Reliability Analysis

Module 6A and 6B: System Reliability Analysis

Prof. Katrina M. Groth

Mechanical Engineering Department

Center for Risk and Reliability

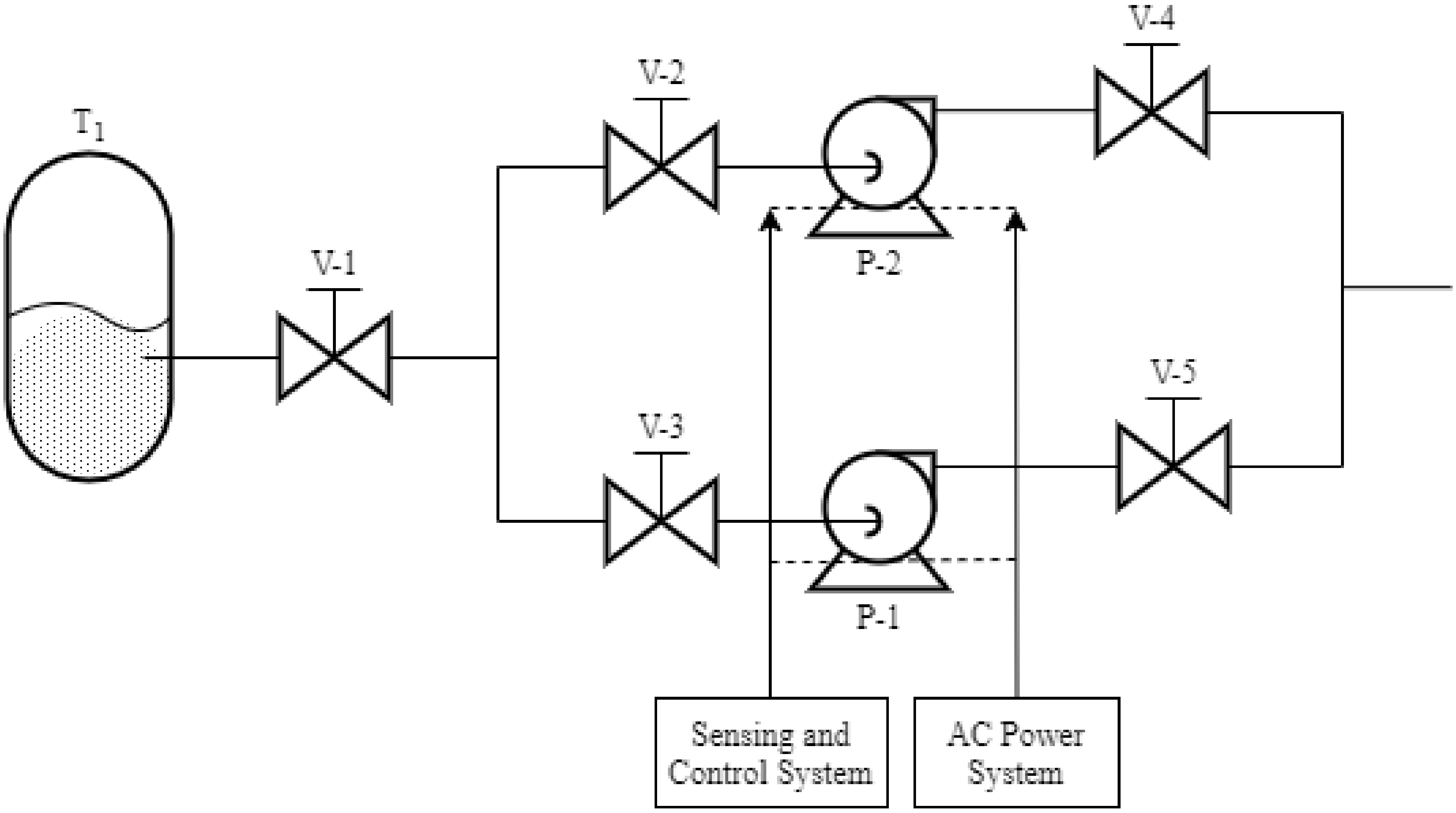
University of Maryland

kgroth@umd.edu

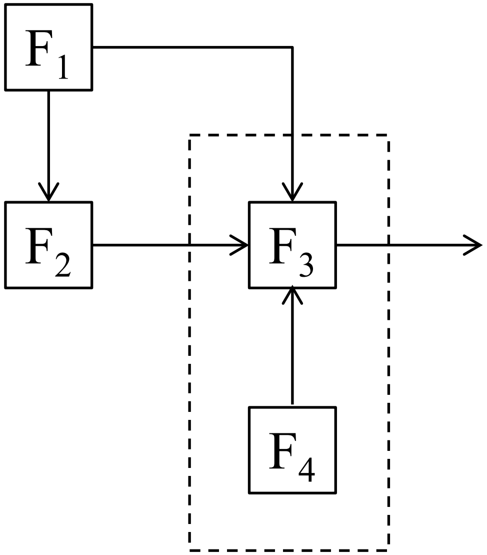
System reliability analysis: Outline

- We will talk about $R_s = f\left(R_{c_{i=1}}(t), R_{c_2}(t), \dots, R_{c_n}(t)\right)$
- Reliability Block Diagrams & Types of Systems
  1. Parallel, Series, *k*-out-of-*n*, Standby and Shared load systems
  2. Complex systems
- Complex system evaluation methods
- Fault trees/Success trees
- Event trees & Event Sequence Diagrams
- Failure Mode and Effect Analysis (and Failure Mode and Effect Criticality Analysis)

System reliability analysis: An example of a pumping system



Functional block diagram for the pumping system



Function	**Functional Description**	**Components Involved**
F_1	AC Power	AC
F_2	Sensing & Control	S
F_3	Pumping	V-2, V-3, V-4, V-5, P-1, P-2
F_4	Source	T-1, V-1

Failure modes of some relevant components (reminder: Chapter 1 defines failure modes)

Component Type	Failure Modes
All Valves	1 – Fail to open 2 – Fail to close 3 – Spurious closure 4 – Plug 5 – Leak 6 – Partially closed
All Pumps	1 – Fail to start 2 – Fail to run 3 – Leak 4 – High internal circulation
Tank	1 – Rupture 2 – Frozen 3 – Leak
AC Power	1 – Lost
Controller	1 – Failed 2 – Biased

Notation

- **Be very careful with your notation.**
  - Overbar always indicates negation
- **Typically, we use:**
  - $\overline{A}$ or R_A for the event that the corresponding item *works*
  - A or F_A for the event that the corresponding item *fails*
  - But this gets flipped in some contexts and problems. Pay attention to the problem statement to determine which is which!
  - Make sure your notation & problem is set up correctly: know what is success and what is failure. Define your own notation if needed.
  - In general: λ and similar parameters usually refer to *failure rate*, but this is not always the case (especially as we progress in this class).

Reminders & Notes for Systems problems

- There are two aspects to system models: qualitative & quantitative.
  - Qualitative: The system structure functions describe the system (failure) logic as a function of its components.
  - Quantitative: The probabilities & mathematics used in the quantification of the system models.
- We use Boolean algebra to manipulate events & sets.
- We use probabilities to talk about uncertainty of events.
- In general: Do the Boolean algebra first, then the probabilities. Don’t start quantifying too early.
- Most of the quantification in this chapter assumes independent events.
  - You **must** verify independence before assuming it!

