Dependable Systems

Definitions and Metrics (III)

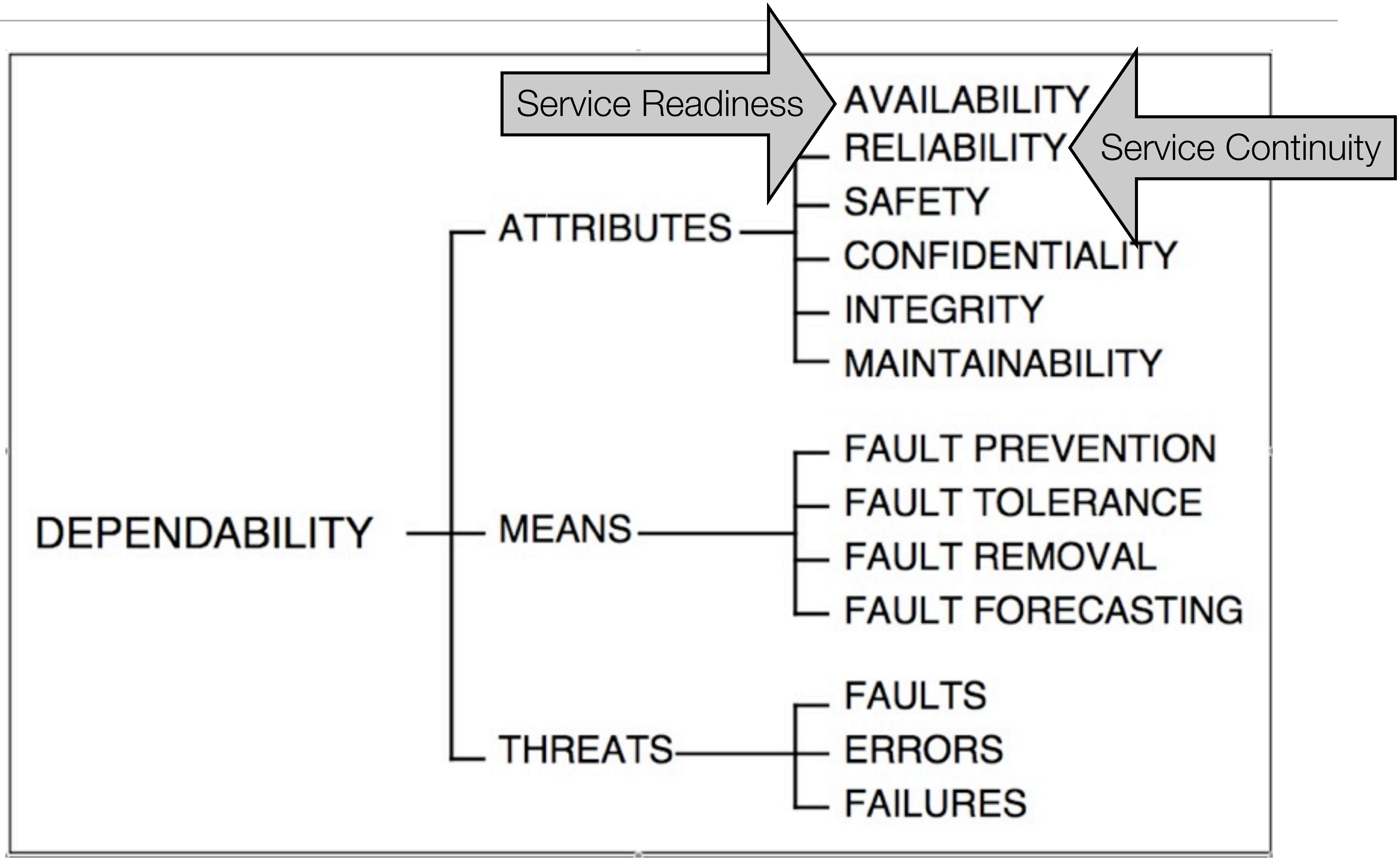
Dr. Peter Tröger

Sources:

J.C. Laprie. Dependability: Basic Concepts and Terminology

Eusgeld, Irene et al.: Dependability Metrics. 4909. Springer Publishing, 2008

Dependability Tree (Laprie)



Attributes of Dependability

- **Reliability** - Continuity of service
  - Initial goal for computer system trustworthiness
  - *„Reliability is not doing the wrong thing.“* [Gray85]
  - *„Reliability: Ability of a system or component to perform its required functions under stated conditions for a specified period of time*“ [IEEE]
- **Availability** - Readiness for usage
  - *„Availability is doing the right thing within the specified response time.“*
- Availability is always required - but maybe to a different degree
- Reliability, safety, and security - may or may not be required

