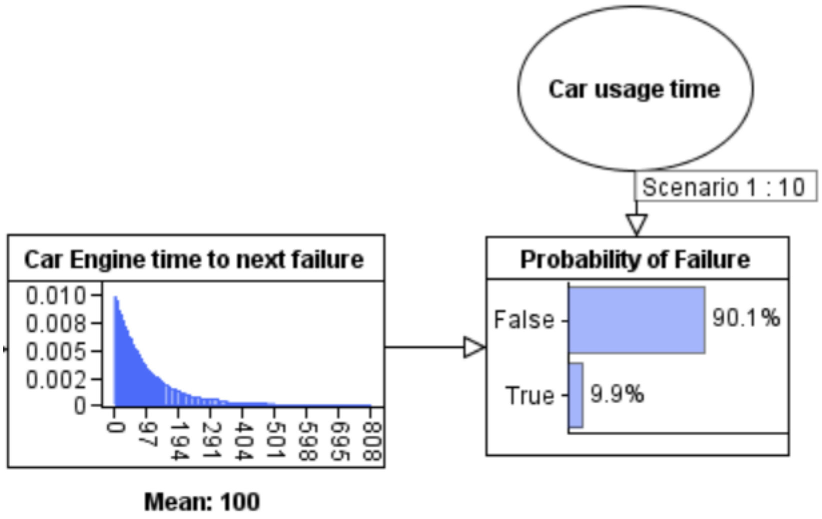


Figure 49 Probability of failure within a specified time idiom instance

6.2.2 Rework Idiom

For some products, faults identified during the hazard identification phase are repairable; however, the success of the repair will depend on the probability of fixing the fault. The *rework idiom* [151] shown in Figure 50 incorporates knowledge of the manufacturer’s rework process quality and rework effort to estimate the probability of fixing the fault (i.e., design and physical faults). This idiom uses ranked nodes [95] to define ‘rework process quality’ and ‘rework effort’ since their values can be measured using a subjective ranked scale such as {‘low’, ‘medium’, ‘high’}. These nodes are then combined to determine ‘rework process overall effectiveness’ (also a ranked node) and the ‘probability of fixing the fault’ (defined as a continuous node ranging from 0 to 1). The NPTs for the nodes in the idiom (see Table 12) can easily be adapted given the product or system. An instance of this idiom is shown in Figure 51. In Figure 51, for the hammer example (see Section 6.1), suppose that the manufacturer's rework process quality and effort are 'very low'; the idiom predicts that the overall rework process effectiveness would be 'very low' or 'low'. As a result, the mean probability of fixing the hammer is very low (i.e., 0.03). Product manufacturers, safety regulators and model experts may use or adapt this idiom to revise the estimated reliability of the product given rework and to inform risk management decisions such as product recall.

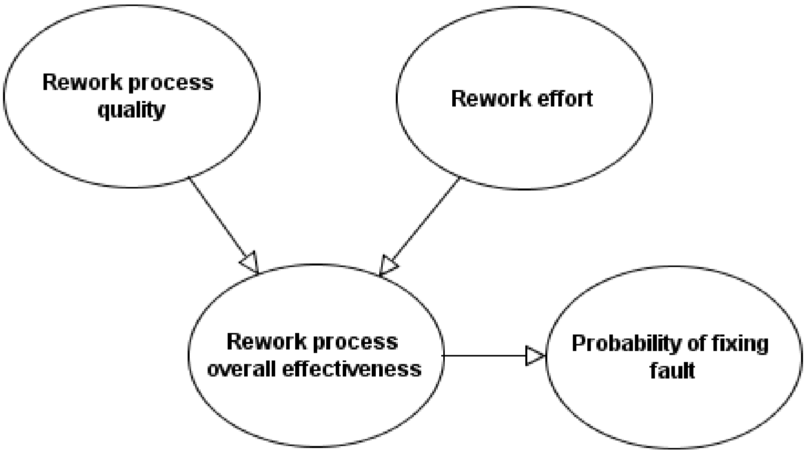

Rework process quality
Rework effort
Rework process overall effectiveness
Probability of fixing fault

Figure 50 Rework idiom

Table 12 NPTs for the nodes of the *Rework idiom*

Node Name	**NPT**
Rework process quality	States ('very low', 'low', 'medium', 'high', 'very high') = 0.2
Rework effort	States ('very low', 'low', 'medium', 'high', 'very high') = 0.2
Rework process overall effectiveness	TNormal (wmean(1.0,rework_process,1.0,rework_effort), 0.001, 0, 1)
Probability of fixing fault	Partitioned expression (Very low: TNormal(0.01,0.001,0.0,1.0), Low: TNormal(0.15,0.001,0.0,1.0), Medium: TNormal(0.4,0.001,0.0,1.0), High: TNormal(0.6,0.001,0.0,1.0), Very High: TNormal(0.8,0.001,0.0,1.0))

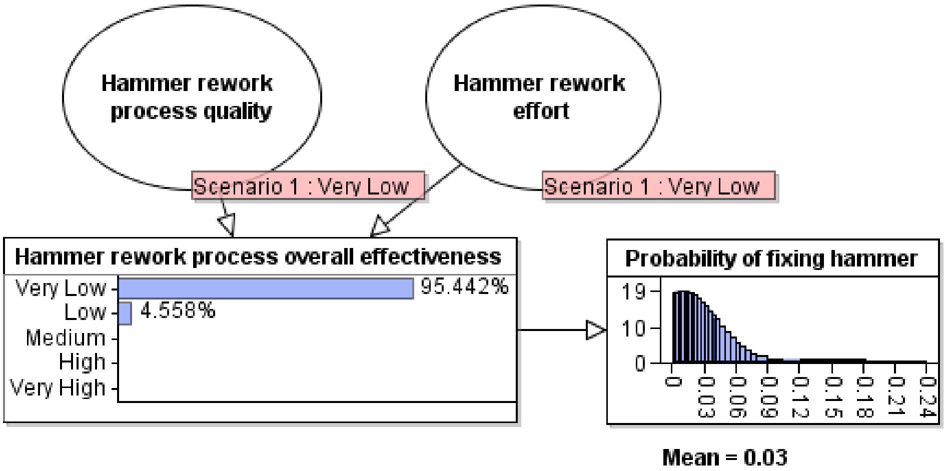


Figure 51 Rework idiom instance

6.2.3 Requirement Idiom

For any product, we will be interested in whether the safety and reliability of the product satisfy safety and reliability requirements defined by standards or safety regulators. Defined safety and reliability requirements ensure that a system operates as intended and is acceptably safe for use. For instance, as an extreme example, a commercial aircraft must satisfy a defined safety and reliability requirement of MTTF > 10^9 flying hours to be approved for commercial use. Hence to determine if a product is compliant, we need to consider the defined safety and reliability value and the actual safety and reliability value of the product. However, testing alone may not be sufficient to determine the actual safety and reliability value of products, especially those with very high reliability requirements, e.g., commercial aircraft, or with limited testing data, e.g., novel products. In these situations, we need to combine testing information with other factors, such as information about the quality of the processes and people involved in product development, to determine the actual safety and reliability value of a product. The quality of processes or people can be estimated using the *Quality idiom* (see Section 6.2.4).

The *requirement idiom* shown in Figure 52 models whether the actual value of an attribute A satisfies the defined requirement value of the attribute R by computing the probability A is less than or equal to R, i.e., $P(Compliant) = P(A \leq R)$. This idiom uses a discrete node called 'Assessed value of attribute' to compute $P(A \leq R)$. An instance of this idiom is shown in Figure 53. In Figure 53, for the hammer example (see Section 6.1), the idiom estimates that there is a 15% chance that the defined safety requirement (0.01 in this example) is satisfied given the probability distribution of the hammer head detaching (hazard) per demand (mean 0.03 in this example). Please note that the requirement idiom can be implemented by encoding the requirement value into the 'Assessed value or attribute' node, as shown in Figure 54. Product manufacturers, model experts and safety regulators may use or adapt the requirement idiom to inform risk management decisions such as rework.

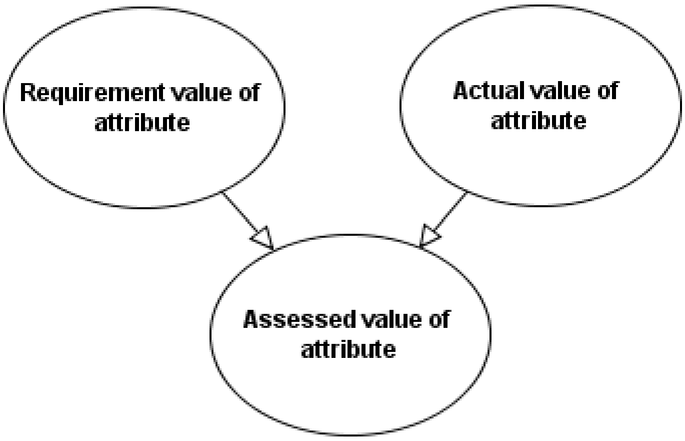

Requirement value of attribute
Actual value of attribute
Assessed value of attribute

Figure 52 Requirement idiom

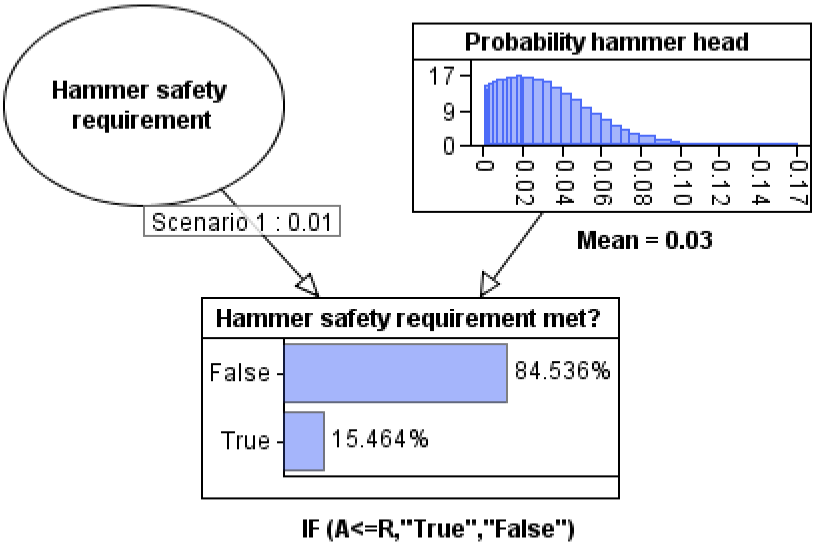


Figure 53 Requirement idiom instance

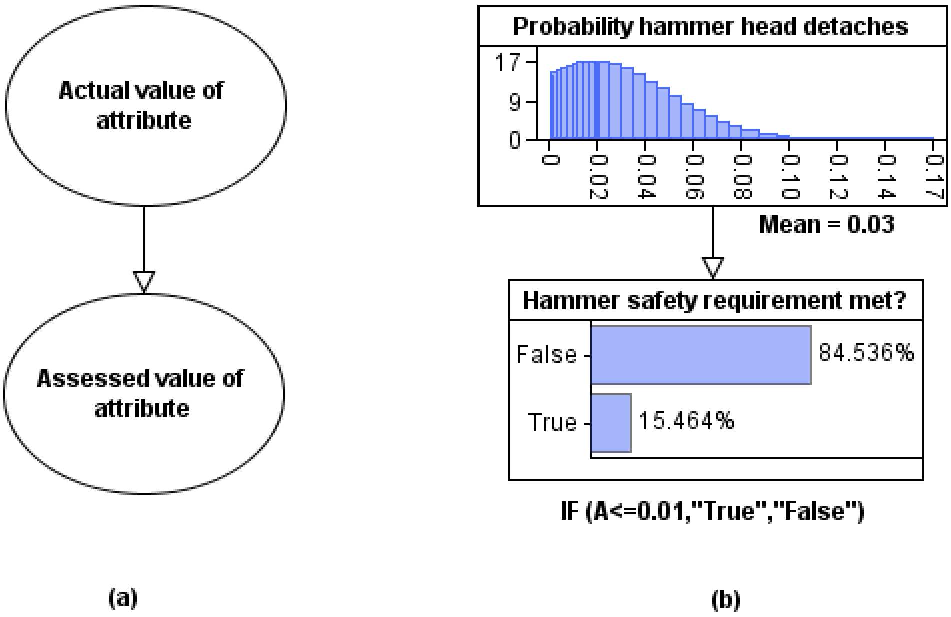

Actual value of attribute
Assessed value of attribute
(a)
Probability hammer head detaches
17
9
0
0
0.02
0.04
0.06
0.08
0.10
0.12
0.14
0.17
Mean = 0.03
Hammer safety requirement met?
False
84.536%
True
15.464%
IF (A<=0.01,"True","False")
(b)

Figure 54 Implicit Requirement idiom (a) and instance (b)

6.2.4 Quality Idiom

For novel products, products with limited testing data and products with very high reliability requirements, other product-related information, such as the quality of the processes and people involved in its development, can be considered when estimating the reliability of the product. For instance, for the hammer example, if the manufacturing process quality is poor, this can increase the likelihood of the hammer head detaching. However, the quality of a particular process or activity, such as the manufacturing process, may be latent, difficult to measure or observe. In these situations, we can use measurable indicators and causal factors to measure the quality of a particular process or activity.

The *quality idiom* (shown in Figure 55) models the quality of an activity, process or variable using indicators and causal factors. This idiom uses ranked nodes [95] to define variables since their values can be measured using a subjective ranked scale such as {'low', 'medium', 'high'}. Please note that the NPT values for the node 'Latent quality value' (see Figure 55) can easily be adapted given the process or activity. Instances of this idiom are shown in Figure 56 for the hammer example. In Figure 56a, the idiom measures the quality of the manufacturing process, using knowledge about product defects and process drifts. In Figure 56b, the idiom measures the quality of the organisation using knowledge about customer satisfaction and years in operation.

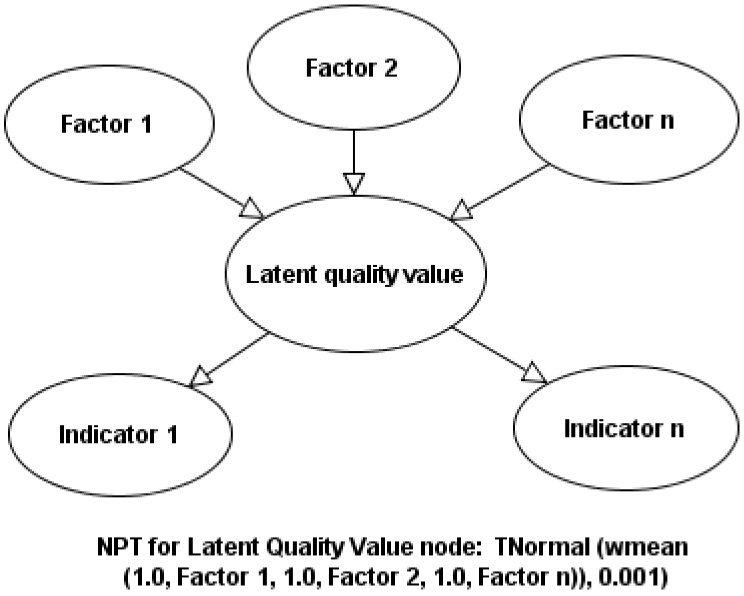

Factor 2
Factor 1
Factor n
Latent quality value
Indicator 1
Indicator n
NPT for Latent Quality Value node: TNormal (wmean (1.0, Factor 1, 1.0, Factor 2, 1.0, Factor n)), 0.001)

Figure 55 Quality idiom

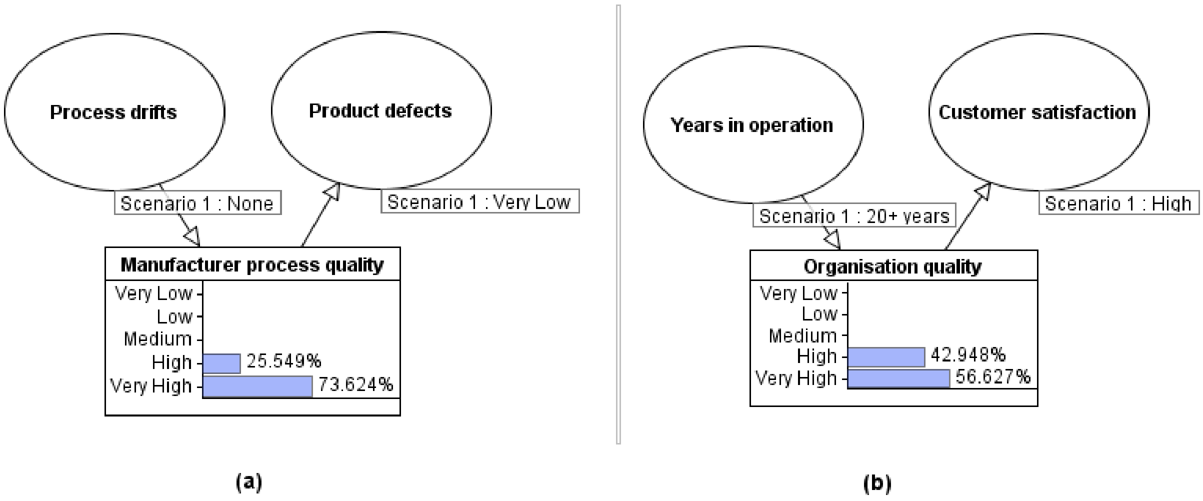


Figure 56 (a) Manufacturer process quality instance (b) Organisation quality instance

6.2.5 Idioms for Modelling Product Failures, Hazards and Injury Occurrences

Determining the occurrence of failures or hazards and related injuries for a product (system) is essential for informing appropriate risk control measures to prevent harm to users and damage to the environment. In this section, we describe the idioms associated with determining the occurrence of failures or hazards and related injuries for a product. These idioms address interaction faults and system degradation that can result in failures or hazards and harm to the user. There are three idioms in this category:

1. Hazard or failure occurrence idiom
2. Injury event (occurrence) idiom
3. Product injury idiom

6.2.5.1 Hazard or Failure Occurrence Idiom

System degradation and consumer behaviour when using a product, e.g., misuse and frequency of use, can greatly influence the occurrence of failures or hazards for a product. Therefore, it is essential to understand how these factors impact the occurrence of failures or hazards for a product to reduce potential harm to consumers.

The *hazard or failure occurrence idiom* shown in Figure 57 is an instance of the cause-consequence idiom [19] (see Section 4.3.1.1) that models the relationship between a hazard(s) or failure(s) and its causal factors. A factor can be any observable attribute or situation that increases or decreases the likelihood or uncertainty of a hazard or failure occurring, such as consumer behaviour. An instance of this idiom is shown in Figure 58. In Figure 58, for the hammer example, suppose that the consumer does not use the hammer as intended (minor deviations from intended use), then we expect that the probability of the hammer head detaching per demand (use) will increase. In this example, the idiom shows that the mean probability of the hammer head detaching per demand increases from 0.15 to 0.18. Product manufacturers and safety regulators may find this idiom useful since it can incorporate all causal factors that affect the occurrence of failures and hazards for a product.

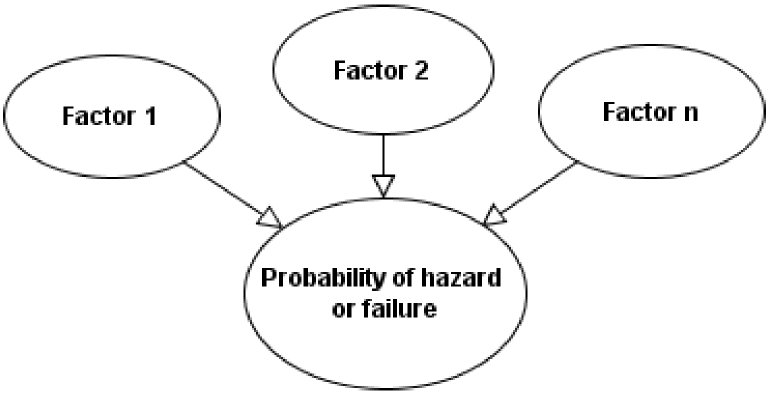


Figure 57 Hazard or failure occurrence idiom

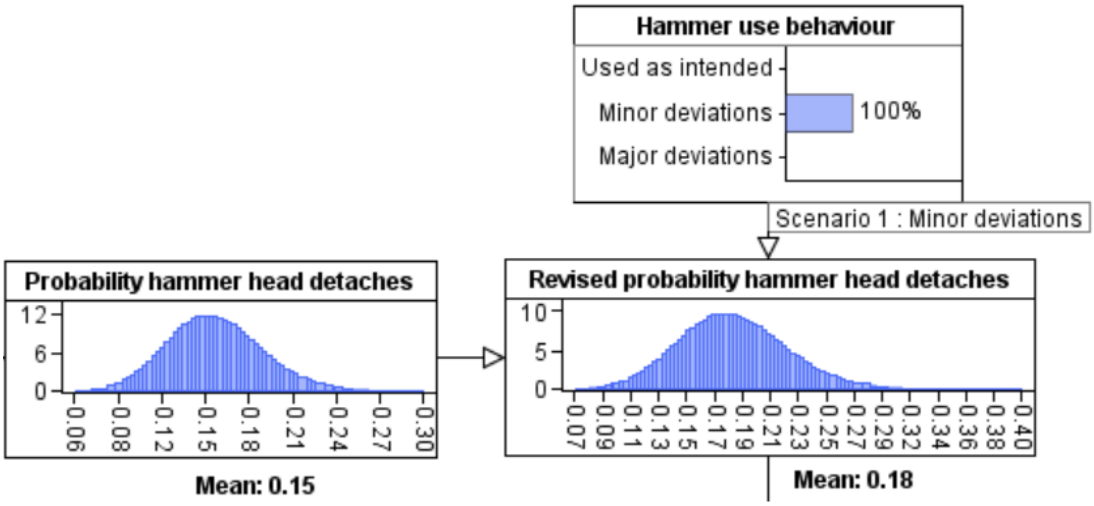


Figure 58 Hazard or failure occurrence idiom instance

6.2.5.2 Injury Event (occurrence) Idiom

Given the injury scenario for a product, we will be interested in the probability of injury given a failure or hazard. We can estimate the probability of an injury given a failure or hazard by considering the probability of the failure or hazard occurring and the probability of the failure or hazard causing an injury. The probability of the failure or hazard occurring can be estimated using *reliability idioms* (see Section 6.2.1) and the *hazard or failure occurrence idiom* (see Section 6.2.5.1); the probability of the failure or hazard causing an injury can be estimated from injury data obtained from reputable sources such as hospitals and injury databases.

The *injury event (occurrence) idiom* shown in Figure 59 models the probability of an injury event (i.e., an occurrence of injury) during product use. It estimates the probability of an injury event $P(I)$ by combining the probability of the failure or hazard occurring $P(H)$, and the probability of the failure or hazard causing an injury $P(I|H)$ i.e., $P(I) = P(H) \times (I|H)$. An instance of this idiom is shown in Figure 60. In Figure 60, for the hammer example, if the mean probability of the hammer head detaching and causing a head injury is 0.08 and the mean probability of the hammer head detaching is 0.18, then the estimated mean probability of a head injury occurring while using the hammer is 0.015.

Please note that for the injury event idiom, we are assuming a single known type of hazard; however, a product (system) usually has multiple potential hazards. In situations where a product has multiple potential different hazards that are unique in terms of properties they possess, e.g., small parts, electric shock and toxicity, we can add other nodes to the idiom representing different hazards. However, in situations where the hazards, though unique, are similar in terms of properties they possess, e.g., hot surfaces, open flames and hot gases, we can identify and define hazard groups or classes, e.g., ‘extreme temperature’. The idiom can use the defined hazard groups to consider multiple similar hazards rather than a single hazard.

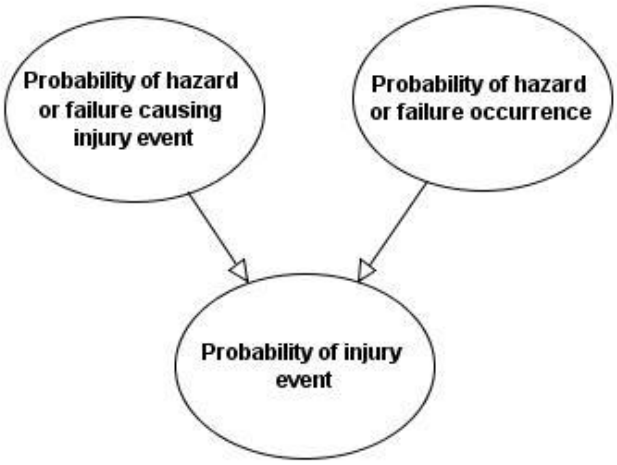

Probability of hazard or failure causing injury event
Probability of hazard or failure occurrence
Probability of injury event

Figure 59 Injury event idiom

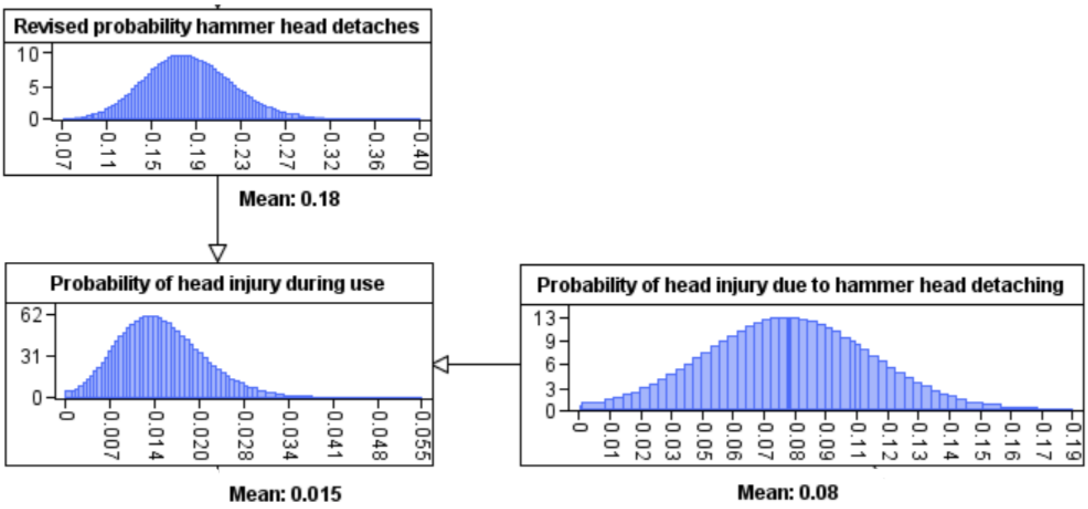


Figure 60 Injury event idiom instance

6.2.5.3 Product Injury Idiom

For some products, we may be interested in estimating the number of injuries due to product failures, hazards or hazardous situations. In these situations, we have to consider the probability of the injury event and the number of product instances (i.e., the total number of products manufactured or available on the market). The probability of the injury event can be obtained using the *injury event idiom* (see Section 6.2.5.2), and the number of product instances can be obtained using manufacturing or sales data.

The *product injury idiom* shown in Figure 61 models the number of injury events for a set of product instances. This idiom uses a Binomial distribution for the number of injury events. An instance of this idiom is shown in Figure 62. In Figure 62, for the hammer example, suppose there are 100000 hammer instances, and the mean probability of a head injury is 0.015; the idiom estimates that the mean number of head injuries is 1500.

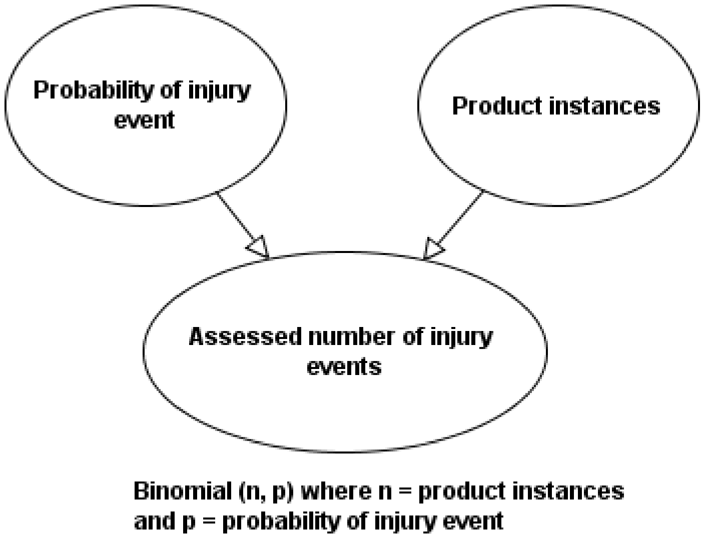

Probability of injury event
Product instances
Assessed number of injury events
Binomial (n, p) where n = product instances
and p = probability of injury event

Figure 61 Product injury idiom

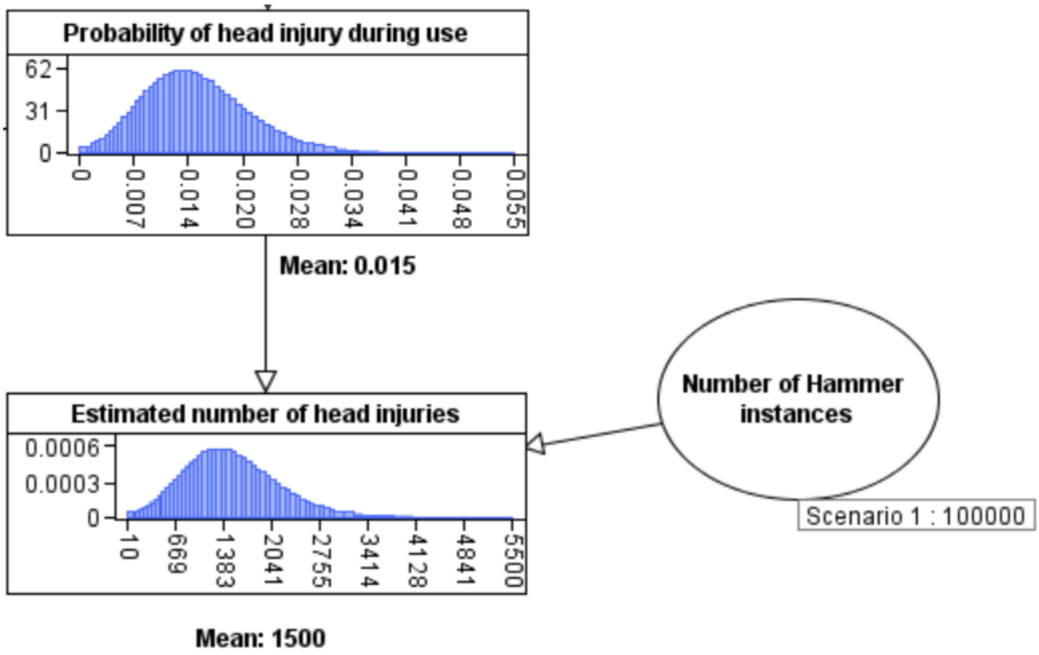


Figure 62 Product injury idiom instance

6.2.6 Idioms for Modelling Risk

Determining the overall risk of a product (system) is essential for informing risk management decisions such as product recall and risk controls. In this section, we describe idioms associated with determining the risk of a product. These idioms satisfy the final task of the risk analysis phase, i.e., the risk estimation phase, which determines the overall risk of the product. There are two idioms in this category:

1. Risk control idiom
2. Risk idiom

6.2.6.1 Risk Control Idiom

For most products, we may be interested in estimating the effect of risk controls on the occurrence of failures, hazards and related injuries. In these situations, we need to consider the probability of the risk control to mitigate the event (i.e., failures, hazards and injuries) and the probability of the event occurring in the absence of risk controls. *Risk control* is any measure or action taken to mitigate the consequence of an event.

The *risk control idiom* shown in Figure 63 models the effect of risk controls on an event, e.g., hazard, failure or injury. It uses the probability of the risk control to mitigate the event C, and the probability of the event E, to compute the residual probability of the event consequence $RE,$ i.e., $RE = (1 - C) \times E.$ The risk control idiom can be adapted to model the occurrence of hazards and harm (injury). An instance of this idiom is shown in Figure 64. In Figure 64, for the hammer example, suppose the probability of the risk control mitigating the head injury is 0.5, and the mean probability of a head injury in the absence of the risk control is 0.08; the idiom computes that the mean probability of a head injury is 0.04 after the risk control is implemented.

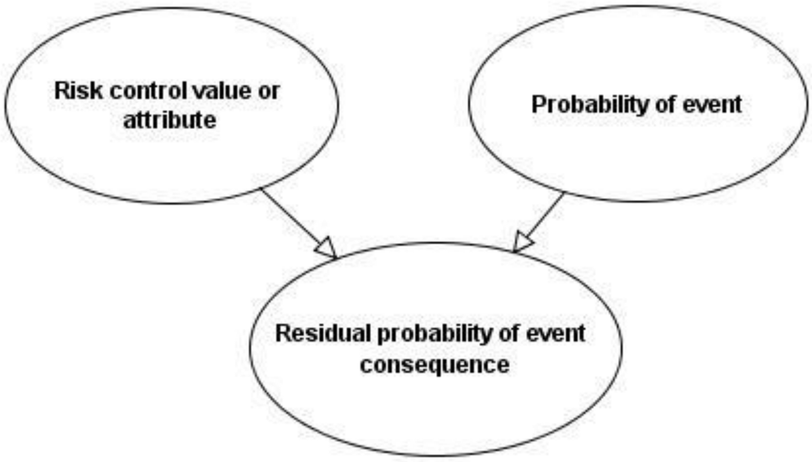

Risk control value or attribute
Probability of event
Residual probability of event consequence

Figure 63 Risk control idiom (generic)

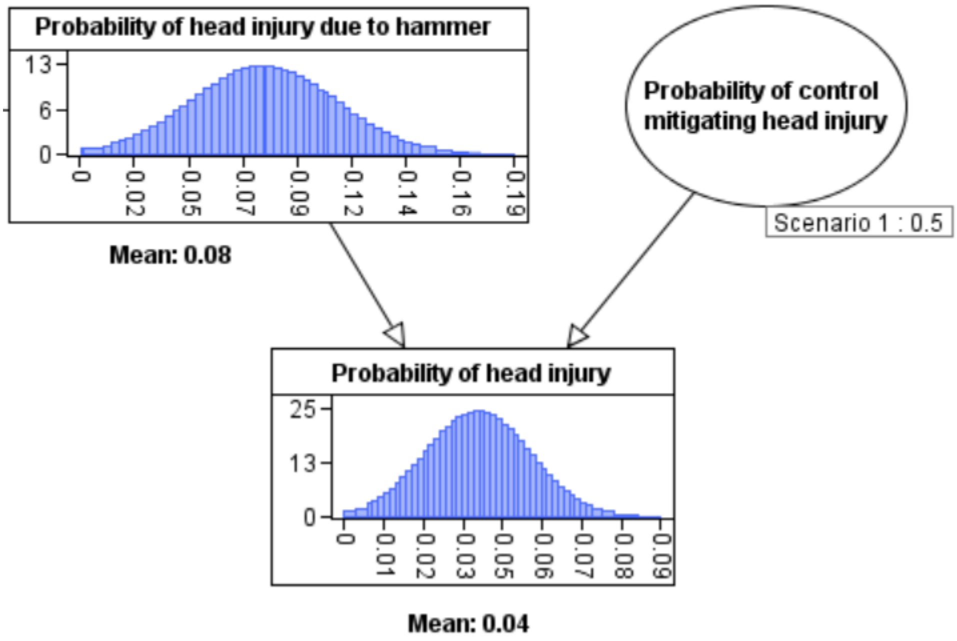

Probability of head injury due to hammer
13
6
0
0
0.02
0.05
0.07
0.09
0.12
0.14
0.16
0.19
Mean: 0.08
Probability of control mitigating head injury
Scenario 1 : 0.5
Probability of head injury
25
13
0
0
0.01
0.02
0.03
0.05
0.06
0.07
0.08
0.09
Mean: 0.04

Figure 64 Risk control idiom instance

6.2.6.2 Risk Idiom

Previous product safety idioms provide the probability distributions for events, including failures, hazards and injuries associated with a product and its use. We can use this information to estimate the risk of a product using the *risk idiom*. The *risk idiom* shown in Figure 65 is used to generate a discrete risk score (e.g., a 5-point scale for regulatory purposes) that is a combination of a set of complex measures. This idiom model risk in terms of its factors and is a special case of the generic definitional idiom [19]; however, the specific mapping from the continuous function into a discrete set will be specific to the context. For example, in the RAPEX method for product risk assessment (discussed in Chapter 8), the risk level for a consumer product is defined based on specific injury probability bounds and injury severity levels. For instance, a product is judged as 'low risk' given any injury severity level if the probability of the product causing an injury is less than 0.000001. An instance of the risk idiom is shown in Figure 66. In Figure 66, for the hammer example, the idiom estimates the risk of the hammer using a ranked node [95] with a 5-point scale ranging from 'very low' to 'very high', considering the probabilities of the hammer causing a head injury and minor injuries, respectively. In this example, there is a 98% chance that the risk of the hammer is 'very high'.

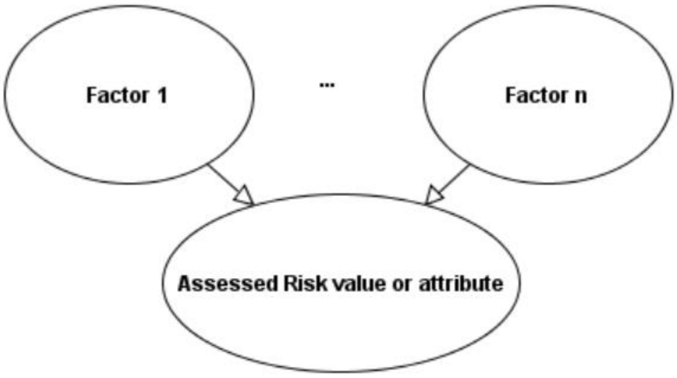


Figure 65 Risk idiom

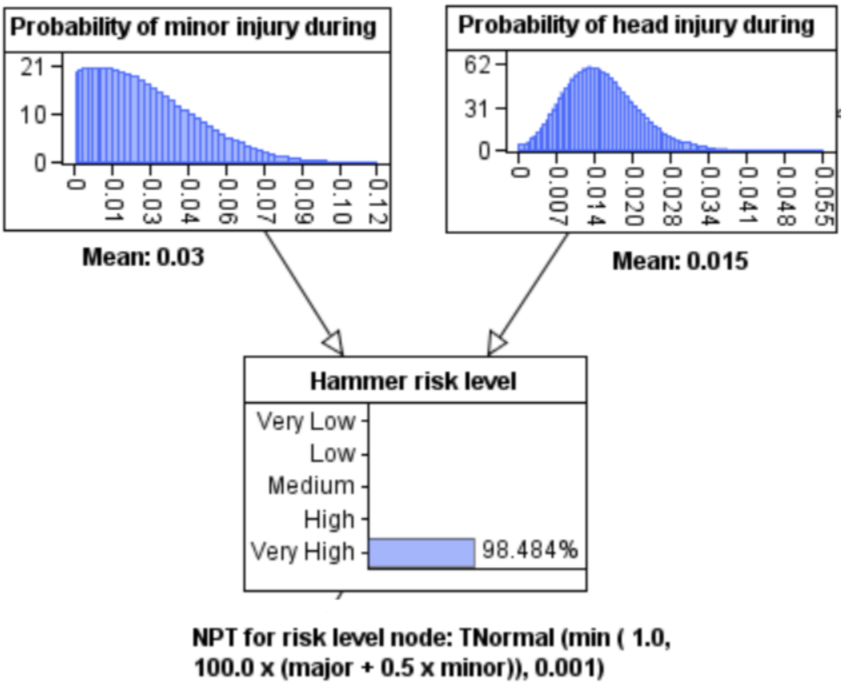


Figure 66 Risk idiom instance

6.3 Product Safety Idioms for Risk Evaluation

The last phase of the risk assessment process is risk evaluation (see Figure 1). Risk evaluation "is the process by which the outcome of the risk analysis is combined with policy considerations to characterise the risk and inform decisions on risk management" [15], [26]. It entails determining whether the estimated risk of the product is acceptable or tolerable given its benefits. In this section, we describe two idioms for risk evaluation:

1. Risk tolerability (acceptability) idiom
2. Consumer risk perception idiom

6.3.1 Risk Tolerability (Acceptability) Idiom

In situations where the overall risk of a product is judged unacceptable and additional risk controls are not practical, the product manufacturer or safety regulator may need to determine if the benefit of the product outweighs its risks. The *risk tolerability (acceptability) idiom* shown in Figure 67 models the trade-off between risk and benefit (or utility) for a product. It evaluates whether the estimated risk score (level) of a product is acceptable or tolerable given the benefit (or utility). The benefits of a product may be determined from literature or consumer surveys. An instance of this idiom is shown in Figure 68. In Figure 68, for the hammer example, we define the benefit and risk values using ranked nodes [95]. In this example, we assume that the benefit of the hammer is average (‘medium’) and the risk of the hammer is ‘very high’; the idiom estimates that the risk tolerability for the hammer is ‘low’ (or 95% chance the risk tolerability is ‘low’ or ‘very low’).

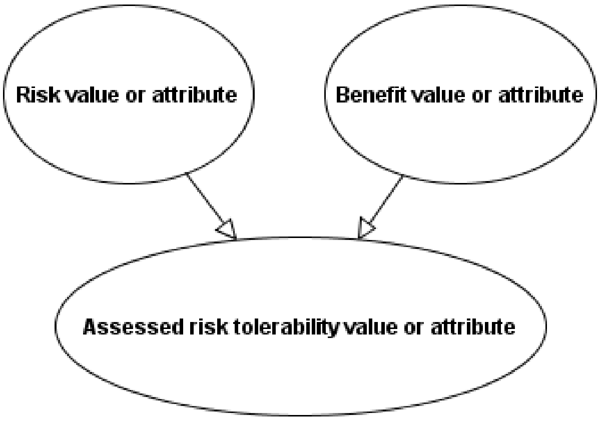

Risk value or attribute
Benefit value or attribute
Assessed risk tolerability value or attribute

Figure 67 Risk tolerability idiom

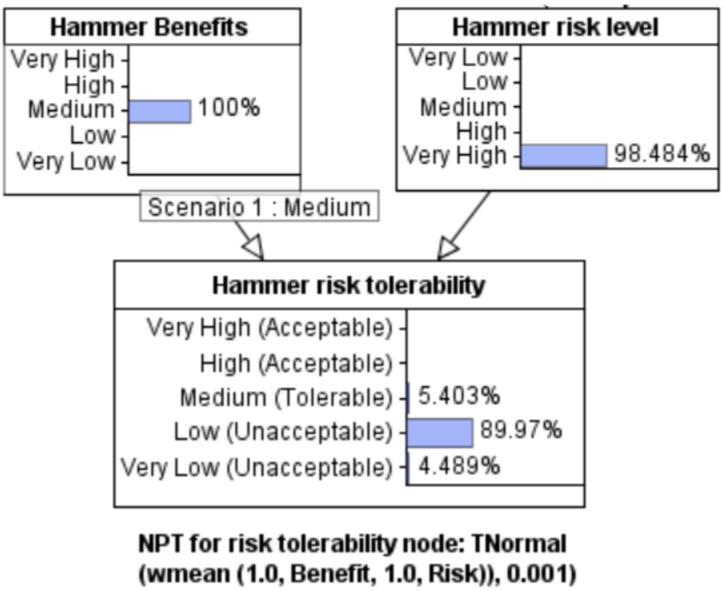


Figure 68 Risk tolerability idiom instance

6.3.2 Consumer Risk Perception Idiom

Consumers may judge the risk and benefits of products differently from experts. For instance, experts tend to judge the risk of a product using quantitative risk assessments, whereas consumers judge risk using a combination of subjective measures such as risk propensity. Therefore, it is essential to understand consumers' perceived risk and benefits of a product to inform risk management decisions. Since the actual value of consumers' perceived risk or benefits may be latent or difficult to measure, we have to use measurable indicators and causal factors to estimate their perceived risk and benefits.

The *consumer risk perception idiom* shown in Figure 69 estimates consumer risk perception of a product using causal factors (or interventions) and indicators. Please note that this idiom does not incorporate different user profiles. Instances of this idiom are shown in Figure 70 and Figure 71. In Figure 70 and Figure 71, for the hammer example, we define the variables using ranked nodes [95]. In Figure 70, the idiom shows that consumers may perceive the risk of the hammer as 'high' since they judge the likelihood of injury and the severity of the injury as 'high'. In Figure 71, the idiom shows the impact of a product recall, negative media stories and consumer feedback on consumer risk perception of the hammer.

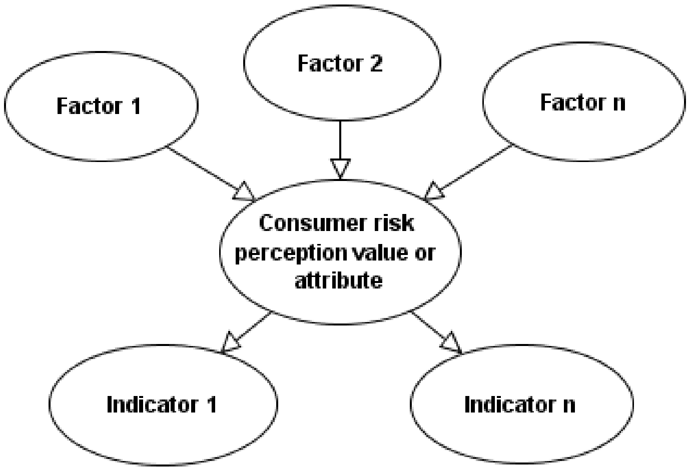


Figure 69 Consumer risk perception idiom

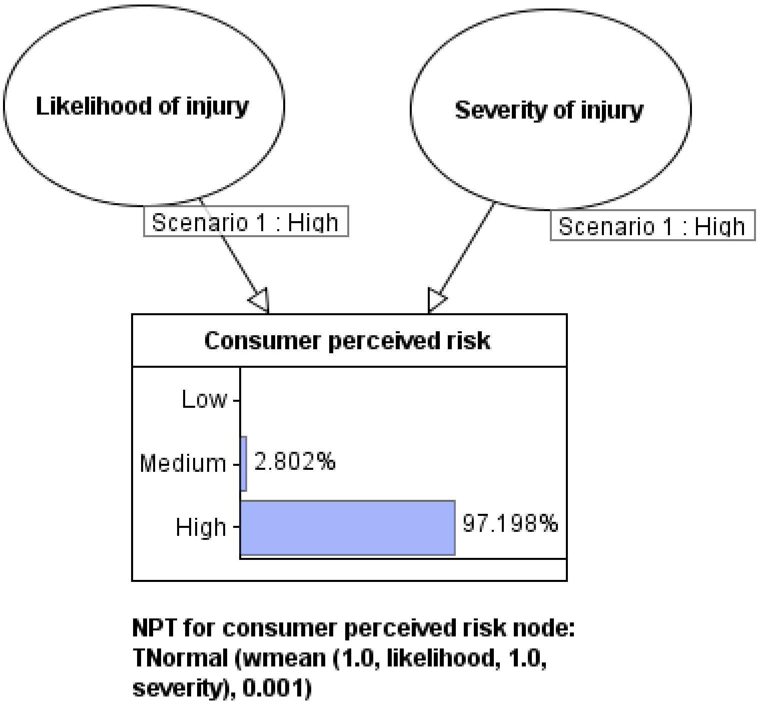


Figure 70 Consumer risk perception idiom instance 1

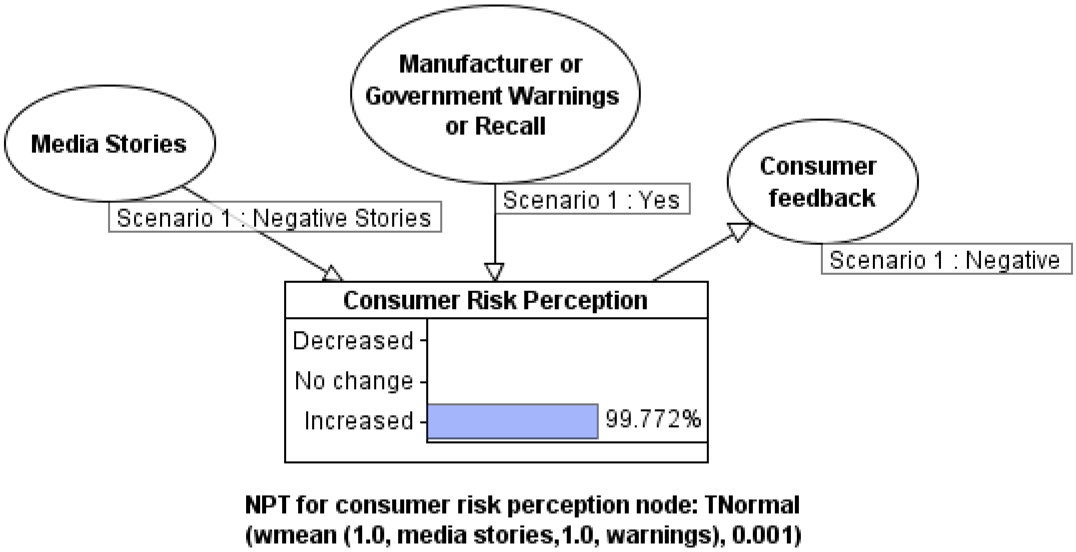

Media Stories
Manufacturer or Government Warnings or Recall
Consumer feedback
Scenario 1 : Negative Stories
Scenario 1 : Yes
Scenario 1 : Negative
Consumer Risk Perception
Decreased
No change
Increased
99.772%
NPT for consumer risk perception node: TNormal (wmean (1.0, media stories,1.0, warnings), 0.001)

Figure 71 Consumer risk perception idiom instance 2

6.4 Building a BN using the Product Safety Idioms

In this section, the process for building BNs using product safety idioms is described (see Section 6.4.1). We also show examples of BNs created using the product safety idioms (see Section 6.4.2 for the hammer example and Section 6.4.3 for the aircraft example).

6.4.1 BN Development Process

The process of building a BN for product safety risk management using the product safety idioms can be illustrated using the BN development process model shown in Figure 72, proposed by Neil et al. [19].

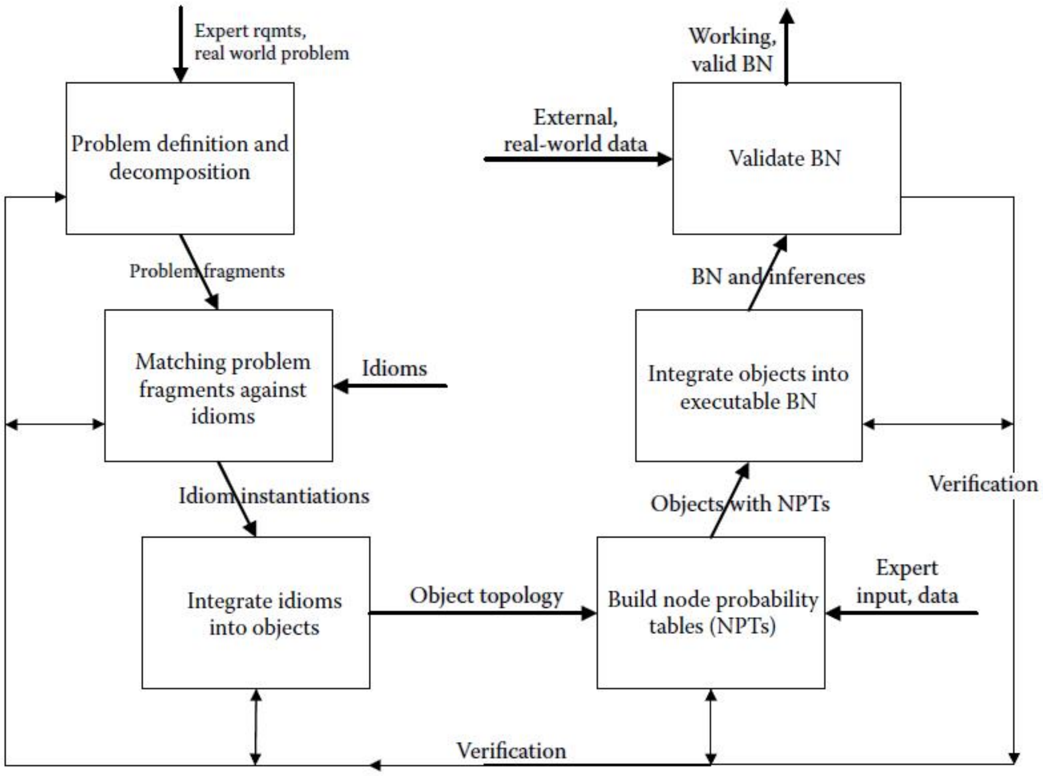

Expert rqmts,
real world problem
Problem definition and decomposition
Problem fragments
Matching problem fragments against idioms
Idioms
Idiom instantiations
Integrate idioms into objects
Object topology
Build node probability tables (NPTs)
Expert input, data
Objects with NPTs
Integrate objects into executable BN
BN and inferences
Validate BN
External, real-world data
Working, valid BN
Verification
Verification

Figure 72 BN Development Process Model taken from [19]

As shown in Figure 72, the BN development process consists of six stages ranging from problem definition to BN validation. The first stage is problem definition and decomposition. During this stage, the scope and objectives of the BN and other relevant information, such as model variables, are elicited from experts and literature. In the second stage, the elicited knowledge is organised into groups of related random variables (called ‘fragments’), which are matched against the idioms. During this stage, the groups of related variables are implemented as instances of suitable idioms. In the third stage, the idiom instances are integrated into objects. In the fourth stage, the NPTs for the variables in the objects are defined, and in the fifth stage, the objects are linked to build the complete BN. In the last stage, the BN is used to perform inferences, and its results are validated. Verification is done at each stage of the process to ensure that the output of each stage is accurate and satisfies the requirements of the problem definition.

6.4.2 Example 1: Hammer Reliability BN

In Figure 73, for the hammer example, we show how the product safety idioms may be combined to determine the overall reliability of the hammer. In this example, using testing data only (i.e., hammer head detaches 20 times in 400 demands), the BN model estimates the mean probability of the hazard per demand is 0.05 (modelled using the hazard per demand idiom). However, given information about the manufacturing process quality (modelled using the quality idiom), the mean probability of the hazard per demand is revised. In this example, the mean probability of the hazard per demand increased to 0.08 due to a poor manufacturing process. Finally, the BN model shows that the reliability of the hammer did not satisfy the defined safety and operational requirements (modelled using the requirement idiom).

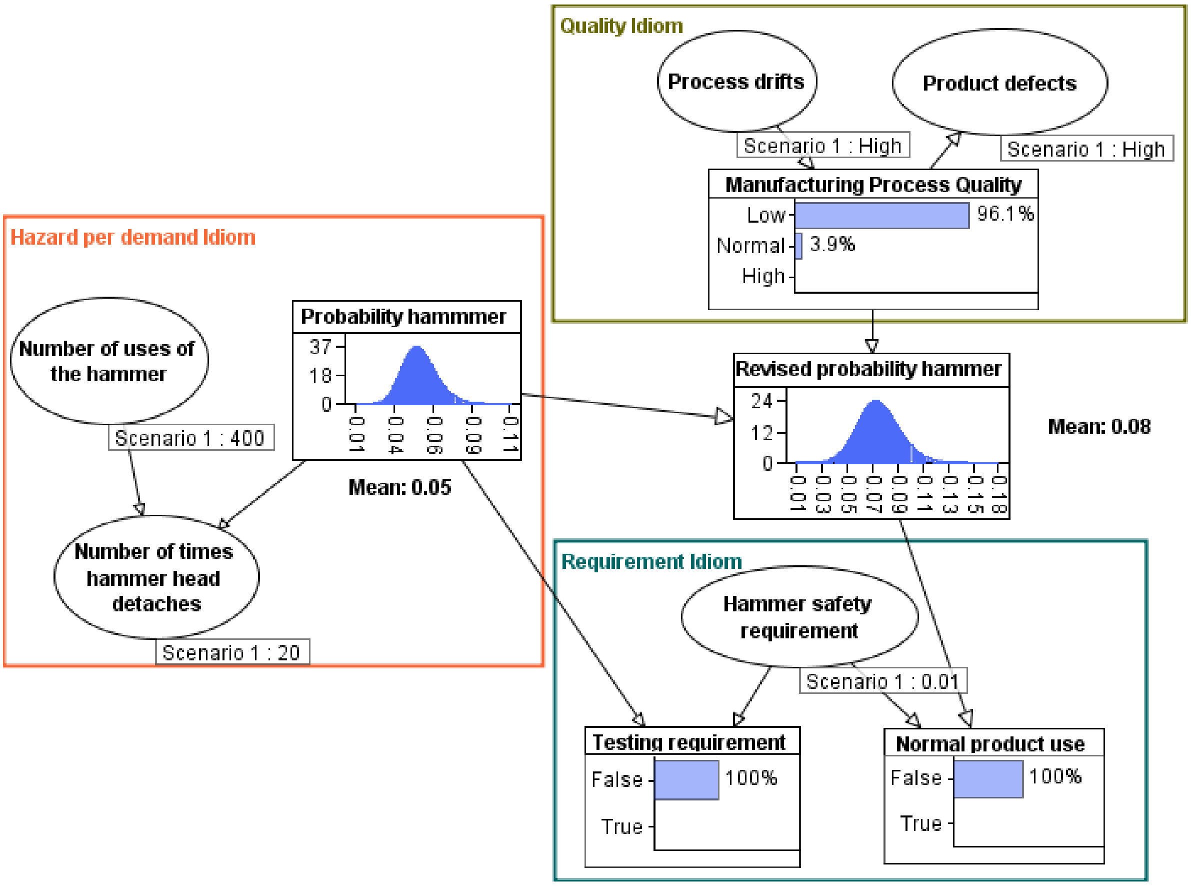


Figure 73 Hammer reliability BN with visible product safety idioms

6.4.3 Example 2: Aircraft Reliability BN

In the previous section, the hammer example was chosen as a particularly simple product to illustrate the basic idioms approach. In this section, we now go to the other extreme of complexity and consider an aircraft. The aircraft reliability BN shown in Figure 74 shows a fragment of the safety assessment for a new military aircraft that focuses on estimating the probability of failure during a mission due to engine and/or braking system failure. It incorporates both TTF and PFD measures to determine the overall reliability since the reliability measure for the engine is TTF, and the braking system is PFD. The product safety idioms connected causally to estimate the reliability of a military aircraft during a mission are highlighted in Figure 74.

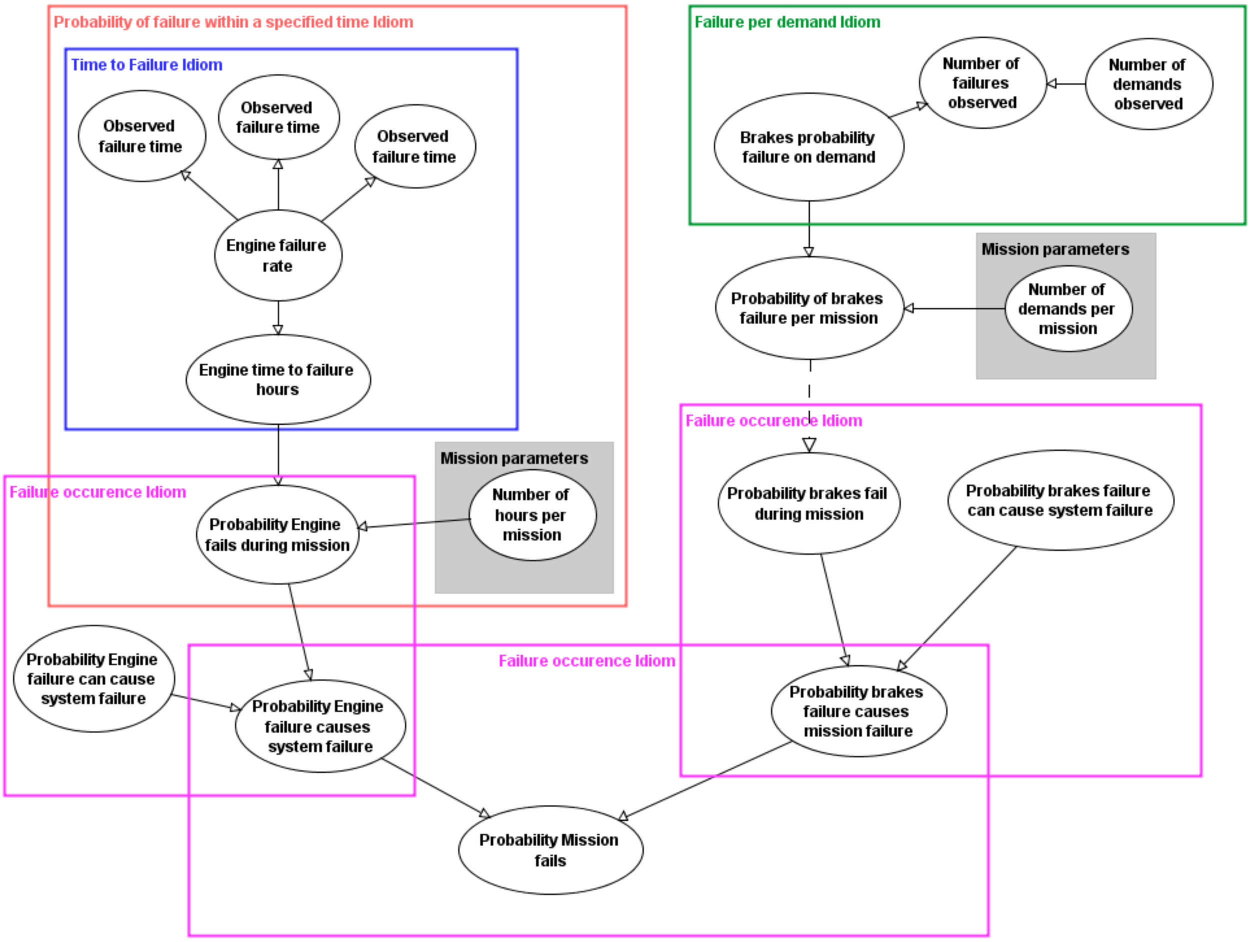

Probability of failure within a specified time Idiom
Time to Failure Idiom
Observed failure time
Observed failure time
Observed failure time
Engine failure rate
Engine time to failure hours
Mission parameters
Number of hours per mission
Failure occurence Idiom
Probability Engine fails during mission
Probability Engine failure can cause system failure
Probability Engine failure causes system failure
Failure occurence Idiom
Probability Mission fails
Failure per demand Idiom
Number of failures observed
Number of demands observed
Brakes probability failure on demand
Mission parameters
Probability of brakes failure per mission
Number of demands per mission
Failure occurence Idiom
Probability brakes fail during mission
Probability brakes failure can cause system failure
Probability brakes failure causes mission failure

Figure 74 Aircraft reliability BN with visible product safety idioms

In Figure 75, the BN model estimates the probability of failure for a military aircraft during a mission due to engine failure and braking system failure is 0.0008 (0.08%). In this example, we assume that for the engine, we observed failure times of 6000, 5000 and 4000 hours, respectively, and the engine is used for 6 hours during the mission. We assume that there is a 50% chance that the engine can cause a system failure. For the braking system, we assume that we observed 10 failures in 1000000 demands and that the braking system was used once during the mission. We also assume that there is a 50% chance that the braking system can fail. Please note that this BN model can be extended to incorporate other aircraft systems, such as flight control systems, to determine the overall reliability of an aircraft.

