NOTE A positive focus can encourage greater ownership and participation.

Limitations include the following.

- The separation of causal factors into major categories at the start of the analysis means that interactions between the categories might not be considered adequately.
- Potential causes not covered by the categories selected are not identified.

B.3.3.6 Reference documents

[30] ISHIKAWA, K. Guide to Quality Control

See also IEC 62740 [16] for other causal analysis techniques.

B.4 Techniques for analysing controls

B.4.1 General

The techniques in Clause B.4 can be used to check whether controls are appropriate and adequate.

Bow tie analysis (B.4.2) and LOPA (B.4.4) identify the barriers between a source of risk and its possible consequences and can be used to check that the barriers are sufficient.

HACCP (B.4.3) seeks points in a process where conditions can be monitored and controls introduced when there is an indication that the conditions are changing.

Event tree analysis (B.5.6) can also be used as a quantitative means of controls analysis by calculating the influence of different controls on the probability of consequences.

Any causal analysis technique can be used as a basis for checking that each cause is controlled.

B.4.2 Bow tie analysis

B.4.2.1 Overview

A bow tie is a graphical depiction of pathways from the causes of an event to its consequences. It shows the controls that modify the likelihood of the event and those that modify the consequences if the event occurs. It can be considered as a simplified representation of a fault tree or success tree (analysing the cause of an event) and an event tree (analysing the consequences). Bow tie diagrams can be constructed starting from fault and event trees, but are more often drawn directly by a team in a workshop scenario.

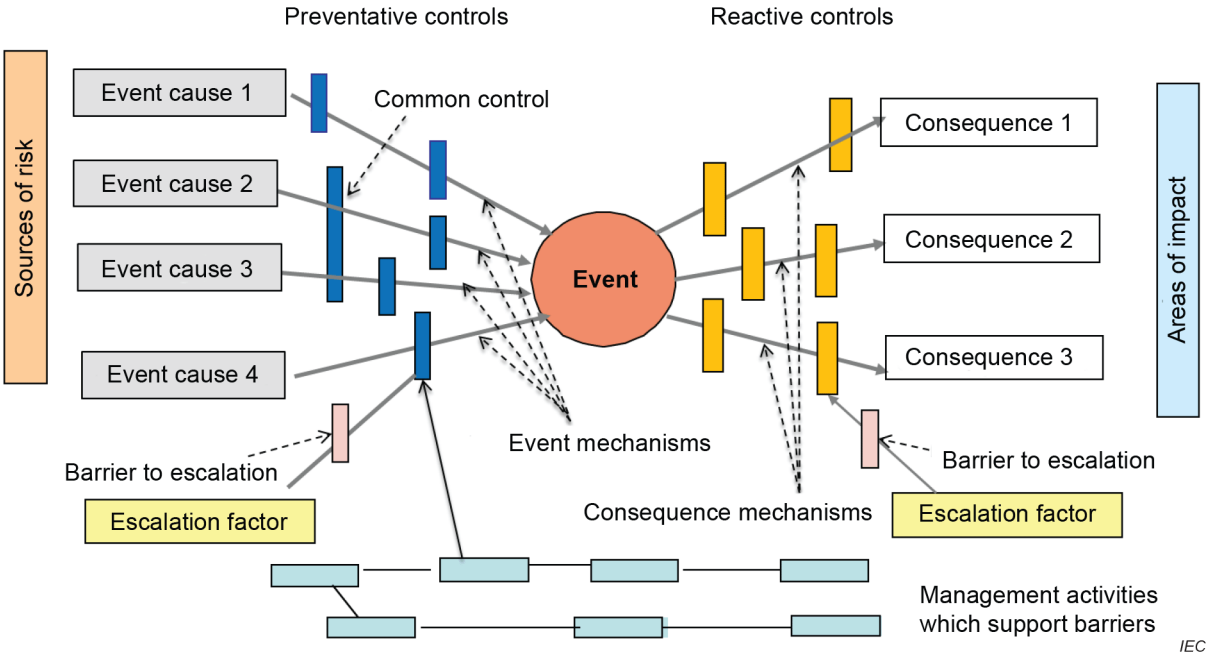

Figure B.2 – Example of Bowtie

The bow tie is drawn as follows.