In Detail

- **Reliability** - Function *R(t)*
  - Probability that a system is functioning properly and constantly over time period t
    - Assumes that system was fully operational at t=0
    - Denotes failure-free interval of operation
- **Availability** - Fraction of / points in time were a system is operational
  - Describe system behavior in presence of fault tolerance
  - **Instantaneous availability** - Probability that a system is performing correctly at time t, equal to reliability of non-repairable systems: $A(t) = R(t)$
  - **Steady-state availability** - Probability that a system will be operational at any random point of time, expressed as the fraction of time a system is operational during its expected lifetime: $A_S(t) = Uptime / Lifetime$

PDF & CDF

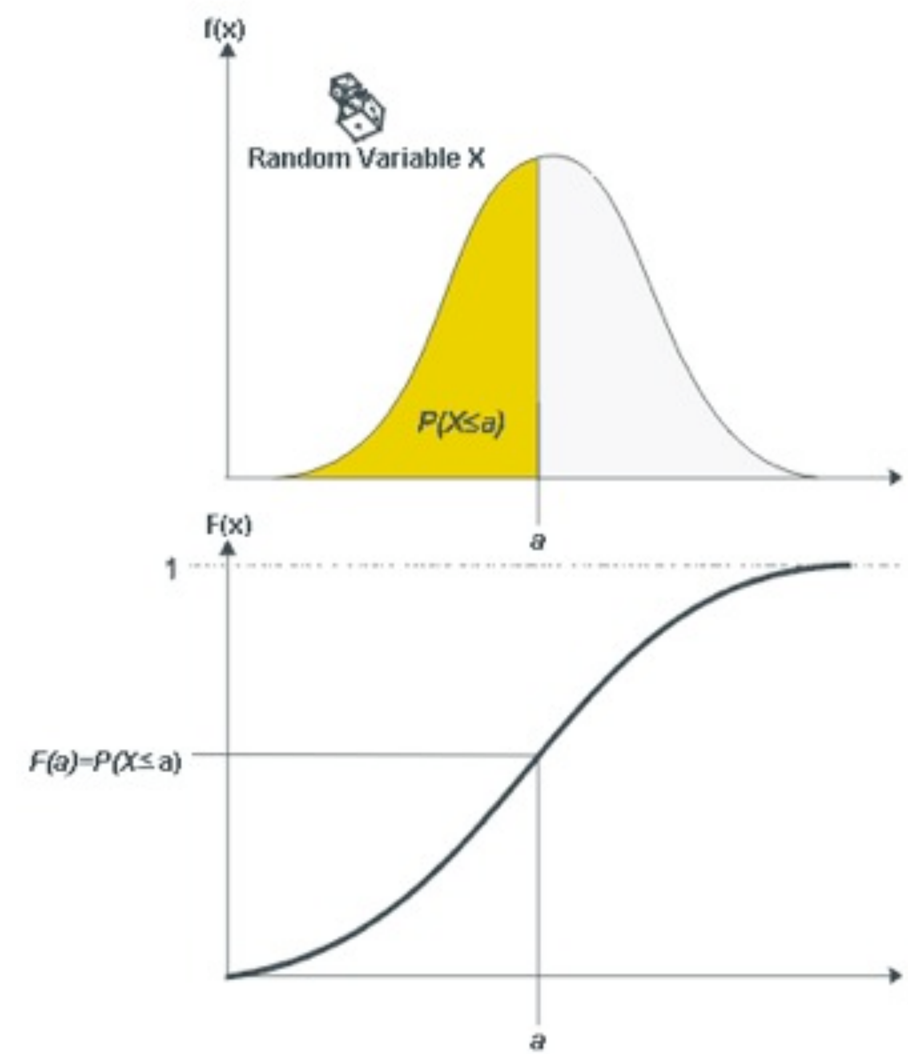
- Probability density function *pdf* for random variable *X*
  - Discrete variable: Probability that *X* will be *x*
  - Continuous variable: Probability that *X* is in *[a, b]*
    - Computed as area under the density function in this range

$$P(a \le X \le b) = \int_a^b f(x)dx \text{ and } f(x) \ge 0 \text{ for all } x$$

- Cumulative distribution function *cdf(x)*: Probability that the value of X is at most x

