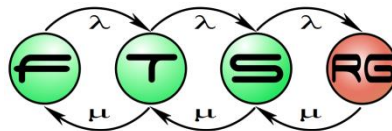


Dependability Analysis

Istvan Majzik

Budapest University of Technology and Economics
Fault Tolerant Systems Research Group



Main topics of the course

- Overview (1)
 - V&V techniques, Critical systems
- Static techniques (2)
 - Verifying specifications
 - Verifying source code
- Dynamic techniques: Testing (7)
 - Developer testing, Test design techniques
 - Testing process and levels, Test generation, Automation
- System-level verification (3)
 - Verifying architecture, **Dependability analysis**
 - Runtime verification

Learning outcomes

- Explain the **attributes of dependability** and the objectives of **dependability analysis** (K2)
- Perform dependability analysis with **reliability block diagrams** (K3)
- Perform dependability analysis of simple redundancy structures with **Markov chains** (K3)
- Identify how **stochastic Petri nets** can be used for dependability analysis (K1)

Table of Contents

- Attributes of dependability
 - Reliability, availability
 - Safety, integrity, maintainability
- Combinational models for dependability analysis
 - Reliability block diagrams
- Stochastic modeling of system dependability
 - Markov models (CTMC)
 - Stochastic Petri-nets

Attributes of dependability

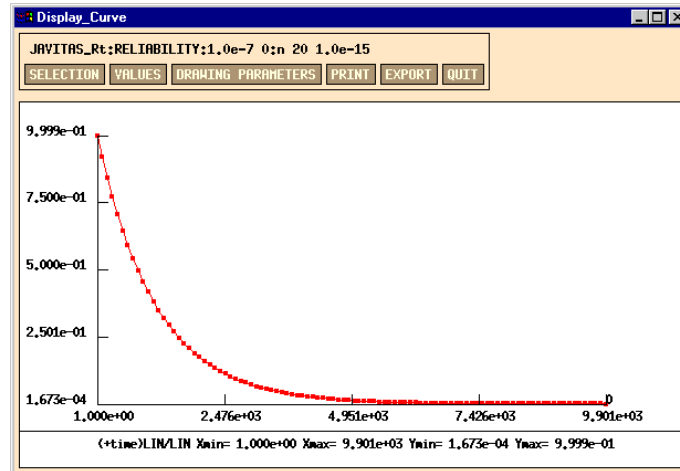
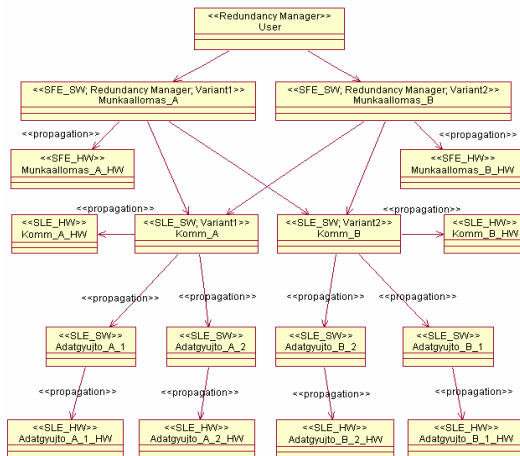


Table of Contents

- **Attributes of dependability**
 - **Reliability, availability**
 - **Safety, integrity, maintainability**
- **Combinational models for dependability analysis**
 - Reliability block diagrams
- **Stochastic modeling of system dependability**
 - Markov models (CTMC)
 - Stochastic Petri-nets

Characterizing the system services

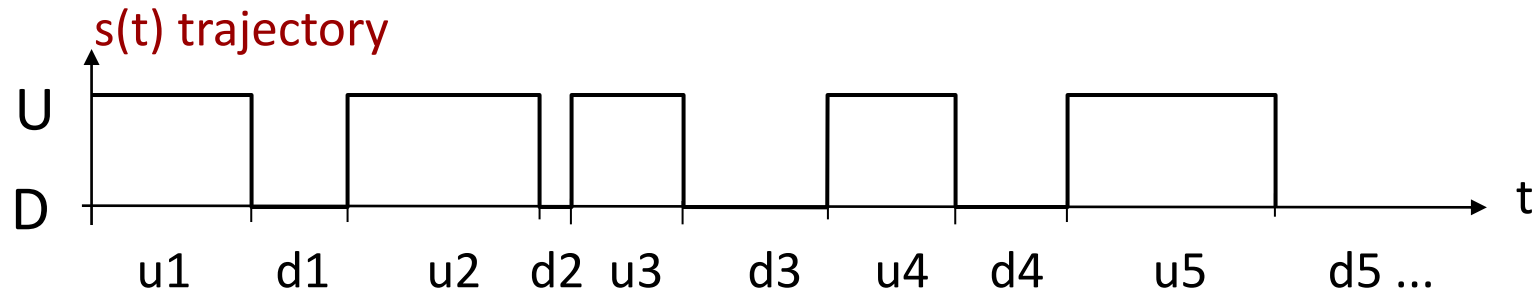
- Typical extra-functional characteristics
 - Reliability, availability, integrity, ...
 - Depend on the faults occurring during the use of the services
- Composite characteristic: **Dependability**
 - **Definition:** Ability to provide service in which reliance can justifiably be placed
 - **Justifiably:** based on analysis, evaluation, measurements
 - **Reliance:** the service satisfies the needs
- Role of dependability
 - Service Level Agreements (IT service providers)
 - Tolerable Hazard Rate (safety-critical systems)

Attributes of dependability

Attribute	Definition
Availability	Probability of correct service (considering repairs and maintenance) “Availability of the web service shall be 95%”
Reliability	Probability of continuous correct service (until the first failure) “After departure the onboard control system shall function correctly for 12 hours”
Safety	Freedom from unacceptable risk of harm
Integrity	Avoidance of erroneous changes or alterations
Maintainability	Possibility of repairs and improvements

Dependability metrics: Mean values

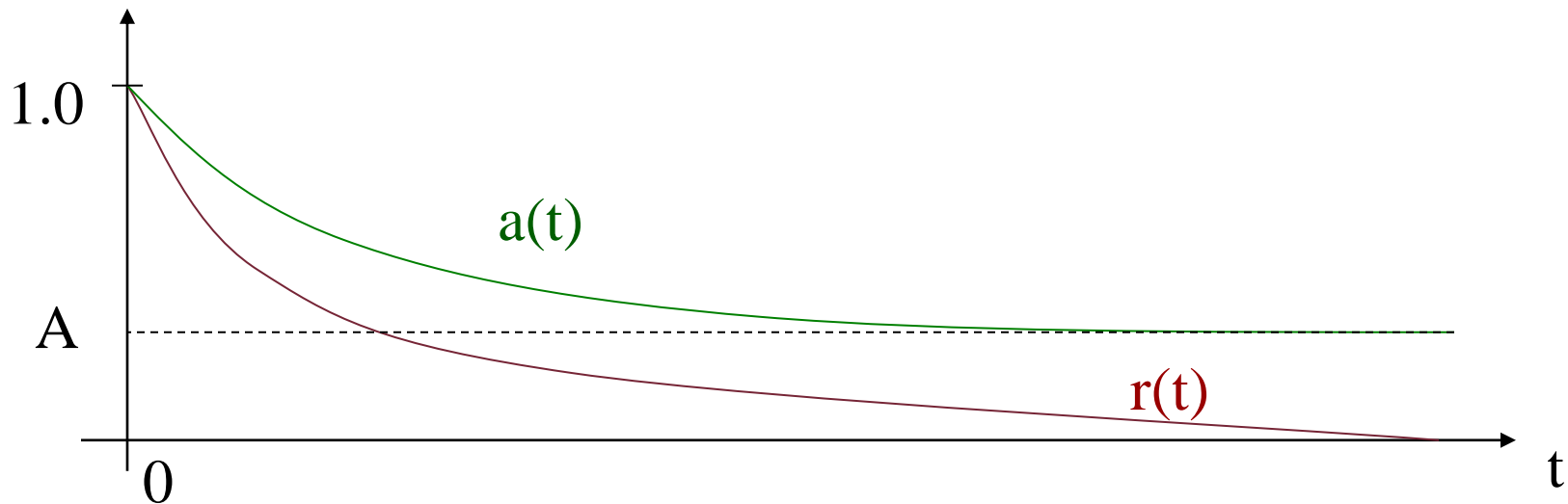
- Basis: Partitioning the states of the system
 - Correct (**U**, up) and incorrect (**D**, down) state partitions



- Mean values:
 - Mean Time to First Failure: $MTFF = E\{u_1\}$
 - Mean Up Time:
(Mean Time To Failure) $MUT = MTTF = E\{u_i\}$
 - Mean Down Time:
(Mean Time To Repair) $MDT = MTTR = E\{d_i\}$
 - Mean Time Between Failures: $MTBF = MUT + MDT$

Dependability metrics: Probability functions

- Availability: $a(t) = P\{s(t) \in U\}$
- Asymptotic availability: $A = \lim_{t \rightarrow \infty} a(t)$
$$A = \frac{MTTF}{MTTF + MTTR}$$
- Reliability: $r(t) = P\{s(t') \in U, \forall t' < t\}$



Availability related requirements

Availability	Failure period per year
99%	~ 3,5 days
99,9%	~ 9 hours
99,99% („4 nines”)	~ 1 hour
99,999% („5 nines”)	~ 5 minutes
99,9999% („6 nines”)	~ 32 sec
99,99999%	~ 3 sec

