PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
TAHRI MOHAMMED UNIVERSITY OF BÉCHAR
FACULTY OF TECHNOLOGY
DEPARTMENT OF ELECTRICAL ENGINEERING

Intended course for Master's students in Electrical Control.

Maintenance and Operational Safety
(Maintenance et sûreté de fonctionnement)

Author: Dr. BENHAMMOU Aissa.

2025/2026

Abstract of the course

The course "Maintenance and Operational Safety (MSdF in French)" focuses on the principles and practices to ensure the reliability, availability, maintainability and safety of industrial and technical systems. This course covers the theoretical aspects of preventive and corrective maintenance, risk management, reliability analysis, as well as continuous improvement methodologies. Students will learn how to implement effective maintenance strategies to extend equipment life, reduce maintenance costs, and minimize operational interruptions. In addition, the course covers current standards and regulations, as well as the use of modern tools and technologies in the field of maintenance.

Objectives of the course

To formulate objectives for this course on "Maintenance and Operational Safety " , we can organize them into six cognitive levels. Here's a structured set of objectives based on typical content in electrical engineering:

Knowledge (Remembering)

Identify key concepts in system reliability, including safety, maintainability, and fault tolerance.

List historical milestones in electrical engineering and common methodologies .

Comprehension (Understanding)

Explain the purpose and applications of reliability measures such as Mean Time Between Failures (MTBF) and reliability prediction techniques.

Summarize the impact of redundancy on system reliability and the role of preventive maintenance.

Application (Applying)

Construct basic fault trees for analyzing independent system failures.

Apply Markov chain methods to simple systems to estimate system reliability under different conditions.

Analysis (Analyzing)

Analyze failure modes in complex systems, considering dependencies between components.

Differentiate between active and passive redundancy strategies in operational systems.

Synthesis (Creating)

Design a basic maintenance plan that incorporates reliability prediction and fault tolerance methods.

Formulate a simplified reliability model using Boolean logic for a multi-component system.

Evaluation (Evaluating)

Assess the effectiveness of various reliability analysis methods, such as fault tree analysis and Petri nets, in different operational contexts.

Critique existing system configurations and propose improvements based on calculated reliability metrics.

Content Table

1.1 Introduction

The work and activities involved in project development require adherence to stringent specifications regarding operational safety: SIL (Safety Integrity Level), reliability levels, safety, etc. These specifications align with the ongoing concerns of improving operational availability and controlling the total cost of ownership. The goal of maintenance is to prevent and correct problems as much as possible, and the aim of Safety of Operation (SdF) is to achieve the ideal system design: zero accidents, zero downtime, zero defects (and even zero maintenance).

1.2 Brief History

The history of reliability and operational safety continued to evolve in subsequent decades, driven by the need for greater precision and the prevention of catastrophic events.
In the 1960s, significant advancements were made with the introduction of Failure Mode and Effects Analysis (FMEA)**,** a structured approach to identifying potential failure points and their impacts. Space research programs, such as those involving the Minuteman missile, employed fault tree analysis to evaluate and mitigate risks. Boeing and NASA introduced Cause Trees**,** further refining safety engineering methodologies. Influential books on reliability, such as those by Barlow and Proschan, provided foundational knowledge in the field. However, accidents such as the Torrey Canyon oil spill in 1967 highlighted the ongoing challenges in applying these methods universally, especially in complex systems.
The 1970s saw a focus on risk analysis and the collection of operational feedback through Return of Experience (REX). These efforts helped organizations learn from past incidents and improve safety standards. The decade marked a shift toward data-driven decision-making, enabling better risk assessment and management.
From the 1980s onward, advances in computational power and modeling techniques have profoundly transformed reliability engineering. The introduction of simulation-based methods, stochastic modeling, and formal tools such as Petri nets has enabled engineers to represent, analyze, and predict the behavior of increasingly complex and interconnected systems with greater accuracy. Major technological disasters, notably the Chernobyl nuclear accident in 1986, highlighted the severe consequences of inadequate reliability assessment and reinforced the necessity of rigorous system modeling and verification.

Subsequent failures, including the Ariane V launcher explosion in 1996 and later aerospace incidents such as NASA's DART mission anomaly in the mid-2000s, further demonstrated that software faults, integration errors, and insufficient validation can be as critical as hardware failures. Aviation accidents, including those involving commercial flights, have continued to emphasize the vital role of reliability analysis, fault tolerance, and safety-critical system design.

In recent years, reliability engineering has entered a new phase driven by digitalization and data-centric approaches. The integration of machine learning, digital twins, big data analytics, and real-time monitoring has shifted the discipline toward predictive and self-adaptive reliability frameworks. These modern techniques enable early fault detection, remaining useful life estimation, and proactive maintenance strategies across domains such as aerospace, energy systems, autonomous vehicles, and cyber-physical infrastructures.
Overall, the historical development of reliability engineering reflects a clear transition from reactive, experience-based practices to proactive and predictive methodologies. This evolution has been shaped by technological progress as well as by lessons learned from high-impact failures, ultimately leading to more resilient, intelligent, and safety-oriented engineering systems.

1.3 Maintenance

Maintenance encompasses all technical, administrative, and management actions throughout the lifecycle of an asset, intended to keep it or restore it to a state in which it can perform the required function.

1.3.1 Types of Maintenance

a. Preventive Maintenance: Involves intervening on equipment before it fails, attempting to prevent any breakdowns. Preventive maintenance is further divided into:

- ✓ **Systematic Maintenance:** Operations are performed systematically, either according to a fixed time schedule or based on usage (operating hours, number of units produced, number of movements made, etc.).
- ✓ **Conditional Maintenance:** Conducted following readings or measurements (mileage, operating time, etc.) and inspections that reveal the degradation state of the equipment (infrared thermography, vibration analysis, non-destructive testing, thickness measurement, oil analysis, etc.).
- ✓ **Predictive Maintenance:** Carried out following an analysis of the equipment's degradation state evolution (e.g., periodic inspections defined by the manufacturer or based on experience).

b. Corrective Maintenance: Involves intervening on equipment when it fails; it is subdivided into:

- ✓ **Palliative Maintenance:** Temporary repair of the equipment, allowing it to ensure all or part of a required function; it must be followed by a curative action as soon as possible.
- ✓ **Curative Maintenance:** Durable repair, restoring the equipment to its initial state or enabling it to perform the required function.

1.4 Safety of Operation

Safety of operation is often called the science of failures; it includes their understanding, evaluation, prediction, measurement, and control. It is a cross-disciplinary field that requires comprehensive knowledge of the system, including usage conditions, external risks, functional and hardware architectures, and the structure and characteristics of materials. This field proposes methods to increase the reliability and safety of systems within reasonable timeframes and costs.

1.5 Objective of Safety of Operation

The main objective is to ensure that the system operates as much as possible and to achieve the ideal system design: zero accidents, zero downtime, zero defects, and even to avoid maintenance as much as possible.

1.5.1 The System

A system is a set of three essential parts: personnel, software, and equipment, organized to meet needs and provide expected services in a given environment.

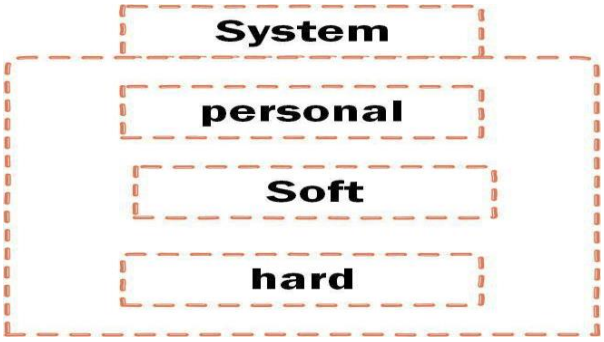


Figure.1.1: System contents.

1.5.2 Function definition

Every system is defined by at least one function (or mission) that it must perform under exceptional conditions and environments. A function can be defined as the action of an entity or one of its components expressed in terms of reliability. Different types of functions include:

1.5.2.1 Main Function

The primary purpose of a system.

- **Example 1:** For a generator, the main function is to supply power to a circuit.
- **Example 2:** For a mobile phone, the main function is communication between two entities.

1.5.2.2 Secondary Function

Functions performed in addition to the main function.

- **Example 1:** SMS, MMS, email, alarm, games, etc.
- **Example 2:** Current tester, voltage tester, etc.

1.5.2.3 Protection Function

Means to ensure the safety of assets, people, and environments.

- **Example 1:** Circuit breaker, differential switch, fuse, etc.
- **Example 2:** Password, protection software, etc.

1.5.2.4 Redundant Function

Multiple components ensure the same function.

1.6 Key Concepts of Operational Safety (SdF)

Operational safety is organized with the help of several concepts, which we clarify in this section by providing precise definitions. Operational safety can be considered as comprising the following three parts:

- **Attributes:** Perspectives for evaluating operational safety;
- **Impediments:** Events that can affect the system's operational safety;
- **Means:** Methods to improve operational safety.

These notions are summarized in Figure 1.2:

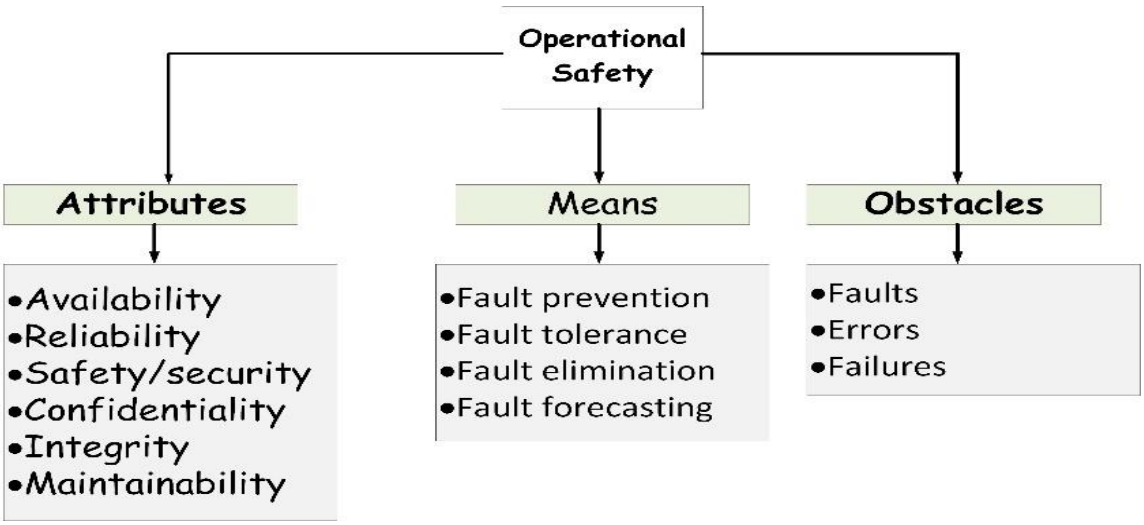


Figure 1.2: Operational Safety Tree.

a. Attributes

The attributes of operational safety are sometimes referred to as FDMS (Reliability, Availability, Maintainability, and Safety).

1. **Availability:** Availability is the ability of an entity to be in a state to perform a required function under given conditions at a given time or during a given time interval (readiness for service).
2. **Reliability:** Reliability is the ability of a device to perform a required function under given conditions for a given period (continuity of service).
3. **Safety:** Safety is the ability of an entity to avoid causing critical events under given conditions (the ability to prevent catastrophic accidents).
4. **Maintainability:** Maintainability is the ability of an entity to be maintained or restored within a given time to a state in which it can perform a required function (the ability of a system to return to proper functioning after modifications and repairs).

b. Means

Means are proven solutions to break the chain of fault-error-failure, thereby improving the system's reliability.

c. **Impediments (obstacles)**

Impediments are divided into three notions: faults, errors, and failures.

1. **Fault (Fault):** The cause of an error is a fault (e.g., short circuit on a component).
2. **Error (Defect):** The cause of a failure is an error affecting a part of the system's state.

3. **Failure (Failure):** A failure is the cessation of an entity's ability to perform a required function.
4. **Breakdown:** A breakdown is the inability of an entity to perform a mission. A breakdown always results from a failure.
5. **Failure Mode:** A failure mode is the effect by which a failure is observed. Failure modes are generally classified into four categories:

Table 1.1: Classification of Failure Modes.

Failure Mode	Explanation
Premature Operation	Operates when it is not supposed to.
Fails to Operate at Required Time	Does not start when solicited.
Fails to Stop at Required Time	Continues to operate when it is not supposed to.
Operational Failure	/

2.1 Introduction

Fault Tree Analysis (FTA) was historically the first method developed to systematically examine risks. It was created in the early 1960s by the American company "Bell Telephone" and was tested for evaluating missile launch systems' safety. Aiming to determine the sequences and combinations of events that can lead to a feared event taken as a reference, FTA is now applied in various fields such as aerospace, nuclear, chemical industries, etc. It is also used to retrospectively analyze the causes of accidents. In these cases, the feared final event is generally known because it has been observed. This is referred to as root cause analysis, with the main objective being to determine the actual causes that led to the accident. A predictive analysis of operational safety is a process of studying a real system to produce an abstract model of the system related to an operational safety characteristic (reliability, availability, maintainability, safety). The elements of this model will be events that may occur in the system and its environment.

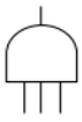
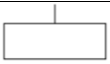
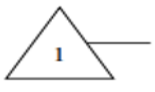
2.2 Fault Tree Analysis

Fault Tree Analysis is a deductive method based on prior knowledge of system behavior. Starting from a predefined feared event, the goal is to determine the sequences or combinations of events that can ultimately lead to this event. This analysis allows tracing back from causes to causes up to the basic events likely to be at the origin of the feared event. Fault Tree Analysis identifies the sequences and combinations of events that lead from basic events to the retained undesirable event. The links between the different identified events are made using logical gates such as "AND" and "OR."

