MODULE 2 :

Risks Diagnostic and Analysis

2025

Source: *https://www.thegrcinstitute.org*

ISIC-GSCP
Group of
Chemical and
Physical Safety

Introduction: Is reality far away ?

Time 2`42``

Source: https://www.imdb.com , BP Spills Coffee: a PARODY by UCB Comedy

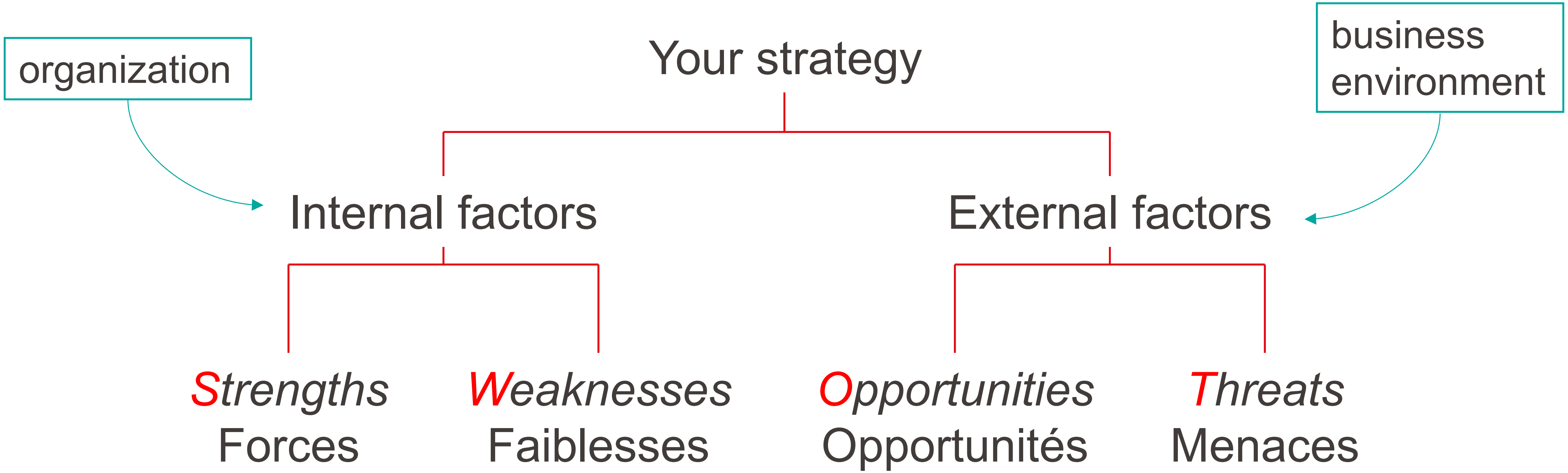
Source: https://www.123rf.com

Module 2.1

Strategic analysis - SWOT

SWOT: What is it ?

- A SWOT analysis systematically identifies internal strengths and weaknesses.
- A SWOT analysis can be conducted through structured processes or more informal brainstorming or self-assessment activities.
- Steps:
  - Review the organization's strategy.
  - Analyzing both internal and external factors impacting the organization.



organization

Your strategy

business environment

Internal factors

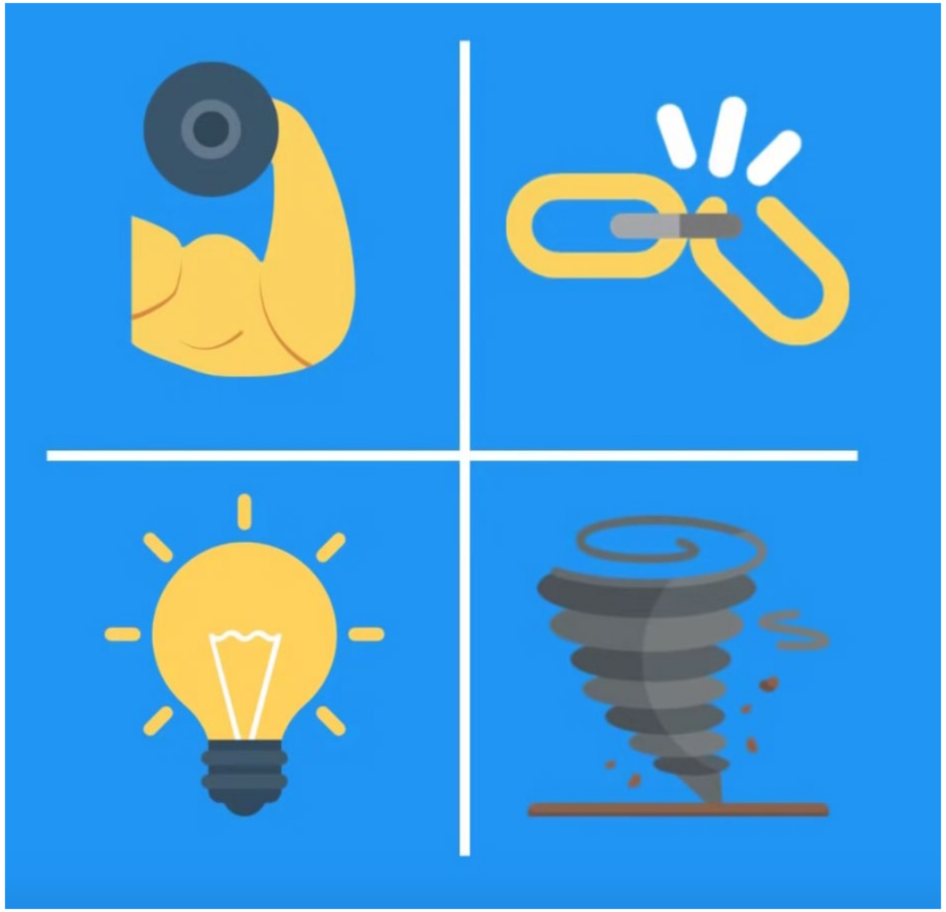
External factors

Strengths
Forces

Weaknesses
Faiblesses

Opportunities
Opportunités

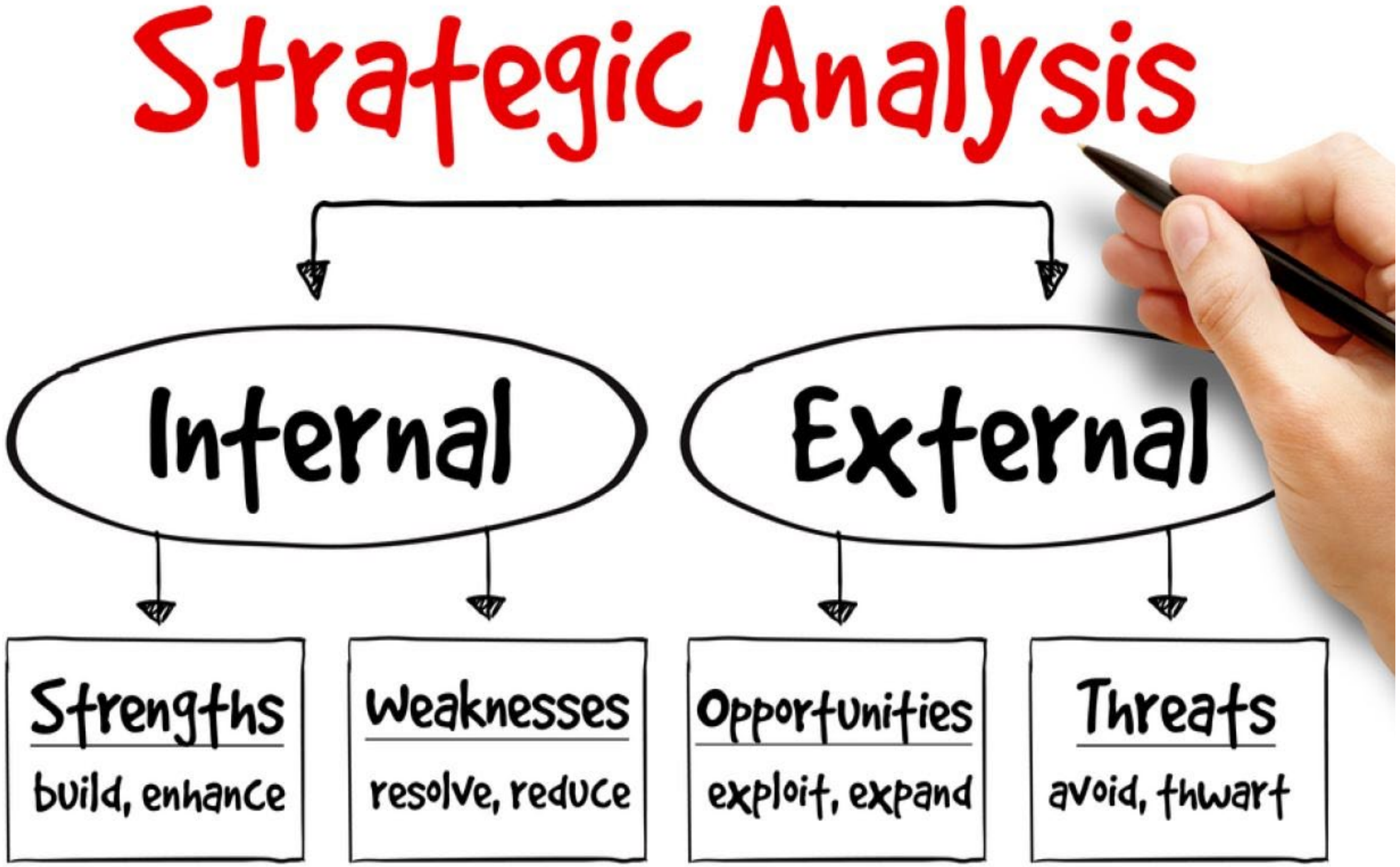
Threats
Menaces



When do you use SWOT ?

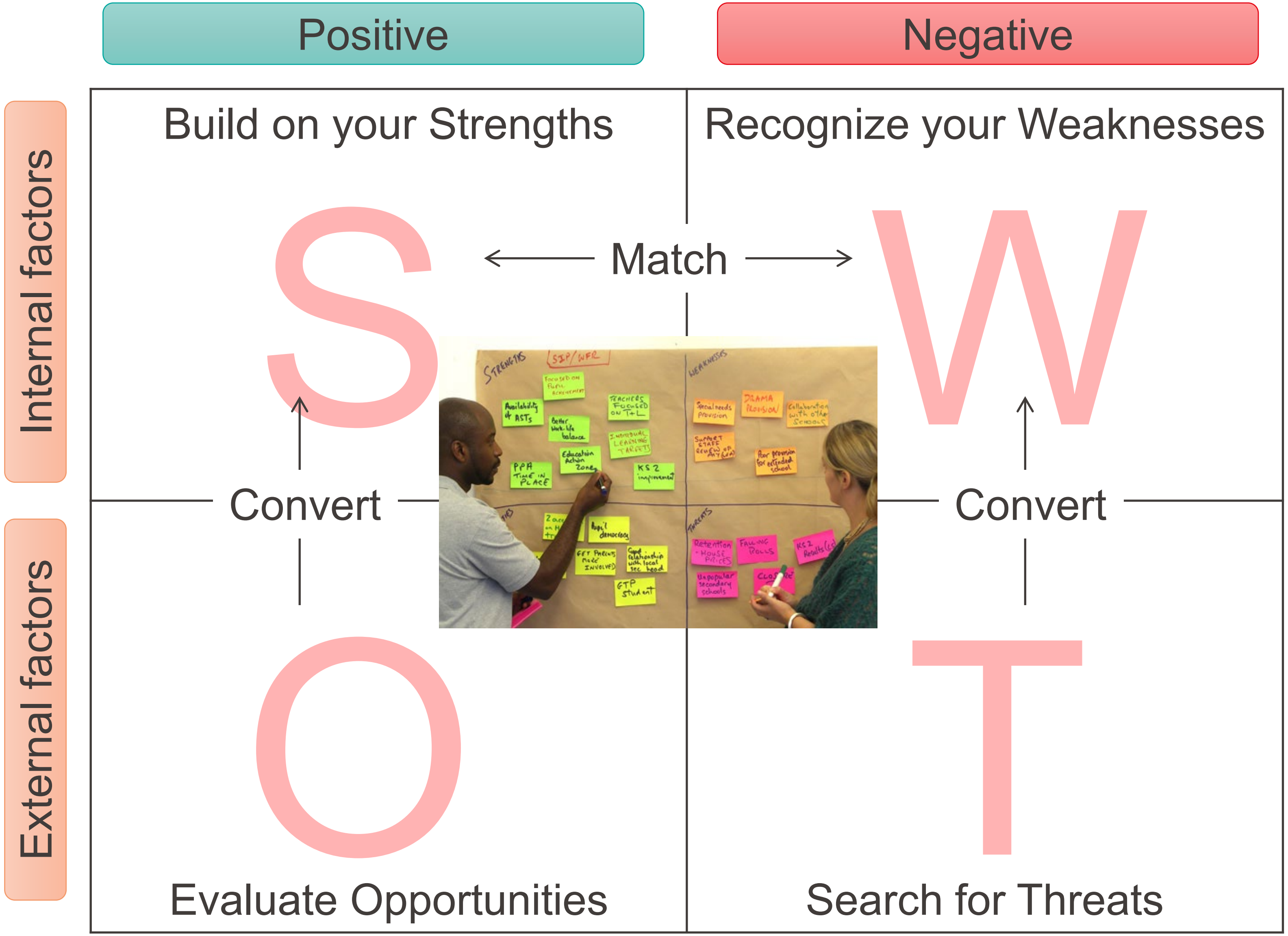
- Explore solutions to issues.
- Make decisions for your project.
- Identify areas where change is feasible.
- Adapt and improve plans during the course.

SWOT: What ?



- Establishes logical connections between activities and their effects.
- Maintains visual engagement (neither overly simplistic nor overly complicated).
- Sparks thought and prompts questions.
- Incorporates recognized influences to achieve desired results.

Source: http://oldror.lbp.world/UploadedData/12717.pdf



	Positive	Negative
Internal factors	Build on your Strengths S	Recognize your Weaknesses W
External factors	O Evaluate Opportunities	T Search for Threats

← Match →

Convert

Convert

SWOT: Some sample questions

	Positive	Negative
Internal factors	S • What are the organization's benefits? • Where does the organization excel? • What distinctive resources are available? • What are considered the organization's strengths by others? • What has been successful? • What are the innovative components?	W • What improvements are needed for the future? • What aspects can be enhanced? • What knowledge, contacts, and resources are lacking? • What skills are in shortage? • What requires modification? • What internal weaknesses are perceived by others?
External factors	O • What are the key success factors? • What additional services can be provided? • Which trends can be leveraged? • Is it possible to adapt current products for new markets? • What weaknesses do competitors have?	T • What obstacles are encountered in the external environment? • What hinders progress? • What could be the consequences of competitors' actions? • Are there potential regulatory concerns? • Is there a risk of losing key personnel? • Are there political and social implications to consider?

SWOT: Exercise

	Positive	Negative
Internal factors	S • What do you excel at? • Which unique skills or resources can you emphasize? • What strengths do others perceive in you?	W • Where can you make improvements? • In what areas do you possess fewer resources or skills compared to others? • What are potential weaknesses perceived by others?
External factors	O • What opportunities are within your reach? • Which trends can you capitalize on? • How can you convert your strengths into opportunities?	T • What are the threats that could pose a risk to you? • What are your competitors or colleagues doing? • Which threats do your weaknesses make you susceptible to?

Consider yourself as a student !

SWOT: Brainstorming & Prioritization in SWOT Analysis

The outputs of the brainstorming exercise are prioritized.

Brainstorming → **Prioritization**

Begin the brainstorming with the following questions:

- What opportunities exist in our external environment?
- What are the threats to the institution in our external environment?
- What are the strengths of our institution?
- What are the weaknesses of our institution?

At the end of the brainstorming exercise:

- Narrow down the list of strengths and weaknesses < 5
  - Strengths that are distinctive skills
  - Weaknesses that are disabling
- Reduce the threats and opportunities to the top five of each.

Source: *https://www.techeblog.com/*

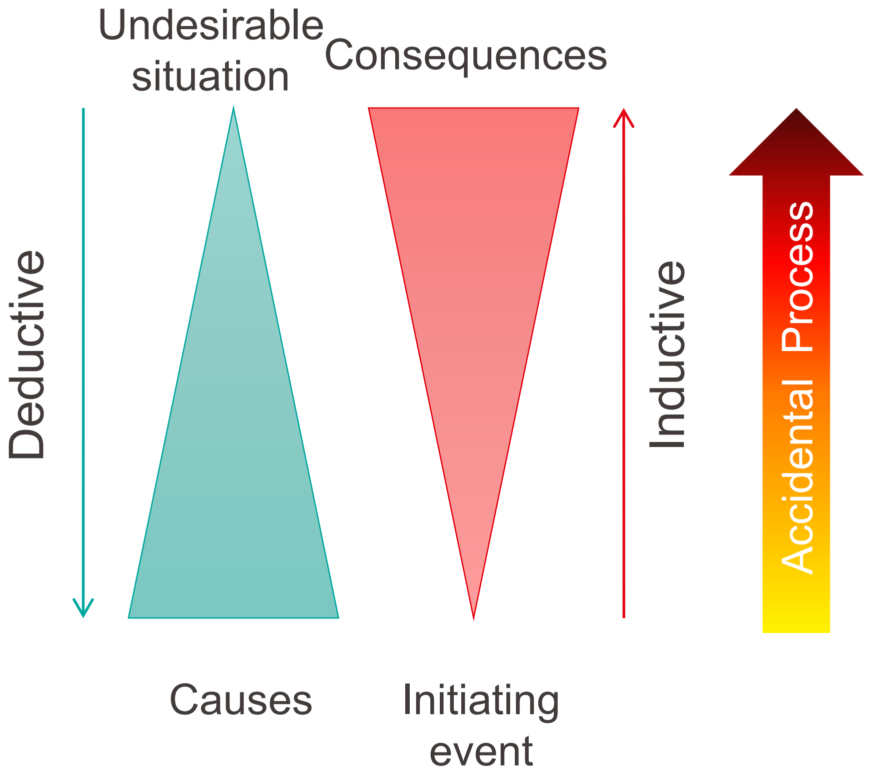
Module 2.2

Risk analysis families

Risk analysis: Inductive - Deductive

Two primary risk analysis approaches exist: inductive (bottom-up) and deductive (top-down).

- Deductive methodologies analyze the causes of an adverse event (accident) by addressing the question “how did this event occur?” (search for the causes).
- Inductive methodologies analyze the consequences of a failure (initiating event) and respond to the question "what undesirable events can arisew from the failure?” (search for consequences).