Availability of a system built up from components,

- the availability of single a component is 95%,
- all components are needed to perform the system function
- system built from 2 components: 90%
- system built from 5 components : 77%
- system built from 10 components : 60%

Attributes of components

- **Fault rate:** $\lambda(t)$

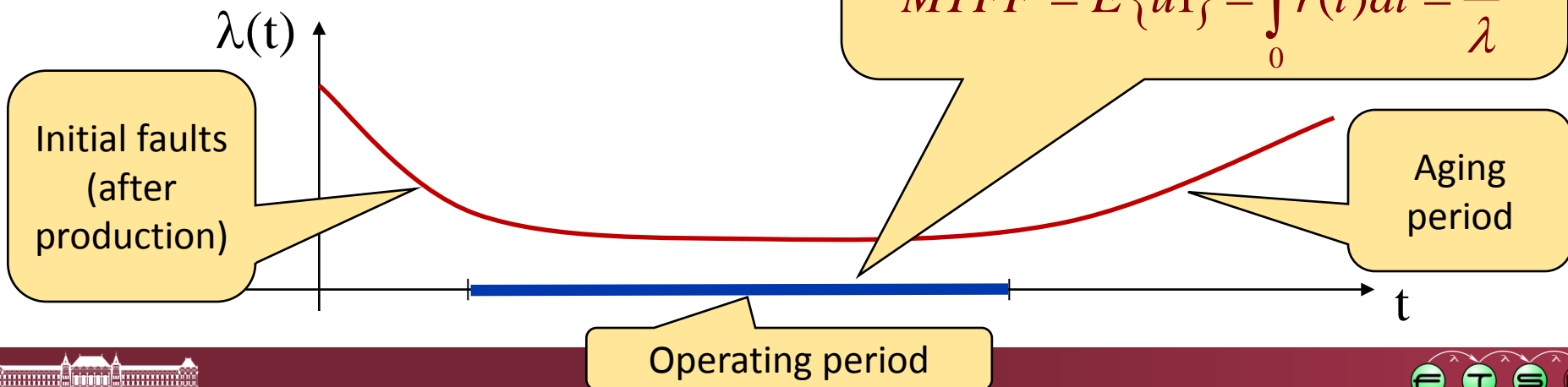
Probability that the component will fail at time point t given that it has been correct until t

$$\lambda(t)\Delta t = P\{s(t+\Delta t) \in D \mid s(t) \in U\} \text{ while } \Delta t \rightarrow 0$$

- Reliability of a component on the basis of this definition:

$$r(t) = e^{-\int_0^t \lambda(t) dt}$$

- For electronic components:



Analysis techniques

■ Qualitative analysis techniques:

- **Fault effects analysis:** What are the **component level failures** (failure modes), that cause **system level failure**?
 - Identification of single points of failure
- **Techniques:** Systematic causes and effects analysis
 - Fault tree analysis (FTA), Event tree analysis (ETA), Cause-consequence analysis (CCA), Failure modes and effects analysis (FMEA)

■ Quantitative analysis techniques:

- **Dependability analysis:** How can the system level dependability be calculated on the basis of component level fault properties?
 - System level reliability, availability, ...
- **Techniques:** Construction and solution of dependability models
 - Reliability block diagrams (RBD)
 - Markov-chains (MC)
 - Stochastic Petri nets (SPN)

Goals of the dependability analysis

- On the basis of **component characteristics**
 - fault rate (continuous operation), FIT: 10^{-9} faults/hour
 - fault probability (on-demand operation)
 - reliability function

calculation of **system level** characteristics

- reliability function
- availability function
- asymptotic availability
- MTFF
- safety

Calculations are based on the system architecture and the failure modes

Using the results of the analysis

- Design: **Comparison of alternative** architectures
 - Having the same components, which architecture guarantees better dependability attributes?
- Design, maintenance: **Sensitivity analysis**
 - What are the effects of selecting another component?
 - Which components have to be changed in case of inappropriate attributes?
 - Which component characteristics have to be investigated in more detail? → Fault injection and measurements
- Handover: **Justification of dependability attributes**
 - Approval and startup of services
 - Certification (for safety critical systems)

Combinational models for dependability analysis

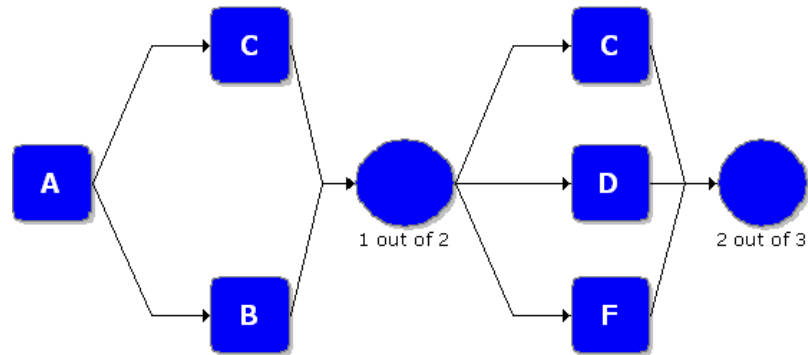


Table of Contents

- Attributes of dependability
 - Reliability, availability
 - Safety, integrity, maintainability
- **Combinational models for dependability analysis**
 - **Reliability block diagrams**
- Stochastic modeling of system dependability
 - Markov models (CTMC)
 - Stochastic Petri-nets

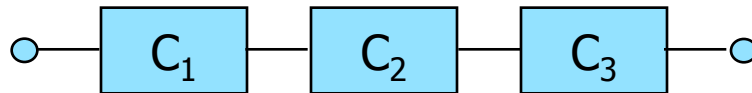
Boole models for calculating dependability

- Two states of components: **Fault-free** or **faulty**
- There are no dependences among the components
 - Neither from the point of view of faults
 - Nor from the point of view of repairs
- **Interconnection of components** from the point of view of dependability: What kind of redundancy is used?
 - **Serial connection**: The components are **not redundant**
 - If both components are necessary for the system operation
 - **Parallel connection**: The components are **redundant**
 - If the components may replace each other

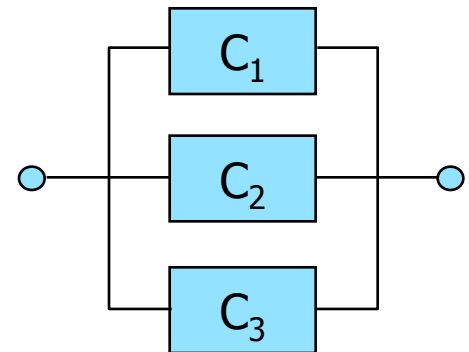
Reliability block diagram

- **Blocks:** Components (failure modes)
- **Connection:** Serial or parallel connection
- **Paths:** Operation system configurations
 - The system is **operational** (correct) if **there is a path** from the start point to the end point of the diagram through fault-free components

