Risk analysis

Professor P John Clarkson
October 2013

INTRODUCTION

- The patient leaves the safety of their home to enter the healthcare system

INTRODUCTION

- At the health centre the patient seeks help to control ongoing pain from arthritis
- The patient is referred to the local hospital

INTRODUCTION

- At the outpatient clinic the patient is assessed and started on weekly doses of Methotrexate

INTRODUCTION

- Back home the patient manages their weekly medication regime
- The take methotrexate weekly and folic acid daily

INTRODUCTION

- The patient's blood is monitored
- The methotrexate dose is varied to control toxicity

What could possibly go wrong?

INTRODUCTION

- A locum GP prescribes Methotrexate daily
- The error is not corrected despite routine practice checks

INTRODUCTION

- The pharmacist dispenses a daily dose of Methotrexate
- The patient dutifully takes a daily dose

INTRODUCTION

- The patient is admitted to the ENT ward with symptoms of a severe sore throat
- The patient's blood tests fail to detect problem

INTRODUCTION

- In specialist care blood test results finally show abnormal conditions
- A methotrexate overdose is suspected

Patient dies

INTRODUCTION

- What level of safety is required?

Frequency of Occurrence	Severity			
	(1) Catastrophic	(2) Critical	(3) Marginal	(4) Negligible
(A) Frequent	1A	2A	3A	4A
(B) Probable	1B	2B	3B	4B
(C) Occasional	1C	2C	3C	4C
(D) Remote	1D	2D	3D	4D
(E) Improbable	1E	2E	3E	4E

US Air Force

INTRODUCTION

- How many people can we kill?

Frequency of Occurrence	Severity			
	(1) Death	(2) Severe injury	(3) Injury	(4) Minor injury
(A) Daily	1A	2A	3A	4A
(B) Weekly	1B	2B	3B	4B
(C) Monthly	1C	2C	3C	4C
(D) Annually	1D	2D	3D	4D
(E) Improbable	1E	2E	3E	4E

Scales need to be defined

INTRODUCTION

- Develop a means of providing efficient, safe and realistic fire fighting training for all ship-board personnel
- You are permitted to kill one training officer every ten years

http://en.wikipedia.org/wiki/Firefighting#mediaviewer/File:Aircraft_Rescue_Firefighting_training.jpg

INTRODUCTION

- Project driven by active risk assessment on safety and delivery
- Project manager personally involved in the commissioning trials

http://en.wikipedia.org/wiki/Firefighting#mediaviewer/File:Aircraft_Rescue_Firefighting_training.jpg

INTRODUCTION

- Training in service across the UK with a level of realism and safety second to none
- You are permitted to kill one trainee every one hundred years

http://en.wikipedia.org/wiki/Firefighting#mediaviewer/File:Aircraft_Rescue_Firefighting_training.jpg

INTRODUCTION

“ Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events. ”

Source: Douglas Hubbard, The Failure of Risk Management.

INTRODUCTION

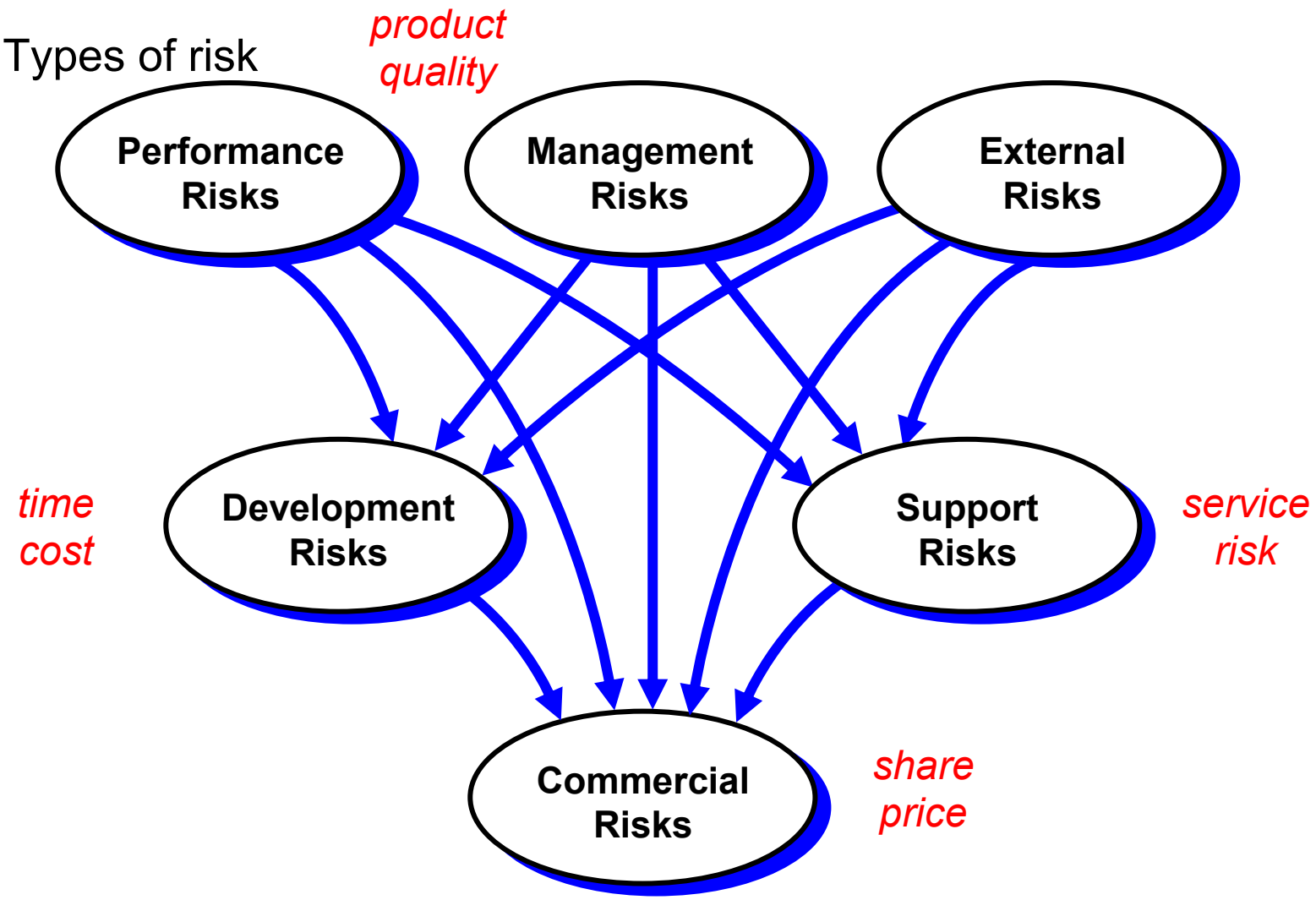
“ Risks can come from uncertainty in financial markets, project failures, legal liabilities, credit risk, accidents, natural causes and disasters as well as deliberate attacks from an adversary.

“ The strategies to manage risk include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk. ”

Source: Douglas Hubbard, The Failure of Risk Management.

INTRODUCTION

- Types of risk



INTRODUCTION

- All systems are designed with a particular purpose in mind, for example, a car is designed to meet a variety of performance, comfort, safety and cost requirements
- There is a possibility that a system will not perform as expected, leading to some undesirable behaviour, where:

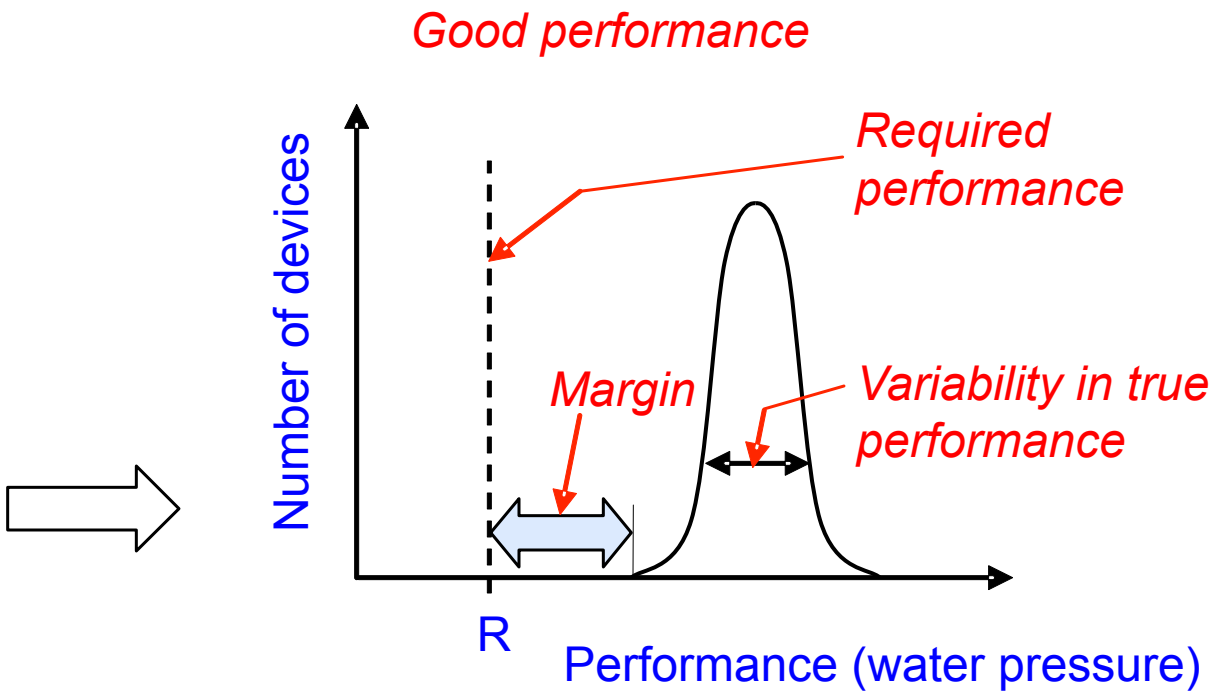
risk = likelihood x impact

PERFORMANCE RISK

- Consider a device that must resist water ingress
- Several components may work in combination to meet this performance requirement – for example, an enclosure, a lid and an o-ring seal
- Their collective performance will exhibit a certain degree of variability – as illustrated by a normal distribution curve
- The fundamental properties of the design dictate the position of the curve and the expected variabilities in manufacturing dictate its shape
- R is the required performance, which all devices must satisfy