Risk analysis: Types of methods

The analysis techniques can be divided as follows:

- Basic methods
  - These are typically used in the early stages to comprehend process flow. They are primarily inductive.
  - Functional analysis, PHA, FMEA, HAZOP, …
- Static methods
  - These methods provide a structural perspective of the process.
  - They employ a Boolean algorithm and don't consider temporality.
  - FTA, ETA, Reliability bloc diagram, …
- Dynamic methods
  - These approaches incorporate temporal and behavioral aspects.
  - Petri networks, Markov chains, Monte-Carlo, Bayesian belief networks, …

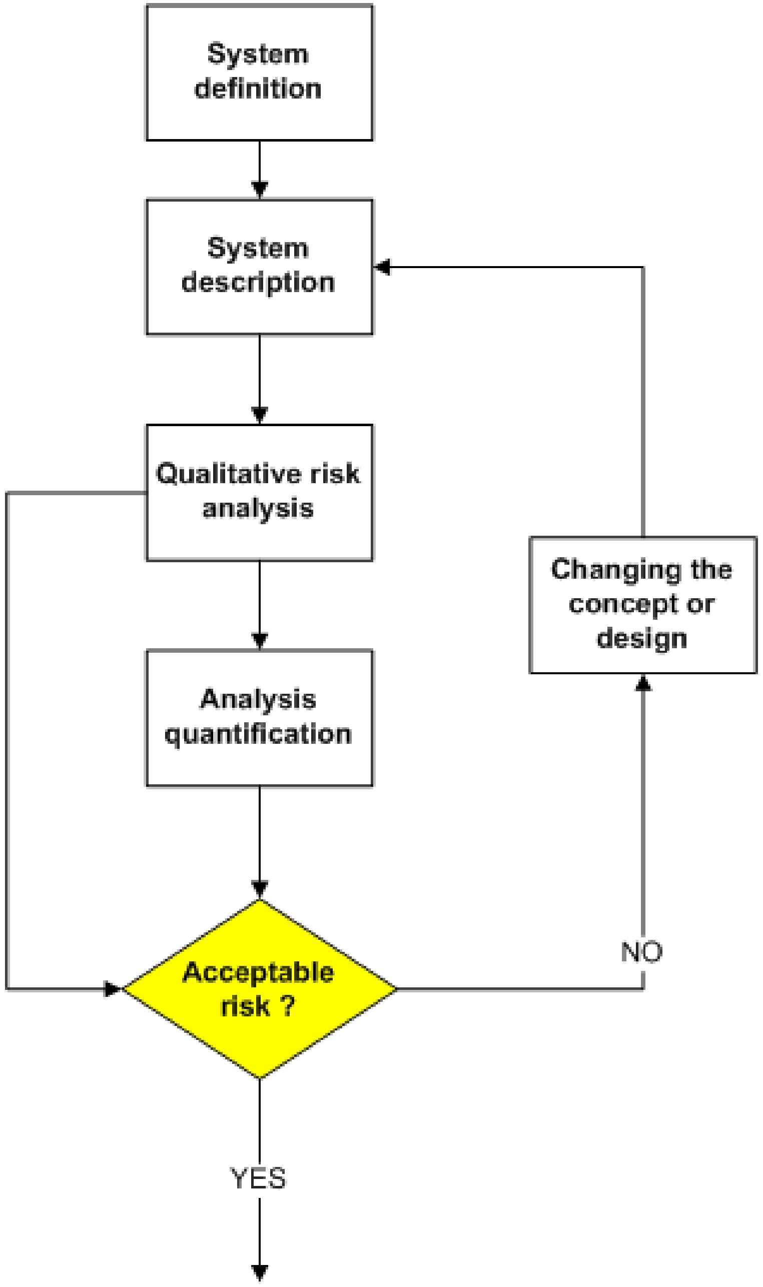
Risk analysis: Methods suited to engineering projects

Project phase	Objectives	When	Required documentation	Analysis method
Conception	• Selection Process • Identification of unacceptable risks • Input into the design process • Identification of changes that reduce risk	Design Evaluation	• Basic documentation	1.PHA 2.Functional analysis 3.What-if 4.Brainstorming 5.Check-list 6.FMECA Project
Preliminary	• Identify hazards associated with the process	Process design Flowcharts completed	• PFD • Control flowchart • P&ID • Process description	1.What-if 2.Check-list 3.FMECA 4.HAZOP 5.FTA
Before start-up	• Verify that the production system is safe before introducing chemicals.	Before operational tests	• Risk Analysis • HAZOP Report • Training • List of deficiencies	1.Plant inspection 2.Check-list

More information available in the book

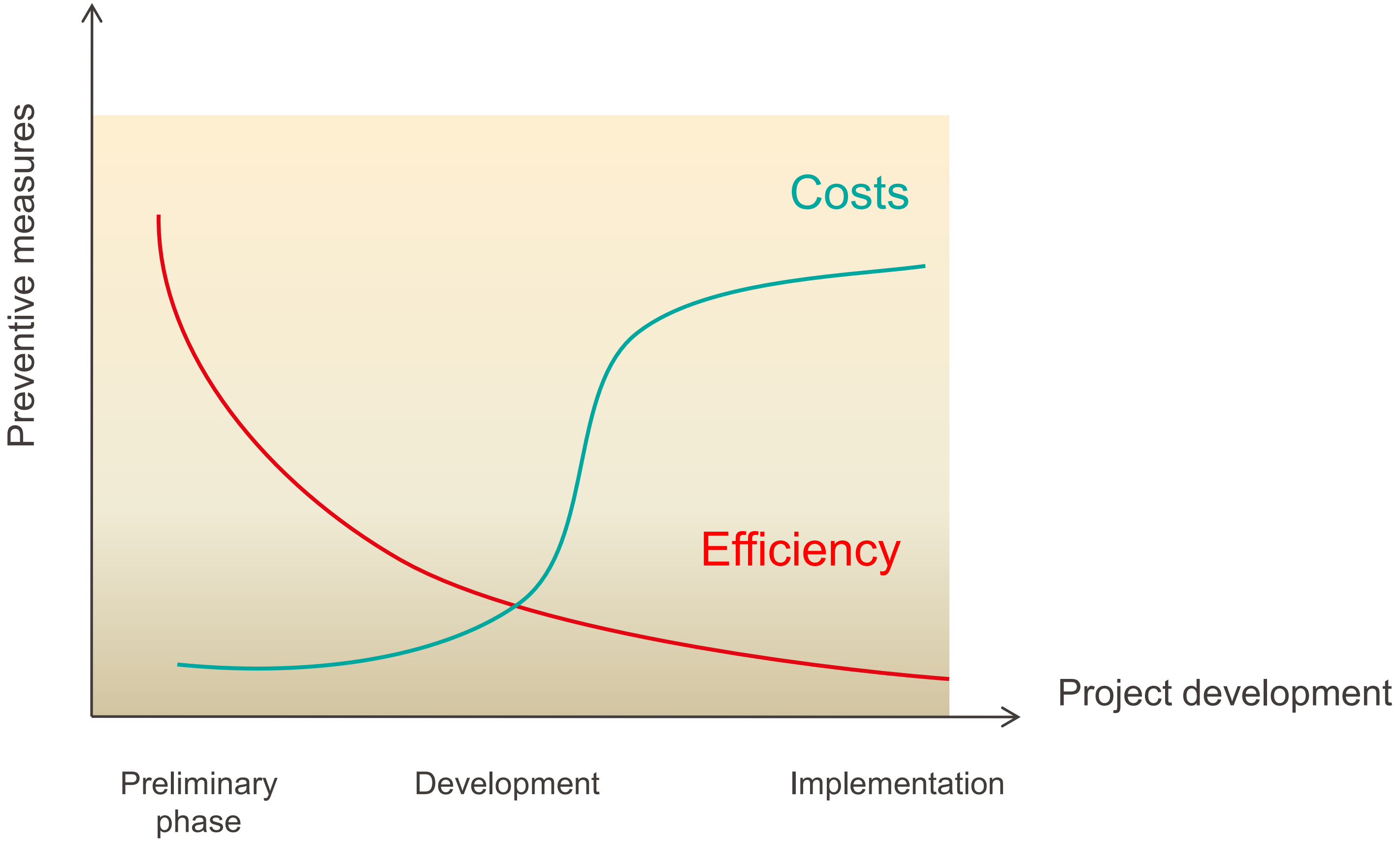
Risk analysis: Global process

- Iterative process → risk considered acceptable.
- In practice ≤ 2 iterations, except for systems with exceptionally critical safety and reliability requirements, like nuclear power plants and space shuttles.



Risk analysis: Cost analysis

For economic and efficiency considerations → integrate risk analysis during the project's design phase.



Risk analysis: Who needs them ?

Time 1`22``

Source: https://www.zurich.com/en/knowledge/topics/natural-hazards/

Module 2.3

PHA

PHA: Introduction

- Preliminary Hazard Analysis (PHA) is a relatively straightforward method used to identify major hazards within a system.
- PHA is applied in two ways:
    - Independent Use: As a stand-alone risk analysis for systems characterized by simple or easily recognizable hazards, rather than complex accidental processes.
    - Combined with Other Methods: In this scenario, PHA serves as a preliminary risk assessment to prepare for complex or less well-defined cases. It is primarily employed during the early design phase of a project.
- The PHA methodology was established and disseminated by the developers of the “U.S. Air Force standard practice for system safety” in 1969.

PHA: Method

Steps:

- List known potential hazards
  - Literature
  - Previous projects
  - Reportable events
  - Complaints
- Severity estimate
- Likelihood of occurrence estimate
- Propose measures

- The primary purpose of PHA is to identify all sources of hazards within a system, which can include hazardous materials, equipment, and processes.

- Each element is linked to adverse events, potential causes, and compensatory measures.

- This initial phase of PHA involves identifying hazardous components, as:
  - Hazardous substances and preparations, including raw materials, finished products, and utilities.
  - Hazardous equipment like storage, reception areas, shipping, reactors, and energy sources such as boilers.
  - Hazardous procedures connected to the process.

PHA: Example

Example of a partial PHA for a storage tank of flammable gas under pressure

Element	Hazard	Hazardous event	Causes	Consequences	Risk		Measures
					S	O	
Tank	Heat stress (fire outside the tank)	Explosion of the tank and important release of gas	Presence of combustible elements near the tank	Fire Property damage Casualties	H	L	Change storage logistics Remove individual hazards
Tank	Mechanical impact against the tank shell	Gas release	Accident with another vehicle crossing, intentional damage	Fire Property damage Casualties	H	M	Inspection program
Tank	Weakening of the tank shell	Gas release Explosion of the tank and important release of gas	Corrosion, fatigue, inadequate tank size (cannot withstand filling pressure)	Fire Property damage Casualties	H	M	Inspection program Design verification Continuous monitoring of air quality
Valve	Unexpected opening	Gas release	Valve or control system failed, error during routine maintenance, ...	Gas release	M	H	Inspection program Continuous monitoring of air quality

Thierry Meyer

Course 2025 RM / Module 2 : Risk diagnostic and analysis

PHA: Conclusion

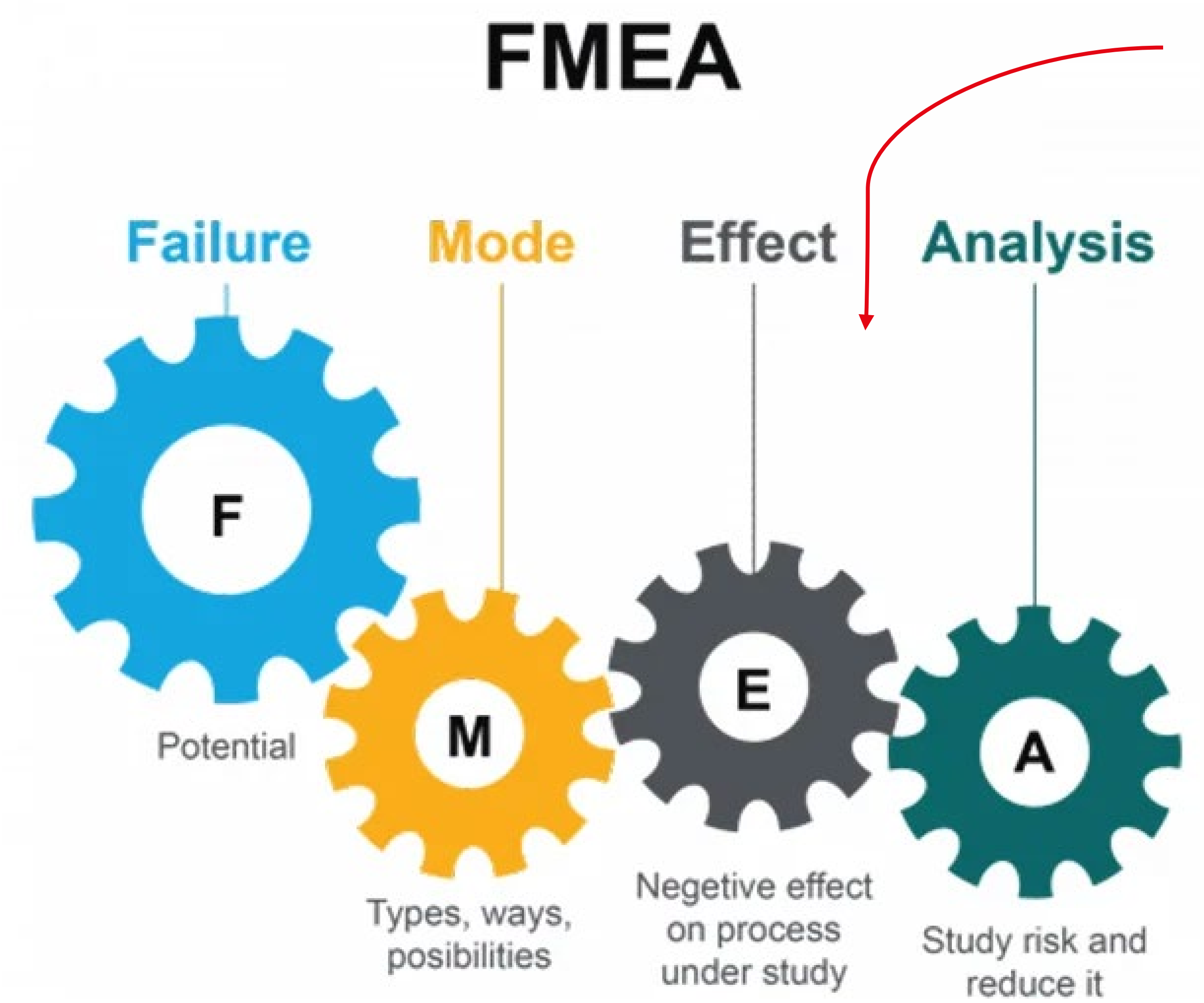
- PHA is a quick and cost-effective method for examining facility-related hazards.
- It's particularly useful during the design phase and doesn't require a detailed system description.
- However, it's limited in assessing failure propagation and multiple failure consequences.
- PHA benefits include:
  - Identifying potential hazards and accidents.
  - Prioritizing them by severity.
  - Identifying hazard controls and necessary actions.

Module 2.4

FMECA

Source: https://sandalwood.com/project/

FMECA/FMEA: Definition



FMECA

Failure Mode, Effects and Criticality Analysis

FMECA: History

- The U.S. Army has developed the FMECA. Ref. MIL-P-1629, entitled "Procedures for Failure Mode Analysis, Criticality Effects" published November 9, 1949 (now standardized IEC 60812:2018).
  - The standard (International Electrotechnical Commission) IEC 60812:2018 details the planning, execution, documentation, and maintenance of FMECA.

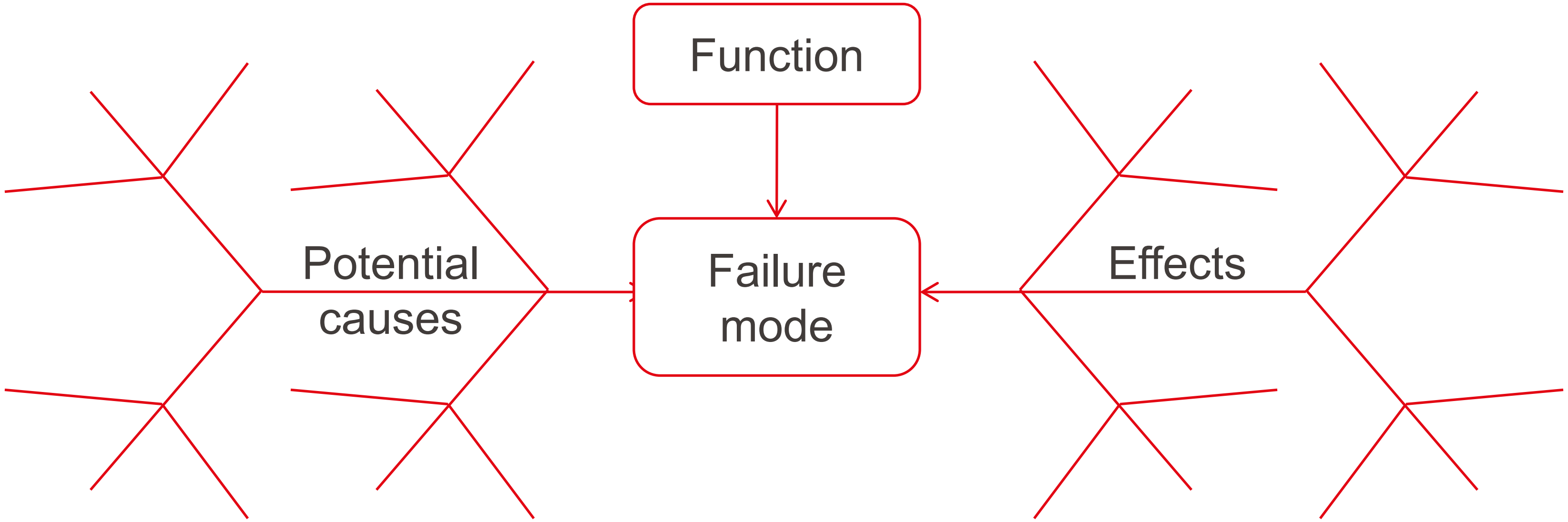
- FMECA serves as a technique for assessing failures to determine equipment or system reliability, with failures categorized based on their impact on personnel and mission success for equipment safety.

- This method was extensively applied in aerospace development during the 1960s.

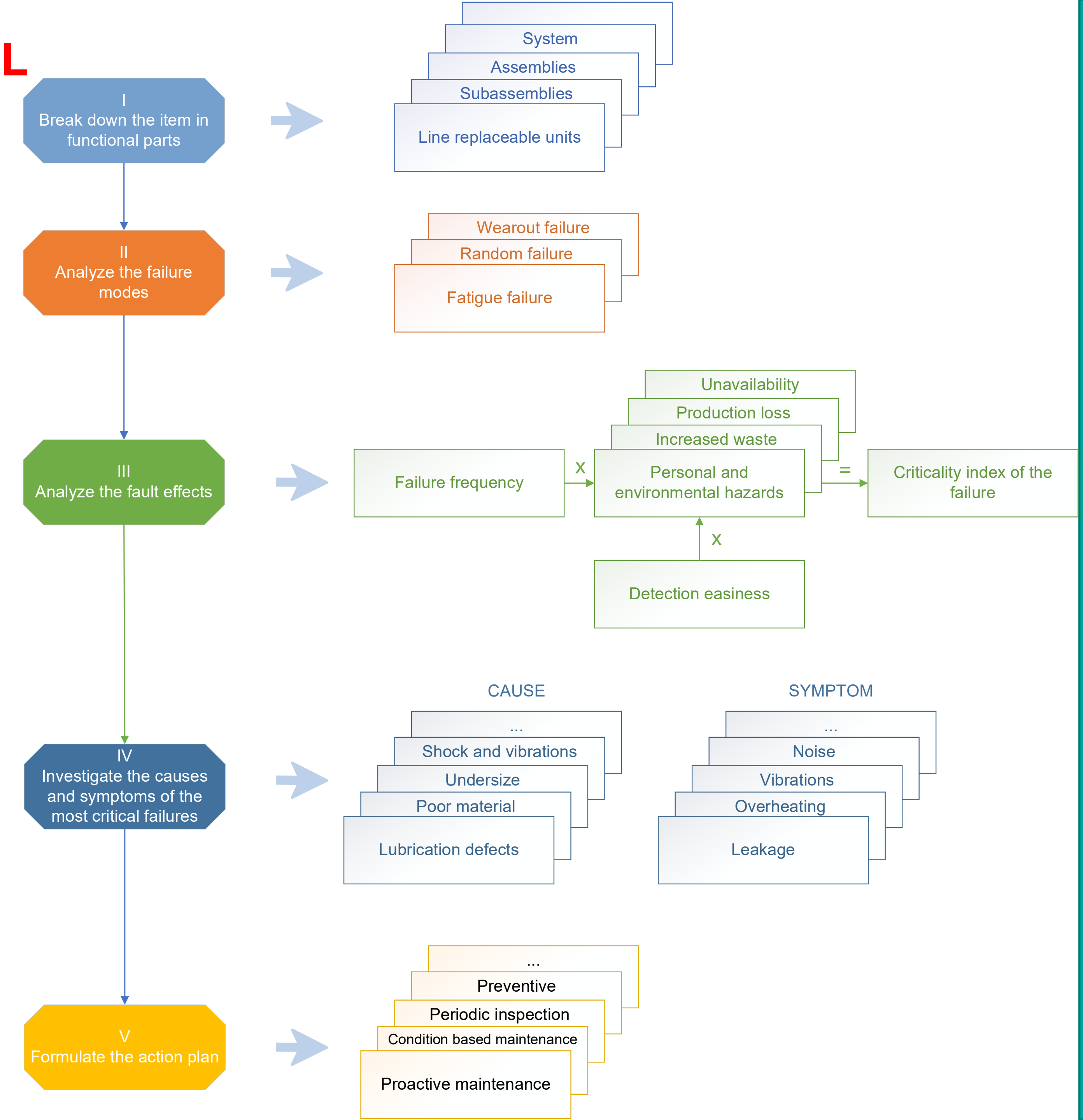
- Ford reintroduced it in the 1970s following major industrial accidents.

FMECA: Causes - Effects

- Failures occur as a result of a cause leading to an effect.
- A single cause can trigger multiple effects, while a combination of causes can result in a single or multiple effects. Causes can also have their own underlying causes, and effects can lead to subsequent effects.



