Dependability Evaluation

Industrial Automation

Dr. Jean-Charles TOURNIER

Spring 2025

The material of this course has been initially created by Prof. Dr. H. Kirrmann and adapted by Dr. J-C. Tournier.

Schedule

- 1: Overview Dependable Systems
  - Definitions: Reliability, Safety, Availability etc.,
  - Failure modes in computers
- 2: Dependability Analysis
  - Combinatorial analysis
  - Markov models
- 3: Dependable Architectures
  - Fault detection
  - Redundant Hardware, Recovery
- 4: Dependable Software
  - Fault Detection,
  - Recovery Blocks, Diversity
- 5: Safety analysis
  - Qualitative Evaluation (FMEA, FTA)
  - Examples

06-May-2025

Dependability Evaluation

- This part of the course applies to any system that may fail.
- Dependability evaluation (*fiabilité prévisionnelle*, Verlässlichkeitsabschätzung) determines:
  - the expected reliability,
  - the requirements on component reliability,
  - the repair and maintenance intervals and
  - the amount of necessary redundancy.
- Dependability analysis is the base on which risks are taken and contracts established
- Dependability evaluation must be part of the design process, it is quite useless once a system has been put into service.

Agenda

- Reliability definitions
- Reliability of series and parallel systems without repair
- Considering repair
- Markov models
- Availability evaluation
- Examples

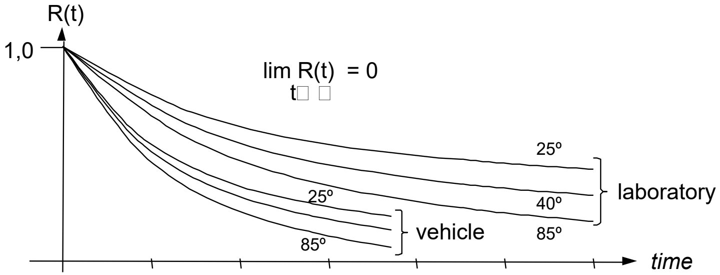
Reliability Definitions

Reliability

- Reliability = probability that a mission is executed successfully
  - definition of success? a question of satisfaction…

- Reliability depends on:
  - duration
  - environment: temperature, vibrations, radiations, etc...

- Such graphics are obtained by observing a large number of systems,
  or calculated for a system knowing the expected behaviour of the elements

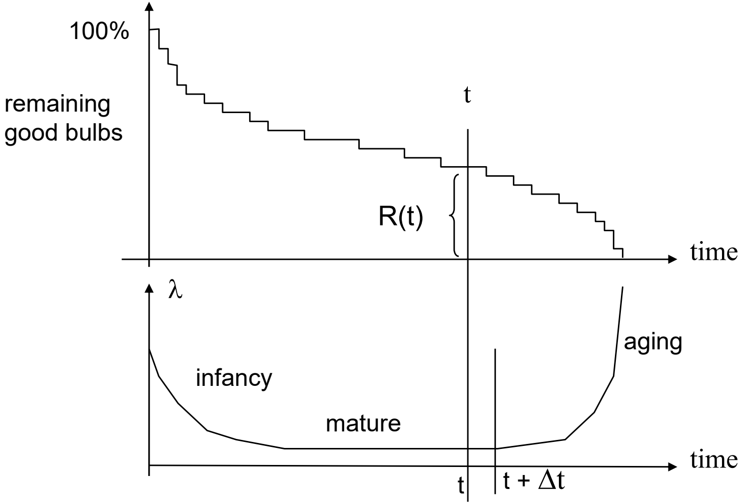


Reliability and Failure Rate Experimental View

- Experiment: large quantity of light bulbs

- Reliability $\boldsymbol{R(t)}$:
  - number of good bulbs remaining at time t divided by initial number of bulbs

- Failure rate $\boldsymbol{\lambda(t)}$:
  - number of bulbs that failed in interval $[\mathrm{t}; t + \Delta\mathrm{t}]$ divided by number of remaining bulbs

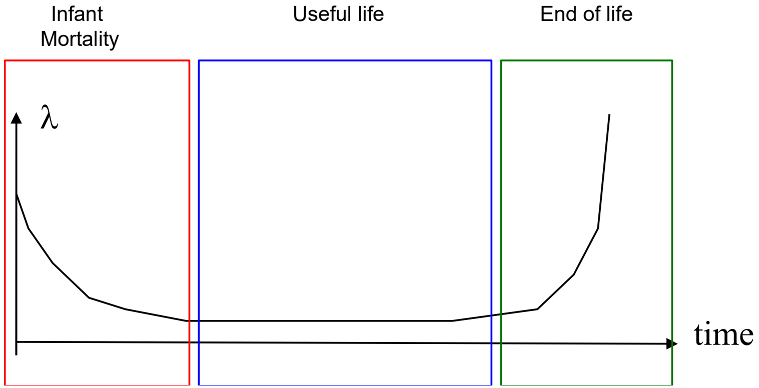


Failure Rate
Bathtub Curve

- Empirical studies showed that the evolution of the failure rate over time usually follows a *bathtub* curve.

- A typical bathtub curve comprises three phases:
  - Infant mortality
    - Failure rate is decreasing
  - Useful life
    - Failure rate is constant
  - End of life
    - Failure rate is increasing

- *Reminder*: a bathtub curve does not depict the failure rate of a single item, but describes the relative failure rate of an entire population of products over time



Hardware Failure

- Hardware failures during a products life can be attributed to the following causes:

- Design failures:
  - This class of failures take place due to inherent design flaws in the system. In a well-designed system this class of failures should make a very small contribution to the total number of failures.
- Infant Mortality:
  - This class of failures cause newly manufactured hardware to fail. This type of failures can be attributed to manufacturing problems like poor soldering, leaking capacitor etc. These failures should not be present in systems leaving the factory as these faults will show up in factory system burn in tests.

- Random Failures:
  - Random failures can occur during the entire life of a hardware module. These failures can lead to system failures. Redundancy is provided to recover from this class of failures.

- Wear Out:
  - Once a hardware module has reached the end of its useful life, degradation of component characteristics will cause hardware modules to fail. This type of faults can be weeded out by preventive maintenance and routing of hardware.

Infant Mortality

- For critical system, infant mortality is unacceptable
  - Stress test and burn-in tests should be implemented
  - Stress tests are used to identify failure root cause (design, process, material)
  - Burn-in tests are used to identify failure for which root cause can not be found
  - Both tests are similar, but one is implemented before a massive production (stress test), while the other one is implemented on the product leaving the factory (burn-in)

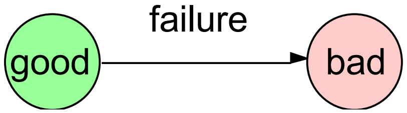
- Stress testing
  - Should be started at the earliest development phases and used to evaluate design weaknesses and uncover specific assembly and materials problems.
  - The failures should be investigated and design improvements should be made to improve product robustness. Such an approach can help to eliminate design and material defects that would otherwise show up with product failures in the field.
  - Parameters: temperature, humidity, vibrations, etc.

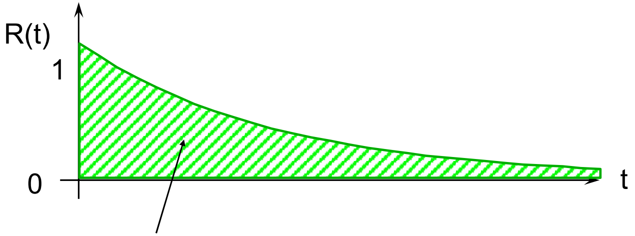
- Burn-in tests
  - Ensure that a device or system functions properly before it leaves the manufacturing plant
  - For example, running a new computer for several days before committing it to its real intent
  - For ships or craft, and in general for complete system, burn-in tests are called shakedown tests

Dr. Jean-Charles Tournier

R(t), $\lambda(t)$ Definitions

- Reliability R(t): probability that a system does not enter a terminal state until time t, while it was initially in a good state at time t=0
  - $R(0) = 1$
  - $\lim_{t\to\infty} R(t) = 0$
- Failure rate $\boldsymbol{\lambda(t)}$
  - Probability that a (still good) element fails during the next time unit Δt
- Definition
  - $\lambda(t) = -\frac{dR(t)/dt}{R(t)}$
  - $R(t) = e^{-\int_0^t \lambda(x)\,dx}$
  - $\boldsymbol{MTTF = \int_0^\infty R(t)dt}$



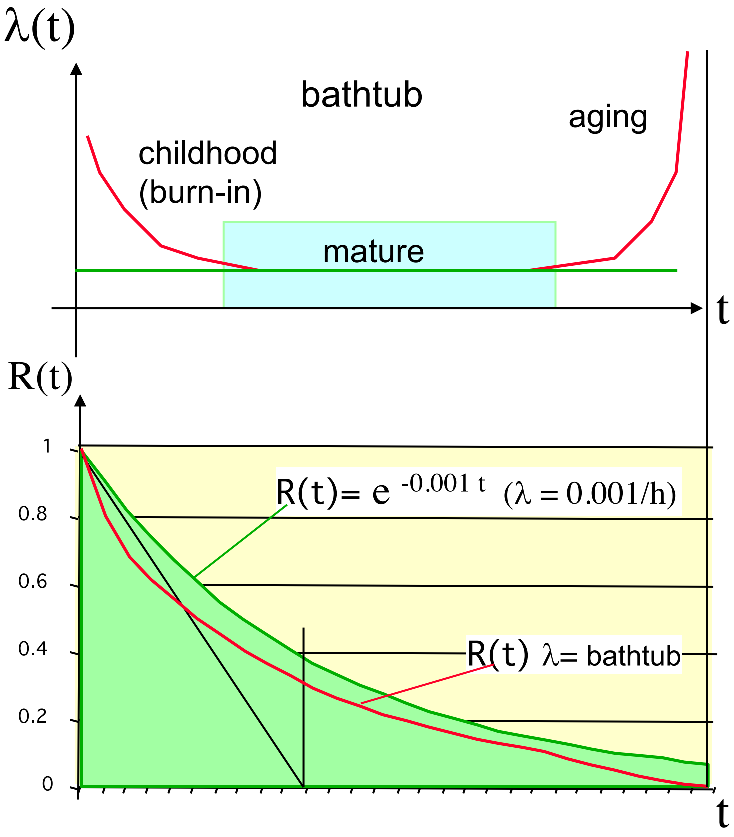


MTTF = mean time to fail = surface below R(t)

INDUSTRIAL AUTOMATION

Constant failure rate

- Reliability = probability of not having failed until time t expressed:
  - Discrete expression
    - $R(t+\Delta t) = R(t) - R(t).\lambda(t).\Delta t$
  - Continuous expression simplified when $\lambda(t) = \lambda$
    - $\boxed{\boldsymbol{R(t) = e^{-\lambda t}}}$
- Assumption of constant λ is justified by
  - Experience
  - Stress and burn-in tests
  - Maintenance
- It greatly simplifies the computation without loosing too much information
- MTTF is the surface below $R(t)$ (integral of $R(t)$)
  - $\boxed{\boldsymbol{MTTF = \int_0^{\infty} e^{-\lambda t} dt = \frac{1}{\lambda}}}$



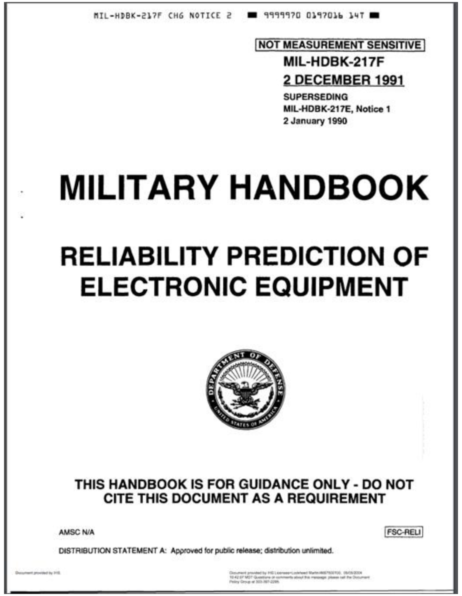
Examples of failure rates

Element	Rating	failure rate
resistor	0.25 W	0.1 fit
capacitor	(dry) 100 nF	0.5 fit
capacitor	(elect.) 100 ∝F	10 fit
processor	486	500 fit
RAM	4MB	1 fit
Flash	4MB	12 fit
FPGA	5000 gates	80 fit
PLC	compact	6500 fit
digital I/O	32 points	2000 fit
analog I/O	8 points	1000 fit
battery	per element	400 fit
VLSI	per package	100 fit
soldering	per point	0.01 fit

- To avoid the negative exponentials, λ values are often given in FIT (Failures in Time)
  - $1\ \text{FIT} = 10^{-9}.\,h^{-1} = \frac{1}{114000\ \text{year}}$
  - FIT reports the number of expected failures per one billion hours of operation for a device
- This term is used particularly in the semiconductor industry
- These figures can be obtained from catalogues such as MIL Standard 217F or from the manufacturer’s data sheets
- Warning: Design failures outweigh hardware failures for small series
- E.g. PLC = 6500 FIT, i.e. 0.05 failures/year
  - Installation with hundreds of PLC can expect several failures per year

MIL HDBK 217

- MIL Handbook 217B lists failure rates of common elements.
- Failure rates depend strongly on the environment: temperature, vibration, humidity, and especially the location:
  - Ground benign, fixed, mobile
  - Naval sheltered, unsheltered
  - Airborne, Inhabited, Uninhabited, cargo, fighter
  - Airborne, Rotary, Helicopter
  - Space, Flight
- Usually the application of MIL HDBK 217 results in pessimistic results in terms of the overall system reliability (computed reliability is lower than actual reliability).
- To obtain more realistic estimations it is necessary to collect failure data based on the actual application instead of using the generic values from MIL HDBK 217.



MIL-HDBK-217F CHG NOTICE 2 ■ 9999970 0197016 14T ■

NOT MEASUREMENT SENSITIVE

MIL-HDBK-217F

2 DECEMBER 1991

SUPERSEDING
MIL-HDBK-217E, Notice 1
2 January 1990

MILITARY HANDBOOK

RELIABILITY PREDICTION OF ELECTRONIC EQUIPMENT

THIS HANDBOOK IS FOR GUIDANCE ONLY - DO NOT CITE THIS DOCUMENT AS A REQUIREMENT

AMSC N/A

FSC-RELI

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited.

Document provided by IHS

Document provided by IHS Licensee=Lockheed Martin/[illegible], [illegible]
[illegible] Questions or comments about this message: please call the Document
Policy Group at [illegible]

Failure rate catalogue MIL HDBK 217

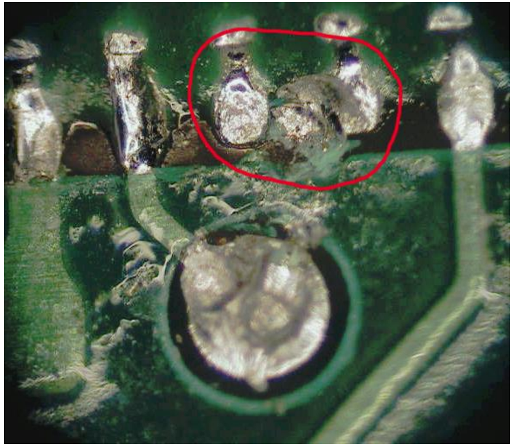
- Stress is expressed by lambda factors

- Basic models:
  - discrete components (e.g. resistor, transistor etc.)
    $\lambda = \lambda_b \, p_E \, p_Q \, p_A$
  - integrated components (ICs, e.g. microprocessors etc.)
    $\lambda = p_Q \, p_L \, (C_1 \, p_T \, p_V + C_2 \, p_E)$

- MIL handbook gives curves/rules for different element types to compute factors,
  - λ_b based on ambient temperature Q_A and electrical stress S
  - p_E based on environmental conditions
  - p_Q based on production quality and burn-in period
  - p_A based on component characteristics and usage in application
  - C_1 based on the complexity
  - C_2 based on the number of pins and the type of packaging
  - p_T based on chip temperature Q_J and technology
  - p_V based on voltage stress

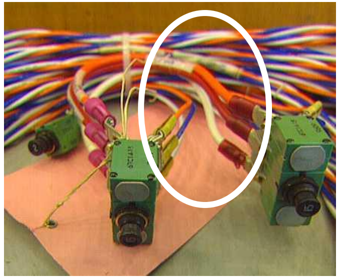
- Example: λ_b usually grows exponentially with temperature Θ_A (Arrhenius law)

What can go wrong?