PERFORMANCE RISK

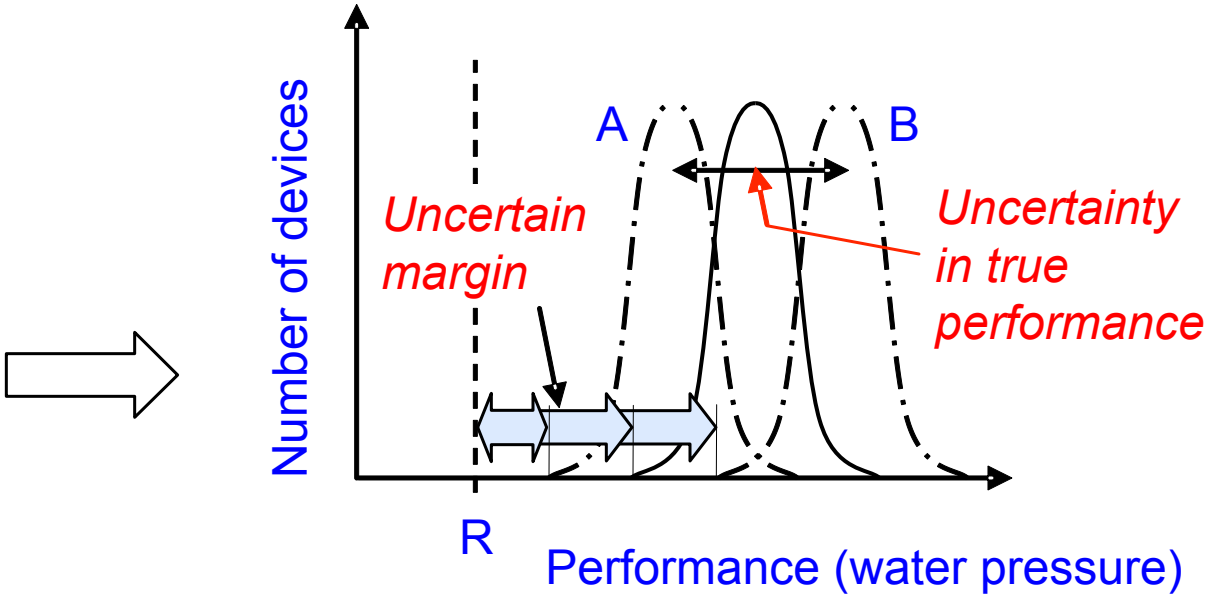
- **Good performance** – the concept device design appears to perform well; there is a considerable margin, or safety factor, between worst-case and target performance and the device has a high chance of exceeding its performance requirement



PERFORMANCE RISK

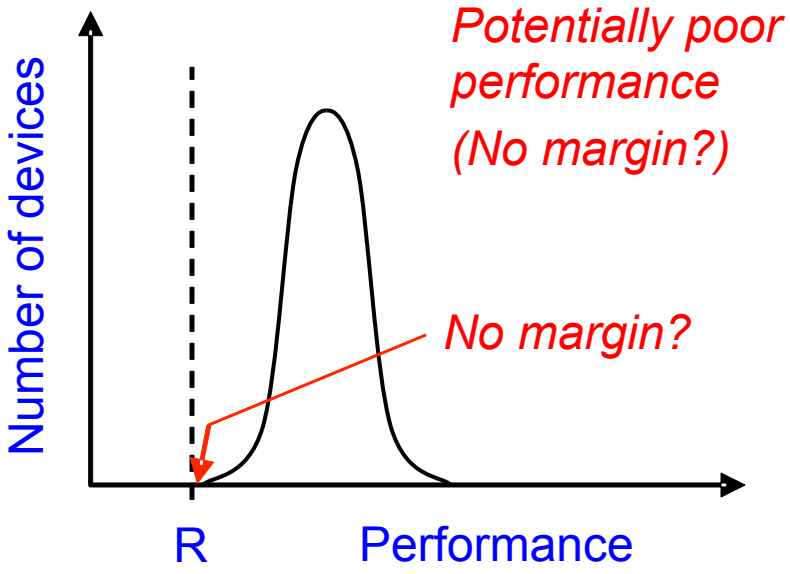
- **Potentially good performance** – there may be some degree of uncertainty in the location of the 'worst-case' (A) and the 'best-case' (B) estimations of performance, but even if the worst-case scenario (A) is true the device will easily meet its requirement

Good but uncertain performance



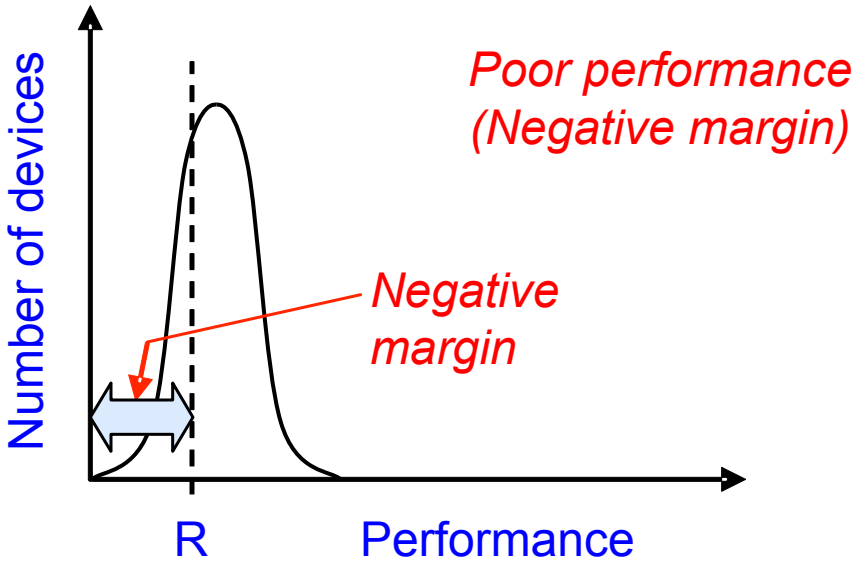
PERFORMANCE RISK

- **Potentially poor performance** – a different design may have an estimated performance that is much closer to the required performance, where there is a significantly greater chance that the design could fail



PERFORMANCE RISK

- **Poor performance** – in the worst scenario there is little chance that the device will perform as required and it either needs to be redesigned or the requirements need to be modified



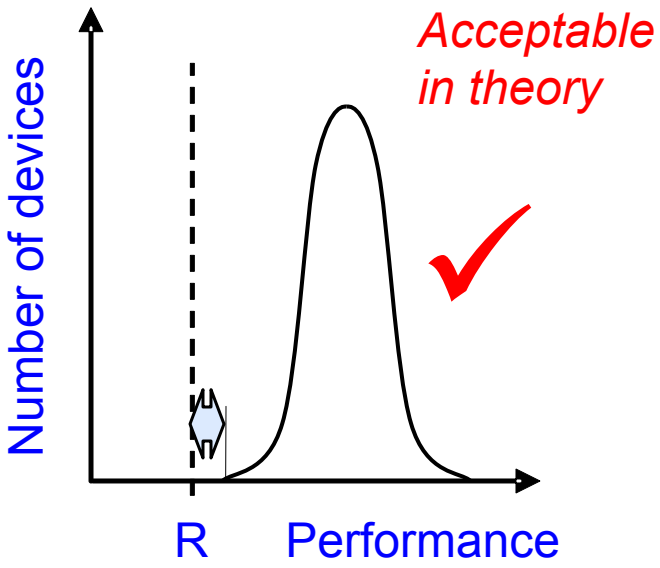
PERFORMANCE RISK

“ If maintaining a seal were a safety-critical requisite (perhaps to prevent microbiological contamination) the device manufacturer would feel more confident if the performance in this respect exceeded requirements by a considerable margin. Thus, the device should be designed so that the chance of seal failure is remote. ”

Source: James Ward and John Clarkson, Design Verification.

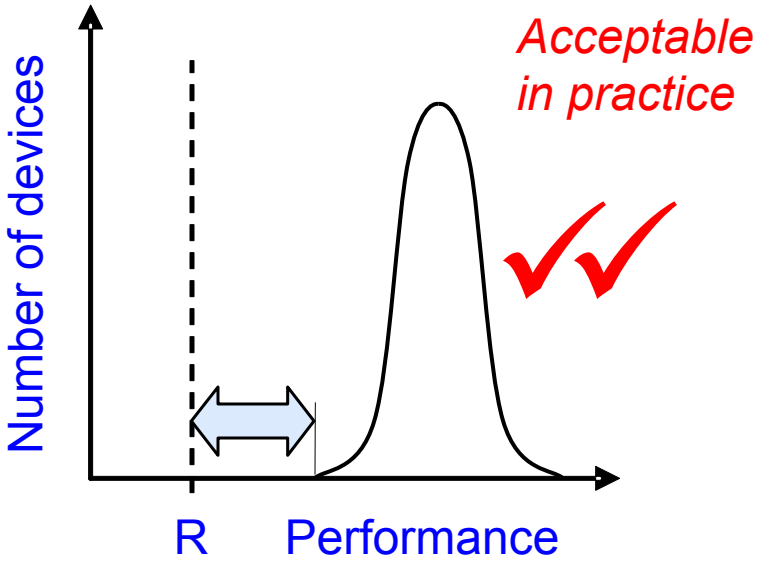
PERFORMANCE RISK

- Risk is normally defined as a combination of the probability of an event occurring and the resulting impact
- Theoretical risk should be verified through practical evaluation