$$F(x) = P(X \le x) = \int_{0,-\infty}^{x} f(s)ds$$

  - Limits of integration depend on the nature of the distribution function



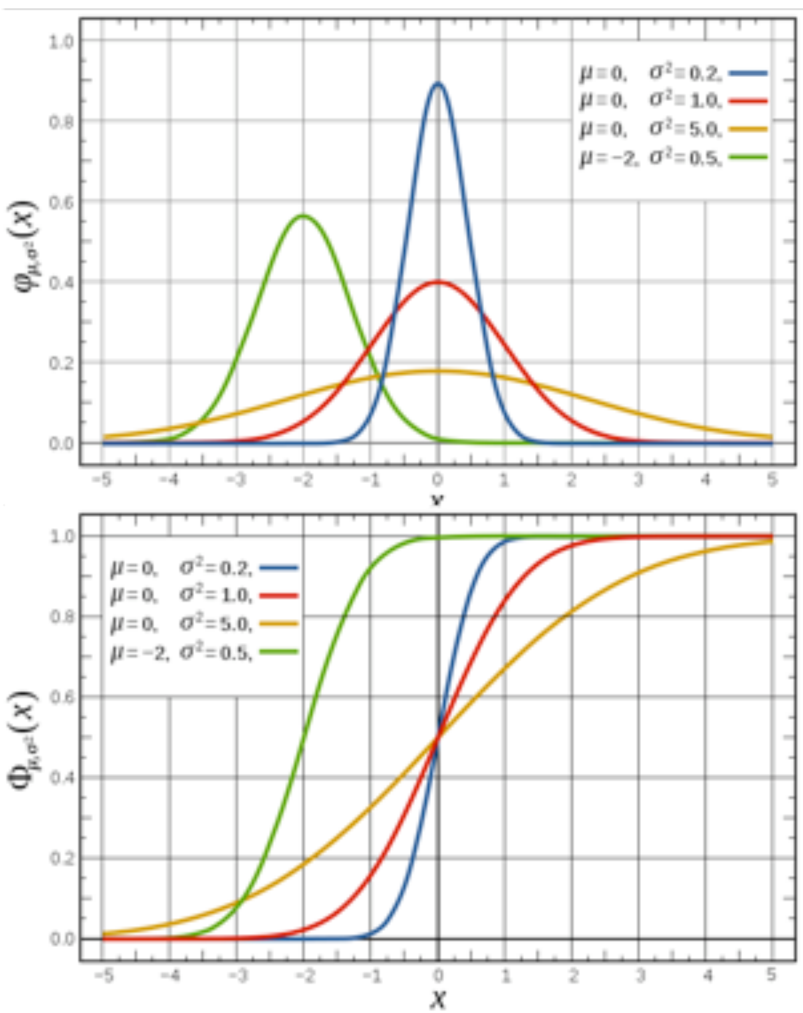
(C) weibull.com

- Value of the *cdf* at *x* is always area under the *pdf* up to *x*

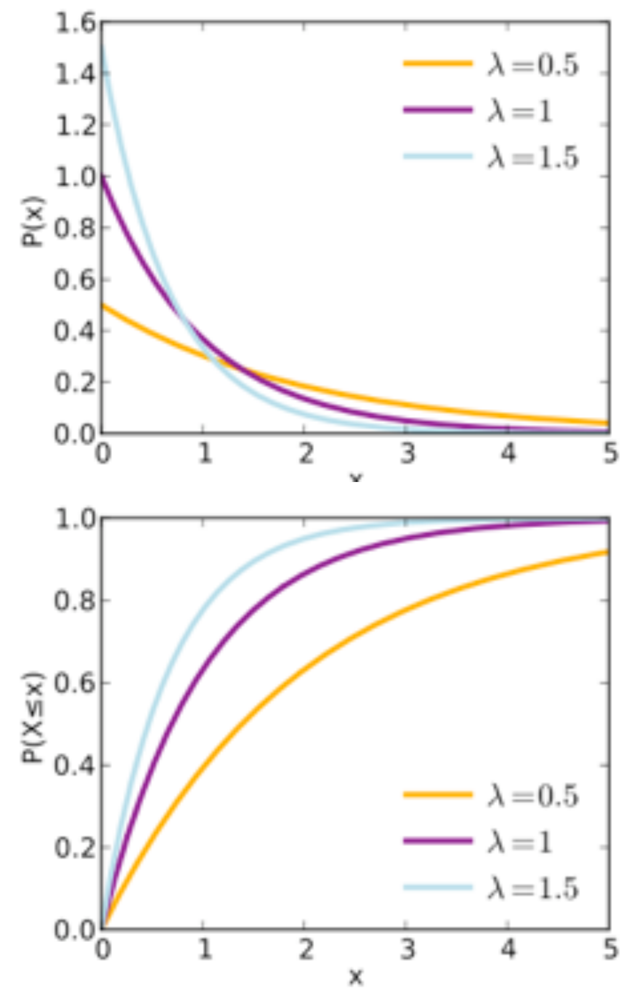
PDF Examples

- Different popular statistical distributions, each describing a random variable behavior
- Parameters of the distribution derived from data, complete description then by *pdf*

Normal distribution
(mean, variance)



Exponential distribution
(rate parameter)

