Chapter 10
Reliability of Safety Systems
Markov Approach

Marvin Rausand
marvin.rausand@ntnu.no

RAMS Group
Department of Production and Quality Engineering
NTNU

(Version 0.1)

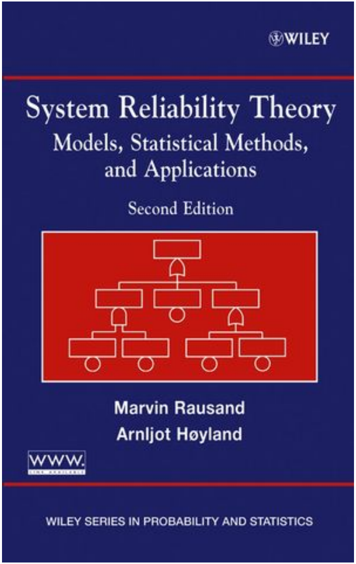
NTNU – Trondheim
Norwegian University of
Science and Technology

Slides related to the book

System Reliability Theory
Models, Statistical Methods,
and Applications

Wiley, 2004

Homepage of the book:
http://www.ntnu.edu/ross/books/srt



Basic assumptions

- A safety instrumented system (SIS) is tested periodically tested with test interval τ
- When a failure is detected, the system is repaired
- The time required for testing and repair is considered to be negligible

- Let $X(t)$ denote the state of the system at time t
- Let $\mathcal{X} = \{0, 1, \ldots, r\}$ be the (finite) set of all possible states

Split the *state space* $\mathcal{X}$ in two parts, a set B of functioning states, and a set F of failed states, such that $F = \mathcal{X} - B$.

Probability of failure on demand

The probability of failure on demand (PFD) in test interval n is

$$\mathrm{PFD}(n) = \frac{1}{\tau} \int_{(n-1)\tau}^{n\tau} \Pr(X(t) \in F)\, dt$$

If a demand for the safety system occurs in interval n, the (average) probability that the safety system is not able to shut down the process (or EUC) is $\mathrm{PFD}(n)$

$\mathrm{PFD}(n)$ also denotes the average proportion of test interval n where the safety system is not able to perform its safety function.

Further assumptions

Assume that $\{X(t)\}$ behaves like a homogeneous Markov process with transition rate matrix $\mathbb{A}$ as long as time runs inside a test interval, that is, inside intervals $(n-1)\tau \leq t < n\tau$, for $n = 1, 2, \ldots$.

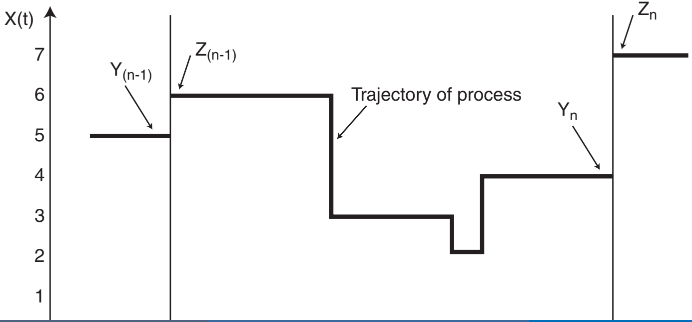
Let $P_{jk}(t) = \Pr(X(t) = k \mid X(0) = j)$ denote the transition probabilities for $j, k \in \mathcal{X}$, and let $\mathbb{P}(t)$ denote the corresponding matrix.

Note:
Failures detected by diagnostic self-testing and ST failures may occur and be repaired within the test interval.

States before and after a test

Let $Y_n = X(n\tau-)$ denote the state of the system immediately before time $n\tau$, that is, immediately before test n.

If a malfunctioning state is detected during a test, a repair action is initiated, and changes the state from Y_n to a state Z_n, where Z_n denotes the state of the system just after the test (and possible repair) n.



Repair matrix

When Y_n is given, we assume that Z_n is independent of all transitions of the system before time $n\tau$. Let

$$\Pr(Z_n = j \mid Y_n = i) = R_{ij} \quad \text{for all } i,j \in \mathcal{X}$$

denote the transition probabilities, and let $\mathbb{R}$ denote the corresponding transition matrix.