2.3 Construction of a Fault Tree

Fault Tree Analysis focuses on a specific undesirable or feared event because it is not desired to occur. This event becomes the top of the tree, and the analysis aims to determine all its causes. The syntax of fault trees is described in following table.

Table 2.1 : Syntax of a Fault Tree.

Event/Report	Name	Gates/portes	Name
	Basic elements		AND
	Medium		OR
	The subtree under this "flag" is to be duplicated		OR exclusive

Fault Tree Analysis of a feared event can be broken down into four successive steps:

- Understanding the system.
- Defining the studied feared event.
- Developing the tree.
- Exploiting the tree.

In addition to these steps, a preliminary step of understanding the system is essential. This step is crucial for conducting the analysis and often requires prior knowledge of the risks.

Example : Figure 2.2 illustrates an electrical circuit comprising subsystems as follows:

- Power supply system (Battery) providing DC voltage to the lamps.
- Protection system to protect the lamps against short circuits.

Control system to control the lamps'

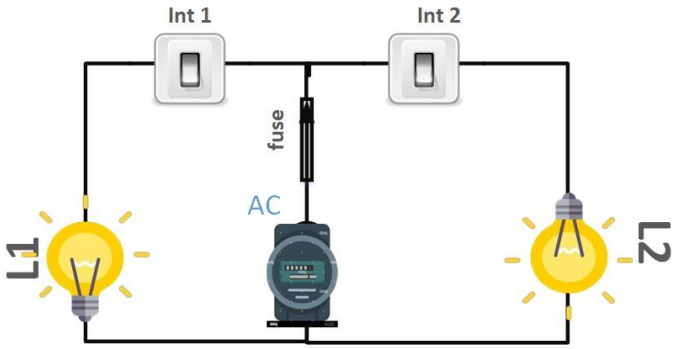


Figure 2.2: Electrical Circuit.

The fault tree of this circuit is shown in the figure below:

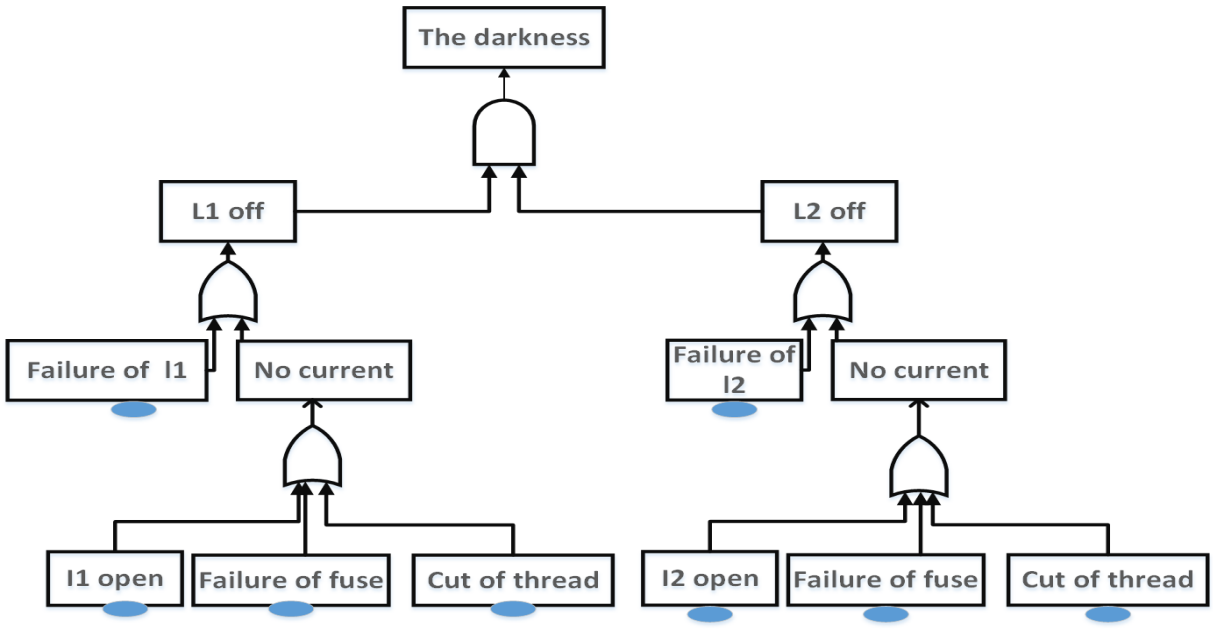


Figure 2.3: Fault Tree.

2.4 Qualitative Analysis

All these qualitative methods are based on the nomenclature of hazards and risks, their origins, and causes. They use standard tables to classify data and events.

2.4.1 Tree Coding

- Identify identical basic events across all Intermediate Events (EI) and assign them the same code.
- Code the other basic events.
- Use letters of the alphabet and numbers.

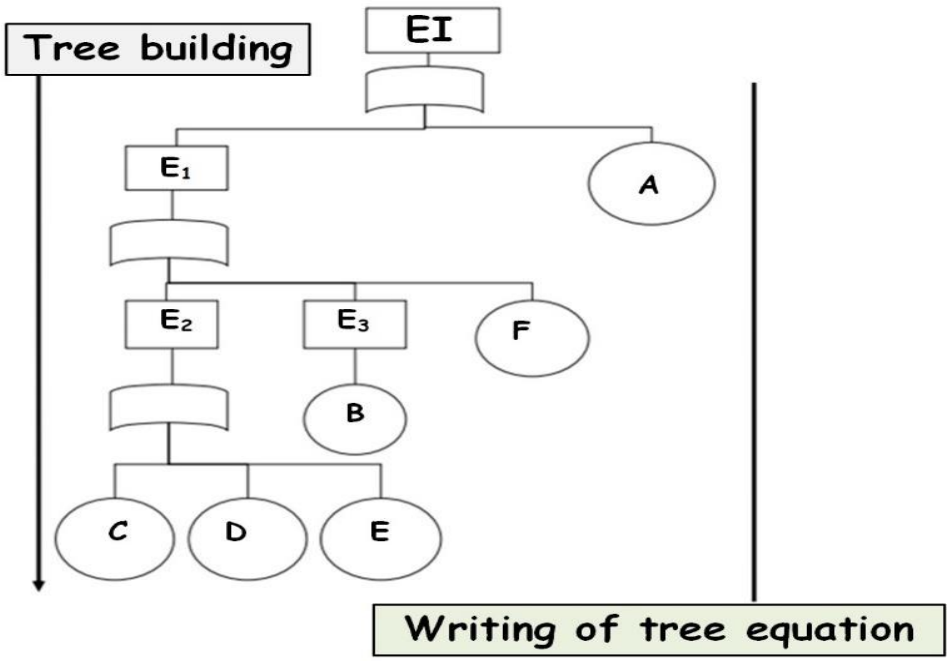


Figure 2.4: Construction and Writing of the Tree Equation.

Boolean Equations of the Tree:

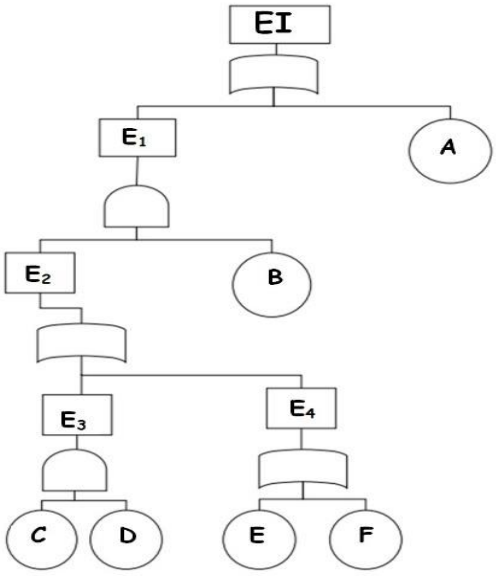
$$E_2 = C + D + E \quad (2.1)$$

$$E_3 = B \quad (2.2)$$

$$E_1 = E_2 + E_3 + F \Longrightarrow E_1 = C + D + E + B + F \quad (2.3)$$

$$EI = E_1 + A \Longrightarrow EI = A + B + C + D + E + F \quad (2.4)$$

Example : Write the Boolean equation of the tree illustrated in the figure below:



Solution

$E_3 = CD$, $E_4 = E + F$, $E2 = E_3 + E_4$, $E1 = E_2\ B$; $EI = E_1 + A$ (2.5)

2.4.2 Reduction of the Boolean Equation

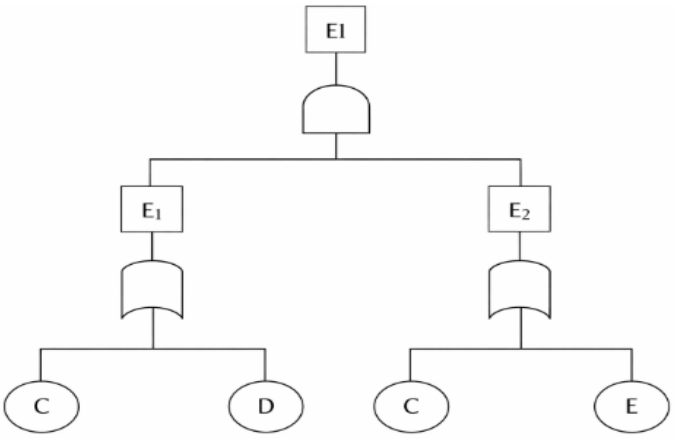
After writing the Boolean equation of the fault tree, we can reduce this resulting equation using the following properties:

$$A \times A = A$$

$$A + A = A$$

$$A + AB = A$$

Example :



Boolean Equation:

$E_1=C+D$ (2.6)

$E_2=C+E$ (2.7)

$EI= E_1 \times E_2 = (C+D)\times(C+E) = C\times C+C\times E+C\times D+D\times E$ (2.8)

Simplification equation after appliying the proprties:

$EI=C+CD+D\times E=C+D\times E$ (2.9)

2.5 Quantitative Analysis

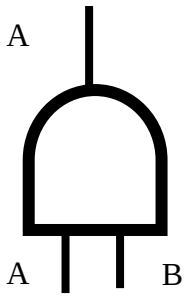
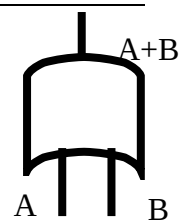
2.5.1 Quantification with Fixed Probabilities

The main processes that can be performed from a fault tree with probabilities are as follows:

- Enumeration of minimal cuts or first associated cuts with their probabilities. The possibility of quantifying them allows listing only those whose probability exceeds a certain threshold, which is an effective way to limit the combinatorial explosion that this type of processing can lead to.
- Calculation of the probability of the event.
- Calculation of various importance factors associated with basic events.

2.6 Mathematical Significance of AND and OR Gates

Table 2.2 : Mathematical Significance of AND and OR Gates

<table>
<tr><th>Symbole</th><th>Name</th><th>Truth Table & Boolean Expression</th><th>Probability of output across n inputs</th></tr>
<tr><td> 
</td><td>And</td><td>A.B
<table><tr><th>A</th><th>B</th><th>A and B</th></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table></td><td>$P = \prod_{i=1}^{n} P_i$</td></tr>
<tr><td> 
</td><td>Or</td><td>A+B
<table><tr><th>A</th><th>B</th><th>A or B</th></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table></td><td>$\mathrm{P} = \sum_{i=1}^{n} P_i - \sum_{i<j} P_i P_j - \sum_{i<j<k} + P_i P_j P_k - \cdots + (-1)^{n-1} \prod_{i=1}^{n} P_i$</td></tr>
</table>

Example :

$P(A.\ B.\ C) = P(A) \times P(B) \times P(C)$ (2.10)

$$P(A+B+C) = P(A) + P(B) + P(C) - P(A) \times P(B) - P(A) \times P(C) - P(B) \times P(C) + P(A) \times P(B) \times P(C) \quad (2.11)$$

Example: The figure below represents the fault tree of a system.

P(A) = 0.3

P(B) = 0.5

P(C) = 0.1

P(D) = 0.2

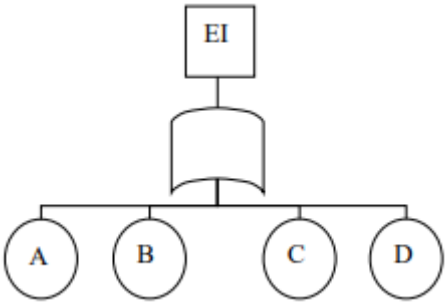


Figure 2.5: Fault Tree.

$$P(EI) = P(A+B+C+D) = P(A) + P(B) + P(C) + P(D) - P(A) \times P(B) - P(A) \times P(C) - P(A) \times P(D) - P(B) \times P(C) - P(B) \times P(D) - P(C) \times P(D) + P(A) \times P(B) \times P(C) + P(A) \times P(B) \times P(D) + P(A) \times P(C) \times P(D) + P(B) \times P(C) \times P(D) - P(A) \times P(B) \times P(C) \times P(D). \quad (2.12)$$

Numerical Application:

$$(EI) = 0.3 + 0.5 + 0.1 + 0.2 - 0.3 \times 0.5 - 0.3 \times 0.1 - 0.3 \times 0.2 - 0.5 \times 0.1 - 0.5 \times 0.2 - 0.1 \times 0.2 + 0.3 \times 0.5 \times 0.1 + 0.3 \times 0.5 \times 0.2 + 0.3 \times 0.1 \times 0.2 + 0.5 \times 0.1 \times 0.2 - 0.3 \times 0.5 \times 0.1 \times 0.2 \quad (2.13)$$

$$P\,(EI) = 1.1 - 0.15 - 0.03 - 0.06 - 0.05 - 0.1 - 0.02 + 0.015 + 0.03 + 0.006 + 0.01 - 0.003 \quad (2.14)$$

So : (EI) = 0.748

2.7 Advantages and Limitations

2.7.1 Advantages

1. Its graphical aspect is particularly important, providing an effective means of representing the logic of failure combinations. It significantly contributes to the method's ease of implementation and understanding of the model. Thus, it is an excellent support for multidisciplinary teams.

