Risk Assessment Methods
Understanding, Selecting & Applying

Developing Risk Information for Decision Making

Workshop Ground Rules

- ❑ Start and stop on time/breaks
- ❑ Housekeeping, emergency response
- ❑ Technology/connectivity
- ❑ Participation is necessary
- ❑ Anything else?

Getting to Know You and Your Objectives

- ❑ Name
- ❑ Organization
- ❑ What is your experience with and knowledge of risk assessment?
- ❑ What do you hope to gain from this workshop?
- ❑ If you could pick one person from any place in history to have dinner with, who would you choose and why?

Workshop Objectives

1. **To increase your comfort and confidence in developing risk information that supports decision making.**
2. **To heighten your awareness of international expectations in risk assessment based on ISO 31010 - Risk Assessment Standard**

We'll do that by…

- using a common risk management process
- describing key risk assessment concepts
- learning how to select and apply risk assessment method(s)
- situating the risk assessment results in relation to organizational objectives and an ERM framework

Workshop Agenda

- Foundation & Overview
- Module 1: Key Concepts in Risk Assessment: Establishing Context & Risk Criteria
- Module 2: Understanding, Selecting & Applying Risk Assessment Methods
- Module 3: Key Concepts in Risk Assessment: Presenting Results & Using/Integrating Results
- Module 4: Challenges in Risk Assessment

RISK ASSESSMENT
WORKSHOP FOUNDATION & OVERVIEW

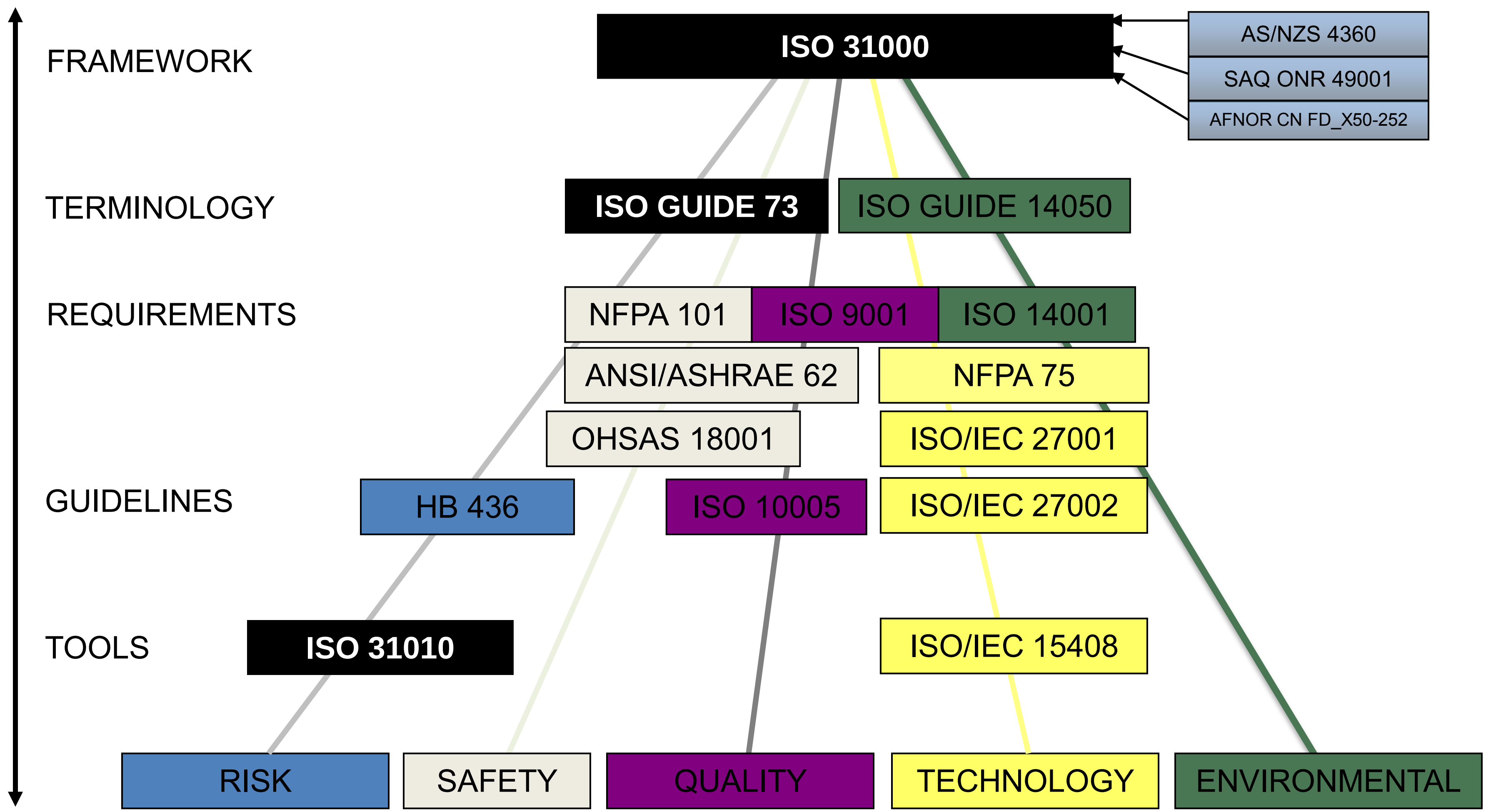
The World of Standards

What Standards Are ✔	What Standards Are Not ✘
• A collection of best practices and guidelines • Developed collaboratively • Evolutionary • Can be in form of management systems, product specifications, service levels, procedures or definitions	• Regulations • Just controls • Necessarily “how to implement” documents • “Certifications” (nor require that an organization be certified to use a standard)

Question

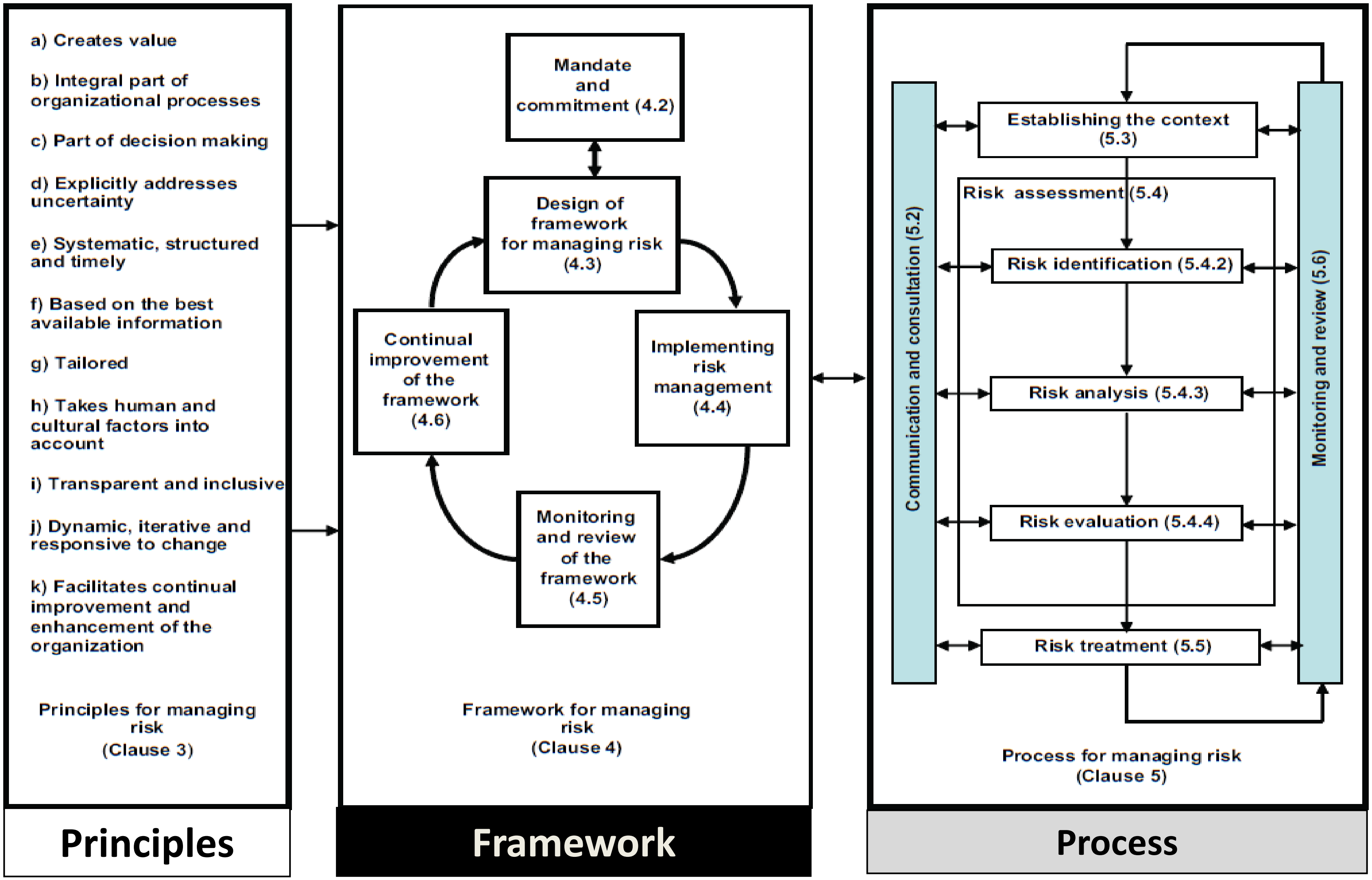
Does your organization use any particular risk, quality, safety, technological or environmental standards? Which ones?

Risk Standards Hierarchy



All relevant ISO standards are being aligned to ISO 31000 (2009) Risk Management

ISO 31000 Risk Management at a Glance



The Pivotal Definition

Risk

the effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected — positive and/or negative.

NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3 Risk is often characterized by reference to potential events and consequences, or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.
[ISO Guide 73:2009]

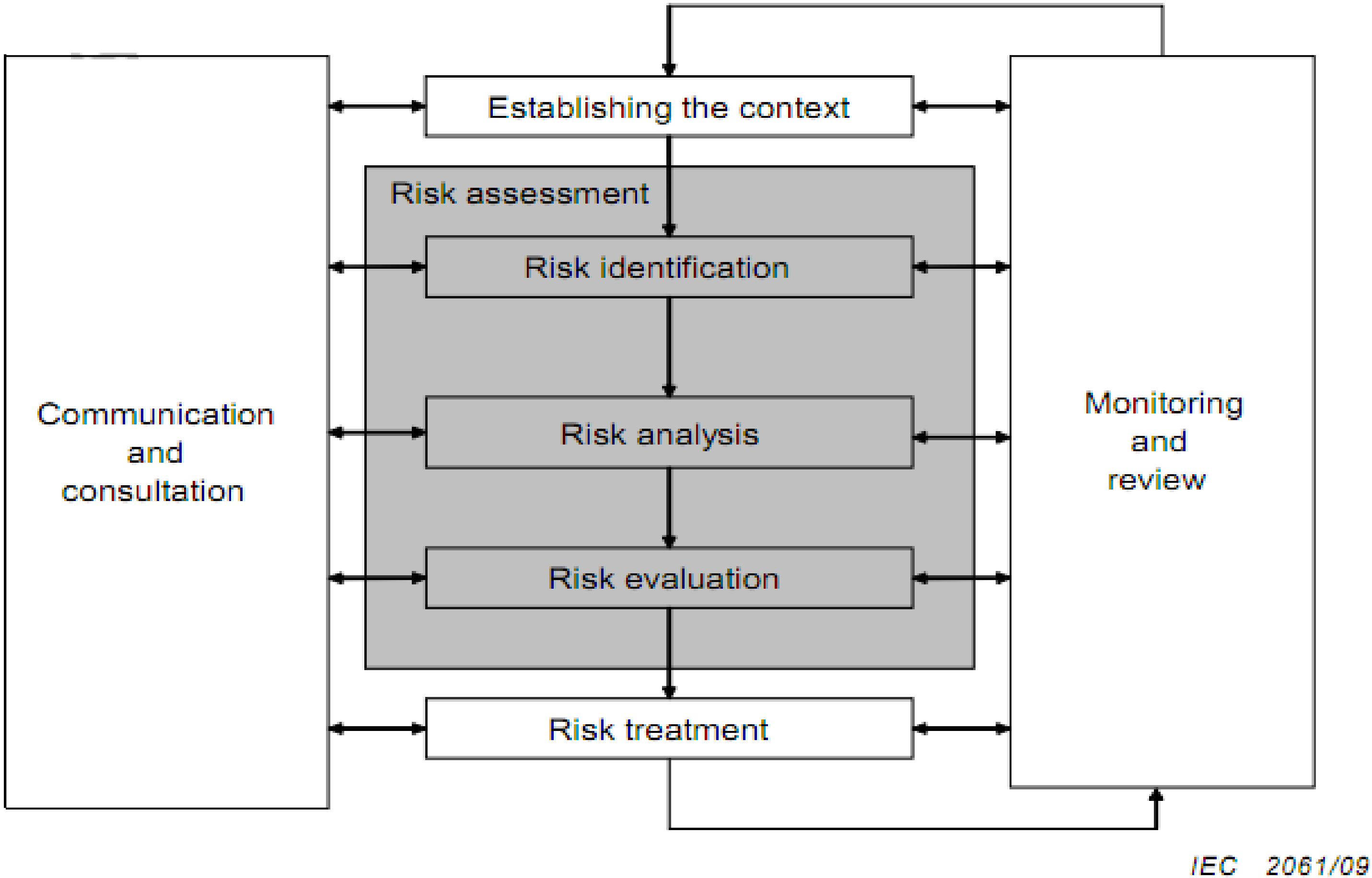
RIMS ERM Definition

Enterprise Risk Management ("ERM") is a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.

]

IEC/ISO 31010

Edition 1.0 2009-11



Reproduced from *ISO 31000* with permission from ISO at www. iso.org. Copyright remains with ISO

ISO/IEC 31010:2009
Risk Management - Risk Assessment Techniques

Technical Questions answered by a Risk Assessment

- What can happen and why (by risk identification)?
- What is the likelihood of their future occurrence?
- What are the possible consequences?
- Are there any factors that affect the likelihood of the risk or the consequence of the risk?

Management Questions answered by a Risk Assessment

- How effective are the controls we currently have in place?
- Which of our/my objectives could be most impacted (positively or negatively)?
- Given what we now know about risks/opportunities associated with this decision
  - Is the net RA result within my/our appetite for risk?
  - Should we proceed?
  - If yes, what should we change about the way we currently work and place our resources?

Discussion

- When does your organization assess risk?
- How similar is this risk management process to the one(s) used by your organization?
- How is this process different from the one(s) you know?
- What steps of the process are typically strong in your organization?
- What areas of the process could your organization learn more about?

MODULE 1

THE FIRST TWO KEY CONCEPTS IN RISK ASSESSMENT

1. Establish the Context for Risk Assessment

2. Risk Criteria

Key Concept: Establish the Context for Risk Assessment

A simple and effective technique to improve the focus and value of risk assessment is to clarify:

- **Why** the risk assessment is being performed (to answer what question or inform what decision)
- **Who** could be impacted by the risk assessment results and decision
- The **significance** of the decision to your organization

The risk assessment context can affect assumptions, conclusions and decisions in other stages of the risk management process.

Four Steps to Establish the Context

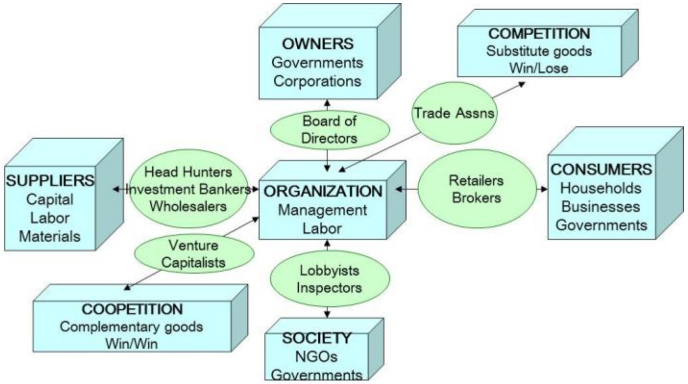
1. **Clarify the decision to be made**
   – Is it a 'Yes or No' type of decision?
   – Will the risk assessment be used to inform option analysis? If yes, be clear on what the options are. For risk assessment purposes you will use the current state as your 'Option 1'
   – How significant is the decision to organizational objectives (e.g. major significance = significant risk assessment effort)?
   – Which organizational objective(s) does this decision support?

2. **Clarify the time frame available for risk assessment**
   – When does the decision maker need the information?
   – What are all the steps that your decision maker will take – do you know where risk assessment step fits in that process? First? last?

Four Steps to Establish the Context

3. **What resources will you need to inform your risk assessment?**
   - Internal colleagues: business area, technical knowledge, internal auditors, corporate functions
   - External knowledge: specialized expertise
   - Information: stakeholder/customer or employee satisfaction surveys, studies, audits, reports, claims history, industry or other environmental/social/economic trend analysis, interviews, etc.
4. **Who are the stakeholders that could be impacted by the decision?**
   - Develop a stakeholder map like this one OR
   - Reach out to your communications resource to see if they have one

Graphic requires clearance
From RA Techniques course



KEY CONCEPT:
RISK CRITERIA

Risk Criteria

risk criteria

terms of reference against which the significance of a risk is evaluated

NOTE 1 Risk criteria are based on organizational objectives, and external and internal context (of the organization).

NOTE 2 Risk criteria can be derived from standards, laws, policies and other requirements

(ISO Guide 73:2009, definition 3.3.1.3)

Some organizations also call risk criteria

- Risk appetite
- Level of tolerable or acceptable risk (risk tolerance; acceptable risk, etc.)

Risk Criteria Reality Check

Not all risks and opportunities can or should be managed. Risk criteria is a tool that helps organizations distinguish the value of one risk from another to establish significance and priority.

Q: Risk assessments can result in hundreds of risks and opportunities identified but which ones should we address?

A: The ones we address should align to our values and strategy as an organization.

Q: How do we do that?

A: Clarify the range of "desired to acceptable" performance in relation to performance targets

Samples of Risk Rating/Risk Criteria

Moderate | High

Public Health Hazard Risk Analysis Tool
April 2008

Event	Probability	Human Impact	Property Impact	Business Impact	Overall Impact Rating	Risk Rating
	A,B,C or D (Table 1)	1,2,3 or 4	1,2,3 or 4	1,2,3 or 4	4-12 (Table 2)	(Table 3)
Transportation Emergency (e.g. plane, train, multi-vehicle crashes)	A	4	3	2	9	A9
Water System Emergency	A	4	1	4	9	A9
Electricity System Failures	B	2	2	4	8	B8
Flooding	B	1	4	3	8	B8
Tornado	B	2	3	3	8	B8
HAZMAT Events	B	4	3	3	10	B10
Air Quaility Episode, e.g. severe prolonged smog episode	A	2	1	2	5	A5
Extreme Heat	A	3	1	1	5	A5
Severe Thunderstorm	A	2	2	2	6	A6
Blizzard	B	1	2	2	5	B5
Ice Storm	B	2	2	3	7	B7
Epidemic	B	3	1	3	7	B7

Trades Union Congress (UK) A Guide for Safety Representatives
Source: http://www.health.gov.on.ca/english/providers/program/pubhealth/oph_standards/ophs/progstds/workshops/phep_phhazard_identification_and_risk_assessment_betty_schepens.pdf

Plenary Discussion: Rating Risks

1. How does your organization approach risk rating?

- Multiple rating systems
- Single rating systems
- Aligned to our values, mission and strategy
- Other?

2. How was the current risk rating approach developed?

- Borrowed from another organization
- Borrowed and adapted from another organization
- Adapted from another source
- Developed our own

3. In your experience, what happens when an inconsistent or conflicting risk rating occurs within the same organization?

4. What happens when there are no established risk criteria or a risk rating system?

Plenary Exercise - Developing Risk Criteria

What to do

Decisions we will need to make include:

1. How would we describe this organization's risk appetite?
2. To help rate risks and opportunities, will we use dual or tri-attribute criteria?
   - Likelihood (probability)
   - Impact (consequence)
   - Exposure (relevant?)
2. What scale makes sense? (3X3, 4X4, 5X5, 10X10?)
3. What is your own experience in developing or using risk criteria?

MODULE 2

UNDERSTANDING, SELECTING & APPLYING RISK ASSESSMENT METHODS

Case Study
Manufacturer Operational Decision

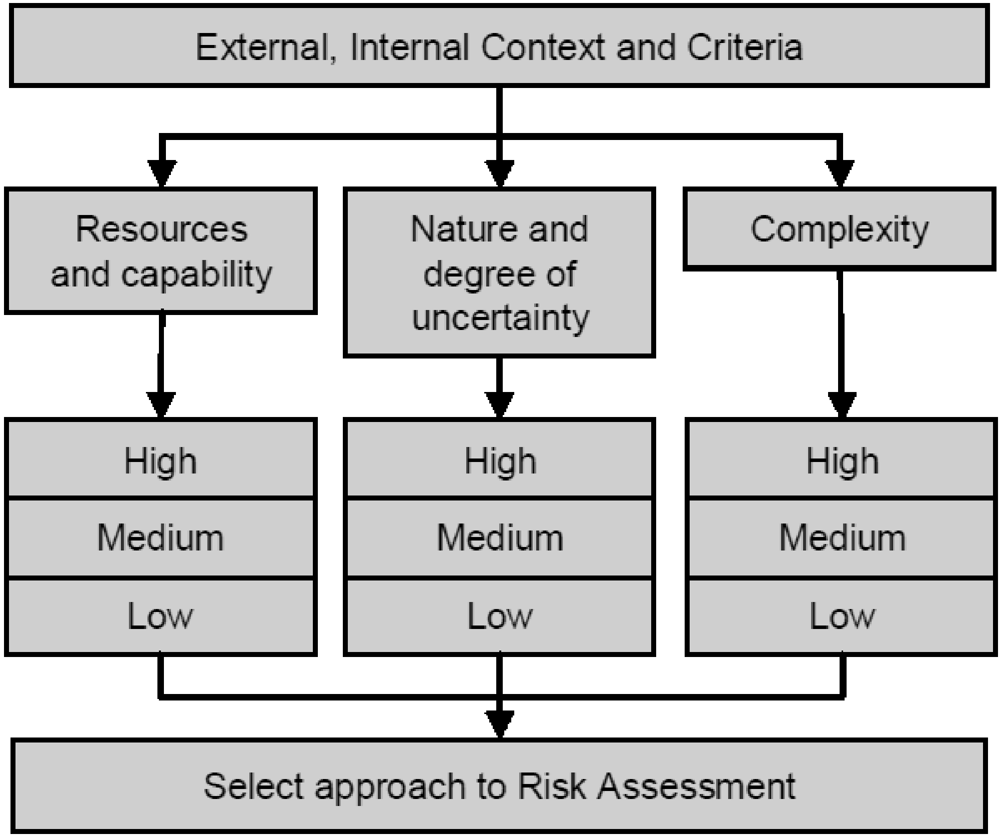
Organization: IT4U Incorporated

Description: IT4U is a mid-sized manufacturer based on the west coast. They research, design and manufacture accessories for smart phones and other devices with worldwide sales and distribution.

Size/Location: IT4U employs 2,500 people in Seattle (corporate, sales & marketing, customer service, warehouse & shipping), Raleigh (research) and Vancouver (production). Their head office is in Seattle.

Decision Setting: IT4U is doubling their Vancouver office space within the next 6 months to accommodate increased sales with China. They have leased the space adjacent to their existing downtown office and need to ensure continuous operations through the refit, construction, staffing and physical move. Some staff from Seattle and Raleigh will be moved to Vancouver to help strengthen corporate/marketing and research presence.

Selecting Risk Assessment Methods



1. **Confirm the Context.** Where several options are available, risk assessment can be used to evaluate options relative to a baseline or status quo state, to help decide which provides the best balance of risks. *Think: organizational objectives, the significance of the decision, stakeholders.*

2. **Resources:** What resources do you have? What resources do you need? *Think: time, money, people, expertise.*

3. **Do you have enough/quality information?** *Think: where can you go to get data, is it accessible to you, is it good quality?*

4. **What other factors could affect the complexity of the risk assessment?** *Think: interdependent factors of this decision on existing decisions, range of impacts .*

Dealing with Uncertainty

- Available data do not always provide a reliable basis for the prediction of the future.
- For unique types of risks, historical data may not be available or there may be different interpretations of available data by different stakeholders.
- Those undertaking risk assessment need to understand the type and nature of the uncertainty and appreciate the implications for the reliability of the risk assessment results.
- These should always be communicated to decision makers.

Dealing with Complexity

Risks can be complex in themselves, as, for example, in complex systems which need to have their risks assessed across the system rather than treating each component separately and ignoring interactions.

- In other cases, treating a single risk can have implications elsewhere and can impact on other activities.
- Consequential impacts and risk dependencies need to be understood to ensure that in managing one risk, an intolerable situation is not created elsewhere.
- Understanding the complexity of a single risk or of a portfolio of risks of an organization is crucial for the selection of the appropriate method or techniques for risk assessment.

The Effect of Time

Many activities, projects and products can be considered to have a life cycle starting from initial concept and definition through realization to a final completion which might include decommissioning and disposal of hardware.

- Risk assessment can be applied at all stages of the life cycle and is usually applied many times with different levels of detail to assist in the decisions that need to be made at each phase.
- Life cycle phases have different needs and require different techniques. For example, during the concept and definition phase, when an opportunity is identified, risk assessment may be used to decide whether to proceed or not.

Selecting a Risk Assessment Method

Suitable techniques should exhibit the following characteristics:

- The method should be justifiable and appropriate to the situation or organization under consideration;
- The method should provide results in a form which enhances understanding of the nature of the risk and how it can be treated;
- The method should be capable of use in a manner that is traceable, repeatable and verifiable.

