Dependable Systems

Quantitative Evaluation (I)

Dr. Peter Tröger

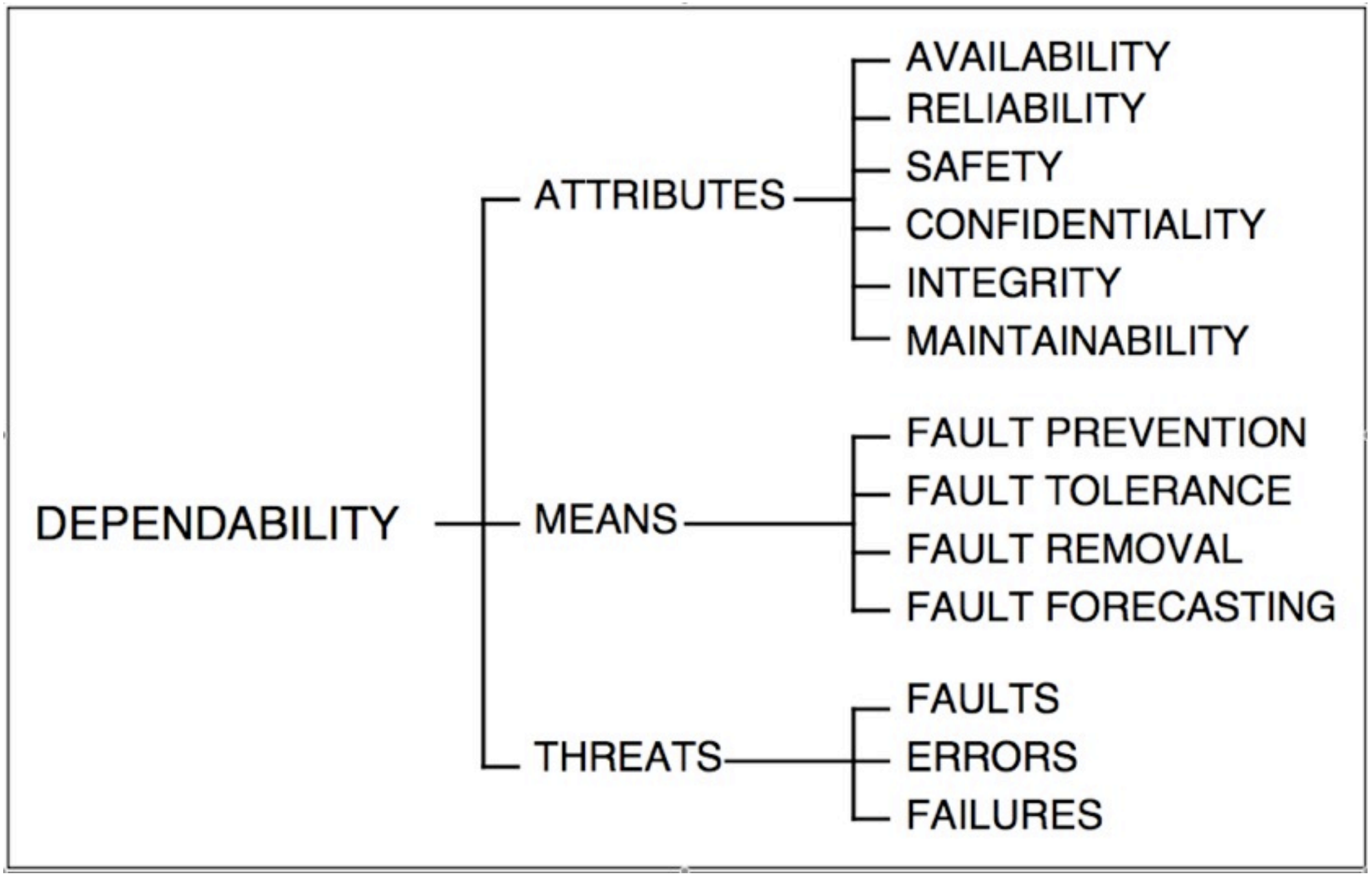
Sources:

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

Menasce, Daniel A.; Almeida, Virgilio A.: Capacity Planning for Web Services: Metrics, Models, and Methods. Prentice Hall, 2002. , 0-13-065903-7

www.fault-tree.net

Dependability Tree (Laprie)



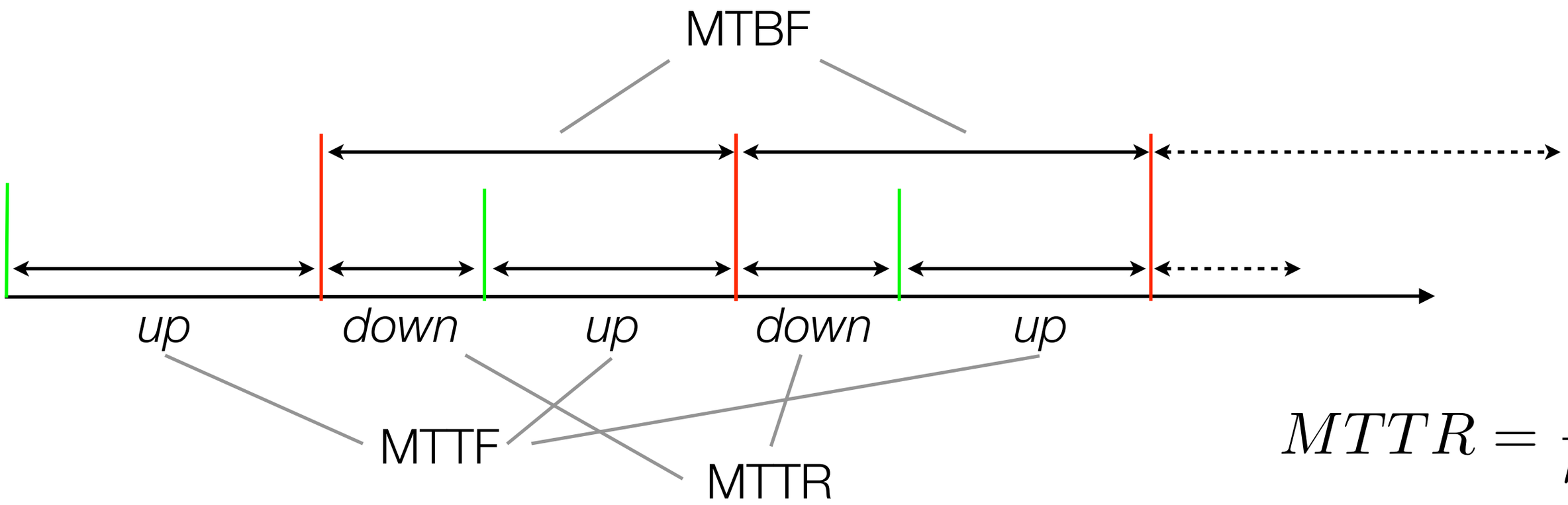
In Detail

- **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: $A_S(t) = Uptime / Lifetime$

Steady-State 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



$$MTTR = \frac{1}{\mu}$$

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

PDF & CDF

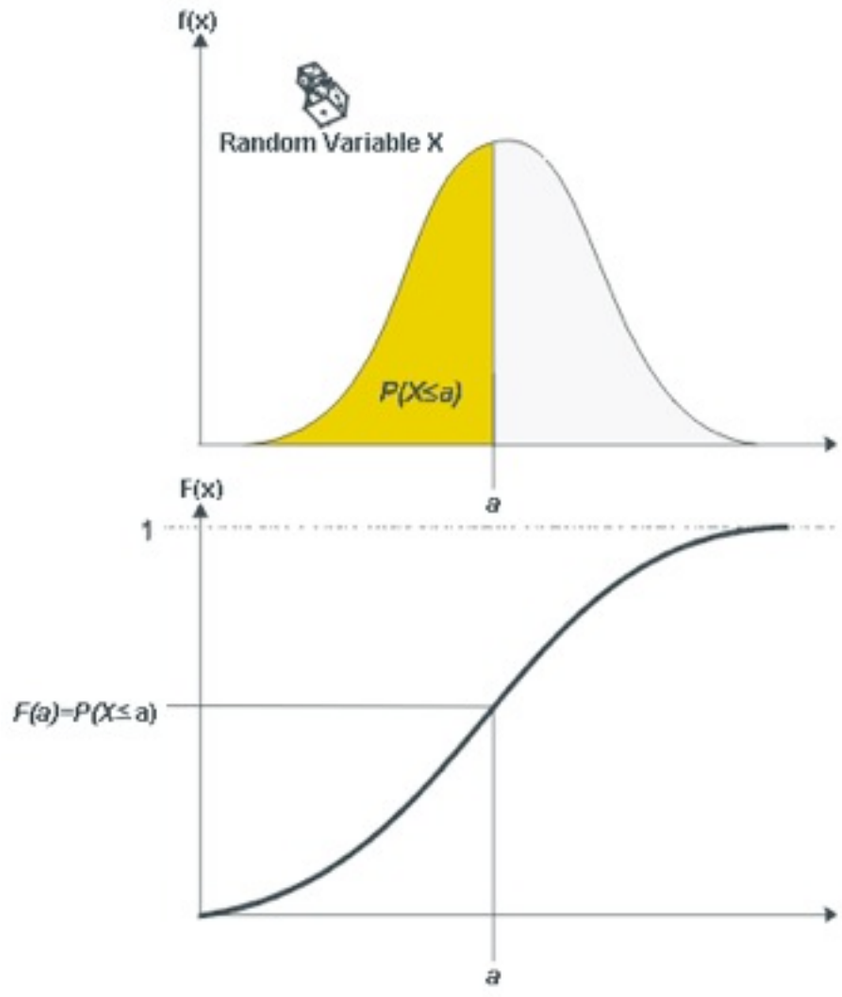
- Probability density function *pdf* for random variable *X*
  - Discrete variable: Probability that *X* will be *x*
  - Continuous variable: Probability that *X* is in *[a, b]*
    - Computed as area under the density function in this range