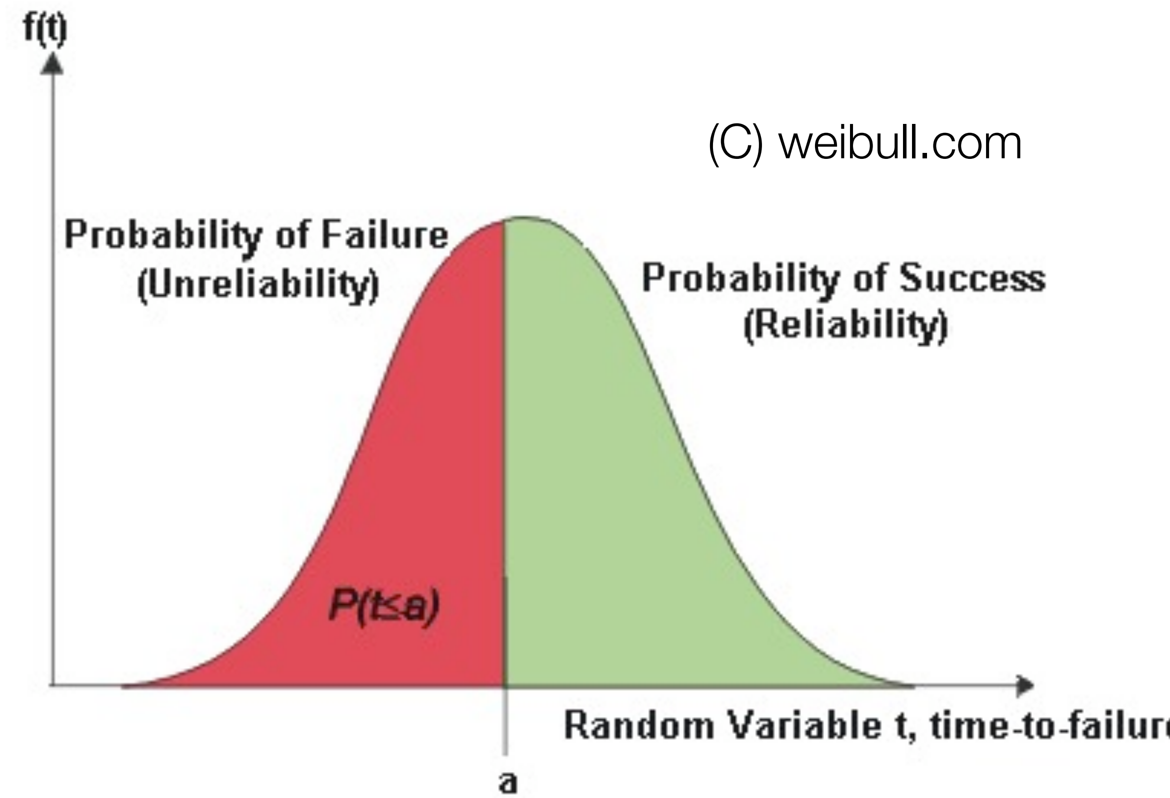


Probability density function

Cumulative distribution function

The Reliability Function R(t)

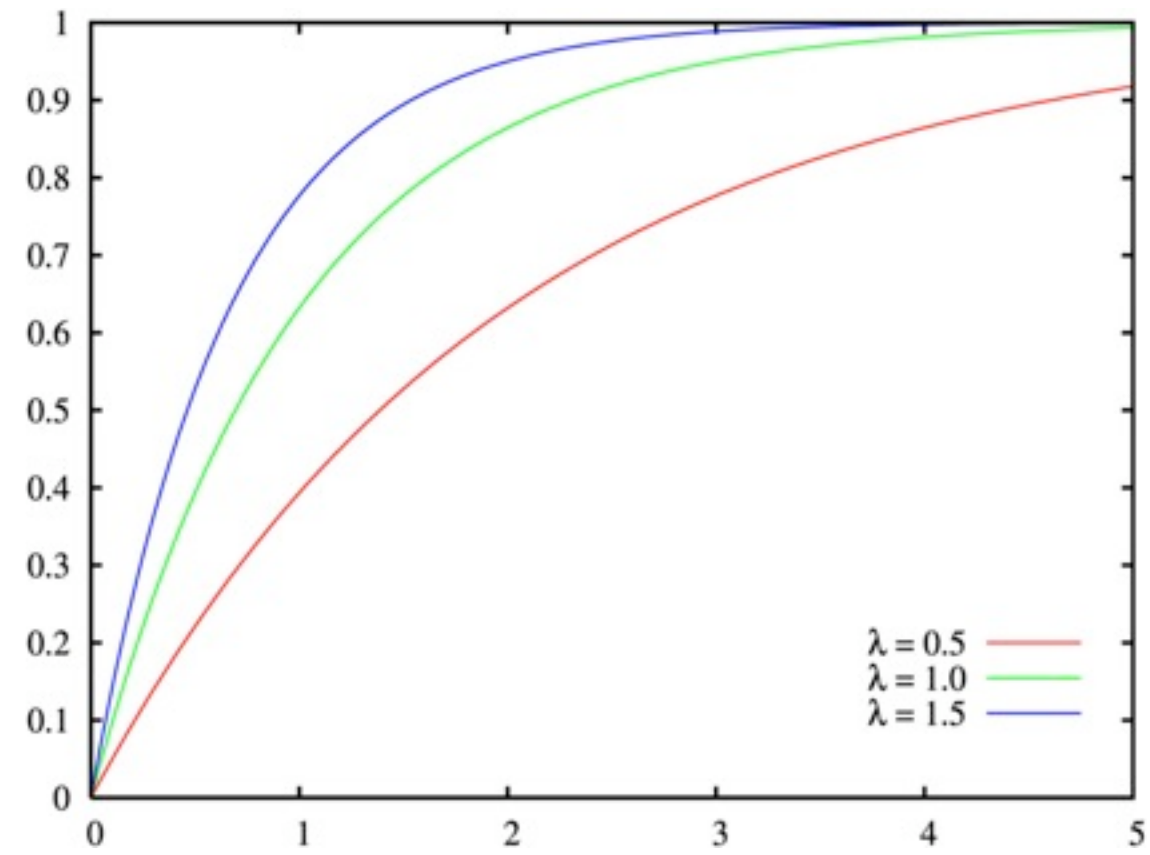
- Reliability: Probability *R(t)* that a component works for time period [0,*t*]
  - Failure probability *F(t)=1-R(t)*
- Idea: Take continuos random variable *X* over time, representing time-to-failure
  - *cdf(t)=F(t)* describes probability of failure before t -> **Unreliability Function**
  - *R(t)=1-cdf(t)* describes probability of a failure after t -> **Reliability Function**
- Typically, the exponential distribution is used
  - Distribution is again exponential if some time *t* has elapsed (memoryless property)
-



