2. Failure & repair rates of each element are *constant* (time indep.) during the *sojourn time in each state*; not necessarily at a state change (e. g. load sharing).
3. Each element has *constant failure rate* (as in assumption 2).
4. The flow of failures is a *Poisson process* (homogeneous or nonhomogeneous).
5. *No further failures are considered* (can occur) *at system down* (*no FF*, (6.2)).
6. *No common cause failures can occur* & *redundant elements are repaired on-line*.
7. After each repair, *the repaired element is as-good-as-new* (6.5).
8. After a repair *the system is as-good-as-new with respect to the state* Z_i *entered after the repair*.
9. *Only one repair crew is available for the system*, and repair is performed according to a stated strategy, *first-in first-out or given repair priority* (6.3).
10. Totally independent elements (*totally IE*); i. e. each element operates and is repaired *independently of every other element* (n repair crews for n elements).
11. Ideal failures detection and localization; in particular, no *hidden failures*.
12. For each element E_i, $MTTR_i << MTTF_i$ (6.6).
13. Switches & *switching operations* are 100% reliable (have no aftereffect).
14. *Preventive maintenance* is not considered and logistic support is ideal (6.7).

Often it is tacitly assumed that each element has only 2 states (good / failed), one *failure mode* (e. g. shorts or opens), and a time invariant required function (e. g. continuous operation). Elements with more than 2 states or one failure mode are discussed in Section 6.8.5. A time dependent operation and / or required function can be investigated by assuming constant failure rates (Section 6.8.6.2). However,

to avoid ambiguities, a careful formulation of assumptions made is important to fix the validity of results obtained.

The following is a brief discussion of above assumptions. Assumption 1 often holds in practical applications. With assumption 2, time behavior of the system can generally be described by a time-homogeneous *Markov process* with finite number of states (pp. 496, 503). Equations can be established using a *diagram of transition rates* and Table 6.2. Difficulties can arise for the *large number of states involved* (p. 226). In such cases, a first possibility is to limit investigations to the mean time to failure $MTTF_{Si}$ and the asymptotic & steady-state point and average availability $PA_S = AA_S$. A second possibility is to use *approximate expressions* (Section 6.7) or special software tools (Section 6.9.6). Assumption 3 assures the existence of a *regenerative process with at least one regeneration state* (footnote on p. 386). Assumption 4 often applies to large systems. As shown in Sections 6.3-6.7, assumption 5 simplifies calculation of the point availability & interval reliability, it has

no influence on reliability function & $MTTF_{Si}$, and can be used for approximate expressions for $PA_S = AA_S$ when assumption 12 holds (Section 6.7.2).

Assumptions 6 & 11 must be met during *system design* (pp. 259, 274); if not satisfied,

improvements given by redundancy are questionable (Sections 4.2.1, 6.8.4).

of Markov processes is less appropriate because of their *memoryless property*). It

turns out that these processes constitute a new subclass of semi-Markov processes called in this book particular semi-Markov processes (allowing thus the use of the simple mathematical tools known for Markov processes).

For this purpose, all models of this section consider that *reaction times are common* (as for human reliability on pp. 295-96), and assume

that neither failures nor external events occur during human intervention (state $Z_{1'}$*), fail-safe procedure* ($Z_{2'}$)*, restart* (Z_{FS})*, and barriers activation* ($Z_E, Z_{E'}, Z_{E_1}, Z_{E_2}$); +) *moreover, fail-safe state* Z_{FS}*, entered after a successful fail-safe procedure, is an up state for safety (independently if fail-safe has been activated by intrinsic failure* ($Z_1 \to Z_{2'}$)*, human error* ($Z_{1'} \to Z_{2'}$)*, or not stopped external event* ($Z_E, Z_{E'}, Z_{E_1}, Z_{E_2} \to Z_{2'}$))*, and a restart (distribution* $F_r(x)$*, mean* M_r*) is necessary to bring the system in the operating state* Z_1. ++)

Consider first the case of Fig. 6.46 on p. 296, i. e. a *1-out-of-2 active redundancy with possible human error at failure* (two identical elements, constant failure & repair rates λ_{cr} & μ_{cr}, probability p_h for a false action causing failure of the not failed element and $\tau_h > 0$ (distribution $F_h(x)$, mean $E[\tau_h] = M_h < \infty$) as time to take the decision and make the corresponding action). Furthermore, let p_{fs} be the *success probability of the fail-safe procedure* (duration $\tau_{fs} > 0$, distribution $F_{fs}(x)$, mean $E[\tau_{fs}] = M_{fs} < \infty$) and $\tau_r > 0$ the *restart time* after a successful fail-safe procedure (distribution $F_r(x)$, mean $E[\tau_r] = M_r < \infty$). Considering above *general assumption* and *constant* failure & repair rates (λ_{cr} & μ_{cr}), the system can be investigated using a *particular semi-Markov process* (footnote on p. 296). Figure 6.49 gives the corresponding state transitions diagram for safety calculation. In Z_A the system is down for accident / disaster; Z_{FS} is a *system down state for reliability, not for safety*; in $Z_{2'}$ the fail-safe and in Z_{FS} the restart procedure is running ++). From Fig. 6.49 and Table 6.2 or Eq. (A7.173), $MTTA_{S0}$ (mean time to accident / disaster for system entering Z_0 at $t=0$) follows as solution of