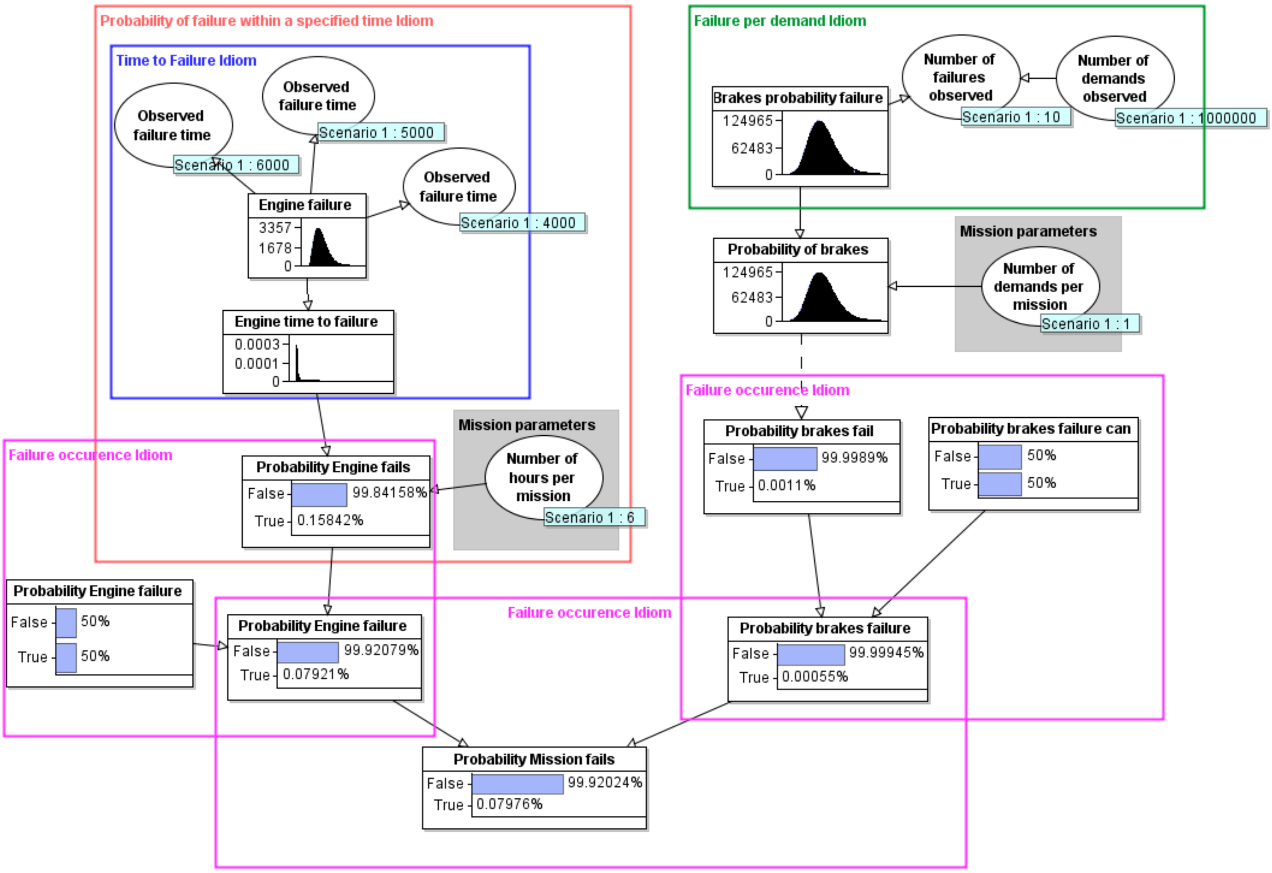


Figure 75 Aircraft reliability BN with observations

6.5 Benefits of Product Safety Idioms

The principal merit of the product safety idioms is to provide a robust systematic method and guide for building BNs for product safety risk management. The product safety idioms improve BN development in the following ways:

1. **Integration of different types of knowledge sources:** As demonstrated in Section 6.4.2, the idioms can combine objective evidence, e.g., PFD, and subjective evidence, e.g., manufacturing process quality, to provide

reasonable risk estimates for products. Combining objective and subjective evidence is especially useful for handling uncertainty in situations when there is limited or no historical testing and operational data for products, but expert knowledge is available.

2. **Handle uncertainty in data:** Some risks associated with products can be characterised by high levels of uncertainty and ambiguity. Uncertainty can be caused by limited or lack of relevant data. Product safety idioms can handle and communicate uncertainties in the data explicitly since they express uncertainty in terms of probability distributions.

3. **Standardise and assist product safety BN development:** To the best of our knowledge, there is no standard method for developing BNs specifically for product safety risk management. The product safety idioms improve BN development by simplifying the knowledge elicitation task. They provide a library of reusable BN patterns for product safety that facilitates the easy development of practical product safety BNs. They also guide the knowledge elicitation process by allowing model experts and safety risk professionals to identify relevant information (known or unknown) required to build custom idioms and BNs for product safety assessments.

4. **Enhance the communication, interpretability and explainability of complex BNs:** The graphical structure and results of the BNs developed using the idioms can be easily interpreted, explained, and reviewed by model experts and safety risk professionals. For example, the graphical structure of BNs facilitates easy communication of uncertainty and risks. Stakeholders can easily identify sources of uncertainty in the model. In addition, product safety idioms can serve as a validation method for future product safety risk BNs, ensuring that their structure is practical and logical.

6.6 BN Development and Validation Challenges

Despite the benefits of using the product safety idioms for BN development, it is important to note the challenges of accurately quantifying and validating the accuracy of the BN models. These challenges include:

1. Determining the number and meaning of node states, particularly where they relate to abstract attributes like, for example, '*Rework process Quality*' being *'High', 'Medium, or 'Low.'*

2. Quantifying and validating the strength of causal relationships.

3. Being confident that the aggregated results of the model are valid, in particular where independent data to validate against does not exist.

6.7 Chapter Summary

In this chapter, a novel set of idioms, called *product safety idioms,* for developing BNs specifically for product safety risk management are presented. The product safety idioms complement and extend the idiom-based approach proposed by Neil et al. [19] and other established methods of BN development discussed in previous research (see Section 4.3 and Section 5.2). While the proposed idioms are sufficiently generic to be applied to a wide range of product safety cases, they are not prescriptive or complete and should be considered as a guide for developing suitable idioms for product safety risk management (given available product-related information). As discussed in Section 6.5, the idioms offer the following benefits: handle uncertainty in data; standardise and assist product safety BN development; enhance communication, interpretability and explainability of complex BNs.

We believe that the product safety idioms discussed in this chapter are meaningful reasoning patterns that guide the development of complex BNs for product safety risk management. In the next chapter, we show how they are used to develop a generic BN for medical device risk management.

Chapter 7 Case Study 1: Medical Device Risk Management

In this chapter, a case study on medical device risk management is presented. This work was supported by medical device safety risk experts affiliated with Medtronic (a leading medical device company). The safety risk experts provided invaluable insights on medical device risk management and feedback on the proposed BN for medical device risk management. The BN approach complements and enhances existing medical device risk management approaches used in the industry.

In Section 7.1, medical device risk management is introduced. In Section 7.2, a brief overview of existing methods and their limitations for medical device risk management (previously discussed in Chapters 1 and 3) is presented. In Section 7.3, to address the limitations of existing risk analysis methods, we developed a generic BN for medical device risk management using the product safety idioms discussed in Chapter 6. In Section 7.4, we evaluate the proposed BN using different risk management scenarios, and the results are validated using real-world data. Finally, the results of the risk management scenarios and benefits of the proposed BN are discussed in Section 7.5.

This chapter supports Hypothesis 2 (it is possible to use Bayesian networks for safety risk management for many different types of products, including novel products or products with limited or no available data) and Hypothesis 3 (it is possible to use Bayesian networks to model consumer risk perception and/or perform benefits-risk analysis for products). Please note that the material presented in this chapter was previously presented in Publication 4 [24] published by Arxiv.org.

7.1 Overview of Medical Device Risk Management

Approximately 2 million medical devices are available on the world market [170]. They range from non-invasive devices, such as wheelchairs, to implantable devices, such as pacemakers. Despite the many benefits these devices offer, they can pose a serious risk to our health and safety when they fail. For example, failure of an AED defibrillator, such as LIFEPAK 1000, during patient treatment can expose patients to serious harm or death [171]. Therefore, the medical device industry requires that devices used by patients and healthcare professionals are acceptably safe. There are several standards for medical device safety, such as IEC 60601-1 [172], but ISO 14971 [7] is the primary standard used by medical device manufacturers. In fact, other standards for medical device safety make normative references to ISO 14971. This standard provides a framework for medical device manufacturers to manage the risks associated with medical devices throughout their life cycle (i.e., from initial conception to final decommissioning and disposal). It specifies a set of requirements and expectations for medical device risk management. For instance, ISO 14971 includes requirements for risk analysis (i.e., hazard identification and risk estimation), risk evaluation, risk control and evaluation of overall residual risk. However, ISO 14971 does not specify a particular method or process for medical device risk management. Hence, the methods used for medical device risk management by medical device manufacturers may vary due to the type of medical device and available information (e.g., testing data) and may require validation. In particular, there are several risk analysis methods for medical devices (discussed in Chapter 3), including the commonly used Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA). However, these classical risk analysis methods have limitations such as: unable to handle dependencies among system components; limited approach to handling uncertainty in data; limited approach to assessing the risk for novel products or products with limited or no historical data. These limitations are resolved using Bayesian networks (BNs) [13], [15], [18], [54], [110].

In this chapter, we propose a novel systematic method for medical device risk management using Bayesian networks (BNs) that: improves the handling of uncertainty; uses causal knowledge of the risk management process; incorporates relevant factors affecting the safety and risk of medical devices; complements existing medical device risk management tools and methods; uses quantitative data and expert judgement. Bayesian networks (BNs) are suitable for medical device risk management due to their ability to handle uncertainty and produce results using objective and subjective evidence [13], [76]. Also, they are used for safety risk assessment in several domains, including systems reliability, health, railway, finance and consumer product safety (see Chapter 5 for a review of BN applications in the safety domain). The proposed generic BN for medical device risk management provides a robust systematic method for medical device manufacturers to meet the requirements of ISO 14971.

Please note that the main standard referred to throughout this chapter is ISO 14971 [7] and its accompanying guidelines for application i.e., ISO/TR 24971 [6]. Unless other references are provided, all definitions in this chapter refer to this standard and its guidelines.

In the following subsections, we define medical devices and medical device risk management.

7.1.1 What is a medical device?

A *medical device* is "any instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination for a medical purpose" [7]. There are two main types of medical devices based on use, i.e., *single-use* and *multiple-use.* A *single-use medical device* is a medical device "intended to be used on an individual patient during a single procedure and then discarded" [173]. A *multiple-use (reusable) medical device* is a medical device "that health care providers can reprocess and reuse on multiple patients" [174]. Though single-use and multiple-use medical devices may contain software, the software can be considered a medical device on its own (Software as a medical device). *Software as a medical device* (SaMD) is "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware" [175]. Other classifications of medical devices include by purpose and by inherent risk [167] (see Table B1 and Table B2 in Appendix B for further information).

7.1.2 Medical Device Risk Management

Medical device risk management is the "systematic application of management policies, procedures and practices to the tasks of analysing, evaluating, controlling and monitoring risk" of medical devices [7]. Manufacturers of medical devices perform risk management for several reasons, including making safer products, legal and regulatory requirements, and cost savings [12]. The international standard for medical device risk management is ISO 14971[7]. This standard requires that medical device manufacturers have a documented process for managing the risks associated with medical devices. It specifies a set of requirements and expectations for the documented risk management process (see Figure 76) applicable to the complete life cycle of the medical device (i.e., from initial conception to decommissioning and disposal).

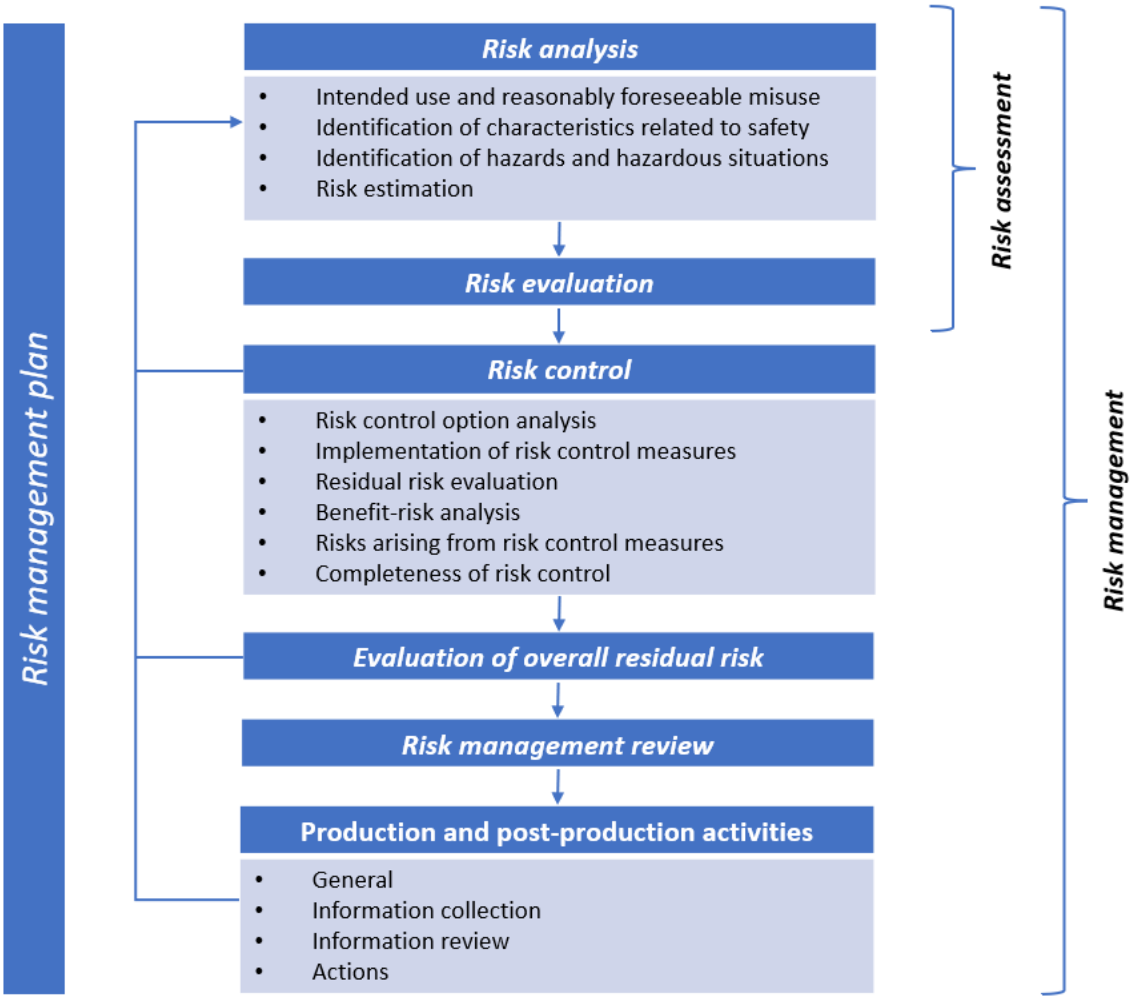

Risk management plan
Risk analysis
• Intended use and reasonably foreseeable misuse
• Identification of characteristics related to safety
• Identification of hazards and hazardous situations
• Risk estimation
Risk evaluation
Risk control
• Risk control option analysis
• Implementation of risk control measures
• Residual risk evaluation
• Benefit-risk analysis
• Risks arising from risk control measures
• Completeness of risk control
Evaluation of overall residual risk
Risk management review
Production and post-production activities
• General
• Information collection
• Information review
• Actions
Risk assessment
Risk management

Figure 76 ISO 14971 Risk Management Process

As shown in Figure 76, the ISO 14971 risk management process consists of the following activities:

1. ***Risk Management Plan***: ISO 14971 requires that all risk management activities are planned. The risk management plan includes the scope of risk management activities (medical device and life cycle phases), responsibilities and authorities for risk management activities, criteria for risk acceptability (i.e., the amount of risk judged acceptable) and verification and review activities.

2. ***Risk Analysis***: This phase consists of the following activities:
    a. ***Identify the intended use of the medical device***: The intended use, foreseeable misuse, intended users and intended use environment for the medical device are identified and documented.

    b. ***Identify the safety characteristics of the medical device***: The characteristics (quantitative and qualitative) of the medical device that can affect its safety are identified and documented.

    c. ***Identify hazards associated with the medical device***: All hazards associated with the use of the medical device are identified and documented. Techniques such as Preliminary Hazard Analysis (PHA) and FMEA (discussed in Chapter 3) are used to identify hazards associated with medical devices [6].

    d. ***Estimate the risk for each identified hazard***: In this phase, the risk associated with each hazard or hazardous situation is determined. The schematic shown in Figure 77 provides an overview of ISO 14971 risk estimation [7]. As shown in Figure 77, the *risk* is "the combination of the probability of occurrence of harm P and the severity of the harm S" i.e., $Risk = P \times S$. The probability of occurrence of harm P is the product of the probability of the hazardous situation occurring P_1 and the probability of the hazardous situation causing harm P_2, i.e., $P = P_1 \times P_2$. A *hazardous situation* is a "circumstance in which people, property, or the environment are exposed to one or more hazards", such as normal device use [7]. The severity of the harm is defined qualitatively using five (5) severity levels ranging from negligible injury to fatal injury (see Table B4 in Appendix B). Methods used to estimate risk include qualitative and semi-quantitative methods, such as a risk matrix and quantitative methods, such as the FTA (previously discussed in Chapter 3[12]).

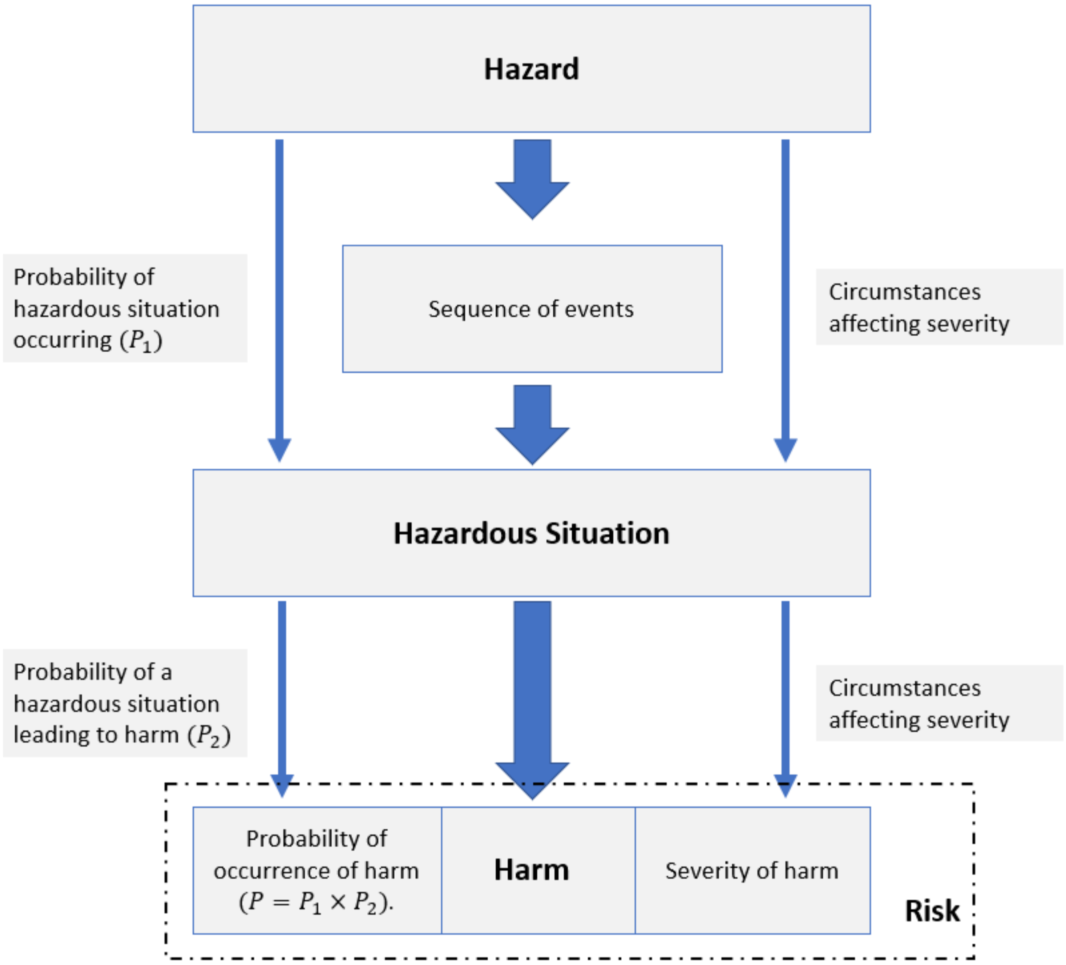

Hazard
Probability of hazardous situation occurring (P_1)
Sequence of events
Circumstances affecting severity
Hazardous Situation
Probability of a hazardous situation leading to harm (P_2)
Circumstances affecting severity
Probability of occurrence of harm ($P = P_1 \times P_2$).
Harm
Severity of harm
Risk

Figure 77 ISO 14971 Risk Estimation

3. ***Risk Evaluation***: The estimated risk for each hazard or hazardous situation is evaluated to determine risk acceptability using the criteria for risk acceptability (defined in the risk management plan). In situations where the estimated risk is judged not acceptable, risk control measures are implemented to reduce the risk to an acceptable level. However, when the estimated risk is judged acceptable, it is viewed as the *residual risk* (i.e., the risk remaining after risk control measures are applied).

4. ***Risk Control***: Appropriate risk control measures are used to reduce risks judged not acceptable to an acceptable level. Risk control measures for medical devices (in priority order) are inherently safe design and manufacture, protective measures and information for safety. Once risk control measures are implemented, the residual risk of the medical device is recalculated and re-evaluated. In situations where the risk is judged not acceptable, additional risk

control measures are implemented. However, when risk reduction is not practical, a benefit-risk analysis is done to determine if the benefit of the medical device outweighs its residual risk. The benefits of a medical device can be determined from several factors, including the patient population and the clinical outcome expected from the use of the device.

5. ***Evaluation of overall residual risk***: The overall residual risk is evaluated to determine whether it is acceptable given the risk acceptability criteria specified in the risk management plan. In situations where the overall residual risk is judged acceptable, manufacturers will inform users about significant residual risks. However, if the overall residual risk is judged not acceptable, additional risk control measures or rework may be implemented.

6. ***Risk Management Review***: The risk management plan is reviewed to ensure that it was implemented correctly and that the overall residual risk of the medical device is acceptable. The findings of the review are documented in the risk management report.

7. ***Production and Post-Production Activities***: Production and post-production activities are used to collect and review relevant information about the medical device during the production and post-production phases. The information obtained about the medical device is used to ensure that the medical device is acceptably safe for use and to inform future risk management activities. Examples of production and post-production activities include quality control testing, customer surveys and reviewing incident reports and databases.

7.2 Risk Analysis Methods and Limitations

As mentioned in Section 7.1, though ISO 14971 specifies the requirements for the risk management process, it does not specify a particular process or method for performing risk assessment and management for medical devices. Therefore, medical device manufacturers are free to develop or use appropriate risk management methods and processes to satisfy the requirements of ISO 14971. There are several methods for assessing the risk of medical devices (as discussed in Chapter 3), such as Preliminary Hazard Analysis (PHA), static Fault Tree Analysis (FTA) and Failure Mode and

Effects Analysis (FMEA). However, these classical risk analysis methods have the following limitations (as discussed in Section 1.3):

1. Limited approach to assessing the risk for novel products or products with limited or no historical data.
2. Unable to combine objective and subjective evidence to estimate risk.
3. Unable to handle variables with multiple states.
4. Does not consider the causal nature of the risk.

In this thesis, we propose using BNs to address all these limitations. The generic BN for medical device risk management is introduced in the next section.

7.3 Constructing the Medical Device Risk Management BN

In this section, we describe the process used to construct the Bayesian network for medical device risk management. This section is organised as follows. In Section 7.3.1, we present the scope, requirements and objectives of the BN. In Section 7.3.2, the way model variables are identified is described. In Section 7.3.3, we describe how the BN structure is developed, and in Section 7.3.4, we describe the process of parameter learning and elicitation.

7.3.1 Scope, requirements, and objectives of the BN

To determine the scope, requirements, and objectives of the BN for medical device risk management, a core team of three (3) domain experts reviewed the literature on medical device risk management and held discussions with medical device safety risk experts affiliated with Medtronic (a leading medical device company). The literature and medical device safety risk experts indicated that manufacturers of medical devices are required to perform risk management during production and post-production; hence the high-level requirements for the BN model were:

1. *Production Risk Management:* This involves predicting and evaluating the risk of a medical device before it is launched (i.e., predictive engineering) using design and production process information and real data collected from trials or previous systems.

2. *Post-production Risk Management*: This involves predicting and evaluating the risk of the medical device after it is launched (i.e., post-market risk management) using operational field data such as reported injuries and failures.

At the device level, the BN needs to:

1. Assess the reliability and risk of the device at all stages of development using subjective and objective evidence such as design and production process information and real data collected from trials or previous systems.
2. Handle the uncertainty in the data.
3. Provide quantified, auditable risk estimates for novel products or products with limited or no historical data.
4. Estimate the overall risk of the device considering the different types of injury risks and their criteria for risk acceptability.
5. Estimate the effect of rework or risk controls on the risk of the device.
6. Perform a benefit-risk analysis considering information about the benefits of the device and the estimated risk of the device.

Given the requirements of the BN model, we used a *soft systems* approach to risk and safety modelling. In this approach, we think of the system as a whole and analyse risks and safety at a high level based on soft factors related to the design, manufacture or use of the system. A soft systems approach was used since medical device risk management includes processes, people, procedures, as well as systems, machines and the interaction between all of these. However, we recognise that there are situations where a granular analysis that considers the causal interaction of each component of the system is required to estimate the overall risk of the system. In this case, the granular analysis can be performed using standalone BNs approaches (i.e., developing BNs for analysis of a particular system) or mapping approaches (i.e., translating risk analysis methods, such as Fault Tree Analysis, described in Chapter 3, using the mapping approaches described in Section 5.2 for analysis of a system). The results of a granular causal analysis can then be incorporated as priors or factors that affect the overall risk of the system (if available) in the proposed BN.

In the following subsections, we identify the model variables and develop the BN structure using the product safety idioms discussed in Chapter 6. Product safety idioms are suitable for BN development since they provide a library of reusable BN patterns for developing BNs for product safety risk management. In fact, the product safety idioms include BN patterns for modelling soft factors, such as the quality of the manufacturing process, and hard factors, such as the failure rate of the system.

7.3.2 Identifying Model Variables

Given the requirements of the BN model, the core team of three (3) domain experts identified relevant variables using the literature [6], [7], [12], [14], [54], [172], [176] and industry experience. The identified variables were organised into specific categories based on their purpose as follows:

1. *Reliability*: These are variables that are required to estimate the reliability of a system.
2. *Rework*: These are variables that are required to estimate the probability of repairing identified faults in a system.
3. *Requirement*: These are variables that are required to predict whether the system complies with defined operational and safety requirements.
4. *Manufacturer Process Quality:* These are variables that are required to estimate the quality of the design and production process for a system.
5. *Injury Occurrence*: These are variables that are required to estimate the likelihood of injury occurrence during use of the system.
6. *Risk:* These are variables that are required to estimate the overall risk of a system.
7. *Risk Evaluation:* These are variables that are required to evaluate the risk of a system.
8. *Benefits*: These are variables that are required to estimate the benefits of a system.
9. *Benefit-Risk Analysis*: These are variables that are required to perform a benefit-risk analysis.

For instance, in Table 13, we show the variables used in the BN to estimate the quality of the production process for a medical device. A complete table of all the variables included in the BN is presented in Appendix B.

Table 13 Variables used to estimate the quality of the production process

Variable Name	**Abbrev.**	**NPT**	**Category**
Process quality	pq	TNormal (pdri, 0.005, 0, 1)	Manufacturer Process Quality
Product defects	pdef	TNormal (pq, 0.05, 0, 1)	Manufacturer Process Quality
Process drifts	pdri	Ranked: (Major: 0.333, Minor: 0.333, None: 0.333)	Manufacturer Process Quality
Process additives	padd	TNormal (pq ,0.05, 0, 1)	Manufacturer Process Quality

7.3.3 BN Structure

To construct the BN structure, the groups of variables organised by purpose were matched against relevant idioms proposed in Chapter 6 and then implemented as instances of these idioms. For example, the variables identified to estimate the quality of the production process shown in Table 13 were matched with the quality idiom (see Section 6.2.4) and implemented as an instance of this idiom, as shown in Figure 78.

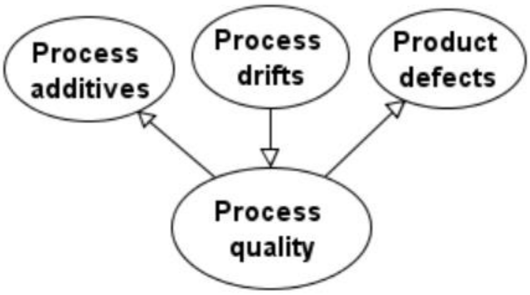


Figure 78 An instance of the quality idiom

Once each group of variables was implemented as instances of idioms, we combined them to construct the BN structure. However, instead of building the complete model altogether, we first built BN subnets for the main components, i.e., risk estimation and risk evaluation. Once the subnets were built, we then connected them using variables that were common to each of the subnets. Figure 79 shows schematically the structure and prediction process for the medical device risk management BN and Figure 80 shows the risk evaluation subnet that includes the benefits-risk analysis component. The complete BN, the model assumptions, and the instructions for using the BN are presented in Appendix B. Once the BN structure was completed, it was reviewed and agreed upon by the medical device safety risk experts.

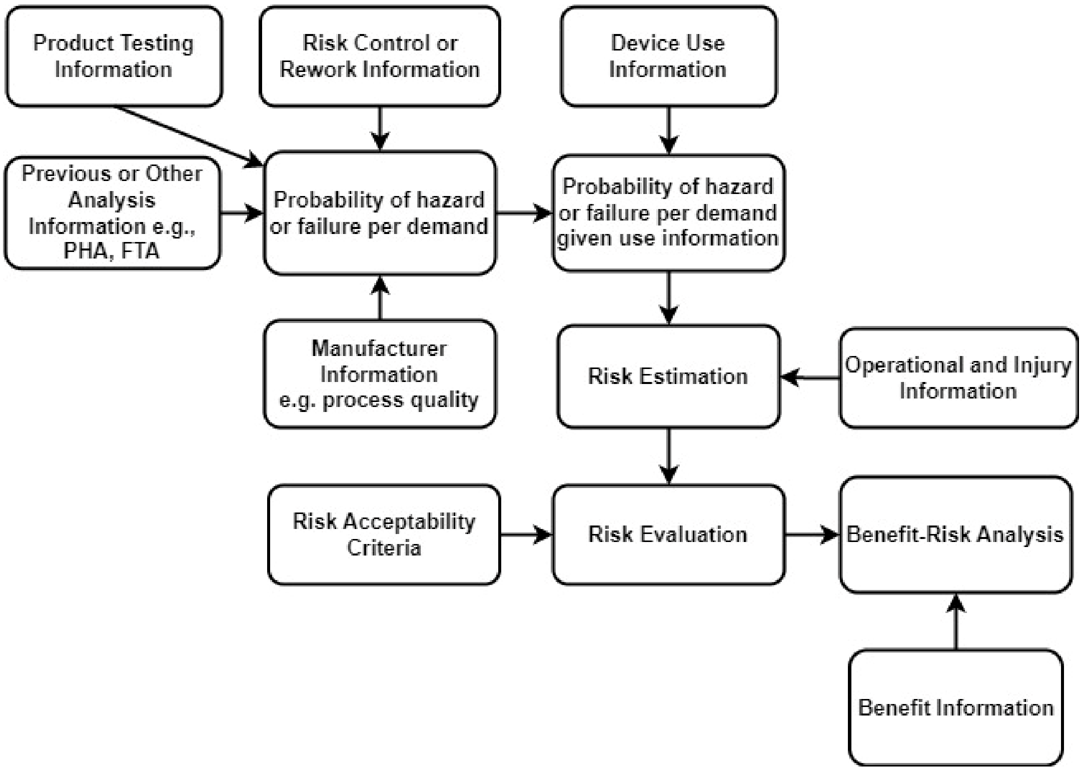

Product Testing Information
Risk Control or Rework Information
Device Use Information
Previous or Other Analysis Information e.g., PHA, FTA
Probability of hazard or failure per demand
Probability of hazard or failure per demand given use information
Manufacturer Information e.g. process quality
Risk Estimation
Operational and Injury Information
Risk Acceptability Criteria
Risk Evaluation
Benefit-Risk Analysis
Benefit Information

Figure 79 Schematic of Medical Device Risk Management BN

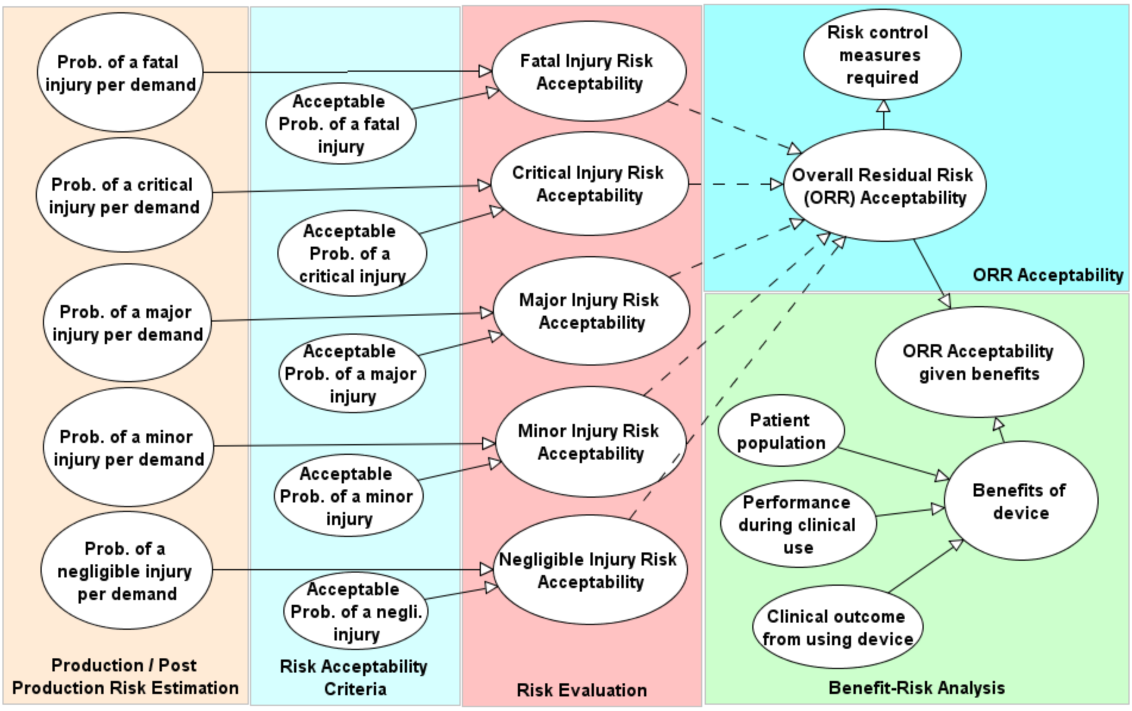

Prob. of a fatal injury per demand
Prob. of a critical injury per demand
Prob. of a major injury per demand
Prob. of a minor injury per demand
Prob. of a negligible injury per demand
Production / Post Production Risk Estimation
Acceptable Prob. of a fatal injury
Acceptable Prob. of a critical injury
Acceptable Prob. of a major injury
Acceptable Prob. of a minor injury
Acceptable Prob. of a negli. injury
Risk Acceptability Criteria
Fatal Injury Risk Acceptability
Critical Injury Risk Acceptability
Major Injury Risk Acceptability
Minor Injury Risk Acceptability
Negligible Injury Risk Acceptability
Risk Evaluation
Risk control measures required
Overall Residual Risk (ORR) Acceptability
ORR Acceptability
ORR Acceptability given benefits
Patient population
Performance during clinical use
Clinical outcome from using device
Benefits of device
Benefit-Risk Analysis

Figure 80 Risk Evaluation Subnet for Medical Device Risk Management BN

7.3.4 BN Parameters

The node probability tables (NPTs) for the variables in the BN (see Appendix B) were defined by the three (3) domain experts using ranked nodes, mathematical functions, statistical distributions, and comparative expressions. Ranked nodes [95] were used to define discrete variables whose states represent a ranked ordinal scale, for example, the *Benefits of device* node with states: ‘low’, ‘medium’, ‘high’. A ranked node maps the states of a variable to subintervals of a numerical scale [0,1]. Since ranked nodes use a numerical scale, their NPTs can be defined using statistical distributions. In the BN model, ranked nodes with parents are defined using a TNormal distribution with mean μ as a weighted function of its parents and variance σ^2, whereas ranked nodes without parents are defined using a Uniform distribution.

Mathematical functions were used to define the NPTs for some continuous (numeric) variables given their parents. For example, the NPT for the variable *probability of a fatal injury per demand* is the mathematical function: *probability of hazard per demand* × *probability hazard causes a fatal injury*.

Statistical distributions were used to define the NPTs for some continuous (numeric) variables based on their purpose. For instance, continuous variables without parents are defined using a Uniform distribution or a TNormal distribution given prior data for a medical device. Continuous variables with parents are defined using a TNormal distribution with mean μ as a weighted function of its parents and variance σ^2 or using a Binomial distribution, *B(n,p)*. Comparative expressions were used to define the NPTs for discrete variables with binary states. For instance, the NPT for the variable *Fatal injury risk acceptability* is defined using the following IF statement: *IF (prob. of fatal injury per demand <= acceptable fatal injury probability, "Acceptable", "Not Acceptable")*.

Please note that since this is a generic BN, the NPTs used for some of the variables in the BN will be revised, given the data and requirements for a particular medical device. In this case study, NPTs with statistical distributions include a sufficiently large variance to make them applicable to the different risk management scenarios used for model evaluation.

7.4 Model Validation

In this section, we evaluate the BN for medical device risk management by assessing the risk of a generic Defibrillator during production and post-production. We show how the BN can assess the risk of medical devices with available testing data and with little or no testing data. In Section 7.4.1, we present the Defibrillator case study, and in Section 7.4.2, we evaluate the BN using a range of hypothetical data scenarios for the generic Defibrillator. In Section 7.4.3, we validate the BN using publicly available real-world data from the LIFEPAK 1000 Defibrillator.

7.4.1 Case Study: Defibrillator Risk Assessment

This subsection presents the necessary background information for the Defibrillator case study.

1. ***Product Description*****:** An automated external defibrillator (AED) that sends an electric shock to the heart to treat serious heart arrhythmias, e.g., ventricular fibrillation. It is designed to be easy to use by trained users.
2. ***Hazard*****:** Incorrect shock advice.

3. ***Hazardous Situation*****:** The defibrillator gave an incorrect shock advice leading to asystole.
4. ***Injury Information*****:** Injuries range from normal sinus rhythm (negligible) to asystole (fatal).
5. ***Benefits Information*****:** The patient population is ‘very high’. Furthermore, the performance expected during clinical use is ‘high’, and the clinical outcome expected from the use of the device is ‘very high’.
6. ***Risk Acceptability Criteria*****:** We assume the following risk acceptability criteria presented in Table 14.

Table 14 Risk Acceptability Criteria for Defibrillator

Injury severity class	Probability of injury per demand
	Acceptable value (A)
Fatal	6.2E-5
Critical	9.9E-5
Major	2.5E-4
Minor	7.6E-3
Negligible	1.0E-2

7. ***Product Testing Information*****:** The product was tested ‘typical of normal use’. The test report reveals that there were 5 hazard occurrences in 1000 demands.
8. ***Rework Information*****:** The manufacturer’s rework process quality and effort are ‘very high’.
9. ***Manufacturer Information*****:** The manufacturer has been in operation for more than 20 years and has a very good safety record for medical devices. The manufacturer also has a ‘high’ customer satisfaction rating, and there are no product defects, process additives, or process drifts.
10. ***Reported Field and Injury Information***: Injury statistics for the defibrillator are based on data reported in a study that analysed the performance of AEDs used in the Netherlands between January 2012 and December 2014 [177]. According to the study data, there were “1091 shock advices in 3310 analysis periods (demands). 44 of the 1091 shock advices were incorrect. 15 incorrect shock advices were caused by device-related errors, and 28 were caused by operator-related errors”. Injuries caused by device-related errors include 3

asystole, 5 narrow complex tachycardia, 4 bradycardia, 2 normal sinus rhythms, and 1 multiple PVCs. Based on the injury severity classes used in the BN model (see Appendix B), we assume that asystole is a fatal injury, bradycardia, narrow complex tachycardia, and multiple PVCs are major injuries, and normal sinus rhythm is a negligible injury. Therefore, we assume 3 fatal injuries, 0 critical injuries, 10 major injuries,, 0 minor injuries and 2 negligible injuries given 15 incorrect shock advices.

7.4.2 Risk Management Scenarios and Results

In this subsection, we evaluate the model and its results using different risk management scenarios.

Scenario 1 – Production Risk Management (with available testing data)

In this scenario, we assess the risk of the Defibrillator given the information in Section 7.4.1.

Scenario 1 Results

The BN risk results for the Defibrillator are summarised in Table 15 (see Figure B5 in Appendix B for additional information).

Table 15 Defibrillator (with available testing data) BN risk results

Injury severity class	Probability of injury per demand		Risk Acceptability i.e., P (P <= A)	Overall Residual Risk (ORR) Acceptability Probability	ORR Acceptability Probability given Benefits	Probability additional risk control required
	Acceptable value (A)	Predicted value (P) (median)				
Fatal	6.2E-5	1.1E-3	1.3E-3	0.14	0.67	0.86
Critical	9.9E-5	2.07E-4	0.29			
Major	2.5E-4	3.25E-3	7E-4			
Minor	7.6E-3	2.07E-4	1			
Negligible	1.0E-2	8.0E-4	1			

According to Table 15, the BN model predicted that the median value of the probability distribution for fatal, critical, and major injuries per demand exceeded the risk acceptability criteria. When the median value of the risk distribution exceeds the acceptable value, this means that less than 50% of the predicted or estimated risk is acceptable. The BN shows the probability that the estimated risk is acceptable is 1.3E-3, 0.29 and 7E-4 for fatal, critical, and major injuries, respectively. Regarding the overall residual risk (ORR) per demand, the BN shows that the probability that it is acceptable is 0.14. However, given the benefits of the device, the probability that the ORR per demand is acceptable is 0.67. Finally, the BN predicts that the probability that additional risk controls are required to reduce risk to an acceptable level is 0.86. According to ISO 14971 [6], risk control options include inherent safe design and manufacture, protective measures and information for safety. Please note that although there is no available data for critical and minor injuries, the BN model provides reasonable probabilities estimates based on the number of reported hazards and other evidence in the model.

In Table 16 (see Figure B6 in Appendix B for additional information), we show the risk results if additional risk controls are implemented. As stated in Section 7.4.1, the manufacturer has a 'very high' quality rework process and effort.

Table 16 Defibrillator (with available testing data) BN risk results – Rework Information

Injury severity class	Probability of injury per demand		Risk Acceptability i.e., P (P <= A)	Overall Residual Risk (ORR) Acceptability Probability	ORR Acceptability Probability given Benefits	Probability additional risk control required
	Acceptable value (A)	Predicted value (P) (median)				
Fatal	6.2E-5	2.2E-4	0.045	0.29	0.72	0.71
Critical	9.9E-5	4.2E-5	0.78			
Major	2.5E-4	6.6E-4	0.044			
Minor	7.6E-3	4.2E-5	1			
Negligible	1.0E-2	1.6E-4	1			

Compared to the results presented in Table 15, the BN model revised the risk estimates given additional risk controls. Table 16 shows that the probability that the estimated risk is acceptable for fatal, critical, and major injuries per demand would increase to 0.045, 0.78 and 0.044, respectively. The probability of ORR acceptability would increase to 0.29, and given the benefits of the device, it would increase to 0.72. Although the probability that additional risk controls are required was reduced to 0.71, this result indicates that further risk controls are required to reduce risk to an acceptable level.

Scenario 2 – Production risk management (with limited or no testing data)

In this scenario, we assume that the defibrillator is a novel device with no testing data, and we have testing data from a previous similar defibrillator (5 hazards in 700 demands). We also assume that the P_1 estimate (i.e., probability of hazard per demand) for the novel device is also dependent on P_1 estimated from field data (ratio 60:40 i.e., $P_1 = (0.60 \times P_1\ test\ data) + (0.40 \times P_1\ field\ data)$). All other information used in the model is stated in Section 7.4.1.

Scenario 2 Results

The BN risk results for the Defibrillator are summarised in Table 17 (see Figure B7 in Appendix B for additional information). According to Table 17, the BN model predicted that the median value of the probability distribution for fatal, critical, and major injuries per demand exceeded the risk acceptability criteria. The BN shows that the probability that the estimated risk is acceptable is 3E-4, 0.23 and 0 for fatal, critical, and major injuries, respectively. Regarding the overall residual risk (ORR) per demand, the BN shows that the probability that it is acceptable is 0.13. However, given the benefits of the device, the probability that the ORR per demand is acceptable is 0.66. Finally, the BN predicts that the probability that additional risk controls are required to reduce risk to an acceptable level is 0.87.

Table 17 Defibrillator (with limited or no testing data) BN risk results

Injury severity class	Probability of injury per demand		Risk Acceptability i.e., P (P <= A)	Overall Residual Risk (ORR) Acceptability Probability	ORR Acceptability Probability given Benefits	Probability additional risk control required
	Acceptable value (A)	Predicted value (P) (median)				
Fatal	6.2E-5	1.4E-3	3E-4	0.13	0.66	0.87
Critical	9.9E-5	2.6E-4	0.23			
Major	2.5E-4	4.0E-3	0			
Minor	7.6E-3	2.6E-4	1			
Negligible	1.0E-2	1.0E-3	1			

Scenario 3 – Production risk management (generic data)

In this scenario, we assume that the defibrillator is a completely new device with no testing data and there are no relevant testing data from a previous similar device. We assume we are using generic probabilities for the hazard occurrence (see Table B5 in Appendix B for additional information). We assume that the hazard occurrence is probable (i.e., 1E-4 ≤ P_1< 1E-3), and the P_1 estimate for the novel device is also dependent on P_1 estimated from field data (ratio 60:40). All other information used in the model is stated in Section 7.4.1.

Scenario 3 Results

The BN risk results for the Defibrillator are summarised in Table 18 (see Figure B8 in Appendix B for additional information). According to Table 18, the BN model predicted that the median value of the probability distribution for fatal and major injuries per demand exceeded the risk acceptability criteria. The BN shows that the probability that the estimated risk is acceptable is 2.4E-3 and 0 for fatal and major injuries, respectively. Regarding the overall residual risk (ORR) per demand, the BN shows that the probability that it is acceptable is 0.20. However, given the benefits of the device, the probability that the ORR per demand is acceptable is 0.69. Finally, the BN predicts that the probability that additional risk controls are required to reduce risk to an acceptable level is 0.80.

Table 18 Defibrillator (with generic data) BN risk results

Injury severity class	Probability of injury per demand		Risk Acceptability i.e., P (P <= A)	Overall Residual Risk (ORR) Acceptability Probability	ORR Acceptability Probability given Benefits	Probability additional risk control required
	Acceptable value (A)	Predicted value (P) (median)				
Fatal	6.2E-5	4.8E-4	2.4E-3	0.20	0.69	0.80
Critical	9.9E-5	9.2E-5	0.53			
Major	2.5E-4	1.4E-3	0			
Minor	7.6E-3	9.2E-5	1			
Negligible	1.0E-2	3.5E-4	1			

Scenario 4 – Post-production risk management

In this scenario, we assume that we are reassessing the risk of a previous model of the defibrillator available on the market based on reported hazards and injuries. We assume 10,000 demands, 50 reports of incorrect shock advices resulting in 1 major injury and 49 negligible injuries. The risk acceptability criteria and benefits information used in the model is stated in Section 7.4.1.

Scenario 4 Results

The BN risk results for the Defibrillator are summarised in Table 19 (see Figure B9 in Appendix B for additional information). According to Table 19, the BN model predicted that the median value of the probability distribution for fatal injury per demand exceeded the risk acceptability criteria. The BN shows that the probability that the estimated risk is acceptable is 0.47. Regarding the overall residual risk (ORR) per demand, the BN shows that the probability that it is acceptable is 0.62. However, given the benefits of the device, the probability that the ORR per demand is acceptable is 0.85. Finally, the BN predicts that the probability that additional risk controls are required to reduce risk to an acceptable level is 0.38.

Table 19 Defibrillator (post-production) BN risk results

Injury severity class	Probability of injury per demand		Risk Acceptability i.e., P (P <= A)	Overall Residual Risk (ORR) Acceptability Probability	ORR Acceptability Probability given Benefits	Probability additional risk control required
	Acceptable value (A)	Predicted value (P) (median)				
Fatal	6.2E-5	6.8E-5	0.47	0.62	0.85	0.38
Critical	9.9E-5	6.8E-5	0.63			
Major	2.5E-4	1.6E-4	0.72			
Minor	7.6E-3	6.8E-5	1			
Negligible	1.0E-2	4.3E-3	1			

7.4.3 LIFEPAK 1000 Defibrillator

In this subsection, we validate the results of the model obtained in the risk management scenarios by assessing the risk of the LIFEPAK 1000 Defibrillator (Product Part Numbers: 320371500XX), which Physio-Control recalled in 2017 due to reports of the device shutting down unexpectedly during device use [171], [178]. This hazard can cause the device not to deliver therapy during use, exposing the patient to serious harm or death. A total of 133,330 devices were affected by this hazard. There were 34 reports of the hazard and 8 adverse events. In this example, we assume the risk acceptability criteria and benefits information stated in Section 7.4.1 since this information is not publicly available. We also assume that the number of potentially fatal injuries is 8 and the number of potentially minor injuries was 26 based on the injury reports. The BN model results are shown in Table 20 and Figure B10 in Appendix B.

According to the results of the model shown in Table 20, the BN model predicted that the median value of the probability distribution for fatal injuries per demand exceeded the risk acceptability criteria. The BN shows that the probability that the estimated risk is acceptable is 0.47 for a fatal injury. Therefore, the BN model validates and supports Physio-Control product recall decision (on the assumption that the probability of meeting the risk acceptability criteria for a fatal injury per demand to be at least 90%).

Table 20 BN model risk results for LIFEPAK 1000 Defibrillator

Injury severity class	Probability of injury per demand		Risk Acceptability i.e., P (P <= A)	Overall Residual Risk (ORR) Acceptability Probability	ORR Acceptability Probability given Benefits	Probability additional risk control required
	Acceptable value (A)	Predicted value (P) (median)				
Fatal	6.2E-5	6.3E-5	0.47	0.73	0.90	0.27
Critical	9.9E-5	5.1E-6	1			
Major	2.5E-4	5.1E-6	1			
Minor	7.6E-3	1.9E-4	1			
Negligible	1.0E-2	5.1E-6	1			

7.5 Discussion

The BN for medical device risk management developed with the support of medical device safety risk experts affiliated with Medtronic (a leading medical device company) can estimate the risk of medical devices during different stages of their life cycle. The Defibrillator case study shows that the BN model can estimate the risk of medical devices during production and post-production, with available relevant data and with limited or no relevant data. In Scenario 1 - Production risk management, the BN model estimated the risk and acceptability of the risk for the defibrillator given relevant information (see Table 15 and Table 16). In Scenario 2 - Production risk management (with limited or no testing data), the BN model estimated the risk and acceptability of the risk for the defibrillator given limited product testing data using manufacturer information and previous similar device data (see Table 17). In Scenario 3 - Production risk management (generic data), the BN model estimated the risk and acceptability for the defibrillator using generic probabilities of hazard occurrence along with manufacturer information and field data from other similar devices (see Table 18). In Scenario 4 - Post-production risk management and model validation using LIFEPAK 1000 defibrillator data, the BN model estimated the risk and acceptability of the defibrillator based on operational and injury information (see Table 19 and Table 20). In all scenarios, the risk estimate is comprehensive since the BN incorporates relevant factors that affect the risk of medical devices, such as the quality of the manufacturing process. Moreover, these factors are causally linked, supporting ease of interpretability and explanation of risk estimates. In fact, the BN model incorporates both discrete and continuous variables to estimate risk, illustrating the flexibility and power of using (hybrid) BNs to solve complex problems. The BN uses continuous variables with conditionally deterministic functions, statistical distributions and mixture distributions conditioned on different discrete assumptions. Furthermore, the BN can estimate risks using prior assumptions and learn parameters from observations (induction). Since the BN can easily revise risk estimates given new information, this allows easy risk management of any medical device throughout its life cycle.

The BN model also performs a benefit-risk analysis by estimating the risk acceptability given the benefits of the medical device (see Figure 80). The benefit of a medical device is the degree of improvement in a patient's health and clinical management that is expected from the use of that device. As shown in Figure 80, information such as device performance and clinical outcomes can help determine the benefit of a medical device [6]. A Benefit-Risk analysis is essential for informing risk management decisions such as product recalls, especially in situations where additional risk control measures are not applicable.

In situations where there are little or inadequate data to provide reasonable risk estimates for medical devices, the BN can incorporate data from previous similar devices, expert judgement, and manufacturer information to estimate the risk of the medical device. Previous similar device data, expert judgement and manufacturer information, can be included as prior distributions or values in the BN, as illustrated in Risk Management Scenario 2 and Scenario 3. Therefore, the BN model can estimate the risk of novel medical devices (i.e., devices with little or no historical data) with known or unknown hazards or faults since it can handle uncertainty and incomplete data, combine subjective and objective evidence, and revise risk estimates given new evidence. In situations where the BN is used to assess the risk of a continuous use medical device, the BN can estimate the failure rate by considering the mean and variance of the observed failure times (demands) and the mean and variance of the number of observed failures.

In situations where the BN is used to assess the risk of software, information such as development team experience is required to determine the quality of the software development process. The BN can be adapted using the Software BN fragment shown in Figure 81 to estimate the quality of the software development process. The quality of the software development process is then combined with the software failure data to provide a more accurate estimate of the probability of software failure. Like novel medical devices, the BN can provide reasonable risk estimates for new software with little or no testing data by combining previous similar software failure data, expert judgement and knowledge about the development process. The estimated risk for the new software will be revised, given new evidence throughout its life cycle, such as rework information (risk control measure) and injury information.

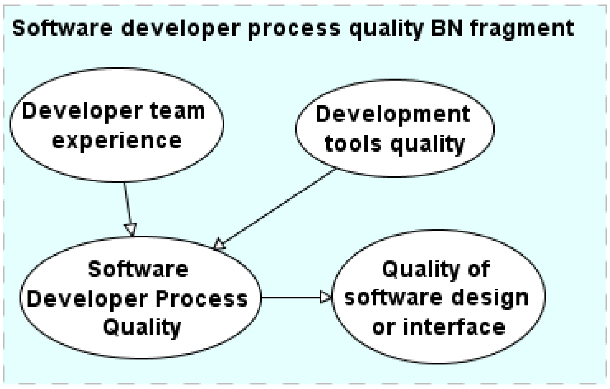

Software developer process quality BN fragment
Developer team experience
Development tools quality
Software Developer Process Quality
Quality of software design or interface

Figure 81 Software developer process quality BN fragment

In situations where the BN model is used to assess individual risk, the model can be extended to include information such as device use to estimate risk for a particular user. The BN model revises the P_1 (i.e., probability of hazard or failure) estimated from field data (or testing data) using device use information for that particular user. The revised P_1 estimate is then combined with P_2 (i.e., probability hazard causes an injury) computed from field data to estimate the risk of injury, as shown in Figure 82 (see Figure B4 in Appendix B for the complete BN subnet).

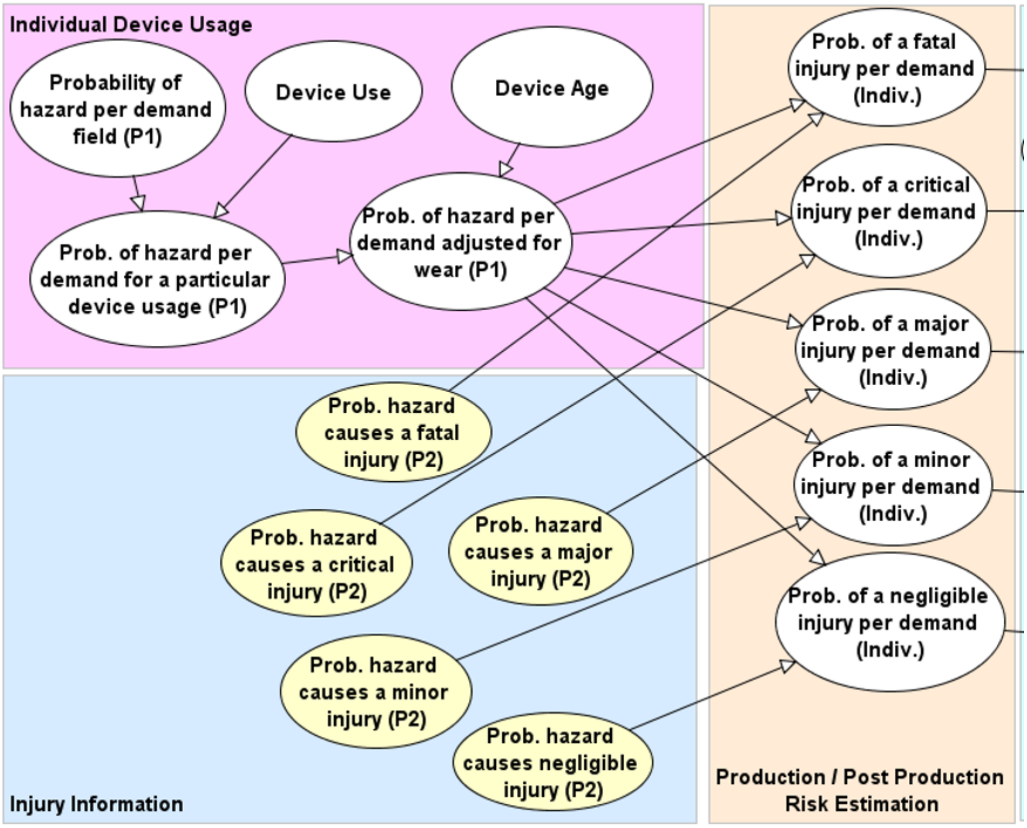

Individual Device Usage
Probability of hazard per demand field (P1)
Device Use
Device Age
Prob. of hazard per demand for a particular device usage (P1)
Prob. of hazard per demand adjusted for wear (P1)
Prob. hazard causes a fatal injury (P2)
Prob. hazard causes a critical injury (P2)
Prob. hazard causes a major injury (P2)
Prob. hazard causes a minor injury (P2)
Prob. hazard causes negligible injury (P2)
Injury Information
Prob. of a fatal injury per demand (Indiv.)
Prob. of a critical injury per demand (Indiv.)
Prob. of a major injury per demand (Indiv.)
Prob. of a minor injury per demand (Indiv.)
Prob. of a negligible injury per demand (Indiv.)
Production / Post Production Risk Estimation

Figure 82 Individual Device Use Information BN fragment

The BN for medical device risk management provides risk estimates for a single hazard; however medical devices usually have multiple hazards. We can combine the results of multiple hazards using a matrix or table. In the example shown in Table 21, the risk acceptability probability value for each class of injury for a particular hazard is obtained from the model, and we compute the combined risk acceptability probability values as the mean *μ* for each class of injury. We assume that all values included in the table are satisfactory. The risk acceptability table will allow risk assessors to determine the overall risk acceptability for the medical device given all its hazards.

Table 21 Risk Acceptability Table for multiple hazards

Risk Acceptability Table							
Hazards List	Risk Acceptability Probability					Overall Residual Risk (ORR) Acceptability Probability	ORR Acceptability Probability given Benefits
	Fatal Injury	Critical Injury	Major Injury	Minor Injury	Negligible Injury		
Hazard 1	0.89	0.6	0.8	0.25	0.3	0.67	0.85
Hazard 2	0.5	0.75	1	0.99	0.75	0.75	0.9
Combined Results (Mean)	0.7	0.68	0.9	0.62	0.53	0.71	0.875

Contributions and Limitations

The principal merit of the proposed generic BN for medical device risk management is to provide a robust systematic method for medical device manufacturers to manage the risk of medical devices throughout their life cycle (i.e., initial conception to final decommissioning and disposal). The generic BN for medical device risk management proposed in this thesis improves the risk assessment of medical devices in the following ways:

1. It provides a robust method for managing the risk of medical devices throughout their life cycle. The proposed BN incorporates different types of data (subjective and objective) to estimate the risk of a medical device at any

stage of the life cycle. It also explicitly shows the risk distribution for each type of injury and the overall combined risk.

2. It informs risk control measures/ risk treatment given the risk acceptability criteria. The BN predicts the need for additional risk control measures based on the defined risk criteria. It also supports iterative risk treatment.
3. It improves the interpretability and explanation of risk estimates. The graphical structure of the BN allows for easy communication and interpretation of uncertainty and risk.
4. It handles uncertainty in the data, especially for novel medical devices and software with little or no relevant historical data.
5. It provides individual risk estimates since it considers device use and device age information when estimating risk.
6. It supports market surveillance and review (post-market activities). The BN can easily update risk estimates given new information, such as reported injuries.
7. It complements existing risk management techniques and methods (see Chapter 3), such as Fault Tree Analysis (FTA) and Preliminary Hazard Analysis (PHA). This enables easy adoption of the proposed BN in the industry.
8. It improves benefit-risk analysis by considering information about the benefits of the medical device and the estimated risk. To the best of our knowledge, the proposed BN is the only method that automatically combines subjective information about benefits together with the estimated risk to determine risk acceptability for a medical device.