2. The tree construction process based on a deductive method allows the analysis to focus only on events contributing to the occurrence of the feared event.
3. Once the tree construction is completed, two exploitation modes are possible:
   - ✓ Qualitative exploitation, which serves to identify combinations of critical events, aiming to determine the system's weak points.
   - ✓ Quantitative exploitation, which allows ranking these event combinations by their probability of occurrence and estimating the probability of the top event. The ultimate goal is to provide criteria for determining priorities to prevent the feared event.
4. Unlike simulation methods, the analytical approach offered by the fault tree has the advantage of performing quick and exact calculations (a relative advantage considering the continuous evolution of computing).
5. The method allows estimating not only the probability.

2.7.2 Limitations

1. Interdependence of Events

The probability calculations performed using fault tree analysis assume the independence of basic events from one another. For example, the probability of a basic event occurring cannot be dependent on the occurrence of other basic events.

2. Temporal Aspects of Events

Fault tree analysis does not account for the temporal sequence of events. Consequently, it cannot consider functional dependencies or historical states. Additionally, it does not allow for the inclusion of a predetermined order in which events must occur to lead to a failure.

3. Degraded System States

Fault tree analysis operates on a binary basis: an event either occurs or does not occur, with no consideration of capacity or efficiency levels. For example, a valve is classified as either open or closed, without accounting for any intermediate states.

4. Tree Size

Although size is not a limitation in itself, a significant increase in tree size necessitates the division of the tree into sub-trees, making the model more challenging to read and interpret.

3.1 Introduction

The **State Space Method (SSM)** was developed for the reliability analysis of repairable systems. Fault trees, discussed in the previous chapter, provide excellent static descriptions of systems but fail to account for reconfigurations, such as repairs. Early applications of stochastic processes in the 1950s utilized Markov processes, which were later generalized. In this chapter, we focus on Markov processes.

Andrei Markov published his first results in 1906, which were later extended to an infinite countable state space by Andrei Kolmogorov in 1936. A stochastic process is a set of random variables$(x_t)_t \geq 0$ that take values in the set of observations. A process is considered **Markovian** if the probability of transitioning from the current state to the next depends solely on the present state and not on the past:

$$P\big(X_t \in A \mid X_{t_n} \in A_n, \dots, X_1 \in A_1\big) = P\big(X_t \in A \mid X_{t_n} \in A_n\big) \tag{3.1}$$

3.2 Basic Concepts of Markov Chains

3.2.1 Methodology

To construct a state graph for a system, the following factors must be considered:

- Number of components constituting the system.
- System structure, including interdependencies.
- Number of repair personnel available.
- Maintenance policies applied to the system.

3.2.2 Construction

- Identify the states E_i of the system based on the states of its components.
  - ✓ A system with n components can have a maximum of $p = 2^n$ states.
- Define transitions between system states and identify their causes, such as:
  - ✓ Failures.
  - ✓ Shutdowns.
  - ✓ Repairs.
  - ✓ Commissioning of components.
- Classify the states into operational states or failure states.

3.2.3 Representation

- **System states**: Each state of the system is represented as a node in the graph, depicted by a circle.
  - ✓ Each state E_i is associated with a probability that varies over time:

$$P_i(t) = P(E(t) = E_i) \tag{3.2}$$

- **Transitions**: Transitions between states are represented by directed arrows from the initial state to the final state.

- ✓ Each transition is associated with a rate defined by the conditional probability of the transition occurring:

$$a_{ij}(t)dt = P(E(t+dt) = E_j(E(t) = E_i) \quad (3.3)$$

This structured approach allows for a dynamic analysis of system behavior, incorporating dependencies such as repair and maintenance activities.

Remark: If the probability of transitioning from state i to state j between time t and $t + dt$ is $\mathbf{a_{ij}}$ dt, then $\mathbf{a_{ij}}$ is the transition rate between states i and j. If the transition rates are constant, the process is a homogeneous Markov process

3.2.4 Transition Rates

- $a_{ij} = \lambda$: If the transition corresponds to an operational failure.
- $a_{ij} = \mu$: If the transition corresponds to a repair.

3.3 Single-Entity System

All systems where the future operational state depends only on the current state can be described by a Markov process. Specifically, this applies to systems where the transition probabilities between any two states are independent of time. Such systems are considered **homogeneous**. This is typically the case for phenomena with an exponential distribution.

3.3.1 Probability Matrix

Consider a simple system with two states, as shown in Figure 3.1.

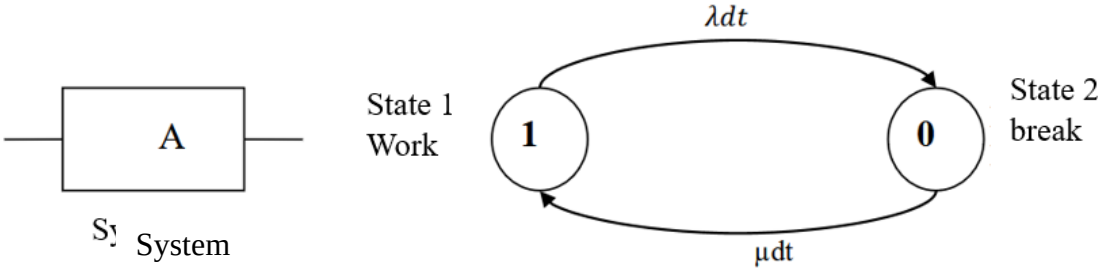


Figure 3.1: State Diagram Modelling Availability

Initial conditions

$P(0) = (1,0) \Leftrightarrow$ Initially, the system is operational: $P_1(0) = 1 \; and \; P_2(0) = 0$.
$reminder$:

$$\sum P_i = 1 \; where \; \sum \frac{P_i(t)}{dt} = \sum \acute{P}_1 + \acute{P}_2 = 0 \rightarrow here \; P_1 + P_2 \acute{=} 1 \forall t \; where \; \acute{P}_1 + \acute{P}_2 = 0 \quad (3.4)$$

$$P_1(t+dt) = P_1(t) \times (1 - \lambda \, dt) + P_2(t) \times \mu \, dt \quad (3.5)$$

$$P_2(t+dt) = P_1(t) \times \lambda \, dt + P_2(t) \times (1 - \mu \, dt) \quad (3.6)$$

In the Matrix form

$$\begin{pmatrix} P_1(t+dt) \\ P_2(t+dt) \end{pmatrix} = \begin{pmatrix} P_1(t) \\ P_2(t) \end{pmatrix} \times \begin{pmatrix} 1-\lambda\, dt & \mu\, dt \\ \lambda\, dt & 1-\mu\, dt \end{pmatrix} \quad (3.7)$$

Or:

$$\mathbf{P}(t+dt) = \mathbf{P}(t) \times \mathbf{M} \quad (3.8)$$

Where the probability matrix is:

$$\mathbf{M} = \begin{pmatrix} 1-\lambda\, dt & \mu\, dt \\ \lambda\, dt & 1-\mu\, dt \end{pmatrix} \quad (3.9)$$

$$P_1(t+dt) = P_1(t) \times (1-\lambda\, dt) + P_2(t) \times \mu\, dt \quad (3.10)$$

$$P_2(t+dt) = P_1(t) \times \lambda\, dt + P_2(t) \times (1-\mu\, dt) \quad (3.11)$$

In matrix form, we obtained:

$$(P_1(t+dt) \quad P_2(t+dt)) = (P_1(t) \quad P_2(t)) \times \begin{pmatrix} 1-\lambda\, dt & \lambda\, dt \\ \mu\, dt & 1-\mu\, dt \end{pmatrix} \quad (3.12)$$

$$\mathrm{P}(t+dt) = \mathrm{P}(t) \times \mathrm{M}, \quad \mathrm{M} = \begin{bmatrix} 1-\lambda\, dt & \lambda\, dt \\ \mu\, dt & 1-\mu\, dt \end{bmatrix} \quad (3.13)$$

It is the probability matrix that characterizes the system.We expand and arrange it systematically

$$\frac{dP_1(t)}{dt} = \lim_{h\to 0} \frac{P_1(t+dt) - P_1(t)}{h} = -\lambda P_1(t) + \mu P_2(t) \quad (3.14)$$

$$\frac{dP_2(t)}{dt} = \lim_{h\to 0} \frac{P_2(t+dt) - P_2(t)}{h} = \lambda P_1(t) - \mu P_2(t) \quad (3.15)$$

Remarque : $\frac{dP_1(t)}{dt} + \frac{dP_2}{dt} = 0$ .In matrix form, we obtained :

$$\begin{pmatrix} \frac{dP_1(t)}{dt} & \frac{dP_2(t)}{dt} \end{pmatrix} = (P_1(t) \quad P_2(t)) \times \begin{pmatrix} -\lambda & \lambda \\ \mu & -\mu \end{pmatrix} \quad (3.16)$$

where:

$$\frac{d\mathbf{P}(t)}{dt} = \mathbf{P}(t) \times \mathbf{Q} \quad (3.17)$$

$$\frac{d\mathbf{P}(t)}{dt} = \left(\frac{dP_1(t)}{dt}, \frac{dP_2(t)}{dt}\right), \quad \mathbf{P}(t) = (P_1(t), P_2(t)) \text{ and } \mathrm{Q} = \begin{pmatrix} -\lambda & \lambda \\ \mu & -\mu \end{pmatrix} \quad (3.18)$$

This new matrix Q, called the transition rate matrix, can be easily constructed based on the following principle:

Table 3.1: Transition Rate Matrix

	State 1	State 1	The sum of each ligne probabilities is zero
State 1	−λ	Λ	
State 2	M	−μ	

3.4 Solving the Differential Equation

The equations derived from the Markov state diagram are presented below:

$$\begin{cases} d\frac{p_1(t)}{dt} = -\lambda p_1(t) + \mu\, p_2(t) \\ d\frac{p_2(t)}{dt} = \lambda p_1(t) - \mu\, p_2(t) \end{cases} \quad (3.19)$$

We know that : $\sum p_i = 1 \;\rightarrow\; p_1(t) + p_2(t) = 1$

$$p_2(t) = 1 - p_1(t) \quad (3.20)$$

If by substituting (3.20) into (3.19) we obtain the following:

$$(3.19) \rightarrow \dot{p_1}(t) = -\lambda p_1(t) + \mu\big(1 - p_1(t)\big) \rightarrow \dot{p_1}(t) + \lambda p_1(t) - \mu\big(1 - p_1(t)\big) = 0 \quad (3.21)$$

$$\dot{p_1}(t) + \lambda p_1(t) - \mu + \mu\, p_1(t) = 0 \quad (3.22)$$

$$\dot{p_1}(t) + \lambda p_1(t) + \mu\, p_1(t) = \mu \quad (3.23)$$

$$\dot{p_1}(t) + (\lambda + \mu)\, p_1(t) = \mu \quad (3.24)$$

Homogeneous equation

$$\dot{p_1}(t) + (\lambda + \mu)\, p_1(t) = 0 \quad (3.25)$$

Homogeneous solution

$$p_H(t) = Ce^{(\lambda+\mu))} \quad (3.26)$$

Particular solution

$$p_A(t) = A \quad (3.27)$$

$$p_1(t) = A \rightarrow \dot{p_1}(t) = 0\ so\ , (\lambda + \mu)A = \mu \rightarrow A = \frac{\mu}{\lambda + \mu} \quad (3.28)$$

Global solution

$$P_1(t) = Ce^{-(\lambda+\mu)t} + \frac{\mu}{\lambda + \mu} \quad (3.29)$$

The initial conditions are:

$$P_1(0) = 1 \quad \text{and} \quad P_2(0) = 0 \quad (3.30)$$

$$P_1(0) = Ce^0 + \frac{\mu}{\lambda+\mu} \quad \Rightarrow \quad 1 = C + \frac{\mu}{\lambda+\mu} \tag{3.31}$$

$$\Rightarrow \quad C = 1 - \frac{\mu}{\lambda+\mu} \tag{3.32}$$

$$\Rightarrow \quad C = \frac{\lambda}{\lambda+\mu} \tag{3.33}$$

The final equation becomes:

$$P_1(t) = \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t} + \frac{\mu}{\lambda+\mu} \tag{3.34}$$

Availability is:

$$A(t) = P_1(t) = \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t} + \frac{\mu}{\lambda+\mu} \tag{3.35}$$

Unavailability is:

$$1 - A(t) = P_2(t) = \frac{\lambda}{\lambda+\mu}\left(1 - e^{-(\lambda+\mu)t}\right) \tag{3.36}$$

3.5.2 Repairable Device

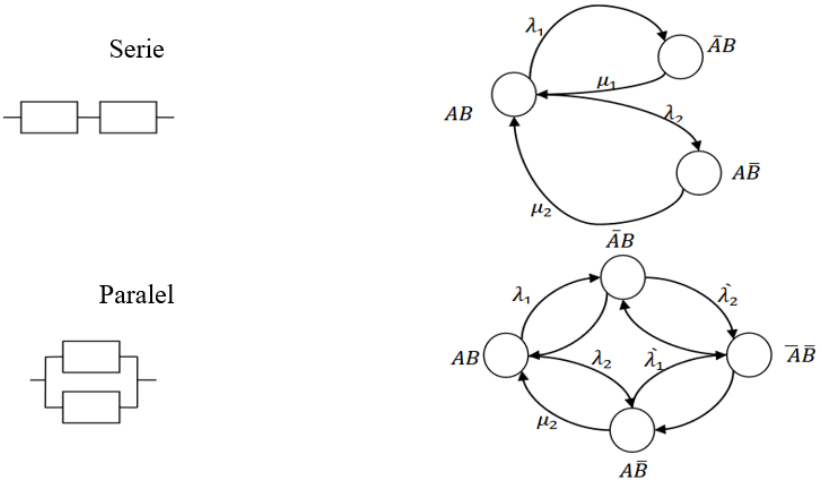


Figure 3.4: Repairable Device in a Two-Entity System

3.6 Simplification

When modeling a system using a Markov chain, we encounter the problem of state-space explosion, as the chain has 2^n states for a system with n two-state elements. However, it is possible to reduce the size of the chain by aggregating states. This assumes that the components are identical with the same failure and repair rates.In the case of a system with two active components, the previously discussed chains can be simplified as follows. State i corresponds to the set of states where there are i failures.

