Reliability, Safety and Risk Analysis

Lecture notes

Francesco Circhetta

July 11, 2022

Contents

Chapter 1

Introduction

1.1 Why reliability is so important?

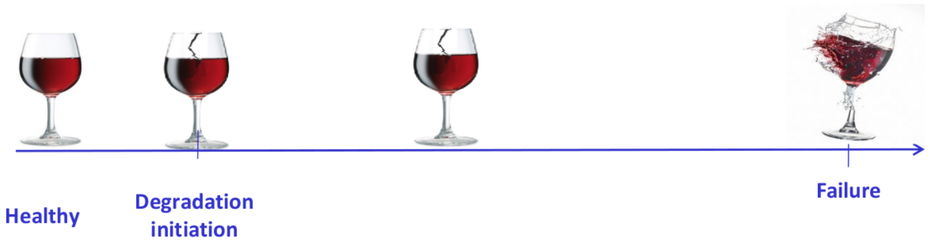

Figure 1.1: Evolution to failure...

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!

1.2 Examples of Degradation

1.2.1 Creep of turbine blades

Creep failure is one of the most important failure modes of turbine blade. Creep is the progressive time-dependent inelastic deformation under mechanical load and high temperature.

The deformation may become so large that a turbine blade could cause the blade to contact the casing, resulting in the failure of the blade.

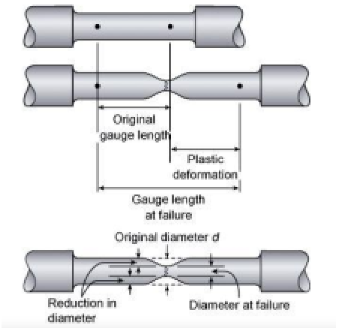

Figure 1.2: Cree of turbine blades

The rupture of one of multiple blades renders the turbine unbalanced, leading to the failure of the turbine bearings. The shock from such an accident can produce projectiles with a range in the order of a hundred metres.

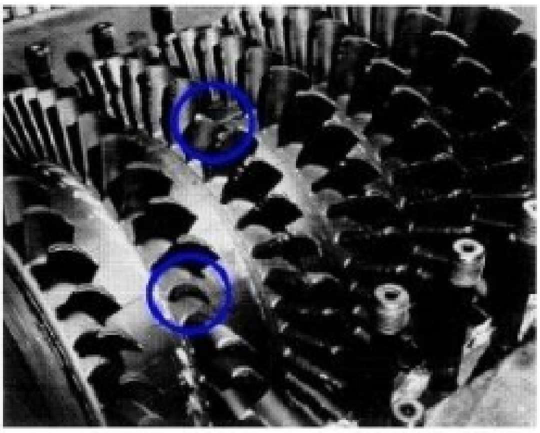

Figure 1.3: Turbine with blades damaged by creeping

1.2.2 Erosion of choke valves

The *choke valve* is a type of control valve, mostly used in oil and gas production wells to control the flow of well fluids being produced.

Choke valves allow fluid flow through a very small opening, designed to kill the reservoir pressure while regulating the well production. The reservoir fluids can contain sand particles. Hence the choke valves are usually designed to handle an erosive service.

Replacing a valve hundreds of metres under the sea level is a challenging task and should happen *as infrequently as possible.*

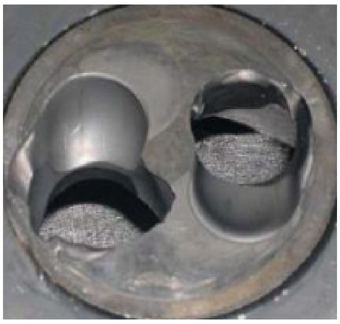

Figure 1.4: Erosion of a choke valve

1.2.3 Crack propagation

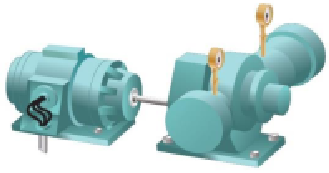

Figure 1.5: Pump driven by an electric motor

Bearings can suffer crack propagation, leading to possible catastrophic consequences in an engine.

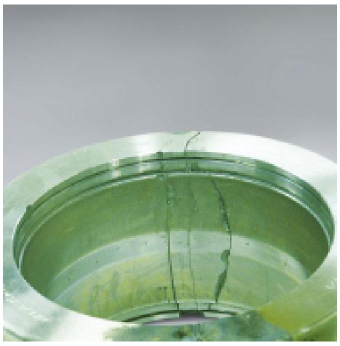

Figure 1.6: Crack propagation in bearing

1.3 Examples of Failure

1.3.1 From the Nuclear industry: the Devis-Besse accident

In March 2002, plant staff discovered that the borated water that serves as the reactor coolant had leaked from cracked control rod drive mechanisms directly above the reactor and eaten through more than 150 mm of the carbon steel reactor pressure vessel head (Fig. 1.7) over an area roughly the size of a football.

