



## Reliability of Simple Systems



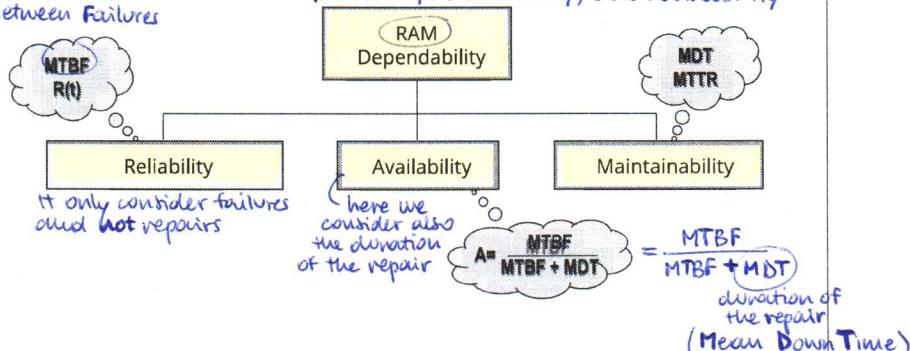
Prof. Enrico Zio

Politecnico di Milano  
Dipartimento di Energia

### Background

#### Reliability, Availability, Maintainability

CRC



- 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.

Prof. Enrico Zio

POLITECNICO DI MILANO

### Index

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

## 1. Probability theory: basic definitions

## 2. Reliability analysis: theory and examples

## Introduction: reliability and availability

They characterize the performance of a system or a component in terms of its functionality, in terms of its ability to provide the task for which they are designed.

- **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

### Maintainability:

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.

we want to know the ability of a system/component to provide its functional task for a given time without interruption (e.g. a train must be reliable because we cannot stop a race, repair it and restart the race).

availability allows describing a different situation of usage of a system. It's used for systems in which components can accept a failure (an interruption of the system) and then have an maintenance requirement and then restart again.

Availability says if a system is available at a given time.

## Basic definitions (1)

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

It's not for any possible condition and any time in the future.

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)

CRC

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.

Prof. Enrico Zio

POLITECNICO DI MILANO

CRC

## 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  $t$  (conditional density function)

It gives the probability of failure in the next  $dt$  given that the system has not failed yet

$$h_T(t)dt = P(t < T \leq t + dt | T > t) = \frac{P(t < T \leq t + dt)}{P(T > t)} = \frac{f_T(t)dt}{R(t)}$$

it's random because we do not have having full understanding and full knowledge of the process of degradation, effects of corrosion and so on

cumulative density function

probability density function

complementary cumulative distribution function

Prof. Enrico Zio

POLITECNICO DI MILANO

CRC

## 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.

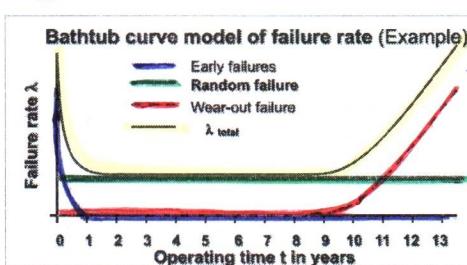
Characteristic: The failure rate increases monotonically.

(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



the  $\lambda_{\text{total}}$  represents the total (the sum of the three types of failures)  
→ BATH-TUB CURVE

Prof. Enrico Zio

POLITECNICO DI MILANO

## Hazard function: the bath-tub curve

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



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

We can introduce the failure in time w.r.t. the scale of the mission time

Prof. Enrico Zio

POLITECNICO DI MILANO

CRC

## 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.

Prof. Enrico Zio

POLITECNICO DI MILANO

CRC

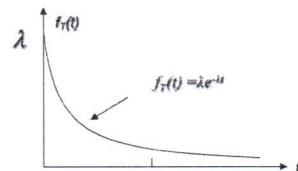
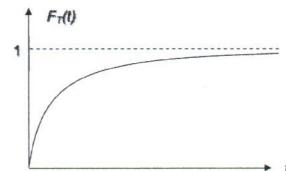
## The exponential distribution (1)

The only distribution with constant failure rate:  $\lambda$ .