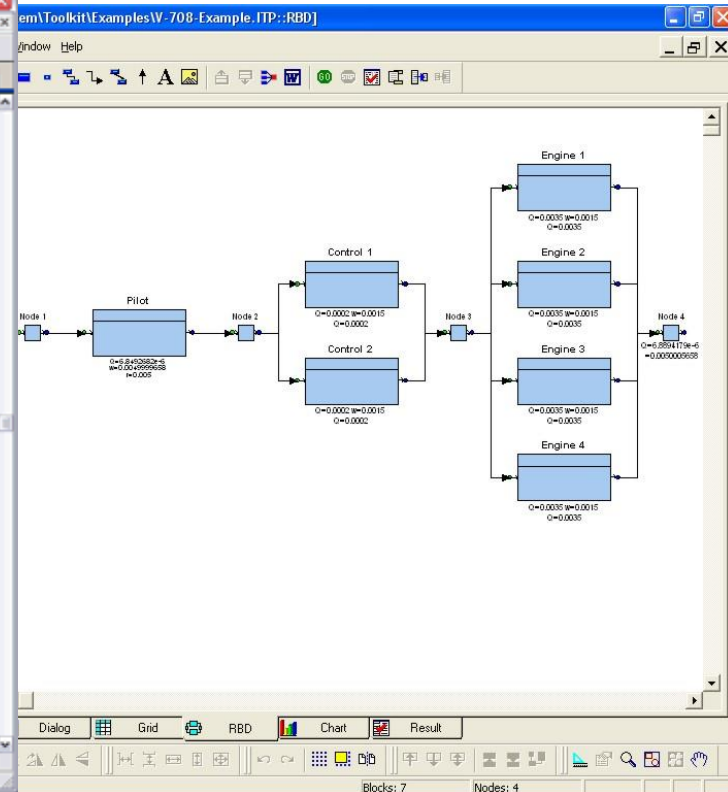
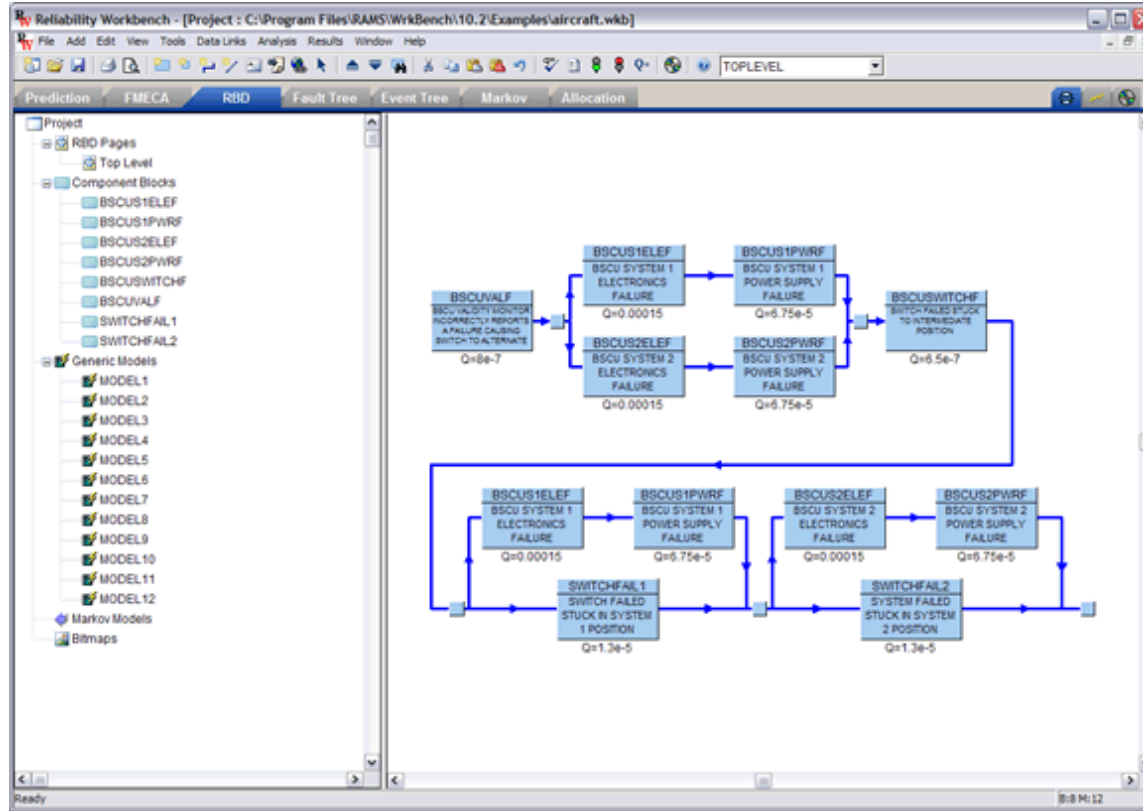
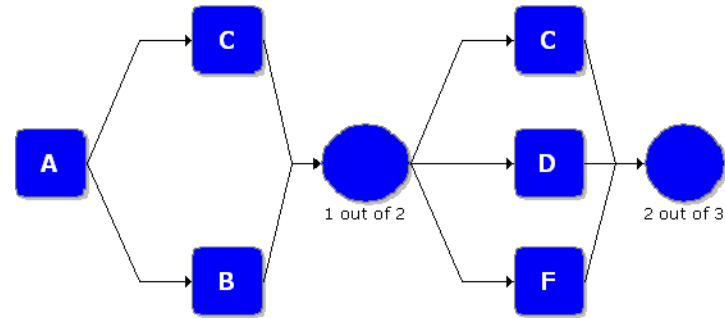
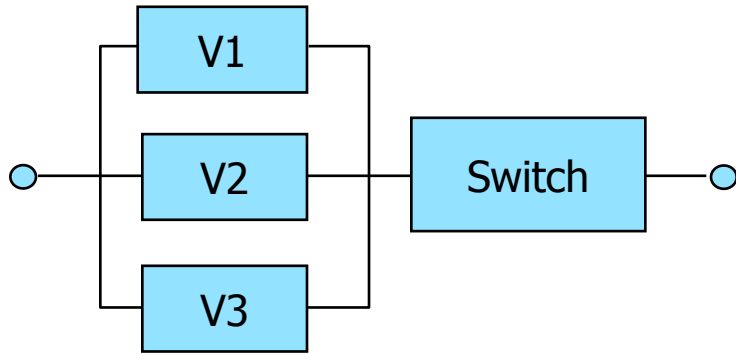
Serial:



Parallel:

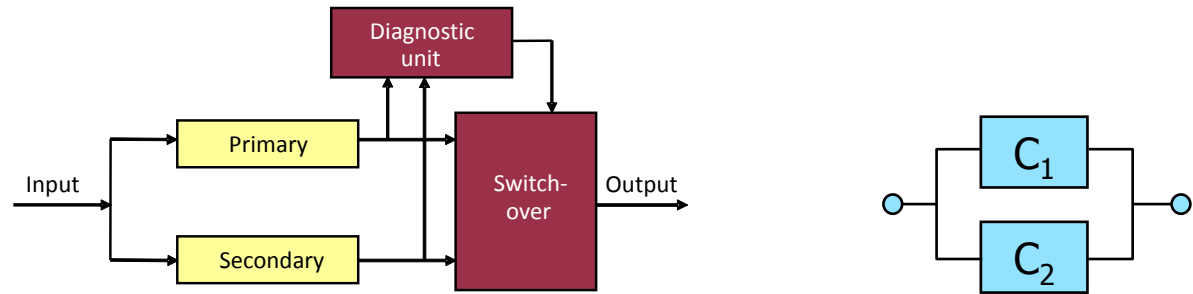


Reliability block diagram examples

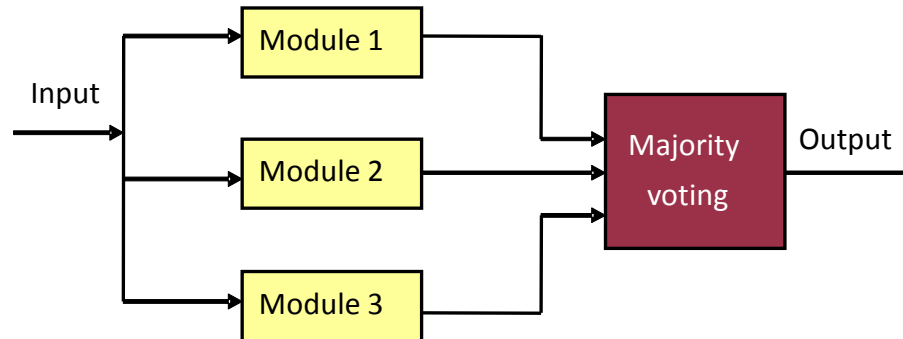


Overview: Typical system configurations

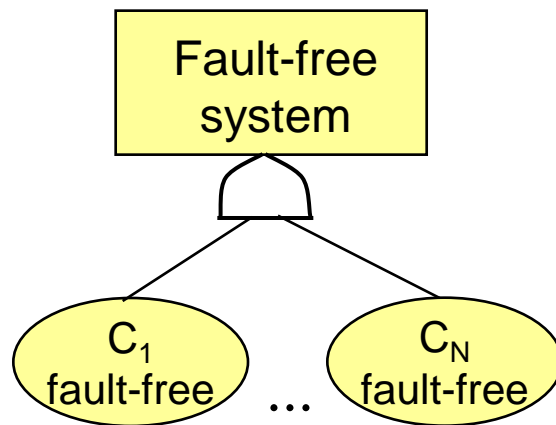
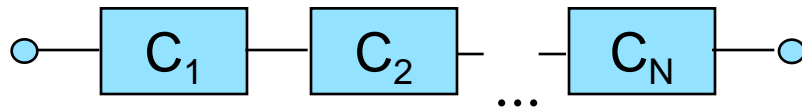
- Serial system model: **no redundancy**
- Parallel system model: **redundancy** (replication)



- Complex canonical system: redundant subsystems
- M faulty out of N components: **Majority voting** (TMR)



Serial system model



$P(A \wedge B) = P(A) \cdot P(B)$
If independent

- Reliability for N components:

$$r_R(t) = \prod_{i=1}^N r_i(t)$$

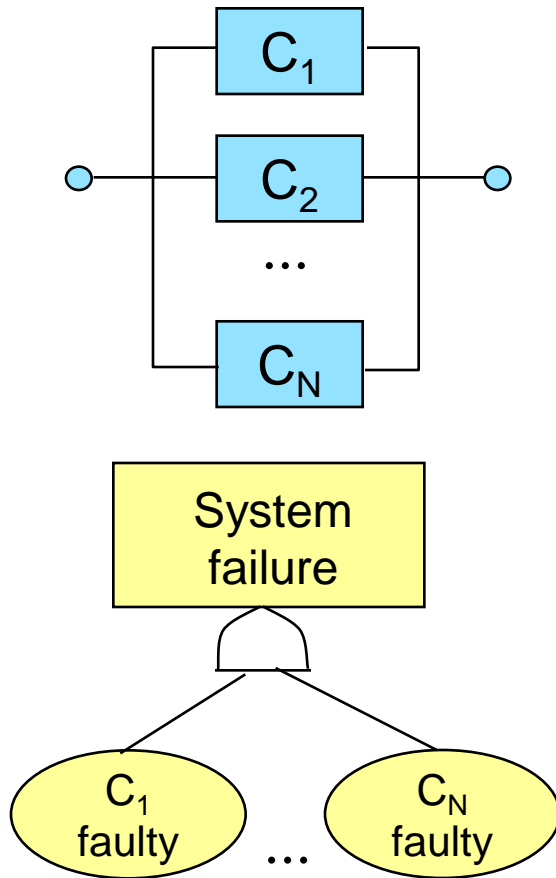
System reliability

Components' reliability

- MTFF:

$$MTFF = \frac{1}{\sum_{i=1}^N \lambda_i}$$

Parallel system model



$P(A \wedge B) = P(A) \cdot P(B)$
if independent

- Reliability:

$$1 - r_R(t) = \prod_{i=1}^N (1 - r_i(t))$$

- Identical N components:

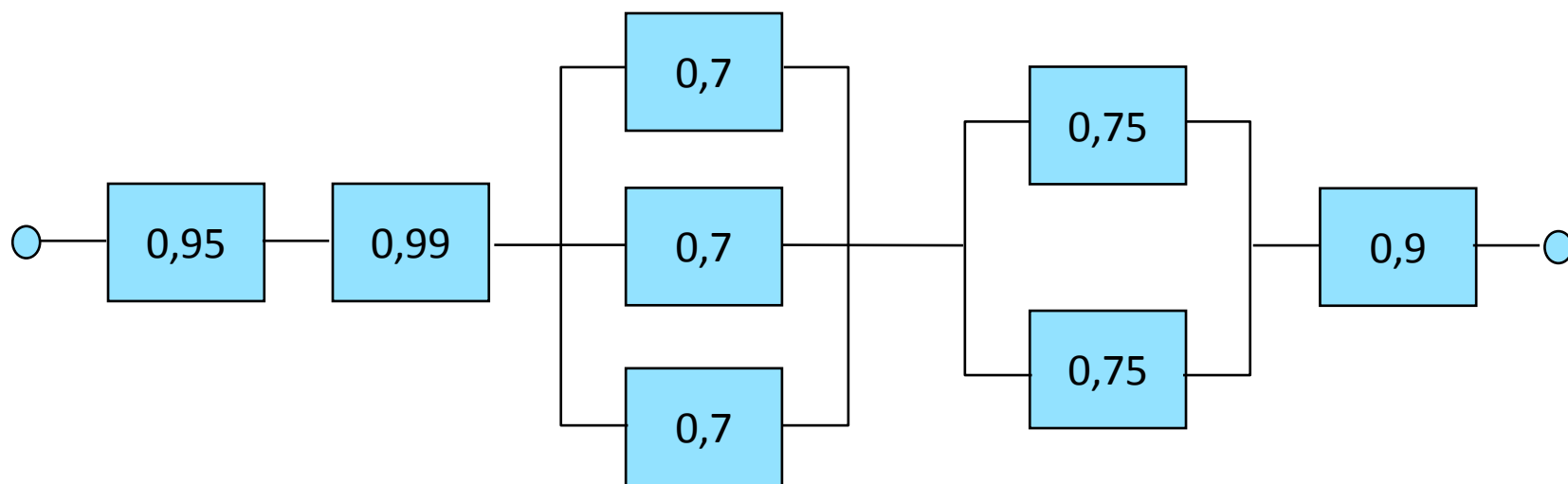
$$r_R(t) = 1 - (1 - r_C(t))^N$$

- MTFF:

$$MTFF = \frac{1}{\lambda} \sum_{i=1}^N \frac{1}{i}$$

Complex canonical system

- Calculation on the basis of parts with basic connections
 - Example: Calculation of asymptotic availability



$$K_R = 0,95 \cdot 0,99 \cdot \left[1 - (1 - 0,7)^3 \right] \cdot \left[1 - (1 - 0,75)^2 \right] \cdot 0,9$$

M faulty out of N components

- **N** replicated components;

If **M** or more components faulty: the system is faulty

$$r_R = \sum_{i=0}^{M-1} P \{ \text{"there are } i \text{ faulty components"} \}$$

$$r_R = \sum_{i=0}^{M-1} \binom{N}{i} (1-r)^i \cdot r^{N-i}$$

- Application: Majority voting (TMR): N=3, M=2

$$r_R = \sum_{i=0}^1 \binom{3}{i} (1-r)^i \cdot r^{3-i} = \binom{3}{0} (1-r)^0 \cdot r^3 + \binom{3}{1} (1-r)^1 \cdot r^2 = 3r^2 - 2r^3$$

$$MTFF = \int_0^{\infty} r_R(t) dt = \int_0^{\infty} (3r^2 - 2r^3) dt = \frac{5}{6} \cdot \frac{1}{\lambda}$$

Less than in case of a single component!

Cold redundant system

- A new component is switched on to replace a faulty component:

$$MTFF = \sum_{i=1}^N MTFF_i$$

- In case of uniform replicated components, the system reliability function:

$$r_R(t) = \sum_{i=0}^{N-1} \frac{(\lambda t)^i}{i!} e^{-\lambda t}$$

A SCADA system consists of the following components:

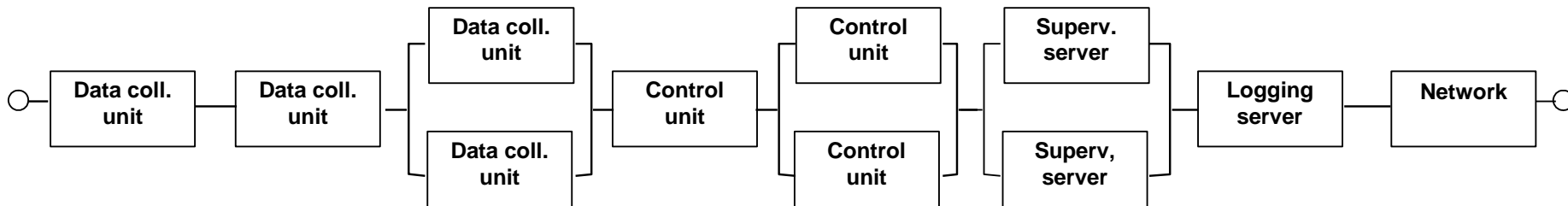
4 data collector units, 3 control units, 2 supervisory servers, 1 logging server and the corresponding network

- The 2 supervisory servers are in a hot redundancy structure.
- 2 data collector units and 2 control units are hot redundant units
- The reliability data of the system components are given as follows (measured in hours, with independent repairs in case of faults):

	Data coll. unit	Control unit	Superv.. server	Logging server	Network
MTTF	9000	12000	4500	2000	30000
MTTR	2	3	5	1	2

- Evaluate the system level availability using a reliability block diagram.
- Compute the asymptotic availability of the system using the above given parameters of the system components.
- How many hours is the system out of service per year?

Reliability block diagram:



Component level asymptotic availability: $K = \text{MTTF} / (\text{MTTF} + \text{MTTR})$

	Data coll. unit (D)	Control unit (C)	Superv. server (S)	Logging server (L)	Network (N)
MTTF	9000	12000	4500	2000	30000
MTTR	2	3	5	1	2
K	KD=0.99977	KC=0.99975	KS=0.99889	KL=0.9995	KN=0.99993

System level asymptotic availability:

$$KD * KD * (1 - (1 - KD) * (1 - KD)) * KC * (1 - (1 - KC) * (1 - KC)) * (1 - (1 - KS) * (1 - KS)) * KL * KN = 0.9987362$$

Approx. 11 hours out of service per year

Component reliability data

- Component level **reliability data** are available in handbooks
 - **MIL-HDBK-217**: The Military Handbook Reliability Prediction of Electronic Equipment (for military applications. pessimistic)
 - **Telcordia SR-332**: Reliability Prediction Procedure for Electronic Equipment (for telco applications)
 - **IEC TR 62380**: Reliability Data Handbook - Universal Model for Reliability Prediction of Electronic Components, PCBs, and Equipment (less pessimistic, supporting new component types)
- **Dependencies** of component level reliability data:
 - Temperature, weather conditions, shocking (e.g., in vehicles), height, ...
 - Operational profiles
 - Ground; stationary; weather protected (e.g., in rooms)
 - Ground; non stationary; moderate (e.g., in vehicles)
- **Computations**: hierarchic approach (with redundancy schemes)
 - Component → Module → Subsystem → System

Tool example: The ALD MTBF Calculator

MTBF Calculator by ALD

Perform reliability prediction and MTBF/FR calculation for electronic and mechanical components in 5 simple steps:

1. Select Component Family and Type

Family: **ELECTRONIC**
MECHANICAL

Item Code: **IC-Memory**
IC-Analog
IC-Digital
Bubble Memory
Resistor
Potentiometer
Capacitor
Switch
Relay
Connector
LF Diode
LF Transistor
HF Diode
HF Transistor

2. Select Reliability Prediction Method

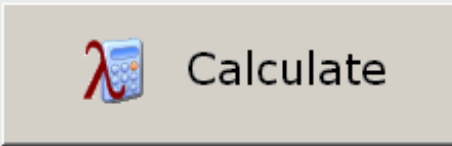
CNET RDF93 rev 02/95
FIDES
GJB/Z 299B Part count
GJB/Z 299B Part stress
HDBK-217Plus
HRD5 TELECOMM
IEC 62380
ITALTEL IRPH93
NPRD-95
Telcordia Issue 1
Telcordia Issue 2

3. Select Environment and Temperature

Mission profile: **GB Switching**


Temperature: **25** degrees Centigrade

4. Enter Component Parameters

 Calculate

5. Get MTBF and FR

MTBF: 0.0 hours
Failure Rate: 0.0 failures per million hours
Failure Rate: 0.0 FIT

 ALD MTBF Calculator is a free tool suitable for simple reliability prediction of single components. If you need professional Reliability Tool for reliability engineering of complex systems, including product tree building, Reliability Block Diagrams, Reports, Report Generator, Pareto Analysis, Temperature Curve, Fault Tree Analysis, FMEA/FMECA, Safety Module, Derating Module and much more - please check our RAM Commander Software. You may download its evaluation version for free from our website. Copyright ALD Ltd. 2009 support@ald.co.il www.aldservice.com

Tool example: The ALD MTBF Calculator

MTBF Calculator by ALD

Perform reliability prediction and MTBF/FR calculation

1. Select Component Family and Type

Family: **ELECTRONIC**
MECHANICAL

Item Code:
IC-Memory
IC-Analog
IC-Digital
Bubble Memory
Resistor
Potentiometer
Capacitor
Switch
Relay
Connector
LF Diode
LF Transistor
HF Diode
HF Transistor