FMECA: Process

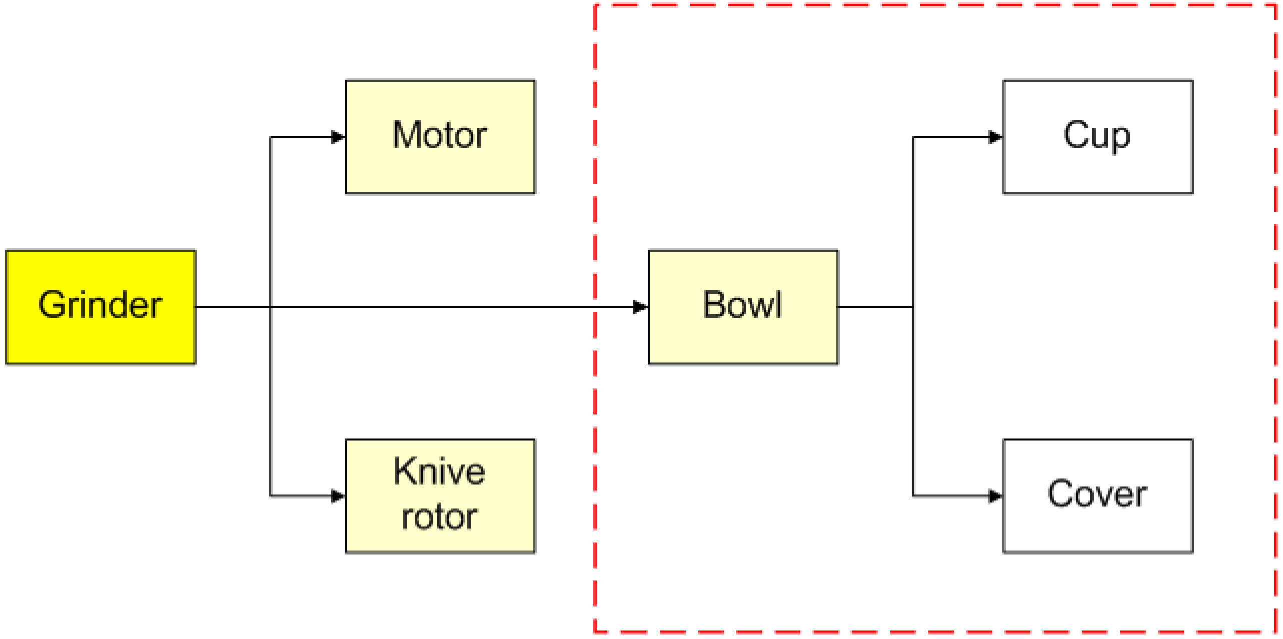


- 5 steps
- Input:
  - Construction and operating drawings
  - Potential failures
  - Types of failure mode
  - Frequency of failures
- Output:
  - Failure mode
  - Consequences
  - System reliability
  - Hazards and risks
  - List of criticalities

FMECA: Functional analysis - example

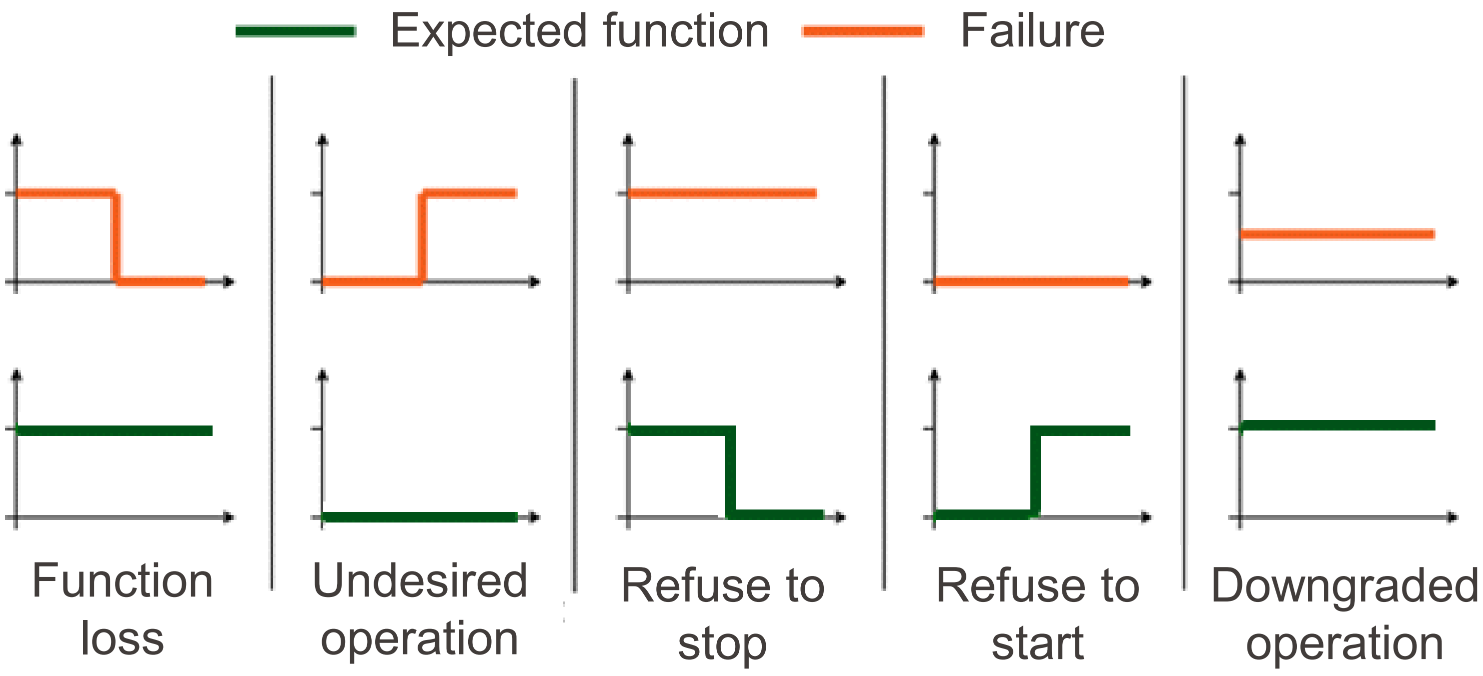
- The aim is to understand how the product or process functions by breaking it down into subsystems and organizing them hierarchically.

Example of a grinder



FMECA: Potential failure mode

There are 5 generic failure modes :



Expected function
Failure

Function loss

Undesired operation

Refuse to stop

Refuse to start

Downgraded operation

FMECA: Determination of the failure mode

FMECA is mainly based on 5 questions:

Possible effects

What could be the effects?

Potential failure mode

What could go wrong ?

Possible causes

What could be the causes?

Occurrence

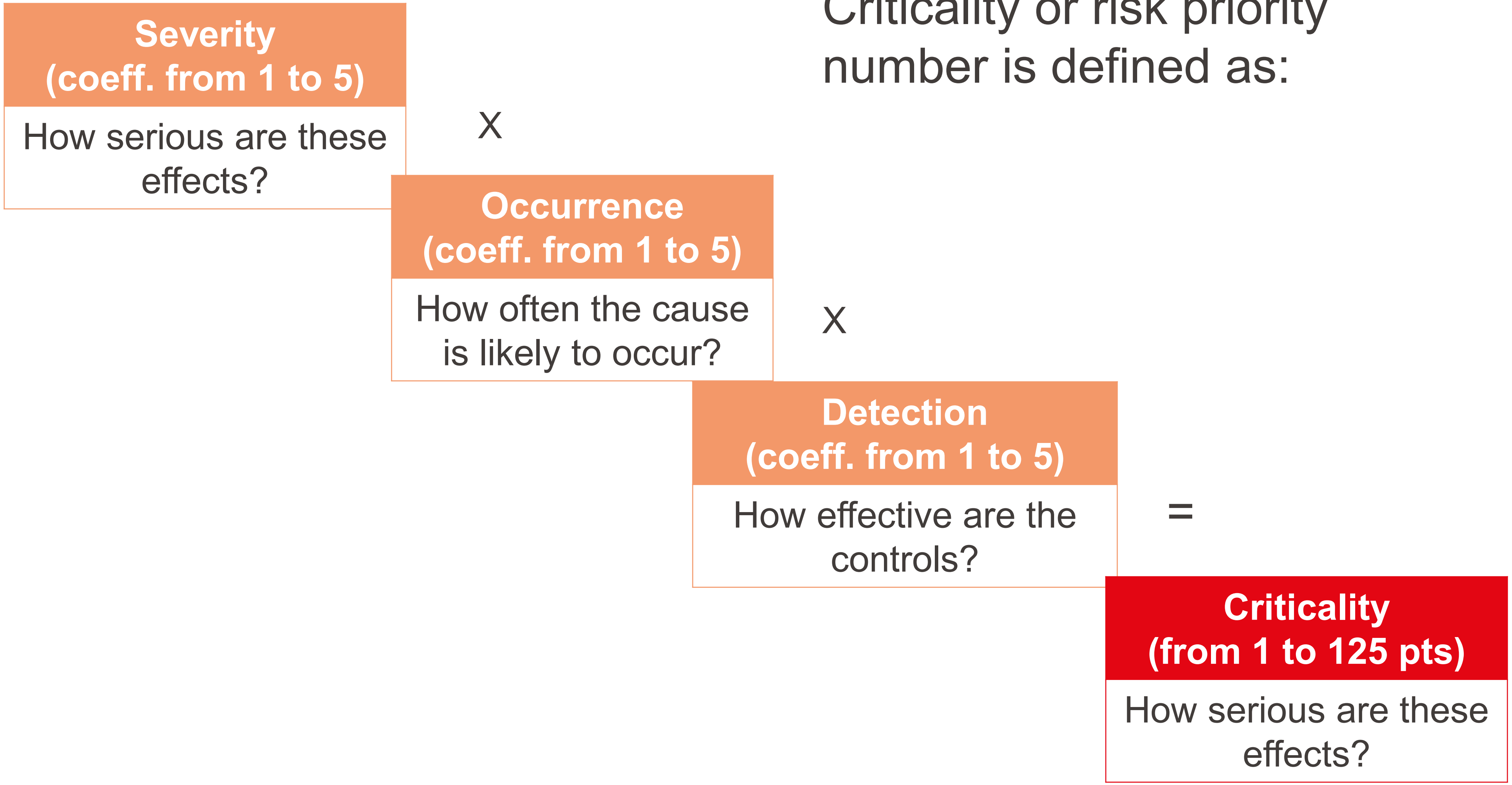
How often does the failure occur?

Detection

What are the control actions?
How to detect it if it happens?

FMECA: Criticality index

Criticality or risk priority number is defined as:



Severity (coeff. from 1 to 5)

How serious are these effects?

X

Occurrence (coeff. from 1 to 5)

How often the cause is likely to occur?

X

Detection (coeff. from 1 to 5)

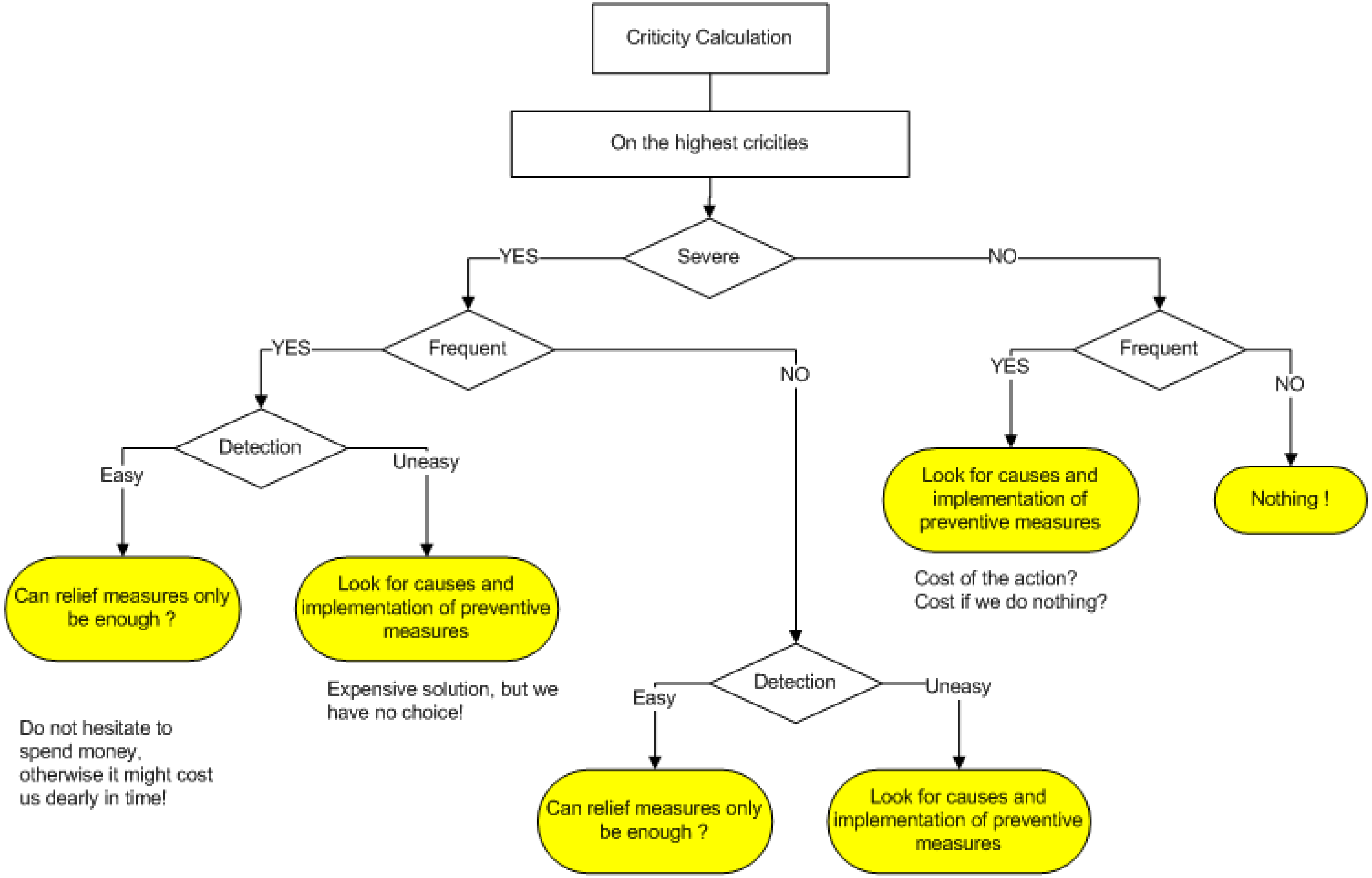
How effective are the controls?

=

Criticality (from 1 to 125 pts)

How serious are these effects?

FMECA: Criticality diagram


Criticity Calculation
On the highest cricities
Severe
YES
NO
Frequent
YES
NO
Frequent
YES
NO
Detection
Easy
Uneasy
Can relief measures only be enough ?
Look for causes and implementation of preventive measures
Detection
Easy
Uneasy
Can relief measures only be enough ?
Look for causes and implementation of preventive measures
Look for causes and implementation of preventive measures
Nothing !

Cost of the action?
Cost if we do nothing?

Expensive solution, but we have no choice!

Do not hesitate to spend money, otherwise it might cost us dearly in time!

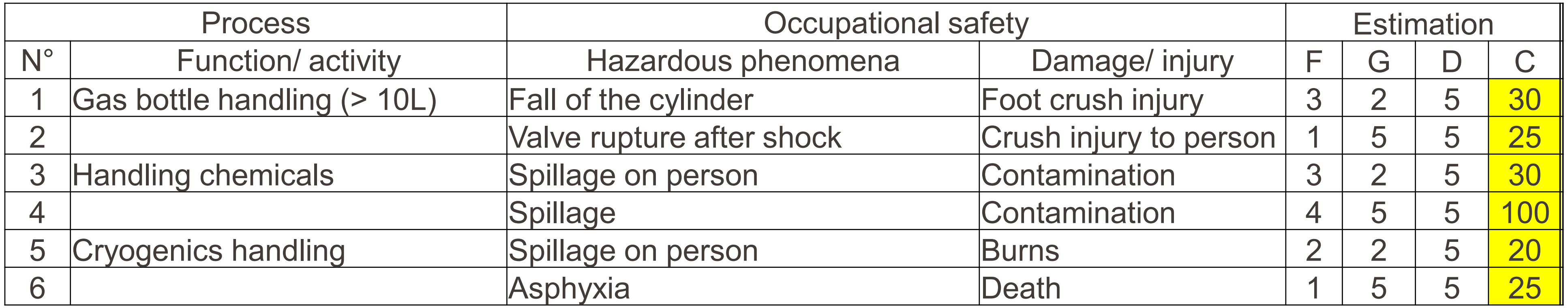
Expensive solution, but do we have the choice?

FMECA: Corrective measures

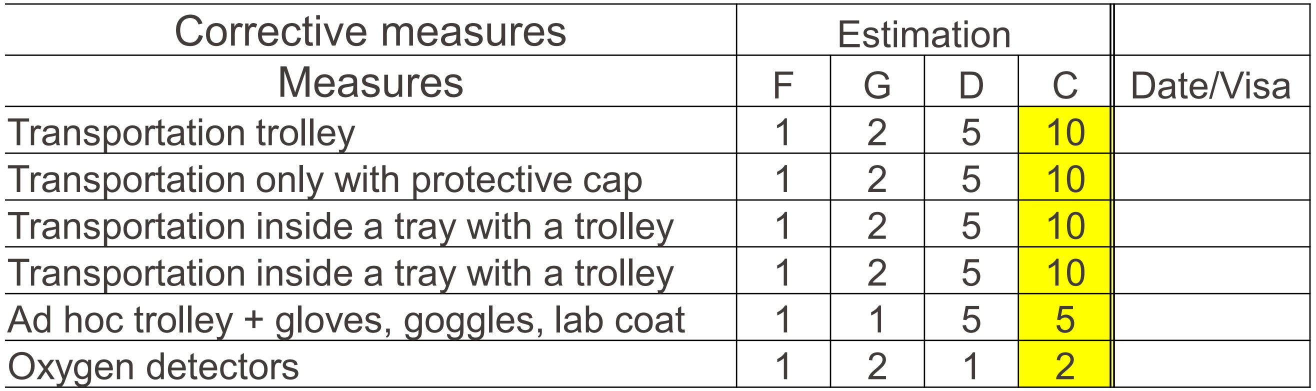
Each corrective measure is described with a list of defects, impacts, and mitigation strategies.