The main limitation of the case study is obtaining all relevant information for a medical device to perform risk assessment using the BN model. Since the results of the manufacturer’s safety and reliability tests are not publicly available, some of the data used to assess the risk of the defibrillator were fictitious, such as the risk acceptability criteria. Given actual data for medical devices such as LIFEPAK 1000, the BN can provide reasonable and auditable risk estimates.

In addition, the proposed BN was developed in the context of risk management done by manufacturers of medical devices (or product manufacturers in general); hence, its variables and structure are somewhat different from the consumer product safety risk assessment BN (discussed in Chapter 8) developed in the context of risk management done by national safety regulators and market surveillance authorities in the UK and EU.

7.6 Chapter Summary

This chapter serves as a good example for the practical use and benefits of the product safety idioms for BN development discussed in Chapter 6. By developing the BN for medical device risk management, we show that product safety idioms can be used to construct complex BNs in a modular fashion. In addition, this chapter demonstrates how manufacturers can use BNs for product safety risk management. The proposed BN for medical device risk management can handle uncertainty and incomplete data, estimate risks using prior assumptions, and learn parameters from observations (induction). It supports comprehensive and practical risk analysis since it decomposes the risk of a medical device into a causal chain of events, including risk controls, unlike the classical approach, i.e., $Risk = P \times S$. The BN also complements existing risk analysis methods such as FTA discussed in Chapter 3. The results of existing risk analysis methods can be incorporated into the BN to determine the risk of medical devices.

Additionally, the BN model informs risk management decisions by providing information on the acceptability of the risk and benefit-risk analysis. Finally, the BN resolves the limitations of existing methods, provides a standard systematic method for medical device risk management during production and post-production, is generalisable, and considers the ISO 14971 risk management process. Future work includes investigating the risk perception of medical devices since users may judge their risk and benefits differently from experts. For instance, experts tend to judge the risk of a product using quantitative risk assessments, whereas consumers judge risk using a combination of subjective measures such as risk propensity. The risk perception information can then be incorporated in the BN using the risk perception idiom discussed in Chapter 6.

Chapter 8 Case Study 2: Consumer Product Safety and Risk Assessment

In this chapter, a case study on consumer product risk assessment is presented. This work was supported by the UK Government Office for Product Safety and Standards (OPSS). In Section 8.1, the topic is introduced, while Section 8.2, provides an overview of product risk assessment and presents the RAPEX methodology. In Section 8.3, the limitations of the RAPEX methodology are presented. In Section 8.4, to address the limitations of the RAPEX methodology, we developed a generic BN for consumer product safety risk assessment using the product safety idioms discussed in Chapter 6. In Section 8.5, we evaluate the proposed BN by assessing the risk of consumer products with relevant data and with no relevant data. Finally, the results and benefits of the proposed BN are discussed in Section 8.6.

This chapter also supports Hypothesis 2 (it is possible to use Bayesian networks for safety risk management for many different types of products, including novel products or products with limited or no available data) and Hypothesis 3 (it is possible to use Bayesian networks to model consumer risk perception and/or perform benefits-risk analysis for products). Please note that the material presented in this chapter was previously presented in Publication 2 [15] published by the Journal of Safety Research.

8.1 Introduction

It is essential that the products we use in our homes are acceptably safe. To ensure our safety, national regulators perform product risk assessments to limit consumer harm [5], [8], [179], [180]. There are several different methods used for product risk assessment, including Nomograph [179] and Matrix [179], but RAPEX [5], [8], [179] is the primary method used by national safety regulators and market surveillance authorities (MSA) in the UK and EU.

While the RAPEX methodology is valid and useful, in this chapter, we identify a number of limitations of this methodology and explain the need for a systematic method for product risk assessment that: improves the management of uncertainty; uses causal knowledge of both the testing and operational environment and the process by which data are generated; is able to produce auditable quantified risk assessments even where there is limited product testing and instance data; considers the user population at risk and the product risk tolerability (acceptability).

We propose that Bayesian networks (BNs) can provide such a systematic method as they are a rigorous, normative method for modelling uncertainty and causality [13], [181]–[184]. We present a generic BN that significantly extends the previous work on BNs for product risk assessment. It incorporates hazard and injury data, product instances, manufacturer process information, product usage data, consumer benefits and risk perception to estimate product risk. The proposed generic BN also complements traditional risk assessment methods such as RAPEX. In the next section, we provide an overview of product risk assessment and the RAPEX methodology.

8.2 Overview of Product Risk Assessment and the RAPEX Methodology

A *product* is any physical non-food item offered in a market to meet consumer needs; it could be anything from a kitchen appliance to a toy (see Section 2.2.1). *Product risk assessment* is the overall process of determining whether a product is safe for consumers to use. Specifically, it is the process by which the level of risk associated with a particular (product) hazard is identified and categorised. The risk assessment process includes *risk analysis* and *risk evaluation* (see Figure 1) [8], [185]:

1. **Risk Analysis**: This phase involves hazard identification and risk estimation [185]. *Hazard identification* is the process of finding, recognising, and describing the hazards of the product. *Hazards* are potential sources of harm or injury and are intrinsic to the product [5], [8], [185]. *Risk Estimation* is the process of determining the risk level of the product. *Risk* is the combination of the likelihood of a hazard causing injury to a consumer and the severity of that injury. The *risk level* is the degree of the product risk on a scale from ‘low’ to ‘serious’ [5], [8].

2. **Risk Evaluation***:* The process by which the outcome of the risk analysis is combined with policy considerations to characterise the risk and inform decisions on risk management. It includes determining whether the risk is acceptable [8], [185].

As RAPEX is the most widely used method for evaluating the risk of consumer products by national safety regulators in the EU and the UK [5], [8], [185], this thesis will review the RAPEX methodology and its limitations.

8.2.1 The RAPEX Methodology

The EU Rapid Information System (RAPEX) risk assessment guidelines were developed for the rapid exchange of information between the Member States of the EU on measures and actions relating to products that pose a serious risk to the safety and health of consumers [5], [8]. An essential component of RAPEX is product risk assessment which determines the risk of a product and informs risk management response [5], [8]. The following steps or guidelines and schematic shown in Figure 83 describe the RAPEX methodology for assessing product risk:

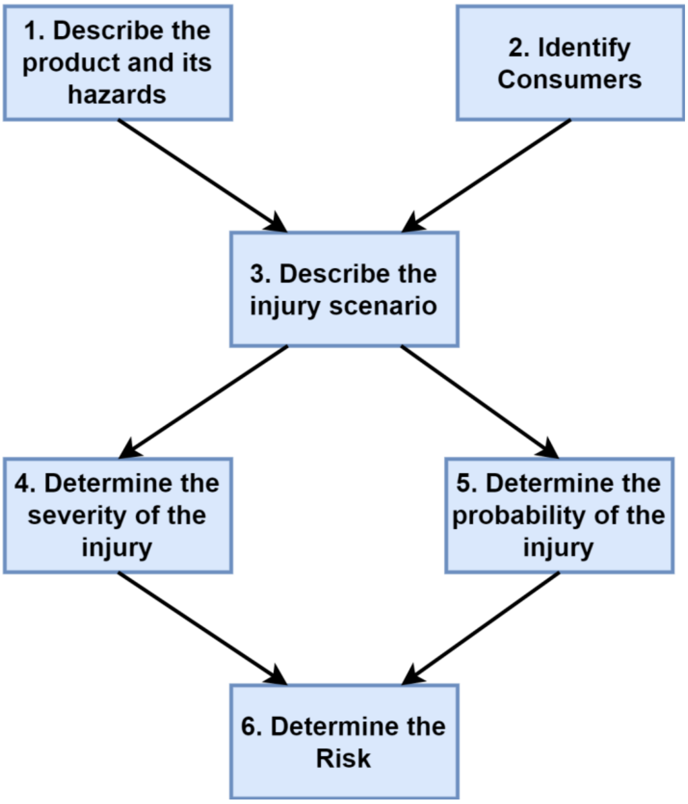

1. Describe the product and its hazards
2. Identify Consumers
3. Describe the injury scenario
4. Determine the severity of the injury
5. Determine the probability of the injury
6. Determine the Risk

Figure 83 Schematic flow of RAPEX risk assessment

1. ***Describe the product and its hazards***: Product details such as name, brand and model are documented during this stage. Hazards associated with products are identified by tests and standards or by the manufacturer’s product labelling and instructions. Identified hazards are classified using RAPEX’s hazard taxonomy, e.g., electrical energy, extreme temperatures and toxicity.

2. ***Identify consumers***: In this step, the consumers at risk are identified. Consumer types include intended users, non-intended users and vulnerable users.

3. ***Describe the injury scenario***: Injury scenarios that causally describe how the product hazard may harm the consumer via a series of steps are developed. Suppose we imagine that the product is an axe, an example of an injury scenario is “the axe breaks, and the ejected part strikes the user’s head”.

4. ***Determine the probability of injury***: Probabilities are assigned to each step of the injury scenario to determine the probability of injury. For example, to determine the probability of injury while using an axe, we combine the following probabilities:

   a. Probability of axe breaking = 1/100

   b. Probability of a broken part hitting the body = 1/10

   c. Probability of the broken part hitting the head = 1/10

   Total probability of injury = 0.01 × 0.1× 0.1 = 0.0001

   The probabilities used in this step are assumed to be independent and are obtained from what are assumed to be reliable sources, such as the European Injury Database and hospital injury databases.

5. ***Determine the severity of the injury***: The severity of the injury is determined by the type of medical intervention required for the injury scenario. The injury severity level and associated medical intervention are shown in Table 22.

Table 22 Injury severity level and associated medical intervention

Injury Severity Level	**Medical Intervention**
1	First Aid
2	Visit Accident and Emergency Department (A&E)
3	Hospitalisation
4	Fatal or loss of a limb(s)

For example, we assign a severity level of 2 for the injury scenario “an axe breaks and the ejected part strikes the user's head", since it may require a visit to A&E.

6. ***Determine the risk***: The risk of the product is determined using a risk matrix that combines the severity of the injury and the probability of the injury described in the injury scenario (see Table C1 in Appendix C for RAPEX's risk matrix). The estimated risk of the product will contain some level of uncertainty, since the probability of injury and severity of injury are estimated parameters. RAPEX handles uncertainty in the estimated risk using a sensitivity analysis which determines how variations in the estimated parameters (i.e., probability of injury and severity of injury) affect the overall risk result. It entails repeating the risk assessment process using different probabilities for the steps in the injury scenario and different injury severity levels. If the sensitivity analysis shows that there is no significant change in the risk, then there is increased confidence in the initial estimated risk. On the contrary, a significant change will reduce confidence and require a review of the estimated parameters. For example, if the risk of the axe is 'low' and the sensitivity analysis also shows that there is no significant change in the risk, then the risk of the axe is confidently considered as 'low'. However, a product can have many different risk levels due to many hazards, many injury scenarios or varying probabilities or severities of injuries. In these situations, the risk of the product is the highest risk level identified for that product.

8.3 Limitations of the RAPEX Methodology

Despite the widespread use of the RAPEX methodology, it has the following limitations:

1. *Limited approach to handling uncertainty:* In RAPEX, probabilities are assigned using point values instead of distributions (i.e., the assignment of probability values to each of the possible states of a random variable). RAPEX attempts to handle second-order uncertainty (i.e., the uncertainty in the estimation of the parameters of interest [186]) using a sensitivity analysis which entails repeating the risk assessment process using different probabilities for the steps in the injury scenario and different injury severity

levels. This method of handling uncertainty is not practical for probabilities that are not directly observable, nor where there is uncertainty about the data.

2. *Cannot be applied where there is little or no product data*: RAPEX cannot produce risk assessments for genuinely novel products (i.e., those for which little or no relevant historical data exist) or products for which limited testing data are available.

3. *Does not incorporate causal explanations for using and interpreting the data*: RAPEX provides no systematic or rigorous method for taking account of causal knowledge and explanations of the statistical data it uses, which may lead to inaccurate results. Also, RAPEX does not consider the causal factors that generate the data it uses since it assumes that the data is reliable because it is obtained from credible sources. The most general example is that lack of incident data for a product may be due to lack of reporting on the product rather than a lack of incidents, while, at the other extreme, multiple incidents associated with a product may be the result of testing the product beyond its intended scope.

4. *Does not differentiate between different types of users – i.e., their usage profile and risk tolerability (acceptability)*: In the RAPEX methodology, product risk is based on the likelihood of a product causing injury to a 'generic' user and the severity of that injury without any consideration of the context of use [5], [8], [179]. Hence, a product formally classified as 'high risk' may actually be 'low risk' or 'tolerable' for different classes of users, taking into account the way they use the product, the benefits they receive from it and risk controls and mitigants. Risk controls and mitigants vary for different types of users due to their knowledge of the hazard and the environment in which they use the product. For instance, users that are aware of a fire hazard from a device are likely to have a smoke alarm installed nearby, thus reducing the likelihood of injury, e.g., burn, even if the hazard occurs.

5. *Does not consider different product combinations and interactions with different classes of users when estimating product risk*: RAPEX's injury

scenario assumes that the events leading to an injury are independent and that the product is used by a user independent of other classes of products and users. Hence RAPEX cannot assess the injury scenarios with different product combination interactions with different classes of users—for example, the risk of an axe used by a student supervised by a trainer.

6. *Does not consider the user exposure to the risk*: RAPEX does not include the usage frequency when determining the probability of a product causing injury to a user. Usage frequency is essential to determining the probability of injury since injury can only occur during product use. For instance, a consumer that uses a product often will have a higher probability of being injured due to repeated exposure to the hazard when compared to a consumer that rarely uses the product.

7. *Does not include information on risk tolerability (acceptability)*: Risk tolerability (acceptability) is the trade-off between risk and benefits (or utility). For instance, a 'high risk' product may be considered 'tolerable' for some users since they value the benefits of the product sufficiently high and are willing to tolerate the 'high risk' as a trade-off for the benefits. Hence, risk tolerability is an essential component of product risk assessment since it informs risk management response to a non-compliant product.

8. *Does not consider increased risk of hazards over the lifetime of a product*: Due to wear and tear, the 'hazard rate' of a product will generally increase over time, with different classes of products having very different increasing hazard rates. An estimated hazard rate of a product – based only on testing instances of the product when new – will underestimate the true hazard rate of the product in operation.

9. *Cannot assess the risk of products with unknown hazards or unknown product usage information*: RAPEX cannot assess the risk of products, especially novel products, with unknown hazards or unknown product usage information since it requires an injury scenario to estimate product risk. Nor does it provide a method for recognising when novelty in hazard or usage arises.

Given the limitations of the RAPEX methodology, we propose using BNs for consumer product safety risk assessment. The generic BN for consumer product safety risk assessment is presented in the next section.

8.4 Constructing the Consumer Product Safety Risk Assessment BN

In this section, we describe the process used to construct the Bayesian network for consumer product safety risk assessment. This section is organised as follows. In Section 8.4.1, we present the scope, requirements and objectives of the BN. In Section 8.4.2, the way model variables are identified is described. In Section 8.4.3, we describe how the BN structure is developed, and in Section 8.4.4, we describe the process of parameter learning and elicitation.

8.4.1 Scope, requirements, and objectives of the BN

To determine the scope, requirements, and objectives of the BN for consumer product safety risk assessment, a core team of three (3) domain experts reviewed the literature on consumer product safety risk assessment and held discussions with senior government safety and risk experts. Given the limitations of the RAPEX methodology, the high-level requirements for the BN model were:

1. *Product Safety Risk Assessment:* This involves predicting and evaluating the risk of a (non-compliant) product using testing and operational data, information about the manufacturer, such as reputation, and other relevant information about the product, such as product use and age.

2. *Risk Perception and Risk Tolerability (Acceptability) Assessment*: This involves predicting risk perception and risk tolerability of the product using information about consumer risk perception (i.e., perceived benefits and risk) and risk communication, e.g., product recall.

At the product level, the BN needs to:

1. Assess the risk of the product using subjective and objective evidence such as manufacturer process information and real data collected from trials or previous systems.
2. Handle the uncertainty in the data.
3. Provide quantified, auditable risk estimates for novel products or products with limited or no historical data.
4. Estimate the overall risk of the product considering the different types of injury risks.
5. Estimate the effect of risk controls on the risk of the product.
6. Perform risk tolerability and risk perception analysis considering information about the perceived benefits and risk of the product.

Given the requirements of the BN model, we used a *soft systems* approach to risk and safety modelling. In this approach, we think of the product as a whole and analyse risks and safety at a high level based on soft factors related to the design, manufacture or use of the product. A soft systems approach was used since product risk assessment includes processes, people, procedures as well as systems, machines and the interaction between all of these. However, we recognise that there are situations where a granular analysis that considers the causal interaction of each component of the product is required to estimate the overall risk of the product. In this case, the granular analysis can be performed using standalone BNs approaches (i.e., developing BNs for analysis of a particular product) or mapping approaches (i.e., translating risk analysis methods, such as Fault Tree Analysis, described in Chapter 3, using the mapping approaches described in Section 5.2 for analysis of a product). The results of a granular causal analysis can then be incorporated as priors or factors that affect the overall risk of the product (if available) in the proposed BN.

In the following subsections, we identify the model variables and develop the BN structure using product safety idioms discussed in Chapter 6. Product safety idioms are suitable for BN development since they provide a library of reusable BN patterns for modelling soft factors, such as the quality of the manufacturing process, and hard factors, such as the failure rate of the product.

8.4.2 Identifying Model Variables

Given the requirements of the BN model, the core team of three (3) domain experts identified relevant variables using the literature [5], [8], [185] and industry experience. The identified variables were organised into specific categories based on their purpose as follows:

1. *Reliability*: These are variables that are required to estimate the reliability of a product e.g., failure and hazard rates.
2. *Requirement*: These are variables that are required to predict whether a product complies with defined operational and safety requirements.
3. *Manufacturer Process Quality:* These are variables that are required to estimate the quality of the design and production process for a product.
4. *Injury Occurrence*: These are variables that are required to estimate the likelihood of injury occurrence during product use.
5. *Risk:* These are variables that are required to estimate the overall risk of a product.
6. *Risk Tolerability (Acceptability):* These are variables that are required to evaluate the risk tolerability for a product.
7. *Benefits*: These are variables that are required to estimate the benefits of a product.
8. *Risk Perception*: These are variables that are required to estimate the perceived risk of a product.

For instance, in Table 23, we show the variables used in the BN to estimate the quality of the production process for a product. A complete table of all the variables included in the BN is presented in Appendix C.

Table 23 Variables used to estimate the quality of the production process

Variable Name	**Abbrev.**	**NPT**	**Category**
Product design	prod_design	TNormal (m_quality,0.05, 0, 1)	Manufacturer Process Quality
Years in operation	years_operating	Ranked: (< 1 year: 0.2, 1 - 5 years: 0.2, 5 - 10 years: 0.2, 10 - 20 years: 0.2, 20+ years: 0.2)	Manufacturer Process Quality
Manufacturer reputation	reputation	Ranked: (Disreputable: 0.33333334, Reputable: 0.33333334, Highly Reputable: 0.33333334)	Manufacturer Process Quality
Customer satisfaction	cust_sat	TNormal (m_quality,0.05, 0, 1)	Manufacturer Process Quality
Manufacturer process quality	m_quality	TNormal (wmean (1.0,years_operating,2.0,reputation),0.001,0, 1))	Manufacturer Process Quality

8.4.3 BN Structure

To construct the BN structure, the groups of variables organised by purpose were matched against relevant idioms proposed in Chapter 6 and then implemented as instances of these idioms. For example, the variables identified to estimate the quality of the production process shown in Table 23 were matched with the quality idiom (see Section 6.2.4) and implemented as an instance of this idiom as shown in Figure 84.

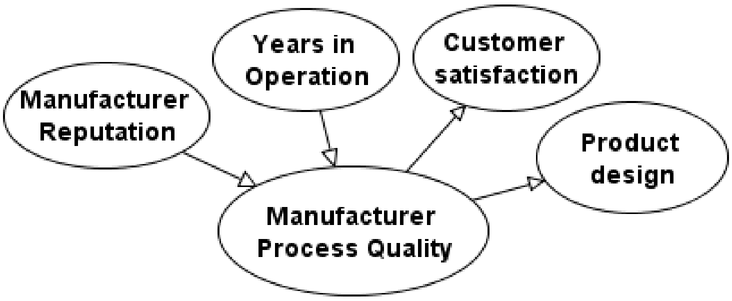


Figure 84 An instance of the quality idiom

Once each group of variables was implemented as instances of idioms, we combined them to construct the BN structure. However, instead of building the complete model altogether, we first built BN subnets for the main components, i.e., risk estimation and risk tolerability/risk perception. Once the subnets were built, we then connected them using variables that were common to each of the subnets. The complete BN structure was then presented for discussion in a workshop with six (6) senior government safety and risk experts and was revised accordingly both at the workshop and in subsequent iterations (mainly by email as, due to the Covid-19 crisis, no further in-person workshops were conducted). A consensus on the proposed BN model was reached when the model included all relevant variables (connected causally) required for product risk assessment. Figure 85 shows schematically the structure and prediction process for the consumer product safety risk assessment BN. Figure 86 and Figure 87 show the BN subnet for risk estimation and risk evaluation, respectively. Please see Appendix C for larger images of these subnets, the model assumptions, and the instructions for using the BN.

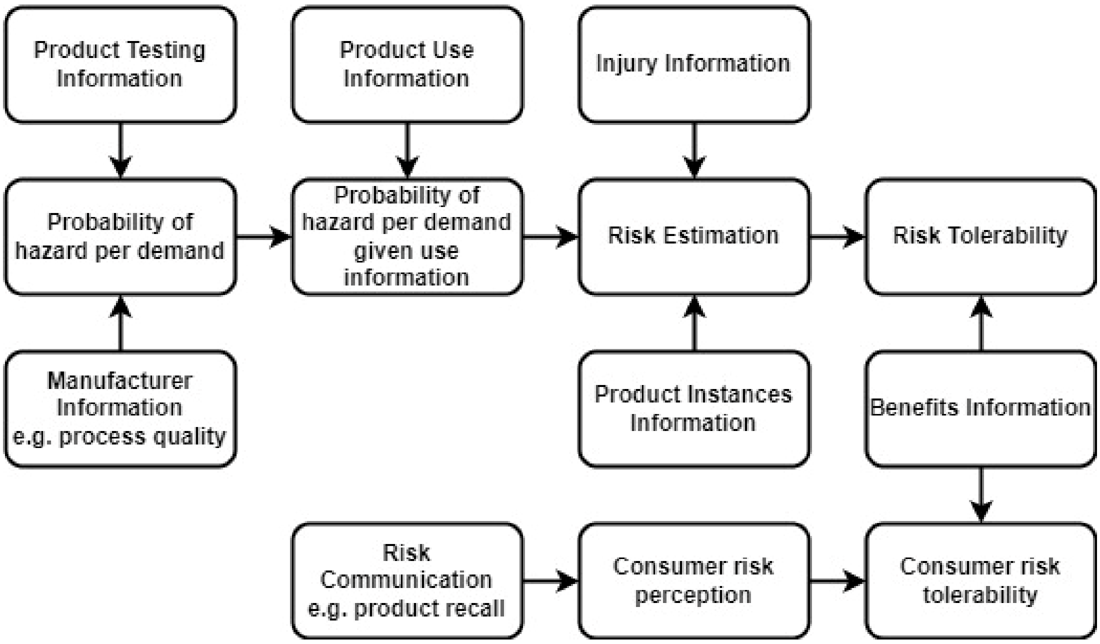

Product Testing Information
Product Use Information
Injury Information
Probability of hazard per demand
Probability of hazard per demand given use information
Risk Estimation
Risk Tolerability
Manufacturer Information e.g. process quality
Product Instances Information
Benefits Information
Risk Communication e.g. product recall
Consumer risk perception
Consumer risk tolerability

Figure 85 Schematic of Consumer Product Safety Risk Assessment BN

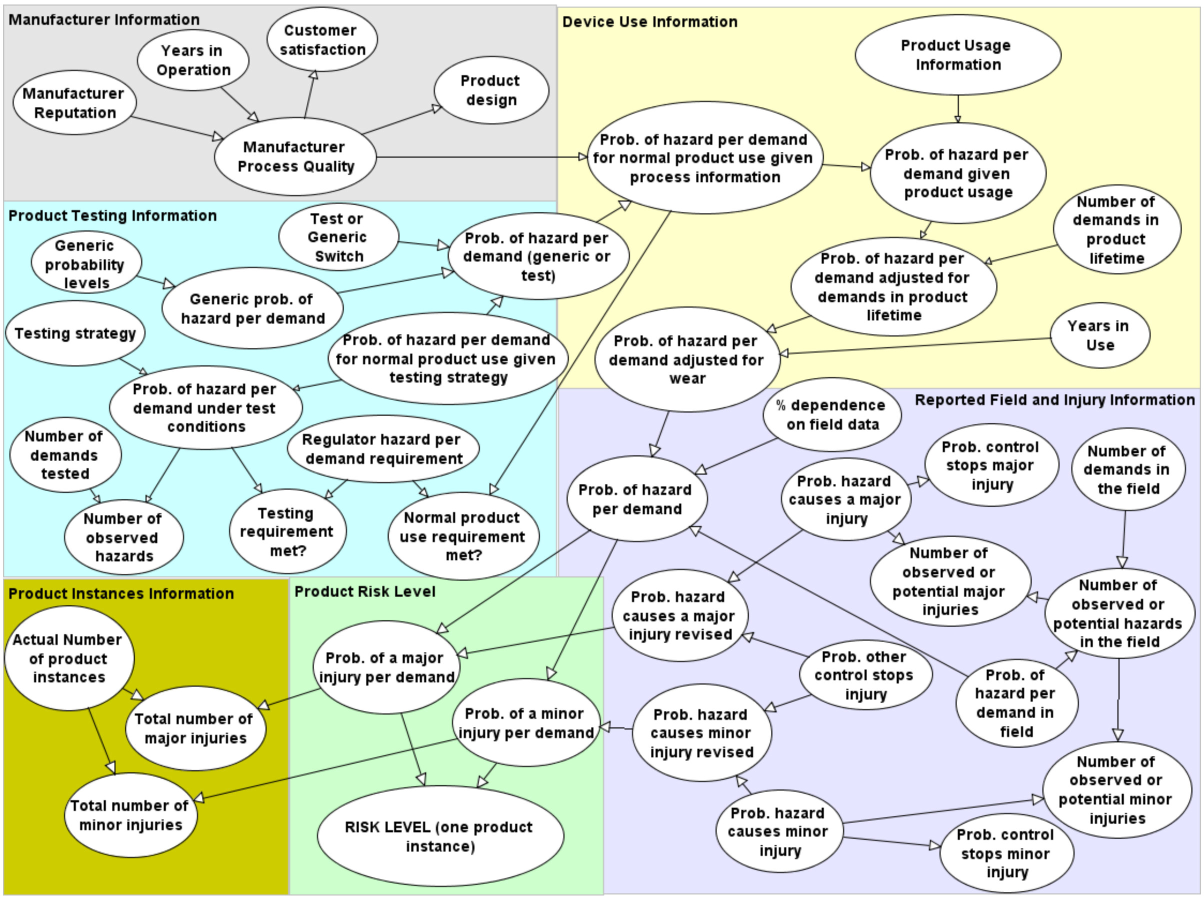

Manufacturer Information
Customer satisfaction
Years in Operation
Manufacturer Reputation
Product design
Manufacturer Process Quality
Device Use Information
Product Usage Information
Prob. of hazard per demand for normal product use given process information
Prob. of hazard per demand given product usage
Number of demands in product lifetime
Prob. of hazard per demand adjusted for demands in product lifetime
Years in Use
Prob. of hazard per demand adjusted for wear
Product Testing Information
Test or Generic Switch
Generic probability levels
Prob. of hazard per demand (generic or test)
Generic prob. of hazard per demand
Testing strategy
Prob. of hazard per demand for normal product use given testing strategy
Prob. of hazard per demand under test conditions
Number of demands tested
Regulator hazard per demand requirement
Number of observed hazards
Testing requirement met?
Normal product use requirement met?
Reported Field and Injury Information
% dependence on field data
Prob. control stops major injury
Number of demands in the field
Prob. hazard causes a major injury
Prob. of hazard per demand
Number of observed or potential major injuries
Number of observed or potential hazards in the field
Prob. hazard causes a major injury revised
Prob. other control stops injury
Prob. of hazard per demand in field
Prob. hazard causes minor injury revised
Number of observed or potential minor injuries
Prob. hazard causes minor injury
Prob. control stops minor injury
Product Instances Information
Actual Number of product instances
Total number of major injuries
Total number of minor injuries
Product Risk Level
Prob. of a major injury per demand
Prob. of a minor injury per demand
RISK LEVEL (one product instance)

Figure 86 Consumer Product Risk Assessment BN - Risk Estimation Subnet

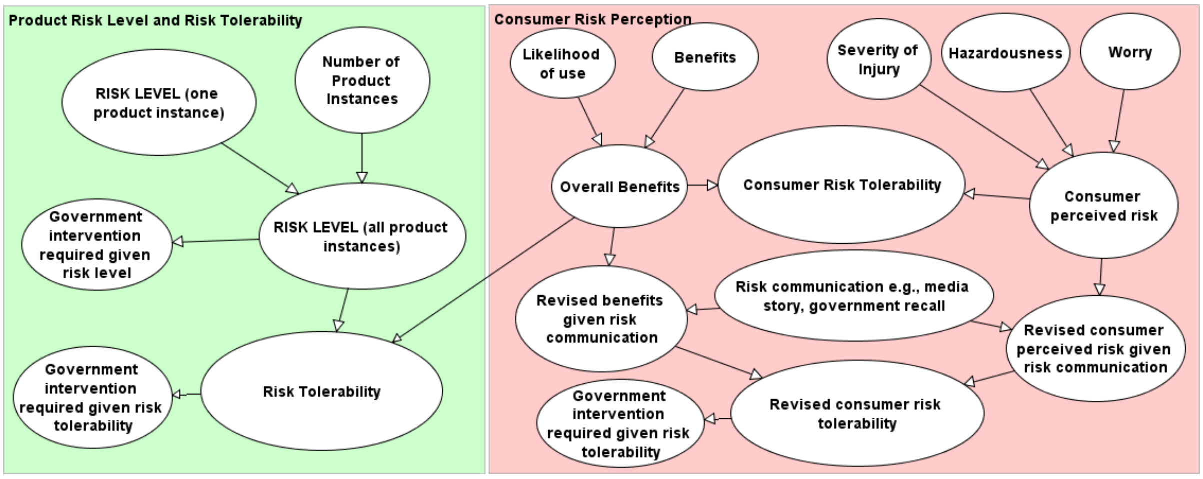

Product Risk Level and Risk Tolerability
Number of Product Instances
RISK LEVEL (one product instance)
Government intervention required given risk level
RISK LEVEL (all product instances)
Government intervention required given risk tolerability
Risk Tolerability
Consumer Risk Perception
Likelihood of use
Benefits
Severity of Injury
Hazardousness
Worry
Overall Benefits
Consumer Risk Tolerability
Consumer perceived risk
Risk communication e.g., media story, government recall
Revised benefits given risk communication
Revised consumer perceived risk given risk communication
Government intervention required given risk tolerability
Revised consumer risk tolerability

Figure 87 Consumer Product Safety Risk Assessment BN - Risk Evaluation Subnet

8.4.4 BN Parameters

The node probability tables (NPTs) for the variables in the BN (see Appendix C) were defined by the three (3) domain experts using ranked nodes, mathematical functions, statistical distributions, and comparative expressions. Ranked nodes [95] were used in the BN model to represent discrete variables with states expressed on an ordinal scale, e.g., *Customer satisfaction* node with states (*very low, low, medium, high, very high*). A ranked node maps the variable states to an underlying numerical scale ranging from 0 to 1 in equal intervals. Given the underlying numerical scale, the NPT for a ranked node can be defined as a statistical distribution such as a truncated normal distribution (TNormal) with mean μ and variance $\sigma^{2,}$ i.e., *TNormal* (μ, σ^2). In the BN model, the NPT for a ranked node without parents is a uniform distribution (i.e., the probability of each state is the same). The NPT for a ranked node with parents is a TNormal distribution with mean μ defined as the weighted average of its parents and variance σ^2.

Standard mathematical or statistical assumptions and distributions were used to define the NPT for numeric variables (nodes) in the BN model. For example, the NPT for *Number of times hazard observed* node is a Binomial(n,p) distribution where n is the number of demands made during testing and p is the probability of observing a hazard per demand. The NPT for some numeric nodes is deterministic and self-explanatory; for instance, the NPT for *Probability the hazard causes a major injury* node is an arithmetic expression, i.e., *probability of uncontrolled hazard causing a major injury x* (*1 – probability of control stops injury*). The NPT for numeric nodes without parents is a uniform distribution, and those with parents are a TNormal distribution. The mathematical expressions and statistical distributions used to define the NPT for each numeric node are dependent on the function of the node, its input, and its output. Comparative expressions were used to define the NPT for discrete variables with binary states and parents. For instance, the NPT for *Government intervention required given risk level* node with states (True, False) and parent *Risk level* is an IF statement i.e., *if (risk_level > 0.5,"True","False").*

Although the proposed BN structure and variables are relevant for assessing the risk of any consumer product, it is important to note that the NPT for some of these variables will be revised given specific data about a particular product or class of product. However, NPTs with prior statistical distributions are defined with a sufficiently large variance to enable them to be applied to the very different product examples used to evaluate and validate the model in Section 8.5.

8.5 Model Validation

In this section, we evaluate the BN for consumer product safety risk assessment by comparing the process and results of the BN and the RAPEX methodology in terms of their ability to assess the risk of products with relevant data, e.g., Teddy Bear (Section 8.5.1) and products with limited or no relevant data, e.g., a new uncertified kettle (Section 8.5.2).

8.5.1 Case Study 1: Teddy Bear

In the UK and the EU, the RAPEX methodology is used by safety regulators and market surveillance authorities to assess the risk associated with toys identified as non-compliant to prevent harm to children. In this case study, we evaluated the BN by assessing the risk of a teddy bear using two hypothetical scenarios and compared the results with the RAPEX methodology.

8.5.1.1 Background Information

This subsection presents the necessary background information and assumptions for the teddy bear risk scenarios.

1. ***Product Description*:** Brown teddy bear with a bow
2. ***Hazard and Injury Scenario*:** The eyes and suction cup can easily detach from the toy, generating small parts; the detached part is swallowed by a child resulting in an injury.
3. ***Benefits Information*:** The likelihood of use and benefits of the teddy bear is moderate.
4. ***Reported Field and Injury Information*:** We assume that injury reports for the teddy bear indicate that there were 10 hazard occurrences with 1 major injury and 2 minor injuries.
5. ***Consumer risk perception*:** Consumers perceive the severity of the injury and hazardousness of the teddy bear as ‘high’ and are very worried about the risk of injury. There is no risk communication such as a product recall.
6. ***Product Testing Information*:** The product was tested ‘typical of normal use’. The test report reveals that there was one hazard occurrence (the eye detached) in 5000 demands.

7. ***Product Instances Information*****:** There are 20,000 teddy bears available on the market.
8. ***Manufacturer Information*****:** The manufacturer has been in operation for 5-10 years and is from a country with a good safety record for toys. The manufacturer also has a ‘high’ customer satisfaction rating, and there are no changes in product design (i.e., product design is the same as previous similar products).

8.5.1.2 Risk Scenarios and Results

In this subsection, we evaluate the BN model and the RAPEX methodology using different risk scenarios for the teddy bear.

Scenario 1 Description

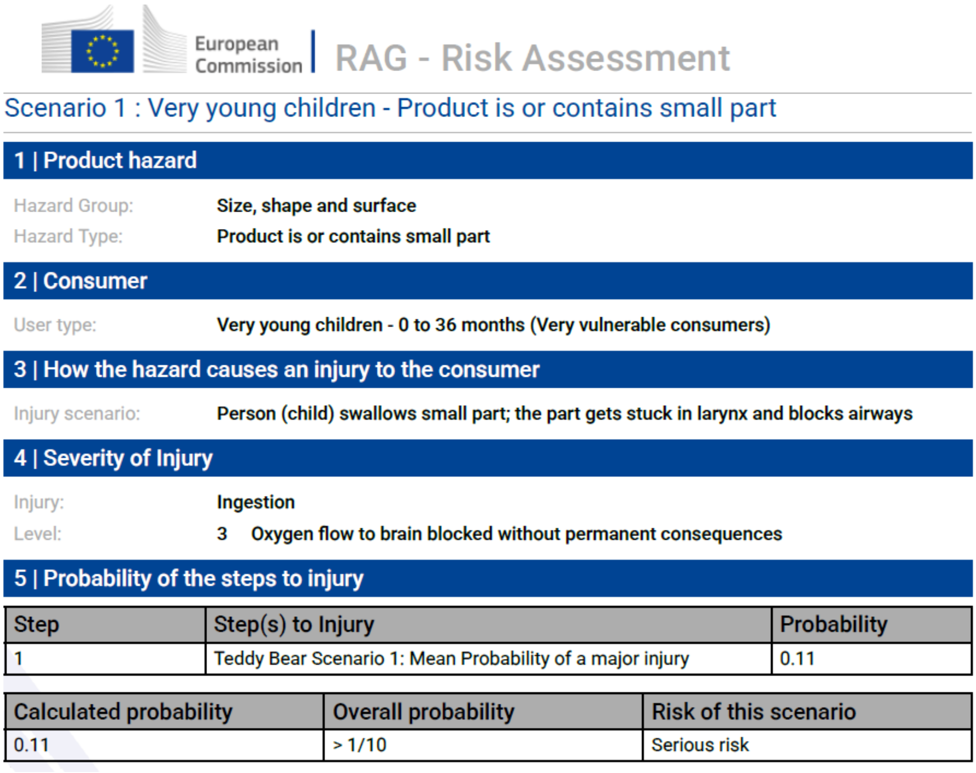
In this scenario, we assume that the teddy bear is used by a child aged 0-36 months as intended for one year with a high number of demands (i.e., 4000) and no carer intervention (i.e., the child is not sufficiently supervised so the carer cannot take away the small detached part, e.g. teddy bear eye, before it is ingested by the child). All other information used in the BN is the same as presented in the background information.

Scenario 1 - BN Results

The BN model (see Figure C4 in Appendix C) learns that the risk level for the teddy bear is ‘very high’ with little uncertainty. The BN model calculates that the mean probability of a major injury (per demand) for this scenario is 0.11 and for a minor injury (per demand) it is 0.17. It also calculates that the mean number of potential major and minor injuries for 20,000 product instances is 2325 and 3478, respectively. Regarding risk tolerability and consumer risk perception, the BN model shows that the risk tolerability for the teddy bear is ‘low’ or ‘very low’ given the benefits and consumers perceive the risk of the teddy bear as ‘high’. Finally, the BN predicts that a government intervention, such as a product recall, is required.

Scenario 1 - RAPEX Results

One of the limitations of the RAPEX methodology is that it does not consider the number of demands for a particular product when determining risk. So, although we are unable to make a direct comparison to the BN model, we can compare the product risk result of the BN model to the RAPEX methodology by using the mean probability of a major injury (per demand) learnt by the BN model as the probability of injury for the RAPEX method. In the RAPEX method, we set the injury severity level to ‘3’ as this corresponds to a major injury such as internal airway obstruction. The RAPEX method assesses the risk level of the teddy bear as ‘serious’, as shown in Figure 88. This result is the same as the BN model, even though the BN model also uses the probability of a minor injury and product instances to compute the risk of the product.



European Commission | RAG - Risk Assessment

Scenario 1 : Very young children - Product is or contains small part

1 | Product hazard

Hazard Group: Size, shape and surface
Hazard Type: Product is or contains small part

2 | Consumer

User type: Very young children - 0 to 36 months (Very vulnerable consumers)

3 | How the hazard causes an injury to the consumer

Injury scenario: Person (child) swallows small part; the part gets stuck in larynx and blocks airways

4 | Severity of Injury

Injury: Ingestion
Level: 3 Oxygen flow to brain blocked without permanent consequences

5 | Probability of the steps to injury

Step	Step(s) to Injury	Probability
1	Teddy Bear Scenario 1: Mean Probability of a major injury	0.11

Calculated probability	Overall probability	Risk of this scenario
0.11	> 1/10	Serious risk

Figure 88 RAPEX results for Teddy Bear Scenario 1

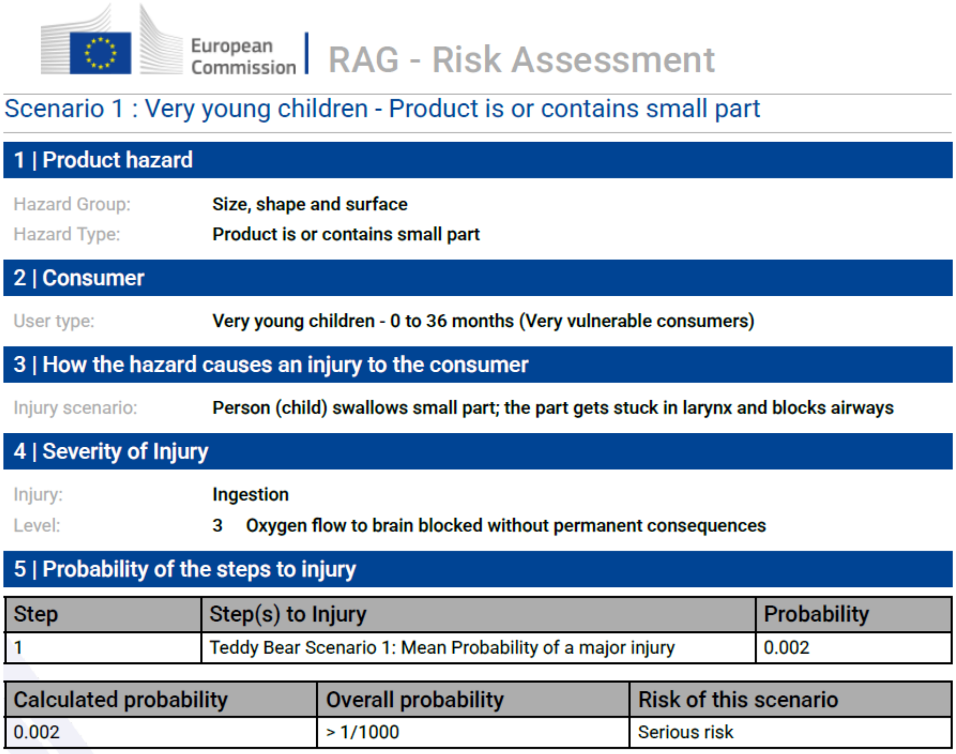
Scenario 2 Description

In this scenario, we assume that the teddy bear is used by a child aged 0-36 months as intended for one year with a low number of demands (i.e. 200) and an 85% chance of carer intervention (i.e. the child is sufficiently supervised so that the carer can take away the small detached part, e.g. teddy bear eye, before it is ingested by the child). All other information used in the BN is the same as presented in the background information.

Scenario 2 – BN Results

The BN model (see Figure C5 in Appendix C) learns that there is a 70% chance that the risk level for the teddy bear is ‘low’ or ‘very low’ with some uncertainty (15% chance it is ‘medium’ and 15% chance it is ‘high’ or ‘very high’). The BN model also calculates the mean probability of a major injury (per demand), which for this scenario is 0.002, and for a minor injury (per demand) it is 0.003. The BN model calculates that the mean number of potential major and minor injuries for 20,000 product instances is 38 and 57, respectively. Finally, the BN model shows that there is a 60% chance that the risk tolerability (acceptability) will be ‘high’ or ‘very high’ for the teddy bear given the benefits and recommends no government intervention such as a recall with some uncertainty. Regarding consumer risk perception, the BN model shows that the risk of the teddy bear is perceived as ‘high’, risk tolerability is mostly ‘low’ or ‘very low’ (88% chance) and government intervention is required (94% chance).

Scenario 2 – RAPEX Results



European Commission | RAG - Risk Assessment

Scenario 1 : Very young children - Product is or contains small part

1 | Product hazard

Hazard Group: Size, shape and surface

Hazard Type: Product is or contains small part

2 | Consumer

User type: Very young children - 0 to 36 months (Very vulnerable consumers)

3 | How the hazard causes an injury to the consumer

Injury scenario: Person (child) swallows small part; the part gets stuck in larynx and blocks airways

4 | Severity of Injury

Injury: Ingestion

Level: 3 Oxygen flow to brain blocked without permanent consequences

5 | Probability of the steps to injury

Step	Step(s) to Injury	Probability
1	Teddy Bear Scenario 1: Mean Probability of a major injury	0.002

Calculated probability	Overall probability	Risk of this scenario
0.002	> 1/1000	Serious risk

Figure 89 RAPEX results for Teddy Bear Scenario 2

The RAPEX method assesses the risk level of the teddy bear as ‘serious’, as shown in Figure 89. This result is not the same as the BN model for the given probability of a major injury since the BN model also uses the probability of a minor injury and the number of product instances to compute the risk of the product.

8.5.2 Case Study 2: A new uncertified electric kettle

Every year, new uncertified products are available on the market that pose a serious risk to the health and safety of consumers. However, regulators may find it difficult to assess the risk for these products using RAPEX since they may not have access to the manufacturer testing data generated during product development (even if such data was collected) and the number of product instances is unknown. In this section, we demonstrate risk assessment of products with limited or no available data using the proposed BN by assessing the risk of a new uncertified kettle on the market for which there are no testing data, and the number of product instances is unknown. We also demonstrate the model's ability to predict the effect of risk communication on risk perception.

8.5.2.1 Background Information

This subsection presents the necessary background information and assumptions for the electric kettle risk scenarios.

1. ***Product Description*:** Stainless steel electric kettle. Capacity 2.3L, 2000W
2. ***Hazard and Injury Scenario*:** The electric kettle may overheat and cause burns or fire.
3. ***Benefits Information:*** The likelihood of use is 'high', and the benefits are moderate for the electric kettle.
4. ***Reported Field and Injury Information*:** We assume that injury reports for similar kettles indicate that for 7000 demands, there were 200 hazard occurrences with 0 major injuries and 1 minor injury.
5. ***Consumer risk perception*:** Consumers perceive the severity of the injury as 'high', and product hazardousness and worry (their concern about the hazard) as 'moderate'.
6. ***Product Testing Information*:** Three (3) previous similar products were tested 'typical of normal use' for a number of demands ranging from 7500-10000. The test report reveals that there was one hazard occurrence during testing.

7. ***Product Instances Information*****:** Product instances on the market range from 50000-100000 based on data from similar kettles.
8. ***Manufacturer Information*****:** The manufacturer has been in operation for 4 years and is from a country with a poor safety record for consumer electrical appliances. The manufacturer also has a ‘low’ customer satisfaction rating, and there are no changes in product design (i.e., product appearance is the same as previous similar products).
9. ***Product Use Information*****:** Since we are uncertain about consumer behaviour during use, we assume that the kettle is used as intended 90% of the time, with major and minor deviations of 7% and 3%, respectively, based on the data for similar kettles. Also, we assume that the kettle will be used on average 3000 times.
10. ***External Risk Control Information*****:** We assume that the probability of external risk controls in the environment preventing or mitigating the hazard is 0.5.

8.5.2.2 Risk Scenarios and Results

In this subsection, we evaluate the BN model using different risk scenarios for the new uncertified electric kettle for which there are no testing data, and the number of product instances is unknown.

Scenario 1 Description

In this scenario, we assess the risk and risk tolerability of the electric kettle using data from previous similar kettles as presented in the background information. We also assume that there is no risk communication, e.g., product recall.

Scenario 1 Method

Given the background information, we are uncertain about the ‘true’ number of demands at which the hazard will appear for this particular kettle. We are also uncertain about the number of demands in product lifetime, product use information and the number of product instances. Therefore, we use the data from previous similar kettles (presented in the background information) as priors in the model to estimate the risk of the new uncertified electric kettle. For example, in the BN model, we use a uniform distribution (i.e., Uniform [7500,10000]) to define the NPT for the node ‘number of demands tested’. The node ‘number of demands in product lifetime’ was defined using a TNormal distribution with a mean of 3000. The ‘number of product instances’ node was defined using a uniform distribution (i.e., Uniform [50000, 100000]). All other information used in the BN is the same as presented in the background information.

Scenario 1 – BN Results

The BN model (see Figure C6 in Appendix C) learns that there is an 80% chance that the risk level of the kettle is ‘low’ or ‘very low’. The BN model also calculates the mean probability of a major injury (per demand), which for this scenario is 0.001 and for a minor injury (per demand) it is 0.002. The BN model predicts that the mean number of potential major and minor injuries for all product instances is 93 and 185, respectively. Finally, the BN model shows there is an 80% chance that the risk tolerability (acceptability) will be ‘high’ or ‘very high’ for the kettle given the benefits and recommends no government intervention, such as a recall with some uncertainty. Regarding consumer risk perception, the BN shows that the risk of the kettle is perceived as mostly ‘moderate’ (24% chance it will be considered ‘high’), there is 50% chance that the overall benefits is ‘high’ and there is a 76% chance that risk will be acceptable or tolerable. Given no risk communication, there is no change in the perceived risk, benefits and risk tolerability (acceptability); however, the BN indicates that government intervention may be required (48% chance).

Scenario 2 Description

In this scenario, we assume that we have reported injury data for the electric kettle. We assume that the reported injury data for this particular kettle indicate that there were 50 hazard occurrences in 7000 demands. 10 of the 50 hazards resulted in major injuries, and 30 resulted in minor injuries. We also assume that there is a product recall (risk communication) for the kettle. All other information used in the BN is the same as presented in the background information.

Scenario 2 – BN Results

The BN model (see Figure C7 in Appendix C) learns that there is a 99% chance that the risk level of the kettle is ‘very high’ with little uncertainty. The BN model also calculates the mean probability of a major injury (per demand), which for this scenario is 0.05 and for a minor injury (per demand), it is 0.14. The BN model predicts that the mean number of potential major and minor injuries for all product instances are 3859 and 10832, respectively. Finally, the BN model shows that there is an 88% chance that the risk tolerability (acceptability) will be ‘very low’ or ‘low’ for the kettle given the benefits and recommends a government intervention such as a recall with some uncertainty. Regarding consumer risk perception, the BN shows that the risk of the kettle is perceived as mostly ‘moderate’ (24% chance it will be considered ‘high’) and a 76% chance that risk will be acceptable or tolerable. However, given risk communication, in this example a product recall, the perceived risk of the kettle increased (i.e., 62% chance it is ‘high’ compared to 24% chance before the product recall). Additionally, consumer perceived benefits decreased (i.e., 10% chance that it is ‘high’ compared to 50% chance before the product recall) and risk tolerability (acceptability) decreased (i.e., 35% chance the risk is ‘tolerable or ‘acceptable’ compared to 77% chance before the product recall).

8.6 Discussion

The case study results for the teddy bear presented in Section 8.5.1.2 show that the BN model and the RAPEX method may estimate different product risk levels for a particular product. In Teddy Bear Scenario 1, the BN model and the RAPEX method estimated the risk level as ‘very high’ or ‘serious’ (see Figure C4 in Appendix C and Figure 88). However, in Teddy Bear Scenario 2, the BN model shows that there is a 70% chance that the risk level is ‘low’ or ‘very low’ (see Figure C5 in Appendix C), whereas the RAPEX method predicted the risk level as ‘serious’ (see Figure 89). This difference in risk level estimates is due to the method used by the BN model to estimate product risk. The BN model includes additional information, such as manufacturer process information, risk control information and product usage information (such as the number of demands and product wear) when estimating product risk. This allows the BN model risk estimates to be comprehensive as it incorporates all relevant factors that affect product risk. Also, since these factors are causally linked, they support ease of interpretation and explanation of risk level estimates.

The BN results for Teddy Bear Scenario 2 also illustrate how consumers may judge the risk and benefits of products differently from experts. For instance, experts tend to judge the risk of a product using quantitative risk assessments, whereas consumers judge risk using a combination of subjective measures such as hazardousness. In this example, though the BN assessed the risk of the teddy bear as ‘low’ or ‘very low’, it predicts that consumers would perceive the risk as ‘high’. Hence, regardless of the results of the quantitative risk assessment, consumer risk perception should not be overlooked and must be considered when evaluating risk.

The results of the case study for the new uncertified kettle in Section 8.5.2.2 show that, while RAPEX is unable to assess the risk of novel products or products for which there are little or no available data, the BN model can provide auditable and quantified risk assessments. For these scenarios, the BN model estimates the risk of the product by combining manufacturer process information with testing information from previous similar products. This estimated product risk is also revised, given new data, e.g., reported injuries. This ability of the BN model to revise the risk given new data is essential for regulators to adequately assess and monitor the risk of novel products over time. In fact, the BN model will also perform better than RAPEX for novel products given new data since it incorporates all the factors that causally affect product risk and takes full account of uncertainty when estimating product risk. This case study example also illustrates the BN ability to analyse consumer risk perception, including the impact of risk communication, such as product recall. For example, as illustrated in Scenario 1 for the electric kettle, if there is no risk communication, the BN model predicts no change in consumer risk perception (see Figure C6 in Appendix C). However, as illustrated in Scenario 2 for the electric kettle, if there is risk communication such as a product recall, the BN model predicts that the perceived risk will increase, and the perceived benefit and risk tolerability (acceptability) will decrease.

The BN for consumer product safety risk assessment provides risk estimates for a single known type of hazard; however, products usually have multiple hazards. In situations where the hazards though possibly unique, are similar in terms of properties they possess, e.g., hot surfaces and open flames, we can identify and define hazard groups or classes, e.g., ‘extreme temperature’. The BN can use the defined hazard groups to consider multiple similar hazards rather than a single hazard. Another solution is to use a risk matrix or table to combine the risk results of multiple hazards. In Section 7.5, we proposed a risk table to combine the risk results of multiple hazards for medical devices that can be adapted for consumer products.

Contributions and Limitations

The principal merit of the proposed generic BN for consumer product safety risk assessment is to provide a robust systematic method for safety regulators, market surveillance authorities (MSA) and manufacturers to assess the risk of consumer products. The case study results show that the BN model resolves the issues with RAPEX discussed in Section 8.3 and meets the model requirements specified in Section 8.4.1. We believe that the BN model provides the following improvements to consumer product risk assessment:

1. *Properly handles uncertainty about probabilities assigned during risk assessment*: The BN model handles second-order uncertainty by incorporating distributions rather than point values for probabilities that are not directly observable.

2. *Can assess the risk of novel products or products with little or no historical data:* In situations where it will neither be feasible nor possible to get any extensive data from testing or details on product instances, the BN model can incorporate expert judgement and/or data from previous similar products to provide quantified and auditable risk estimates.

3. *Incorporates causal explanations for using and interpreting the data*: The BN model explicitly describes the risk assessment process and the causal relationship between the data used.

4. *Considers the usage behaviour for different types of users and the number of product instances when determining product risk*: The BN model can take full account of the distributions of different types of users when estimating product risk by simply assigning priors to the 'particular product usage' node that capture the population distribution. For instance, if for a particular product we estimate that only 30% of the population will 'use it as intended' then we set the prior probability of that node state at 30%. In addition, the BN model explicitly includes 'controls' that can prevent a hazard from causing an injury. For example, in households with a smoke alarm and fire extinguisher, the probability that a fire from a washing machine leads to injury is greatly

reduced. In households where young children are under close supervision, there is a much lower probability that a hazard from a toy (such as an eye pulled off a teddy bear) will lead to injury compared to households where children are left unsupervised. Lastly, the BN model can provide individualised risk assessments. For instance, for a particular user, the model can estimate the probability that this user will suffer an injury during the product lifetime.

5. *Considers the user exposure to risk:* The BN model uses the usage frequency of the product (i.e. the number of demands) to determine the probability of injury for a particular user or class of user.

6. *Models consumer risk perception and risk tolerability (acceptability)*: The BN predicts consumer risk perception and risk tolerability for a particular user or class of users. This is essential since consumer risk perception and risk tolerance must be considered when evaluating risk.

7. *Considers the increased risk of hazards over the lifetime of a product:* The BN model considers the effect of wear and tear on the 'hazard rate' of the product when estimating product risk.

The BN model also improves product risk assessment by modelling:

1. *The effect of risk communication, such as product recall, on the consumer perception of the risk*: For example, as illustrated in Scenario 1 for the electric kettle, if there is no risk communication, the BN model predicts no change in consumer risk perception (see Figure C6 in Appendix C). However, as illustrated in Scenario 2 for the electric kettle, if there is risk communication such as a product recall, the BN model predicts that the perceived risk will increase, and the perceived benefit and risk tolerability (acceptability) will decrease (see Figure C7 in Appendix C). However, these results need to be validated. In Chapter 9, we discuss two studies and their results used to validate the risk perception predictions of the BN model.

2. *The mean number of major and minor injuries, respectively*: The BN model can estimate the mean number of major and minor injuries for a particular

product based on the total number of product instances and the probability distribution of major and minor injuries, respectively.

The proposed BN for consumer product safety risk assessment is a more powerful and flexible approach for systematic product risk assessment than traditional methods like RAPEX. However, it is important to note that it can also complement traditional methods like RAPEX. For instance, since the BN approach estimates product risk using additional parameters such as product usage data and manufacturer process information, it can be used in the interim to validate RAPEX risk assessments.

The main limitation of this case study is obtaining all the relevant information for a consumer product to perform a risk assessment using the BN model. Since the results of the safety and reliability tests conducted by the product manufacturers are not publicly available, the data used to evaluate the BN model were fictitious. However, given actual data for a particular product, the NPTs for the BN can be revised, and the BN can provide reasonable and auditable risk estimates. In addition, the proposed BN was developed in the context of risk management carried out by national safety regulators and market surveillance authorities in the UK and EU; hence its variables and structure are somewhat different from the medical device risk management BN (discussed in Chapter 7).

8.7 Chapter Summary

This chapter serves as another good example for the practical use and benefits of the product safety idioms for BN development discussed in Chapter 6. By developing the BN for consumer product safety risk assessment, we show that product safety idioms can be used to construct complex BNs in a modular fashion. In addition, this chapter demonstrates how national safety regulators and market surveillance authorities can use BNs for consumer product safety risk assessment. The proposed BN for consumer product safety risk assessment is a more powerful and flexible approach for systematic product risk assessment than traditional methods like RAPEX. In particular, it can: produce quantified, auditable assessments with limited or no data; properly handle second-order uncertainty; incorporate causal explanations for using and interpreting data; allow for different types of users, including different exposure to risk and risk tolerability; incorporate increased risk of hazards over the lifetime of a product;

complement traditional risk analysis methods; handle incomplete data; combine objective and subjective evidence; revise risk estimates given new data.

In addition, it informs risk management decisions and predicts the effect of risk communication, such as product recall, on consumer risk perception. However, the BN predictions for the latter require validation; hence in the next chapter, we present two empirical studies to validate the BN predictions.

Chapter 9 The effect of risk communication on consumer risk perception of consumer products

In this chapter, the results of two empirical studies used to investigate the effect of risk communication on consumer risk perception of consumer products (non-food) are presented. These empirical studies, done in collaboration with the UK Government Office for Product Safety and Standards (OPSS) were used to validate the results of the risk perception component of the consumer product risk assessment BN presented in Chapter 8. In addition, they provided OPSS with novel insights on the risk perception of consumer products (smart and non-smart) and how it is influenced by risk communication from different actors in the network, such as government and the media. They also contribute to the existing body of literature in this domain.

Section 9.1 introduces the topic while Section 9.2 presents the required background information. In Section 9.3, Study 1 is presented. This study advances our understanding of consumer risk perception, risk tolerance and benefits (or utility) of novel technologies (e.g., smart functionality) in home appliances. It also investigates how these perceptions are affected by risk communication from various sources such as the government, manufacturer and media. In Section 9.4, Study 2 is presented. This study validates Study 1 and advances our understanding of how the reliability of the source of the risk communication (reliable versus unreliable) and product compliance information (compliant versus non-compliant) can influence willingness to pay (WTP) and risk perception of consumer products. The material presented in this chapter was previously presented in Publications 5 and 6.

9.1 Introduction

Home appliances can present serious risks such as fire and electric shock [187], [188]. Moreover, risk perception, risk tolerance and benefits (utility) of home appliances may differ due to demographic variables such as gender and education [48], [189]–[193]. Despite the differences in the perceived risk of home appliances, it is essential that consumers are informed about the risks associated with these devices to protect them from potential harm or damage to their environment [46]. Consumers are informed about product risks by manufacturers, safety regulators (both government and independent bodies) and consumers via several media vehicles such as traditional media (e.g., television), social media platforms (e.g., Twitter), events (e.g., community meetings) and product-related material (e.g., product labels) [46], [47]. The method used for risk communication by different actors in the network (i.e., manufacturers, government and media) depends on the target audience and the purpose and objectives of the risk communication [46]. Since sources of risk communication can influence consumer risk perception, risk tolerance, and utility or benefits of products, including home appliances [194], [195], it is essential to understand their impact for better risk communication management and to protect consumers from potential harm associated with products' risks. However, there is little or no previous research on the impact of risk communication sources, such as manufacturers, on consumer risk perception, risk tolerance and benefits (utility) of home appliances. In fact, risk tolerance is rarely studied in this domain.

Furthermore, advances in information technology, such as the internet of things (IoT) and artificial intelligence, have transformed traditional home appliances into "smart" devices. These smart home appliances can collect, process and store information and interact with their operating environment [196]. Since smart home appliances may pose novel and unknown risks to consumers, it is essential to understand how consumers perceive these devices' risks and whether there are unique differences (or not) when compared to non-smart versions before and after risk communication.

In this chapter, we provide novel insights on consumers' perception of home appliances. In Study 1, we investigate differences in risk perception between smart and non-smart versions of such appliances. We evaluate how communication from various sources e.g., manufacturers, about risks and hazards associated with home appliances influence consumers' perceived risk, utility (benefit) and risk tolerance of these devices. This study is the first of its kind to have directly contrasted smart with non-smart equivalent products to examine the relative impact of smartness on judged risk, utility (benefit) and risk tolerance. In Study 2, we investigate whether consumer risk perceptions and willingness to pay (WTP) for a product differ based on the reliability of the source of the risk communication (reliable versus unreliable) and product compliance information (compliant versus non-compliant). This study is the first of its kind to examine the relative impact of source reliability and product compliance information on risk perception and WTP.