Table A.1

Table A.1 – Applicability of tools used for risk assessment

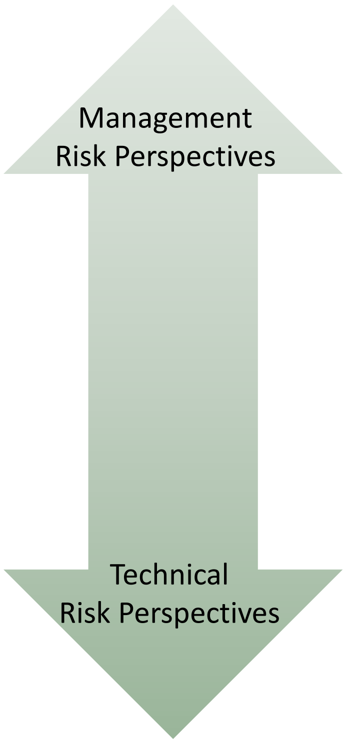
Tools and techniques	Risk assessment process					See Annex
	Risk Identification	Risk analysis			Risk evaluation	
		Consequence	Probability	Level of risk		
Brainstorming	SA[1)]	NA[2)]	NA	NA	NA	B 01
Structured or semi-structured interviews	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Check-lists	SA	NA	NA	NA	NA	B 04
Primary hazard analysis	SA	NA	NA	NA	NA	B 05
Hazard and operability studies (HAZOP)	SA	SA	A[3)]	A	A	B 06
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA	B 07
Environmental risk assessment	SA	SA	SA	SA	SA	B 08
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA	B 09
Scenario analysis	SA	SA	A	A	A	B 10
Business impact analysis	A	SA	A	A	A	B 11
Root cause analysis	NA	SA	SA	SA	SA	B 12
Failure mode effect analysis	SA	SA	SA	SA	SA	B 13
Fault tree analysis	A	NA	SA	A	A	B 14
Event tree analysis	A	SA	A	A	NA	B 15
Cause and consequence analysis	A	SA	SA	A	A	B 16
Cause-and-effect analysis	SA	SA	NA	NA	NA	B 17
Layer protection analysis (LOPA)	A	SA	A	A	NA	B 18
Decision tree	NA	SA	SA	A	A	B 19

Legend
SA = Strongly Applicable
A = Applicable
NA = Not Applicable

Reproduced from *ISO 31000* with permission from ISO at www. iso.org. Copyright remains with ISO

Types of Risk Assessment Methods

More
Qualitative



More
Quantitative

- Lookup (e.g. checklist)
- Supporting Methods (e.g. interviews, ‘what if’)
- Scenario Analysis (e.g. root cause, BIA)
- Functional Analysis (e.g. FMEA, HAZOP)
- Controls Assessment (e.g. Bow-tie)
- Statistical Methods (e.g. Monte-Carlo, Bayesian)

Lookup Method
Sample Checklist

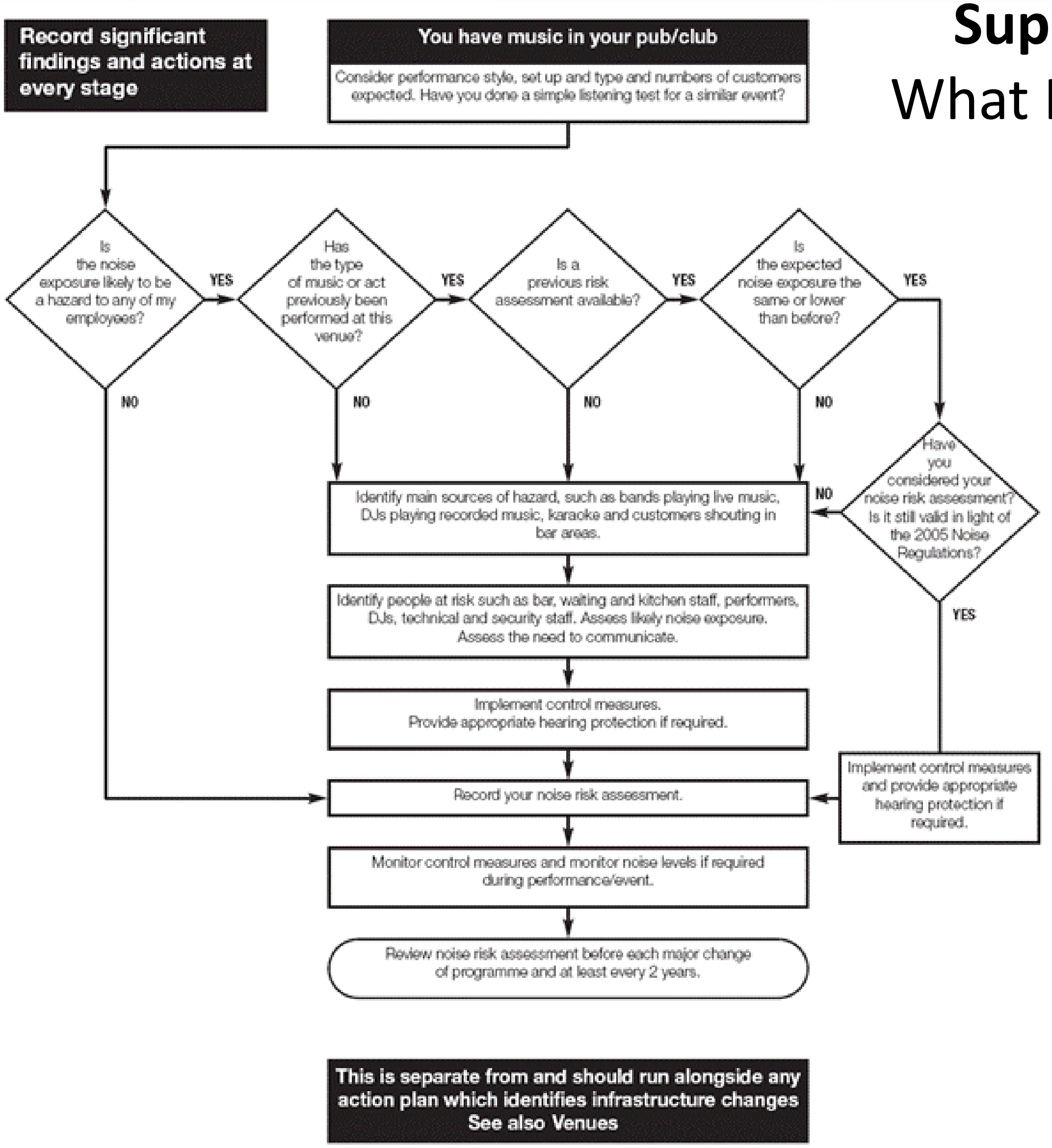
POPSICLE:
- Products
- Operations
- Physical
- Social
- Information
- Cognitive
- Legal
- Economic

Your operation:
- P________________
- O________________
- P________________
- S________________
- I________________
- C________________
- L________________
- E________________

Case Study:
- P________________
- O________________
- P________________
- S________________
- I________________
- C________________
- L________________
- E________________

Supporting Method

What If Analysis Example

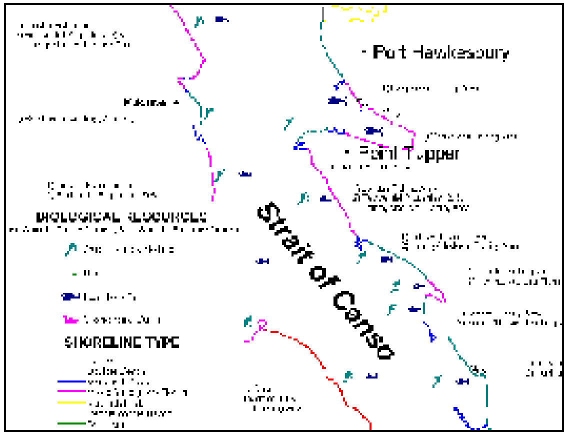


Risk assessment for amplified music played in nightclubs, pubs and restaurants

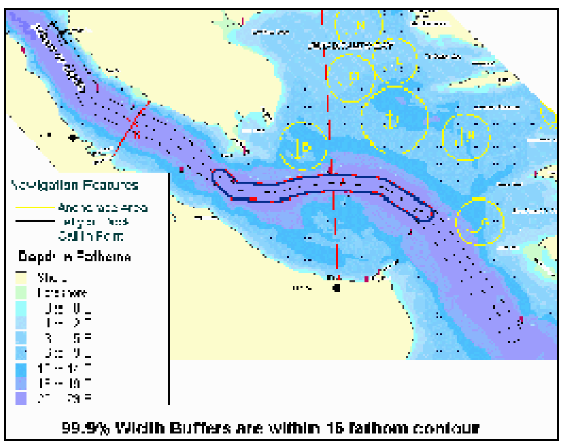
Source-http://www.soundadvice.info/thewholestory/san11.htm

Scenario Analysis Method

Root Cause Analysis: Transport Canada



Loss potential Map



Electronic navigation chart showing track plot and buffer zones

Objective of the Risk Assessment: To assess the risks associated with the passage of tankers through the Canso Strait, under various configurations of fixed and floating aids to navigation.

Method: This assessment took into account aids to navigation in the waterways, in conjunction with on-board navigation aids, vessel characteristics, traffic density, and weather conditions. Risk estimates for tanker spill, human injury, and property damage consequences were developed, as well as risk frequencies for various casualty types. The aim was to acquire sufficient data to support decisions on the aids to navigation required in Canso Strait. The data will extend TDC's tanker navigation safety system, a risk model developed in previous work. To ensure the validity of the assessment, TDC worked in close collaboration with the Canadian Coast Guard's Marine Navigation Services.

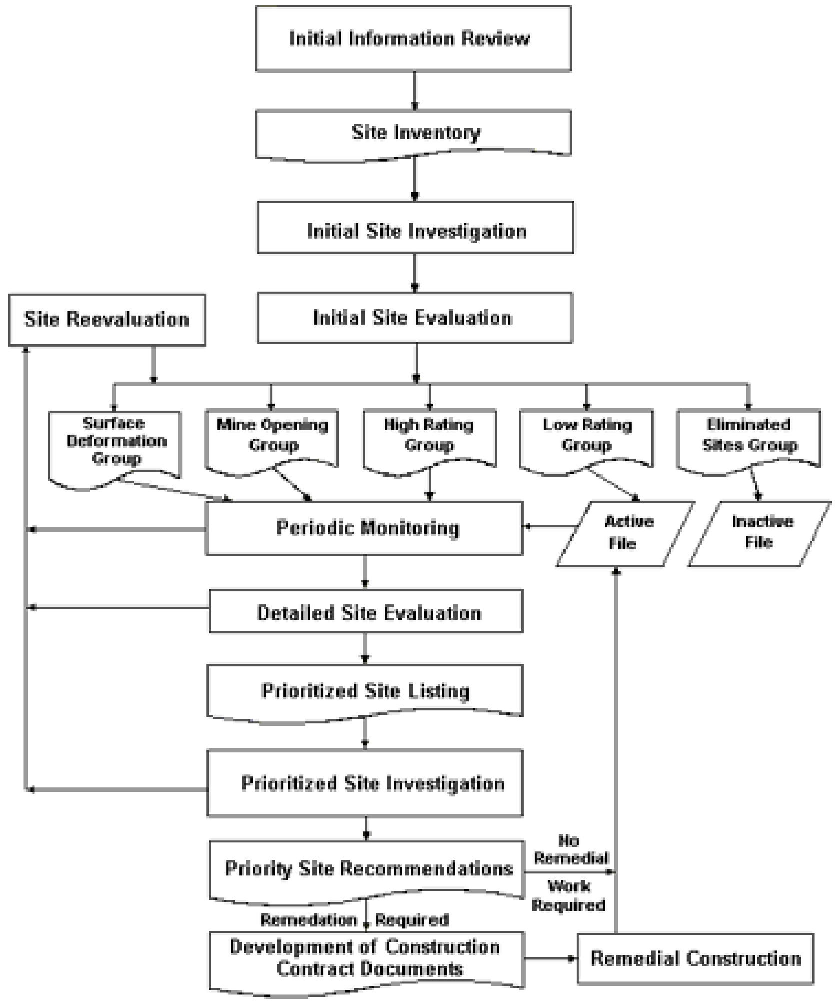
Results: The analysis team examined the components of a passage through the Canso Strait, determined and validated the traffic patterns, and reviewed the key design parameters for systems of aids to navigation for day, night, and poor visibility.

They then developed a pre-processor to arrive at the requirements for safe channel marking for various ship types, processed the acquired data, and analysed a number of scenarios. The upgraded version of the tanker navigation safety system, renamed the marine navigation safety system (MNSS), was compared with the U.S. Waterways Analysis Management System. This helped to validate the pre-processor and demonstrated the strengths and weaknesses of each system. Further research in this area was recommended.

Source: http://www.tc.gc.ca/eng/innovation/tdc-projects-marine-a-9077-1194.htm

Functional Analysis Method

Sample HAZOP-Abandoned Underground Mine Inventory & Risk Assessment



Source: US Department of Transportation, Federal Highways - http://www.fhwa.dot.gov/engineering/geotech/hazards/mine/manual/mm01.cfm

Exercise 2 – Selecting Risk Assessment Methods

What you will need

- ISO 31010 Annex A Table A 2 pp 23-26 (Summary)
- ISO 31010 Annex B, pp 27-89 (detailed methods)

What to do

Review the variety of risk assessment methods (ISO 31010: Table A2). Make your selection(s). Be prepared to present a high level simple summary of your group's risk context, criteria and method(s) selected.

APPLYING THE RISK ASSESSMENT METHOD(S): RISK IDENTIFICATION

Purpose

- The purpose of risk identification is to identify what might happen or what situations might exist that might affect the achievement of the objectives of the system or organization.
- Once a risk is identified, the organization should identify any existing controls such as design features, people, processes and systems

•ISO 31010 IEC: 2009

Techniques to Help

Sample techniques that help identify risk:

- Check lists
- Past data
- Structured interview
- ‘What if’/scenario analysis
- Brainstorming
- Delphi, HAZOP

Question: What others do you know about or use?

Sources of Information

1. Contracts: leases, sales & purchase agreements, etc.
2. Charts: operational, flow, organizational, stakeholder
   - graphic depiction of bottlenecks
   - single source/sole source identifiers
   - play the ‘what if’ game (ripple effect)
3. Checklists/surveys: insurance, risk management
4. Personal inspection
   - the grapevine
   - the company picnic
   - MBWA

Sources of information

5. Reports:
   - Financial statement disclosures: (past) financial reports (10-K, prospectus, Management Disclosure & Analysis-MD&A)
   - Internal reports: proforma statements, budgets, etc. audits, reviews, self-assessments, employee or customer surveys, third party or internal reviews
6. Experts
   - inside: VP’s, managers, line workers
   - outside: attorneys, brokers, accountants, consultants
7. Statistics:
   - internal: loss runs, HR data, performance data..
   - external: industry, insurance data, ISO, OSHA, IBC

APPLYING THE RISK ASSESSMENT METHOD(S): RISK ANALYSIS

Purpose of Risk Analysis

- The purpose of risk analysis is to establish the level of risk for each identified risk using an estimation of likelihood (probability) and impact (consequence).

- One risk can have a range of impacts and affect multiple organizational objectives.

Risk Analysis Examples

Negative Outcome Example

Given a national labor shortage, there is a risk that we may not be able to maintain continuous service.

This may result in

- Lowered staff morale
- Service interruptions

Our organizational objectives potentially impacted by this include

1. Being an employer of choice
2. Providing service excellence to our customers

Positive Outcome Example

We may be able to further transform our business processes using technology and new skills.

This may result in

- Increased morale through employee creativity and initiative
- Service quality improvements

Our organizational objectives potentially impacted by this include

1. Being an employer of choice
2. Providing service excellence to our customers

Risk Analysis: Controls

What controls are in place today to help us address this negative/positive outcome? Think – people, processes, systems.

Negative Outcome Example

Given a national labor shortage, there is a risk that we may not be able to maintain continuous service.

Controls in place today:

- We have identified which services are the most valued by customers (e.g. customer survey process)
- Our staff is cross-trained (HR system)
- Our HR strategy exists and is funded and resourced to identify which skills we need and where we can recruit them (people, system)

Positive Outcome Example

We may be able to further transform our business processes using technology and new skills.

Controls in place today:

- A recent business process review was conducted this year and identified which business processes require updating and would add the most value
- We have an IT and HR strategy that aligns to and supports our business strategy
- A creativity fund exists to reward and formally recognize employee innovation in the way we work

Risk Analysis – Controls

Caution!

1. Controls can exist but may not be effective
2. Others in your organization may be aware of key controls. Involve them in the review of risk assessment results. (e.g. internal auditors, etc.)
3. Summarize what the controls are

Risk Analysis – Rating

Rate each negative outcome

•**Likelihood**: given the controls in place today, how likely is the risk to occur and impact organizational objectives?

•**Impact**: If the risk occurred, how significant would the impact be on objectives?

Rate each positive outcome:

•**Likelihood**: given the controls in place today, how likely is the positive outcome to be realized?

•**Impact**: if the positive outcome were realized, how significant would that be for your objectives?

APPLYING THE RISK ASSESSMENT METHOD(S): RISK EVALUATION

Risk Evaluation

Risk evaluation results in the answer to the question **“which major risks and opportunities matter most?”**

Given the overall view of risks and opportunities

- Should this activity/decision/option be taken?
- If so, which risks or opportunities need to be treated?
- What is the best (affordable, timely, easy to implement, effective, etc.) way to treat these risks and opportunities so that they can be brought within our organization’s risk appetite?

Case Study Exercise 3- Applying Risk Assessment Methods

What you need

- Your chosen case study
- Objectives relevant to your case study
- A risk rating system of your choice or the course-supplied rating system in the Risk Assessment Toolkit

What to do

1. Identify risks and opportunities using the risk assessment method of your choice
2. For each negative and each positive, briefly list the key controls in place today (people, processes and systems)
3. Rate the likelihood and impact on objectives for each negative outcome. Repeat for each positive outcome.
4. Summarize the results to present the priority risks and opportunities (use Executive Summary checklist).

MODULE 3

THE LAST TWO KEY CONCEPTS IN RISK ASSESSMENT

The Last Two Key Concepts in Risk Assessment

Concept #3: Presenting risk assessment results

Concept #4: Using/integrating risk assessment results

Key Concept 3
Presenting Risk Assessment Results

Do

- ✓ Develop a written executive summary of the results (optional 6-8 slides)
- ✓ Be enthusiastic about the level of support you've received from across the organization in developing the results and from management
- ✓ Engage corporate risk management support prior to presenting results for significant decisions: they can and should be partners and advocates
- ✓ Develop a brief risk assessment report for more significant decisions to expand with more detail on the areas of the executive summary

Don't

- ✖ Drown the decision maker with technical details that obfuscate the 'so what' of the results: get to the point
- ✖ Surprise the decision maker and influencers with the results: pre-brief where possible
- ✖ Exceed more than 10 minutes in presentation time for any risk assessment results: be clear, concise and focused

The Executive Summary

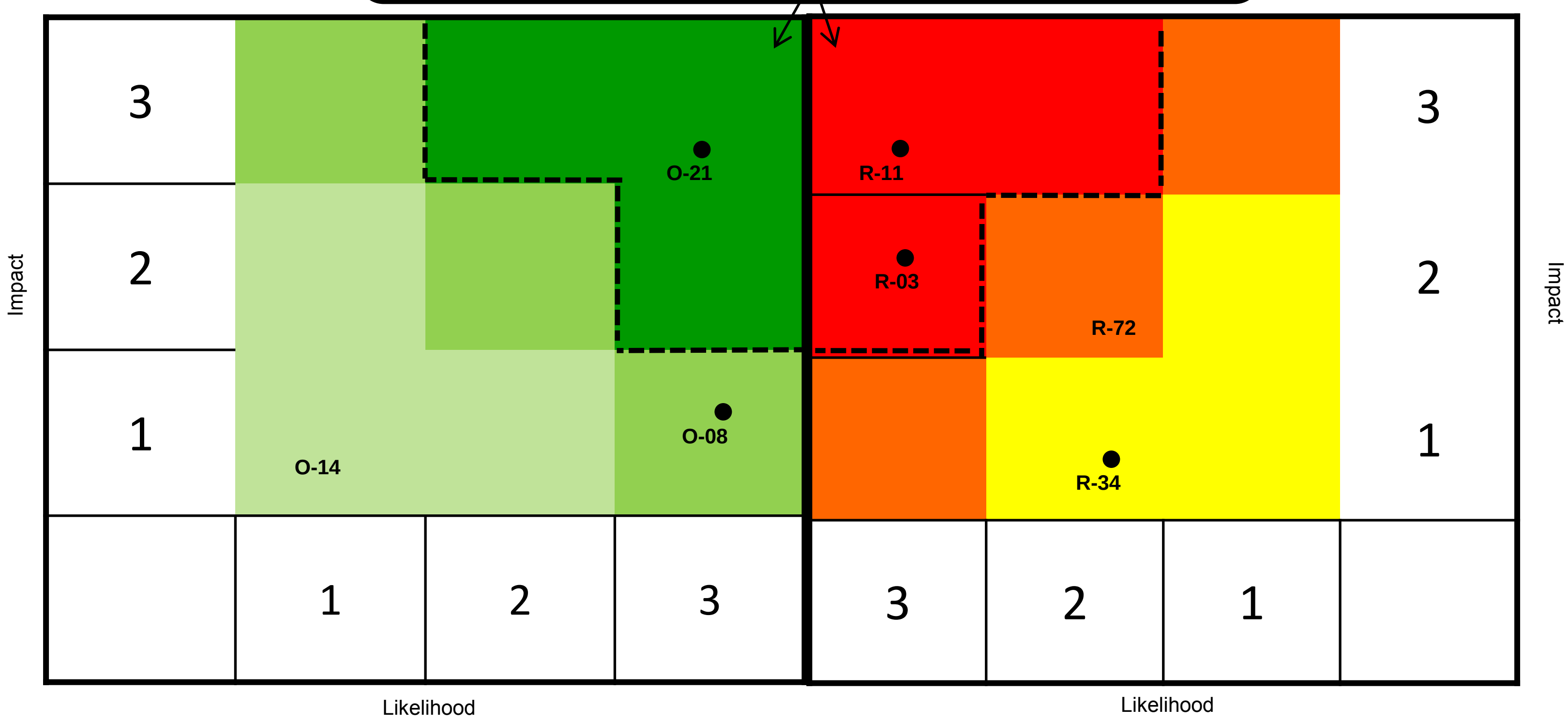
The executive summary of risk assessment results should contain:

- The decision context
- How many risks/opportunities were identified
- Who was involved over what time period
- What level of confidence the team places in the results
- What the top few risks and opportunities are
- How the results relate to current risks/opportunities being managed
- Implications of the results for staffing, funding, working in relation to current setting
- Your/team recommendation

Sample Reporting Views

ISO 31000 Illustrative Risk Heat Map

Management addresses these key risks and opportunities in its plans and priorities
Note: Some adjustment to current priorities may be required



Opportunities

Risks

RiskResults Consulting Inc. 2012

Key Concept 4: Using/Integrating Risk Assessment Results

Business Planning & Operations

Risk Assessments inform decisions about…

- Business plans
- Financial plans
- Human resource strategies
- Projects
- Operational plans

Key Concept 4: Using/Integrating Risk Assessment Results

Risk Assessment in Relation to Business Planning & Operations

Guidance:

- The Risk Management Process is applied to support one of these activities. You'll establish which activity(ies) at the 'Establish the Context' step of the Process. Risk Assessment results should be viewed in relation to current activity in your organization.
- The Risk Assessment Results should answer the question 'So What?": For example, if we proceed with this decision, given what we know about the risks and opportunities, we will need to adjust our funding, people, work priorities (in our operations, this project, our budget and staffing plans/business plans)

KEY LEARNING

To realize the benefit of risk assessment you will need to consider change implications to your funding, staffing and work.

1. **How do the results affect those risks and opportunities you are currently managing? Do they displace any?**
2. **What do we need to stop/start doing/do more or less of?**

Key Concept 4: Using /Integrating Risk Assessment Results

Risk Assessment in Relation to Enterprise Risk Management

Ensure that risk assessment results align to ERM framework requirements

- Centered on organizational objectives
- Viewed in relation to your organization's risk criteria (e.g. is the result within or outside of your risk appetite?)
- Use of a common RM process
- Cross-functional involvement through the RM process
- Involvement of ERM owners for advice and support
- Use of organizational/corporate risk profile results (if available)

Situating Risk Assessment Results in Relation to Organizational/Corporate Risk Profile Results (Actual Example)

Significant Risks	Alignment to Organization/Corporate Risk Profile (and ranking)	Significant Opportunities
R4-Scientific Validity of health Information R8-Ongoing management of health care services R15-Quality of health care Assessments for seniors	• Incident Resulting in Harm to Health of Citizens (1st) • Inadequate Laboratory and Physical Infrastructure (3rd) • Financial Integrity of Key Programs (2nd)	O2-Ability to consolidate and improve lab infrastructure in certain regions O4-We may be able to streamline and harmonize our health care services
R19-Stakeholder Risk Perceptions R22-Delivery of our Outcomes R30-Risk Communication	• Decision Resulting in Harm to Health of Citizens (7th) • Information Management (8th) • Public, Regulatory and Shareholder Expectations/Need for Information (10th)	O17-We may be able to improve information quality, privacy and security with fewer locations and more consistent controls O21-By following our regulator's approach to regional locations, we may be able to strengthen our relationship with them and influence policy and programs
R13-Increased Industry Burden R14-Competing Internal Priorities	• Internal Horizontal Management (4th)	O9-Fewer locations may provide us with clearer, more consistent governance and decision making

Sample Executive Summary

Relationship of Current Corporate Priorities and Division Business Goals to Major Risks & Opportunities

Question: "Given where our major risks & opportunities are, how well do our current priorities/business goals address them? Where are our gaps?"

Corporate Priorities	Division Business Goals
Achieving excellence in the workplace	Goal 1: Plan for the succession of division employees Goal 2: Preserve and share corporate knowledge
Improving management practices	Goal 3: Find efficient ways of doing business, strengthening accountability, improving management practices and performance Goal 4: Strengthen strategic focus, coherence and integration of organization-wide activities

Major Risks		
Div-R12: That the security & privacy of information may be compromised	●●●	❍ (G3)
Div R-37: That Divisional priorities may not be fulfilled due to misallocations of resources	●●	❍ (G1/4)

Major Opportunities		
Div O-11: There may be an opportunity to improve the level of awareness and support for corporate governance	●●●	❍ (G3/4)
Div O-1: There may be an opportunity to improve succession planning	●	●● (G1)

Legend: ●●●=very well/●●=well/●=somewhat/❍=not at all

Situating Risk Assessment Results in Relation to Organizational/Corporate Risk Profile Results (Actual Example)

ABC Organization – Sample Corporate Risk Profile - Current Year

Attracting and Retaining Key Scientific Talent

There is a risk that our organization may be unable to successfully achieve its objective of ensuring the safety of products and the environment for our stakeholders due to challenges with attracting and retaining key scientific talent. Our organization has recognized the significant shortage of experienced health scientists and researchers. Key scientists are required to ensure we meet health, food and environmental/ industrial product regulations.

Shortage of Health Professionals (Corporate Risk Profile - Current Year)

The national shortage of nurses and community medicine specialists is expected to continue and to put significant pressure on our healthcare services business area, particularly in remote locations. The shortage of other members of the health care team also adds pressure on service delivery in these communities. This risk could impact our contractual responsibilities for providing health care services and programs to designated communities.

Detailed Risk Assessment Results (Priority Risks Only)

Decision: Close down and consolidate half of our twelve regional offices

ID	Risk Statement	Context	Risk Rating
R2	That regions may be unable to attract and retain sufficient, skilled human resources	A more significant challenge has been the ability of the regions to attract and retain sufficient human resources with necessary technical skills in the face of competition from other employers competing for the relatively small pool of qualified candidates. • Difficulties were also encountered in recruiting and retaining staff with needed skills, as well as the availability of suitably experienced middle managers to manage and direct regional activities and support front line staff. • Certain major regional offices with lab facilities are at risk of being unable to recruit staff with specialized expertise, particularly middle managers in scientific categories. As a results we may not be able to find the right mix of people and skills to deliver its programs.	
R17	That we may be unable to maintain the service levels for seniors health care assessments	In some instances, this was an issue of having sufficient staff to handle the workloads generated by current service commitments resulting in significant workload pressures. It is unclear if or how we can maintain the current pace of health care assessments for seniors into next year, given increasing service demands. How can assessments maintain the current level of quality?	

MODULE 4

CHALLENGES IN RISK ASSESSMENT

Checkpoint

- What are the key things you've learned about risk assessment and method selection/application so far?
- What challenges do you expect to encounter or have you encountered in conducting risk assessments? How would you deal with them?

