



MACQUARIE
University

Risk Analysis in Robotics and Automation

(MTRN 6060)



Presented by: Professor Mohsen Asadnia

Outline

- ☐ Risk Analysis
- ☐ Qualitative Risk Assessment
- ☐ Quantitative Risk Assessment
- ☐ Human Reliability Assessment Techniques
- ☐ Maintenance Scheduling

Introduction (Risk Analysis)

- ❑ Risk analysis is a systematic and scientific method to predict and subsequently assist to prevent occurrence of accident in a system.
- ❑ It can be applied in all stages of design, development, construction, and operation of engineering system



Risk Analysis (Terminology)

- ❑ **Event consequence:** For an event of failure, consequences can be defined as the degree of damage or loss from a failure
- ❑ **Safety:** Safety can be defined as the judgment of risk acceptability for the system. It is based on avoidance of risk
- ❑ **Qualitative risk analysis:** The potential loss is qualitatively estimated using linguistic scales such as low, medium, high. A risk matrix is formed to categorize the level of the risk in form of frequency (or likelihood) of losses versus potential magnitude (amount) of losses in qualitative scales
- ❑ **Quantitative risk analysis:** The quantitative risk analysis attempt to estimate the risk in form of probability (or frequency) of a loss

Risk Assessment

- ❑ Risk assessment process answers three important questions:
 1. What can go wrong? : identifies the set of undesirable (e.g., incident) scenarios.
 2. What is the likelihood that it will go wrong? -Determine the probability or chances or frequencies of these scenarios.
 3. What are the consequences if it does go wrong?-Estimates the magnitude of potential losses.

Methodology

Risk assessment methodology involve following steps:

- 1. Definition of system:** Define the system boundaries and objectives of the analysis, Collect information for assessing failure likelihood, Collect information for assessing failure consequences.
- 2. Identification of hazards:** identifies the possible hazards of concern for the defined system. Example :- toxins, corrosive agents, smoke, explosions, fire, dropping or moving object.
- 3. Identification of System barriers:**
 - Physically surround and isolate the hazard (e.g., passive structures - walls, pipes, valves, fuel clad structures)
 - Minimize exposure to the hazard (e.g., protective clothing, bunkers)
 - Mitigate the hazardous condition (e.g., a cooling unit, a sprinkle system, an emergency evacuation system)



Methodology (Conti.)

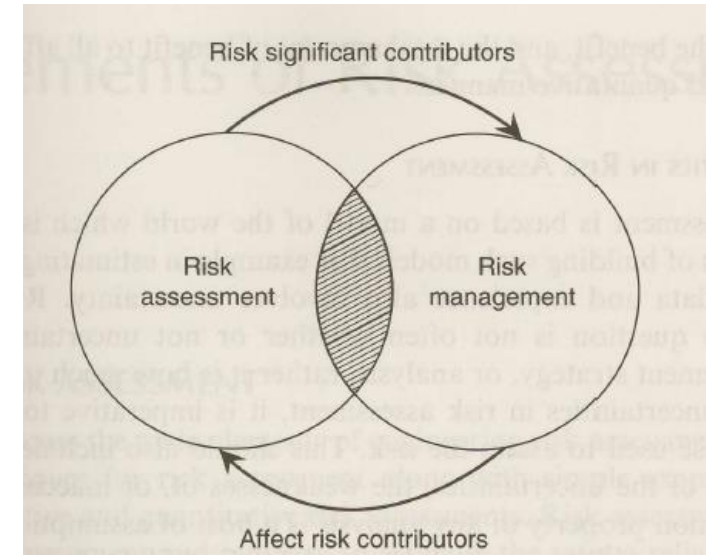
4. **Event consequence assessment:** This step involve analytical modeling tool to assess the hazard potential and subsequently translate into the potential consequences (e.g., harm to people, damage to assets, contamination of environment)
5. **Estimation of frequency (or Probability):** This step involve estimation of probability of occurrence of failure scenario and associated consequences
6. **Risk assessment and evaluation:**
 - Assess risk by combining results of previous event likelihood and event consequence steps for each failure scenario
 - Define risk acceptance criteria
 - Develop strategies to avoid hazards, failure of barriers
 - Optimize at the system level

Category: Type of Risk

- ❑ Risk categorization can be done on the basis of the causes of risk or the nature of loss (consequences) or both.
 - 1. Health risk analysis:** Determine potential diseases and losses of life affecting humans, animals, and plants.
 - 2. Safety risk analysis:** Estimate potential harms caused by accidents (climatic conditions, earthquakes, brush fire, etc.
 - 3. Security risk analysis:** Estimate access and harm caused due to war, terrorism, riot, crime
 - 4. Financial risk analysis:** Determine potential individual, institutional and societal monetary losses
 - 5. Environmental risk analysis:** Determine losses due to noise, contamination, and pollution in ecosystem

Risk Management

- **Risk management:** A practice involving coordinated activities to prevent, control, and minimizes losses incurred due to a risk exposure, weighing alternatives, and selecting appropriate actions by taking into account risk values, economic and technology constraints, legal and political issues



Relationship: Risk assessment and risk management

Uncertainty Analysis

- ❑ **Uncertainty** in risk analysis can be attributed to ambiguity, approximations and inconsistency in defining the architecture, variables, parameters and performances.
- ❑ **Uncertainty modeling** include characterization of the uncertainties, weaknesses or inaccuracies in the available data.
- ❑ Improper uncertainty characterization may lead to greater likelihood of an adverse event occurring.
- ❑ Uncertainty modeling started with the employment of safety factors that is followed by probabilistic analysis.
- ❑ Uncertainty can be classified as:
 - ❑ Objective uncertainty: It included the physical and statistical variability.
 - ❑ Subjective uncertainty: It included lack of knowledge, inconsistency in knowledge.

Qualitative Risk Assessment

Risk Matrices

- ❑ **Risk Matrices:** It is a two-dimensional presentation of likelihood and consequences of risk estimation. Qualitative scales for both dimensions to characterize the risk by categorizing probabilities and consequences on the two axes of a matrix.
- ❑ **Example**

Possibility Category	A	L	M	M	H	H	H
	B	L	L	M	M	H	H
	C	L	L	L	M	M	H
	D	L	L	L	L	M	M
	E	L	L	L	L	L	M
	F	L	L	L	L	L	L
		VI	V	IV	III	II	I
	Consequence Category						



HAZard and OPerability (HAZOP) study

- ❑ Hazards arise in a plant due to deviations from normal behavior.
- ❑ HAZOP study gives insight into the hazards that are present in the plant.
- ❑ A comprehensive HAZOP analysis identifies the all possible hazards and operability problems, recommended changes and studies etc.

- ❑ **Required Information**
 - ❑ Up-to-date process flow diagrams (PFDs)
 - ❑ Process and instrumentation diagrams (P&IDs)
 - ❑ Detailed equipment specifications, materials of construction, and mass and energy balances
 - ❑ A team of experts having a cross-section of experienced plant, laboratory, technical, and safety professionals..

HazOp Guide Word

- ❑ Simple words that are combined with the process parameters/variables to identify:
 - ❑ Any perceived **Deviations** from intended design/operation
 - ❑ The **Causes** of those perceived deviations
 - ❑ The **Consequences** of those perceived deviations
 - ❑ **Safeguards** to prevent causes and mitigate
 - ❑ Consequences of the perceived deviations
 - ❑ Recommended **Actions** (recommendations) in design or operation modification to improve safety and operability of the plant.



Procedure of HazOp Study

1. Discrete the PFDs and P&IDs into a number of small process units.
2. Select a study node.
3. Illustrate the design intent of the study node.
4. Choose a specific process parameter.
5. Combines a guide word with process parameter to suggest possible deviations.
6. Find the possible causes and note any protective systems for the deviation.
7. Examine the probable consequences for the deviation (if any).
8. Recommend the probable action item (what? by whom? by when?)
9. Record all information in to the HazOp report.