Process		Occupational safety		Estimation				Corrective measures	Estimation				
N°	Function / activity	Hazards	Damage/ injury	F	G	D	C	Measures	F	G	D	C	Date/ visa
							🟨					🟨	
							🟨					🟨	
							🟨					🟨	
							🟨					🟨	

FMECA: Example at EPFL



Process		Occupational safety		Estimation			
N°	Function/ activity	Hazardous phenomena	Damage/ injury	F	G	D	C
1	Gas bottle handling (> 10L)	Fall of the cylinder	Foot crush injury	3	2	5	30
2		Valve rupture after shock	Crush injury to person	1	5	5	25
3	Handling chemicals	Spillage on person	Contamination	3	2	5	30
4		Spillage	Contamination	4	5	5	100
5	Cryogenics handling	Spillage on person	Burns	2	2	5	20
6		Asphyxia	Death	1	5	5	25



Corrective measures	Estimation				
Measures	F	G	D	C	Date/Visa
Transportation trolley	1	2	5	10	
Transportation only with protective cap	1	2	5	10	
Transportation inside a tray with a trolley	1	2	5	10	
Transportation inside a tray with a trolley	1	2	5	10	
Ad hoc trolley + gloves, goggles, lab coat	1	1	5	5	
Oxygen detectors	1	2	1	2	

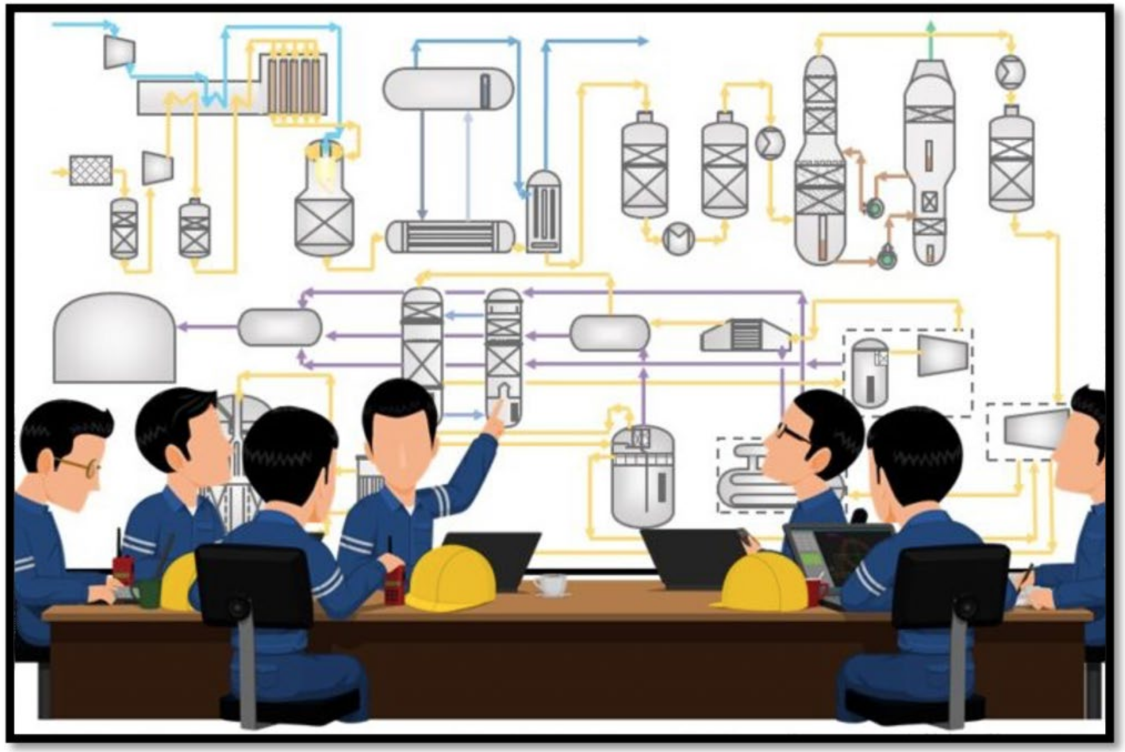
FMECA: Exercise

Perform an FMECA analysis of a deep fryer for the process

“From potato to French fries”

FMECA: Conclusions

- FMECA is a simple, systematic methodology.
- Applicable to various facilities.
- Evaluates potential component failure modes.
- May not identify consequences of multiple failures.
- Highlights areas for further study.
- There are several FMECAs:
  - Design FMECA (identify risks at the design stage)
  - Process FMECA (Identify the risks of the production process)
  - Product FMECA (Identify risks induced by the concept)
  - Production FMECA (Identify risks related to production facilities)
  - Service FMECA, Procedure FMECA



Source: https://processsafetylms.com/

Module 2.5

HAZOP

HAZOP: Introduction

- HAZOP = HAZard and OPerability analysis

- Developed in the early 1970s by ICI (Imperial Chemical Industries) in the UK, to assess safety in chemical plants. (Now standard IEC 61882:2016).

- Follows a similar procedure to that developed for FMECA.

- HAZOP considers the potential deviation in key operational parameters related to plant operations, with a distinct focus on the plant setup.

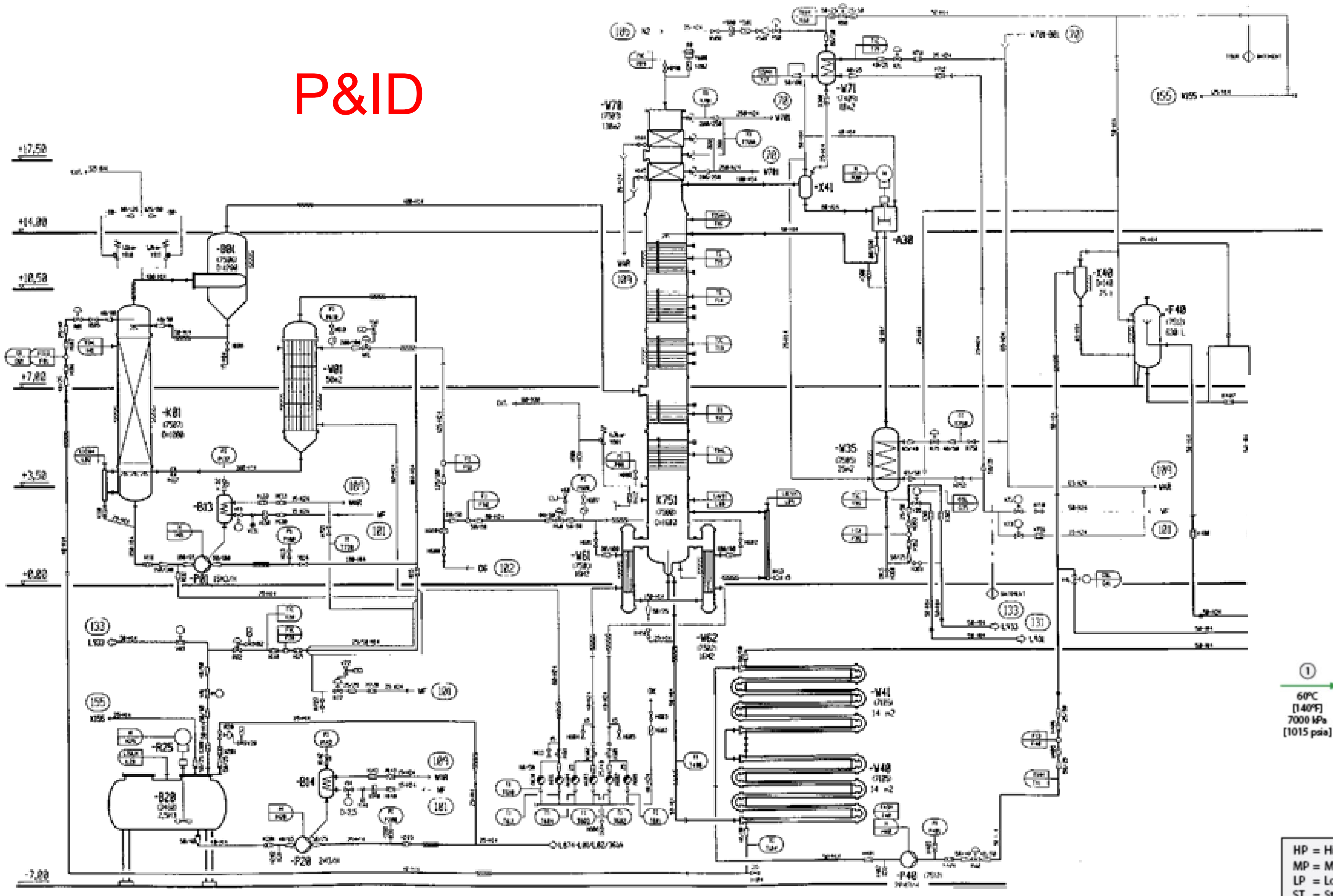
- In contrast, FMECA concentrates on the components.

HAZOP: Information

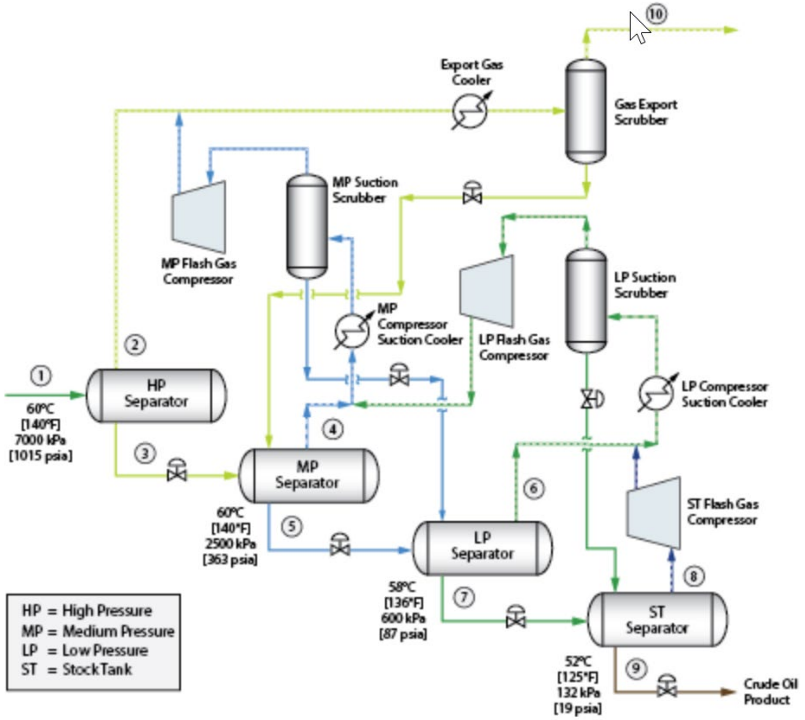
- HAZOP is an inductive process that systematically assesses plant parameter deviations to anticipate their potential outcomes.
- It is especially valuable for evaluating thermo-hydraulic systems, where parameters like speed, temperature, pressure, level, and concentration significantly impact safety.
- Implementing HAZOP necessitates fluid flow diagrams, as well as drawings such as P&ID (Piping and Instrumentation Diagram) and PFD (Process Flow Diagram).

HAZOP: P&ID/PFD

P&ID



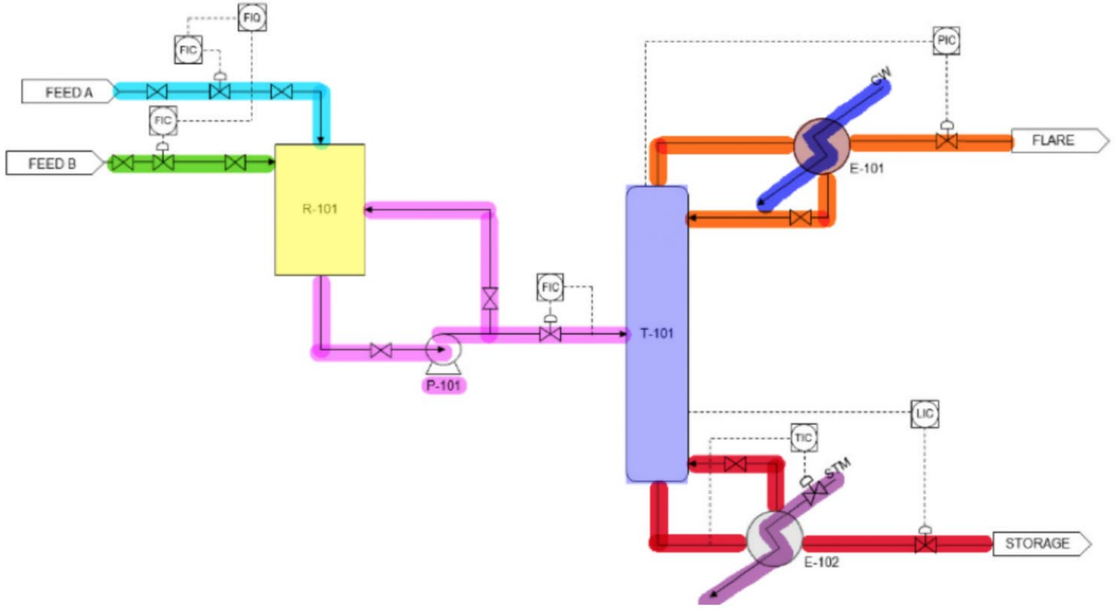
PFD



Courtesy :Ciba-Geigy Inc.

HAZOP: Splitting the setup into nodes

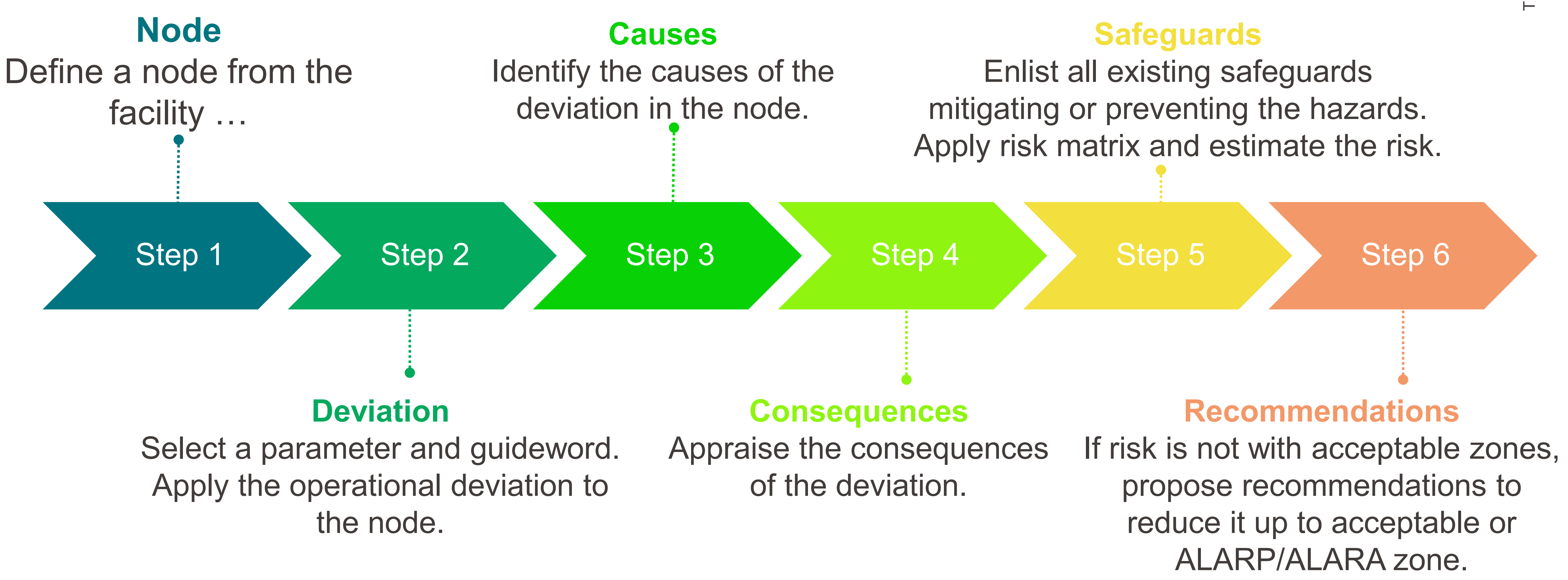
- A node is a section where one or more process conditions undergo a significant change.
- For instance, a pump can serve as a node due to the increase in fluid pressure it induces.
- A furnace is another node since it involves a transformation in the chemical and physical composition of materials.
- Likewise, a heat exchanger constitutes a node as it results in a temperature change in the fluid.
- A node can also include material transfer between vessels via a valve, focusing on flow changes in the pipeline.



Nodes are marked with different colors on the P&IDs for easy identification.

Source: https://www.bearprocesssafety.com

HAZOP: The methodology



Step 1

Node
Define a node from the facility …

Step 2

Deviation
Select a parameter and guideword. Apply the operational deviation to the node.

Step 3

Causes
Identify the causes of the deviation in the node.

Step 4

Consequences
Appraise the consequences of the deviation.

Step 5

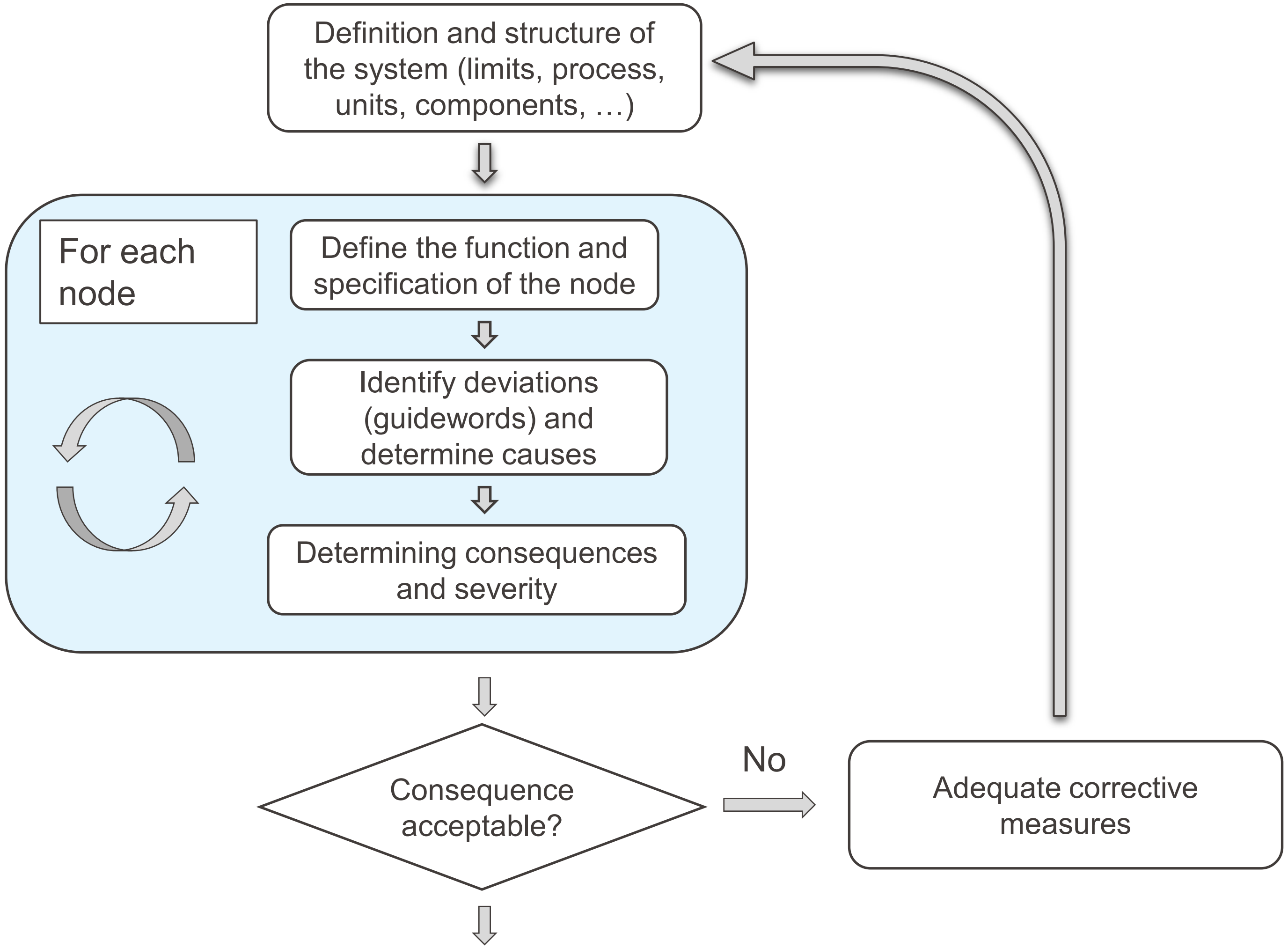
Safeguards
Enlist all existing safeguards mitigating or preventing the hazards. Apply risk matrix and estimate the risk.

Step 6

Recommendations
If risk is not with acceptable zones, propose recommendations to reduce it up to acceptable or ALARP/ALARA zone.

HAZOP necessitates a skilled team of experts, each with specific competencies, guided by a moderator (the HAZOP facilitator) overseeing the process.

HAZOP: Process


Definition and structure of the system (limits, process, units, components, …)
For each node
Define the function and specification of the node
Identify deviations (guidewords) and determine causes
Determining consequences and severity
Consequence acceptable?
No
Adequate corrective measures

- Input:
  - PID/PFD
  - Process
  - Team leader
  - Team members
  - Directives, methodology
- Output:
  - Hazards and risks
  - Deviations
  - Correctives measures/actions

HAZOP: guide/key-words

Keywords	Signification	Commentary	Examples
No or not (Non/Pas de)	No part of the function is fulfilled	The purpose or function is not fulfilled at all, not even partially.	No agitation No flow
More (Plus de)	Overrun, or increase, quantitatively	Refers to the quantities and properties (T, P), but also activities (heating, reaction).	Higher temperature Too much product
Less (Moins de)	Insufficient or quantitative reduction.		Lower flow rate than expected Less agitation
As well as (Aussi bien que)	Qualitative increase	The function (design and procedure) is performed with additional activity. Concomitant adverse effect.	Heating started at the same time as the addition of reagent A.
Part of (Partie de)	Qualitative modification/diminution	Only part of the function is realized.	Only part of the reagent is added
Reverse (Inverse)	The logical opposite of the function	Reversal of the activity or sequence	Liquid flows in the opposite direction It heats instead of cooling
Other than (Autre que)	Total substitution	Result different from that of function.	Reagent A is loaded in place of B
Earlier than (Plus tôt que)	On the time clock	The action takes place before or after a defined time.	We started heating 15 minutes before the deadline.
Later than (Plus tard que)	On the time clock		The reaction has been left taking place over the defined two hours.
Before (Avant que)	On the sequence or order	The action is taken before or after the defined sequence	A was loaded before B
Later (Après que)	On the sequence or order		The sample was cooled after stirring

HAZOP: Operating parameters

Measurable physical quantities		Operations		Actions	Functions-situations
Temperature	pH	Loading	Control	Start-up	Protection
Pressure	Intensity	Dilution	Separation	Sampling	Utility default
Level	Speed	Heating	Cooling	Stop	Freezing
Flow rate	Frequency	Stirring	Transfer	Isolate	Spill
Concentration	Amount	Mixing	Maintenance	Purge	Earthquake
Contamination	Time	Reaction	Corrosion	Close	Malevolence

HAZOP: Safety barriers or safeguards

Safety Barriers		Definition	Example
Technical	Passive safety devices	Individual components designed to execute a safety function independently, without an external power source or the involvement of any mechanical system	• Retention tank/tray. • Rupture disc.
	Active safety devices	Active components intended to deliver a safety function without relying on an external power source.	• Safety valve • Excess flow valve
	Safety instrumented systems	An integrated system comprising sensors, processing units, and terminal elements with the goal of performing a safety function or a sub-safety function.	• Measuring elements that control a valve or a power switch.
Organizational		Human activities or operations that lack technical safety barriers to halt an ongoing accident.	• Emergency plan. • Containment.
Systems with manual action		Interface between a technical barrier and a human activity responsible for a safety function.	• Press an emergency button. • Low flow alarm, followed by manual closure of a safety valve.