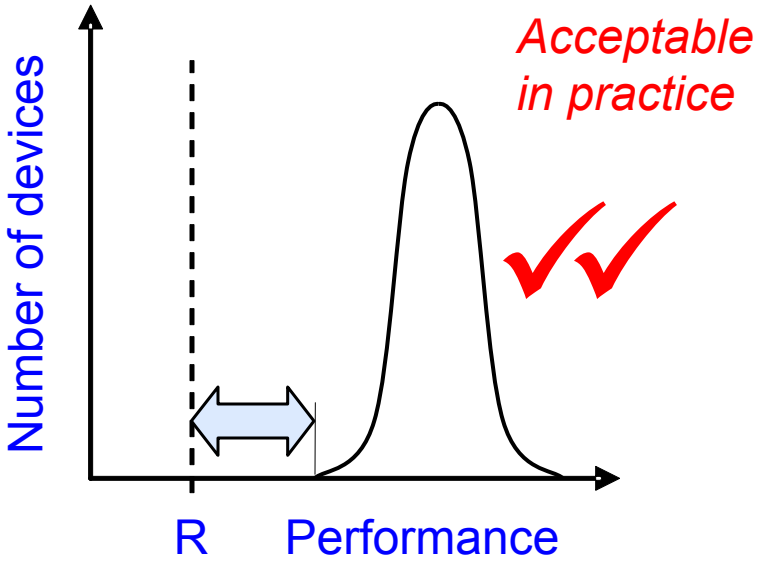
PERFORMANCE RISK

- Ultimately, it is essential to be confident that risks have been reduced to an acceptable level
- This is accomplished through appropriate verification

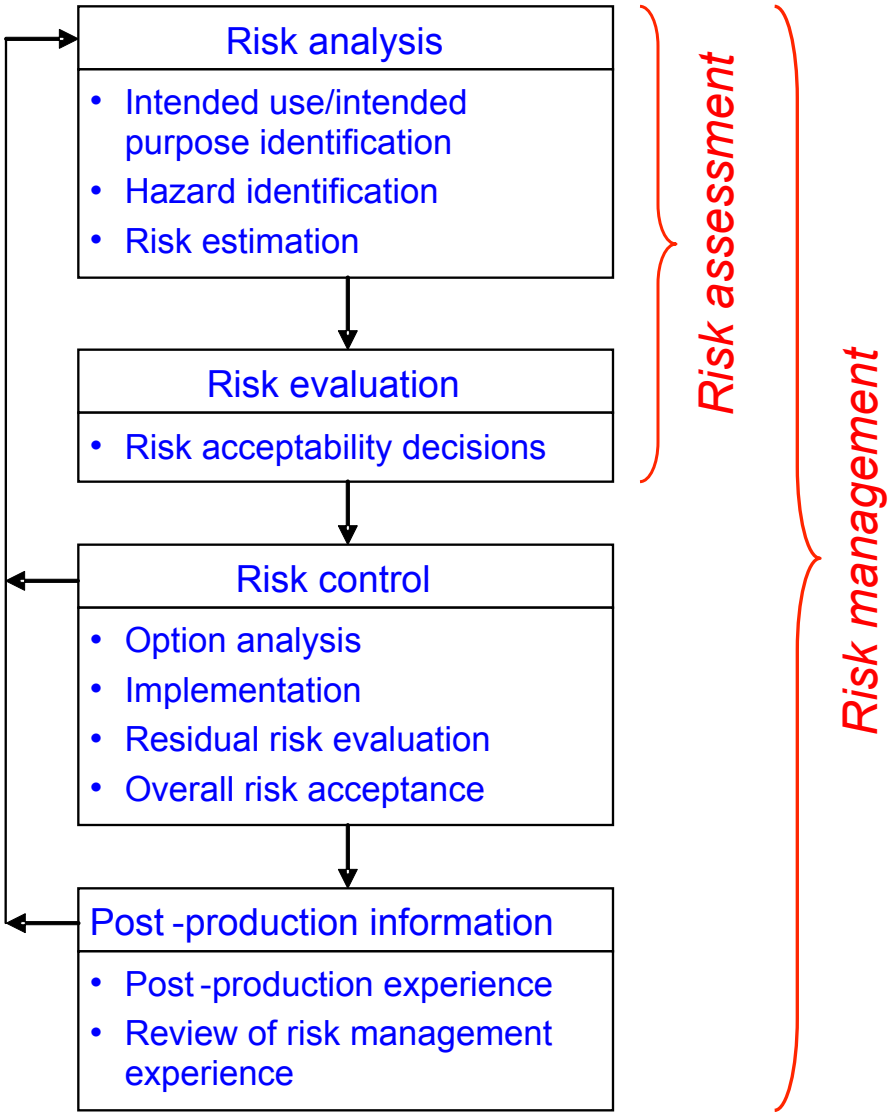


PERFORMANCE RISK

- Performance evaluation approaches can also be applied to development and commercial risk



RISK MANAGEMENT

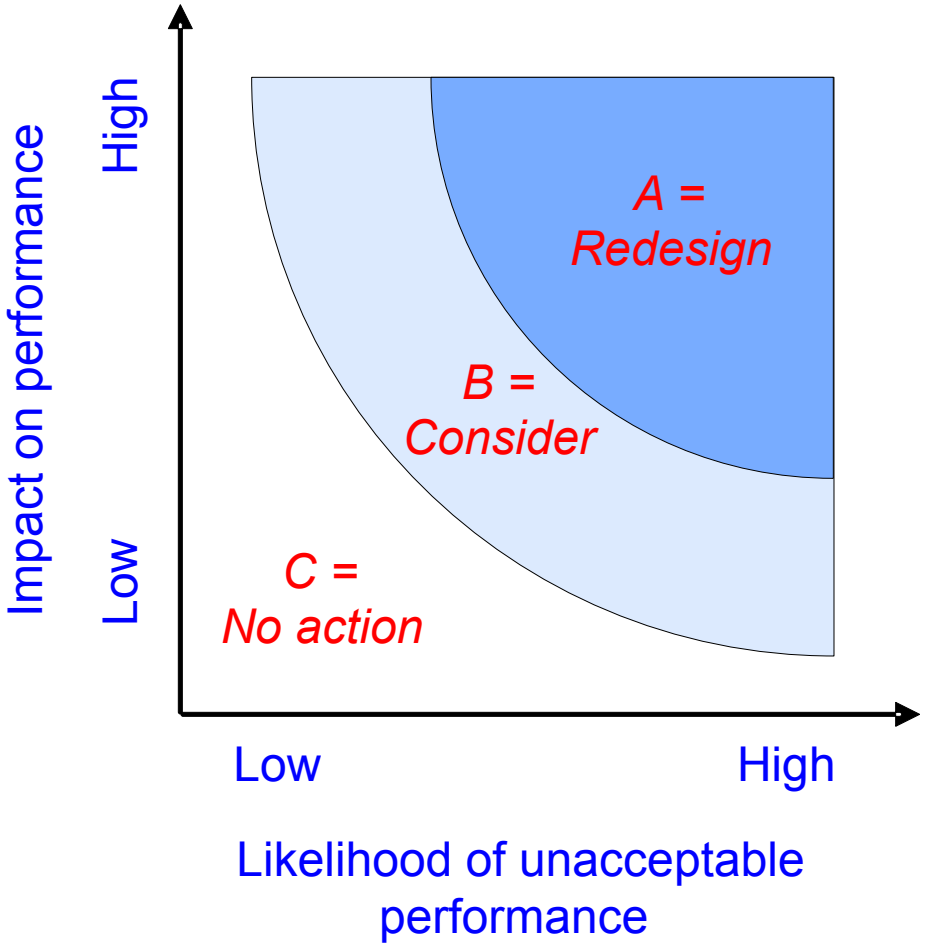


RISK MANAGEMENT

- Risk analysis involves the systematic identification of hazards (potential sources of harm) and their risks, how likely they are to cause a problem and how severe it would be if they did
- Risk management refers to the entire process of identifying hazards, analysing risks and controlling them and can be outlined as follows:
  1) hazard identification – identify what can go wrong
  2) risk estimation – assess the likelihood and severity of each hazard
  3) risk evaluation – decide whether risks are acceptable
  4) risk control – reduce any unacceptable risks to acceptable levels
  5) risk monitoring – checking that acceptable risk levels are maintained