HazOp Parameters

Guide words	Meaning	Parameters
No, Not, None	The complete negation of intention	Flow and Concentration
More, Higher, Greater	Quantitative increase	Flow, Temperature, Pressure, Concentration, pH, Viscosity, & State
Less, Lower	Quantitative decrease	Flow, Temperature, Pressure, Concentration, pH, Viscosity, & State
As Well As	Qualitative increase	Flow, Pressure, Concentration, State
Part of	Qualitative decrease	Flow, Concentration
Reverse	The logical opposite of	Flow
Other Than	Complete substitution	Flow, Concentration
Sooner Than	Too early or in the wrong order	Flow, Temperature, Pressure, Concentration, pH, Viscosity, & State
Later Than	Too late or in wrong Order	Flow, Temperature, Pressure, Concentration, pH, Viscosity, & State
Where Else	In additional location	

HazOp Report

HazOp Report Format

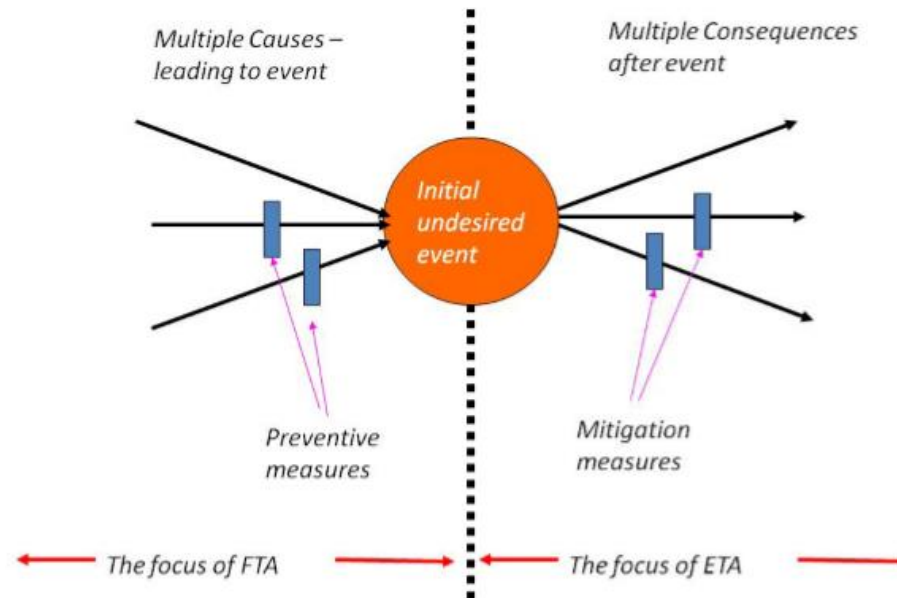
Deviation	Cause	Consequence	Safeguards	Action

Quantitative Risk Analysis

- ❑ QRA is a technique used to quantify the risk associated with a particular hazard
- ❑ Different techniques available for QRA, however, Fault Tree Analysis, Event Tree Analysis, and Bow-tie Analysis are the famous and user-friendly ones that are discussed here

Fault Tree Analysis (FTA) & Event Tree Analysis (ETA)

- ❑ Fault Tree (FT) and Event Tree (ET) two are in fact complimentary (and are often used together) but focus on opposite sides of an undesired event



Integration of FTA and ETA is called “Bow-tie Analysis”

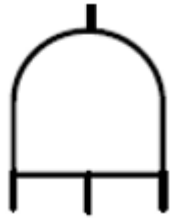


Fault Tree Analysis (FTA)

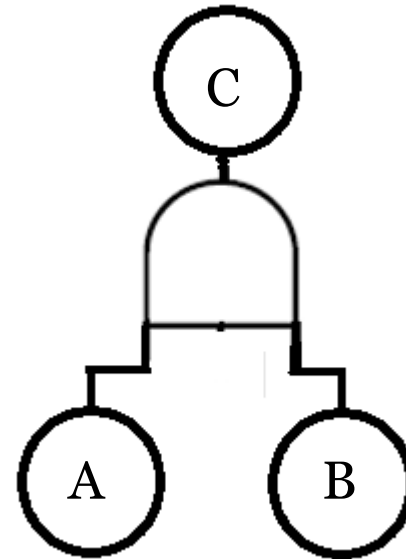
- ❑ It defines multiple causes leading to an undesired event
- ❑ Used in accident investigation and in a detailed hazard assessment
- ❑ FT is a logic diagram based on the principle of multi-causality defining all branches of events which could contribute to an accident or failure
- ❑ The relation between causes and an undesired event in FT is based on Boolean algebra basic operators

Operators in FTA

(AND Gate)



AND Gate (output exists only if all inputs exist)



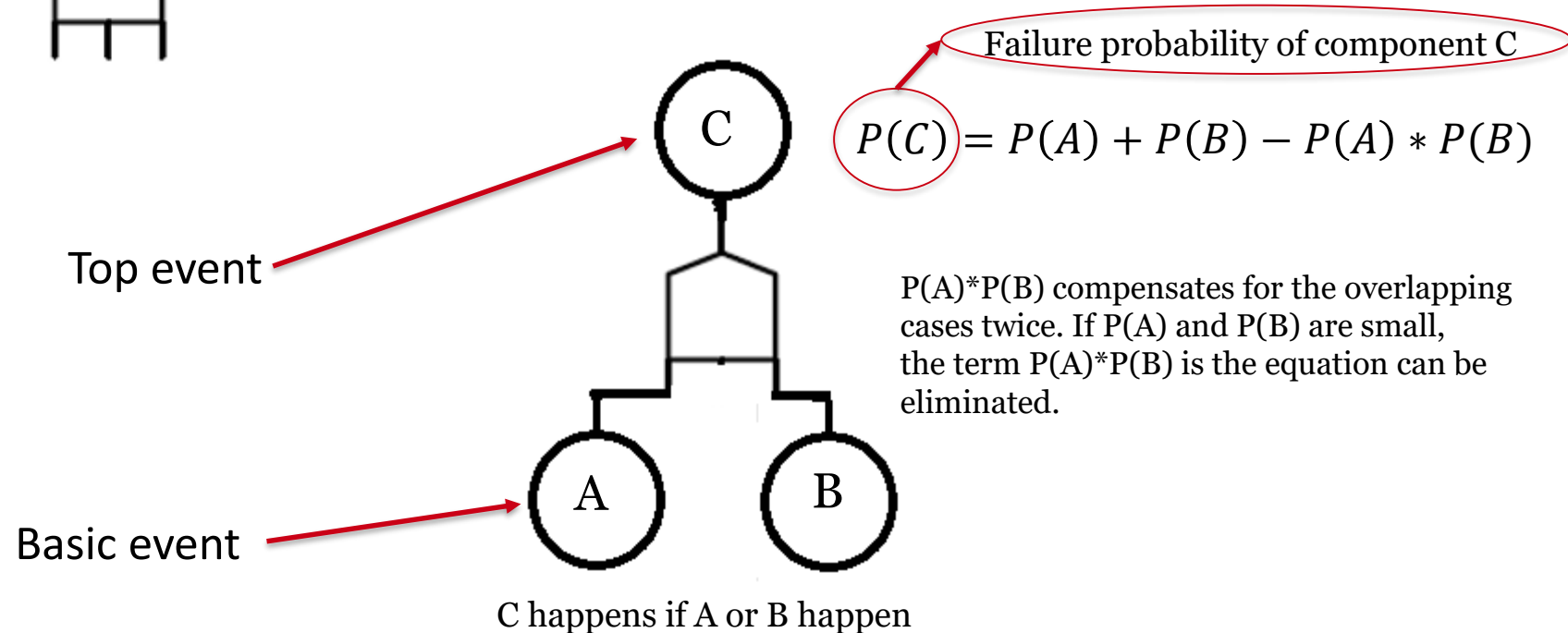
C happens if both A and B happen

For example, you **get virus** if you are **not careful** and you are in **contact with a sick person**

Operators in FTA (OR Gate)



OR Gate (output exits only if one input exists)



For example, you **get sick** if you **walk in a cold weather** or you are in **contact with a sick person**

Operators in FTA

OR GATE



If we have more components that are connected with the OR Gate:

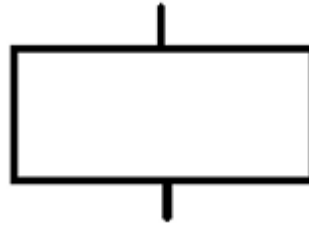
$$P = 1 - \prod_{i=1}^n (1 - P_i)$$

The above equation simply means the probability of A OR B OR C is:

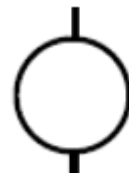
$$1 - (1 - P_A)(1 - P_B)(1 - P_C)$$

Operators in FTA

RECTANGLE AND CIRCLE



Fault event usually resulting from more basic fault event (It is a useful operator when we have a very large FT and we can break it to the different smaller FTs and integrate them with this operator)