If the state of the system is $Y_n = i$ just before test n, the matrix $\mathbb{R}$ tells us the probability that the system is in state $Z_n = j$ just after test/repair n. The matrix $\mathbb{R}$ depends on the repair strategy, and also on the quality of the repair actions. Probabilities of maintenance-induced failures and imperfect repair may be included in $\mathbb{R}$. The matrix $\mathbb{R}$ is called the *repair matrix* of the system.

Repair matrix example

Consider a system with states $\{0, 1, 2, 3\}$ of which state 3 denotes the "perfect" state. If we repair *all* failures after each test and bring the system back to the "perfect" state, the repair matrix becomes:

$$\mathbb{R} = \begin{pmatrix} R_{00} & R_{01} & R_{02} & R_{03} \\ R_{10} & R_{11} & R_{12} & R_{13} \\ R_{20} & R_{21} & R_{22} & R_{23} \\ R_{30} & R_{31} & R_{32} & R_{33} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Initial state

The state of the system at time $t = 0$ is $X(0)$ which is the same as Z_0.

Let $\rho = [\rho_0, \rho_1, \ldots, \rho_r]$, where $\rho_i = \Pr(Z_0 = i)$, and $\sum_{i=0}^{r} \rho_i = 1$, denote the distribution of Z_0.

In most cases the system will be started in a "perfect" state, say state r, in which case we have

$$\rho = [\rho_0, \rho_1, \ldots, \rho_r] = [0, 0, \ldots, 1]$$

To get a general set-up we assume, however, that the system may start in any state (with a probability distribution)

State just before first test

The distribution of the state of the system just before the first test, at time τ, is

$$\begin{aligned}\Pr(Y_1 = k) &= \Pr(X(\tau-) = k) \\ &= \sum_{j=0}^{r} \Pr(X(\tau-) = k \mid X(0) = j) \cdot \Pr(X(0) = j) \\ &= \sum_{j=0}^{r} \rho_j \cdot P_{jk}(\tau) = [\rho \cdot \mathbb{P}(\tau)]_k\end{aligned}$$

for any $k \in \mathcal{X}$, where $[\mathbf{B}]_k$ denotes the kth entry of the vector $\mathbf{B}$.

Test interval $n - 1$

Consider test interval n. Just after test n the state of the system is Z_n.

$$\begin{aligned}
&\Pr(Y_{n+1} = k \mid Y_n = j) \\
&\quad = \sum_{i=0}^{r} \Pr(Y_{n+1} = k \mid Z_n = i, Y_n = j) \cdot \Pr(Z_n = i \mid Y_n = j) \\
&\quad = \sum_{i=0}^{r} P_{ik}(\tau) R_{ji} = [\mathbb{R} \cdot \mathbb{P}(\tau)]_{jk}
\end{aligned}$$

where $[\mathbb{B}]_{jk}$ denotes the (jk)th entry of the matrix $\mathbb{B}$. It follows that $\{Y_n, n = 0, 1, \ldots\}$ is a discrete-time Markov chain with transition matrix

$$\mathbb{Q} = \mathbb{R} \cdot \mathbb{P}(\tau)$$

Test interval $n - 2$

In the same way,

$$
\begin{aligned}
&\Pr(Z_{n+1} = k \mid Z_n = j) \\
&\quad = \sum_{i=0}^{r} \Pr(Z_{n+1} = k \mid Y_{n+1} = i, Z_n = j) \cdot \Pr(Y_{n+1} = i \mid Z_n = j) \\
&\quad = \sum_{i=0}^{r} P_{ji}(\tau) \cdot R_{ik} = [\mathbb{P}(\tau) \cdot \mathbb{R}]_{jk}
\end{aligned}
$$

and $\{Z_n, n = 0, 1, \ldots\}$ is a discrete-time Markov chain with transition matrix

$$\mathbb{T} = \mathbb{P}(\tau) \cdot \mathbb{R}$$

Stationary distribution – 1

Let $\pi = [\pi_0, \pi_1, \ldots, \pi_r]$ denote the stationary distribution of the Markov chain $\{Y_n, n = 0, 1, \ldots\}$. Then π is the unique probability vector satisfying the equation

$$\pi \cdot \mathbb{Q} \equiv \pi \cdot \mathbb{R} \cdot \mathbb{P}(\tau) = \pi$$

where π_i is the long-term proportion of times the system is in state i just before a test.