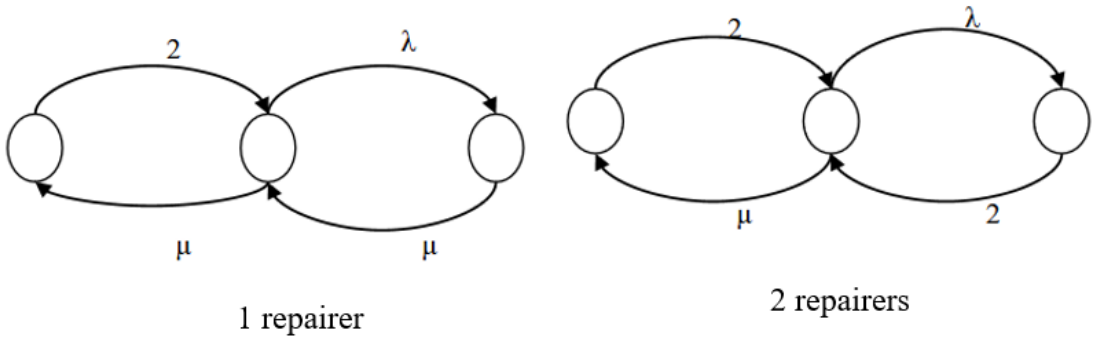


Figure 3.5: Simplification of a Markov Chain for a Two-Component System

3.7 Redundancy

Redundancy refers to the existence of more than one means within an entity to perform a required function.

3.7.1 Active or Hot Redundancy

In this case, all means are implemented simultaneously. When the system operates if and only if at least one of its components is functioning, the components are said to be in active redundancy.In k-out-of-n redundancy, the system functions if and only if at least k components out of n are operational.

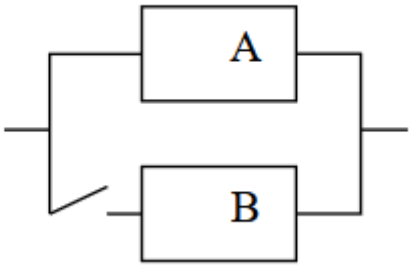


Figure 3.6: Active Redundancy

3.7.2 Passive or Cold Redundancy (Sequential, Standby, Reserve)

In this case, part of the means are operational while the rest are on standby, with a device ensuring the switching. When components are in passive redundancy, component Si is normally operational while the others are on standby. Only one component functions at a time, and when it fails, another takes over.

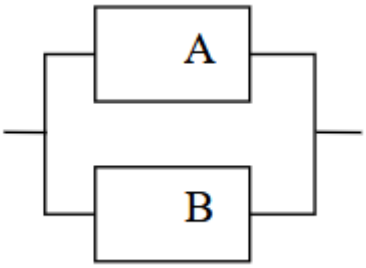


Figure 3.7: Passive Redundancy

Example

A PV (photovoltaic) system is assumed to operate for 30 years. This period is divided into four (4) intervals (T_1,T_2,T_3,, and T_4) of 7 years each:

- 1 to 7 years (T_1)
- 8 to 14 years (T_2)
- 15 to 21 years (T_3)
- 22 to 28 years (T_4)

Table 3.2: Transition Probabilité Matrix

Period	T1	T2	T3	T4
Start	0.9	0.06	0.04	0
Minor defects	0	0.5	0.3	0.2
Major defects	0	0	0.3	0.7
Complete failure	0	0	0	1

Field studies have shown that the degradation of a photovoltaic system is estimated at 1% per year.

There are four possible states for constructing the Markov chain, and the probabilities are determined based on the inspection results. Initially, the system is in good condition. The probability matrix is provided above:

$$\begin{bmatrix} 0.9 & 0.06 & 0.04 & 0 \\ 0 & 0.5 & 0.3 & 0.2 \\ 0 & 0 & 0.3 & 0.7 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (3.37)$$

The four states (S) of the photovoltaic system are:

- **S1**: System in good condition.
- **S2**: System with partial degradation but fully operational.
- **S3**: System with major defects and partially operational.
- **S4**: System completely failed.

The states S_i are defined based on the thresholds of the characteristics of the studied system: The PV system is in good working condition at the beginning, which can be expressed as: $p_1(0) = 1$.

The probability of the system after:

- First inspection or after 7 years is:

$$[P_1(1)\ \ P_2(1)\ \ P_3(1)\ P_4(1)] = [P_0(1)\ P_0(1)\ P_0(1)\ P_0(1)] \times \begin{bmatrix} 0.9 & 0.06 & 0.04 & 0 \\ 0 & 0.5 & 0.3 & 0.2 \\ 0 & 0 & 0.3 & 0.7 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (3.38)$$

$$[P_1(1)\ \ P_2(1)\ \ P_3(1)\ P_4(1)] = [1\ \ 0\ \ 0\ \ 0] \times \begin{bmatrix} 0.9 & 0.06 & 0.04 & 0 \\ 0 & 0.5 & 0.3 & 0.2 \\ 0 & 0 & 0.3 & 0.7 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (3.39)$$

$$\begin{cases} P_1(1) = 0.9 \\ P_2(1) = 0.06 \\ P_3(1) = 0.04 \\ P_4(1) = 0 \end{cases} \quad (3.40)$$

2nd state:

$$[P_1(2)\ \ P_2(2)\ \ P_3(2)\ P_4(2)] = [P_1(1)\ P_1(1)\ P_1(1)\ P_1(1)] \times \begin{bmatrix} 0.9 & 0.06 & 0.04 & 0 \\ 0 & 0.5 & 0.3 & 0.2 \\ 0 & 0 & 0.3 & 0.7 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (3.41)$$

$$[P_1(2)\ \ P_2(2)\ \ P_3(2)\ P_4(2)] = [0.9\ \ 0.6\ \ 0.04\ \ 0] \times \begin{bmatrix} 0.9 & 0.06 & 0.04 & 0 \\ 0 & 0.5 & 0.3 & 0.2 \\ 0 & 0 & 0.3 & 0.7 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (3.42)$$

$$\begin{cases} P_1(2) = 0.81 \\ P_2(2) = 0.084 \\ P_3(2) = 0.066 \\ P_4(2) = 0.04 \end{cases} \quad (3.43)$$

3rd state:

$$[P_1(3)\ \ P_2(3)\ \ P_3(3)\ P_4(3)] = [P_1(2)\ P_1(2)\ P_1(2)\ P_1(2)] \times \begin{bmatrix} 0.9 & 0.06 & 0.04 & 0 \\ 0 & 0.5 & 0.3 & 0.2 \\ 0 & 0 & 0.3 & 0.7 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (3.44)$$

$$[P_1(3)\ \ P_2(3)\ \ P_3(3)\ P_4(3)] = [0.81\ \ 0.084\ \ 0.066\ \ 0.04] \times \begin{bmatrix} 0.9 & 0.06 & 0.04 & 0 \\ 0 & 0.5 & 0.3 & 0.2 \\ 0 & 0 & 0.3 & 0.7 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (3.45)$$

$$\begin{cases} P_1(3) = 0.729 \\ P_2(3) = 0.0906 \\ P_3(3) = 0.0774 \\ P_4(3) = 0.103 \end{cases} \quad (3.46)$$

3.8 Reliability Calculation

To calculate the reliability of a system represented as a Markov chain, it is necessary to modify the chain to eliminate all repair transitions from a failure state to a working state. Failure states then become absorbing states.

Thus, the new Markov chain associated with a system with active redundancy and two components becomes:

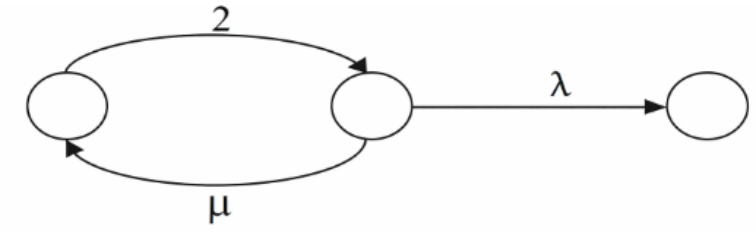


Figure 3.8: Markov Chain with Two Components for Reliability Calculation.

The reliability of the system is: $R(t) = \sum_{i\ \epsilon function\ state} P_i(t)$

3.9 Advantages and Limitations

3.9.1 Advantages

- Possibility to account for complex systems with redundancies.
- A highly useful method for evaluating the availability, reliability, and maintainability of repairable systems.

3.9.2 Limitations

- Difficult representation for large-scale systems.
- Complex numerical calculations (risk of combinatorial explosion).

4.1 Introduction

Carl Adam Petri, a German mathematician, defined a very general mathematical tool that allows for the description of relationships between conditions and events, modeling the behavior of discrete-event dynamic systems.

- **Start of research (1960-1962):** Led to numerous studies and developments.
- **1972-1973:** Application of this tool for describing logical automation, which eventually led to the creation of GRAFCET. This tool enables qualitative analysis.

There are different types of Petri nets: timed, interpreted, stochastic, colored, continuous, and hybrid.

4.2 Basic Concepts of Petri Nets

A Petri Net is a directed graph consisting of:

- A finite set of places, $P=\{P_1,P_2,P_3,...,P_m\}$, represented by circles, which represent conditions:

  ✓ A system resource (e.g., a machine, a stock, a conveyor, etc.)
  ✓ The state of a system resource (e.g., machine available, empty stock, conveyor breakdown, etc.)

- A finite set of transitions, $T=\{T_1,T_2,T_3,...,T_n\}$, represented by bars, which represent the set of events (actions occurring in the system) that trigger changes in the system's state.
- A finite set of events associated with each transition.
- A finite set of directed arcs that link a place to a transition or a transition to a place.

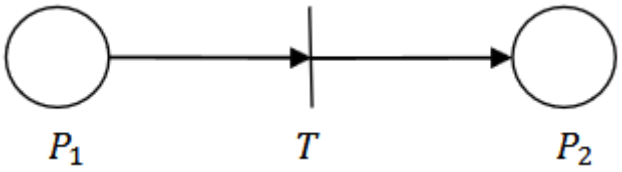


Figure 4.1: Directed Graph

Definition
A synchronized Petri Net is defined by a 5-tuple $R=\{P,T,Pre,Post,M_0\}$, where:

- $P=\{P_1,P_2,P_3,...,P_N\}$ is the set of places.
- $T=\{T_1,T_2,T_3,...,T_L\}$ is the set of transitions.
- **Input (Pre):** An application, input $:P\times T\rightarrow N$, called the pre-incidence application.

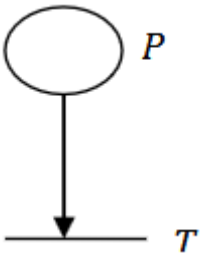


Figure 4.2: Pre-incidence Application

- **Output (Post):** An application, output : P×T→N, called the post-incidence application.

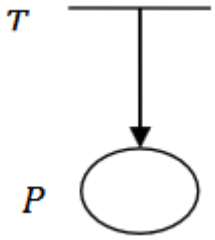


Figure 4.3: Post-incidence Application

- M_0: The initial state P→R.

Example

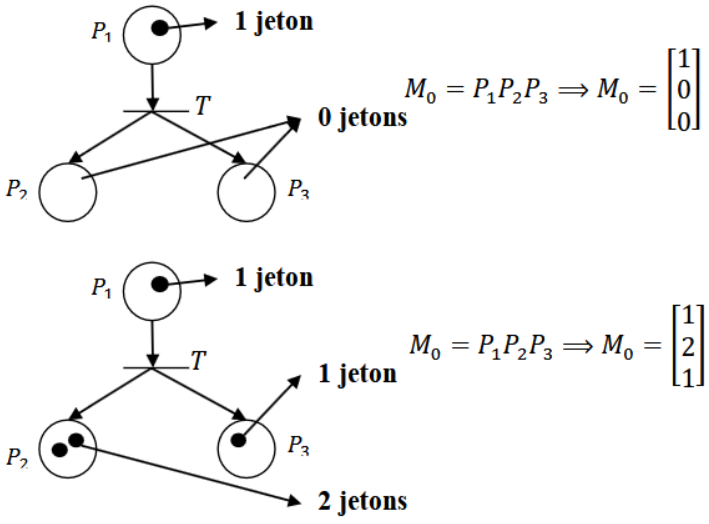


Figure 4.4: Marked Petri Net

Remark
A token can have multiple meanings depending on the place where it is located.

Example

- P_1 represents a stock: The number of tokens in P_1 indicates the number of items in stock.
- P_2 represents a machine in operation: A token in P_2 indicates that the machine is processing an item.
- P_3 represents an available machine: A token in P_3 indicates that the machine is free.