Primary basic event

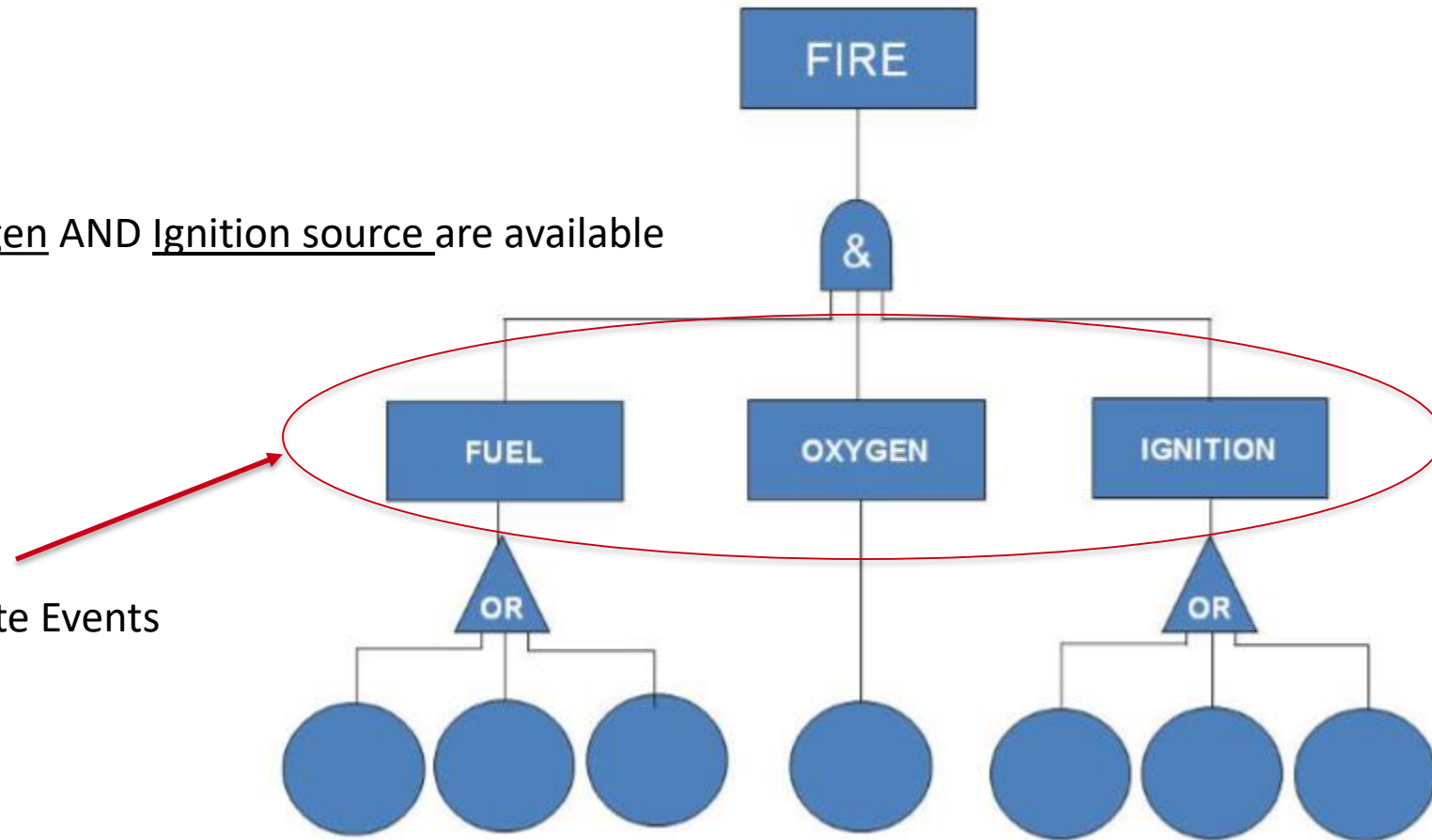
FTA (Probability Estimation)

VIA EXAMPLE

Fire occurs if:

Fuel AND Oxygen AND Ignition source are available

Intermediate Events

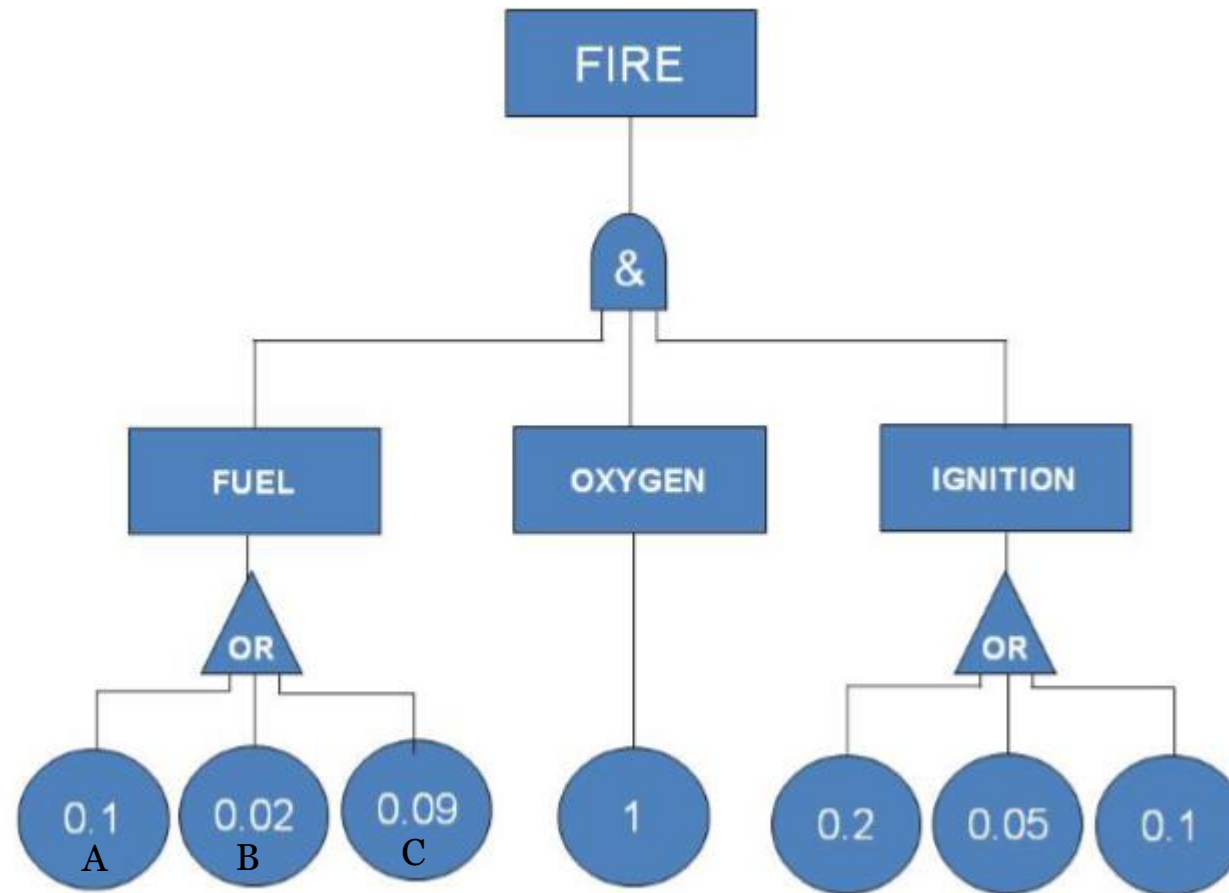


FTA (Probability Estimation)

VIA EXAMPLE



Let's assume fuel is released because of **any** three different failures and the probabilities of these failures are 0.1, 0.02 and 0.09. Simply means if A or B or C fails, fuel is released.



We assign probability of 1 to oxygen as it is always available in the air

FTA (Probability Estimation)

VIA EXAMPLE



- ❑ Add the probabilities which sit below an OR gate (this isn't strictly correct, but is a 'rare event' approximation)
- ❑ Multiply the probabilities which sit below an AND gate

In this example, combining probabilities upwards to the next level gives:

- ❑ Probability of FUEL being present = $0.1 + 0.02 + 0.09 = 0.21$
- ❑ Probability of OXYGEN being present = 1
- ❑ Probability of IGNITION being present = $0.2 + 0.05 + 0.1 = 0.35$

So, the probability of fire to happen:

- ❑ $0.21 * 1 * 0.35 = 0.0735$ (So, the probability of the top event which is the fire in this example is 0.0735)

Event Tree Analysis (ETA)

