CHAPTER 12

Risk Analysis and Assessment

The learning objectives for this chapter are to learn and understand concepts that are commonly used by industry to conduct risk analysis and assessment. This includes:

- Probability theory.
- Event tree and fault tree analysis.
- Risk analysis and assessment methods, including quantitative risk analysis (QRA), layer of protection analysis (LOPA) and bow-tie methods.
- Societal and individual risk, and how these are quantified.
- Risk tolerance criteria.

Risk is a measure of human injury, environmental damage, or economic loss in terms of both the likelihood and the magnitude of the loss. Risk analysis determines all the incident scenarios of a plant having a consequence of concern and their corresponding risks, and then sums the risks to establish the total risk for the plant. Risk assessment considers the risks and the tolerable risk criteria to make decisions regarding risk reduction.

The first part of this chapter explains how to determine the frequency of incident scenarios and how this information is used in event and fault trees. The last part explains how the frequencies are used in QRA, LOPA, qualitative, and bow-tie methods.

12-1 Review of Probability Theory

Equipment failures or faults in a process occur as a result of complex interactions of the individual components. The overall probability of a failure in a process depends on the nature of these interactions. In this section, we define the various types of interactions and describe how to compute failure probabilities.

Data are collected on the failure rate of a particular hardware component. With adequate data, it can be shown that, on average, the component fails after a certain period of time. This is called the average failure rate and is represented by μ with units of faults/time. The probability that the component will not fail during the time interval (0, t) is given by a Poisson distribution:[1]

$$R(t) = e^{-\mu t} \tag{12-1}$$

where R is the reliability. Equation 12-1 assumes a constant failure rate μ. As $t \to \infty$, the reliability goes to 0. The speed at which this occurs depends on the value of the failure rate μ. The higher the failure rate, the more rapidly the reliability decreases. Other, more complex distributions are also available, but this simple exponential distribution is most commonly used because it requires only a single parameter, μ.

The complement of the reliability is called the failure probability (or sometimes the unreliability), P, and it is given by

$$P(t) = 1 - R(t) = 1 - e^{-\mu t} \tag{12-2}$$

The failure density function is defined as the derivative of the failure probability:

$$f(t) = \frac{dP(t)}{dt} = \mu e^{-\mu t} \tag{12-3}$$

The area under the complete failure density function is 1.

The failure density function is used to determine the probability P of at least one failure in the time period t_0 to t_1:

$$P(t_o \to t_1) = \int_{t_0}^{t_1} f(t)\,dt = \mu \int_{t_0}^{t_1} e^{-\mu t}\,dt = e^{-\mu t_0} - e^{-\mu t_1} \tag{12-4}$$

The integral represents the fraction of the total area under the failure density function between time t_0 and t_1.

The time interval between two failures of the component is called the mean time between failures (MTBF) and is given by the first moment of the failure density function:

$$E(t) = MTBF = \int_0^{\infty} tf(t)\,dt = \frac{1}{\mu} \tag{12-5}$$

Typical plots of the functions μ, f, P, and R are shown in Figure 12-1.

Equations 12-1 through 12-5 are valid only for a constant failure rate μ. Many components exhibit a typical bathtub failure rate, shown in Figure 12-2. In this pattern, the failure rate is highest when the component is new (infant mortality) and when it is old (old age). Between these two periods (denoted by the lines in Figure 12-2), the failure rate is reasonably constant and Equations 12-1 through 12-5 are valid.

[1]B. Roffel and J. E. Rijnsdorp. *Process Dynamics, Control, and Protection* (Ann Arbor, MI: Ann Arbor Science, 1982), p. 381.

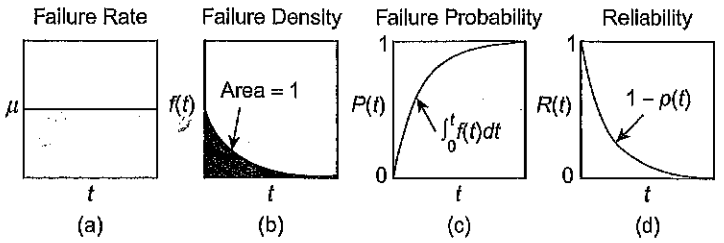

Figure 12-1 Typical plots of (a) the failure rate μ, (b) the failure density $f(t)$, (c) the failure probability $P(t)$, and (d) the reliability $R(t)$.