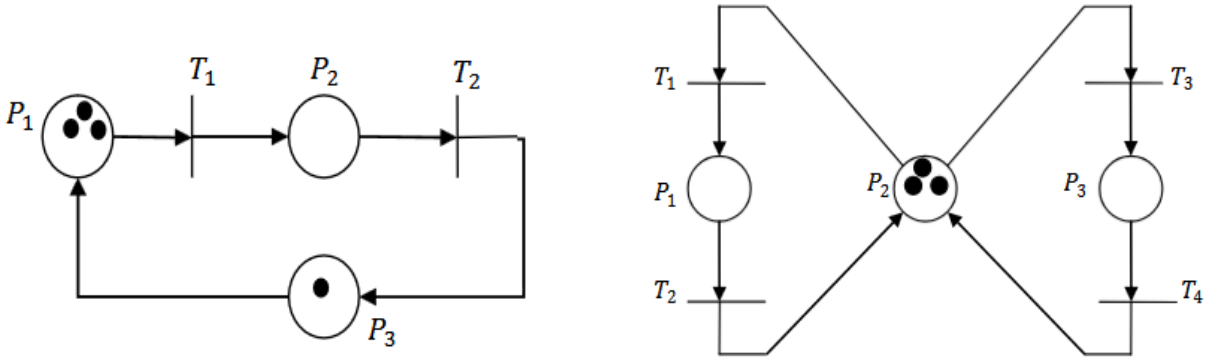


Figure 4.5: Petri Net of a Stock-Machine System

Example

The figure shows a workshop consisting of a cutting machine and a stock. When an order arrives and the cutting machine is available, the order can be processed (cutting operation). After processing, the completed order is stored. Otherwise, the order must wait until the machine is free before being processed.

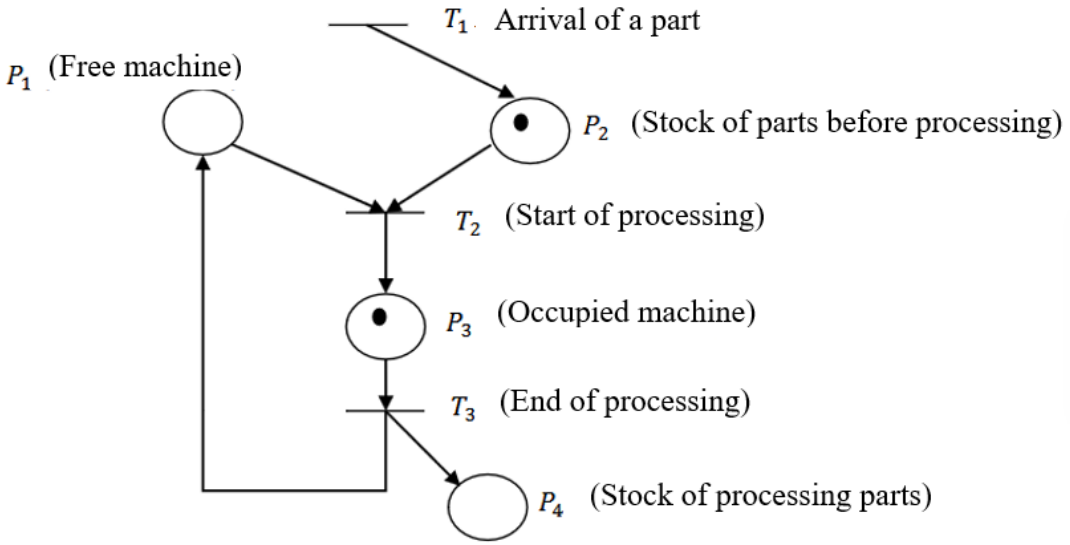


Figure 4.6: Modeling a Wood Cutting Workshop

Incidence Matrix (W)

Instead of Pre and Post, we generally use W, the incidence matrix, which is computed from Pre and Post as follows:

$$W = Post - Pre \tag{4.1}$$

Example

For the Petri Net shown:

1. Indicate the initial marking.
2. Establish the pre-incidence matrix (Pre).
3. Establish the post-incidence matrix (Post).
4. Establish the incidence matrix (W).

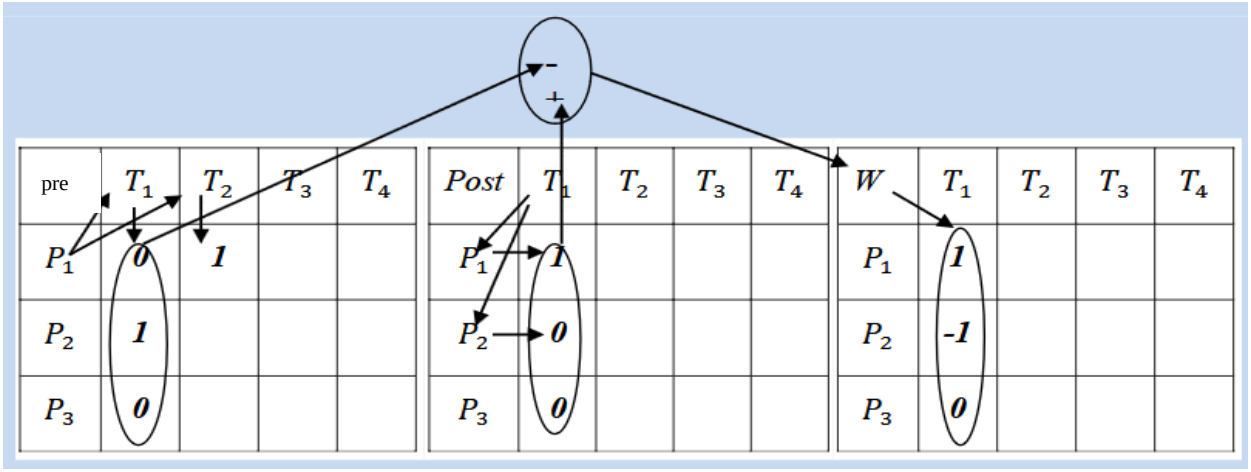
Solution

$$M_0 = \begin{bmatrix} 0 \\ 3 \\ 0 \end{bmatrix} \tag{4.2}$$

$$pre = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}; post = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}; w = \begin{bmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & -1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{4.3}$$

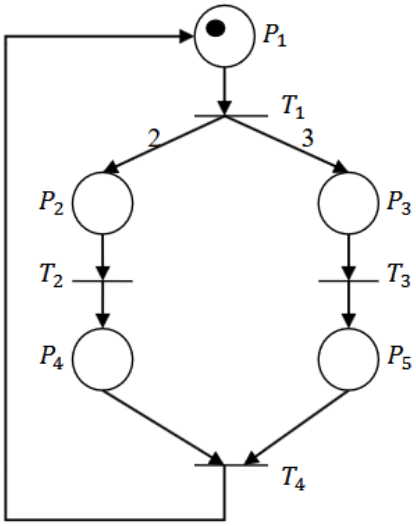
Remark
To simplify the matrix filling process, you can use tables as illustrated below:

Table 4.1: Matrix Filling Process



Exercise 4.2

For the following Petri net:



1. Establish the pre-incidence matrix.
2. Establish the post-incidence matrix.
3. Establish the incidence matrix W.

Solution

$$pre = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}; post = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}; w = \begin{bmatrix} -1 & 0 & 0 & 1 \\ 2 & -1 & 0 & 0 \\ 3 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \quad (4.4)$$

Note 4.3: Each arc has a positive integer representing its weight. By convention, when the weight is not specified on an arc, it is assumed to be 1.

4.3 Properties of Petri Nets

In this section, we consider ordinary Petri nets and present the properties required for introducing our contribution.

Reachable markings: Denoted as M_R, the set of reachable markings of a Petri net R is derived from the initial marking M_0.

Bounded Petri Net: A place P_i is said to be bounded for an initial marking M_0 if there exists a natural number k, such that for every marking reachable from M_0, the number of tokens in Pi is less than or equal to k.

Live transition: A transition T_j is live for an initial marking M_0 if, for every marking $M_i \in M_R$, there exists a firing sequence S containing T_j that can be fired starting from M_i.

Live Petri Net: A Petri net is live for an initial marking M_0 if all its transitions are live for M_0.

Deadlock: A deadlock occurs at a marking where no transition can be fired.

Structural conflict: A structural conflict corresponds to a set of at least two transitions T_1 and T_2 sharing a common input place P_i.

Effective conflict in a Petri net: An effective conflict occurs when at least two enabled transitions are synchronized with the same event.

Invariants: Let R be a Petri net and P the set of its places. A **marking invariant** exists if there is a subset P′ and a weighting vector Q=(q_1,q_2,...,q_r), where all q_i are positive integers, such that:

$$q1M(P1) + q2M(P2) + \ldots + qrM(Pr) = constant, \forall\, M \in MR \quad (4.5)$$

4.4 Transition Firing

A transition can only fire if all its input places contain at least one token. In this case, the transition is said to be **enabled** or **valid**. Firing a transition updates the net's marking by:

1. Removing one token from each input place of the transition.
2. Adding one token to each output place of the transition.

For safe Petri nets, only one transition fires at a time, and the firing duration is considered instantaneous.

In a synchronized Petri net, a valid transition fires upon the occurrence of the associated event.

For example, in Figure 4.7-a, transition T_1 is enabled when event σ_1 occurs. The result of firing this transition is shown in Figure 4.7-b.

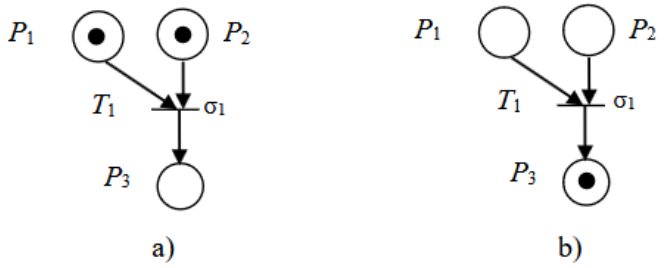


Figure 4.7: Transition firing

Each firing sequence is associated with a characteristic vector, denoted $\bar{s}$. This vector has a dimension L (number of transitions), where the j^{th} component corresponds to the number of times T_j is fired in the sequence S.

If the firing sequence S is realizable from a marking M_i, the resulting marking M_k is given by the fundamental equation:

$$M_K = M_i + W\,\bar{s} \quad (4.6)$$

Here, $\bar{s}$ is the characteristic vector of the firing sequence S, leading from M_i to M_k.

4.5 Reachable Marking Graph and Coverability Graph

To analyze a Petri net's behavior, the simplest idea is to construct the **reachable marking graph**. In this graph:

a) Each node represents a reachable marking.
b) Each arc represents the firing of a transition leading from one marking to another.

The reachable marking graph is ideal for verifying properties like liveness and reachability in bounded nets.

For unbounded nets, however, the number of reachable markings becomes infinite, leading to an infinite number of nodes in the graph. To address this, we construct a coverability graph, which has a finite number of nodes.

In this graph, the symbol ω indicates that the number of tokens in a place is "infinite." This marking remains ω in subsequent developments.

A node corresponding to a marking where no transition can fire is marked as "dead-end" and becomes a leaf of the tree. Nodes not marked as "old" and having at least one descendant are marked as "new".

Example: Reachable marking graph

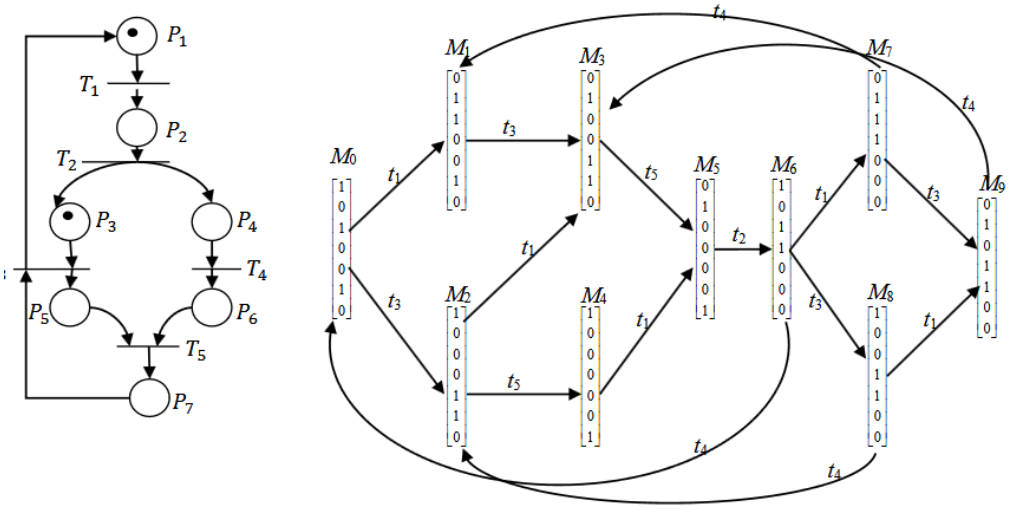


Figure 4.8: Petri net with a finite marking graph

Example: Coverability graph

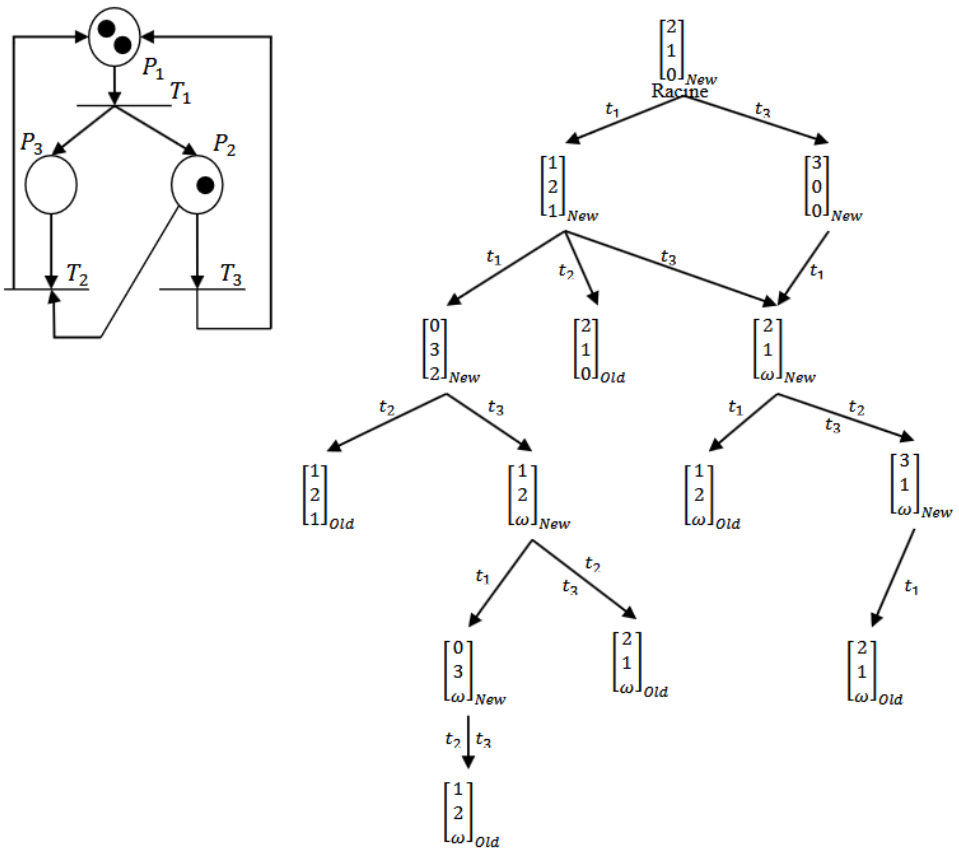


Figure 4.9: Petri net with a coverability graph

Note : For an infinite-dimensional marking graph, the coverability graph cannot analyze liveness due to the introduction of the symbol ω, which leads to a loss of information.