HAZOP: The evaluation table

Example of a HAZOP table used in the Swiss chemical industry

<table>
<tr><td colspan="11">Phase, function: (detailed description, notated)</td></tr>
<tr><td colspan="6"><i>Guide-words: examples</i>
M1: no or not
M2: less
M3: more
M4: As well as
M5: Part of
M6: Reverse
M7: Other than
M8: Lather than
M9: Earlier than
M10: Before
M11: Later</td><td colspan="5">Level of P et G: (F) low, (M)iddle, (H)igh
P1, G1 occurrence and severity before measures
P2, G2, after measures</td></tr>
<tr><td>Guide-word</td><td>Deviation</td><td>Possible cause</td><td>P1</td><td>Consequences</td><td>G1</td><td>Measures</td><td>P2</td><td>G2</td><td>Who</td><td>When</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

HAZOP: Example

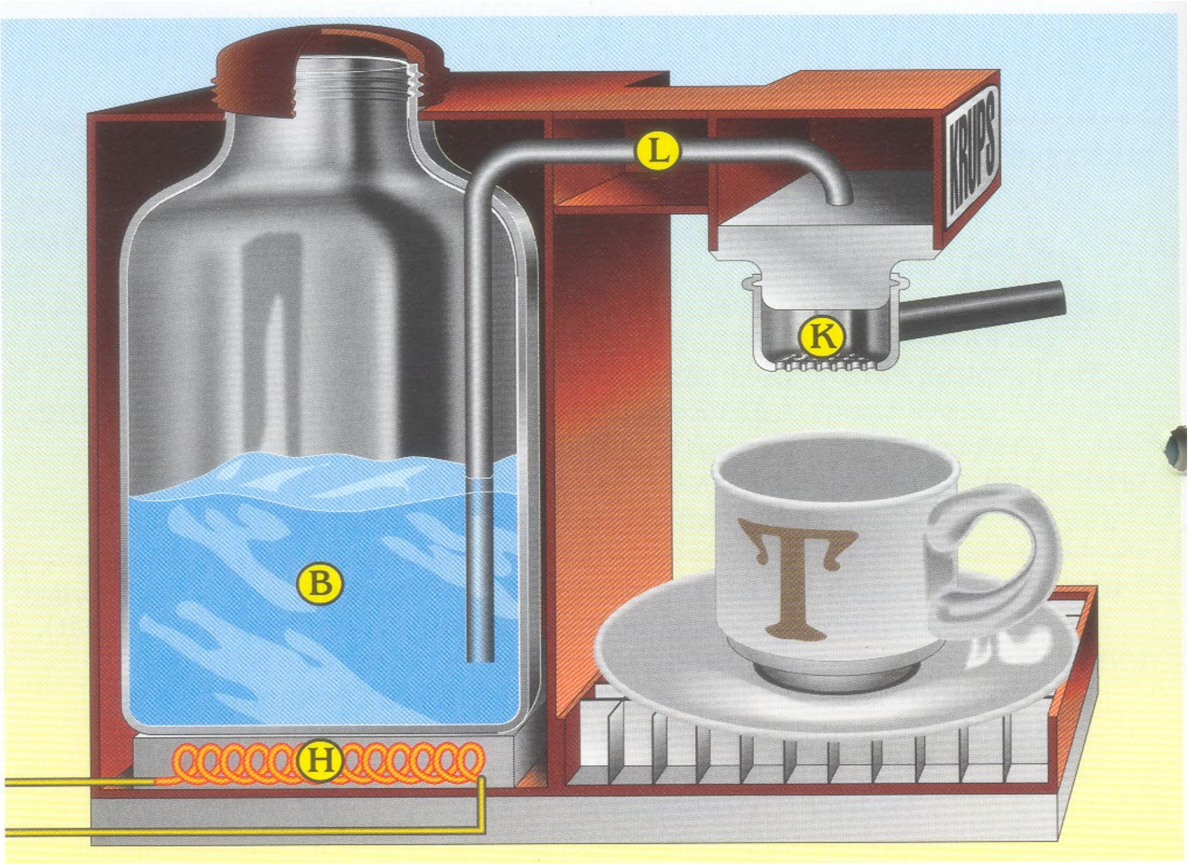
HAZOP analysis

N°	Object	Function	Parameter	Guide-word	Consequence	Cause	Hazard	Risk P/G	Recommendation	Comment
1	Line	Bring water to the system	Fluid	No	Loss of pump cooling	Line rupture	Damaged pump	2D	-	-
2				More	Increased pressure in the line	No pressure regulation	Line rupture	2C	Add a safety valve to the loop	-
3				Less	Not enough cooling capacity of the pump	Leakage at pipe and fittings	Damaged pump	2D	Periodic inspection of connections	
4	Electrical supply	Supply power to the motor M23	Electricity	No	Loss of pump power	Short-circuit, power failure	Loss of control	2D	Emergency power supply	

Occurrence: scale 1 to 5
Severity: scale A to E

HAZOP: Exercise (1)

- Perform a HAZOP analysis of a coffee machine to ensure the safety of its operation and prevent any potential hazards to users.



- Nodes
  - Water reservoir (B)
  - Heating supply (H)
  - Transfer line (l)
  - Filter (K)
  - Cup (T)

HAZOP: Exercise (2)

Function:

1. Upon adding water to the tank and coffee to the filter, the coffee machine is activated.
2. Water in the tank is heated to boiling, and the steam pressure forces it through the coffee powder in the filter into the cup.
3. Initially, hot water flows from the transfer line.
4. Pressure decreases and temperature rises during coffee extraction.
5. Steam is released from the machine at the end.

HAZOP: Exercise (3)

MOM'S PESTO
GET TOGETHER
A FOOD PROCESSOR...
...STUFFED WITH FRESH BASIL LEAVES
ROMANO & PARMESAN
OLIVE OIL
PINE NUTS
GARLIC
SALT
COMBINE
"A BIT" OF OLIVE OIL
GARLIC CLOVES
2 HANDFULS PINE NUTS
BIG HANDFUL CHEESES
"LOTS" OF SALT
ADD MORE OIL AS THE PROCESSOR PROCESSES
UNTIL IT BECOMES A THICK PASTE.
WRRRRR
ENJOY ON TOAST, VEGGIES, OR...
...PASTA!

Source: https://www.news.at/a/leckerbissen-comic-kochbuch-lucy-knisley

Operating mode:

1. Add 100 ml of water to the reservoir and seal it securely.
2. Place 10 g of ground coffee into the filter and attach it securely to the machine's outlet.
3. Begin heating the water by activating the electric heater.
4. Position a cup under the coffee outlet.

HAZOP: Conclusions

- HAZOP as FMECA is systematic and structured.
- It is easy to learn but resource-intensive (20-25 man-days).
- Based on the assumption that risk events result from deviations.
- Complex in analyzing events due to multiple simultaneous failures.
- Assigning keywords to specific parts in complex systems is challenging.
- Predicting implications of deviations across system parts can be complex.

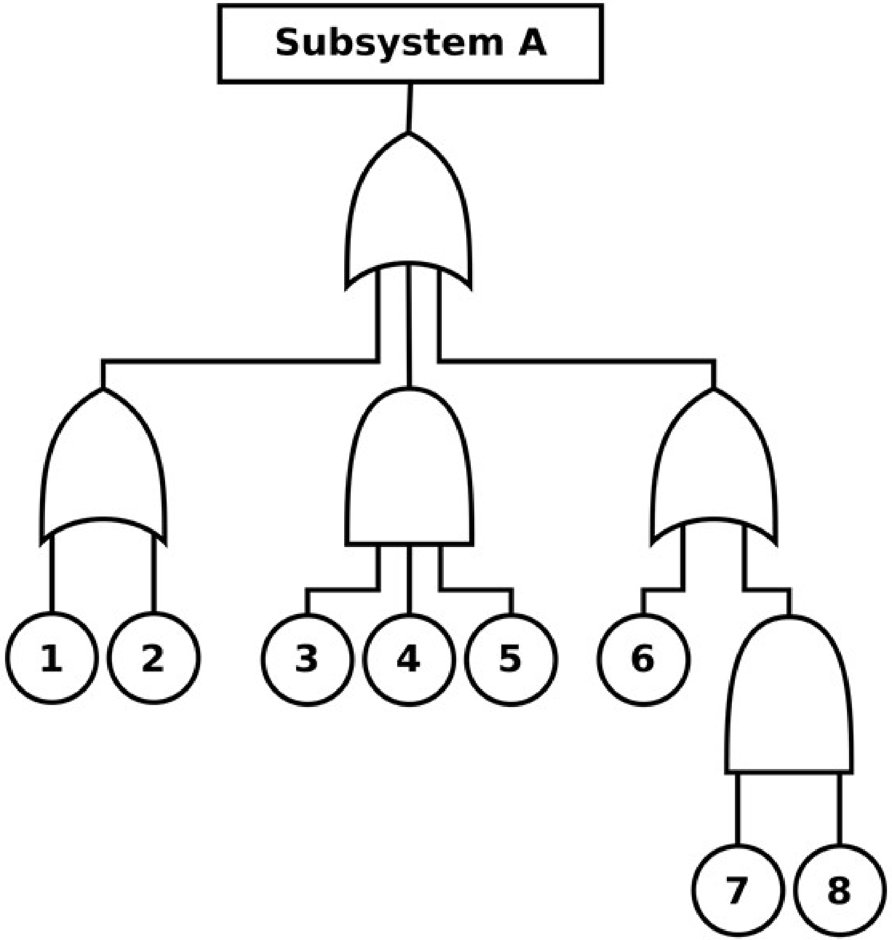
Source: https://www.solvoyo.com

Module 2.6

What if…?

What-if ?

- What-If analysis assesses outcomes of certain actions.
- From various scenarios, prioritize the outcome that most aligns with the goal.
- It's similar to HAZOP but based on a succession of questions like: What happens if?
- Deviations result from deviations from normal expectations.
- Effectiveness depends on team experience.
- It's less cumbersome than HAZOP but requires an experienced team.



Source: *https://en.wikipedia.org/wiki/Fault_tree_analysis*

Module 2.7

FTA
Fault tree analysis

FTA: Introduction

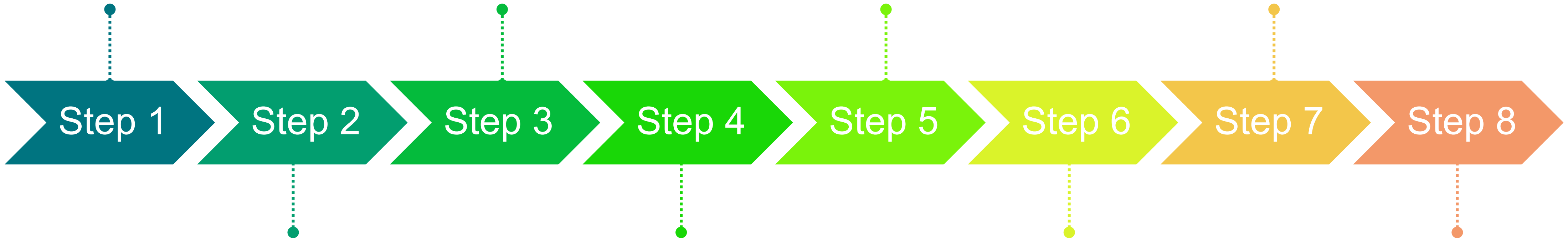
- Fault Tree Analysis (FTA) was developed in the early 1960s by the American Bell Telephone Company and has been widely used for assessing safety, with the standard IEC 61025:2006 now in place.

- FTA is a deductive and quantitative approach used to systematically analyze the causes of adverse events, failures, or accidents.

- It starts with a predefined feared event and works backward to identify the sequences or combinations of events that could lead to that event.

- Through this process, fault trees illustrate the interplay of failures and events within a system and pinpoint the root events, often referred to as basic events, by tracing the causal pathways to the top event.

FTA: Methodology



Define the system
Determine the analysis scope, which involves defining the undesirable top event, typically known as the primary failure or accident.

Define top-level faults
Begin the analysis by clearly defining the specific failure or accident that is the focus of the analysis.

Identify causes for top-level fault
Identify contributing events and link them to the top-level fault using logical gates like AND and OR gates.

Identify next level of events
Each event contributing to the top-level failure may also have its own set of precipitating events..

Identify root causes
Identify the causes of each event to find the root cause of the failure sequence.

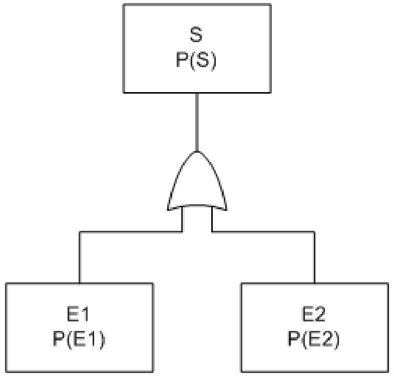
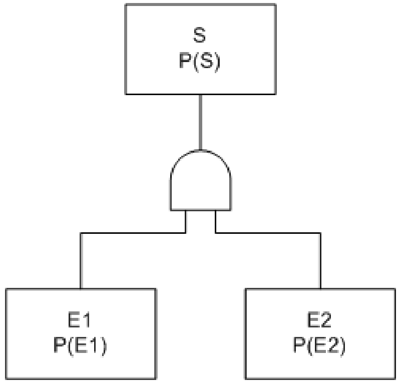
Add probabilities to events
Assign a likelihood of occurrence (LO) to each root event and use Boolean algebra to calculate the LO of the top event.

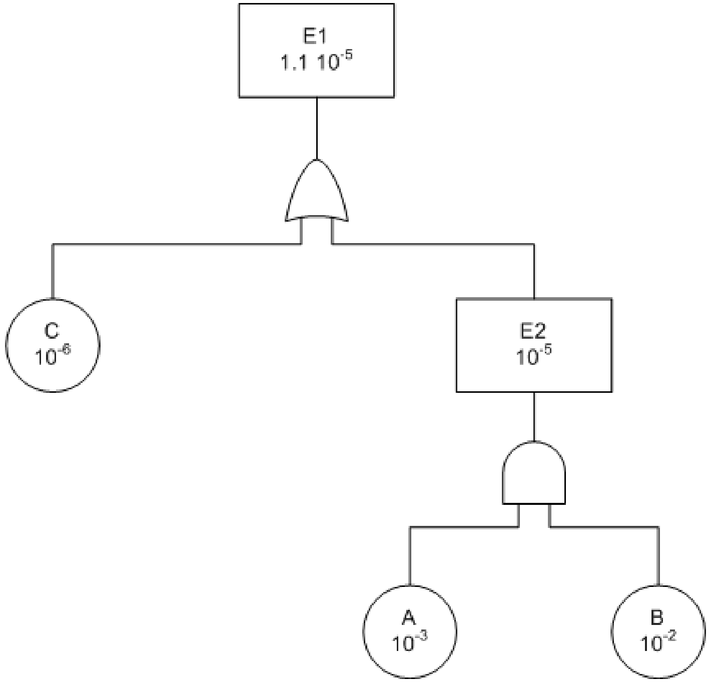
Analysis the fault tree
Identify the most likely events leading to failure, especially those causing multiple failure paths or related to various stressors, usage, or operating conditions. Find solutions to mitigate these failure paths

Document the FTA
Document notes and proposed measures to reduce the top event's occurrence, prioritizing critical paths and addressing common causes among basic events.

FTA: Logical gates (1)

A Boolean variable is associated to each basic event

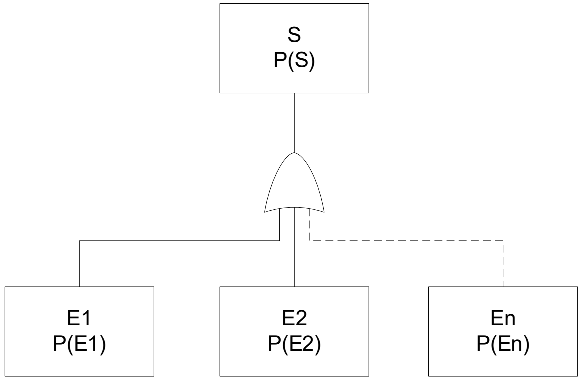
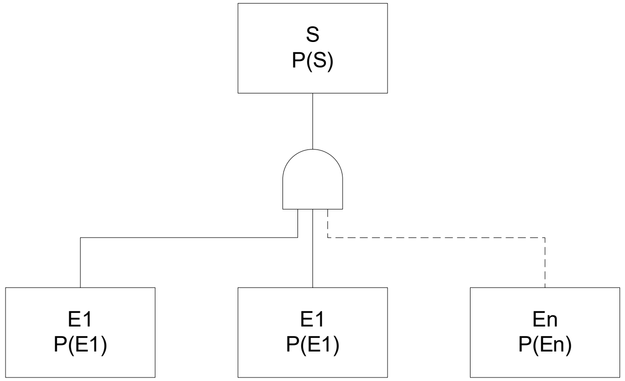
Gate « OR »	Gate « AND »
	
$P(S) = P(E1) + P(E2) - P(E1) \cdot P(E2)$	$P(S) = P(E1) \cdot P(E2)$



Probability calculation

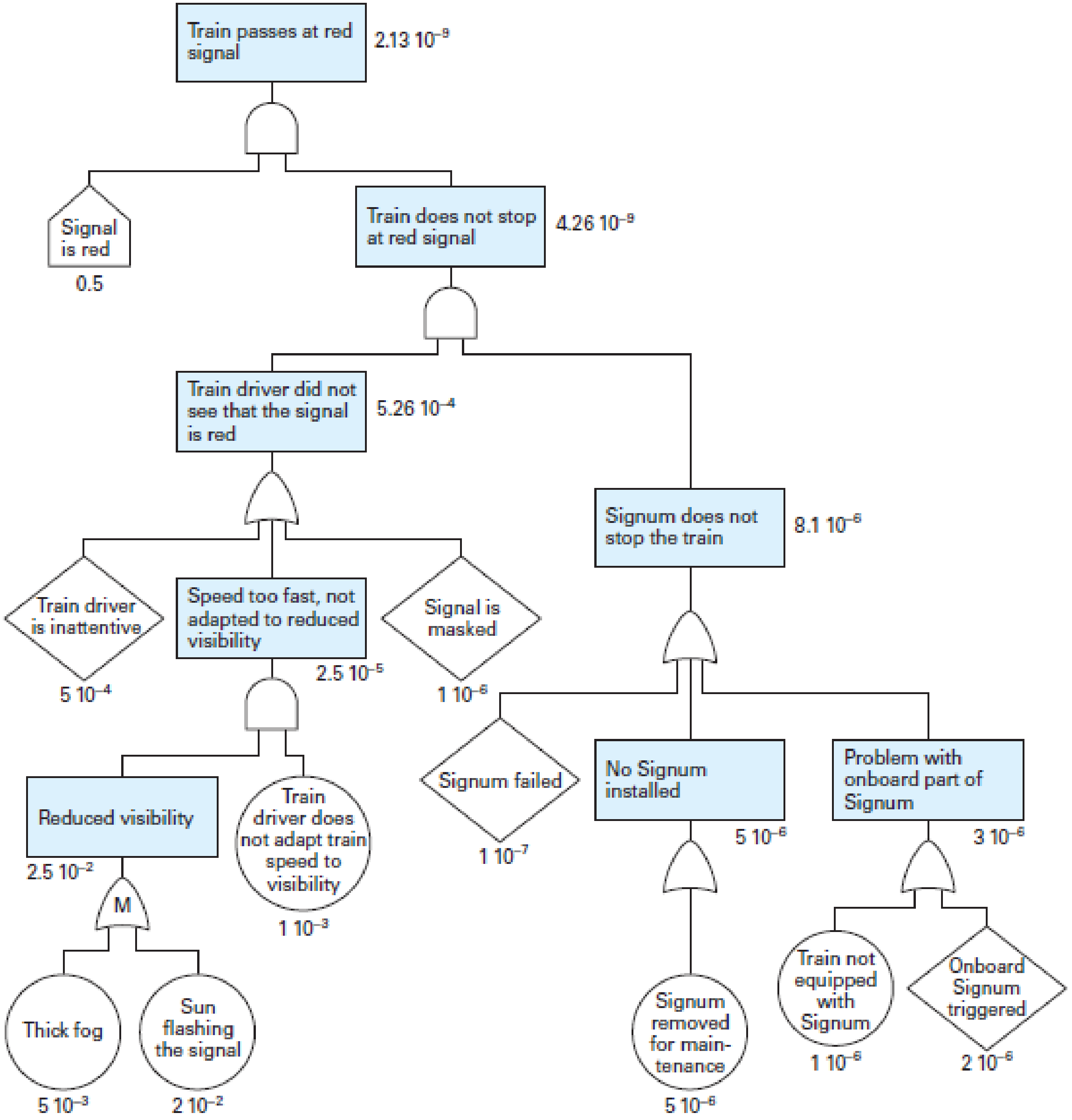
FTA: Logical gates (2)