Types of Systems

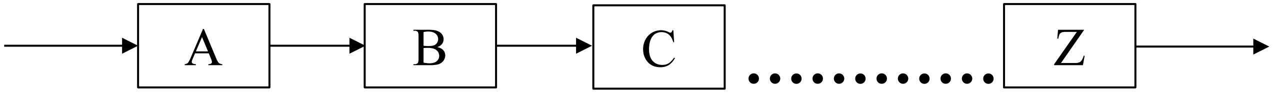
- Series
- Parallel
- *k*-out-of-*n* (combination of above)
- Standby
- Shared Load
- Complex systems—combinations of above

Reliability block diagrams (RBDs)

- Success-oriented method that can provide a good visualization of simpler systems
- Show the functional configuration of the system
  - Which component(s) are required for the system to work
  - Which component(s) failure will cause the system to fail
- RBDs often correspond to the physical configuration of the system
  - **However**, there may be instances when the RBD does not model the physical configuration

RBDs: Series

- **Series System:**



  - When ***all*** of the items ***work***, system ***works***, that is:

$$R_s(t) = \Pr(\bar{A} \cap \bar{B} \cap \bar{C} \cap \cdots \cap \bar{Z})$$
$$R_s(t) = \Pr(R_A \cap R_B \cap R_C \cap \cdots \cap R_Z)$$

  - If these events are **independent** ($A \perp B \perp C \ldots$), this becomes:

$$R_s(t) = R_A(t) \cdot R_B(t) \cdot R_C(t) \cdot \ldots \cdot R_z(t)$$
$$R_s(t) = \prod_{i=1}^{n} R_i(t)$$

  - If they're not independent, use the chain rule of probability

RBDs: Series

- **MTTF of the System (under certain assumptions*):**
  - If each component has a **constant failure rate** (i.e., the times to failure, *t*, are exponentially distributed: $R_i(t) = e^{-\lambda_i t}$ for each component *i*) and they are independent.
  - The reliability of the system is:

$$R_s(t) = \prod_{i=1}^{n} e^{-\lambda_i t} = e^{-\sum_{i=1}^{n} \lambda_i t} = e^{-\lambda_s t}$$

  - Therefore: $\lambda_s = \sum_{i=1}^{n} \lambda_i$

$$MTTF_s = \frac{1}{\lambda_s} = \frac{1}{\sum_{i=1}^{n} \lambda_i}$$

  - ***If these assumptions aren't met, you would calculate MTTF using the formulas in Ch. 3, or another model we'll learn.***

$$MTTF = E(t) = \int_0^\infty x f_s(x)dx = (if \ \lim tf(t) \to 0) \int_0^\infty R_s(x)dx$$

RBDs: Series

- **For n independent & identically distributed (i.i.d) units** with constant failure rate (CFR):

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

$$\lambda_S = n\lambda$$

$$MTTF_S = \frac{1}{n\lambda}$$

Example: Series system

- **Example:**
- You have four-component series system, where the components are iid with constant failure rate. If $R_s(100 \text{ hrs})$ is 0.95, find the individual component $MTTF_i$ and the $MTTF_s$ of the system.

Example: Series system

- **Solution:** Four component series system where the components are iid with CFR. If R_s(100 hrs) is 0.95, find the individual component MTTF.

$$n = 4, \lambda_i = const., R_s(100) = 0.95$$

Find $MTTF_i$

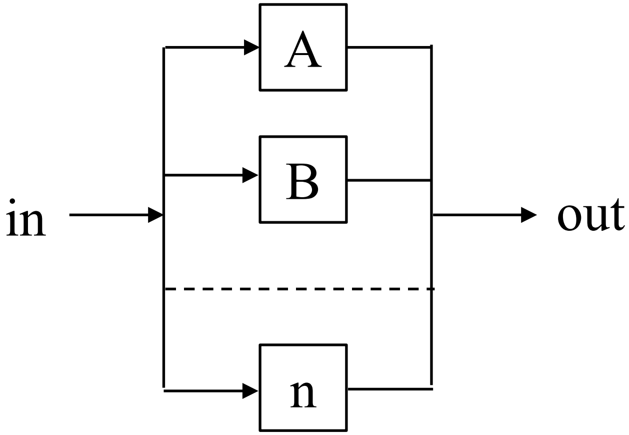
$$R_s = e^{-n\lambda_i t}$$
$$\ln(0.95) = -n\lambda_i t = -400\lambda_i$$
$$-.05129 = -400\lambda_i$$
$$\lambda_i = 1.28 \times 10^{-4}$$
$$\boldsymbol{MTTF_i = \frac{1}{\lambda_i} = 7798.29}$$