Exponential Distribution of Time-To-Failure

- Events occur continuously and independently at a constant average rate (Poisson process)
- Increasing probability of failure with increasing t
- Failure rate Lambda from experience or complexity measures
- Cumulative distribution function:

$$F(x;\lambda) = \begin{cases} 1 - e^{-\lambda x}, & x \geq 0, \\ 0, & x < 0. \end{cases}$$



cdf

- Reliability function for exponential failure distribution, derived from cdf:

$$R(t) = P(X > t) = 1 - F(t) = e^{-\lambda x} \text{ with } F(x) = 1 - e^{-\lambda x}$$

Failure Rate

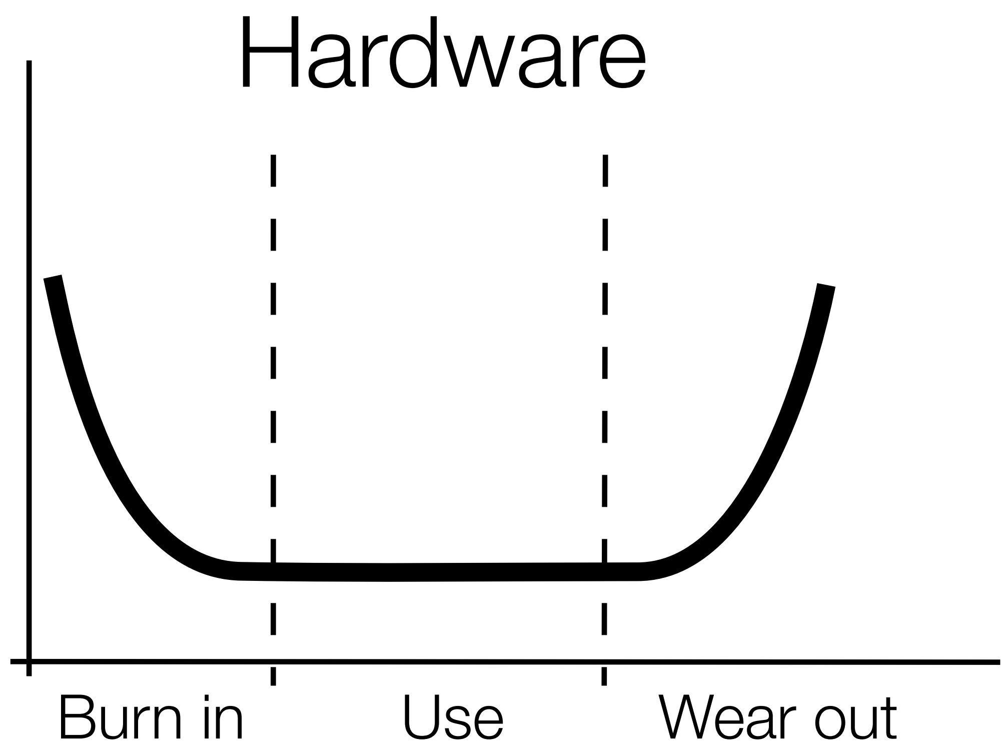
- Treat pdf for time-to-failure random variable X as **failure density function**
  - Can be computed as derivative of the unreliability function