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

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

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

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



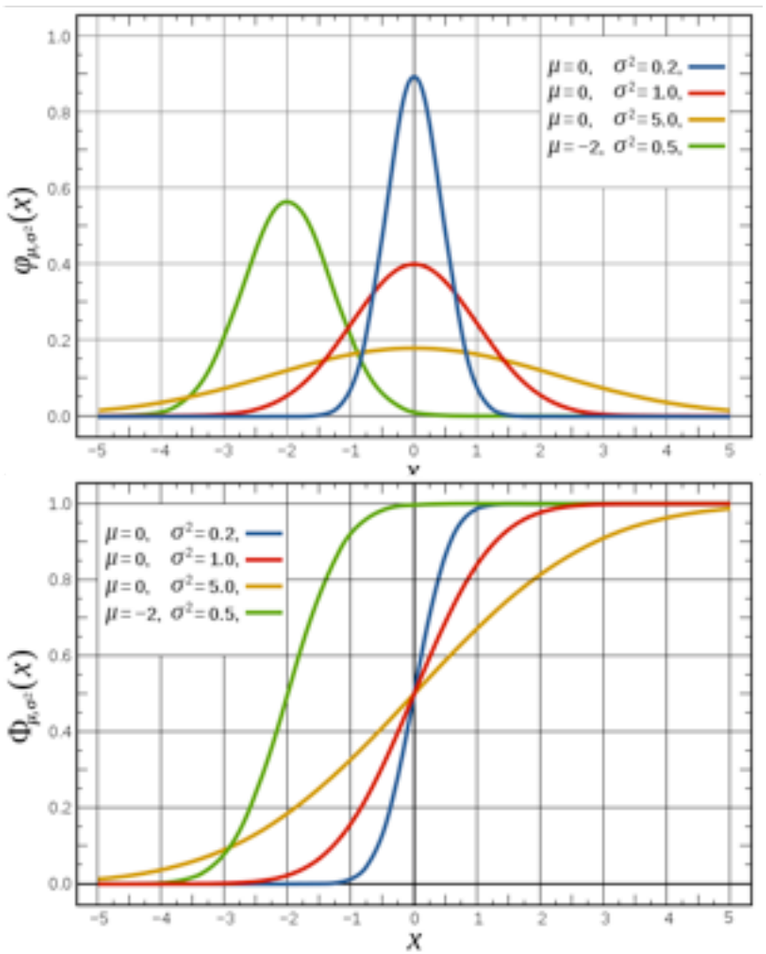
(C) weibull.com

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

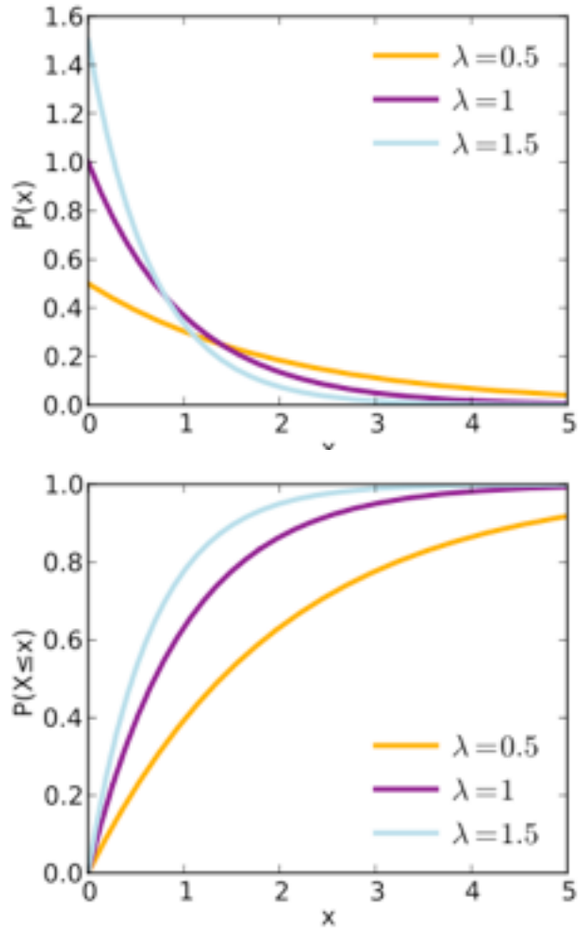
PDF Examples

- 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)

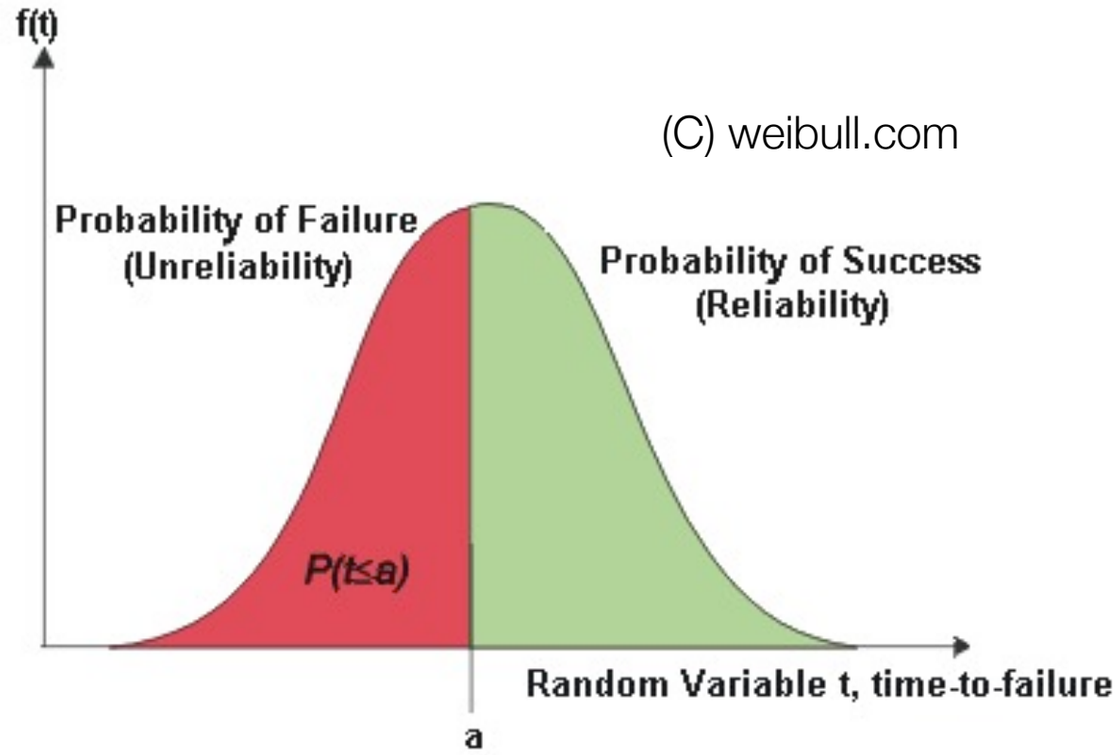


Probability density function

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 **failure time**
  - *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**
    - This works because working / non-working is a binary decision
- Typically, the exponential distribution is used for the ‚failure time' variable
- Distribution function describes ‚surveival probability' at t



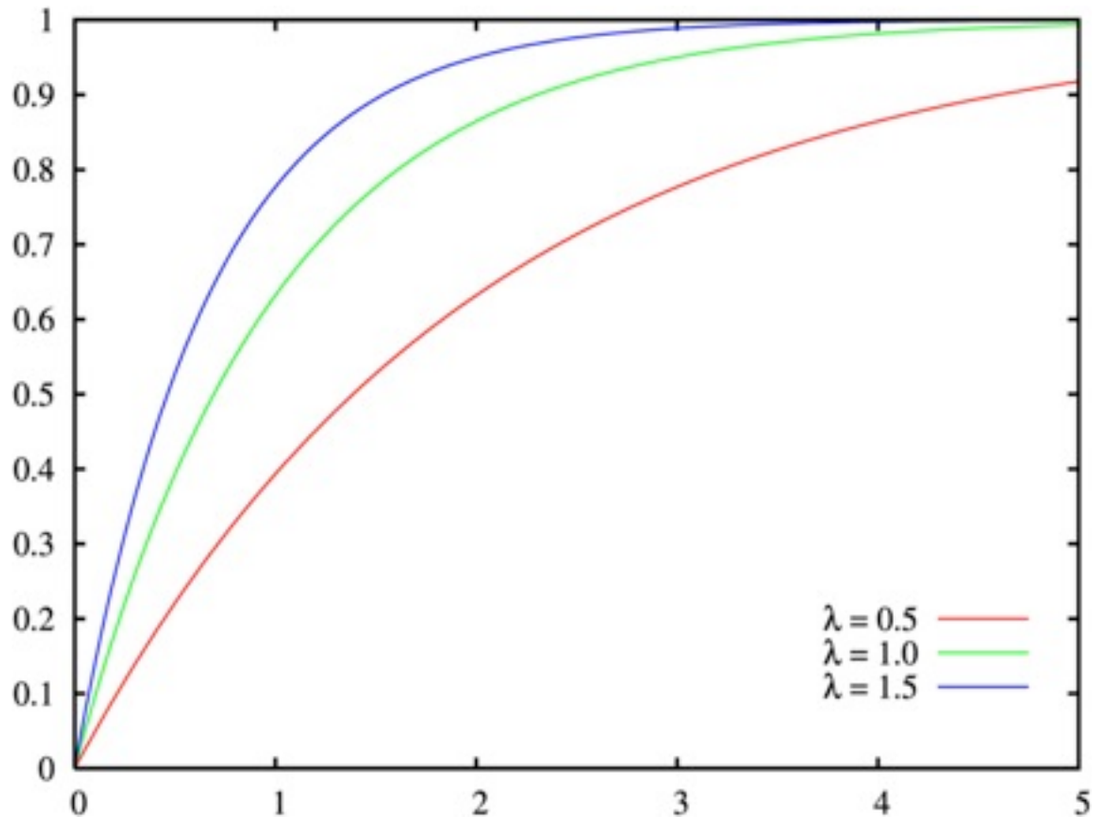
Why Exponential ?

- Only continuous distribution function with memoryless resp. **Markov property**
  - $P(T > t + s|T > t) = P(T > s)$, e.g. $P_{Failure}(5\ years|T > 2\ years) = P_{Failure}(3\ years)$
  - Failure is not the result of wear-out
  - Models ‚intrinsic failure‘ part of the bathtube curve, were most components spend the majority of their life time
    - Weibull distribution can also model tear-in and wear-out
- Some natural phenomena have constant failure rate (e.g. cosmic ray particles)
- Example: Product support determines an outage rate of 5% per day, independent from age
  - Failure rate is 0.005, so MTTF = 200 days
- Numerical formulation for „law of small numbers“

Reliability Function

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

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



- Reliability function (survival probability) for exponential failure distribution:

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

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

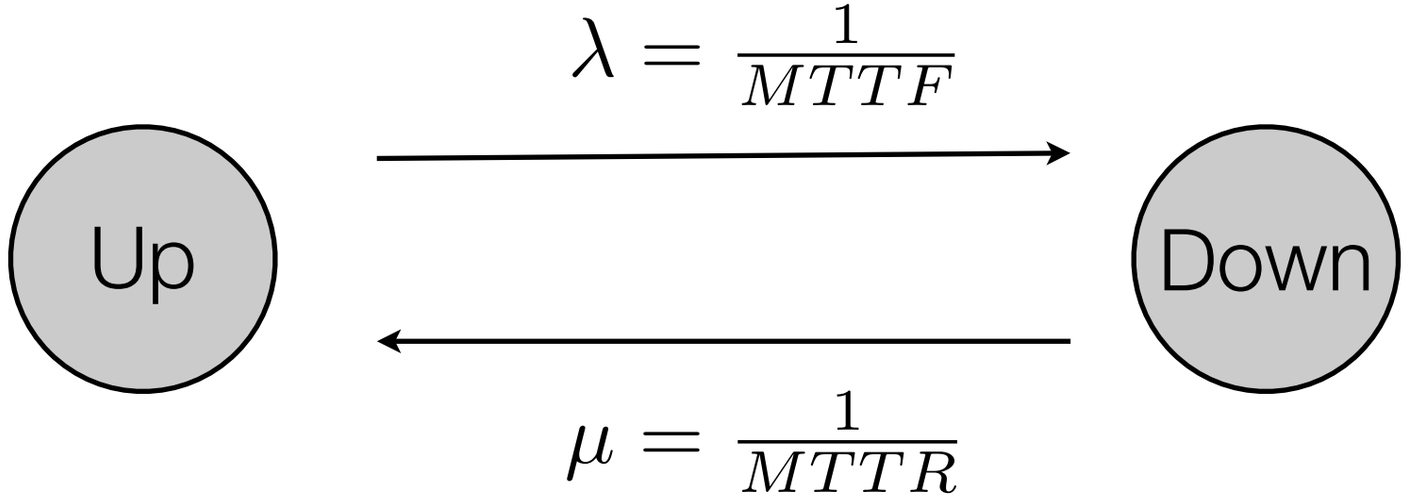
$$\lambda(t) = \frac{f(t)}{R(t)} = \lambda \text{ for constant failure rate}$$

Question: What is a quantitative approach to evaluate system reliability and availability ?

