POLITECNICO DI MILANO

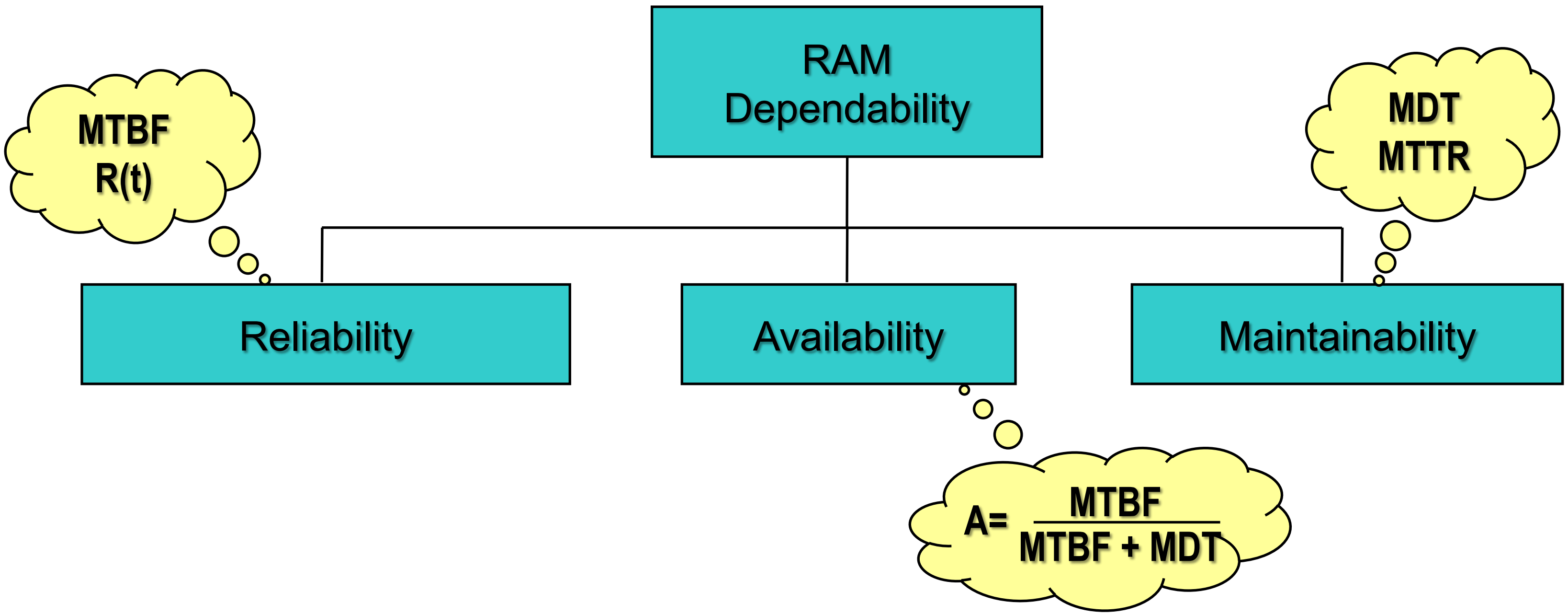
CRC
Centre de recherche sur les Risques et les Crises

Reliability of Simple Systems

Prof. Enrico Zio

Politecnico di Milano
Dipartimento di Energia

Background



- **Definition under IEC 50 (191):**
- **Summarising expression to describe availability and its influencing factors, reliability and maintainability.**
- ***Note*: Dependability is only used for general descriptions of non-quantitative character.**

- **Broad definition:**
- **Dependability is the methodical approach of estimating, analysing and avoiding failures in the future.**

Index

1. Probability theory: basic definitions
2. Reliability analysis: theory and examples

Index

1. Probability theory: basic definitions
2. Reliability analysis: theory and examples

Introduction: reliability and availability

- **Reliability** and **availability**: important performance parameters of a system, with respect to its ability to fulfill the required mission in a given period of time

- Two different system types:
  - Systems which must satisfy a specified mission within an assigned period of time: **reliability** quantifies the ability to achieve the desired objective without failures
  - Systems maintained: **availability** quantifies the ability to fulfill the assigned mission at **any** specific moment of the life time

Maintainablilty:

Ability of a unit, under given circumstances, to maintain or respectively to reset its actual state so that the desired requirements are met, provided that maintenance is carried out using the specified resources and stated procedures.