$$M_0 = T_0 + M_{1'}, \quad M_{1'} = T_{1'} + (1-p_h) M_1 + p_h M_{2'}, \quad M_{2'} = T_{2'} + p_{fs} M_{FS},$$
$$M_1 = T_1 + (M_0 \mu_{cr} + M_{2'} \lambda_{cr}) / (\lambda_{cr} + \mu_{cr}), \quad M_{FS} = T_{FS} + M_1, \tag{6.328}$$

with $M_i \equiv MTTF_{Si}$, $T_i = \int_0^\infty (1 - Q_i(x))\,dx$, $Q_i(x) = \sum_j Q_{ij}(x)$ (Eqs. (A7.166) & (A7.165)). Considering Fig. 6.49 one has $T_0 = 1/2\lambda_{cr}$, $T_{1'} = M_h$, $T_1 = 1/(\lambda_{cr}+\mu_{cr})$, $T_{2'} = M_{fs}$ & $T_{FS} = M_r$, yielding

$$MTTA_{S0} = \frac{(\lambda+\mu)(1+2\lambda M_h) + 2\lambda(1-p_h) + 2\lambda(M_{fs} + M_r p_{fs})(\lambda + \mu p_h) - \lambda p_{fs}(1 + 2\lambda M_h - 2p_h)}{2\lambda(\lambda + \mu p_h)(1 - p_{fs})}$$
$$\approx \frac{\mu(1 + 2\lambda(M_h + p_h M_{fs} + p_h p_{fs} M_r))}{2\lambda(\lambda + \mu p_h)(1 - p_{fs})} \approx \frac{\mu}{2\lambda(\lambda + \mu p_h)(1 - p_{fs})}, \quad \lambda = \lambda_{cr}, \ \mu = \mu_{cr}. \tag{6.329}$$

+) Assumption valid by considering $M_h, M_{fs}, M_r, M_b << 1/\lambda_{cr}, 1/f_e$.

++) Z_1 as per Fig. 6.8; external events act on E_1 & E_2 in Z_0 and on E_1 or E_2 in Z_1, human errors act on E_1 or E_2 in $Z_{1'}$ (with this, E_1 & E_2 are failed when $Z_{2'}$ is entered); other situations are conceivable.

If a repairable system cannot be restored to be as-good-as-new after repair with respect to the up state Z_i entered after the repair, i. e., in particular, if at least one element with *time dependent failure rate* has not been renewed at each repair, *failure intensity* $z(t)$ must be used. The distinction between *failure rate* $\lambda(t)$ and *failure intensity* $z(t)$ or *intensity* $h(t)$ or $m(t)$ (for a renewal or Poisson process) is important. $z(t)$, $h(t)$, $m(t)$ are *unconditional intensities* (Eqs. (A7.229), (A7.24), (A7.194)) and *differ basically* from $\lambda(t)$, even for the case of a *homogeneous Poisson process*, for which $z(t) = h(t) = m(t) = \lambda$ holds (Eq. (A7.42), pp. 7, 482-83, 540). Also it is to note that $\lambda(t)$ *is not a* (probability) *density* (p. 442). For $\lambda(t)$, *force of mortality* [6.1, A7.30] and *hazard rate* have been suggested, both terms should be avoided.

Fault [A1.4]

Inability to perform as required, due to an internal state.

Perform as required means *perform the required function under stated conditions*. A fault is a *state resulting from a failure or a defect*, having as possible cause a *failure mechanism* for failures or a *flaw* (error or mistake) for defects & systematic failures. Not considered as fault are down states caused by external actions or events (e. g. preventive maintenance or loss of resources). For software, a *fault always results from a defect.*

Fault Tree Analysis (FTA) [A1.4 (FT+FTA)]

Deductive analysis using logic diagrams, showing the faults of subitems, external events, or combination thereof, which cause a predefined, undesired event.

Top event is the predefined, undesired event (generally at item (system) level). FTA is a *top-down* approach, which allows inclusion of external causes more easily than for an FMEA/FMECA. However, it does not necessarily go through all possible *fault modes*. Combination of FMEA/FMECA with FTA and *event tree analysis* leads to *causes-to-effects charts*, showing relationships between identified causes and their single or *multiple consequences* (Sections 2.6, 6.9.2, 6.9.3); such a combination of tools is necessary for items (systems) with high safety requirements.

Item [A1.4]

Subject being considered.

An item is a functional or structural *unit*, generally considered as an *entity* for investigations. It can consist of hardware and/or software and include human resources. For hardware it can be, for instance, a component (part, device), assembly, equipment, subsystem or system.

Life-Cycle Cost (LCC) [A1.4]

Total cost incurred during the item's life cycle.

Life-cycle cost is the sum of cost for acquisition, operation, maintenance, and disposal or recycling of the item. They have to consider also effects to the environment of production, use & disposal or recycling of the item considered (sustainable development). Their optimization uses *cost effectiveness* or *systems engineering* tools and can be positively influenced by *concurrent engineering*.