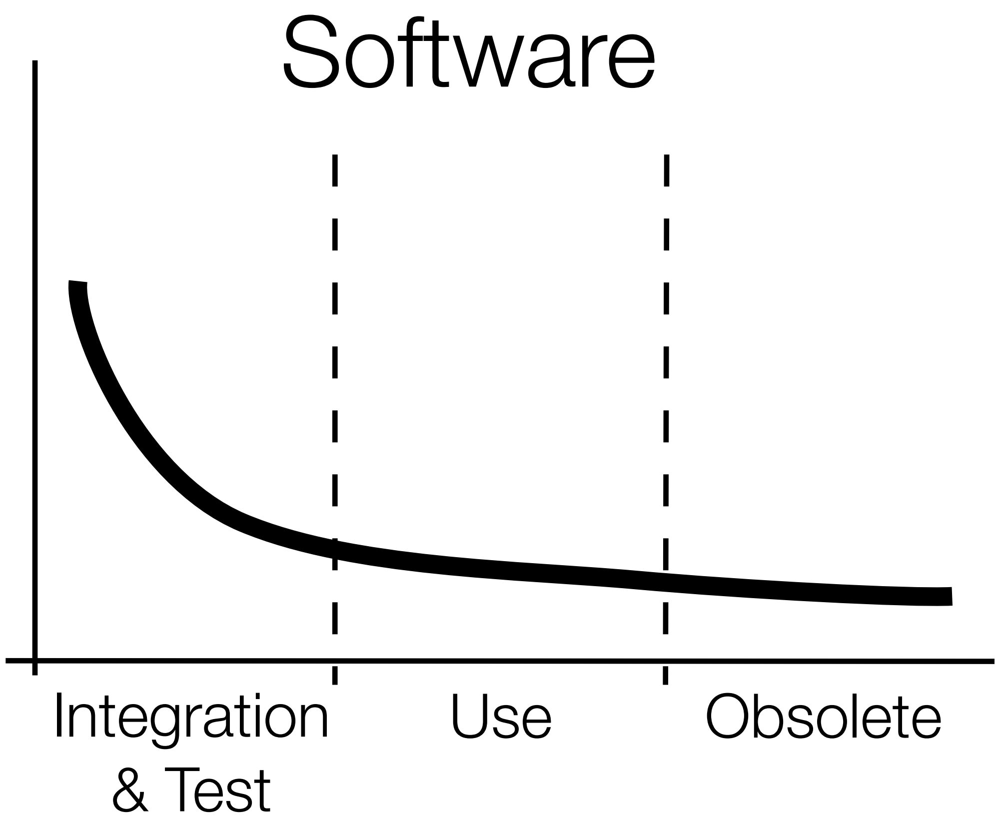
$$f(t) = dF(t)/dt$$

- **Failure rate** / hazard rate function - mean frequency of failures at time t
  - Conditional probability of a failure between a and b, given the survival until t