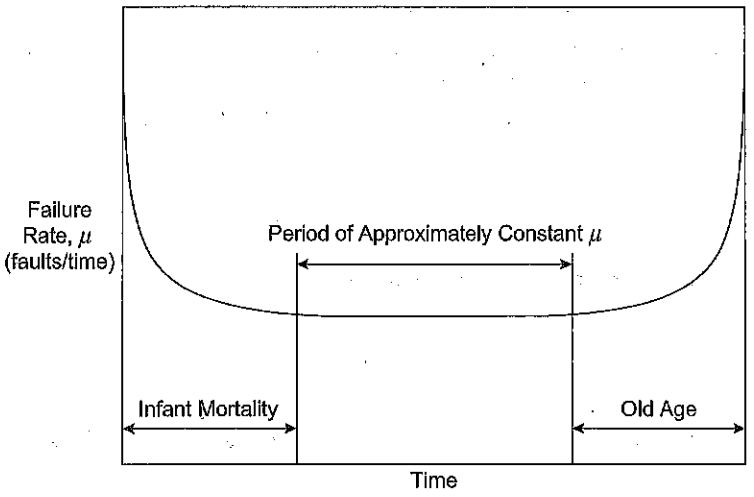

Figure 12-2 A typical bathtub failure rate curve for process hardware. The failure rate is approximately constant over the midlife of the component.

Interactions between Process Units

Incidents in chemical plants are usually the result of a complicated interaction of a number of process components. The overall process failure probability is computed from the individual component probabilities.

Process components interact in two different fashions. In some cases, a process failure requires the simultaneous failure of a number of components in parallel. This parallel structure is represented by the logical AND function. This means that the failure probabilities for the individual components must be multiplied:

$$P = \prod_{i=1}^{n} P_i \tag{12-6}$$

where

n is the total number of components and
P_i is the failure probability of each component.

This rule is easily memorized because for *p*arallel components the *p*robabilities are multiplied.

The total reliability for parallel units is given by

$$R = 1 - \prod_{i=1}^{n} (1 - R_i) \tag{12-7}$$

where R_i is the reliability of an individual process component.

Process components also interact in series. This means that a failure of any single component in the series of components will result in failure of the process. The logical OR function represents this case. For series components, the overall process reliability is found by multiplying the reliabilities for the individual components:

$$R = \prod_{i=1}^{n} R_i \tag{12-8}$$

The overall failure probability is computed from

$$P = 1 - \prod_{i=1}^{n} (1 - P_i) \tag{12-9}$$

For a system composed of two components A and B, Equation 12-9 is expanded to

$$P(A \text{ or } B) = P(A) + P(B) - P(A)P(B) \tag{12-10}$$

The cross-product term $P(A)P(B)$ compensates for counting the overlapping cases twice. Consider the example of tossing a single die and determining the probability that the number of points is even *or* divisible by 3. In this case,

$$P(\text{even } or \text{ divisible by 3}) = P(\text{even}) + P(\text{divisible by 3}) - P(\text{even } and \text{ divisible by 3}).$$

The last term subtracts the cases in which both conditions are satisfied.

If the failure probabilities are small (a common situation), the term $P(A)P(B)$ is negligible, and Equation 12-10 reduces to

$$P(A \text{ or } B) = P(A) + P(B) \tag{12-11}$$

This result is generalized for any number of components. For this special case, Equation 12-9 reduces to

$$P = \sum_{i=1}^{n} P_i \tag{12-12}$$

Failure rate data for a number of typical process components are provided in Table 12-1. These are average values determined at a typical chemical process facility. Actual values would depend on the manufacturer, the materials of construction, the design, the environment, and other factors. The assumptions in this analysis are that the failures are independent, hard, and not intermittent, and that the failure of one device does not stress adjacent devices to the point that the failure probability is increased.

A summary of computations for parallel and series process components is shown in Figure 12-3.

Table 12-1 Failure Rate Data for Various Selected Process Components

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

Source: Selected from Frank P. Lees. *Loss Prevention in the Process Industries* (London, UK: Butterworths, 1986), p. 343.