Dependability Modeling

- Default approach: Utilize a formalism to model system dependability
  - Quantify the availability of components, calculate system availability based on this data and a set of assumptions - the availability model
    - Most models expose the same expressiveness
    - Each formalism allows to focus on certain aspects
      - Component-based models: Reliability block diagram, fault tree
      - State-based models: Markov chains, petri nets
- System understanding evolved from hardware to software to IT infrastructures
  - Example: Organization management influence on business service reliability
    - Information Technology Infrastructure Library (ITIL)
    - CoBiT(Control Objectives for Information and related Technology)

Dependability Modeling



- Some assumptions
  - All failure and repair events are exponentially distributed
  - Components are either fully working or completely failed
  - All failure and repair events are pair-wisely stochastically independent
  - Correct functioning at t can be treated as event
- From component failure rate, derive reliability at a given point in time (same for all modeled components) or availability value, treat as „probability value“ r_i in the model

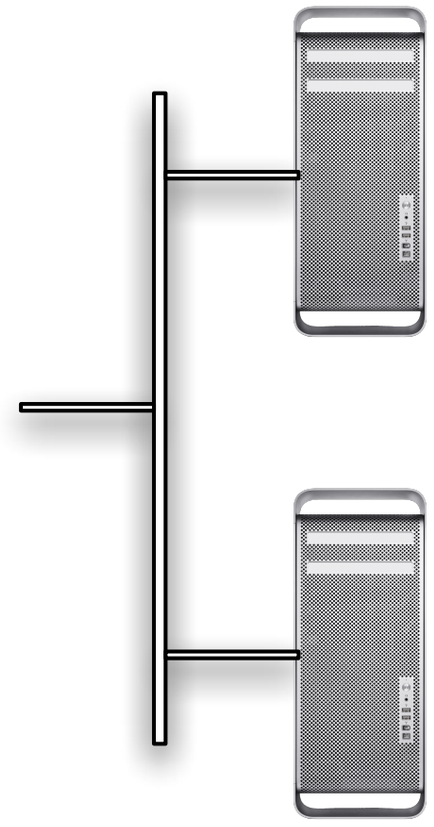
Boolean Algebra Approach

- For stochastically independent events:

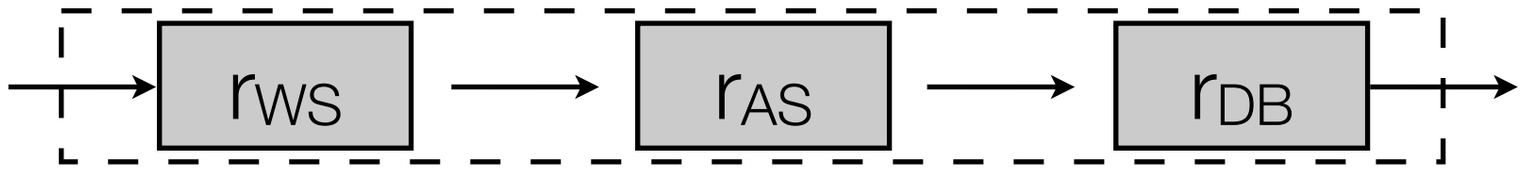
$$Pr(\phi_1 \wedge \phi_2) = Pr(\phi_1) \cdot Pr(\phi_2)$$
$$Pr(\phi_1 \vee \phi_2) = Pr(\phi_1) + Pr(\phi_2) - Pr(\phi_1 \wedge \phi 2)$$
$$Pr(\neg\phi) = 1 - Pr(\phi)$$

- c_i : The event that component c_i is operational
- $r_i = Pr(c_i)$: Probability that c_i occurs

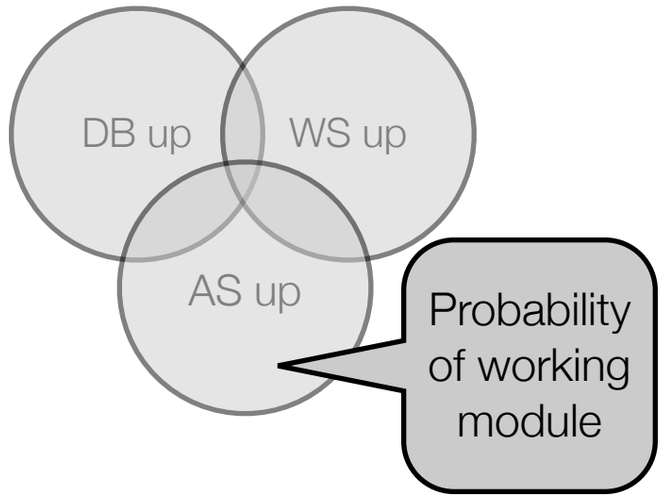
$$\phi = (c_1 \vee c_2) \wedge c_3$$
$$Pr(\phi) = Pr((c_1 \vee c_2) \wedge c3)$$
$$= (r_1 + r_2 - r_1 \cdot r_2) \cdot r_3$$
$$= r_1 r_3 + r_2 r_3 - r_1 r_2 r_3$$



Serial Case



- Help from probability theory: *The probability of an event expressed as the intersection of independent events is the product of the probabilities of the independent events.*



- Example: Chain of web server (r=0.9), application server (r=0.95) and database server (r=0.99)
  - Benefit of replacing the database with an expensive model (r=0.999) ?
  - Benefit of replacing the web server with a new model (r=0.95) ?

$$\phi_S = c_{WS} \wedge c_{AS} \wedge c_{DB}$$

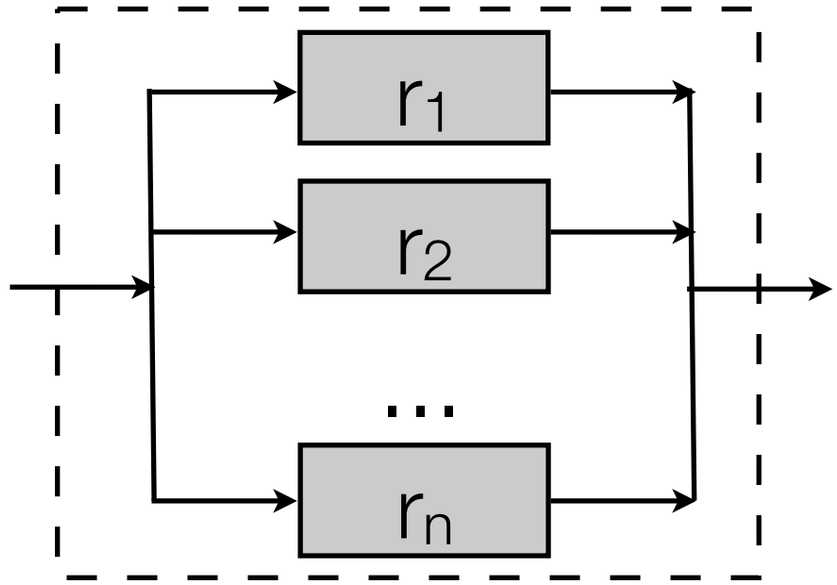
Redundancy structure

Component available

$$R_S = r_1 \times r_2 ... r_n = \prod_{i=1}^{n} r_i$$

Parallel Case

- Parallel case
  - Search engine, cluster node r=0.85 (around 2 months outage / year)
  - How many servers to reach 5 nines of site availability ?



$$\phi_S = c_{WS} \vee c_{AS} \vee c_{DB}$$

Redundancy structure

Component available

$$R_S = 1 - P_{alldown}$$

$$R_S = 1 - ((1 - r_1) \times (1 - r_2) \times ...(1 - r_n))$$

$$R_S = 1 - \prod_{i=1}^{n}(1 - r_i) \qquad n_{min} = \lceil \frac{ln(1-R_S)}{ln(1-r)} \rceil$$

Parallel Case Example

- Two redundant systems, each can handle the entire load
- Case 1: $R_A=R_B=0.5$
  - Reduction of failure probability in half
- Case 2: $R_A=R_B=0.99$
  - Reduction of failure probability to 1/10th

K-of-N Systems

- At least K out of N components need to work to have a functioning system
- Algebraic investigation only possible with exponential failure distribution
  - At the beginning, there are N operational units, so failure rate equals $N \cdot \lambda$
  - After first component failure, the failure rate goes down to $(N-1) \cdot \lambda$
  - This goes until the (K+1)th failure has occurred

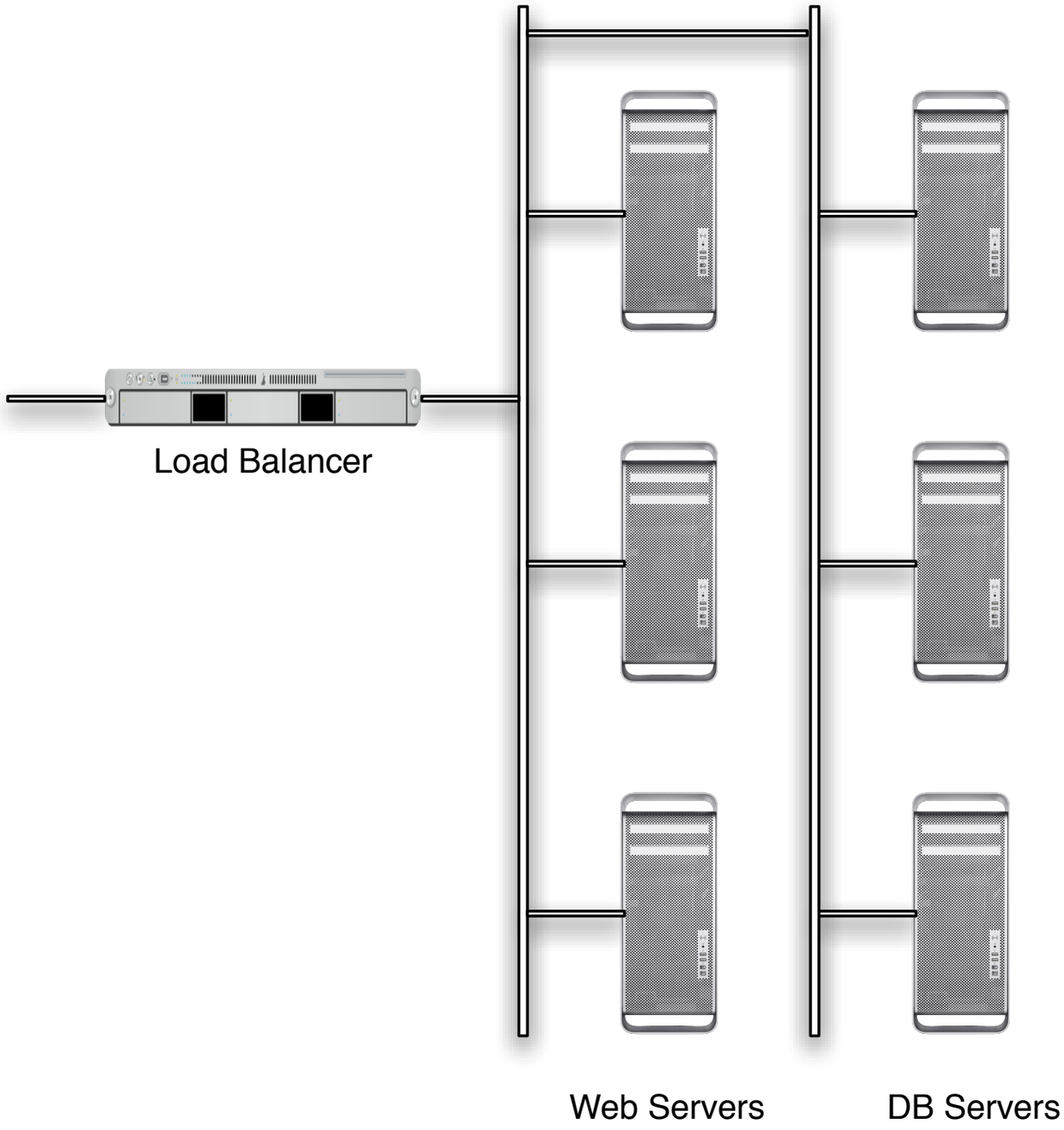
$$MTTF = \frac{1}{\lambda} \sum_{K \leq j \leq N} \frac{1}{j}$$