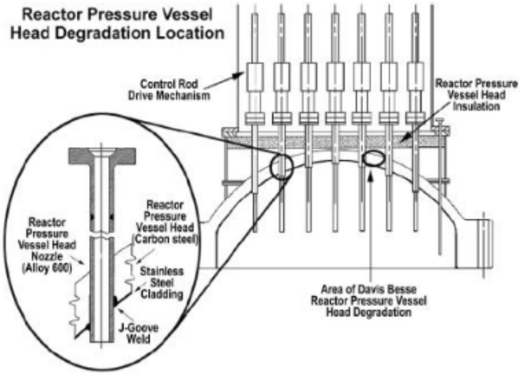

Figure 1.7: Reactor pressure vessel head

This significant reactor head wastage on the exterior of the reactor vessel head left only 9.5 mm of stainless steel cladding holding back the high-pressure (14.6 MPa) reactor coolant.

Consequences:

- 600 M$ spent for a new lid;
- the NRC kept Davis–Besse shut down until March 2004, so that FirstEnergy was able to perform all the necessary maintenance for safe operations (2 years).

Possible consequences in case of failure (rupture):

- *Loss Of Coolant Accident* that triggers emergency safety procedures to protect from core damage or meltdown. However, the jet of reactor coolant might have damaged adjacent control rod drive mechanisms, hampering or preventing reactor shutdown and leading to a core meltdown.

Figure 1.8: Explosion of the platform Deepwater Horizon

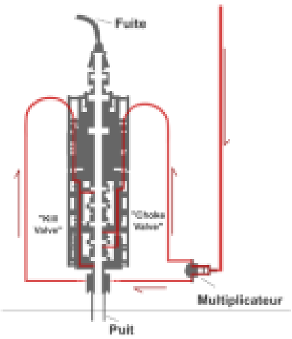

Figure 1.9: Probable cause: leakage in the oil pumping system

1.3.2 From the Oil and Gas industry: Deepwater Horizon oil spill

1.3.3 From the Railway industry: Brétigny-sur-Orge train crash

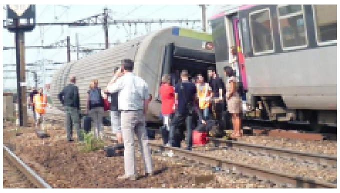

Figure 1.10: TODO

1.3.4 From Construction industry: Collapse of Morandi Bridge

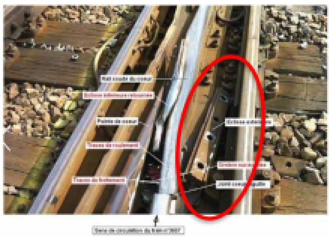

Figure 1.11: TODO

Chapter 2

Reliability of simple systems

2.0.1 Time-dependent systems

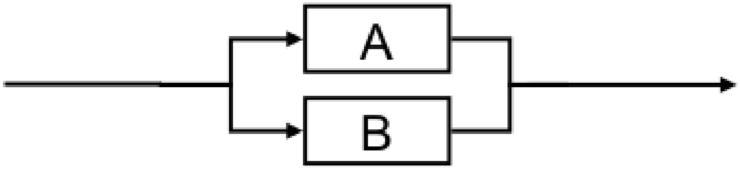

Figure 2.1: A and B are in parallel

When both A and B are fully energized, they share the total load and their failure densities are $f_A(t)$ and $f_B(t)$

If one component fails, the survivor must carry the full load and its failure density becomes $g_A(t)$ or $g_B(t)$

Find the reliability $R(t)$ of the system if:

- $f_A(t) = f_B(t) = \lambda e^{-\lambda t}$
- $g_A(t) = g_B(t) = k\lambda e^{-k\lambda t}$ where $k > 1$

Solution

$$
\begin{aligned}
R(t) &= P\{\text{system survives up to } t\} \\
&= P\{\text{neither component fails before t}\} \\
&\quad + P\{\text{one fails at some time } \tau < t, \\
&\qquad \text{the other one survives up to } \tau \text{, with } f(t), \\
&\qquad \text{and from } \tau \text{ to } t \text{ with } g(t)\}
\end{aligned}
$$

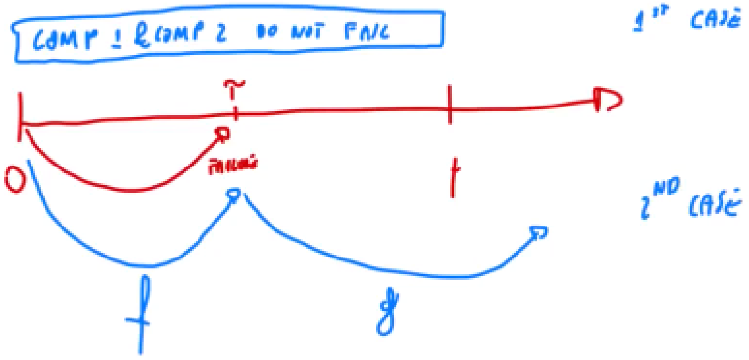

Figure 2.2: Timeline

These two cases are mutually exclusive, hence we can sum their probabilities:

$$
\begin{aligned}
R(t) &= R_f^2(t) + \int_0^t (f(\tau)d\tau)R_f(\tau)R_g(t-\tau) \\
&= e^{-2\lambda t} + 2\int_0^t (\lambda e^{-\lambda\tau}d\tau)(e^{-\lambda\tau})(e^{-k\lambda(t-\tau)}) \\
&= e^{-2\lambda t} + 2\lambda e^{-k\lambda t}\int_0^t e^{-\lambda(2-k)\tau}d\tau \\
&= \frac{2e^{-k\lambda t} - ke^{-2\lambda t}}{2-k}
\end{aligned}
$$

If $k = 1$ our system is equivalent to a parallel system!