For comparison:

$$\boldsymbol{MTTF_S = \frac{1}{4 \cdot \lambda_i} = 1949.6hrs}$$

RBDs: Parallel

- **Parallel System**



- System fails when **all** the blocks fail:

$$F_s(t) = \Pr(F_A \cap F_B \cap F_C \ldots)$$
$$R_S(\mathrm{t}) = 1 - \Pr(F_A \cap F_B \cap F_C \ldots)$$

RBDs: Parallel

- *If* these events are **independent**, $(A \perp B \perp C \ldots)$, this becomes:

$$F_S(t) = F_A(t) \cdot F_B(t) \cdot F_C(t) \ldots = \prod_{i=1}^{n} F_i(t)$$

$$where\ F_i(t) = Unreliability\ of\ one\ component$$

$$R_S(t) = 1 - \prod_{i=1}^{n} F_i(t)$$

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

- As before, if they are not independent, use the chain rule.

RBDs: Parallel

- **MTTF of the System (under certain assumptions):**
  - If each component has a constant failure rate, (i.e., the times to failure are exponentially distributed; i.e., $R_i(t) = e^{-\lambda_i t}$), and they are independent.
  - **The hazard rate of a parallel system is not constant, so $\boldsymbol{MTTF_s \neq \frac{1}{\lambda_s}}$**

Dervice from $h_s(t) = \frac{f(t)}{R(t)} = \frac{-\frac{dR(t)}{dt}}{R(t)}$

$$MTTF_s = \int_0^\infty R_s(t)dt$$

  - For a parallel system of two components:

$$MTTF_s = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}$$

(See textbook for binomial expansion to derive for additional items).

RBDs: Parallel

- Special case: When all n components are i.i.d with CFR λ_i

$$R_s(t) = 1 - (1 - e^{-\lambda_i t})^n$$

$$MTTF_i = \frac{1}{\lambda_i}$$

$$\boxed{MTTF_s = MTTF_i\left(1 + \frac{1}{2} + \frac{1}{3} \dots + \frac{1}{n}\right)}$$

Example: Parallel system

- **Example:**
- Two parallel identical and independent components have CFR. It is desired that $R_s(1000hr) = 0.95$. Find the component $MTTF_i$ and the system $MTTF_s$.

Example: Parallel system

- **Solution:** Two parallel identical and independent components have CFR. It is desired that $R_s(1000hr) = 0.95$. Find the component $MTTF_i$ and the system $MTTF_s$.
- $R_s(1000hr) = 0.95 = 1 - (1 - e^{-\lambda_i t})^2$