  - K=1 is the same as the parallel case
  - K=N is the same as the serial case
- Example: Disk system with K=3, N=4, MTTF=1800h, MTTR=4.5h

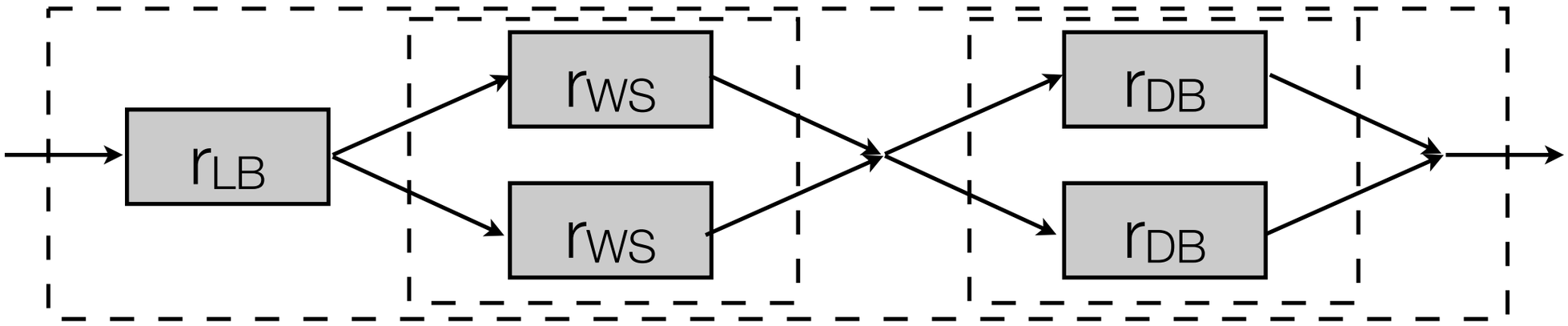
$$A_{Disk} = \frac{1800}{1800+4.5} = 0.9999628 \qquad MTTF = \frac{1}{4}MTTF_{Disk} + \frac{1}{3}MTTF_{Disk} = 1050h$$

Examples

- Online brokerage site to be designed - choice of components
- Site availability aimed at 99.99%
- Setup: Load balancer, similar web server hardware, replicated database
- Question: What is the least expensive configuration that reaches 99.99% ?
  - Choice between low-end (r=0.85) and high-end (R=0.999) servers
  - Must also consider purchase and maintenance costs per setup



Examples



$$\phi_S = c_{LB} \wedge (c_{WS1} \vee c_{WS2}) \wedge (c_{DB1} \vee c_{DB2})$$

$$R_{site} = r_{LB} \times R_{WS} \times R_{DB}$$
$$= r_{LB} \times [1 - (1 - r_{WS})^{n_{WS}}] \times [1 - (1 - r_{DB})^{n_{DB}}]$$

$$R_{site} = 0.9999$$
$$R_{LB} = 0.99999$$

$$n_{WS} = \lceil \frac{ln(1-0.99991/[1-(1-r_{DB})^{n_{DB}}}{ln(1-r_{WS})} \rceil$$

Examples

r_{WS}	r_{DB}	Minimum n_{WS}	Minimum n_{DB}	R_{site}
0,85	0,85	6	5	99,990%
0,85	0,999	5	2	99,991%
0,999	0,999	2	2	99,999%

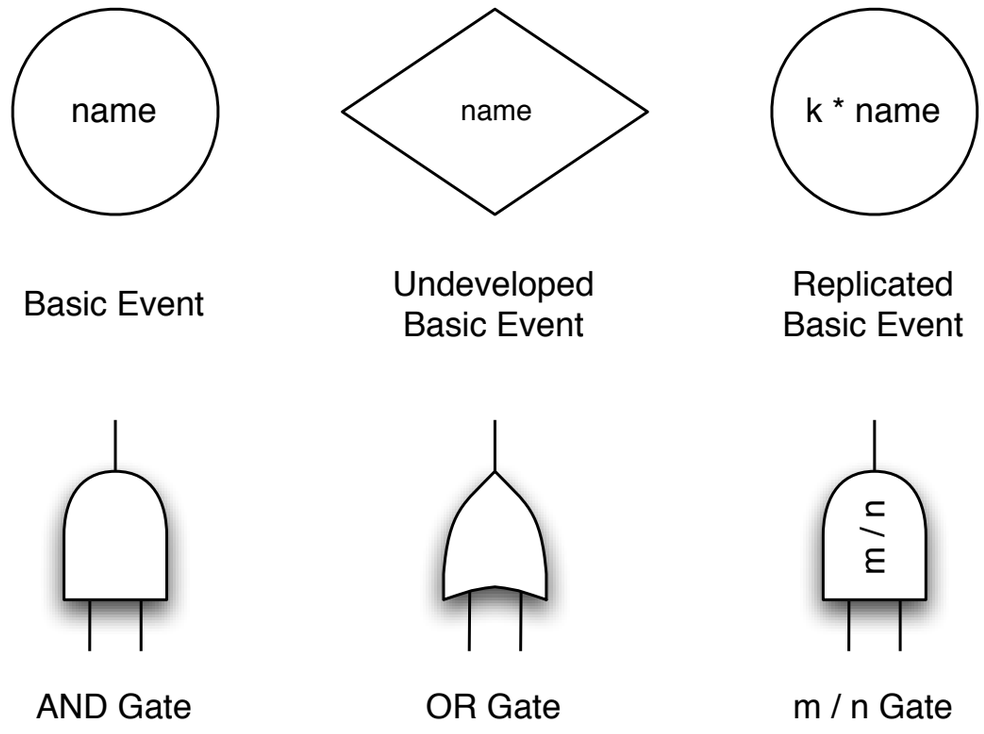
Fault Tree Analysis

- Structure analysis effort grows exponentially with the number of components
- Fault Trees: Application of deductive logic to produce a fault-oriented diagram
  - Invented 1961 by H. Watson (Bell Telephone Laboratories), used by Boeing since 1966, meanwhile adopted by aerospace and nuclear power industry
  - Graphical representation of structure formula, helps to identify fault classes
  - Complex system failures are broken down into simpler subsystem, component, block and single element failures
  - Probability of a higher-level event can be calculated by lower level probabilities
  - Root cause analysis, risk assessment, safety assessment
- Tools: SAVE, SHARPE, Fault Tree+, AvSim+, ReliabilityWorkbench, BlockSim6, Figaro/KB3, BQR Care

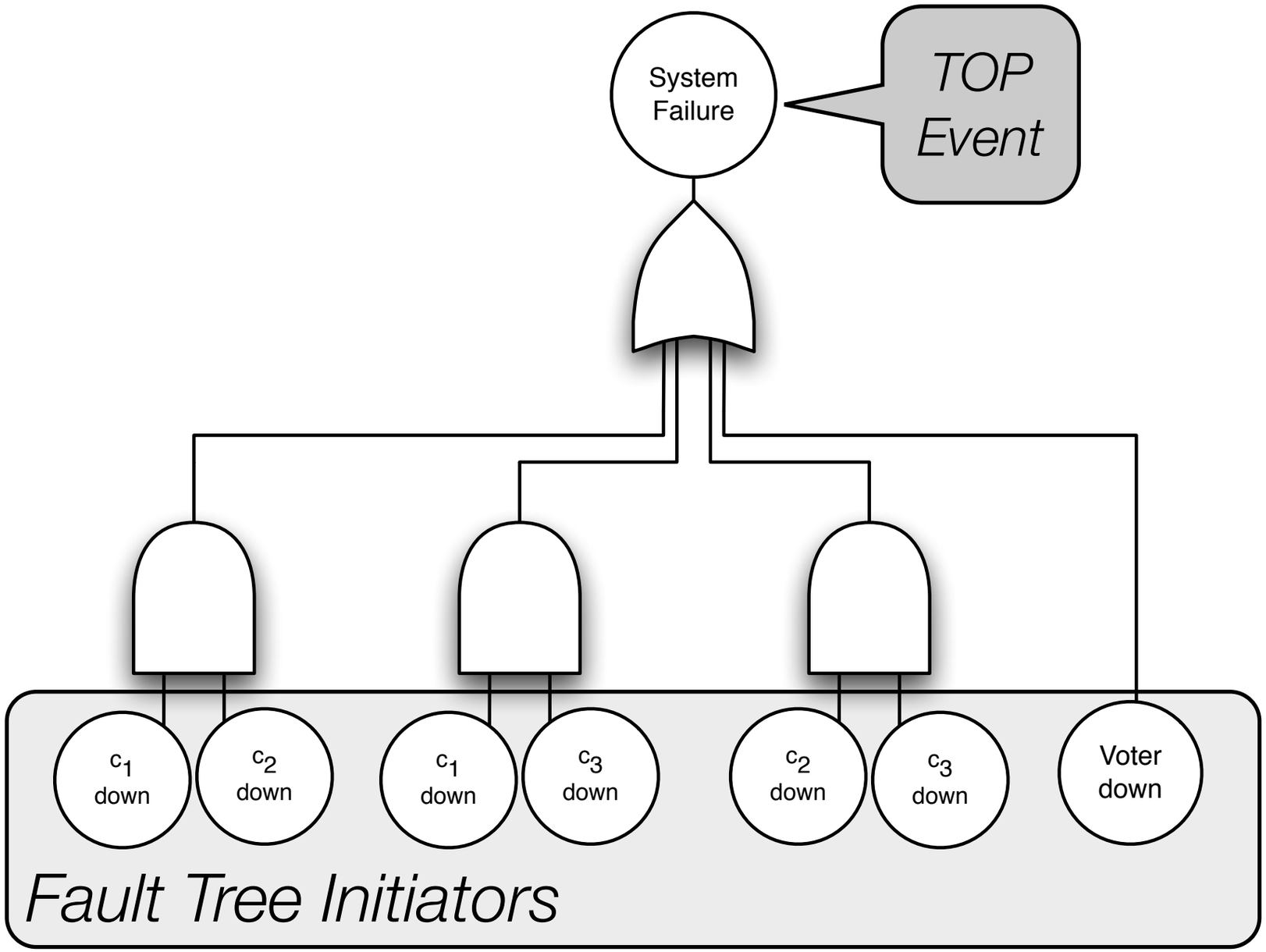
Fault Trees

- Event types, all characterized by failure rate resp. probability
  - Basic event - Component failure event in the system
  - Undeveloped basic event - Component failure event, some unavailable information
  - Replicated basic event - k statistically identical copies of a component

- AND gate - Output event occurs if all input events occur
- OR gate - Output event occurs if one or more input events occur
- m/n gate - Output event occurs if m or more of the n inputs occur
- Events and gates are not system components, but symbols representing the analysis

