# Reliability, Safety and Risk Analysis

***Lecture notes***

Francesco Circhetta

May 25, 2022

# Contents

CHAPTER 1

# Introduction

## 1.1 Why reliability is so important?

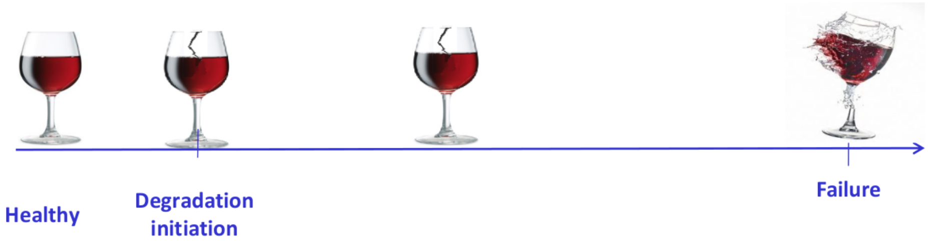

Figure 1.1: Evolution to failure...

A component, even if very well designed, built with durable materials from the best manufacturer in the world, will eventually start degrading → *onset of a degradation process.*

Degradation won't stop and, without proper countermeasures, the component will fail at a given point. We cannot ignore it!

CHAPTER 2

# Availability and Maintainability

## 2.1 Introduction

*Can I repair the system after a failure?* We can classify systems into two categories according to the answer to this question.

- **Non maintained systems** These systems cannot be repaired after a failure (e.g. a telecommunication satellite, a F1 engine, a vessel of a nuclear power plant).

  $\rightarrow$ a good *performance parameter* is the *reliability*, as it quantifies the system capability of satisfying a specified mission within an assigned period of time ($T_M$): $R(T_M) = P(T > T_M)$

- **Maintained systems** These systems can be repaired after the failure (e.g. pump of an energy production plant, a component of the reactor emergency cooling systems).

  $\rightarrow$ a good *performance parameter* is the *availability*, as it quantifies the system ability to fulfill the assigned mission at any specific moment in the lifetime: $A(t)$.

We will now try to give now a more rigorous definition of *availability*.

## 2.2 Definition of Availability

Let's tackle the problem from a mathematical point of view.

We introduce an indicator variable $X(t)$ such that:

$$X(t) = \begin{cases} 1 & \text{system is operating at time } t \\ 0 & \text{system is failed at time } t \end{cases}$$

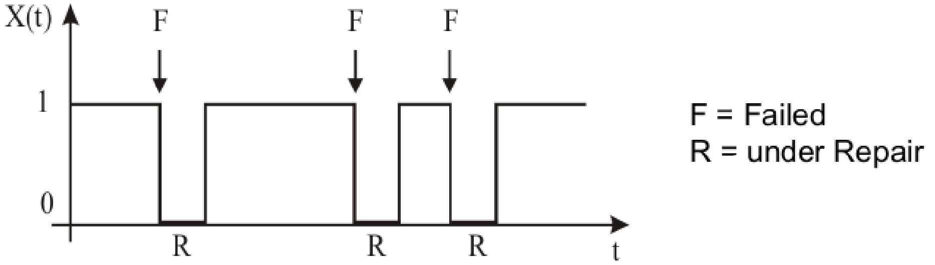

Figure 2.1: An example of $X(t)$ for a given system

### 2.2.1 Instantaneous availability

$$p(t) = P\{X(t) = 1\} = E[X(t)]$$

Notice that:

$$E[X(t)] = \sum_{i=0}^{1} iP\{X(t) = i\} = 0 \cdot P\{X(t) = 0\} + 1 \cdot P\{X(t) = 1\} = p(t)$$

### 2.2.2 Instantaneous unavailability

$$q(t) = P\{X(t) = 0\} = 1 - p(t)$$

where the last equivalence comes from the fact that the two events ”system is operating at time t” and ”system is failed at time t” are mutually exclusive.

## 2.3 Contributions to Unavailability

### 2.3.1 Repair

A component can be unavailable because it is under repair after a failure.

### 2.3.2 Testing / Preventive Maintenance

### 2.3.3 Unrevealed failure

## 2.4 Average availability descriptors