Basic definitions (1)

Reliability **is the ability of an item to perform a required function under stated conditions for a stated period of time.**

Therefore….
the *failure* is an event
whereby a unit or component
under consideration is no longer
capable of fulfilling a required function
under stated conditions
for a stated the period of time.

Basic definitions (2)

The *required function* includes the specification of satisfactory operation as well as unsatisfactory operation. For a complex system, unsatisfactory operation may not be the same as failure.

The *stated conditions* are the total physical environmental including mechanical, thermal, and electrical conditions.

The *stated period of time* is the time during which satisfactory operation is desired, commonly referred to as service life.

Basic definitions (3)

- T = Time to failure of a component (random variable)
  - cdf = $F_T(t)$ = probability of failure before time t: $P(T<t)$
  - pdf = $f_T(t)$ = probability density function at time t:

$$f_T(t)dt = P(t<T<t+dt)$$

  - ccdf = $R(t) = 1- F_T(t)$ = reliability at time t: $P(T>t)$
  - $h_T(t)$ = **hazard function** or failure rate at time t

$$\boxed{h_T(t)dt = P(t < T \le t + dt \mid T > t) = \frac{P(t < T \le t + dt)}{P(T > t)} = \frac{f_T(t)dt}{R(t)}}$$

Hazard function: the bath-tub curve

Three types of failures:

- **Early failures** (Infant mortality), caused by errors in design, defects in manufacturing, etc..

  Characteristic: The failure rate is initially high, but rapidly decreases.

- **Wear-out failures**, caused by ageing.

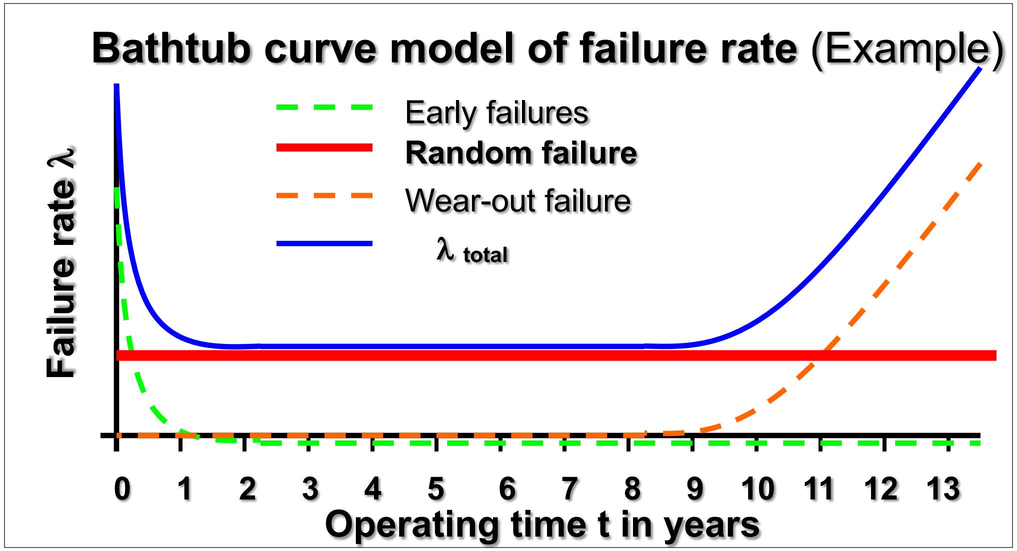
  Characteristic: The failure rate increases monotonically.

(Both types are systematic failures and could be prevented by improvement in design, manufacturing, maintenance).

- **Random failure:** appear spontaneously and purely by chance.