- The event of interest is represented by the central knot of the bow tie, see Figure B.2.
- Sources of risk (or hazards/threats in a safety context) are listed on the left hand side of the knot and joined to the knot by lines representing the different mechanisms by which sources of risk can lead to the event.
- Barriers or controls for each mechanism are shown as vertical bars across the lines.
- On the right-hand side of the knot lines are drawn to radiate out from the event to each potential consequence.
- After the event vertical bars represent reactive controls or barriers that modify consequences.
- Factors that might cause the controls to fail (escalation factors) are added, together with controls for the escalation factors.
- Management functions which support controls (such as training and inspection) can be shown under the bow tie and linked to the respective control.

Some level of quantification of a bow tie diagram can be possible where pathways are independent, the probability of a particular consequence or outcome is known and the probability that a control will fail can be estimated. However, in many situations, pathways and barriers are not independent, and controls may be procedural and their effectiveness uncertain. Quantification is often more appropriately carried out using fault tree analysis (B.5.7) and event tree analysis (B.5.6) or LOPA (B.4.4).

B.4.2.2 Use

Bow tie analysis is used to display and communicate information about risks in situations where an event has a range of possible causes and consequences. It can be used to explore in detail the causes and consequences of events that are recorded in a simple form in a risk register (B.10.2). It is particularly used for analysing events with more serious consequences. A bow tie is used when assessing controls to check that each pathway from cause to event and event to consequence has effective controls, and that factors that could cause controls to fail (including management systems failures) are recognized. It can be used as the basis of a means to record information about a risk that does not fit the simple linear representation of a risk register. It

can be used proactively to consider potential events and also retrospectively to model events that have already occurred.

The bow tie is used when the situation does not warrant the complexity of a full fault tree analysis and event tree analysis but is more complex than can be represented by a single cause-event-consequence pathway.

For some situations cascading bow ties can be developed where the consequences of one event become the cause of the next.

B.4.2.3 Input

Input includes information about the causes and consequences of the pre-defined event, and the controls that might modify it. This information may be taken from the output of techniques to identify risks and controls or from the experience of individuals.

B.4.2.4 Output

The output is a simple diagram showing main risk pathways, the controls in place, and the factors that might lead to control failure. It also shows potential consequences and the measures that can be taken after the event has occurred to modify them.

B.4.2.5 Strengths and limitations

Strengths of bow tie analysis include the following.

- It is simple to understand and gives a clear pictorial representation of an event and its causes and consequences.
- It focuses attention on controls which are supposed to be in place and their effectiveness.
- It can be used for desirable consequences as well as undesirable ones.
- It does not need a high level of expertise to use.

Limitations include the following.

- A bow tie cannot depict a situation where pathways from causes to the event are not independent (i.e. where there would be AND gates in a fault tree).
- It can over-simplify complex situations particularly where quantification is attempted.

B.4.2.6 Reference documents

[31] LEWIS, S. SMITH, K., *Lessons learned from real world application of the bow-tie method*. [31]

[32] HALE, A. R., GOOSSENS L.H.J., ALE, B.J.M., BELLAMY L.A. POST J. *Managing safety barriers and controls at the workplace*

[33] MCCONNELL, P. and DAVIES, M. *Scenario Analysis under Basel II*

B.4.3 Hazard analysis and critical control points (HACCP)

B.4.3.1 Overview

Hazard analysis and critical control points (HACCP) was developed to ensure food safety for the NASA space program but can be used for non-food processes or activities. The technique provides a structure for identifying sources of risk (hazards or threats) and putting controls in place at all relevant parts of a process to protect against them. HACCP is used at operational levels although its results can support the overall strategy of an organization. HACCP aims to ensure that risks are minimized by monitoring and by controls throughout a process rather than through inspection at the end of the process.

HACCP consists of the following seven principles:

1) identify hazards, the factors which influence the risk and possible preventive measures;
2) determine the points in the process where monitoring is possible and the process can be controlled to minimize threats (the critical control points or CCPs);
3) establish critical limits for the parameters which are to be monitored, i.e. each CCP should operate within specific parameters to ensure the risk is controlled;
4) establish the procedures to monitor critical limits for each CCP at defined intervals;
5) establish corrective actions to be used when the process falls outside established limits;
6) establish verification procedures;
7) implement record keeping and documentation procedures for each step.

B.4.3.2 Use

HACCP is a requirement in most countries for organizations operating anywhere within the food chain, from harvesting to consumption, to control risks from physical, chemical or biological contaminants.

It has been extended for use in manufacture of pharmaceuticals, medical devices and in other areas where the biological, chemical and physical risks are inherent to the organization.