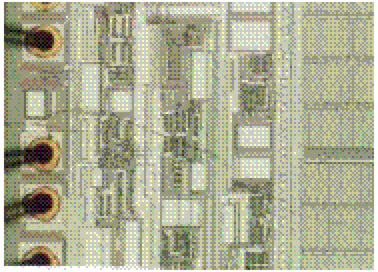


poor soldering (manufacturing)…

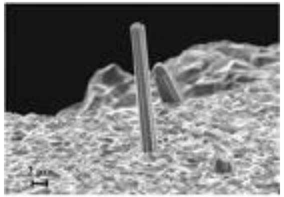
broken wire… (vibrations)



broken isolation (assembly…)



chip cracking
(thermal stress…)



tin whiskers
(lead-free soldering)

Failures that affect logic circuits

- Thermal stress (different dilatation coefficients, contact creeping)
- Electrical stress (electromagnetic fields)
- Radiation stress (high-energy particles, cosmic rays in the high atmosphere)

- Errors that are transient in nature (called “soft-errors”) can be latched in memory and become firm errors. “Solid errors” will not disappear at restart.

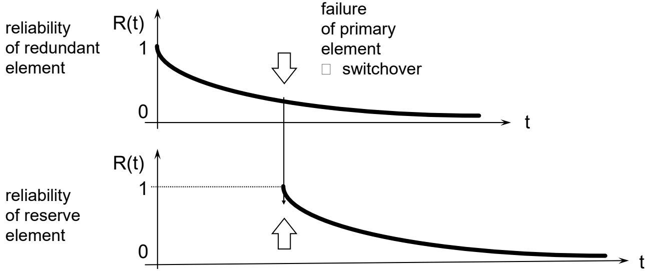
- e.g. FPGA with 3 M gates, exposed to 9.3 10^8 neutrons/cm^2 exhibited 320 FIT at sea level and 150’000 FIT at 20 km altitude

  see: http://www.actel.com/products/rescenter/ser/index.html

- Things are getting worse with smaller integrated circuit geometries !

Cold, Warm and Hot redundancy

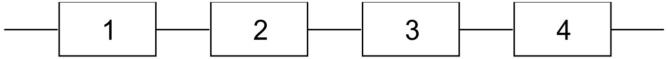
- **Hot redundancy**
  - the reserve element is fully operational and under stress, it has the **same failure rate** as the operating element.
- **Warm redundancy**
  - the reserve element can take over in a short time, it is not operational and has a **smaller failure rate**.
- **Cold redundancy** (cold standby)
  - the reserve is switched off and has **zero failure rate**



Reliability of series and parallel systems

Reliability of a system or unreliable elements

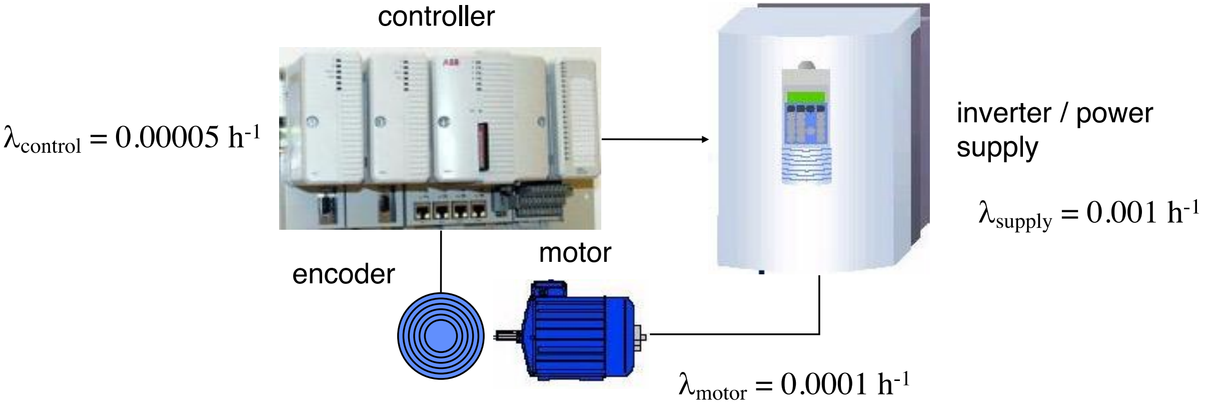
- The reliability of a system consisting of n elements, each of which is necessary for the function of the system, whereby the elements fail independently is:
  - $R_{total}(t) = R_1(t)\,.\,R_2(t)\,\ldots\,R_n(t) = \prod_{i=1}^{n} R_i(t)$



- Assuming a constant failure rate λ allows to compute easily the failure rate of a system by summing the failure rates of individual components
  - $R_{NooN}(t) = e^{-\sum_{i=0}^{n} \lambda_i . t}$

- This is the base for the calculation of the failure rate of systems (MIL-STD-217F)

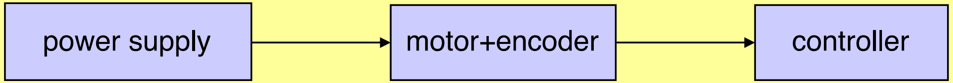
Example



$\lambda_{control} = 0.00005\ h^{-1}$

$\lambda_{supply} = 0.001\ h^{-1}$

$\lambda_{motor} = 0.0001\ h^{-1}$



$R_{tot} = R_{supply} * R_{motor} * R_{control}$

$$= e^{-\lambda_{supply} t} * e^{-\lambda_{motor} t} * e^{-\lambda_{control} t} = e^{-(\lambda_{supply} + \lambda_{motor} + \lambda_{control}) t}$$

$$\lambda_{total} = \lambda_{supply} + \lambda_{motor} + \lambda_{control} = 0.00115\ h^{-1}$$

Warning: This calculation does not apply any more for redundant system !

Exercise
Reliability Estimation

- An electronic circuit consists of the following elements:

1 processor	MTTF= 600 years	48 pins
30 resistors	MTTF= 100’000 years	2 pins/resistor
6 plastic capacitors	MTTF= 50’000 years	2 pins/capacitor
1 FPGA	MTTF= 300 years	24 pins
2 tantalum capacitors	MTTF= 10’000 years	2 pins
1 quartz	MTTF= 20’000 years	2 pins
1 connector	MTTF= 5000 years	16 pins

- the MTTF of one solder point (pin) is 200’000 years

- What is the expected Mean Time To Fail of this system ?

- Repair of this circuit takes 10 hours, replacing it by a spare takes 1 hour.
- What is the availability in both cases ?

- The machine where it is used costs 100 € per hour, 24 hours/24 production, 30 years installation lifetime. What should the price of the spare be ?

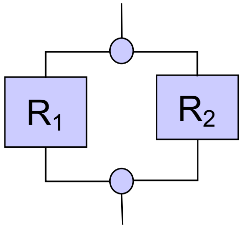
Exercise
MTTF calculation

- An embedded controller consists of:
  - one microprocessor 486
  - 2 x 4 MB RAM
  - 1 x Flash EPROM
  - 50 dry capacitors
  - 5 electrolytic capacitors
  - 200 resistors
  - 1000 soldering points
  - 1 battery for the real-time-clock

- what is the MTTF of the controller and what is its weakest point ?
  - (use the numbers given in slide #12)

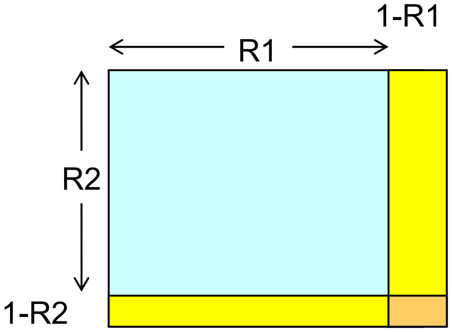
Redundant, parallel system 1-out-of-2 with no repair
Combinatorial approach

simple redundant system:
the system is good if any (or both) are good



R_1	ok		ok	
R_2	ok	ok		

$$R_{1oo2} = \overbrace{R_1R_2}^{R_1 \text{ good},\ R_2 \text{ good}} + \overbrace{R_1\,(1-R_2)}^{R_1 \text{ good},\ R_2 \text{ down}} + \overbrace{(1-R_1)\,R_2}^{R_1 \text{ down},\ R_2 \text{ good}}$$



$$R_{1oo2} = 1 - (1-R_2)(1-R_1)$$

with $R_1 = R_2 = R$:

$$R_{1oo2} = 2\,R - R^2$$

with $R = e^{-\lambda t}$

$$R_{1oo2} = 2\,e^{-\lambda t} - e^{-2\lambda t}$$

Combinatorial
R1oo2, no repair

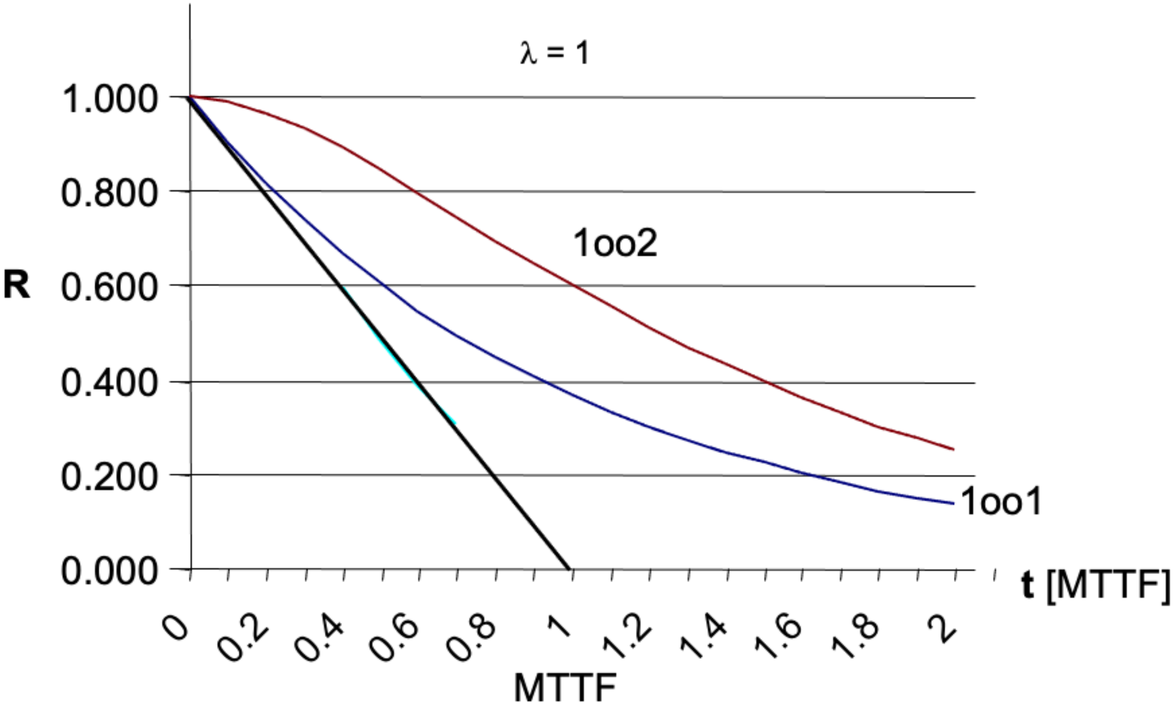
- Example R_{1oo2}: airplane with two motors
  - MTTF of one motor = **1000 hours** (this value is rather pessimistic)
  - Flight duration, t = **2 hours**

  - what is the probability that both motors did not fail until time t (landing)?
  - what is the probability that one of the two motor fails ?
  - What is the probability that at least one of the motor still works until time t?

Combinatorial R1oo2, no repair

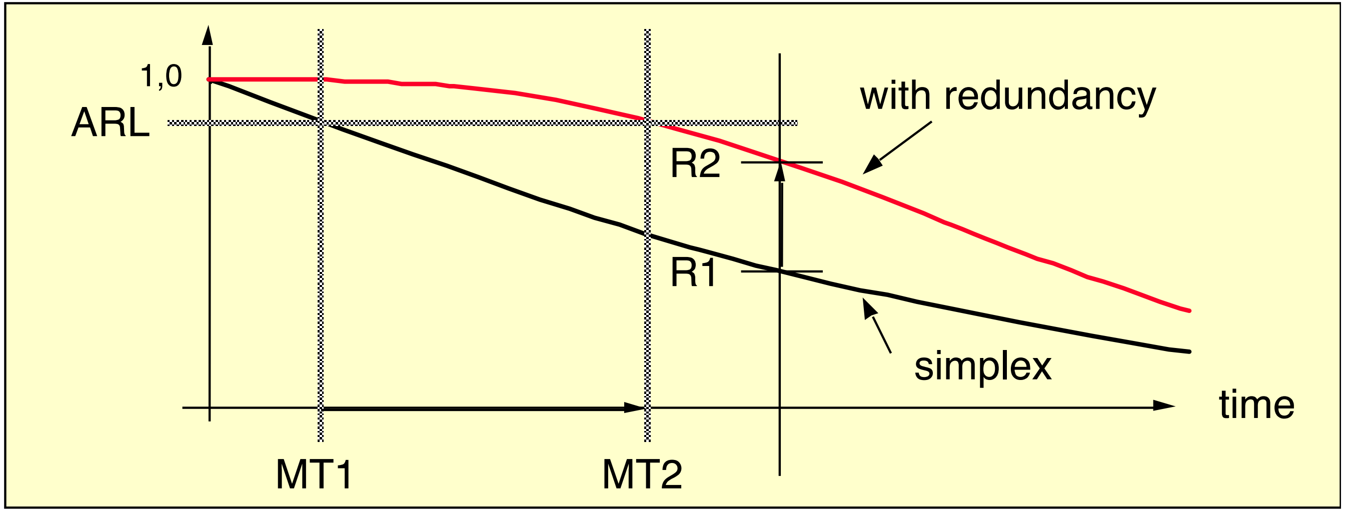
- Example R_{1oo2}: airplane with two motors
  - MTTF of one motor = **1000 hours** (this value is rather pessimistic)
  - Flight duration, t = **2 hours**
  - what is the probability that one of the two motor fails ?
  - what is the probability that both motors did not fail until time t (landing)?
- One of the two motors fails
  - $Ra(t) = R_1.(1 - R_2) + (1 - R_1).\ R_2$
- Both motors do not fail
  - $Rb(t) = R_1.R_2$
- At least one motor works
  - $R(t) = Ra(t) + Rb(t)$
- Compute the function $R(t)$ with $t = 2$

R(t) for 1oo2 Redundancy



MIF, ARL, RIF of redundant structures

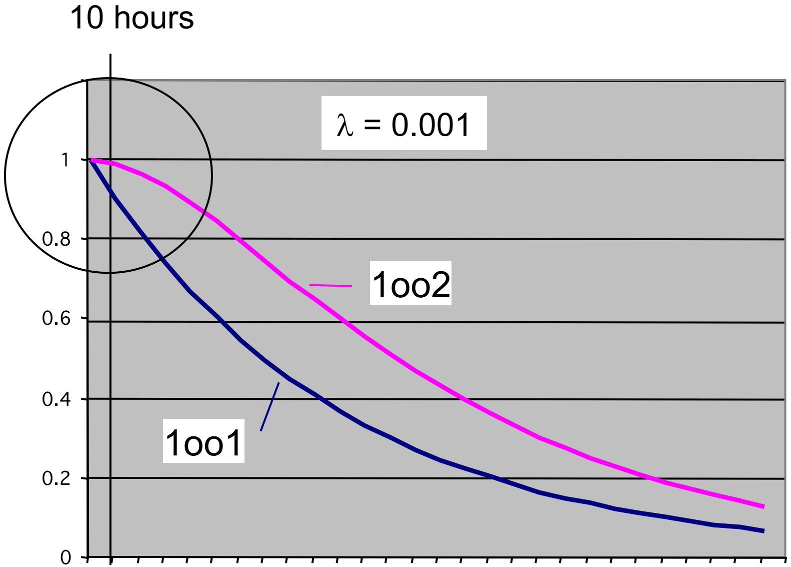
ARL: Acceptable Reliability Level



MIF: Mission Time Improvement Factor (for given ARL)
MIF = MT2/MT1

RIF: Reliability Improvement Factor (at given Mission Time)
RIF = (1-Rwithout) / (1-Rwith) = quotient of unreliability

R1oo2 Reliability Improvement Factor



Reliability improvement factor (RIF)
= $(1-R_{without}) / (1-R_{with})$

RIF for 10 hours mission:
R1oo1 = 0.990; R1oo2 = 0.999901
RIF = 100

but:

$$MTTF_{1oo2} = \int_0^\infty (2\,e^{-\lambda t} - e^{-2\lambda t})\,dt = \frac{3}{2\lambda}$$

no spectacular increase in MTTF !