2.1 Where to study?

Red book

- Chapter 5

Green book

- All problems in Chapter 5

Chapter 3

Availability and Maintainability

3.1 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*.

3.2 Definition of Availability

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

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

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

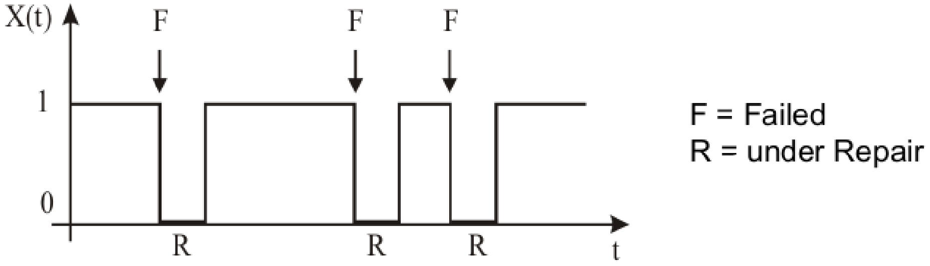

Figure 3.1: An example of $X(t)$ for a given system

3.2.1 Instantaneous availability

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

Notice that:

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

3.2.2 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.

3.3 Contributions to Unavailability

3.3.1 Repair

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

Figure 3.2: A component could be under repair

3.3.2 Testing / Preventive Maintenance

A component can be removed from the system because

a it must undergo preventive maintenance (e.g. periodic replacement of a transmission belt in a car, see Fig. 3.3)

Figure 3.3: Transmission belt in a car

b it has to be tested, i.e. safety systems and standby components are designed to operate only in extremely rare cases and spends most of their time in standby, thus requiring proper testing to ensure that they're still in good working conditions.

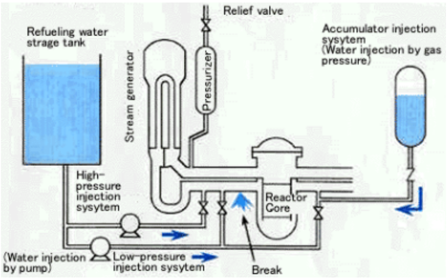
Relief valve
Refueling water strage tank
Stream generator
Pressurizer
Accumulator injection sysytem (Water injection by gas pressure)
High-pressure injection sysytem
Reactor Core
(Water injection by pump)
Low-pressure injection sysytem
Break

Figure 3.4: Emergency Core Cooling System in a Nuclear Power Plant

3.3.3 Unrevealed failure

A stand-by component can fail unnoticed. The system goes on without noticing the component failure until a test on the component is made or the component is demanded to function.

3.4 Average availability descriptors

How to compare different maintenance strategies? We need to define quantities for an *average* description of the system probabilistic behavior:

- If after some initial transient effects, the instantaneous availability assumes a time independent value → Limiting or *steady state availability*:

$$p = \lim_{t \to \infty} p(t)$$

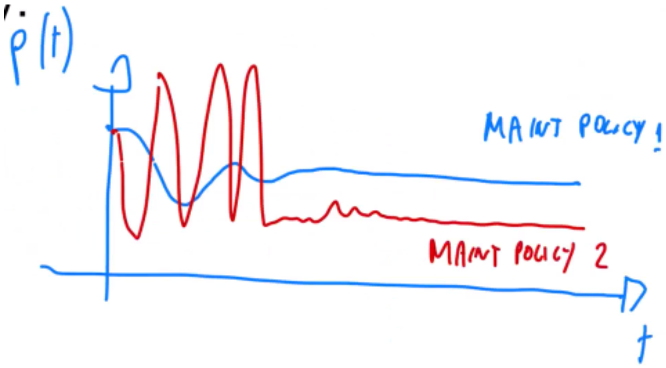

Figure 3.5: Using this descriptor, maintenance policy 2 is *better*

- If the limit does not exist (e.g. periodic behavior) → *Average availability* over a period of time T_p:

$$p_{T_p} = \frac{1}{T_p} \int_0^{T_p} p(t) dt = \cdots = \frac{\overline{\text{UPTIME}}}{T_p}$$

$$q_{T_p} = \frac{1}{T_p} \int_0^{T_p} q(t) dt = \cdots = \frac{\overline{\text{DOWNTIME}}}{T_p}$$