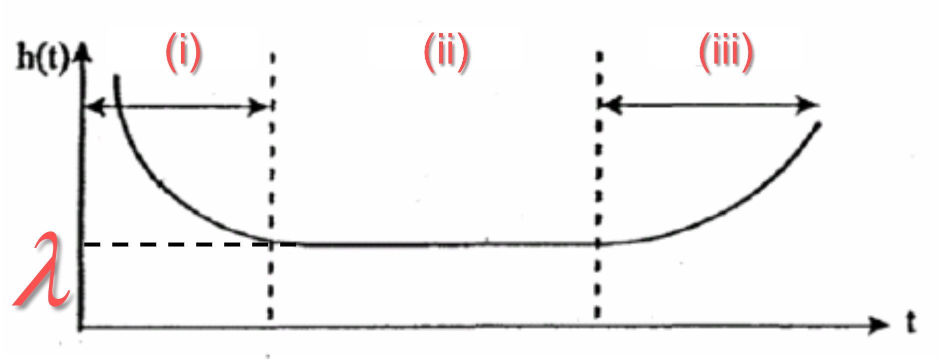
  Characteristic: Constant failure rate during the whole lifetime of the units.

These types of failure rates result in the traditional bathtub curve



Hazard function: the bath-tub curve

- The hazard function shows three distinct phases:
  i. Decreasing - *infant mortality* or *burn in period*
  ii. Constant - *useful life*
  iii. Increasing - *ageing*



The unit of the failure rate λ is failure/time, often indicated as FIT (Failure in Time).
e.g. **1 FIT = 1 Failure per 10^9h in FRU**(Field Replaceable Unit) **employed in the railway industry**

Field-Replaceable Unit (FRU)

In electronic hardware, particularly computer systems, a field-replaceable unit (FRU) is a circuit board or part that can be quickly and easily removed and replaced by the user or by a technician without having to send the entire product or system to a repair facility. The defective unit is found by standard troubleshooting procedures, removed, and either discarded or shipped back to the factory for repair. The new unit is installed directly in place of the defective one.

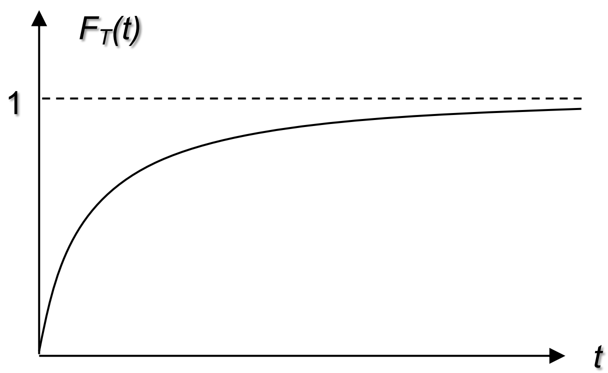
The FRU scheme is often the most cost-effective way to maintain complex systems, and is a major motivating factor behind the evolution of modular construction. When backed up by good parts availability, knowledgeable technical support, and reader-friendly documentation, this approach can minimize system downtime and optimize reliability.

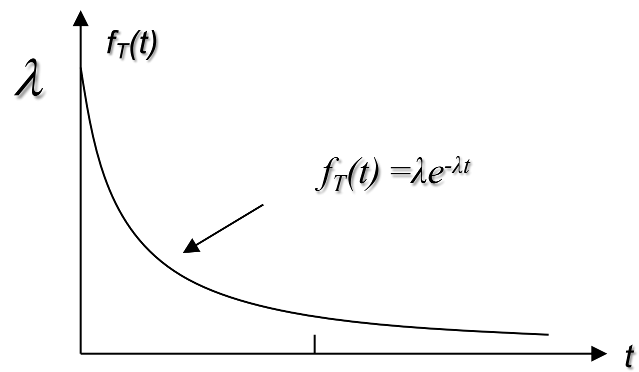
The exponential distribution (1)

- $h_T(t) = \lambda,\ t \geq 0$

$$\boxed{F_T(t) = P(T \leq t) = 1 - e^{-\lambda t}}$$

$$\boxed{\begin{cases} f_T(t) = \lambda e^{-\lambda t} & t \geq 0 \\ \quad = 0 & t < 0 \end{cases}}$$





- Only distribution characterized by a constant hazard rate
- Widely used in reliability practice to describe the constant part of the bath-tub curve

The exponential distribution (2)