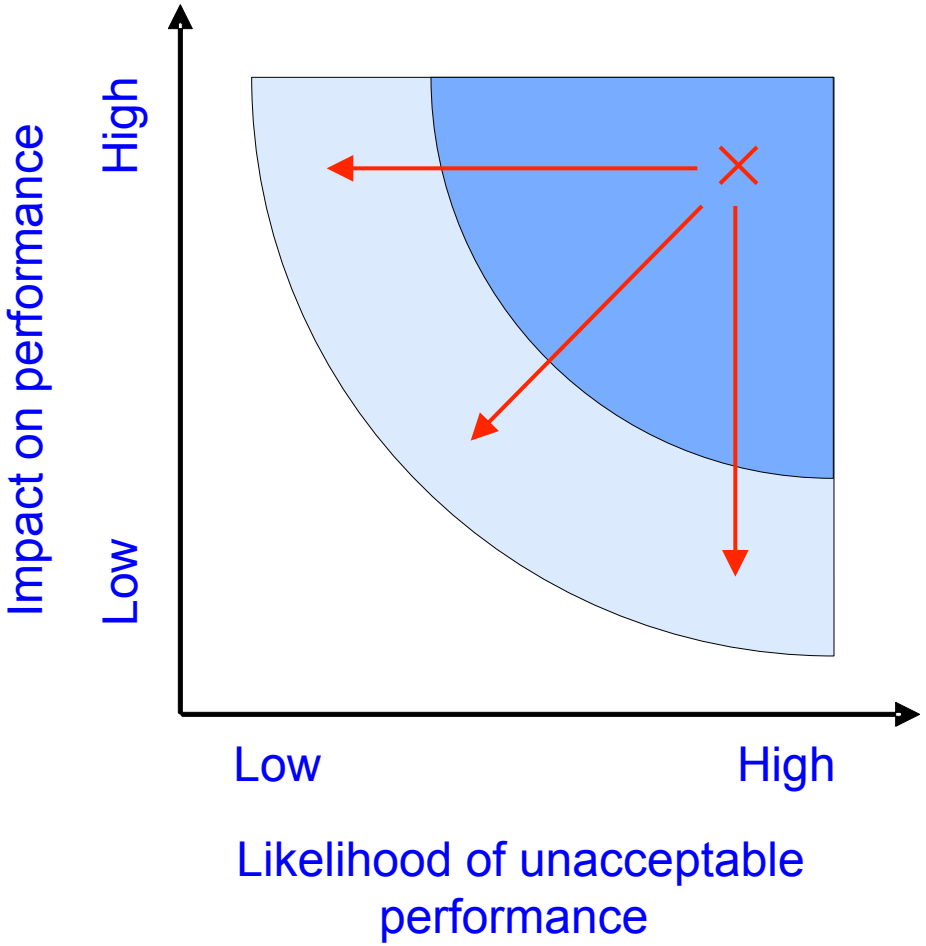
RISK MANAGEMENT

- Risk evaluation – decide whether risks are acceptable

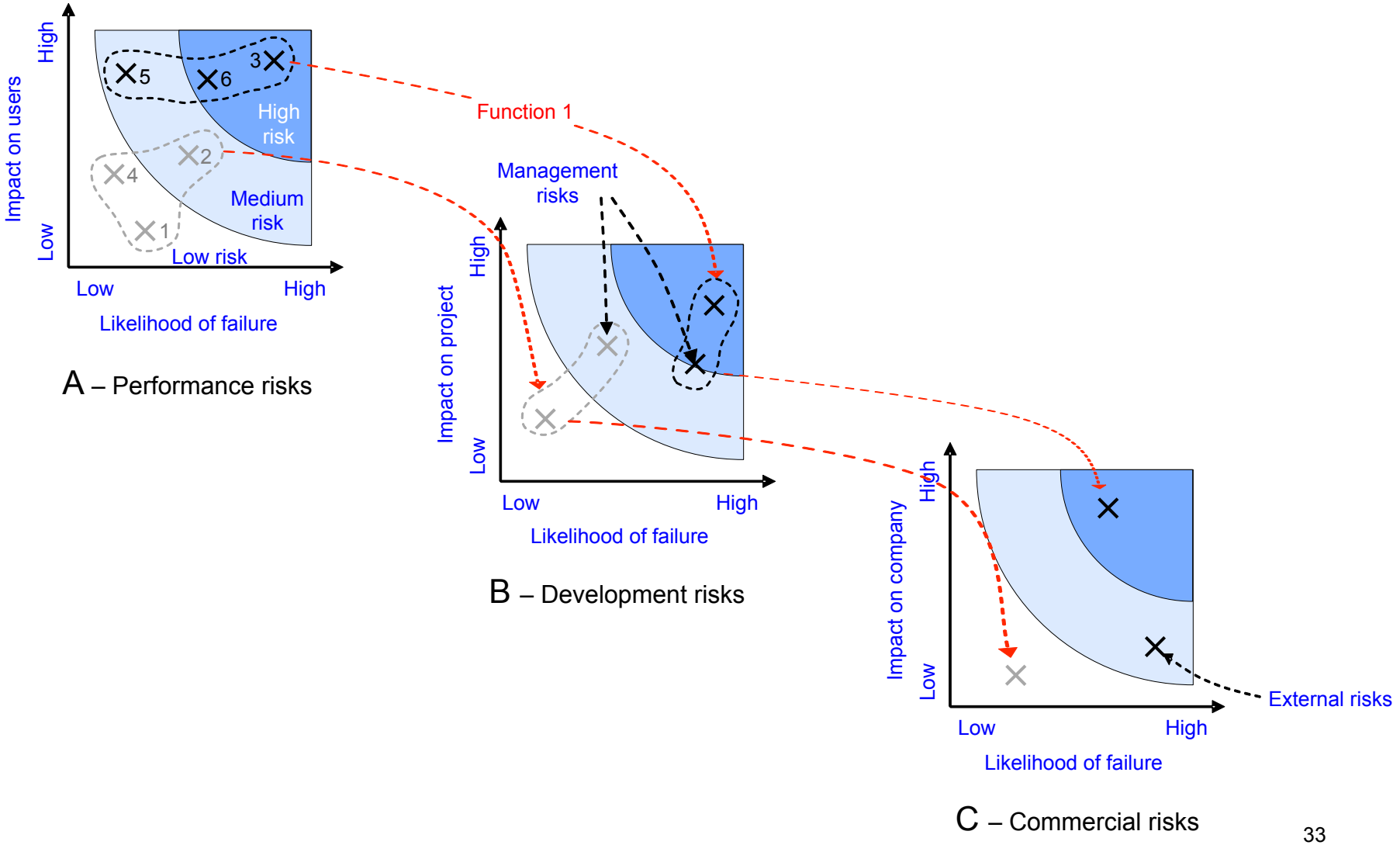


RISK MANAGEMENT

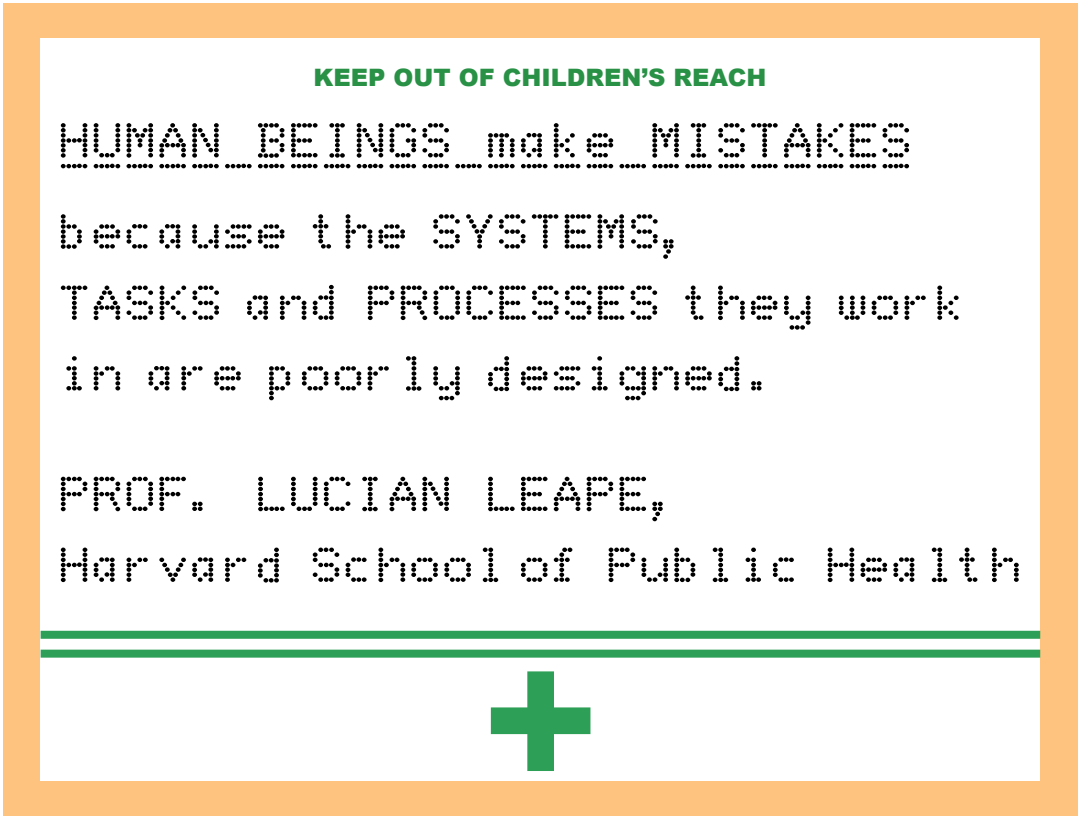
- Risk control – reduce any unacceptable risks to acceptable levels



RISK MANAGEMENT



RISK MANAGEMENT



Source: John Clarkson et al., Design for Patient Safety.

RISK MANAGEMENT

- **Hazard** – The way in which an object or situation may cause harm

  A hazard exists where an object (or substance) or situation has a built-in ability to cause an adverse effect. Such hazards include uneven pavements, unguarded machinery, an icy road, a fire, an explosion and a sudden escape of toxic gas.

- **Exposure** – the extent to which the likely recipient of the harm is exposed to, or can be influenced by, the hazard

  The presence of a potential target in the area and its distance from the hazard will determine the extent of the risk. For instance, a fire or explosion may cause damage to nearby buildings and their contents, or to vehicles and equipment, but will not harm people if there are no people present at the time.