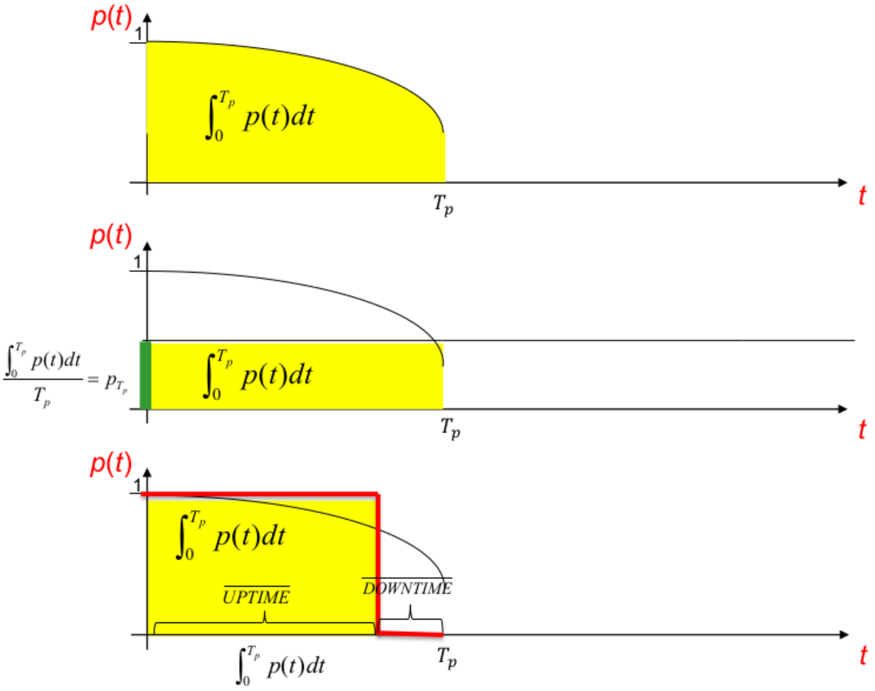

Figure 3.6: Two equivalent representation of the instantaneous availability that make use of the average availability

3.5 Maintainability

How fast a system can be repaired after failure? Repair time T_R depends from many factors as seen in Fig. 3.7

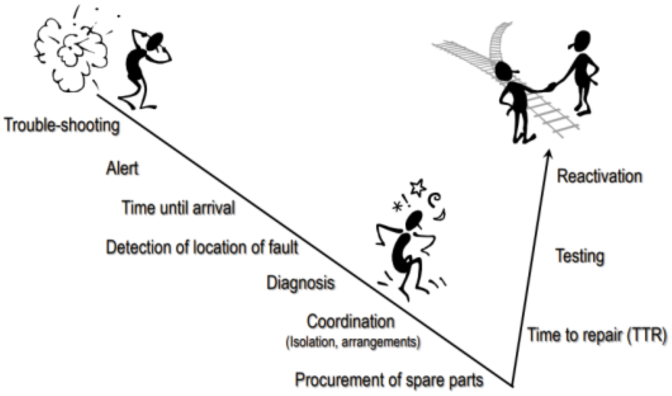

Figure 3.7: Factors that affect repair time

Repair time T_R varies statistically from one failure to another, depending on the conditions associated to the particular maintenance events.

Let T_R denotes the downtime random variable, distributed according to the pdf $g_{T_R}(t)$.

Maintainability is defined as the cumulative distribution function:

$$P(T_R \leq t) = \int_0^t g_{T_R}(\tau) d\tau$$

3.6 Failure classification

Revealed failure A failure that may be immediately or almost immediately apparent through an alarm or indicator system.

Unrevealed failure A stand-by component can fail unnoticed. The system goes on without noticing the component failure until a test on the component is made or the component is demanded to function.

3.7 Revealed failure

3.7.1 Availability of a continuously monitored component

Hypothesis

- Constant failure rate λ;
- Restoration starts immediately after the component failure;
- Probability density function of the random time duration T_R of the repair process = $g_{T_R}(t)$.

Objective

Computation of the availability $p(t)$ of a continuously monitored component.

Method

It is based on a conceptual experiment with N_0 identical components that start at time $t = 0$. We then write a balance equation for the number $N(t)$ of components working between time t and $t + \Delta t$.

The number of systems working at time $t + \Delta t$ is

$$N(t + \Delta t) = N(t) - N_F + N_R$$

where

- N_F is the number of systems that fail between $t + \Delta t$
- N_R is the number of systems that are repaired between $t + \Delta t$

Let's reason in terms of expected value:

$$E[N(t + \Delta t)] = E[N(t)] - E[N_F] + E[N_R]$$

$$E[N(t + \Delta t)] = N_0 \cdot p(t + \Delta t)$$

$$E[N(t)] = N_0 \cdot p(t)$$

$$\begin{aligned} E[N_F] &= N_0 \cdot P\{\text{failure between } t \text{ and } t + \Delta t\} \\ &= N_0 \cdot P\{\text{up at time t}\} \cdot P\{\text{failure in } (t; t + \Delta t) | \text{up at time t}\} \\ &= N_0 \cdot p(t) \cdot \lambda \Delta t \end{aligned}$$

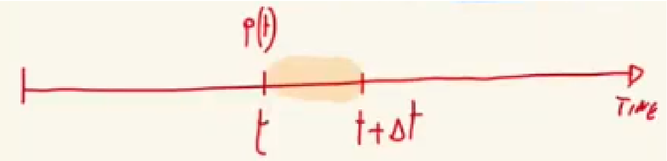

Figure 3.8: Timeline

$$E[N_R] = \int_0^t N_0 \cdot p(\tau) \cdot \lambda d\tau \cdot g_{T_R}(t - \tau) \Delta t$$

$$N_0 p(t + \Delta t) = N_0 p(t) - N_0 p(t) \lambda \Delta t + \int_0^t N_0 \cdot p(\tau) \cdot \lambda d\tau \cdot g_{T_R}(t - \tau) \Delta t$$