Risk Assessment Challenges

Issue	Target Reality	Possible Action
• Sometimes those who are involved in developing Risk Assessments are not able to see how their efforts were considered in the final decision.	• "The risk management process should be open and transparent while respecting the organization's context." (ISO 31000:2009)	❑ Table transparency during the risk assessment and decision making processes as a discussion at the start with the decision maker to get feedback and support.
• Information used in risk assessments can be low quality (e.g. incomplete, unavailable, absent of research or facts, etc.)	• "The risk management process should be applied using the best possible information regarding uncertainty."	❑ Present risk assessment results summarizing who was involved, how much time was taken, the team's general level of confidence in the reliability of the risk information being presented and what further action could be taken to improve the reliability of RA results.

WORKSHOP SUMMARY

Workshop Summary

This course set out to

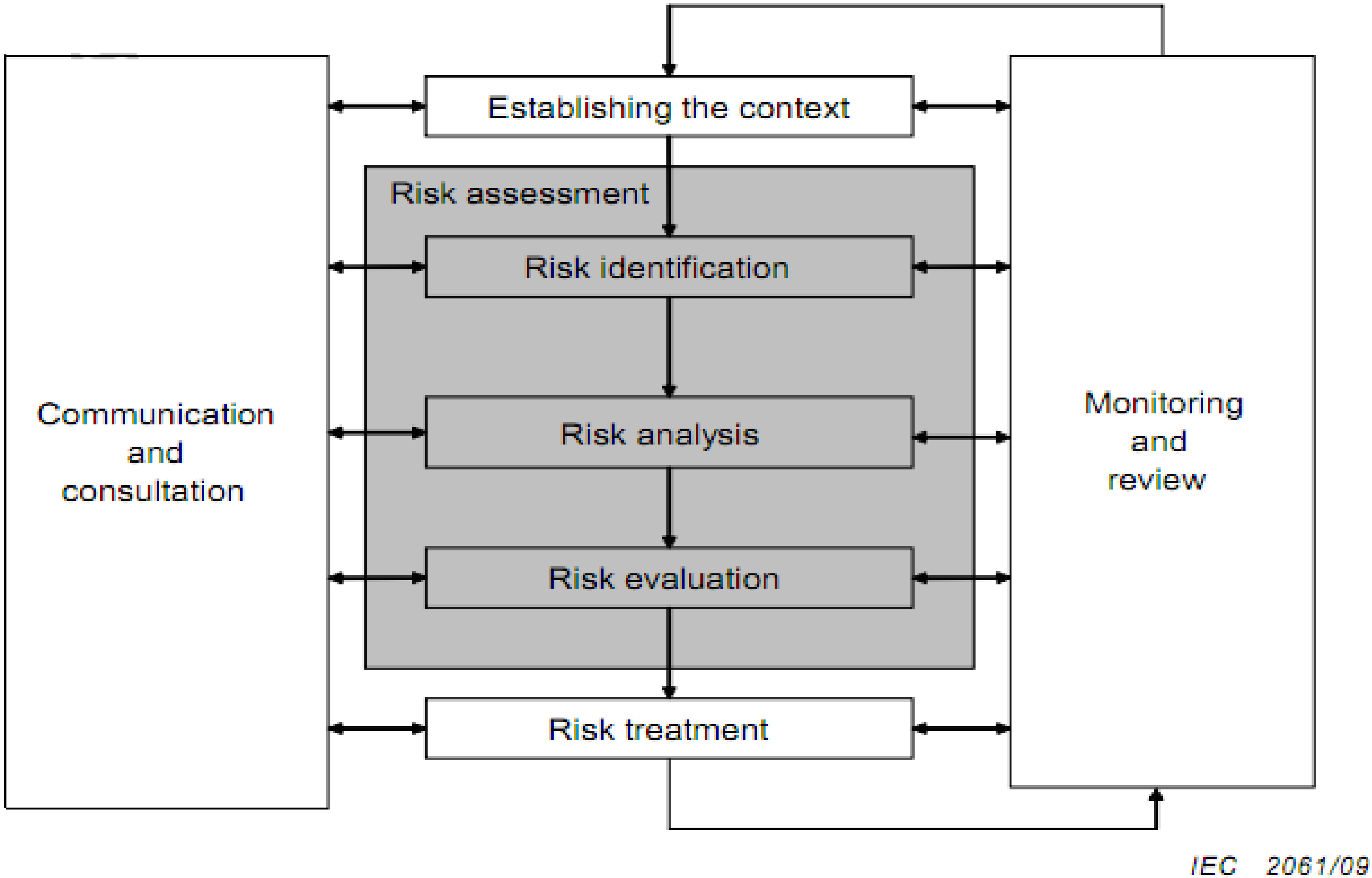
1. Increase your comfort and confidence in developing risk information that supports decision making and adds value to your organization
2. Heighten your awareness of international expectations in risk assessment based on ISO 31010 - Risk Assessment Standard

We did that by…

- ❑ Applying case studies to a common risk management process
- ❑ Describing key risk assessment concepts
- ❑ Learning how to select and apply risk assessment method(s)
- ❑ Situating the risk assessment results in relation to organizational objectives and an ERM framework

IEC/ISO 31010 Recap

Edition 1.0 2009-11



Reproduced from *ISO 31000* with permission from ISO at www. iso.org. Copyright remains with ISO

APPENDIX A: MONITORING/REVIEW & COMMUNICATION/CONSULTATION

Triggers for Monitoring Risk Assessment Results

You will want to revisit risk assessments when….

a) There have been major changes to your internal or external environment
b) Organizational objectives/mandate/legislation changes
c) Senior leadership shifts
d) Major events happen (to your industry or supply chain, natural or intentional acts, etc.)
e) To check on whether or not a risk treatment is being properly applied and effective

Designate who is accountable for reviewing and monitoring risk assessment results.

Communication and Consultation

Involving stakeholders in the risk management process will assist in

- developing a communication plan,
- defining the context appropriately,
- ensuring that the interests of stakeholders are understood and considered,
- bringing together different areas of expertise for identifying and analysing risk,
- ensuring that different views are appropriately considered in evaluating risks,
- ensuring that risks are adequately identified,
- securing endorsement and support for a treatment plan.

Stakeholders should contribute to the interfacing of the risk assessment process with other management disciplines, including change management, project and programme management, and also financial management.

•ISO 31010 2009 Section 4.3.2

All communication and consultation that occurs at any step of the risk management process should occur within the current communication and consultation policy, framework, style and requirements of your organization

The RIMS Risk Assessment Toolkit

Applies to: Module 2 - Exercise 1 (Slides 21/22) **Key Concepts: Setting the Risk Assessment Context & Criteria**	
1. Clarify the decision to be made - Is it a 'Yes or No' type of decision? - Will the risk assessment be used to inform option analysis? If yes, be clear on what the options are. For risk assessment purposes you will use the current state as your 'Option 1' - How significant is the decision to organizational objectives (e.g. major significance = significant risk assessment effort)? - Which organizational objective(s) does this decision support?	My Response & Assumptions
2. Clarify the time frame available for risk assessment - When does the decision maker need the information? - What are <u>all</u> the steps that your decision maker will take – do you know where risk assessment step fits in that process? First? last?	
3. What resources will you need to inform your risk assessment? - Internal colleagues: business area, technical knowledge, internal auditors, corporate functions - External knowledge: specialized expertise - Information: stakeholder/customer or employee satisfaction surveys, studies, audits, reports, claims history, industry or other environmental/social/economic trend analysis, interviews, etc.	
4. Who are the stakeholders that could be impacted by the decision? - Develop a stakeholder map like this one OR - Reach out to your communications resource to see if they have one	

Applies to: Module 2 - Exercise 1 (Continued) (Slide 30)
Key Concepts: Setting the Risk Assessment Context & Criteria

Decisions we will need to make include:	My Responses
a) How would we describe this organization's risk appetite? b) To help rate risks and opportunities, will we use dual or tri-attribute criteria? a. Likelihood (probability) b. Impact (consequence) c. Exposure (relevant?) c) What scale makes sense? (3X3, 4X4, 5X5, 10X10?) **d)** What is your own experience in developing or using risk criteria?	

Sample Risk Criteria

LIKELIHOOD RATING (SAMPLE)	
An estimate of the possibility of a risk occuring	
Almost certain (3)	This event is most likely to occur undercertain circumstances
Medium (2)	This event may occur under certain circumstances.
Unlikely (1)	This event may only occur under exceptional circumstances

IMPACT RATING (SAMPLE)

Measures of Impact	Financial	Operational	Reputational
RISK			
Major (3)	• Death or permanent disability or illness • Loss or disclosure of highly sensitive information	• Significant disruption in service delivery • Significant loss of corporate knowledge • Significant under-achievement of expected results	• Significant loss of international trust • Severe criticism by external stakeholders (regulators, shareholders, etc.)
Moderate (2)	• Serious disability/long-term illness • Disclosure of sensitive information	• Moderate disruption in delivery of some business areas • Some loss of corporate knowledge • Some under-achievement of expected results	• Negative media attention • Public criticism • Some loss of international trust •Strong recommendations by external stakeholders
Nominal (1)	• Minor injury or short-term illness • Disclosure of protected information	• Disruption in program delivery • Setbacks in achievement of expected results	• Unfavourable media attention • Setback in international trust • Improvements suggested by stakeholders
OPPORTUNITY			
Minor (1)	• Improving Productive, motivated and healthy workplace • Comply with procedures, policies (ie. Program authorities, security/personal information, etc.)	• Customers are aware of and can access many of our program/services • Changes to minor projects	• Some favourable media or public attention • Some favourable observations by stakeholders
Moderate (2)	• Productive, motivated and healthy workplace •Client information or disclosure of sensitive information does not occur • Some sustainable development targets met • Budget met	• Some operational objectives exceeded • Significant improvement in projects: 1-2 months; or, important functionality • Key corporate knowledge in most areas of the organization	• Clear evidence of trust from stakeholders • Clear evidence of employee trust • Regarded as an employer of choice •Rare criticism by stakeholders
Major (3)	• Model workplace and target employer of choice • Sustainable development targets met • Legally aware and compliant employee decisions • Budget optimized • Effective asset management strategy	•Ongoing and effective knowledge management • Reliable, continuously available, high quality services • Sustained achievement of operational objectives • Key projects completed successfully	• Significant, sustained trust from stakeholders • Significant employee trust and credibility • Significant and consistently positive Media report

Applies to Module 2 Exercise 2 (Slides 36 & 49) **Selecting Risk Assessment Methods**	
1. Confirm the Context. Where several options are available, risk assessment can be used to evaluate options relative to a baseline or status quo state, to help decide which provides the best balance of risks. *Think: organizational objectives, the significance of the decision, stakeholders.* 2. Resources: What resources do you have? What resources do you need? *Think: time, money, people, expertise.* 3. Do you have enough/quality information? *Think: where can you go to get data, is it accessible to you, is it good quality?* **4.** What other factors could affect the complexity of the risk assessment? *Think: interdependent factors of this decision on existing decisions, range of impacts .*	My Responses

Note: Refer to ISO 31010, Annexes A & B to help

Applies to Module 2 Case Study Exercise 3 (Slide 64) **Applying Risk Assessment Methods**	
What you need ❑ Your chosen case study ❑ Objectives relevant to your case study ❑ A risk rating system of your choice or the course-supplied rating system in the Risk Assessment Toolkit **What to do** 1. Identify risks and opportunities using the risk assessment method of your choice from Exercise 2 and the worksheet below. 2. For each risk and each opportunity, briefly list the key controls in place today (people, processes and systems) 3. Rate the likelihood and impact on objectives for each risk. Repeat for each opportunity. 4. Summarize the results to present the priority risks and opportunities (use Executive Summary checklist).	My Responses Use the worksheets that follow and populate your responses following the 'what to do' instructions.

Risk Assessment Toolkit & Worksheets	
Corporate Objectives:	
Business Unit Objectives:	
Stakeholders (Internal)	
Stakeholders (External)	
Decision context (What is the decision to be made, for who, how much time do you have, how significant is the decision, who should be involved)	

Risk Worksheet (*"that x may occur")*	**Current controls**	**Estimated Likelihood**	**Estimated Impact on objective**
Describe risk or opportunity here	People, processes, systems in place today	3-Almost certain 2-Likely 1-Unlikely	3-Major 2-Moderate 1-Insignificant
R1			
R2			
R3			
R4			
R5			

O1			
O2			
O3			
O4			
O5			

Applies to Module 3 Case Study Exercise 4 (Slides 69 & 77)
Presenting Risk Assessment Results

Our Executive Summary for ______________________________________ Case Study

____
____
____
____
____
____
____
____
____
____
____

Opportunities **Risks**

The executive summary of risk assessment results should contain:

- ❑ The decision context/organizational objectives
- ❑ How many risks/opportunities were identified
- ❑ Who was involved over what time period
- ❑ What level of confidence the team places in the results
- ❑ What the top few risks and opportunities are
- ❑ How the results relate to current risks/opportunities being managed
- ❑ Implications of the results for staffing, funding, working in relation to current setting
- ❑ Your/team recommendation

The following handout includes Appendix A & B from the:
ANSI/ASSE/IEC/ISO 31010 (Z690.3-2011)
Risk Assessment Techniques
National Adoption of:
IEC/ISO 31010:2009

Approved American National Standard
ANSI

AMERICAN NATIONAL STANDARD

ANSI/ASSE/IEC/ISO 31010 (Z690.3-2011)

ANSI/ASSE/IEC/ISO 31010 (Z690.3-2011)
Risk Assessment Techniques

National Adoption of:
IEC/ISO 31010:2009

AMERICAN SOCIETY OF SAFETY ENGINEERS

Annex A
(informative)

Comparison of Risk Assessment Techniques

A.1 Types of Technique.

The first classification shows how the techniques apply to each step of the risk assessment process as follows:

- risk identification;
- risk analysis – consequence analysis;
- risk analysis – qualitative, semi-quantitative or quantitative probability estimation;
- risk analysis – assessing the effectiveness of any existing controls;
- risk analysis – estimation the level of risk;
- risk evaluation.

For each step in the risk assessment process, the application of the method is described as being either strongly applicable, applicable or not applicable (see Table A.1).

A.2 Factors Influencing Selection of Risk Assessment Techniques.

Next the attributes of the methods are described in terms of:

- complexity of the problem and the methods needed to analyze it,
- the nature and degree of uncertainty of the risk assessment based on the amount of information available and what is required to satisfy objectives,
- the extent of resources required in terms of time and level of expertise, data needs or cost,
- whether the method can provide a quantitative output.

Examples of types of risk assessment methods available are listed in Table A.2 where each method is rated as high medium or low in terms of these attributes.

Table A.1 – Applicability of Tools Used for Risk Assessment

Tools and Techniques	Risk Assessment Process					See Annex
	Risk Identification	Risk Analysis			Risk Evaluation	
		Consequence	Probability	Level of Risk		
Brainstorming	SA[1]	NA[2]	NA	NA	NA	B 01
Structured or Semi-Structured Interviews	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Checklists	SA	NA	NA	NA	NA	B 04
Primary Hazard Analysis	SA	NA	NA	NA	NA	B 05
Hazard and Operability Studies (HAZOP)	SA	SA	A[3]	A	A	B 06
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA	B 07
Environmental Risk Assessment	SA	SA	SA	SA	SA	B 08
Structure <<What if?>> (SWIFT)	SA	SA	SA	SA	SA	B 09
Scenario Analysis	SA	SA	A	A	A	B 10
Business Impact Analysis	A	SA	A	A	A	B 11
Root Cause Analysis	NA	SA	SA	SA	SA	B 12
Failure Mode Effect Analysis	SA	SA	SA	SA	SA	B 13
Fault Tree Analysis	A	NA	SA	A	A	B 14
Event Tree Analysis	A	SA	A	A	NA	B 15
Cause and Consequence Analysis	A	SA	SA	A	A	B 16
Cause-and-Effect Analysis	SA	SA	NA	NA	NA	B 17
Layer Protection Analysis (LOPA)	A	SA	A	A	NA	B 18
Decision Tree	NA	SA	SA	A	A	B 19
Human Reliability Analysis	SA	SA	SA	SA	A	B 20
Bow Tie Analysis	NA	A	SA	SA	A	B 21
Reliability Centered Maintenance	SA	SA	SA	SA	SA	B 22
Sneak Circuit Analysis	A	NA	NA	NA	NA	B 23
Markov Analysis	A	SA	NA	NA	NA	B 24
Monte Carlo Simulation	NA	NA	NA	NA	SA	B 25
Bayesian Statistics and Bayes Nets	NA	SA	NA	NA	SA	B 26
FN Curves	A	SA	SA	A	SA	B 27
Risk Indices	A	SA	SA	A	SA	B 28
Consequence/Probability Matrix	SA	SA	SA	SA	A	B 29
Cost/Benefit Analysis	A	SA	A	A	A	B 30
Multi-Criteria Decision Analysis (MCDA)	A	SA	A	SA	A	B 31

[1] Strongly Applicable.

[2] Not Applicable.

[3] Applicable.

Table A.2 – Attributes of a Selection of Risk Assessment Tools

Type of Risk Assessment Technique	Description	Relevance of Influencing Factors			Can Provide Quantitative Output
		Resources and Capability	Nature and Degree of Uncertainty	Complexity	
LOOK-UP METHODS					
Checklists	A simple form of risk identification. A technique which provides a listing of typical uncertainties which need to be considered. Users refer to a previously developed list, codes or standards.	Low	Low	Low	No
Preliminary Hazard Analysis	A simple inductive method of analysis whose objective is to identify the hazards and hazardous situations and events that can cause harm for a given activity, facility or system.	Low	High	Medium	No
SUPPORTING METHODS					
Structured Interview and Brainstorming	A means of collecting a broad set of ideas and evaluation, ranking them by a team. Brainstorming may be stimulated by prompts or by one-on-one and one-on-many interview techniques.	Low	Low	Low	No
Delphi Technique	A means of combining expert opinions that may support the source and influence identification, probability and consequence estimation and risk evaluation. It is a collaborative technique for building consensus among experts. Involving independent analysis and voting by experts.	Medium	Medium	Medium	No
SWIFT Structured <<What-If>>	A system for prompting a team to identify risks. Normally used within a facilitated workshop. Normally linked to a risk analysis and evaluation technique.	Medium	Medium	Any	No
Human Reliability Analysis (HRA)	Human reliability assessment (HRA) deals with the impact of humans on system performance and can be used to evaluate human error influences on the system.	Medium	Medium	Medium	Yes
SCENARIO ANALYSIS					
Root Cause Analysis (Single Loss Analysis)	A single loss that has occurred is analyzed in order to understand contributory causes and how the system or process can be improved to avoid such future losses. The analysis shall consider what controls were in place at the time the loss occurred and how controls might be improved.	Medium	Low	Medium	No
Scenario Analysis	Possible future scenarios are identified through imagination or extrapolation from the present and different risks considered assuming each of these scenarios might occur. This can be done formally or informally qualitatively or quantitatively.	Medium	High	Medium	No
Toxicological Risk Assessment	Hazards are identified and analyzed and possible pathways by which a specified target might be exposed to the hazard are identified. Information on the level of exposure and the nature of harm caused by a given level of exposure are combined to give a measure of the probability that the specified harm will occur.	High	High	Medium	Yes
Business Impact Analysis	Provides an analysis of how key disruption risks could affect an organization's operations and identifies and quantifies the capabilities that would be required to manage it.	Medium	Medium	Medium	No
Fault Tree Analysis	A technique which starts with the undesired event (top event) and determines all the ways in which it could occur. These are displayed graphically in a logical tree diagram. Once the fault tree has been developed, consideration should be given to ways of reducing or eliminating potential causes/sources.	High	High	Medium	Yes
Event Tree Analysis	Using inductive reasoning to translate probabilities of different initiating events into possible outcomes.	Medium	Medium	Medium	Yes
Cause/ Consequence Analysis	A combination of fault and event tree analysis that allows inclusion of time delays. Both causes and consequences of an initiating event are considered.	High	Medium	High	Yes
Cause-and-Effect Analysis	An effect can have a number of contributory factors which may be grouped into different categories. Contributory factors are identified often through brainstorming and displayed in a tree structure or fishbone diagram.	Low	Low	Medium	No

Example Type of Risk Assessment Method and Technique	**Description**	**Relevance of Influencing Factors**			**Quantitative Output Possible?**
FUNCTION ANALYSIS					
FMEA and FMECA	FMEA (Failure Mode and Effect Analysis) is a technique which identifies failure modes and mechanisms, and their effects. There are several types of FMEA: Design (or product) FMEA which is used for components and products. System FMEA which is used for systems. Process FMEA which is used for manufacturing and assembly processes. Service FMEA and Software FMEA. FMEA may be followed by a criticality analysis which defines the significance of each failure mode, qualitatively, semi-qualitatively, or quantitatively (FMECA). The criticality analysis may be based on the probability that the failure mode will result in system failure, or the level of risk associated with the failure mode, or a risk priority number.	Medium	Medium	Medium	Yes
Reliability-Centered Maintenance	A method to identify the policies that should be implemented to manage failures so as to efficiently and effectively achieve the required safety, availability and economy of operation for all types of equipment.	Medium	Medium	Medium	Yes
Sneak Analysis (Sneak Circuit Analysis)	A methodology for identifying design errors. A sneak condition is a latent hardware, software, or integrated condition that may cause an unwanted event to occur or may inhibit a desired event and is not caused by component failure. These conditions are characterized by their random nature and ability to escape detection during the most rigorous of standardized system tests. Sneak conditions can cause improper operation, loss of system availability, program delays, or even death or injury to personnel.	Medium	Medium	Medium	No
HAZOP Hazard and Operability Studies	A general process of risk identification to define possible deviations from the expected or intended performance. It uses a guideword based system. The criticalities of the deviations are assessed.	Medium	High	High	No
HACCP Hazard Analysis and Critical Control Points	A systematic, proactive, and preventive system for assuring product quality, reliability and safety of processes by measuring and monitoring specific characteristics which are required to be within defined limits.	Medium	Medium	Medium	No
CONTROLS ASSESSMENT					
LOPA (Layers of Protection Analysis)	(May also be called barrier analysis). It allows controls and their effectiveness to be evaluated.	Medium	Medium	Medium	Yes
Bow Tie Analysis	A simple diagrammatic way of describing and analyzing the pathways of a risk from hazards to outcomes and reviewing controls. It can be considered to be a combination of the logic of a fault tree analyzing the cause of an event (represented by the knot of a bow tie) and an event tree analyzing the consequences.	Medium	High	Medium	Yes

Example Type of Risk Assessment Method and Technique	**Description**	**Relevance of Influencing Factors**			**Quantitative Output Possible?**
STATISTICAL METHODS					
Markov Analysis	Markov analysis, sometimes called *State-space* analysis, is commonly used in the analysis of repairable complex systems that can exist in multiple states, including various degraded states.	High	Low	High	Yes
Monte Carlo Analysis	Monte Carlo simulation is used to establish the aggregate variation in a system resulting from variations in the system, for a number of inputs, where each input has a defined distribution and the inputs are related to the output via defined relationships. The analysis can be used for a specific model where the interactions of the various inputs can be mathematically defined. The inputs can be based upon a variety of distribution types according to the nature of the uncertainty they are intended to represent. For risk assessment, triangular distributions or beta distributions are commonly used.	High	Low	High	Yes
Bayesian Analysis	A statistical procedure which utilizes prior distribution data to assess the probability of the result. Bayesian analysis depends upon the accuracy of the prior distribution to deduce an accurate result. Bayesian belief networks model cause-and-effect in a variety of domains by capturing probabilistic relationships of variable inputs to derive a result.	High	Low	High	Yes

Annex B
(informative)

Risk Assessment Techniques

B.1 Brainstorming.

B.1.1 Overview.

Brainstorming involves stimulating and encouraging free-flowing conversation amongst a group of knowledgeable people to identify potential failure modes and associated hazards, risks, criteria for decisions and/or options for treatment. The term “brainstorming” is often used very loosely to mean any type of group discussion. However true brainstorming involves particular techniques to try to ensure that people's imagination is triggered by the thoughts and statements of others in the group.

Effective facilitation is very important in this technique and includes stimulation of the discussion at kick-off, periodic prompting of the group into other relevant areas and capture of the issues arising from the discussion (which is usually quite lively).

B.1.2 Use.

Brainstorming can be used in conjunction with other risk assessment methods described below or may stand alone as a technique to encourage imaginative thinking at any stage of the risk management process and any stage of the life cycle of a system. It may be used for high-level discussions where issues are identified, for more detailed review or at a detailed level for particular problems.

Brainstorming places a heavy emphasis on imagination. It is therefore particularly useful when identifying risks of new technology, where there is no data or where novel solutions to problems are needed.

B.1.3 Inputs.

A team of people with knowledge of the organization, system, process or application being assessed.

B.1.4 Process.

Brainstorming may be formal or informal. Formal brainstorming is more structured with participants prepared in advance and the session has a defined purpose and outcome with a means of evaluating ideas put forward. Informal brainstorming is less structured and often more ad-hoc.

In a formal process:

- the facilitator prepares thinking prompts and triggers appropriate to the context prior to the session;
- objectives of the session are defined and rules explained;

- the facilitator starts off a train of thought and everyone explores ideas identifying as many issues as possible There is no discussion at this point about whether things should or should not be in a list or what is meant by particular statements because this tends to inhibit free-flowing thought. All input is accepted and none is criticized and the group moves on quickly to allow ideas to trigger lateral thinking;

- the facilitator may set people off on a new track when one direction of thought is exhausted or discussion deviates too far. The idea however, is to collect as many diverse ideas as possible for later analysis.

B.1.5 Outputs.

Outputs depend on the stage of the risk management process at which it is applied, for example at the identification stage, outputs might be a list of risks and current controls.

B.1.6 Strengths and Limitations.

Strengths of brainstorming include:

- it encourages imagination which helps identify new risks and novel solutions;

- it involves key stakeholders and hence aids communication overall;

- it is relatively quick and easy to set up.

Limitations include:

- participants may lack the skill and knowledge to be effective contributors;

- since it is relatively unstructured, it is difficult to demonstrate that the process has been comprehensive, e.g. that all potential risks have been identified;

- there may be particular group dynamics where some people with valuable ideas stay quiet while others dominate the discussion. This can be overcome by computer brainstorming, using a chat forum or nominal group technique. Computer brainstorming can be set up to be anonymous, thus avoiding personal and political issues which may impede free flow of ideas. In nominal group technique ideas are submitted anonymously to a moderator and are then discussed by the group.

B.2 Structured or Semi-Structured Interviews.

B.2.1 Overview.

In a structured interview, individual interviewees are asked a set of prepared questions from a prompting sheet which encourages the interviewee to view a situation from a different perspective and thus identify risks from that perspective. A semi-structured interview is similar, but allows more freedom for a conversation to explore issues which arise.

B.2.2 Use.

Structured and semi-structured interviews are useful where it is difficult to get people together for a brainstorming session or where free-flowing discussion in a group is not appropriate for the situation or people involved. They are most often used to identify risks or to assess effectiveness of existing controls as part of risk analysis. They may be applied at any stage of a project or process. They are a means of providing stakeholder input to risk assessment.

B.2.3 Inputs.

Inputs include:

- a clear definition of the objectives of the interviews;
- a list of interviewees selected from relevant stakeholders;
- a prepared set of questions.

B.2.4 Process.