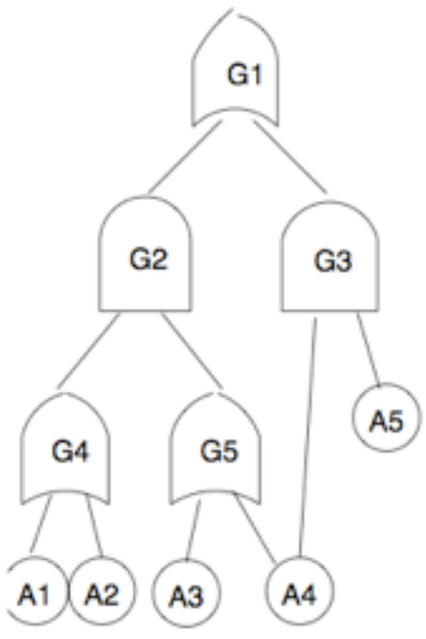


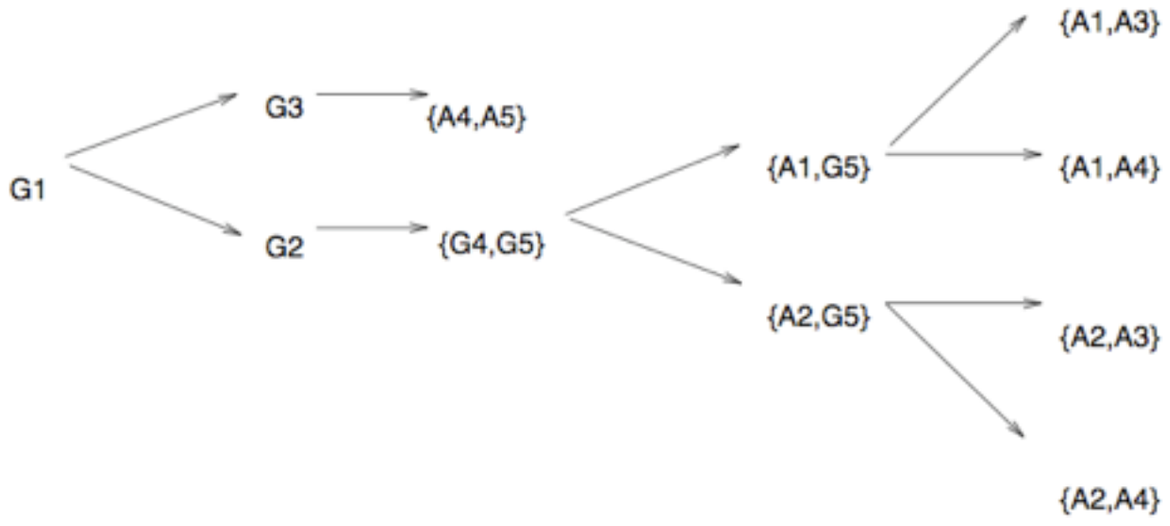
Fault Trees


System Failure
TOP Event
c1 down
c2 down
c1 down
c3 down
c2 down
c3 down
Voter down
Fault Tree Initiators

Cut Sets

- **Cut set:** Any group of initiators which, if all occur, cause the TOP event
- **Minimal cut set (mincut)**: Least group of cut set initiators
- A long mincut signals low vulnerability
- A small mincut signals high vulnerability
- Presence of numerous cut sets signals high vulnerability
- A singleton cutset signals a single point of failure
- Complement are **path sets**





(C) Joanne Bechta Dugan

FTA Cutsets

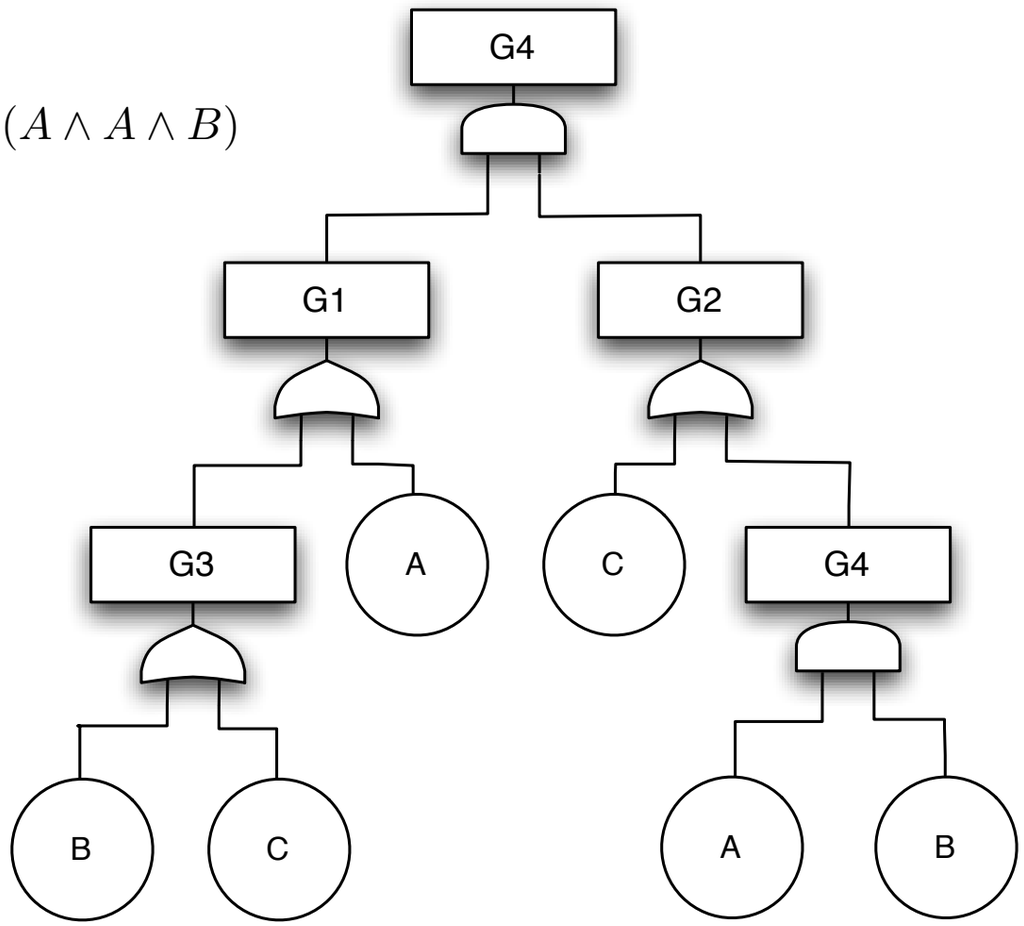
- Determine probabilities for cut sets to find **critical path**
  - Critical and weak links in a system design
- Analyze cutset for
  - Unexpected root cause combinations
  - Weak points in the design
  - Bypass of intended safety features
  - Common cause problems
- Methods for cutset finding
  - Boolean reduction, bottom-up reduction, top-down reduction, mapping to binary decision diagram, shannon decomposition, genetic algorithms, **...**

Boolean Reduction Example

$$(A \vee B) \wedge (C \vee D) = (A \wedge C) \vee (A \wedge D) \vee (B \wedge C) \vee (B \wedge D)$$

$$A \vee A = A \qquad A \wedge A = A \qquad A \vee (A \wedge B) = A$$

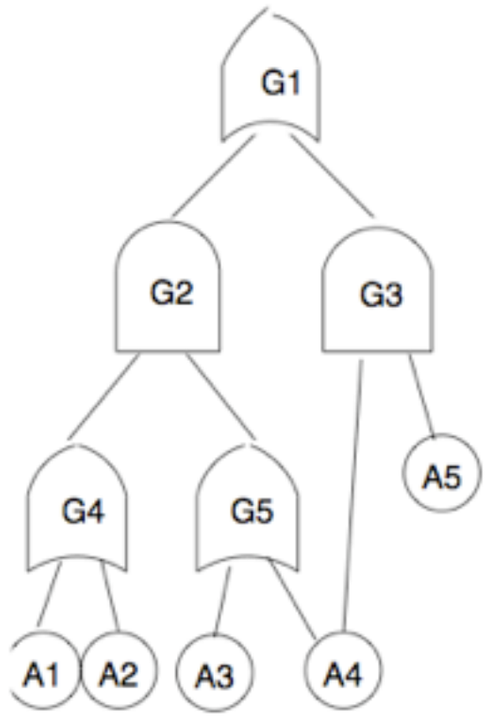
$$\begin{aligned} TOP &= (B \vee C \vee A) \wedge (C \vee A \wedge B) \\ &= (B \wedge C) \vee (B \wedge A \wedge B) \vee (C \wedge C) \vee (C \wedge A \wedge B) \vee (A \wedge C) \vee (A \wedge A \wedge B) \\ &= (B \wedge C) \vee (A \wedge B) \vee C \vee (C \wedge A \wedge B) \vee (A \wedge C) \vee (A \wedge B) \\ &= (B \wedge C) \vee (A \wedge B) \vee C \vee (C \wedge A \wedge B) \vee (A \wedge C) \\ &= A \wedge B \vee C \end{aligned}$$



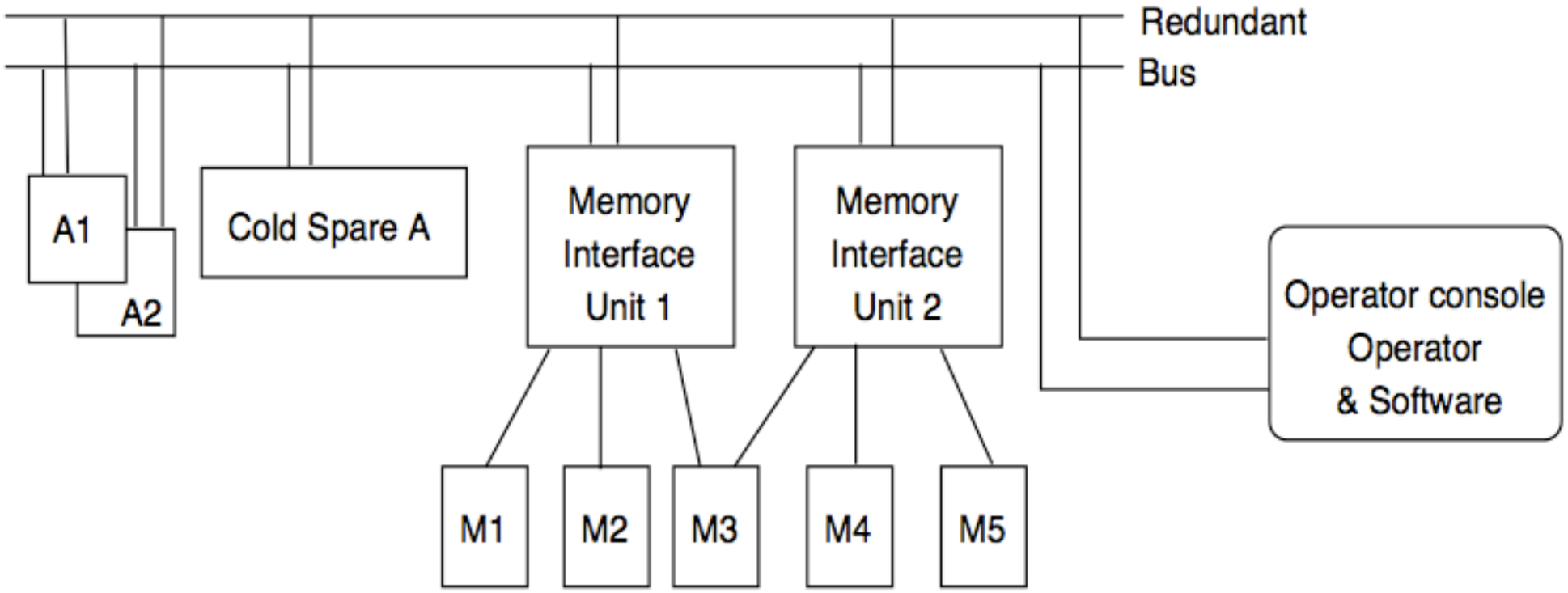
Example by Dr. John Andrews / Loughborough University

Fault Trees for Containment Barrier Analysis

- AND gates can be protected by disallowing one of the inputs
  - Exhaustive testing or formal proof to show that the component cannot fail
  - Test for failure condition and recovery routine
- OR gates can be protected by disallowing all inputs or by providing error recovery
- Example
  - Protect G3 by preventing failure of A4
  - Protect G2 by
    - preventing failure of A3
    - preventing failure of both A1 and A2
    - providing fault tolerance for G4