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

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

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



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

Prof. Enrico Zio

POLITECNICO DI MILANO

## The exponential distribution (2)

CRC

- The expected value and variance of the distribution are:

Mean Time To Failure

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

- Failure process is memoryless

$$\begin{aligned} P(t_1 < T < t_2 | T > t_1) &= \frac{P(t_1 < T < t_2)}{P(T > t_1)} = \frac{F_T(t_2) - F_T(t_1)}{1 - F_T(t_1)} = \\ &= \frac{e^{-\lambda t_1} - e^{-\lambda t_2}}{e^{-\lambda t_1}} = 1 - e^{-\lambda(t_2 - t_1)} \end{aligned}$$

When we move to other values of  $t_1$  and  $t_2$  it doesn't remember that some time has passed (some "life" has passed)

It depends only on the interval length: it has no memory of how long the system lived up to  $t_1$ .

Prof. Enrico Zio

POLITECNICO DI MILANO

CRC

## The exponential distribution (3)

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

parameters which identify the influence of the stress conditions specific to particular variables, process variables and manufacture variables

failure rate characterization of the component as it comes out from production

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

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

base reference value for the failure rate

where  
 $\lambda_{ref}$  is the failure rate under reference conditions;  
 $\pi_U$  is the voltage dependence factor;  
 $\pi_I$  is the current dependence factor;  
 $\pi_T$  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)	$\theta_{amb, ref} = 40^\circ C$
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 1-1, -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.

Prof. Enrico Zio

POLITECNICO DI MILANO

CRC

## The Weibull distribution

Special case: if  $\alpha = 1 \rightarrow$  exponential distribution

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

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

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

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

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

- $\alpha < 1$ : we have a decreasing hazard rate
- $\alpha = 1$ : constant failure/hazard rate
- $\alpha > 1$ : aging period

Prof. Enrico Zio

POLITECNICO DI MILANO

# Index

## 1. Probability theory: basic definitions

## 2. Reliability analysis: theory and examples

Prof. Enrico Zio

POLITECNICO DI MILANO



## Definition of the problem

### • Objective:

- Computation of the system reliability  $R(t)$  : given the system configuration and the probabilistic description over time to failure of each component, how do we compute the system reliability?

### • Hypotheses:

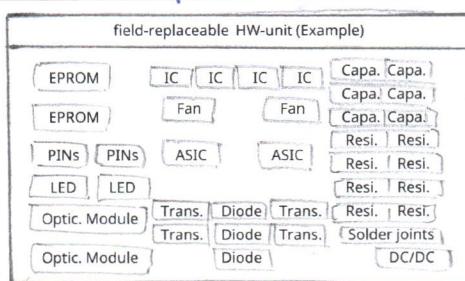
- $N$  = number of system components
- The components' reliabilities  $R_i(t)$ ,  $i = 1, 2, \dots, N$  are known
- The system configuration is known

Prof. Enrico Zio

POLITECNICO DI MILANO



## Series system : example



Name of Components	Failure rates of 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 = 3.010 FIT

we have a number of field-replaceable units (FRUs)

)  
and their characterizations in terms of failure rates expressed in failures in times

we have 8 resistors. If we put 8 resistors in series then the sum of failure rates is 8 ( $\sum_{i=1}^8 1$ )

Prof. Enrico Zio

POLITECNICO DI MILANO

## Series system



- All components must function for the system to function

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

= probability that the system does not fail until time t (before)

= probability that all the components do not fail before the time t

this is an intersection of events

! A system has a constant failure rate if its components have constant failure rates and its configuration is in series.