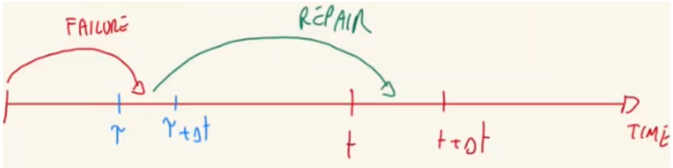

Figure 3.9: Timeline

Dividing both sides by N_0,

$$p(t+\Delta t) = p(t) - p(t)\lambda\Delta t + \int_0^t \cdot p(\tau)\cdot\lambda d\tau \cdot g_{T_R}(t-\tau)\Delta t$$

$$\frac{p(t+\Delta t) - p(t)}{\Delta t} = -p(t)\lambda + \int_0^t p(\tau)\cdot\lambda d\tau \cdot g_{T_R}(t-\tau)$$

The integral-differential form of the balance:

$$\lim_{\Delta t\to 0} \frac{p(t+\Delta t) - p(t)}{\Delta t} = \frac{dp(t)}{dt} = -p(t)\lambda + \int_0^t p(\tau)\cdot\lambda d\tau \cdot g_{T_R}(t-\tau)$$

with $p(0) = 1$

The solution can be obtained introducing the Laplace transforms in Table 3.1.

Time domain	Laplace domain
$p(t)$	$\mathcal{L}[p(t)] = \int_0^{+\infty} e^{-st}p(t)dt = \tilde{p}(s)$
$\frac{dp(t)}{dt}$	$\mathcal{L}\left[\frac{dp(t)}{dt}\right] = s\cdot\tilde{p}(s) - p(0)$
$p(t) * g(t) = \int_0^t p(\tau)g(t-\tau)d\tau$	$\mathcal{L}[p(t) * g(t)] = \tilde{p}(s)\cdot\tilde{g}(s)$

Table 3.1: Laplace transforms

Applying the Laplace transform we obtain:

$$s\cdot\tilde{p}(s) - 1 = -\lambda\cdot\tilde{p}(s) + \lambda\cdot\tilde{p}(s)\cdot\tilde{g}(s)$$

which yields:

$$\tilde{p}(s) = \frac{1}{s + \lambda\cdot(1-\tilde{g}(s))}$$

Applying the inverse Laplace transform to $\tilde{p}(s)$, the instantaneous availability $p(t)$ is determined.

Furthermore, to determine the limiting availability p_∞, the final value theorem can be exploited:

$$p_\infty = \lim_{t\to\infty} p(t) = \lim_{s\to 0}[s \cdot \tilde{p}(s)] = \lim_{s\to 0}\left[\frac{s}{s+\lambda\cdot(1-\tilde{g}(s))}\right]$$

As s tends to 0, a first order approximation of $\tilde{g}(s)$ can be considered:

$$\begin{aligned}\tilde{g}(s) &= \int_0^\infty e^{-s\tau} g(t) d\tau \\ &= \int_0^\infty (1 - s\tau + \dots) g(\tau) d\tau \\ &\cong 1 - s\cdot\int_0^\infty \tau g(\tau) d\tau = 1 - s \cdot \mathrm{MTTR}\end{aligned}$$

where the mean-time-to-repair is $\mathrm{MTTR} = \overline{\tau_R} = E_G[T_R]$, that is to say the expected value of the restoration time distribution $G(t)$.

Hence,

$$\begin{aligned}p_\infty &= \lim_{s\to 0}\frac{s}{s+\lambda s\overline{\tau_R}} \\ &= \frac{1}{1+\lambda\overline{\tau_R}} = \frac{1/\lambda}{1/\lambda+\overline{\tau_R}} \\ &= \frac{MTTF}{MTTF+MTTR} \\ &= \frac{\text{average time the component is UP}}{\text{average period of a failure/repair ”cycle”}}\end{aligned}$$

This result is valid for any repair process $G(t)$!

3.7.2 Example 6.1 (Red Book)

Find the instantaneous and the limiting availabilites for a component whose restoration probability density is:

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

Solution

The limiting availability is:

$$p_\infty = \lim_{t \to \infty} p(t) = \frac{MTTF}{MTTF + MTTR} = \frac{1/\lambda}{1/\lambda + 1/\mu}$$

$$\begin{aligned}\tilde{g}(s) &= \int_0^\infty e^{-s\tau} g(t) d\tau \\ &= \mu \int_0^{+\infty} e^{-(s+\mu)\tau} d\tau \\ &= \frac{\mu}{s+\mu}\end{aligned}$$

$$\begin{aligned}\tilde{p}(s) &= \frac{1}{s + \lambda \cdot (1 - \tilde{g}(s))} \\ &= \frac{1}{s + \lambda \cdot \frac{s}{s+\mu}} = \frac{s+\mu}{s^2 + \mu s + \lambda s}\end{aligned}$$

$$p(t) = \mathcal{L}^{-1}\left[\frac{s+\mu}{s^2 + \mu s + \lambda s}\right]$$

$$\tilde{p}(s) = \frac{A}{s} + \frac{B}{s + (\mu + \lambda)}$$

$$\begin{aligned}\mathcal{L}^{-1}[1] &= \frac{1}{s} \\ \mathcal{L}^{-1}\left[\frac{1}{s+a}\right] &= e^{-at}\end{aligned}$$