The principle of the technique is to identify sources of risk related to the quality of the output of a process, and to define points in that process where critical parameters can be monitored and sources of risk controlled. This can be generalized to many other processes, including for example financial processes.

B.4.3.3 Inputs

Inputs include:

- a basic flow diagram or process diagram;
- information on sources of risk that might affect the quality, safety or reliability of the product or process output;
- information on the points in the process where indicators can be monitored and controls can be introduced.

B.4.3.4 Outputs

Outputs include records, including a hazard analysis worksheet and a HACCP plan.

The hazard analysis worksheet lists for each step of the process:

- hazards which could be introduced, controlled or exacerbated at that step;
- whether the hazards present a significant risk (based on consideration of consequence and probability using a combination of experience, data and technical literature);
- a justification for the significance rating;
- possible preventative measures for each hazard;
- whether monitoring or control measures can be applied at this step (i.e. is it a CCP?).

The HACCP plan delineates the procedures to be followed to assure the control of a specific design, product, process or procedure. The plan includes a list of all CCPs and for each CCP lists:

- the critical limits for preventative measures;
- monitoring and continuing control activities (including what, how, and when monitoring will be carried out and by whom);
- corrective actions required if deviations from critical limits are detected;

- verification and record-keeping activities.

B.4.3.5 Strengths and limitations

Strengths of HACCP include the following.

- HACCP is a structured process that provides documented evidence for quality control as well as identifying and reducing risks.
- It focuses on the practicalities of how and where, in a process, sources of risk can be found and risk controlled.
- It provides risk control throughout a process rather than relying on final product inspection.
- It draws attention to risk introduced through human actions and how this can be controlled at the point of introduction or subsequently.

Limitations include the following.

- HACCP requires that hazards are identified, the risks they represent defined, and their significance understood as inputs to the process. Appropriate controls also need to be defined. HACCP might need to be combined with other tools to provide these inputs.
- Taking action only when control parameters exceed defined limits can miss gradual changes in control parameters which are statistically significant and hence should be actioned.

B.4.3.6 Reference documents

[34] ISO 22000, *Food safety management systems – Requirements for any organization in the food chain*

[35] *Food Quality and Safety Systems – A Training Manual on Food Hygiene and the Hazard Analysis and Critical Control Point (HACCP) System*

B.4.4 Layers of protection analysis (LOPA)

B.4.4.1 Overview

LOPA analyses the reduction in risk that is achieved by set of controls. It can be considered as a particular case of an event tree (B.5.6) and is sometimes carried out as a follow up to a HAZOP study (B.2.4).

A cause-consequence pair is selected from a list of identified risks and the independent protection layers (IPLs) are identified. An IPL is a device, system or action that is capable of preventing a scenario from proceeding to its undesired consequence. Each IPL should be independent of the causal event or of any other layer of protection associated with the scenario and should be auditable. IPLs include:

- design features;
- physical protection devices;
- interlocks and shutdown systems;
- critical alarms and manual intervention;
- post event physical protection;
- emergency response systems.

Standard procedures and/or inspections do not directly add barriers to failure so in general should not be considered to be IPLs. The probability of failure of each IPL is estimated and an order of magnitude calculation is carried out to determine whether the overall protection is adequate to reduce risk to a tolerable level.

The frequency of occurrence of the undesired consequence can be found by combining the frequency of the initiating cause with the probabilities of failure of each IPL, taking into account any conditional modifiers. (An example of a conditional modifier is whether a person will be

present and might be influenced.) Orders of magnitude are used for frequencies and probabilities.

B.4.4.2 Use

LOPA can be used qualitatively to review the layers of protection between a causal factor and a consequence. It can also be used quantitatively to allocate resources to treatments by analysing the risk reduction produced by each layer of protection. It can be applied to systems with a long- or short-term time horizon and is usually used in dealing with operational risks.

LOPA can also be used quantitatively for the specification of IPLs and safety integrity levels (SIL levels) for instrumented systems, as described in IEC 61508 (all parts) and in IEC 61511 (all parts), and to demonstrate that a specified SIL is achieved.

NOTE An SIL is a discrete level (one out of a possible four) for specifying the reliability required of a safety-related system. Level 4 has the highest level of safety integrity and level 1 has the lowest.

B.4.4.3 Inputs

Inputs to LOPA include:

- basic information about sources, causes and consequences of events;
- information on controls in place or proposed treatments;
- the frequency of the causal event, and the probabilities of failure of the protection layers, measures of consequence and a definition of tolerable risk.