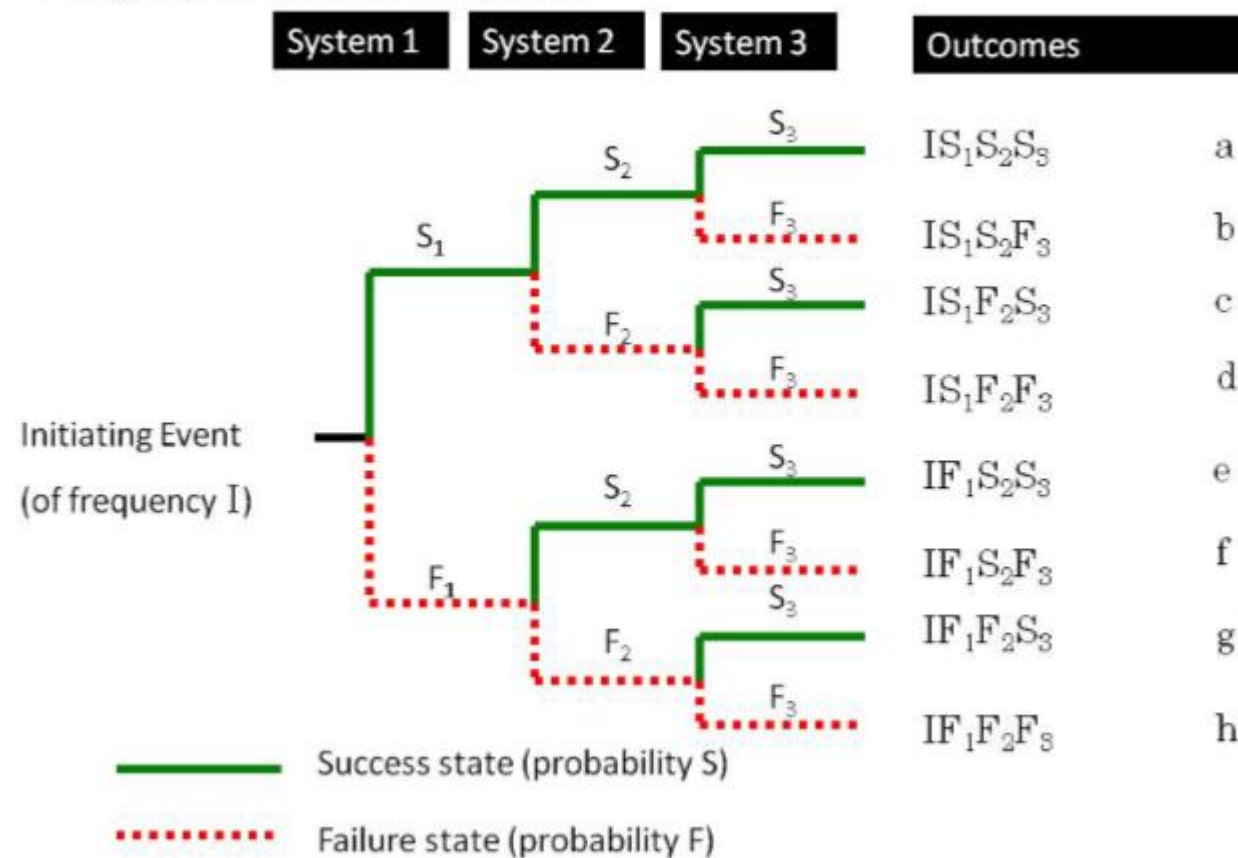
- ❑ An ETA defines the consequential events which flow from the primary 'initiating' event
- ❑ It uses to investigate the consequences of loss-making events in order to find ways of mitigating, rather than preventing, losses

Different steps in an ETA:

1. Identify the primary event of concern
2. Identify the controls that are assigned to deal with the primary event such as automatic safety systems, alarms on operator actions
3. Construct the event tree beginning with the initiating event and proceeding through failures of the safety functions
4. Establish the resulting accident sequences
5. Identify the critical failures that need to be addressed

ETA (Generic Example)

3 stage system failure sequence

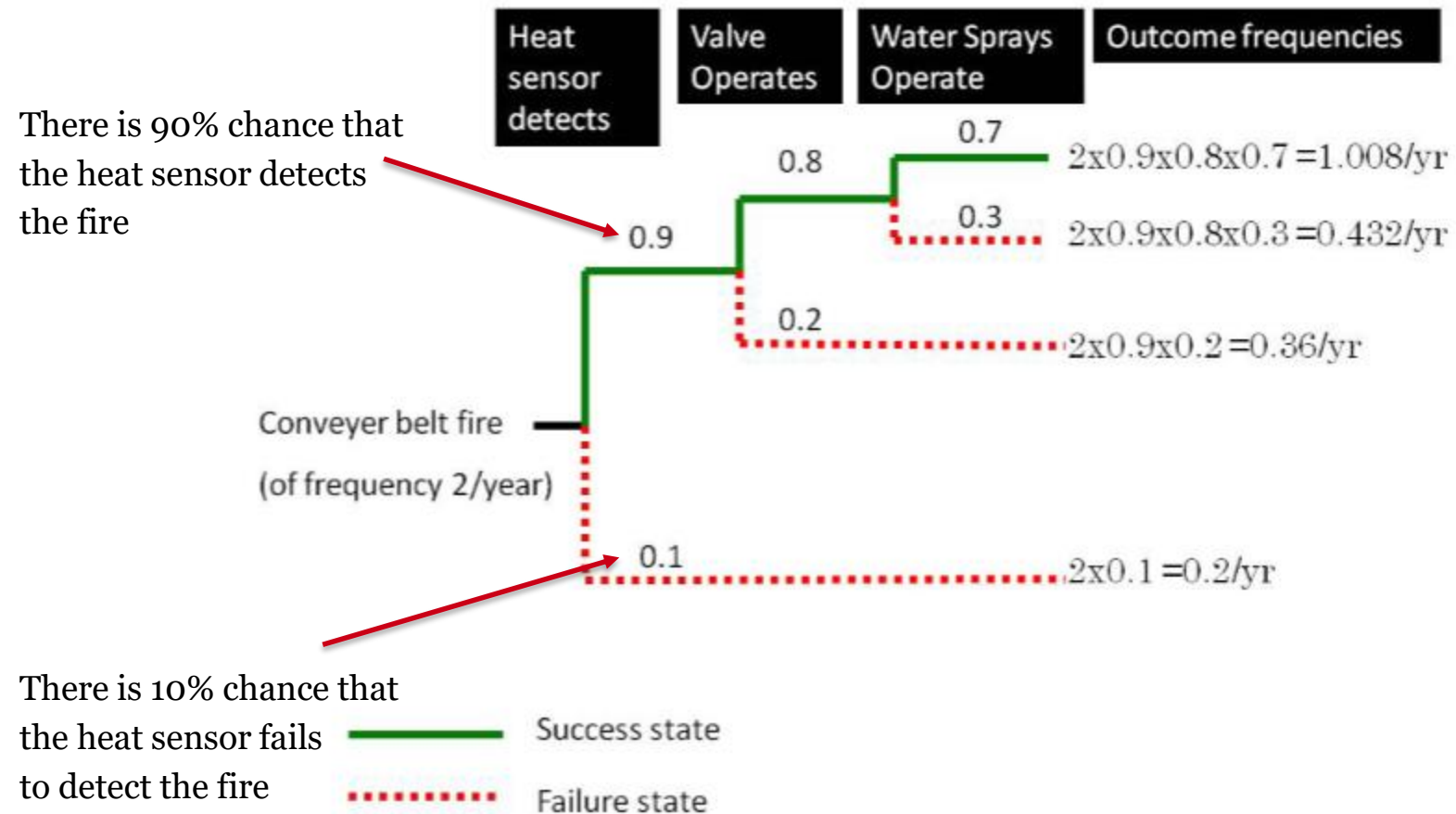


IN THE PREVIOUS GENERIC EXAMPLE OF AN ETA

- ❑ To calculate the frequency of each final outcome (labelled a to h in the diagram), you multiply along the branches, travelling from left to right from initiating event to final outcome. Thus, from the diagram, the frequency of the initiating event happening AND systems 1 AND 2 AND 3 working properly is $I \times S1 \times S2 \times S3$.
- ❑ The sum of each success/failure probability pair, at each specific node adds up to 1. So, for example, $S1 + F1 = 1$. This means that if you are only given the value for success probability of a particular system, it is easy to calculate the failure probability for that same system, because the two will add up to give 1.