- The expected value and variance of the distribution are:

$$E[T] = \frac{1}{\lambda} = MTTF \qquad ; \qquad Var[T] = \frac{1}{\lambda^2}$$

- Failure process is **memoryless**

$$P(t_1 < T < t_2 \mid T > t_1) = \frac{P(t_1 < T < t_2)}{P(T > t_1)} = \frac{F_T(t_2) - F_T(t_1)}{1 - F_T(t_1)} =$$

$$= \frac{e^{-\lambda t_1} - e^{-\lambda t_2}}{e^{-\lambda t_1}} = 1 - e^{-\lambda (t_2 - t_1)}$$

The exponential distribution (3)

IEC 61709: Electronic components –Reliability – Reference conditions for failure rates and stress models for conversion

The failure rate under given operating conditions is calculated as follows:

$$\lambda = \lambda_{Ref} \cdot \pi_U \cdot \pi_I \cdot \pi_T$$

where
λ_{ref} is the failure rate under reference conditions;
π_U is the voltage dependence factor;
π_I is the current dependence factor;
π_T is the temperature dependence factor.
These Parameter are listed, e.g in the SN29000 library!

Reference conditions for climatic and mechanical stresses

Type of stress	Reference condition [1)]
Ambient temperature [2)]	$\theta_{amb, ref} = 40$ °C
Climatic conditions	Class 3K3 as per IEC 721-3-3
Mechanical stress	Class 3M3 as per IEC 721-3-3
Special stresses [3)]	None

For details of notes (-1, -2,-3) please refer to IEC 61709

The definitions, reference conditions and conversion models used in the IEC 61709 fully correspond with the already existing SIEMENS standard SN 29500 method.

The Weibull distribution

- In practice, the age of a component influences its failure process so that the hazard rate does not remain constant throughout the lifetime

$$F_T(t) = P(T \le t) = 1 - e^{-\lambda t^{\alpha}}$$

$$\begin{cases} f_T(t) = \lambda \alpha t^{\alpha-1} e^{-\lambda t^{\alpha}} & t \ge 0 \\ \quad\quad = 0 & t < 0 \end{cases}$$

$$E[T] = \frac{1}{\lambda}\Gamma\left(\frac{1}{\alpha}+1\right) \quad ; \quad Var[T] = \frac{1}{\lambda^2}\left(\Gamma\left(\frac{2}{\alpha}+1\right) - \Gamma\left(\frac{1}{\alpha}+1\right)\right)^2$$