RISK MANAGEMENT

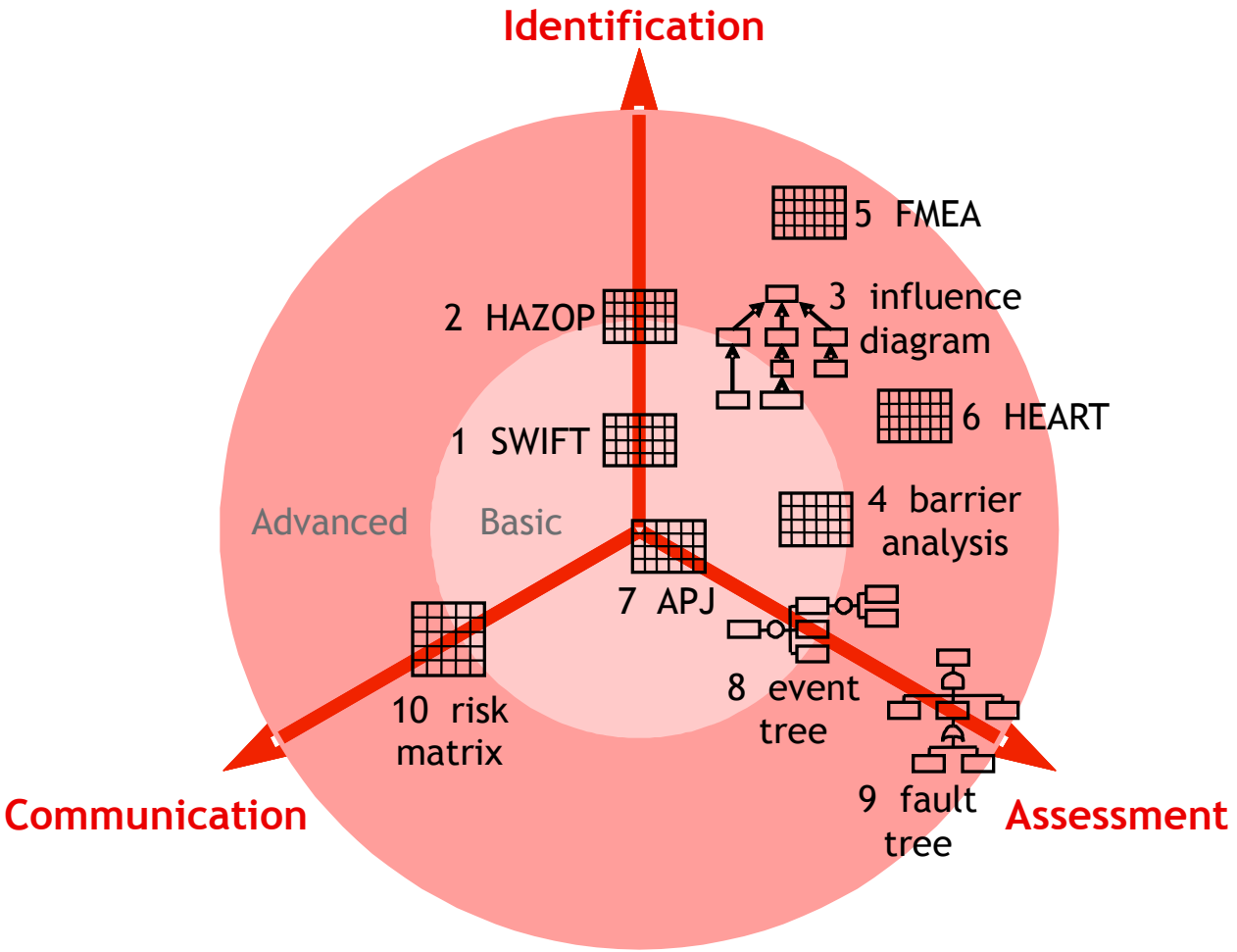
- For harm to occur in practice – in other words, for there to be a risk – there must be BOTH the hazard AND the exposure to that hazard; without both these at the same time, there is no risk.

- **Risk** – the chance that harm will actually occur

  Risk, on the other hand, is the chance that such effects will occur: the risk can be high or negligible.

risk = hazard + exposure

RISK ASSESSMENT



RISK ASSESSMENT

Risk assessment approach / Characteristics of interest	1 SWIFT	2 HAZOP	3 Influence diagram	4 Barrier analysis	5 FMEA	6 HEART	7 APJ	8 Event tree	9 Fault tree	10 Risk matrix
Hazard identification	✓	✓	✓		✓					
Risk identification					✓	✓	✓			
Existing safeguard identification			✓	✓				✓	✓	
Required safeguard identification			✓	✓				✓	✓	
Risk prioritisation					✓	✓	✓	✓	✓	
Risk communication										✓

RISK ASSESSMENT

- The rigorous examination of a system can be assisted by reference to structural systems mappings such as task, information and organisational diagrams.
- For many risk assessment methods, such as SWIFT, HAZOP, barrier analysis, FMEA, APJ and HEART, structural mappings provide the basis for investigating the impact of the partial or complete failure of each component and/or interface in the system.
- For other methods, such as event and fault trees and influence diagrams, structural mappings provide an excellent background to the assessment. In both cases, the failure of interfaces to components outside of the system boundary should also be considered.

RISK ASSESSMENT

- The rigorous examination of a system can be assisted by reference to behavioural systems mappings such as system, flow and communication diagrams.
- For many risk assessment methods, such as SWIFT, HAZOP, barrier analysis, FMEA, APJ and HEART, behavioural mappings provide the fundamental basis for investigating the impact of the partial or complete failure of each component and/or interface in the system. Such investigation should be systematic and exhaustive, considering all aspects of system behaviour.
- For other methods, such as event and fault trees and influence diagrams, behavioural mappings provide an excellent background to the assessment.

STRUCTURED WHAT IF TECHNIQUE

- SWIFT is a structured team-based study that uses “what-if” questions to help a team think about and identify relevant hazards and risks. It focuses on deviations from normal operations and the impact they may have on a system, procedure or organisation.
- SWIFT facilitates discussions to help the team explore differing scenarios, their consequences, causes and impacts. From these discussions hazards, risks and controls are identified and summarised.
- SWIFT enables hazards and risks to be ranked, based on the perceived severity of the risk and suitability of the existing risk controls, to help identify relevant actions. It is most effective where a good description of the system is available.

STRUCTURED WHAT IF TECHNIQUE

id.	What-if questions	Hazards and risks	Relevant controls	Risk ranking	Action notes
X	how much?				
A					
B					
C					
D					
E					
F					
G					
H					
I					
J					

HAZARD AND OPERABILITY ANALYSIS

- HAZOP is a team-based hazard identification method which provides a systematic and structured analysis of a system, focusing not only on hazards, but also on operability issues. It provides a qualitative assessment of the presence of hazards, their potential consequence and appropriate actions.
- HAZOP focuses on deviation from the intended performance of the system. It can reveal shortcomings in the overall activity, the design of its component parts, proposed methods of operation, or interactions between these.
- HAZOP is used where a good description of the system is available and draws on the expertise and understanding of a group of people who are experienced either in the specific or similar systems.

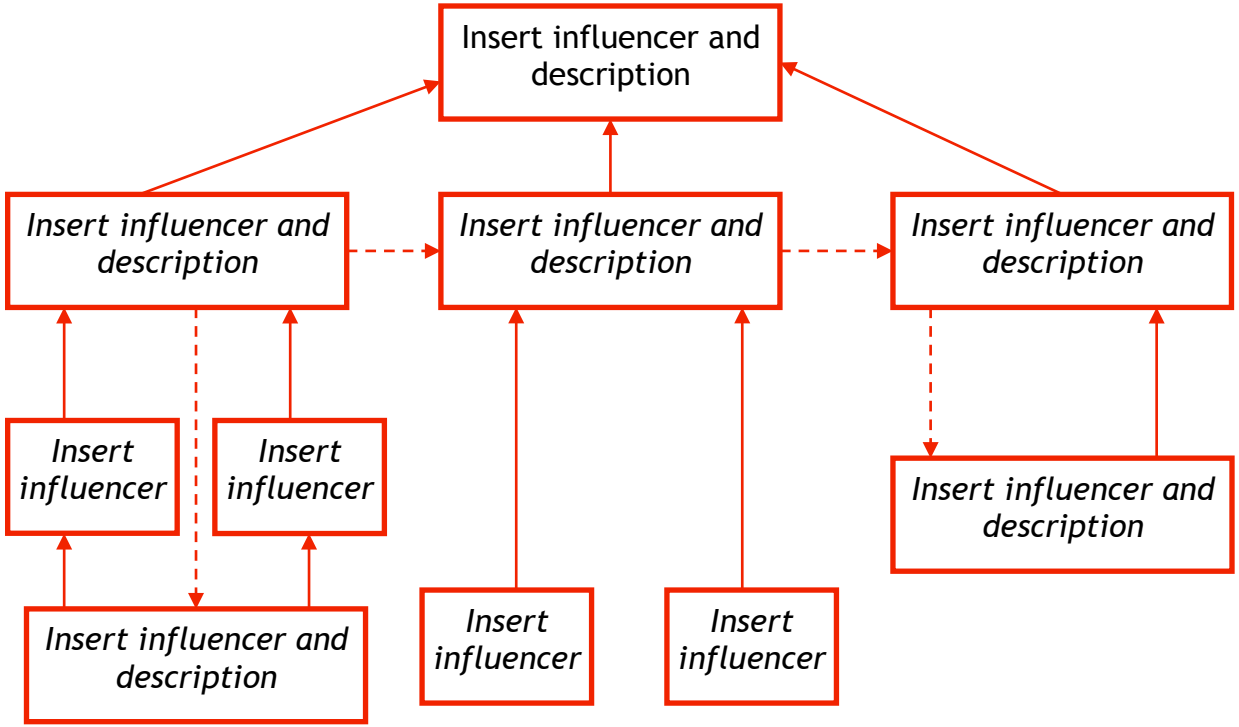
HAZARD AND OPERABILITY ANALYSIS

id.	Prompt words	Deviation	Causes	Conse-quences	Existing barriers	Actions
X	less than					
A						
B						
C						
D						
E						
F						
G						
H						
I						
J						

INFLUENCE DIAGRAM

- An influence diagram is a graphical technique for representing all relevant factors that can influence the occurrence of an event, including organisational, individual, team, system and external influencers.
- Influence diagrams are developed through defining and describing the conditions, setting and high-level actions that lead up to events. All relevant influencers are identified and evaluated qualitatively and where applicable quantitatively.
- Influence diagrams require a team containing a range of experienced individuals who can offer a variety of different perspectives on a given system/process and are knowledgeable regarding possible influencers, contexts and relevant conditions.

INFLUENCE DIAGRAM



BARRIER ANALYSIS

- Barrier analysis is a safety analysis technique that focuses on how harmful energy is passed to vulnerable people (objects) and provides qualitative and functional analysis of the barriers that are/ need to be in place to prevent the transfer of energy and enhance safety.
- Barrier analysis defines four factors that are needed for an accident or adverse event to occur: a harmful energy flow or environmental condition; vulnerable people or objects; failure or loss of barriers to provide protection; and a set of events leading to accident/adverse event.
- Barrier analysis relies on the use of data collection methods such as observations and structured interviews to gather system and event information, while the use of task analysis helps to represent activity/event/task sequences.