Probability calculation with n gates

	Gate « OR »	Gate « AND »
		
n gates	$P(S) = \sum(singles) - \sum(pairs) + \sum(triples) - \sum(fours) + \sum(fives) - \sum(sixes) + \cdots$	$P(S) = \prod_{1}^{n} P(E_n)$
3 gates	P(S) = P(E1) + P(E2) + P(E3) - P(E1) · P(E2) - P(E2) · P(E3) - P(E3) · P(E1) + P(E1) · P(E2) · P(E3)	P(S) = P(E1) · P(E2) · P(E3)

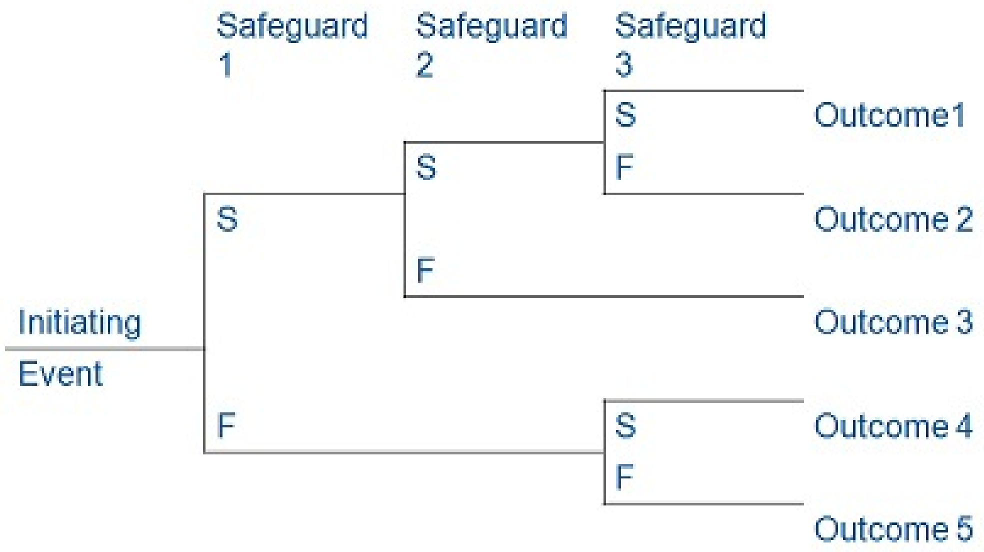
FTA: Example

- Consider the event "Train passes at red signal".
- The mentioned likelihood of occurrence are fictitious and used for illustrative purposes.


Train passes at red signal
$2.13\ 10^{-9}$
Signal is red
0.5
Train does not stop at red signal
$4.26\ 10^{-9}$
Train driver did not see that the signal is red
$5.26\ 10^{-4}$
Signum does not stop the train
$8.1\ 10^{-6}$
Train driver is inattentive
$5\ 10^{-4}$
Speed too fast, not adapted to reduced visibility
$2.5\ 10^{-5}$
Signal is masked
$1\ 10^{-6}$
Reduced visibility
$2.5\ 10^{-2}$
M
Train driver does not adapt train speed to visibility
$1\ 10^{-3}$
Thick fog
$5\ 10^{-3}$
Sun flashing the signal
$2\ 10^{-2}$
Signum failed
$1\ 10^{-7}$
No Signum installed
$5\ 10^{-6}$
Problem with onboard part of Signum
$3\ 10^{-6}$
Signum removed for maintenance
$5\ 10^{-6}$
Train not equipped with Signum
$1\ 10^{-6}$
Onboard Signum triggered
$2\ 10^{-6}$

FTA: Conclusions

- FTAs are logical block diagrams showing how a system's state depends on its components' states (deductive method).
- Useful for considering event combinations leading to a final undesirable event and prioritizing accident prevention.
- Not suitable for systems with many adverse events.
- Quantification can be challenging due to unknown event occurrence rates.
- Incorrect construction can lead to inaccurate and potentially dangerous results, especially for beginners.



Source: https://egertonconsulting.com/

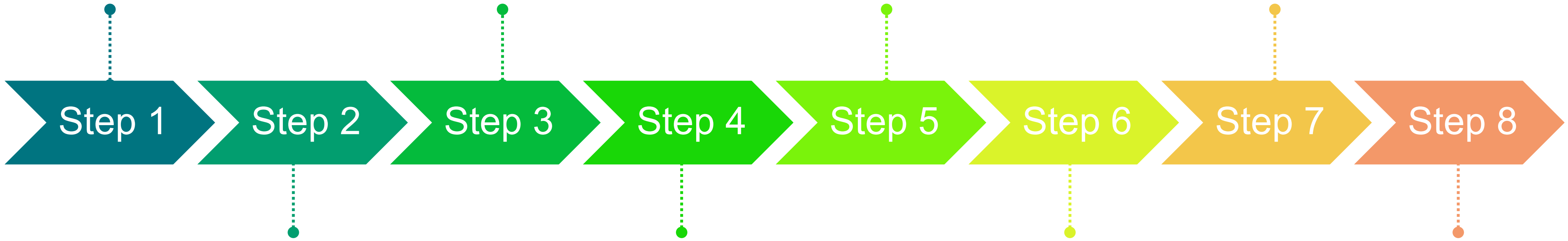
Module 2.8

ETA
Event tree analysis

FTA: Introduction

- Event tree analysis was developed in the early 1970s for risk assessment in light water nuclear power plants (now standard IEC 62502:2010).
- ETA methodology has several similarities with FTA approach, in that both develop a tree structure and both describe scenarios related to adverse events.
- Unlike FTA approach, ETA is built in chronological order.
- ETA starts with a triggering event and examines the consequences that follow, with a focus on component failures and subsequent events. It is therefore an inductive approach.
- ETA allows for the analysis of scenarios related to adverse events.

ETA: Methodology



Step 1

Define the system and initiating event

This involves defining the scope of the analysis, including the identification of the initiating event.

Step 2

Define controls

Identify safety functions, system components, or controls assigned to address the primary event, such as automatic safety systems or alarms for operator actions.

Step 3

Construct the tree

Starting with the initiating event and moving through safety function failures, using Boolean values for success (Y/N).

Step 4

Accident Sequence

Determine the ultimate consequences of each scenario, including material, human, and environmental impacts.

Step 5

Calculate probabilities

Assign probabilities to each branch of the tree and calculate the likelihood of occurrence for each scenario by multiplying the probabilities.

Step 6

Critical failures

Identify the critical failures that require attention.

Step 7

Mitigation

Suggest suitable mitigation measures if the criticality of specific scenarios is deemed too high.

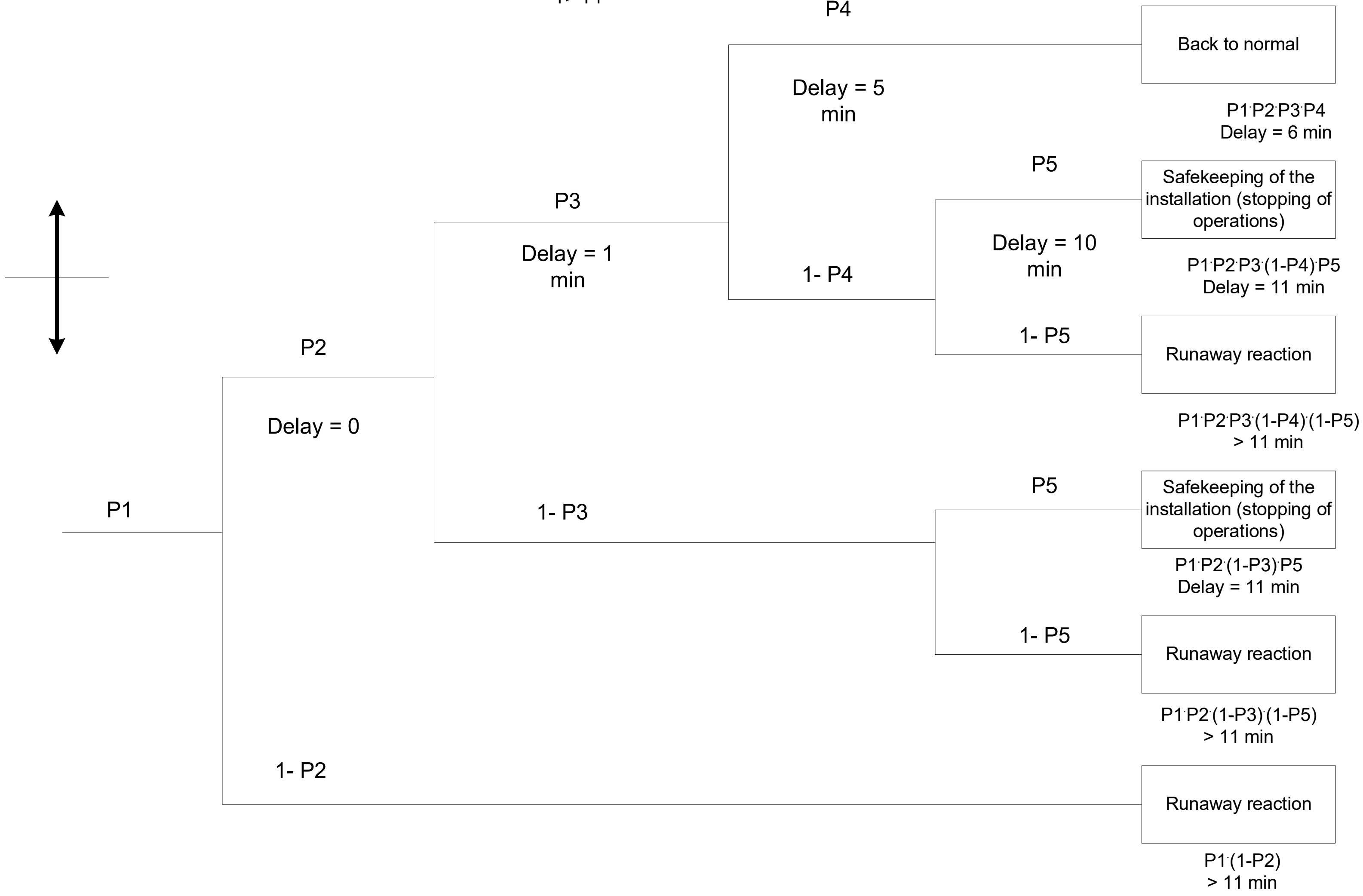
Step 8

Document the FTA

Document notes and proposed measures for addressing critical failures.

ETA: Probabilities (1)

Top event	Conditioning event	Safety function			Outcome event
Initiating Event : Failure of cooling system	Temperature measurement in the reactor	Alarm signifying the increase of the temperature to an operator T> T1	Restoration of the cooling system by an operator	Automatic inhibition of the reaction at T> T2	Sequences leading to:



P1

P2

Delay = 0

1- P2

P3

Delay = 1 min

1- P3

P4

Delay = 5 min

1- P4

P5

Delay = 10 min

1- P5

P5

1- P5

Back to normal

P1·P2·P3·P4
Delay = 6 min

Safekeeping of the installation (stopping of operations)

P1·P2·P3·(1-P4)·P5
Delay = 11 min

Runaway reaction

P1·P2·P3·(1-P4)·(1-P5)
> 11 min

Safekeeping of the installation (stopping of operations)

P1·P2·(1-P3)·P5
Delay = 11 min

Runaway reaction

P1·P2·(1-P3)·(1-P5)
> 11 min

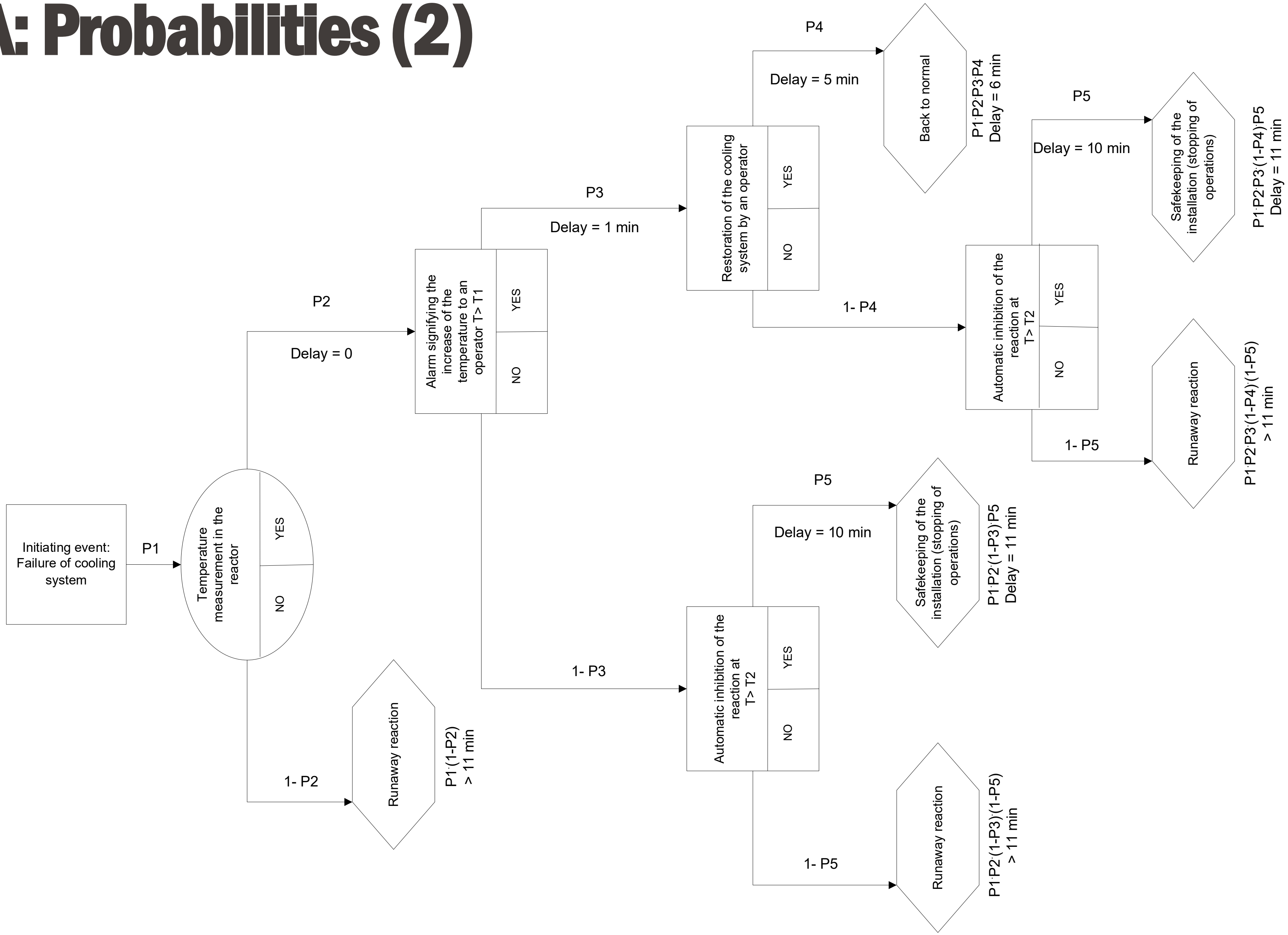
Runaway reaction

P1·(1-P2)
> 11 min

Thierry Meyer

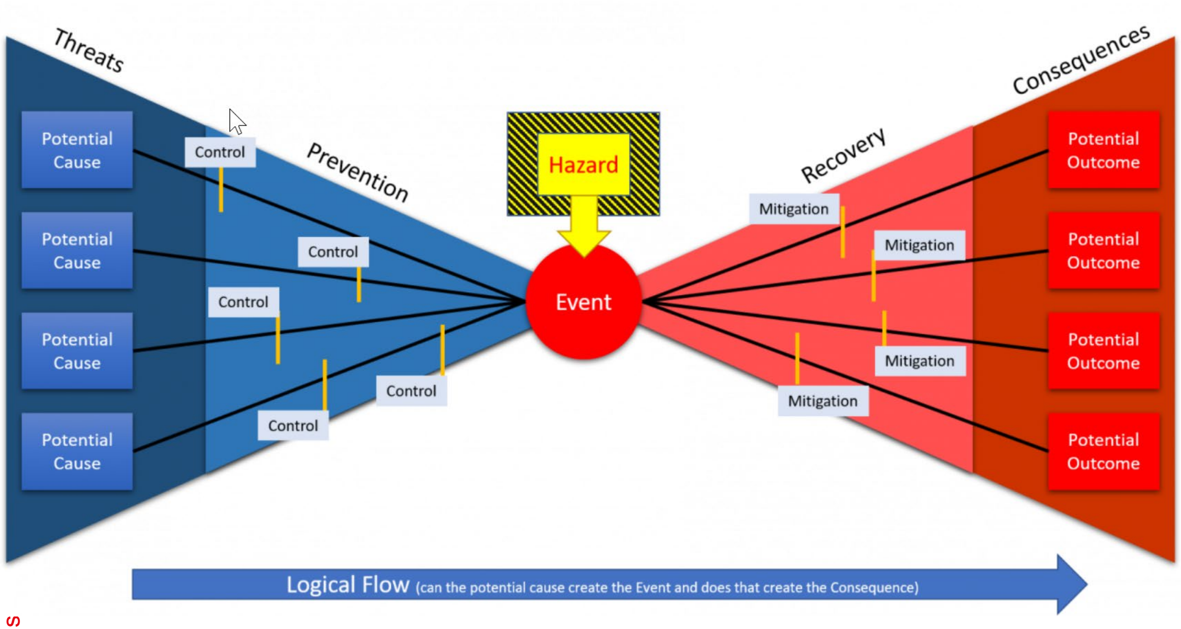
Course 2025 RM / Module 2 : Risk diagnostic and analysis

ETA: Probabilities (2)


Initiating event: Failure of cooling system
P1
Temperature measurement in the reactor
YES
NO
P2
Delay = 0
1- P2
Runaway reaction
P1·(1-P2)
> 11 min
Alarm signifying the increase of the temperature to an operator T> T1
YES
NO
P3
Delay = 1 min
1- P3
Restoration of the cooling system by an operator
YES
NO
P4
Delay = 5 min
Back to normal
P1·P2·P3·P4
Delay = 6 min
1- P4
Automatic inhibition of the reaction at T> T2
YES
NO
P5
Delay = 10 min
Safekeeping of the installation (stopping of operations)
P1·P2·P3·(1-P4)·P5
Delay = 11 min
1- P5
Runaway reaction
P1·P2·P3·(1-P4)·(1-P5)
> 11 min
Automatic inhibition of the reaction at T> T2
YES
NO
P5
Delay = 10 min
Safekeeping of the installation (stopping of operations)
P1·P2·(1-P3)·P5
Delay = 11 min
1- P5
Runaway reaction
P1·P2·(1-P3)·(1-P5)
> 11 min

ETA: Conclusions

- ETA analyzes the consequences of a single failure on overall system risk.
- It considers various outcomes based on accidental events and safety barrier operation.
- ETA focuses on a single initiating event and isn't suitable for multiple events.
- It lacks a systematic approach for identifying initiating events.
- Careful selection of the initiating event is essential for effective analysis



Source: https://www.manycaps.com

Module 2.9

CCA (cause-consequence-analysis) and combination of FTA and ETA

CCA & Bowtie: Introduction

- The origins of Bowtie analysis is believed to come from Imperial Chemical Industries in the 1970’s and from courses given at the University of Queensland (1979).