$$\begin{aligned}\tilde{p}(s) &= \frac{A}{s} + \frac{B}{s + (\mu + \lambda)} \\ &= \frac{A(s + \mu + \lambda) + Bs}{s(s + \lambda + \mu)} \\ &= \frac{s(A+B) + A\mu + A\lambda}{s(s + \lambda + \mu)} \\ &= \frac{s+\mu}{s(s + \lambda + \mu)}\end{aligned}$$

$$\begin{cases} 1 = A + B \\ \mu = A\lambda + A\mu \end{cases}$$

$$\begin{cases} A = \frac{\mu}{\mu+\lambda} \\ B = \frac{\lambda}{\mu+\lambda} \end{cases}$$

$$p(t) = A\mathcal{L}^{-1}\left[\frac{1}{s}\right] + B\mathcal{L}^{-1}\left[\frac{1}{s+(\mu+\lambda)}\right] = A + Be^{-(\lambda+\mu)t} = \frac{\mu}{\mu+\lambda} + \frac{\lambda}{\mu+\lambda}e^{-(\mu+\lambda)t}$$

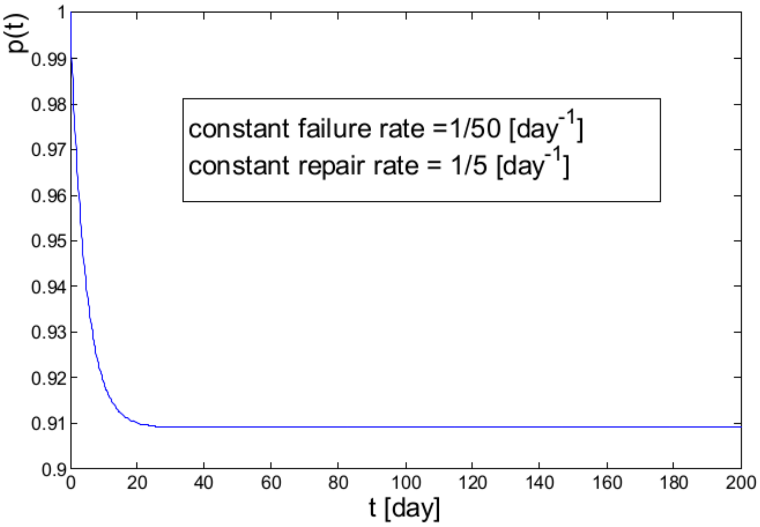

Figure 3.10: Instantaneous availability

3.8 Unrevealed failure

3.8.1 Safety Systems

An example Risk: ignition of the gases in the oil tank, lightning strike or generation of sparks due to electrostatic charges → Fire protection (see Fig. 3.11).

Safety systems are generally in standby until an accident occurs, which calls for their operation. Hence, their *components must be periodically tested*. The components are unattended between tests and their failure is revealed only when tested.

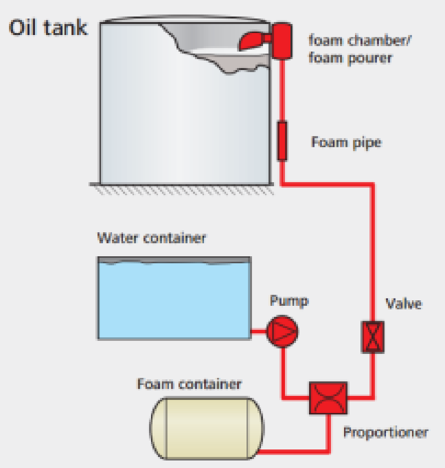

Figure 3.11: Oil tank

3.8.2 Exercise: instantaneous availability of an unattanded component

Find the instantaneous unavailability of an unattended component (no repair is allowed) whose cumulative failure time distribution is $F(t)$.

Solution

The istantaneous unavailability, i.e. the probability $q(t)$ that at time t the component is not functioning is equal to the probability that it fails before t

$$q(t) \equiv F(t)$$

$$q(t) = P\{X(t) = 0\} = P\{T \leq t\} = F_T(t)$$

3.8.3 Availability of a component under periodic test and maintenance

The instantaneous availability is a periodic function of time (the interval between two consecutive test is T_p). See Fig. 3.12.

The performance indicator used is the average unavailability over a period of time T_p:

$$q_{T_p} = \frac{\int_0^{T_p} q(t)dt}{T_p} = \frac{\overline{\text{DOWNtime}}}{T_p}$$

where

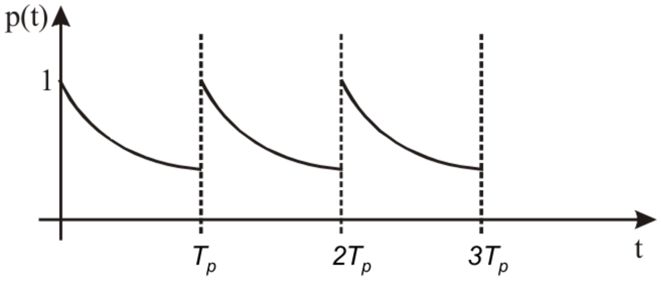

Figure 3.12: Instantaneous availability is periodic

- T_p is the complete maintenance cycle
- $\overline{\text{DOWNtime}}$ is the average time the system is not working

3.8.4 Ideal case: instantaneous testing and maintenance

Let's now assume that:

- unavailability is due to unrevealed random failures (constant failure rate λ)
- *instantaneous* and perfect testing and maintenance procedures are performed every T_p hours

The instantaneous availability within a period T_p coincides with the reliability (Fig. 3.12).