4.6 Stochastic Petri Nets

Stochastic Petri nets (SPNs) were introduced to address reliability and safety issues involving random phenomena. They associate stochastic (non-deterministic) firing times, distributed exponentially, with the transitions of the Petri net.

4.6.1 Definition of Stochastic Petri Nets

A stochastic Petri net is defined as a 5-tuple SPN=(P,T,E,μ,M_0), where:

- ✓ P={P_1,P_2,...,P_n}: Finite, non-empty set of places.
- ✓ T={T_1,T_2,...,T_m}: Finite, non-empty set of transitions. Each T_i is associated with a firing rate μ_i.
- ✓ E: Set of arcs.
- ✓ μ={μ_1,μ_2,...,μ_n}: Set of firing rates.
- ✓ M_0: Initial marking vector.

4.7 Analysis of Stochastic Petri Nets

Two complementary approaches are used to analyze SPNs:

1. **Markov processes**: Construct the reachable marking graph of the underlying autonomous Petri net. Each arc is labeled with a firing rate dependent on the transition's rate and the marking of its input places.
2. **Conservation properties**: Use Petri net invariants to analyze the system.

4.8 Advantages and Limitations of Petri Nets

4.8.1 Advantages

1. **Formal Definition**: Eliminates ambiguity with well-defined semantics for each model.
2. **Executable Models**: Tools exist to interpret Petri net models and simulate system behavior dynamically.
3. **Expressiveness**: Suitable for describing complex, reactive, or concurrent systems.
4. **Graphical Representation**: Enhances interpretation and understanding of the models.

4.8.2 Limitations

1. **Lack of Structuring**: As systems become more complex, models grow larger, making them harder to manage.
2. **Data Representation**: Place (transition) nets do not represent the data structures manipulated by the system.

5.1 Reliability

Reliability refers to the ability of a system or equipment to perform a required function under specified conditions for a given period of time. Reliability is the science of failures based on experience. It is inseparable from quality. The more components a machine has, the more likely its reliability tends to decrease. When components are too numerous or too complex, it often reaches a point where reliability control is no longer feasible, and the likelihood of a failure becomes very high. The unreliability of a product or asset increases after-sales costs (warranty claims, legal fees, etc.). Building more reliable products increases design and production costs. The total cost of the product will take into account these two opposing trends.

5.1.2 Reliability Indicators: λ and MTBF

failure rate and MTBF (Mean Time Between Failures) are the two main reliability indicators used in the industry.

5.1.2.1 Failure Rate (λ)

λ represents the failure rate or breakdown rate. It characterizes the rate of change in reliability over time.

For a given work period, the total time spent in active service:

$$\boldsymbol{\lambda} = \frac{number\ of\ failures}{\text{total time in service}} \tag{5.1}$$

Remark 5.1: Total operating time = total time in service downtime due to failures.
The units used are: the number of failures per hour, failure percentage, etc.

5.1.2.2 Mean Time Between Failures (MTBF)

MTBF is often translated as the average operating time but actually represents the average time between two failures.

time in service	Failure	**time in service**	Failure	**time in service**

Figure 5.1: Operation of equipment.

Physically, the MTBF can be expressed by the ratio of times:

$$\text{MTBF} = \frac{\text{Sum of operating times between the n failures}}{\text{Number of maintenance interventions with downtime}} \tag{5.2}$$

if λ is constant: $\text{MTBF}=\frac{1}{\lambda}$

By definition, the MTBF is the average lifespan of the system.

Example

An industrial compressor has operated for 9,000 hours in continuous service with 5 breakdowns, each lasting respectively: 7, 22, 8.5, 3.5, and 9 hours. Determine its MTBF.

$$MTBF = \frac{\text{Total duration of proper operation}}{\text{Total number of failures during service}} = \frac{9000 - (7 + 22 + 8.5 + 3.5 + 9)}{5} = \frac{8950}{5} = 1790 \text{ h}$$

Example

An asynchronous motor in a cement factory operated for one year, excluding weekends, with 4 breakdowns, each lasting respectively: $24, 48, 100, 96, and\ 72$ hours. Determine its failure rate.

5.1.2.3 The Different Phases of a Product's Lifecycle

The evolution of a product's failure rate throughout its lifecycle is characterized by what is known in reliability analysis as the bathtub curve**.**

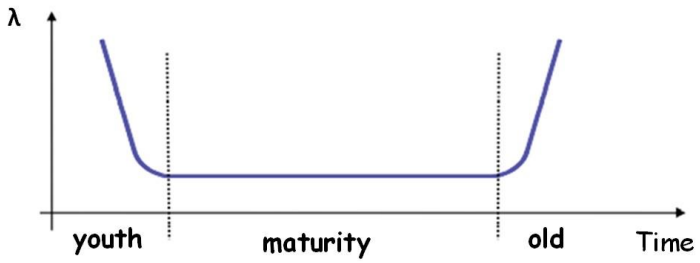


Figure 5.2 : bathtub curve**.**

5.1.3 Reliability of a System Composed of Multiple Components

5.1.3.1 Series System

The reliability R(s) of a system composed of "n" components $A, B, C, \dots, n$, connected in series is equal to the product of the respective reliabilities R_A , R_B , R_C , …, R_n of each component.

Figure 5.3: Components in Series.

The reliability is calculated using the following formula:

$$R_s = R_A \times R_B \times R_C \times \dots\dots\dots \times R_n \Longrightarrow R_s = e^{-\lambda_A t} \times e^{-\lambda_B t} \times e^{-\lambda_C t} \times \dots\dots \times e^{-\lambda_n t} \quad (5.3)$$

where: $MTBF = \frac{1}{\lambda_A + \lambda_B + \lambda_C + \dots\dots + \lambda_n}$

In a series system, the overall reliability decreases as more components are added because the failure of any single component leads to the failure of the entire system.

If, in addition, the components are identical:

$$\lambda_A = \lambda_B = \lambda_C = \cdots = \lambda_n \quad (5.4)$$

$$R_s = e^{-n\lambda t}, \text{ and MBTF} = \frac{1}{n\lambda}$$

Example

Consider a radio set composed of four components connected in series: a power supply with R_A=0.95, a receiver section with R_B=0.92, an amplifier with R_C=0.97, and a speaker with R_D=0.89. Determine the reliability R_s of the device.

$$R_S = R_A . R_B . R_C . R_D = 0.95 \times 0.92 \times 0.97 \times 0.89 = 0.7545 \ (75\%) \quad (5.5)$$

Example

Consider a printer composed of 2000 components connected in series, all assumed to have the same very high reliability R=0.9999. Determine the printer's reliability.

$$Rs = 0.9999^{2000} = 0.82 \quad (5.6)$$

Thus, the reliability of the printer is **82%**.

Exemple

A scanner with a total reliability of Rs=85% contains n components of the same reliability R=0.2. Calculate the number of components in the scanner.

We use the formula for the reliability of components connected in series:

$$R_s = R^n \quad (5.7)$$

Given Rs=0.85 and R=0.2, solve for n:

$$0.85 = 0.2^n \quad (5.8)$$

Take the natural logarithm of both sides:

$$\ln(0.85) = n * \ln(0.2) \quad (5.9)$$

Since n must be an integer, round n to the nearest whole number:

$$n \approx 1.6 \approx 2 \quad (5.10)$$

Thus, the scanner contains approximately **2 components**.

5.1.3.2 Parallel System

Active Redundancy

The reliability of a system can be increased by placing components (identical or not) in parallel. A device composed of "n" components in parallel will only fail if all "n" components fail at the same time.

Consider the "n" components in the figure below, connected in parallel. If the failure probability for each identified component (i) is denoted by F_i , then:

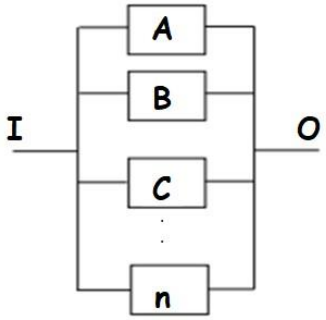


Figure 5.4: Parallel Components

The reliability R_p of the system is given by the following relationship:

$$R_p = 1 - (1 - R_A) \times (1 - R_b) \times (1 - R_c) \times \ldots \times (1 - R_n) \qquad (5.11)$$

If the "n" components are identical ($R=R_A=R_B=\cdots=R_n$) and all have the same reliability R, the expression for the system's reliability R_p becomes:

$$R_p=1-(1-R)^n \qquad (5.12)$$

This formula calculates the overall reliability of a system composed of identical components arranged in parallel. The system's reliability increases as more components are added in parallel, provided each component has the same reliability.

Example

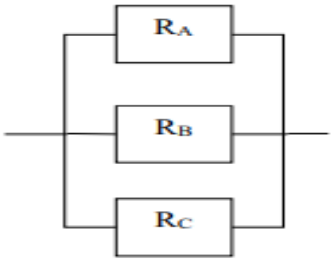
Three devices A, B, and C with the same reliability $R_A= R_B = R_C = 0.75$ are connected in parallel.

a) Determining the reliability of the system

Using the formula for parallel system reliability:

$$R_p=1-(1-R_A)(1-R_B)(1-R_C) \qquad (5.13)$$

Since $R_A=R_B=R_C=0.75$, we can simplify the equation:



$R_p = 1 - (1 - R_A) \times (1 - R_B) \times (1 - R_C) \Longrightarrow R_p = 1 - (1 - 0.75)^3 = 0.984 = 98.4\%$ (5.14)

Thus, the reliability of the system is approximately **0.9844** or **98.44%**.

b) How many devices in parallel would be needed to achieve a global reliability of 99%?

We want to determine the number of identical devices n required to reach a system reliability of 99% (Rp=0.99) when each device has a reliability of R=0.75. The formula is:

$$R_p = 1 - (1 - 0.75)^n = 0.99 \Longrightarrow (0.25)^n = 0.001 \Longrightarrow \ln (0.25)^n = ln(0.01) \quad (5.15)$$

$$\Longrightarrow n = ln(0.01) / \ln(0.25) \Longrightarrow n = 1.38 \quad (5.16)$$

Since n must be an integer, rounding up gives **1 device** in parallel to achieve a global reliability of 99%.

c) What should be the reliability R of each device if we want a global reliability of 99% with only three devices in parallel?

We are given that R_p=0.99 and n=3. The formula is:

$1 - (1 - R)^3 = 0.99 \Longrightarrow (1 - R)^3 = 0.01 \Longrightarrow (1 - R) = \sqrt[3]{0.01} \Longrightarrow R = 1 - \sqrt[3]{0.01} \Longrightarrow R = 1 - 0.2154 = 0.7846 \Longrightarrow R = 78.46\ \%$.

Thus, each device should have a reliability of approximately **0.7846** (or **78.46%**) to achieve a global reliability of 99% with three devices in parallel.

Passive Redundancy

a) Case of Two Standby Components:

If A and B are not identical, the relationship becomes more complex, factoring in the differing reliability of each component.

$$R(t) = \frac{\lambda_A}{\lambda_B - \lambda_A} (e^{-\lambda_A t} - e^{-\lambda_B t}) + \quad (5.17)$$

b) Case of n Standby Components

Following the same approach, if the active component A fails, it is replaced by component B. If B fails, it is automatically replaced by C, and this process continues. If all components are identical and have a constant failure rate λ, the reliability of the system is given by:

$$R(t) = e^{\lambda t}\left(1 + \lambda t + \frac{(\lambda t)^2}{2!} + \cdots + \frac{(\lambda t)^n}{n!}\right) \quad (5.18)$$

c) Combination of Series and Parallel Components

This scenario involves a process of simplifying the system's structure by combining components that are in series or parallel. The goal is to reduce the system into branches that are easy to analyze. For series components, the overall reliability is the product of the individual reliabilities, while for parallel components, the overall reliability is determined by the redundancy formula for parallel systems. The system's total reliability can be computed by iteratively simplifying these combinations into manageable terms.