$$\Gamma(k) = \int_0^{\infty} x^{k-1} e^{-x} dx \qquad k > 0$$

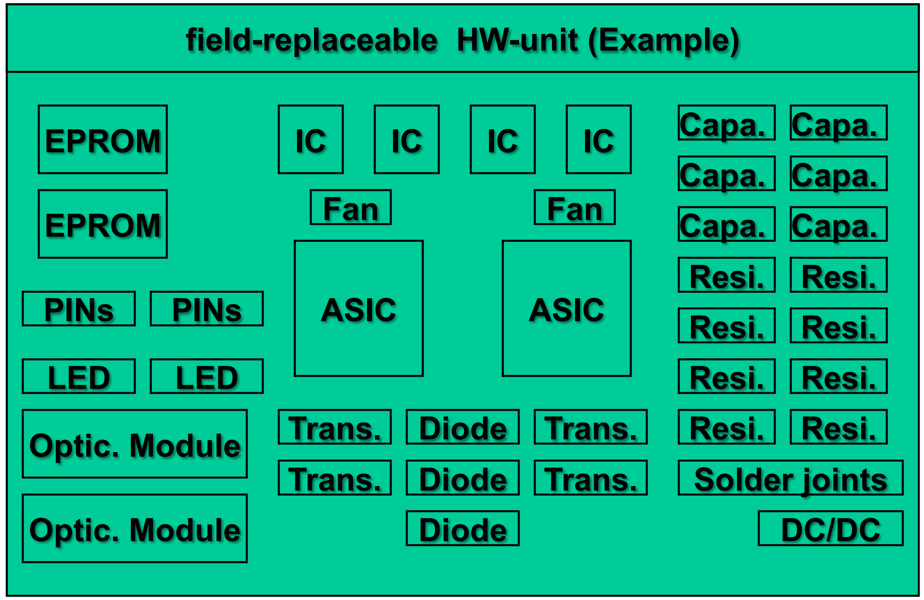
Index

1. Probability theory: basic definitions
2. Reliability analysis: theory and examples

Definition of the problem

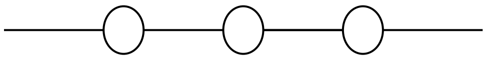
- **Objective**:
  - Computation of the system reliability *R(t)*
- **Hypotheses**:
  - *N* = number of system components
  - The components' reliabilities $R_i(t)$, i = 1, 2, …, *N* are known
  - The system **configuration** is known

Series system



Name of Components	Failure rates of $\lambda_{\text{Components}}$	No.of Comp.	No.of Pins	Sum of failure rates
Resistors	1 FIT	8	16	8 FIT
Capacitors	2 FIT	6	12	12 FIT
Diodes	8 FIT	3	6	24 FIT
Transistors	15 FIT	4	12	60 FIT
ICs	25 FIT	4	64	100 FIT
EPROM	100 FIT	2	64	200 FIT
DC/DC	40 FIT	2	28	80 FIT
ASIC	250 FIT	2	1016	500 FIT
FAN	150 FIT	2	10	300 FIT
Optical Module	800 FIT	2	32	1.600 FIT
Solder joints	0,1 FIT		1260	126 FIT
Example: tot. failure rate of the HW-unit λ_{unit} =3.010 FIT				

Series system



- All components must function for the system to function

$$\boxed{R(t) = \prod_{i=1}^{N} R_i(t)}$$

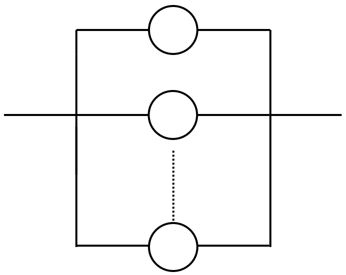
- For *N* **exponential** components:

$$\boxed{R(t) = e^{-\lambda t}} \longrightarrow \boxed{\begin{cases} \lambda = \sum_{i=1}^{N} \lambda_i \\ E[T] = \dfrac{1}{\lambda} \end{cases}}$$

$\lambda = \sum_{i=1}^{N} \lambda_i$ ⟶ System failure rate

$E[T] = \frac{1}{\lambda}$ ⟶ *MTTF*

Parallel system



- All components must fail for the system to fail

$$\boxed{R(t) = 1 - \prod_{i=1}^{N} \left[1 - R_i(t)\right]}$$

- For *N* **exponential** components:

$$\boxed{R(t) = 1 - \prod_{i=1}^{N} \left[1 - e^{-\lambda_i t}\right]} \longrightarrow \boxed{\left\{ \begin{aligned} MTTF = & \sum_{i=1}^{N} \frac{1}{\lambda_i} - \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} \frac{1}{\left[\lambda_i + \lambda_j\right]} + \\ & + \sum_{i=1}^{N-2} \sum_{j=i+1}^{N-1} \sum_{k=j+1}^{N} \frac{1}{\left[\lambda_i + \lambda_j + \lambda_k\right]} - \ldots + (-1)^{N-1} \frac{1}{\sum_{i=1}^{N} \lambda_i} \end{aligned} \right.}$$

Parallel system: an example

- Two exponential units with failure rates λ_1 and λ_2

$$R(t) = 1 - (1 - e^{-\lambda_1 t})(1 - e^{-\lambda_2 t}) = \underbrace{e^{-\lambda_1 t}}_{R_1} + \underbrace{e^{-\lambda_2 t}}_{R_2} - e^{-(\lambda_1+\lambda_2)t} > R_1(t), \quad R_2(t) > e^{-\lambda t} = e^{-(\lambda_1+\lambda_2)t} \ (series)$$

$$MTTF = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{[\lambda_1 + \lambda_2]}$$