The average unavailability and availability are then:

$$q_{T_p} = \frac{\int_0^{T_p} q(t)dt}{T_p} = \frac{\int_0^{T_p} F_T(t)dt}{T_p}$$

$$p_{T_p} = \frac{\int_0^{T_p} p(t)dt}{T_p} = \frac{\int_0^{T_p} R(t)dt}{T_p} = 1 - q_{T_p}$$

For different systems, we can compute q_{T_p} and p_{T_p} by first computing their failure probability distribution $F_T(t)$ and reliability $R(t)$ and then applying the above expressions.

For a system with constant failure rate λ (good approximation only when $\lambda t < 0.1$):

$$q_{T_p} = \frac{\int_0^{T_p} q(t)dt}{T_p} = \frac{\int_0^{T_p} F_T(t)dt}{T_p} = \frac{\int_0^{T_p}(1 - e^{-\lambda t})dt}{T_p} \approx \frac{\int_0^{T_p} \lambda t\, dt}{T_p} = \frac{\lambda T_p^2}{2T_p} = \frac{1}{2}\lambda T_p$$

$$p_{T_p} = 1 - q_{T_p} = 1 - \frac{1}{2}\lambda T_p$$

3.8.5 A more realistic case: test and maintenance time is finite

Let's assume that:

- the test is performed after a time τ from the end of the previous test
- the test time τ_R is *finite*
- unavailability is due to unrevealed random failures (constant failure rate λ)

We're asked to:

- Draw the qualitative time evolution of the instantaneous availability
- Estimate the average unavailability and availability over the complete maintenance cycle period $T_p = \tau + \tau_R$.

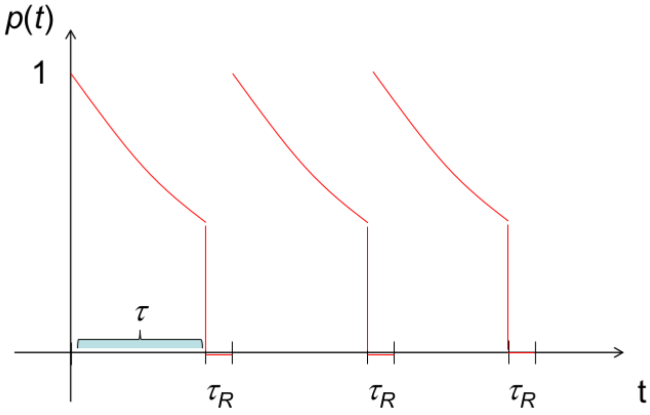

Figure 3.13: Qualitative time evolution of the instantaneous availability

Assuming a finite repair time τ_R , this must be counted as DOWNtime, if significant. Hence, the average unavailability and availability over the complete maintenance cycle period $\tau + \tau_R$ will change into:

$$\overline{q} = \frac{\tau_R + \int_0^\tau F_T(t)dt}{\tau + \tau_R}$$

$$\overline{p} = \frac{\int_0^\tau R(t)dt}{\tau + \tau_R}$$

If the repair time τ_R is small compared with the period τ , we get:

$$\overline{q} = \frac{\tau_R + \int_0^\tau F_T(t)dt}{\tau}$$

$$\overline{p} = \frac{\int_0^\tau R(t)dt}{\tau}$$

3.8.6 Single component under periodic maintenance

Hypothesis

- The safety system is initially working: $q(0) = 0$; $p(0) = 1$;
- τ time interval between two consecutive maintenance interventions;
- τ_r duration of the maintenance intervention;
- Failure causes:
  - random failure at any time $T \sim F_T(t)$;
  - on-line switching failure on demand $\sim Q_0$;
  - maintenance disables the component $\sim \gamma_0$ (human error during inspection, testing or repair).

Objective

Computation of the average unavailability over the lifetime $[0, T_M]$:

$$q_{[0,T_M]} = \frac{\overline{\text{DOWNtime}}}{T_M}$$

Method

In order to compute the component average unavailability $\overline{q_{0T}}$, we refer to its timeline (Fig. 3.14).

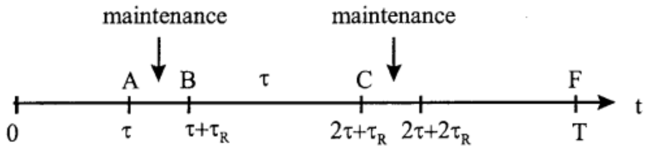

Fig. 6.5: Timeline of a component under periodic maintenance

Figure 3.14: Timeline

$$
\begin{aligned}
q_{[0,T_M]} &= \frac{\int_0^{T_M} q(t)dt}{T_M} = \frac{\int_0^{A} q(t)dt + \int_A^{T_M} q(t)dt}{T_M} \\
&= \frac{\int_0^{A} q(t)dt + k\left[\int_A^{B} q(t)dt + \int_B^{C} q(t)dt\right]}{T_M} \\
&= \frac{\overline{\text{DOWNtime}_{0A}} + K[\overline{\text{DOWNtime}_{AB}} + \overline{\text{DOWNtime}_{BC}}]}{T_M} \\
&= \frac{\overline{\text{DOWNtime}_{0T_M}}}{T_M}
\end{aligned}
$$

where

$$k = \frac{T - \tau}{\tau + \tau_r}$$

Period from 0 to A

Possible failure causes:

- random failure (E_1);
- on-line switching failure on demand (E_2).

$$\forall t \in [0, A] \quad q_{0A}(t) = P(E_1) + P(E_2) - P(E_1 \cap E_2) = F(t) + Q_0 - F(t)Q_0$$

$$
\begin{aligned}
\overline{\text{DOWNtime}_{0A}} &= \int_0^{\tau} q_{0A}(t)dt \\
&= \int_0^{\tau} [Q_0 + (1 - Q_0)F_T(t)]dt \\
&= Q_0\tau + (1 - Q_0)\int_0^{\tau} F_T(t)dt
\end{aligned}
$$

$\boxed{\text{Period from A to B}}$

System under maintenance!

$$\forall t \in [A, B] \quad q_{AB}(t) = 1$$

$$\begin{aligned}
\overline{\text{DOWNtime}_{AB}} &= \int_A^B q_{AB}(t)dt \\
&= \int_\tau^{\tau_r} 1dt \\
&= \tau_r
\end{aligned}$$

$\boxed{\text{Period from B to C}}$

Possible failure causes:

- random failure (E_1);
- on-line switching failure on demand (E_2);
- maintenance disables the component (E_3)

$$\begin{aligned}
\forall t \in [B, C] \quad q_{BC}(t) &= P(E_1) + P(E_2) + P(E_3) - P(E_1 \cap E_2) - P(E_2 \cap E_3) \\
&\quad - P(E_1 \cap E_3) + P(E_1 \cap E_2 \cap E_3) \\
&= \gamma_0 + (1 - \gamma_0)(Q_0 + (1 - Q_0)F(t))
\end{aligned}$$

$$\begin{aligned}
\overline{\text{DOWNtime}_{BC}} &= \int_0^\tau q_{BC}(t)dt \\
&= \gamma_0\tau + (1 - \gamma_0)\left[Q_0\tau + (1 - Q_0)\int_0^\tau F_T(t)dt\right]
\end{aligned}$$

$$\begin{aligned}
\overline{\text{DOWNtime}_{0T_M}} &= Q_0\tau + (1 - Q_0)\int_0^\tau F_T(t)dt + \\
&+ \frac{T - \tau}{\tau + \tau_r}\left\{\tau_R + \gamma_0\tau + (1 - \gamma_0)\left[Q_0\tau + (1 - Q_0)\int_0^\tau F_T(t)dt\right]\right\}
\end{aligned}$$

$$\begin{aligned} q_{[0,T_M]} &= \frac{\overline{\text{DOWNtime}_{0T_M}}}{T_M} \\ &= \frac{Q_0\tau}{T_M} + \frac{1-Q_0}{T_M}\int_0^\tau F_T(t)dt + \\ &+ \frac{1}{\tau+\tau_r}\left\{\tau_R + \gamma_0\tau + (1-\gamma_0)\left[Q_0\tau + (1-Q_0)\int_0^\tau F_T(t)dt\right]\right\} \end{aligned}$$

We simplify under the following assumptions:

- $\tau \ll T_M$
- $\int_0^\tau F_T(t)dt \leq \tau$
- $\tau_R \ll \tau$

$$\begin{aligned} q_{[0,T_M]} &= \frac{\overline{\text{DOWNtime}_{0T_M}}}{T_M} \\ &= \cancel{\frac{Q_0\tau}{T_M}} + \cancel{\frac{1-Q_0}{T_M}\int_0^\tau F_T(t)dt} + \\ &+ \frac{1}{\tau+\cancel{\tau_r}}\left\{\tau_R + \gamma_0\tau + (1-\gamma_0)\left[Q_0\tau + (1-Q_0)\int_0^\tau F_T(t)dt\right]\right\} \\ &= \frac{\tau_R}{\tau} + \gamma_0 + (1-\gamma_0)\left[Q_0 + \frac{1-Q_0}{\tau}\int_0^\tau F_T(t)dt\right] \end{aligned}$$

Often in practice, $\gamma_0 \ll 1$, $Q_0 \ll 1$. Then:

$$q_{[0,T_M]} \cong \frac{\tau_R}{\tau} + \gamma_0 + (1-\cancel{\gamma_0})\left[Q_0 + \frac{1-\cancel{Q_0}}{\tau}\int_0^\tau F_T(t)dt\right]$$

We now consider an exponential system with small, constant failure rate:

$$\lambda \implies F_T(t) = 1 - e^{-\lambda t} \cong \lambda \cdot t$$

The average unavailability reads:

$$q_{[0,T_M]} \cong \frac{\tau_R}{\tau} + \gamma_0 + Q_0 + \frac{1}{2}\lambda\tau$$

From this formula it is possible to distinguish each contribution to the unavailability of the component, as in Table 3.2

Term	Cause
$\frac{\tau_R}{\tau}$	unavailability during maintenance
γ_0	unavailability due to an error which leaves the unit DOWN after test
Q_0	unavailability due to the switch failing on demand
$\frac{1}{2}\lambda\tau$	unavailability due to random, unrevealed failures between successive tests

Table 3.2: Terms of $q_{[0,T_M]}$ vs. the respective causes

3.9 Where to study?

Red book

- Chapter 6

Green book

- All problems in Chapter 6