A relevant question set, is created to guide the interviewer. Questions should be open-ended where possible, should be simple, in appropriate language for the interviewee and cover one issue only. Possible follow-up questions to seek clarification are also prepared.

Questions are then posed to the person being interviewed. When seeking elaboration, questions should be open-ended. Care should be taken not to “lead” the interviewee.

Responses should be considered with a degree of flexibility in order to provide the opportunity of exploring areas into which the interviewee may wish to go.

B.2.5 Outputs.

The outputs are the stakeholder’s views on the issues which are the subject of the interviews.

B.2.6 Strengths and Limitations.

The strengths of structured interviews are as follows:

- structured interviews allow people time for considered thought about an issue;
- one-to-one communication may allow more in-depth consideration of issues;
- structured interviews enable involvement of a larger number of stakeholders than brainstorming which uses a relatively small group.

Limitations are as follows:

- it is time-consuming for the facilitator to obtain multiple opinions in this way;
- bias is tolerated and not removed through group discussion;

- the triggering of imagination which is a feature of brainstorming may not be achieved.

B.3 Delphi Technique.

B.3.1 Overview.

The Delphi technique is a procedure to obtain a reliable consensus of opinion from a group of experts. Although the term is often now broadly used to mean any form of brainstorming, an essential feature of the Delphi technique, as originally formulated, was that experts expressed their opinions individually and anonymously while having access to the other expert's views as the process progresses.

B.3.2 Use.

The Delphi technique can be applied at any stage of the risk management process or at any phase of a system life cycle, wherever a consensus of views of experts is needed.

B.3.3 Inputs.

A set of options for which consensus is needed.

B.3.4 Process.

A group of experts are questioned using a semi-structured questionnaire. The experts do not meet so their opinions are independent.

The procedure is as follows:

- formation of a team to undertake and monitor the Delphi process;
- selection of a group of experts (may be one or more panels of experts);
- development of round 1 questionnaire;
- testing the questionnaire;
- sending the questionnaire to panelists individually;
- information from the first round of responses is analyzed and combined and recirculated to panelists;
- panelists respond and the process is repeated until consensus is reached.

B.3.5 Outputs.

Convergence toward consensus on the matter in hand.

B.3.6 Strengths and Limitations.

Strengths include:

- as views are anonymous, unpopular opinions are more likely to be expressed;
- all views have equal weight, which avoids the problem of dominating personalities;
- achieves ownership of outcomes;
- people do not need to be brought together in one place at one time.

Limitations include:

- it is labor intensive and time consuming;
- participants need to be able to express themselves clearly in writing.

B.4 Checklists.

B.4.1 Overview.

Checklists are lists of hazards, risks or control failures that have been developed usually from experience, either as a result of a previous risk assessment or as a result of past failures.

B.4.2 Use.

A checklist can be used to identify hazards and risks or to assess the effectiveness of controls. They can be used at any stage of the life cycle of a product, process, or system. They may be used as part of other risk assessment techniques but are most useful when applied to check that everything has been covered after a more imaginative technique that identifies new problems has been applied.

B.4.3 Inputs.

Prior information and expertise on the issue, such that a relevant and preferably validated checklist can be selected or developed.

B.4.4 Process.

The procedure is as follows:

- the scope of the activity is defined;
- a checklist is selected which adequately covers the scope. Checklists need to be carefully selected for the purpose. For example a checklist of standard controls cannot be used to identify new hazards or risks;
- the person or team using the checklist steps through each element of the process or system and reviews whether items on the checklist are present.

B.4.5 Outputs.

Outputs depend on the stage of the risk management process at which they are applied. For example output may be a list of controls which are inadequate or a list of risks.

B.4.6 Strengths and Limitations.

Strengths of checklists include:

- they may be used by non experts;
- when well designed, they combine wide ranging expertise into an easy to use system;
- they can help ensure common problems are not forgotten.

Limitations include:

- they tend to inhibit imagination in the identification of risks;
- they address the ‘known known’s’, not the ‘known unknown’s or the ‘unknown unknowns’.
- they encourage ‘tick the box’ type behavior;
- they tend to be observation based, so miss problems that are not readily seen.

B.5 Preliminary Hazard Analysis (PHA).

B.5.1 Overview.

PHA is a simple, inductive method of analysis whose objective is to identify the hazards and hazardous situations and events that can cause harm for a given activity, facility or system.

B.5.2 Use.

It is most commonly carried out early in the development of a project when there is little information on design details or operating procedures and can often be a precursor to further studies or to provide information for specification of the design of a system. It can also be useful when analyzing existing systems for prioritizing hazards and risks for further analysis or where circumstances prevent a more extensive technique from being used.

B.5.3 Inputs.

Inputs include:

- information on the system to be assessed;
- such details of the design of the system as are available and relevant.

B.5.4 Process.

A list of hazards and generic hazardous situations and risks is formulated by considering characteristics such as:

- materials used or produced and their reactivity;
- equipment employed;
- operating environment;
- layout;
- interfaces among system components, etc.

Qualitative analysis of consequences of an unwanted event and their probabilities may be carried out to identify risks for further assessment.

PHA should be updated during the phases of design, construction and testing in order to detect any new hazards and make corrections, if necessary. The results obtained may be presented in different ways such as tables and trees.

B.5.5 Outputs.

Outputs include:

- a list of hazards and risks;
- recommendations in the form of acceptance, recommended controls, design specification or requests for more detailed assessment.

B.5.6 Strengths and Limitations.

Strengths include:

- that it is able to be used when there is limited information;
- it allows risks to be considered very early in the system lifecycle.

Limitations include:

- a PHA provides only preliminary information; it is not comprehensive, neither does it provide detailed information on risks and how they can best be prevented.

B.6 HAZOP.

B.6.1 Overview.

HAZOP is the acronym for **HAZ**ard and **OP**erability study and, is a structured and systematic examination of a planned or existing product, process, procedure or system. It is a technique to identify risks to people, equipment, environment and/or organizational objectives. The study team is also expected, where possible, to provide a solution for treating the risk.

The HAZOP process is a qualitative technique based on use of guide words which question how the design intention or operating conditions might not be achieved at each step in the design, process, procedure or system. It is generally carried out by a multi-disciplinary team during a set of meetings.

HAZOP is similar to FMEA in that it identifies failure modes of a process, system or procedure their causes and consequences. It differs in that the team considers unwanted outcomes and deviations from intended outcomes and conditions and works back to possible causes and failure modes, whereas FMEA starts by identifying failure modes.

B.6.2 Use.

The HAZOP technique was initially developed to analyze chemical process systems, but has been extended to other types of systems and complex operations. These include mechanical and electronic systems, procedures, and software systems, and even to organizational changes and to legal contract design and review.

The HAZOP process can deal with all forms of deviation from design intent due to deficiencies in the design, component(s), planned procedures and human actions.

It is widely used for software design review. When applied to safety critical instrument control and computer systems it may be known as CHAZOP (**C**ontrol **HAZ**ards and **OP**erability Analysis or computer hazard and operability analysis).

A HAZOP study is usually undertaken at the detail design stage, when a full diagram of the intended process is available, but while design changes are still practicable. It may however, be carried out in a phased approach with different guidewords for each stage as a design develops in detail. A HAZOP study may also be carried out during operation but required changes can be costly at that stage.

B.6.3 Inputs.

Essential inputs to a HAZOP study include current information about the system, the process or procedure to be reviewed and the intention and performance specifications of the design. The inputs may include: drawings, specification sheets, flow sheets, process control and logic diagrams, layout drawings, operating and maintenance procedures, and emergency response procedures. For non-hardware related HAZOP the inputs can be any document that describes functions and elements of the system or procedure under study. For example, inputs can be organizational diagrams and role descriptions, a draft contract or even a draft procedure.

B.6.4 Process.

HAZOP takes the “design” and specification of the process, procedure or system being studied and reviews each part of it to discover what deviations from the intended performance can occur, what are the potential causes and what are the likely consequences of a deviation. This is achieved by systematically examining how each part of the system, process or procedure will respond to changes in key parameters by using suitable guidewords. Guidewords can be customized to a particular system, process or procedure or generic words can be used that encompass all types of deviation. Table B.1 provides examples of commonly used guidewords for technical systems. Similar guidewords such as ‘too early’, ‘too late’, ‘too much’, ‘too little’, ‘too long’, ‘too short’, ‘wrong direction’, on ‘wrong object’, ‘wrong action’ can be used to identify human error modes.

The normal steps in a HAZOP study include:

- nomination of a person with the necessary responsibility and authority to conduct the HAZOP study and to ensure that any actions arising from the study are completed;
- definition of the objectives and scope of the study;
- establishing a set of key or guidewords for the study;
- defining a HAZOP study team; this team is usually multidisciplinary and should include design and operations personnel with appropriate technical expertise to evaluate the effects of deviations from intended or current design. It is recommended that the team include persons not directly involved in the design or the system, process or procedure under review;
- collection of the required documentation.

Within a facilitated workshop with the study team:

- splitting the system, process or procedure into smaller elements or sub-systems or sub-processes or sub-elements to make the review tangible;
- agreeing the design intent for each subsystem, sub-process or sub-element and then for each item in that subsystem or element applying the guidewords one after the other to postulate possible deviations which will have undesirable outcomes;
- where an undesirable outcome is identified, agreeing the cause and consequences in each case and suggesting how they might be treated to prevent them occurring or mitigate the consequences if they do;
- documenting the discussion and agreeing specific actions to treat the risks identified.

Table B.1 – Example of Possible HAZOP Guidewords

Terms	Definitions
No or not	No part of the intended result is achieved or the intended condition is absent.
More (higher)	Quantitative increase in output or in the operating condition.
Less (lower)	Quantitative decrease.
As well as	Quantitative increase (e.g. additional material).
Part of	Quantitative decrease (e.g. only one or two components in a mixture).
Reverse / opposite	Opposite (e.g. backflow)
Other than	No part of the intention is achieved, something completely different happens (e.g. flow or wrong material).
Compatibility	Material; environment.
Guide words are applied to parameters such as:	
	Physical properties of a material or process.
	Physical conditions such as temperature, speed.
	A specified intention of a component of a system or design (e.g. information transfer).
	Operational aspects.

B.6.5 Outputs.

Minutes of the HAZOP meeting(s) with items for each review point recorded. This should include: the guide word used, the deviation(s), possible causes, actions to address the identified problems and person responsible for the action.

For any deviation that cannot be corrected, then the risk for the deviation should be assessed.

B.6.6 Strengths and Limitations.

A HAZOP analysis offers the following advantages:

- it provides the means to systematically and thoroughly examine a system, process or procedure;
- it involves a multidisciplinary team including those with real-life operational experience and those who may have to carry out treatment actions;
- it generates solutions and risk treatment actions;
- it is applicable to a wide range of systems, processes and procedures;
- it allows explicit consideration of the causes and consequences of human error;

- it creates a written record of the process which can be used to demonstrate due diligence.

The limitations include:

- a detailed analysis can be very time-consuming and therefore expensive;
- a detailed analysis requires a high level of documentation or system/process and procedure specification;
- it can focus on finding detailed solutions rather than on challenging fundamental assumptions (however, this can be mitigated by a phased approach);
- the discussion can be focused on detail issues of design, and not on wider or external issues;
- it is constrained by the (draft) design and design intent, and the scope and objectives given to the team;
- the process relies heavily on the expertise of the designers who may find it difficult to be sufficiently objective to seek problems in their designs.

B.6.7 Reference Document.

IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

B.7 Hazard Analysis and Critical Control Points (HACCP).

B.7.1 Overview.

Hazard analysis and critical control point (HACCP) provides a structure for identifying hazards and putting controls in place at all relevant parts of a process to protect against the hazards and to maintain the quality reliability and safety of a product. HACCP aims to ensure that risks are minimized by controls throughout the process rather than through inspection of the end product.

B.7.2 Use.

HACCP was developed to ensure food quality for the NASA space program. It is now used by organizations operating anywhere within the food chain to control risks from physical, chemical or biological contaminants of food. It has also been extended for use in manufacture of pharmaceuticals and to medical devices. The principle of identifying things which can influence product quality, and defining points in a process where critical parameters can be monitored and hazards controlled, can be generalized to other technical systems.

B.7.3 Inputs.

HACCP starts from a basic flow diagram or process diagram and information on hazards which might affect the quality, safety or reliability of the product or process output. Information on the hazards and their risks and ways in which they can be controlled is an input to HACCP.

B.7.4 Process.

HACCP consists of the following seven principles:

- identifies hazards and preventive measures related to such hazards;
- determines the points in the process where the hazards can be controlled or eliminated (the critical control points or CCPs);
- establishes critical limits needed to control the hazards, i.e. each CCP should operate within specific parameters to ensure the hazard is controlled;
- monitors the critical limits for each CCP at defined intervals;
- establishes corrective actions if the process falls outside established limits;
- establishes verification procedures;
- implements record keeping and documentation procedures for each step.

B.7.5 Outputs.

Documented 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 this step;
- whether the hazards present a significant risk (based on consideration of consequence and probability from a combination of experience, data and technical literature);
- a justification for the significance;
- 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:

- 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.7.6 Strengths and Limitations.

Strengths include:

- a structured process that provides documented evidence for quality control as well as identifying and reducing risks;
- a focus on the practicalities of how and where, in a process, hazards can be prevented and risks controlled;
- better risk control throughout the process rather than relying on final product inspection;
- an ability to identify hazards introduced through human actions and how these can be controlled at the point of introduction or subsequently.

Limitations include:

- 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. These are required in order to specify critical control points and control parameters during HACCP and may need to be combined with other tools to achieve this;
- taking action when control parameters exceed defined limits may miss gradual changes in control parameters which are statistically significant and hence should be actioned.

B.7.7 Reference Document.

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

B.8 Toxicity Assessment.

B.8.1 Overview.

Environmental risk assessment is used here to cover the process followed in assessing risks to plants, animals and humans as a result of exposure to a range of environmental hazards. Risk management refers to decision-making steps including risk evaluation and risk treatment.

The method involves analyzing the hazard or source of harm and how it affects the target population, and the pathways by which the hazard can reach a susceptible target population. This information is then combined to give an estimate of the likely extent and nature of harm.

B.8.2 Use.

The process is used to assess risks to plants, animals and humans as a result of exposure to hazards such as chemicals, micro-organisms or other species.

Aspects of the methodology, such as pathway analysis which explore different routes by which a target might be exposed to a source of risk, can be adapted and used across a very wide range of different risk areas, outside human health and the environment, and is useful in identifying treatments to reduce risk.

B.8.3 Inputs.

The method requires good data on the nature and properties of hazards, the susceptibilities of the target population (or populations) and the way in which the two interact. This data is normally based on research which may be laboratory based or epidemiological.

B.8.4 Process.

The procedure is as follows:

a) Problem formulation – this includes setting the scope of the assessment by defining the range of target populations and hazard types of interest;

b) Hazard identification – this involves identifying all possible sources of harm to the target population from hazards within the scope of the study. Hazard identification normally relies on expert knowledge and a review of literature;

c) Hazard analysis – this involves understanding the nature of the hazard and how it interacts with the target. For example, in considering human exposure to chemical effects, the hazard might include acute and chronic toxicity, the potential to damage DNA, or the potential to cause cancer or birth defects. For each hazardous effect, the magnitude of the effect (the response) is compared to the amount of hazard to which the target is exposed (the dose) and, wherever possible, the mechanism by which the effect is produced is determined. The levels at which there is No Observable Effect (NOEL) and no Observable Adverse Effect (NOAEL) are noted. These are sometimes used as criteria for acceptability of the risk.

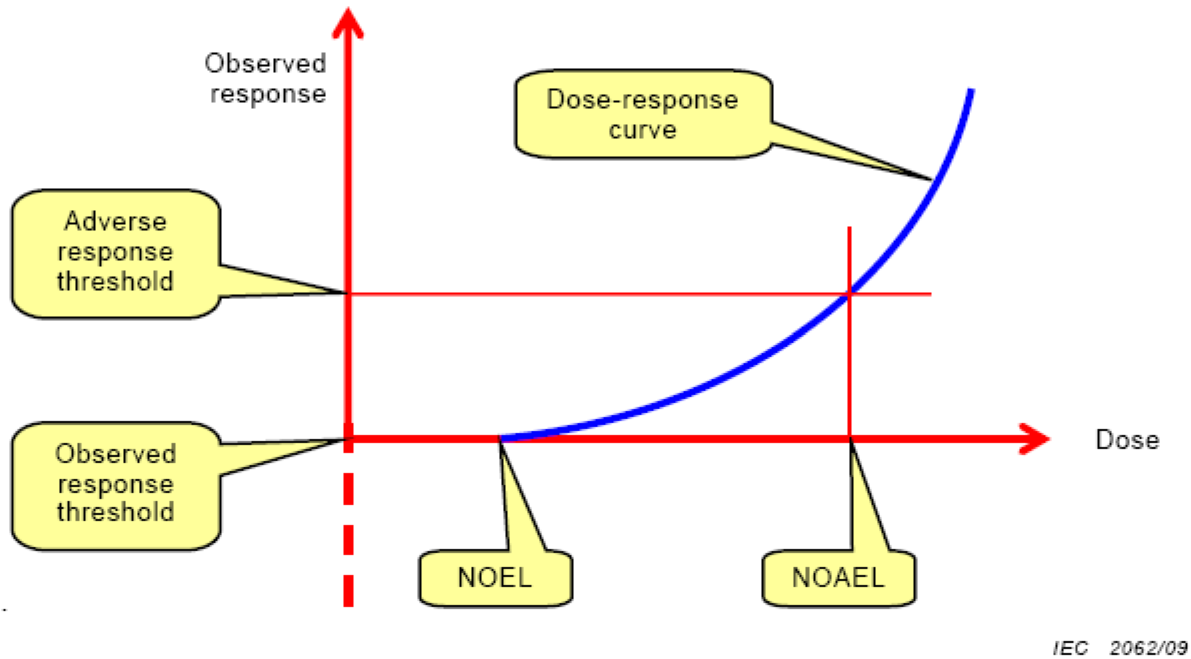


Figure B.1 – Dose-Response Curve

For chemical exposure, test results are used to derive dose-response curves such as that shown schematically in Figure B.1. These are usually derived from tests on animals or from experimental systems such as cultured tissues or cells.

Effects of other hazards such as micro-organisms or introduced species may be determined from field data and epidemiological studies. The nature of the interaction of diseases or pests with the target is determined and the probability that a particular level of harm from a particular exposure to the hazard is estimated.

d) Exposure analysis – this step examines how a hazardous substance or its residues might reach a susceptible target population and in what amount. It often involves a pathway analysis which considers the different routes the hazard might take, the barriers which might prevent it from reaching the target and the factors that might influence the level of exposure. For example, in considering the risk from chemical spraying the exposure analysis would consider how much chemical was sprayed, in what way and under what conditions, whether there was any direct exposure of humans or animals, how much might be left as residue on plant life, the environmental fate of pesticides reaching the ground, whether it can accumulate in animals or whether it enters groundwater. In bio security, the pathway analysis might consider how any pests entering the country might enter the environment, become established and spread.

e) Risk characterization – in this step, the information from the hazard analysis and the exposure analysis are brought together to estimate the probabilities of particular consequences when effects from all pathways are combined. Where there are large numbers of hazards or pathways, an initial screening may be carried out and the detailed hazard and exposure analysis and risk characterization carried out on the higher risk scenarios.

B.8.5 Outputs.

The output is normally an indication of the level of risk from exposure of a particular target to a particular hazard in the context concerned. The risk may be expressed quantitatively semi-quantitatively or qualitatively. For example, the risk of cancer is often expressed quantitatively as the probability, that a person will develop cancer over a specified period given a specified exposure to a contaminant. Semi-quantitative analysis may be used to derive a risk index for a particular contaminant or pest and qualitative output may be a level of risk (e.g. high, medium, low) or a description with practical data of likely effects.

B.8.6 Strengths and Limitations.

The strength of this analysis is that it provides a very detailed understanding of the nature of the problem and the factors which increase risk.

Pathway analysis is a useful tool, generally, for all areas of risk and permits the identification of how and where it may be possible to improve controls or introduce new ones.

It does, however, need good data which is often not available or has a high level of uncertainty associated with it. For example, dose response curves derived from exposing animals to high levels of a hazard should be extrapolated to estimate the effects of very low levels of the contaminants to humans and there are multiple models by which this is achieved. Where the target is the environment rather than humans and the hazard is not chemical, data which is directly relevant to the particular conditions of the study may be limited.

B.9 Structured "What-if" Technique (SWIFT).

B.9.1 Overview.

SWIFT was originally developed as a simpler alternative to HAZOP. It is a systematic, team-based study, utilizing a set of 'prompt' words or phrases that is used by the facilitator within a workshop to stimulate participants to identify risks. The facilitator and team use standard 'what-if' type phrases in combination with the prompts to investigate how a system, plant item, organization or procedure will be affected by deviations from normal operations and behavior. SWIFT is normally applied at more of a systems level with a lower level of detail than HAZOP.

B.9.2 Use.

While SWIFT was originally designed for chemical and petrochemical plant hazard study, the technique is now widely applied to systems, plant items, procedures, organizations generally. In particular it is used to examine the consequences of changes and the risks thereby altered or created.

B.9.3 Inputs.

The system, procedure, plant item and/or change has to be carefully defined before the study can commence. Both the external and internal contexts are established through interviews and through the study of documents, plans and drawings by the facilitator. Normally, the item, situation or system for study is split into nodes or key elements to facilitate the analysis process but this rarely occurs at the level of definition required for HAZOP.

Another key input is the expertise and experience present in the study team which should be carefully selected. All stakeholders should be represented if possible together with those with experience of similar items, systems, changes or situations.

B.9.4 Process.

The general process is as follows:

a) Before the study commences, the facilitator prepares a suitable prompt list of words or phrases that may be based on a standard set or be created to enable a comprehensive review of hazards or risks.

b) At the workshop the external and internal context of the item, system, change or situation and the scope of the study are discussed and agreed.

c) The facilitator asks the participants to raise and discuss:

   – known risks and hazards;

   – previous experience and incidents;

   – known and existing controls and safeguards;

   – regulatory requirements and constraints.

d) Discussion is facilitated by creating a question using a ‘what-if’ phrase and a prompt word or subject. The ‘what-if’ phrases to be used are “what if…”, “what would happen if…”, “could someone or something…”, “has anyone or anything ever…” The intent is to stimulate the study team into exploring potential scenarios, their causes and consequences and impacts.

e) Risks are summarized and the team considers controls in place.

f) The description of the risk, its causes, consequences and expected controls are confirmed with the team and recorded.

g) The team considers whether the controls are adequate and effective and agree a statement of risk control effectiveness. If this is less than satisfactory, the team further considers risk treatment tasks and potential controls are defined.

h) During this discussion further ‘what-if’ questions are posed to identify further risks.

i) The facilitator uses the prompt list to monitor the discussion and to suggest additional issues and scenarios for the team to discuss.

j) It is normal to use a qualitative or semi-quantitative risk assessment method to rank the actions created in terms of priority. This risk assessment is normally conducted by taking into account the existing controls and their effectiveness.

B.9.5 Outputs.

Outputs include a risk register with risk-ranked actions or tasks. These tasks can then become the basis for a treatment plan.

B.9.6 Strengths and Limitations.

Strengths of SWIFT:

- it is widely applicable to all forms of physical plant or system, situation or circumstance, organization or activity;
- it needs minimal preparation by the team;
- it is relatively rapid and the major hazards and risks quickly become apparent within the workshop session;
- the study is ‘systems orientated’ and allows participants to look at the system response to deviations rather than just examining the consequences of component failure;
- it can be used to identify opportunities for improvement of processes and systems and generally can be used to identify actions that lead to and enhance their probabilities of success;
- involvement in the workshop by those who are accountable for existing controls and for further risk treatment actions, reinforces their responsibility;
- it creates a risk register and risk treatment plan with little more effort;
- while often a qualitative or semi-quantitative form of risk rating is used for risk assessment and to prioritize attention on the resulting actions, SWIFT can be used to identify risks and hazards that can be taken forward into a quantitative study.

Limitations of SWIFT:

- it needs an experienced and capable facilitator to be efficient;
- careful preparation is needed so that the workshop team’s time is not wasted;
- if the workshop team does not have a wide enough experience base or if the prompt system is not comprehensive, some risks or hazards may not be identified;
- the high-level application of the technique may not reveal complex, detailed or correlated causes.

B.10 Scenario Analysis.

B.10.1 Overview.

Scenario analysis is a name given to the development of descriptive models of how the future might turn out. It can be used to identify risks by considering possible future developments and exploring their implications. Sets of scenarios reflecting (for example) ‘best case’, ‘worst case’ and ‘expected case’ may be used to analyze potential consequences and their probabilities for each scenario as a form of sensitivity analysis when analyzing risk.

The power of scenario analysis is illustrated by considering major shifts over the past 50 years in technology, consumer preferences, social attitudes, etc. Scenario analysis cannot predict the probabilities of such changes but can consider consequences and help organizations develop strengths and the resilience needed to adapt to foreseeable changes.

B.10.2 Use.

Scenario analysis can be used to assist in making policy decisions and planning future strategies as well as to consider existing activities. It can play a part in all three components of risk assessment. For identification and analysis, sets of scenarios reflecting (for example) best case, worst case and ‘expected’ case may be used to identify what might happen under particular circumstances and analyze potential consequences and their probabilities for each scenario.

Scenario analysis may be used to anticipate how both threats and opportunities might develop and may be used for all types of risk with both short and long term time frames. With short time frames and good data, likely scenarios may be extrapolated from the present. For longer time frames or with weak data, scenario analysis becomes more imaginative and may be referred to as futures analysis.

Scenario analysis may be useful where there are strong distributional differences between positive outcomes and negative outcomes in space, time and groups in the community or an organization.

B.10.3 Inputs.

The prerequisite for a scenario analysis is a team of people who between them have an understanding of the nature of relevant changes (for example possible advances in technology) and imagination to think into the future without necessarily extrapolating from the past. Access to literature and data about changes already occurring is also useful.

B.10.4 Process.

The structure for scenario analysis may be informal or formal.

Having established a team and relevant communication channels, and defined the context of the problem and issues to be considered, the next step is to identify the nature of changes that might occur. This will need research into the major trends and the probable timing of changes in trends as well as imaginative thinking about the future.

Changes to be considered may include:

- external changes (such as technological changes);

- decisions that need to be made in the near future but which may have a variety of outcomes;
- stakeholder needs and how they might change;
- changes in the macro environment (regulatory, demographics, etc). Some will be inevitable and some will be uncertain.

Sometimes, a change may be due to the consequences of another risk. For example, the risk of climate change is resulting in changes in consumer demand related to food miles. This will influence which foods can be profitably exported as well as which foods can be grown locally.

The local and macro factors or trends can now be listed and ranked for (1) importance (2) uncertainty. Special attention is paid to the factors that are most important and most uncertain. Key factors or trends are mapped against each other to show areas where scenarios can be developed.

A series of scenarios is proposed with each one focusing on a plausible change in parameters.

A “story” is then written for each scenario that tells how you might move from here towards the subject scenario. The stories may include plausible details that add value to the scenarios.

The scenarios can then be used to test or evaluate the original question. The test takes into account any significant but predictable factors (e.g. use patterns), and then explores how ‘successful’ the policy (activity) would be in this new scenario, and ‘pre-tests’ outcomes by using ‘what if’ questions based on model assumptions.