B.4.4.4 Outputs

The outputs are recommendations for any further treatments and estimates of the residual risk.

B.4.4.5 Strengths and limitations

Strengths of LOPA include the following.

- It requires less time and resources than event tree analysis or fully quantitative risk assessment but is more rigorous than subjective qualitative judgments.
- It helps identify and focus resources on the most critical layers of protection.
- It identifies operations, systems and processes for which there are insufficient safeguards.
- It focuses on the most serious consequences.

Limitations of LOPA include the following.

- It focuses on one cause-consequence pair and one scenario at a time; complex interactions between risks or between controls are not covered.
- When used quantitatively it might not account for common mode failures.
- It does not apply to very complex scenarios where there are many cause-consequence pairs or where there are a variety of consequences affecting different stakeholders.

B.4.4.6 Reference documents

[36] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[37] IEC 61511 (all parts), *Functional safety – Safety instrumented systems for the process industry sector*

[38] *Layer of protection analysis – Simplified process risk assessment*

B.5 Techniques for understanding consequences and likelihood

B.5.1 General

Techniques described in Clause B.5 aim to provide a greater understanding of consequences and their likelihood. In general the consequences can be explored by:

- experimentation, such as cell studies to explore consequences of exposure to toxins with results applied to human and ecological health risks;
- research into past events, including epidemiological studies;
- modelling to determine the way in which consequences develop following some trigger, and how this depends on the controls in place. This can include mathematical or engineering models and logic methods such as event tree analysis (B.5.6);
- techniques to encourage imaginative thinking such as scenario analysis (B.2.5).

The likelihood of an event or of a particular consequence can be estimated by:

- extrapolation from historical data (provided there is sufficient relevant historical data for the analysis to be statistically valid). This especially applies for zero occurrences, when one cannot assume that because an event or consequence has not occurred in the past it will not occur in the near future;
- synthesis from data relating to failure or success rates of components of the systems: using techniques such as event tree analysis (B.5.6), fault tree analysis (B.5.7) or cause-consequence analysis (B.5.5);
- simulation techniques, to generate, for example, the probability of equipment and structural failures due to ageing and other degradation processes.

Experts can be asked to express their opinion on likelihoods and consequences, taking into account relevant information and historical data. There are a number of formal methods for eliciting expert judgement that make the use of judgment visible and explicit (see Clause B.1).

Consequence and likelihood can be combined to give a level of risk. This can be used to evaluate the significance of a risk by comparing the level of risk with a criterion for acceptability, or to put risks in a rank order.

Techniques for combining qualitative values of consequence and likelihood include index methods (B.8.6) and consequence/likelihood matrices (B.10.3). A single measure of risk can also be produced from a probability distribution of consequences (see for example VaR (B.7.2) and CVaR (B.7.3) and S-curves (B.10.4)).

B.5.2 Bayesian analysis

B.5.2.1 Overview

It is common to encounter problems where there is both data and subjective information. Bayesian analysis enables both types of information to be used in making decisions. Bayesian analysis is based on a theorem attributed to Reverend Thomas Bayes (1760). At its simplest, Bayes' theorem provides a probabilistic basis for changing one's opinion in the light of new evidence. It is generally expressed as in Formula (1):

$$\Pr(A \mid B) = \frac{\Pr(B \mid A)\Pr(A)}{\Pr(B)} \tag{1}$$

where

$\Pr(A)$ is the prior assessment of the probability of A;

$\Pr(B)$ is the prior assessment of the probability of B;

Pr($A|B$) is the probability of A given that B has occurred (the posterior assessment);

Pr($B|A$) is the probability of B given A has occurred.

Bayes' theorem can be extended to encompass multiple events in a particular sample space.

For example, assume we have some data, D, that we wish to use to update our previous understanding (or lack thereof) of risk. We want to use these data to assess the relative merits of a number (N) of competing and non-overlapping hypotheses, which we will denote by H_n (where n = 1, 2, …, N). Then Bayes' theorem can be used to calculate the probability of the jth hypothesis using Formula (2):

$$\Pr\left(H_j \mid D\right) = \Pr\left(H_j\right)\left[\frac{\Pr\left(D \mid H_j\right)}{\sum \Pr\left(H_n\right)\Pr\left(D \mid H_n\right)}\right] \tag{2}$$

where j = 1, 2 …, n.

This shows that once the new data is accounted for, the updated probability for hypothesis j [i.e. Pr($H_j|D$)] is obtained by multiplying its prior probability Pr(H_j) by the bracketed fraction.