Stationary distribution – 2

In the same way, let $\gamma = [\gamma_0, \gamma_1, \ldots, \gamma_r]$ denote the stationary distribution of the Markov chain $\{Z_n, n = 0, 1, \ldots\}$. Then γ is the unique probability vector satisfying the equation

$$\gamma \cdot \mathbb{T} \equiv \gamma \cdot \mathbb{P}(\tau) \cdot \mathbb{R} = \gamma$$

where γ_i is the long-term proportion of times the system is in state i just after a test/repair.

Dangerous undetected failures

Let F denote the states representing dangerous undetected (DU) failure, and define $\pi_F = \sum_{i \in F} \pi_i$.

π_F denotes the long-run proportion of times the system has a DU failure just before a test. If, for example, $\pi_F = 5 \cdot 10^{-3}$, the system will have a critical failure, on the average, in one out of 200 tests.

Moreover, $1/\pi_F$ is the mean time, in the long run, between visits to F (measured with time unit τ). The mean time between DU failures is hence

$$\mathrm{MTBF}_{\mathrm{DU}} = \frac{\tau}{\pi_F}$$

and the average rate of DU failures is

$$\lambda_{\mathrm{DU}} = \frac{1}{\mathrm{MTBF}_{\mathrm{DU}}} = \frac{\pi_{\mathrm{F}}}{\tau}$$

Probability of failure on demand

The average PFD(n) in test interval n is now

$$\begin{aligned}\mathrm{PFD}(n) &= \frac{1}{\tau}\int_{(n-1)\tau}^{n\tau} \Pr(X(t) \in F)\, dt \\ &= \frac{1}{\tau}\int_0^{\tau} \sum_{j=0}^{r} \sum_{k\in F} P_{jk}(t) \cdot \Pr(Z_n = j)\, dt\end{aligned}$$

Average PFD

Since $\Pr(Z_n = j) \rightarrow \gamma_j$ when $n \rightarrow \infty$, we get the *long-term average* PFD as

$$\text{PFD} = \lim_{n\rightarrow\infty} \text{PFD}(n) = \frac{1}{\tau}\int_0^\tau \sum_{j=0}^{r}\sum_{k\in F} P_{jk}(t)\cdot\gamma_j\,dt = \sum_{j=0}^{r}\gamma_j Q_j$$

where

$$Q_j = \frac{1}{\tau}\int_0^\tau \sum_{k\in F} P_{jk}(t)\,dt$$

is the PFD given that the system is in state j at the beginning of the test interval.

Example 10.16 – 1

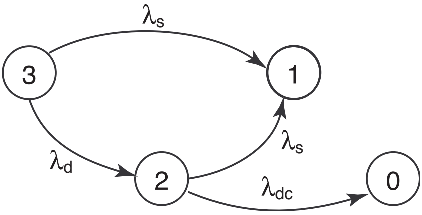
Consider a single component that is subject to various types of failure mechanisms. The following states are defined:

State	Description
3	Component as good as new
2	Degraded (noncritical) failure
1	Critical failure caused by sudden shock
0	Critical failure caused by degradation

The component is able to perform its intended function when it is in state 3 or state 2 and has a critical failure if it is in state 1 or state 0. State 1 is produced by a random shock, while state 0 is produced by degradation. In state 2 the component is able to perform its intended function but has a specified level of degradation.

Example 10.16 – 2

The Markov process is defined by the state transition diagram



Example 10.16 – 3

The transition rate matrix is

$$\mathbb{A} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \lambda_{\text{dc}} & \lambda_s & -(\lambda_{\text{dc}} + \lambda_s) & 0 \\ 0 & \lambda_s & \lambda_d & -(\lambda_s + \lambda_d) \end{pmatrix}$$

where λ_s is the rate of failures caused by a random shock, λ_d is the rate of degradation failures, and λ_{dc} is the rate of degraded failures that become critical.

Example 10.16 – 4

No repair is performed within the test interval, and the failed states 0 and 1 are therefore absorbing states.