5.2 **Maintainability**

5.2.1 Definition

For a given entity, used under specified operating conditions, maintainability is the probability that a given active maintenance operation can be performed within a specified time interval, assuming maintenance is carried out under given conditions using prescribed procedures and tools. Maintainability aims to optimize intervention time to increase production time by reducing delays caused by:

- Time spent waiting for replacement parts;
- Time spent completing documentation;
- Time spent preparing for the action.

Its indicator is **MTTR** (Mean Time to Repair), which is calculated as follows:

$$MTTR = \frac{\text{Total downtime}}{\text{Number of downtimes}} \quad (5.19)$$

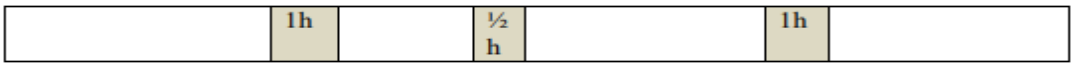
This calculation provides an average time it takes to repair a system or component, contributing to better planning and efficiency in maintenance operations.

5.2.2 Repair Rate (μ)

The repair rate μ is the reciprocal of the MTTR, and is calculated as: $\mu = \frac{1}{MTTR}$

Example

The figure below illustrates the operation of a piece of equipment over a 24-hour period.



Calculate the MTTR and the repair rate μ.

Solution

$MTTR = 2.5 / 3 = 0.83h$, $\mu = 1.2h^{-1}$ (5.19)

The repair rate indicates the ability of an asset to be repaired or restored to operation. When the repair rate μ is constant, the maintainability function is given by:

$$M(t) = 1 - e^{-\mu t} \quad (5.20)$$

This formula represents the probability that a system will be repaired within time t.

5.3 Availability

5.3.1 Definition

Availability is the ability of an asset to be in a state to perform a required function under given conditions, at a specific moment or over a given time interval, assuming that the provision of necessary external resources is ensured. This ability depends on the combination of reliability, maintainability, and maintenance logistics.

Example

My car is "ready" when I want to use it (it is not at the mechanic's, it is operational). If the life durations and repair durations follow an exponential distribution with constant failure rate λ and repair rate μ, the instantaneous availability is given by the expression:

$$A(t) = \frac{\mu}{\mu + \lambda} + \frac{\lambda}{\mu + \lambda} e^{-(\lambda+\mu)t} \quad (5.21)$$

5.3.2 Availability Indicators

Availability (D) over a given time interval can be evaluated by the ratio:

$$D = \frac{UpTime}{UpTime + DownTime} = \frac{MUT}{MUT + MDT} = \frac{MTBF}{MTBF + MTTR} \quad (5.22)$$

Where:

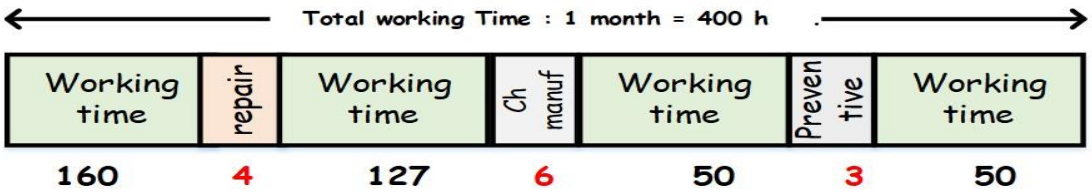
- **MUT**: Mean Up Time (average time of availability),
- **MDT**: Mean Down Time (average time of unavailability).

Example

A machine tool manufacturer agrees with its client on the intrinsic availability of a machine, taking into account ideal operating and maintenance conditions:

- 1 production change per month, with an average change time of 6 hours.
- Corrective maintenance:
  - ✓ Failure rate: 1 failure per month.
  - ✓ Average repair time: 4 hours.
- 3 hours of preventive maintenance per month.

Calculate the intrinsic availability (times are expressed in hours): Operating time per month = 400 hours.



Solution:

$$D = \frac{available\ time}{available\ time + unavailable\ time} = \frac{160 + 127 + 50 + 50}{400} = \frac{387}{400} = 97\%$$

5.4 Safety

5.4.1 Definition

Safety is the ability of a system to avoid catastrophic failures over a given period.

5.4.2 Safety Measures

We can distinguish safety measures based on their mode of action: **passive safety** and **active safety**.

5.4.2.1 Passive Safety

Passive safety refers to all elements that aim to reduce the consequences of an accident when it cannot be avoided. It operates solely by its presence, without human intervention or energy requirements. However, passive safety should not be limited to minimizing accident consequences (e.g., electrical insulation is both a passive and preventive measure).

5.4.2.2 Active Safety

Active safety refers to all elements aimed at preventing accidents. It requires action, energy, and maintenance (e.g., detectors, valves). The safety of an installation relies on both passive and active safety measures. Preference is given to passive measures when technically possible. Active measures require high-quality standards, particularly **first failure tolerance** (e.g., redundancy of safety devices). Functional safety remains one of the most important means of addressing risks. Other means, such as **safety integrated into design**, are also critically important for risk reduction or elimination.

6.1 Predictive Reliability

Predictive reliability allows the estimation of the a priori reliability of a component, equipment, or system. This is achieved by assimilating the behavior of each elementary constituent to mathematical probability models and physical aging processes. Experience feedback and testing are the basis for constructing these behavioral models from a reliability perspective.

6.1.1 Predictive Calculations

In the field of electronics, there are several collections of predictive models for elementary components such as resistors, capacitors, integrated circuits, etc. The most widely used electronic reliability prediction standards are:

- **MIL-HDBK-217F**: A U.S. military standard designed to estimate the reliability of equipment.
- **RDF2000**: A reliability guide built from France Telecom's experience feedback, which has been transformed into a standard known as **UTE C 80-810**.
- **FIDES**: A predictive reliability guide built on the basis of previous collections, using experience feedback from a consortium of French industrial companies. This collection was transformed into a standard known as **UTE C 80-811**.

6.1.2 Objectives

- Determine the constraints that influence the reliability of each component.
- Estimate the potential reliability of new equipment.
- Compare different solutions.
- Evaluate the stock of spare parts needed for maintenance.
- Identify manufacturing deviations.

6.2 System Failures

6.2.1 Failure Classification

Failures can be classified into four types:

- **Loss of function**: The function ceases to be performed.
- **Degradation of function**: The function is performed, but with diminished performance.
- **No function**: The function does not occur when needed.
- **Unintentional function**: The function occurs when it is not solicited.

This classification helps in analyzing and addressing reliability concerns in systems based on the nature of the failure.

Table 1: Failure Classification and Examples of Quality Defects and Failure Modes

Failure Classification	Examples of Quality Defects and Failure Modes
Process Failure	- Cracking, scratching - Incorrect dimensions or shape - Poor surface finish - Deformation - Misalignment - Positioning defect - Assembly defect - Missing part
Loss of Element Function	- Breakage - Blockage, seizing, jamming - Obstruction - Leakage
Degradation of Element Function	- Play, poor guidance - Friction - Wear, fatigue, corrosion - Misalignment, eccentricity - Loosening, disintegration - Clogging - Contamination

6.2.2 Causes of Failure

Failure causes may be related to the design, manufacturing, or operation of the system. Failure causes can be:

- **Internal** to the element.
- **External** to the element.

6.2.2.1 Classification of Failure Causes

Table 2: Classification of Failure Causes and Examples

Failure Cause Classification	Examples of Failure Causes
Design	- Non-compliance with specifications - Underdimensioning, low safety factor - Unreliable component - Inadequate technology - Tolerance or dimensioning errors - Poor choice of shape or material
Manufacturing and Production	- Non-compliance with plans or materials - Internal material defect - Poorly executed operation - Worn or damaged tool - Faulty installation - Handling error
Operating Environment	- Temperature - Humidity - Vibrations, shocks - Pollution - Tools, processed product - Fixation, installation

Operation	- Adjustment - Improper or overloaded usage - Maintenance defect - Natural or accelerated wear, fatigue - Mechanical stresses
Other System	- Power source - Upstream, downstream system

6.2.3 Effects of Failure

Consequences of failure on:

- System functionality and physical condition
- System availability
- System maintenance
- User safety
- System environment

6.2.3.1 Classification of Failure Effects

Effects on subsequent operations:

- Disruption of flow
- Production stoppage
- Process degradation
- Operator safety
- Environmental impact

Table 3: Classification of Failure Effects and Examples

Classification of Failure Effects	Examples of Failure Effects
Effect on System Functionality and Physical State	- Functional failure - Performance losses - Material damage, breakdowns - Failures, stoppages
Effect on Availability	- Production flow downtime - Slowed cadence - Cycle lengthening - Product non-compliance - Rework, downgrading, derogation
Effect on Maintenance	- Repair costs - Direct maintenance costs
Effect on User Safety and System Environment	- Bodily harm - Pollution, contamination
Effect on Subsequent Operations	- Flow disruption - Production halt - Process degradation - Operator safety - Environment

6.2.4 Failure Criticality

Each failure can be assigned a criticality level based on frequency, severity, and probability of non-detection.

- **Frequency**: Likelihood or occurrence of a failure due to a specific cause.
- **Severity**: Impact of failure effects on the system or user.
- **Probability of Non-Detection**: Risk of a failure going undetected before it reaches the system user.

Criticality is determined by its frequency, severity, and probability of non-detection levels.

- **Criticality Threshold**: A limit (reached by criticality or by one of the criteria) at which a failure is deemed critical.

6.2.4.1 Principle of Criticality Evaluation

Rating scales are used to assess the frequency (F), severity (G), and probability of non-detection (N) criteria.

The criticality C value is calculated as the product of the three criteria:

$$C=F\times G\times N. \quad (6.1)$$

The evaluation applies to each cause-failure-effect association.

6.2.4.2 Principle of Rating Scales

Table 4: Rating Scale for Frequency, Severity, and Non-Detection Probability

Rating	Frequency F	Severity G	Non-Detection Probability N
1	Very Low	Minor	Detectable with certainty
2	Low	Significant	Detection possible
3	Medium	Medium	Detection improbable
4	High	Major	Undetectable
5	Catastrophic	Catastrophic	Not detectable

6.3 Failure Mode and Criticality Analysis (FMEA)

FMEA is a qualitative analysis technique for evaluating the functional reliability of industrial systems by analyzing failure risks. This method can be applied throughout the system's life cycle:

- Design of a new product
- Improvement of an existing product
- Industrialization and manufacturing
- Operation and maintenance
  FMEA is an inductive, systematic, and predictive analysis method focused on:
- System failures
- Their causes and consequences
  The method enables:

- Identification of critical points
- Definition of appropriate corrective actions

6.3.1 Types of FMEA

Table 5: FMEA Types and Objectives

Type	Objectives
Product FMEA	Ensure product reliability by improving its design.
Process FMEA	Ensure product quality by improving production operations.
Production Equipment FMEA (Machine FMEA)	Ensure the availability and safety of production equipment by improving its design, operation, or maintenance.

6.3.3 Advantages and Limitations of FMEA

6.3.3.1 Advantages

Indirect Benefits

1. Increased productivity.
2. Centralization of technical documentation.
3. Implementation of follow-up sheets for operator visits.

Impact on Maintenance

1. Optimization of cause/consequence pairs.
2. Enhanced monitoring and testing.
3. Maintenance optimization.

Impact on Quality

1. Better material/functional alignment.
2. Increased efficiency in development/manufacturing.
3. Enhanced operational efficiency.

Common Errors to Avoid

- An incompetent working group facilitator.
- An oversized working group.
- Focusing on an external failure outside the study scope (poorly defined subject).
- Confusing Production Equipment FMEA with Process FMEA.

6.3.3.2 Limitations of the FMEA Method

Although widely used, it is incorrect to claim that FMEA is a universal tool. FMEA has several limitations:

- It depends on a thorough functional analysis.
- It requires a rigorous and often resource-intensive methodology for preparation, analysis, and implementation within the company.

- Although primarily used for preventive treatment of failures, it must rely on existing expertise within the company, from which the working group can extrapolate its findings.

6.4 Fault Diagnosis and Maintenance Techniques

Diagnosis is a crucial phase of corrective maintenance. The effectiveness of the intervention depends on the accuracy and speed of the diagnosis. Generally, 90% of faults are easy to identify (the maintenance technician is familiar with the machine); however, many failures do not have an obvious cause. It is necessary to conduct a diagnosis to identify the root cause. This search is not random; for it to be effective, it must follow a method. This document aims to explain the method, but for it to be fully applicable, the following conditions must be met:

- **Knowledge Requirement**: Anyone performing a system diagnosis must have a comprehensive understanding of the system's function and the process it enables. This knowledge should include the machine's purpose, its cycle, composition, and associated risks in all operating modes, especially in setup and manual modes, where the operator must act responsibly.
- **Up-to-Date Documentation**: The system's documentation must be available and current. Unfortunately, this requirement is rarely met in the industry (incomplete documentation, missing updates). It is essential to remember that maintaining documentation is as crucial as maintaining the system itself, and it often falls to the maintenance department to ensure documentation accuracy.

Step 1: Identifying the Failure

The failure can be identified:

- **Visually**: For example, an operator notices and reports the failure, providing more or less precise details.
- **Automatically**: Through the detection of an abnormal situation (e.g., exceeding a movement recovery time, triggering an alarm by the automation system).

The indication of a problem can range from the illumination of a simple indicator light to a signal sent to a supervisory system, or a local display on the machine.