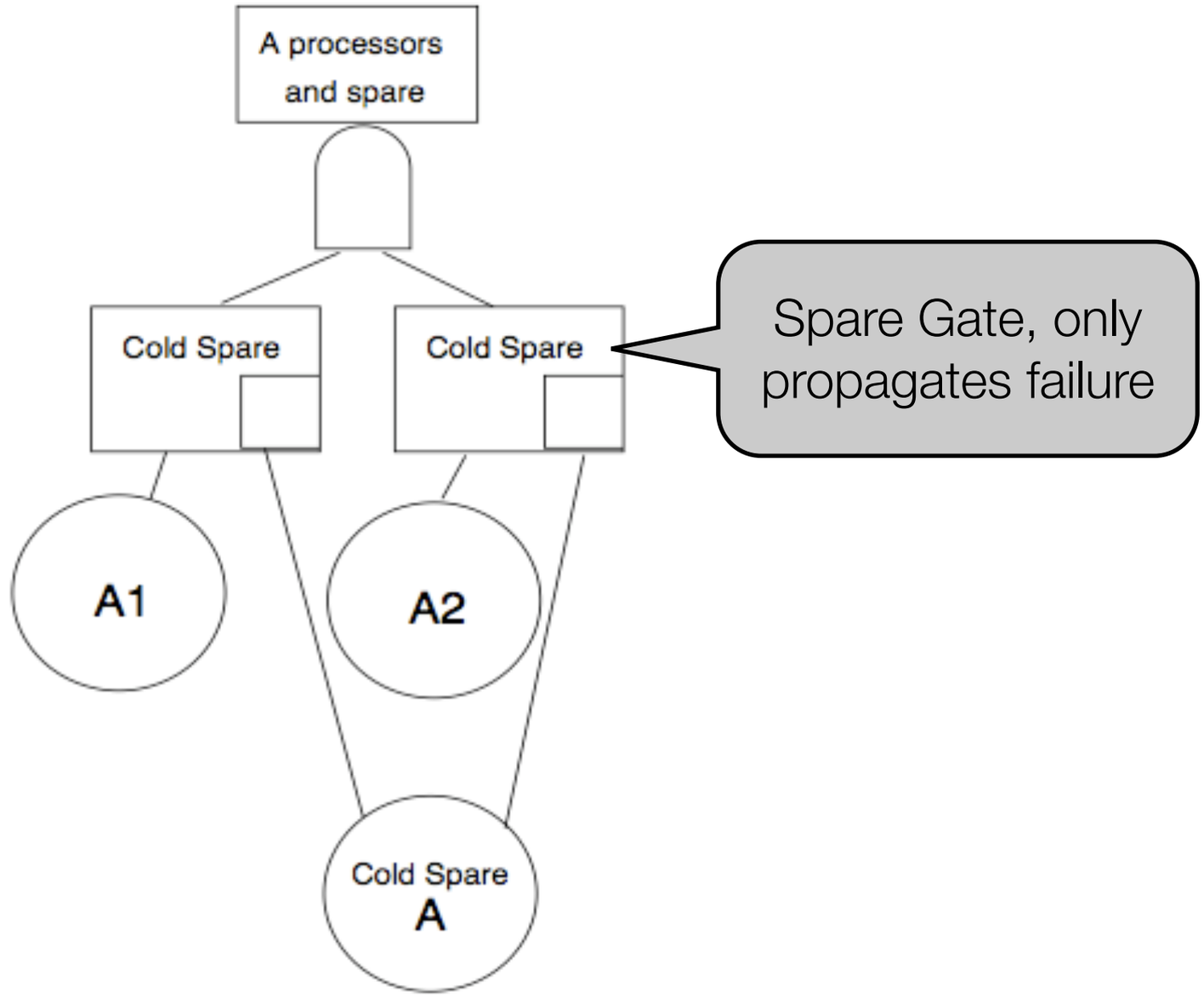


Hypothetic Example Computer System (HECS)

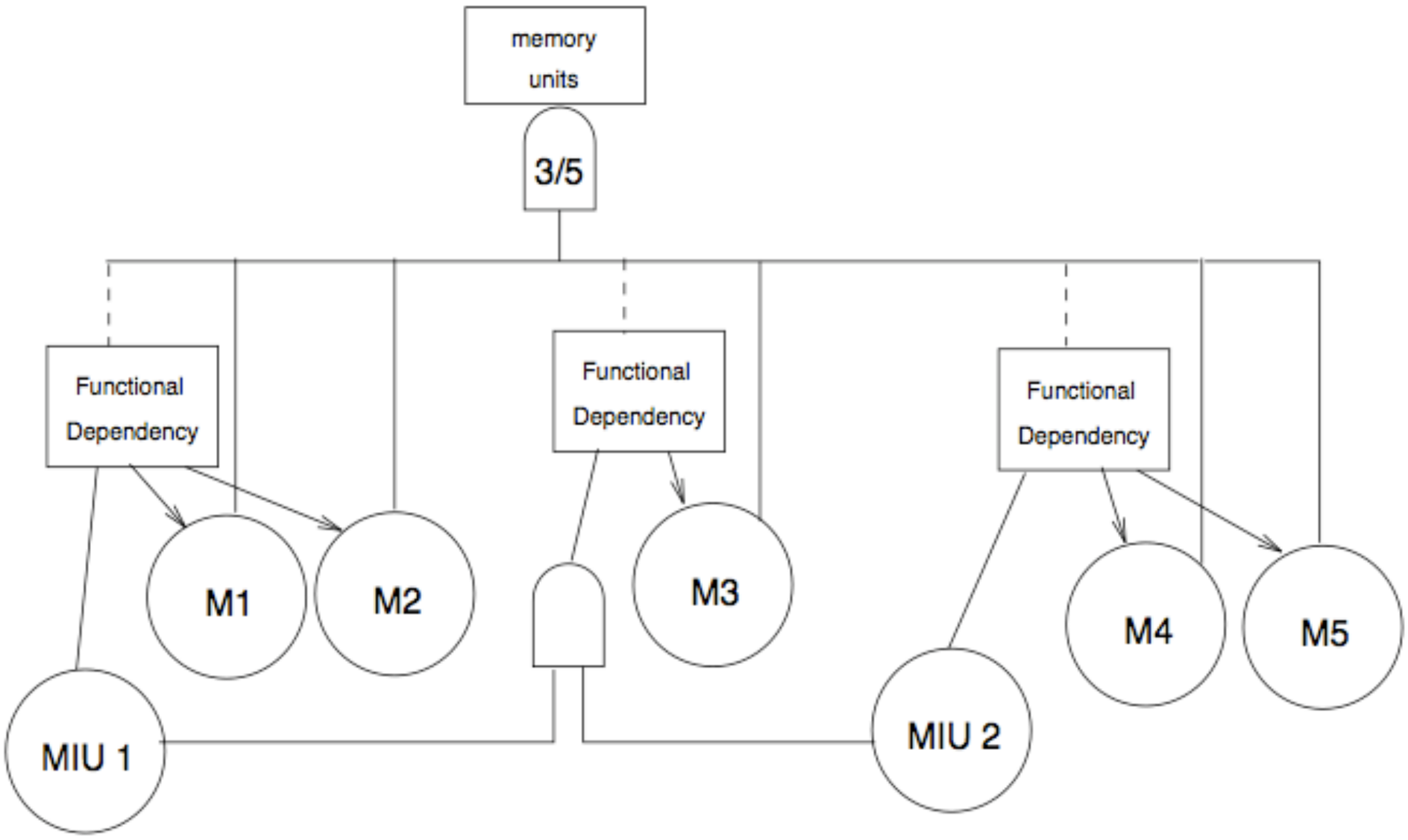


- Minimum demands for operation
  - One functional processor, three memory modules, one bus, operator + console
- Example taken from Joanne Bechta Dugan, University of Virginia (www.fault-tree.net)