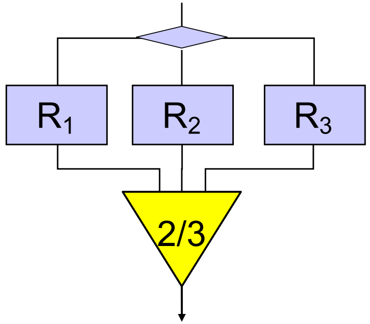
→ 1oo2 without repair is only suited when mission time << $1/\lambda$

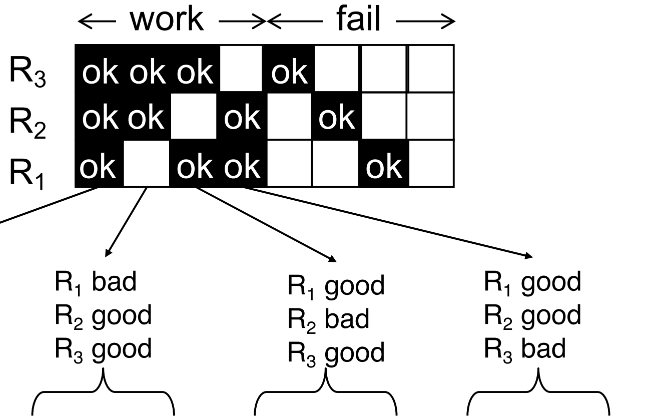
2oo3 No repair – Combinatorial Approach

Dr. Jean-Charles Tournier

E.g. three computers,

majority voting





	work	work	work	work	fail	fail	fail	fail
R_3	ok	ok	ok		ok			
R_2	ok	ok		ok		ok		
R_1	ok		ok	ok			ok	

R_1 good, R_2 good, R_3 good

R_1 bad, R_2 good, R_3 good

R_1 good, R_2 bad, R_3 good

R_1 good, R_2 good, R_3 bad

$$R_{2oo3} = R_1R_2R_3 + (1-R_1)R_2R_3 + R_1(1-R_2)R_3 + R_1R_2(1- R_3)$$

with identical elements: $R_1=R_2=R_3= R$

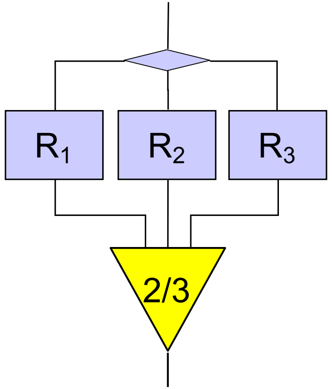
$$R_{2oo3} = 3R^2-2R^3$$

with $R = e^{-\lambda t}$

$$R_{2oo3} = 3\, e^{-2\lambda t} - 2\, e^{-3\lambda t}$$

INDUSTRIAL AUTOMATION

2oo3 No repair – Combinatorial Approach

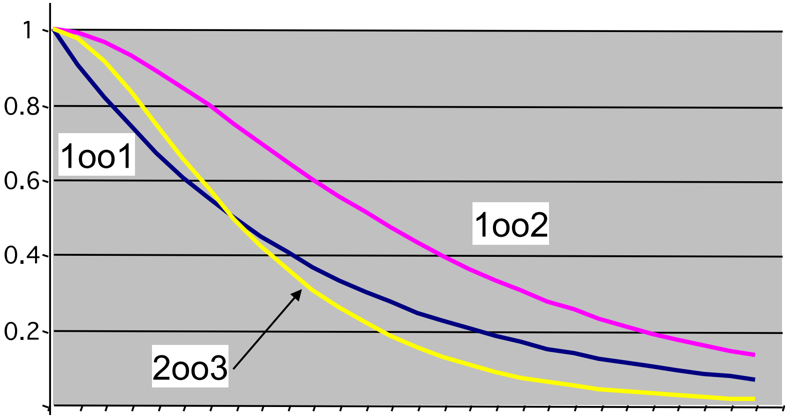


$$R_{2oo3} = 3R^2 - 2R^3 = 3e^{-2\lambda t} - 2e^{-3\lambda t}$$

$$MTTF_{2oo3} = \int_0^\infty (3e^{-2\lambda t} - 2\,e^{-3\lambda t})\,dt = \frac{5}{6\lambda}$$

RIF < 1 when t > 0.7 MTTF !

2003 without repair
is not interesting for long mission



General case
k out of N redundancy

- K-out-of-N computer (KooN)
  - N units perform the function in parallel
  - K fault-free units are necessary to achieve a correct result
  - N – K units are “reserve” units, but can also participate in the function

- Examples
  - aircraft with 8 engines: 6 are needed to accomplish the mission.
  - voting in computers: If the output is obtained by voting among all N units
  - $N \leq 2K - 1$ worst-case assumption: all faulty units fail in same way

Which plane is better?

- 12 motors, 8 of which are sufficient to accomplish the mission
- fly 21 days, MTTF = 5'000 h per motor

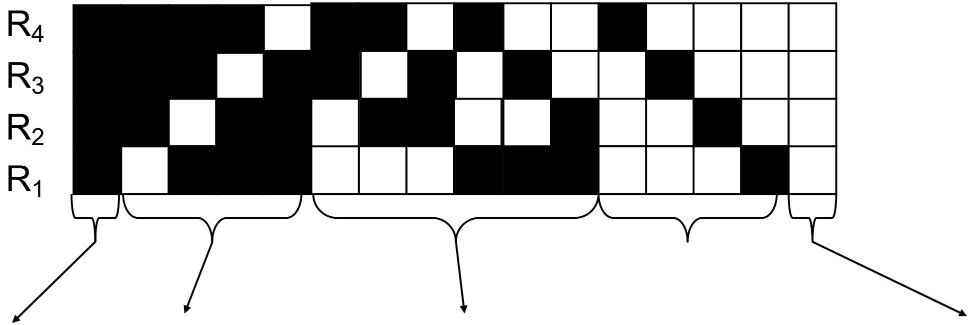
NASA Dryden flight Research Center Photo Collection
http://www.dfrc.nasa.gov/gallery/photo/index.html
NASA Photo: ED03-0152-1 Date: June 7, 2003 Photo By: Carla Thomas

Equipped with an experimental fuel cell system to power the aircraft at night, the solar-electric Helios Prototype is shown during a checkout flight prior to its long-endurance flight demonstration in the summer of 2003.

- 4 motors, three of which are sufficient to accomplish the mission
- fly 21 days, MTTF = 10'000 h per motor

General case
k out of N redundancy

Example with
N = 4



$$R_{KooN} = \overbrace{R^N}^{\text{no fail}} + \overbrace{\binom{N}{1}(1-R)\,R^{N-1}}^{\text{one of N fail}} + \overbrace{\binom{N}{2}(1-R)^2R^{N-2}}^{\text{two of N fail}} + \dots + \overbrace{\binom{N}{K}(1-R)^KR^{N-K}}^{\text{K of N fail}} + \dots + \overbrace{(1-R)^N}^{\text{all fail}} = 1$$

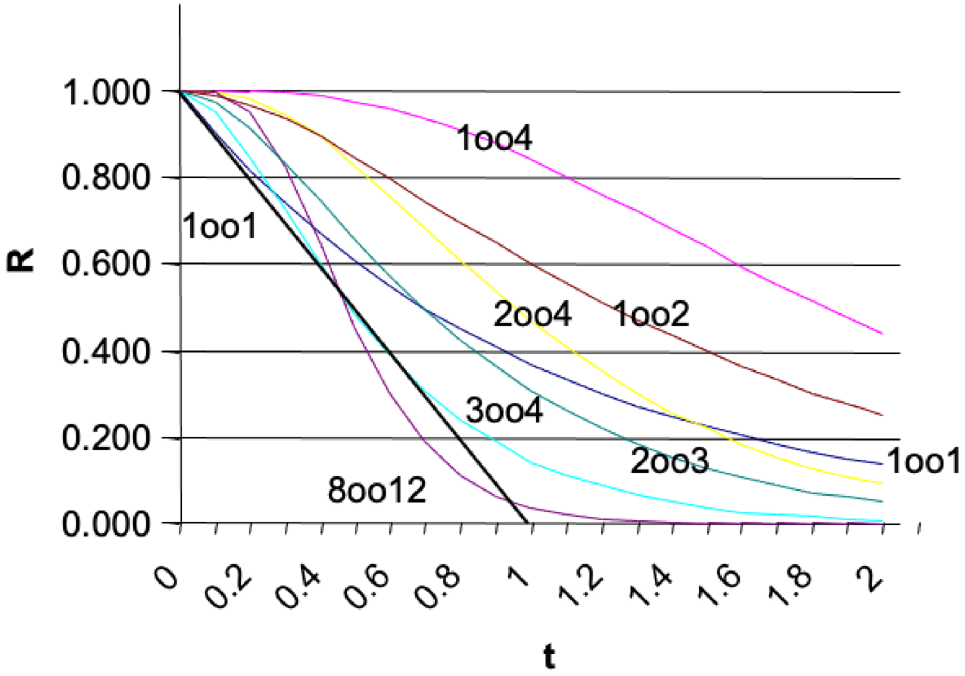
N of N

N + (N-1) of N

N + (N-1) + (N-2) of N

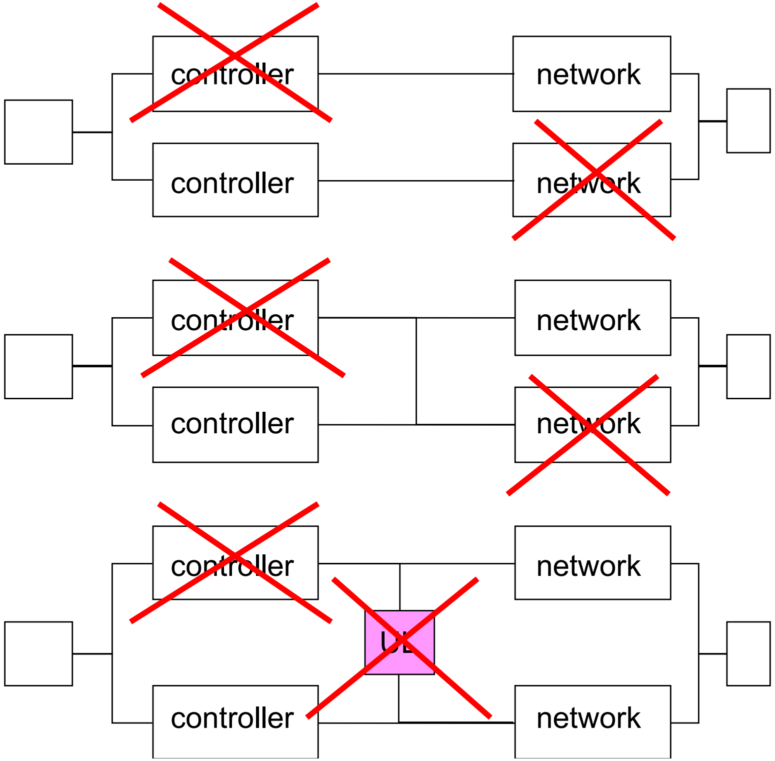
$$\boxed{R_{KooN} = \sum_{i=0}^{N-k} \binom{N}{i} (1-R)^i \; R^{N-i}}$$

Comparison Chart



What does cross redundancy bring?

Reliability chain



separate: double fault brings system down

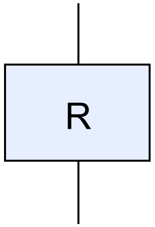
cross-coupling – better in principle since some double faults can be outlived

but cross-coupling needs a switchover logic – availability sinks again.

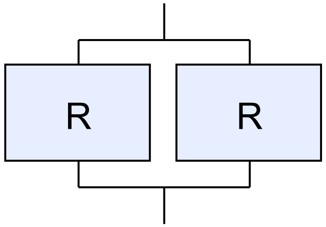
Summary

Assumes: all units have identical failure rates and comparison/voting hardware does not fail.