- For N identical elements, compare series and parallel

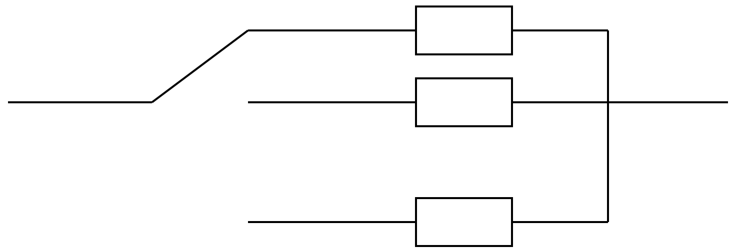
$$\left.\begin{array}{ll} parallel & MTTF = \sum_{n=1}^{N} \frac{1}{n\lambda} \\ series & MTTF = \frac{1}{N\lambda} \end{array}\right\} \longrightarrow \lambda \cdot MTTF_{series} = \frac{1}{N} < \sum_{n=1}^{N} \frac{1}{n} = \lambda \cdot MTTF_{parallel}$$

r-out-of-N system

- N identical components function in parallel but only r are needed (parallel system: $r = 1$)
- For N identical **exponential** components:

$$\boxed{R(t) = \sum_{k=r}^{N} \binom{N}{k} e^{-\lambda k t} \left(1 - e^{-\lambda t}\right)^{N-k}} \longrightarrow \boxed{MTTF = \sum_{k=r}^{N} \frac{1}{k\lambda}}$$

Standby system



- One component is functioning and when it fails it is replaced immediately by another component (sequential operation of one component at a time)
- The system configuration is **time-dependent** $\Rightarrow$ the story of the system from t = 0 must be considered
- Two types of standby:
  - **Cold**: the standby unit cannot fail until it is switched on
  - **Hot**: the standby unit can fail also while in standby

Cold standby (1)

- Since the components are operated sequentially, the system fails at time $T=\sum_{i=1}^{N} T_i$, which is a random variable sum of *N* independent random variables

- **Convolution** theorem

Example: 2 components

$$\left.\begin{array}{l} T_1, f_{T1}(t) \\ T_2, f_{T2}(t) \end{array}\right\} \Rightarrow T = T_1 + T_2,\ f_T(t) = f_{T1}(t) * f_{T2}(t) = \int_{-\infty}^{\infty} f_{T1}(x) f_{T2}(t-x)dx$$

$$L[f(x)] = \tilde{f}(s) = \int_0^{\infty} e^{-s\cdot x} f(x)dx \quad \tilde{f}_T(s) = L[f_{T1}(t) * f_{T2}(t)] = \tilde{f}_{T1}(s)\tilde{f}_{T2}(s)$$

Cold standby (2)

Example: N components

$$\tilde{f}_T(s) = \prod_{i=1}^{N} \tilde{f}_{Ti}(s)$$

$$\boxed{R(t) = 1 - \int_0^t f_T(x)dx}$$

Cold standby: an example

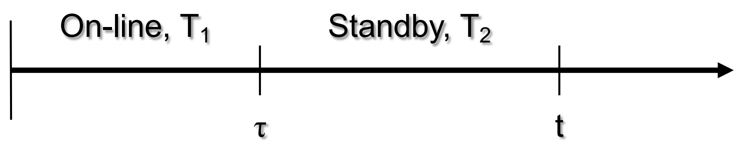
- Consider a "cold" standby system of two units
- The on-line unit has an *MTTF* of 2 years
- When it fails, the standby unit comes on line and its *MTTF* is 3 years
- Assume that each component has an exponential failure times distribution

(1) What is the probability density function of the system failure time? What is the *MTTF* of the system?
(2) Repeat assuming that the two components are in parallel in a one-out-of-two configuration

