System risks, reliability and costs

Systems always have risks attached to them. How do we deal with risks? How reliable are systems? And what do systems cost anyway? That's what we'll look at in this chapter.

1 Risk Management

1.1 What is Risk Management?

When designing a system, unexpected things can always pop up. That's the risk of designing. In fact, the **risk** is defined as the measure of uncertainty, when attaining a goal. Risk is always present. So it needs to be dealt with. The process of managing risk is (surprisingly) called **Risk Management** (RM).

Risk Management has two main branches. First, there is **Project Risk Management** (PRM). This branch deals with technical risks: anything having to do with development. The second branch is **Environmental Risk Management**. This concerns the management of environmental health and safety risks.

1.2 Determining risks

When performing risk management, we should first identify the risks. But once that is done, how do we know which risks we should reduce?

To see that, we need to look at two things. We need to examine the **likelihood of occurrence** and the **consequence of the event**. Multiplying these to things gives us the risk. (For example, if a lightning strike has a 20% chance of occurring in a year, and would cost ten thousand euros, then the risk in a year is two thousand euros.)

When risks are too high, two things can be done. Either the likelihood of occurrence can be decreased, or the consequence of the event can be decreased. (Of course we could also do both.)

1.3 The Risk Map

A way to visualize risks, is by using a Risk Map. One axis of the Risk Map denotes the likelihood of occurrence. The other axis indicates the consequence of the event. An empty risk map can be seen in figure 1.

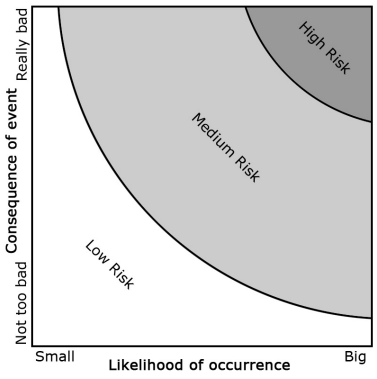

Figure 1: An empty risk map.

An event is represented by a point on the risk map. The seriousness (the risk) of the event can then be read from the diagram. The darker the region it is in, the more serious the risk is.

2 Reliability, maintainability and availability

2.1 The reliability function

In this part, we will examine reliability. The **reliability** R is the probability that a system will perform in a satisfactory manner, for a given period of time. The reliability of a system usually depends on time. It is therefore described by the **reliability function** $R(t)$.

From the reliability function, we can derive several other functions. The **failure distribution** $F(t)$ (also known as the **unreliability function**) is given by $F(t) = 1 - R(t)$. This failure distribution is then, in turn, related to the **failure density function** $f(t)$, according to

$$F(t) = \int_0^t f(\tau)d\tau. \tag{2.1}$$

Finally, the **hazard function** $r(t)$ (also known as the **failure rate**) is defined as

$$r(t) = \frac{\text{Failure Density}}{\text{Reliability}} = \frac{f(t)}{R(t)} = \frac{f(t)}{1 - \int_0^t f(\tau)d\tau}. \tag{2.2}$$

2.2 A probability refreshment

We saw that reliability is defined as a probability. So let's quickly refresh our knowledge of the world of probabilities. We define $P(A)$ as the probability that event A occurs. We also define $P(A|B)$ as the probability that event A occurs, given that event B occurs. There are several rules and definitions concerning this probability.

Two events A and B are **independent** if $P(B)$ does not depend on whether A occurs or not. (In an equation, $P(B|A) = P(B)$.)

The **conditional theorem** states that $P(A \cap B) = P(A)P(B|A) = P(B)P(A|B)$. For two independent events A and B, we can simplify this to $P(A \cap B) = P(A)P(B)$. This relation is also known as the **multiplication theorem**.

Two events A and B are **mutually exclusive** if they can not occur at the same time. So if A occurs, then B does not occur. (In an equation, $P(A \cap B) = 0$.)

The **addition theorem** states that $P(A \cup B) = P(A) + P(B) - P(A \cap B)$. If A and B are mutually exclusive, this can be simplified to $P(A \cup B) = P(A) + P(B)$. So to find the probability that either of two mutually exclusive events A and B occurs, we can simply add up their probabilities $P(A)$ and $P(B)$.