ETA Example

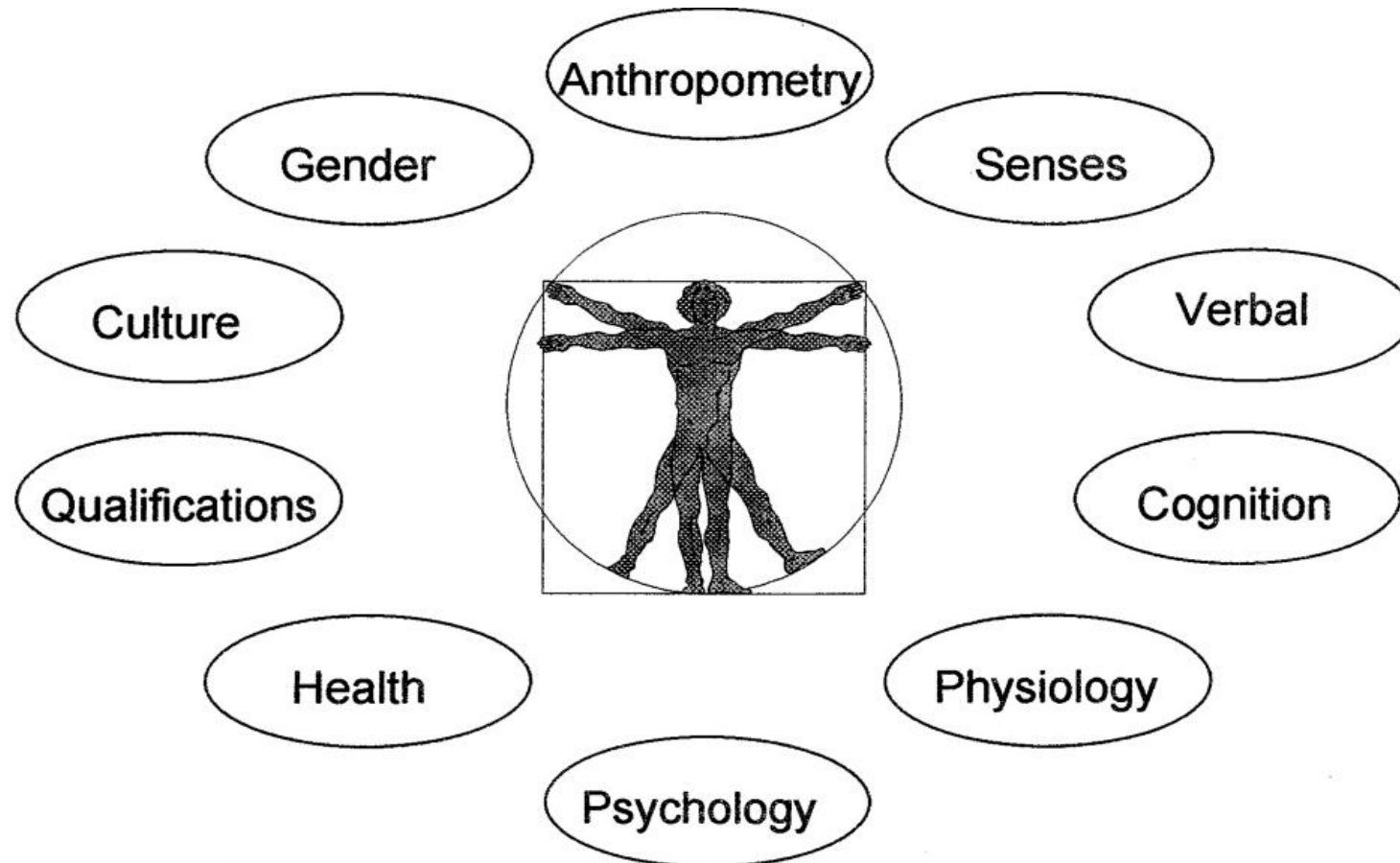


Human Factors

- ❑ Human Factors is the branch of engineering concerned with human efficiency and safety in man-machine system
- ❑ Human Factors deals with the psychological, social, physical, biological and safety characteristics of a user and the system the user is in
- ❑ **Goals:** making human interaction with the system such that
 - ✓ Reduce errors
 - ✓ Increase production
 - ✓ Enhance safety and comfort



Model of a Human





Important attributes of Human

Anthropometry

- Height
- Weight
- Reach
- Hand size

Senses

- Vision
- Color-blindness
- Hearing
- Kinesthetics

Verbal skills

Cognition

- Attention
- Decision making
- Diagnosis
- Information processing
 - Quality
 - Speed
- Judgement
- Language skills
- Memory
- Mental workload capacity
- Perception
- Problem solving
- Reading ability
- Reasoning
- Recognition
- Thinking

Physiology

- Motor skills
 - Reaction time
 - Speed of movement
 - Regulation of movement
- Strength (static and dynamic)

Dexterity

- Stamina
- Physical workload capacity
- Physical conditioning

Psychology

- Aptitude
- Attitudes
- Beliefs
- Biases
- Emotions
- Feelings
- Habits
- Moods
- Motivation
- Perception
- Personality
- Stress

Medical and health

- Side effects from prescription drugs
- Drug or alcohol abuse
- Ill health or stress
- Handicaps
- Aging factors

Qualifications

- Education
- Experience
- Knowledge
- Skills
- Training

Culture

Gender

Human Error

- ❑ is an inappropriate or undesirable human decision or behaviour that reduces or has the potential for reducing the:
 - ❑ effectiveness
 - ❑ safety
 - ❑ system performance

Human Error Classification

Discrete Action Classifications

- ❑ One of the simplest (Swain & Guttman 1983)
- ❑ Errors of omission - forget to do something
- ❑ Errors of commission - doing the task incorrectly
- ❑ Sequence errors - out of order
- ❑ Timing errors - too slow - too fast - too late

Human Error Classification

Errors depend on the type of behaviour involved

☐ Skill-based

- Controlled by sub-conscious behavior and stored patterns of behavior
- Errors usually errors of execution

☐ Rule-based (incorrect application of a good rule)

- Applies to familiar situations - stored rules are applied
- Errors involve recognizing the salient features of the situation

☐ Knowledge-based

- Errors result from inadequate analysis or decision making

Human Error Probability (HEP)

- ❑ Human error quantification techniques all involve the calculation of human error probability which is the measure of human reliability assessment (HRA)

- ❑ The goal of HEP is (Skelton, 1997):
 - ❑ Preventing of death or injury of the workers
 - ❑ Preventing of death or injury to the general public
 - ❑ Avoiding damage to a plant
 - ❑ Stopping any harmful effects on the environment
 - ❑ Preventing damage to third parties

Available Techniques to Estimate HEP

Some Available techniques:

- ☐ Success likelihood index method (SLIM)
- ☐ Human error assessment and reduction technique (HEART)
- ☐ Absolute probability judgment (APJ)
- ☐ Paired comparison
- ☐ Technique for human error rate prediction (THERP)

Success likelihood Index Method (SLIM)

Purpose: Evaluating the probability of a human error occurring throughout the completion of a specific task

Outcome: Measures to reduce the likelihood of errors occurring within a system and therefore lead to an improvement in the overall levels of safety

Success likelihood Index Method (SLIM)



MACQUARIE
University

PROCEDURES

Step 1: The selection of the expert panel

Step 2: The definition of situations and subsets

Step 3: The elicitation of PSFs

Step 4: The rating of the tasks on the PSF scale

Step 5: PSF weighting

Step 6: The calculation of Success Likelihood Index (SLIs)

Step 7: Conversion of SLIs into probabilities



Success likelihood Index Method (SLIM)

SLI CALCULATION

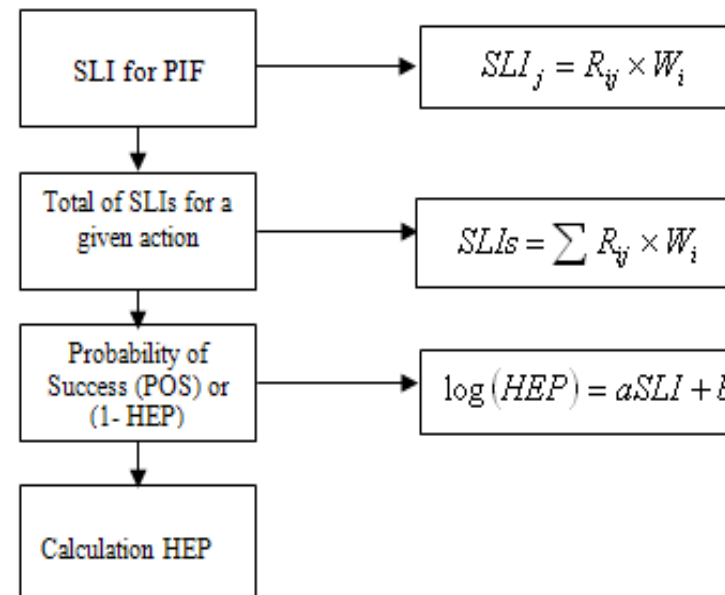
$$SLI_j = SUM (R_{ij} \times W_i) \text{ for } i = 1 \text{ to } i = x$$

Where: SLI_j = Success likelihood index for task j

W_i = Normalized importance weighting for the i th PSF

R_{ij} = (Scaled) rating of task j on the i th PSF

x = The number of PSFs considered



Success likelihood Index Method (SLIM)

EXAMPLE

Step 1: A production facility employs sensors to monitor process operations (e.g. temperature, vibration, etc.). An operator with a minimum 10 years of experience, who is a mechatronic engineer and is very familiar with the process failed to calibrate Sensor T0201 correctly. This resulted in inaccurate temperature readings, leading to overheating of a machine and its subsequent breakdown. A sensor, S0301, used to detect product defects malfunctioned. The root cause was the omission of routine maintenance checks. Finally, a sensor system installed to monitor equipment vibration levels (Sensor V0401) detected excessive vibrations in a critical machine. The operator, preoccupied with other tasks, ignored the warning.

Step 2: Possible human errors:

Failed to calibrate Sensor T0201 (H1)

Omission of routine maintenance checks for Sensor S0301(H2)

Ignore the warning of sensor V0401 (H3)

Success likelihood Index Method (SLIM)

EXAMPLE

Step 3: 5 PSFs identified: Training, Procedures, Feedback, The perceived level of risk and Time pressure involved

Step 4: PSF rating

<i>Errors</i>	<i>Training</i>	<i>Procedures</i>	<i>Feedback</i>	<i>Perceived risk</i>	<i>Time</i>
H1	6	5	2	9	6
H2	5	3	2	7	4
H3	4	5	7	7	2

Step 5: PSF weighting

<i>PSF</i>	<i>Importance</i>
Training	0.15
Procedures	0.15
Feedback	0.3
Perceived risk	0.3
Time	0.10
Sum	1.00

Success likelihood Index Method (SLIM)

EXAMPLE

Step 6: SLI calculation

<i>PSFs</i>	<i>Rating</i>	<i>Weighting</i>	<i>SLI (H1)</i>
Training	6	0.15	0.9
Procedures	5	0.15	0.75
Feedback	2	0.3	0.6
Perceived risk	9	0.3	2.7
Time	6	0.10	0.6
Total SLI			5.55

Calculate for H2 and H3?