BARRIER ANALYSIS

id.	Activity	Energy/ people	Barrier function	Barrier failures	Barrier actions
X	Prescribing				
A					
B					
C					
D					
E					
F					
G					
H					
I					
J					

FAILURE MODE AND EFFECTS ANALYSIS

- FMEA is a team-based technique that can be used to consider and identify the effects of human error on systems. It is a flexible approach that can be used to consider individual operator failure and/or team failures.
- FMEA identifies the likelihood of the failure and severity of consequence for each failure mode identified by the team. The combined influence of severity and likelihood is then used to rank failure modes and prioritise corrective actions.
- FMEA requires a team containing a range of experienced individuals who can offer a variety of different perspectives on a given system/process. It is most effective where a good description of the system is available.

FAILURE MODE AND EFFECTS ANALYSIS

id.	Task steps	Failure modes	Causes	Likelihood /severity	Recovery steps	Actions
X	Infusion					
A						
B						
C						
D						
E						
F						
G						
H						
I						
J						

HUMAN ERROR ASSESSMENT AND REDUCTION TECHNIQUE

- HEART is a human reliability method that is used to evaluate the probability of a human error occurring during the execution of a specific task.
- HEART is based on the principle that every time a task is undertaken there is a possibility of failure and the probability of failure is affected by error producing conditions, for example distraction, experience, tiredness.
- HEART should be used when there is a requirement to understand and determine a quantified probability of task failure. Thus for high-risk systems and activities, where task failure can have significant adverse impact on employees and the public, HEART can help identify probability levels of task failure, the error producing conditions and what could be done to help reduce potential task failure.

HUMAN ERROR ASSESSMENT AND REDUCTION TECHNIQUE

id.	Task class	Error condition	Total effect	Assess affect	Assessed affect	Prob of failure
X	Complex					
A						
B						
C						
D						
E						
F						
G						
H						
I						
J						

ABSOLUTE PROBABILITY JUDGEMENT

- APJ is a human reliability method that is used to evaluate the probability of a human error occurring during the execution of a specific task. It involves a group of experts (front line staff, engineers, managers etc) using their knowledge and experience to estimate and determine human error probabilities.
- APJ is best utilised when there is limited data to calculate human error probabilities, or when the data is unsuitable, unreliable and/or difficult to understand. However, it can be used in conjunction with techniques that provide information on tasks, potential failures and errors to help the experts estimate error probabilities.
- APJ is also able to provides insights into the types of strategies that can be put in place to reduce the probability of error and task failure.

ABSOLUTE PROBABILITY JUDGEMENT

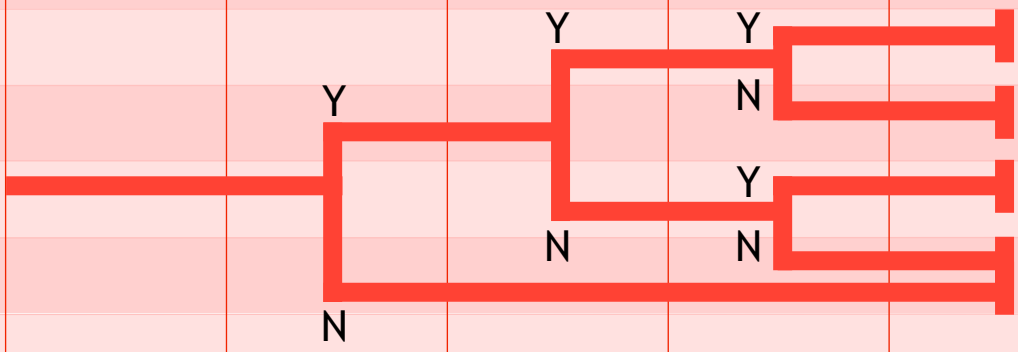
id.	Potential errors	Maximum probability	Minimum probability	Range	Geometric mean
X	Overdose				
A					
B					
C					
D					
E					
F					
G					
H					
I					
J					

EVENT TREE

- An event tree is a graphical device used to logically depict an event sequence in order to help investigate the sequence of operator actions leading to an event and identify the possible consequences of these sequences.
- Event trees use nodes to depict each task within an event sequence and paths leading from the nodes to indicate possible outcomes of the task. These are usually defined as success or failure.
- Event trees can be used throughout the lifecycle of a system or procedure to identify potential scenarios for testing, help identify operator behaviour and ways to improve system reliability and help represent adverse events that have occurred and the impact of operator behaviour on that event.

EVENT TREE

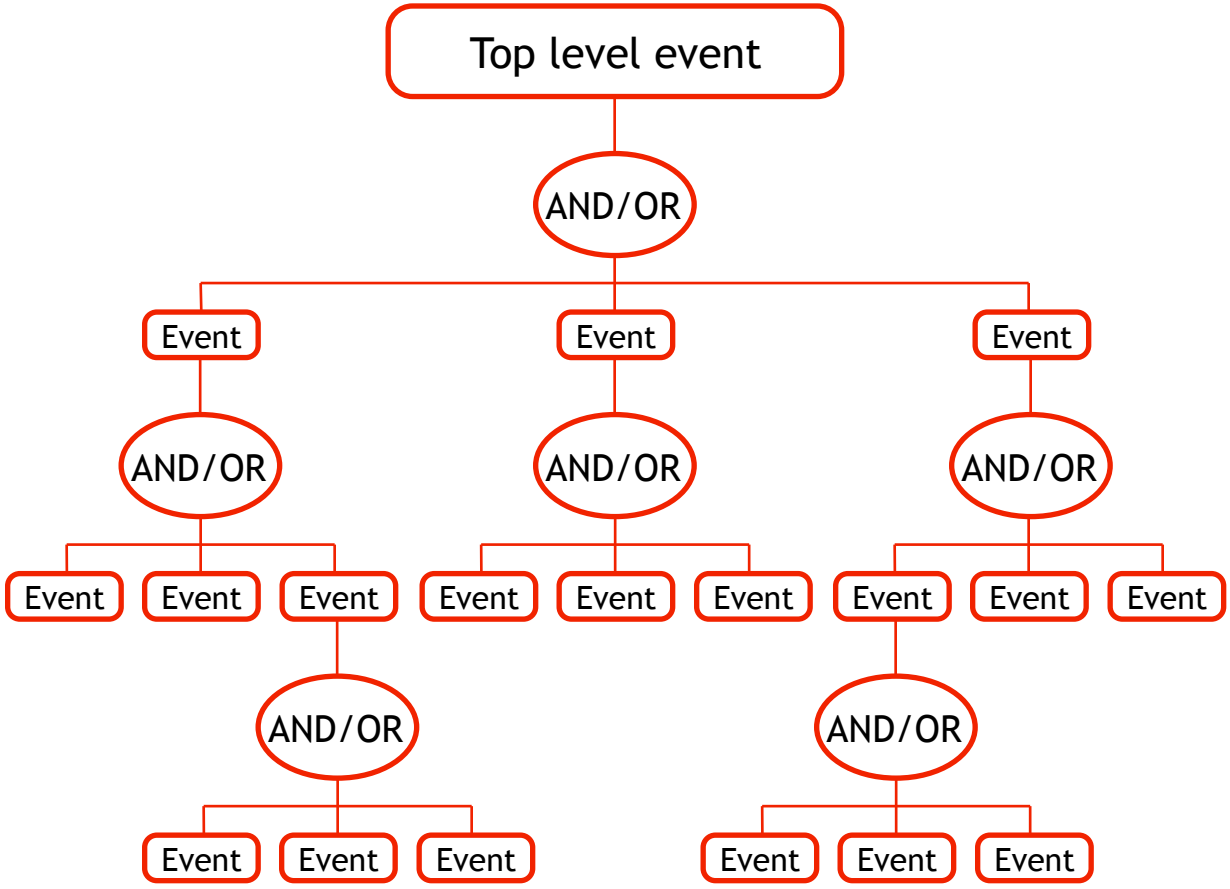
id.	Initiating event	1st defence active?	2nd defence active?	3rd defence active?	Resultant event
X	Overdose				
A					
B					
C					
D					
E					
F					
G					
H					
I					
J					



FAULT TREE

- A fault tree is a graphical device for identifying and analysing factors that contribute to the occurrence of an adverse or undesired event. They are tree-like diagrams that pictorially represents such factors and their logical relationship to the adverse/undesired event.
- Fault trees provide insight into the relevant causes of failure and highlight interrelationships between system components and potential weaknesses in system reliability. They can also be used to analyse the causes of human error, their impact on system reliability and when quantified help determine system risk.
- Fault trees can be used either to quantitatively assess the likelihood of an undesirable event occurring or to qualitatively assess causes of failures.