These empirical studies complement our previous work on using causal Bayesian networks (BNs) for product safety risk assessment [15] discussed in Chapter 8. The proposed BN for consumer product risk assessment estimates the risk of consumer products by considering factors such as device use and manufacturer process information. The BN model resolves the limitations with traditional risk assessment methods such as the RAPEX methodology and provides reasonable risk estimates for products, including novel products or products with little or no relevant historical data. A key feature of the BN model is modelling consumer risk perception and risk tolerance. The BN fragment (i.e., a component of the BN model) shown in Figure 90 models the impact of risk communication from the media, manufacturer and government about potential risks associated with products on consumer risk perception, perceived benefits (utility) and risk tolerance. The risk communication sources included in the BN model (i.e., media, manufacturer and government) were selected since they are the most common and familiar sources of risk communication about products' risks for the general public [47]. However, due to the lack of research on the impact of these different sources of risk communication on consumers' risk perception, benefits (or utility) and risk tolerance of products, the model structure, variables and results require validation. Therefore, the findings obtained from these studies can inform and validate the results of the BN model.

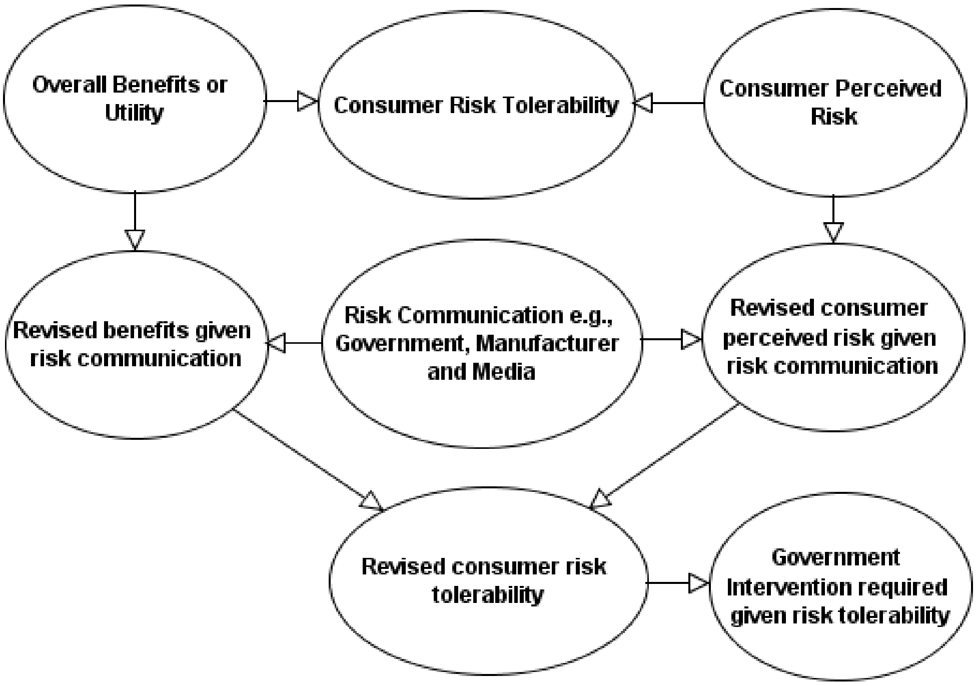

Overall Benefits or Utility
Consumer Risk Tolerability
Consumer Perceived Risk
Revised benefits given risk communication
Risk Communication e.g., Government, Manufacturer and Media
Revised consumer perceived risk given risk communication
Revised consumer risk tolerability
Government Intervention required given risk tolerability

Figure 90 Consumer risk perception and risk tolerability BN fragment

9.2 Background

9.2.1 Home appliances: Smart and Non-smart

Modern home appliances can now operate autonomously, interact with their environment and communicate with other devices [196]. These “smart” products use artificial intelligence (AI), IoT technology (e.g., Wi-Fi), and embedded technology (e.g., sensors) to collect, process and store information and to communicate and interact with their operating environment, users, and other products. Examples of such smart products are robot vacuum cleaners, smart microwaves, smart refrigerators and smart TVs [196]–[199]. Products that are not dependent on information technology are described as “non-smart”. However, to a limited extent, non-smart products may possess some of the characteristics of smart products [196]. For instance, modern washing machines have some level of autonomy.

9.2.2 Consumers’ perception of risk, benefit, risk tolerance and willingness to pay (WTP)

Perceived risk is consumers’ subjective judgement of risk when purchasing or using a product or service [30], [31]. Previous research suggests that risk perception consists of two dimensions: *dread* and *unknown* [32]. *Dread risk* refers to the lay-person feelings about risks or hazards. It is defined in terms of the likelihood of consequence (harm) and its severity, lack of control and feelings of fear. *Unknown risk* refers to risks considered new, unobservable, unknown, and delayed in their manifestation and consequences.

The risks associated with products, including home appliances, consists of two components: the probability of harm *P* and the severity of that harm *S* [8], [185]. Previous research shows that both components can influence the risk perception of products [200], [201]. For instance, Vaubel et al. [200] show that risk perception is multidimensional and is influenced by both risk components and product familiarity.

The perceived risk of a product may depend on a single attribute (feature) of the product or the product as a whole [193]. In situations where the perceived risk is dependent on a single attribute of the product, if that particular attribute is perceived as risky, then the whole product is perceived as risky. This is usually the case with novel technology, such as autonomous products, which are generally considered high risk and more complex compared to other products [193], [202]–[204]. In situations where the perceived risk of the product is based on the product as a whole, the perceived risk may depend on the trade-off between risk and benefit (utility) [193], [205]. For example, the risk of using a mobile phone, such as electromagnetic radiation, is perceived as low due to the benefits, such as instant communication with family and friends [193], [206].

The effect of consumer characteristics on risk perception is usually investigated using the psychometric risk perception model [193]. This risk perception model assumes that risk is subjective and is influenced by socio-demographic factors such as gender. It measures risk perception of different hazards by asking questions directly about them and using psychometric scaling methods such as numerical rating scales to capture responses [32], [207]. When applied to products, consumers perceive risks as high if they lead to serious harm or damages, e.g., death or if they are unknown and novel [32], [193], [207]. Additionally, men perceived risks are lower than women, and higher education is associated with lower perceived risk [48], [189]–[192].

Benefit or Utility is the (perceived) benefits (or advantages) consumers receive from using a product. Since each consumer is unique, benefit (or utility) is personal and situational. For example, a consumer will assign utility to a product based on their personality, situation and experience [33]–[35]. In general, the perceived benefit has an inverse relationship with perceived risk [36]–[38]. For instance, Alhakami and Slovic (1994) found that when persons perceive an item as having high benefit or utility, they perceive it as low risk (and vice-versa). In this thesis, we use the terms *utility* and *benefit* interchangeably.

Risk tolerance (acceptance) is the amount of (perceived) risk consumers are willing to accept or tolerate to obtain the benefits (value or utility) of a product [39]. It is influenced by individual characteristics, knowledge (or experience) of the product, product risks, risk controls and benefits. For instance, some research suggests that risk tolerance is a personality trait [40]–[42]. For example, consumers with a high propensity to take risks are more tolerant of risks. On the other hand, other research suggests that risk tolerance is based on experience and knowledge [43]–[45]. For example, consumers that are more familiar with a particular product via experience or knowledge will be more tolerant of its risks.

Willingness to pay (WTP) “is the maximum price a customer is willing to pay for a product or service” [208]. Based on the results of previous research [209]–[211], it can be implied that when a product is perceived as risky and risk reduction measures are not applicable, the WTP will decrease. However, there is little or no research investigating this assumption. Understanding the relationship between WTP and perceived risk is important since WTP taps into perceived risk more subtly.

9.2.3 Risk communication and risk perception

Risk communication is the exchange of information between different stakeholders (such as consumers and the government) about the risks associated with products [46]. The most common and familiar sources of risk communication about risks associated with products are the government, manufacturers and the media [47]. Overall, the success of risk communication depends on the risk information (message) and the media vehicle. For instance, the risk message should be accurate and understandable, and the chosen media vehicle should be suitable for the risk message [46].

Additionally, the source of the risk communication can influence risk perception [194], [195]. For instance, media coverage and its availability (i.e. the amount of coverage) can influence risk perception since consumers become more concerned about potential risks when exposed to several news and reports about the risk [212]–[216]. However, the effect of media coverage on risk perception is not permanent and usually fades when the media coverage fades [212]. Likewise, trust in the risk communication source can affect risk perception. For example, if consumers perceive the risk communication source as reliable and trustworthy, e.g., the government, they will most likely adhere to the risk message. However, they may ignore or reject the risk message if they perceive the risk communication source as unreliable and untrustworthy, e.g., non-experts. Hence, a lack of trust in the risk communication source will limit the effect of the risk communication [48], [49]

Since consumers are usually informed about potential risks associated with home appliances by safety regulators, manufacturers, and media coverage, it is essential to understand the impact of the safety information from these sources on consumers’ risk perception, benefit (or utility) and risk tolerance of home appliances (smart and non-smart). However, there is little or no previous research in this domain.

9.3 Study 1

In this study, we investigate how different sources of risk communication affect consumers' risk perception, utility (or benefit) and risk tolerance of smart and non-smart home appliances to explore whether changes in risk perception, utility and risk tolerance conform to the BN model predictions. This study also investigates the difference in risk perception, utility and risk tolerance of smart and non-smart home appliances and whether it varies by gender and education. In this study, we used the following hypotheses to investigate these questions:

- **Hypothesis 1:** The perceived risk is greater for smart home appliances when compared to non-smart home appliances.
- **Hypothesis 2:** The perceived utility is greater for smart home appliances when compared to non-smart home appliances.
- **Hypothesis 3:** The perceived risk tolerance is less for smart home appliances when compared to non-smart home appliances.
- **Hypothesis 4:** Risk communication from the government, manufacturer and media will increase perceived risk, decrease utility and decrease risk tolerance of smart and non-smart products.
- **Hypothesis 5:** The perceived risk of smart and non-smart home appliances is less for men when compared to women.
- **Hypothesis 6:** The perceived risk of smart and non-smart home appliances is less for consumers with higher education.

See Figure D1 in Appendix D for the conceptual framework that guided this study. In this study, the terms *utility* and *benefit* were used interchangeably.

9.3.1 Method

Design and Material

We conducted two experiments to test the study hypotheses. In each experiment, consumers were given information about a home appliance (i.e., its type and features) and a risk communication scenario and were asked questions on risk perception, utility (benefit) and risk tolerance. In Experiment 1, the *microwave oven* was investigated, and in Experiment 2, the *vacuum cleaner* was investigated. These home appliances were chosen because they are familiar products and are available on the market as smart and non-smart (traditional) versions (see Figure 91). The following between-subject independent variables were manipulated in each experiment:

- **Product type**: (1) Smart (2) Non-smart

Risk communication scenarios (see Table 24):

- **Risk information**: (1) Government recall (2) Manufacturer recall.
- **Media coverage**: (1) Large media coverage/story (2) Small media coverage/story.

These independent variables were chosen based on the study's aims and hypotheses.

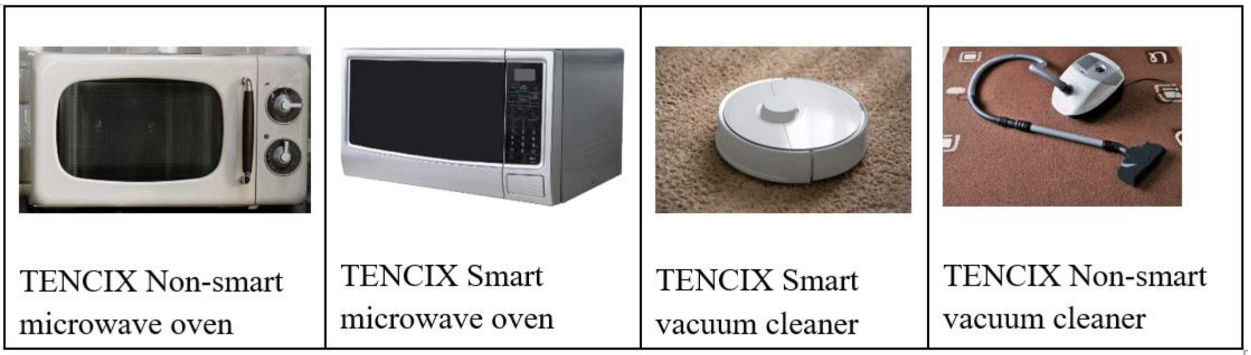

TENCIX Non-smart microwave oven
TENCIX Smart microwave oven
TENCIX Smart vacuum cleaner
TENCIX Non-smart vacuum cleaner

Figure 91 Types of home appliances used in Experiments

Table 24 Description of risk communication scenarios used in Experiments

Scenario Name	**Scenario Description**
Government recall	Imagine you have bought the [product name] and the government announces a product recall due to a fire risk as follows: "The manufacturer has identified the [product name] to be recalled or replaced due to a potential risk of fire. If you have this [product type], please immediately stop using it and contact the manufacturer's hotline for a full refund or replacement".
Manufacturer recall/warning	Imagine you have bought the [product name] and the manufacturer issues the following warning about a fire risk: "The [product name] has a potential risk of fire during use. If you have this [product name], please immediately stop using it and contact our hotline for a full refund or replacement."
Large media coverage/story	Imagine you have bought the [product name] and there are media stories on several news outlets for many months about a fire risk including the following headline. "My [product name] catches on fire: Consumers fear for their safety as there are multiple reports of the [product name] catching fire".

Small media coverage/story	Imagine you have bought the [product name] and there is one media story that appeared online about a fire risk with the following headline. "My [product name] catches on fire: Consumer warns of fire risk while using [product name]".

Each experiment had a 2 x 2 x 2 design, and the dependent variables, i.e., risk, utility (benefit) and risk tolerance, were assessed using the following questions:

1. *Risk:* To what extent do you consider the [product name] as posing a risk?
   Scale 1 to 100 (low risk to high risk)
2. *Utility or Benefit:* How useful do you think the [product name] is?
   Scale 1 to 100 (not useful to very useful)
3. *Risk tolerance:* Please rate your ability to tolerate the risk associated with the [product name].
   Scale 1 to 100 (low tolerance to high tolerance)

Participants

British consumers were recruited for each experiment using Prolific (www.prolific.co). The inclusion criteria were that they were UK residents, born in the UK, their first language is English and a pre-specified age range of 18 to 65.

400 participants (263 women) were recruited for Experiment 1 (Microwave oven) and for Experiment 2 (Vacuum cleaner), 400 participants (254 women) were recruited.

In each experiment, the participants were randomly assigned to one of the eight experimental groups (2 product types x 2 risk information scenarios x 2 media coverage scenarios); group sizes varied between *n* = 49 and *n* = 51.

Data Analysis

This study used the Bayesian approach to hypothesis testing [13] to investigate the study hypotheses (see Appendix D for additional details).

9.3.2 Results

Risk perception, utility and risk tolerance for smart and non-smart home appliances

A summary of the mean perceived risk, mean utility and mean risk tolerance for smart and non-smart microwave ovens and vacuum cleaners is shown in Figure 92, and the patterns indicated here were statistically examined to assess support for our hypotheses.

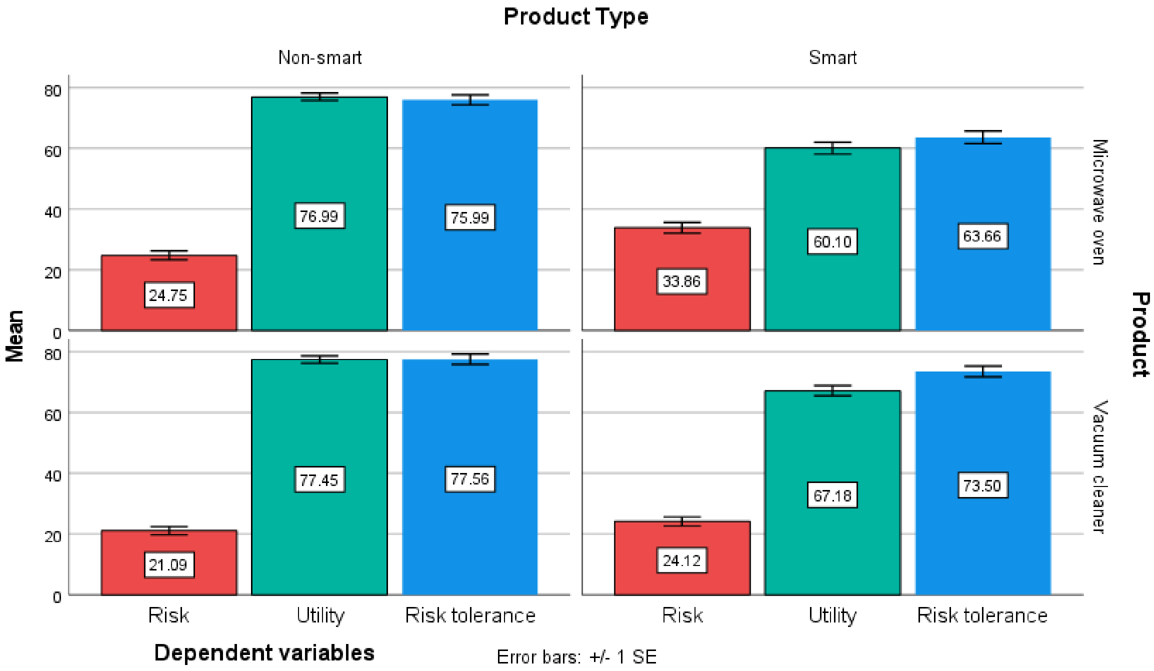


Figure 92 Mean perceived risk, utility and risk tolerance for non-smart and smart microwave ovens and vacuum cleaners

Experiment 1 Results

For the microwave oven, Figure 92 and the results of the Bayesian analysis revealed that, in support of Hypothesis 1, consumers judged the smart microwave oven as riskier (*M* = 33.86, 95% CI [30.28, 37.48]) compared to the non-smart version (*M* = 24.75, 95% CI [21.71, 27.73]). The mean difference was 9.13, 95% CI [4.42, 13.92]. However, contrary to Hypothesis 2, consumers judged the smart microwave oven as having less utility (*M* = 60.10, 95% CI [56.12, 64.09]) compared to the non-smart version (*M* = 76.99, 95% CI [74.36, 79.60]). The mean difference was -16.88, 95% CI [-21.68, -12.07]. In support of Hypothesis 3, consumers were less tolerant of the risks associated with the smart microwave oven (*M* = 63.66, 95% CI [59.51, 67.82]) compared to the non-smart version (*M* = 75.99, 95% CI [72.55, 79.47]). The mean difference was -12.34, 95% CI [-17.80, -6.63].

Experiment 2 Results

For the vacuum cleaner, contrary to Hypothesis 1, the results revealed that there was little or no difference in the way consumers judged the risk of the smart vacuum cleaner (*M* = 24.12, 95% CI [21.05, 27.16]) and the non-smart version (*M* = 21.09, 95% CI [18.28, 23.87]). The mean difference was 3.03, 95% CI [-1.1, 7.18]. Like the smart microwave oven, and contrary to Hypothesis 2, consumers judged the smart vacuum cleaner as having less utility (M = 67.18, 95% CI [63.73, 70.64]) compared to the non-smart version (*M* = 77.45, 95% CI [74.83, 80.09]). The mean difference was -10.27, 95% CI [-14.68, -5.89]. Similar to the perceived risk, and contrary to Hypothesis 3, there was little or no difference in the way consumers judged the risk tolerance of the smart vacuum cleaner (*M* = 73.50, 95% CI [69.69, 77.32]) and the non-smart version (*M* = 77.56, 95% CI [74.02, 81.09]). The mean difference was -4.05, 95% CI [-9.29, 1.27].

The effect of different sources of risk communication on consumers' risk perception, utility and risk tolerance of smart and non-smart home appliances

Experiment 1 Results

To investigate support for Hypothesis 4, we used Bayesian analysis to examine the effect of different sources of risk communication on risk perception, utility and risk tolerance of non-smart and smart microwave ovens. We computed the mean difference for the perceived risk, utility and risk tolerance for non-smart and smart microwave ovens before and after each risk communication scenario. The mean difference was computed as $y - x$, where x is the mean value of the perceived risk, utility and risk tolerance for a particular product before the risk communication scenario and y is the mean value of perceived risk, utility and risk tolerance for a particular product after the risk communication scenario. For instance, as shown in Figure 93, given a government recall, the mean increase in the perceived risk is 58.10, the mean decrease in perceived utility is 33.58, and the mean decrease in perceived risk tolerance is 51.98.

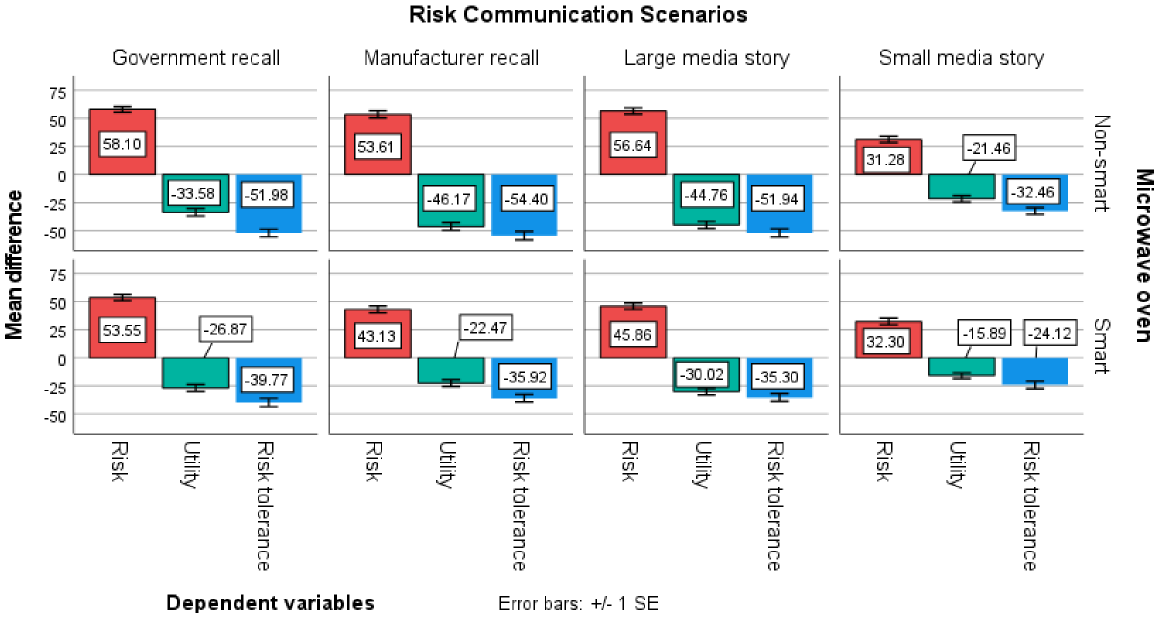


Figure 93 The mean difference in the perceived risk, utility and risk tolerance for non-smart and smart microwave ovens for each risk communication scenario

According to the mean difference plot shown in Figure 93 and the results of the Bayesian analysis shown in Table D2 and Table D3 in Appendix D for non-smart and smart microwave ovens, respectively, risk communication from the government, manufacturer and media stories increased perceived risk, decreased perceived utility and decreased perceived risk tolerance. Thus, we find support for Hypothesis 4.

Experiment 2 Results

Similar to the results obtained in Experiment 1, Experiment 2 also supports Hypothesis 4. Risk communication from the government, manufacturer and media stories increased perceived risk, decreased perceived utility and decreased perceived risk tolerance for non-smart and smart vacuum cleaners (see Figure 94 and Table D4 and Table D5 in Appendix D).

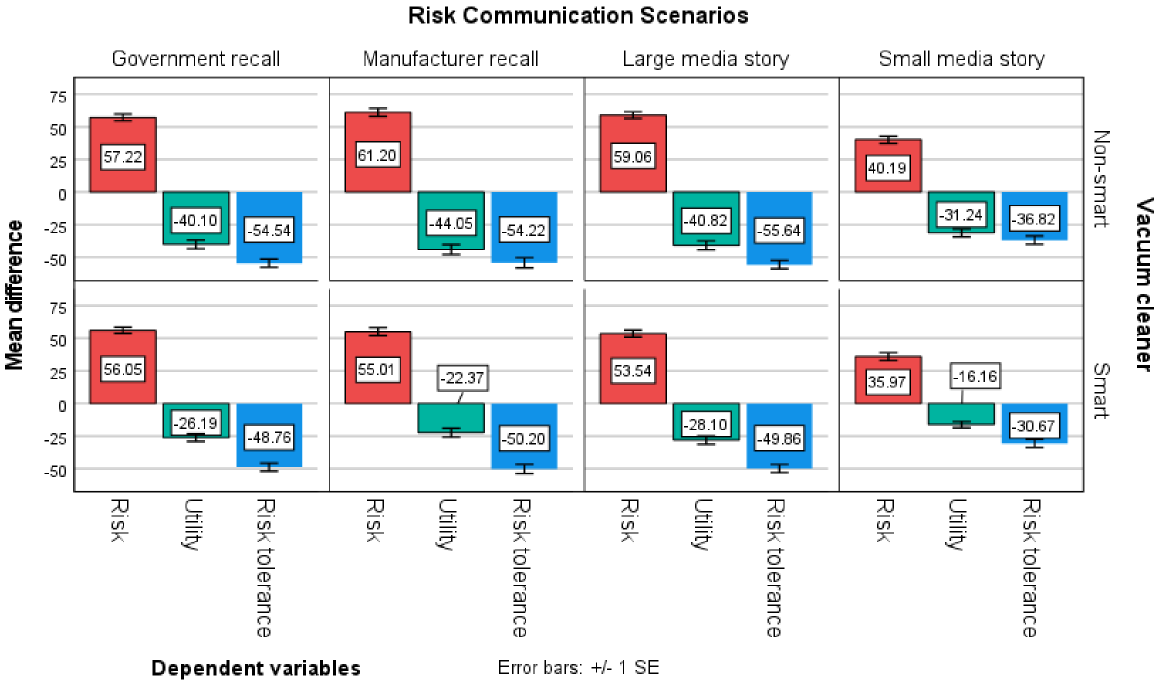


Figure 94 The mean difference in the perceived risk, utility and risk tolerance for non-smart and smart vacuum cleaners for each risk communication scenario

The effect of demographics on risk perception of smart and non-smart home appliances

According to the combined results shown in Figure 95, and Table D6 in Appendix D, we did not find support for Hypothesis 5. There was little difference in the perceived risk for smart and non-smart microwave ovens and vacuum cleaners between men and women.

Regarding level of education, in general, for the smart and non-smart microwave ovens, the perceived risk decreases as the level of education increases (see Figure 96), lending support for Hypothesis 6. This pattern was the same for the smart vacuum cleaner; however, for the non-smart vacuum cleaner, there was little difference between the perceived risk for lower and higher education levels.

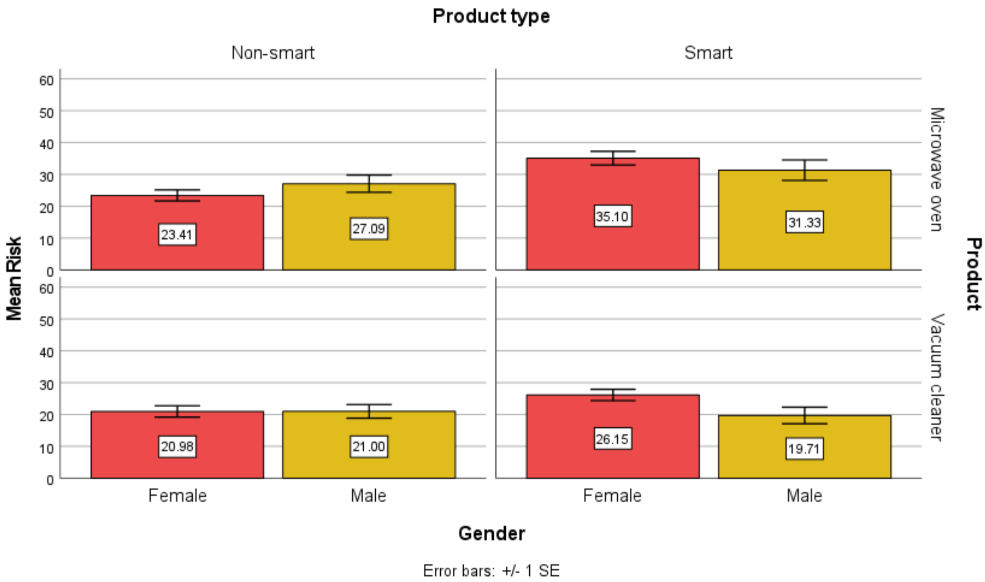


Figure 95 Mean perceived risk for microwave oven and vacuum cleaner by gender

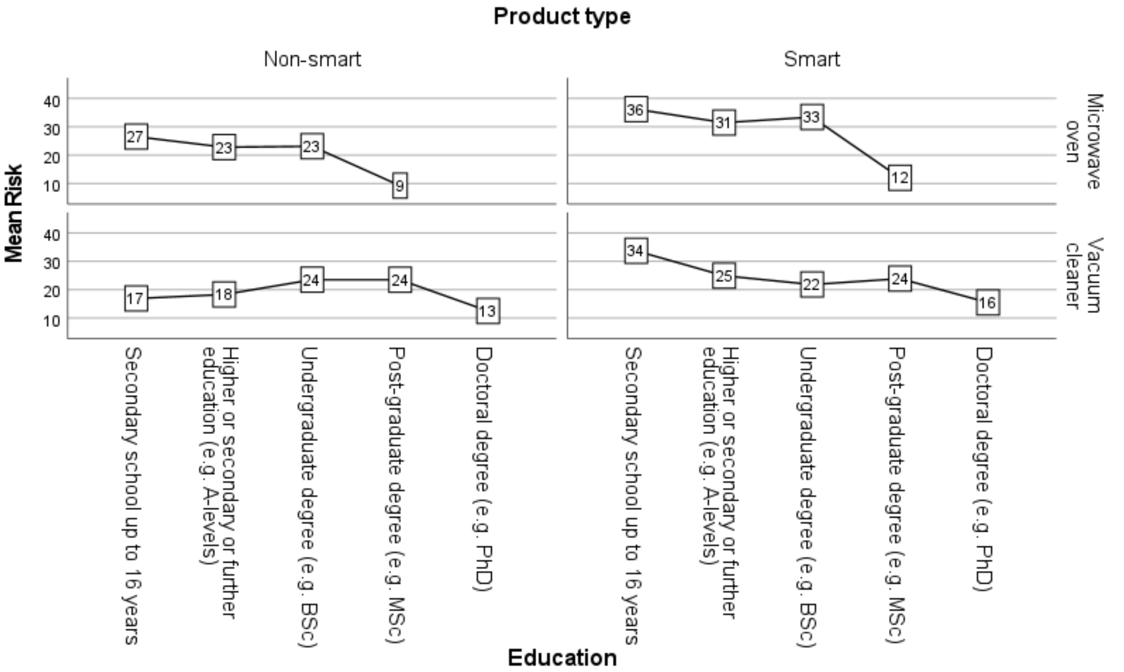


Figure 96 Mean perceived risk vs Education level by product and product type

9.3.3 Discussion

The present study advances our understanding of consumers’ risk perception, risk tolerance and utility of smart and non-smart home appliances and the extent to which consumers’ risk perception changes given risk communication from different actors in the network (e.g., government, manufacturer and media). Overall, the results show that risk perception of home appliances is influenced by product type (smart and non-smart), risk communication and demographics. In the following subsections, we will discuss the results and their implications, the strengths and limitations of the study and recommendations for further research.

Risk Perception

As expected, we found that consumers generally judge smart home appliances as riskier and were less tolerant of their risks when compared to non-smart home appliances. Our results corroborate previous research, suggesting that smart products or products with novel technology are perceived as riskier when compared to other products [32], [193], [196], [202]–[204], [217]. For instance, Slovic [32] demonstrated this through the unknown risk dimension of the psychometric approach. This finding suggests that product manufacturers should aim to reduce the perceived risk associated with smart products. Product manufacturers could do this by informing consumers about product functionality and safety controls, while retail stores could do it through product trials and demonstrations which will allow consumers to evaluate the product functionality and safety controls before purchase [196].

Contrary to our expectations, we found that consumers perceived smart home appliances as having less utility than non-smart home appliances. Our results contradict previous research suggesting that smart products generally offer better utility than non-smart products [196]. However, our results are consistent with previous research highlighting the inverse relationship between perceived risk and utility, i.e., higher risks are associated with less utility or benefits [36], [37], [218]. Since the inverse relationship between risk and utility explains our results, product manufacturers should aim to reduce the perceived risk associated with smart products since it also impacts the perceived utility or benefit. Our finding also suggests that product demonstrations and trials may increase the perceived utility of smart products by focusing on the additional functionalities and benefits offered, such as autonomy and time-savings.

Risk Communication

As expected, our results found that risk communication from different sources impacted risk perception. The government, manufacturer, and large media coverage/story each contributed to a similar level of increase in perceived risk, and they each lowered the level of utility and risk tolerance to a similar degree. On the other hand, small media coverage/story had the least impact on perceived risk, utility and risk tolerance. Our findings corroborate the results of the BN model and previous research [48], [49], [212], [213], [215], [216]. These results have implications for risk communicators – identifying which source of risk communication significantly influences risk perception means that risk communication strategies can be tailored to increase awareness of risk and hazards associated with products.

Unsurprisingly, we found that large media coverage had a greater impact on risk perception when compared to small media coverage, hence confirming previous research [216], [219]–[221]. These results have implications for risk communicators – identifying the amount of media coverage that significantly influences risk perception means that risk communication strategies can be tailored to increase awareness of risks and hazards associated with products. Also, providing the public with frequent, accurate and complete information about risks can ensure that the effect of risk communication on the public's risk perception is maintained [219]–[221].

These results also have implications for the BN model – identifying the impact of different sources of risk communication on risk perception can improve predictions. For instance, the node *risk communication* in the BN model was defined as a ranked node with states (*none, small media story, large media story/product recall*) since product recall and large media story affected risk perception the same and small media story had the least impact.

Demographics

Contrary to our expectations, we found no difference in the risk perception of smart and non-smart home appliances between men and women. This finding contradicts previous research suggesting that men tend to judge risks smaller when compared to women [32], [222], [223]. On the other hand, some research suggests that gender differences are not evident for all types of risk and are dependent on environment or context [222], [224]–[226]. For instance, David and Freudenburg [222] observed that gender differences are most evident for technologies that pose a risk of contamination, such as nuclear technology. Hence, our results and previous research highlight the need to understand the impact of contextual factors such as environment and socio-demographics on risk perception. This will allow better characterisation of gender differences and their impact on risk perception.

Regarding level of education, we found that higher educational level was associated with less perceived risk and so confirmed previous research [32], [227], [228]. This suggests that risk communication should be tailored for different subpopulations to effectively influence risk perception and behaviour. Also, product manufacturers may reduce perceived risk via product trials, demonstrations, focus group sessions and safety information.

Strengths, Limitations and Recommendations

In this study, response bias and demand characteristics were minimised in several ways. We performed two experiments with different products and participants. Hence the findings in Experiment 1 are validated by Experiment 2. Also, in each experiment, we used between-subjects design whereby participants were randomly assigned a product type, risk information and media coverage scenario.

Although our work captured the perceived risk, utility (benefits) and risk tolerance of smart and non-smart home appliances, we recognise that the extent to which our results can be generalised for all home appliances is limited, especially since only two types of home appliances were investigated. Hence the results of this study may vary given other types of home appliances since the perception of risk, utility and risk tolerance is product dependent [196]. In addition, our study did not include variables such as product price, which may well impact the perceived utility of the products.

Further research should seek to examine the risk perception of other home appliances, especially since risk perception is product dependent [32], [196]. Examining other types of home appliances would allow for a better understanding of the differences in risk perception between different home appliances and their smart and non-smart versions. Also, further research should consider product price and willingness to pay (WTP) since they may impact the perceived utility of the products. In Study 2, we address some of these limitations.

9.4 Study 2

The principal merit of Study 2 is to complement and corroborate the results of Study 1 and the BN model. This study done in collaboration with researchers at the Royal Holloway University of London aims to advance our understanding on how consumers perceive the risks associated with consumer products and whether risk perceptions and willingness to pay (WTP) differ based on the reliability of the source of the risk communication (reliable versus unreliable) and product compliance information (compliant versus non-compliant). The product, product compliance information and source reliability were manipulated between participants. Ratings for risk perception and WTP for the products were captured before and after product compliance information from different sources to assess the effect of source reliability and product compliance information on risk perception. Our main study hypotheses are summarised in Table 25. This study used the term “dread risk” to denote the perceived risk.

Table 25 Study 2 Hypotheses

Hypotheses	**Product Compliance Information**	**Source Reliability**	**Dread (Risk)**	**Benefits**	**WTP**
H1$_a$	Compliant				
H1$_b$	Non-Compliant		+	-	-
H2	Compliant	Reliable			
H3	Non-Compliant	Reliable	+	-	-
H4	Compliant	Unreliable	+	-	-
H5	Non-Compliant	Unreliable	+	-	-

Legend	Increase	+
	Decrease	-
	No Change	

9.4.1 Method

Participants

496 participants (251 male) aged 18-65+ were recruited from Prolific Academic (www.prolific.co). The inclusion criteria were that they were residents of the UK, born

in the UK, and their first language is English. The participants received £0.80 for participating.

Design

In this study, a 2 × 2 × 2 design was used. The product, product compliance information and source reliability were manipulated between participants. Two products were investigated, namely, a carbon monoxide detector and a microwave oven[1] (see Appendix D for full product descriptions). Product compliance information had two classifications, i.e., compliant and non-compliant. Source reliability had two classifications, i.e., reliable and unreliable.

Materials and Procedure

After consenting to participate, participants indicated their age, gender and if they had children within specified age groups. The participants then read the instructions for the task. On the next screen, participants were presented with one of the two products. They provided initial scores for five risk characteristics, i.e., benefits, severity, worry, the likelihood of use and hazardousness (see Table 26), using a 7-point Likert scale as in [38], [229]. Participants also had to indicate their willingness to pay (WTP). The WTP was measured on a scale ranging from £0 to 2 × recommended retail price (RRP).

Table 26 Risk Characteristics and WTP - Examples for TENCIX Microwave Oven

Risk Characteristics	**Questions**
Benefits	How great are the benefits associated with the TENCIX Microwave Oven to you personally? (1 = no benefits at all, 7 = very great benefits)
Severity	How severely (i.e., degree, extent or magnitude) might you, or anyone else, be injured by the TENCIX Microwave Oven? (1 = not at all severe, 7 = extremely severe)
Worry	How worried are you about potential risks associated with use of the TENCIX Microwave Oven? (1 = Not worried at all, 7 = Extremely worried)

[1] The products used in this study were identified from a previous study, "Understanding the Psychological and Cultural Factors Underpinning Risk Perception of Products", undertaken by researchers at Royal Holloway University of London (RHUL). This study investigated risk perceptions of several products. The study results revealed that microwave oven and carbon monoxide detector are perceived the same by consumers, i.e., high benefits and moderate dread.

Likelihood of use	If you were to buy the TENCIX Microwave Oven, how likely would you be to use it? (1 = not at all likely, 7 = extremely likely)
Hazardousness	How hazardous do you consider the TENCIX Microwave Oven to be? (1 = not at all hazardous, 7 = extremely hazardous)
Willingness to pay (WTP)	If you decided to buy the TENCIX Microwave Oven, how much would you be willing to pay? (£0 - £180)

On the following screen, participants were informed about product compliance (either compliant or non-compliant) by a reliable or unreliable source (see Table 27). They were then asked to re-rate the product on the five risk characteristics, i.e., benefits, severity, worry, the likelihood of use and hazardousness.

Table 27 Description of conditions used in the Study 2

Source Reliability	
Reliable source: Imagine you are currently looking to purchase [product name] for yourself or a member of your household. Whilst you are browsing online, you see the [product] for sale for less than the recommended retail price [RRP] on BuyBuyNow.com - a popular e-commerce website. Before buying the [product name], you see a media story about the safety of the [product name] on SafeProducts101.info – a website specialising in product safety information, which has a reputation for publishing trustworthy product reviews.	**Unreliable source:** Imagine you are currently looking to purchase [product name] for yourself or a member of your household. Whilst you are browsing online, you see the [product name] for sale for less than the recommended retail price [RRP] on BuyBuyNow.com – a popular e-commerce website. Before buying the [product name], you see a media story about the safety of the [product name] on TopElectricDevice101.info – a website specialising in electrical products, which has a reputation for sometimes publishing fake reviews.
Product Compliance	
Compliance information: This story reports that the manufacturer has a good safety compliance record, and this particular model of [product name] complies with [safety standard]	**Non-compliance information:** This story reports that the manufacturer has a poor safety compliance record, and this particular model of [product name] does not comply with [safety standard]. There is an increased likelihood of the product malfunctioning resulting in harm to the user.

The participants then completed the General Risk Propensity Scale [230] (an eight-item risk propensity scale) and a shortened and amended version of the Cultural Cognition Worldview Scale [231]. We examined risk propensity and cultural worldviews since participants respond differently to the same information [232]. The two cultural worldviews are ‘hierarchical individualist’ (i.e., individuals with the view that social inequality is fair, and they are responsible for their own wellbeing) and ‘egalitarian communitarian’ (i.e., individuals with the view that social inequality is unfair, and the collective responsibility is responsible for their wellbeing). Therefore, the two scales used in this study were ‘individualism-communitarianism’ and ‘hierarchy-egalitarianism’, labelled GROUP and GRID respectively. Finally, participants were thanked, debriefed, and given a code to claim their payment.

Data Analysis

Before performing the analysis, we completed the following data pre-processing tasks:

1. *Dimensionality reduction*: We reduced the five product characteristics into the following two characteristics:
    a. Benefits = benefits + likelihood of use
    b. Dread (perceived risk) = severity + worry + hazardousness
2. *Standardisation*: We standardised the values for benefits, dread and willingness to pay (WTP).

We used Bayesian modelling to investigate which factors (i.e. demographics and product) predicted benefits, dread, and WTP before and after product compliance information (see Appendix D for additional details).

9.4.2 Results

The effect of individual characteristics and product on perceived benefits, dread and willingness to pay at T1

The Bayesian analysis results and Figure 97 revealed that consumers judged the microwave oven as having lower benefits and greater dread when compared to the carbon monoxide detector. As a result, consumers were willing to pay less for the microwave oven when compared to the carbon monoxide detector. Regarding the other predictors, such as gender and age, there was no strong, robust evidence for differences between their groupings.

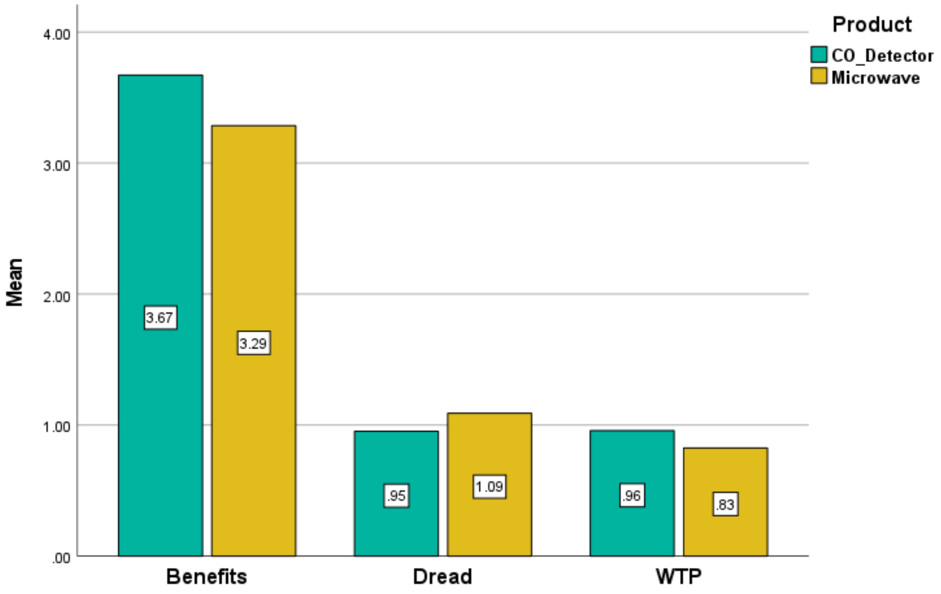


Figure 97 Benefits, Dread and WTP scores at T1 for Products

Interaction effects between product compliance information and source reliability on the change in perceived benefits, dread and willingness to pay

To investigate support for Hypotheses 2-5, we examined the interaction effect between product compliance information and source reliability on the change in perceived benefits, dread and WTP. The combined results for both products are summarised in Table 28. Please note that there are some significant differences in the results between the two products (i.e., carbon monoxide detector and microwave oven). For instance, the decrease in benefits given non-compliant information from reliable and unreliable sources is greater for the carbon monoxide detector when compared to the microwave oven. Also, the increase in dread is greater for the carbon monoxide detector when compared to the microwave oven, given non-compliant information from an unreliable source. For further information on the differences in the results between the two products, please see Figure D10 in Appendix D.

Table 28 Summary of Study Results (Combined results for both products)

Product Compliance Information	**Source Reliability**	**Dread (Risk)**	**Benefits**	**WTP**
Compliant				
Non-Compliant		+++	- - -	- -
Compliant	Reliable			
Non-Compliant	Reliable	+++	- - -	- -
Compliant	Unreliable	+		-
Non-Compliant	Unreliable	+++	- -	-

Legend	Increase	+
	Decrease	-
	No Change	

The symbols +, ++, +++ and -, --, --- represent different levels of change based on relative increase or decrease.

9.4.3 Discussion

The present study advances our understanding of how the reliability of the source of the risk communication and product compliance information can influence willingness to pay (WTP) and risk perception of consumer products. In support of Hypothesis 1, non-compliance information decreased benefits, increased dread (perceived risk) and decreased WTP when compared to compliance information. Consistent with Hypothesis 2, we found that compliance information from a reliable source caused no change in the perceived dread, benefits and WTP. In support of Hypothesis 3, we found that non-compliance information from a reliable source increased dread and decreased the benefits and WTP. We found partial support for Hypothesis 4; compliance information from an unreliable source slightly increased dread and decreased WTP but caused little or no change in the perceived benefits. Finally, in support of Hypothesis 5, we found that non-compliance information from an unreliable source increased dread, decreased benefits and WTP.

The findings of our study are consistent with Study 1 and previous research suggesting that when a product is perceived as having high dread (risk), in this instance, non-compliant, it is generally perceived as having lower benefits [36]–[38]. Furthermore, the reliability of the source of the risk information can affect how the information is perceived and the perception of risk [32], [48], [49], [212], [233]. For instance, when the source is judged reliable, it will mostly influence risk perception and behaviour than if it was judged unreliable. Overall, the study results revealed that product compliance information is the main driver of change in risk perception and WTP for consumer products when compared to the reliability of the source. In each scenario with non-compliance information, whether from a reliable or unreliable source, perceived benefits decreased, dread increased, and WTP decreased. This corroborates the results of Study 1 and the BN model (on the assumption that risk communication primarily concerns non-compliant products).

Our findings have several implications for risk communicators and national safety regulators. Since the reliability of the source can affect the way people react to risk information and perceive risk, especially when they lack knowledge, all sources used to disseminate information should be perceived by the public as trustworthy and credible. This may be achieved by ensuring that all information (past and future) disseminated by the source is accurate and complete. Sources with a reputation for good and accurate information will gain public trust and influence risk perception and behaviour [49], [234]. With regard to the technologies used for risk communication, it is important that they are appropriate and trusted by the public. Since different technologies have different features that determine the extent to which the public trusts them, risk communicators and safety regulators should disseminate information using trusted technologies.

Our present study is the first to investigate how consumers perceive the risks associated with consumer products and whether risk perceptions and WTP differ based on the reliability of the source of the risk communication and product compliance information. The findings of this study have to be seen in light of some limitations. This study examined only two products (i.e., carbon monoxide detector and microwave oven). Since some of the results differed between the products, this suggests that future work should examine other products since risk perception is product-dependent [32]. Another limitation of this study is that it only examined risk communication from consumer safety websites. Hence future work should examine the reliability of other sources of risk communication since different sources have inherent factors that differentiate how they are perceived and trusted by the public.

9.5 Chapter Summary

The empirical studies discussed in this chapter provide novel insights on the effect of risk communication and its source on the risk perception of consumer products. The principal merit of these studies is to inform and validate the results of the consumer risk perception component of the BN for consumer product safety risk assessment discussed in Chapter 8. This BN component models risk perception and the effect of risk communication on risk perception. It predicts that risk communication will increase perceived risk and decrease perceived benefits and risk tolerance. In Study 1, we found that risk communication from different sources impacted risk perception. The government, manufacturer, and large media coverage/story each contributed to a similar level of increase in perceived risk, and they each lowered the level of utility and risk tolerance to a similar degree. On the other hand, small media coverage/story had the least impact on perceived risk, utility and risk tolerance. In Study 2, we found that product compliance information is the main driver of change in risk perception and WTP for consumer products when compared to the reliability of the source of the risk communication. In each scenario with non-compliance information (i.e., risk communication about a non-compliant product), whether from a reliable or unreliable source, perceived benefits decreased, dread (perceived risk) increased, and WTP decreased. Therefore, the results of Study 1 and Study 2 corroborate the results of the BN model. In general, the findings of these studies add to the existing literature in this field.

Chapter 10 Deployment of Bayesian Networks for Safety Risk Management

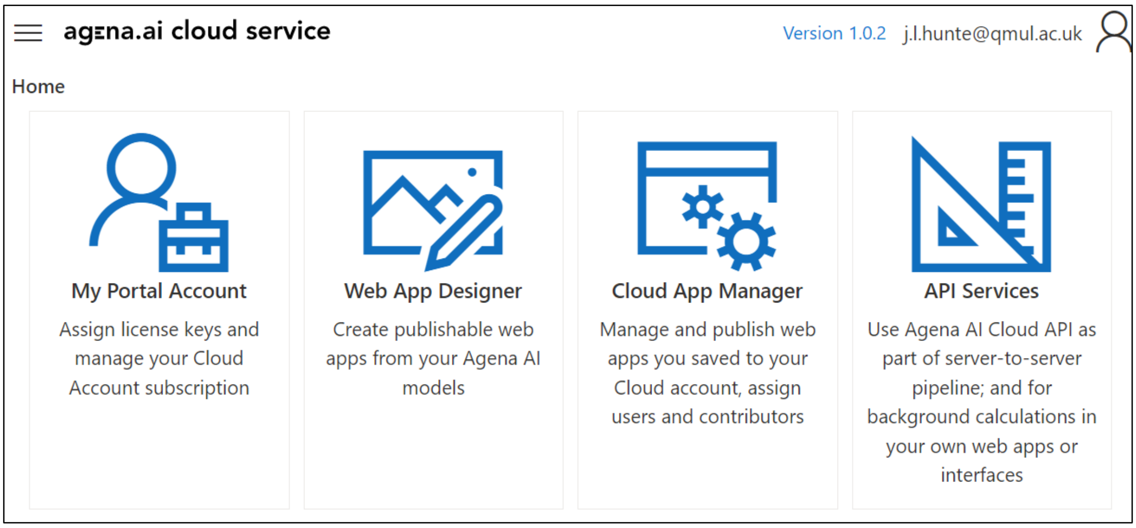
In Chapters 7 and 8, we developed BNs for safety risk assessment of medical devices and consumer products. Despite the many benefits offered by these BNs, their use is limited if they are not deployed to end users in a practical and efficient manner. In this chapter, the deployment of BNs as web-based applications (or web applications) using the *Agena.ai cloud service* is discussed. In Section 10.1, the necessary background information is provided. In Section 10.2, the method for deploying a BN to end users is demonstrated using a case study, and the results are discussed in Section 10.3.

This chapter supports Hypothesis 4 (it is possible to deploy BNs for product safety risk management in production in a practical format for easy access and use by end users, including manufacturers, consumers, and safety regulators).

10.1 Introduction

Traditionally, BN software such as AgenaRisk [16], Hugin [235] and Netica [236] aimed to help model experts develop BNs and perform inferences efficiently. This was achieved using a graphical user interface and novel inference algorithms, such as dynamic discretization (discussed in Chapter 4) [237]. Despite the many benefits offered by the BNs developed using these tools, their widespread use is limited due to a lack of methods for easy deployment to end users. However, Agena Ltd [22] (the developer of AgenaRisk) recently launched a new product called *Agena.ai cloud service* for easy development and deployment of BNs to end users. This solution helps model experts to deploy BNs as web-based applications and consists of the following three tools shown in Figure 98: *Web App Designer* (a tool to create web applications), *Cloud App Manager* (a tool to publish web applications and manage users), and *API Services* (AgenaRisk cloud API for background calculations in your own apps or interfaces).

Given the benefits of BNs for safety risk assessment and management, we demonstrate how they can be easily deployed to end users using the Agena.ai cloud service in the next section.



agena.ai cloud service

Version 1.0.2 j.l.hunte@qmul.ac.uk

Home

My Portal Account

Assign license keys and manage your Cloud Account subscription

Web App Designer

Create publishable web apps from your Agena AI models

Cloud App Manager

Manage and publish web apps you saved to your Cloud account, assign users and contributors

API Services

Use Agena AI Cloud API as part of server-to-server pipeline; and for background calculations in your own web apps or interfaces

Figure 98 Agena.ai cloud service portal homepage

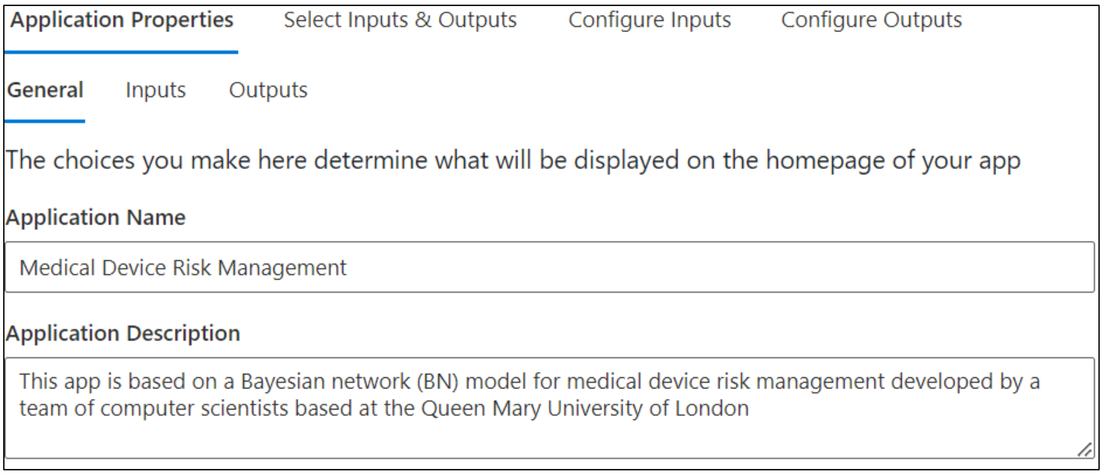
10.2 Case Study: Medical Device Risk Management BN

In this section, we use the BN for medical device risk management to test and evaluate the Agena.ai cloud service. This BN was presented in Chapter 7 (see Figure B2 and Figure B3 in Appendix B for the BN structure).

The following steps were used to construct and deploy a web app using the Agena.ai cloud service:

1. **Upload the model file to Agena.ai cloud service**: In this step, the BN model was exported from AgenaRisk Desktop in JSON format. The AgenaRisk JSON file was then uploaded to the Agena.ai cloud service using the Web App Designer tool.

2. **Configure the app:** Once the model file was uploaded, we configured the app using the Web App Designer tool. The app configuration includes selecting input and output nodes, name, description, and image, as shown in Figure 99. In the web app, the input nodes are represented as text boxes or drop-down lists, and the output nodes are represented as graphs.



The choices you make here determine what will be displayed on the homepage of your app

Application Name

Medical Device Risk Management

Application Description

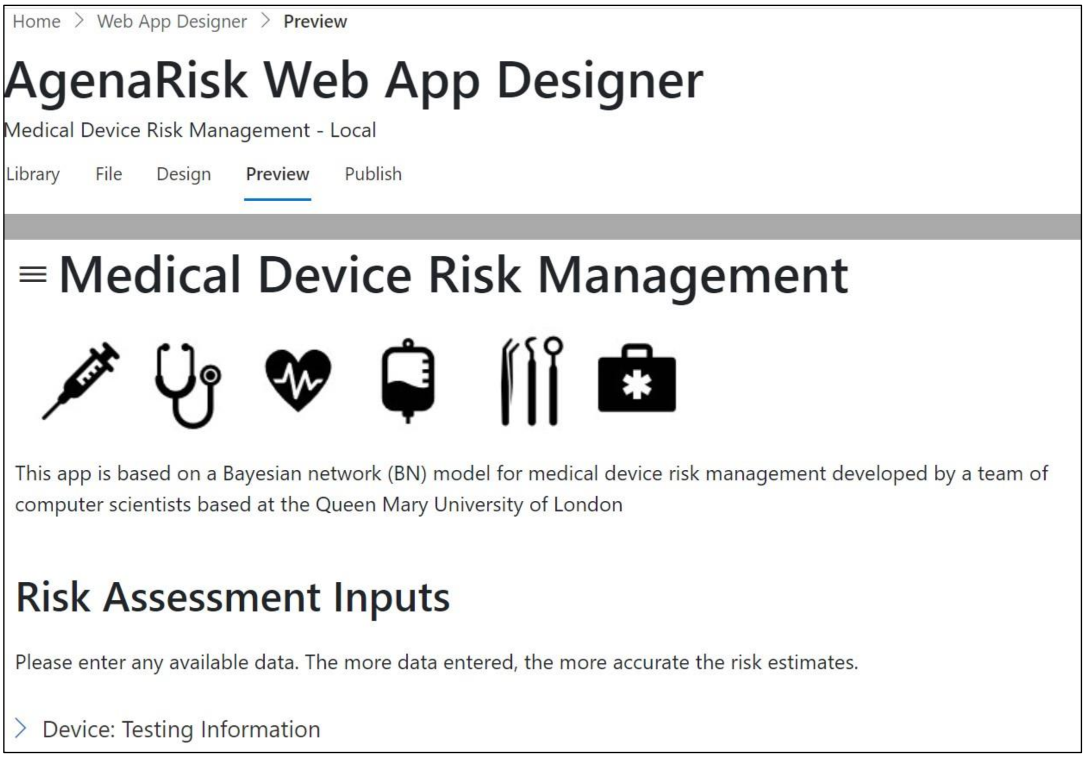
This app is based on a Bayesian network (BN) model for medical device risk management developed by a team of computer scientists based at the Queen Mary University of London

Figure 99 Web App Configuration

3. **Preview and Fine Tune:** Once we configured the web app, we previewed it to see how it looks and works with the current settings (see Figure 100). During the preview, we validated the results of the web app by entering observations and comparing the results with those obtained using AgenaRisk Desktop. For instance, in Figure 101 we compare the results of the web app and AgenaRisk Desktop for risk management scenario 1 (see Section 7.4.2). In this example, the web app results are the same as AgenaRisk Desktop.

4. **Publish App:** Once the app is judged acceptable, we then deployed it using the Cloud App Manager tool (see Figure 98). App deployment was done via a three-step process: (1) save the app to your online account on Agena.ai cloud service (2) enter a subdomain in *agenaai.app* domain (3) mark the app as published.

Finally, once the web app was published (see Appendix E), we used it to make predictions. We did this by accessing it via its website address (or URL) and entering relevant observations using the input text boxes or drop-down lists. The results of the web app were displayed as graphs, as shown in Figure 101.



AgenaRisk Web App Designer

Medical Device Risk Management - Local

≡ Medical Device Risk Management

This app is based on a Bayesian network (BN) model for medical device risk management developed by a team of computer scientists based at the Queen Mary University of London

Risk Assessment Inputs

Please enter any available data. The more data entered, the more accurate the risk estimates.

> Device: Testing Information

Figure 100 Web App Preview

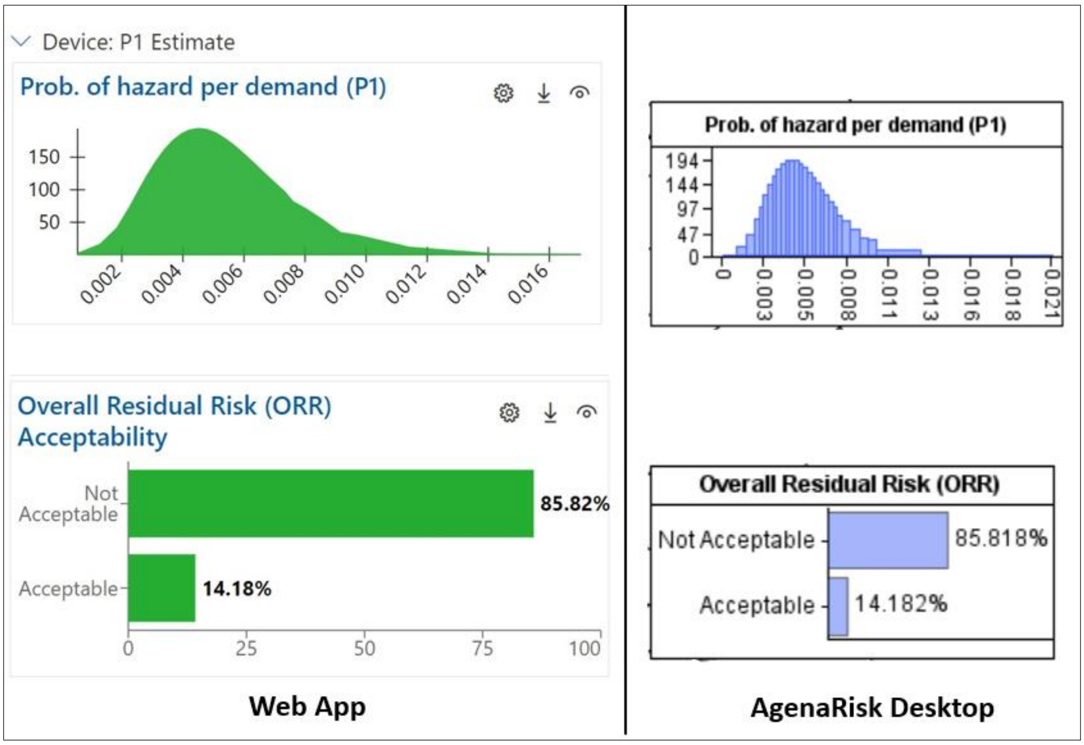


Figure 101 Web app results validation

10.3 Discussion

The case study results show that the Agena.ai cloud service can easily create and deploy a BN model as a web app to end users. Furthermore, the results of the web app are identical to the results obtained using AgenaRisk Desktop. These results support Hypothesis 4 and have implications for risk modellers – the ability to easily develop and deploy BNs as web apps to end users will further promote the use of BNs in industry and everyday life. In the context of safety risk management, for example, medical device risk management, the web app provides a user-friendly interface for end users to assess the risk of medical devices. In fact, end users would not require any knowledge of BNs to perform a risk assessment. Therefore, issues such as complexity and adoption barriers associated with using BNs for safety risk management and other applications are resolved.