Success likelihood Index Method (SLIM)

EXAMPLE

Step 6: SLI calculation (Cont.)

<i>PSFs</i>	<i>H1</i>	<i>H2</i>	<i>H3</i>
Training	0.9	0.75	0.6
Procedures	0.75	0.45	0.75
Feedback	0.6	0.6	2.1
Perceived risk	2.7	2.1	2.1
Time	0.6	0.4	0.2
Total SLI	5.55	4.3	5.75

Success likelihood Index Method (SLIM)

EXAMPLE

Step 7: Calculating HEP

$$\text{Log} (HEP) = a (SLI) + b$$

Two additional tasks X and Y were assessed, which had HEP values of 0.5 and 10^{-4} respectively and SLIs respectively of 4.00 and 6.00

Solve these two equations to find a and b

Finally, $\text{Log} (HEP) = -1.85 * SLI + 7.1$

Calculated HEPs are:

$$HEP1 = 0.0007$$

$$HEP2 = 0.14$$

$$HEP3 = 0.0003$$

Human Error Assessment & Reduction Technique (HEART)

Step 1: Identifying the full range of sub-tasks.

Step 2: Determining a nominal human unreliability score for the particular task by consulting with local experts.

Step 3: Determining the error-producing conditions (EPCs), which are apparent in the given situation and highly probable to have a negative effect on the outcome. Get the total HEART effect of each EPC.

Step 4: Get experts' assessed proportion of effect (from 0 to 1).

Step 5: Calculate effect = $((\text{Max effect} - 1) \times \text{Proportion of effect}) + 1$

Step 6: Calculate final HEP as a product of all calculated effect and nominal human unreliability.

Human Error Assessment & Reduction Technique (HEART)



GENERIC TASK UNRELIABILITY

<i>Generic task</i>		<i>Proposed nominal human unreliability (5th–95th percentile boundaries)</i>
A	Totally unfamiliar, performed at speed with no real idea of likely consequences	0.55 (0.35–0.97)
B	Shift or restore system to a new or original state on a single attempt without supervision or procedures	0.26 (0.14–0.42)
C	Complex task requiring high level of comprehension and skill	0.16 (0.12–0.28)
D	Fairly simple task performed rapidly or given scant attention	0.09 (0.06–0.13)
E	Routine, highly practised, rapid task involving relatively low level of skill	0.02 (0.007–0.045)
F	Restore or shift a system to original or new state following procedures, with some checking	0.003 (0.0008–0.007)
G	Completely familiar, well-designed, highly practised, routine task occurring several times per hour, performed to highest possible standards by highly motivated, highly trained and experienced person, totally aware of implications of failure, with time to correct potential error, but without the benefit of significant job aids	0.0004 (0.00008–0.009)
H	Respond correctly to system command even when there is an augmented or automated supervisory system providing accurate interpretation of system stage	0.00002 (0.000006–0.00009)
M	Miscellaneous task for which no description can be found. (Nominal 5th to 95th percentile data spreads were chosen on the basis of experience suggesting log-normality)	0.03 (0.008–0.11)

Human Error Assessment & Reduction Technique (HEART)

ERROR PRODUCING CONDITIONS



Error-producing condition	Maximum predicted nominal amount by which unreliability might change going from 'good' conditions to 'bad'
1. Unfamiliarity with a situation which is potentially important but which only occurs infrequently or which is novel	× 17
2. A shortage of time available for error detection and correction	× 11
3. A low signal-to-noise ratio	× 10
4. A means of suppressing or overriding information or features which is too easily accessible	× 9
5. No means of conveying spatial and functional information to operators in a form which they can readily assimilate	× 8
6. A mismatch between an operator's model of the world and that imagined by the designer	× 8
7. No obvious means of reversing an unintended action	× 8
8. A channel capacity overload, particularly one caused by simultaneous presentation of non-redundant information	× 6
9. A need to unlearn a technique and apply one which requires the application of an opposing philosophy	× 6
10. The need to transfer specific knowledge from task to task without loss	× 5.5
11. Ambiguity in the required performance standards	× 5
12. A mismatch between perceived and real risk	× 4
13. Poor, ambiguous or ill-matched system feedback	× 4
14. No clear direct and timely confirmation of an intended action from the portion of the system over which control is to be exerted	× 3
15. Operator inexperienced (e.g. a newly qualified tradesman, but not an 'expert')	× 3
16. An impoverished quality of information conveyed by procedures and person-person interaction	× 3
17. Little or no independent checking or testing of output	× 3
18. A conflict between immediate and long-term objectives.	× 2.5
19. No diversity of information input for veracity checks	× 2.5
20. A mismatch between the educational achievement level of an individual and the requirements of the task	× 2
21. An incentive to use other more dangerous procedures	× 2
22. Little opportunity to exercise mind and body outside the immediate confines of the job	× 1.8
23. Unreliable instrumentation (enough that it is noticed)	× 1.6
24. A need for absolute judgements which are beyond the capabilities or experience of an operator	× 1.6
25. Unclear allocation of function and responsibility	× 1.6
26. No obvious way to keep track of progress during an activity	× 1.4
27. A danger that finite physical capabilities will be exceeded	× 1.4
28. Little or no intrinsic meaning in a task	× 1.4
29. High-level emotional stress	× 1.3
30. Evidence of ill-health amongst operatives, especially fever	× 1.2
31. Low workforce morale	× 1.2
32. Inconsistency of meaning of displays and procedures	× 1.2
33. A poor or hostile environment (below 75% of health or life-threatening severity)	× 1.15
34. Prolonged inactivity or highly repetitious cycling of low mental workload tasks	× 1.1 for first half-hour × 1.05 for each hour thereafter
35. Disruption of normal work-sleep cycles	× 1.1
36. Task pacing caused by the intervention of others	× 1.06
37. Additional team members over and above those necessary to perform task normally and satisfactorily	× 1.03 per additional man
38. Age of personnel performing perceptual tasks	× 1.02

EXAMPLE

An engineer has the task of assessing the probability of a plant operator failing to carry out the task of **isolating a plant bypass route as required by procedure**. However, the operator is fairly inexperienced in fulfilling this task and therefore typically does not follow the correct procedure; the individual is therefore unaware of the hazards created when the task is carried out

Human Error Assessment & Reduction Technique (HEART)

EXAMPLE

From the relevant tables, it can be established that the type of task in this situation is of the type (F) which is defined as “**Restore or shift a system to original or new state following procedures, with some checking**”. This task type has the proposed nominal human unreliability value of **0.003**

Human Error Assessment & Reduction Technique (HEART)

EXAMPLE

Error producing conditions (EPCs)	Total HEART effect	Assessed proportion of effect	Assessed effect
<i>Inexperience</i>	X 3	0.4	$(3-1)*0.4+1=1.8$
<i>Opposite technique</i>	X 6	1.0	$(6-1)*1+1=6$
<i>Risk Misperception</i>	X 4	0.8	$(4-1)*0.8+1=3.4$
<i>Conflict of Objectives</i>	X 2.5	0.8	$(2.5-1)*0.8+1=2.2$
<i>Low morale</i>	X 1.2	0.6	$(1.2-1)*0.6+1=1.12$

The final calculation for the normal likelihood of failure can therefore be formulated as:
 $0.003 \times 1.8 \times 6.0 \times 3.4 \times 2.2 \times 1.12 = 0.27$

Human Error Assessment & Reduction Technique (HEART)

HEART ADVANTAGES

- ❑ HEART is very quick and straightforward to use and also has a small demand for resource usage
- ❑ The technique provides the user with useful suggestions as to how to reduce the occurrence of errors

Reducing Accidents

ATTENDING TO HUMAN ERRORS



MACQUARIE
University

- ▶ Apply HF principles to design
- ▶ Provide procedural checklists
- ▶ Provide training
- ▶ Provide appropriate & meaningful feedback
- ▶ Incentive programs
- ▶ Eliminate/reduce risk through design



Home Work Activity

TEAM DISCUSSION



MACQUARIE
University

Case Study: Human Errors in an Industrial Robotic Assembly Line

Background:

In a modern manufacturing facility, an industrial robotic assembly line is used to automate the assembly of complex electronic devices. The mechatronic system consists of various robots, conveyor belts, sensors, and quality control stations.

Please discuss:

- ☐ How each human error contributed to system failures and operational issues.
- ☐ The financial and operational impact of these errors.
- ☐ What preventive measures or system design changes could have mitigated or prevented these errors.

Example: Programming Error: An operator responsible for updating the robotic assembly line's programming accidentally uploaded the wrong program. This program contained incorrect assembly instructions, leading to a significant deviation from the product's specifications.