$$0.05 = (1 - e^{-\lambda_i t})^2$$

$$\ln(0.05) = -2.99 = 2\ln(1 - e^{-\lambda_i t})$$

$$e^{(-2.99/2)} = 0.223 = 1 - e^{-\lambda_i t}$$

$$0.776 = e^{-\lambda_i t}$$

$$\lambda_i = 2.531e^{-4} \Rightarrow \boldsymbol{MTTF_i = 3951.1hr}$$

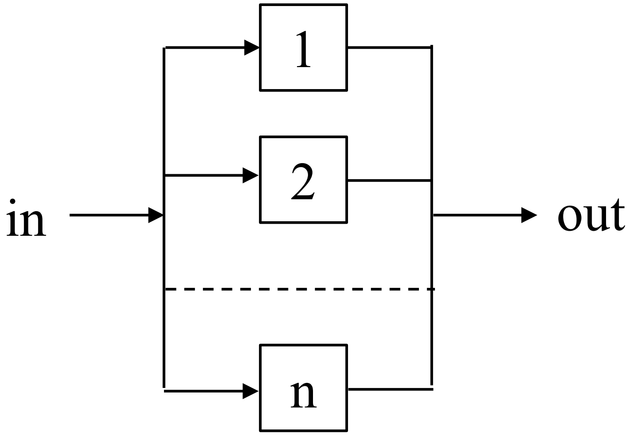
$$\boldsymbol{MTTF_s} = MTTF_i\left(1 + \frac{1}{2} + \frac{1}{3} \dots + \frac{1}{n}\right) = 3951.1 \cdot (1 + 0.5) = \boldsymbol{5926hr}$$

RBDs: *k*-out-of-*n* redundant system

- ***k*-out-of-*n* system**
  - If any of the **k** blocks **out of n** iid blocks **works** so that **the system works**, then:

$$R_s(t) = \sum_{x=k}^{n} \binom{n}{x} [R_i(t)]^x [1 - R_i(t)]^{n-x}$$

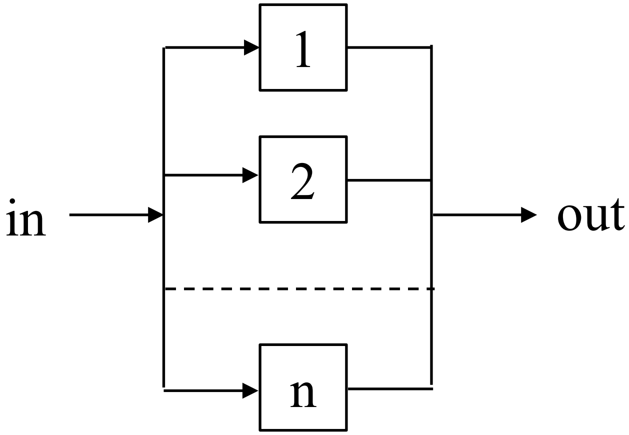
$$= 1 - \sum_{x=0}^{k-1} \binom{n}{x} [R_i(t)]^x [1 - R_i(t)]^{n-x}$$



  - Recall: $\binom{n}{x} = \frac{n!}{x!(n-x)!}$

Example (*k*-out-of-*n* redundant system)

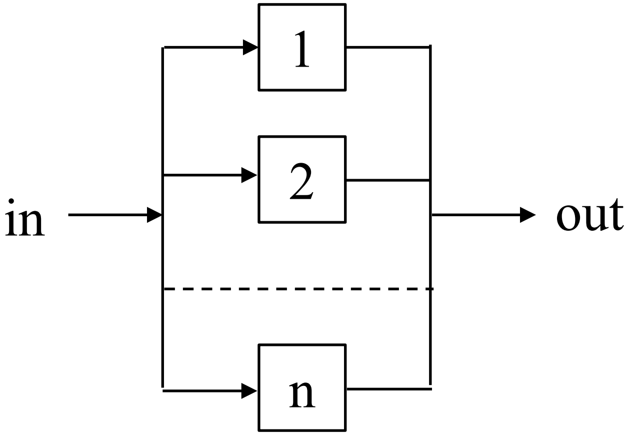
- **Example:** Calculate R_S the reliability of a system for a 2-out-of-3 for success case. Assume that the 3 components are i.i.d and each has reliability R.



Example (*k*-out-of-*n* redundant system): Solution

- **Solution:** Calculate R_S the reliability of a system for a 2-out-of-3 for success case. Assume that the 3 components are iid and each has reliability R.