The case study results also have implications for organisations that use BNs in production. Novel technologies like Agena.ai cloud service will allow organisations to easily deploy new and existing BNs as web apps in production. In addition, organisations can manage access to these web-based systems more efficiently. Also, since the web app can be accessed anywhere, anytime by end users via the internet, this can increase productivity in the workplace.

The main limitation of this work is that only Agena.ai cloud service was evaluated as a method to deploy BNs as web apps in production since the BNs were developed using AgenaRisk Desktop. Future work should include evaluating similar BN deployment technologies, such as Netica-Web [236].

10.4 Chapter Summary

This chapter describes a method for deploying BNs for safety risk management using *Agena.ai cloud service*. In the case study, we developed a web app for the BN for medical device risk management. The case study results show that BNs can easily be deployed to end users as a web app practically and efficiently. As a web app, end users can access the BN anywhere, anytime, via the internet. Furthermore, the user-friendly interface of the web app does not require end users to have knowledge of BNs to perform a specific task such as risk assessment, hence promoting the use of BNs for safety risk management and other applications in industry and everyday life.

Chapter 11 Conclusions, Contribution, and Future Directions

This chapter revisits the research hypotheses of this thesis and summarises the related contributions. The chapter ends with the future directions of research.

11.1 Research Hypotheses and Contributions

Though BNs have been used extensively in the safety domain, their use for product safety risk management is limited. In this thesis, we bridged this research gap by proposing a novel method for developing robust, accurate BN models for product safety risk management. We also investigate how BNs can be deployed to end users using recent technological innovations. These research objectives were investigated using four hypotheses. In this section, each hypothesis is reviewed, and their supporting arguments and contributions are summarised.

Hypothesis 1: It is possible to develop a generic method to build Bayesian networks for product safety risk management.

There are many techniques and approaches used in the industry to assess and model the risks of products and systems, including the commonly used Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) (see Chapter 3 for a review of risk analysis methods). However, these risk analysis methods have several limitations, such as a limited approach to handling uncertainty, which can lead to inaccurate or ill-defined risk estimates (see Section 1.3, Section 7.2 and Section 8.3) for more details). Although some extensions of these methods, such as Dynamic Fault Trees (DFTs), have resolved some of these limitations, BNs can resolve all limitations.

However, despite the many advantages of using BNs for safety risk management, the literature review presented in Chapter 5 revealed that their widespread acceptance and use as a standard systematic method for product safety risk management are limited. This may be due to limited or no standard method or guidelines for building BNs for the many different product safety cases. Furthermore, the few published BNs in this area are presented with little information on how the BN was developed and why it is suitable for the specific application. In other cases, the BN development process is ad hoc and presents little or no opportunity for repeatability and standardisation. In addition, some established methods for BN development (see Section 4.3 and Section 5.2 for additional details) may not be feasible for many product safety cases due to adoption barriers, e.g., lack of knowledge and the complexity of safety risk (dependent on the interaction between hard factors, e.g., systems and soft factors, e.g., processes). In these situations, the BN must be developed using expert knowledge and literature. However, the literature lacks a systematic, repeatable method or guidelines for developing BNs for product safety risk management using expert knowledge and literature.

Contribution

In Chapter 6, we proposed a novel method for developing BNs for product safety risk management using causal idioms. This novel set of idioms, called *product safety idioms*, complements and extends the idiom-based approach proposed by Neil et al. [19] and other methods for BN development (see Section 4.3 and Section 5.2). Product safety idioms are tailored to the requirements of the safety risk management process (see Figure 1). They are based on the logical causal relationship among the factors used to estimate and evaluate product risk. While the proposed idioms are sufficiently generic to be applied to a wide range of product safety cases, they are not prescriptive or complete and should be considered as a guide for developing suitable idioms for product safety risk management. As discussed in Section 6.5, the benefits offered by the product safety idioms include:

1. *Integration of different types of knowledge sources*: As demonstrated in Section 6.4.2, the idioms can combine objective evidence, e.g., PFD, and subjective evidence, e.g., manufacturing process quality, to provide reasonable risk estimates for products. Combining objective and subjective evidence is especially useful for handling uncertainty in situations when there is limited or no historical testing and operational data for products, but expert knowledge is available.

2. *Handle uncertainty in data*: Some risks associated with products can be characterised by high levels of uncertainty and ambiguity. Uncertainty can be caused by limited or lack of relevant data. Product safety idioms can handle and communicate uncertainties in the data explicitly since they express uncertainty in terms of probability distributions.

3. *Standardise and assist product safety BN development*: To the best of our knowledge, there is no standard method for developing BNs specifically for product safety risk management. The product safety idioms improve BN development by simplifying the knowledge elicitation task. They provide a library of reusable BN patterns for product safety that facilitates the easy development of practical product safety BNs. They also guide the knowledge elicitation process by allowing model experts and safety risk professionals to identify relevant information (known or unknown) required to build custom idioms and BNs for product safety assessments.

4. *Enhance the communication, interpretability and explainability of complex BNs:* The graphical structure and results of the BNs developed using the idioms can be easily interpreted, explained, and reviewed by model experts and safety risk professionals. For example, the graphical structure of BNs facilitates easy communication of uncertainty and risks. Stakeholders can easily identify sources of uncertainty in the model. In addition, product safety idioms can serve as a validation method for future product safety risk BNs, ensuring that their structure is practical and logical.

We believe that the product safety idioms are meaningful reasoning patterns that guide the development of complex BNs for product safety risk management and can help promote the use of BNs in this domain.

Hypothesis 2: It is possible to use Bayesian networks for safety risk management for many different types of products, including novel products or products with limited or no available data.

Many traditional risk analysis techniques, such as FTA, compute risk as the product of the probability of occurrence of harm P and the severity of the harm S, i.e., $Risk = P \times S$. As a result, these methods are unable to provide reasonable risk estimates for novel products or products with limited or no available data since the probability of occurrence of harm P may be uncertain or unknown. However, BNs can be used to assess the risk of novel products or products with limited or no historical data since it is a rigorous normative method for modelling uncertainty and causality.

Contribution

In Chapter 7 and Chapter 8, we developed BNs for medical device risk management and consumer product safety risk assessment using product safety idioms, expert knowledge and literature. For each BN, we demonstrated risk estimation for products with available data and products with limited or no historical data (see Section 7.4 and Section 8.5). We show that the risk of products with limited or no historical data can be estimated using data from previous similar systems (or generic probabilities) together with information about the quality of the processes and people involved in their development. Most importantly, we show that risk estimates can be revised once relevant data is available, such as reported injury reports.

The principal merit of the proposed generic BN for medical device risk management is to provide a robust systematic method for medical device manufacturers to manage the risk of medical devices throughout their life cycle (i.e., initial conception to final decommissioning and disposal). We believe that the BN improves the risk management of medical devices in the following ways (see Section 7.5 for more details):

1. It provides a robust method for managing the risk of medical devices throughout their life cycle (i.e., production and post-production).
2. It informs risk control measures/ risk treatment given the risk acceptability criteria and supports iterative risk treatment.
3. It improves the interpretability and explanation of risk estimates.
4. It handles uncertainty in the data, especially for novel medical devices and software with little or no relevant historical data.
5. It provides individual risk estimates since it considers device use and device age information when estimating risk.
6. It supports market surveillance and review (post-market/post-production activities). The BN can easily update risk estimates given new information, such as reported injuries.
7. It complements existing risk management methods such as FTA. This enables easy adoption of the proposed BN in the industry.

8. It performs and improves benefit-risk analysis.

The principal merit of the proposed generic BN for consumer product safety risk assessment is to provide a robust systematic method for safety regulators, manufacturers and market surveillance authorities to assess the risk of consumer products. We believe that the BN model provides the following improvements to consumer product risk assessment (see Section 8.6 for more details):

1. Properly handles uncertainty about probabilities assigned during risk assessment.

2. Can assess the risk of novel products or products with little or no historical data.

3. Incorporates causal explanations for using and interpreting the data.

4. Considers the usage behaviour for different types of users and the number of product instances when determining product risk. Hence it supports individual and population risk assessment.

5. Models risk tolerability (acceptability), risk perception and the effect of risk communication on risk perception. To the best of our knowledge, this is the first BN to model risk tolerability, risk perception and the effect of risk communication on risk perception.

6. Considers the increased risk of hazards over the lifetime of a product when estimating risk.

7. It complements and resolves the limitations with existing methods such as RAPEX.

Other significant contributions of our work on consumer product safety risk assessment include the development of the UK Government Office for Product Safety and Standards (OPSS) risk lexicon [24]. OPSS risk lexicon is the organisational definitions of terms concerned with risk and risk-related matters. It was informed by the material presented in Chapter 2. Most importantly, our work contributed to the development of OPSS new product safety risk assessment methodology ‘PRISM’ [238]. PRISM introduced in December 2022, is used by safety regulators in UK to assess the risk associated with consumer products (non-food). It improves consumer product risk assessment by resolving some of the limitations of the RAPEX methodology identified in our work (in fact, the ‘PRISM’ guide references our work presented in Chapter 8). For instance, it considers other relevant factors, such as frequency of use and product instances when estimating risk.

Hypothesis 3: It is possible to use Bayesian networks to model consumer risk perception and/or perform benefits-risk analysis for products.

1. Consumers may judge the risk and benefits of products differently from experts. For instance, experts tend to judge the risk of a product using quantitative risk assessments, whereas consumers judge risk using a combination of subjective measures such as hazardousness. Regardless of the results of the quantitative risk assessment, consumer risk perception should not be overlooked and must be considered when evaluating risk. In addition, previous research and our empirical work show that risk communication can influence risk perception (see Chapter 9). For instance, risk communication about non-compliant products increased perceived risk and decreased benefits. However, there are no automated methods for predicting risk perception of products and the effect of risk communication on risk perception. BNs are suitable for this task due to their ability to combine objective and subjective evidence to make predictions.

2. During medical device risk management, in situations where risk reduction measures are not practical, a benefit-risk analysis is done to determine if the benefit of a device outweighs its risk. However, there are no automated methods for performing this task since it is usually based on subjective evidence, such as the clinical outcome expected from using the device and objective evidence, such as risk estimates. BNs are suitable for this task due to their ability to combine objective and subjective evidence to make predictions.

Contribution

1. To the best of our knowledge, the proposed BN for consumer product safety risk assessment discussed in Chapter 8 is the only method that models consumer risk perception and the effect of risk communication on risk perception. The model can predict the perceived risk, benefits and risk

tolerance of products and the effect of risk communication on all these perceptions. The predictions of the BN model are validated by the empirical work presented in Chapter 9 done in collaboration with the UK Government Office for Product Safety and Standards (OPSS) and researchers at Royal Holloway University of London (RHUL). The empirical studies provided OPSS with novel insights on the risk perception of consumer products (smart and non-smart) and how it is influenced by risk communication. It improved OPSS risk communication strategies concerning non-compliant products and reduced potential harm to consumers. In addition, this work extends the literature in this domain since there is little or no previous research on the risk perception of consumer products (smart and non-smart), and how it is influenced by risk communication from different sources such as the government, manufacturer and media.

2. To the best of our knowledge, the proposed BN for medical device risk management presented in Chapter 7 is the only method that automatically combines subjective evidence about the benefits of a medical device together with the estimated risk (objective evidence), to determine risk acceptability for a medical device. Hence, the BN improves risk management since the benefit-risk analysis can be performed quickly and more efficiently. Moreover, any uncertainty in the subjective evidence can be incorporated before making predictions.

Hypothesis 4: It is possible to deploy BNs for product safety risk management in production in a practical format for easy access and use by end users, including manufacturers, consumers and safety regulators.

Traditionally, BN software such as AgenaRisk [16], Hugin [235] and Netica [236] aimed to help model experts develop BNs and perform inferences efficiently. Despite the many benefits offered by the BNs developed using these tools, their widespread use is limited due to a lack of methods for easy deployment to end users.

Contribution

In Chapter 10, we described a method for deploying BNs for safety risk management using *Agena.ai cloud service* (a novel technology for deploying BNs as web apps to end users). The case study results show that BNs can easily be deployed to end users as a web app practically and efficiently. As a web app, end users can access the BN for safety risk management anywhere, anytime, via the internet. Furthermore, the user-friendly interface of the web app does not require end users to have knowledge of BNs to perform tasks, such as risk assessment, hence promoting the use of BNs for safety risk management and other applications in industry and everyday life.

11.2 Future Directions

The novel contributions presented in this thesis provide a guide for developing and deploying BNs for product safety risk management. In this section, we present some interesting future directions for the work presented in this thesis, considering recent advancements in Artificial Intelligence (AI), in particular Generative AI and Explainable AI.

11.2.1 BN Improvements

The BN for medical device risk management presented in Chapter 7 could be extended to model consumer risk perception of medical devices. This will require empirical studies to understand how consumers perceive the risk of medical devices and how these perceptions change given risk communication. The risk perception information can be incorporated in the BN using the *consumer risk perception idiom* presented in Chapter 6.

A limitation of the product safety idioms and BNs presented in this thesis is that they are not aligned to risk acceptance principles like ALARP (as low as reasonably practicable), SFAIRP (so far as is reasonably practicable), GAMAB ("globalement au moins aussi bon", generally at least as good) and MEM (minimum endogenous mortality).

The ALARP principle [239]–[242] requires that the risk of a system be reduced to a "reasonably practicable" level. Determining whether the risk of a system is ALARP entails considering whether risk control measures are "good practice" and whether the cost of additional risk control measures is grossly disproportionate to its benefits; the latter is facilitated by a Cost Benefit Analysis (CBA). The BN models presented in this thesis can be extended to incorporate a Cost Benefit Analysis (CBA) to support ALARP decisions. The CBA component of the BN will include nodes representing the cost of the risk control measures, the benefits of the risk control measures (defined using the same units as the cost) and the results of the CBA; the latter used for assessing ALARP. It is important to note that the risk is only considered ALARP when the cost of the risk control measures is judged grossly disproportionate to its benefits. In situations where the cost of the risk control measures is not judged grossly disproportionate to its benefits, then the risk control measures must be implemented. The *risk tolerability idiom* presented in Chapter 6 can be adapted to model a CBA. In this thesis, SFAIRP is considered the same as ALARP.

The GAMAB principle [243] requires that the risk of new systems should not exceed the risks of previous similar systems. The MEM principle [243] requires that a new system does not significantly increase the minimum endogenous mortality (i.e., lowest natural mortality rate). The BN models can be extended to support GAMAB and MEM decisions using the *requirement idiom* presented in Chapter 6.

Other future work includes applying the product safety idioms to other industries in the safety domain, such as aviation and conducting additional empirical studies to gain a comprehensive understanding of the risk perception of products since it is product dependent.

11.2.2 Generative AI for BN Development

The novel method for developing BNs using causal idioms presented in Chapter 6 can provide the basis for the use of Generative AI for the development of BNs. Generative AI is an artificial intelligence technology that can generate different types of content, such as text and imagery given instructions, e.g., questions or text [244]. For example, the AI tool “DALL-E2” developed by OpenAI can create realistic images and art from a text description [245]. Regarding BN development, a generative model can be trained on the product safety idioms since they represent the generic logical causal patterns of reasoning for safety risk management. Once trained, end users can enter text describing a desired model for safety risk management, and the system would generate reasonable model structures based on the structure of the pre-defined idioms. In addition, the generative model can also create new idioms or structures as required by combining and mixing different idioms. Using generative models for BN development would further increase the use of BNs in industry and everyday life.

11.2.3 Generative AI for explaining BN Model and Results

Although the product safety idioms support the explainability of the BN model results, this can be further improved by using Generative AI tools like ChatGPT [246], also developed by OpenAI. ChatGPT is an AI tool that supports human-like conversations with a chatbot. When applied to BNs, ChatGPT can provide a creative description of the structure and results of the model for end users, as requested. In addition, it can explain the reason for the results since the processes by which BNs make predictions are causal and explicit. Explainability can help model experts ensure that the model predictions are accurate and help end users understand the model results, further promoting the use of BNs in industry and everyday life.

Bibliography

[1] The Guardian, “Grenfell costs surpass £500m as council bill revealed | Grenfell Tower fire | The Guardian,” 2021. https://www.theguardian.com/uk-news/2021/may/21/grenfell-costs-surpass-500m-as-council-bill-revealed (accessed Aug. 03, 2022).

[2] BBC, “Grenfell Tower: What happened - BBC News,” *Article*, 2018. https://www.bbc.co.uk/news/uk-40301289 (accessed Aug. 03, 2022).

[3] The Guardian, “Boeing 737 Max disaster casts long shadow as planemaker tries to rebuild fortunes | Boeing | The Guardian,” 2022. https://www.theguardian.com/business/2022/jun/25/max-disaster-casts-long-shadow-as-boeing-tries-to-rebuild-its-fortunes (accessed Aug. 03, 2022).

[4] The Guardian, “Whirlpool recall: is your machine a fire risk, and what should you do? | Consumer affairs | The Guardian,” 2020. https://www.theguardian.com/money/2020/jan/10/whirlpool-recall-washing-machine-fire-risk-hotpoint-and-indesit (accessed Aug. 02, 2022).

[5] European Commission, “Commission Implementing Decision (EU) 2019/417 of 8 November 2018 laying down guidelines for the management of the European Union Rapid Information System ‘RAPEX’ established under Article 12 of Directive 2001/95/EC on general product safety,” *Official Journal of the European Union*, vol. 2018, no. November 2018, 2018, [Online]. Available: http://data.europa.eu/eli/dec/2019/417/oj

[6] ISO, “ISO 24971 Medical devices — Guidance on the application of ISO 14971,” 2020.

[7] ISO, “ISO 14971 Medical devices - Application of risk management to medical devices,” 2019.

[8] European Commission, “EU general risk assessment methodology (Action 5 of Multi-Annual Action Plan for the surveillance of products in the EU (COM(2013)76),” 2015. [Online]. Available: http://ec.europa.eu/DocsRoom/documents/17107/attachments/1/translations/

[9] ISO/IEC/IEEE 15288, “International Standard ISO/IEC/IEEE 15288 Systems and Software engineering - System life cycle processes,” *ISO*, vol. 17, no. 1, p. 108, 2015.

[10] ISO/IEC, “ISO/IEC Guide 63:2019 Guide to the development and inclusion of aspects of safety in International Standards for medical devices,” 2019.

[11] ISO, “ISO 31000:2018(en), Risk management — Guidelines,” 2018. Accessed: Sep. 15, 2022. [Online]. Available: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

[12] B. Elahi, *Safety Risk Management for Medical Devices*. 2022. doi: 10.1016/c2020-0-02307-8.

[13] N. Fenton and M. Neil, *Risk assessment and decision analysis with bayesian networks*. Crc Press, 2018. doi: 10.1201/b21982.

[14] S. Ramakrishna, L. Tian, C. Wang, S. Liao, and W. E. Teo, “Risk assessment management for a new medical device,” in *Medical Devices,* Elsevier, 2015, pp. 123–135. doi: 10.1016/b978-0-08-100289-6.00005-3.

[15] J. Hunte, M. Neil, and N. E. Fenton, “A causal Bayesian network approach for consumer product safety and risk assessment,” *J Safety Res*, vol. 80, pp. 198–214, Dec. 2022, doi: 10.1016/j.jsr.2021.12.003.

[16] K. Durga Rao, V. Gopika, V. V. S. Sanyasi Rao, H. S. Kushwaha, A. K. Verma, and A. Srividya, “Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment,” *Reliab Eng Syst Saf*, vol. 94, no. 4, pp. 872–883, Apr. 2009, doi: 10.1016/j.ress.2008.09.007.

[17] W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl, “Fault Tree Handbook,” Systems and Reliability Research, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1981. Accessed: Aug. 01, 2023. [Online]. Available: http://www.stormingmedia.us/37/3794/A379453.pdf%5Cnhttp://ocw.mit.edu/courses/aeronautics-and-astronautics/16-63j-system-safety-fall-2012/related-resources/MIT16_63JF12_faulttree.pdf%5Cnhttp://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/

[18] A. Bobbio, L. Portinale, M. Minichino, and E. Ciancamerla, “Improving the analysis of dependable systems by mapping Fault Trees into Bayesian Networks,” *Reliab Eng Syst Saf,* vol. 71, no. 3, pp. 249–260, Mar. 2001, doi: 10.1016/S0951-8320(00)00077-6.

[19] M. Neil, N. Fenton, and L. Nielsen, “Building large-scale Bayesian networks,” *Knowledge Engineering Review,* vol. 15, no. 3, pp. 257–284, 2000, doi: 10.1017/S0269888900003039.

[20] G. Bearfield and W. Marsh, “Generalising event trees using Bayesian networks with a case study of train derailment,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics),* Springer, Berlin, Heidelberg, 2005, pp. 52–66. doi: 10.1007/11563228_5.

[21] M. Scutari, C. E. Graafland, and J. M. Gutiérrez, “Who learns better Bayesian network structures: Accuracy and speed of structure learning algorithms,” *International Journal of Approximate Reasoning,* vol. 115, pp. 235–253, Dec. 2019, doi: 10.1016/J.IJAR.2019.10.003.

[22] Agena Ltd, “AgenaRisk: Bayesian Network Software,” 2022. www.agenarisk.com

[23] J. Hunte, M. Neil, and N. Fenton, “A causal Bayesian network approach for consumer product safety and risk assessment: Research Summary Report,” 2021. Accessed: Nov. 11, 2022. [Online]. Available:

https://www.gov.uk/government/publications/bayesian-product-safety-summary-report

[24] J. Hunte, M. Neil, and N. Fenton, “Product safety idioms: a method for building causal Bayesian networks for product safety and risk assessment,” Jun. 2022, doi: 10.48550/arxiv.2206.02144.

[25] J. Hunte, M. Neil, and N. Fenton, “A hybrid Bayesian network for medical device risk assessment and management,” Sep. 2022, doi: 10.48550/arxiv.2209.03352.

[26] OPSS, “OPSS risk lexicon - GOV.UK,” May 21, 2021. https://www.gov.uk/guidance/opss-risk-lexicon (accessed Jun. 16, 2021).

[27] ISO, “ISO GUIDE 73:2009 - Risk management - Vocabulary,” 2009.

[28] J. C. Laprie, “Dependability of computer systems: concepts, limits, improvements,” in *Proceedings of the International Symposium on Software Reliability Engineering, ISSRE*, 1995, pp. 2–11. doi: 10.1109/issre.1995.497638.

[29] A. Avižienis, J. C. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,” *IEEE Trans Dependable Secure Comput*, vol. 1, no. 1, pp. 11–33, 2004, doi: 10.1109/TDSC.2004.2.

[30] D. F. Cox and S. U. Rich, “Perceived Risk and Consumer Decision-Making—The Case of Telephone Shopping,” *Journal of Marketing Research*, vol. 1, no. 4, pp. 32–39, Nov. 1964, doi: 10.1177/002224376400100405.

[31] Y. Gidron, “Perceived Risk,” in *Encyclopedia of Behavioral Medicine*, Springer, New York, NY, 2013, pp. 1453–1453. doi: 10.1007/978-1-4419-1005-9_1554.

[32] P. Slovic, “Perception of risk,” *Science (1979)*, vol. 236, no. 4799, pp. 280–285, Apr. 1987, doi: 10.1126/science.3563507.

[33] S. Balasubramanian, R. Raghunathan, and V. Mahajan, “Consumers in a multichannel environment: Product utility, process utility, and channel choice,” *Journal of Interactive Marketing*, vol. 19, no. 2, pp. 12–30, 2005, doi: 10.1002/dir.20032.

[34] K. Horn, “Consumer values and product perception,” in *Consumer Perception of Product Risks and Benefits*, Springer International Publishing, 2017, pp. 283–299. doi: 10.1007/978-3-319-50530-5_16.

[35] S. Leroi-Werelds, S. Streukens, M. K. Brady, and G. Swinnen, “Assessing the value of commonly used methods for measuring customer value: A multi-setting empirical study,” *J Acad Mark Sci*, vol. 42, no. 4, pp. 430–451, 2014, doi: 10.1007/s11747-013-0363-4.

[36] A. S. Alhakami and P. Slovic, “A Psychological Study of the Inverse Relationship Between Perceived Risk and Perceived Benefit,” *Risk Analysis*,

vol. 14, no. 6, pp. 1085–1096, 1994, doi: 10.1111/j.1539-6924.1994.tb00080.x.

[37] P. Slovic, N. Kraus, H. Lappe, and M. Major, “Risk perception of prescription drugs: Report on a survey in Canada,” in *Canadian Journal of Public Health*, 1991.

[38] B. Fischhoff, P. Slovic, S. Lichtenstein, S. Read, and B. Combs, “How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits,” *Policy Sci*, vol. 9, no. 2, pp. 127–152, Apr. 1978, doi: 10.1007/BF00143739.

[39] M. J. Roszkowski, “Risk Perception and Risk Tolerance Changes Attributable to the 2008 Economic Crisis: A Subtle but Critical Difference,” 2010.

[40] S. B. Eysenck and H. J. Eysenck, “Impulsiveness and venturesomeness: their position in a dimensional system of personality description.,” *Psychol Rep*, vol. 43, no. 3 Pt 2, pp. 1247–1255, 1978, doi: 10.2466/pr0.1978.43.3f.1247.

[41] A. Wong and B. J. Carducci, “Sensation seeking and financial risk taking in everyday money matters,” *J Bus Psychol*, vol. 5, no. 4, pp. 525–530, Jun. 1991, doi: 10.1007/BF01014500.

[42] R. B. Barsky, F. T. Juster, M. S. Kimball, and M. D. Shapiro, “Preference parameters and behavioral heterogeneity: An experimental approach in the health and retirement study,” *Quarterly Journal of Economics*, vol. 112, no. 2, pp. 537–579, 1997, doi: 10.1162/003355397555280.

[43] P. Slovic, “Assessment of risk taking behavior,” *Psychol Bull*, vol. 61, no. 3, pp. 220–233, Mar. 1964, doi: 10.1037/h0043608.

[44] J. E. Corter and Y. J. Chen, “Do investment risk tolerance attitudes predict portfolio risk?,” *J Bus Psychol*, vol. 20, no. 3, pp. 369–381, Mar. 2006, doi: 10.1007/s10869-005-9010-5.

[45] R. V. Kemp, “Risk tolerance and safety management,” *Reliab Eng Syst Saf*, vol. 31, no. 3, pp. 345–353, Jan. 1991, doi: 10.1016/0951-8320(91)90076-J.

[46] H. K. Kim, “Risk communication,” in *Consumer Perception of Product Risks and Benefits*, Springer International Publishing, 2017, pp. 125–149. doi: 10.1007/978-3-319-50530-5_7.

[47] J. Prior, E. Partridge, and R. Plant, “We get the most information from the sources we trust least: Residents’ perceptions of risk communication on industrial contamination,” *Australasian Journal of Environmental Management*, vol. 21, no. 4, pp. 346–358, Oct. 2014, doi: 10.1080/14486563.2014.954011.

[48] P. Slovic, “Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield,” *Risk Analysis*, vol. 19, no. 4, pp. 689–701, Aug. 1999, doi: 10.1023/A:1007041821623.

[49] J. Fessenden-Raden, J. M. Fitchen, and J. S. Heath, “Providing risk information in communities: Factors influencing what is heard and accepted,” *Sci Technol Human Values*, vol. 12, no. 3, pp. 94–101, 1987.

[50] Y. Zhang, P. L. Jones, and R. Jetley, “A hazard analysis for a generic insulin infusion pump,” *J Diabetes Sci Technol*, vol. 4, no. 2, pp. 263–283, 2010, doi: 10.1177/193229681000400207.

[51] P. Masci, Y. Zhang, P. Jones, H. Thimbleby, and P. Curzon, “A generic user interface architecture for analyzing use hazards in infusion pump software,” in *OpenAccess Series in Informatics*, Schloss Dagstuhl- Leibniz-Zentrum fur Informatik GmbH, Dagstuhl Publishing, 2014, pp. 1–14. doi: 10.4230/OASIcs.MCPS.2014.1.

[52] A. Torrez, “Hazard and safety analysis of the Integra^{TM} UltraVS^{TM} neonate valve,” in *Advances in Intelligent Systems and Computing*, Springer Verlag, 2018, pp. 593–599. doi: 10.1007/978-3-319-60483-1_61.

[53] A. Aloqaily, “Identification of Hazards Associated With Pipelines,” in *Cross-Country Pipeline Risk Assessments and Mitigation Strategies*, Gulf Professional Publishing, 2018, pp. 13–40. doi: 10.1016/b978-0-12-816007-7.00002-0.

[54] M. Rausand and A. Hoyland, *System reliability theory: models, statistical methods, and applications*, 2nd ed., vol. 396. John Wiley & Sons., 2003.

[55] IEC, *Failure modes and effects analysis (FMEA and FMECA) BS EN IEC 60812-2018*. 2018.

[56] R. Onofrio, F. Piccagli, and F. Segato, “Failure Mode, Effects and Criticality Analysis (FMECA) for Medical Devices: Does Standardization Foster Improvements in the Practice?,” *Procedia Manuf*, vol. 3, pp. 43–50, Jan. 2015, doi: 10.1016/j.promfg.2015.07.106.

[57] F. Clemente, G. Faiella, G. Rutoli, P. Bifulco, M. Romano, and M. Cesarelli, “Critical failures in the use of home ventilation medical equipment,” *Heliyon*, vol. 5, no. 12, p. e03034, Dec. 2019, doi: 10.1016/j.heliyon.2019.e03034.

[58] S. Ramakrishna, L. Tian, C. Wang, S. Liao, and W. E. Teo, “Risk assessment management for a new medical device,” in *Medical Devices*, Elsevier, 2015, pp. 123–135. doi: 10.1016/b978-0-08-100289-6.00005-3.

[59] IEC, “Fault tree analysis IEC 61025:2006,” 2006. https://www.en-standard.eu/iec-61025-2006-fault-tree-analysis-fta/ (accessed Oct. 08, 2022).

[60] W. A. Hyman, “A Generic Fault Tree for Medical Device Error,” *J Clin Eng*, vol. 27, no. 2, pp. 134–140, 2002, doi: 10.1097/00004669-200202720-00045.

[61] W. A. Hyman and E. Johnson, “Fault tree analysis of clinical alarms,” *Journal of Clinical Engineering*, vol. 33, no. 2. pp. 85–94, Apr. 2008. doi: 10.1097/01.JCE.0000305872.86942.66.

[62] W. P. Rice, “Medical device risk based evaluation and maintenance using fault tree analysis,” *Biomedical Instrumentation and Technology*, vol. 41, no. 1. pp. 76–82, 2007. doi: 10.2345/0899-8205(2007)41[76:MDRBEA]2.0.CO;2.

[63] W. Marsh and G. Bearfield, “Representing parameterised fault trees using Bayesian networks,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer, Berlin, Heidelberg, 2007, pp. 120–133. doi: 10.1007/978-3-540-75101-4_13.

[64] S. Kabir, “An overview of fault tree analysis and its application in model based dependability analysis,” *Expert Systems with Applications*, vol. 77. Elsevier Ltd, pp. 114–135, Jul. 01, 2017. doi: 10.1016/j.eswa.2017.01.058.

[65] J. B. Dugan, S. J. Bavuso, and M. A. Boyd, “Dynamic Fault-Tree Models for Fault-Tolerant Computer Systems,” *IEEE Trans Reliab*, vol. 41, no. 3, pp. 363–377, 1992, doi: 10.1109/24.159800.

[66] Y. A. Mahmood, A. Ahmadi, A. K. Verma, A. Srividya, and U. Kumar, “Fuzzy fault tree analysis: A review of concept and application,” *International Journal of System Assurance Engineering and Management*, vol. 4, no. 1. Springer, pp. 19–32, Feb. 16, 2013. doi: 10.1007/s13198-013-0145-x.

[67] J. Borcsok, S. Schaefer, … E. U.-I. C. on, and undefined 2007, “Estimation and evaluation of common cause failures,” *ieeexplore.ieee.org*, 2007, Accessed: Jul. 25, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4196343/

[68] A. Summers, K. Ford, G. R.-C. E. Progress, and undefined 1999, “Estimation and evaluation of common cause failures in SIS,” *sis-tech.com*, pp. 85–90, 1999, Accessed: Jul. 25, 2023. [Online]. Available: https://sis-tech.com/wp-content/uploads/2011/05/Estimation_and_Evaluation_of_Common_Cause_Failure_in_the_Safety_Instrumented_Systems.pdf

[69] IEC, “IEC 62502:2010 - European Standards,” 2010.

[70] A. de Ruijter and F. Guldenmund, “The bowtie method: A review,” *Saf Sci*, vol. 88, pp. 211–218, Oct. 2015, doi: 10.1016/j.ssci.2016.03.001.

[71] V. De Dianous and C. Fiévez, “ARAMIS project: A more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance,” *J Hazard Mater*, vol. 130, no. 3 SPEC. ISS., pp. 220–233, Mar. 2006, doi: 10.1016/j.jhazmat.2005.07.010.

[72] S. Raychaudhuri, “Introduction to monte carlo simulation,” in *Proceedings - Winter Simulation Conference*, 2008, pp. 91–100. doi: 10.1109/WSC.2008.4736059.

[73] R. L. Harrison, “Introduction to Monte Carlo simulation,” in *AIP Conference Proceedings*, NIH Public Access, Jan. 2009, pp. 17–21. doi: 10.1063/1.3295638.

[74] Department of Defense of the USA, “Reliability Prediction of Electronic Equipment,” *Military Handbook MIL-HDBK-217F*, p. 205, 1991, Accessed: Jul. 26, 2023. [Online]. Available: http://everyspec.com/MIL-HDBK/MIL-HDBK-0200-0299/MIL-HDBK-217F_14591/

[75] J. Pearl, *Causality: Models, Reasoning, and Inference. 2nd edition*. 2009. doi: 10.1017/S0266466603004109.

[76] J. Pearl and D. Mackenzie, *The Book of Why: The New Science of Cause and Effect*, vol. 1. 2018.

[77] T. Bayes, “LII. An essay towards solving a problem in the doctrine of chances. By the late Rev. Mr. Bayes, F. R. S. communicated by Mr. Price, in a letter to John Canton, A. M. F. R. S,” *Philos Trans R Soc Lond*, vol. 53, pp. 370–418, Dec. 1763, doi: 10.1098/rstl.1763.0053.

[78] T. Stephenson, “An introduction to Bayesian network theory and usage,” IDIAP, 2000.

[79] D. Koller and N. Friedman, *Probabilistic graphical models: principles and techniques*. 2009.

[80] N. Friedman, D. Geiger, and M. Goldszmidt, “Bayesian Network Classifiers,” *Mach Learn*, vol. 29, no. 2–3, pp. 131–163, 1997, doi: 10.1023/a:1007465528199.

[81] D. Heckerman, “A tutorial on learning with Bayesian networks,” *Studies in Computational Intelligence*, vol. 156, pp. 33–82, 2008, doi: 10.1007/978-3-540-85066-3_3.

[82] D. J. Spiegelhalter and S. L. Lauritzen, “Sequential updating of conditional probabilities on directed graphical structures,” *Networks*, vol. 20, no. 5, pp. 579–605, 1990, doi: 10.1002/net.3230200507.

[83] A. C. Constantinou and N. Fenton, “Things to know about Bayesian networks: Decisions under uncertainty, part 2,” *Significance*, vol. 15, no. 2, pp. 19–23, 2018, doi: 10.1111/j.1740-9713.2018.01126.x.

[84] S. M. Mahoney and K. B. Laskey, “Network Engineering for Complex Belief Networks,” Feb. 1996.

[85] K. B. Laskey and S. M. Mahoney, “Network Fragments : Representing Knowledge for Constructing Probabilistic Models,” *Proceedings of the Thirteenth conference on Uncertainty in artificial intelligence*, pp. 334–341, 1997.

[86] D. Koller and A. Pfeffer, “Object-Oriented Bayesian Networks,” 1997.

[87] E. M. Helsper and L. C. Van der Gaag, “Building Bayesian networks through ontologies,” *ECAI2002, Proceedings of the 15th European Conference on Artificial Intelligence*, pp. 680–684, 2002.

[88] E. Kyrimi, M. R. Neves, S. McLachlan, M. Neil, W. Marsh, and N. Fenton, “Medical idioms for clinical Bayesian network development,” *J Biomed Inform*, vol. 108, p. 103495, Aug. 2020, doi: 10.1016/J.JBI.2020.103495.

[89] D. A. Lagnado, N. Fenton, and M. Neil, “Legal idioms: A framework for evidential reasoning,” *Argument and Computation*, vol. 4, no. 1, pp. 46–63, Mar. 2013, doi: 10.1080/19462166.2012.682656.

[90] G. F. Cooper, “A simple constraint-based algorithm for efficiently mining observational databases for causal relationships,” *Data Min Knowl Discov*, vol. 1, no. 2, pp. 203–224, 1997, doi: 10.1023/A:1009787925236.

[91] J. Cheng, D. A. Bell, and W. Liu, “Learning belief networks from data: An information theory based approach,” in *International Conference on Information and Knowledge Management, Proceedings*, 1997, pp. 325–331.

[92] K. B. Korb and A. E. Nicholson, *Bayesian artificial intelligence, second edition*. 2010. doi: 10.1201/b10391.

[93] R. Peter Norvig, “Artificial intelligence—a modern approach by Stuart,” *Cambridge University Press*, 2010.

[94] M. Scutari, C. Elisabeth Graafland, and J. Manuel Gutiérrez MANUELGUTIERREZ, “Who learns better bayesian network structures: Constraint-based, score-based or hybrid algorithms?,” *proceedings.mlr.press*, vol. 72, pp. 416–427, 2018.

[95] N. Fenton, M. Neil, and J. G. Caballero, “Using ranked nodes to model qualitative judgments in bayesian networks,” *IEEE Trans Knowl Data Eng*, vol. 19, no. 10, pp. 1420–1432, Oct. 2007, doi: 10.1109/TKDE.2007.1073.

[96] A. P. Dempster, N. M. Laird, and D. B. Rubin, “Maximum Likelihood from Incomplete Data Via the EM Algorithm,” *Journal of the Royal Statistical Society: Series B (Methodological)*, vol. 39, no. 1, pp. 1–22, Sep. 1977, doi: 10.1111/j.2517-6161.1977.tb01600.x.

[97] C. S. Spetzler and C. A. S. Stael von Holstein, “PROBABILITY ENCODING IN DECISION ANALYSIS.,” *Manage Sci*, vol. 22, no. 3, pp. 340–358, 1975, doi: 10.1287/mnsc.22.3.340.

[98] A. O’Hagan *et al.*, *Uncertain judgements: Eliciting experts’ probabilities*. wiley, 2006. doi: 10.1002/0470033312.

[99] T. G. Martin *et al.*, “Eliciting Expert Knowledge in Conservation Science,” *Conservation Biology*, vol. 26, no. 1. pp. 29–38, Feb. 2012. doi: 10.1111/j.1523-1739.2011.01806.x.

[100] S. L. Lauritzen and D. J. Spiegelhalter, “Local Computations with Probabilities on Graphical Structures and Their Application to Expert Systems,” *Journal of the Royal Statistical Society: Series B (Methodological)*, vol. 50, no. 2, pp. 157–194, Jan. 1988, doi: 10.1111/j.2517-6161.1988.tb01721.x.

[101] T. Richardson and F. V. Jensen, “An Introduction to Bayesian Networks.,” *J Am Stat Assoc*, vol. 92, no. 439, p. 1215, 1997, doi: 10.2307/2965591.

[102] J. H. Kim and J. Pearl, “COMPUTATIONAL MODEL FOR CAUSAL AND DIAGNOSTIC REASONING IN INFERENCE SYSTEMS.,” in *dl.acm.org*, 1983, pp. 190–193.

[103] M. Neil, M. Tailor, and D. Marquez, “Inference in hybrid Bayesian networks using dynamic discretization,” *Stat Comput*, 2007, doi: 10.1007/s11222-007-9018-y.

[104] D. Marquez, M. Neil, and N. Fenton, “Improved reliability modeling using Bayesian networks and dynamic discretization,” *Reliab Eng Syst Saf*, vol. 95, no. 4, pp. 412–425, Apr. 2010, doi: 10.1016/j.ress.2009.11.012.

[105] D. Marquez, M. Neil, and N. E. Fenton, “A new Bayesian Network approach to Reliability modelling,” *5th International Mathematical Methods in Reliability Conference (MMR 07)*. 2007.

[106] A. V. Kozlov and D. Koller, “Nonuniform Dynamic Discretization in Hybrid Networks,” *Uncertainty in Artificial Intelligence (UAI)*, pp. 314–325, Feb. 2013, doi: 10.48550/arxiv.1302.1555.

[107] J. Pearl, “Causal inference in statistics: An overview,” *Stat Surv*, vol. 3, no. September, pp. 96–146, 2009, doi: 10.1214/09-SS057.

[108] J. Pearl, *Probabilistic reasoning in intelligent systems: networks of plausible inference*. 1988.

[109] A. Balke and J. Pearl, “Probabilistic evaluation of counterfactual queries,” *Proceedings of the National Conference on Artificial Intelligence*, vol. 1, pp. 230–237, 1994.

[110] P. Weber, G. Medina-Oliva, C. Simon, and B. Iung, “Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas,” *Eng Appl Artif Intell*, vol. 25, no. 4, pp. 671–682, 2012, doi: 10.1016/j.engappai.2010.06.002.

[111] S. Kabir and Y. Papadopoulos, “Applications of Bayesian networks and Petri nets in safety, reliability, and risk assessments: A review,” *Safety Science*, vol. 115. pp. 154–175, 2019. doi: 10.1016/j.ssci.2019.02.009.

[112] C. J. Lee and K. J. Lee, “Application of Bayesian network to the probabilistic risk assessment of nuclear waste disposal,” *Reliab Eng Syst Saf*, vol. 91, no. 5, pp. 515–532, 2006, doi: 10.1016/j.ress.2005.03.011.

[113] G. Wu, J. Tong, L. Zhang, Y. Zhao, and Z. Duan, “Framework for fault diagnosis with multi-source sensor nodes in nuclear power plants based on a Bayesian network,” *Ann Nucl Energy*, vol. 122, pp. 297–308, Dec. 2018, doi: 10.1016/j.anucene.2018.08.050.

[114] R. K. Ur, M. Zubair, and G. Heo, “Reliability analysis of nuclear I&C architecture using Bayesian networks,” in *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2014*, IEEE Computer Society, 2014, pp. 169–174. doi: 10.1109/IBCAST.2014.6778141.

[115] E. Chojnacki, W. Plumecocq, and L. Audouin, “An expert system based on a Bayesian network for fire safety analysis in nuclear area,” *Fire Saf J*, vol. 105, pp. 28–40, Apr. 2019, doi: 10.1016/j.firesaf.2019.02.007.

[116] D. C. Yu, T. C. Nguyen, and P. Haddawy, “Bayesian network model for reliability assessment of power systems,” *IEEE Transactions on Power Systems*, vol. 14, no. 2, pp. 426–432, 1999, doi: 10.1109/59.761860.

[117] T. Daemi, A. Ebrahimi, and M. Fotuhi-Firuzabad, “Constructing the Bayesian Network for components reliability importance ranking in composite power systems,” *International Journal of Electrical Power and Energy Systems*, vol. 43, no. 1, pp. 474–480, Dec. 2012, doi: 10.1016/j.ijepes.2012.06.010.

[118] Z. Yongli, H. Limin, Z. Liguo, and W. Yan, “Bayesian network based time-simulation for power system reliability assessment,” *7th Mexican International Conference on Artificial Intelligence - Proceedings of the Special Session, MICAI 2008*, pp. 271–277, 2008, doi: 10.1109/MICAI.2008.35.

[119] H. Jie, H. Limin, G. Lirui, Y. Jinliang, and X. Yunfang, “Reliability assessment of power systems based on element time sequential by Bayesian networks,” in *3rd International Conference on Innovative Computing Information and Control, ICICIC’08*, 2008. doi: 10.1109/ICICIC.2008.441.

[120] M. Sýkora, J. Marková, and D. Diamantidis, “Bayesian network application for the risk assessment of existing energy production units,” *Reliab Eng Syst Saf*, vol. 169, pp. 312–320, Jan. 2018, doi: 10.1016/j.ress.2017.09.006.

[121] M. Neil, N. Fenton, S. Forey, and R. Harris, “Using Bayesian belief networks to predict the reliability of military vehicles,” *Computing and Control Engineering Journal*, vol. 12, no. 1, pp. 11–20, 2001, doi: 10.1049/cce:20010103.

[122] M. Banghart, L. Bian, L. Strawderman, and K. Babski-Reeves, “Risk assessment on the EA-6B aircraft utilizing Bayesian networks,” *Qual Eng*, vol. 29, no. 3, pp. 499–511, Jul. 2017, doi: 10.1080/08982112.2017.1319957.

[123] J. Crispim, J. Fernandes, and N. Rego, “Customized risk assessment in military shipbuilding,” *Reliab Eng Syst Saf*, vol. 197, p. 106809, May 2020, doi: 10.1016/j.ress.2020.106809.

[124] L. D. Hudson, B. S. Ware, K. B. Laskey, and S. M. Mahoney, “An application of Bayesian networks to antiterrorism risk management for military planners,” 2005, Accessed: Apr. 06, 2023. [Online]. Available: http://jbox.gmu.edu/handle/1920/268

[125] W. Marsh and G. Bearfield, “Using Bayesian Networks to Model Accident Causation in the UK Railway Industry,” in *Probabilistic Safety Assessment and Management*, 2004, pp. 3597–3602. doi: 10.1007/978-0-85729-410-4_575.

[126] E. Castillo, Z. Grande, and A. Calviño, “Bayesian Networks-Based Probabilistic Safety Analysis for Railway Lines,” *Computer-Aided Civil and Infrastructure Engineering*, vol. 31, no. 9, pp. 681–700, Sep. 2016, doi: 10.1111/mice.12195.

[127] A. Leśniak and F. Janowiec, “Risk assessment of additional works in railway construction investments using the Bayes network,” *Sustainability (Switzerland)*, vol. 11, no. 19, 2019, doi: 10.3390/su11195388.

[128] W. Huang, Y. Zhang, X. Kou, D. Yin, R. Mi, and L. Li, “Railway dangerous goods transportation system risk analysis: An Interpretive Structural Modeling and Bayesian Network combining approach,” *Reliab Eng Syst Saf*, vol. 204, 2020, doi: 10.1016/j.ress.2020.107220.

[129] J. T. Luxhøj and D. W. Coit, “Modeling low probability/high consequence events: An aviation safety risk model,” in *Proceedings - Annual Reliability and Maintainability Symposium*, 2006, pp. 215–221. doi: 10.1109/RAMS.2006.1677377.

[130] F. Netjasov and M. Janic, “A review of research on risk and safety modelling in civil aviation,” *J Air Transp Manag*, vol. 14, no. 4, pp. 213–220, Jul. 2008, doi: 10.1016/j.jairtraman.2008.04.008.

[131] M. Neil, B. Malcolm, and R. Shaw, “Modelling an Air Traffic Control Environment Using Bayesian Belief Networks,” in *21st International System Safety Conference*, 2003, pp. 1689–1699.

[132] A. Washington, R. Clothier, N. Neogi, J. Silva, K. Hayhurst, and B. Williams, “Adoption of a Bayesian Belief Network for the System Safety Assessment of Remotely Piloted Aircraft Systems,” *Saf Sci*, vol. 118, pp. 654–673, Oct. 2019, doi: 10.1016/J.SSCI.2019.04.040.

[133] A. Shih, E. Ancel, … S. J.-C. of the A. S. for, and undefined 2012, “Object-oriented Bayesian networks (OOBN) for aviation accident modeling and technology portfolio impact assessment,” *ntrs.nasa.gov*, Accessed: Apr. 06, 2023. [Online]. Available: https://ntrs.nasa.gov/citations/20120015511

[134] X. Zhang, S. M.-R. E. & S. Safety, and undefined 2021, “Bayesian network modeling of accident investigation reports for aviation safety assessment,” *Elsevier*, Accessed: Apr. 06, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0951832020308607

[135] H. Wang, J. G.-M. P. in Engineering, and undefined 2013, “Bayesian network assessment method for civil aviation safety based on flight delays,” *hindawi.com*, Accessed: Apr. 06, 2023. [Online]. Available: https://www.hindawi.com/journals/mpe/2013/594187/

[136] W. Chen and S. Huang, “Human reliability analysis for visual inspection in aviation maintenance by a Bayesian network approach,” *Transportation Research Record*, vol. 2449. SAGE PublicationsSage CA: Los Angeles, CA, pp. 105–113, Jan. 01, 2014. doi: 10.3141/2449-12.

[137] B. J. M. Ale *et al.*, “Further development of a Causal model for Air Transport Safety (CATS): Building the mathematical heart,” *Reliab Eng Syst Saf*, vol. 94, no. 9, pp. 1433–1441, Sep. 2009, doi: 10.1016/j.ress.2009.02.024.

[138] M. Hänninen and P. Kujala, “Influences of variables on ship collision probability in a Bayesian belief network model,” *Reliab Eng Syst Saf*, vol. 102, pp. 27–40, Jun. 2012, doi: 10.1016/j.ress.2012.02.008.

[139] S. Fan, E. Blanco-Davis, Z. Yang, J. Zhang, and X. Yan, “Incorporation of human factors into maritime accident analysis using a data-driven Bayesian network,” *Reliab Eng Syst Saf*, vol. 203, p. 107070, Nov. 2020, doi: 10.1016/j.ress.2020.107070.

[140] P. Trucco, E. Cagno, F. Ruggeri, and O. Grande, “A Bayesian Belief Network modelling of organisational factors in risk analysis: A case study in maritime transportation,” *Reliab Eng Syst Saf*, vol. 93, no. 6, pp. 845–856, Jun. 2008, doi: 10.1016/J.RESS.2007.03.035.

[141] J. Montewka, S. Ehlers, F. Goerlandt, T. Hinz, K. Tabri, and P. Kujala, “A framework for risk assessment for maritime transportation systems—A case study for open sea collisions involving RoPax vessels,” *Reliab Eng Syst Saf*, vol. 124, pp. 142–157, Apr. 2014, doi: 10.1016/J.RESS.2013.11.014.

[142] G. Zhang and V. V. Thai, “Expert elicitation and Bayesian Network modeling for shipping accidents: A literature review,” *Saf Sci*, vol. 87, pp. 53–62, Aug. 2016, doi: 10.1016/J.SSCI.2016.03.019.

[143] T. Haddad, A. Himes, and M. Campbell, “Fracture prediction of cardiac lead medical devices using Bayesian networks,” *Reliab Eng Syst Saf*, vol. 123, pp. 145–157, Mar. 2014, doi: 10.1016/j.ress.2013.11.005.

[144] L. A. Medina, M. Jankovic, G. E. Okudan Kremer, and B. Yannou, “An investigation of critical factors in medical device development through Bayesian networks,” *Expert Syst Appl*, vol. 40, no. 17, pp. 7034–7045, Dec. 2013, doi: 10.1016/j.eswa.2013.06.014.

[145] H. Zhang, J. Liu, and R. Li, “Fault Detection for Medical Body Sensor Networks under Bayesian Network Model,” in *Proceedings - 11th International Conference on Mobile Ad-Hoc and Sensor Networks, MSN 2015*, Institute of Electrical and Electronics Engineers Inc., Feb. 2016, pp. 37–42. doi: 10.1109/MSN.2015.21.

[146] K. R. Rieger and M. Rahimi, “Bayesian risk identification model (BRIM): A predictive model to reduce use error risk in medical device interface design,” in *Proceedings of the Human Factors and Ergonomics Society*, SAGE

PublicationsSage CA: Los Angeles, CA, Sep. 2011, pp. 798–802. doi: 10.1177/1071181311551165.

[147] M. Li, Z. Liu, X. Li, and Y. Liu, “Dynamic risk assessment in healthcare based on Bayesian approach,” *Reliab Eng Syst Saf*, vol. 189, pp. 327–334, Sep. 2019, doi: 10.1016/j.ress.2019.04.040.

[148] E. Kyrimi, S. McLachlan, K. Dube, M. R. Neves, A. Fahmi, and N. Fenton, “A comprehensive scoping review of Bayesian networks in healthcare: Past, present and future,” *Artif Intell Med*, vol. 117, p. 102108, Jul. 2021, doi: 10.1016/j.artmed.2021.102108.

[149] P. J. F. Lucas, L. C. Van Der Gaag, and A. Abu-Hanna, “Bayesian networks in biomedicine and health-care,” *Artificial Intelligence in Medicine*, vol. 30, no. 3. Elsevier, pp. 201–214, Mar. 01, 2004. doi: 10.1016/j.artmed.2003.11.001.

[150] S. McLachlan, K. Dube, G. A. Hitman, N. E. Fenton, and E. Kyrimi, “Bayesian networks in healthcare: Distribution by medical condition,” *Artif Intell Med*, vol. 107, p. 101912, Jul. 2020, doi: 10.1016/j.artmed.2020.101912.

[151] N. Fenton *et al.*, “Predicting software defects in varying development lifecycles using Bayesian nets,” *Inf Softw Technol*, vol. 49, no. 1, pp. 32–43, Jan. 2007, doi: 10.1016/j.infsof.2006.09.001.

[152] N. Fenton, P. Krause, and M. Neil, “Software measurement: Uncertainty and causal modeling,” *IEEE Softw*, vol. 19, no. 4, pp. 116–122, Jul. 2002, doi: 10.1109/MS.2002.1020298.

[153] N. E. Fenton and M. Neil, “A critique of software defect prediction models,” *IEEE Transactions on Software Engineering*, vol. 25, no. 5, pp. 675–689, Sep. 1999, doi: 10.1109/32.815326.

[154] M. Neil, P. Krause, and N. Fenton, “Software Quality Prediction Using Bayesian Networks,” in *Software Engineering with Computational Intelligence*, Springer, Boston, MA, 2003, pp. 136–172. doi: 10.1007/978-1-4615-0429-0_6.

[155] D. Koller and A. Pfeffer, “Object-Oriented Bayesian Networks,” *Proceedings of the Thirteenth Conference on Uncertainty in Artificial Intelligence*, 2013.

[156] A. Helminen and U. Pulkkinen, “Reliability assessment using Bayesian networks. Case study on quantative reliability estimation of a software-based motor protection relay,” 2003, Accessed: Apr. 06, 2023. [Online]. Available: https://inis.iaea.org/search/search.aspx?orig_q=RN:34068263

[157] B. A. Gran and A. Helminen, “A Bayesian belief network for reliability assessment,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2187, pp. 35–45, 2001, doi: 10.1007/3-540-45416-0_4.

[158] C. G. Bai, “Bayesian network based software reliability prediction with an operational profile,” *Journal of Systems and Software*, vol. 77, no. 2, pp. 103–112, Aug. 2005, doi: 10.1016/j.jss.2004.11.034.

[159] R. Roshandel, N. Medvidovic, and L. Golubchik, “A bayesian model for predicting reliability of software systems at the architectural level,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer, Berlin, Heidelberg, 2007, pp. 108–126. doi: 10.1007/978-3-540-77619-2_7.

[160] J. Suh, “Development of a Product Risk Assessment System using Injury Information in Korea Consumer Agency,” *Journal of Digital Convergence*, vol. 15, no. 4, pp. 181–190, 2017, doi: 10.14400/jdc.2017.15.4.181.

[161] P. Berchialla, C. Scarinzi, S. Snidero, and D. Gregori, “Adaptive Bayesian Networks for quantitative risk assessment of foreign body injuries in children,” *J Risk Res*, vol. 13, no. 3, pp. 367–377, 2010, doi: 10.1080/13658810903233419.

[162] P. Berchialla *et al.*, “Comparing models for quantitative risk assessment: An application to the European Registry of foreign body injuries in children,” *Stat Methods Med Res*, vol. 25, no. 4, pp. 1244–1259, 2016, doi: 10.1177/0962280213476167.

[163] M. Abimbola, F. Khan, N. Khakzad, and S. Butt, “Safety and risk analysis of managed pressure drilling operation using Bayesian network,” *Saf Sci*, vol. 76, pp. 133–144, Jul. 2015, doi: 10.1016/J.SSCI.2015.01.010.

[164] E. Castillo, C. Solares, and P. Gómez, “Tail uncertainty analysis in complex systems,” *Artif Intell*, vol. 96, no. 2, pp. 395–419, 1997, doi: 10.1016/S0004-3702(97)00052-0.

[165] M. Abimbola, F. Khan, N. Khakzad, and S. Butt, “Safety and risk analysis of managed pressure drilling operation using Bayesian network,” *Saf Sci*, vol. 76, no. 3, pp. 133–144, Jan. 2015, doi: 10.1016/j.ssci.2015.01.010.

[166] N. Khakzad, F. Khan, and P. Amyotte, “Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network,” *Process Safety and Environmental Protection*, vol. 91, no. 1–2, pp. 46–53, Jan. 2013, doi: 10.1016/j.psep.2012.01.005.

[167] European Commission, “Safety Gate for dangerous non-food products - A12/1765/12 Hammer.” https://ec.europa.eu/safety-gate-alerts/screen/webReport/alertDetail/51938?origin=PDF (accessed Dec. 01, 2022).

[168] European Commission, “Safety Gate for dangerous non-food products - A12/1733/12 Engine.” https://ec.europa.eu/safety-gate-alerts/screen/webReport/alertDetail/51527?origin=PDF (accessed Dec. 01, 2022).

[169] European Commission, “Safety Gate for dangerous non-food products.” https://ec.europa.eu/safety-gate-alerts/screen/webReport#recentAlerts (accessed Dec. 01, 2022).

[170] WHO, “Medical devices,” 2023. https://www.who.int/health-topics/medical-devices#tab=tab_1 (accessed Jan. 25, 2023).

[171] FDA, “Physio-Control Launches Voluntary Field Action for LIFEPAK 1000 Defibrillator | FDA,” 2018. https://www.fda.gov/safety/recalls-market-withdrawals-safety-alerts/physio-control-launches-voluntary-field-action-lifepak-1000-defibrillator (accessed Aug. 24, 2022).

[172] IEC, *IEC 60601-1-11:2015 - Medical electrical equipment — Part 1-11: General requirements for basic safety and essential performance*. 2015.

[173] MHRA, “Single-use Medical Devices : Implications and Consequences of Reuse,” vol. V2.4, 2021.

[174] FDA, “What are Reusable Medical Devices?,” 2018. https://www.fda.gov/medical-devices/reprocessing-reusable-medical-devices/what-are-reusable-medical-devices (accessed Jul. 06, 2021).

[175] IMDRF, “International Medical Device Regulators Forum. Software as a Medical Device (SaMD): Key Definitions,” 2013.

[176] IEC, *IEC 62366-1:2015 Medical devices — Part 1: Application of usability engineering to medical devices*. 2015.

[177] J. A. Zijlstra, L. E. Bekkers, M. Hulleman, S. G. Beesems, and R. W. Koster, “Automated external defibrillator and operator performance in out-of-hospital cardiac arrest,” *Resuscitation*, vol. 118, pp. 140–146, Sep. 2017, doi: 10.1016/J.RESUSCITATION.2017.05.017.

[178] FDA, “Class 1 Device Recall LIFEPAK 1000 defibrillator,” 2017. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfres/res.cfm?id=152589 (accessed Aug. 24, 2022).

[179] RPA, “Establishing a Comparative Inventory of Approaches and Methods Used by Enforcement Authorities for the Assessment of the Safety of Consumer Products Covered by Directive 2001/95/EC on General Product Safety and Identification of Best Practices,” 2006. [Online]. Available: https://rpaltd.co.uk/uploads/report_files/j497-consumer-products.pdf

[180] PROSAFE, *Best Practice Techniques in Market Surveillance*. 2013. [Online]. Available: https://www.prosafe.org/index.php/best-practice/item/best-practices-techniques-in-market-surveillance

[181] I. Maglogiannis, E. Zafiropoulos, A. Platis, and C. Lambrinoudakis, “Risk analysis of a patient monitoring system using Bayesian Network modeling,” *J Biomed Inform*, vol. 39, no. 6, pp. 637–647, Dec. 2006, doi: 10.1016/j.jbi.2005.10.003.

[182] K. Masmoudi, L. Abid, and A. Masmoudi, “Credit risk modeling using Bayesian network with a latent variable,” *Expert Syst Appl*, 2019, doi: 10.1016/j.eswa.2019.03.014.

[183] J. É. G. Torres-Toledano and L. E. Sucar, “Bayesian networks for reliability analysis of complex systems,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 1484, pp. 195–206, 1998, doi: 10.1007/3-540-49795-1_17.

[184] R. Welch and T. Thelen, “Dynamic reliability analysis in an operational context: the Bayesian network perspective.,” *Dynamic reliability: future directions.*, 2000.

[185] ISO/IEC, *Safety aspects — Guidelines for their inclusion in standards*. 2014.

[186] A. H. Briggs, M. C. Weinstein, E. A. L. Fenwick, J. Karnon, M. J. Sculpher, and A. D. Paltiel, “Model parameter estimation and uncertainty: A report of the ISPOR-SMDM modeling good research practices task force-6,” *Value in Health*, vol. 15, no. 6, pp. 835–842, 2012, doi: 10.1016/j.jval.2012.04.014.

[187] Which.co.uk, “Whirlpool announces recall of up to 519,000 Hotpoint and Indesit fire-risk washing machines in the UK,” 2019. https://www.which.co.uk/news/2019/12/whirlpool-announces-recall-of-up-to-519000-indesit-and-hotpoint-fire-risk-washing-machines-in-the-uk/ - Which?

[188] European Commission, “Safety Gate for dangerous non-food products,” 2021. https://ec.europa.eu/safety-gate-alerts/screen/webReport (accessed Apr. 20, 2021).

[189] J. M. Gutteling and O. Wiegman, “Gender-specific reactions to environmental hazards in the Netherlands,” *Sex Roles*, vol. 28, no. 7–8, pp. 433–447, Apr. 1993, doi: 10.1007/BF00289606.

[190] D. M. DeJoy, “An examination of gender differences in traffic accident risk perception,” *Accid Anal Prev*, vol. 24, no. 3, pp. 237–246, Jun. 1992, doi: 10.1016/0001-4575(92)90003-2.

[191] P. Slovic, J. H. Flynn, and M. Layman, “Perceived risk, trust, and the politics of nuclear waste,” *Science (1979)*, vol. 254, no. 5038, pp. 1603–1607, Dec. 1991, doi: 10.1126/science.254.5038.1603.

[192] J. Flynn, P. Slovic, and C. K. Mertz, “Gender, Race, and Perception of Environmental Health Risks,” *Risk Analysis*, vol. 14, no. 6, pp. 1101–1108, Dec. 1994, doi: 10.1111/J.1539-6924.1994.TB00082.X.

[193] A. R. H. Fischer, “Perception of product risks,” in *Consumer Perception of Product Risks and Benefits*, Springer International Publishing, 2017, pp. 175–190. doi: 10.1007/978-3-319-50530-5_9.