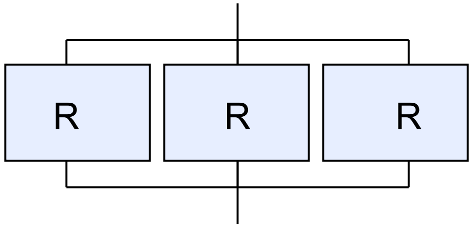
1oo1 (non redundant)



1oo2 (duplication and error detection)



2oo3 (triplication and voting)



$R_{1oo1} = R$

$R_{1oo2} = 2R - R^2$

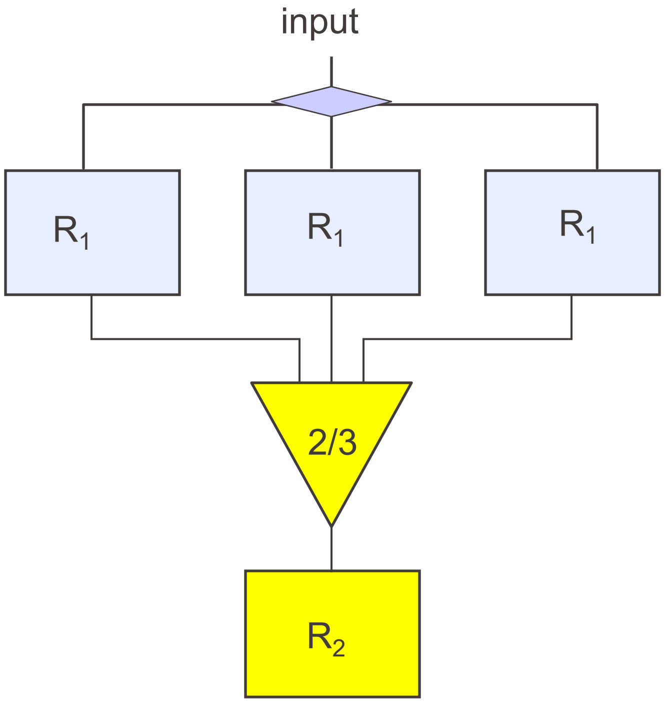
$R_{2oo3} = 3R^2 - 2R^3$

kooN (k out of N must work)

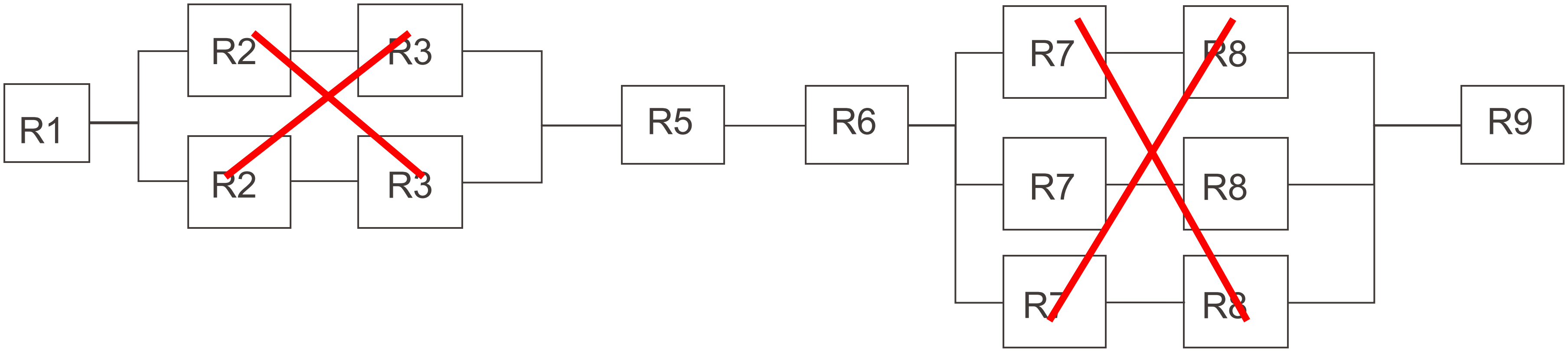
$$\boxed{R_{KooN} = \sum_{i=0}^{N-K} \binom{N}{i} (1 - R)^i \; R^{N-i}}$$

Exercise
1oo3 considering voter

- Compute the MTTF of the following 1-out-of-3 system with the component failure rates:
  - redundant units λ_1 = 0.1 h^{-1}
  - voter unit λ_{23} = 0.001 h^{-1}
  - single unit λ_2 = 0.15 h^{-1}



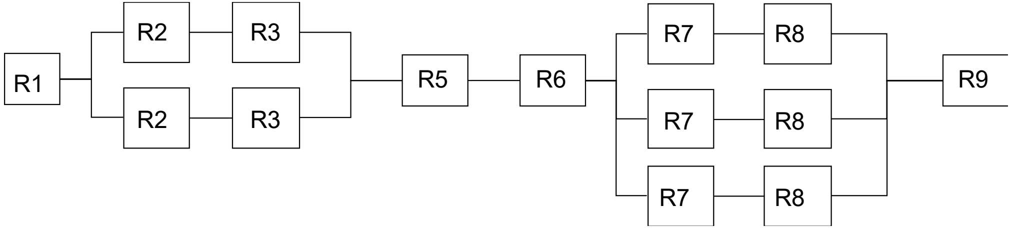
Complex Systems



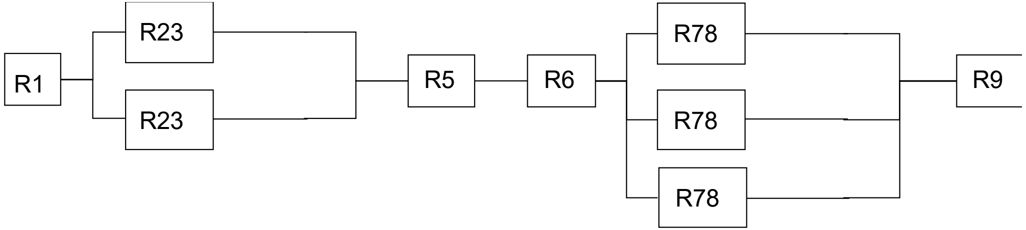
Reliability is dominated by the non-redundant parts, in a first approximation, forget the redundant parts.

Dr. Jean-Charles Tournier

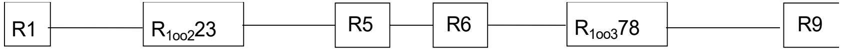
Complex Systems Simplification



Reduction Step 1



Reduction Step 2



Considering Repair

Repair

- Fault-tolerance does not improve reliability under all circumstances
- It is a solution for short mission duration

- Solution: repair (preventive maintenance, off-line repair, on-line repair)

- Example
  - short Mission time
    - pilot, co-pilot for commercial flights
  - long Mission time: how to reach the stars ?
    - Hibernation?, reproduction in space?

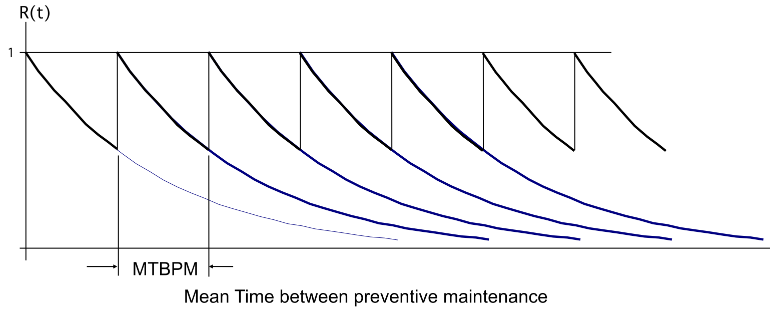
- Problem: exchange of faulty parts during operation (safety !)
  - reintegration of new parts
  - teaching and synchronization

Preventive Maintenance

- Preventive maintenance reduces the probability of failure, but does not prevent it

- In systems with wear, preventive maintenance prevents aging (e.g. replace oil, filters)

- Preventive maintenance is a regenerative process (maintained parts as good as new)



Considering Repair

- Beyond the combinatorial approach to compute reliability, other approaches are required
  - Combinatorial approach can **not** be used when considering repair
- The primary tool when considering repair is Markov Chain (or Markov Process)
  - Note that markov chain can also be used when repair is not considered

Markov Models to Compute Reliability and Availability

Markov Model

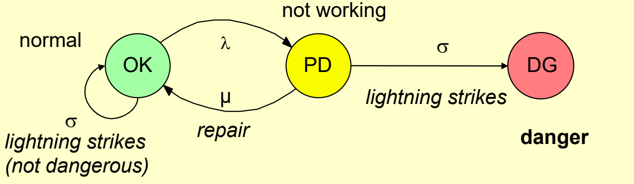
- Describe system through states, with transitions depending on fault-relevant events

- States must be
  - mutually exclusive
  - collectively exhaustive

- Let p_i (t) = Probability of being in state S_i at time t
  - $\sum_{i=0}^{AllStates} p_i(t) = 1$

- The probability of leaving that state depends only on current state
  - It is independent of how much time was spent in state or how state was reached

Example: protection failure

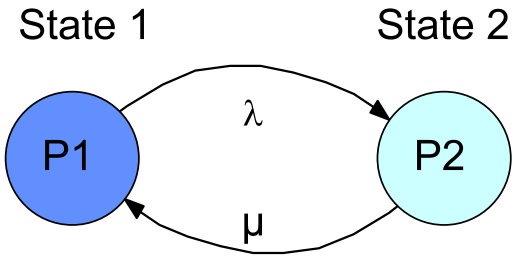


what is the probability that protection is down when lightning strikes ?

Continuous Markov Chains

- Time is considered continuous.
- Instead of transition probabilities, the temporal behavior is given by *transition rates*
  - i.e. transition probabilities per infinitesimal time step
- A system will remain in the same state unless going to a different state.
- Relationship between state probabilities are modeled by <u>differential equations</u>
  - e.g. $dP1/dt = \mu\ P2 - \lambda\ P1,$

    $dP2/dt = \lambda\ P1 - \mu\ P2$

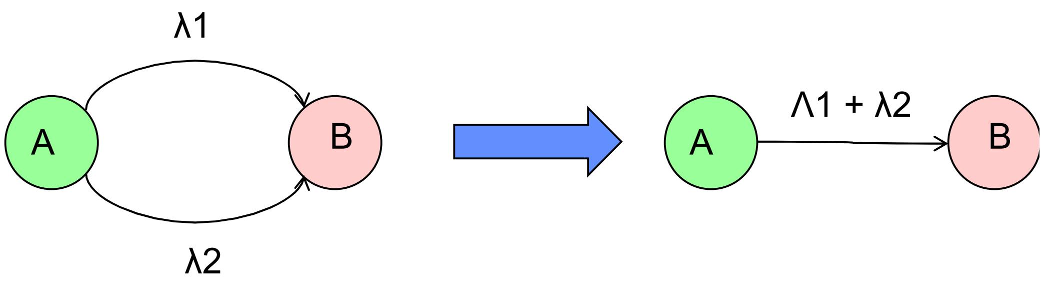


for any state:

$$\frac{dp_i(t)}{dt} = \overbrace{\sum \lambda_{\mathbf{k}}\, p_k(t)}^{\textbf{inflow}} - \overbrace{\sum \lambda_{\mathbf{i}}\, p_i(t)}^{\textbf{outflow}}$$

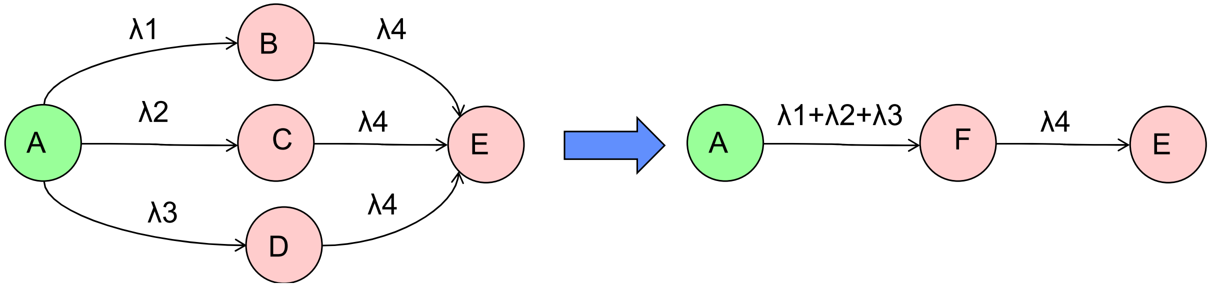
Markov Chain Simplification Rules

Parallel Transitions



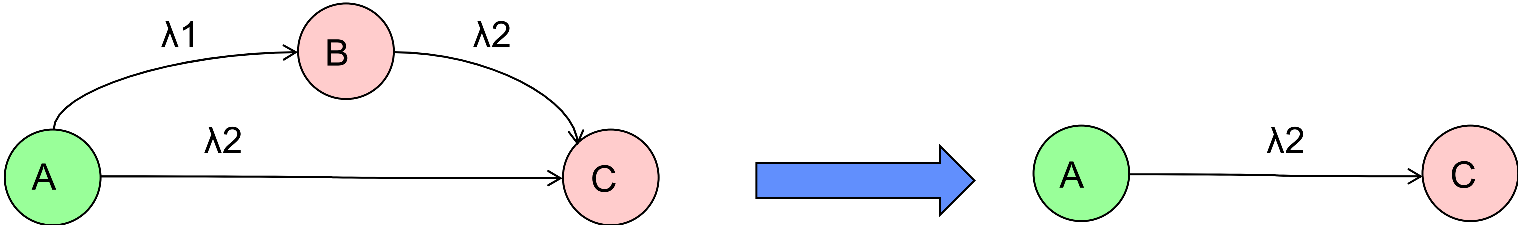
Intermediate States

- The states have the same outgoing events leading to the same state(s).
- No other incoming/outgoing exist.

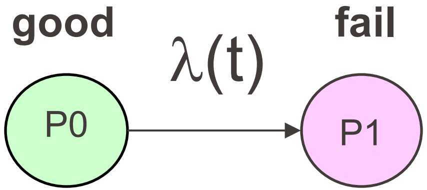


Markov Chain Simplification Rules

Side Step Events



Reliability Expressed as State Transition



$$\frac{dp_0}{dt} = - \lambda \, p_0$$

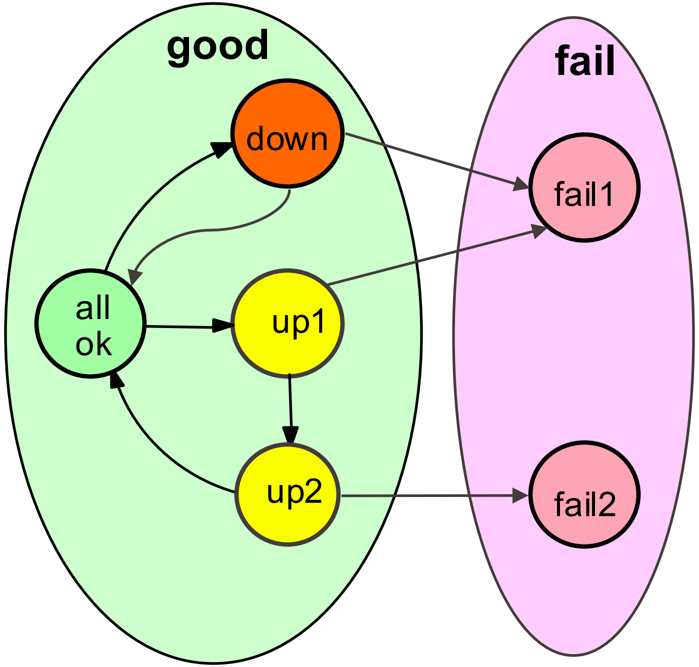
$$\frac{dp_1}{dt} = + \lambda \, p_0$$

$$R(t) = p_0(t) = e^{-\lambda t}$$

$R(t=0) = 1$

Reliability Expressed as State Transition

arbitrary transitions:



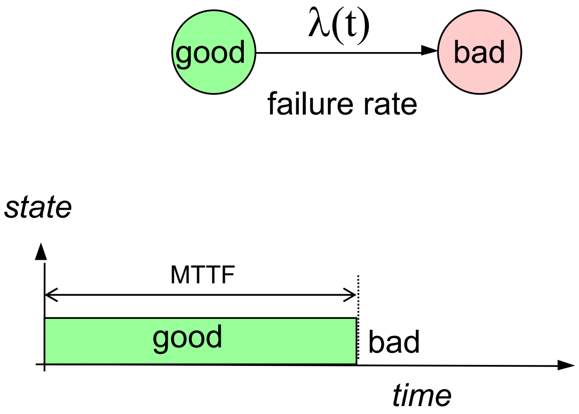
$$R(t) = 1 - (p_{fail1} + p_{fail2})$$

non-terminal states

terminal states

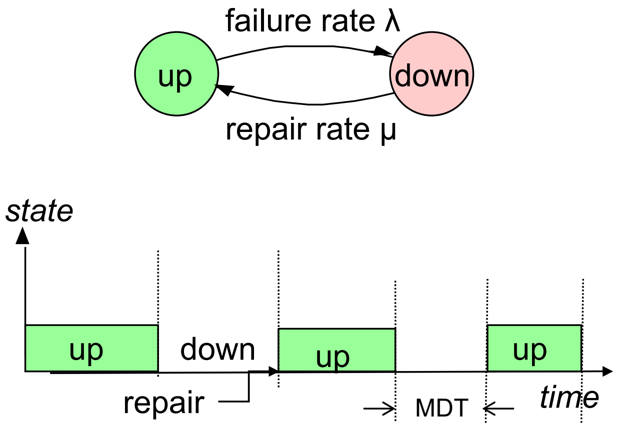
Reliability and Availability Expressed as Markov Models