Failure Probability	Reliability	Failure Rate
P_1, P_2 — OR — P	R_1, R_2 — OR — R	μ_1, μ_2 — OR — μ
$P = 1 - (1 - P_1)(1 - P_2)$	$R = R_1 R_2$	$\mu = \mu_1 + \mu_2$
$P = 1 - \prod_{i=1}^{n} (1 - P_i)$	$R = \prod_{i=1}^{n} R_i$	$\mu = \sum_{i=1}^{n} \mu_i$
Series link of components:	The failure of either component adds to the total system failure.	
P_1, P_2 — AND — P	R_1, R_2 — AND — R	
$P = P_1 P_2$	$R = 1 - (1 - R_1)(1 - R_2)$	$\mu = (-\ln R)/t$
$P = \prod_{i=1}^{n} P_i$	$R = 1 - \prod_{i=1}^{n} (1 - R_i)$	
Parallel link of components:	The failure of the system requires the failure of both components. Note that there is no convenient way to combine the failure rate.	

Figure 12-3 Computations for various types of component linkages.

Example 12-1

The flow of water to a chemical reactor cooling coil is controlled by the system shown in Figure 12-4. The flow is measured by a differential pressure (DP) flow meter, the controller is designed to control the flow, and the control valve manipulates the flow of coolant. Determine the overall failure rate, the unreliability, the reliability, and the MTBF for this system. Assume a 1-year period of operation.

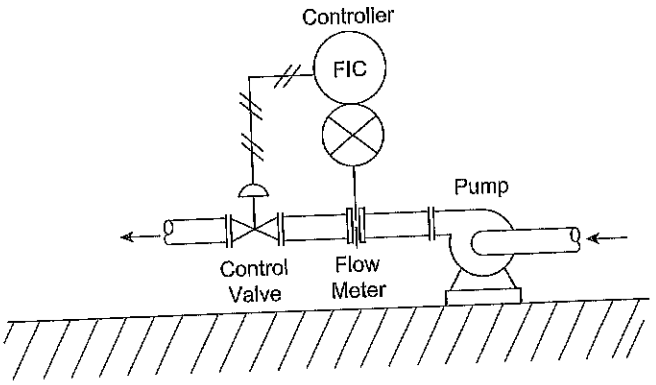

Figure 12-4 Flow control system. The components of the control system are linked in series.

Solution

These process components are related in series. Thus, if any one of the components fails, the entire system fails. The reliability and failure probability are computed for each component using Equations 12-1 and 12-2. The results are shown in the following table. The failure rates are from Table 12-1.

Component	Failure rate μ (faults/yr)	Reliability ($R = e^{-\mu t}$)	Failure probability ($P = 1 - R$)
Control valve	0.60	0.55	0.45
Controller	0.29	0.75	0.25
DP cell	1.41	0.24	0.76

The overall reliability for components in series is computed using Equation 12-8. The result is

$$R = \prod_{i=1}^{3} R_i = (0.55)(0.75)(0.24) = 0.10$$

The failure probability is computed from Equation 12-2:

$$P = 1 - R = 1 - 0.10 = 0.90/\text{yr}$$

The overall failure rate is computed using the definition of the reliability (Equation 12-1):

$$R = 0.10 = e^{-\mu}$$
$$\mu = -\ln(0.10) = 2.3 \text{ failures/yr}$$

The MTBF is computed using Equation 12-5:

$$\text{MTBF} = \frac{1}{\mu} = 0.43\,\text{yr}$$

This system is expected to fail, on average, once every 0.43 yr.

Example 12-2

A diagram of the safety systems for a chemical reactor is shown in Figure 12-5. This reactor contains a high-pressure alarm to alert the operator in the event of dangerous reactor pressures. It consists of a pressure switch on the reactor connected to an alarm light indicator. For additional safety, an automatic high-pressure reactor shutdown system is installed. This system is activated at a pressure somewhat higher than the alarm system and consists of a pressure switch connected to a solenoid valve in the reactor feed line. The automatic system stops the flow of reactant in the event of high pressure. Compute the overall failure rate, the failure probability, the reliability, and the MTBF for a high-pressure condition. Assume a 1-year period of operation. Also, develop an expression for the overall failure probability based on the component failure probabilities.