This fraction's numerator is the probability of getting these data if the jth hypothesis is true. The denominator comes from the "law of total probability" – the probability of getting these data if, one by one, each hypothesis were to be true. The denominator is the normalization factor.

A Bayesian probability can be more easily understood if it is considered as a person's degree of belief in a certain event as opposed to the classical probability which is based upon physical evidence.

B.5.2.2 Use

Bayesian analysis is a means of inference from data, both judgemental and empirical. Bayesian methods can be developed to provide inference for parameters within a risk model developed for a particular context; for example, the probability of an event, the rate of an event, or the time to an event.

Bayesian methods can be used to provide a prior estimate of a parameter of interest based upon subjective beliefs. A prior probability distribution is usually associated with subjective data since it represents uncertainties in the state of knowledge. A prior can be constructed using subjective data only or using relevant data from similar situations. A prior estimate can provide a probabilistic prediction of the likelihood of an event and be useful for risk assessment for which there is no empirical data.

Observed event data can then be combined with the prior distribution through a Bayesian analysis to provide a posterior estimate of the risk parameter of interest.

Bayes' theorem is used to incorporate new evidence into prior beliefs to form an updated estimate.

Bayesian analysis can provide both point and interval estimates for a parameter of interest. These estimates capture uncertainties associated with both variability and the state of knowledge. This is unlike classical frequentist inference which represents the statistical random variation in the variable of interest.

The probability model underpinning a Bayesian analysis depends on the application. For example, a Poisson probability model might be used for events such as accidents, non-conformances or late deliveries, or a binomial probability model might be used for one-shot

items. Increasingly it is common to build a probability model to represent the causal relationships between variables in the form of a Bayesian network (B.5.3).

B.5.2.3 Inputs

The inputs to a Bayesian analysis are the judgemental and empirical data needed to structure and quantify the probability model.

B.5.2.4 Outputs

Like classical statistics, Bayesian analysis provides estimates, both single numbers and intervals, for the parameter of interest and can be applied to a wide range of outputs.

B.5.2.5 Strengths and limitations

Strengths are the following.

- Inferential statements are easy to understand.
- It provides a mechanism for using subjective beliefs about a problem.
- It provides a mechanism for combining prior beliefs with new data.

Limitations are the following.

- It can produce posterior distributions that are heavily dependent on the choice of the prior.
- Solving complex problems can involve high computational costs and be labour intensive.

B.5.2.6 Reference documents

[39] GHOSH, J., DELAMPADY, M. and SAMANTA, T. *An introduction to Bayesian analysis*, New York Springer-Verlag, 2006

[40] QUIGLEY, J.L., BEDFORD, T.J. and WALLS, L.A. *Prior Distribution Elicitation*

B.5.3 Bayesian networks and influence diagrams

B.5.3.1 Overview

A Bayesian network (Bayes' net or BN) is a graphical model whose nodes represent the random variables (discrete and/or continuous) (Figure B.3). The nodes are connected by directed arcs that represent direct dependencies (which are often causal connections) between variables.

The nodes pointing to a node X are called its parents, and are denoted pa(X). The relationship between variables is quantified by conditional probability distributions (CPDs) associated with each node, denoted P(X|pa(X)), where the state of the child nodes depends on the combination of the values of the parent nodes. In Figure B.3 probabilities are indicated by point estimates.

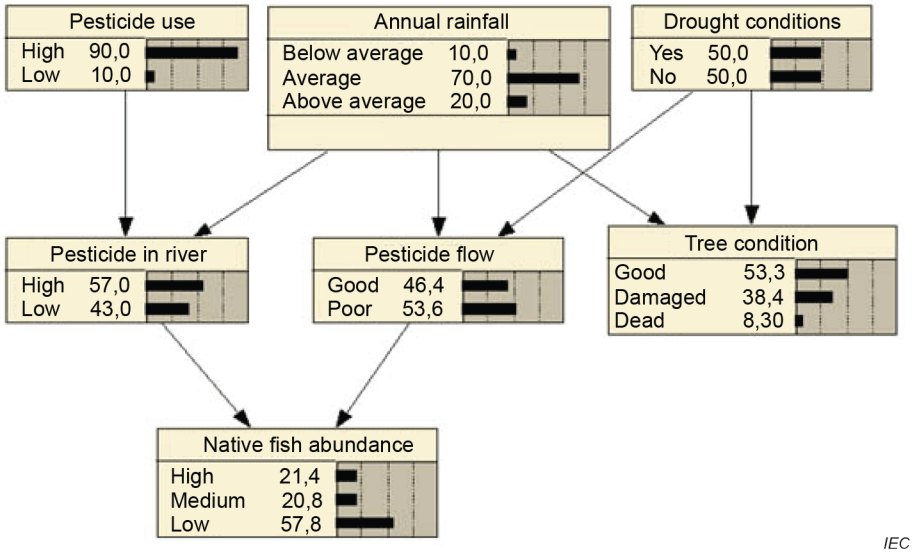

Figure B.3 – A Bayesian network showing a simplified version of a real ecological problem: modelling native fish populations in Victoria, Australia