Finally there is Bayes' rule, stating that

$$P(A|B) = \frac{P(B|A)P(A)}{\sum_{i=1}^{n} P(B|A_i)P(A_i)}. \tag{2.3}$$

2.3 Failure types and distributions

Reliability is all about predicting failures. This is difficult, because there are many types of failures. (Think of fatigue, structural overload, electrical overload, wear, etcetera.) And every failure mode often has its own type of failure distribution.

There are many types of failure distributions. The type of failure distribution mainly depends on the failure rate. If there is, for example, a constant failure rate $r(t) = \lambda$, then we will get a **negative exponential distribution**. This distribution is described by

$$f(t) = \frac{1}{\theta} e^{-t/\theta}, \tag{2.4}$$

where $\theta = 1/\lambda$ is the **Mean Time Between Failures** (MTBF). From this, we can derive the reliability function. It is given by

$$R(t) = e^{-t/\theta} = e^{-\lambda t}. \tag{2.5}$$

Negative exponential distributions often occur when considering failures caused by a random event, like bad weather, bird strikes, etcetera.

Of course not all failure distributions have a constant failure rate. Many types of failures have an increasing failure rate as time progresses. (Older products are more likely to fail.) An increasing failure rate can be described by a **normal distribution**. The average of the normal distribution then indicates the average life time of the product.

Some failure types have a decreasing failure rate. (An example is the failure of humans. In the first few years, humans are relatively likely to fail. But if they live through their first years, they'll quite likely survive the next 50 years too.) Such failure rates can be described by a **Weibull distribution** or a **gamma distribution**.

2.4 Reliability of systems

Let's suppose we have a system consisting of n components. Also suppose that the system is build up, such that, if one component fails, then the whole system fails. (The components are said to be in **series**.) The reliability of the system can now be found, by multiplying all individual reliabilities. In an equation,

$$R_{system}(t) = \prod_{i=1}^{n} R_i(t). \tag{2.6}$$

We can also build up the system a bit differently. This time all components have to fail, for the system to fail. (The components are said to be in **parallel**). We now have

$$R_{system}(t) = 1 - \prod_{i=1}^{n} (1 - R_i(t)). \tag{2.7}$$

2.5 Fault Tree Analysis

As stated before, there are many ways in which a system can fail. To investigate those ways, a **Fault Tree** can come in handy. A fault tree describes what events are necessary to cause a certain type of failure. An example of a Fault Tree is shown in figure 2.

When examining failures, it is important to know the minimum cut sets. A **minimum cut set** is defined as a minimum set of events leading to failure. For example, for the Fault Tree in figure 2, events F and H would cause failure. The set (F, H) is thus a minimum cut set. The set (E, C) would also cause failure. This set is, however, not a minimum cut set. (Note the word 'minimum'.) This is because event C is not necessary to cause failure. (Event E by itself already ensures failure.)

2.6 Maintainability

The **maintainability** M of a system is defined as the ease, accuracy, safety, and economy in the performance of maintenance actions. There are two important kinds of maintenance. There is **preventive**

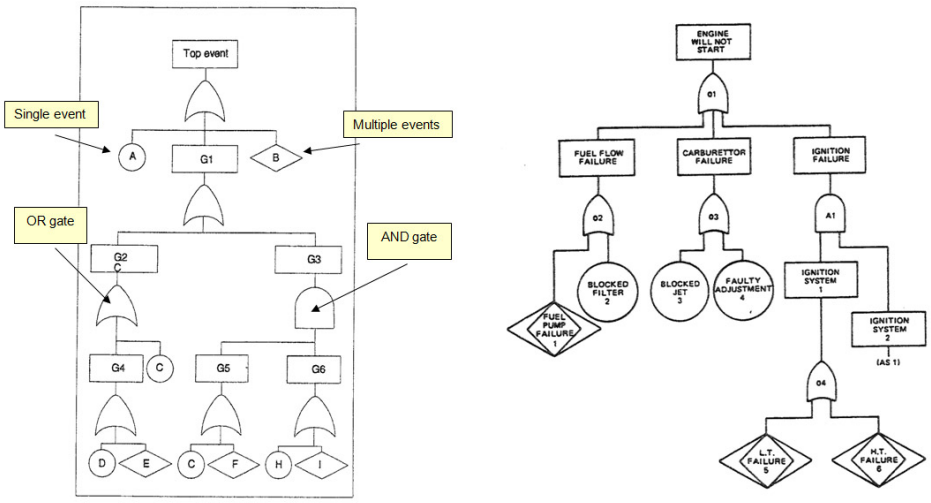

Figure 2: The general Fault Tree form (left) and an example applied to engine failure (right).