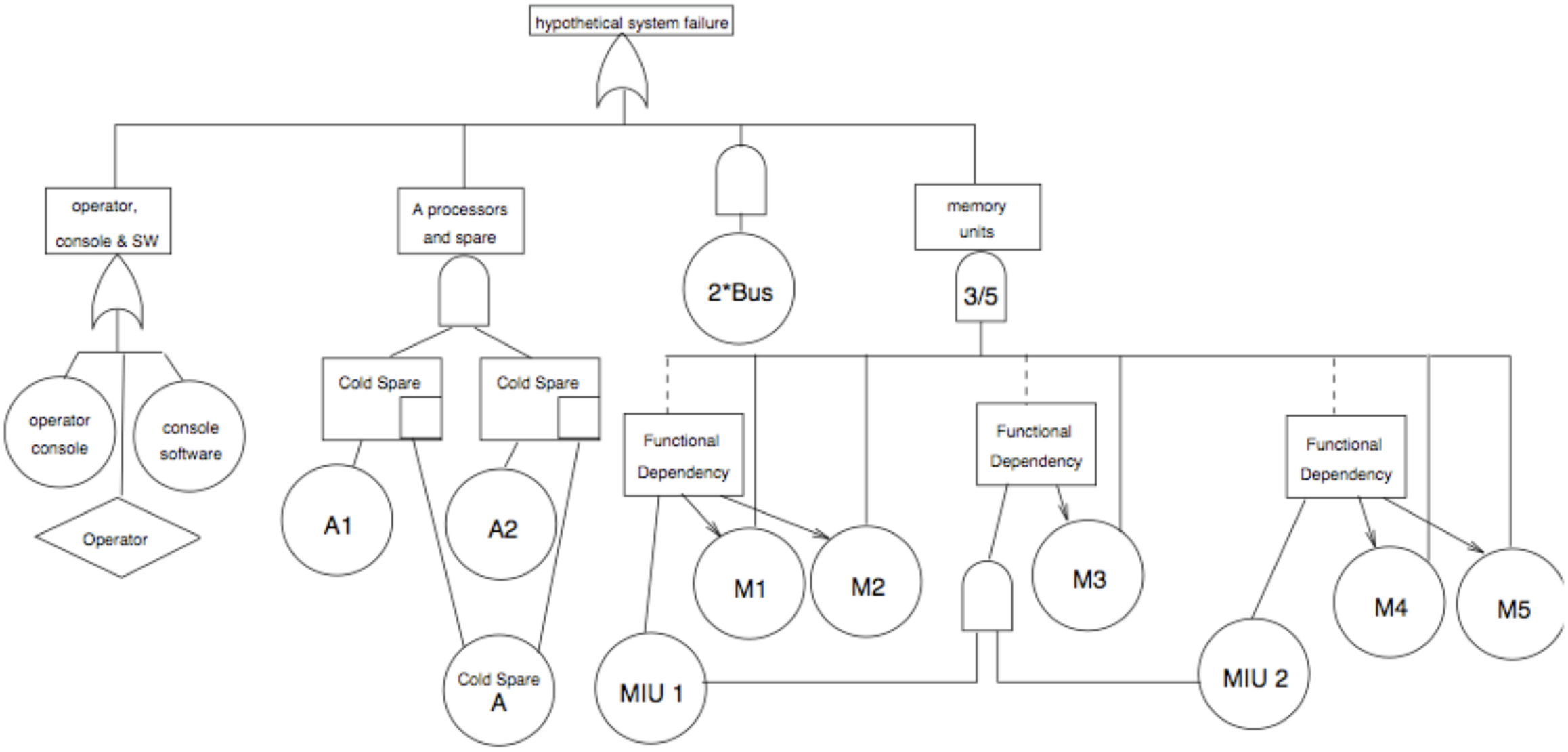
HECS Example



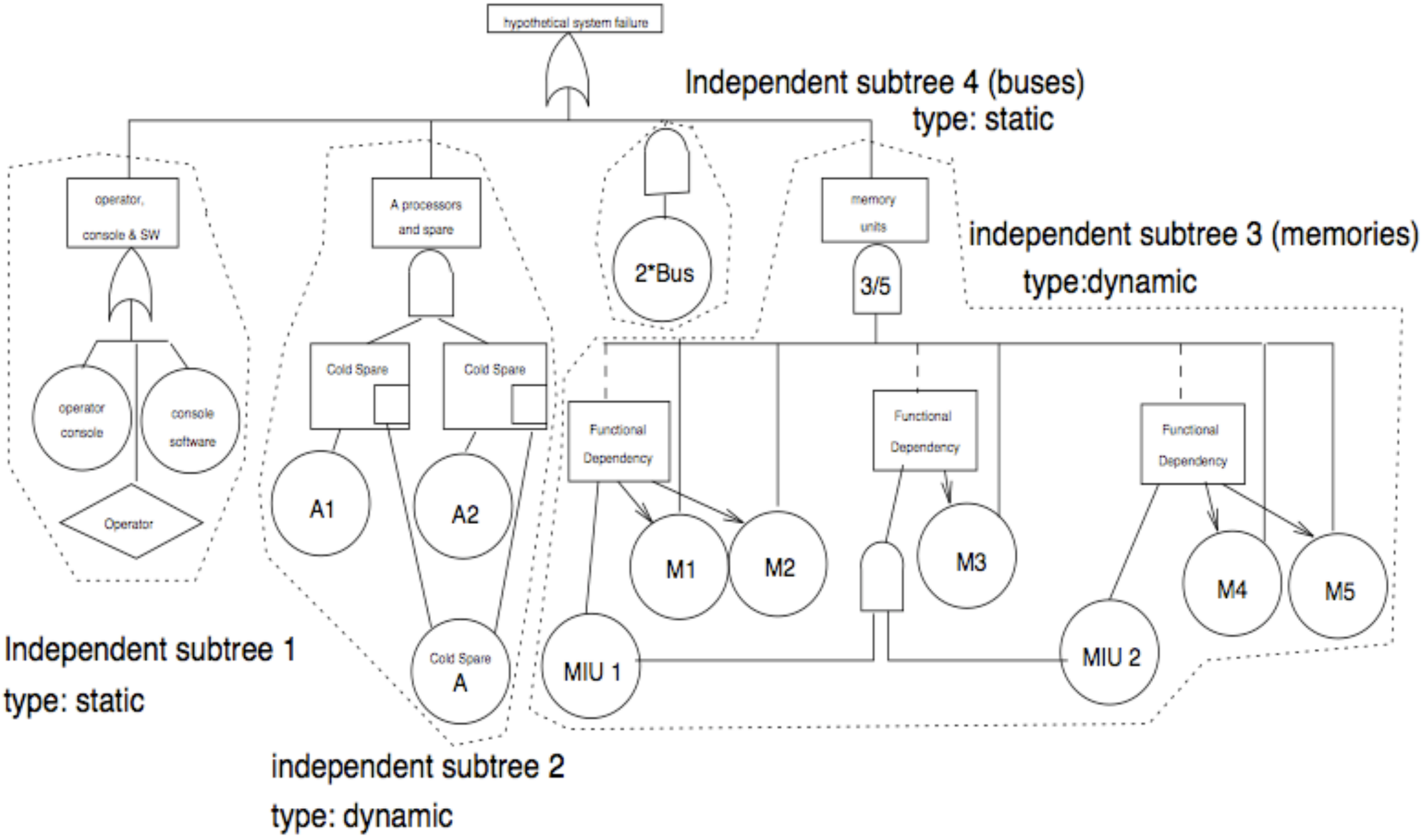
HECS Example



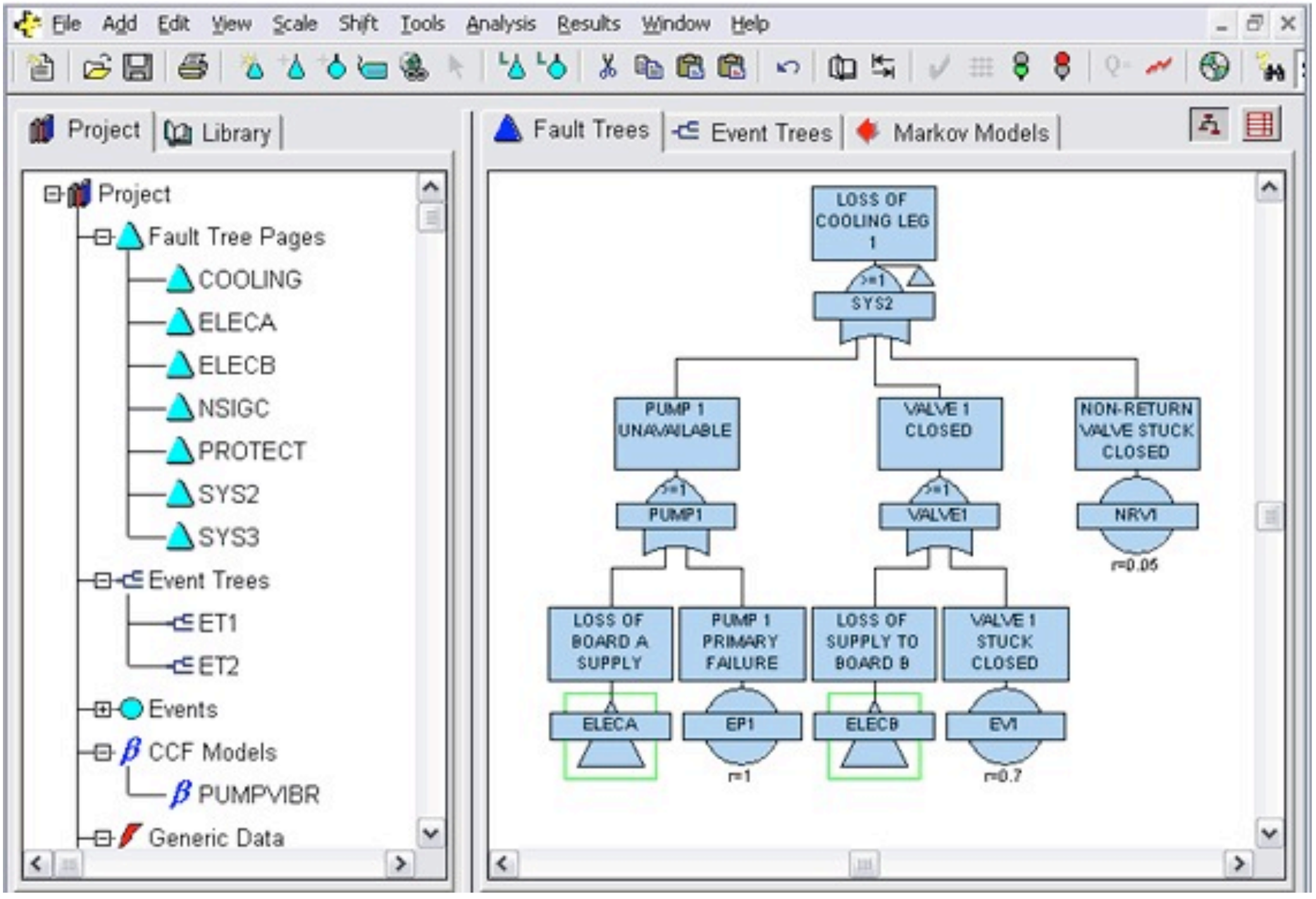
HECS Example



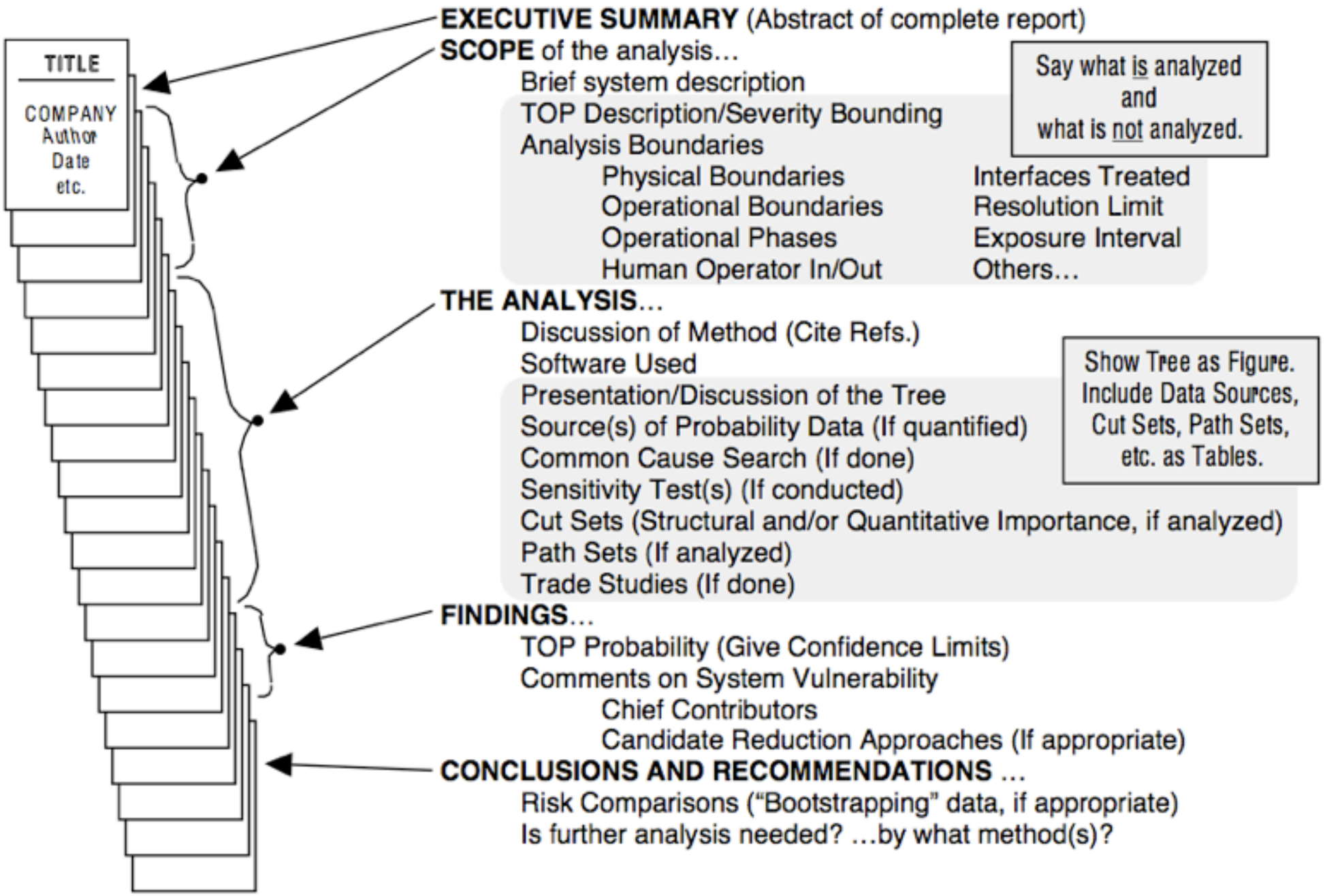
HECS Example



FTA Tools


File Add Edit View Scale Shift Tools Analysis Results Window Help
Project
Library
Fault Trees
Event Trees
Markov Models
Project
Fault Tree Pages
COOLING
ELECA
ELECB
NSIGC
PROTECT
SYS2
SYS3
Event Trees
ET1
ET2
Events
CCF Models
PUMPVIBR
Generic Data
LOSS OF COOLING LEG 1
>=1
SYS2
PUMP 1 UNAVAILABLE
VALVE 1 CLOSED
NON-RETURN VALVE STUCK CLOSED
>=1
PUMP1
>=1
VALVE1
NRV1
r=0.05
LOSS OF BOARD A SUPPLY
PUMP 1 PRIMARY FAILURE
LOSS OF SUPPLY TO BOARD B
VALVE 1 STUCK CLOSED
ELECA
EP1
ELECB
EV1
r=1
r=0.7