Reliability



definition: "probability that an item will perform its required function in the specified manner and under specified or assumed conditions *over a given time period*"

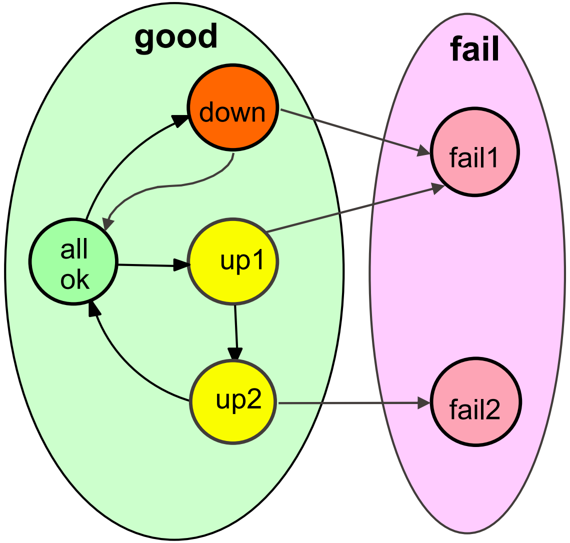
Availability



definition: "probability that an item will perform its required function in the specified manner and under specified or assumed conditions *at a given time* "

Absorbing states

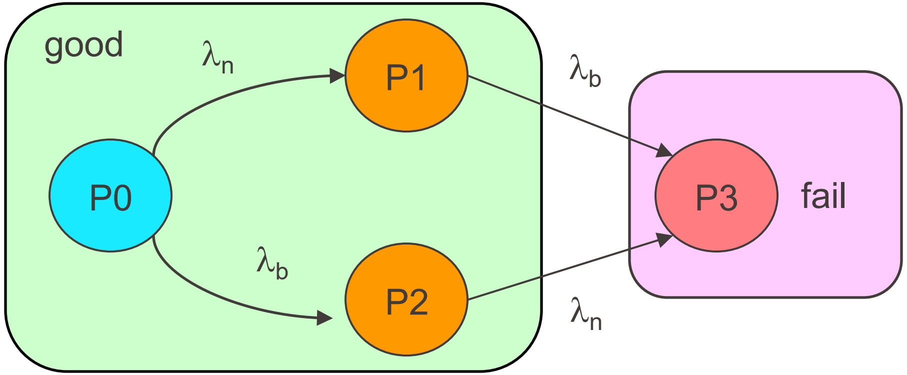
- Reliable systems have absorbing states, they may include repair, but eventually they will fail



non-terminal states

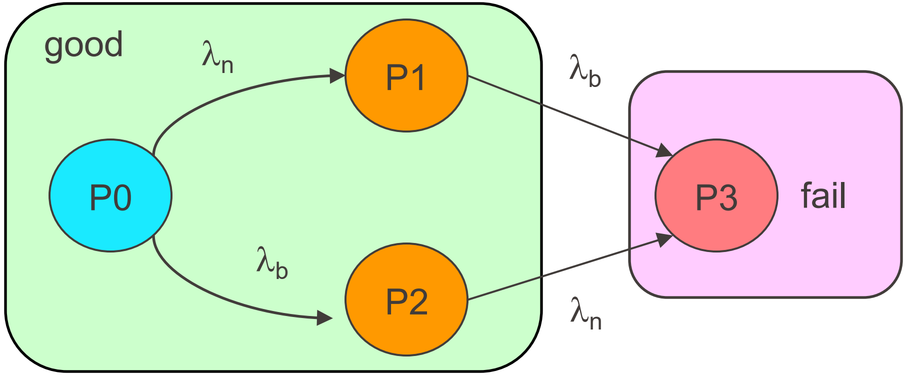
terminal states

Redundancy calculation with Markov: 1oo2 no repair

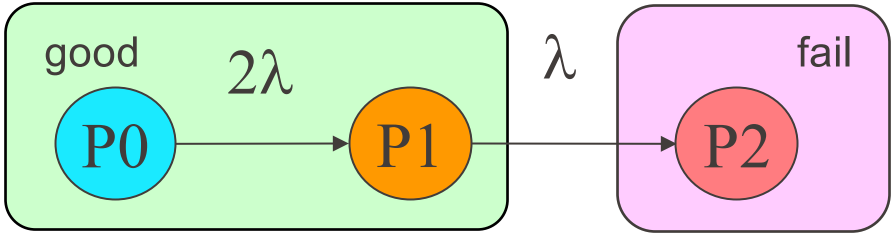


What is the probability that system be in state S_0 or S_1 or S_2 until time t ?

Redundancy calculation with Markov: 1oo2 no repair



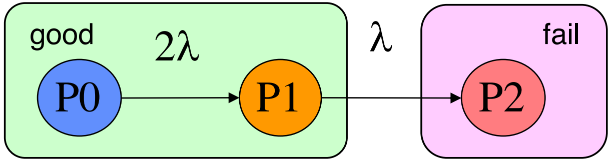
$$\lambda = \text{constant}$$



What is the probability that system be in state S_0 or S_1 until time t ?

Redundancy calculation with Markov: 1oo2 no repair

Markov:



λ = constant

What is the probability that system be in state S_0 or S_1 until time t ?

Linear Differential Equation

$$\frac{dp_0}{dt} = -2\lambda\, p_0$$

$$\frac{dp_1}{dt} = +2\lambda\, p_0 - \lambda p_1$$

$$\frac{dp_2}{dt} = \qquad + \lambda p_1$$

initial conditions:

$p_0\ (0) = 1$ (initially good)

$p_1\ (0) = 0$

$p_2\ (0) = 0$

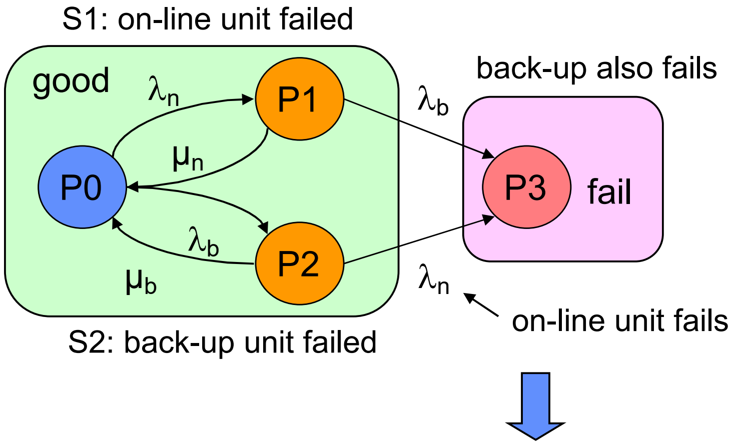
Solution:

$p_0\ (t) = e^{-2\lambda t}$

$p_1\ (t) = 2\, e^{-\lambda t} - 2\, e^{-2\lambda t}$

$R(t) = p_0\ (t) + p_1\ (t) = 2\, e^{-\lambda t} - e^{-2\lambda t}$ (same result as combinatorial - QED)

1oo2 with on-line repair



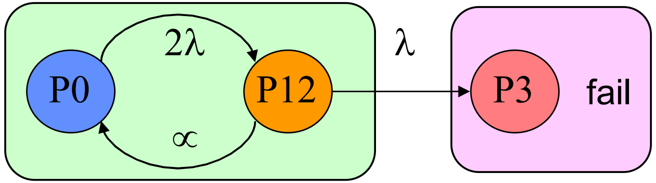
$$\frac{dp_0}{dt} = -2\lambda\, p_0 + \propto p_1 + \propto p_2$$

$$\frac{dp_1}{dt} = +\lambda\, p_0 - (\lambda+\propto)\, p_1$$

$$\frac{dp_2}{dt} = +\lambda\, p_0 - (\lambda+\propto)\, p_2$$

$$\frac{dp_3}{dt} = +\lambda\, p_1 + \lambda\, p_2$$

is equivalent to:



with $\propto_n = \propto_b$; $\lambda_n = \lambda_b$

$$\frac{dp_0}{dt} = -2\lambda\, p_0 + \propto p_{1+2}$$

$$\frac{dp_{1+2}}{dt} = +2\lambda\, p_0 - (\lambda+\propto)\, p_{1+2}$$

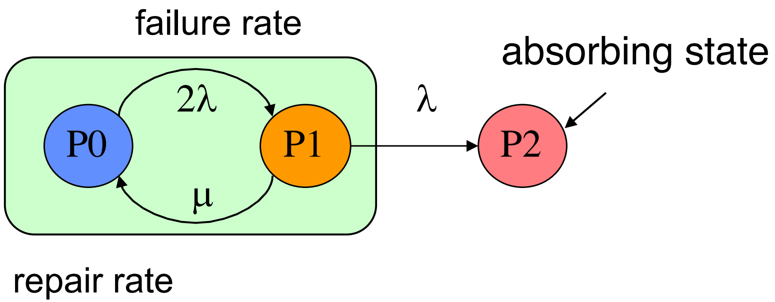
$$\frac{dp_3}{dt} = +\lambda\, (p_1+p_2)$$

it is easier to model with a repair team for each failed unit (no serialization of repair)

1oo2 with on-line repair

What is the probability that a system fails while one failed element awaits repair ?

Markov:



First order Differential Equations:

$$\frac{dp_0}{dt} = -2\lambda p_0 + \mu p_1$$

$$\frac{dp_1}{dt} = +2\lambda p_0 - (\lambda+\mu) p_1$$

$$\frac{dp_2}{dt} = +\lambda p_1$$

initial conditions:

$p_0(0) = 1$ (initially good)

$p_1(0) = 0$

$p_2(0) = 0$

Ultimately , the absorbing states will be “filled”, the non-absorbing will be “empty”.

Results: R(t) of 1oo2 with repair

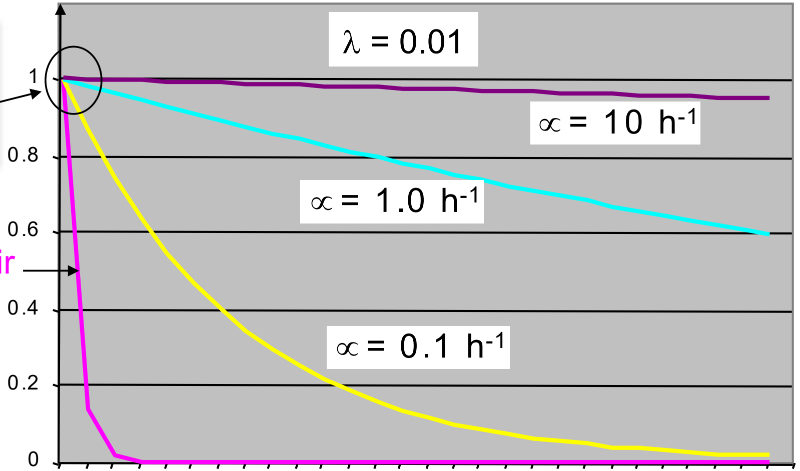
$$R(t) = P_0 + P_1 = \frac{(3\lambda+\mu)+W}{2W}\, e^{-(3\lambda+\mu-W)\, t} - \frac{(3\lambda+\mu)-W}{2W}\, e^{-(3\lambda+\mu+W)\, t}$$

with:

$$W = \sqrt{\lambda^2 + 6\lambda\mu + \mu^2}$$

we do not consider short mission time

1oo2 no repair



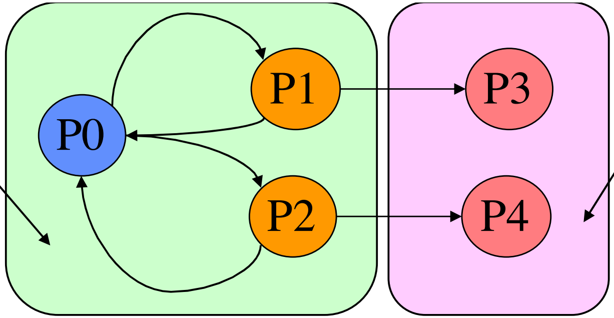
Time in hours

repair does not interrupt mission

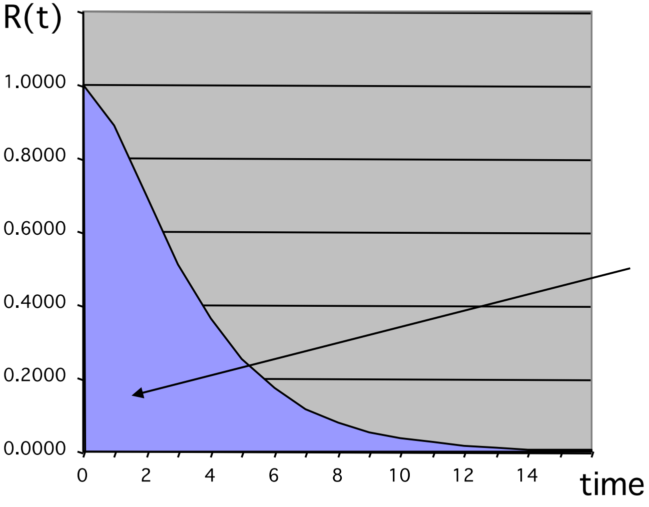
R(t) accurate, but not very helpful - MTTF is a better index for long mission time