When the question or proposal has been evaluated with respect to each scenario, it may be obvious that it needs to be modified to make it more robust or less risky. It should also be possible to identify some leading indicators that show when change is occurring. Monitoring and responding to leading indicators can provide opportunity for change in planned strategies.

Since scenarios are only defined ‘slices’ of possible futures, it is important to make sure that account is taken of the probability of a particular outcome (scenario) occurring, i.e. to adopt a risk framework. For example, where best case, worst case and expected case scenarios are used, some attempt should be made to qualify, or express the probability of each scenario occurring.

B.10.5 Outputs.

There may be no best-fit scenario but one should end with a clearer perception of the range of options and how to modify the chosen course of action as indicators move.

B.10.6 Strengths and Limitations.

Scenario analysis takes account of a range of possible futures which may be preferable to the traditional approach of relying on high-medium-low forecasts that assume, through the use of historical data, that future events will probably continue to follow past trends. This is important for situations where there is little current knowledge on which to base predictions or where risks are being considered in the longer term future.

This strength however has an associated weakness which is that where there is high uncertainty some of the scenarios may be unrealistic.

The main difficulties in using scenario analysis are associated with the availability of data, and the ability of the analysts and decision makers to be able to develop realistic scenarios that are amenable to probing of possible outcomes.

The dangers of using scenario analysis as a decision-making tool are that the scenarios used may not have an adequate foundation; that data may be speculative; and that unrealistic results may not be recognized as such.

B.11 Business Impact Analysis (BIA).

B.11.1 Overview.

Business impact analysis, also known as business impact assessment, analyzes how key disruption risks 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 identification and 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;
- the capacity and capability needed to manage the impact of a disruption and recover the organization to agreed levels of operation.

B.11.2 Use.

BIA is used to determine the criticality and recovery timeframes of processes and associated resources (people, equipment, information technology) to ensure the continued achievement of objectives. Additionally, the BIA assists in determining interdependencies and interrelationships between processes, internal and external parties and any supply chain linkages.

B.11.3 Inputs.

Inputs include:

- a team to undertake the analysis and develop a plan;
- information concerning the objectives, environment, operations and inter-dependencies of the organization;
- details on the activities and operations of the organization, including processes, supporting resources, relationships with other organizations, outsourced arrangements, stakeholders;
- financial and operational consequences of loss of critical processes;

- prepared questionnaire;
- list of interviewees from relevant areas of the organization and/or stakeholders that will be contacted.

B.11.4 Process.

A BIA can be undertaken using questionnaires, interviews, structured workshops or combinations of all three, to obtain an understanding of the critical processes, the effects of the loss of those processes and the required recovery timeframes and supporting resources.

The key steps include:

- based on the risk and vulnerability assessment, confirmation of the key processes and outputs of the organization to determine the criticality of the processes;
- determination of the consequences of a disruption on the identified critical processes in financial and/or operational terms, over defined periods;
- identification of the interdependencies with key internal and external stakeholders. This could include mapping the nature of the interdependencies through the supply chain;
- determination of the current available resources and the essential level of resources needed to continue to operate at a minimum acceptable level following a disruption;
- identification of alternate workarounds and processes currently in use or planned to be developed. Alternate workarounds and processes may need to be developed where resources or capability are inaccessible or insufficient during the disruption;
- determination of the maximum acceptable outage time (MAO) for each process based on the identified consequences and the critical success factors for the function. The MAO represents the maximum period of time the organization can tolerate the loss of capability;
- determination of the recovery time objective(s) (RTO) for any specialized equipment or information technology. The RTO represents the time within which the organization aims to recover the specialized equipment or information technology capability;
- confirmation of the current level of preparedness of the critical processes to manage a disruption. This may include evaluating the level of redundancy within the process (e.g. spare equipment) or the existence of alternate suppliers.

B.11.5 Outputs.

The outputs are as follows:

- a priority list of critical processes and associated interdependencies;
- documented financial and operational impacts from a loss of the critical processes;
- supporting resources needed for the identified critical processes;
- outage timeframes for the critical process and the associated information technology recovery timeframes.

B.11.6 Strengths and Limitations.

Strengths of the BIA include:

- an understanding of the critical processes that provide the organization with the ability to continue to achieve their stated objectives;
- an understanding of the required resources;
- an opportunity to redefine the operational process of an organization to assist in the resilience of the organization.

Limitations include:

- lack of knowledge by the participants involved in completing questionnaires, undertaking interviews or workshops;
- group dynamics may affect the complete analysis of a critical process;
- simplistic or over-optimistic expectations of recovery requirements;
- difficulty in obtaining an adequate level of understanding of the organization's operations and activities.

B.12 Root Cause Analysis (RCA).

B.12.1 Overview.

The analysis of a major loss to prevent its reoccurrence is commonly referred to as Root Cause Analysis (RCA), Root Cause Failure Analysis (RCFA) or loss analysis. RCA is focused on asset losses due to various types of failures while loss analysis is mainly concerned with financial or economic losses due to external factors or catastrophes. It attempts to identify the root or original causes instead of dealing only with the immediately obvious symptoms. It is recognized that corrective action may not always be entirely effective and that continuous improvement may be required. RCA is most often applied to the evaluation of a major loss but may also be used to analyze losses on a more global basis to determine where improvements can be made.

B.12.2 Use.

RCA is applied in various contexts with the following broad areas of usage:

- safety-based RCA is used for accident investigations and occupational health and safety;
- failure analysis is used in technological systems related to reliability and maintenance;
- production-based RCA is applied in the field of quality control for industrial manufacturing;
- process-based RCA is focused on business processes;
- system-based RCA has developed as a combination of the previous areas to deal with complex systems with application in change management, risk management and systems analysis.

B.12.3 Inputs.

The basic input to an RCA is all of the evidence gathered from the failure or loss. Data from other similar failures may also be considered in the analysis. Other inputs may be results that are carried out to test specific hypotheses.

B.12.4 Process.

When the need for an RCA is identified, a group of experts is appointed to carry out the analysis and make recommendations. The type of expert will mostly be dependent on the specific expertise needed to analyze the failure.

Even though different methods can be used to perform the analysis, the basic steps in executing an RCA are similar and include:

- forming the team;
- establishing the scope and objectives of the RCA;
- gathering data and evidence from the failure or loss;
- performing a structured analysis to determine the root cause;
- developing solutions and make recommendations;
- implementing the recommendations;
- verifying the success of the implemented recommendations.

Structured analysis techniques may consist of one of the following:

- “5 whys” technique, i.e. repeatedly asking ‘why?’ to peel away layers of cause and sub cause);
- failure mode and effects analysis;

- fault tree analysis;
- Fishbone or Ishikawa diagrams;
- Pareto analysis;
- root cause mapping.

The evaluation of causes often progresses from initially evident physical causes to human-related causes and finally to underlying management or fundamental causes. Causal factors have to be able to be controlled or eliminated by involved parties in order for corrective action to be effective and worthwhile.

B.12.5 Outputs.

The outputs from an RCA include:

- documentation of data and evidence gathered;
- hypotheses considered;
- conclusion about the most likely root causes for the failure or loss;
- recommendations for corrective action.

B.12.6 Strengths and Limitations.

Strengths include:

- involvement of applicable experts working in a team environment;
- structured analysis;
- consideration of all likely hypotheses;
- documentation of results;
- need to produce final recommendations.

Limitations of an RCA:

- required experts may not be available;
- critical evidence may be destroyed in the failure or removed during clean-up;
- the team may not be allowed enough time or resources to fully evaluate the situation;
- it may not be possible to adequately implement recommendations.

B.13 Failure Modes and Effects Analysis (FMEA) and Failure Modes and Effects and Criticality Analysis (FMECA).

B.13.1 Overview.

Failure modes and effects analysis (FMEA) is a technique used to identify the ways in which components, systems or processes can fail to fulfill their design intent.

FMEA identifies:

- all potential failure modes of the various parts of a system (a failure mode is what is observed to fail or to perform incorrectly);
- the effects these failures may have on the system;
- the mechanisms of failure;
- how to avoid the failures, and/or mitigate the effects of the failures on the system.

FMECA extends an FMEA so that each fault mode identified is ranked according to its importance or criticality.

This criticality analysis is usually qualitative or semi-quantitative but may be quantified using actual failure rates.

B.13.2 Use.

There are several applications of FMEA: Design (or product) FMEA which is used for components and products, System FMEA which is used for systems, Process FMEA which is used for manufacturing and assembly processes, Service FMEA and Software FMEA.

FMEA/FMECA may be applied during the design, manufacture or operation of a physical system.

To improve dependability, however, changes are usually more easily implemented at the design stage. FMEA AND FMECA may also be applied to processes and procedures. For example, it is used to identify potential for medical error in healthcare systems and failures in maintenance procedures.

FMEA/FMECA can be used to:

- assist in selecting design alternatives with high dependability,
- ensure that all failure modes of systems and processes, and their effects on operational success have been considered,
- identify human error modes and effects,
- provide a basis for planning testing and maintenance of physical systems,

- improve the design of procedures and processes,

- provide qualitative or quantitative information for analysis techniques such as fault tree analysis.

FMEA and FMECA can provide input to other analyzes techniques such as fault tree analysis at either a qualitative or quantitative level.

B.13.3 Inputs.

FMEA and FMECA need information about the elements of the system in sufficient detail for meaningful analysis of the ways in which each element can fail. For a detailed Design FMEA the element may be at the detailed individual component level, while for higher level Systems FMEA, elements may be defined at a higher level.

Information may include:

- drawings or a flow chart of the system being analyzed and its components, or the steps of a process;

- an understanding of the function of each step of a process or component of a system;

- details of environmental and other parameters, which may affect operation;

- an understanding of the results of particular failures;

- historical information on failures including failure rate data where available.

B.13.4 Process.

The FMEA process is as follows:

a) define the scope and objectives of the study;

b) assemble the team;

c) understand the system/process to be subjected to the FMECA;

d) breakdown of the system into its components or steps;

e) define the function of each step or component;

f) for every component or step listed identify:

   - how can each part conceivably fail?

   - what mechanisms might produce these modes of failure?

- what could the effects be if the failures did occur?
- is the failure harmless or damaging?
- how is the failure detected?

g) identify inherent provisions in the design to compensate for the failure.

For FMECA, the study team goes on to classify each of the identified failure modes according to its criticality.

There are several ways this may be done. Common methods include:

- the mode criticality index,
- the level of risk,
- the risk priority number.

The model criticality is a measure of the probability that the mode being considered will result in failure of the system as a whole; it is defined as:

Failure effect probability * Mode failure rate * Operating time of the system

It is most often applied to equipment failures where each of these terms can be defined quantitatively and failure modes all have the same consequence.

The risk level is obtained by combining the consequences of a failure mode occurring with the probability of failure. It is used when consequences of different failure modes differ and can be applied to equipment systems or processes. Risk level can be expressed qualitatively, semi-quantitatively or quantitatively.

The risk priority number (RPN) is a semi-quantitative measure of criticality obtained by multiplying numbers from rating scales (usually between 1 and 10) for consequence of failure, likelihood of failure and ability to detect the problem. (A failure is given a higher priority if it is difficult to detect.) This method is used most often in quality assurance applications.

Once failure modes and mechanisms are identified, corrective actions can be defined and implemented for the more significant failure modes.

FMEA is documented in a report that contains:

- details of the system that was analyzed;
- the way the exercise was carried out;
- assumptions made in the analysis;
- sources of data;

- the results, including the completed worksheets;
- the criticality (if completed) and the methodology used to define it;
- any recommendations for further analyzes, design changes or features to be incorporated in test plans, etc.

The system may be reassessed by another cycle of FMEA after the actions have been completed.

B.13.5 Outputs.

The primary output of FMEA is a list of failure modes, the failure mechanisms and effects for each component or step of a system or process (which may include information on the likelihood of failure). Information is also given on the causes of failure and the consequences to the system as a whole. The output from FMECA includes a rating of importance based on the likelihood that the system will fail, the level of risk resulting from the failure mode or a combination of the level of risk and the 'detectability' of the failure mode.

FMECA can give a quantitative output if suitable failure rate data and quantitative consequences are used.

B.13.6 Strengths and Limitations.

The strengths of FMEA/FMECA are as follows:

- widely applicable to human, equipment and system failure modes and to hardware, software and procedures;
- identify component failure modes, their causes and their effects on the system, and present them in an easily readable format;
- avoid the need for costly equipment modifications in service by identifying problems early in the design process;
- identify single point failure modes and requirements for redundancy or safety systems;
- provide input to the development monitoring programs by highlighting key features to be monitored.

Limitations include:

- they can only be used to identify single failure modes, not combinations of failure modes;
- unless adequately controlled and focused, the studies can be time consuming and costly;
- they can be difficult and tedious for complex multi-layered systems.

B.13.7 Reference Document.

IEC 60812, *Analysis techniques for system reliability – Procedures for failure mode and effect analysis (FMEA)*

B.14 Fault Tree Analysis (FTA).

B.14.1 Overview.

FTA is a technique for identifying and analyzing factors that can contribute to a specified undesired event (called the "top event"). Causal factors are deductively identified, organized in a logical manner and represented pictorially in a tree diagram which depicts causal factors and their logical relationship to the top event.

The factors identified in the tree can be events that are associated with component hardware failures, human errors or any other pertinent events which lead to the undesired event.

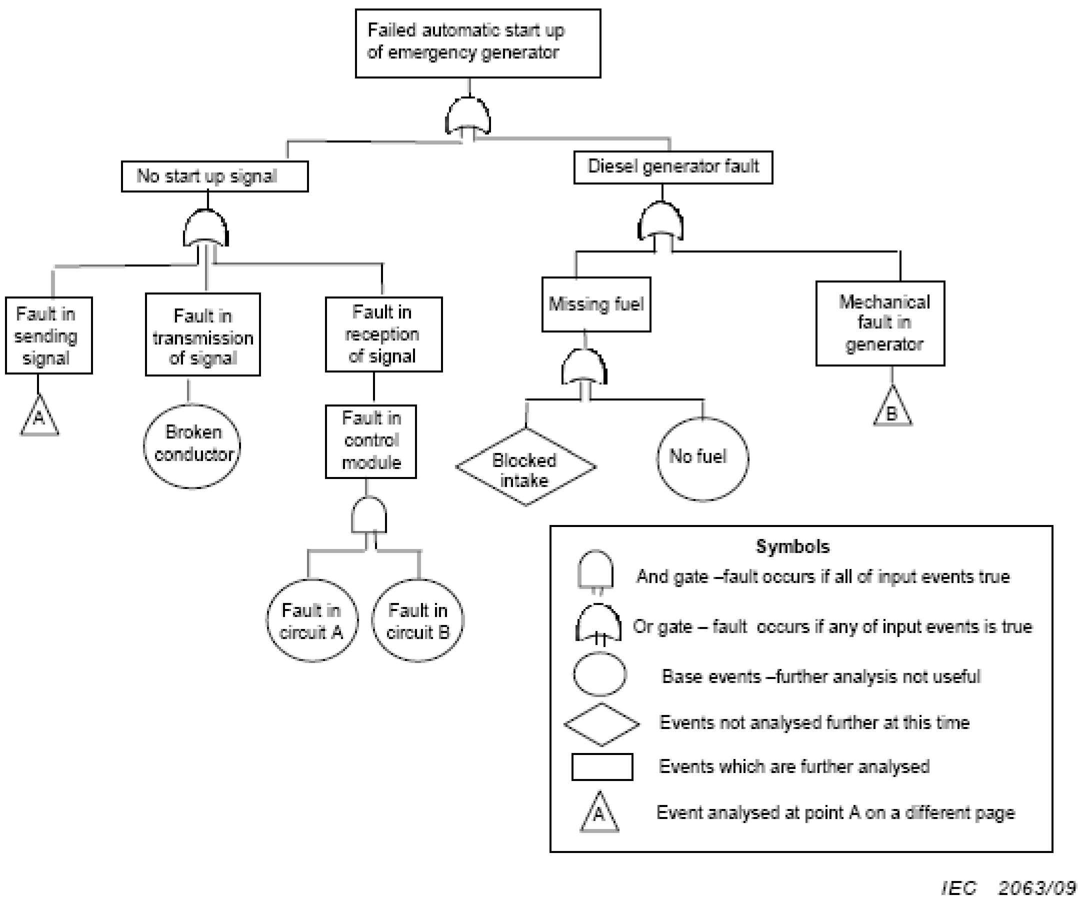


Figure B.2 – Example of an FTA from IEC 60300-3-9

B.14.2 Use.

A fault tree may be used qualitatively to identify potential causes and pathways to a failure (the top event) or quantitatively to calculate the probability of the top event, given knowledge of the probabilities of causal events.

It may be used at the design stage of a system to identify potential causes of failure and hence to select between different design options. It may be used at the operating phase to identify how major failures can occur and the relative importance of different pathways to the head event. A fault tree may also be used to analyze a failure which has occurred to display diagrammatically how different events came together to cause the failure.

B.14.3 Inputs.

For qualitative analysis, an understanding of the system and the causes of failure is required, as well as a technical understanding of how the system can fail. Detailed diagrams are useful to aid the analysis.

For quantitative analysis, data on failure rates or the probability of being in a failed state for all basic events in the fault tree are required.

B.14.4 Process.

The steps for developing a fault tree are as follows:

- The top event to be analyzed is defined. This may be a failure or maybe a broader outcome of that failure. Where the outcome is analyzed, the tree may contain a section relating to mitigation of the actual failure.

- Starting with the top event, the possible immediate causes or failure modes leading to the top event are identified.

- Each of these causes/fault modes is analyzed to identify how their failure could be caused.

- Stepwise identification of undesirable system operation is followed to successively lower system levels until further analysis becomes unproductive. In a hardware system this may be the component failure level. Events and causal factors at the lowest system level analyzed are known as base events.

- Where probabilities can be assigned to base events the probability of the top event may be calculated. For quantification to be valid it must be able to be shown that, for each gate, all inputs are both necessary and sufficient to produce the output event. If this is not the case, the fault tree is not valid for probability analysis but may be a useful tool for displaying causal relationships.

As part of quantification the fault tree may need to be simplified using Boolean algebra to account for duplicate failure modes.

As well as providing an estimate of the probability of the head event, minimal cut sets, which form individual separate pathways to the head event, can be identified and their influence on the top event calculated.

Except for simple fault trees, a software package is needed to properly handle the calculations when repeated events are present at several places in the fault tree, and to calculate minimal cut sets. Software tools help ensure consistency, correctness and verifiability.

B.14.5 Outputs.

The outputs from fault tree analysis are as follows:

- a pictorial representation of how the top event can occur which shows interacting pathways where two or more simultaneous events must occur;
- a list of minimal cut sets (individual pathways to failure) with (where data is available) the probability that each will occur;
- the probability of the top event.

B.14.6 Strengths and Limitations.

Strengths of FTA:

- It affords a disciplined approach which is highly systematic, but at the same time sufficiently flexible to allow analysis of a variety of factors, including human interactions and physical phenomena.
- The application of the "top-down" approach, implicit in the technique, focuses attention on those effects of failure which are directly related to the top event.
- FTA is especially useful for analyzing systems with many interfaces and interactions.
- The pictorial representation leads to an easy understanding of the system behavior and the factors included, but as the trees are often large, processing of fault trees may require computer systems. This feature enables more complex logical relationships to be included (e.g. NAND and NOR) but also makes the verification of the fault tree difficult.
- Logic analysis of the fault trees and the identification of cut sets is useful in identifying simple failure pathways in a very complex system where particular combinations of events which lead to the top event could be overlooked.

Limitations include:

- Uncertainties in the probabilities of base events are included in calculations of the probability of the top event. This can result in high levels of uncertainty where base event failure probabilities are not known accurately; however, a high degree of confidence is possible in a well understood system.
- In some situations, causal events are not bound together and it can be difficult to ascertain whether all important pathways to the top event are included. For example, including all ignition sources in an analysis of a fire as a top event. In this

situation probability analysis is not possible.

- Fault tree is a static model; time interdependencies are not addressed.
- Fault trees can only deal with binary states (failed/not failed) only.
- While human error modes can be included in a qualitative fault tree, in general failures of degree or quality which often characterize human error cannot easily be included.
- A fault tree does not enable domino effects or conditional failures to be included easily.

B.14.7 Reference Document.

IEC 61025, *Fault tree analysis (FTA)*

IEC 60300-3-9, *Dependability management — Part 3: Application guide — Section 9: Risk analysis of technological systems*

B.15 Event Tree Analysis (ETA).

B.15.1 Overview.

ETA is a graphical technique for representing the mutually exclusive sequences of events following an initiating event according to the functioning/not functioning of the various systems designed to mitigate its consequences (see Figure B.3). It can be applied both qualitatively and quantitatively.

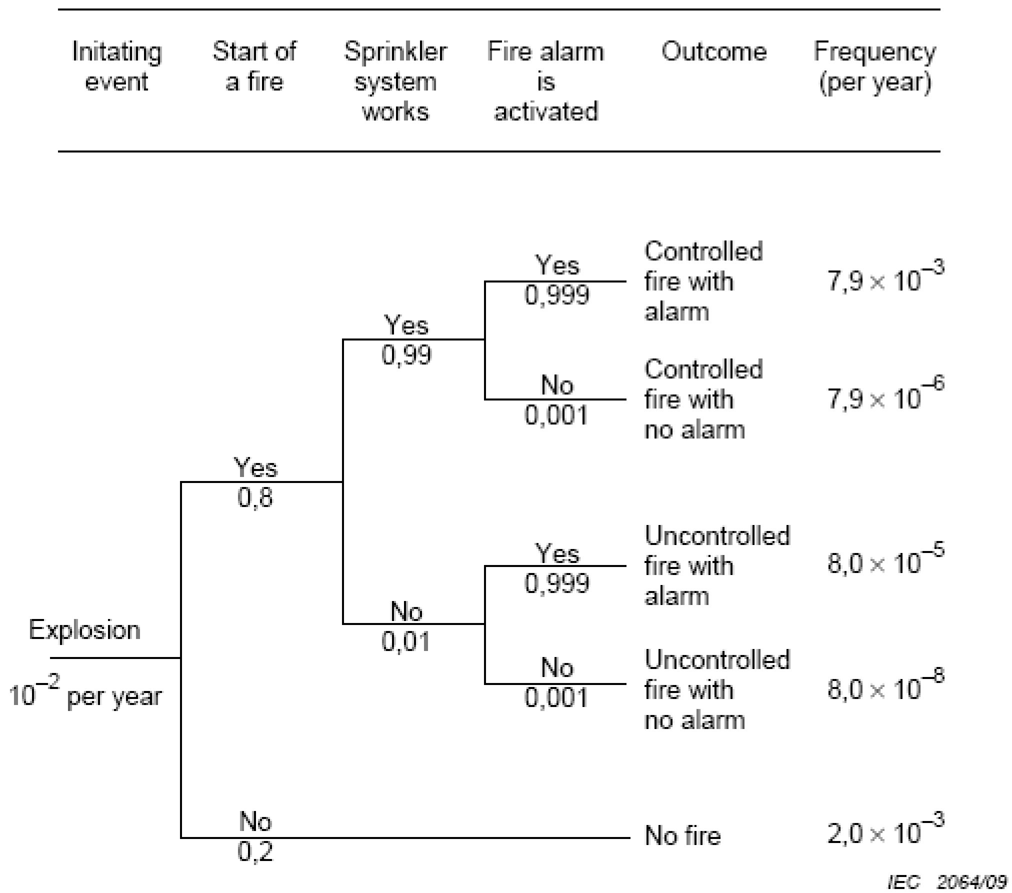


Figure B.3 – Example of an Event Tree

Figure B.3 shows simple calculations for a sample event tree, when branches are fully independent.

By fanning out like a tree, ETA is able to represent the aggravating or mitigating events in response to the initiating event, taking into account additional systems, functions or barriers.

B.15.2 Use.

ETA can be used for modeling, calculating and ranking (from a risk point of view) different accident scenarios following the initiating event.

ETA can be used at any stage in the life cycle of a product or process. It may be used qualitatively to help brainstorm potential scenarios and sequences of events following an initiating event and how outcomes are affected by various treatments, barriers or controls intended to mitigate unwanted outcomes.

The quantitative analysis lends itself to consider the acceptability of controls. It is most often used to model failures where there are multiple safeguards.

ETA can be used to model initiating events which might bring loss or gain. However, circumstances where pathways to optimize gain are sought are more often modeled using a decision tree.

B.15.3 Inputs.

Inputs include:

- a list of appropriate initiating events;
- information on treatments, barriers and controls, and their failure probabilities (for quantitative analyses);
- understanding of the processes whereby an initial failure escalates.

B.15.4 Process.

An event tree starts by selecting an initiating event. This may be an incident such as a dust explosion or a causal event such as a power failure. Functions or systems which are in place to mitigate outcomes are then listed in sequence. For each function or system, a line is drawn to represent their success or failure. A particular probability of failure can be assigned to each line, with this conditional probability estimated e.g. by expert judgment or a fault tree analysis. In this way, different pathways from the initiating event are modeled.

Note that the probabilities on the event tree are conditional probabilities, for example the probability of a sprinkler functioning is not the probability obtained from tests under normal conditions, but the probability of functioning under conditions of fire caused by an explosion.

Each path through the tree represents the probability that all of the events in that path will occur. Therefore, the frequency of the outcome is represented by the product of the individual conditional probabilities and the frequency of the initiation event, given that the various events are independent.

B.15.5 Outputs.

Outputs from ETA include the following:

- qualitative descriptions of potential problems as combinations of events producing various types of problems (range of outcomes) from initiating events;
- quantitative estimates of event frequencies or probabilities and relative importance of various failure sequences and contributing events;
- lists of recommendations for reducing risks;
- quantitative evaluations of recommendation effectiveness.

B.15.6 Strengths and Limitations.

Strengths of ETA include the following:

- ETA displays potential scenarios following an initiating event, are analyzed and the influence of the success or failure of mitigating systems or functions in a clear diagrammatic way;

- it accounts for timing, dependence and domino effects that are cumbersome to model in fault trees;
- it graphically represent sequences of events which are not possible to represent when using fault trees.

Limitations include:

- in order to use ETA as part of a comprehensive assessment, all potential initiating events need to be identified. This may be done by using another analysis method (e.g. HAZOP, PHA), however, there is always a potential for missing some important initiating events;
- with event trees, only success and failure states of a system are dealt with, and it is difficult to incorporate delayed success or recovery events;
- any path is conditional on the events that occurred at previous branch points along the path. Many dependencies along the possible paths are therefore addressed. However, some dependencies, such as common components, utility systems and operators, may be overlooked if not handled carefully, may lead to optimistic estimations of risk.

B.16 Cause-Consequence Analysis.

B.16.1 General.

Cause-consequence analysis is a combination of fault tree and event tree analysis. It starts from a critical event and analyzes consequences by means of a combination of YES/NO logic gates which represent conditions that may occur or failures of systems designed to mitigate the consequences of the initiating event. The causes of the conditions or failures are analyzed by means of fault trees (see Clause B.15)

B.16.2 Use.

Cause-consequence analysis was originally developed as a reliability tool for safety critical systems to give a more complete understanding of system failures. Like fault tree analysis, it is used to represent the failure logic leading to a critical event but it adds to the functionality of a fault tree by allowing time sequential failures to be analyzed. The method also allows time delays to be incorporated into the consequence analysis which is not possible with event trees.