[194] L. J. Frewer, “The public and effective risk communication,” in *Toxicology Letters*, Elsevier, Apr. 2004, pp. 391–397. doi: 10.1016/j.toxlet.2003.12.049.

[195] L. J. Frewer, J. Scholderer, and L. Bredahl, “Communicating about the Risks and Benefits of Genetically Modified Foods: The Mediating Role of Trust,” *Risk Analysis*, vol. 23, no. 6, pp. 1117–1133, Dec. 2003, doi: 10.1111/j.0272-4332.2003.00385.x.

[196] S. A. Rijsdijk and E. J. Hultink, “How Today’s Consumers Perceive Tomorrow’s Smart Products*,” *Journal of Product Innovation Management*, vol. 26, no. 1, pp. 24–42, Jan. 2009, doi: 10.1111/J.1540-5885.2009.00332.X.

[197] M. Abramovici, J. C. Göbel, and P. Savarino, “Virtual twins as integrative components of smart products,” in *IFIP Advances in Information and Communication Technology*, Springer, Cham, 2016, pp. 217–226. doi: 10.1007/978-3-319-54660-5_20.

[198] C. Pardo, B. S. Ivens, and M. Pagani, “Are products striking back? The rise of smart products in business markets,” *Industrial Marketing Management*, vol. 90, pp. 205–220, Oct. 2020, doi: 10.1016/j.indmarman.2020.06.011.

[199] L. Püschel, M. Röglinger, and H. Schlott, “What’s in a Smart Thing? Development of a Multi-Layer Taxonomy,” in *2016 International Conference on Information Systems, ICIS 2016*, 2016.

[200] K. P. Vaubel and S. L. Young, “Components of perceived risk for consumer products,” in *Proceedings of the Human Factors Society*, Publ by Human Factors Soc Inc, 1992, pp. 494–498. doi: 10.1177/154193129203600505.

[201] P. Slovic, B. Fischhoff, and S. Lichtenstein, “RATING THE RISKS.,” Springer, Boston, MA, 1981, pp. 193–217. doi: 10.1007/978-1-4899-2168-0_17.

[202] A. R. H. Fischer, J. C. M. van Trijp, D. J. B. Hofenk, A. Ronteltap, and A. A. Tudoran, “Collation of Scientific Evidence on Consumer Acceptance of New Food Technologies: Three roads to consumer choice.” 2012.

[203] M. Siegrist, N. Stampfli, H. Kastenholz, and C. Keller, “Perceived risks and perceived benefits of different nanotechnology foods and nanotechnology food packaging,” *Appetite*, vol. 51, no. 2, pp. 283–290, Sep. 2008, doi: 10.1016/j.appet.2008.02.020.

[204] S. A. Rijsdijk and E. J. Hultink, “‘Honey, have you seen our hamster?’ Consumer evaluations of autonomous domestic products,” in *Journal of Product Innovation Management*, John Wiley & Sons, Ltd, May 2003, pp. 204–216. doi: 10.1111/1540-5885.2003003.

[205] K. G. Grunert, “Current issues in the understanding of consumer food choice,” in *Trends in Food Science and Technology*, Elsevier, Aug. 2002, pp. 275–285. doi: 10.1016/S0924-2244(02)00137-1.

[206] E. Van Kleef, A. R. H. Fischer, M. Khan, and L. J. Frewer, “Risk and Benefit Perceptions of Mobile Phone and Base Station Technology in Bangladesh,” *Risk Analysis*, vol. 30, no. 6, pp. 1002–1015, Apr. 2010, doi: 10.1111/j.1539-6924.2010.01386.x.

[207] P. Slovic, “Perceptions of Risk: Reflections on the Psychometric Paradigm,” 1990.

[208] T. Stobierski, “Willingness To Pay: What It Is & How To Calculate,” *Harvard Business School Business Insights Blog*, 2020. https://online.hbs.edu/blog/post/willingness-to-pay (accessed Nov. 16, 2022).

[209] R. Sukharomana and R. J. Supalla, “Effect of risk perception on willingness to pay for improved water quality,” vol. 80, no. 5, p. 1206, 1998.

[210] L. Savage, “An empirical investigation into the effect of psychological perceptions on the willingness-to-pay to reduce risk,” *J Risk Uncertain*, vol. 6, no. 1, pp. 75–90, 1993, doi: 10.1007/BF01065351.

[211] W. Moon and S. K. Balasubramanian, “Public Perceptions and Willingness to Pay a Premium for Non-GM foods in the US and UK,” *AgBioforum*, vol. 4, no. 3, pp. 221–231, 2001.

[212] A. Wåhlberg and L. Sjöberg, “Risk perception and the media,” *J Risk Res*, vol. 3, no. 1, pp. 31–50, 2000, doi: 10.1080/136698700376699.

[213] D. Koné and E. Mullet, “Societal Risk Perception and Media Coverage,” *Risk Analysis*, vol. 14, no. 1, pp. 21–24, 1994, doi: 10.1111/j.1539-6924.1994.tb00024.x.

[214] C. F. Keown, “Risk Perceptions of Hong Kongese vs. Americans,” *Risk Analysis*, vol. 9, no. 3, pp. 401–405, 1989, doi: 10.1111/j.1539-6924.1989.tb01005.x.

[215] M. G. Morgan *et al.*, “Powerline Frequency Electric and Magnetic Fields: A Pilot Study of Risk Perception,” *Risk Analysis*, vol. 5, no. 2, pp. 139–149, Jun. 1985, doi: 10.1111/j.1539-6924.1985.tb00161.x.

[216] A. Mazur and J. Lee, “Sounding the Global Alarm: Environmental Issues in the US National News,” *Soc Stud Sci*, vol. 23, no. 4, pp. 681–720, 1993, doi: 10.1177/030631293023004003.

[217] S. A. Rijsdijk and E. J. Hultink, “The impact of product smartness on consumer satisfaction through product advantage, compatibility, and complexity,” in *Proceedings of the 13th PDMA Research Conference, Orlando*, 2002.

[218] B. Fischhoff, P. Slovic, S. Lichtenstein, S. Read, and B. Combs, “How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits,” *Policy Sci*, vol. 9, no. 2, pp. 127–152, Apr. 1978, doi: 10.1007/BF00143739.

[219] A. Mazur, “Nuclear power, chemical hazards, and the quantity of reporting,” *Minerva*, vol. 28, no. 3, pp. 294–323, Sep. 1990, doi: 10.1007/BF01096293.

[220] A. Mazur, “Media Coverage and Public Opinion on Scientific Controversies,” *Journal of Communication*, vol. 31, no. 2, pp. 106–115, Jun. 1981, doi: 10.1111/j.1460-2466.1981.tb01234.x.

[221] O. Wiegman and J. M. Gutteling, “Risk Appraisal and Risk Communication: Some Empirical Data From The Netherlands Reviewed,” *Basic Appl Soc Psych*, vol. 16, no. 1–2, pp. 227–249, Feb. 1995, doi: 10.1080/01973533.1995.9646111.

[222] D. J. Davidson and W. R. Freudenburg, “Gender and environmental risk concerns: a review and analysis of available research,” *Environ Behav*, vol. 28, no. 3, pp. 302–339, Jul. 1996, doi: 10.1177/0013916596283003.

[223] R. P. Barke, H. Jenkins-Smith, and P. Slovic, “Risk perceptions of men and women scientists.,” *Social Science Quarterly*, vol. 78, no. 1. pp. 167–176, 1997.

[224] M. R. Greenberg and D. F. Schneider, “Gender Differences in Risk Perception: Effects Differ in Stressed vs. Non-Stressed Environments,” *Risk Analysis*, vol. 15, no. 4, pp. 503–511, Aug. 1995, doi: 10.1111/j.1539-6924.1995.tb00343.x.

[225] O. Hellesøy, K. Grønhaug, and O. Kvitastein, “Profiling the high hazards perceivers: An exploratory study,” *Risk Analysis*, vol. 18, no. 3, pp. 253–259, Jun. 1998, doi: 10.1111/j.1539-6924.1998.tb01292.x.

[226] J. Hitchcock, “Gender Differences in Risk Perception: Broadening the Contexts,” *RISK: Health, Safety & Environment (1990-2002)*, vol. 12, no. 3, p. 4, 2001.

[227] L. Sjöberg, “Worry and risk perception,” *Risk Analysis*, vol. 18, no. 1, pp. 85–93, Feb. 1998, doi: 10.1111/j.1539-6924.1998.tb00918.x.

[228] L. Sjöberg and B. M. Drottz-Sjöberg, “Public risk perception of nuclear waste,” *Int J Risk Assess Manag*, vol. 11, no. 3–4, pp. 264–296, 2009, doi: 10.1504/ijram.2009.023156.

[229] K. T. Fox-Glassman and E. U. Weber, “What makes risk acceptable? Revisiting the 1978 psychological dimensions of perceptions of technological risks,” *J Math Psychol*, vol. 75, pp. 157–169, 2016, doi: 10.1016/j.jmp.2016.05.003.

[230] D. C. Zhang, S. Highhouse, and C. D. Nye, “Development and validation of the General Risk Propensity Scale (GRiPS),” *J Behav Decis Mak*, vol. 32, no. 2, pp. 152–167, Apr. 2019, doi: 10.1002/bdm.2102.

[231] D. M. Kahan, D. Braman, P. Slovic, J. Gastil, and G. Cohen, “Cultural cognition of the risks and benefits of nanotechnology,” *Nat Nanotechnol*, vol. 4, no. 2, pp. 87–90, Dec. 2009, doi: 10.1038/nnano.2008.341.

[232] M. C. Nisbet and C. Mooney, “Framing Science,” *Science (1979)*, vol. 316, no. 5821, pp. 56–56, 2007, doi: 10.1126/science.1142030.

[233] C. W. Trumbo and K. A. McComas, “The function of credibility in information processing for risk perception,” *Risk Analysis*, vol. 23, no. 2, pp. 343–353, Apr. 2003, doi: 10.1111/1539-6924.00313.

[234] L. J. Frewer, C. Howard, D. Hedderley, and R. Shepherd, “What determines trust in information about food-related risks? Underlying psychological constructs,” *Risk Anal*, vol. 16, no. 4, pp. 473–486, 1996, doi: 10.1111/J.1539-6924.1996.TB01094.X.

[235] Hugin, “Hugin - Bayes Net Software,” 2023. https://www.hugin.com/ (accessed Mar. 04, 2023).

[236] Norsys, “Netica - Bayes Net Software,” 2023, Accessed: Mar. 04, 2023. [Online]. Available: https://www.norsys.com/

[237] M. Neil, M. Tailor, and D. Marquez, “Inference in Hybrid Bayesian Networks using dynamic discretisation,” *researchgate.net*, vol. 17, no. 3, pp. 219–233, Sep. 2007, doi: 10.1007/s11222-007-9018-y.

[238] OPSS, “Product Safety Risk Assessment Methodology (PRISM) - GOV.UK,” Dec. 2022. https://www.gov.uk/guidance/product-safety-risk-assessment-methodology-prism (accessed Mar. 15, 2023).

[239] The Health and Safety Executive, “Risk management: Expert guidance - Cost Benefit Analysis (CBA) checklist,” *HSE Guidance*. 2020. Accessed: Aug. 07, 2023. [Online]. Available: https://www.hse.gov.uk/enforce/expert/alarpcheck.htm

[240] The Health and Safety Executive, “Risk management: Expert guidance - HSE principles for Cost Benefit Analysis in support of ALARP,” 2021. https://www.hse.gov.uk/enforce/expert/alarpcba.htm (accessed Aug. 07, 2023).

[241] Health and Safety Executive, “Risk management: Expert guidance - ALARP at a glance,” *hse.gov.uk*, 2022. https://www.hse.gov.uk/enforce/expert/alarpglance.htm (accessed Aug. 07, 2023).

[242] The Health and Safety Executive, “Risk management: Expert guidance - Principles and guidelines to assist HSE.” 2021. Accessed: Aug. 07, 2023. [Online]. Available: https://www.hse.gov.uk/enforce/expert/alarp1.htm#P130_16948

[243] P. Junietz, U. Steininger, and H. Winner, “Macroscopic Safety Requirements for Highly Automated Driving,” *https://doi.org/10.1177/0361198119827910*, vol. 2673, no. 3, pp. 1–10, Feb. 2019, doi: 10.1177/0361198119827910.

[244] W. M. Lim, A. Gunasekara, J. L. Pallant, J. I. Pallant, and E. Pechenkina, “Generative AI and the future of education: Ragnarök or reformation? A paradoxical perspective from management educators,” *The International Journal of Management Education*, vol. 21, no. 2, p. 100790, Jul. 2023, doi: 10.1016/J.IJME.2023.100790.

[245] OpenAI, “DALL·E 2,” 2023. https://openai.com/product/dall-e-2 (accessed Mar. 16, 2023).

[246] OpenAI, “Introducing ChatGPT,” 2023. https://openai.com/blog/chatgpt (accessed Mar. 16, 2023).

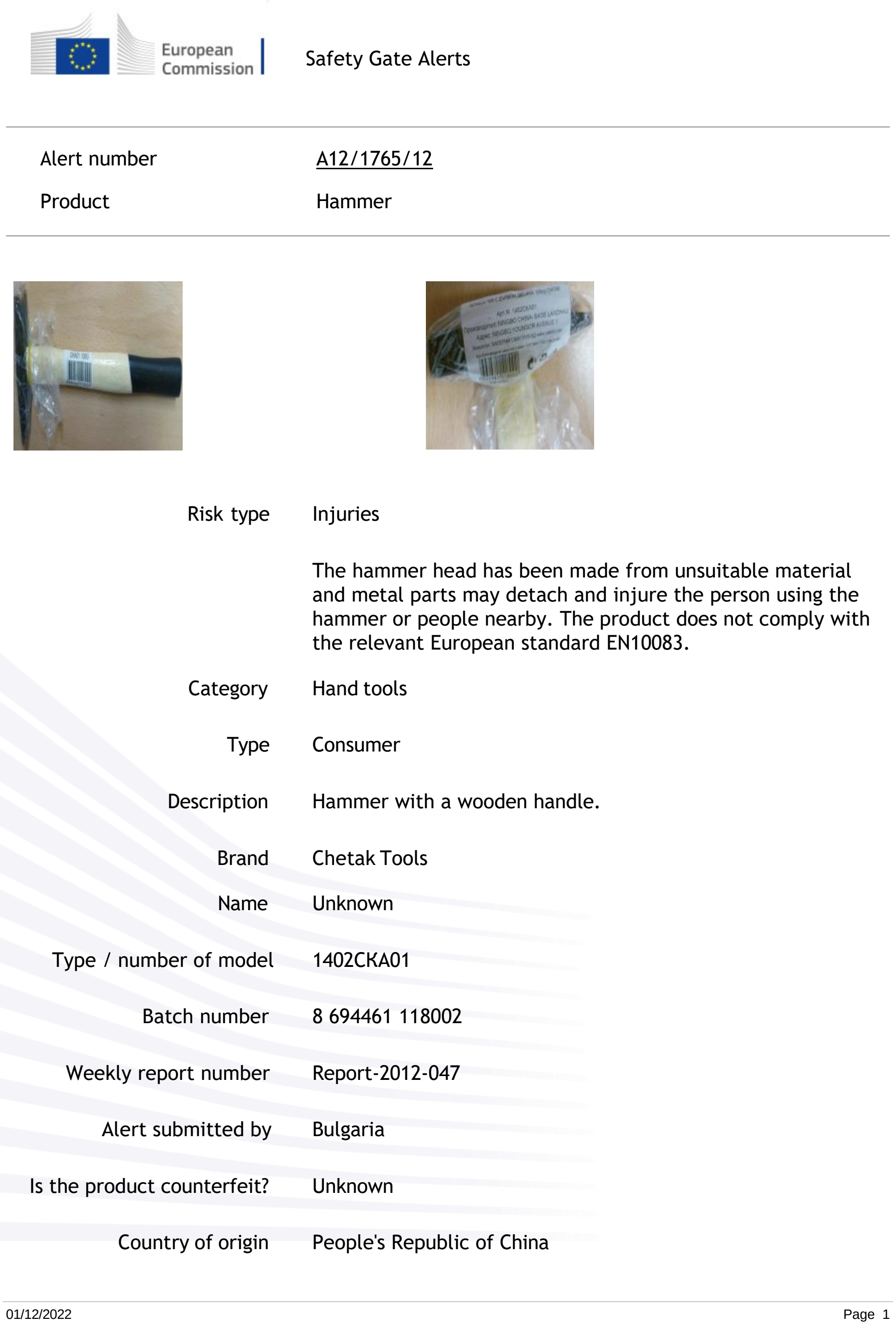
[247] R Core Team, “The R Project for Statistical Computing,” 2022. https://www.r-project.org/ (accessed Aug. 17, 2022).

[248] P. C. Bürkner, “brms: An R package for Bayesian multilevel models using Stan,” *J Stat Softw*, vol. 80, 2017, doi: 10.18637/jss.v080.i01.

Appendix A Chapter 6 Supplemental Material

This section of the Appendix presents the safety risk reports for the hammer and car engine examples discussed in Chapter 6.

Hammer Risk Report [167]



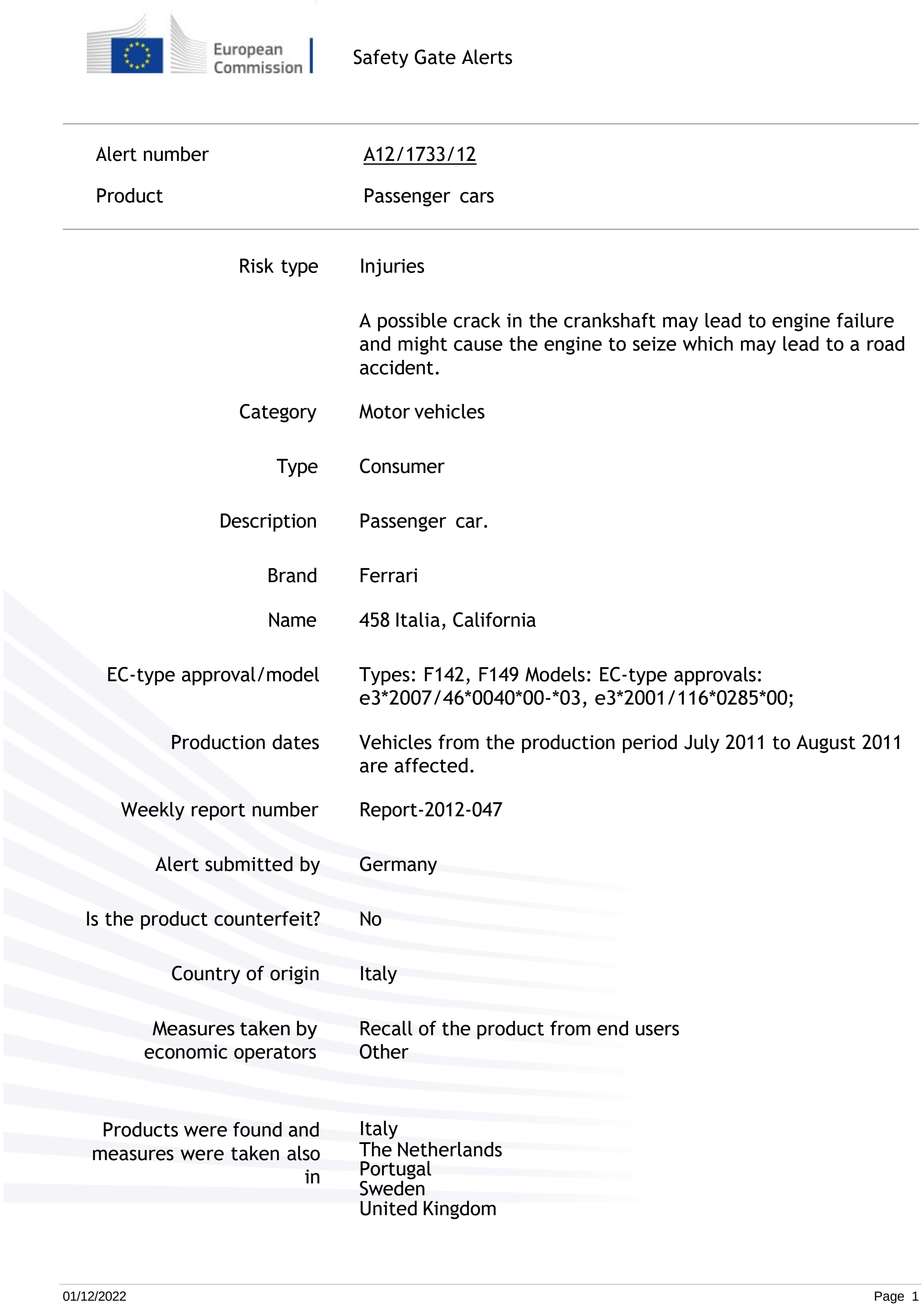
European Commission | Safety Gate Alerts

Alert number	A12/1765/12
Product	Hammer

Risk type	Injuries
	The hammer head has been made from unsuitable material and metal parts may detach and injure the person using the hammer or people nearby. The product does not comply with the relevant European standard EN10083.
Category	Hand tools
Type	Consumer
Description	Hammer with a wooden handle.
Brand	Chetak Tools
Name	Unknown
Type / number of model	1402CKA01
Batch number	8 694461 118002
Weekly report number	Report-2012-047
Alert submitted by	Bulgaria
Is the product counterfeit?	Unknown
Country of origin	People's Republic of China

01/12/2022 Page 1

Car Engine Risk Report [168]



Safety Gate Alerts

Alert number	A12/1733/12
Product	Passenger cars
Risk type	Injuries A possible crack in the crankshaft may lead to engine failure and might cause the engine to seize which may lead to a road accident.
Category	Motor vehicles
Type	Consumer
Description	Passenger car.
Brand	Ferrari
Name	458 Italia, California
EC-type approval/model	Types: F142, F149 Models: EC-type approvals: e3*2007/46*0040*00-*03, e3*2001/116*0285*00;
Production dates	Vehicles from the production period July 2011 to August 2011 are affected.
Weekly report number	Report-2012-047
Alert submitted by	Germany
Is the product counterfeit?	No
Country of origin	Italy
Measures taken by economic operators	Recall of the product from end users Other
Products were found and measures were taken also in	Italy The Netherlands Portugal Sweden United Kingdom

01/12/2022 Page 1

Appendix B Chapter 7 Supplemental Material

B1 Classes of Medical Devices

This section of Appendix B presents the different categories and classes of medical devices.

Table B1 Categories of medical devices by purpose

Category	**Definition**	**Example**
Non-invasive	Devices which do not enter the body	Wheelchairs
Invasive	Devices inserted into the body's orifices	Examination gloves
Surgically invasive	Devices used or inserted in surgery	Needles
Active	Devices requiring an external source of power	ultrasound
Implantable	Devices implanted into the body	Breast implants

Table B2 Classes of medical devices by inherent risk

Class	**Inherent Risk Level**	**Example**
Class I	Low	Wheelchairs
Class II	Medium	Dental fillings
Class III	High	Pacemakers

B2 Model Variables and NPT

This section of Appendix B presents the variables and NPTs used in the BN for medical device risk management.

Table B3. Variables and NPTs for Medical Device Risk Management BN

Variable /Name	**Abbrev**	**Node Probability Tables (NPT)**	**Category**
Number of demands (test)	nd	Uniform (0, 1000000)	Reliability
Number of observed hazards (test)	no	Binomial (nd, phd)	Reliability
Prob. of hazard per demand (test)	phd	Uniform (0, 1)	Reliability

Current or previous device?	device	States: (Current device: 0.985, Previous device similar: 0.005, Previous device Minor Difference:0.005, Previous device Major Difference: 0.005)	Reliability
Prob. hazard per demand given device	phd_device	Partitioned Expression (Current device: phd, Previous device similar: phd, Previous device Minor Difference: phd×1.25, Previous device Major Difference: phd×2)	Reliability
Generic or Test Data?	genswitch	States: (Testing: 0.99, Generic: 0.01)	Reliability
Generic prob. levels	levels	States: (Frequent: 0.2, Probable: 0.2, Occasional: 0.2, Remote: 0.2, Improbable: 0.2)	Reliability
Generic prob. hazard per demand	genprob	Partitioned Expression (Frequent: Uniform (0.001, 1), Probable: Uniform (1E-4, 0.99E-3), Occasional: Uniform (1E-5, 0.99E-4), Remote: Uniform (1E-6, 0.99E-5), Improbable: Uniform (0, 0.99E-6))	Reliability
Prob. of hazard per demand (generic or test)	phdtest	Partitioned Expression (Testing: phd_device, Generic: genprob)	Reliability
Prob. of hazard given testing strategy	phd_ts	Partitioned Expression (Less strenuous: (phd_test+0.5×phd_test), Typical of normal use: (phd_ts), More strenuous: (phd_ts−0.5×phd_test))	Reliability
Test strategy	ts	States: (Less strenuous: 0.333, Typical of normal use: 0.333, More strenuous: 0.333)	Reliability, Requirement
Testing requirement met	treq	IF(dreq >= phd_ts,"True","False")	Requirement
Defined safety requirement by standards	dreq	Uniform(0,1)	Requirement
Intended use requirement	ureq	IF(dreq >= phd_df,"True","False")	Requirement
Prob. of hazard per demand given process information	phd_pc	Partitioned Expression (Yes: (Low: (phd_ts×1.1), Normal: (phd_ts, high:phd_ts×0.9)), No: (phd_ts)	Reliability
Years in operation	yo	Ranked: (<1 year: 0.2, 1-5 years: 0.2, 5-10 years: 0.2, 10-20 years: 0.2, 20+ years: 0.2)	Manufacturer Process Quality
Manufacturer reputation	mr	Ranked: (Highly reputable: 0.333, Reputable: 0.333, Disreputable: 0.333)	Manufacturer Process Quality
Customer satisfaction	cs	TNormal (oq, 0.05, 0, 1)	Manufacturer Process Quality
Organisation quality	oq	TNormal (wmean(1, yo, 1, mr), 0.001, 0, 1)	Manufacturer Process Quality
Process quality	pq	TNormal (pdri, 0.005, 0, 1)	Manufacturer Process Quality
Product defects	pdef	TNormal (pq, 0.05, 0, 1)	Manufacturer Process Quality

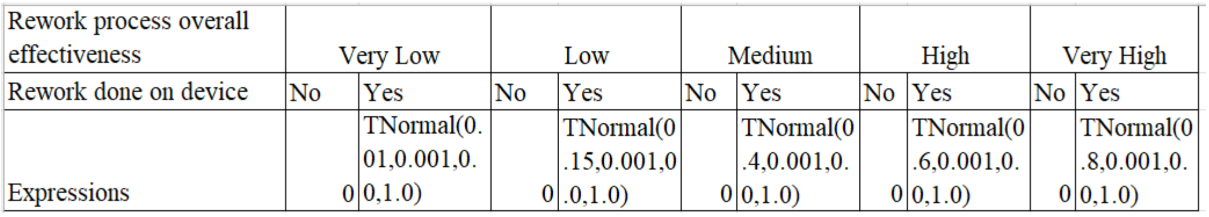
Process drifts	pdri	Ranked: (Major: 0.333, Minor: 0.333, None: 0.333)	Manufacturer Process Quality
Process additives	padd	TNormal (pq ,0.05, 0, 1)	Manufacturer Process Quality
Organisation and Process Quality	org_pro	TNormal (wmean (1, oq, 2, pq), 0.001, 0, 1)	Manufacturer Process Quality, Reliability
Manufacturer information available?	man_info	States: (Yes: 1E-4, No: 0.9999)	Manufacturer Process Quality, Reliability
Rework effort	re	States: (Very high: 0.2, High: 0.2, Medium: 0.2, Low: 0.2, Very low: 0.2)	Rework
Rework process quality	rpq	Ranked: (Very high: 0.2, High: 0.2, Medium: 0.2, Low: 0.2, Very low: 0.2)	Rework
Rework process overall effectiveness	rpo	TNormal (wmean(1, re, 1, rpq), 0.001, 0, 1)	Rework
Rework done on device	rd	States: (Yes: 0.5, No:0.5)	Rework
Prob. hazard per demand after fix (P1)	phd_df	phd_pc×(1.0−prob_fix)	Reliability, Requirement
Probability of fixing defect	prob_fix	See Table B3a	Rework, Reliability
Prob. of hazard per demand (P1)	P1	(r/100.0)×p_hazard_field+((100.0-r)/100.0)×phd_df	Reliability, Risk
% Dependence on field data	r	TNormal(0, 0.001, 0, 100)	Reliability
Actual number of demands (field)	ad	Uniform (0, 1000000)	Reliability
Accuracy of estimated demands	accuracy	States: (Very low: 0.2, Low: 0.2, Medium: 0.2, High: 0.2, Very high: 0.2)	Reliability
Number of estimated demands (field)	estdemands	Partitioned Expression (Very low: TNormal (ad, ad×10000, 0, 1E12), Low: TNormal (ad, ad×1000, 0, 1E12), Medium: TNormal (ad, ad×100, 0, 1E12), High: TNormal (ad, ad×10, 0, 1E12), Very high: (ad)	Reliability
Number of reported or potential hazards (field)	field_haz	Binomial (ad, p_hazard_field)	Reliability
Prob. of hazard per demand (field)	p_hazard_field	Uniform (0, 1000000)	Reliability
Number of reported or	n_fatal	Binomial (field_haz, ph_fatal)	Injury Occurrence

potential fatal injuries			
Number of reported or potential critical injuries	n_critical	Binomial (field_haz, ph_critical)	Injury Occurrence
Number of reported or potential major injuries	n_major	Binomial (field_haz, ph_major)	Injury Occurrence
Number of reported or potential minor injuries	n_minor	Binomial (field_haz, ph_minor)	Injury Occurrence
Number of reported or potential negligible injuries	n_negligible	Binomial (field_haz, ph_neglibile)	Injury Occurrence
Prob. hazard causes a fatal injury	ph_fatal	Uniform(0,1)	Injury Occurrence, Risk
Prob. hazard causes a critical injury	ph_critical	Uniform(0,1)	Injury Occurrence, Risk
Prob. hazard causes a major injury	ph_major	Uniform(0,1)	Injury Occurrence, Risk
Prob. hazard causes a minor injury	ph_minor	Uniform(0,1)	Injury Occurrence, Risk
Prob. hazard causes a negligible injury	ph_neglibile	Uniform(0,1)	Injury Occurrence, Risk
Prob. risk control stops fatal injury	control_f	1−ph_fatal	Injury Occurrence, Risk
Prob. risk control stops critical injury	control_c	1−ph_critical	Injury Occurrence
Prob. risk control stops major injury	control_ma	1−ph_major	Injury Occurrence
Prob. risk control stops minor injury	control_mi	1−ph_minor	Injury Occurrence
Prob. risk control stops negligible injury	control_n	1−ph_negligbile	Injury Occurrence
Prob. of fatal injury per demand	pfatal	P1×ph_fatal	Risk

Prob. of critical injury per demand	pcritical	P1×ph_critical	Risk
Prob. of major injury per demand	pmajor	P1×ph_major	Risk
Prob. of minor injury per demand	pminor	P1×ph_minor	Risk
Prob. of negligbile injury per demand	pnegligible	P1×ph_negligible	Risk
Acceptable prob. of a fatal injury per demand	a_pfatal	Uniform(0,1)	Risk Evaluation
Acceptable prob. of a critical injury per demand	a_pcritical	Uniform(0,1)	Risk Evaluation
Acceptable prob. of a major injury per demand	a_pmajor	Uniform(0,1)	Risk Evaluation
Acceptable prob. of a minor injury per demand	a_pminor	Uniform(0,1)	Risk Evaluation
Acceptable prob. of a negligible injury per demand	a_pnegligble	Uniform(0,1)	Risk Evaluation
Fatal injury risk acceptability	accept_fatal	IF(pfatal<=a_pfatal,"Acceptable","Not Acceptable")	Risk Evaluation
Critical injury risk acceptability	accept_critical	IF(pcritical<=a_pcritical,"Acceptable","Not Acceptable")	Risk Evaluation
Major injury risk acceptability	accept_major	IF(pmajor<=a_pmajor,"Acceptable","Not Acceptable")	Risk Evaluation
Minor injury risk acceptability	accept_minor	IF(pminor<=a_pminor,"Acceptable","Not Acceptable")	Risk Evaluation
Negligible injury risk acceptability	accept_negl	IF(pnegligible<=a_pnegligble,"Acceptable"," Not Acceptable")	Risk Evaluation
Overall residual risk (ORR)	orr	TNormal (wmean (10, accept_fatal, 4, accept_critical, 3, accept_major, 2, accept_minor, 1, accept_negl), 0.001, 0, 1)	Risk Evaluation, Benefit-Risk Analysis

Risk control required	control_req	Partitioned Expression: (Acceptable (Yes: 0, No: 1), Not Acceptable (Yes: 1, No: 0))	Risk Evaluation
ORR risk acceptability given benefits	orr_accept	TNormal (wmean (1, orr, 1, benefits), 0.001, 0, 1)	Risk Evaluation, Benefit-Risk Analysis
Benefits of device	benefits	TNormal (wmean (2, pop, 1, perf, 1, outcome, 1), 0.001, 0, 1)	Benefits, Benefit-Risk Analysis
Performance during clinical use	perf	Ranked: (Very low:0.2, Low:0.2, Medium:0.2, High:0.2, Very high:0.2)	Benefits
Patient population	pop	Ranked: (Very low:0.2, Low:0.2, Medium:0.2, High:0.2, Very high:0.2)	Benefits
Clinical outcome from using device	outcome	Ranked: (Very low:0.2, Low:0.2, Medium:0.2, High:0.2, Very high:0.2)	Benefits

Table B3a. NPT for Probability of Fixing Defect



Rework process overall effectiveness	Very Low		Low		Medium		High		Very High	
Rework done on device	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes
Expressions	0	TNormal(0.01,0.001,0.0,1.0)	0	TNormal(0.15,0.001,0.0,1.0)	0	TNormal(0.4,0.001,0.0,1.0)	0	TNormal(0.6,0.001,0.0,1.0)	0	TNormal(0.8,0.001,0.0,1.0)

B3 The Complete BN for Medical Device Risk Management

This section of Appendix B presents the schematic and complete BN for medical device risk management.

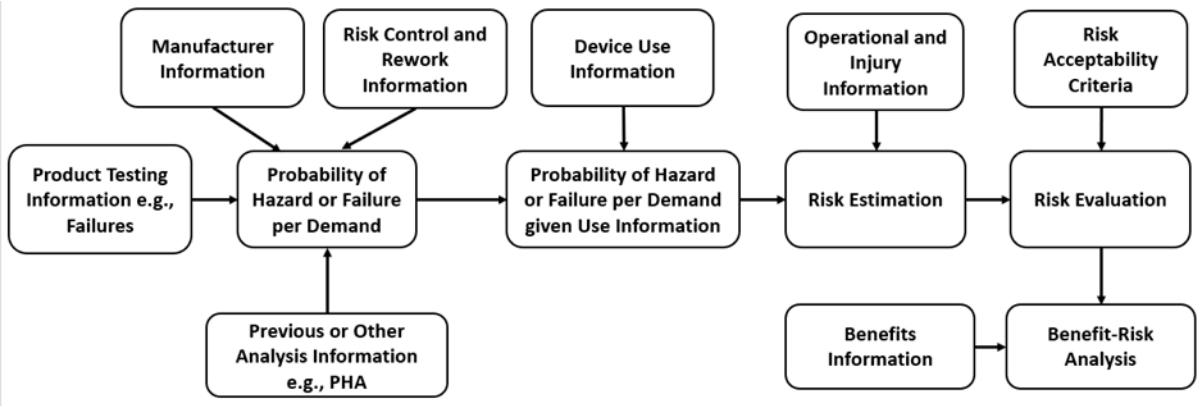
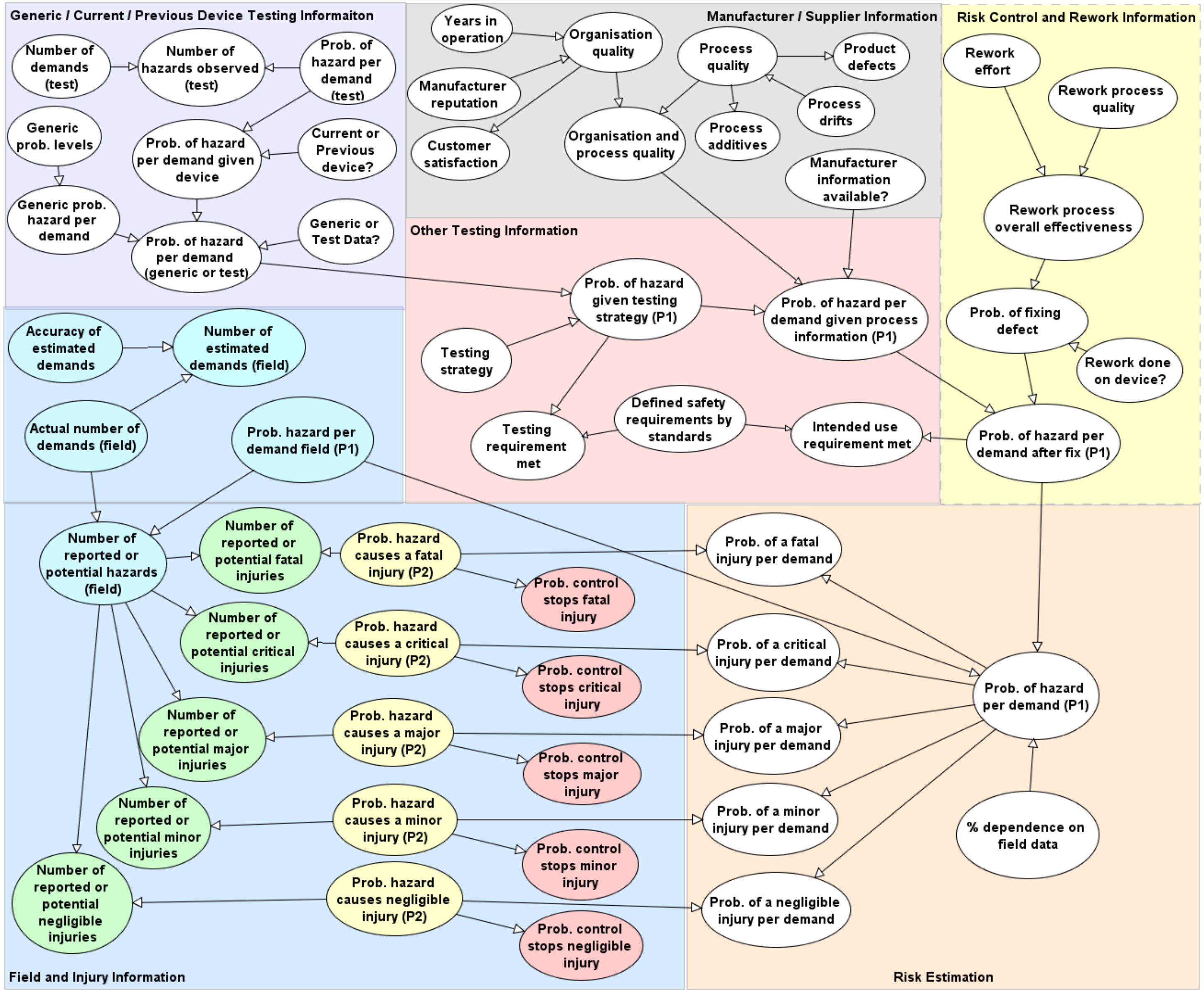

Manufacturer Information
Risk Control and Rework Information
Device Use Information
Operational and Injury Information
Risk Acceptability Criteria
Product Testing Information e.g., Failures
Probability of Hazard or Failure per Demand
Probability of Hazard or Failure per Demand given Use Information
Risk Estimation
Risk Evaluation
Previous or Other Analysis Information e.g., PHA
Benefits Information
Benefit-Risk Analysis

Figure B1 Schematic of the Medical Device Risk Management BN

Figure B2. Medical Device Risk Management BN – Risk Estimation Subnet


Generic / Current / Previous Device Testing Informaiton
Number of demands (test)
Number of hazards observed (test)
Prob. of hazard per demand (test)
Generic prob. levels
Prob. of hazard per demand given device
Current or Previous device?
Generic prob. hazard per demand
Prob. of hazard per demand (generic or test)
Generic or Test Data?
Manufacturer / Supplier Information
Years in operation
Organisation quality
Manufacturer reputation
Customer satisfaction
Organisation and process quality
Process quality
Product defects
Process drifts
Process additives
Manufacturer information available?
Risk Control and Rework Information
Rework effort
Rework process quality
Rework process overall effectiveness
Prob. of fixing defect
Rework done on device?
Prob. of hazard per demand after fix (P1)
Other Testing Information
Prob. of hazard given testing strategy (P1)
Prob. of hazard per demand given process information (P1)
Testing strategy
Testing requirement met
Defined safety requirements by standards
Intended use requirement met
Accuracy of estimated demands
Number of estimated demands (field)
Actual number of demands (field)
Prob. hazard per demand field (P1)
Number of reported or potential hazards (field)
Number of reported or potential fatal injuries
Number of reported or potential critical injuries
Number of reported or potential major injuries
Number of reported or potential minor injuries
Number of reported or potential negligible injuries
Prob. hazard causes a fatal injury (P2)
Prob. hazard causes a critical injury (P2)
Prob. hazard causes a major injury (P2)
Prob. hazard causes a minor injury (P2)
Prob. hazard causes negligible injury (P2)
Prob. control stops fatal injury
Prob. control stops critical injury
Prob. control stops major injury
Prob. control stops minor injury
Prob. control stops negligible injury
Field and Injury Information
Prob. of a fatal injury per demand
Prob. of a critical injury per demand
Prob. of a major injury per demand
Prob. of a minor injury per demand
Prob. of a negligible injury per demand
Prob. of hazard per demand (P1)
% dependence on field data
Risk Estimation

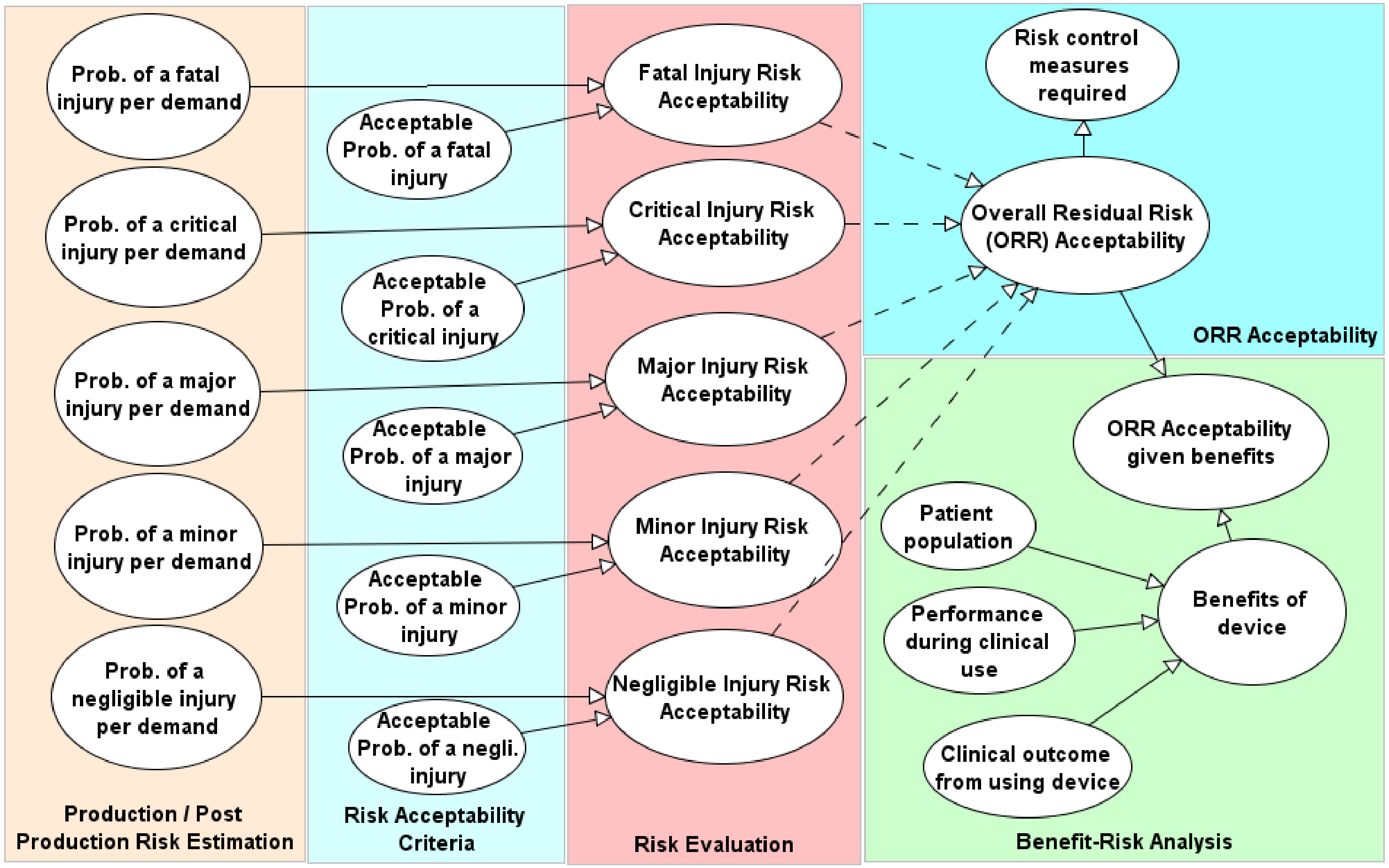

Prob. of a fatal injury per demand
Prob. of a critical injury per demand
Prob. of a major injury per demand
Prob. of a minor injury per demand
Prob. of a negligible injury per demand
Production / Post Production Risk Estimation
Acceptable Prob. of a fatal injury
Acceptable Prob. of a critical injury
Acceptable Prob. of a major injury
Acceptable Prob. of a minor injury
Acceptable Prob. of a negli. injury
Risk Acceptability Criteria
Fatal Injury Risk Acceptability
Critical Injury Risk Acceptability
Major Injury Risk Acceptability
Minor Injury Risk Acceptability
Negligible Injury Risk Acceptability
Risk Evaluation
Risk control measures required
Overall Residual Risk (ORR) Acceptability
ORR Acceptability
ORR Acceptability given benefits
Patient population
Performance during clinical use
Clinical outcome from using device
Benefits of device
Benefit-Risk Analysis

Figure B3. Medical Device Risk Management BN –Risk Evaluation Subnet

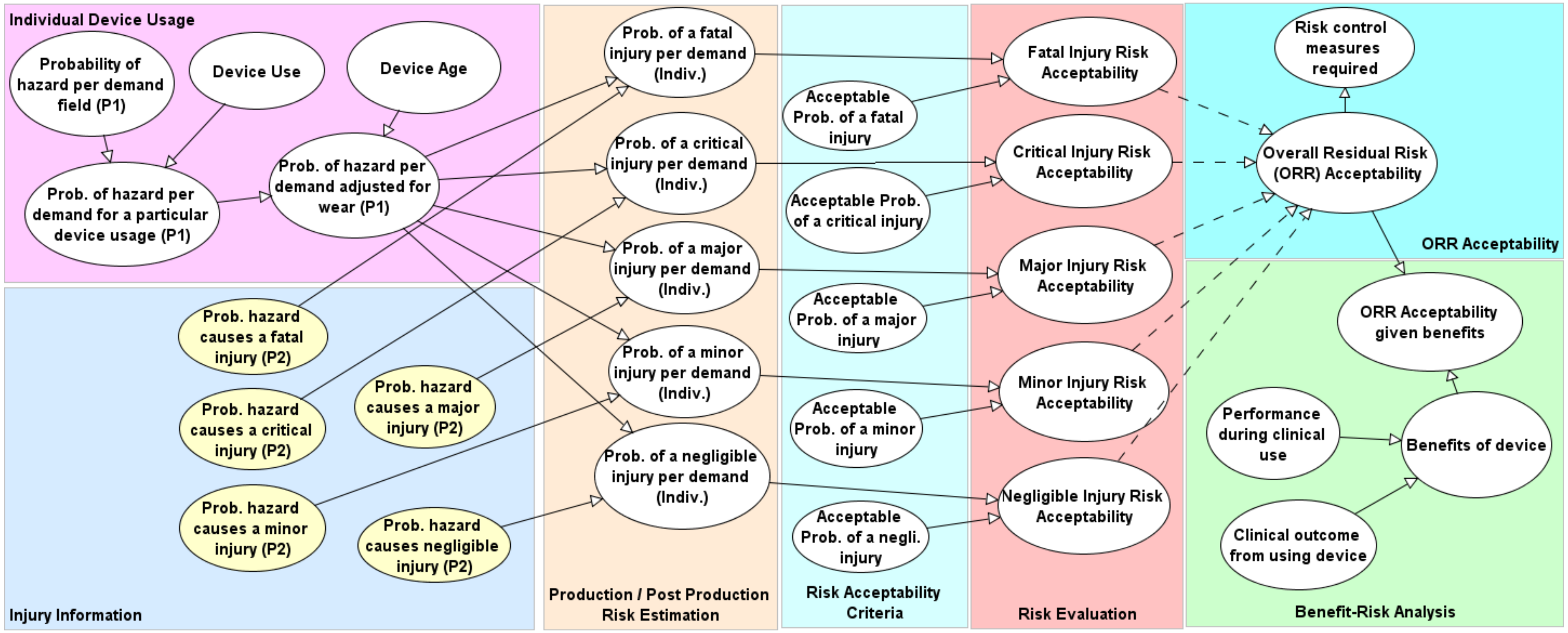

Individual Device Usage
Probability of hazard per demand field (P1)
Device Use
Device Age
Prob. of hazard per demand for a particular device usage (P1)
Prob. of hazard per demand adjusted for wear (P1)
Injury Information
Prob. hazard causes a fatal injury (P2)
Prob. hazard causes a critical injury (P2)
Prob. hazard causes a major injury (P2)
Prob. hazard causes a minor injury (P2)
Prob. hazard causes negligible injury (P2)
Production / Post Production Risk Estimation
Prob. of a fatal injury per demand (Indiv.)
Prob. of a critical injury per demand (Indiv.)
Prob. of a major injury per demand (Indiv.)
Prob. of a minor injury per demand (Indiv.)
Prob. of a negligible injury per demand (Indiv.)
Risk Acceptability Criteria
Acceptable Prob. of a fatal injury
Acceptable Prob. of a critical injury
Acceptable Prob. of a major injury
Acceptable Prob. of a minor injury
Acceptable Prob. of a negli. injury
Risk Evaluation
Fatal Injury Risk Acceptability
Critical Injury Risk Acceptability
Major Injury Risk Acceptability
Minor Injury Risk Acceptability
Negligible Injury Risk Acceptability
ORR Acceptability
Risk control measures required
Overall Residual Risk (ORR) Acceptability
Benefit-Risk Analysis
ORR Acceptability given benefits
Performance during clinical use
Benefits of device
Clinical outcome from using device

Figure B4. Medical Device Risk Management BN – Individual User Risk Estimation Subnet

B4 Model Assumptions

This section of Appendix B presents the model assumptions.

Model Assumptions:

1. Five injury severity levels i.e., fatal, critical, major, minor and negligible, see Table B4.
2. An injury risk is judged acceptable if it is less than or equal to risk acceptability criteria.
3. There are hidden nodes whose parents are the ‘Injury Risk Acceptability’ nodes. These hidden nodes are used to translate the results of the discrete nodes used for ‘Injury Risk Acceptability’ to ranked nodes for computing the ‘Overall Residual Risk Acceptability’ (defined as a ranked node). This explains why there are dotted lines in the model.
4. The NPT for ‘Overall Residual Risk Acceptability’ node is defined as *TNormal (wmean (10.0, fatal injury acceptability, 4.0, critical injury acceptability, 3.0, major injury acceptability, 2.0, minor injury acceptability, 1.0 negligible injury acceptability), 0.001, 0,1).* We used a weighted mean function to combine the respective scores for injury risk acceptability to produce an overall residual risk acceptability score. The nodes with higher weights will have a greater impact on the overall residual risk acceptability score.
5. A single known type of hazard is investigated. In Section 7.5, we discuss combining the risk results of different hazards for a medical device.

Table B4 Qualitative severity levels for harm

Rank	**Terms**	**Description**
5	Fatal	Result in death
4	Critical	Result in irreversible injury
3	Major	Results in injury requiring medical intervention
2	Minor	Results in temporary injury
1	Negligible	Results in temporary discomfort

Table B5 probability levels for the occurrence of harm

Rank	**Terms**	**Probability range**
5	Frequent	$\geq 10^{-3}$
4	Probable	$<10^{-3}$ and $\geq 10^{-4}$
3	Occasional	$<10^{-4}$ and $\geq 10^{-5}$
2	Remote	$<10^{-5}$ and $\geq 10^{-6}$
1	Improbable	$<10^{-6}$

B5 Instructions for using Medical Device Risk Management BN

This section of Appendix B presents the instructions for using the medical device risk management BN.

Instructions:

1. Define the scope and objectives of the analysis, including the hazards to be investigated and the risk acceptability criteria.
2. Describe the device, including its requirements, functions, users, intended use, safety characteristics, benefits, risk controls and life cycle phase.
3. Collate and organise other relevant information for the analysis:
    a. *Product testing information*: Information about the number of hazards observed in a set of demands during testing will allow the BN to estimate the probability of the hazard per demand. We define a demand as a measure of usage, e.g., single use, years etc.
    b. *Injury information*: Information about hazard occurrences and related injuries in the field will allow the BN to estimate the probability of the hazard or hazardous situation resulting in injury. Injury information can be obtained from hospitals and injury databases.
    c. *Manufacturer information*: Information such as manufacturer reputation, customer satisfaction, and product defects will allow the BN to estimate the quality of the manufacturing process. Since the quality of the manufacturing process can influence the occurrence of hazards, it will be used to revise the probability of the hazard per demand, especially in situations where there are little or no product testing data.
4. Perform the analysis using the BN:

a. Populate product testing information, manufacturer information, injury information and risk acceptability criteria.
b. Compute the risk and overall residual risk acceptability.
c. Estimate the effect of additional risk controls: In situations where the overall residual risk is not acceptable, populate risk control and rework information to estimate the residual risk given additional risk controls.
d. Perform benefit-risk analysis: Populate the benefits information to determine whether the risk of the device is acceptable given its benefits. This is useful, especially in situations where the overall residual risk is not acceptable after additional risk controls are implemented or situations where risk control measures are not practicable.

B6 Model Validation Results – AgenaRisk Screenshots

This section of Appendix B presents the model results for the risk management scenarios discussed in Section 7.4.