- For N exponential components:

$$R(t) = e^{-\lambda t}$$

$$\begin{cases} \lambda = \sum_{i=1}^N \lambda_i \\ E[T] = \frac{1}{\lambda} \end{cases}$$

→ System failure rate

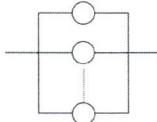
→ MTTF

Prof. Enrico Zio

POLITECNICO DI MILANO

CRC

## Parallel system



- All components must fail for the system to fail

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

= probability that the system does not fail before time t

= probability that at least one component does not fail until time t

- For N exponential components:

$$R(t) = 1 - \prod_{i=1}^N [1 - e^{-\lambda_i t}]$$

$$\begin{aligned} MTTF &= \sum_{i=1}^N \frac{1}{\lambda_i} - \sum_{i=1}^{N-1} \sum_{j=i+1}^N \frac{1}{[\lambda_i + \lambda_j]} + \\ &+ \sum_{i=1}^{N-2} \sum_{j=i+1}^{N-1} \sum_{k=j+1}^N \frac{1}{[\lambda_i + \lambda_j + \lambda_k]} - \dots + (-1)^{N-1} \frac{1}{\sum_{i=1}^N \lambda_i} \end{aligned}$$

Prof. Enrico Zio

POLITECNICO DI MILANO

CRC

## Parallel system: an example

- Two exponential units with failure rates  $\lambda_1$  and  $\lambda_2$

1.

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

2.

3.

Mean Time To Fail

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

- For N identical elements, compare series and parallel

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

$$\rightarrow \lambda \cdot MTTF_{\text{series}} = \frac{1}{N} < \sum_{n=1}^N \frac{1}{n} = \lambda \cdot MTTF_{\text{parallel}}$$

$MTTF_{\text{series}} < MTTF_{\text{parallel}}$

The probability of a system in parallel (1) to not fail is bigger than the probability of not failing of the singular components (2). Both (1) and (2) are bigger probs. than the probability of a system in series to not fail. "To not fail" means "to not fail until time t".

Prof. Enrico Zio

POLITECNICO DI MILANO

## 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:

$$R(t) = \sum_{k=r}^N \binom{N}{k} e^{-\lambda kt} (1 - e^{-\lambda t})^{N-k} \rightarrow MTTF = \sum_{k=r}^N \frac{1}{k\lambda}$$

This because the system works if we have exactly  $r$  components or  $r+1$  or  $r+2$  or.. or  $N$ . Since we have "or" and the events are exclusive (we have either  $r$  or  $r+1$  components working) we can sum.

BINOMIAL:

$k$  out of  $N$  functioning probability of functioning of each one is:  $e^{-\lambda t}$

→  $k$  functioning:  $(e^{-\lambda t})^k$

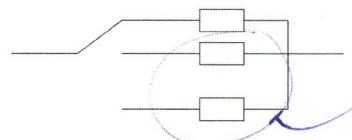
→  $N-k$  not functioning:  $(1 - e^{-\lambda t})^{N-k}$

Prof. Enrico Zio

POLITECNICO DI MILANO

CRC

## Standby system



some components "of reserve". We connect them to the production only if the main component fails. This is neither series nor parallel or r-out-of-N.

- 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 ⇒ 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

(simplification of the reality)  
the failure probability is smaller since the component is not stressed

Prof. Enrico Zio

POLITECNICO DI MILANO

CRC

## 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

The system fails when the last stand-by component fails. The main component fails at  $T_1$ , the second (first stand-by) activates and lasts for a time  $T_2$  and so on. The ultimate failure is after:  
 $T = \sum_{i=1}^N T_i$

- Convolution theorem

Example: 2 components

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

$$L[f(x)] = \tilde{f}(s) = \int_0^{\infty} e^{-sx} f(x) dx \quad \tilde{f}_T(s) = L[f_{T_1}(t) * f_{T_2}(t)] = \tilde{f}_{T_1}(s) \tilde{f}_{T_2}(s)$$

If we have a large number of components it may be convenient to switch to the LAPLACE TRANSFORM