The method is used to analyze the various paths a system could take following a critical event and depending on the behavior of particular subsystems (such as emergency response systems). If quantified they will give an estimate of the probability of different possible consequences following a critical event.

As each sequence in a cause-consequence diagram is a combination of sub-fault trees, the cause-consequence analysis can be used as a tool to build big fault trees.

Diagrams are complex to produce and use and tend to be used when the magnitude of the potential consequence of failure justifies intensive effort.

B.16.3 Inputs.

An understanding of the system and its failure modes and failure scenarios is required.

B.16.4 Process.

Figure B.4 shows a conceptual diagram of a typical cause-consequence analysis.

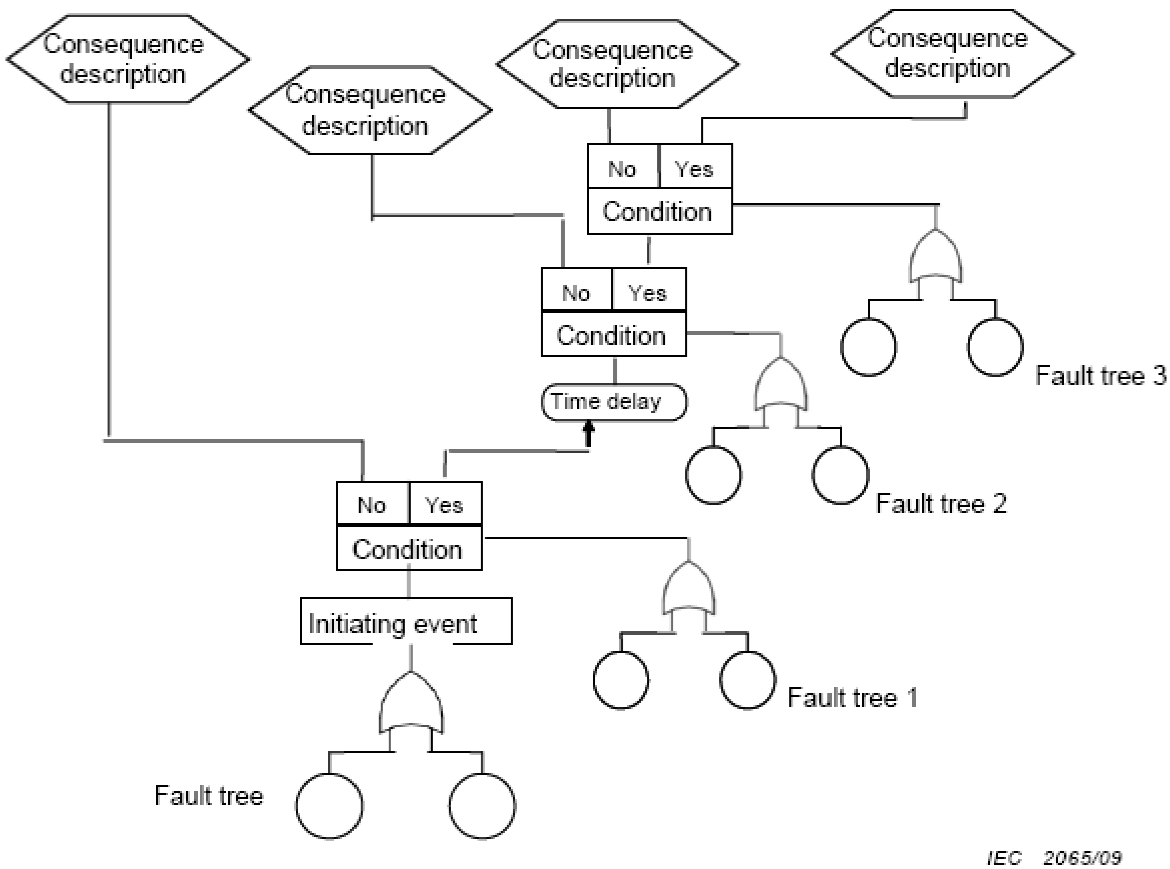


Figure B.4 – Example of Cause-Consequence Analysis

The procedure is as follows:

a) Identify the critical (or initiating) event (equivalent to the top event of a fault tree and the initiating event of an event tree).

b) Develop and validate the fault tree for causes of the initiating event as described in Clause B.14. The same symbols are used as in conventional fault tree analysis.

c) Decide the order in which conditions are to be considered. This should be a logical sequence such as the time sequence in which they occur.

d) Construct the pathways for consequences depending on the different conditions. This is similar to an event tree but the split in pathways of the event tree is shown as a box labeled with the particular condition that applies.

e) Provided the failures for each condition box are independent, the probability of each consequence can be calculated. This is achieved by first assigning probabilities to each output of the condition box (using the relevant fault trees as appropriate) The probability of any one sequence leading to a particular consequence is obtained by multiplying the probabilities of each sequence of conditions which terminates in that particular consequence. If more than one sequence ends up with the same consequence, the probabilities from each sequence are added. If there are dependencies between failures of conditions in a sequence (for example a power failure may cause several conditions to fail) then the dependencies should be dealt with prior to calculation.

B.16.5 Output.

The output of cause-consequence analysis is a diagrammatic representation of how a system may fail showing both causes and consequences. An estimation of the probability of occurrence of each potential consequence based on analysis of probabilities of occurrence of particular conditions following the critical event.

B.16.6 Strengths and Limitations.

The advantages of cause-consequence analysis are the same as those of event trees and fault trees combined. In addition, it overcomes some of the limitations of those techniques by being able to analyze events that develop over time. Cause-consequence analysis provides a comprehensive view of the system.

Limitations are that it is more complex than fault tree and event tree analysis, both to construct and in the manner in which dependencies are dealt with during quantification.

B.17 Cause-and-Effect Analysis.

B.17.1 Overview.

Cause-and-effect analysis is a structured method to identify possible causes of an undesirable event or problem. It organizes the possible contributory factors into broad categories so that all possible hypotheses can be considered. It does not, however, by itself point to the actual causes, since these can only be determined by real evidence and empirical testing of hypotheses. The information is organized in either a Fishbone (also called Ishikawa) or sometimes a tree diagram (see B.17.4).

B.17.2 Use.

Cause-and-effect analysis provides a structured pictorial display of a list of causes of a specific effect. The effect may be positive (an objective) or negative (a problem) depending on context.

It is used to enable consideration of all possible scenarios and causes generated by a team of experts and allows consensus to be established as to the most likely causes which can then be tested empirically or by evaluation of available data. It is most valuable at the beginning of an analysis to broaden thinking about possible causes and then to establish potential hypotheses that can be considered more formally.

Constructing a cause-and-effect diagram can be undertaken when there is need to:

- identify the possible root causes, the basic reasons, for a specific effect, problem or condition;
- sort out and relate some of the interactions among the factors affecting a particular process;
- analyze existing problems so that corrective action can be taken.

Benefits from constructing a cause-and-effect diagram include:

- concentrates review members' attention on a specific problem;
- to help determine the root causes of a problem using a structured approach;
- encourages group participation and utilizes group knowledge for the product or process;
- uses an orderly, easy-to-read format to diagram cause-and-effect relationships;
- indicates possible causes of variation in a process;
- identifies areas where data should be collected for further study.

Cause-and-effect analysis can be used as a method in performing root cause analysis (see Clause B.12).

B.17.3 Input.

The input to a cause-and-effect analysis may come from expertise and experience from participants or a previously developed model that has been used in the past.

B.17.4 Process.

The cause-and-effect analysis should be carried out by a team of experts knowledgeable with the problem requiring resolution.

The basic steps in performing a cause-and-effect analysis are as follows:

- establish the effect to be analyzed and place it in a box. The effect may be positive (an objective) or negative (a problem) depending on the circumstances;
- determine the main categories of causes represented by boxes in the Fishbone

diagram. Typically, for a system problem, the categories might be people, equipment, environment, processes, etc. However, these are chosen to fit the particular context;

- fill in the possible causes for each major category with branches and sub-branches to describe the relationship between them;
- keep asking "why?" or "what caused that?" to connect the causes;
- review all branches to verify consistency and completeness and ensure that the causes apply to the main effect;
- identify the most likely causes based on the opinion of the team and available evidence.

The results are normally displayed as either a Fishbone or Ishikawa diagram or tree diagram. The Fishbone diagram is structured by separating causes into major categories (represented by the lines off the fish backbone) with branches and sub-branches that describe more specific causes in those categories.

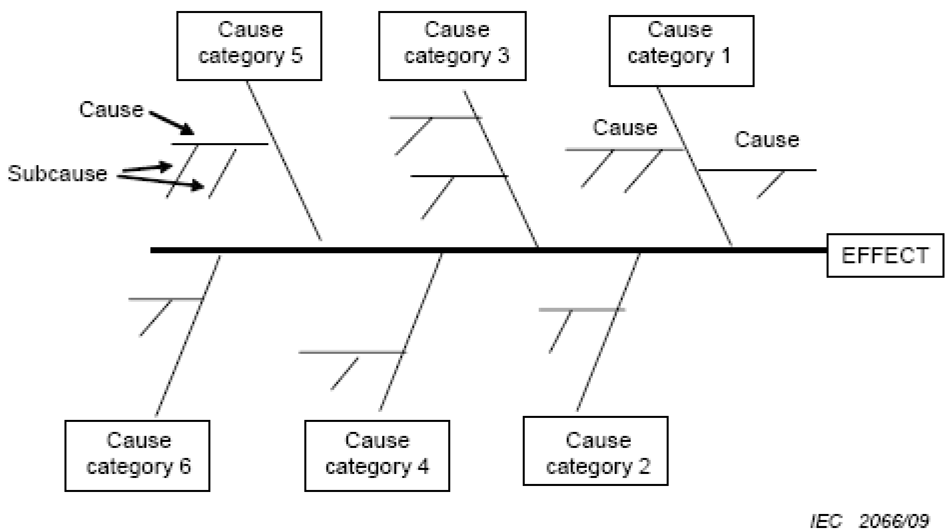


Figure B.5 – Example of Ishikawa or Fishbone Diagram

The tree representation is similar to a fault tree in appearance, although it is often displayed with the tree developing from left to right rather than down the page. However, it cannot be quantified to produce a probability of the head event as the causes are possible contributory factors rather than failures with a known probability of occurrence.

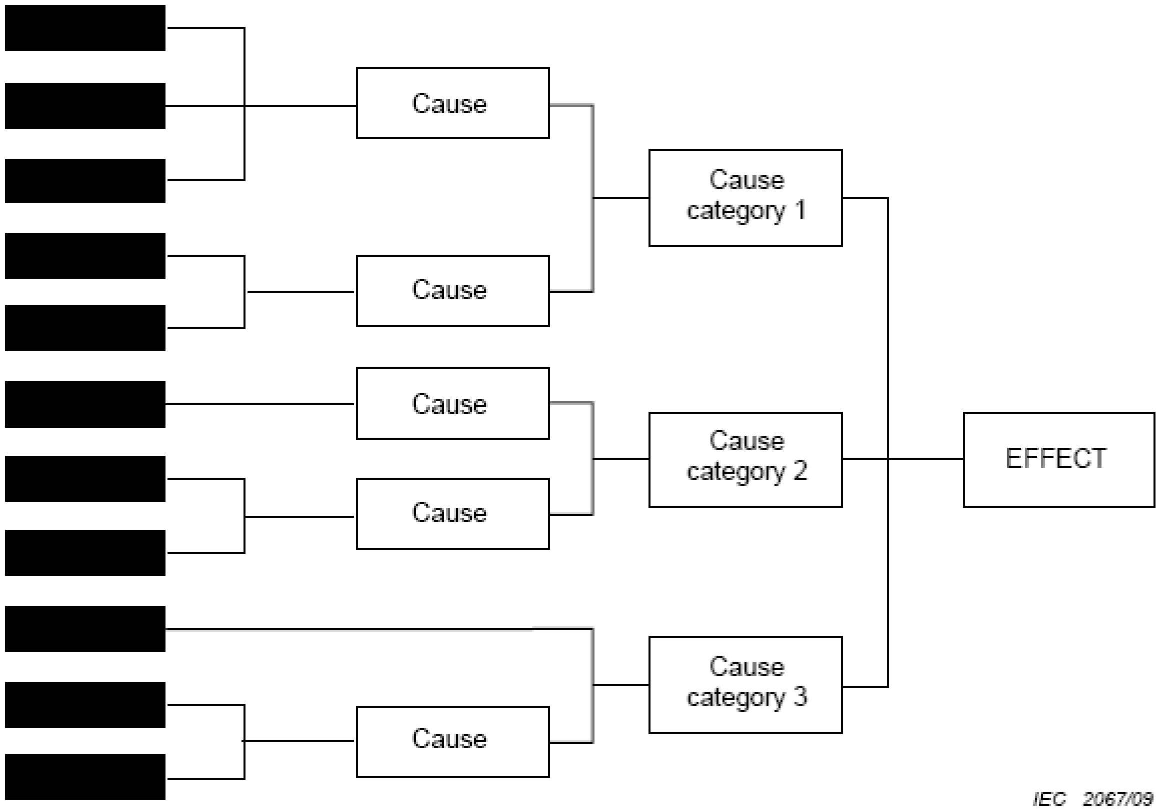


Figure B.6 – Example of Tree Formulation of Cause-and-Effect Analysis

Cause-and-effect diagrams are generally used qualitatively. It is possible to assume the probability of the problem is 1 and assign probabilities to generic causes, and subsequently to the sub-causes, on the basis of the degree of belief about their relevance. However, contributory factors often interact and contribute to the effect in complex ways which make quantification invalid.

B.17.5 Output.

The output from a cause-and-effect analysis is a Fishbone or tree diagram that shows the possible and likely causes. This has then to be verified and tested empirically before recommendations can be made.

B.17.6 Strengths and Limitations.

Strengths include:

- involvement of applicable experts working in a team environment;
- structured analysis;
- consideration of all likely hypotheses;

- graphical easy-to-read illustration of results;
- areas identified where further data is needed;
- can be used to identify contributory factors to wanted as well as unwanted effects. Taking a positive focus on an issue can encourage greater ownership and participation.

Limitations include:

- the team may not have the necessary expertise;
- it is not a complete process in itself and needs to be a part of a root cause analysis to produce recommendations;
- it is a display technique for brainstorming rather than a separate analysis technique;
- the separation of causal factors into major categories at the start of the analysis means that interactions between the categories may not be considered adequately, e.g. where equipment failure is caused by human error, or human problems are caused by poor design.

B.18 Layers of Protection Analysis (LOPA).

B.18.1 Overview.

LOPA is a semi-quantitative method for estimating the risks associated with an undesired event or scenario. It analyzes whether there are sufficient measures to control or mitigate the risk.

A cause-consequence pair is selected and the layers of protection which prevent the cause leading to the undesired consequence are identified. An order of magnitude calculation is carried out to determine whether the protection is adequate to reduce risk to a tolerable level.

B.18.2 Uses.

LOPA may be used qualitatively simply to review the layers of protection between a hazard or causal event and an outcome. Normally a semi-quantitative approach would be applied to add more rigor to screening processes for example following HAZOP or PHA.

LOPA provides a basis for the specification of independent protection layers (IPLs) and safety integrity levels (SIL levels) for instrumented systems, as described in the IEC 61508 series and in IEC 61511, in the determination of safety integrity level (SIL) requirements for safety instrumented systems. LOPA can be used to help allocate risk reduction resources effectively by analyzing the risk reduction produced by each layer of protection.

B.18.3 Inputs.

Inputs to LOPA include:

- basic information on risks including hazards, causes and consequences such as provided by a PHA;
- information on controls in place or proposed;
- causal event frequencies, and protection layer failure probabilities, measures of consequence and a definition of tolerable risk;
- initiating cause frequencies, protection layer failure probabilities, measures of consequence and a definition of tolerable risk.

B.18.4 Process.

LOPA is carried out using a team of experts who apply the following procedure:

- identify initiating causes for an undesired outcome and seek data on their frequencies and consequences;
- select a single cause-consequence pair;
- layers of protection which prevent the cause proceeding to the undesired consequence are identified and analyzed for their effectiveness;
- identify independent protection layers (IPLs) (not all layers of protection are IPLs);
- estimate the probability of failure of each IPL;
- the frequency initiating cause is combined with the probabilities of failure of each IPL and the probabilities of any conditional modifiers (a conditional modifier is for example whether a person will be present to be impacted) to determine the frequency of occurrence of the undesired consequence. Orders of magnitude are used for frequencies and probabilities;
- the calculated level of risk is compared with risk tolerance levels to determine whether further protection is required.

An IPL is a device system or action that is capable of preventing a scenario proceeding to its undesired consequence, independent of the causal event or any other layer of protection associated with the scenario.

IPLs include:

- design features;
- physical protection devices;
- interlocks and shutdown systems;
- critical alarms and manual intervention;

- post event physical protection;
- emergency response systems (procedures and inspections are not IPLs).

B.18.5 Output.

Recommendations for any further controls and the effectiveness of these controls in reducing risk shall be given.

LOPA is one of the techniques used for SIL assessment when dealing with safety related/instrumented systems.

B.18.6 Strengths and Limitations.

Strengths include:

- it requires less time and resources than a fault tree analysis or fully quantitative risk assessment but is more rigorous than qualitative subjective 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 include:

- LOPA focuses on one cause-consequence pair and one scenario at a time. Complex interactions between risks or between controls are not covered;
- quantified risks may not account for common mode failures;
- LOPA 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.18.7 Reference Documents.

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

IEC 61511, *Functional safety – Safety instrumented systems for the process industry sector*

B.19 Decision Tree Analysis.

B.19.1 Overview.

A decision tree represents decision alternatives and outcomes in a sequential manner which takes account of uncertain outcomes. It is similar to an event tree in that it starts from an initiating event or an initial decision and models different pathways and outcomes as a result of events that may occur and different decisions that may be made.

B.19.2 Use.

A decision tree is used in managing project risks and in other circumstances to help select the best course of action where there is uncertainty. The graphical display can also help communicate reasons for decisions.

B.19.3 Input.

A project plan with decision points. Information on possible outcomes of decisions and on chance events which might affect decisions.

B.19.4 Process.

A decision tree starts with an initial decision, for example to proceed with project A rather than project B. As the two hypothetical projects proceed, different events will occur and different predictable decisions will need to be made. These are represented in tree format, similar to an event tree. The probability of the events can be estimated together with the cost or utility of the final outcome of the pathway.

Information concerning the best decision pathway is logically that which produces the highest expected value calculated as the product of all the conditional probabilities along the pathway and the outcome value.

B.19.5 Outputs.

Outputs include:

- a logical analysis of the risk displaying different options that may be taken
- a calculation of the expected value for each possible path

B.19.6 Strengths and Limitations.

Strengths include:

- they provide a clear graphical representation of the details of a decision problem;
- they enable a calculation of the best pathway through a situation.

Limitations include:

- large decisions trees may become too complex for easy communication with others;
- there may be a tendency to oversimplify the situation so as to be able to represent it as a tree diagram.

B.20 Human Reliability Assessment (HRA).

B.20.1 Overview.

Human reliability assessment (HRA) deals with the impact of humans on system performance and can be used to evaluate human error influences on the system.

Many processes contain potential for human error, especially when the time available to the operator to make decisions is short. The probability that problems will develop sufficiently to become serious can be small. Sometimes, however, human action will be the only defense to prevent an initial failure progressing towards an accident.

The importance of HRA has been illustrated by various accidents in which critical human errors contributed to a catastrophic sequence of events. Such accidents are warnings against risk assessments that focus solely on the hardware and software in a system. They illustrate the dangers of ignoring the possibility of human error contribution. Moreover, HRAs are useful in highlighting errors that can impede productivity and in revealing ways in which these errors and other failures (hardware and software) can be "recovered" by the human operators and maintenance personnel.

B.20.2 Use.

HRA can be used qualitatively or quantitatively. Qualitatively, it is used to identify the potential for human error and its causes so the probability of error can be reduced. Quantitative HRA is used to provide data on human failures into FTA or other techniques.

B.20.3 Input.

Inputs to HRA include:

- information to define tasks that people should perform;
- experience of the types of error that occur in practice and potential for error;
- expertise on human error and its quantification.

B.20.4 Process.

The HRA process is as follows:

- **Problem definition**, what types of human involvements are to be investigated/assessed?
- **Task analysis**, how will the task be performed and what type of aids will be needed to support performance?
- **Human error analysis**, how can task performance fail: what errors can occur and how can they be recovered?

- **Representation**, how can these errors or task performance failures be integrated with other hardware, software, and environmental events to enable overall system failure probabilities to be calculated?

- **Screening**, are there any errors or tasks that do not require detailed quantification?

- **Quantification**, how likely are individual errors and failures of tasks?

- **Impact assessment**, which errors or tasks are most important, i.e. which ones have the highest contribution to reliability or risk?

- **Error reduction**, how can higher human reliability be achieved?

- **Documentation**, what details of the HRA need to be documented?

In practice, the HRA process proceeds step-wise although sometimes with parts (e.g. tasks analysis and error identification) proceeding in parallel with one another.

B.20.5 Output.

Outputs include:

- a list of errors that may occur and methods by which they can be reduced – preferably through redesign of the system;

- error modes, error types causes and consequences;

- a qualitative or quantitative assessment of the risk posed by the errors.

B.20.6 Strengths and Limitations.

Strengths of HRA include:

- HRA provides a formal mechanism to include human error in consideration of risks associated with systems where humans often play an important role;

- formal consideration of human error modes and mechanisms can help reduce the probability of failure due to error.

Limitations include:

- the complexity and variability of humans, which make defining simple failure modes and probabilities difficult;

- many activities of humans do not have a simple pass/fail mode. HRA has difficulty dealing with partial failures or failure in quality or poor decision-making.

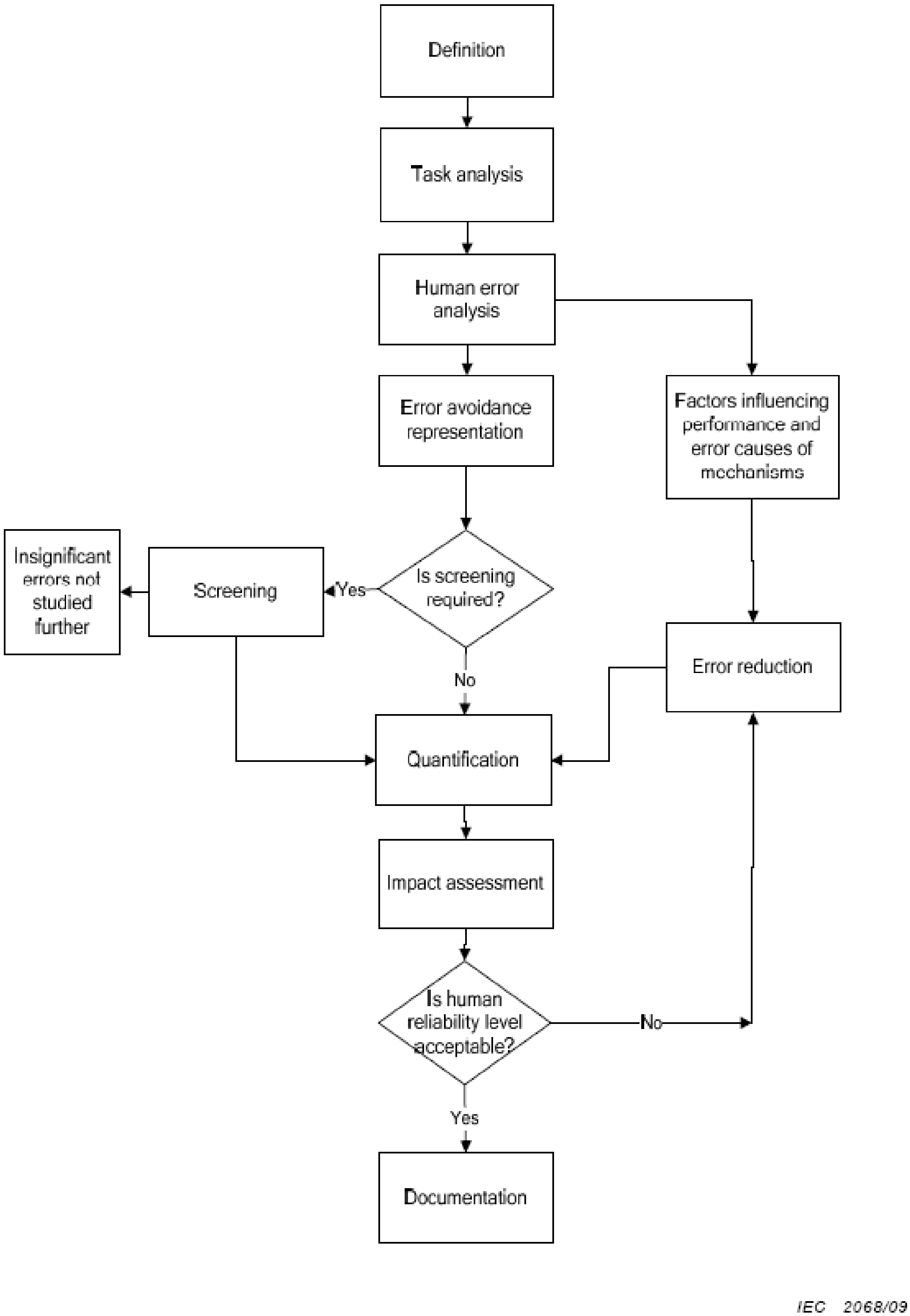


Figure B.7 – Example of Human Reliability Assessment

B.21 Bow Tie Analysis.

B.21.1 Overview.

Bow tie analysis is a simple diagrammatic way of describing and analyzing the pathways of a risk from causes to consequences. It can be considered to be a combination of the thinking of a fault tree analyzing the cause of an event (represented by the knot of a bow tie) and an event tree analyzing the consequences. However the focus of the bow tie is on the barriers between the causes and the risk, and the risk and consequences. Bow tie diagrams can be constructed starting from fault and event trees, but are more often drawn directly from a brainstorming session.

B.21.2 Use.

Bow tie analysis is used to display a risk showing a range of possible causes and consequences. It is used when the situation does not warrant the complexity of a full fault tree analysis or when the focus is more on ensuring that there is a barrier or control for each failure pathway. It is useful where there are clear independent pathways leading to failure.

Bow tie analysis is often easier to understand than fault and event trees, and hence can be a useful communication tool where analysis is achieved using more complex techniques.

B.21.3 Input.

An understanding is required of information on the causes and consequences of a risk and the barriers and controls which may prevent, mitigate or stimulate it.

B.21.4 Process.

The bow tie is drawn as follows:

a) A particular risk is identified for analysis and represented as the central knot of a bow tie.

b) Causes of the event are listed considering sources of risk (or hazards in a safety context).

c) The mechanism by which the source of risk leads to the critical event is identified.

d) Lines are drawn between each cause and the event forming the left-hand side of the bow tie. Factors which might lead to escalation can be identified and included in the diagram.

e) Barriers which should prevent each cause leading to the unwanted consequences can be shown as vertical bars across the line. Where there were factors which might cause escalation, barriers to escalation can also be represented. The approach can be used for positive consequences where the bars reflect ‘controls’ that stimulate the generation of the event.

f) On the right-hand side of the bow tie different potential consequences of the risk are identified and lines drawn to radiate out from the risk event to each potential consequence.

g) Barriers to the consequence are depicted as bars across the radial lines. The approach can be used for positive consequences where the bars reflect ‘controls’ that support the generation of consequences.

h) 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 may be possible where pathways are independent, the probability of a particular consequence or outcome is known and a figure can be estimated for the effectiveness of a control. However, in many situations, pathways and barriers are not independent and controls may be procedural and hence the effectiveness unclear. Quantification is often more appropriately carried out using FTA and ETA.