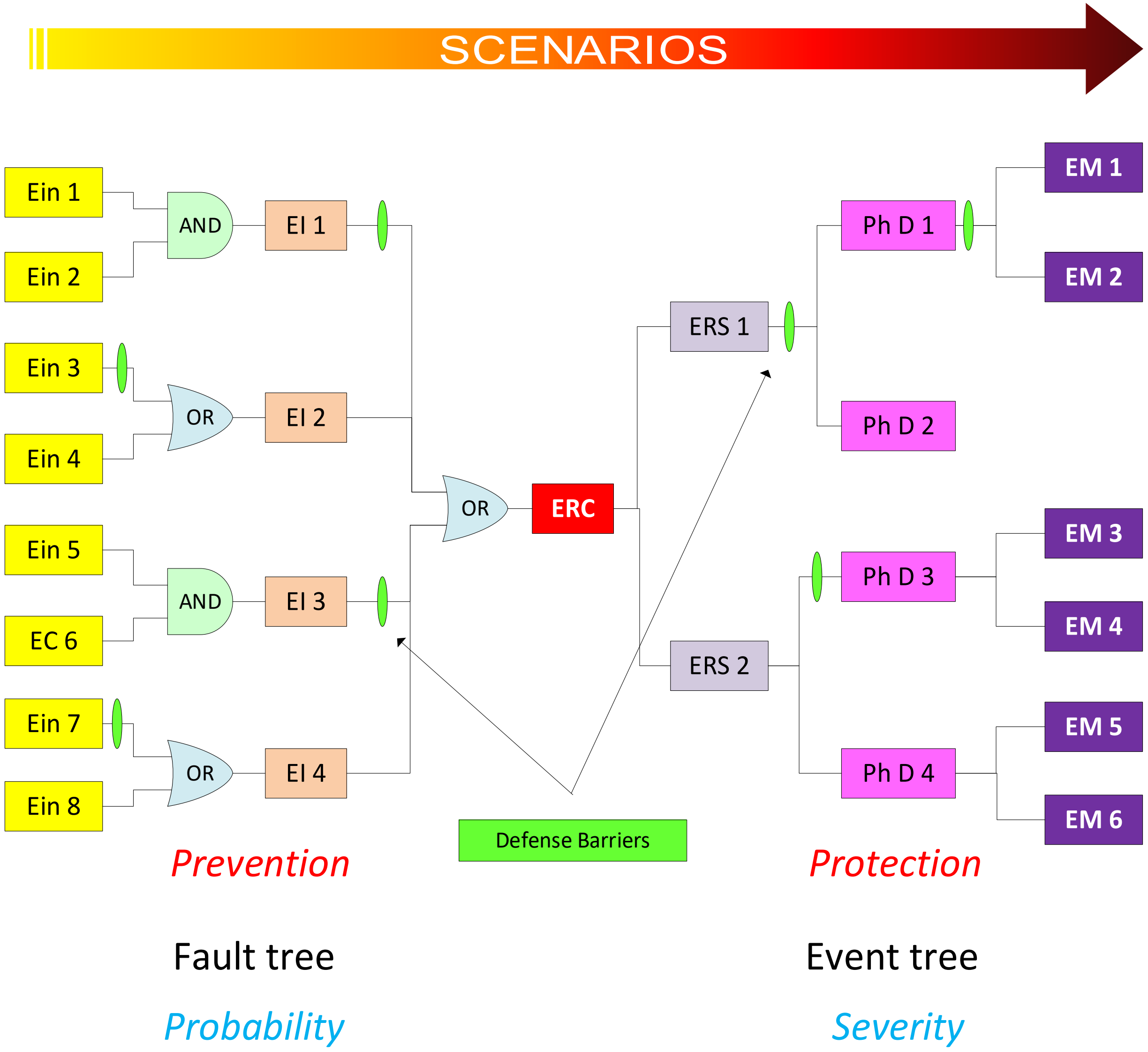
- Fault Tree Analysis (FTA) offers a specific aspect study and is non-inductive in nature.

- Event Tree Analysis (ETA) may have challenges in quantification and depth for precise risk assessment, despite being inductive.

- Combining FTA and ETA, known as bowtie and CCA (cause-consequence analysis), creates one of the most rigorous and powerful methodologies.

- CCA and bowtie employ a simultaneous inductive-deductive approach to effectively address both general and specific situations.

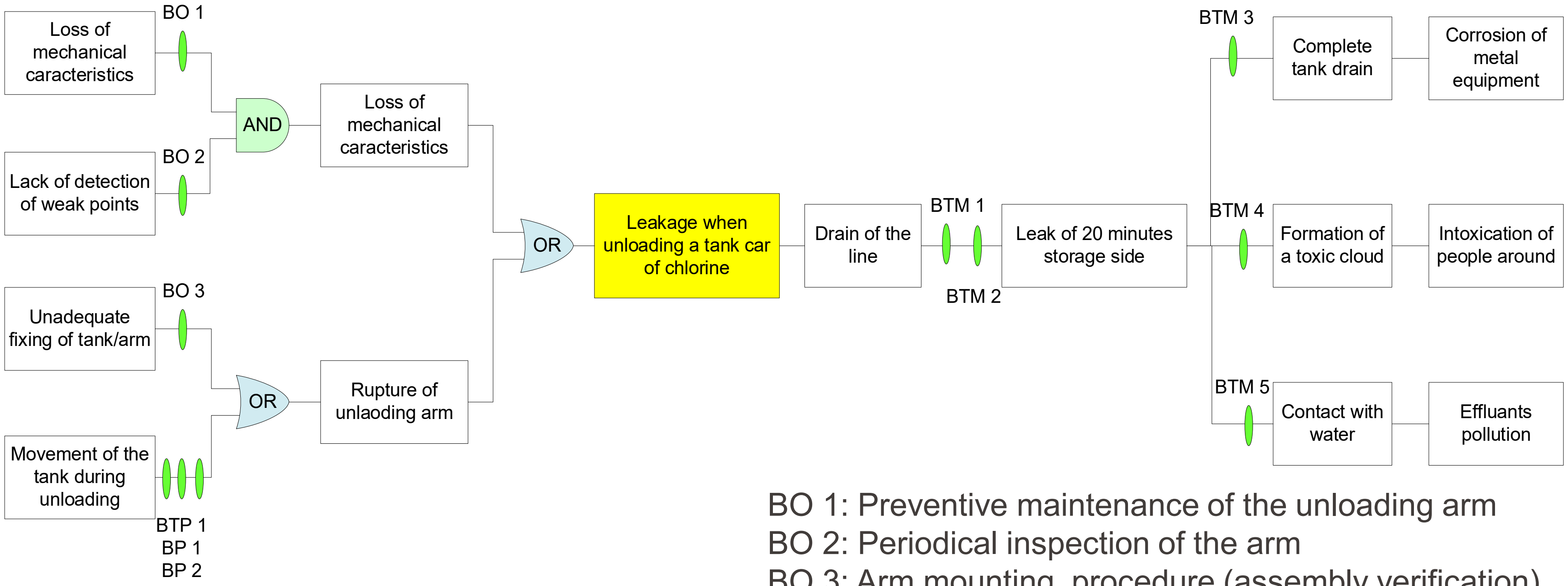
CCA : Representation



CCA : Acronyms

Acronym	*Signification*	*Definition*	*Examples*
Ein	Undesired event	Drift or failure outside the defined normal operating conditions	Fire starts near hazardous equipment
EC	Frequent event	An event that occurs repeatedly over the lifespan of a facility.	The actions of testing, maintenance or fatigue of equipment
EI	Initiating event	Direct cause of containment loss or physical integrity	Corrosion, erosion, mechanical aggression, pressure rise
ERC	Feared event	Loss of containment of dangerous equipment or loss of physical integrity of a hazardous substance	Rupture, breach, decomposition of a hazardous substance (loss of physical integrity)
ERS	Secondary feared event	As a direct consequence of the feared event, the secondary event presents another source of accident	Formation of a puddle or a cloud due to a substance release
Ph D	Hazardous phenomenon	Physical phenomenon that can cause major damage	Fire, explosion, dispersion of a toxic cloud
EM	Major consequences	Damage at the target (person, environment, property) by the effects of a hazardous phenomenon	Lethal or irreversible effects on the population, synergies accident
Barriers or prevention measures		Barriers or measures to prevent loss of containment or physical integrity	Anti-corrosion paint, automatic stop in case of alarm, ...
Barriers or protection measures		Barriers or measures limiting the consequences of a loss of containment or physical integrity	Means of intervention, containment, protective equipment, ...

CCA : Example – Unloading a tank of chlorine

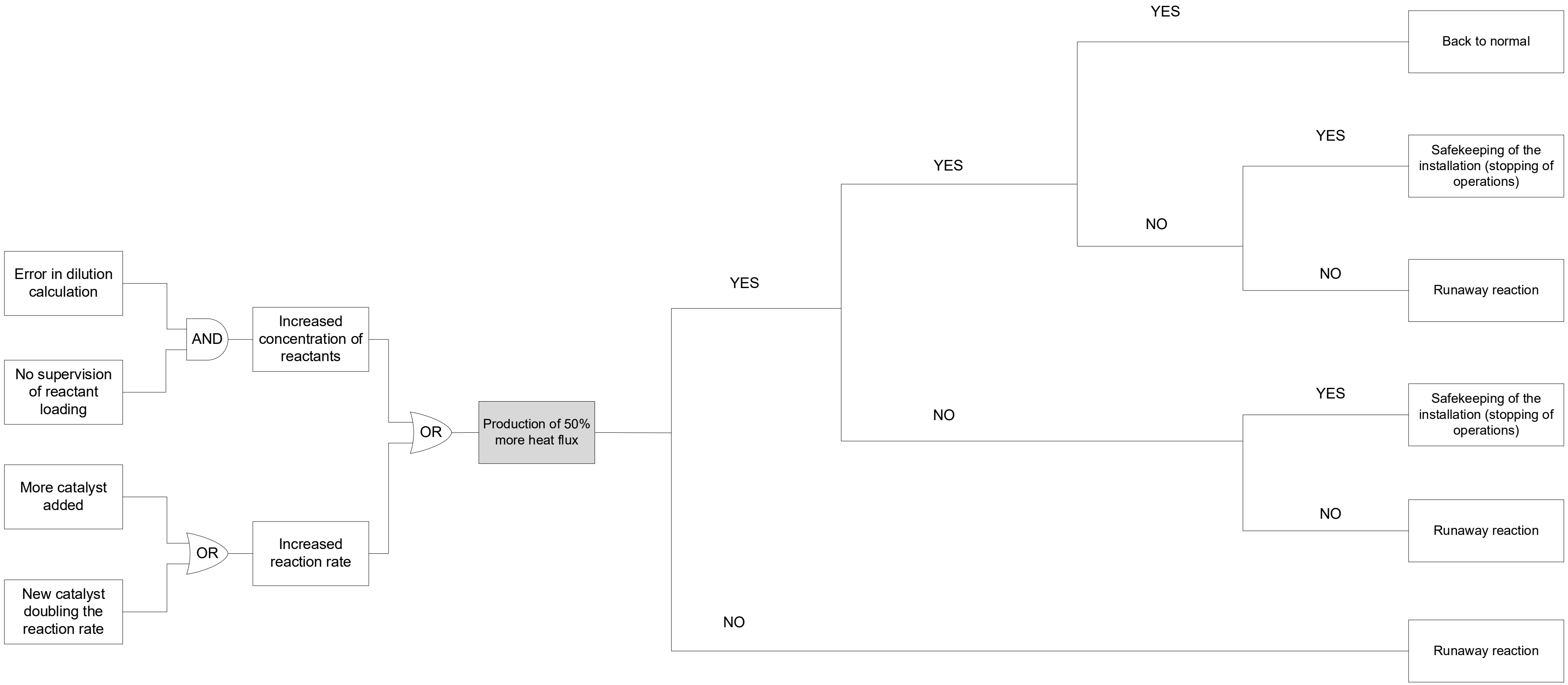

Loss of mechanical caracteristics
BO 1
Lack of detection of weak points
BO 2
AND
Loss of mechanical caracteristics
Unadequate fixing of tank/arm
BO 3
Movement of the tank during unloading
BTP 1
BP 1
BP 2
OR
Rupture of unlaoding arm
OR
Leakage when unloading a tank car of chlorine
Drain of the line
BTM 1
BTM 2
Leak of 20 minutes storage side
BTM 3
Complete tank drain
Corrosion of metal equipment
BTM 4
Formation of a toxic cloud
Intoxication of people around
BTM 5
Contact with water
Effluants pollution

BO 1: Preventive maintenance of the unloading arm
BO 2: Periodical inspection of the arm
BO 3: Arm mounting procedure (assembly verification)
BTP 1: Unloading signalization by a red light
BP 1: Guardrail along the unloading route
BP 2: Equipment avoiding the tank to slip off rails
BTM 1: Safety valve on the stock side
BTM 2: Safety valve on tank
BTM 3: Manual valve on tank
BTM 4: Watering by water spray
BTM 5: Retention basin isolated from the drainage

Acronyms:
BO: Organizational prevention barrier
BP: Passive barrier
BTP: Technical prevention barrier
BTM: Technical protection barrier

Bowtie FTA/ETA: Example - Representation

Top event	Conditioning event	Safety function			Outcome event
Event originator: Failure of cooling system	Temperature measure in the reactor	Alarm signifying the rise in temperature to an operator T> T1	Restoration of cooling system by an operator	Automatic inhibition of the reaction at T> T2	Sequences leading to:



Error in dilution calculation

No supervision of reactant loading

AND

Increased concentration of reactants

More catalyst added

New catalyst doubling the reaction rate

OR

Increased reaction rate

OR

Production of 50% more heat flux

YES

YES

YES

Back to normal

NO

YES

Safekeeping of the installation (stopping of operations)

NO

Runaway reaction

NO

YES

Safekeeping of the installation (stopping of operations)

NO

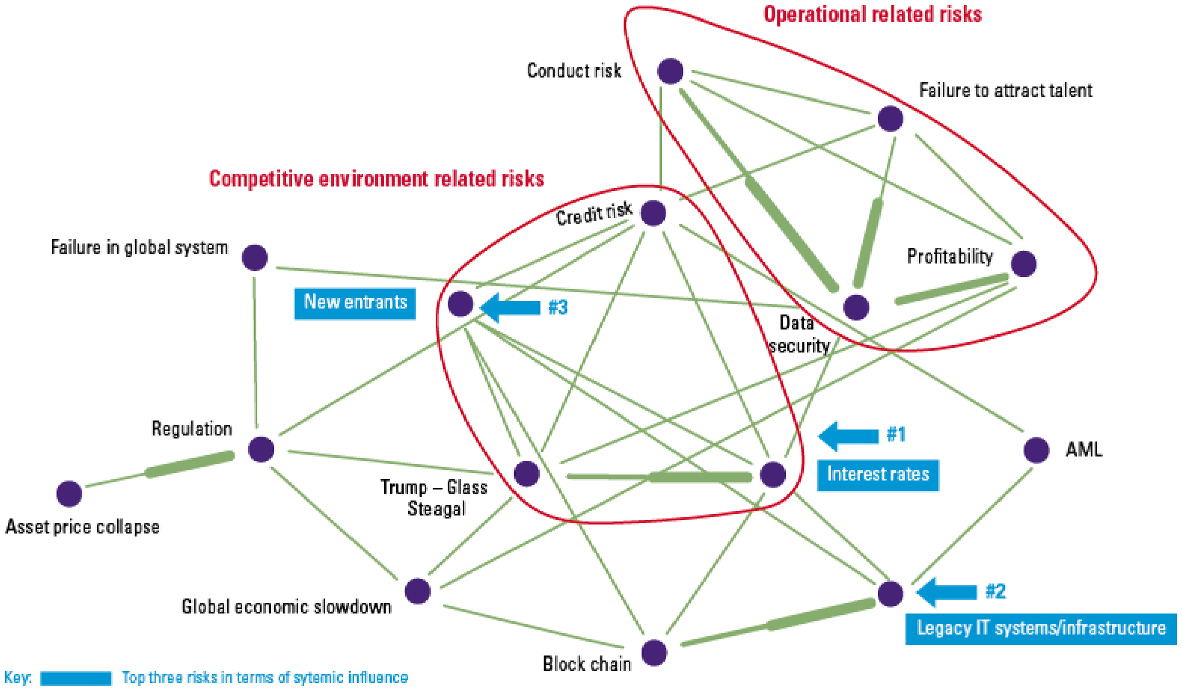
Runaway reaction

NO

Runaway reaction

CCA & Bowtie: Conclusions

- Implementing a CCA and bowtie analysis is demanding and requires experts.
- These methodologies focus on one triggering event at a time and lack systemic assessment.
- They combine the strengths of fault trees, illustrating how factors combine to cause hazardous events and various outcomes.
- The techniques are suitable for quantification but can lead to complex diagrams.
- These tools effectively demonstrate the role of safety barriers in managing risk.
- Analyzing a complex system with numerous initiating events using CCA or FTA/ETA approaches can be impractical and time-consuming.
- Analyzing a complex system with numerous initiating events using CCA or FTA/ETA approaches can be impractical and time-consuming, as this will require years of work.



Source: https://www.compact.nl/en/articles/dynamic-risk-assessment/

Module 2.10

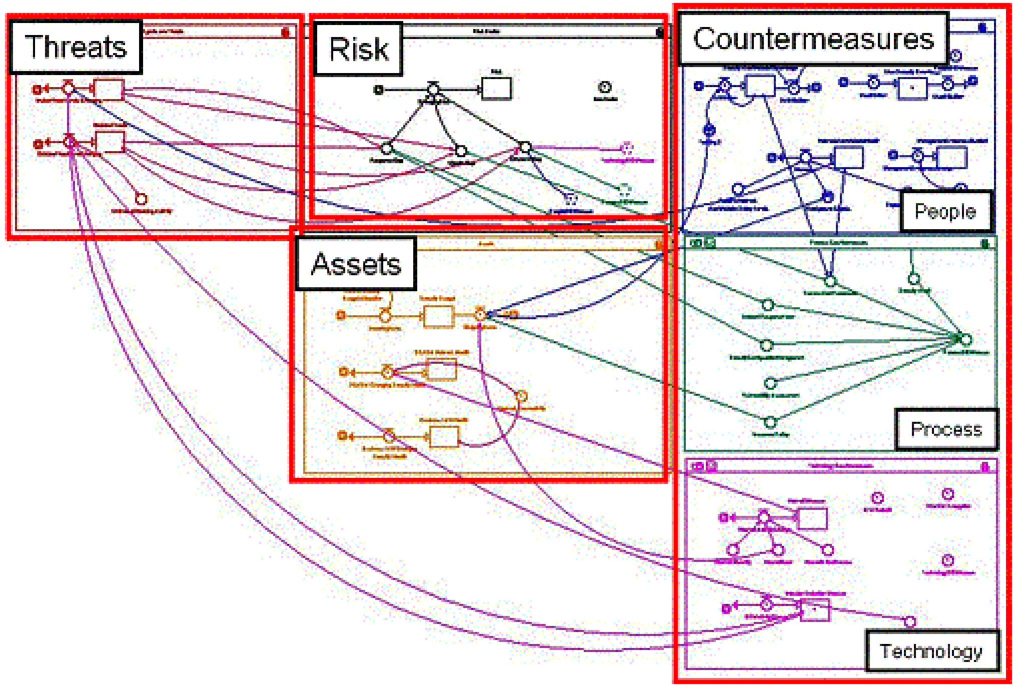
Dynamic methods

Dynamic methods: Introduction

- Dynamic methods are used to analyze industrial systems that experience changes in their states over time due to various factors such as breakdowns, repairs, reconfigurations, or weather conditions.

- These systems can be described as undergoing random or stochastic processes, where the term "random process" and "stochastic process" are interchangeable and signify that the changes occur in a random manner as the name suggests.Some methods:
  - Petri networks
  - Markov chains
  - Neural networks
  - Bayesian belief networks
  - …

Dynamic methods: Motivation



Source: A Dynamic Risk Model for Information Technology Security in a Critical Infrastructure Environment, John H. Saunders, 2003

- n a risk analysis, a scenario can be defined as the way a specific initiating event propagates and leads to a wide range of undesirable consequences.