B.5.3.2 Use

A basic BN contains variables that represent uncertain events and can be used to estimate likelihood or risk or to infer key risk drivers leading to specified consequences.

A BN can be extended to include decision actions and valuations as well as uncertainties, in which case it is known as an influence diagram, which can be used to assess the impact of risk controls/mitigations or to value intervention options.

A BN model can be built as a qualitative representation of a problem by stakeholders then quantified using relevant data, including judgemental (e.g. medicine distribution centre risk analysis), or a BN model can be learnt from empirical data only (e.g. web search engines, financial risk). Regardless of the form of a BN, the underlying inference mechanism is based on Bayes' theorem and possesses the general properties of Bayesian analysis (B.5.2).

BN have been used across a wide range of applications: including environmental decision making, medical diagnosis, critical infrastructure life extension, supply chain risk, new product and process development image modelling, genetics, speech recognition, economics, space exploration and in web search engines.

In general BNs provide visual models that support articulation of problems and communication between stakeholders. BN models allow sensitivity analysis to be conducted to explore "what if?" scenarios. Constructing the qualitative BN structure can be supported by the use of causal mapping (B.6.1) and a BN can be used in conjunction with scenario analysis (B.2.5) and cross impact analysis (B.6.2).

BNs are useful for gaining stakeholder input and agreement for decisions where there is high uncertainty and a divergence of stakeholder views. The representation is readily comprehensible although expertise is required to produce it.

BNs can be useful for mapping risk analyses for non-technical stakeholders, by promoting transparency of assumptions and process and by treating uncertainty in a way that is mathematically sound.

B.5.3.3 Inputs

The inputs for BNs require an understanding of system variables (nodes), the causal links between them (directed arcs) and the prior and conditional probabilities for these relationships.

In the case of an influence diagram, the valuations are also required (e.g. financial loss, injuries, etc.).

B.5.3.4 Outputs

BNs provide conditional and marginal distributions in a graphical output that is generally considered easy to interpret, at least compared with other, black box models. The BN model and the data can be readily modified to easily visualize relationships and explore the sensitivity of parameters to different inputs.

B.5.3.5 Strengths and limitations

Strengths of BNs include the following.

- There is readily available software that is relatively easy to use and understand.
- They have a transparent framework and are able to rapidly run scenarios and analyse sensitivity of output to different assumptions.
- They can include subjective beliefs about a problem, together with data.

Limitations include the following.

- Defining all interactions for complex systems is difficult, and can become computationally intractable when conditional probability tables become too large.
- BNs are often static and don't typically include feedback loops. However, the use of dynamic BNs is increasing.
- Setting parameters requires knowledge of many conditional probabilities which are generally provided by expert judgement. BNs can only provide answers based on these assumptions (a limitation that is common to other modelling techniques).
- The user can input errors but the output might still give a believable answer; checking extremes can help to locate errors.

B.5.3.6 Reference documents

[41] NEIL, Martin and FENTON, Norman. *Risk Assessment and Decision Analysis with Bayesian Networks* CRC Press, 2012

[42] JENSEN, F.V., NIELSEN T. D. *Bayesian Networks and Decision Graphs*, 2nd ed. Springer, New York, 2007

[43] NICHOLSON, A., WOODBERRY O and TWARDY C, The "Native Fish" Bayesian networks. *Bayesian Intelligence Technical Report 2010/3*, 2010

[44] NETICA TUTORIAL

B.5.4 Business impact analysis (BIA)

B.5.4.1 Overview

Business impact analysis analyses how incidents and events could affect an organization's operations, and identifies and quantifies the capabilities that would be needed to manage it. Specifically, a BIA provides an agreed understanding of:

- the criticality of key business processes, functions and associated resources and the key interdependencies that exist for an organization;
- how disruptive events will affect the capacity and capability of achieving critical business objectives;