Assume that we know that the system is in state 3 at time 0, such that $\rho = [1, 0, 0, 0]$. We may now use the methods outlined in Section 8.9 to solve the forward Kolmogorov equations $\mathbf{P}(t) \cdot \mathbb{A} = \dot{\mathbf{P}}(t)$ and find the distribution $\mathbb{P}(t)$. Hence, $\mathbb{P}(t)$ can be written as

$$\mathbb{P}(t) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ P_{20}(t) & P_{21}(t) & P_{22}(t) & 0 \\ P_{30}(t) & P_{31}(t) & P_{32}(t) & P_{33}(t) \end{pmatrix}$$

Example 10.16 – 5

The first two rows of $\mathbb{P}(t)$ are obvious since state 0 and state 1 are absorbing. The entry $P_{23}(t) = 0$ since it is impossible to have a transition from state 2 to state 3. From the state transition diagram the diagonal entries are seen to be

$$P_{22}(t) = e^{-(\lambda_s + \lambda_{\text{dc}})t}$$
$$P_{33}(t) = e^{-(\lambda_s + \lambda_d)t}$$

Example 10.16 – 6

The remaining entries were shown by Lindqvist and Amundrustad (1998) to be

$$
\begin{aligned}
P_{20}(t) &= \frac{\lambda_{\text{dc}}}{\lambda_s + \lambda_{\text{dc}}}\left(1 - e^{-(\lambda_s+\lambda_{\text{dc}})t}\right) \\
P_{21}(t) &= \frac{\lambda_s}{\lambda_s + \lambda_{\text{dc}}}\left(1 - e^{-(\lambda_s+\lambda_{\text{dc}})t}\right) \\
P_{30}(t) &= \frac{\lambda_d\lambda_{\text{dc}}}{(\lambda_d+\lambda_s)(\lambda_s+\lambda_{\text{dc}})} + \frac{\lambda_d\lambda_{\text{dc}}}{(\lambda_d-\lambda_{\text{dc}})(\lambda_d+\lambda_s)}\,e^{-(\lambda_s+\lambda_{\text{d}})t} \\
&\quad + \frac{\lambda_d\lambda_{\text{dc}}}{(\lambda_{\text{dc}}-\lambda_d)(\lambda_s+\lambda_{\text{dc}})}\,e^{-(\lambda_s+\lambda_{\text{dc}})t} \\
P_{31}(t) &= \frac{\lambda_s(\lambda_d+\lambda_s+\lambda_{\text{dc}})}{(\lambda_d+\lambda_s)(\lambda_s+\lambda_{\text{dc}})} + \frac{\lambda_s\lambda_{\text{dc}}}{(\lambda_d-\lambda_{\text{dc}})(\lambda_d+\lambda_s)}\,e^{-(\lambda_s+\lambda_d)t} \\
&\quad + \frac{\lambda_s\lambda_d}{(\lambda_{\text{dc}}-\lambda_d)(\lambda_s+\lambda_{\text{dc}})}\,e^{-(\lambda_s+\lambda_{dc})t}
\end{aligned}
$$

Example 10.16 – 7

Several repair policies may be adopted:

1. All failures are repaired after each test, such that system always starts in state 3 after each test.
2. All critical failures are repaired after each test. In this case, the system may have a degraded failure when it starts up after the test.
3. The repair action may be imperfect, meaning that there is a probability that the failure will not be repaired.

Example 10.16 – 8

All Failures Are Repaired after Each Test

In this case all failures are repaired, and we assume that the repair is perfect, such that the system will be in state 3 after each test. The corresponding repair matrix $\mathbb{R}_1$ is therefore

$$\mathbb{R}_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

With this policy, all test intervals have the same stochastic properties. The average PFD is therefore given by

$$\text{PFD} = \frac{1}{\tau} \int_0^{\tau} (P_{31}(t) + P_{30}(t))\, dt$$

Example 10.16 – 9

All Critical Failures Are Repaired after Each Test

In this case the $\mathbb{R}$ matrix is

$$\mathbb{R}_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Example 10.16 – 10

Imperfect Repair after Each Test

In this case the $\mathbb{R}$ matrix is

$$\mathbb{R}_3 = \begin{pmatrix} r_0 & 0 & 0 & 1-r_0 \\ 0 & r_1 & 0 & 1-r_1 \\ 0 & 0 & r_2 & 1-r_2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$