Mean Time To Failure - MTTF

non-absorbing states i



absorbing states j



non-absorbing states i

$$\text{MTTF} = \int_0^\infty \Sigma p_i(t)\, dt$$

MTTF Calculation using Laplace Transform

Laplace transform
initial conditions:
p_0 (t=0) = 1 (initially good)

$$sP_0(s) - p_0(t=0) = -2\lambda P_0(s) + \mu P_1(s)$$
$$sP_1(s) - 0 = +2\lambda P_0(s) - (\lambda+\mu) P_1(s)$$
$$sP_2(s) - 0 = + \lambda P_1(s)$$

apply boundary theorem
(Final Value Theorem)

$$\lim_{t \to \infty} \int_0^{\infty} p(t)\, dt = \lim_{s \to 0} s\, P(s)$$

only include non-absorbing states
(number of equations =
number of non-absorbing states)

$$-1 = -2\lambda P_0 + \mu P_1$$
$$0 = +2\lambda P_0 - (\lambda+\mu) P_1$$

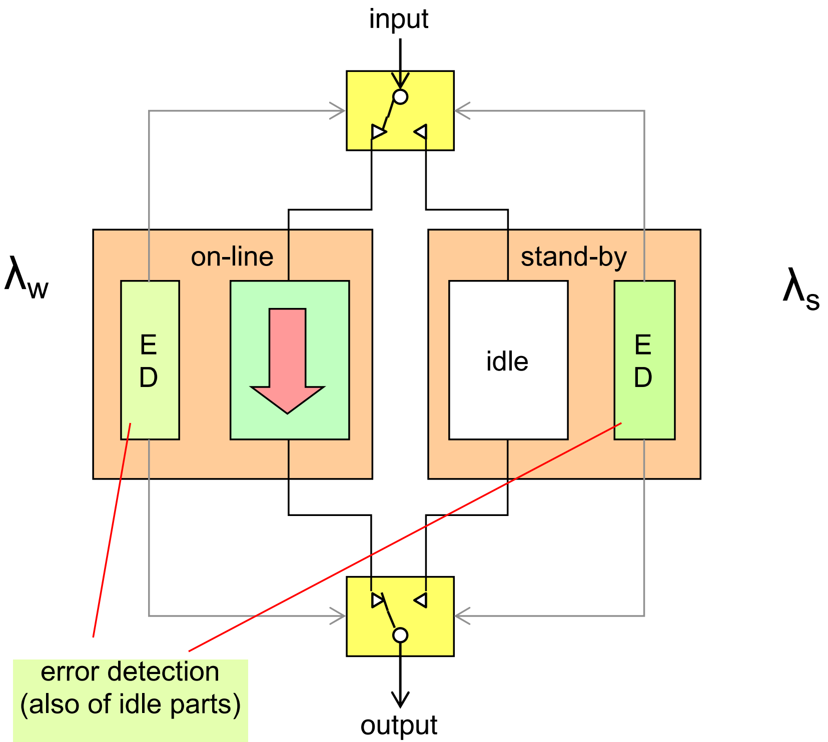
solution of linear equation system:

$$\text{MTTF} = P_0 + P_1 = \frac{(\mu + \lambda)}{2\lambda^2} + \frac{1}{\lambda} = \frac{\mu/\lambda + 3}{2\lambda}$$

General Approach to compute MTTF

1. Set up the differential equations
2. Identify the terminal states (absorbing)
3. Set up Laplace transform for non-absorbing states
4. Solve the linear equation system
5. The MTTF is the sum of the non-absorbing state integrals

Example 1oo2 control computer in standby



repair rate μ same for both

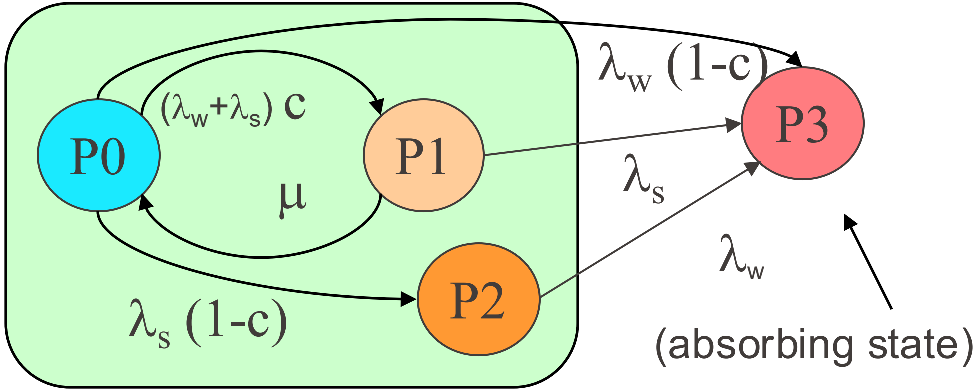
error detection
(also of idle parts)

coverage = c

Correct Markov Model for 1oo2

- Consider that the failure rate λ of a device in a 1oo2 system is divided into two failure rates:
    - a benign failure, immediately discovered with probability c
        - if device is on-line, switchover to the stand-by device is successful and repair called
        - if device is on stand-by, repair is called
    - a malicious failure, which is not discovered, with probability (1-c)
        - if device is on-line, switchover to the standby device fails, the system fails
        - if device is on stand-by, switchover will be unsuccessful should the online device fail

Correct Markov Model for 1oo2



1: on-line fails, fault detected
(successful switchover and repair)
or standby fails, fault detected,
successful repair
2: standby fails, fault not detected
3: both fail, system down or online fails fault not detected

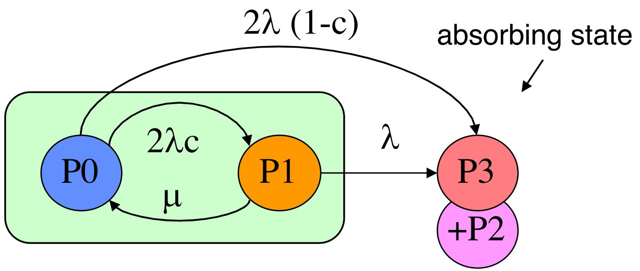
$$\begin{aligned} 1 &= -2\lambda P_0 + \mu P_1 \\ 0 &= +2\lambda c P_0 - (\lambda+\mu)P_1 \\ 0 &= +\lambda(1-c) P_0 - \lambda P_2 \end{aligned}$$

$$\text{MTTF} = \frac{(2+c) + \mu/\lambda\,(2-c)}{2\,(\lambda + \mu\,(1-c)\,)}$$

Approximation found in the literature

This simplified diagram considers that the undetected failure of the spare causes immediately a system failure

simplified when $\lambda_w = \lambda_s = \lambda$



$$-1 = -2\lambda P_0 + \mu P_1$$

$$0 = +2\lambda c P_0 - (\lambda+\mu) P_1$$

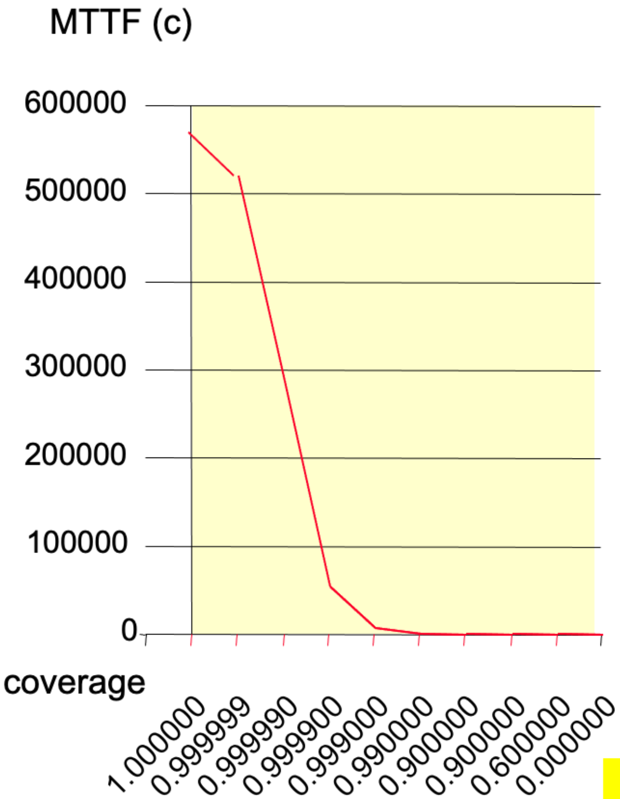
$$\cancel{0 = +2\lambda(1-c) P_0 + \lambda P_1}$$

applying Markov:

$$\mathrm{MTTF} = \frac{(1+2c) + \mu/\lambda}{2\,(\lambda + \mu\,(1-c))}$$

The results are nearly the same as with the previous four-state model, showing that the state 2 has a very short duration …

Considering coverage



Example:

$\lambda = 10^{-5}\ h^{-1}$ (MTTF = 11.4 year),
$\mu = 1\ hour^{-1}$
MTTF with perfect coverage = 570468 years

When coverage falls below 60%, the redundant (1oo2) system performs no better than a simplex one !

Therefore, coverage is a critical success factor for redundant systems !

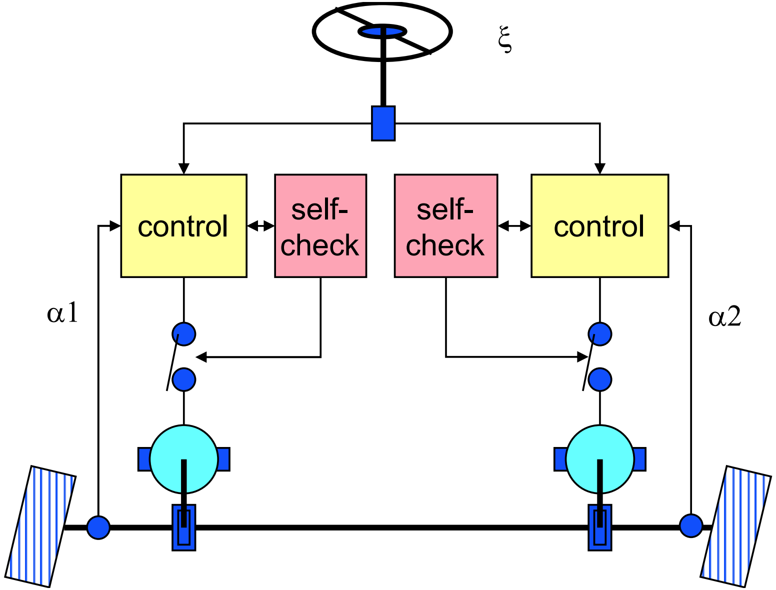
In particular, redundancy is useless if failure of the spare remains undetected (lurking error).

$$\lim_{\mu \to 0} \text{MTTF} = \frac{1}{\lambda}\left(\frac{3}{2} + \frac{\mu}{2\lambda}\right)$$

$$\lim_{\lambda/\mu \to 0} \text{MTTF} = \frac{1}{\lambda\,(1-c)}$$

Application
1oo2 for drive-by-wire

- coverage is assumed to be the probability that self-check detects an error in the controller.
- when self-check detects an error, it passivates the controller (output is disconnected) and the other controller takes control.
- one assumes that an accident occurs if both controllers act differently, i.e. if a computer does not fail to silent behaviour.
- Self-check is not instantaneous, and there is a probability that the self-check logic is not operational, and fails in underfunction (overfunction is an availability issue)

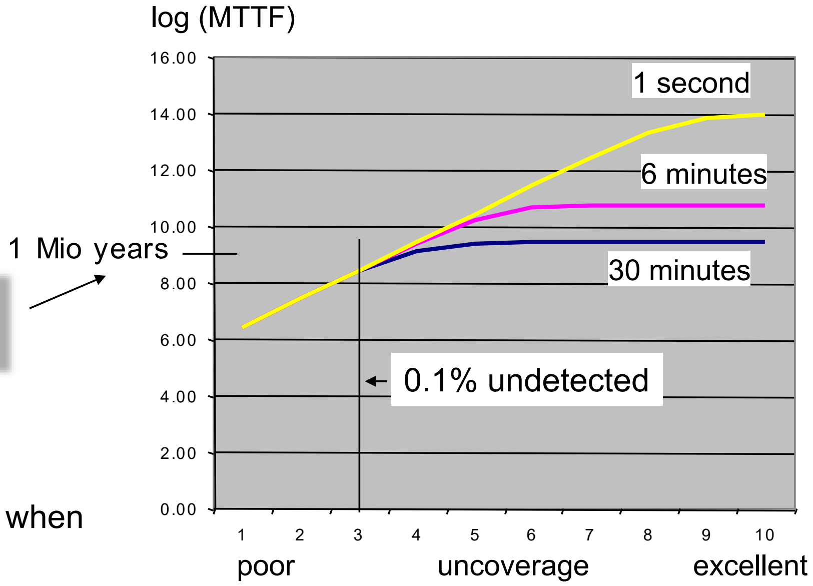


Results 1oo2c, applied to drive-by-wire

λ = reliability of one chain (sensor to brake) = 10^{-5} h^{-1} (MTTF = 10 years)

c = coverage: variable (expressed as uncoverage: 3nines = 99.9 % detected)

μ = repair rate = parameter
- 1 Second: reboot and restart
- 6 Minutes: go to side and stop
- 30 Minutes: go to next garage

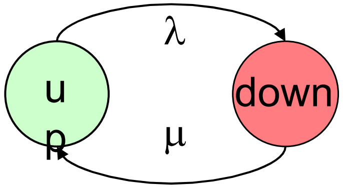


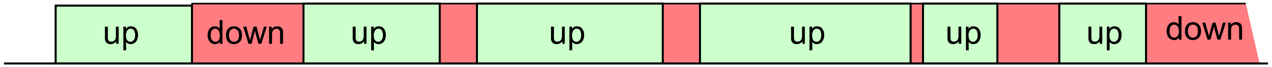
or once per year on a million vehicles

conclusion:
the repair interval does not matter when coverage is poor

Availability Evaluation

Availability





Availability expresses how often a piece of repairable equipment is functioning it depends on failure rate λ and repair rate μ.

Punctual or point availability = probability that the system working at time t (not relevant for most processes).

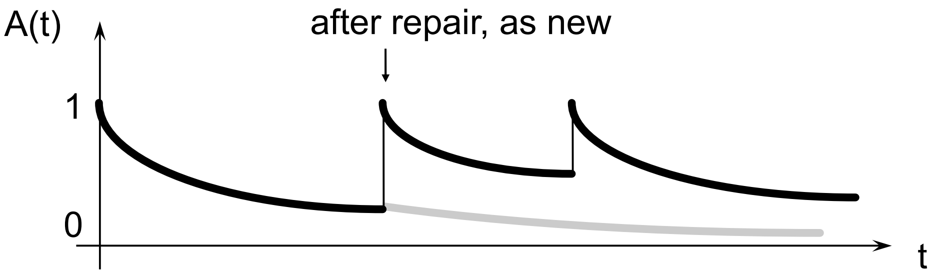
Stationary availability = duty cycle (Percentage of time spent in up state) (impacts financial results)

$$A_\infty = \text{availability} = \lim_{t \to \infty} \frac{\sum \text{up times}}{\sum (\text{up times} + \text{down times})} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$$

Unavailability is the complement of availability (U = 1,0 – A) as convenient expression.
(e.g. 5 minutes downtime per year = availability is 0.999%)

Assumption: renewable system

R(t) ≤ A(t) due to repair or preventive maintenance
(exchange parts that did not yet fail)

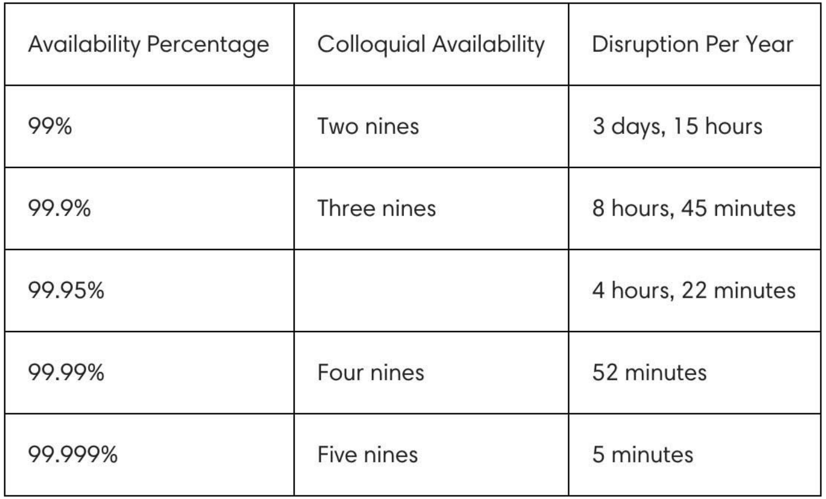


Stationary availability $A = \dfrac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$ over the lifetime

Examples of availability requirements

- Substation automation
  - >99.95%
  - ~ 4 hours per year
- Telecom power supply
  - Unavailability of $5.10^{-5}\%$
  - ~ 15 seconds per year
- Emergency response system
  - 99.999% availability
  - 5 minutes per year