Cold standby: an example – solution (1)

$$MTTF_i = \int_0^{\infty} t f_{Ti}(t)dt = \int_0^{\infty} \lambda_i t e^{-\lambda_i t} dt = \frac{1}{\lambda_i}$$

$$\boxed{\lambda_1 = \frac{1}{2yrs}} \qquad \boxed{\lambda_2 = \frac{1}{3yrs}}$$



- T_1 and T_2 are independent random variables denoting the times when the on-line and standby units are operating, respectively
- The system failure time is also a random variable, $T = T_1+T_2$

$$\boxed{f_T(t) = \int_0^t \lambda_1 e^{-\lambda_1 \tau} \lambda_2 e^{-\lambda_2 (t-\tau)} d\tau = \lambda_1 \lambda_2 \int_0^t e^{-(\lambda_1-\lambda_2)\tau} e^{-\lambda_2 t} d\tau = \lambda_1 \lambda_2 e^{-\lambda_2 t} \int_0^t e^{-(\lambda_1-\lambda_2)\tau} d\tau =}$$

$$\boxed{= \frac{\lambda_1 \lambda_2}{\lambda_2 - \lambda_1} e^{-\lambda_2 t} \left(e^{-(\lambda_1-\lambda_2)\tau} \right)_0^t = \frac{\lambda_1 \lambda_2}{\lambda_2 - \lambda_1} \left(e^{-\lambda_1 t} - e^{-\lambda_2 t} \right) = e^{-t/3yrs} - e^{-t/2yrs}}$$

Cold standby: an example – solution (2)

$$u = \frac{t}{3yrs} \int_{o}^{\infty} t f_T(t) dt = \int_{0}^{\infty} (t e^{-t/3yrs} - t e^{-t/2yrs}) dt$$

$$u = \frac{t}{3yrs} \qquad \xi = \frac{t}{2yrs}$$

$$MTTF = (3yrs)^2 \left[-ue^{-u} - e^{-u} \right]_0^{\infty} - (2yrs)^2 \left[-\xi e^{-\xi} - e^{-\xi} \right]_0^{\infty} =$$

$$= (3yrs)^2 \left(\frac{1}{yr} \right) - (2yrs)^2 \left(\frac{1}{yr} \right) = 5yrs$$

(3.8*yrs* for parallel!)

Hot standby (1)

- The convolution theorem can no longer be used to calculate the reliability of the system, because there is no independence of failures any more
- Simple case of two components: the system will perform its task in the interval (0, t) in either of the two mutually exclusive ways:
  - the online component 1 does not fail in (0, t)
    [probability = $R_1(t)$]
  - the online component fails in (0, τ) [probability = $f_{T1}(\tau)d\tau$];
    the standby component 2 does not fail in (0, τ) [probability $R_s(\tau)$]

    and it operates successfully from τ to t [probability $R_2(t-\tau)$]

Hot standby (2)

- The system reliability is given by the sum of the probabilities of the two mutually exclusive events:

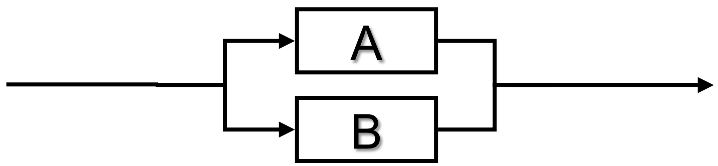
$$R(t) = R_1(t) + \int_0^t f_1(\tau)\,d\tau\, R_s(\tau)\, R_2(t-\tau)$$

- For 2 **exponential** components:

$$R(t) = e^{-\lambda_1 t} + \int_0^t \lambda_1 e^{-\lambda_1 \tau} e^{-\lambda_s \tau} e^{-\lambda_2 (t-\tau)} d\tau =$$

$$= e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_1 + \lambda_s - \lambda_2}\left[e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_s)t}\right]$$

Time-dependent systems: an example



- When both A and B are fully energized they share the total load and the failure densities are $f_A(t)$ and $f_B(t)$
- If either one 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

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

Time-dependent systems: an example - solution

- *R(t)* = P{system survives up to *t*} = P{neither component fails before *t*}+P{one fails at some time $\tau < t$, the other one survives up to τ, with *f(t)*, and from τ to *t* with *g(t)*} =

$$\boxed{= e^{-2\lambda t} + 2\int_0^t \left(\lambda e^{-\lambda\tau} d\tau\right)\left(e^{-\lambda\tau}\right)\left(e^{-k\lambda(t-\tau)}\right) = e^{-2\lambda t} + 2\lambda e^{-k\lambda t}\int_0^t e^{-\lambda(2-k)\tau} d\tau =}$$

$$= \frac{2e^{-k\lambda t} - ke^{-2\lambda t}}{2-k}$$