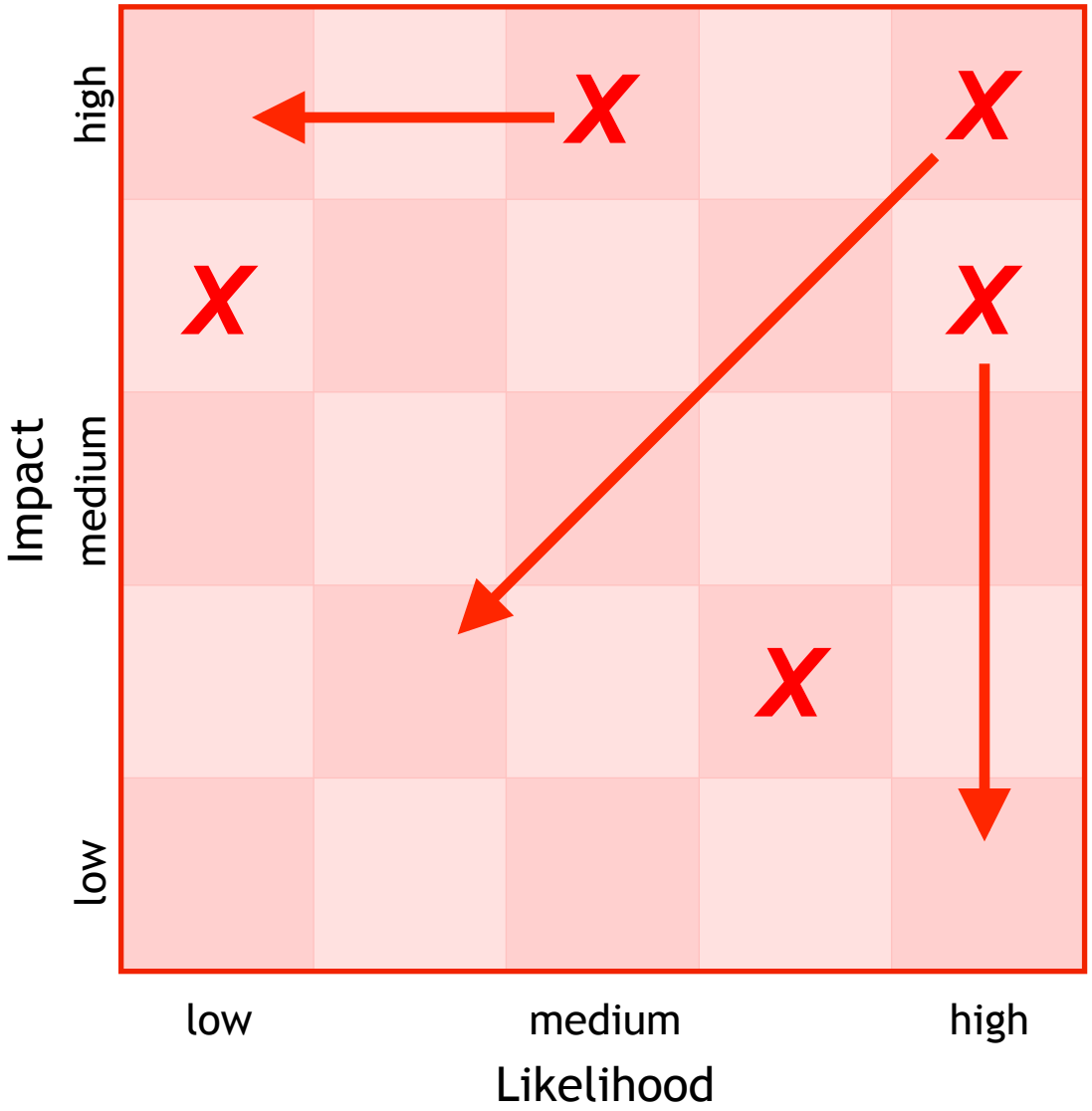
FAULT TREE


Top level event
AND/OR
Event
Event
Event
AND/OR
AND/OR
AND/OR
Event
Event
Event
Event
Event
Event
Event
Event
Event
AND/OR
AND/OR
Event
Event
Event
Event
Event
Event

RISK MATRIX

- Risk matrices allow individuals to rank the consequence and likelihood of an undesired event, act or activity to provide a risk rating. They can be used in conjunction with a range of methods, such as HAZOP and FMEA, to rank and prioritise risk.
- Risk matrices are made up of two axes – likelihood and impact, often using a scoring system from 1(low) to 5 (high). Impact can take many forms including injury to persons, property and/or profit.
- Risk matrices may also be partitioned to into regions of acceptable and unacceptable risk. In general entries in the upper right of the matrix are not desirable, while those in the lower are likely to be acceptable.

RISK MATRIX



HAZARD AND OPERABILITY ANALYSIS

- A hazard and operability study (HAZOP) takes a product or process design which is assumed to be sound and systematically assesses the consequences and likely causes of abnormal behaviour.
- Hazard and operability studies:
  - were developed for the *chemical* industry
  - identify hazards and operational problems
  - normally used to assess process designs
  - may be used on any development program
  - are qualitative
  - involve teams

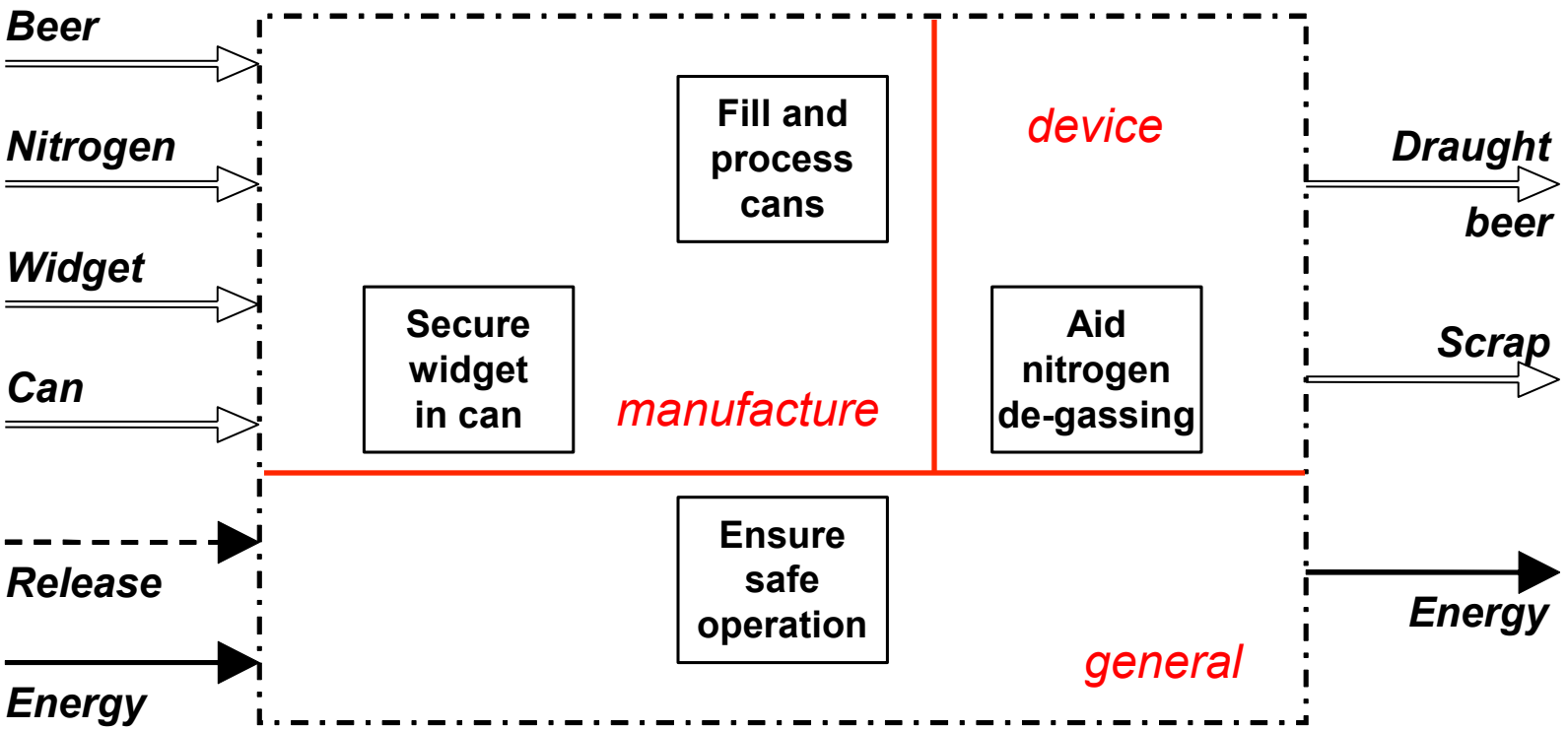
HAZARD AND OPERABILITY ANALYSIS

- Individual *process 'flows'* are assessed for the effects of deviation from normal operating conditions.
- The following key words are used to assist the HAZOP team:
  - NONE - none of any relevant physical property
  - MORE OF - more of any relevant physical property
  - LESS OF - less of any relevant physical property
  - PART OF - composition different
  - MORE THAN - more components present
  - OTHER THAN - other non-normal states (e.g. maintenance)

HAZARD AND OPERABILITY ANALYSIS

- The HAZOP team should include:
  - design engineers
  - production engineers
  - product / service users
  - safety manager
  - program manager
  - *independent chairperson*
- The output of the study is an action list specifying required design changes or further more detailed hazard analysis.

EXAMPLE: DRAUGHT BEER IN A CAN



HAZARD AND OPERABILITY ANALYSIS

Consider the parameter ***'beer volume'***

No.	Keyword	Effect	Cause	Action
1	*MORE OF (too much beer)*	*Spill on opening*	*Filling error*	*Reject can*
2	*LESS OF (too little beer)*	*Low volume*	*Filling error*	*Reject can*
3	*PART OF (wrong recipe)*	*Poor taste*	*Beer making fault*	*Reject batch*
4	*MORE THAN (contamination)*	*Poor taste*	*Process fault*	*Reject batch*

Check weigh

FAILURE MODE AND EFFECTS ANALYSIS

- A failure modes and effects analysis (FMEA) assesses the consequence of failure of a single component in a system. Failure may be total or partial and may effect more than one physical property.
- Failure modes and effects analyses:
  - were developed for the *automotive* industry
  - assess effects of single component failures
  - may be used to assess product or process designs
  - are used as a check on the adequacy of safety systems
  - are normally qualitative but can be qualitative (FMECA)
  - may be done by a team or individual

FAILURE MODE AND EFFECTS ANALYSIS

- Components are taken in turn and the effects of failure considered in terms of safety and reliability. Quantitative results may be derived if real component failure rates are used. The output of the analysis is an action list specifying required design changes or further hazard analysis.