Consequence: Production was significantly delayed, leading to financial losses.

Maintenance

- The technical meaning of maintenance involves functional checks, servicing, repairing or replacing of necessary devices, equipment, machinery, building infrastructure, and supporting utilities
- Maintenance is often the largest controllable operating cost in different industries

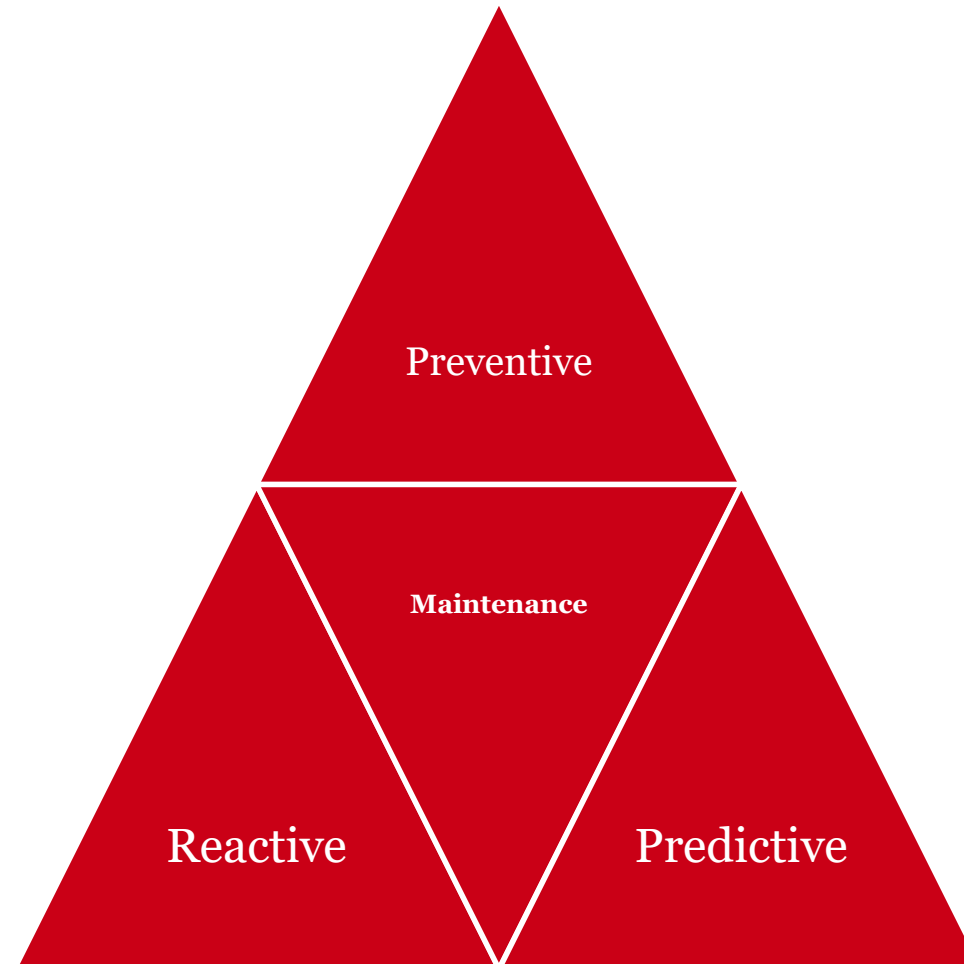


Maintenance

DIFFERENT TYPES



MACQUARIE
University



REACTIVE MAINTENANCE

- ❑ Reactive maintenance is basically the “run it till it breaks” maintenance mode.
- ❑ No actions or efforts are taken to maintain the equipment as the designer originally intended to ensure design life is reached.

Advantages

- Low cost
- Less staff

Disadvantages

- Increased cost due to unplanned downtime of equipment
- Increased labour cost, especially if overtime is needed
- Cost involved with repair or replacement of equipment
- Possible secondary equipment or process damage from equipment failure
- Inefficient use of staff resources

Maintenance

PREVENTIVE MAINTENANCE

- ❑ In preventive maintenance, actions performed on a time- or machine-run-based schedule that detect, preclude, or mitigate degradation of a component or system with the aim of sustaining or extending its useful life through controlling degradation to an acceptable level
- ❑ By performing the preventive maintenance as the equipment designer envisioned, we will extend the life of the equipment closer to design



Maintenance

PREVENTIVE MAINTENANCE

Advantages

- ☐ Cost effective in many capital intensive processes
- ☐ Flexibility allows for the adjustment of maintenance periodically
- ☐ Increased component life cycle
- ☐ Energy saving
- ☐ Reduce equipment or process failure
- ☐ Estimated 12 to 18% cost savings over reactive maintenance program

Disadvantages

- ☐ Catastrophic failure still likely to occur
- ☐ Labor intensive
- ☐ Includes performance of unneeded maintenance
- ☐ Potential for incidental damage to components in conducting unneeded maintenance

Maintenance

PREDICTIVE MAINTENANCE

Predictive maintenance is defined as the measurements that detect the onset of system degradation (lower functional state), thereby allowing causal stressors to be eliminated or controlled prior to any significant deterioration in the component physical state.

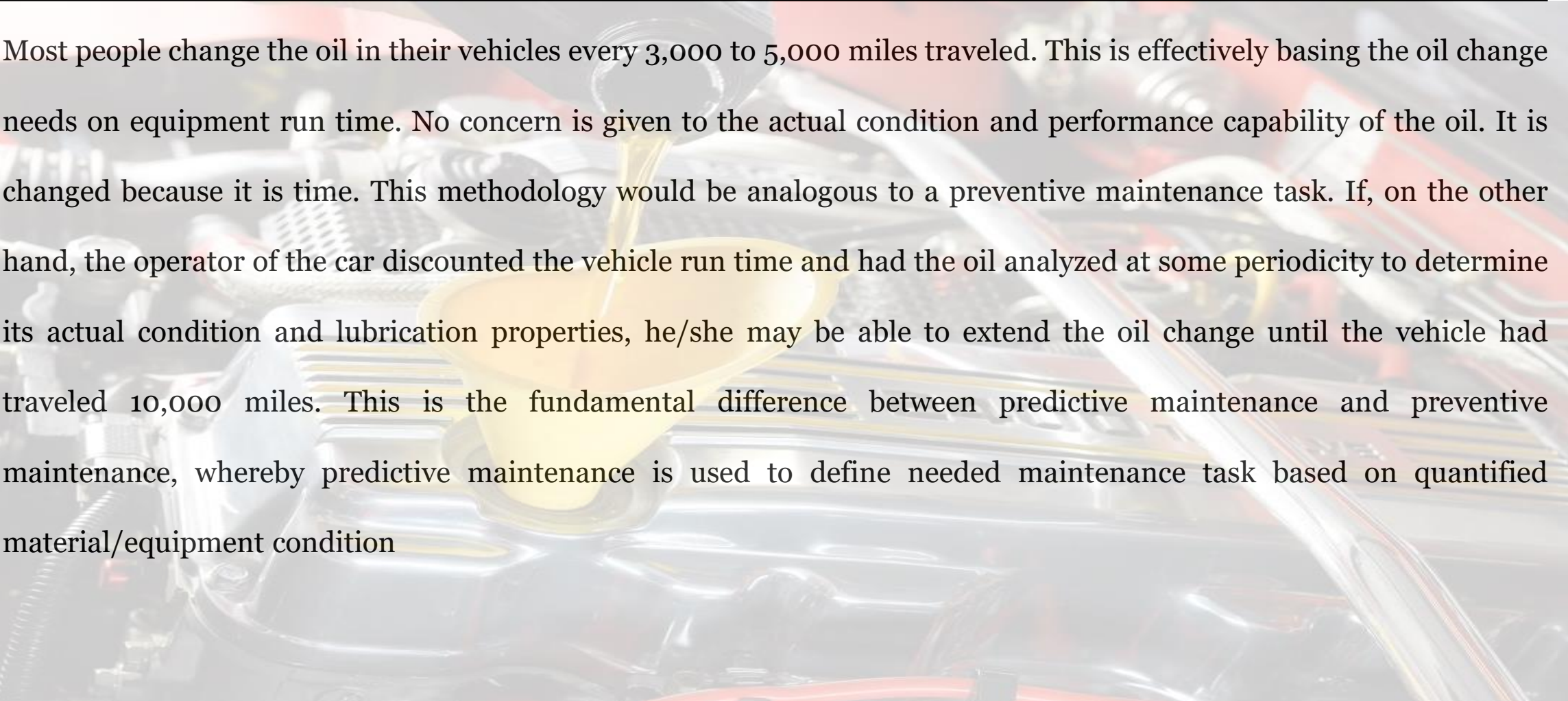
Results indicate current and future functional capability

Basically, predictive maintenance differs from preventive maintenance by basing maintenance need on the actual condition of the machine rather than on some pre-set schedule.