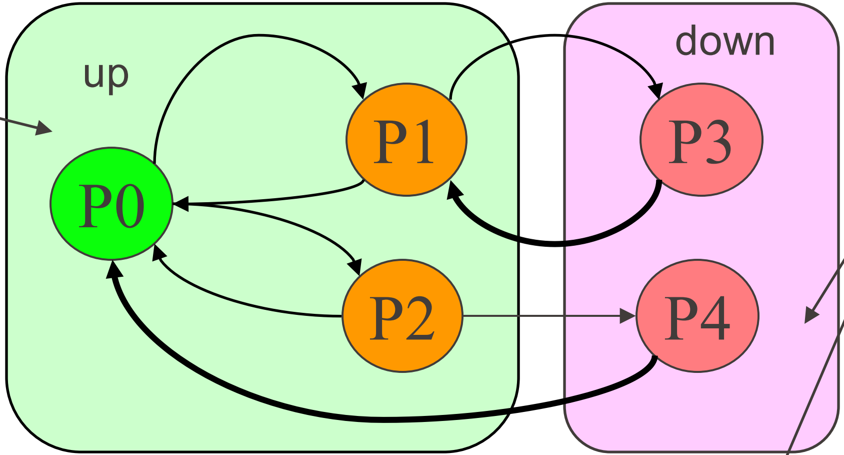
  - https://aws.amazon.com/blogs/publicsector/achieving-five-nines-cloud-justice-public-safety/



Availability Percentage	Colloquial Availability	Disruption Per Year
99%	Two nines	3 days, 15 hours
99.9%	Three nines	8 hours, 45 minutes
99.95%		4 hours, 22 minutes
99.99%	Four nines	52 minutes
99.999%	Five nines	5 minutes

Availability Expressed in Markov Models

up states i



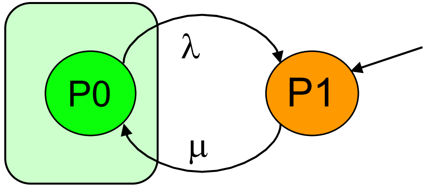
down states j (non-absorbing)

Availability = $\Sigma p_i(t = \infty)$

Unavailability = $\Sigma p_j\ (t = oo)$

Availability of repairable systems

Markov states:



down state
(but not absorbing)

$$\frac{dp_0}{dt} = -\lambda p_0 + \mu p_1$$

$$\frac{dp_1}{dt} = +\lambda p_0 - \mu p_1$$

stationary state: $\lim_{t\to\infty} \frac{dp_0}{dt} = \frac{dp_1}{dt} = 0$

due to linear dependency add condition: $p_0 + p_1 = 1$

$$A = \frac{1}{1 + \frac{\lambda}{\mu}}$$

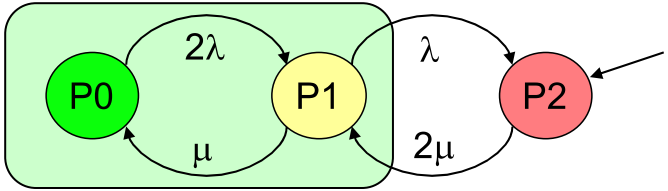
unavailability $U = (1 - A) = \frac{1}{1 + \mu/\lambda}$

e.g. = MTBF = 100 Y -> $\lambda = 1 / (100 * 8765)\ h^{-1}$ -> A = 99.991 %

MTTR = 72 h -> $\mu = 1/ 72\ h^{-1}$ -> U = 43 mn / year

Availability of 1oo2

Markov states:



down state
(but not absorbing)

assumption: devices can be repaired independently (little impact when $\lambda << \mu$)

$$\frac{dp_0}{dt} = -2\lambda\, p_0 \qquad + \mu p_1$$

$$\frac{dp_1}{dt} = +2\lambda\, p_0 - (\lambda+\mu)\, p_1 + 2\mu\, p_2$$

$$\frac{dp_2}{dt} = \qquad + \lambda p_1 - 2\mu\, p_2$$

stationary state: $\lim\limits_{t\to\infty} \frac{dp_0}{dt} = \frac{dp_1}{dt} = \frac{dp_2}{dt} = 0$

due to linear dependency add condition: $p_0 + p_1 + p_2 = 1$

$$A = \frac{1}{1 + \frac{2\lambda^2}{\mu^2 + 2\lambda\mu}}$$

unavailability $U = (1 - A) = \quad \lim_{U<<1} \quad \frac{2}{(\mu/\lambda)^2 + 2(\mu/\lambda)}$

e.g. = MTBF = 100 Y -> $\lambda = 1 / (100 * 8765)\ h^{-1}$ -> A = 99.9999993 %
MTTR = 72 h -> $\mu = 1/\ 72\ h^{-1}$ -> U = 0.2 s / year

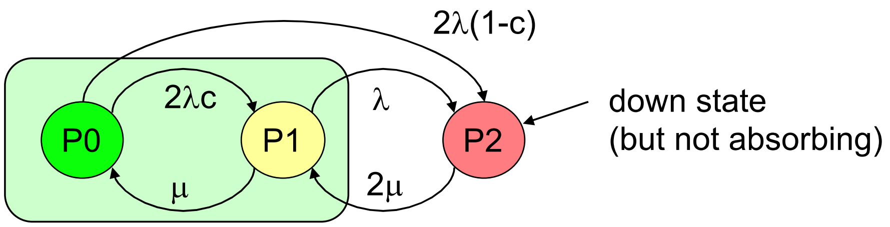
Availability Calculation

1. Set up the differential equations for all states
2. Identify up and down states (no absorbing states!)
3. Remove one state equation (arbitrary, for numerical reasons remove the most unlikely state)
4. Add as first equation the pre-condition:$\sum p_{i(t)} = 1$
5. The degree of the system of equation is equal to the number of states
6. Solve the linear system, yielding the percentage of time each state is visited
7. The availability is the sum of all up states

- We do not use Laplace transform for availability calculation!

Availability 1oo2 considering coverage

Markov states:



down state
(but not absorbing)

assumption: devices can be repaired independently (little impact when λ << μ)

$$\frac{dp_0}{dt} = -2\lambda\, p_0 \qquad + \mu p_1$$

$$\frac{dp_1}{dt} = +2\lambda c\, p_0 - (\lambda+\mu)\, p_1 + 2\mu\, p_2$$

$$\frac{dp_2}{dt} = +2\lambda(1-c)\, p0 + \lambda p_1 - 2\mu\, p_2$$

stationary state: $\lim_{t \to \infty} \frac{dp_0}{dt} = \frac{dp_1}{dt} = \frac{dp_2}{dt} = 0$

due to linear dependency add condition: $p_0 + p_1 + p_2 = 1$

Exercise

- A repairable system has a constant failure rate $\lambda = 10^{-4}$ / h.
- Its mean time to repair (MTTR) is one hour.

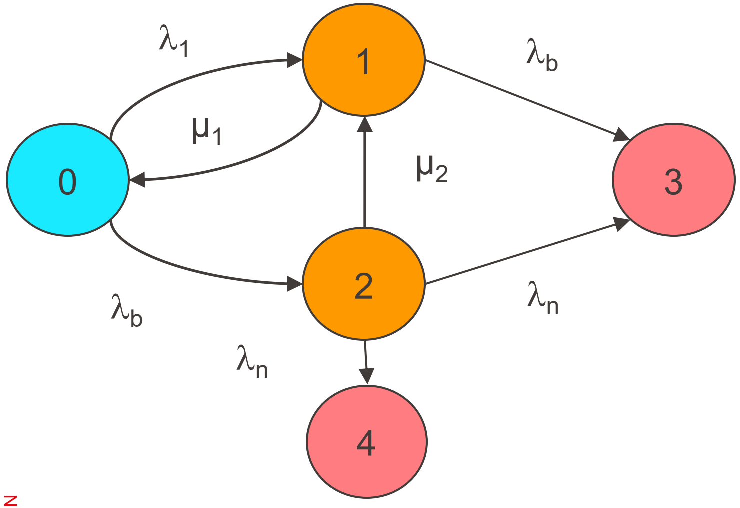
1. Compute the mean time to failure (MTTF).
2. Compute the MTBF and compare with the MTTF.
3. Compute the stationary availability.

- Assume that the unavailability has to be halved. How can this be achieved

1. by only changing the repair time?
2. by only changing the failure rate?
3. Make a drawing that shows how a varying repair time influences availability.

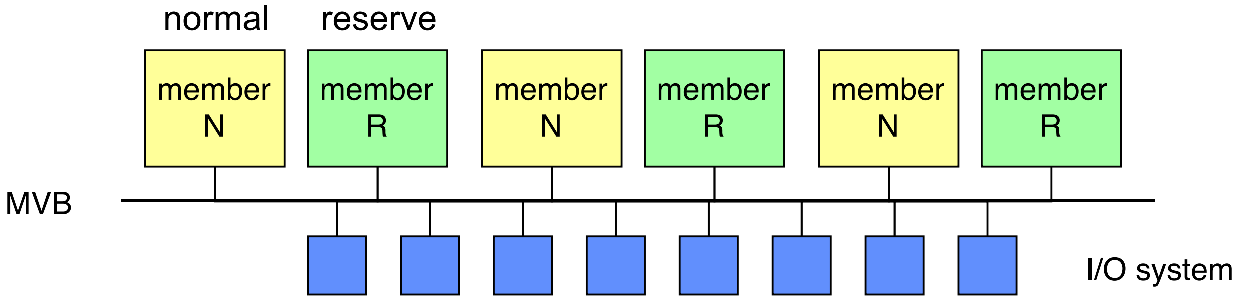
Example

Exercise Markov Diagram



- Is this a reliable or an available evaluation ?
- Set up the differential equations for this Markov model.
- Compute the probability of not reaching state 4 (set up equations)

Case Study
Swiss Locomotive 460 control system availability



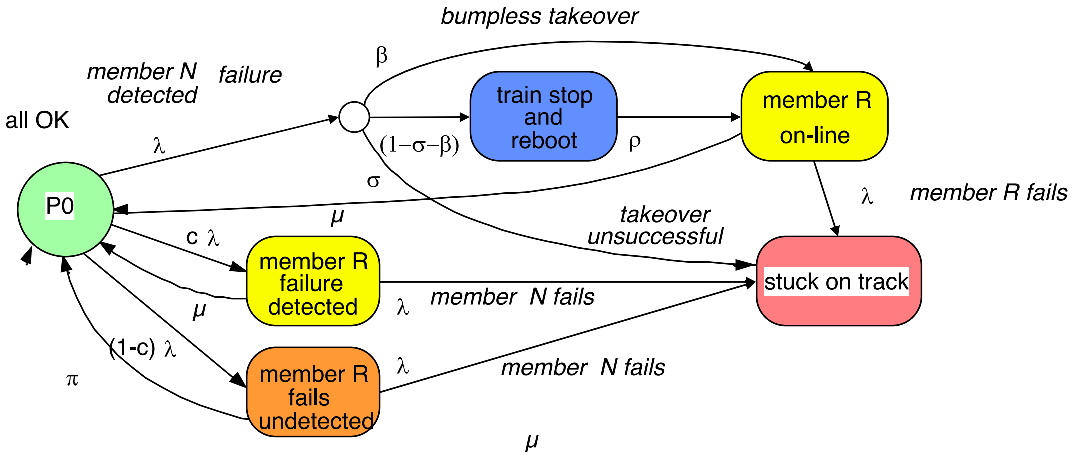
Assumption: each unit has a back-up unit which is switched on when the on-line unit fails

The error detection coverage c of each unit is imperfect

The switchover is not always bumpless - when the back-up unit is not correctly actualized, the main switch trips and the locomotive is stuck on the track

What is the probability of the locomotive to be stuck on track ?

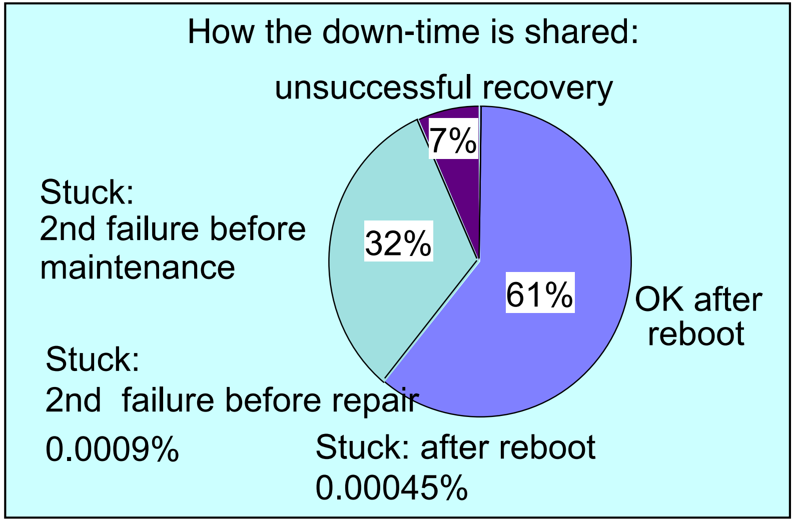
Case Study
Swiss Locomotive 460 control system availability



λ	probability that member N or member R fails
μ	mean time to repair for member N or member P
c	probability of detected failure (coverage factor)
β	probability of bumpless recovery (train continues)
σ	probability of unsuccessful recovery (train stuck)
ρ	time to reboot and restart train
π	periodic maintenance check

$\lambda = 10^{-4}$	(MTTF is 10000 hours or 1,2 years)
$\mu = 0.1$	(repair takes 10 hours, including travel to the works)
$c = 0.9$	(probability is 9 out of 10 errors are detected)
$\beta = 0.9$	(probability is that 9 out of 10 take-over is successful)
$\sigma = 0.01$	(probability is 1 failure in 100 cannot be recovered)
$\rho = 10$	(mean time to reboot and restart train is 6 minutes)
$\pi = 1/8765$	(mean time to periodic maintenance is one year).