IC Digital IEC 62380

Ref. des.: QTY: MP:

Part name: Temp: °C

Mil. num.:

Cat. num.:

Generic name:

Type: Package:

Subtype(GaAs): # of Pins:

Tech: Substrate Material:

of gates: Interface Circuits:

Year of manufacturing:

T junction: or

Delta Tjc:

REF 54HC00 54HC08 54HC36 54F280 68000 80386

Component Parameters

Calculate

MTBF and FR

<input type="text" value="0.0"/>	hours
<input type="text" value="0.0"/>	failures per million hours
<input type="text" value="0.0"/>	FIT

Close

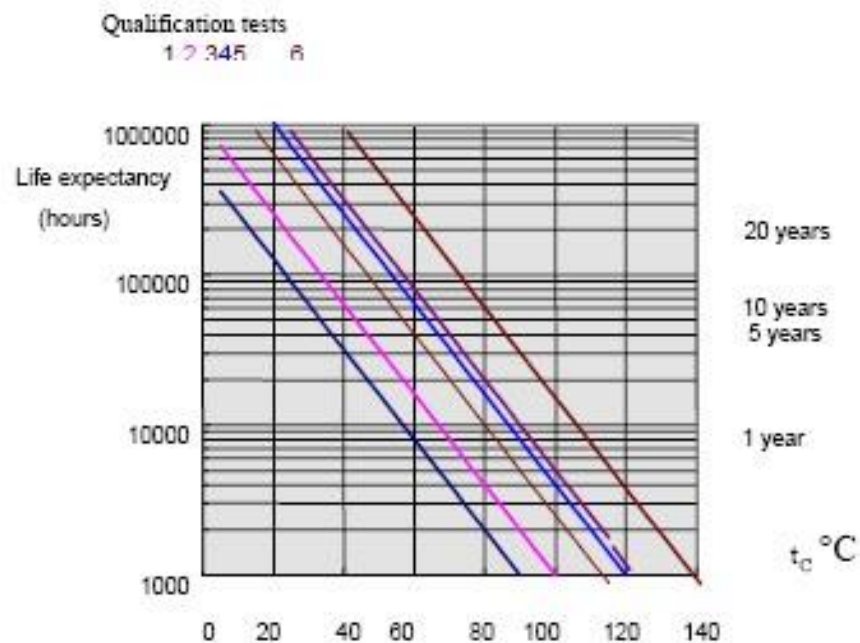
ALD MTBF Calculator is a free tool suitable for simple reliability prediction of single components.
If you need professional Reliability Tool for reliability engineering of complex systems, including product tree building, Reliability Block Diagrams, Reports, Report Generator, Pareto Analysis, Temperature Curve, Fault Tree Analysis, FMEA/FMECA, Safety Module, Derating Module and much more - please check our RAM Commander Software. You may download its evaluation version for free from our website.
Copyright ALD Ltd. 2009 support@ald.co.il www.aldservice.com

Example: Reliability of a module (serial system)

Component name	Type	Additional data	IEC 62380 reference	Failure rate	Quantity
Panduit D461612	Connector	Rectangular	Default value	0,003625	1
Panduit D461612	Connector	Rectangular	Default value	0,007200	1
74AHCT14	IC-Digital	Standard	Substituted with - SN74AHCT14D	0,014200	3
74HC/HCT540	IC-Digital	Standard	Substituted with - CD74HC540E	0,019000	2
74HC/HCT541	IC-Digital	Standard	Substituted with - SN74AHCT541DW	0,014000	3
PALCE16V8	IC-Digital	PAL	Exact matching	0,036000	1
HMA124	Optoelectronic	Optocoupler	Default value	0,011600	16
MB6S	IC-Digital	Standard	Default value	0,012700	16
Resistor	Resistor	General purpose	Default value	0,000232	32
Resistor	Resistor	Fixed, high dissipation film	Default value	0,001047	32
Capacitor	Capacitor	Tantalum - solid electrolyte	Default value	0,000725	17
Capacitor	Capacitor	Ceramic class II.	Default value	0,000223	41
SMD led	Optoelectronic	Solid State Lamp	Default value	0,002000	16
U22-DI016-C3	PWB		Default value	0,003403	1
SOD80 BZV55C	LF Diode	Zener	Default value	0,011500	64
Module:	1,392021 failure per million hours				

Estimation of life expectancy

- What is the **lifetime** of electronic components?
 - When does the fault rate start increasing?
 - At this time **scheduled maintenance** (change) is required
- IEC 62380: „Life expectancy”
- Especially limited: In case of electrolyte capacitors
 - Depends on temperature
 - Depends on qualification
 - Example: ~ 100 000 hours (~ 11 years)



Markov models for dependability analysis

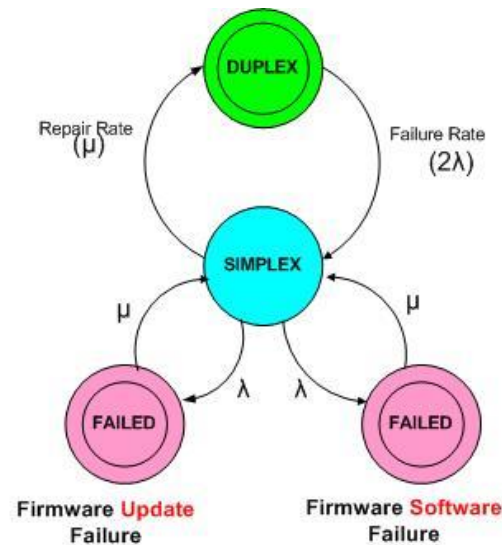


Table of Contents

- Attributes of dependability
 - Reliability, availability
 - Safety, integrity, maintainability
- Combinational models for dependability analysis
 - Reliability block diagrams
- **Stochastic modeling of system dependability**
 - **Markov models (CTMC)**
 - Stochastic Petri-nets

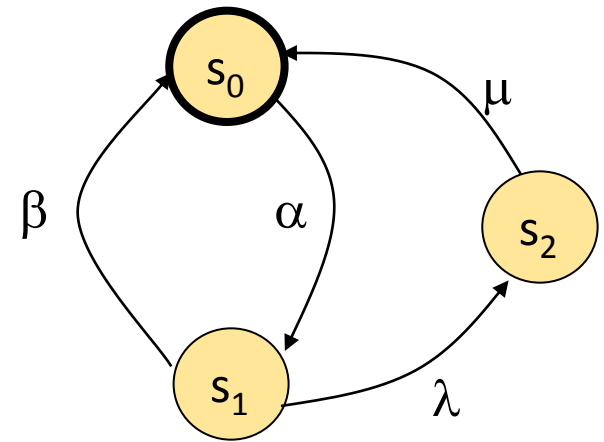
Model: Continuous Time Markov Chain

■ Definition: CTMC = (S , \underline{R})

- S set of discrete states:

$$s_0, s_1, \dots, s_n$$

- $\underline{R}: S \times S \rightarrow \mathbb{R}_{\geq 0}$ state transition rates



■ Notation:

- Rate of leaving a state: $E(s) = \sum_{s' \in S, s' \neq s} R_{s,s'}$

- $\underline{Q} = \underline{R} - \text{diag}(E)$ infinitesimal generator matrix

- $\sigma = s_0, t_0, s_1, t_1, \dots$ path (s_i is left at t_i)

- $\sigma @ t$ the state at time t

- $\text{Path}(s)$ set of paths from s

Solution of a CTMC

■ Transient state probabilities:

- $\pi(s_0, s, t) = P\{\sigma \in \text{Path}(s_0) \mid \sigma @ t = s\}$ probability that starting from s_0 the system is in state s at time t
- $\underline{\pi}(s_0, t)$ starting from s_0 , the probabilities of the states at t
- CTMC transient solution:

$$\frac{d \underline{\pi}(s_0, t)}{dt} = \underline{\pi}(s_0, t) \underline{Q}$$

$$P\{\text{being in } s \text{ for } t\} = e^{-E(s)t}$$
$$E\{\text{time spent in } s\} = \frac{1}{E(s)}$$

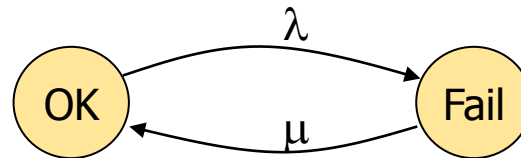
■ Steady state probabilities:

- $\pi(s_0, s) = \lim_{t \rightarrow \infty} \pi(s_0, s, t)$ state probabilities (starting from s_0)
- $\underline{\pi}(s_0)$ state probabilities (vector)
- CTMC steady state solution:

$$\underline{\pi}(s_0) \underline{Q} = 0 \quad \text{where} \quad \sum_s \pi(s_0, s) = 1$$