maintenance, aimed to prevent failure. (Inspection and periodic replacement of parts are part of preventive maintenance.) There is also **corrective maintenance**. The goal of this is to patch up the system after a failure has occurred. (Repairs are thus part of corrective maintenance.)

There are several parameters with which the maintainability can be expressed. The most important ones are...

- **Mean Time Till Failure** (MTTF): Average time until the system fails.
- **Mean Time To Repair** (MTTR): Average time needed to repair/restore the system.
- **Mean Preventive Maintenance Time** (MPMT): Average time needed to perform preventive maintenance.
- **Mean Time To Maintain** (MTTM): Average time needed to perform both preventive and corrective maintenance.
- **Mean Down Time** (MDT): The MTTM plus delays (for example, due to logistic reasons).
- **Mean Time Between Maintenances** (MTBM): The average time that is between two maintenance sessions.

2.7 Availability

The **availability** A is the probability that a system will be available when required for use. If we only consider the effects of failures and ignore maintenance, then we are examining the **inherent availability** A_i. It is given by

$$A_i = \frac{MTTF}{MTTF + MTTR}. \tag{2.8}$$

If we, however, don't consider failure, but only maintenance, then we are dealing with the **achieved availability** A_a. This is given by

$$A_a = \frac{MTBM}{MTBM + MTTM}. \tag{2.9}$$

3 Life Cycle Costs

3.1 Cost types

A system of course has costs. All the costs that are made in the life of a system/product are called the **Life Cycle Costs** (LCC).

The LCC can be split up into two important categories: Recurring and non-recurring costs. **Non-recurring costs** are costs that only occur once for every product type. (Examples include design costs, machines/tool costs and facility costs.) **Recurring costs** are costs that are present for every product of a specific type. (Examples are material costs, labour costs and energy costs.)

3.2 The Cost Breakdown Structure

There can be a lot of different types of costs, in the life of a system. One way to display these costs, is by using a **Cost Breakdown Structure** (CBS). The CBS is a tree, in which the Life Cycle Costs are split up into categories. An example of a CBS for an aircraft can be seen in figure 3.

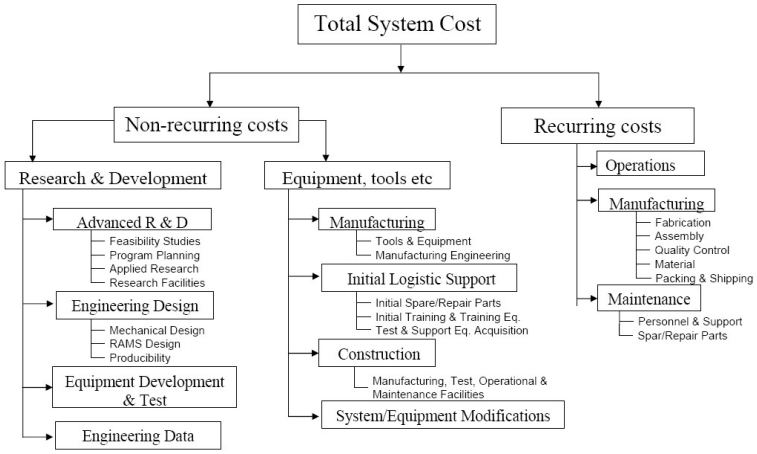

Figure 3: A Cost Breakdown Structure for an aircraft.

After the CBS has been created, numbers often need to be attached to categories. For this, **Cost Estimating Relations** (CER's) are often used. These relations are usually derived from experiences from earlier projects.