Maintenance

PREDICTIVE MAINTENANCE - EXAMPLE



Most people change the oil in their vehicles every 3,000 to 5,000 miles traveled. This is effectively basing the oil change needs on equipment run time. No concern is given to the actual condition and performance capability of the oil. It is changed because it is time. This methodology would be analogous to a preventive maintenance task. If, on the other hand, the operator of the car discounted the vehicle run time and had the oil analyzed at some periodicity to determine its actual condition and lubrication properties, he/she may be able to extend the oil change until the vehicle had traveled 10,000 miles. This is the fundamental difference between predictive maintenance and preventive maintenance, whereby predictive maintenance is used to define needed maintenance task based on quantified material/equipment condition

Maintenance

PREDICTIVE MAINTENANCE - EXAMPLE

Advantages

- Increase component operational life/availability
- Allows for predictive corrective action
- Decrease in cost for parts and labours
- Better product quality
- Improved worker and environmental safety
- Improved worker morale
- Energy saving
- Estimated 8% to 12% cost savings over preventive maintenance program

Disadvantages

- Increased investment in diagnostic equipment
- Increased investment in staff training
- Saving potential not readily seen by management



RISK-BASED MAINTENANCE

- ❑ Risk-based maintenance (RBM) prioritizes maintenance resources toward assets that carry the most risk if they were to fail
- ❑ RBM helps in determining the most economical use of maintenance resources
- ❑ A risk-based maintenance strategy is based on two main phases:
 - ❖ Risk assessment
 - ❖ Maintenance planning based on the risk

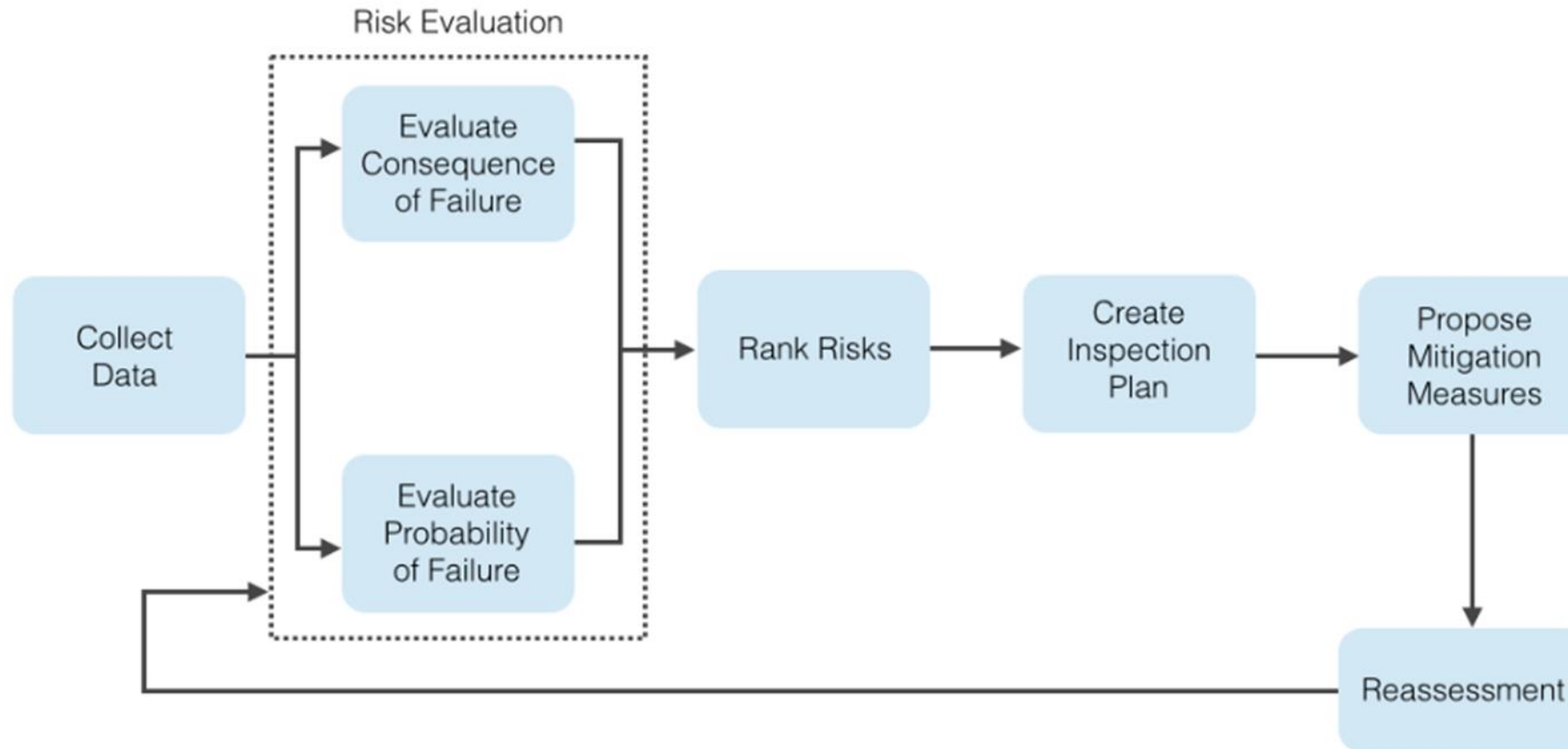
Assets that have a greater risk and consequence of failure are maintained and monitored more frequently

Risk-based Maintenance



MACQUARIE
University

FRAMEWORK



Failure Rate

- ❑ Data are collected on the failure rate of a particular component
- ❑ With adequate data, it can be shown that, on average, the component fails after a certain period of time
- ❑ This is called average failure rate and is represented by μ with units of faults/time
- ❑ The probability that the component is not fail during the time interval (0,t) (called reliability) is given by a Poisson distribution as below

$$R(t) = e^{-\mu t}$$

As $t \rightarrow \infty$, the reliability goes to 0

Failure Rate Data



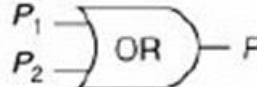

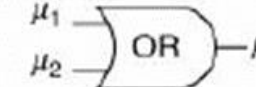


EXAMPLE FOR A FEW SELECTED PROCESS COMPONENTS

Instrument	Faults/year
Controller	0.29
Control valve	0.60
Flow measurement (fluids)	1.14
Flow measurement (solids)	3.75
Flow switch	1.12
Gas-liquid chromatograph	30.6
Hand valve	0.13
Indicator lamp	0.044
Level measurement (liquids)	1.70
Level measurement (solids)	6.86
Oxygen analyzer	5.65
pH meter	5.88
Pressure measurement	1.41
Pressure relief valve	0.022
Pressure switch	0.14
Solenoid valve	0.42
Stepper motor	0.044
Strip chart recorder	0.22
Thermocouple temperature measurement	0.52
Thermometer temperature measurement	0.027
Valve positioner	0.44

Reliability



SYSTEMS IN SERIES AND PARALLEL

Failure Probability	Reliability	Failure Rate
 $P = 1 - (1 - P_1)(1 - P_2)$ $P = 1 - \prod_{i=1}^n (1 - P_i)$ <p>Series link of components:</p>	 $R = R_1 R_2$ $R = \prod_{i=1}^n R_i$ <p>The failure of either component adds to the total system failure.</p>	 $\mu = \mu_1 + \mu_2$ $\mu = \sum_{i=1}^n \mu_i$
 $P = P_1 P_2$ $P = \prod_{i=1}^n P_i$ <p>Parallel link of components:</p>	 $R = 1 - (1 - R_1)(1 - R_2)$ $R = 1 - \prod_{i=1}^n (1 - R_i)$ <p>The failure of the system requires the failure of both components. Note that there is no convenient way to combine the failure rate.</p>	$\mu = (-\ln R)/t$

Failure Probability

❑ Exponential Distribution – Constant Failure Rate

$$\lambda(t) = \text{constant} = \lambda$$

which leads to

$$R(t) = \exp(-\lambda t)$$

$$F(t) = 1 - \exp(-\lambda t)$$

This is the simplest failure rate assumption and leads to the time to failure having a negative exponential distribution. It is appropriate when system failure is caused by environmental effects (severe winds, storms, floods, earthquakes) or when wearing in and wearing out are not issues (perhaps because only the early operation/maintenance period is being considered). It is also commonly used simply because it is the easiest mathematical form.

Maintenance Scheduling

BASED ON A FAILURE PROBABILITY



Consider the below equation:

$$P(t) = 1 - e^{-\mu t}$$

The maintenance interval (t) required to achieve the target probability

$$t = \frac{-\ln(1 - P(t))}{\mu}$$

So, if we know the probability of failure (P(t)) for a component and the failure rate (μ), it is possible to estimate the time required for the maintenance from the above equation. The component should be maintained before the failure occurs.

Example

Assume the failure rate of a critical component is $1.5 \times 10^{-5}/\text{year}$, and the failure probability considering the failures of its sub-components is estimated to be 1.0269×10^{-6} . What is the optimal time for maintenance inspection of the support beam?

$$t = \frac{-\ln(1-P(t))}{\mu}$$