CTMC dependability model

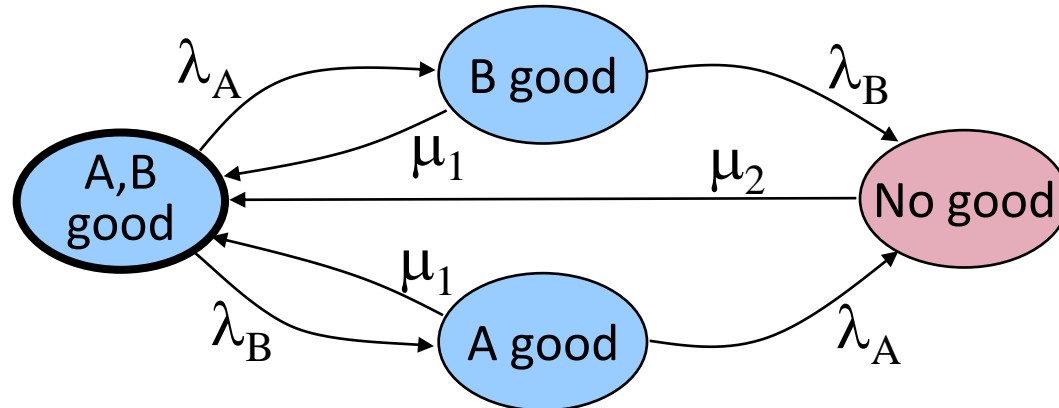
- CTMC states
 - **System level states:** Combination of component states (fault-free, or faulty according to a failure mode)
- CTMC transitions
 - **Component level fault occurrence:**
Rate of the transition is the component **fault rate** (λ)
 - **Component level repair:**
Rate of the transition is the component **repair rate** (μ), which is the reciprocal of the repair time



- **System level repair:**
Rate of the transition is the system repair rate (which is the reciprocal of the system repair time)

Example: CTMC dependability model

- System consisting of two servers, A and B:
 - The servers may independently fail
 - The servers can be repaired independently or together
- System states: Combination of the server states (good/faulty)
- Transition rates:
 - Fault of server A: λ_A failure rate
 - Fault of server B: λ_B failure rate
 - Repair of a server: μ_1 repair rate
 - Repair of both servers: μ_2 repair rate



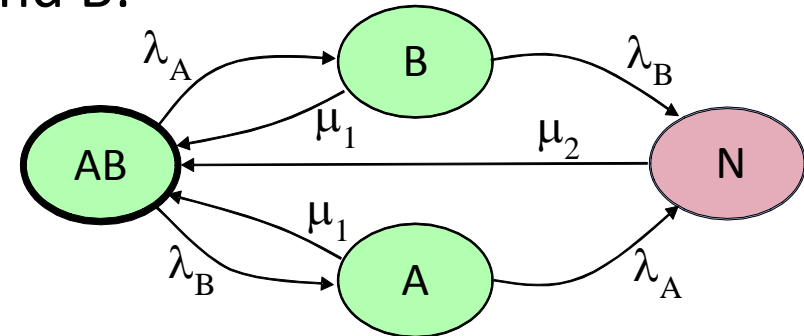
Computation of system level attributes

- Identifying state partitions
 - System level “up” state partition **U** and “down” partition **D**
- Solution of the CTMC model:
 - Transient solution: $\pi(s_0, s, t)$ time functions
 - Steady state solution: $\pi(s_0, s)$ probabilities
- Availability:
$$a(t) = \sum_{s_i \in U} \pi(s_0, s_i, t)$$
- Asymptotic availability:
$$A = \sum_{s_i \in U} \pi(s_0, s_i)$$
- Reliability:
$$r(t) = \sum_{s_i \in U} \pi(s_0, s_i, t)$$
 - Here: Before the solution the model shall be modified: state transitions from partition **D** to **U** shall be deleted

Example: CTMC dependability model

- System consisting of two servers, A and B:

- The servers may independently fail
- The servers can be repaired independently of together



- State partitions:

- $U = \{s_{AB}, s_A, s_B\}, \quad s_0 = s_{AB}$
- $D = \{s_N\}$

- Availability:**

$$a(t) = \pi(s_0, s_{AB}, t) + \pi(s_0, s_A, t) + \pi(s_0, s_B, t)$$

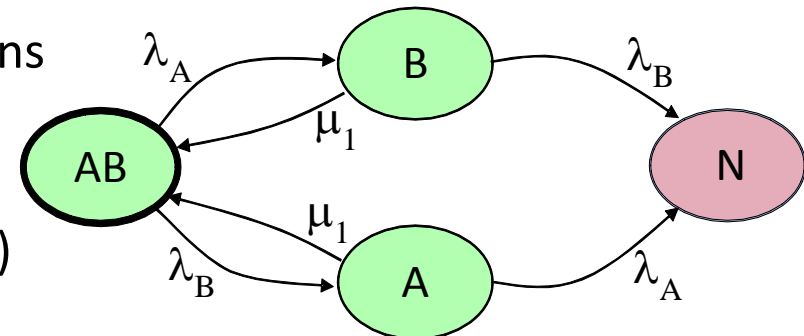
- Asymptotic availability:**

$$K = A = \pi(s_0, s_{AB}) + \pi(s_0, s_A) + \pi(s_0, s_B)$$

- Reliability:**

- Modifying the model: Deleting transitions from $D = \{s_N\}$ partition to U
- Solution of the modified model:

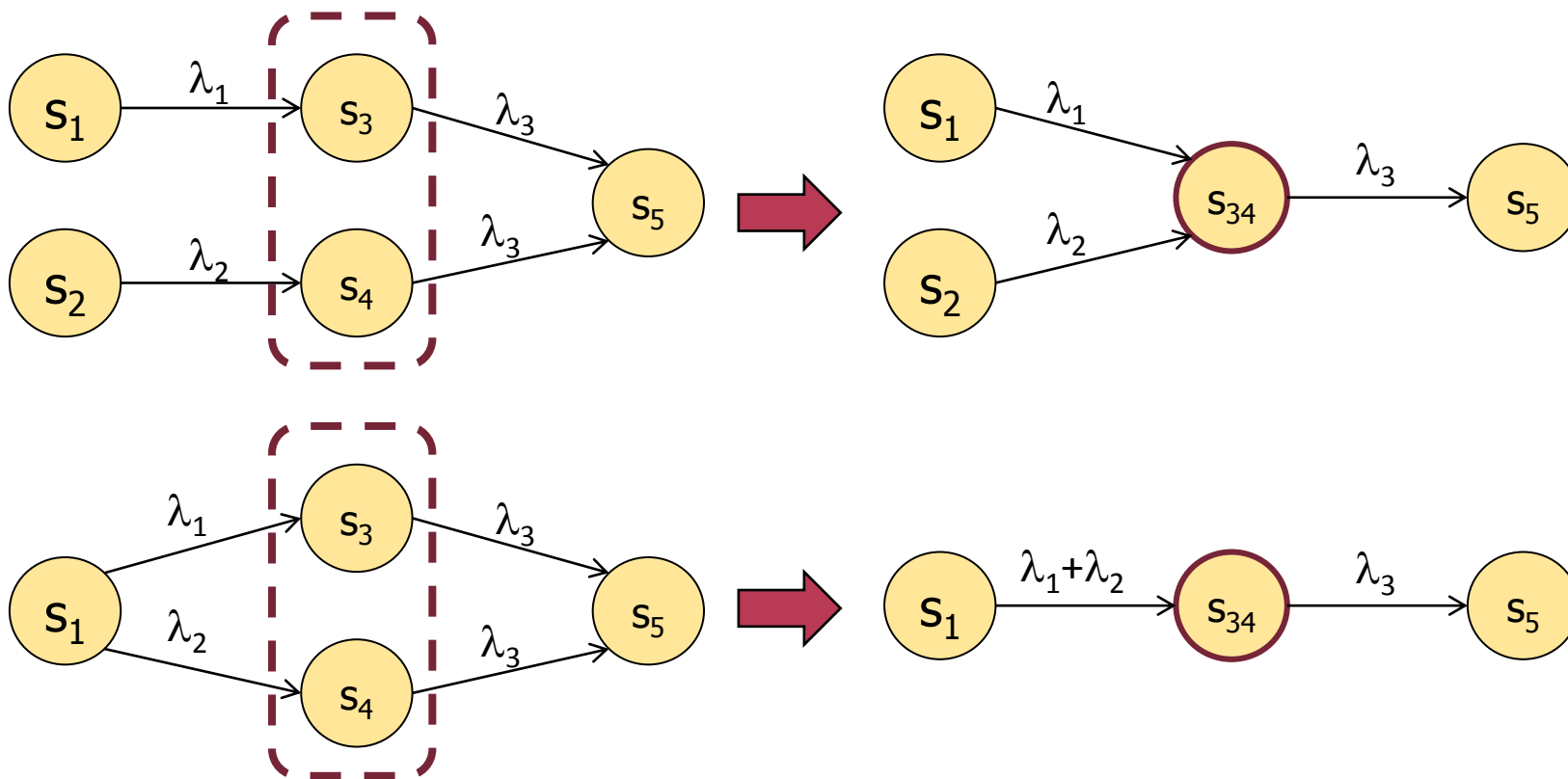
$$r(t) = \pi(s_0, s_{AB}, t) + \pi(s_0, s_A, t) + \pi(s_0, s_B, t)$$