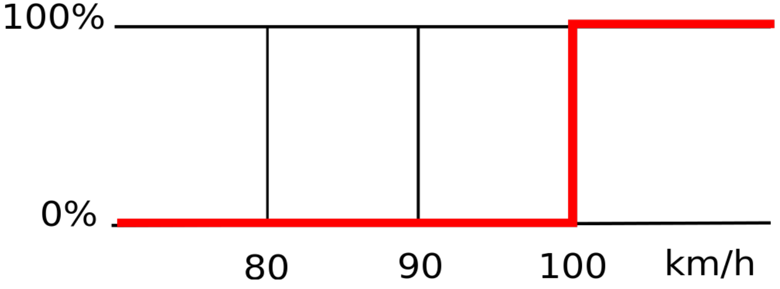
- When multiple scenarios are considered, the risk analysis becomes more complex than when analyzing a single scenario in isolation.

Risk: How to manage uncertainty? (1)

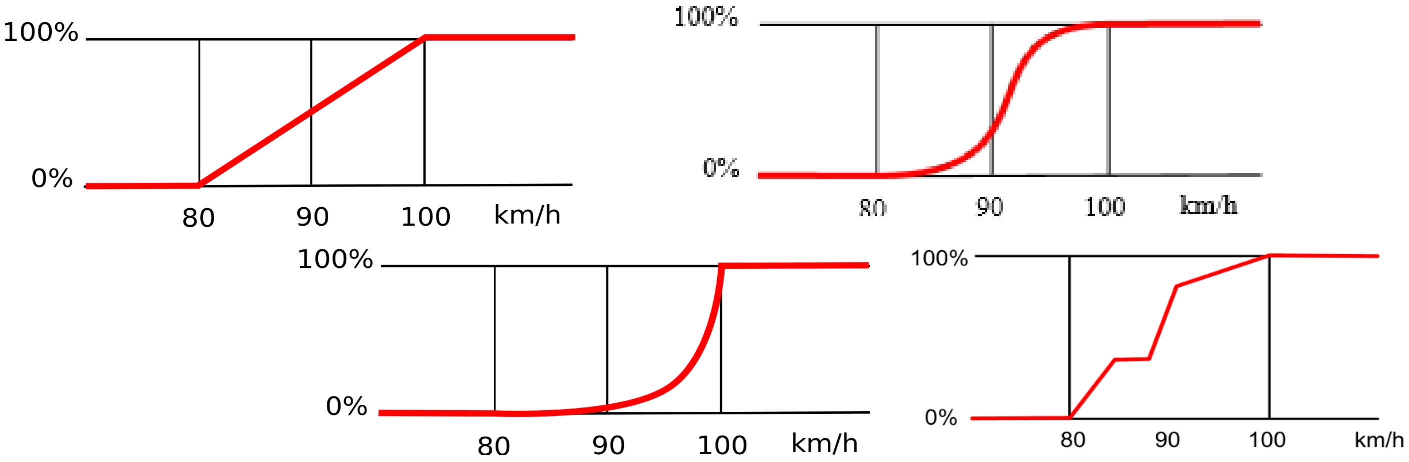
- On French roads, legal speed limit is 90 km/h, speeds above 100 km/h are considered high, and speeds below 80 km/h are considered normal.

- Let’s try to answer this question « Is the speed of the car high?»:

In Boolean logic, the answer to this question is:



In fuzzy logic, it can be expressed as follows:

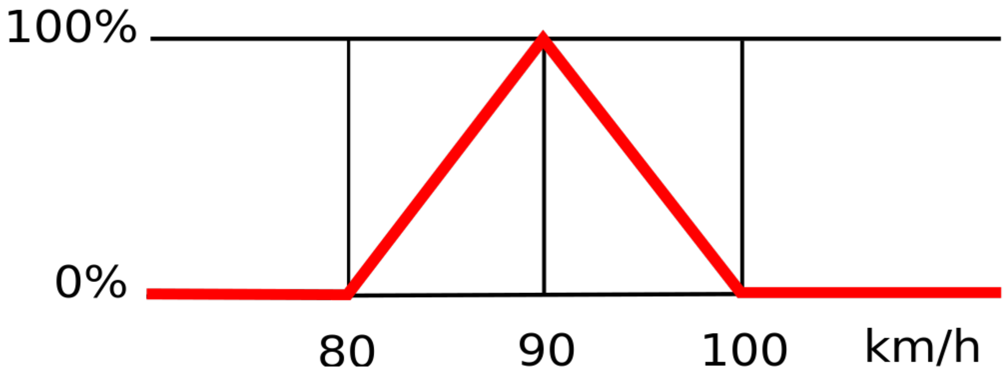


Risk: How to manage uncertainty? (2)

Let’s ask ourselves : « Is the speed of the car average? »

In Boolean logic, only 90 km/h gives a 100% positive answer, the rest is 0%.

In fuzzy logic, it can be expressed as follows:



The answer comprises values ranging from 80 to 100 km/h with a specific distribution that needs to be determined.

Risk: How to manage uncertainty? (3)

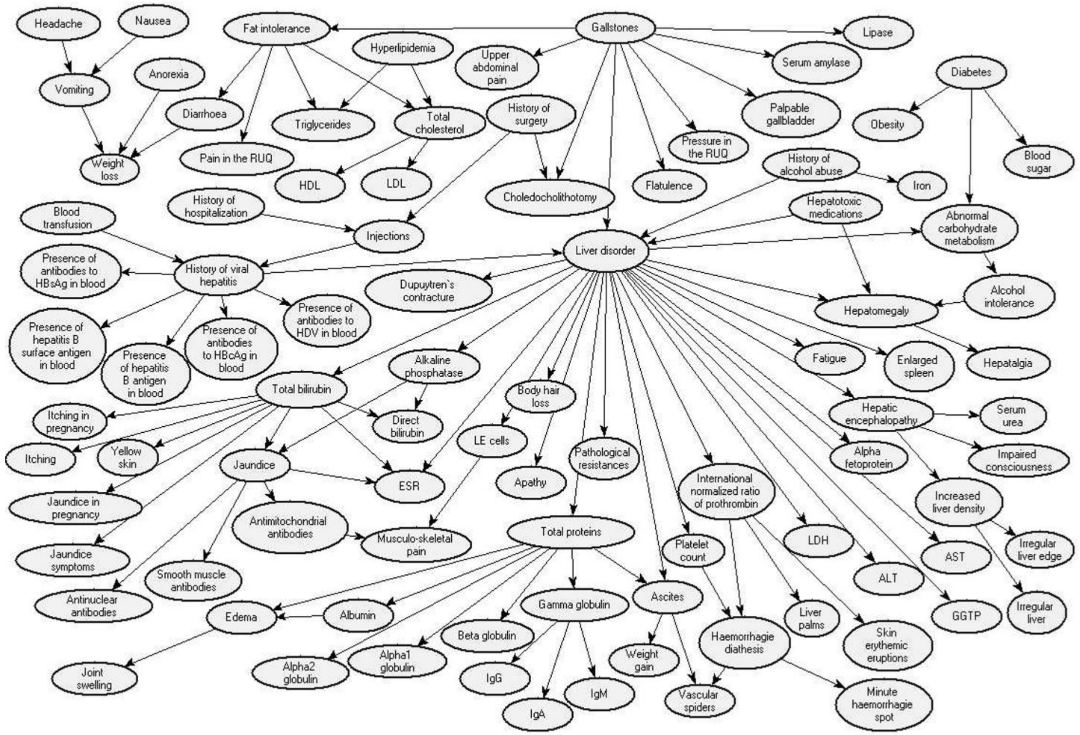
- Uncertainties can be addressed through the use of mathematical models, including:
  - Neural networks
  - Bayesian belief networks
  - Fuzzy logic
  - Stochastic modeling (e.g. Monte-Carlo)
  - Polynomial chaos
  - …

- The majority of these models share a common objective: to depict elements that are challenging to precisely define or observe. They also aim to quantify variables that are typically described in verbal terms, such as "a lot“, "too much" or "enough", ...

For example: They say this man is tall !

But how tall do you think he is ?

Risk: Bayesian networks

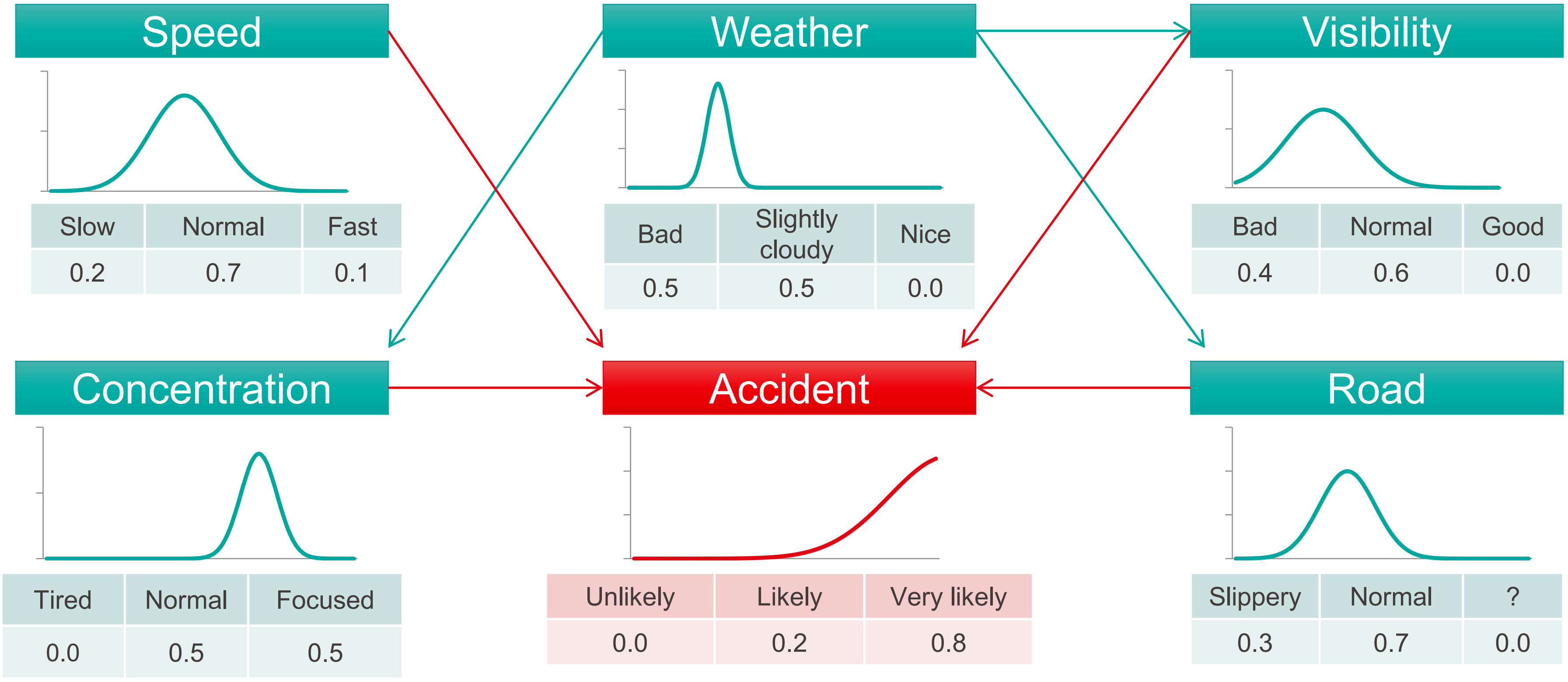


Source: A Bayesian Network Model for Diagnosis of Liver Disorders" – Agnieszka Onisko, M.S. et al., Research Report CBMI-99-27 September 1999

- Enable predictive calculations using uncertain or fuzzy statements and distributions.
- Utilize graphical models to illustrate random variables and their dependencies.
- Facilitate predictions based on all relevant variables.

Risk: Bayesian networks - example

1. Define all variables
2. Determine interrelations
3. Determine accident probability
4. Calculate the risk



Speed

Slow	Normal	Fast
0.2	0.7	0.1

Weather

Bad	Slightly cloudy	Nice
0.5	0.5	0.0

Visibility

Bad	Normal	Good
0.4	0.6	0.0

Concentration

Tired	Normal	Focused
0.0	0.5	0.5

Accident

Unlikely	Likely	Very likely
0.0	0.2	0.8

Road

Slippery	Normal	?
0.3	0.7	0.0

High risk

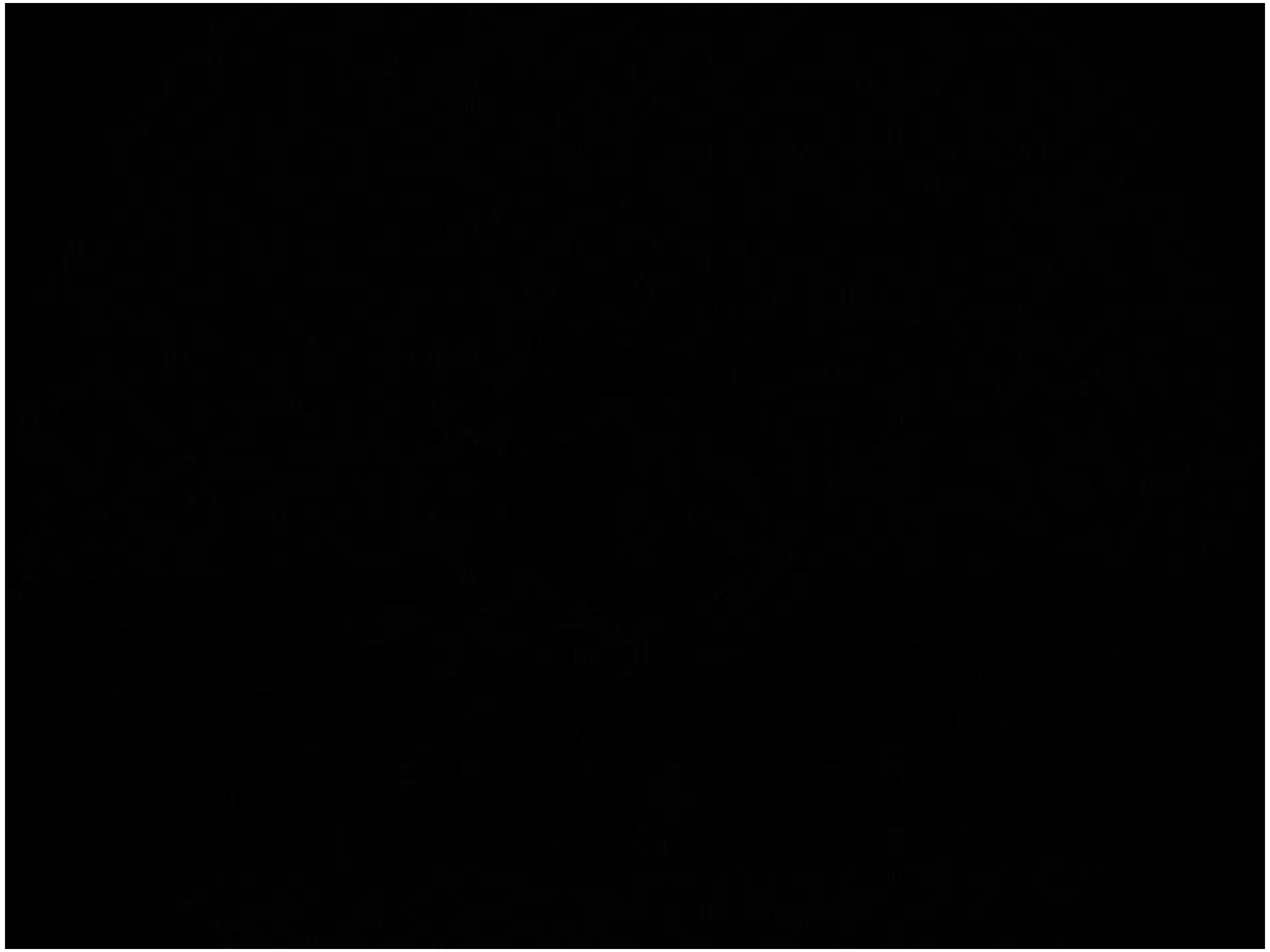
Source: https://evoke.ie/2017

Module 2.11

Risk diagnostic conclusions

Conclusions: Learning by accident ?

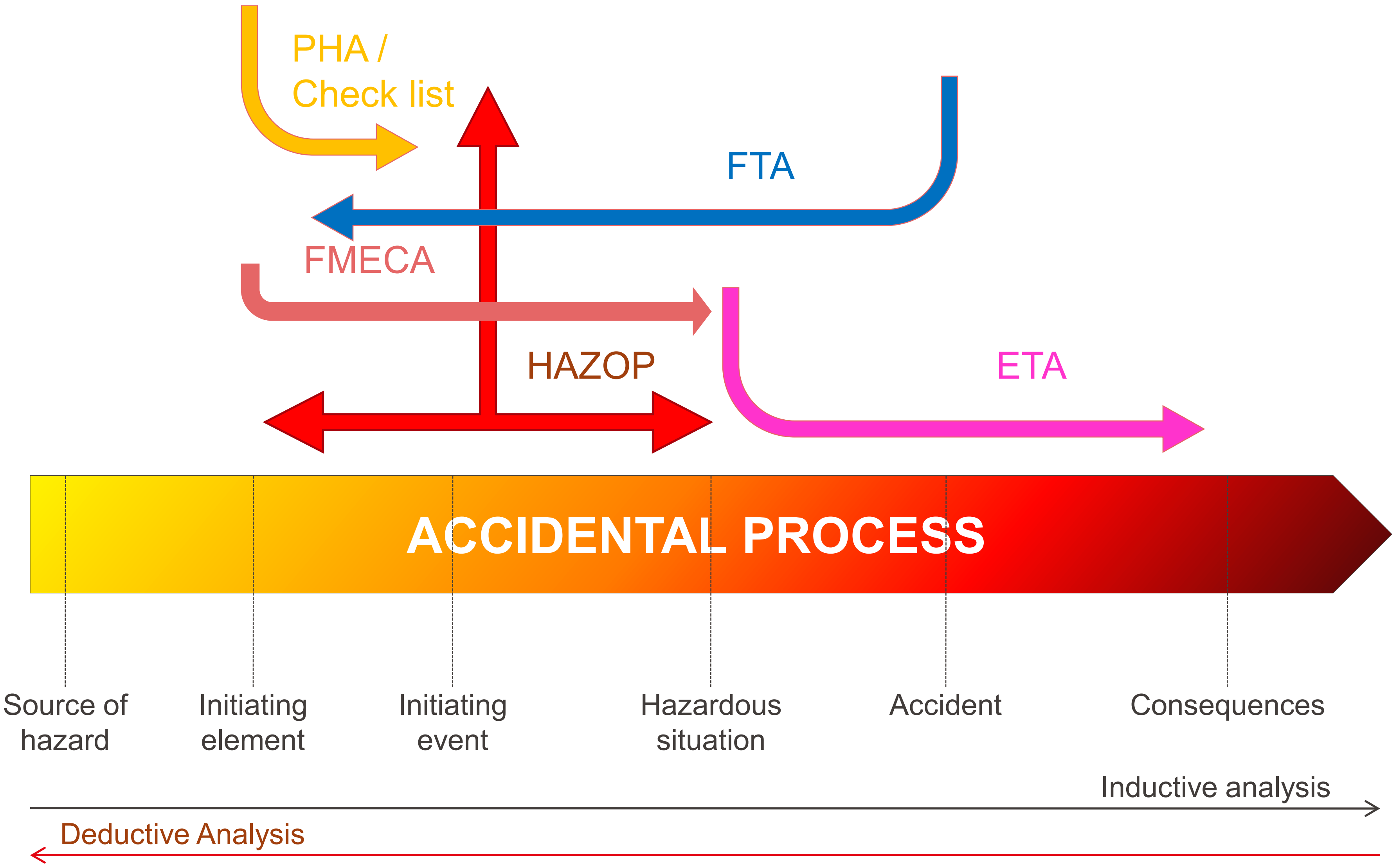
- 2007.12.17 Jacksonville, FL : T2 laboratories Inc.
- Runaway chemical reaction likely due to inadequate reactor cooling system
- Report indicates that the company failed to recognize the hazards of a chemical process
- 4 deaths, over 30 injuries



Time 9`25``

Source: https://www.csb.gov/

Conclusions: Entry point and development


PHA /
Check list
FTA
FMECA
HAZOP
ETA
ACCIDENTAL PROCESS
Source of hazard
Initiating element
Initiating event
Hazardous situation
Accident
Consequences
Inductive analysis
Deductive Analysis