B.21.5 Output.

The output is a simple diagram showing main risk pathways and the barriers in place to prevent or mitigate the undesired consequences or stimulate and promote desired consequences.

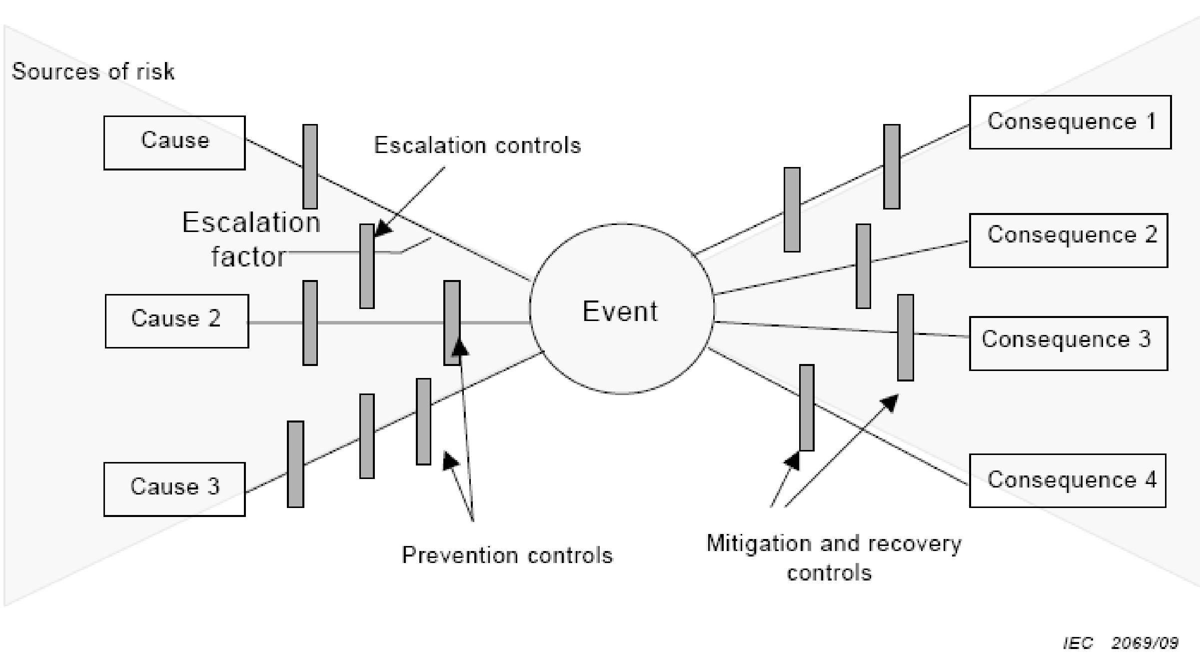


Figure B.8 – Example Bow Tie Diagram for Unwanted Consequences

B.21.6 Strengths and Limitations.

Strengths of bow tie analysis:

- it is simple to understand and gives a clear pictorial representation of the problem;

- it focuses attention on controls which are supposed to be in place for both prevention and mitigation and their effectiveness;
- it can be used for desirable consequences;
- it does not need a high level of expertise to use.

Limitations include:

- it cannot depict where multiple causes occur simultaneously to cause the consequences (i.e. where there are AND gates in a fault tree depicting the left-hand side of the bow);
- it may over-simplify complex situations, particularly where quantification is attempted.

B.22 Reliability Centered Maintenance.

B.22.1 Overview.

Reliability centered maintenance (RCM) is a method to identify the policies that should be implemented to manage failures so as to efficiently and effectively achieve the required safety, availability and economy of operation for all types of equipment.

RCM is now a proven and accepted methodology used in a wide range of industries.

RCM provides a decision process to identify applicable and effective preventive maintenance requirements for equipment in accordance with the safety, operational and economic consequences of identifiable failures, and the degradation mechanism responsible for those failures. The end result of working through the process is a judgment as to the necessity of performing a maintenance task or other action such as operational changes. Details regarding the use and application of RCM are provided in IEC 60300-3-11.

B.22.2 Use.

All tasks are based on safety in respect of personnel and environment, and on operational or economic concerns. However, it should be noted that the criteria considered will depend on the nature of the product and its application. For example, a production process will need to be economically viable, and may be sensitive to strict environmental considerations, whereas an item of defense equipment should be operationally successful, but may have less stringent safety, economic and environmental criteria. Greatest benefit can be achieved through targeting of the analysis to where failures would have serious safety, environmental, economic or operational effects.

RCM is used to ensure that applicable and effective maintenance is performed, and is generally applied during the design and development phase and then implemented during operation and maintenance.

B.22.3 Input.

Successful application of RCM needs a good understanding of the equipment and structure, the operational environment and the associated systems, subsystems and items of equipment, together with the possible failures, and the consequences of those failures.

B.22.4 Process.

The basic steps of an RCM program are as follows:

- initiation and planning;
- functional failure analysis;
- task selection;
- implementation;
- continuous improvement.

RCM is risk based since it follows the basic steps in risk assessment. The type of risk assessment is a failure mode, effect and criticality analysis (FMECA) but requires a specific approach to analysis when used in this context.

Risk identification focuses on situations where potential failures may be eliminated or reduced in frequency and/or consequence by carrying out maintenance tasks. It is performed by identifying required functions and performance standards and failures of equipment and components that can interrupt those functions.

Risk analysis consists of estimating the frequency of each failure without maintenance being carried out. Consequences are established by defining failure effects. A risk matrix that combines failure frequency and consequences allows categories for levels of risk to be established.

Risk evaluation is then performed by selecting the appropriate failure management policy for each failure mode.

The entire RCM process is extensively documented for future reference and review. Collection of failure and maintenance-related data enables monitoring of results and implementation of improvements.

B.22.5 Output.

RCM provides a definition of maintenance tasks such as condition monitoring, scheduled restoration, scheduled replacement, failure-finding or non preventive maintenance. Other possible actions that can result from the analysis may include redesign, changes to operating or maintenance procedures or additional training. Task intervals and required resources are then identified.

B.22.6 Reference Documents.

IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

B.23 Sneak Analysis (SA) and Sneak Circuit Analysis (SCI).

B.23.1 Overview.

Sneak analysis (SA) is a methodology for identifying design errors. A sneak condition is a latent hardware, software or integrated condition that may cause an unwanted event to occur or may inhibit a desired event and is not caused by component failure. These conditions are characterized by their random nature and ability to escape detection during the most rigorous of standardized system tests. Sneak conditions can cause improper operation, loss of system availability, program delays, or even death or injury to personnel.

B.23.2 Use.

Sneak circuit analysis (SCA) was developed in the late 1960s for NASA to verify the integrity and functionality of their designs. It served as a useful tool for discovering unintentional electrical circuit paths, and assisted in devising solutions to isolate each function. However, as technology advanced, the tools for sneak circuit analysis also had to advance. Sneak analysis includes and far exceeds the coverage of sneak circuit analysis. It can locate problems in both hardware and software using any technology. The sneak analysis tools can integrate several analyses such as fault trees, failure mode and effects analysis (FMEA), reliability estimates, etc. into a single analysis saving time and project expenses.

B.23.3 Input.

Sneak analysis is unique from the design process in that it uses different tools (network trees, forests, and clues or questions to help the analyst identify sneak conditions) to find a specific type of problem. The network trees and forests are topological groupings of the actual system. Each network tree represents a sub-function and shows all inputs that may affect the sub-function output. Forests are constructed by combining the network trees that contribute to a particular system output. A proper forest shows a system output in terms of all of its related inputs. These, along with others, become the input to the analysis.

B.23.4 Process.

The basic steps in performing a sneak analysis consist of:

- data preparation;
- construction of the network tree;
- evaluation of network paths;
- final recommendations and report.

B.23.5 Output.

A sneak circuit is an unexpected path or logic flow within a system which, under certain conditions, can initiate an undesired function or inhibit a desired function. The path may consist of hardware, software, operator actions, or combinations of these elements. Sneak circuits are not the result of hardware failure but are latent conditions, inadvertently designed into the system, coded into the software program, or triggered by human error. There are four categories of sneak circuits:

a) sneak paths: unexpected paths along which current, energy, or logical sequence flows in an unintended direction;

b) sneak timing: events occurring in an unexpected or conflicting sequence;

c) sneak indications: ambiguous or false displays of system operating conditions that may cause the system or an operator to take an undesired action;

d) sneak labels: incorrect or imprecise labeling of system functions, e.g. system inputs, controls, display buses that may cause an operator to apply an incorrect stimulus to the system.

B.23.6 Strengths and Limitations.

Strengths include:

- sneak analysis is good for identifying design errors;
- it works best when applied in conjunction with HAZOP;
- it is very good for dealing with systems which have multiple states such as batch and semi-batch plant.

Limitations may include:

- the process is somewhat different depending on whether it is applied to electrical circuits, process plants, mechanical equipment or software;
- the method is dependent on establishing correct network trees.

B.24 Markov Analysis.

B.24.1 Overview.

Markov analysis is used where the future state of a system depends only upon its present state. It is commonly used for the analysis of repairable systems that can exist in multiple states and the use of a reliability block analysis would be unsuitable to adequately analyze the system. The method can be extended to more complex systems by employing higher order Markov processes and is only restricted by the model, mathematical computations and the assumptions.

The Markov analysis process is a quantitative technique and can be discrete (using probabilities of change between the states) or continuous (using rates of change across the states).

While a Markov analysis can be performed by hand, the nature of the techniques lends itself to the use of computer programs, many of which exist in the market.

B.24.2 Use.

The Markov analysis technique can be used on various system structures, with or without repair, including:

- independent components in parallel;
- independent components in series;
- load-sharing system;
- stand-by system, including the case where switching failure can occur;
- degraded systems.

The Markov analysis technique can also be used for calculating availability, including taking into account the spares components for repairs.

B.24.3 Input.

The inputs essential to a Markov analysis are as follows:

- list of various states that the system, sub-system or component can be in (e.g. fully operational, partially operation (i.e. a degraded state), failed state, etc);
- a clear understanding of the possible transitions that are necessary to be modeled. For example, failure of a car tire needs to consider the state of the spare wheel and hence the frequency of inspection;
- rate of change from one state to another, typically represented by either a probability of change between states for discrete events, or failure rate (λ) and/or repair rate (μ) for continuous events.

B.24.4 Process.

The Markov analysis technique is centered around the concept of “states”, e.g. “available” and “failed”, and the transition between these two states over time based on a constant probability of change. A stochastic transitional probability matrix is used to describe the transition between each of the states to allow the calculation of the various outputs.

To illustrate the Markov analysis technique, consider a complex system that can be in only three states; functioning, degraded and failed, defined as states S1, S2, S3 respectively. Each day, the system exists in one of these three states. Table B.3 shows the probability that tomorrow, the system is in state S*i* where *i* can be 1, 2 or 3.

Table B.2 – Markov Matrix

		State Today		
		S1	S2	S3
State Tomorrow	S1	0,95	0,3	0,2
	S2	0,04	0,65	0,6
	S3	0,01	0,05	0,2

This array of probabilities is called a Markov matrix, or transition matrix. Notice that the sum for each of the columns is 1 as they are the sum of all the possible outcomes in each case. The system, can also be represented by a Markov diagram where the circles represent the states, and the arrows represent the transition, together with the accompanying probability.

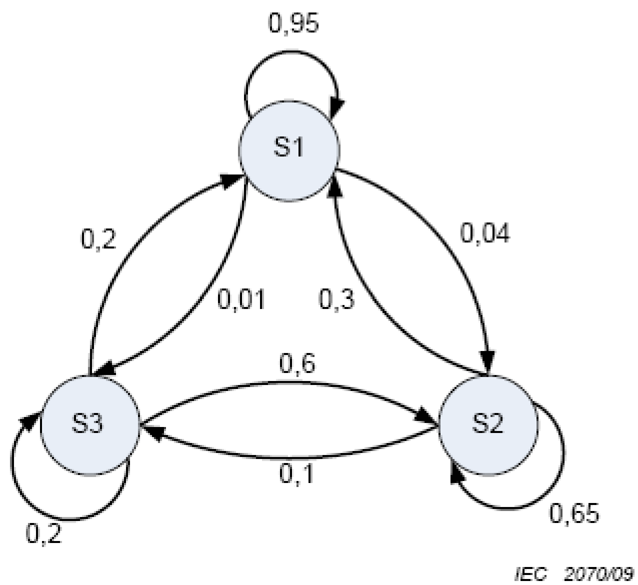


Figure B.9 – Example of System Markov Diagram

The arrows from a state to itself are not usually shown, but are shown within these examples for completeness.

Let P*i* represent the probability of finding the system in state *i* for *i* = 1, 2, 3, then the simultaneous equations to be solved are:

$$P1 = 0{,}95\ P1 + 0{,}30\ P2 + 0{,}20\ P3 \qquad (B.1)$$

$$P2 = 0{,}04\ P1 + 0{,}65\ P2 + 0{,}60\ P3 \qquad (B.2)$$

$$P3 = 0{,}01\ P1 + 0{,}05\ P2 + 0{,}20\ P3 \qquad (B.3)$$

These three equations are not independent and will not solve the three unknowns. The following equation should be used and one of the above equations discarded.

$$1 = P1 + P2 + P3 \qquad (B.4)$$

The solution is 0,85, 0,13, and 0.02 for the respective states 1, 2, 3. The system is fully functioning for 85% of the time, in the degraded state for 13% of the time and failed for 2% of the time.

Consider two items operating in parallel with either required to be operational for the system to function. The items can either be operational or failed and the availability of the system is dependent upon the status of the items.

The states can be considered as:

State 1 Both items are functioning correctly;
State 2 One item has failed and is undergoing repair, the other is functioning;
State 3 Both items have failed and one is undergoing repair.

If the continuous failure rate for each item is assumed to be λ and the repair rate to be μ, then the state transition diagram is:

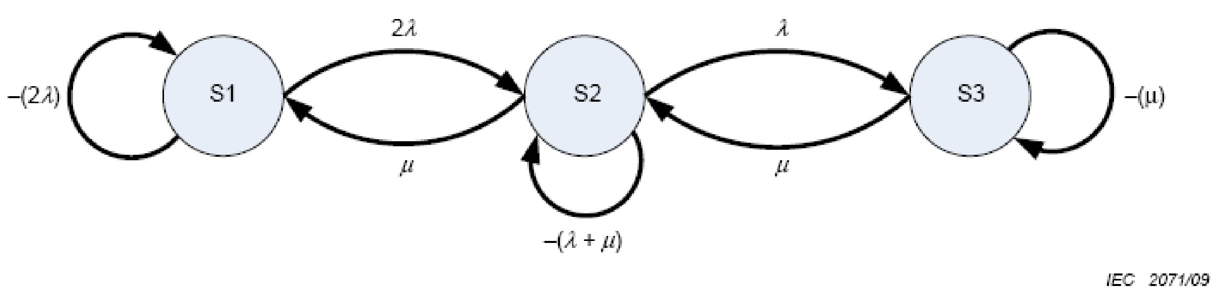


Figure B.10 – Example of State Transition Diagram

Note that the transition from state 1 to state 2 is 2λ as failure of either of the two items will take the system to state 2.

Let P*i*(*t*) be the probability of being in an initial state *i* at time *t*; and

Let P*i*(*t* + *δt*) be the probability of being in a final state at time *t* + *δt*

The transition probability matrix becomes:

Table B.3 – Final Markov Matrix

		Initial State		
		P1(t)	P2(t)	P3(t)
Final State	P1($t + \delta t$)	–2λ	μ	0
	P2($t + \delta t$)	2λ	- (λ + μ)	μ
	P3($t + \delta t$)	0	λ	– μ

It is worth noting that the zero values occur as it is not possible to move from state 1 to state 3 or from state 3 to state 1. Also, the columns sum to zero when specifying rates.

The simultaneous equations become:

$$dP1/dt = -2\lambda\ P1(t) + \mu\ P2(t) \qquad \text{(B.5)}$$

$$dP2/dt = 2\lambda\ P1(t) + -\ (\lambda + \mu)\ P2(t) + \mu\ P3(t) \qquad \text{(B.6)}$$

$$dP3/dt = \lambda\ P2(t) + -\mu\ P3(t) \qquad \text{(B.7)}$$

For simplicity, it will be assumed that the availability required is the steady state availability.

When δt tends to infinity, dPi/dt will tend to zero and the equations become easier to solve. The additional equation as shown in Equation (B.4) above should also be used:

Now the equation $A(t) = P1(t) + P2(t)$ can be expressed as:

$A = P1 + P2$

Hence $A = (\mu^2 + 2\lambda\mu) / (\mu^2 + 2\lambda\mu + \lambda^2)$

B.24.5 Output.

The output from a Markov analysis is the various probabilities of being in the various states, and therefore an estimate of the failure probabilities and/or availability, one of the essential components of a system.

B.24.6 Strengths and Limitations.

Strengths of a Markov analysis include:

- ability to calculate the probabilities for systems with a repair capability and multiple degraded states.

Limitations of a Markov analysis include:

- assumption of constant probabilities of change of state; either failure or repairs;
- all events are statistically independent since future states are independent of all past states, except for the state immediately prior;
- needs knowledge of all probabilities of change of state;
- knowledge of matrix operations;
- results are hard to communicate with non-technical personnel.

B.24.7 Comparisons.

Markov analysis is similar to a Petri-Net analysis by being able to monitor and observe system states, although different since Petri-Net can exist in multiple states at the same time.

B.24.8 Reference Documents.

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and Boolean methods*

IEC 61165, *Application of Markov techniques*

ISO/IEC 15909 (all parts), *Software and systems engineering – High-level Petri nets*

B.25 Monte Carlo Simulation.

B.25.1 Overview.

Many systems are too complex for the effects of uncertainty on them to be modeled using analytical techniques, but they can be evaluated by considering the inputs as random variables and running a number N of calculations (so-called simulations) by sampling the input in order to obtain N possible outcomes of the wanted result.

This method can address complex situations that would be very difficult to understand and solve by an analytical method. Systems can be developed using spreadsheets and other conventional tools, but more sophisticated tools are readily available to assist with more complex requirements, many of which are now relatively inexpensive. When the technique was first developed, the number of iterations required for Monte Carlo simulations made the process slow and time consuming, but advances in computers and theoretical developments, such as Latin-hypercube sampling, have made processing time almost insignificant for many applications.

B.25.2 Use.

Monte Carlo simulation provides a means of evaluating the effect of uncertainty on systems in a wide range of situations. It is typically used to evaluate the range of possible outcomes and the relative frequency of values in that range for quantitative measures of a system such as cost, duration, throughput, demand and similar measures. Monte Carlo simulation may be used for two different purposes:

- uncertainty propagation on conventional analytical models;
- probabilistic calculations when analytical techniques do not work.

B.25.3 Input.

The input to a Monte Carlo simulation is a good model of the system and information on the types of inputs, the sources of uncertainty that are to be represented and the required output. Input data with uncertainty is represented as random variables with distributions which are more or less spread according to the level of uncertainties. Uniform, triangular, normal and log normal distributions are often used for this purpose.

B.25.4 Process.

The process is as follows:

a) A model or algorithm is defined which represents as closely as possible the behavior of the system being studied.

b) The model is run multiple times using random numbers to produce outputs of the model (simulations of the system); Where the application is to model the effects of uncertainty the model is in the form of an equation providing the relationship between input parameters and an output. The values selected for the inputs are taken from appropriate probability distributions that represent the nature of the uncertainty in these parameters.

c) In either case a computer runs the model multiple times (often up to 10,000 times) with different inputs and produces multiple outputs. These can be processed using conventional statistics to provide information such as average values, standard deviation, confidence intervals.

An example of a simulation is given below.

Consider the case of two items operating in parallel and only one is required for the system to function. The first item has a reliability of 0,9 and the other 0,8.

It is possible to construct a spreadsheet with the following columns.

Table B.4 – Example of Monte Carlo Simulation

	Item 1		Item 2		
Simulation Number	Random Number	Functions?	Random Number	Functions?	System
1	0,577 243	YES	0,059 355	YES	1
2	0,746 909	YES	0,311 324	YES	1
3	0,541 728	YES	0,919 765	NO	1
4	0,423 274	YES	0,643 514	YES	1
5	0,917 776	NO	0,539 349	YES	1
6	0,994 043	NO	0,972 506	NO	0
7	0,082 574	YES	0,950 241	NO	1
8	0,661 418	YES	0,919 868	NO	1
9	0,213 376	YES	0,367 555	YES	1
10	0,565 657	YES	0,119 215	YES	1

The random generator creates a number between 0 and 1 which is used to compare with the probability of each item to determine if the system is operational. With just 10 runs, the result of 0,9 should not be expected to be an accurate result. The usual approach is to build in a calculator to compare the total result as the simulation progresses to achieve the level of accuracy required. In this example, a result of 0,979 9 was achieved after 20,000 iterations.

The above model can be extended in a number of ways. For example:

- by extending the model itself (such as considering the second item becoming immediately operational only when the first item fails);
- by changing the fixed probability to a variable (a good example is the triangular distribution) when the probability cannot be accurately defined;
- using failure rates combined with the randomizer to derive a time of failure (exponential, Weibull, or other suitable distribution) and building in repair times.

Applications include, amongst other things, the assessment of uncertainty in financial forecasts, investment performance, project cost and schedule forecasts, business process interruptions and staffing requirements.

Analytical techniques are not able to provide relevant results or when there is uncertainty in the input data and so in the outputs.

B.25.5 Output.

The output could be a single value, as determined in the above example, it could be a result expressed as the probability or frequency distribution or it could be the identification of the main functions within the model that has the greatest impact on the output.

In general, a Monte Carlo simulation will be used to assess either the entire distribution of outcomes that could arise or key measures from a distribution such as:

- the probability of a defined outcome arising;
- the value of an outcome in which the problem owners have a certain level of confidence that it will not be exceeded or beaten, a cost that there is less than a 10% chance of exceeding or a duration that is 80% certain to be exceeded.

An analysis of the relationships between inputs and outputs can throw light on the relative significance of the factors at work and identify useful targets for efforts to influence the uncertainty in the outcome.

B.25.6 Strengths and Limitations.

Strengths of the Monte Carlo analysis include the following:

- the method can, in principle, accommodate any distribution in an input variable, including empirical distributions derived from observations of related systems;
- models are relatively simple to develop and can be extended as the need arises;
- any influences or relationships arising in reality can be represented, including subtle effects such as conditional dependencies;
- sensitivity analysis can be applied to identify strong and weak influences;
- models can be easily understood as the relationship between inputs and outputs is transparent;
- efficient behavioral models such as Petri Nets (future IEC 62551) are available which prove to be very efficient for Monte Carlo simulation purposes;
- provides a measure of the accuracy of a result;
- software is readily available and relatively inexpensive.

Limitations are as follows:

- the accuracy of the solutions depends upon the number of simulations which can be performed (this limitation is becoming less important with increased computer speeds);
- it relies on being able to represent uncertainties in parameters by a valid distribution;
- large and complex models may be challenging to the modeler and make it difficult for stakeholders to engage with the process;

- the technique may not adequately weigh high-consequence/low probability events and therefore not allow an organization's risk appetite to be reflected in the analysis.

B.25.7 Reference Documents.

IEC 61649, *Weibull analysis*

IEC 62551, *Analysis techniques for dependability – Petri net techniques*[1]

ISO/IEC Guide 98-3:2008, *Uncertainty measurement – Part 3: Guide to the of uncertainty in measurement (GUM:1995)*

B.26 Bayesian Statistics and Bayes Nets.

B.26.1 Overview.

Bayesian statistics are attributed to the Reverend Thomas Bayes. Its premise is that any already known information (the Prior) can be combined with subsequent measurement (the Posterior) to establish an overall probability. The general expression of the Bayes Theorem can be expressed as:

$$P(A \mid B) = \{P(A)\,P(B \mid A)\} / \sum_i P(B \mid E_i)P(E_i)$$

where:

the probability of X is denoted by $P(X)$;

the probability of X on the condition that Y has occurred is denoted by $P(X|Y)$; and

E_i is the ith event.

In its simplest form this reduces to $P(A \mid B) = \{P(A)P(B \mid A)\} / P(B)$.

Bayesian statistics differs from classical statistics in that is does not assume that all distribution parameters are fixed, but that parameters are random variables. 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 which is based upon physical evidence. As the Bayesian approach is based upon the subjective interpretation of probability, it provides a ready basis for decision thinking and the development of Bayesian nets (or Belief Nets, belief networks or Bayesian networks).

Bayes nets use a graphical model to represent a set of variables and their probabilistic relationships. The network is comprised of nodes that represent a random variable and arrows which link a parent node to a child node, (where a parent node is a variable that directly influences another (child) variable).

[1] Currently under consideration.

B.26.2 Use.

In recent years, the use of Bays' theory and Nets has become widespread partly because of their intuitive appeal and also because of the availability of software computing tools. Bayes nets have been used on a wide range of topics: medical diagnosis, image modeling, genetics, speech recognition, economics, space exploration and in the powerful web search engines used today. They can be valuable in any area where there is the requirement for finding out about unknown variables through the utilization of structural relationships and data. Bayes nets can be used to learn causal relationships to give an understanding about a problem domain and to predict the consequences of intervention.

B.26.3 Input.

The inputs are similar to the inputs for a Monte Carlo model. For a Bayes net, examples of the steps to be taken include the following:

- define system variables;
- define causal links between variables;
- specify conditional and prior probabilities;
- add evidence to net;
- perform belief updating;
- extract posterior beliefs.

B.26.4 Process.

Bayes theory can be applied in a wide variety of ways. This example will consider the creation of a Bayes table where a medical test is used to determine if the patient has a disease. The belief before taking the test is that 99% of the population do not have this disease and 1% have the disease, i.e the Prior information. The accuracy of the test has shown that if the person has the disease, the test result is positive 98% of the time. There is also a probability that if you do not have the disease, the test result is positive 10% of the time. The Bayes table provides the following information:

Table B.5 – Bayes' Table Data

	PRIOR	PROBABILITY	PRODUCT	POSTERIOR
Have Disease	0,01	0,98	0,009 8	0,090 1
No Disease	0,99	0,10	0,099 0	0,909 9
SUM	1		0,108 8	1

Using Bayes rule, the product is determined by combining the prior and probability. The posterior is found by dividing the product value by the product total. The output shows that a positive test result indicates that the prior has increased from 1% to 9%. More importantly, there is a strong chance that even with a positive test, having the disease is unlikely. Examining the equation $(0,01×0,98)/((0,01×0,98)+(0,99×0,1))$ shows that the 'no disease-positive result' value plays a major role in the posterior values.