Reducing CTMC models

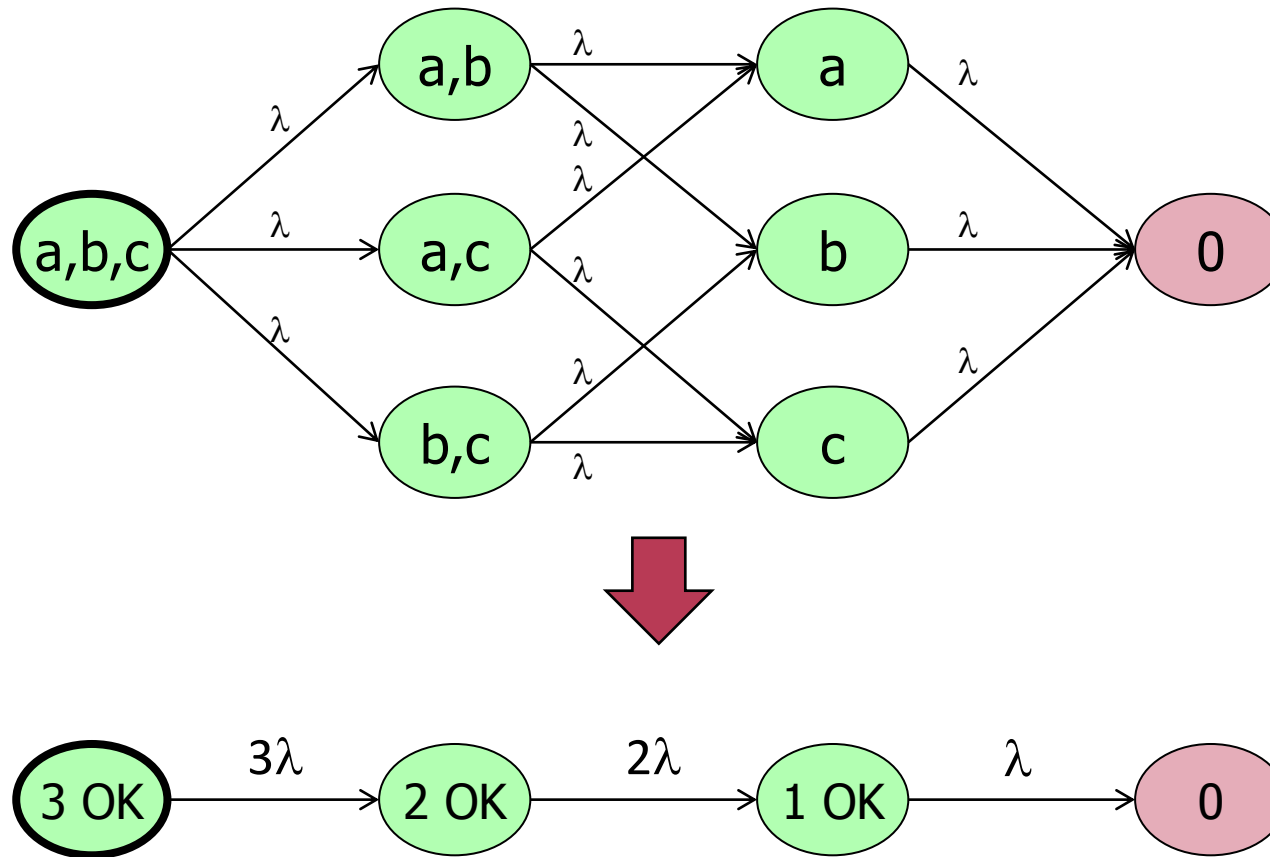
■ Merging states

- Condition: Transitions to the same states with the same rates (outgoing transitions and rates do not distinguish the states)
- After merging, the outgoing rate and the incoming rates remain the same (from the same state: incoming rates are summarized)



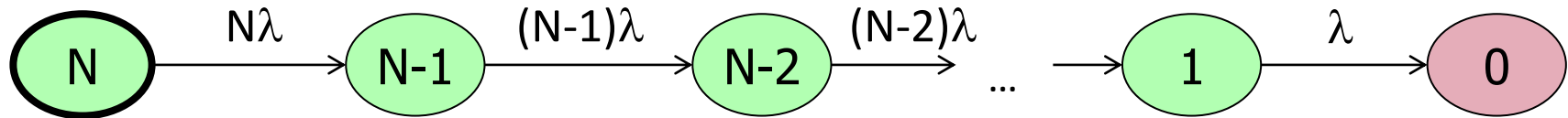
Example: Merging states

- Model: 3 redundant (replicated) components
- The components (a, b, c) have the same fault rate λ



CTMC dependability models (1)

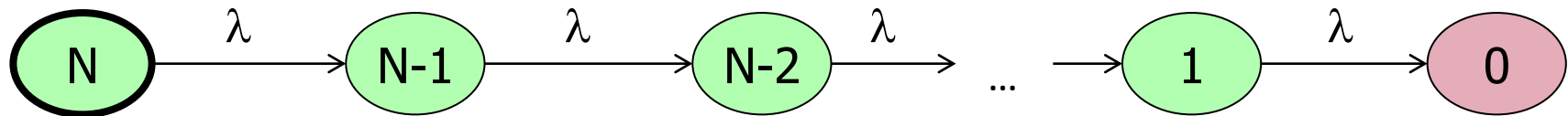
- Hot redundancy, N components:



- Computing MTTF in case of hot redundancy

- Time spent in state where k components are good: $\frac{1}{k\lambda}$

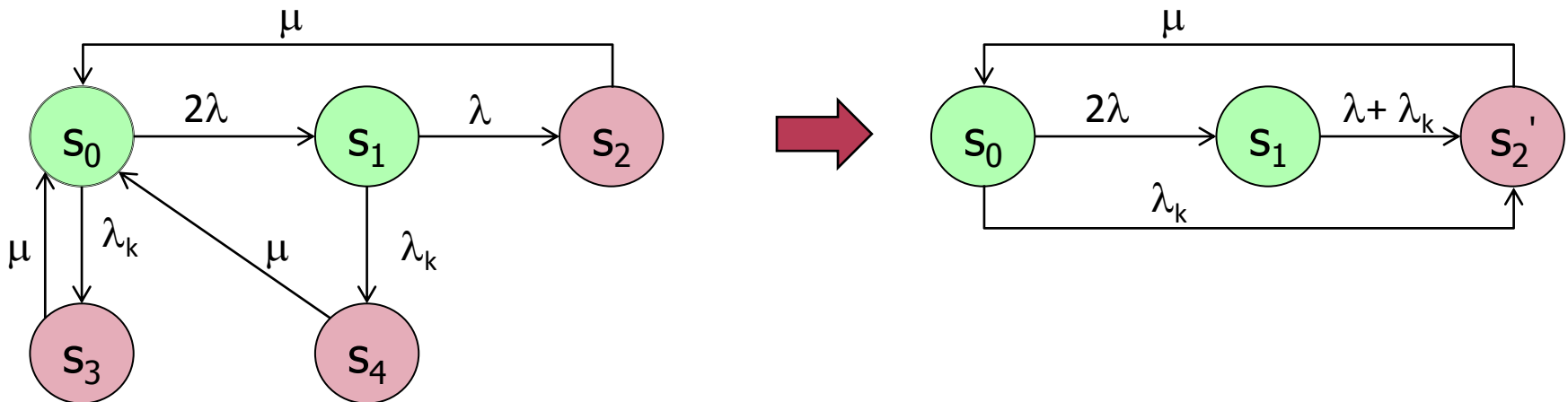
- Cold redundancy, N components:



CTMC dependability models (2)

■ Active redundancy

- 2 components, each with λ failure rate
- Switch between components, with λ_k failure rate
- In case of a fault complete repair, with μ repair rate



Tools for dependability analysis

For both combinational dependability models

- Fault tree,
- Event tree,
- Reliability block diagram,
- FME(C)A, ...

and Markov chains:

- Relex 2009 (www.relex.com)
- Item Toolkit (www.itemuk.com)
- RAM Commander, ... (www.aldservice.com)
- Functional Safety Suite

Stochastic Petri nets for dependability analysis

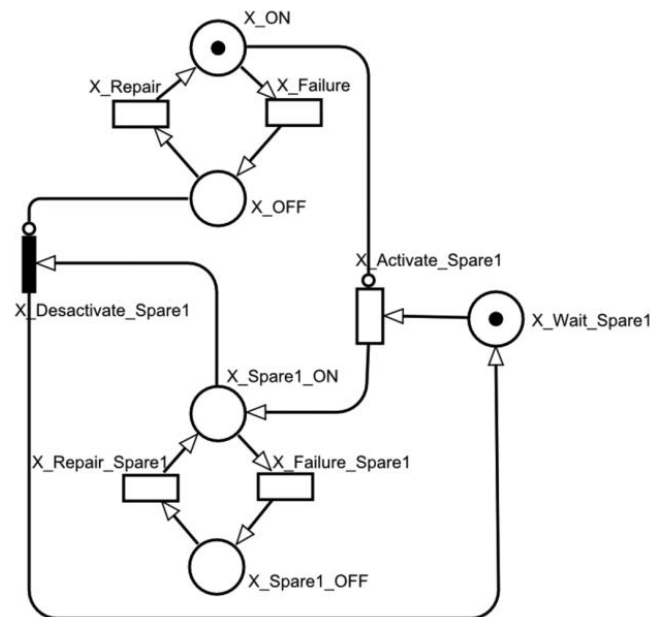


Table of Contents

- Attributes of dependability
 - Reliability, availability
 - Safety, integrity, maintainability
- Combinational models for dependability analysis
 - Reliability block diagrams
- **Stochastic modeling of system dependability**
 - Markov models (CTMC)
 - **Stochastic Petri-nets**

Model: Stochastic Petri-nets (SPN)

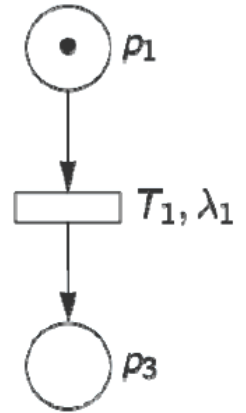
- SPN: Stochastic Petri Net
- Extension of simple Petri-nets
 - Transitions have random firing delay
 - Firing delay is sampled from a negative exponential probability distribution function
- Modified semantics of firing
 - Enabled transitions: Conditions do not change
 - Firing rule: A transition may fire at $t+d$, if
 - It became enabled at time t
 - It sampled delay d from the probability distribution
 - It remained enabled in time period $[t, t+d)$