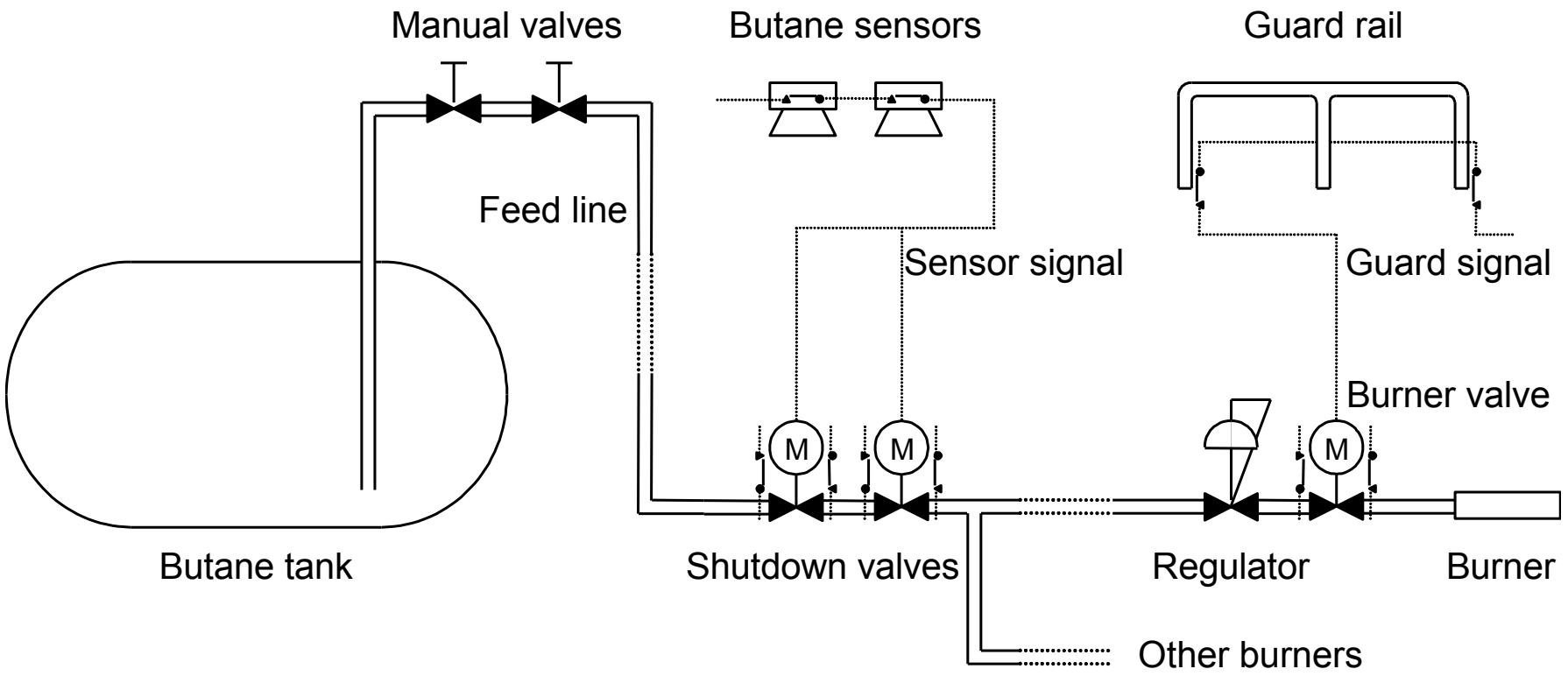
FAILURE MODE AND EFFECTS ANALYSIS

Consider the ***'filling valve'*** sub-system

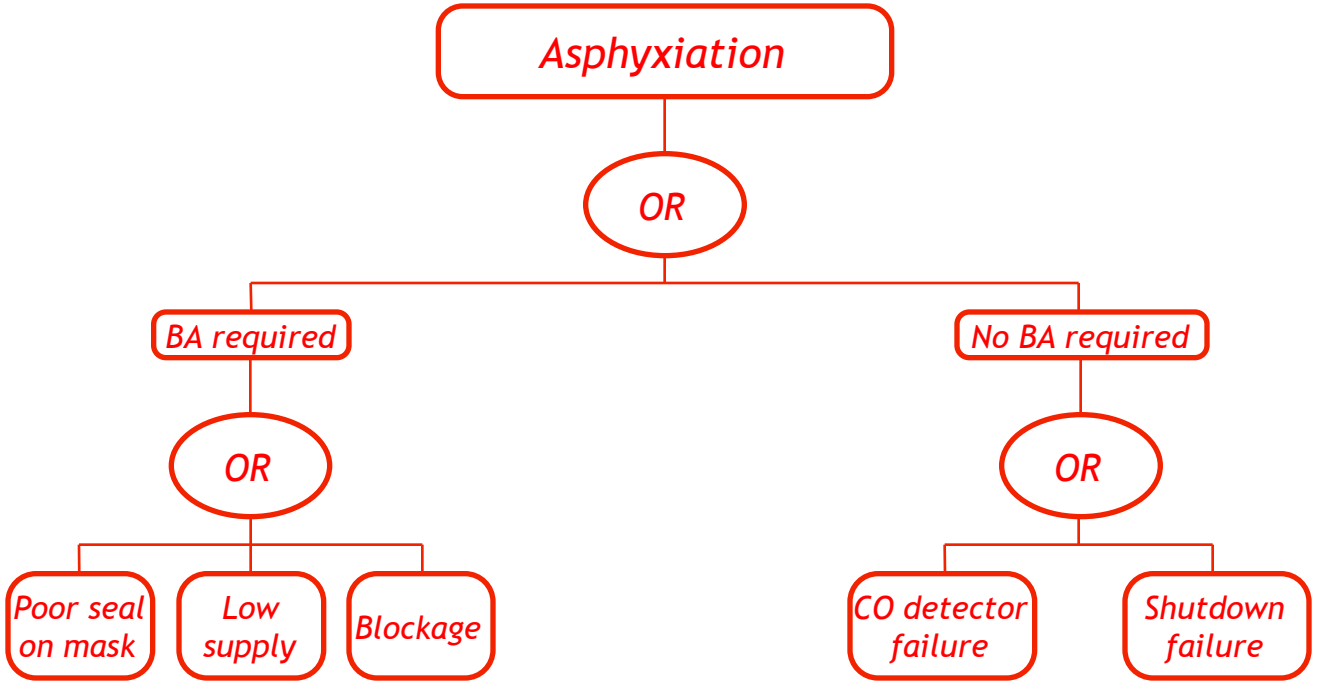
No.	Failure mode	Effect	Action
1	*VALVE FAILS OPEN*	*Beer everywhere*	*Shut down filler, monitor open*
2	*VALVE FAILS CLOSED*	*No beer in can*	*Reject can, monitor closing*
3	*VALVE TIMING ERROR*	*Incorrect volume*	*Reject can, monitor timing*
4	*VALVE SEAT WEAR*	*Contamination*	*Inspect valve regularly*

Check weigh

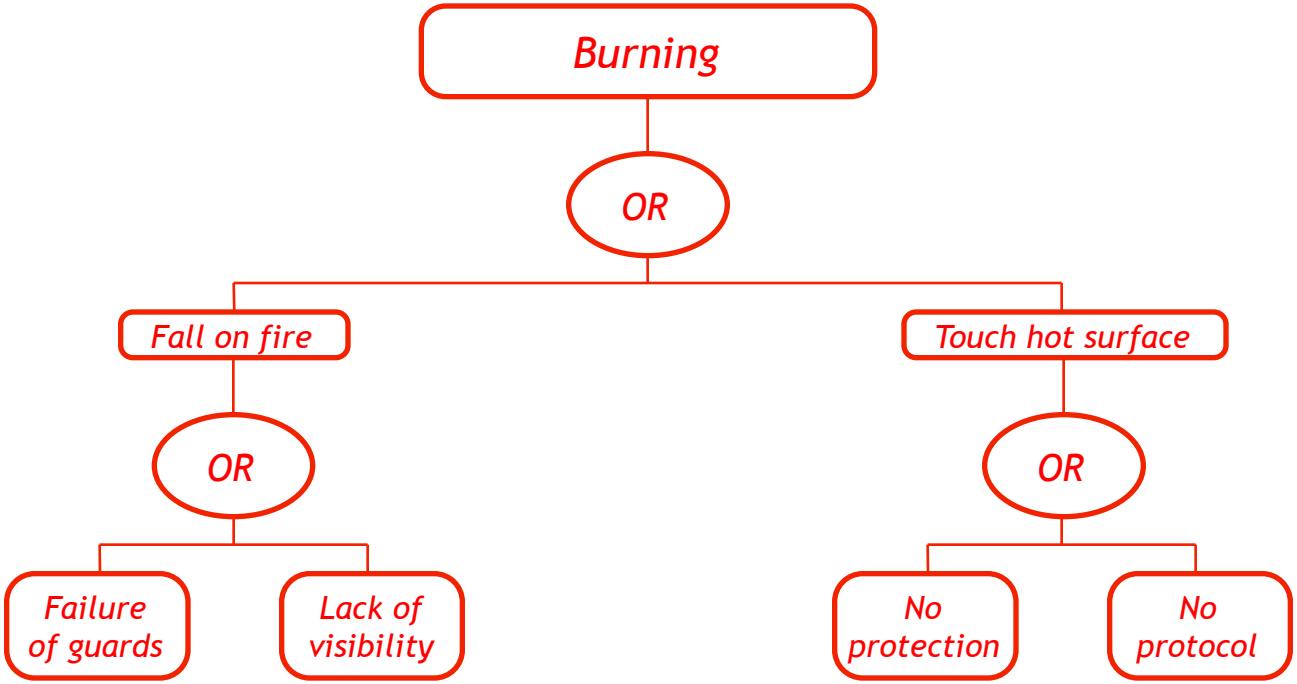
FIRE FIGHTING TRAINING UNIT



FAULT TREE


Asphyxiation
OR
BA required
No BA required
OR
OR
Poor seal on mask
Low supply
Blockage
CO detector failure
Shutdown failure

FAULT TREE


Burning
OR
Fall on fire
Touch hot surface
OR
OR
Failure of guards
Lack of visibility
No protection
No protocol