$$\lambda(t) = \frac{f(t)}{R(t)} = \lambda \text{ for constant failure rate}$$

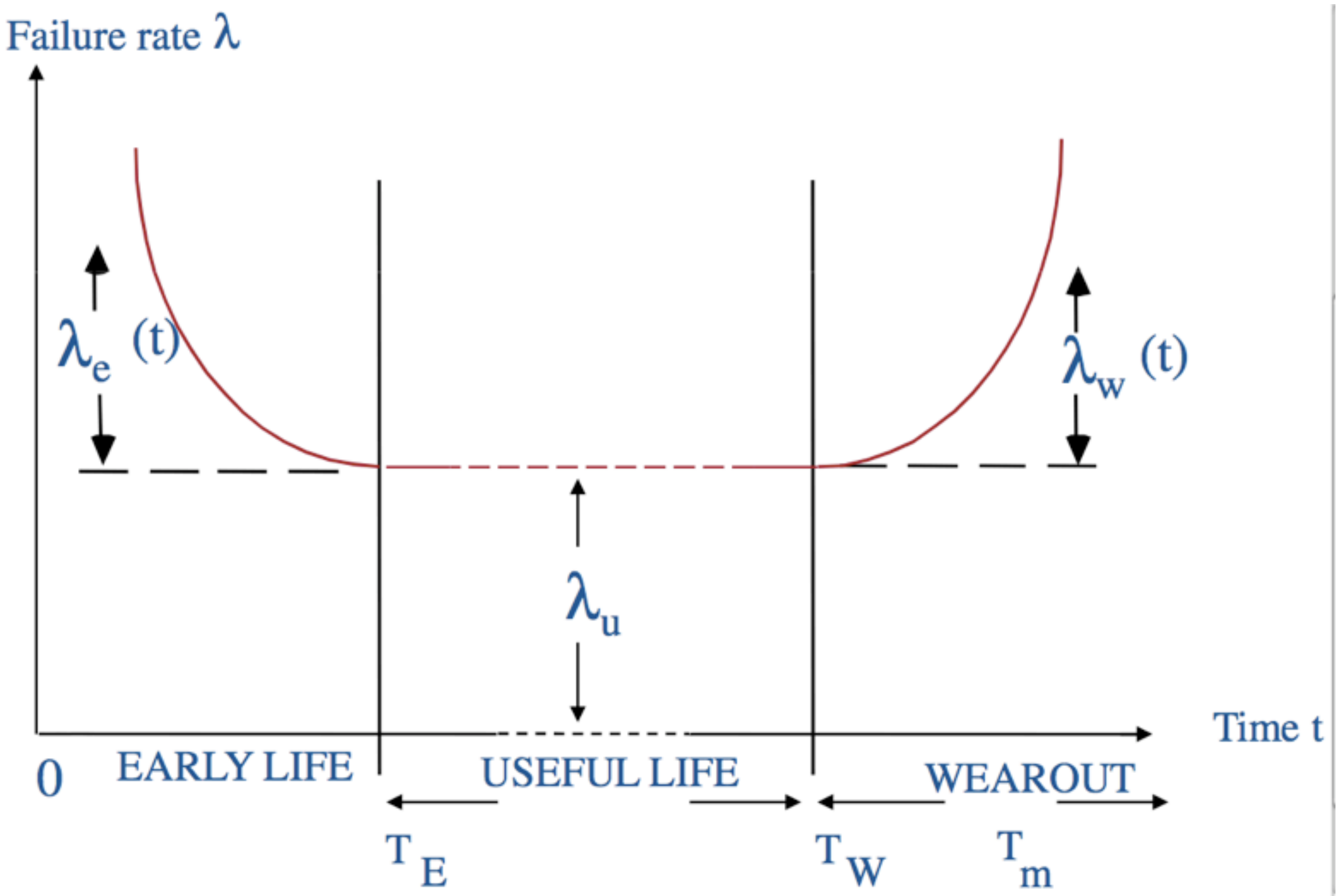
Variable Failure Rate in Real World





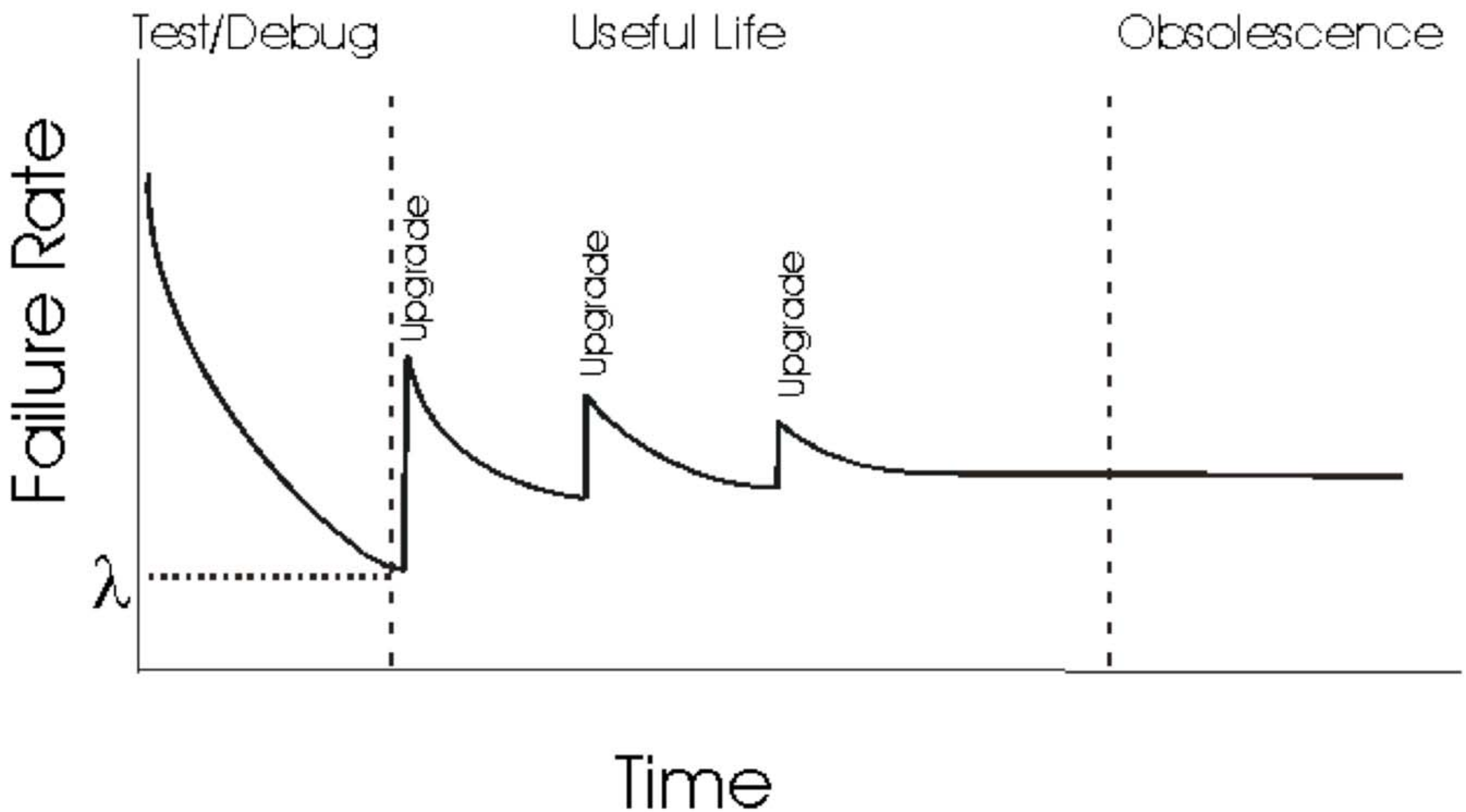
- Failure rate is treated as constant parameter of the exponential distribution
- (maybe invalid) simplification, combined solution:
    - Exponential distribution when failure rate is constant
    - Weibull distribution when failure rate is monotonic decreasing / increasing

Hardware Failure Rate



Software Failure Rate

- Industrial practice
- When do you stop testing ? - No more time, or no more money ...