Figure B5 - BN Results for Defibrillator Scenario 1

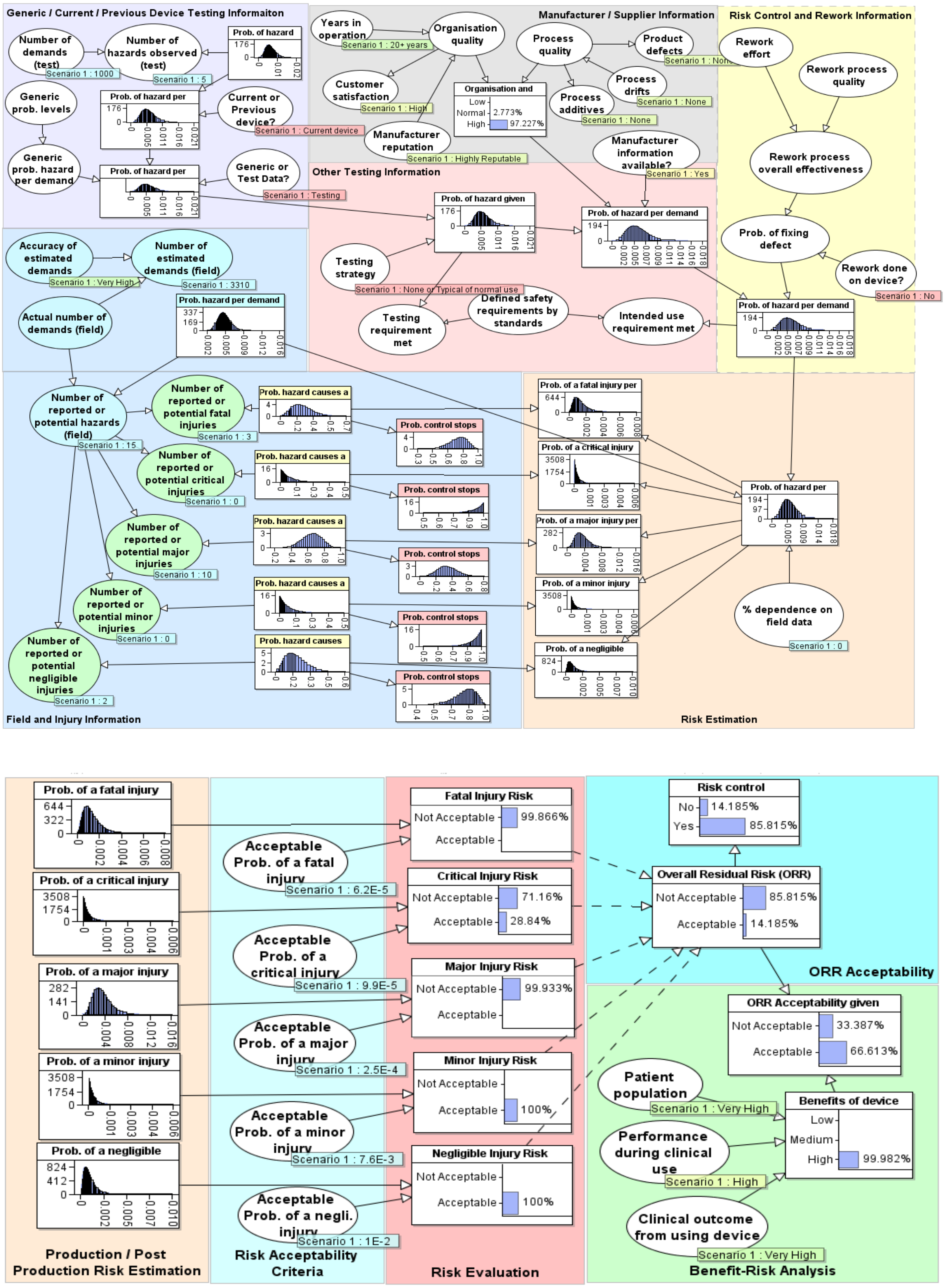
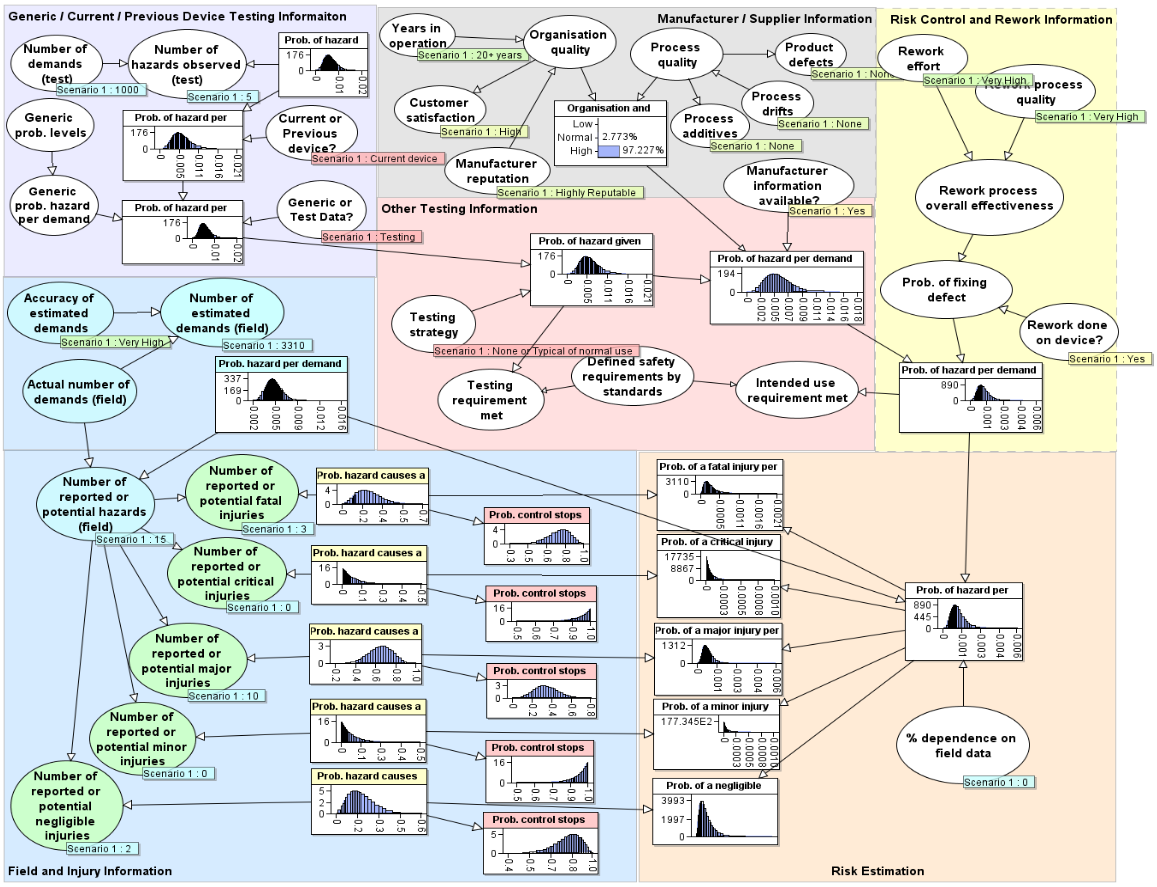


Figure B6 - BN Results for Defibrillator Scenario 1 – Rework Information


Generic / Current / Previous Device Testing Informaiton
Number of demands (test)
Scenario 1 : 1000
Number of hazards observed (test)
Scenario 1 : 5
Prob. of hazard
Generic prob. levels
Prob. of hazard per
Current or Previous device?
Scenario 1 : Current device
Generic prob. hazard per demand
Prob. of hazard per
Generic or Test Data?
Scenario 1 : Testing
Manufacturer / Supplier Information
Years in operation
Scenario 1 : 20+ years
Organisation quality
Process quality
Product defects
Scenario 1 : None
Customer satisfaction
Scenario 1 : High
Organisation and
Low
Normal 2.773%
High 97.227%
Process additives
Scenario 1 : None
Process drifts
Scenario 1 : None
Manufacturer reputation
Scenario 1 : Highly Reputable
Manufacturer information available?
Scenario 1 : Yes
Other Testing Information
Prob. of hazard given
Prob. of hazard per demand
Testing strategy
Scenario 1 : None or Typical of normal use
Defined safety requirements by standards
Testing requirement met
Intended use requirement met
Risk Control and Rework Information
Rework effort
Scenario 1 : Very High
Rework process quality
Scenario 1 : Very High
Rework process overall effectiveness
Prob. of fixing defect
Rework done on device?
Scenario 1 : Yes
Prob. of hazard per demand
Accuracy of estimated demands
Scenario 1 : Very High
Number of estimated demands (field)
Scenario 1 : 3310
Actual number of demands (field)
Prob. hazard per demand
Number of reported or potential hazards (field)
Scenario 1 : 15
Number of reported or potential fatal injuries
Scenario 1 : 3
Number of reported or potential critical injuries
Scenario 1 : 0
Number of reported or potential major injuries
Scenario 1 : 10
Number of reported or potential minor injuries
Scenario 1 : 0
Number of reported or potential negligible injuries
Scenario 1 : 2
Prob. hazard causes a
Prob. hazard causes
Prob. control stops
Field and Injury Information
Prob. of a fatal injury per
Prob. of a critical injury
Prob. of a major injury per
Prob. of a minor injury
Prob. of a negligible
Prob. of hazard per
% dependence on field data
Scenario 1 : 0
Risk Estimation

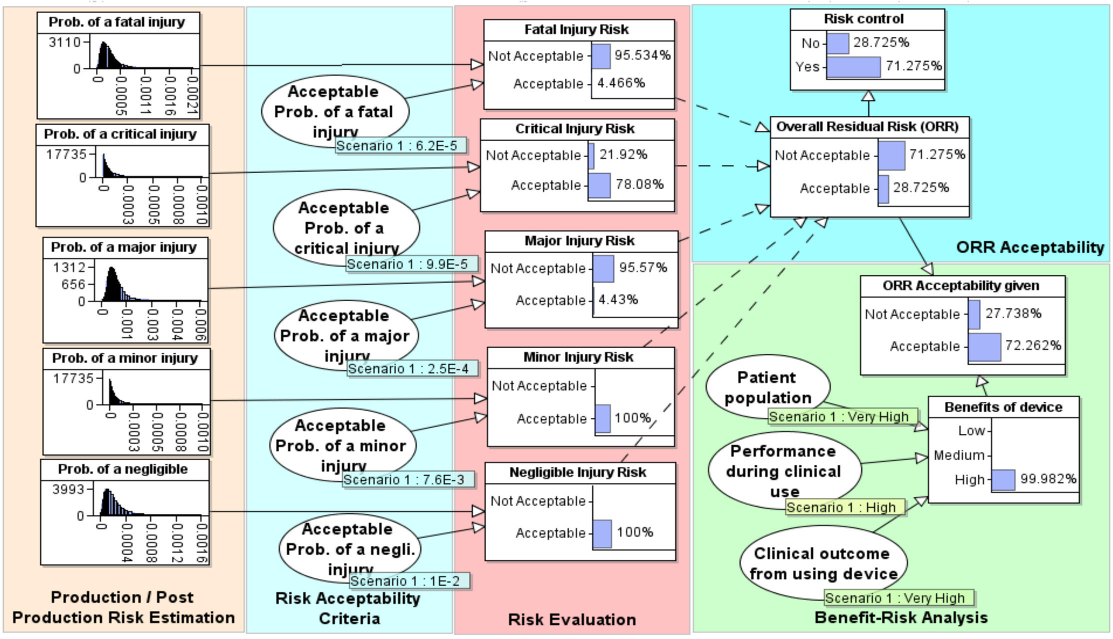


Figure B7 - BN Results for Defibrillator Scenario 2

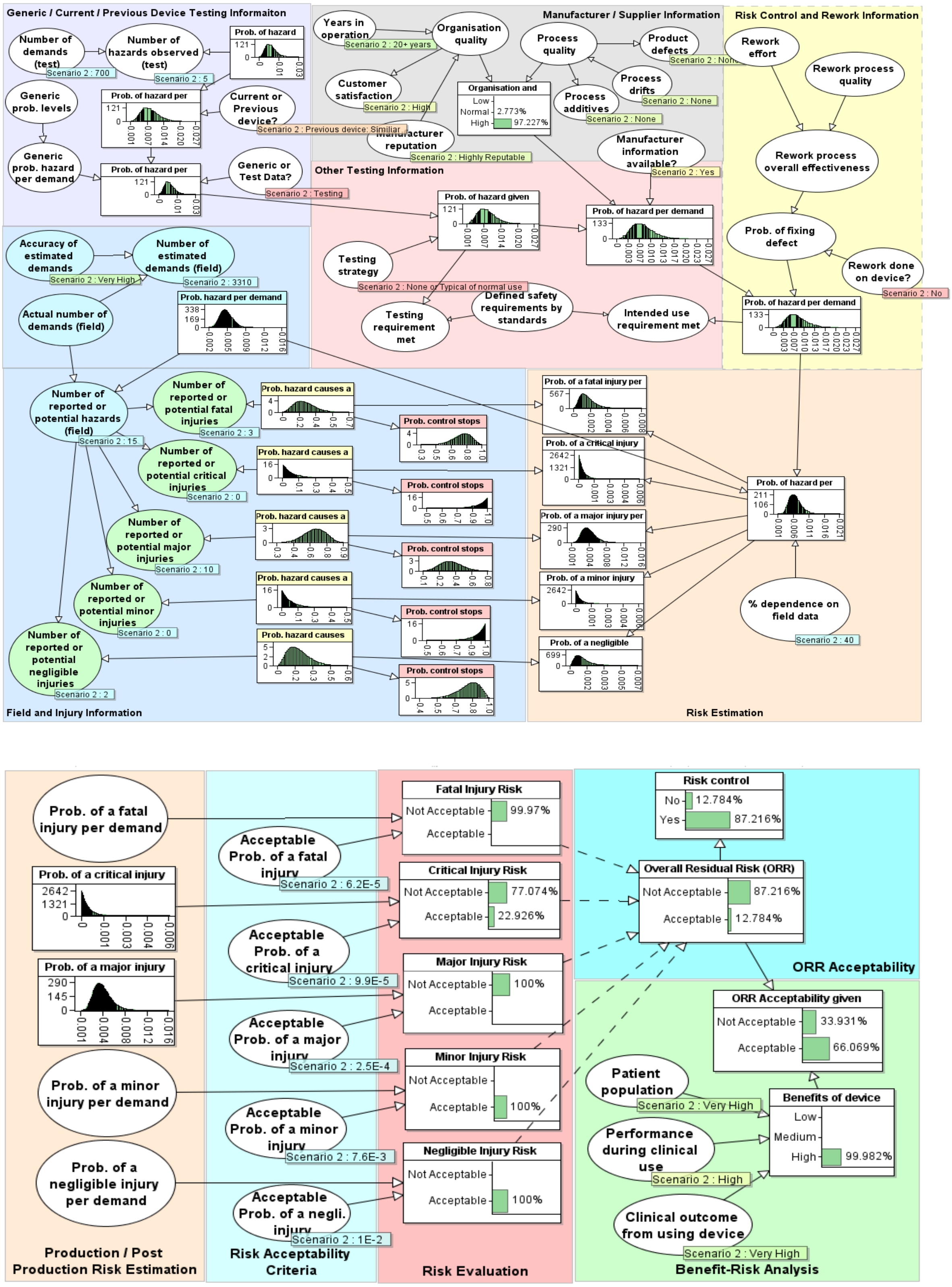


Figure B8 - BN Results for Defibrillator Scenario 3

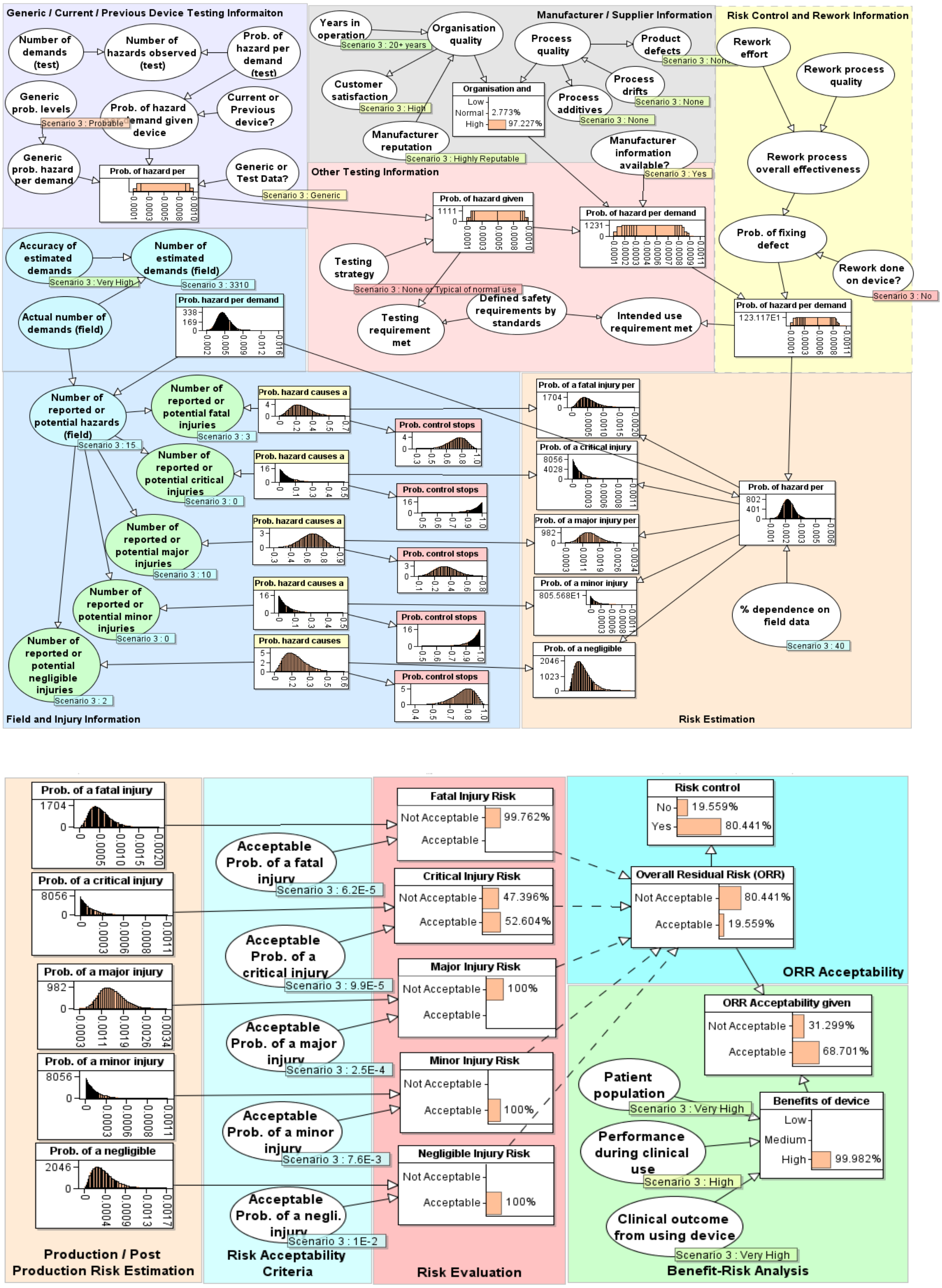


Figure B9 - BN Results for Defibrillator Scenario 4

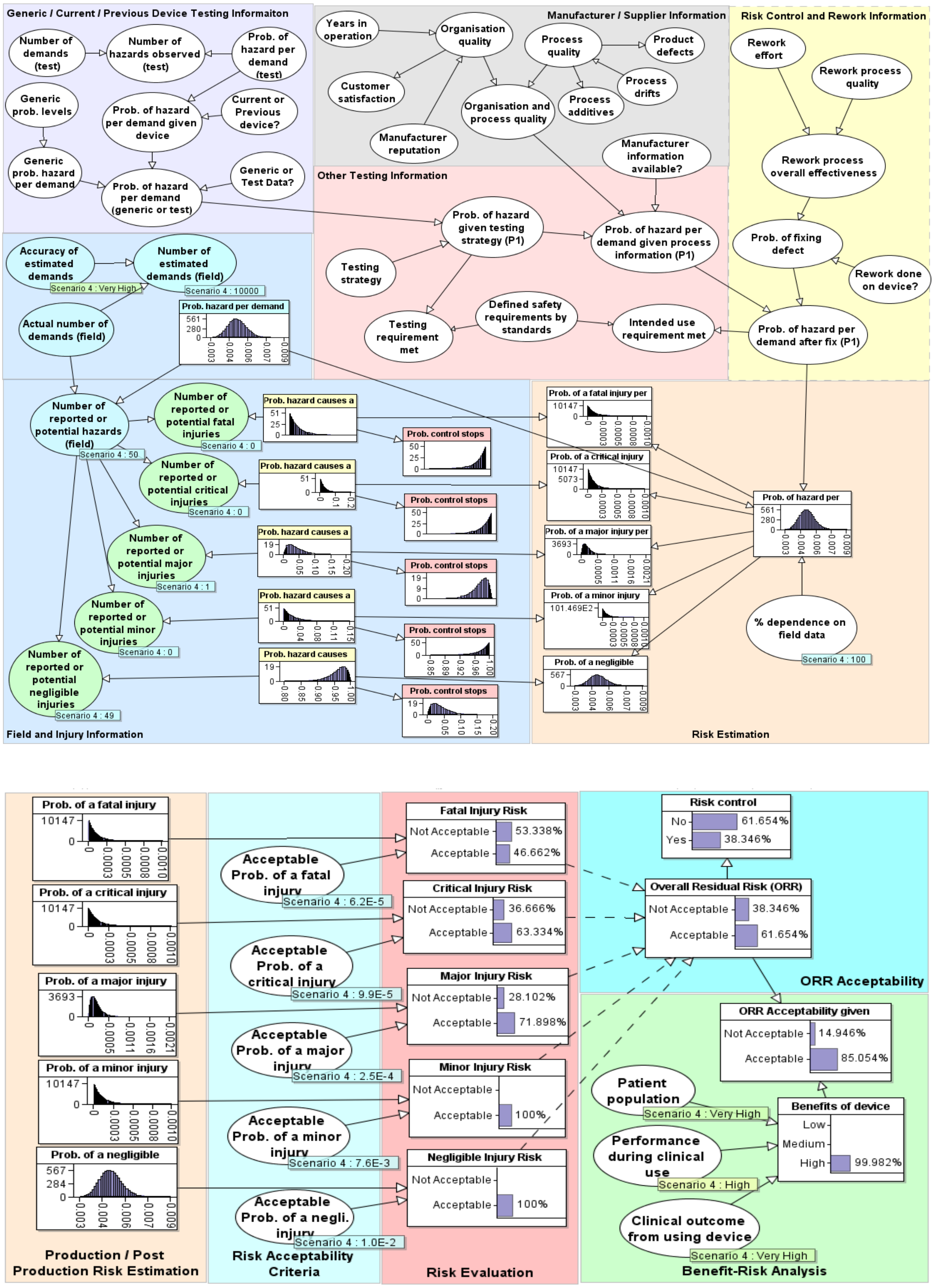
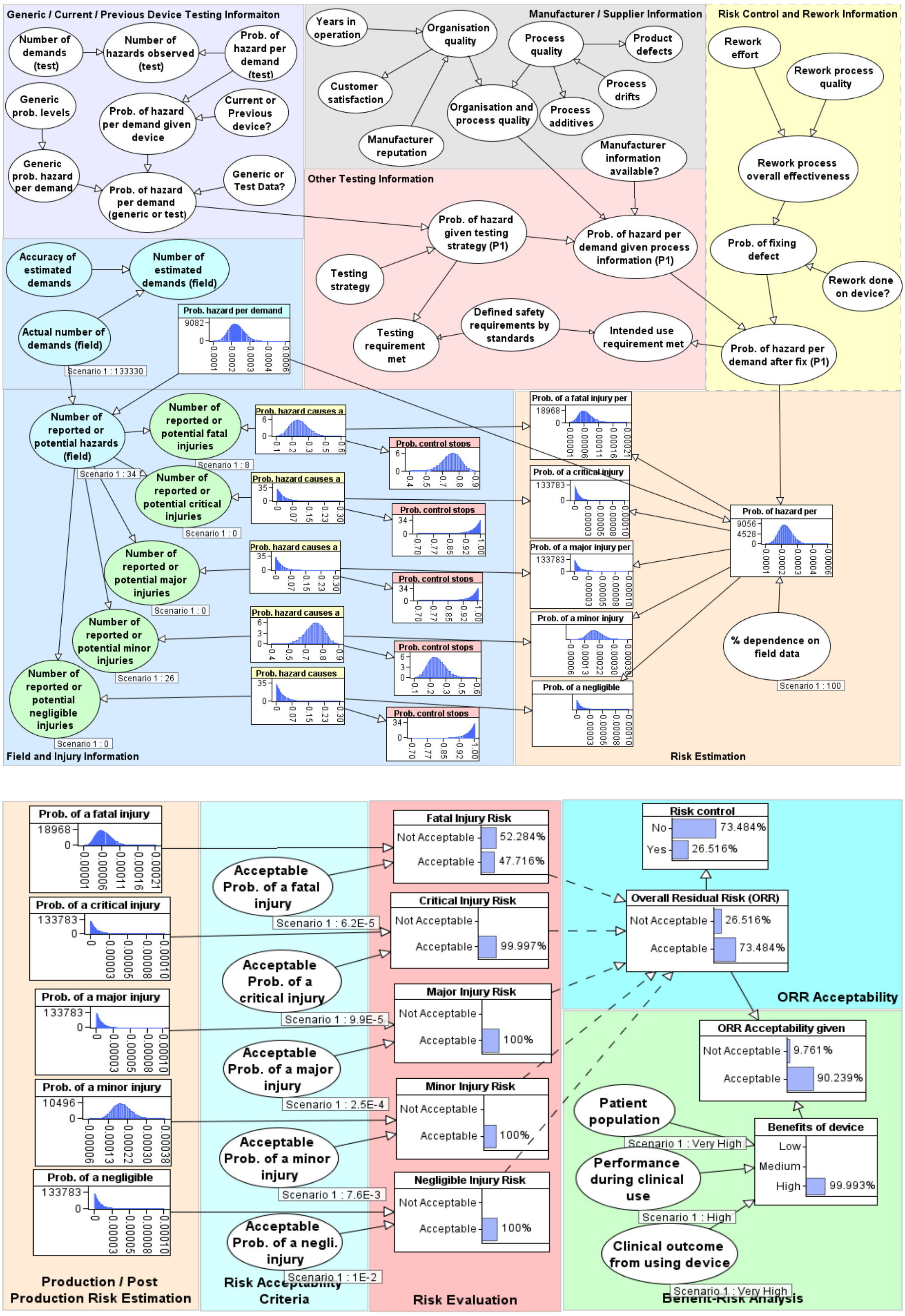

Generic / Current / Previous Device Testing Informaiton
Number of demands (test)
Number of hazards observed (test)
Prob. of hazard per demand (test)
Generic prob. levels
Prob. of hazard per demand given device
Current or Previous device?
Generic prob. hazard per demand
Prob. of hazard per demand (generic or test)
Generic or Test Data?
Manufacturer / Supplier Information
Years in operation
Organisation quality
Process quality
Product defects
Customer satisfaction
Process drifts
Organisation and process quality
Process additives
Manufacturer reputation
Manufacturer information available?
Risk Control and Rework Information
Rework effort
Rework process quality
Rework process overall effectiveness
Prob. of fixing defect
Rework done on device?
Prob. of hazard per demand after fix (P1)
Other Testing Information
Prob. of hazard given testing strategy (P1)
Prob. of hazard per demand given process information (P1)
Testing strategy
Testing requirement met
Defined safety requirements by standards
Intended use requirement met
Accuracy of estimated demands
Scenario 4 : Very High
Number of estimated demands (field)
Scenario 4 : 10000
Actual number of demands (field)
Prob. hazard per demand
561
280
0
0.003
0.004
0.006
0.007
0.009
Number of reported or potential hazards (field)
Scenario 4 : 50
Number of reported or potential fatal injuries
Scenario 4 : 0
Prob. hazard causes a
Prob. control stops
Number of reported or potential critical injuries
Scenario 4 : 0
Number of reported or potential major injuries
Scenario 4 : 1
Number of reported or potential minor injuries
Scenario 4 : 0
Number of reported or potential negligible injuries
Scenario 4 : 49
Field and Injury Information
Prob. of a fatal injury per
Prob. of a critical injury
Prob. of a major injury per
Prob. of a minor injury
Prob. of a negligible
Prob. of hazard per
% dependence on field data
Scenario 4 : 100
Risk Estimation
Prob. of a fatal injury
10147
0
0.0003
0.0005
0.0008
0.0010
Prob. of a critical injury
10147
Prob. of a major injury
3693
0.0005
0.0011
0.0016
0.0021
Prob. of a minor injury
10147
Prob. of a negligible
567
284
0.003
0.004
0.006
0.007
0.009
Production / Post Production Risk Estimation
Acceptable Prob. of a fatal injury
Scenario 4 : 6.2E-5
Acceptable Prob. of a critical injury
Scenario 4 : 9.9E-5
Acceptable Prob. of a major injury
Scenario 4 : 2.5E-4
Acceptable Prob. of a minor injury
Scenario 4 : 7.6E-3
Acceptable Prob. of a negli. injury
Scenario 4 : 1.0E-2
Risk Acceptability Criteria
Fatal Injury Risk
Not Acceptable 53.338%
Acceptable 46.662%
Critical Injury Risk
Not Acceptable 36.666%
Acceptable 63.334%
Major Injury Risk
Not Acceptable 28.102%
Acceptable 71.898%
Minor Injury Risk
Not Acceptable
Acceptable 100%
Negligible Injury Risk
Not Acceptable
Acceptable 100%
Risk Evaluation
Risk control
No 61.654%
Yes 38.346%
Overall Residual Risk (ORR)
Not Acceptable 38.346%
Acceptable 61.654%
ORR Acceptability
ORR Acceptability given
Not Acceptable 14.946%
Acceptable 85.054%
Patient population
Scenario 4 : Very High
Benefits of device
Low
Medium
High 99.982%
Performance during clinical use
Scenario 4 : High
Clinical outcome from using device
Scenario 4 : Very High
Benefit-Risk Analysis

Figure B10 - BN Results for LIFEPAK Defibrillator 1000


Generic / Current / Previous Device Testing Informaiton
Number of demands (test)
Number of hazards observed (test)
Prob. of hazard per demand (test)
Generic prob. levels
Prob. of hazard per demand given device
Current or Previous device?
Generic prob. hazard per demand
Prob. of hazard per demand (generic or test)
Generic or Test Data?
Manufacturer / Supplier Information
Years in operation
Organisation quality
Process quality
Product defects
Customer satisfaction
Process drifts
Organisation and process quality
Process additives
Manufacturer reputation
Manufacturer information available?
Risk Control and Rework Information
Rework effort
Rework process quality
Rework process overall effectiveness
Prob. of fixing defect
Rework done on device?
Prob. of hazard per demand after fix (P1)
Other Testing Information
Prob. of hazard given testing strategy (P1)
Prob. of hazard per demand given process information (P1)
Testing strategy
Defined safety requirements by standards
Testing requirement met
Intended use requirement met
Accuracy of estimated demands
Number of estimated demands (field)
Actual number of demands (field)
Prob. hazard per demand
Scenario 1 : 133330
Number of reported or potential hazards (field)
Scenario 1 : 34
Number of reported or potential fatal injuries
Scenario 1 : 8
Number of reported or potential critical injuries
Scenario 1 : 0
Number of reported or potential major injuries
Scenario 1 : 0
Number of reported or potential minor injuries
Scenario 1 : 26
Number of reported or potential negligible injuries
Scenario 1 : 0
Prob. hazard causes a
Prob. hazard causes
Prob. control stops
Field and Injury Information
Prob. of a fatal injury per
Prob. of a critical injury
Prob. of a major injury per
Prob. of a minor injury
Prob. of a negligible
Prob. of hazard per
% dependence on field data
Scenario 1 : 100
Risk Estimation
Prob. of a fatal injury
Prob. of a critical injury
Prob. of a major injury
Prob. of a minor injury
Prob. of a negligible
Production / Post Production Risk Estimation
Acceptable Prob. of a fatal injury
Scenario 1 : 6.2E-5
Acceptable Prob. of a critical injury
Scenario 1 : 9.9E-5
Acceptable Prob. of a major injury
Scenario 1 : 2.5E-4
Acceptable Prob. of a minor injury
Scenario 1 : 7.6E-3
Acceptable Prob. of a negli. injury
Scenario 1 : 1E-2
Risk Acceptability Criteria
Fatal Injury Risk
Not Acceptable 52.284%
Acceptable 47.716%
Critical Injury Risk
Not Acceptable
Acceptable 99.997%
Major Injury Risk
Not Acceptable
Acceptable 100%
Minor Injury Risk
Not Acceptable
Acceptable 100%
Negligible Injury Risk
Not Acceptable
Acceptable 100%
Risk Evaluation
Risk control
No 73.484%
Yes 26.516%
Overall Residual Risk (ORR)
Not Acceptable 26.516%
Acceptable 73.484%
ORR Acceptability
ORR Acceptability given
Not Acceptable 9.761%
Acceptable 90.239%
Patient population
Scenario 1 : Very High
Benefits of device
Low
Medium
High 99.993%
Performance during clinical use
Scenario 1 : High
Clinical outcome from using device
Scenario 1 : Very High
Benefit-Risk Analysis

Appendix C Chapter 8 Supplemental Material

C1 RAPEX Risk Matrix

This section of Appendix C presents the risk matrix used in the RAPEX methodology.

Table C1 RAPEX Risk Matrix

Probability of harm over life of product	**Severity of harm**			
	Level 1	**Level 2**	**Level 3**	**Level 4**
>50%	High	Serious	Serious	Serious
>1 in 10	Medium	Serious	Serious	Serious
>1 in 100	Medium	Serious	Serious	Serious
>1 in 1000	Low	High	Serious	Serious
>1 in 10,000	Low	Medium	High	Serious
>1 in 100,000	Low	Low	Medium	High
>1 in 1,000,000	Low	Low	Low	Medium
<1 in 1,000,000	Low	Low	Low	Low

C2 Model Variables and NPT

This section of Appendix C presents the variables and NPTs used in the BN for consumer product safety risk assessment.

Table C2. Variables and NPTs for Consumer Product Safety Risk Assessment BN

Variable name	**Abbrev**	**Node type**	**NPT**
Number of demands tested	ndt	Simulation (integer interval)	Uniform(0, 1000000)
Number of times hazard observed in tests	nho	Simulation (integer interval)	Binomial(ndt, p_h_testcond)
Testing strategy	ts	Labelled (Less strenuous than normal use, Typical of normal use, More strenuous than normal use, Generally poor testing)	Less strenuous than normal use: 0.1, Typical of normal use 0.6, More strenuous than normal use 0.2, Generally poor testing 0.1
Probability of hazard per demand under testing conditions	p_h_testcond	Simulation (continuous interval)	Partitioned Expression (Less strenuous than normal use: p_h_strat-0.5*p_h_strat, Typical of normal use: p_h_strat, More strenuous than normal use:

			p_h_strat + 0.5*p_h_strat, Generally poor testing: TNormal(p_h_strat,0.001,0,1))
Probability of hazard per demand given testing strategy	p_h_strat	Simulation (continuous interval)	TNormal(0.001, 0.01, 0,1)
Generic or Test Data?	genswitch	Boolean (Testing, Generic)	Testing: 0.99, Generic: 0.01
Generic prob. levels	levels	Labelled (Frequent, Probable, Occasional, Remote, Improbable)	Frequent: 0.2, Probable: 0.2, Occasional: 0.2, Remote: 0.2, Improbable: 0.2
Generic prob. hazard per demand	genprob	Simulation (continuous interval)	Partitioned Expression (Frequent: Uniform (0.001, 1), Probable: Uniform (1E-4, 0.99E-3), Occasional: Uniform (1E-5, 0.99E-4), Remote: Uniform (1E-6, 0.99E-5), Improbable: Uniform (0, 0.99E-6))
Prob. of hazard per demand (generic or test)	phdtest	Simulation (continuous interval)	Partitioned Expression (Testing: p_h_strat, Generic: genprob)
Testing requirement result	test_req	Boolean (True, False)	if(reg_hpd>=p_h_testcond,"True","False")
Regulator hazard per demand requirement	reg_hpd_req	Simulation (continuous interval)	TNormal(0,0.001,0,1)
Normal product use requirement result	norm_req	Boolean (True, False)	if(reg_hpd>=p_h_normal_use,"True","False")
Manufacturer Reputation	reputation	Ranked (Disreputable, Reputable, Highly Reputable)	Disreputable: 0.33333334, Reputable: 0.33333334, Highly Reputable: 0.33333334
Years in operation	years_operating	Ranked (< 1 year, 1 - 5 years, 5 - 10 years, 10 - 20 years, 20+ years)	< 1 year: 0.2, 1 - 5 years: 0.2, 5 - 10 years: 0.2, 10 - 20 years: 0.2, 20+ years: 0.2
Customer satisfaction	cust_sat	Ranked (Very Low, Low, Medium, High, Very High)	TNormal(m_quality,0.05, 0, 1)
Product design	prod_design	Ranked (No change, Minor improvements,	TNormal(m_quality,0.05, 0, 1)

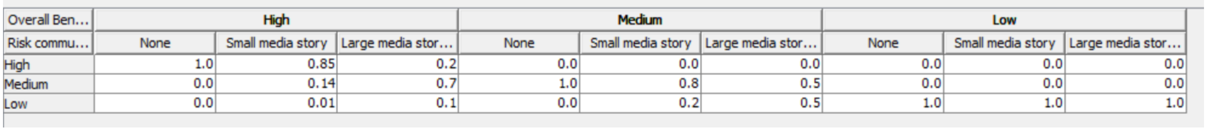
		Major improvements)	
Manufacturer process quality	m_quality	Ranked (Low, Normal, High)	TNormal(wmean(1.0,years_operating,2.0,reputation),0.001,0,1)
Probability of hazard per demand for normal product use given process information	p_h_normal_use	Simulation (continuous interval)	Partitioned Expression (Low: phdtest *1.1, Normal: phdtest, High: 0.9* phdtest)
Product usage informaiton	prod_usage	Labelled (Used as intended, Minor deviations, Major deviations)	Used as intended: 0.9, Minor deviations: 0.07, Major deviations: 0.03
Probability of hazard per demand given product usage	p_h_usage	Simulation (continuous interval)	Partitioned Expression (Used as intended: p_h_normal_use, Minor deviations: p_h_normal_use + 0.1*p_h_normal_use, Major deviations: p_h_normal_use + 0.5*p_h_normal_use)
Number of demands in particular product lifetime	demands	Simulation (integer interval)	TNormal(100, 1000, 0, 1E8)
Probability of hazard per demand adjusted for demands in product lifetime	p_h_demands	Simulation (continuous interval)	1.0-(1.0-p_h_usage)^demands
Years in use	years	Simulation (continuous interval)	TNormal(0, 10, 0, 30)
Probability of hazard per demand adjusted for wear	p_h_wear	Simulation (continuous interval)	min(1.0,p_h_demands+p_h_demands*years^2.0/1000.0)
Number of demands in the field	f_demands	Simulation (continuous interval)	Uniform(0,1E9)
Number of observed hazards in the field	f_hazards	Simulation (integer interval)	Binomial(f_demands, ph_field)
Probability of hazard per demand in field	ph_field	Simulation (continuous interval)	Uniform(0,1)
Number of observed major injuries	num_maj	Simulation (integer interval)	Binomial(f_hazards, p_uh_major)
Number of observed minor injuries	num_min	Simulation (integer interval)	Binomial(f_hazards, p_uh_minor)

Probability hazard causes a major injury	p_uh_major	Simulation (continuous interval)	Uniform(0,1)
Probability hazard causes a minor injury	p_uh_minor	Simulation (continuous interval)	Uniform(0,1)
Probability control stops major injury	pcontrolmajor	Simulation (continuous interval)	1.0-p_uh_major
Probability controls stops minor injury	pcontrolminor	Simulation (continuous interval)	1.0-p_uh_minor
Probability other control stops injury	p_control	Simulation (continuous interval)	Uniform(0,1)
Probability hazard causes a major injury revised	p_h_major	Simulation (continuous interval)	p_uh_major*(1.0-p_control)
Probability hazard causes a minor injury revised	p_h_minor	Simulation (continuous interval)	p_uh_minor*(1.0-p_control)
Probability of hazard per demand	P1	Simulation (continuous interval)	(percentage/100.0)*ph_field+((100.0-percentage)/100.0)*p_h_wear
% Dependence on field data	percentage	Simulation (continuous interval)	TNormal(50, 0.001, 0, 100)
Probability of major injury per demand	p_major_L	Simulation (continuous interval)	P1*p_h_major
Probability of minor injury per demand	p_minor_L	Simulation (continuous interval)	P1*p_h_minor
Actual Number of product instances	t_prod	Simulation (integer interval)	Uniform(0,1000000000)
Total number of major injuries	t_major	Simulation (integer interval)	P_major_L* t_prod
Total number of minor injuries	t_minor	Simulation (integer interval)	t_prod * p_minor_L
Risk level (one product instance)	risk_level	Ranked (Very Low, Low, Medium, High, Very High)	TNormal((min(1.0,100.0*(p_major_L + 0.5*p_minor_L)),0.001, 0,1)

Number of product instances	Num_prod	Ranked (Very Low: <10k, Low: 10k - 100k, Medium: 100k - 500k, High: 500k - 1m, Very High: > 1m)	Very Low: <10k: 0.2, Low: 10k -100k: 0.2, Medium: 100k - 500k: 0.2, High: 500k – 1m: 0.2, Very High: > 1m: 0.2
Likelihood of use	likelihood	Ranked (High, Medium, Low)	High: 0.33333334, Medium: 0.33333334, Low: 0.33333334
Benefits	benefits	Ranked (High, Medium, Low)	High: 0.33333334, Medium: 0.33333334, Low: 0.33333334
Overall benefits	util	Ranked (High, Medium, Low)	TNormal((wmean(1.0, likelihood, 1.0 benefits)), 0.001, 0, 1)
Government intervention required given risk level	gov_int_req	Boolean(True, False)	if(risk_level>0.5,"True","False")
Risk tolerability	risk_toler	Ranked (Very High (Acceptable), High (Acceptable), Medium (Tolerable), Low (Unacceptable), Very Low (Unacceptable))	TNormal((wmean(2.0,risk_level,1.0,util)), 0.001, 0, 1)
Government intervention required given risk tolerability	gov_int_req2	Boolean(True, False)	if(risk_toler>0.5,"True","False")
Severity of injury	severity	Ranked (Low, Medium, High)	Low: 0.33333334, Medium: 0.33333334, High: 0.33333334
Hazardousness	hazardousness	Ranked (Low, Medium, High)	Low: 0.33333334, Medium: 0.33333334, High: 0.33333334
Worry	worry	Ranked (Low, Medium, High)	Low: 0.33333334, Medium: 0.33333334, High: 0.33333334
Consumer perceived risk	c_risk_per	Ranked (Low, Medium, High)	TNormal((wmean(1.0,severity,1.0, worry,1.0, hazardousness)), 0.001,0,1)
Consumer risk tolerability	crt	Ranked (Very High (Acceptable), High (Acceptable), Medium (Tolerable), Low (Unacceptable), Very Low (Unacceptable))	TNormal((wmean(1.0,c_risk_per,1.0, util)), 0.001,0,1)
Risk communication	rc	Ranked (None, Small media story,	None: 0.33333334 Small media story: 0.33333334, large media

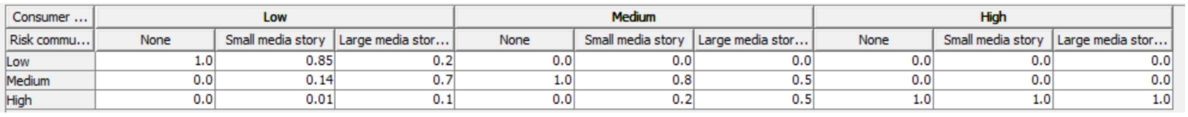
		large media story / product recall)	story / product recall: 0.33333334
Revised benefits given risk communication	rev_util		See Table C2a for NPT
Revised consumer perceived risk given risk communication	rev_c_risk_per		See Table C2b for NPT
Government intervention announced	govt_int_ann	Ranked (No, Yes)	No: 0.5, Yes: 0.5
Revised consumer risk tolerability	risk_toler2	Ranked (Very High (Acceptable), High (Acceptable), Medium (Tolerable), Low (Unacceptable), Very Low (Unacceptable))	TNormal((wmean(2.0,rev_c_risk_per,1.0,rev_util)),0.001,0,1)
Government intervention required given revised risk tolerability	gov_int_req3	Boolean(True, False)	if(risk_toler2>0.5,"True","False")

Table C2a NPT for the node Revised benefits given risk communication



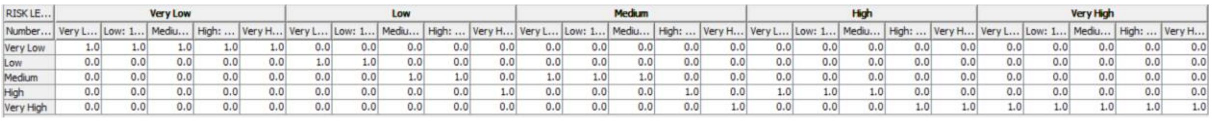
Overall Ben…	High			Medium			Low		
Risk commu…	None	Small media story	Large media stor…	None	Small media story	Large media stor…	None	Small media story	Large media stor…
High	1.0	0.85	0.2	0.0	0.0	0.0	0.0	0.0	0.0
Medium	0.0	0.14	0.7	1.0	0.8	0.5	0.0	0.0	0.0
Low	0.0	0.01	0.1	0.0	0.2	0.5	1.0	1.0	1.0

Table C2b NPT for the node Revised consumer perceived risk given risk communication



Consumer …	Low			Medium			High		
Risk commu…	None	Small media story	Large media stor…	None	Small media story	Large media stor…	None	Small media story	Large media stor…
Low	1.0	0.85	0.2	0.0	0.0	0.0	0.0	0.0	0.0
Medium	0.0	0.14	0.7	1.0	0.8	0.5	0.0	0.0	0.0
High	0.0	0.01	0.1	0.0	0.2	0.5	1.0	1.0	1.0

Table C2c NPT for the node risk level (all products instances)



RISK LE…	Very Low					Low					Medium					High					Very High				
Number…	Very L…	Low: 1…	Mediu…	High: …	Very H…	Very L…	Low: 1…	Mediu…	High: …	Very H…	Very L…	Low: 1…	Mediu…	High: …	Very H…	Very L…	Low: 1…	Mediu…	High: …	Very H…	Very L…	Low: 1…	Mediu…	High: …	Very H…
Very Low	1.0	1.0	1.0	1.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Low	0.0	0.0	0.0	0.0	0.0	1.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Medium	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0	1.0	0.0	1.0	1.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
High	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	1.0	0.0	1.0	1.0	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Very High	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.0	0.0	0.0	0.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0

C3 The Complete BN for Consumer Product Risk Assessment

This section of Appendix C presents the complete BN for consumer product safety risk assessment.

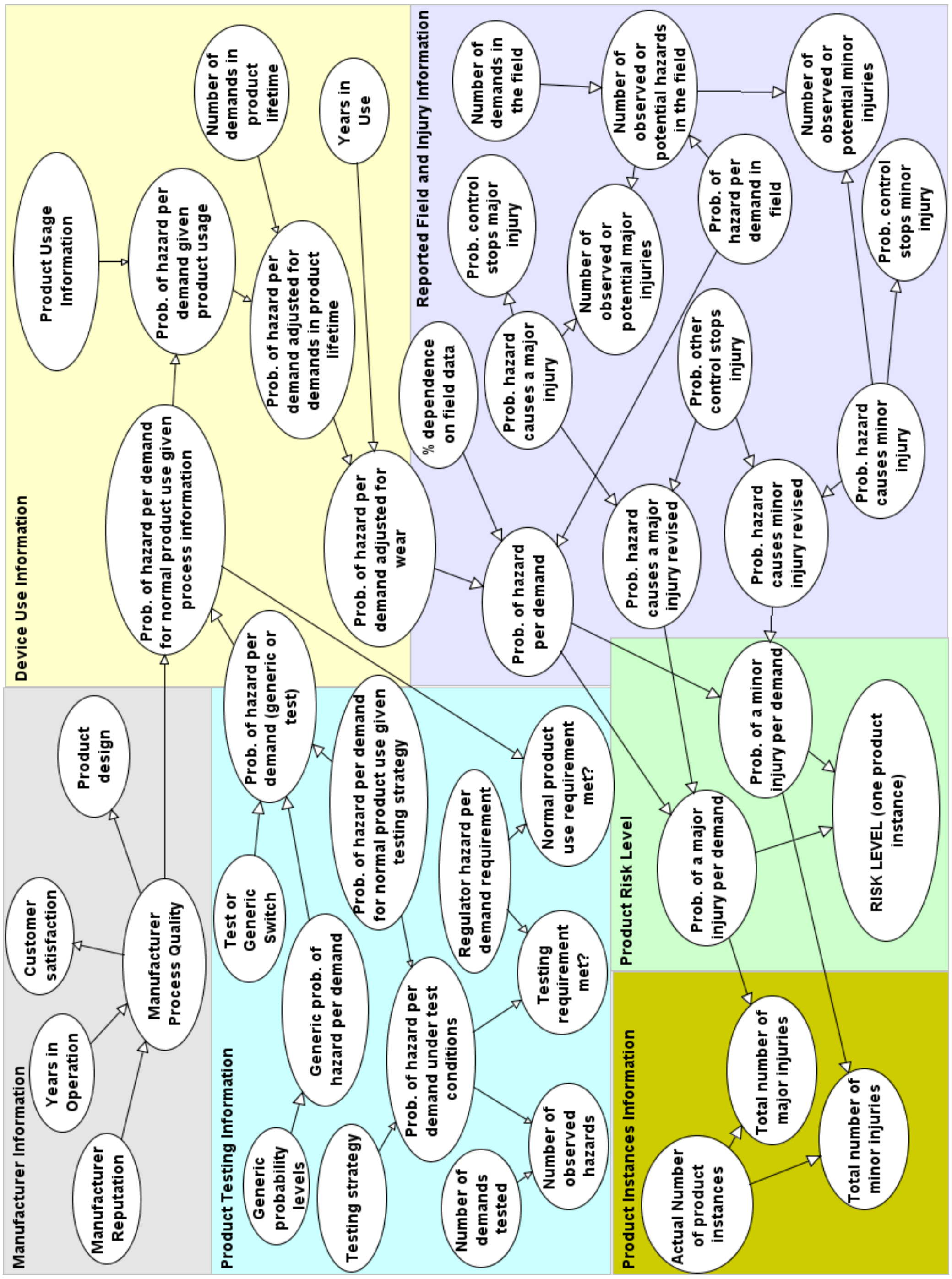

Device Use Information
Product Usage Information
Prob. of hazard per demand given product usage
Number of demands in product lifetime
Prob. of hazard per demand adjusted for demands in product lifetime
Years in Use
Prob. of hazard per demand for normal product use given process information
Prob. of hazard per demand adjusted for wear
Reported Field and Injury Information
Number of demands in the field
Number of observed or potential hazards in the field
Number of observed or potential minor injuries
Prob. control stops major injury
Number of observed or potential major injuries
Prob. of hazard per demand in field
Prob. control stops minor injury
% dependence on field data
Prob. hazard causes a major injury
Prob. other control stops injury
Prob. hazard causes minor injury
Prob. of hazard per demand
Prob. hazard causes a major injury revised
Prob. hazard causes minor injury revised
Manufacturer Information
Product design
Customer satisfaction
Years in Operation
Manufacture Process Quality
Manufacturer Reputation
Product Testing Information
Prob. of hazard per demand (generic or test)
Prob. of hazard per demand for normal product use given testing strategy
Test or Generic Switch
Generic prob. of hazard per demand
Generic probability levels
Testing strategy
Prob. of hazard per demand under test conditions
Regulator hazard per demand requirement
Normal product use requirement met?
Testing requirement met?
Number of demands tested
Number of observed hazards
Product Risk Level
Prob. of a minor injury per demand
Prob. of a major injury per demand
RISK LEVEL (one product instance)
Product Instances Information
Actual Number of product instances
Total number of major injuries
Total number of minor injuries

Figure C1. Consumer Product Safety Risk Assessment BN –Risk Estimation Subnet

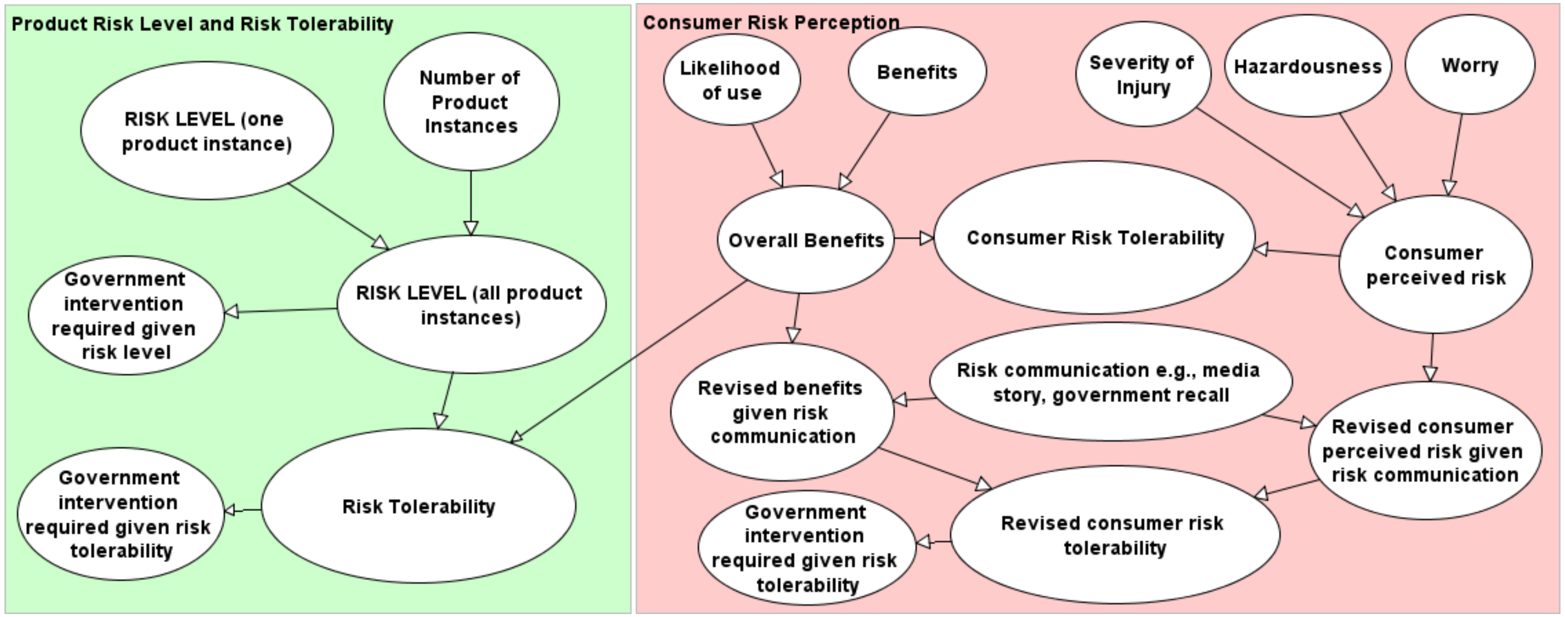

Product Risk Level and Risk Tolerability
RISK LEVEL (one product instance)
Number of Product Instances
RISK LEVEL (all product instances)
Government intervention required given risk level
Risk Tolerability
Government intervention required given risk tolerability
Consumer Risk Perception
Likelihood of use
Benefits
Severity of Injury
Hazardousness
Worry
Overall Benefits
Consumer Risk Tolerability
Consumer perceived risk
Revised benefits given risk communication
Risk communication e.g., media story, government recall
Revised consumer perceived risk given risk communication
Government intervention required given risk tolerability
Revised consumer risk tolerability

Figure C2. Consumer Product Risk Assessment BN – Risk Estimation, Risk Tolerability and Risk Perception Subnet – Population (all product instances)

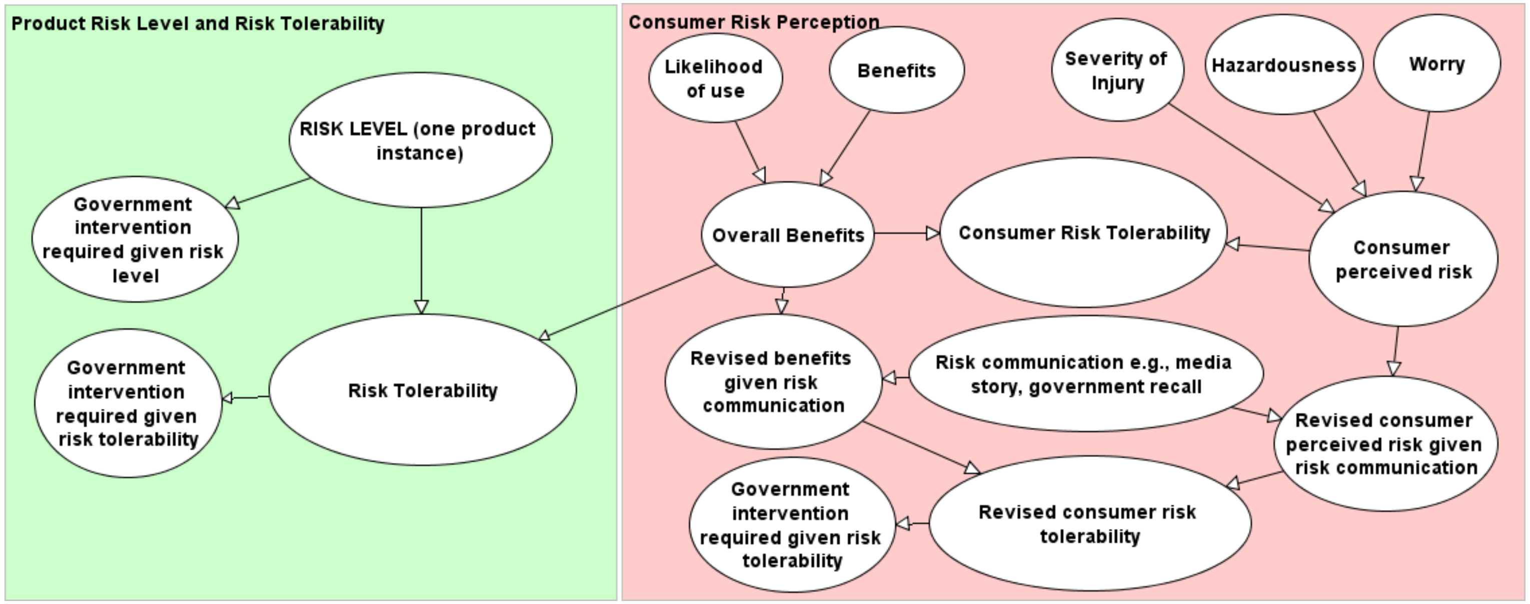

Product Risk Level and Risk Tolerability
RISK LEVEL (one product instance)
Government intervention required given risk level
Risk Tolerability
Government intervention required given risk tolerability
Consumer Risk Perception
Likelihood of use
Benefits
Severity of Injury
Hazardousness
Worry
Overall Benefits
Consumer Risk Tolerability
Consumer perceived risk
Revised benefits given risk communication
Risk communication e.g., media story, government recall
Revised consumer perceived risk given risk communication
Government intervention required given risk tolerability
Revised consumer risk tolerability

Figure C3. Consumer Product Risk Assessment BN – Risk Estimation, Risk Tolerability and Risk Perception Subnet – Individual/single product instance

C4 Model Assumptions

This section of Appendix C presents the model assumptions.

Model Assumptions:

1. Consumer perceived risk is dependent on three factors i.e., severity of injury, hazardousness and worry.
2. Benefits of the product is dependent on two factors i.e., likelihood of use and benefits.
3. Risk communication can influence risk perception of the product.
4. A single known type of hazard is investigated. In Section 8.6, we discuss combining the risk results of different hazards for a product.

C5 Instructions for using Consumer Product Risk Assessment BN

This section of Appendix C presents the instructions for using the consumer product risk assessment BN.

Instructions:

1. Define the scope and objectives of the analysis, including the hazards to be investigated.
2. Describe the device, including its requirements, functions, users, intended use, safety characteristics, and benefits.
3. Collate and organise other relevant information for the analysis:
    a. *Product testing information:* Information about the number of hazards observed in a set of demands during testing will allow the BN to estimate the probability of the hazard per demand. We define a demand as a measure of usage, e.g., single use, years etc.
    b. *Injury information:* Information about hazard occurrences and related injuries in the field will allow the BN to estimate the probability of the hazard or hazardous situation resulting in injury. Injury information can be obtained from hospitals and injury databases.
    c. *Manufacturer information:* Information such as manufacturer reputation will allow the BN to estimate the quality of the manufacturing process. Since the quality of the manufacturing process can influence the occurrence of hazards, it will be used to revise the

probability of the hazard per demand, especially in situations where there are little or no product testing data.

   d. *Product usage information*: Information about product usage e.g., frequency of use, and product age will allow the BN to revise the estimated failure (or hazard) rate and the overall risk as needed.
   e. *Product instances information*: Information such as the number of product instances available on the market will allow the BN to estimate the number of injuries and risk associated with the product.
   f. *Benefits and risk perception information:* Information such as the likelihood of use and severity of injury will allow the BN to estimate the benefits and perceived risk of the product.
   g. *Risk communication information:* Information relating to risk communication such as product recall, media stories etc.

4. Perform the analysis using the BN:
   a. Populate product testing information, benefits information, manufacturer information, product usage information, product instances information and injury information.
   b. Compute the risk and risk tolerability.
   c. Perform a consumer risk perception analysis: Populate risk perception information and risk communication information to estimate consumer perceived benefits, risk and risk tolerability for the product.

C6 Model Validation Results – AgenaRisk Screenshots

This section of Appendix C presents the model results for the risk assessment scenarios discussed in Section 8.5.