In all cases, the following questions must be addressed:

- ✓ How is the failure manifesting?
- ✓ Machine stopped?
- ✓ Non-compliant movement?
- ✓ Motor not running?
- ✓ Cylinder not moving?
- ✓ At what stage of the cycle did the system fail? What can be observed at this stage?
- ✓ Indicator lights on the PLC and machine.
- ✓ Messages (if a display is present).
- ✓ State of the machine.
- ✓ Etc.
- ✓ Do we already have an initial idea of the potential area of failure?

The analysis conducted during this step will guide the subsequent diagnostic efforts. It becomes evident how critical it is to have thorough knowledge of the machine to ensure accurate guidance.

The goal of the diagnostic process is to narrow down the failure by reducing the scope of investigation step by step until the fault is identified.

Step 2: Risk Analysis

Before starting the work, it is essential to define the safety measures to be implemented. The objectives are as follows:

- **Protect yourself**: Ensure personal safety during the intervention.
- **Protect others**: Safeguard bystanders, especially those who may unintentionally interfere with the machine.
- **Protect the equipment**: Prevent potential damage to the machine.

Key risk factors to consider include:

- Pressurized fluids.
- Thermal hazards.
- Electrical energy.
- Incoming and outgoing production flows of the machine.
- Mechanical hazards.

Recommended safety measures

1. Use protective equipment (e.g., gloves, goggles, insulating mats, insulated tools, etc.).
2. Delimit the work area with barriers to prevent unauthorized access.
3. Display warning signs to indicate potential dangers.
4. Issue a work permit if required.
5. Lock out or tag out the equipment when necessary.
6. Verify measuring instruments to ensure accuracy.

If measurements (such as voltage or current) are required, do not immediately lock out the entire system. Only isolate or disable the faulty section as necessary for repairs.

Important Notes:

- When locking out or tagging out the equipment, ensure that there is no residual voltage.
- Electrical interventions require proper certification or authorization.

Step 3: Identifying the Functional Chain

This step involves interpreting observations based on a thorough understanding of the machine and its operating cycle to identify all functional chains related to the failure.

This is the most critical and delicate point of the analysis.

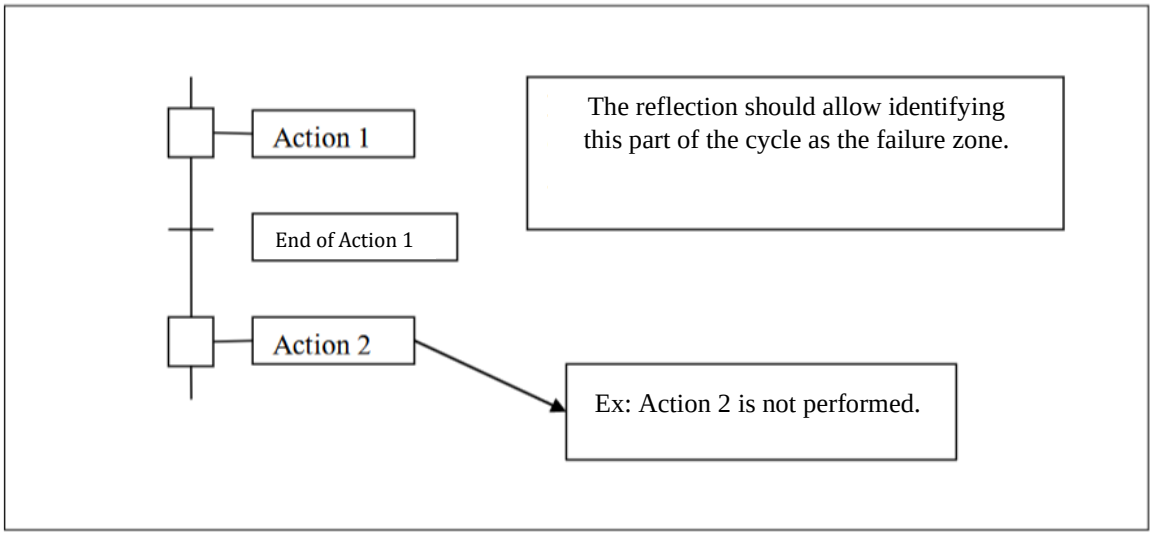


Figure 6.1: Functional Chain Analysis

Process

Identify one or more functional chains that might be responsible for the failure:

1. **Control chains**: These are responsible for initiating actions.
2. **Acquisition chains**: These receive and process information to trigger actions.

These functional chains can be represented as block diagrams for clarity and better analysis (see Figure 6.1).

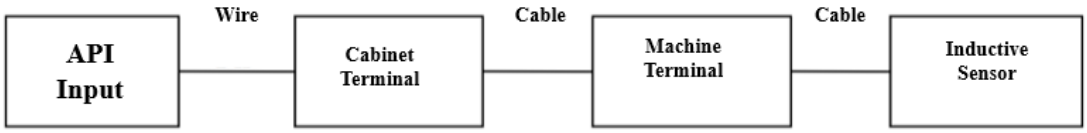


Figure 6.2: Functional Chain

Logical Reasoning

Once the functional chains are identified, the next step is to determine which chain is defective. This requires logical reasoning, supported by:

- Detailed knowledge of the machine's operating cycle.
- Comprehensive review of the available technical documentation.

Diagnostic Tips

- Use indicators on the PLC's I/O boards:
  - ✓ **Input and output indicators off**: Likely a sensor chain failure.
  - ✓ **Input and output indicators on**: Likely an actuator chain failure.

By narrowing down the analysis systematically, you can identify the defective functional chain and proceed with the appropriate corrective actions.

Additional Diagnostic Tests for Validation

Some simple, overarching tests can be performed to confirm the diagnostic reasoning:

- **Testing a sensor functional chain**
  A sensor chain can be easily tested by manually triggering the sensor:
  - ✓ For example, using a hand to trigger a photoelectric sensor or a mechanical contact.
  - ✓ For an inductive sensor, a metallic object can be used. Simply observe whether the signal reaches the programmable logic controller (PLC) by checking the corresponding input indicator light.
- **Testing an actuator**
  Actuators can also be tested manually, provided that safety is not compromised and the technician knows what they are doing.
  - ✓ For instance, manually forcing the contacts of a contactor can help verify whether the electrical power chain downstream is functioning properly or not. However, such manual forcing should be brief to avoid any risk of damage to the machine.
  - ✓ Similarly, manually actuating a pneumatic distributor can be used to confirm the proper functioning of the pneumatic circuit downstream of the distributor.

Remark : The use of the programming console proves to be very useful here for those who know how to use it.

Step 4: Listing the Chain Components

Once the functional chain has been identified, the next step is to exhaustively list its components. This includes all the elements that make up the chain:

Acquisition Chain (Input)

- PLC input card.
- Wires and terminals.
- Connectors and terminals.
- Contacts and their connections.
- Sensors and their settings.

Control Chain (Output)

- PLC output card.
- Wires and terminals.
- Connectors and terminals.
- Relay and contactor contacts with their connections.
- Relay and contactor coils with their connections.
- Electro-distributors (connectors, coils, solenoid valves, distributors).
- Pneumatic tubes or hydraulic pipes.
- Fittings.
- Flow limiters.
- Cylinders.

- Motors.
- Mechanical couplings.

An up-to-date technical dossier (electrical, pneumatic, hydraulic, mechanical) is particularly useful at this stage.

Step 5: Listing Failure Modes

For each component in the chain, identify possible failure modes that could explain the observed malfunction.

Example

- If a motor does not run, it could be due to a broken wire between the PLC output and the contactor coil.
- A mechanical misalignment or adjustment can also be considered a failure (e.g., misaligned photoelectric sensor, loose coupling).

This analysis can be presented in a user-friendly format, such as:

- Cause-and-effect tables.
- Ishikawa diagrams (Fishbone diagrams).
- Other visual tools.

Step 6: Test Criteria

Each component in the chain, along with its failure modes, must be tested using criteria designed to minimize downtime. These criteria include:

- **Speed**: Prioritize quick checks.
- **Probability**: Focus on the most likely causes.
- **Accessibility**: Test easily reachable components first.

This applies across various domains:

- Electrical.
- Pneumatic.
- Hydraulic.
- Mechanical.

Example
If a lightbulb doesn’t light up, it is more reasonable to suspect it is burnt out (based on probability and speed) rather than breaking the wall to locate a cable fault.

Start with "visual" tests that do not require instruments, such as checking connections. Tests requiring disassembly should be performed last.

For electrical measurements, prioritize voltage tests over continuity checks. Continuity tests require isolating the circuits, while current measurements should be done only when absolutely

necessary since they involve connecting the device in series with the circuit and observing amperage limits.

Step 7: Testing Procedures

For each failure mode identified in Step 5, design a test. These tests should be presented in the order defined in Step 6.

TableFormat:
The test table should include the following:

- **Component to be tested**.
- **Test method** (visual, with instrument, etc.).
- **Instrument used**, if applicable.
- **Specific testing points** (e.g., where to place voltmeter probes).
- **Expected results** of the test.
- **Additional observations**, if any.

Example
Measure voltage with a multimeter between 0V and terminal X1/7. The expected result is 24V.

Once all tests are exhaustively defined, proceed to the active diagnostic phase, performing the tests one by one. Document the results in the "measurement" column of the test table. When a result deviates from the expected value, the defective component has been identified.

Example
In a given configuration, the sensor contact should be closed.

- If the sensor is closed, Test 2 should show 24V at the input terminal.
- A 0V reading indicates a faulty or misaligned sensor or a connection issue at the sensor.

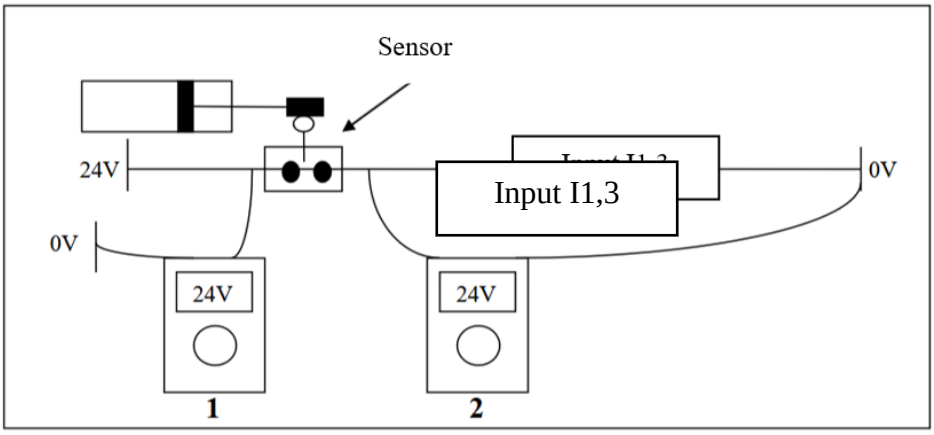


Figure 6.3: Voltage Measurement Using a Multimeter

Step 8: Repair

Once the defective component is identified, replace it and test the machine again.

If immediate repair is not possible (e.g., due to unavailability of parts), evaluate options for operating the system in degraded mode to avoid production downtime.

Step 9: Maintenance Report

Corrective maintenance interventions must be documented within the company's maintenance system. This documentation serves as a historical record that can be used for future analysis.

The report can be written or digital and should include the following minimum information:

- Machine reference.
- Nature of the intervention.
- Date and time of the intervention.
- Identification of the technician.
- Duration of the intervention.
- Details of replaced parts, if an

References

[1] :Patrick Lyonnet, Ingénierie de fiabilité. Edition TEC & DOC, Lavoisier, 2006.

[2] : Roger Serra, Fiabilité et maintenance industrielle. Cours, Ecole de technologie supérieure ETS, Université de Québec, 2013.

[3] : Yann Morère, Cours de réseau de Petri. Avril 2002. http://www.morere.eu/IMG/pdf/cours_petri2.pdf

[4] : Claire Pagetti, Module de sûreté de fonctionnement. décembre 2012.

https://www.onera.fr/sites/default/files/u490/cours.pdf

[5] : David Smith, Fiabilité, Maintenance et risque. DUNOD, Paris 2006.

[6] : Laurence Gardes, Méthodologie d'analyse des dysfonctionnements des systèmes pour une meilleure maitrise des risques industriels dans les PME : application au secteur du traitement de surface. Sciences de l'environnement. Ecole Nationale Supérieure des Mines de Saint-Etienne; INSA de Lyon, 2001. Français. https://tel.archives-ouvertes.fr/tel-00806215

[7] : Pierre-Yves Chaux, Formalisation de la cohérence et calcul des séquences de coupe minimales pour les systèmes binaires dynamiques et réparables. Autre. École normale supérieure de Cachan - ENS Cachan, 2013. Français.https://tel.archives-ouvertes.fr/tel-00910331

[8] : Malika MEDKOUR , K Azzedine BOUZAOUIT, Diagnostic des défauts par la

[9] Patrick Lyonnet, "Ingénierie de la fiabilité, Edition TEC & DOC, Lavoisier, 2006.

[10] : Roger Serra, "Fiabilité et maintenance industrielle", Cours, Ecole de technologie supérieure ETS, Université de Québec, 2013.

[11] : David Smith, Fiabilité, maintenance et risque, DUNOD, Paris 2006 conversion d'un arbre de défaillance en Réseau Bayésien. Actes de la 2ème Conférence Internationale de Mécanique (ICM'15). Constantine, Algérie. 25-26 Novembre 2015.

http://archives.umc.edu.dz/bitstream/handle/123456789/132853/article6.pdf?sequence=1&isAllowed=y

[12]: A. Rauzy, New algorithms for fault trees analysis. Reliab Engng Syst Saf 40 (1993),pp. 203-211 http://iml.univ-mrs.fr/~arauzy/publis/Rau93a.pdf.zip

[13] : Polycopié de cours du module ''Maintenance et sûreté de fonctionnement'' Dr. Belhadj

Djilali Abdelkadir , à l'Université de chlef.