The probability that the system fails at time  $t$  is the probability that the 1<sup>st</sup> component fails at time  $x$  and the 2<sup>nd</sup> fails  $t-x$  time after. Obviously the failure of the 1<sup>st</sup> can occur anywhere, that's why we do the integral (we consider all the possible scenarios). Actually in our case:

$$\int_{-\infty}^{+\infty} \rightarrow \int_0^t$$

Prof. Enrico Zio

POLITECNICO DI MILANO

## Cold standby (2)

CRC

Example: N components

in the LAPLACE TRANSFORM

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

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

Prof. Enrico Zio

POLITECNICO DI MILANO

CRC

## 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

Prof. Enrico Zio

POLITECNICO DI MILANO

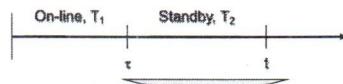
CRC

## Cold standby: an example – solution (1)

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

$$\lambda_1 = \frac{1}{2 \text{ yrs}}$$

$$\lambda_2 = \frac{1}{3 \text{ yrs}}$$



- $T_1$  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,  $T = T_1 + T_2$

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

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

Prof. Enrico Zio

POLITECNICO DI MILANO

## Cold standby: an example – solution (2)

CRC

$$u = \frac{t}{3\text{yrs}} \int_0^\infty t f_T(t) dt = \int_0^\infty (te^{-t/3\text{yrs}} - te^{-t/2\text{yrs}}) dt$$

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



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

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

*(3.8yrs for parallel!)*  
On average the parallel configuration fails earlier (w.r.t. the standby)

Prof. Enrico Zio

POLITECNICO DI MILANO

CRC

## 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:
  1. > the online component 1 does not fail in  $(0, t)$  [probability =  $R_1(t)$ ]
  2. > the online component fails in  $(0, \tau)$  [probability =  $f_{T_1}(\tau)d\tau$ ]; the standby component 2 does not fail in  $(0, \tau)$  [probability  $R_2(\tau)$ ]; and it operates successfully from  $\tau$  to  $t$  [probability  $R_2(t-\tau)$ ]

This scenario has  $\infty$  probabilities (since  $\tau$  can be anything in  $(0, t)$ )

Prof. Enrico Zio

POLITECNICO DI MILANO

CRC

## Hot standby (2)

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

$$R(t) = R_1(t) + \int_0^t f_{T_1}(\tau) d\tau R_2(\tau) R_2(t-\tau)$$

- For 2 exponential components:

$$\begin{aligned} R(t) &= e^{-\lambda_1 t} + \int_0^t \lambda_1 e^{-\lambda_1 \tau} e^{-\lambda_2 (t-\tau)} d\tau = \\ &= e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_1 + \lambda_2 - \lambda_1} \left[ e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t} \right] \end{aligned}$$

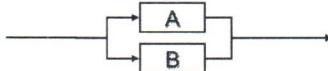
Prof. Enrico Zio

POLITECNICO DI MILANO

## Time-dependent systems: an example

CRC

**Shared-load system:** parallel system that shares a load. If one of the two components fails, the load goes all on the other component, however, the remaining component is overstressed and therefore its failure probability increases (since it's in overstressed conditions).



- 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

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

Prof. Enrico Zio

POLITECNICO DI MILANO

CRC

## Time-dependent systems: an example - solution

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

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

probability  
that A doesn't  
fail and B  
doesn't fail

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

A fails at time  $\tau$  and B continues for both up to time  $t$   
 or  
 B fails at time  $\tau$  and A continues up to time  $t$   
 this is the reason for "2"

Prof. Enrico Zio

POLITECNICO DI MILANO

$$P(\text{one of the two fails at time } \tau) = \lambda e^{-\lambda \tau} d\tau$$

$$P(\text{the other survives up to } \tau \text{ under normal conditions}) = e^{-\lambda \tau}$$

$$P(\text{the one survived continues to survive up to } t \text{ under "extreme" conditions}) = e^{-k\lambda(t-\tau)}$$