FTA Report (Clemens & Sverdrup)



FTA Shortcomings (Clemens & Sverdrup)

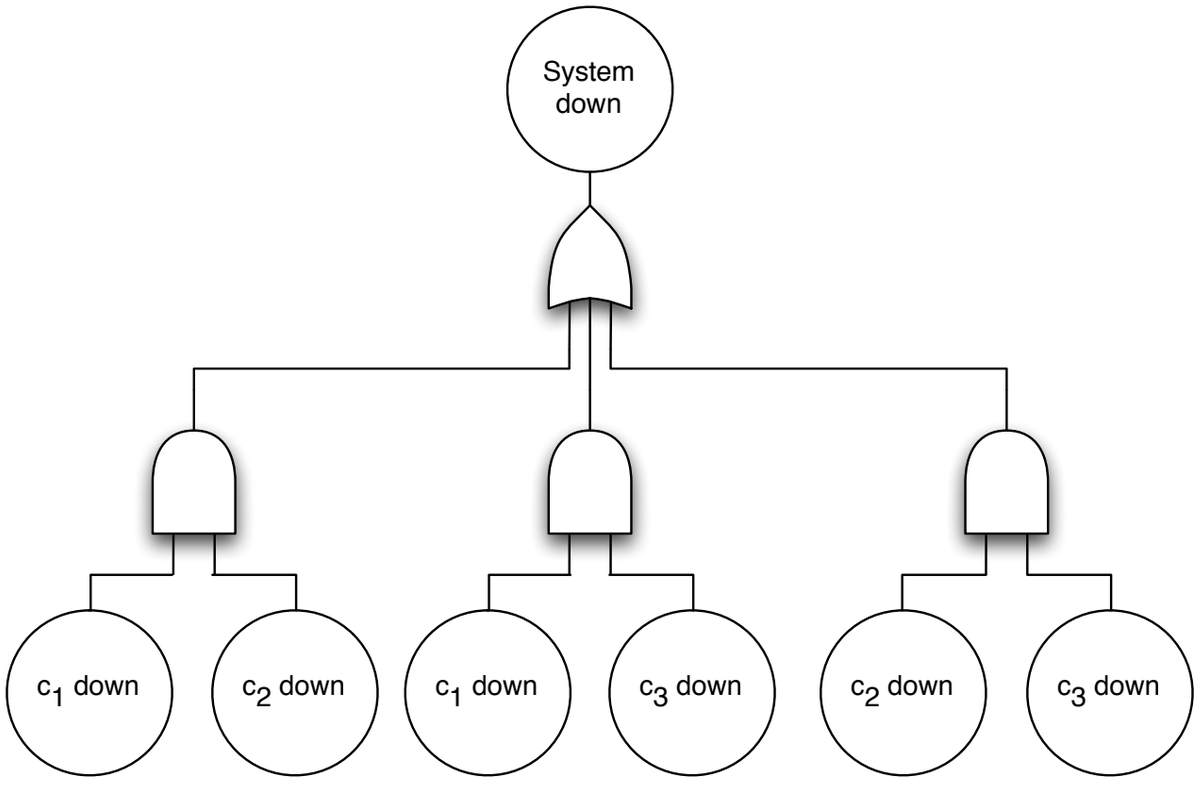
- Undesirable events must be foreseen
- All significant failure contributors must be foreseen
- Each initiator must be constrained to two conditional modes when modeled
- Initiators beneath a common gate must be independent of each other
- Events must be immediate contributors to next higher level (timing)
- Each initiators failure rate must be predictable
  - Amount of data must justify a quantitative analysis !

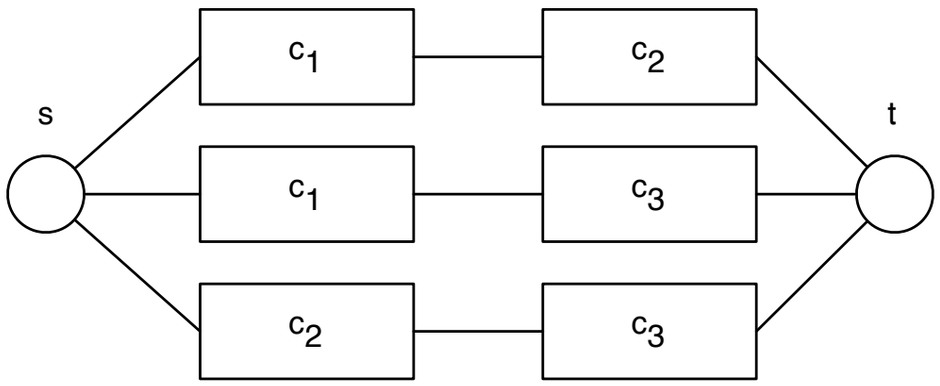
FTA Remarks

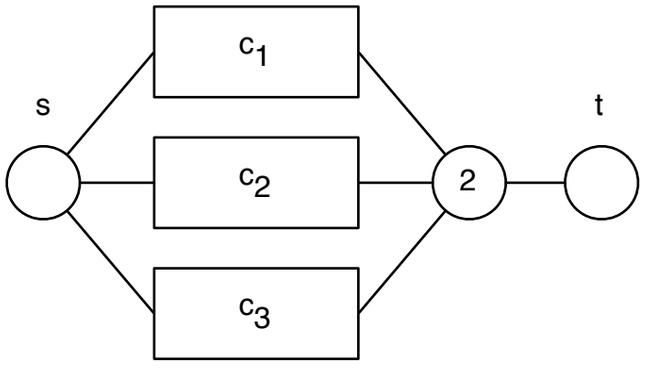
- Proper and consistent naming is very important
  - Per event: WHAT failed and HOW
- Initiators must be statistically independent of one another
- Contributing elements must be an IMMEDIATE contributor
- At a given level under a given gate, each fault must be independent from all others
- Logic can be tested in SUCCESS DOMAIN - invert all statements and gates and check correctness
- Analyze no further down than is necessary to enter probability data with confidence

Reliability Block Diagrams (RBD)

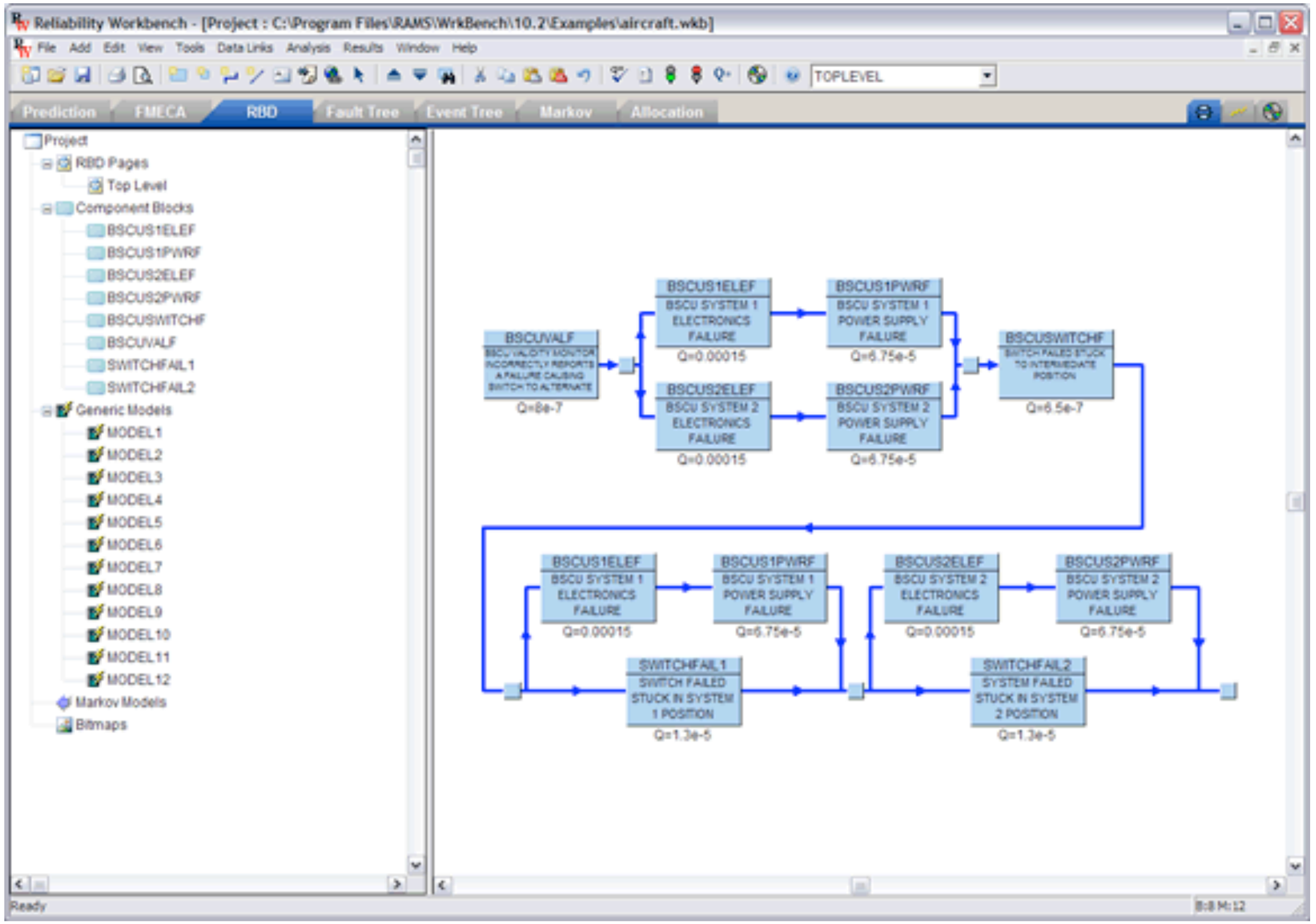
- Alternative way to model logical interaction of failures
- System is available only if there is a path between s and t
- Structure formula can be obtained by identifying all minimal cut sets
  - Subset of edges that disconnects s from t if removed







RBD Tools


Reliability Workbench - [Project : C:\Program Files\RAMS\WrkBench\10.2\Examples\aircraft.wkb]
File Add Edit View Tools Data Links Analysis Results Window Help
TOPLEVEL
Prediction FMECA RBD Fault Tree Event Tree Markov Allocation
Project
RBD Pages
Top Level
Component Blocks
BSCUS1ELEF
BSCUS1PWRF
BSCUS2ELEF
BSCUS2PWRF
BSCUSWITCHF
BSCUVALF
SWITCHFAIL1
SWITCHFAIL2
Generic Models
MODEL1
MODEL2
MODEL3
MODEL4
MODEL5
MODEL6
MODEL7
MODEL8
MODEL9
MODEL10
MODEL11
MODEL12
Markov Models
Bitmaps
BSCUVALF
BSCU VALIDITY MONITOR INCORRECTLY REPORTS A FAILURE CAUSING SWITCH TO ALTERNATE
Q=8e-7
BSCUS1ELEF
BSCU SYSTEM 1 ELECTRONICS FAILURE
Q=0.00015
BSCUS1PWRF
BSCU SYSTEM 1 POWER SUPPLY FAILURE
Q=6.75e-5
BSCUS2ELEF
BSCU SYSTEM 2 ELECTRONICS FAILURE
Q=0.00015
BSCUS2PWRF
BSCU SYSTEM 2 POWER SUPPLY FAILURE
Q=6.75e-5
BSCUSWITCHF
SWITCH FAILED STUCK TO INTERMEDIATE POSITION
Q=6.5e-7
SWITCHFAIL1
SWITCH FAILED STUCK IN SYSTEM 1 POSITION
Q=1.3e-5
SWITCHFAIL2
SYSTEM FAILED STUCK IN SYSTEM 2 POSITION
Q=1.3e-5
Ready