Consider the following Bayes net:

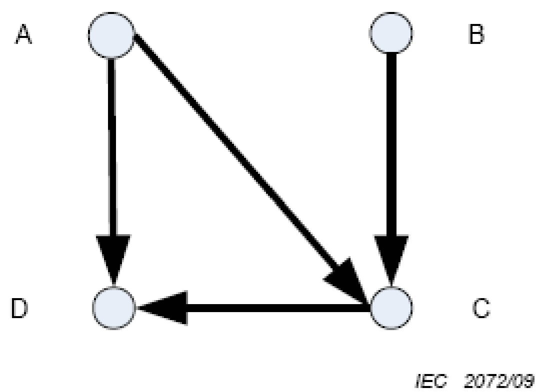


Figure B.11 – Sample Bayes' Net

With the conditional prior probabilities defined within the following tables and using the notation that Y indicates positive and N indicates negative, the positive could be "have disease" as above, or could be High and N could be Low.

Table B.6 – Prior Probabilities for Nodes A and B

P(*A* = *Y*)	P(*A* = *N*)	P(*B* = *Y*)	P(*B* = *N*)
0,9	0,1	0,6	0,4

Table B.7 – Conditional Probabilities for Node C with Node A and Node B Defined

A	*B*	P(*C* = *Y*)	P(*C* = *N*)
Y	*Y*	0,5	0,5
Y	*N*	0,9	0,1
N	*Y*	0,2	0,8
N	*N*	0,7	0,3

Table B.8 – Conditional Probabilities for Node D with Node A and Node C Defined

A	*C*	P(*D* = *Y*)	P(*D* = *N*)
Y	*Y*	0,6	0,4
Y	*N*	1,0	0,0
N	*Y*	0,2	0,8
N	*N*	0,6	0,4

To determine the posterior probability of P(*A*|*D*=*N*,*C*=*Y*), it is necessary to first calculate P(*A*,*B*|*D*=*N*,*C*=*Y*).

Using Bayes' rule, the value P(*D*|*A*,*C*)P(*C*|*A*,*B*)P(*A*)P(*B*) is determined as shown below and the last column shows the normalized probabilities which sum to 1 as derived in the previous example (result rounded).

Table B.9 – Posterior Probability for Nodes A and B with Node D and Node C Defined

A	*B*	P(*D*|*A*,*C*)P(*C*|*A*,*B*)P(*A*)P(*B*)	P(*A*,*B*|*D*=*N*,*C*=*Y*)
Y	*Y*	0,4 × 0,5 × 0,9 × 0,6 = 0,110	0,4
Y	*N*	0,4 × 0,9 × 0,9 × 0,4 = 0,130	0,48
N	*Y*	0,8 × 0,2 × 0,1 × 0,6 = 0,010	0,04
N	*N*	0,8 × 0,7 × 0,1 × 0,4 = 0,022	0,08

To derive P(*A*|*D*=*N*,*C*=*Y*), all values of *B* need to be summed:

Table B.10 – Posterior Probability for Node A with Node D and Node C Defined

P(*A*=*Y*|*D*=*N*,*C*=*Y*)	P(*A*=*N*|*D*=*N*,*C*=*Y*)
0,88	0,12

This shows that the prior for P(*A*=*N*) has increased from 0,1 to a posterior of 0,12 which is only a small change. On the other hand, P(*B*=*N*|*D*=*N*,*C*=*Y*) has changed from 0,4 to 0,56 which is a more significant change.

B.26.5 Outputs.

The Bayesian approach can be applied to the same extent as classical statistics with a wide range of outputs, e.g. data analysis to derive point estimators and confidence intervals. Its recent popularity is in relation to Bayes nets to derive posterior distributions. The graphical output provides an easily understood model and the data can be readily modified to consider correlations and sensitivity of parameters.

B.26.6 Strengths and Limitations.

Strengths:

- all that is needed is knowledge on the priors;
- inferential statements are easy to understand;
- Bayes' rule is all that is required;
- it provides a mechanism for using subjective beliefs in a problem.

Limitations:

- defining all interactions in Bayes nets for complex systems is problematic;
- Bayesian approach needs the knowledge of a multitude of conditional probabilities which are generally provided by expert judgment. Software tools can only provide answers based on these assumptions.

B.27 FN Curves.

B.27.1 Overview.

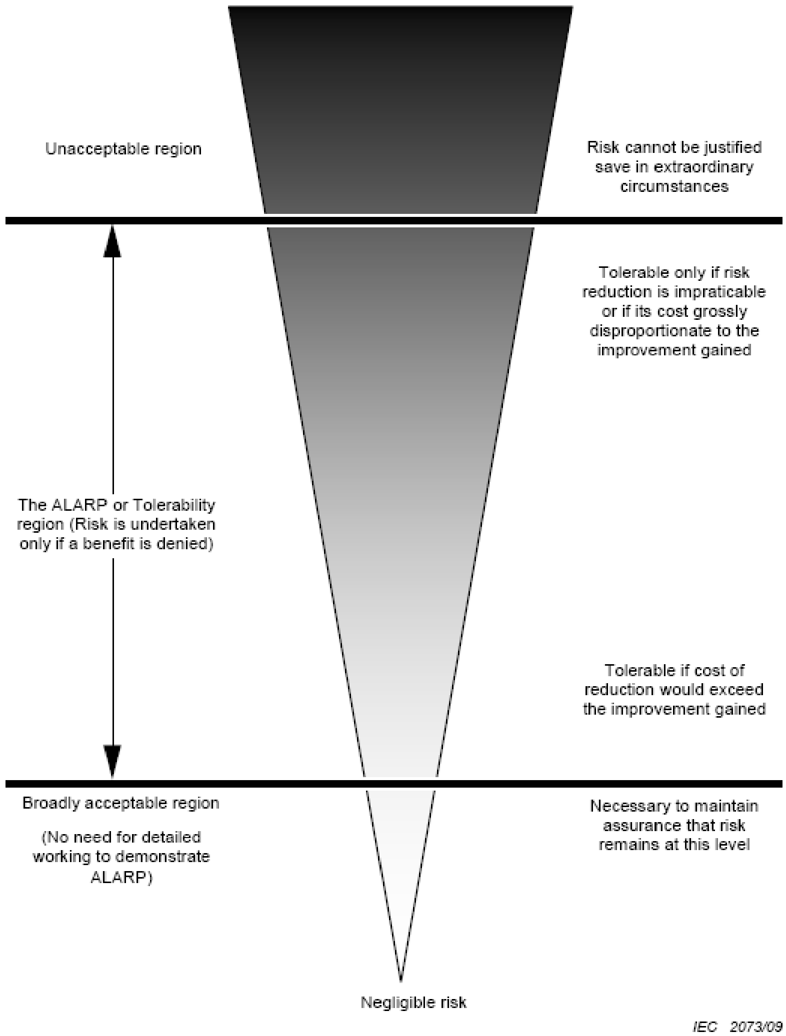


Figure B.12 – The ALARP Concept

FN curves are a graphical representation of the probability of events causing a specified level of harm to a specified population. Most often they refer to the frequency of a given number of casualties occurring.

FN curves show the cumulative frequency (*F*) at which *N* or more members of the population that will be affected. High values of N that may occur with a high frequency *F* are of significant interest because they may be socially and politically unacceptable.

B.27.2 Use.

FN curves are a way of representing the outputs of risk analysis. Many events have a high probability of a low consequence outcome and a low probability of a high consequence outcome. The FN curves provide a representation of the level of risk that is a line describing this range rather than a single point representing one consequence probability pair.

FN curves may be used to compare risks, for example to compare predicted risks against criteria defined as an FN curve, or to compare predicted risks with data from historical incidents, or with decision criteria (also expressed as an F/N curve).

FN curves can be used either for system or process design, or for management of existing systems.

B.27.3 Input.

The inputs are either:

- sets of the probability consequence pairs over a given period of time;
- the output of data from a quantitative risk analysis giving estimated probabilities for specified numbers of casualties;
- data from both historical records and a quantitative risk analysis.

B.27.4 Process.

The available data is plotted onto a graph with the number of casualties (to a specified level of harm, i.e. death) forming the abscissa with the probability of *N* or more casualties forming the ordinate. Because of the large range of values, both axes are normally on logarithmic scales.

FN curves may be constructed statistically using “real” numbers from past losses or they can be calculated from simulation model estimates. The data used and assumptions made may mean that these two types of FN curve give different information and should be used separately and for different purposes. In general, theoretical FN curves are most useful for system design, and statistical FN curves are most useful for management of a particular existing system.

Both derivation approaches can be very time-consuming so it is not uncommon to use a mixture of both. Empirical data will then form fixed points of precisely known casualties that occurred in known accidents/incident in a specified period of time and the quantitative risk analysis providing other points by extrapolation or interpolation.

The need to consider low-frequency, high-consequence accidents may require consideration of long periods of time to gather enough data for a proper analysis. This in turn may make the available data suspect if the initiating events happen to change over time.

B.27.5 Output.

A line representing risk across a range of values of consequence that can be compared with criteria that are appropriate for the population being studied and the specified level of harm.

B.27.6 Strengths and limitations.

FN curves are a useful way of presenting risk information that can be used by managers and system designers to help make decisions about risk and safety levels. They are a useful way of presenting both frequency and consequence information in an accessible format.

FN curves are appropriate for comparison of risks from similar situations where sufficient data is available. They should not be used to compare risks of different types with varying characteristics in circumstances where quantity and quality of data varies.

A limitation of FN curves is that they do not say anything about the range of effects or outcomes of incidents other than the number of people impacted, and there is no way of identifying the different ways in which the level of harm may have occurred. They map a particular consequence type, usually harm to people. FN curves are not a risk assessment method, but one way of presenting the results of risk assessment.

They are a well established method for presenting risk assessment results but require preparation by skilled analysts and are often difficult for non specialists to interpret and evaluate.

B.28 Risk Indices.

B.28.1 Overview.

A risk index is a semi-quantitative measure of risk which is an estimate derived using a scoring approach using ordinal scales. Risk indices can be used to rate a series of risks using similar criteria so that they can be compared. Scores are applied to each component of risk, for example contaminant characteristics (sources), the range of possible exposure pathways and the impact on the receptors.

Risk indices are essentially a qualitative approach to ranking and comparing risks. While numbers are used, this is simply to allow for manipulation. In many cases where the underlying model or system is not well known or not able to be represented, it is better to use a more overtly qualitative approach.

B.28.2 Use.

Indices can be used for classifying different risks associated with an activity if the system is well understood. They permit the integration of a range of factors which have an impact on the level of risk into a single numerical score for level of risk.

Indices are used for many different types of risk usually as a scoping device for classifying risk according to level of risk. This may be used to determine which risks need further in-depth and possibly quantitative assessment.

B.28.3 Input.

The inputs are derived from analysis of the system, or a broad description of the context. This requires a good understanding of all the sources of risk, the possible pathways and what might be affected. Tools such as fault tree analysis, event tree analysis and general decision analysis can be used to support the development of risk indices.

Since the choice of ordinal scales is, to some extent, arbitrary, sufficient data is needed to validate the index.

B.28.4 Process.

The first step is to understand and describe the system. Once the system has been defined, scores are developed for each component in such a way that they can be combined to provide a composite index. For example, in an environmental context, the sources, pathway and receptor(s) will be scored, noting that in some cases there may be multiple pathways and receptors for each source. The individual scores are combined according to a scheme that takes account of the physical realities of the system. It is important that the scores for each part of the system (sources, pathways and receptors) are internally consistent and maintain their correct relationships. Scores may be given for components of risk (e.g. probability, exposure, consequence) or for factors which increase risk.

Scores may be added, subtracted, multiplied and/or divided according to this high level model. Cumulative effects can be taken into account by adding scores (for example, adding scores for different pathways). It is strictly not valid to apply mathematical formulae to ordinal scales. Therefore, once the scoring system has been developed, the model should be validated by applying it to a known system. Developing an index is an iterative approach and several different systems for combining the scores may be tried before the analyst is comfortable with the validation.

Uncertainty can be addressed by sensitivity analysis and varying scores to find out which parameters are the most sensitive.

B.28.5 Output.

The output is a series of numbers (composite indices) that relate to a particular source and which can be compared with indices developed for other sources within the same system or which can be modeled in the same way.

B.28.6 Strengths and Limitations.

Strengths:

- indices can provide a good tool for ranking different risks;
- they allow multiple factors which affect the level of risk to be incorporated into a single numerical score for the level of risk.

Limitations:

- if the process (model) and its output are not well validated, the results may be meaningless. The fact that the output is a numerical value for risk may be misinterpreted and misused, for example in subsequent cost/benefit analysis;
- in many situations where indices are used, there is no fundamental model to define whether the individual scales for risk factors are linear, logarithmic or of some other

form, and no model to define how factors should be combined. In these situations, the rating is inherently unreliable and validation against real data is particularly important.

B.29 Consequence/Probability Matrix.

B.29.1 Overview.

The consequence/probability matrix is a means of combining qualitative or semi-quantitative ratings of consequence and probability to produce a level of risk or risk rating.

The format of the matrix and the definitions applied to it depend on the context in which it is used and it is important that an appropriate design is used for the circumstances.

B.29.2 Use.

A consequence/probability matrix is used to rank risks, sources of risk or risk treatments on the basis of the level of risk. It is commonly used as a screening tool when many risks have been identified, for example to define which risks need further or more detailed analysis, which risks need treatment first, or which need to be referred to a higher level of management. It may also be used to select which risks need not be considered further at this time. This kind of risk matrix is also widely used to determine if a given risk is broadly acceptable, or not acceptable (see 5.4) according to the zone where it is located on the matrix.

The consequence/probability matrix may also be used to help communicate a common understanding for qualitative levels of risks across the organization. The way risk levels are set and decision rules assigned to them should be aligned with the organization's risk appetite.

A form of consequence/probability matrix is used for criticality analysis in FMECA or to set priorities following HAZOP. It may also be used in situations where there is insufficient data for detailed analysis or the situation does not warrant the time and effort for a more quantitative analysis.

B.29.3 Input.

Inputs to the process are customized scales for consequence and probability and a matrix which combines the two.

The consequence scale (or scales) should cover the range of different types of consequence to be considered (for example: financial loss; safety; environment or other parameters, depending on context) and should extend from the maximum credible consequence to the lowest consequence of concern. A part example is shown in Figure B.6.

The scale may have any number of points. 3, 4 or 5 point scales are most common.

The probability scale may also have any number of points. Definitions for probability need to be selected to be as unambiguous as possible. If numerical guides are used to define different probabilities, then units should be given. The probability scale needs to span the range relevant to the study in hand, remembering that the lowest probability must be acceptable for the highest defined consequence, otherwise all activities with the highest consequence are defined as intolerable. A part example is shown in Figure B.7.

A matrix is drawn with consequence on one axis and probability on the other. Figure B.8 shows part of an example matrix with a 6 point consequence and 5 point probability scales.

The risk levels assigned to the cells will depend on the definitions for the probability/ consequence scales. The matrix may be set up to give extra weight to consequences (as shown) or to probability, or it may be symmetrical, depending on the application. The levels of risk may be linked to decision rules such as the level of management attention or the time scale by which response is needed.

Rating	Financial impact AU$ EBITDA	Investment Return AU$ NPV	Health and Safety	Environment and Community	Reputation	Legal and Compliance
6	$100m+ loss or gain	$300 + loss or gain	• Multiple fatalities, or • Significant irreversible effects to 10's of people	• Irreversible long term environmental harm. • Community outrage- potential large-scale class action.	• International press reporting over several days. • Total loss of shareholder support who act to dis-invest. • CEO departs and board is restructured.	• Major litigation or prosecution with damages of $50m+ plus significant costs. • Custodial sentence for company Executive • Prolonged closure of operations by authorities.
5	$10m - $99m loss or gain	$30m - $299m loss or gain	• Single fatality and/or • Severe irreversible disability to one or more persons	• Prolonged environmental impact. • High-profile community concerns raised – requiring significant remediation measures.	• National press reporting over several days. • Sustained impact on the reputation of shareholders. • Loss of shareholder support for grow • Pressu	• Major litigation costing $10m+ • Investigation by regulator body resulting in lo interruption t
4	$1m – $9m loss or gain	$3m – $29m loss or gain	• Extensive injuries or irreversi	• Major spil		
3	$100k – $900 loss or gain					
2	$10k - lo					
1						

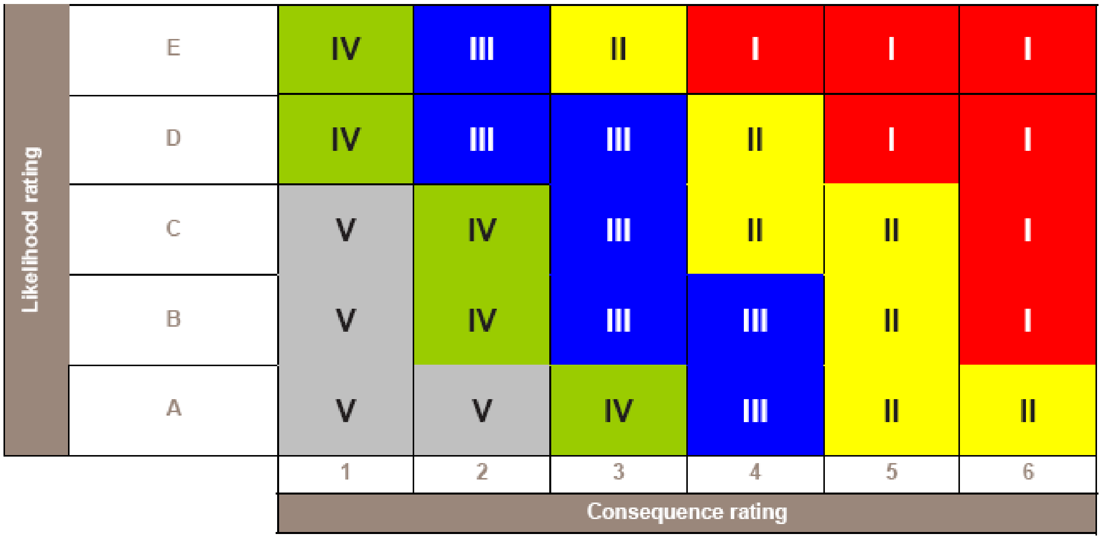
IEC 2074/09

Figure B.13 – Part Example of a Consequence Criteria Table

Rating	Criteria
Likely	- balance of probability will occur, or - could occur within "weeks to months"
Possible	- may occur shortly but a distin - could occur within "mo
Unlikely	- may occur but not - could occur in "y
Rare	- occurrence re - exceptional - only occ
Remote	- theor - fr

IEC 2075/09

Figure B.14 – Part Example of a Risk Ranking Matrix



IEC 2076/09

Figure B.15 – Part Example of a Probability Criteria Matrix

Rating scales and a matrix may be set up with quantitative scales. For example, in a reliability context the probability scale could represent indicative failure rates and the consequence scale the dollar cost of failure.

Use of the tool needs people (ideally a team) with relevant expertise and such data as is available to help in judgments of consequence and probability.

B.29.4 Process.

To rank risks, the user first finds the consequence descriptor that best fits the situation then defines the probability with which those consequences will occur. The level of risk is then read off from the matrix.

Many risk events may have a range of outcomes with different associated probability. Usually, minor problems are more common than catastrophes. There is therefore a choice as to whether to rank the most common outcome or the most serious or some other combination. In many cases, it is appropriate to focus on the most serious credible outcomes as these pose the largest threat and are often of most concern. In some cases, it may be appropriate to rank both common problems and unlikely catastrophes as separate risks. It is important that the probability relevant to the selected consequence is used and not the probability of the event as a whole.

The level of risk defined by the matrix may be associated with a decision rule such as to treat or not to treat the risk.

B.29.5 Output.

The output is a rating for each risk or a ranked list of risk with significance levels defined.

B.29.6 Strengths and Limitations.

Strengths:

- relatively easy to use;
- provides a rapid ranking of risks into different significance levels.

Limitations:

- a matrix should be designed to be appropriate for the circumstances so it may be difficult to have a common system applying across a range of circumstances relevant to an organization;
- it is difficult to define the scales unambiguously;
- use is very subjective and there tends to be significant variation between raters;
- risks cannot be aggregated (i.e. one cannot define that a particular number of low risks or a low risk identified a particular number of times is equivalent to a medium risk);
- it is difficult to combine or compare the level of risk for different categories of consequences.

Results will depend of the level of detail of the analysis, i.e. the more detailed the analysis, the higher the number of scenarios, each with a lower probability. This will underestimate the actual level of risk. The way in which scenarios are grouped together in describing risk should be consistent and defined at the start of the study.

B.30 Cost/Benefit Analysis (CBA).

B.30.1 Overview.

Cost/benefit analysis can be used for risk evaluation where total expected costs are weighed against the total expected benefits in order to choose the best or most profitable option. It is an implicit part of many risk evaluation systems. It can be qualitative or quantitative or involve a combination of quantitative and qualitative elements. Quantitative CBA aggregates the monetary value of all costs and all benefits to all stakeholders that are included in the scope and adjusts for different time periods in which costs and benefits accrue. The net present value (NPV) which is produced becomes an input into to decisions about risk. A positive NPV associated with an action would normally mean the action should occur. However, for some negative risks, particularly those involving risks to human life or damage to the environment the ALARP principle may be applied. This divides risks into three regions: a level above which negative risks are intolerable and should not be taken except in extraordinary circumstances; a level below which risks are negligible and need only to be monitored to ensure they remain low; and a central band where risks are made as low as reasonably practicable (ALARP). Towards the lower risk end of this region, a strict cost benefit analysis may apply but where risks are close to intolerable, the expectation of the ALARP principle is that treatment will occur unless the costs of treatment are grossly disproportionate to the benefit gained.

B.30.2 Uses.

Cost/benefit analysis can be used to decide between options which involve risk.

For example:

- as input into a decision about whether a risk should be treated,
- to differentiate between and decide on the best form of risk treatment,
- to decide between different courses of action.

B.30.3 Inputs.

Inputs include information on costs and benefits to relevant stakeholders and on uncertainties in those costs and benefits. Tangible and intangible costs and benefits should be considered. Costs include resources expended and negative outcomes, benefits include positive outcomes, negative outcomes avoided and resources saved.

B.30.4 Process.

The stakeholders who may experience costs or receive benefits are identified. In a full cost benefit analysis all stakeholders are included.

The direct and indirect benefits and costs to all relevant stakeholders of the options being considered are identified. Direct benefits are those which flow directly from the action taken, while indirect or ancillary benefits are those which are coincidental but might still contribute significantly to the decision. Examples of indirect benefits include reputation improvement, staff satisfaction and “peace of mind”. (These are often weighted heavily in decision-making).

Direct costs are those that are directly associated with the action. Indirect costs are those additional, ancillary and sunk costs, such as loss of utility, distraction of management time or the diversion of capital away from other potential investments. When applying a cost benefit analysis to a decision on whether to treat a risk, costs and benefits associated with treating the risk, and with taking the risk, should be included.

In quantitative cost/benefit analysis, when all tangible and intangible costs and benefits have been identified, a monetary value is assigned to all costs and benefits (including intangible costs and benefits). There are a number of standard ways of doing this including the ‘willingness to pay’ approach and using surrogates. If, as often happens, the cost is incurred over a short period of time (e.g. a year) and the benefits flow for a long period thereafter, it is normally necessary to discount the benefits to bring them into “today’s money” so that a valid comparison can be obtained. All costs and benefits are expressed as a present value. The present value of all costs and all benefits to all stakeholders can be combined to produce a net present value (NPV). A positive NPV implies that the action is beneficial. Benefit cost ratios are also used see B30.5

If there is uncertainty about the level of costs or benefits, either or both terms can be weighted according to their probabilities.

In qualitative cost benefit analysis no attempt is made to find a monetary value for intangible costs and benefits and, rather than providing a single figure summarizing the costs and benefits, relationships and trade-offs between different costs and benefits are considered qualitatively.

A related technique is a cost-effectiveness analysis. This assumes that a certain benefit or outcome is desired, and that there are several alternative ways to achieve it. The analysis looks only at costs and which is the cheapest way to achieve the benefit.

B.30.5 Output.

The output of a cost/benefit analysis is information on relative costs and benefits of different options or actions. This may be expressed quantitatively as a net present value (NPV) an internal rate of return (IRR) or as the ratio of the present value of benefits to the present value of costs. Qualitatively the output is usually a table comparing costs and benefits of different types of cost and benefit, drawing attention to trade offs.

B.30.6 Strengths and Limitations.

Strengths of cost benefit analysis:

- it allows costs and benefits to be compared using a single metric (money);
- it provides transparency of decision making;
- it requires detailed information to be collected on all possible aspects of the decision. This can be valuable in revealing ignorance as well as communicating knowledge.

Limitations:

- quantitative CBA can yield dramatically different numbers, depending on the methods used to assign economic values to non-economic benefits;
- in some applications it is difficult to define a valid discounting rate for future costs and benefits;
- benefits which accrue to a large population are difficult to estimate, particularly those relating to public good which is not exchanged in markets;
- the practice of discounting means that benefits gained in the long term future have negligible influence on the decision depending on the discounting rate chosen. The method becomes unsuitable for consideration of risks affecting future generations unless very low or zero discount rates are set.

B.31 Multi-Criteria Decision Analysis (MCDA).

B.31.1 Overview.

The objective is to use a range of criteria to objectively and transparently assess the overall worthiness of a set of options. In general, the overall goal is to produce a preference of order between the available options. The analysis involves the development of a matrix of options and criteria which are ranked and aggregated to provide an overall score for each option.

B.31.2 Use.

MCDA can be used for:

- comparing multiple options for a first pass analysis to determine preferred and potential options and inappropriate option,
- comparing options where there are multiple and sometimes conflicting criteria,
- reaching a consensus on a decision where different stakeholders have conflicting objectives or values.

B.31.3 Inputs.

A set of options for analysis. Criteria, based on objectives that can be used equally across all options to differentiate between them.

B.31.4 Process.

In general a group of knowledgeable stakeholders undertakes the following process:

a) define the objective(s);

b) determine the attributes (criteria or performance measures) that relate to each objective;

c) structure the attributes into a hierarchy;

d) develop options to be evaluated against the criteria;

e) determine the importance of the criteria and assign corresponding weights to them;

f) evaluate the alternatives with respect to the criteria. This may be represented as a matrix of scores.

g) combine multiple single-attribute scores into a single aggregate multi attribute score;

h) evaluate the results.

There are different methods by which the weighting for each criteria can be elicited and different ways of aggregating the criteria scores for each option into a single multi-attribute score. For example, scores may be aggregated as a weighted sum or a weighted product or using the analytic hierarchy process, an elicitation technique for the weights and scores based on pair-wise comparisons. All these methods assume that the preference for any one criterion does not depend on the values of the other criteria. Where this assumption is not valid, different models are used.

Since scores are subjective, sensitivity analysis is useful to examine the extent to which the weights and scores influence overall preferences between options.

B.31.5 Outputs.

Rank order presentation of the options goes from best to least preferred. If the process produces a matrix where the axes of the matrix are criteria weighted and the criteria score for each option, then options that fail highly weighted criteria can also be eliminated.

B.31.6 Strengths and Limitations.

Strengths:

- provides a simple structure for efficient decision-making and presentation of assumptions and conclusions;
- can make complex decision problems, which are not amenable to cost/benefit analysis, more manageable;
- can help rationally consider problems where tradeoffs need to be made;
- can help achieve agreement when stakeholders have different objectives and hence criteria.

Limitations:

- can be affected by bias and poor selection of the decision criteria;
- most MCDA problems do not have a conclusive or unique solution;
- aggregation algorithms which calculate criteria weights from stated preferences or aggregate differing views can obscure the true basis of the decision.

AhA

AhA