Figure C4 - BN Results for Teddy Bear Scenario 1

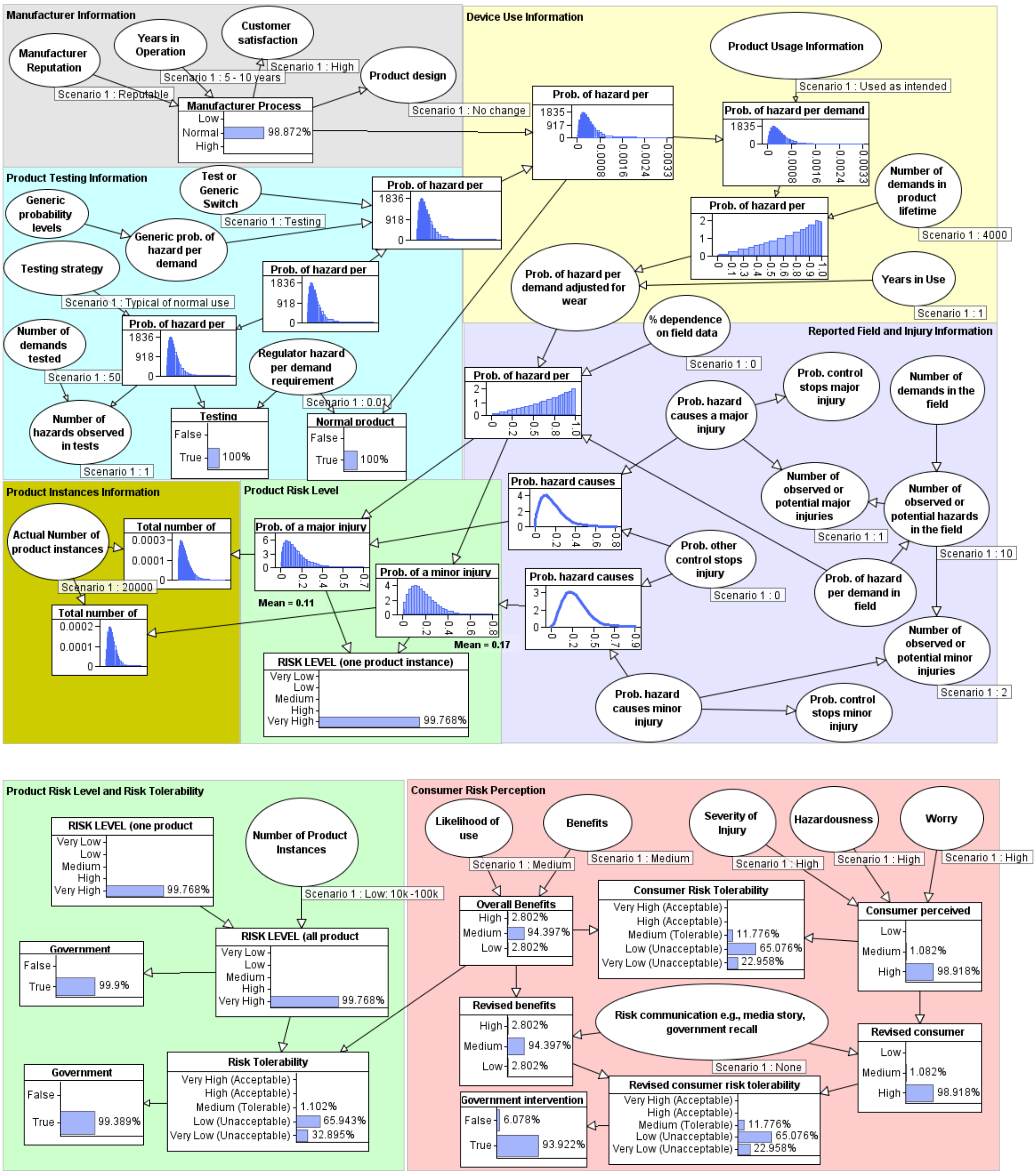
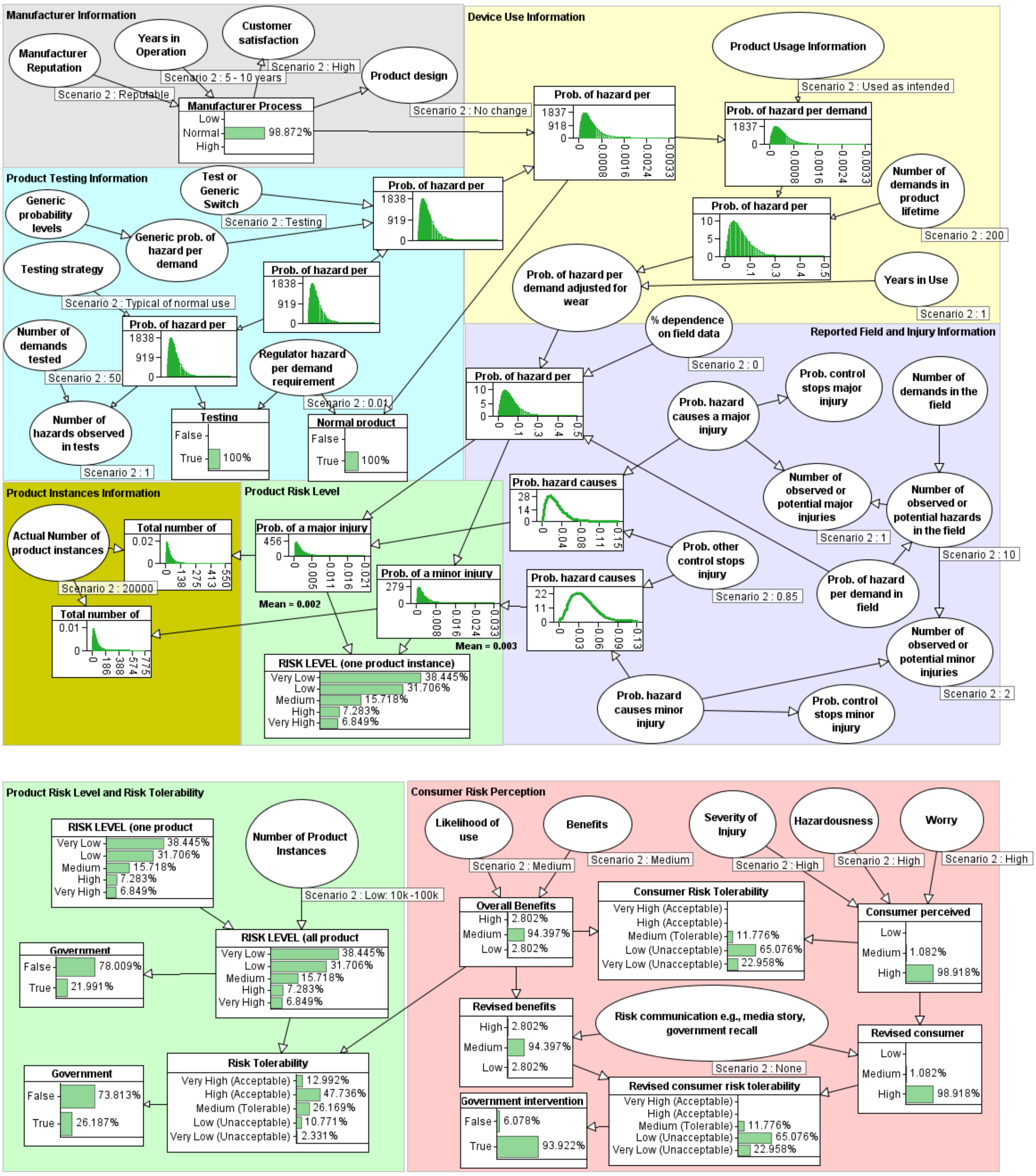


Figure C5 - BN Results for Teddy Bear Scenario 2



Manufacturer Information
Manufacturer Reputation
Years in Operation
Customer satisfaction
Scenario 2 : 5 - 10 years
Scenario 2 : High
Scenario 2 : Reputable
Product design
Manufacturer Process
Low
Normal 98.872%
High
Scenario 2 : No change
Device Use Information
Product Usage Information
Scenario 2 : Used as intended
Prob. of hazard per
Prob. of hazard per demand
Number of demands in product lifetime
Scenario 2 : 200
Prob. of hazard per demand adjusted for wear
Years in Use
Scenario 2 : 1
Product Testing Information
Test or Generic Switch
Scenario 2 : Testing
Generic probability levels
Generic prob. of hazard per demand
Testing strategy
Scenario 2 : Typical of normal use
Number of demands tested
Scenario 2 : 50
Number of hazards observed in tests
Scenario 2 : 1
Regulator hazard per demand requirement
Scenario 2 : 0.01
Testing
False
True 100%
Normal product
False
True 100%
% dependence on field data
Scenario 2 : 0
Reported Field and Injury Information
Prob. control stops major injury
Number of demands in the field
Prob. hazard causes a major injury
Number of observed or potential major injuries
Scenario 2 : 1
Number of observed or potential hazards in the field
Scenario 2 : 10
Prob. hazard causes
Prob. other control stops injury
Scenario 2 : 0.85
Prob. of hazard per demand in field
Number of observed or potential minor injuries
Scenario 2 : 2
Prob. hazard causes minor injury
Prob. control stops minor injury
Product Instances Information
Actual Number of product instances
Total number of
Scenario 2 : 20000
Product Risk Level
Prob. of a major injury
Mean = 0.002
Prob. of a minor injury
Mean = 0.003
RISK LEVEL (one product instance)
Very Low 38.445%
Low 31.706%
Medium 15.718%
High 7.283%
Very High 6.849%
Product Risk Level and Risk Tolerability
RISK LEVEL (one product
Number of Product Instances
Scenario 2 : Low: 10k -100k
RISK LEVEL (all product
Government
False 78.009%
True 21.991%
Risk Tolerability
Very High (Acceptable) 12.992%
High (Acceptable) 47.736%
Medium (Tolerable) 26.169%
Low (Unacceptable) 10.771%
Very Low (Unacceptable) 2.331%
Government
False 73.813%
True 26.187%
Consumer Risk Perception
Likelihood of use
Benefits
Severity of Injury
Hazardousness
Worry
Scenario 2 : Medium
Scenario 2 : Medium
Scenario 2 : High
Scenario 2 : High
Scenario 2 : High
Overall Benefits
High 2.802%
Medium 94.397%
Low 2.802%
Consumer Risk Tolerability
Very High (Acceptable)
High (Acceptable)
Medium (Tolerable) 11.776%
Low (Unacceptable) 65.076%
Very Low (Unacceptable) 22.958%
Consumer perceived
Low
Medium 1.082%
High 98.918%
Revised benefits
High 2.802%
Medium 94.397%
Low 2.802%
Risk communication e.g., media story, government recall
Scenario 2 : None
Revised consumer
Low
Medium 1.082%
High 98.918%
Revised consumer risk tolerability
Very High (Acceptable)
High (Acceptable)
Medium (Tolerable) 11.776%
Low (Unacceptable) 65.076%
Very Low (Unacceptable) 22.958%
Government intervention
False 6.078%
True 93.922%

Figure C6 - BN Results for Kettle Scenario 1

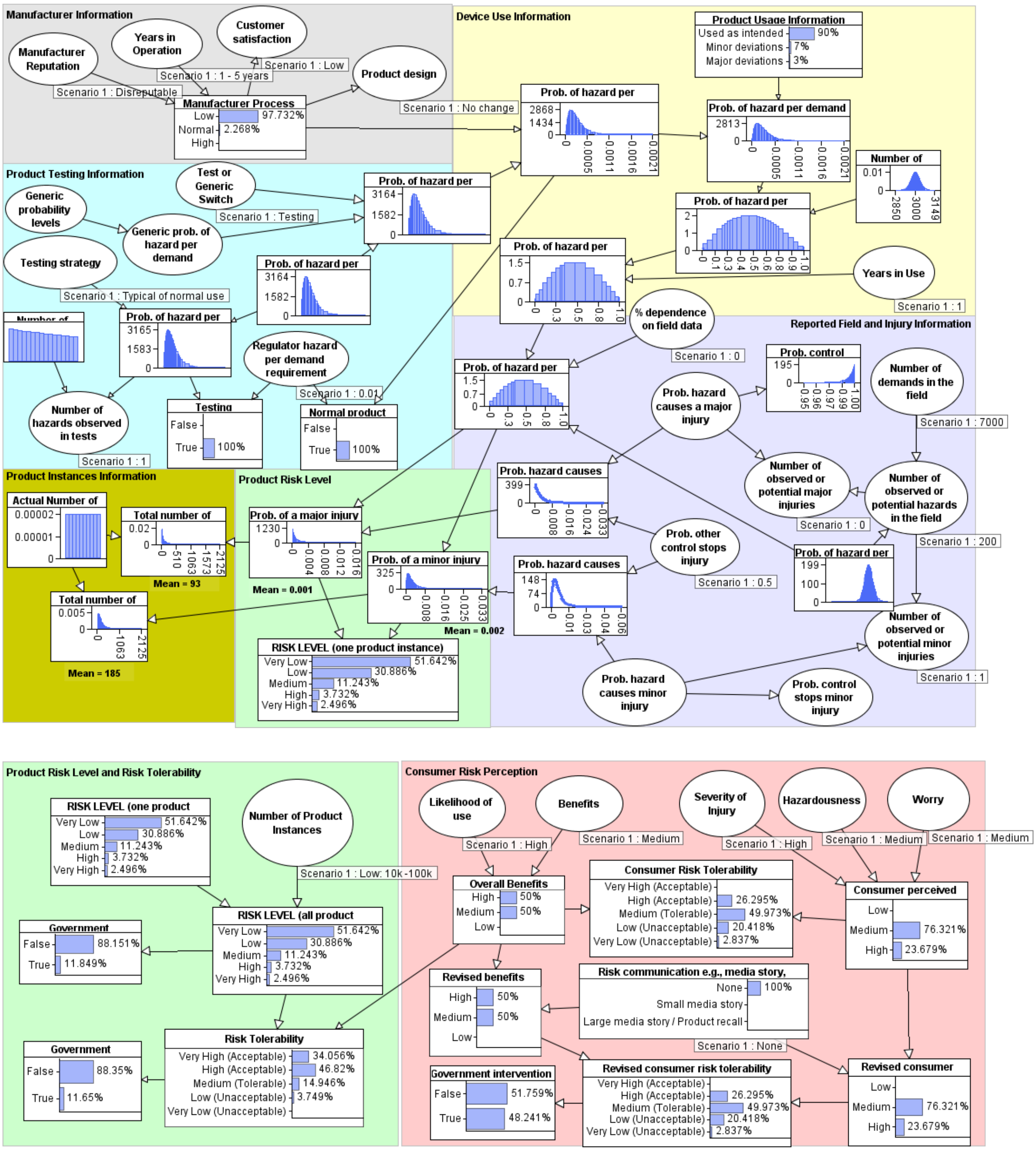
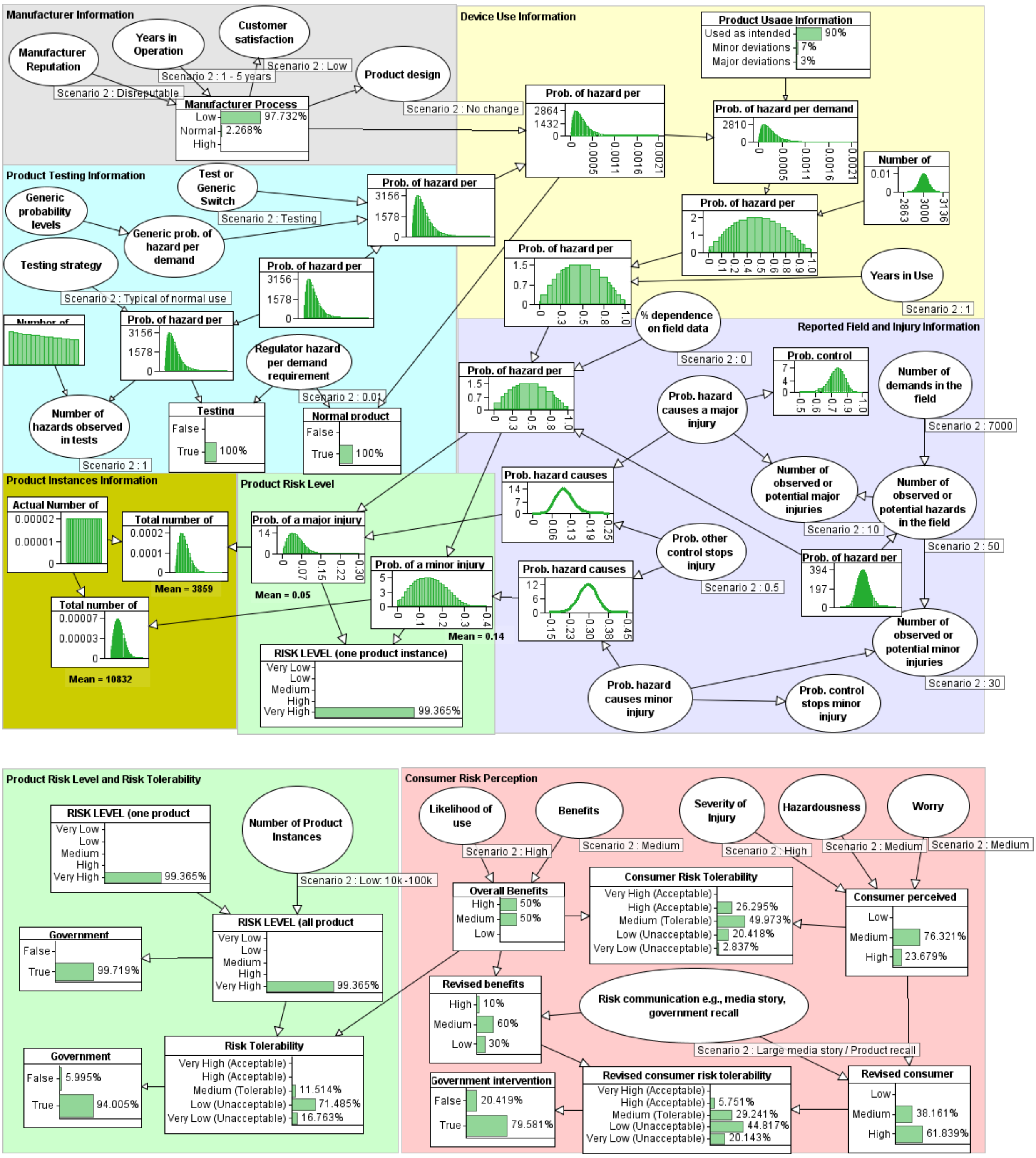


Figure C7 - BN Results for Kettle Scenario 2



Appendix D Chapter 9 Supplemental Material

D1 Study 1: Conceptual Framework

This section of Appendix D presents the conceptual framework for Study 1.

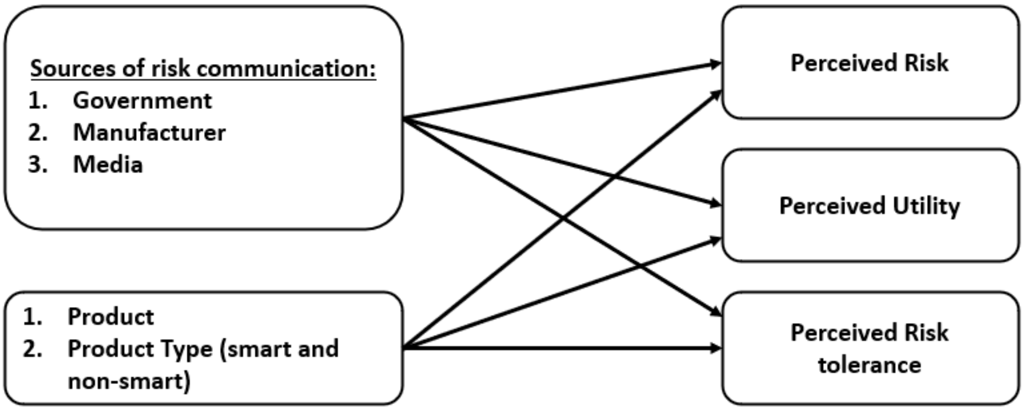


Figure D1. Conceptual framework for Study 1

D2 Study 1: BN models for two means hypothesis tests

This section of Appendix D presents the Bayesian network (BN) model, variables, and node probability tables (NPTs) for comparing two population means and distributions. The Bayesian approach includes the following steps:

1. Learn the population mean and variance from the sample mean and sample variance for each population using the BN model shown in Figure D2. This model uses the following theorem to learn the population distribution:

   $$Sample\ variance\ =\ Chisquared(n-1)\ x\ variance/(n-1)$$

   Where *n* is the sample size. See Table D1 for node probability tables (NPTs).

2. Determine the difference between the two populations by estimating the difference in the population means and distributions using the nodes *pop greater than pop1*, *pm greater than pm1*, and *population mean difference*.

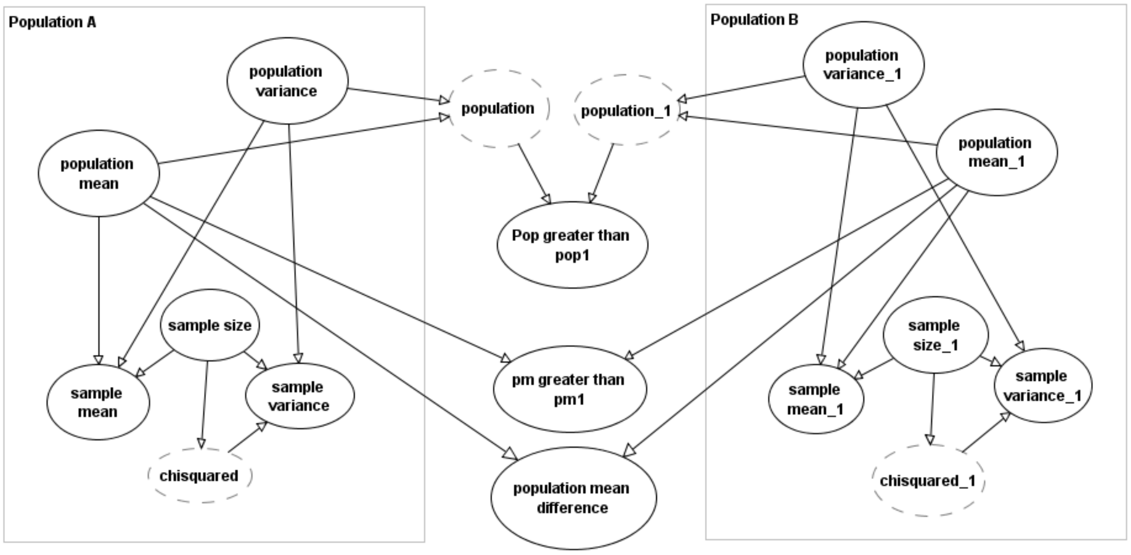


Figure D2. BN model used for two means hypothesis test

Table D1. BN Variables and NPTs for BN model used for two means hypothesis test

Variables	**Abbrev.**	**Node Probability Tables**
Sample size	n	Normal (0, 1000000)
Sample mean	sm	Normal (pm, pv/n)
Sample variance	sv	chisquared x pv/(n−1.0)
Population mean	pm	Normal (0, 1000000)
Population variance	pv	Normal (0, 1000000)
Chisquared	chisquared	Chi Squared(n−1.0)
Population	pop	Normal (pm, pv)
Population_1	pop1	Normal (pm_1, pv_1)
Pop greater than pop1	popcomparison	If (pop > pop_1, “True”, “False”)
PM greater than PM1	pmcomparison	If (pm > pm_1, “True”, “False”)
Population mean difference	pm_difference	pm−pm_1
Population variance_1	pv_1	Normal (0, 1000000)
Population mean_1	pm_1	Normal (0, 1000000)
Sample size_1	n_1	Normal (0, 1000000)

Sample mean_1	sm_1	Normal (pm_1, pv_1/n_1)
Sample variance_1	sv_1	chisquared1 × pv_1/(n_1−1.0)
Chisquared_1	chisquared1	Chi Squared(n_1−1.0)

The BN model shown in Figure D3 was used to investigate the interaction effects between gender, product, product type and risk communication source on perceived risk, utility and risk tolerance. The model NPTs was learnt from the study data.

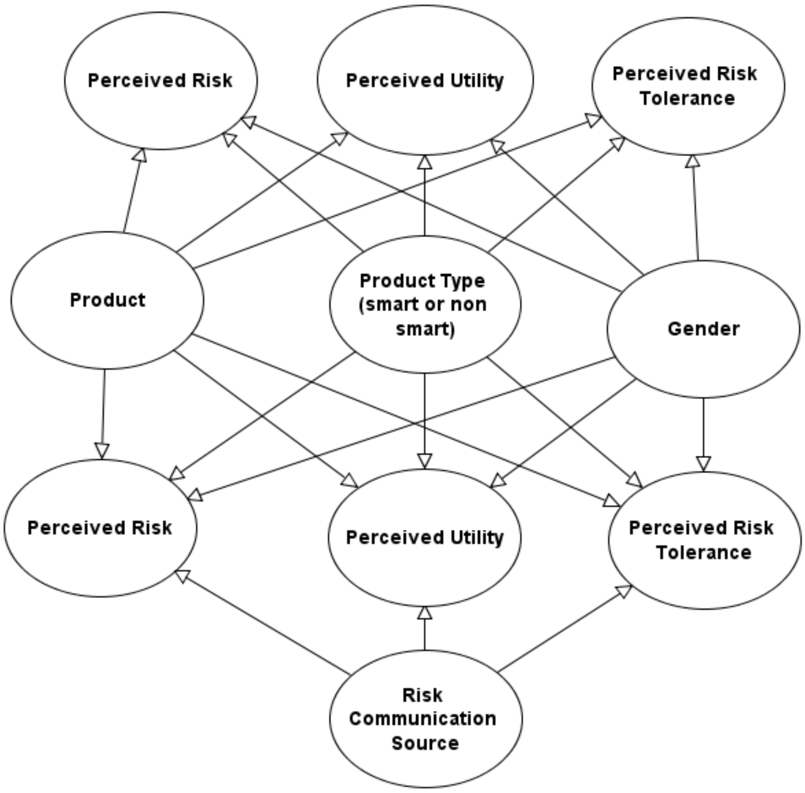


Figure D3. BN model used to investigate interaction effects between variables

D3 Study 1: Correlation Analysis

This section of Appendix D presents correlation analysis results for Study 1.

Experiment 1 Results

A correlation analysis revealed (see Figure D4) a negative correlation between risk and utility ratings (*r* = -0.25, *p* = 6.9e-7) and risk and risk tolerance ratings (*r* = -0.51, *p* = 4.9e-28). However, there was a positive correlation between utility and risk tolerance ratings (*r* = 0.31 *p* = 2.5e-10).

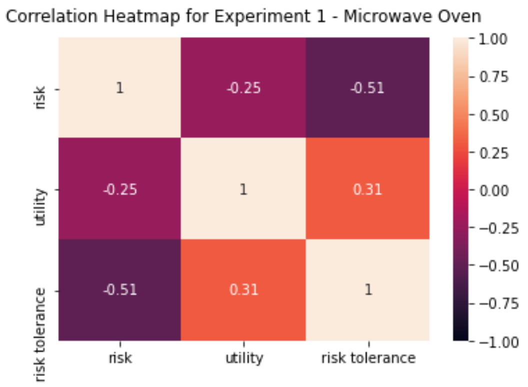


Figure D4. Dependent variables Correlation Heatmap for Experiment 1

Experiment 2 Results

Similar to Experiment 1, a correlation analysis revealed (see Figure D5) a negative correlation between risk and utility ratings (*r* = -0.25, *p* = 4.2e-7) and risk and risk tolerance ratings (*r* = -0.47, *p* = 5.6e-23). However, there was a positive correlation between utility and risk tolerance ratings (*r* = 0.35 *p* = 2.7e-13).

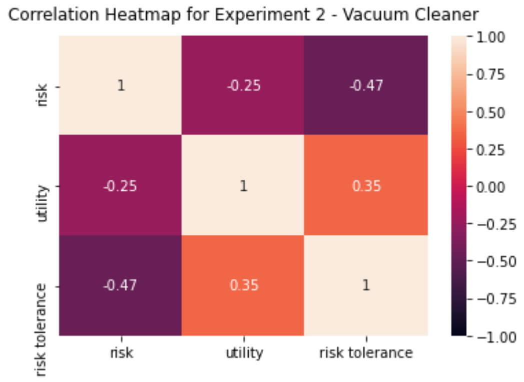


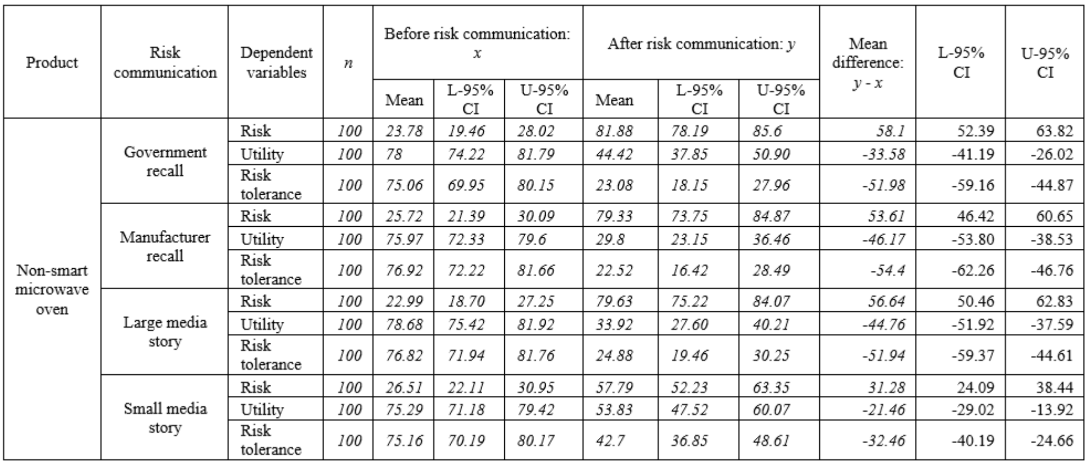
Figure D5. Dependent variables correlation Heatmap for Experiment 2

D4 Study 1: Effect of risk communication on risk perception

This section of Appendix D presents the results of the Bayesian two means hypothesis test for Study 1.

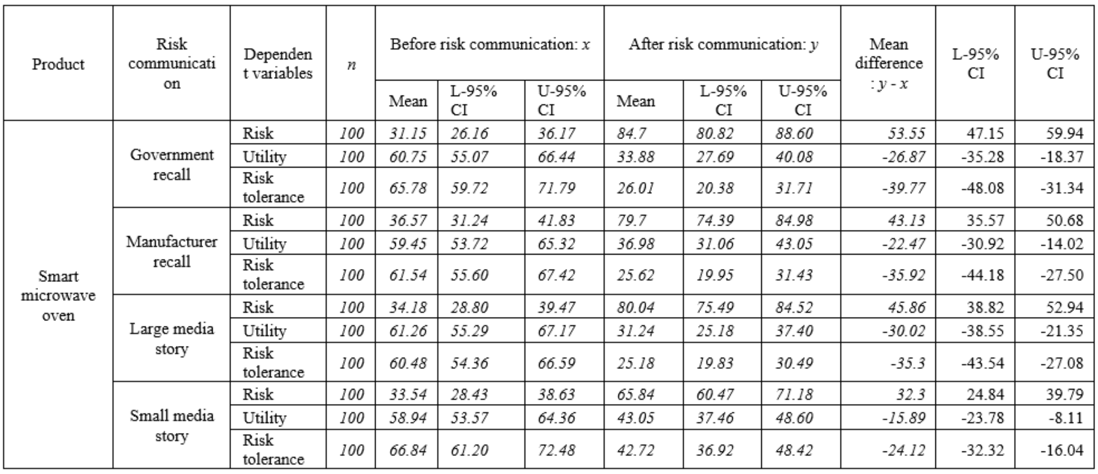
Experiment 1 Results

Table D2. Results of Bayesian two means hypothesis test for non-smart microwave oven



Product	Risk communication	Dependent variables	*n*	Before risk communication: *x*			After risk communication: *y*			Mean difference: *y - x*	L-95% CI	U-95% CI
				Mean	L-95% CI	U-95% CI	Mean	L-95% CI	U-95% CI			
Non-smart microwave oven	Government recall	Risk	100	23.78	19.46	28.02	81.88	78.19	85.6	58.1	52.39	63.82
		Utility	100	78	74.22	81.79	44.42	37.85	50.90	-33.58	-41.19	-26.02
		Risk tolerance	100	75.06	69.95	80.15	23.08	18.15	27.96	-51.98	-59.16	-44.87
	Manufacturer recall	Risk	100	25.72	21.39	30.09	79.33	73.75	84.87	53.61	46.42	60.65
		Utility	100	75.97	72.33	79.6	29.8	23.15	36.46	-46.17	-53.80	-38.53
		Risk tolerance	100	76.92	72.22	81.66	22.52	16.42	28.49	-54.4	-62.26	-46.76
	Large media story	Risk	100	22.99	18.70	27.25	79.63	75.22	84.07	56.64	50.46	62.83
		Utility	100	78.68	75.42	81.92	33.92	27.60	40.21	-44.76	-51.92	-37.59
		Risk tolerance	100	76.82	71.94	81.76	24.88	19.46	30.25	-51.94	-59.37	-44.61
	Small media story	Risk	100	26.51	22.11	30.95	57.79	52.23	63.35	31.28	24.09	38.44
		Utility	100	75.29	71.18	79.42	53.83	47.52	60.07	-21.46	-29.02	-13.92
		Risk tolerance	100	75.16	70.19	80.17	42.7	36.85	48.61	-32.46	-40.19	-24.66

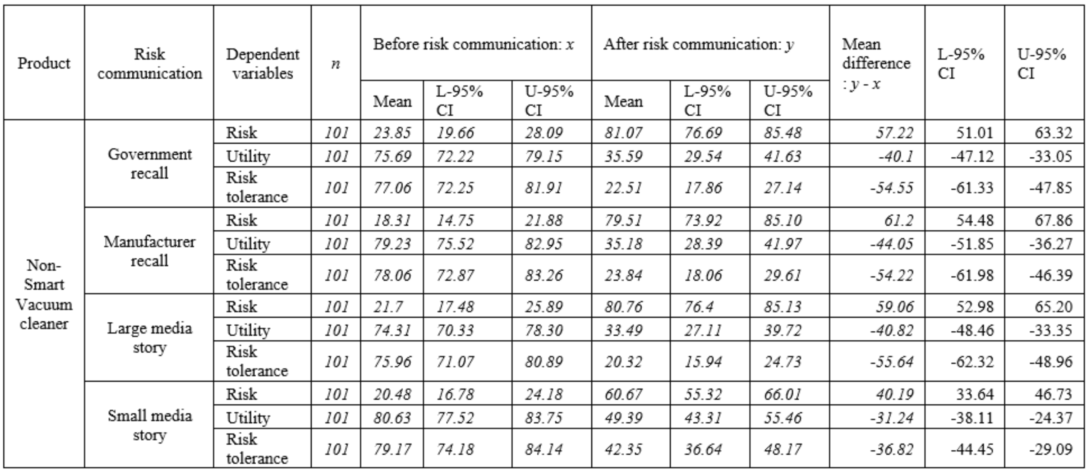
Table D3. Results of Bayesian two means hypothesis test for smart microwave oven



Product	Risk communication	Dependent variables	*n*	Before risk communication: *x*			After risk communication: *y*			Mean difference : *y - x*	L-95% CI	U-95% CI
				Mean	L-95% CI	U-95% CI	Mean	L-95% CI	U-95% CI			
Smart microwave oven	Government recall	Risk	100	31.15	26.16	36.17	84.7	80.82	88.60	53.55	47.15	59.94
		Utility	100	60.75	55.07	66.44	33.88	27.69	40.08	-26.87	-35.28	-18.37
		Risk tolerance	100	65.78	59.72	71.79	26.01	20.38	31.71	-39.77	-48.08	-31.34
	Manufacturer recall	Risk	100	36.57	31.24	41.83	79.7	74.39	84.98	43.13	35.57	50.68
		Utility	100	59.45	53.72	65.32	36.98	31.06	43.05	-22.47	-30.92	-14.02
		Risk tolerance	100	61.54	55.60	67.42	25.62	19.95	31.43	-35.92	-44.18	-27.50
	Large media story	Risk	100	34.18	28.80	39.47	80.04	75.49	84.52	45.86	38.82	52.94
		Utility	100	61.26	55.29	67.17	31.24	25.18	37.40	-30.02	-38.55	-21.35
		Risk tolerance	100	60.48	54.36	66.59	25.18	19.83	30.49	-35.3	-43.54	-27.08
	Small media story	Risk	100	33.54	28.43	38.63	65.84	60.47	71.18	32.3	24.84	39.79
		Utility	100	58.94	53.57	64.36	43.05	37.46	48.60	-15.89	-23.78	-8.11
		Risk tolerance	100	66.84	61.20	72.48	42.72	36.92	48.42	-24.12	-32.32	-16.04

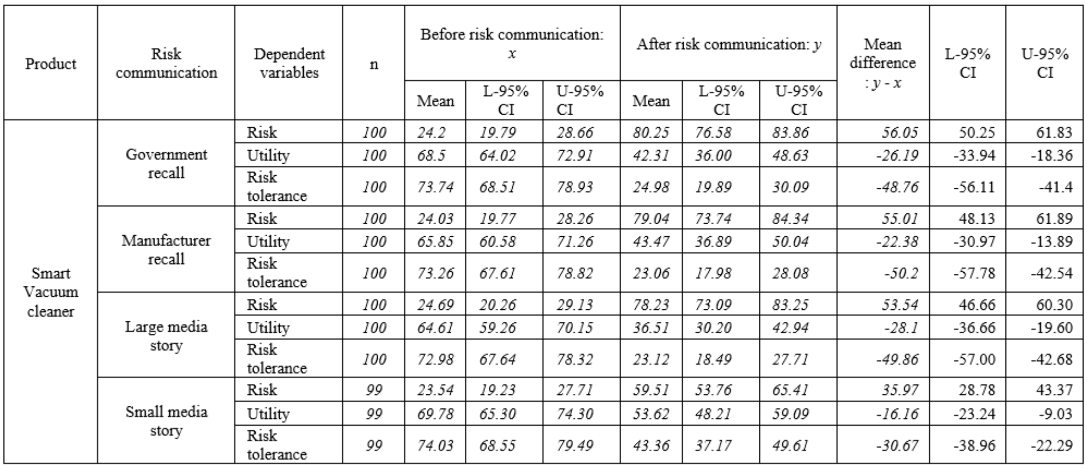
Experiment 2 Results

Table D4. Results of Bayesian two means hypothesis test for non-smart vacuum cleaner



Product	Risk communication	Dependent variables	*n*	Before risk communication: *x*			After risk communication: *y*			Mean difference : *y - x*	L-95% CI	U-95% CI
				Mean	L-95% CI	U-95% CI	Mean	L-95% CI	U-95% CI			
Non-Smart Vacuum cleaner	Government recall	Risk	*101*	*23.85*	*19.66*	*28.09*	*81.07*	*76.69*	*85.48*	*57.22*	51.01	63.32
		Utility	*101*	*75.69*	*72.22*	*79.15*	*35.59*	*29.54*	*41.63*	*-40.1*	-47.12	-33.05
		Risk tolerance	*101*	*77.06*	*72.25*	*81.91*	*22.51*	*17.86*	*27.14*	*-54.55*	-61.33	-47.85
	Manufacturer recall	Risk	*101*	*18.31*	*14.75*	*21.88*	*79.51*	*73.92*	*85.10*	*61.2*	54.48	67.86
		Utility	*101*	*79.23*	*75.52*	*82.95*	*35.18*	*28.39*	*41.97*	*-44.05*	-51.85	-36.27
		Risk tolerance	*101*	*78.06*	*72.87*	*83.26*	*23.84*	*18.06*	*29.61*	*-54.22*	-61.98	-46.39
	Large media story	Risk	*101*	*21.7*	*17.48*	*25.89*	*80.76*	*76.4*	*85.13*	*59.06*	52.98	65.20
		Utility	*101*	*74.31*	*70.33*	*78.30*	*33.49*	*27.11*	*39.72*	*-40.82*	-48.46	-33.35
		Risk tolerance	*101*	*75.96*	*71.07*	*80.89*	*20.32*	*15.94*	*24.73*	*-55.64*	-62.32	-48.96
	Small media story	Risk	*101*	*20.48*	*16.78*	*24.18*	*60.67*	*55.32*	*66.01*	*40.19*	33.64	46.73
		Utility	*101*	*80.63*	*77.52*	*83.75*	*49.39*	*43.31*	*55.46*	*-31.24*	-38.11	-24.37
		Risk tolerance	*101*	*79.17*	*74.18*	*84.14*	*42.35*	*36.64*	*48.17*	*-36.82*	-44.45	-29.09

Table D5. Results of Bayesian two means hypothesis test for smart vacuum cleaner



Product	Risk communication	Dependent variables	n	Before risk communication: *x*			After risk communication: *y*			Mean difference : *y - x*	L-95% CI	U-95% CI
				Mean	L-95% CI	U-95% CI	Mean	L-95% CI	U-95% CI			
Smart Vacuum cleaner	Government recall	Risk	*100*	*24.2*	*19.79*	*28.66*	*80.25*	*76.58*	*83.86*	*56.05*	50.25	61.83
		Utility	*100*	*68.5*	*64.02*	*72.91*	*42.31*	*36.00*	*48.63*	*-26.19*	-33.94	-18.36
		Risk tolerance	*100*	*73.74*	*68.51*	*78.93*	*24.98*	*19.89*	*30.09*	*-48.76*	-56.11	-41.4
	Manufacturer recall	Risk	*100*	*24.03*	*19.77*	*28.26*	*79.04*	*73.74*	*84.34*	*55.01*	48.13	61.89
		Utility	*100*	*65.85*	*60.58*	*71.26*	*43.47*	*36.89*	*50.04*	*-22.38*	-30.97	-13.89
		Risk tolerance	*100*	*73.26*	*67.61*	*78.82*	*23.06*	*17.98*	*28.08*	*-50.2*	-57.78	-42.54
	Large media story	Risk	*100*	*24.69*	*20.26*	*29.13*	*78.23*	*73.09*	*83.25*	*53.54*	46.66	60.30
		Utility	*100*	*64.61*	*59.26*	*70.15*	*36.51*	*30.20*	*42.94*	*-28.1*	-36.66	-19.60
		Risk tolerance	*100*	*72.98*	*67.64*	*78.32*	*23.12*	*18.49*	*27.71*	*-49.86*	-57.00	-42.68
	Small media story	Risk	*99*	*23.54*	*19.23*	*27.71*	*59.51*	*53.76*	*65.41*	*35.97*	28.78	43.37
		Utility	*99*	*69.78*	*65.30*	*74.30*	*53.62*	*48.21*	*59.09*	*-16.16*	-23.24	-9.03
		Risk tolerance	*99*	*74.03*	*68.55*	*79.49*	*43.36*	*37.17*	*49.61*	*-30.67*	-38.96	-22.29

D5 Study 1: The effect of demographics on risk perception

This section of Appendix D presents the supplementary results for the effect of demographics on risk perception for Study 1.

Table D6. Results of Bayesian two means hypothesis test for gender

Product	Dependent variables	Women: *x*				Men: *y*				Mean difference: *y* - *x*	L-95% CI	U-95% CI
		n	Mean	L-95% CI	U-95% CI	*n*	Mean	L-95% CI	U-95% CI			
Non-smart microwave oven	Risk	*127*	*23.41*	*19.84*	*27.23*	*70*	*27.09*	*21.42*	*32.82*	*3.68*	-3.12	10.52
Smart microwave oven	Risk	*136*	*35.1*	*30.64*	*39.49*	*61*	*31.33*	*24.5*	*38.02*	*-3.77*	-12.01	4.33
Non-smart vacuum cleaner	Risk	*118*	*20.98*	*17.32*	*24.68*	*80*	*21*	*16.49*	*25.56*	*0.02*	-5.91	5.96
Smart vacuum cleaner	Risk	*136*	*26.15*	*22.43*	*29.87*	*62*	*19.71*	*14.26*	*25.26*	*-6.44*	-13.1	0.31

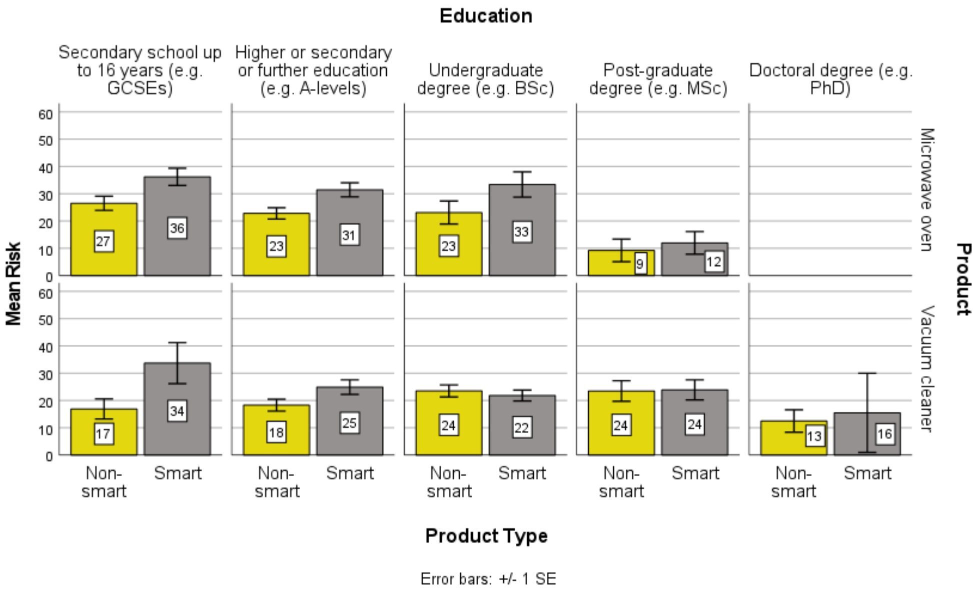


Figure D6. Mean perceived risk for products by Education Level

D6 Study 1: Interaction Effects

This section of Appendix D presents the interaction effects for Study 1.

Experiment 1 Results

For the smart microwave oven, before a large media story, the perceived risk for women (*Median* = 34, IQR [17, 50]) was similar to men (*Median* = 31, IQR [14, 48]) and the perceived utility for women (*Median* = 62, IQR [43, 81]) was greater compared to men (*Median* = 54, IQR [36, 72]). After the large media story, the perceived risk for women was greater (*Median* = 83, IQR [68, 97]) compared to men (*Median* = 72, IQR [58, 87]). The difference in perceived risk between men and women after the large media story though the evidence was not strong, can be explained by the inverse relationship between risk and utility since the perceived utility for women (*Median* = 28, IQR [8, 47]) was lesser compared to men (*Median* = 34, IQR [15,52]) after the large media story.

Experiment 2 Results

For the smart vacuum cleaner, before the government recall, the perceived risk for women (*Median* = 26, IQR [12, 40]) was similar to men (*Median* = 20, IQR [6, 34]) and the perceived utility for women (*Median* = 67, IQR [50, 84]) was the same as men (*Median* = 67, IQR [54, 79]). After the government recall, the perceived risk for women was greater (*Median* = 82 [72, 92]) compared to men (*Median* = 74, IQR [61, 88]). The difference in perceived risk between men and women after the government recall though the evidence was not strong, may be due to the inverse relationship between risk and utility since the perceived utility after the government recall was slightly less for women (*Median* = 42, IQR [24, 63]) compared to men (*Median* = 44, IQR [24, 65]).

D7 Study 2: Study 2 Products

This section of Appendix D presents the two products investigated in Study 2. Please note that TENCIX is a hypothetical brand.

TENCIX Microwave Oven

Recommended Retail Price (RRP): £90

Product Specification	
• 24L Capacity • Touch operated • LED Display • Modern handle-less design • Electronic timer • Child lock feature	• Grill and microwave settings. • 5 power levels for a wide range of cooking requirements. • Power output: 800W • Eco-mode • Warranty: 2 years

TENCIX Carbon Monoxide Detector

Recommended Retail Price (RRP): £20

Product Specification	
• Carbon monoxide alarm • Continuously monitors carbon monoxide levels. • Peak carbon monoxide level memory feature • Suitable for ceiling and wall installation	• Piercing 85dB alarm • Test and reset button: Allow you to test the alarm function and silence the alarm • Battery-powered • Warranty: 2 years

D8 Study 2: Interaction Effects Plots

This section of Appendix D presents the interaction effects for Study 2.

The interaction plots in Figures D7-D9 showed that overall, non-compliance information decreased benefit scores, increased dread scores and decreased WTP scores. However, this effect was dependent on the reliability of the source. Non-compliance information from a reliable source had a greater effect on the change in benefit, dread and WTP scores compared to non-compliance information from an unreliable source. The interaction plots also showed little or no change in benefit, dread and WTP scores, given compliance information from a reliable source. However, compliance information from an unreliable source slightly increased dread scores and slightly decreased WTP scores. For more detailed information, see Table D7. Also, see Figure D10 for differences between products.

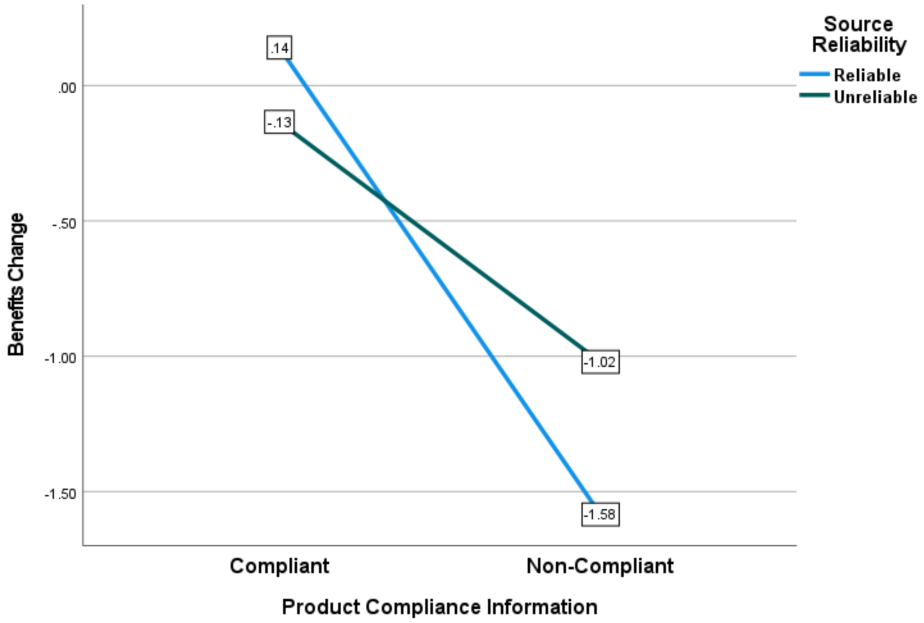


Figure D7 Mean Benefits Change by Product Compliance Information and Source Reliability

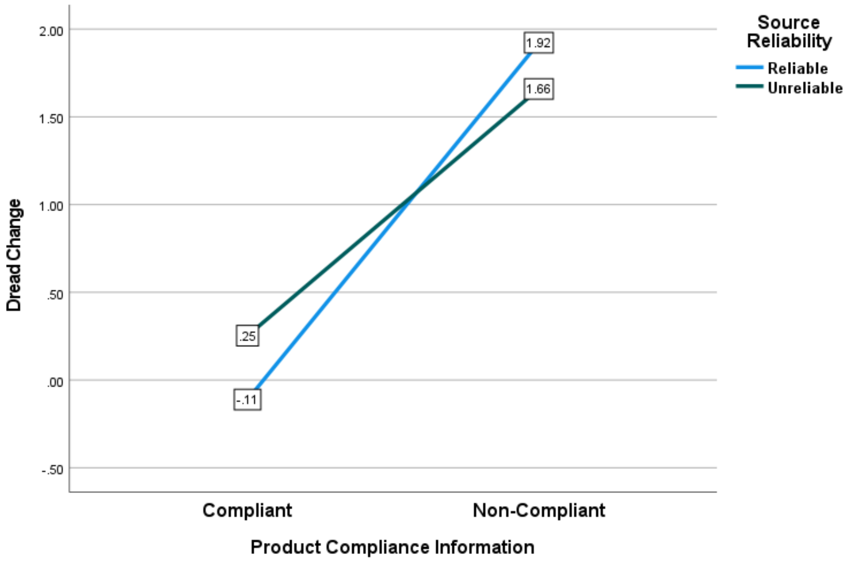


Figure D8 Mean Dread Change by Product Compliance Information and Source Reliability

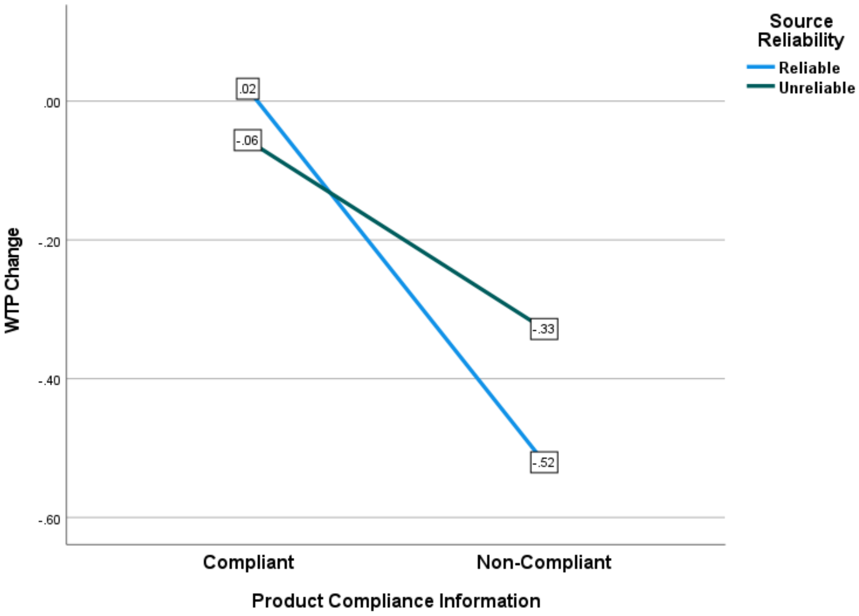


Figure D9 Mean WTP Change by Product Compliance Information and Source Reliability

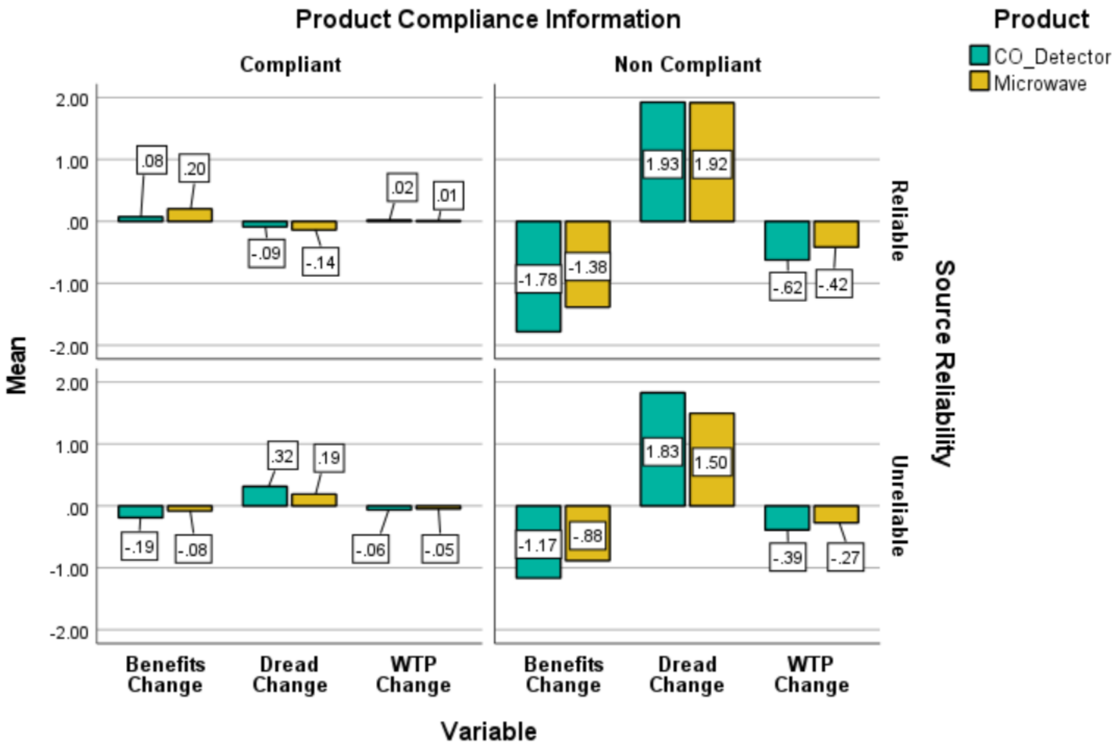


Figure D10 Differences in change in benefits, dread and WTP between products

Table D7. Interaction effect between product compliance information and source reliability on change in benefits, dread and WTP.

Variables	Product Compliance Information	Source Reliability	Estimate	l-95% CI	u-95% CI
Benefits Change	Compliant	Reliable	0.14	-0.02	0.3
	Non-Compliant	Reliable	-1.58	-1.75	-1.42
	Compliant	Unreliable	-0.13	-0.3	0.03
	Non-Compliant	Unreliable	-1.02	-1.18	-0.86
Dread Change	Compliant	Reliable	-0.11	-0.25	0.03
	Non-Compliant	Reliable	1.92	1.78	2.07
	Compliant	Unreliable	0.25	0.1	0.4
	Non-Compliant	Unreliable	1.66	1.51	1.8
WTP Change	Compliant	Reliable	0.02	-0.03	0.07
	Non-Compliant	Reliable	-0.52	-0.57	-0.47
	Compliant	Unreliable	-0.06	-0.11	-0.01
	Non-Compliant	Unreliable	-0.33	-0.38	-0.28

Increase	🟩
Decrease	🟦
No Change	

D9 Study 2: Bayesian Regression Modelling

This section of Appendix D presents the models used for data analysis in Study 2.

We investigated the study hypotheses using the Bayesian approach to regression analysis. We developed four Bayesian regression models using R [247] and the R package *brms* for Bayesian regression modelling [248]:

Model 1: $brm(mvbind(T1\ Benefits, T1\ Dread, T1\ Pay) \sim (GRID\ +\ GROUP\ +\ GRIP + Gender\ +\ Age + Children\ +\ Product\ ))$

We used Model 1 to estimate the mean scores for benefits, dread and willingness to pay at $T1$ (i.e., before manipulations) for predictors and the differences between them.

Model 2: $brm(mvbind(\Delta\ Benefits\ , \Delta\ Dread, \Delta\ Pay) \sim (GRIP\ +\ GROUP\ +\ GRID\ +\ Gender\ +\ Age\ +\ Children) \times (Product\ +\ Product\ Compliance\ +\ Source\ Reliability)\ +\ ((Product\ +\ Product\ Compliance\ +\ Source\ Reliability)\string^2)\ +\ (Product\ \times\ Product\ Compliance\ \times Source\ Reliability))$

We used Model 2 to estimate the mean change (Δ) in benefits, dread, and willingness to pay (WTP) scores for predictors, their interactions and the differences between them. The change (Δ) in benefits, dread and willingness to pay scores was computed as $T2 - T1$, where $T1$ are the scores before manipulations and $T2$ are the scores after manipulations. This model was used to investigate Hypothesis 1.

Model 3: $brm(mvbind(RTMIN, RTSUM) \sim (GRIP\ +\ GROUP\ +\ GRID\ +\ Gender\ +\ Age\ +\ Children) \times (Product\ + Product\ \ Compliance\ +\ Source\ Reliability)\ +\ ((Product\ +\ Product\ Compliance\ +\ Source\ Reliability)\string^2)\ +\ (Product\ \times\ Product\ Compliance\ \times\ Source\ Reliability))$

We used Model 3 to investigate risk tolerance (RT) by estimating the mean for risk tolerance sum (RTSUM) and risk tolerance min (RTMIN) for predictors, their interactions and the differences between them. Risk tolerance consists of two dimensions, i.e., benefits and dread, which change over time. Hence, RTSUM was computed as $\Delta\ benefits + \ \Delta\ dread,$ and RTMIN was computed as $\Delta\ dread - \Delta\ benefits$. High scores for RTSUM indicated high risk tolerance, whereas high scores for RTMIN indicated the effect of manipulations. This model was also used to investigate Hypothesis 1.

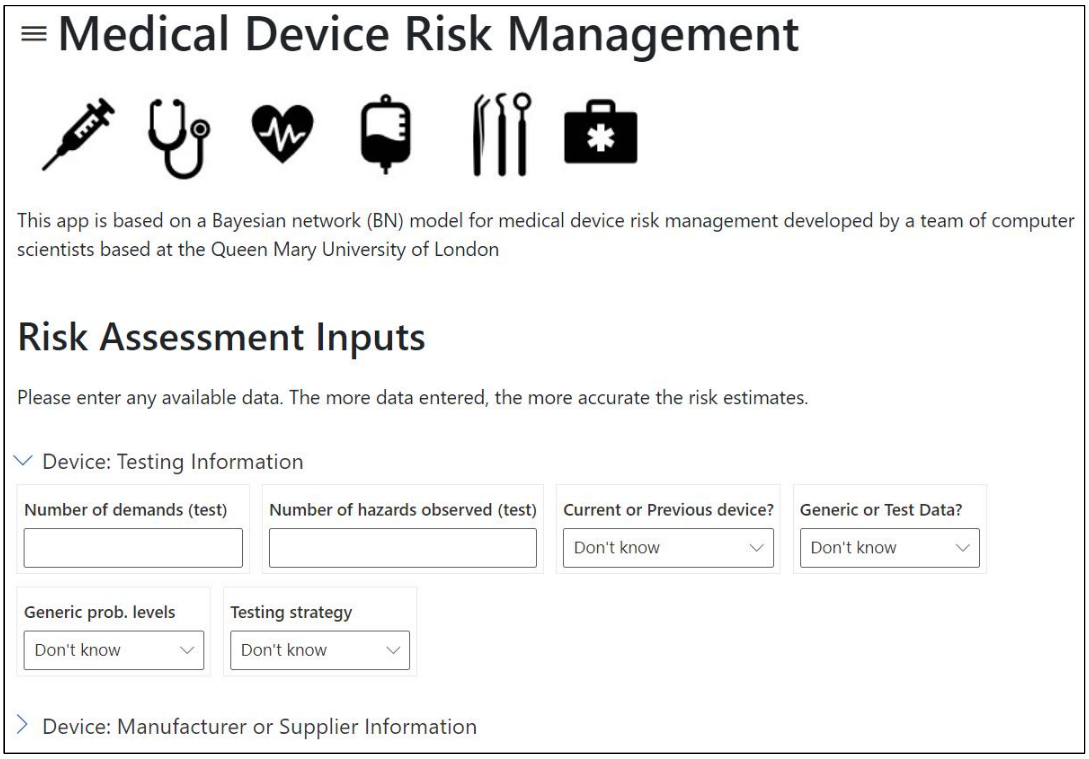
Model 4: $brm(mvbind(\Delta\ Benefits\ , \Delta\ Dread, \Delta\ Pay) \sim 0\ +\ Communication\ scenario)$

We used Model 4 to estimate the mean for Δ benefits, Δ dread, and Δ willingness to pay for the communication scenarios and the differences between them. The communication scenarios combined product compliance and source reliability. This model was used to investigate Hypotheses 2-5.

For each model, we used the default priors of the *brms* package [248]. We ran four sampling chains for 10000 iterations with a warm-up period of 5000 iterations, which resulted in 20000 samples for each parameter tuple. We reported the expected mean values under the posterior distribution and their 95% confidence intervals (CI).

Appendix E Chapter 10 Supplemental Material

In this section of the Appendix, we present screenshots of the web-based application for medical device risk management.



≡ Medical Device Risk Management

This app is based on a Bayesian network (BN) model for medical device risk management developed by a team of computer scientists based at the Queen Mary University of London

Risk Assessment Inputs

Please enter any available data. The more data entered, the more accurate the risk estimates.

Device: Testing Information

Number of demands (test):

Number of hazards observed (test):

Current or Previous device? Don't know

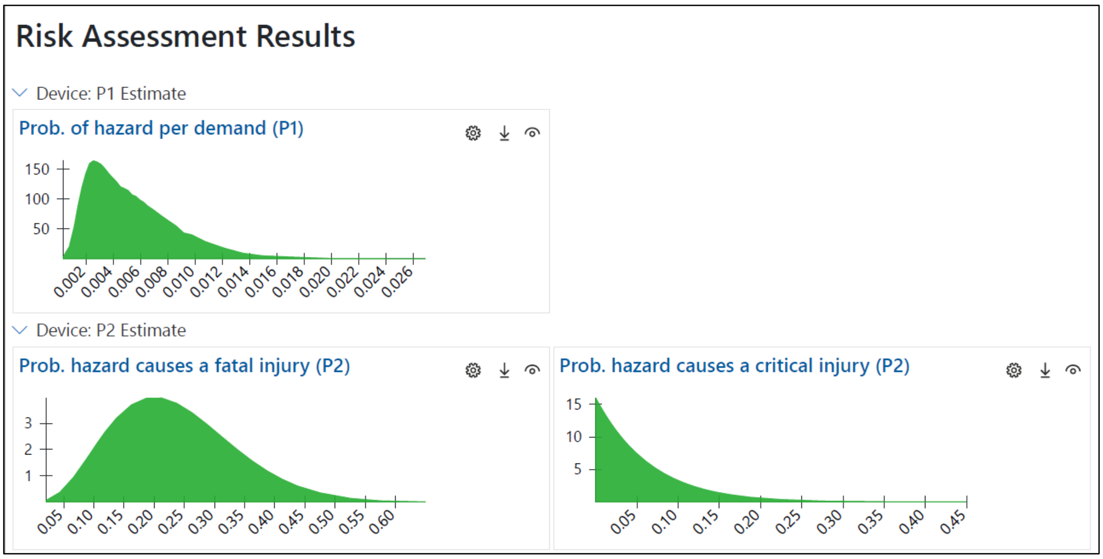
Generic or Test Data? Don't know

Generic prob. levels: Don't know

Testing strategy: Don't know

Device: Manufacturer or Supplier Information

Figure E1. Web application with input fields



Risk Assessment Results

Device: P1 Estimate

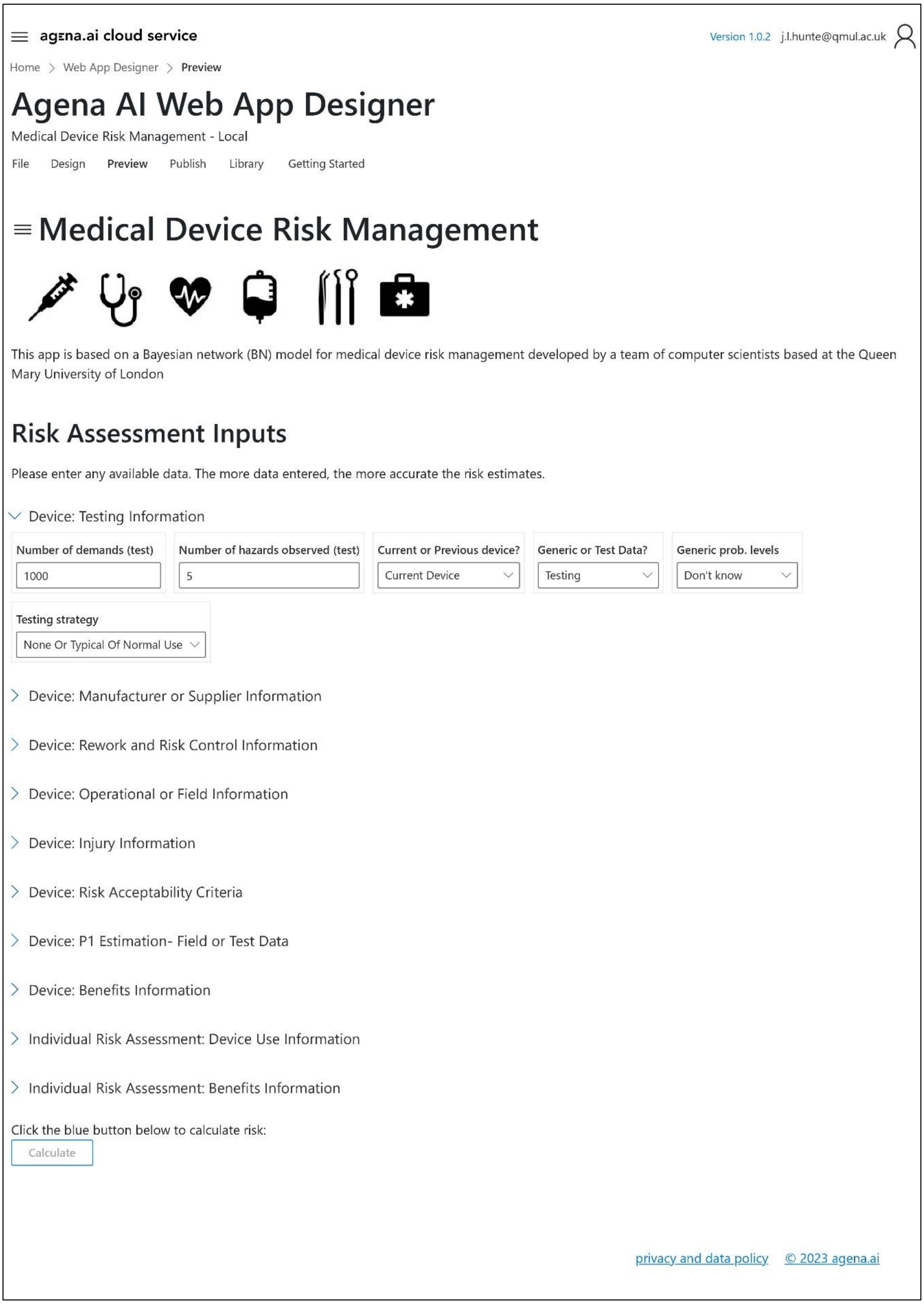
Prob. of hazard per demand (P1)

Device: P2 Estimate

Prob. hazard causes a fatal injury (P2)

Prob. hazard causes a critical injury (P2)

Figure E2. Web application results



Agena AI Web App Designer

Medical Device Risk Management - Local

Medical Device Risk Management

This app is based on a Bayesian network (BN) model for medical device risk management developed by a team of computer scientists based at the Queen Mary University of London

Risk Assessment Inputs

Please enter any available data. The more data entered, the more accurate the risk estimates.

Device: Testing Information

Number of demands (test): 1000

Number of hazards observed (test): 5

Current or Previous device?: Current Device

Generic or Test Data?: Testing

Generic prob. levels: Don't know

Testing strategy: None Or Typical Of Normal Use

Device: Manufacturer or Supplier Information

Device: Rework and Risk Control Information

Device: Operational or Field Information

Device: Injury Information

Device: Risk Acceptability Criteria

Device: P1 Estimation- Field or Test Data

Device: Benefits Information

Individual Risk Assessment: Device Use Information

Individual Risk Assessment: Benefits Information

Click the blue button below to calculate risk:

Figure E3 Complete web application