(C) Malek

Failure Rate Examples

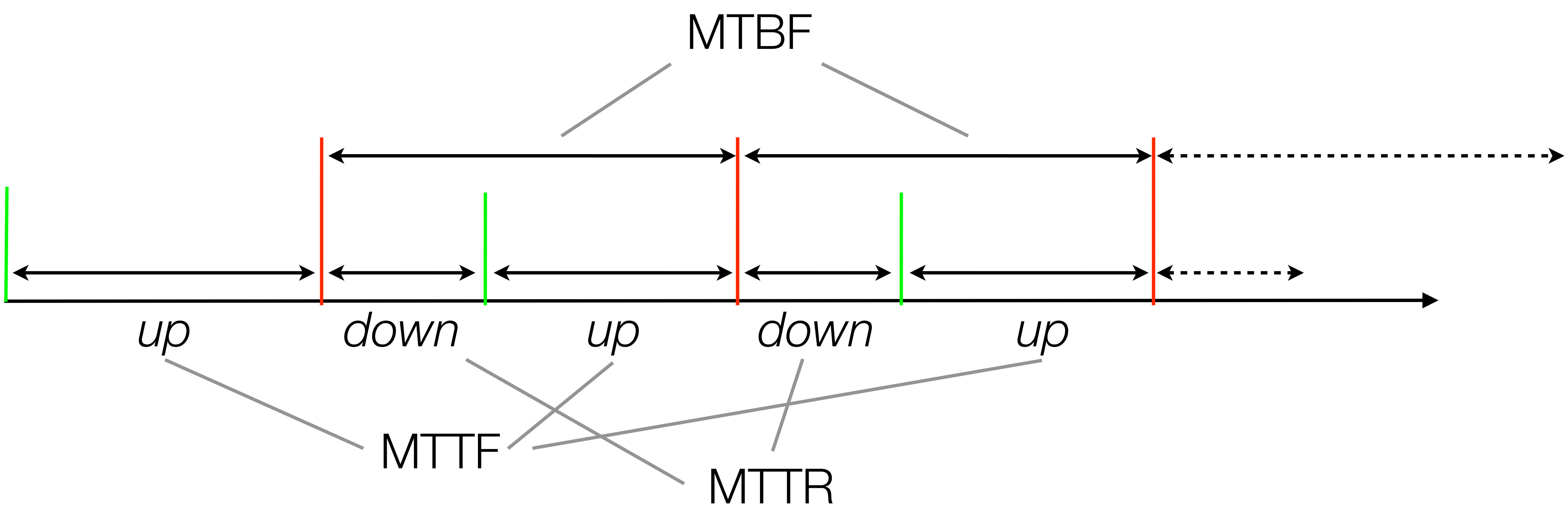
- Standards from experience provide base data for component reliability
- Society of Automotive Engineers (SAE) reliability model

$$\lambda_p = \lambda_b \Pi_{i=1}^{b} \pi_i$$

- Predicted failure rate λ_p
- Base failure rate for the component λ_b
- Various modification factors π_i
  - Component composition
  - Ambient temperature
  - Location in the vehicle

Availability

- **Mean time to failure (MTTF)** - Average time it takes for the system to fail
- **Mean time to recover / repair (MTTR)** - Average time it takes to recover
- **Mean time between failures (MTBF)** - Average time between failures



$$MTTF = \frac{1}{\lambda}$$

Steady-State Availability

$$A = \frac{Uptime}{Uptime + Downtime} = \frac{MTTF}{MTTF + MTTR}$$

Availability	Downtime per year	Downtime per week
90.0 % (1 nine)	36.5 days	16.8 hours
99.0 % (2 nines)	3.65 days	1.68 hours
99.9 % (3 nines)	8.76 hours	10.1 min
99.99 % (4 nines)	52.6 min	1.01 min
99.999 % (5 nines)	5.26 min	6.05 s
99.9999 % (6 nines)	31.5 s	0.605 s
99.99999 % (7 nines)	0.3 s	6 ms

Attributes of Dependability

- **Safety** - Avoidance of catastrophic consequences on the environment
  - Critical applications
  - Specification needs to describe things that should not happen
- **Security** - Prevention of unauthorized access and / or information handling
  - Became relevant with distributed systems
- **Confidentiality** - Absence of unauthorized disclosure of information
- **Integrity** - Absence of improper system alteration
  - With respect to either accidental or intentional faults
- **Maintainability** - Ability to undergo modifications and repairs