Notation

- Graphical notation:
 - Stochastic transitions are empty rectangles
 - Extra λ parameter is assigned: firing rate
- **Firing rate** as parameter of a transition:
 - In case of transition T_i : λ_i is the parameter of the **negative exponential distribution** used to sample the d_i firing delay
 - In case of a transition with λ_i parameter, for the sampled d_i firing delay:

$$P \{ d_i \leq t \} = 1 - e^{-\lambda_i t}$$

$$P \{ d_i > t \} = e^{-\lambda_i t}$$



Summary of the properties of SPNs

- The time needed to reach a new marking has **negative exponential distribution**
 - Even in the case of concurrent or conflicting transitions
- The timed reachability graph is a **CTMC**
 - Its structure is independent from the values of firing rates
 - The **solutions for CTMC** can be used for SPN analysis
- Results of the analysis:
 - **Steady state solution** (existing if the SPN is bounded and reversible):
 - Probabilities of markings (time functions or asymptotic)
 - Throughput of transitions
 - **Transient solution**:
 - Probability time functions of markings

Model: Generalized Stochastic Petri-nets

- **GSPN**: Generalized Stochastic Petri-net
- Extensions of SPN:
 - **Immediate transitions**: Used for modeling dependencies
 - Priority: > 0
 - Weight for resolution of conflicts among transitions of the same priority
 - **Timed transitions**: Used for timed events
 - Priority: 0
 - Firing rate: Parameter of the negative exponential distribution for sampling the firing delay (it may be **marking dependent**)
 - **Inhibitor arcs**
 - **Guards**: Predicates for enabling transitions
- The reachability graph is still a CTMC
 - Vanishing markings (when an immediate transition fires)
 - Tangible markings (when a timed transition fires)

Model: Other types of Petri-nets

- **DSPN: Deterministic and Stochastic Petri Net**
 - **Deterministic firing delay** (constant firing time) of transitions is also possible
 - Useful for modeling **repair time**
 - Solution of the model is easy if in each marking only a single deterministic transition is enabled
- **General timed Petri-nets (TPN)**
 - **General distribution** can be used to sample the firing delay of transitions
 - There are several policies (semantics) to re-sample the firing delay in new markings (after firing of another transition)
 - It is possible to model the **restart** or **continuation** of activities of various timing
 - In general case the reachability graph is not a CTMC: Analysis is possible by simulation or approximation

Model: Assignment of rewards

■ SRN: Stochastic Reward Net

- Reward: “Profit” or “cost” functions can be assigned to markings or firings

■ Rate reward:

- Assigned to markings, **reward/time** value is given by the function
- Example: If the server is healthy then the profit is 300 Ft/hour, otherwise the penalty is 200 Ft/hour:

```
if (m(Healthy)>0) then ra=300 otherwise ra=-200
```

- Computed: Accumulated reward (e.g., profit/penalty) integrated for a given time interval

■ Impulse reward:

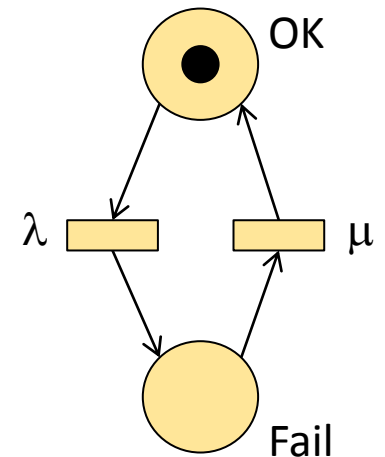
- Assigned to transitions, **reward/firing** value is given by the function
- Example: The cost of a repair is 500 Ft:

```
if (fire(Repair)) then ri=500
```

- Computed: Sum of rewards for a time interval, counting the firings

SPN (GSPN) dependability model

- Advantages in comparison with CTMC:
 - Modeling **concurrent fault occurrences** and **repair activities**
 - It is not necessary to represent system level states
- SPN places
 - **Component level states**: Healthy, faulty according to failure modes; these can be for each component separately
- SPN transitions
 - **Component level fault occurrence**: The parameter is the λ **fault rate**
 - **Component level repair**: The parameter is the μ **repair rate** (reciprocal of the repair time)
 - **System level repair** (transition between multiple places): The parameter is the **repair rate of the system state**



Computation of system attributes

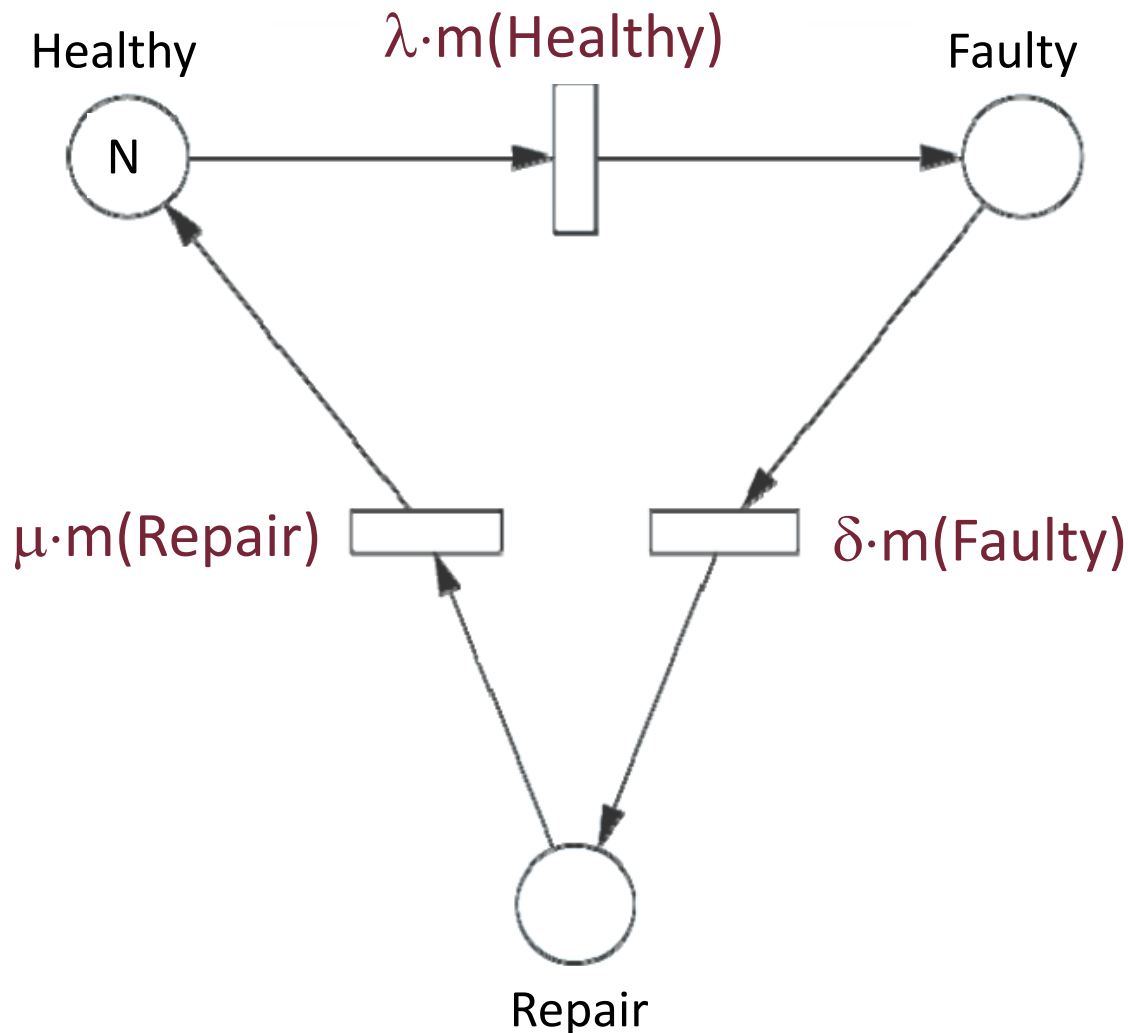
- Definition of state partitions: Based on markings
 - Normal "up" **U** and failure "down" **D** partitions
- Computation of availability
 - Direct: Probability of being in the **U** state partition
 - Reward based:
 - if $(m \in U)$ then $ra=1$ else $ra=0$
 - ra time function: availability function
 - ra expected value: asymptotic availability $A=E\{ra\}$

Example: Redundant servers

- Cluster consisting of N servers with identical fault rates
 - The cluster is “up” is at least one server is healthy
- Fault occurrences:
 - **Fault rate** of a server is λ
 - The faults of servers are independent
- Repair:
 - In case of a detected fault the repair is characterized by the **repair rate** μ (parameter of a negative exponential distribution)
 - The detection delay of faults is characterized by the **detection rate** δ (parameter of a negative exponential distribution)
 - It is possible to detect the faults and repair more servers at a time
- Model:
 - Places: **Healthy, Faulty, Repair** (marking: number of servers)
 - Transitions: Fault occurrence, detection, repair (marking dependent rates)
 - **U** state partition: $m(\text{Healthy}) > 0$
 - Availability: Probability of being in state partition **U**

Example: Redundant servers

- Compact model with marking dependent rates:



Summary

- Attributes of dependability
 - Reliability, availability:
Probability-time functions
- **Combinational** modeling: Reliability block diagram
 - Serial, parallel, majority voting structures
- **State based** modeling: Markov chain
 - Computation: Probability of state partitions
- **Concurrency based** modeling: Stochastic Petri-net
 - Computation: Probability of markings