Case Study
Swiss Locomotive 460 control system availability

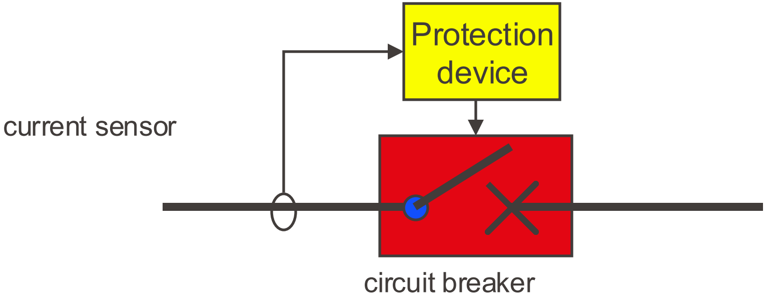


Under these conditions:

unavailability will be **0.5 hours a year**.
stuck on track is once every **20 years**.
recovery will be successful **97%** of the time.

recommendation: increase coverage by using alternatively members N and R
(at least every start-up)

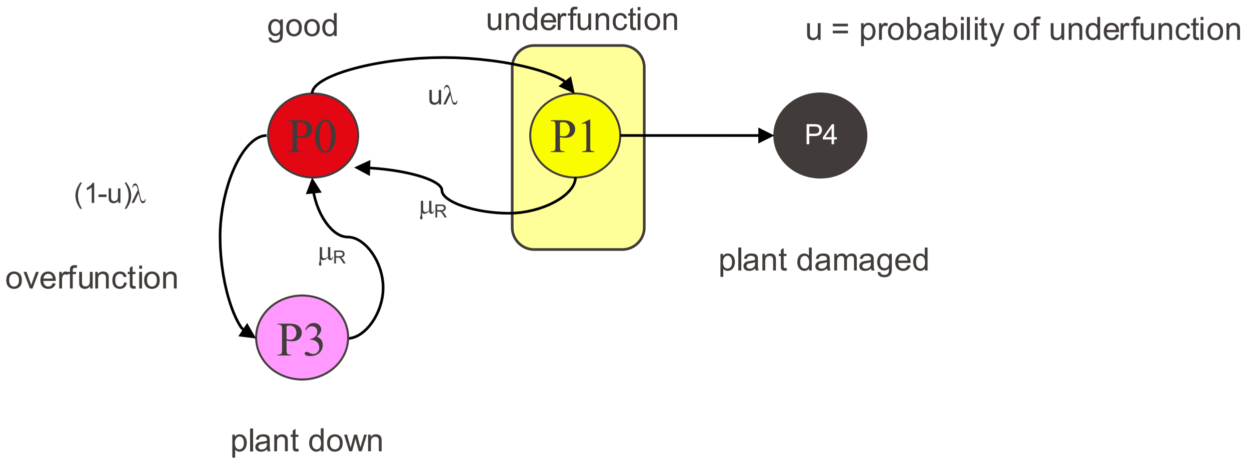
Example protection device



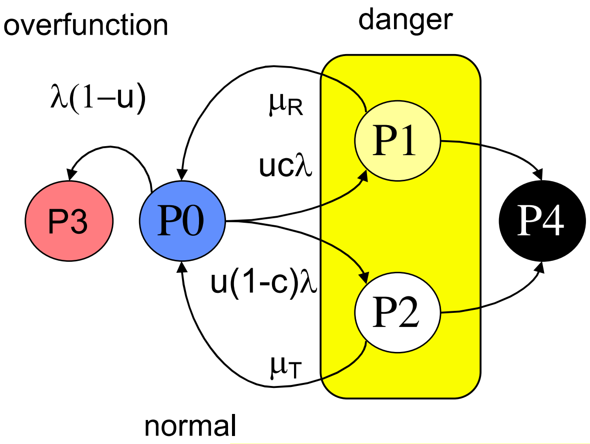
Probability to Fail on Demand for safety (protection) system

IEC 61508 characterizes a protection device by its Probability to Fail on Demand (PFD):

PFD = (1 - availability of the non-faulty system) (State 0)



Protection system with error detection (self-test) 1oo1



λ: protection failure

u: probability of underfunction [IEC 61508: 50%]

C: coverage, probability of failure detection by self-check

P1: protection failed in underfunction, failure detected by self-check (instantaneous), repaired with rate μ_R = 1/MRT

P2: protection failed in underfunction, failure detected by periodic check with rate μ_T = 2/TestPeriod

P3: protection failed in overfunction, plant down

P4: system threatened, protection inactive, danger

$$PFD = 1 - P_0 = 1 - \frac{1}{1 + \frac{\lambda\, u\, (1-c)}{\mu_T} + \frac{\lambda\, u\, c}{\mu_R}} \approx \lambda\, u \left(\frac{(1-c)}{\mu_T} + \frac{c}{\mu_R} \right)$$

with: $\lambda = 10^{-7}\ h^{-1}$

MTTR = 8 hours -> μ_R =0.125 h^{-1}

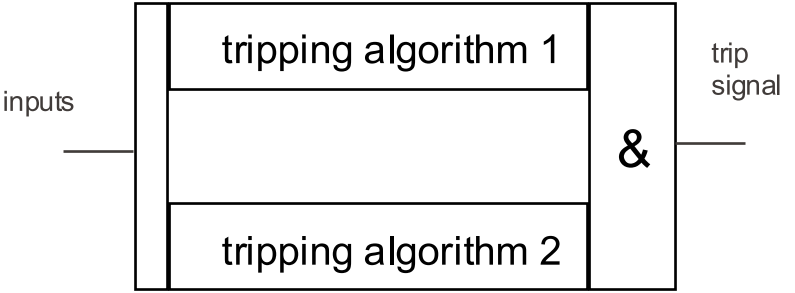
Test Period = 3 months -> μ_T =2/4380

coverage = 90%

$\longrightarrow$ PFD = 1.1 10^{-5}

for S1 and S2 to have same probability: c = 99.8% !

Example: Protection System



inputs

tripping algorithm 1

tripping algorithm 2

&

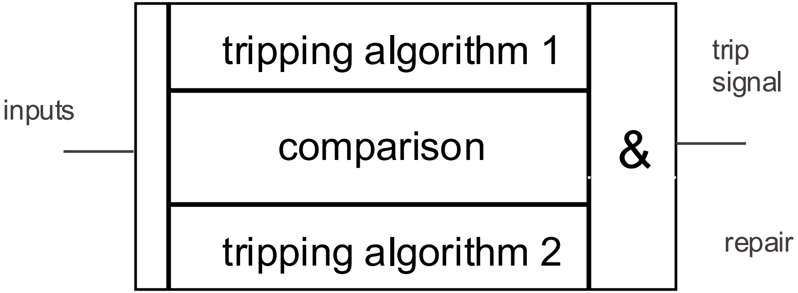
trip signal

overfunctions reduced

$$P_{over} = Po^{2}$$

underfunctions increased

$$P_{under} = 2Pu - Pu^{2}$$



inputs

tripping algorithm 1

comparison

tripping algorithm 2

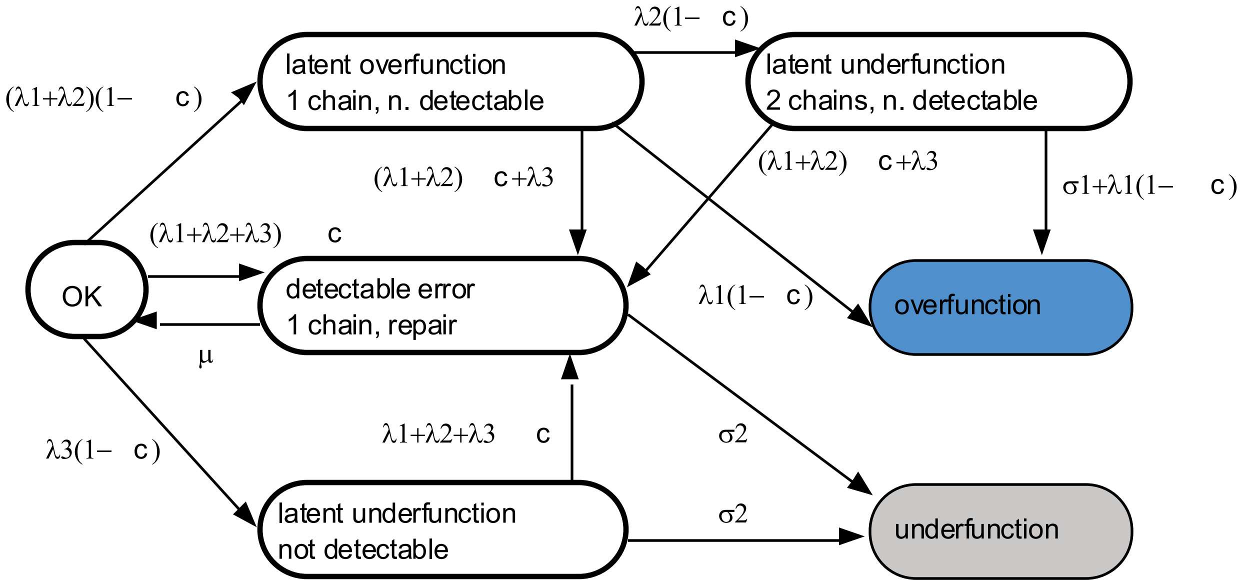
&

trip signal

repair

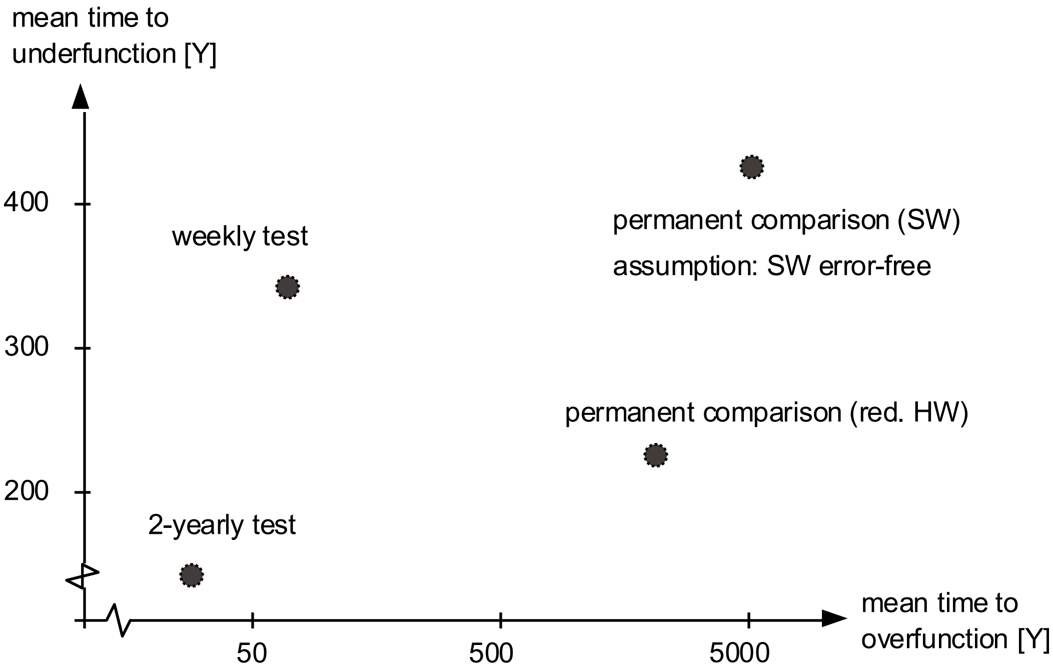
dynamic modeling necessary

Markov Model for a protection system



λ1=0.01, λ2=λ3=0.025, σ1=5, σ2=1, μ=365, c=0.9 [1/ Y]

Analysis Results

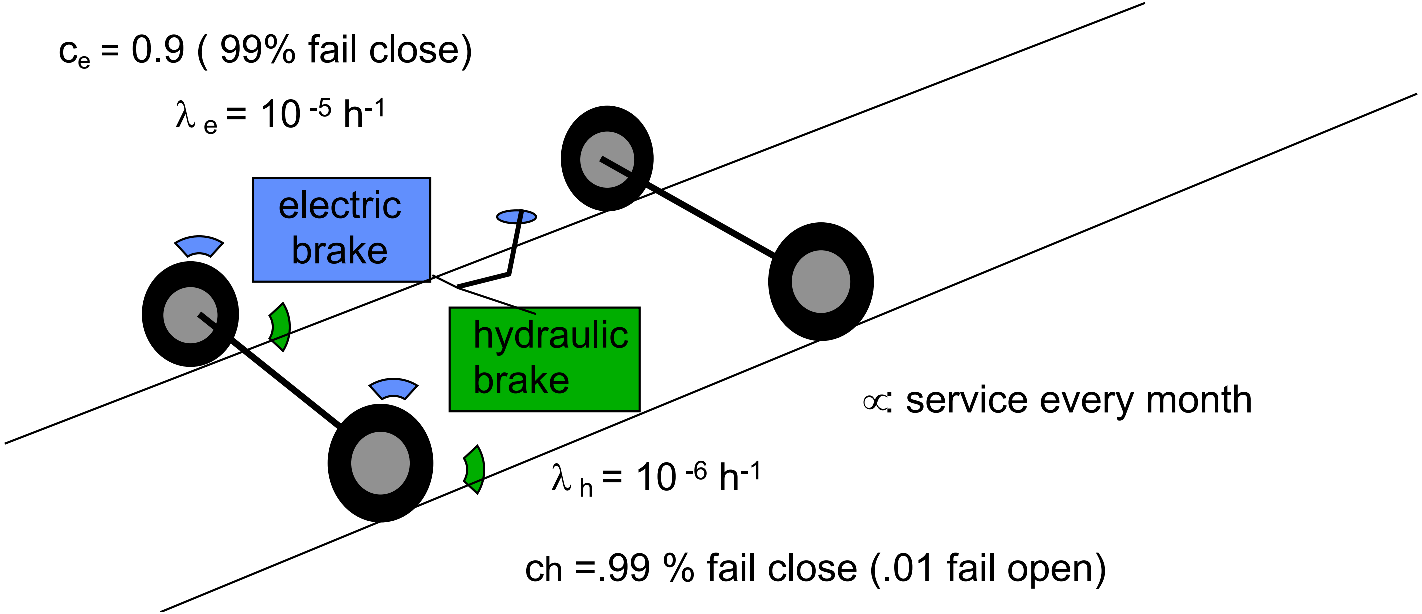


Exercise

A brake can fail open or fail close.
A car is unable to brake if both brakes fail open.
A car is unable to cruise if any of the brakes fail close.
A fail open brake is detected at the next service (rate ∝).
There is an hydaulic and an electric brake.

c_e = 0.9 (99% fail close)

$\lambda_e = 10^{-5}\ h^{-1}$



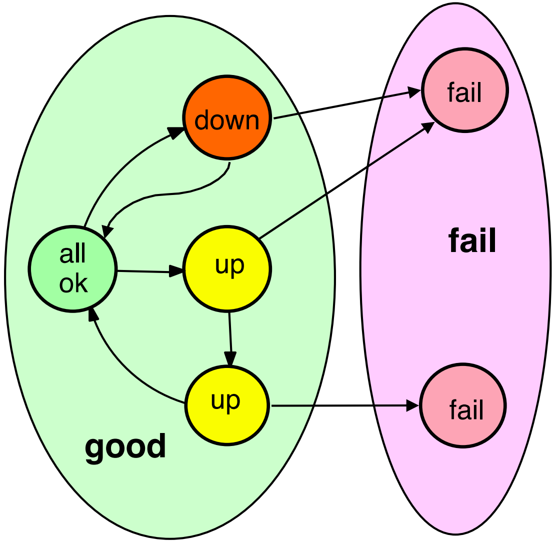
∝: service every month

$\lambda_h = 10^{-6}\ h^{-1}$

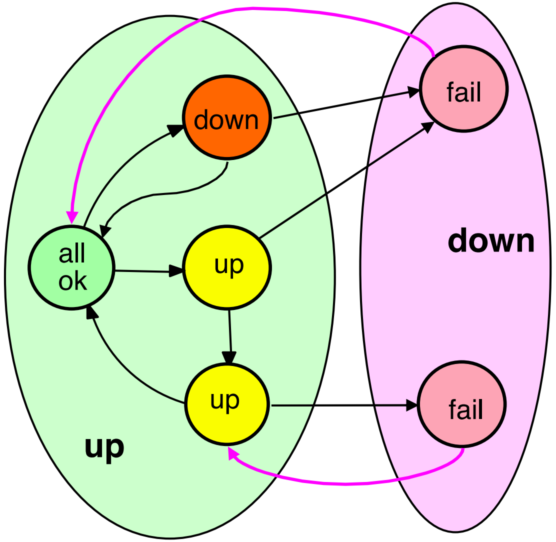
ch =.99 % fail close (.01 fail open)

Summary

Reliability



Availability



look for: Mean Time To Fail
(integral over time of all non-absorbing states)
set up linear equation with s = 0,
initial conditions S(T = 0) =1.0
solve linear equation

look for: stationary availability A (t = ∞)
(duty cycle in UP states)
set up differential equation (no absorbing states!)
initial condition is irrelevant
solve stationary case with ∑p = 1