  Given n = 3, k = 2



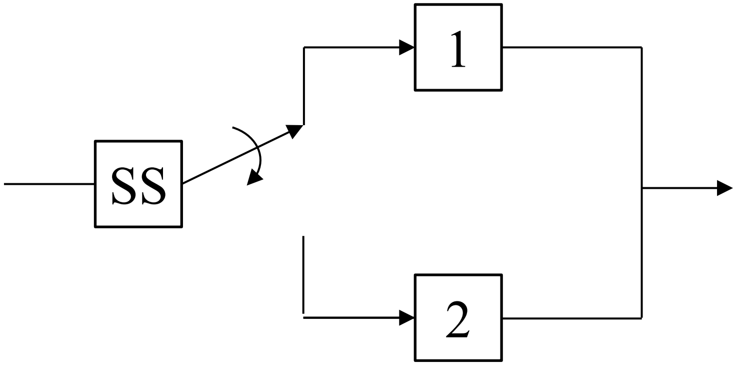
$$R_s(t) = \sum_{x=k}^{n} \binom{n}{x} [R_i(t)]^x [1 - R_i(t)]^{n-x}$$

$$R_s = \frac{3!}{2! \times 1!} (R)^2 (1 - R) + \frac{3!}{3! \times 0!} (R)^3 (1 - R)^0$$

$$= \mathbf{3(R)^2(1 - R) + R^3 = 3R^2 - 2R^3}$$

RBDs: Standby redundant system

- **Standby Redundant System**
  - For simplicity consider the two unit standby system pictured below.



  - Operation can be categorized as:

1. Block 1 operates until it fails
2. Sensing/switch recognizes Block 1 failure and switches to Block 2
3. Block 2 starts to operate (if it has not failed while on standby)
4. Block 2 ultimately fails

After Steps (1)-(4)→**System Fails**

RBDs: Standby system

- **Case I: Two-unit system. Imperfect switching, Standby failures can occur.** Different failure rates for during operation and during standby:

$$R \rightarrow in\ operation \rightarrow \lambda \qquad R' \longrightarrow in\ standby \longrightarrow \lambda'$$

$$R_s(t) = R_1(t) + \int_0^t \left\{ \underbrace{f_1(t_1)dt_1}_{A} \cdot \underbrace{R_{ss}(t_1)}_{B} \cdot \underbrace{R_2{}'(t_1)}_{C} \cdot \underbrace{R_2(t-t_1)}_{D} \right\}$$

  - $R_1(t)$→Reliability of Item 1 (Probability that it works until mission time t)
  - A → Probability that Item 1 fails at a time $t_1, t_1 < t$ (in a small time interval dt1)
  - B → Reliability of sensing and switching device at t_1(Probability that it works at t_1)
  - C → Probability that Item 2 does not fail while in standby mode (Reliability of Item 2 at time t_1)
  - D → Probability that Item 2 works until mission time t (Reliability of Item 2 from t_1 to t).

RBDs: Standby system

- For **independent components, with exponential dist. of TTF** with $\lambda_1, \lambda_2, \lambda'_2, \lambda_{ss}$

$$R_{sys}(t) = R_1(t) + \int_0^t f_1(t_1) R_{ss}(t_1) R'_2(t_1) R_2(t-t_1)\, dt_1$$

$$R_{sys}(t) = e^{-\lambda_1 t} + \int_0^t \lambda_1 e^{-\lambda_1 t_1} e^{-\lambda_{ss} t_1} e^{-\lambda'_2 t_1} \mathrm{e}^{-\lambda_2 (t-t_1)}\, dt_1$$

$$R_{sys}(t) = e^{-\lambda_1 t} + \lambda_1 e^{-\lambda_2 t} \int_0^t e^{-\lambda_1 t_1} e^{-\lambda_{ss} t_1} e^{-\lambda'_2 t_1} e^{-\lambda_2 t_1}\, dt_1$$

$$R_{sys}(t) = e^{-\lambda_1 t} + \lambda_1 e^{-\lambda_2 t} \left\{ \frac{-\mathrm{e}^{-[\lambda_1 + \lambda_{ss} + \lambda'_2 - \lambda_2] t_1}}{\lambda_1 + \lambda_{ss} + \lambda'_2 - \lambda_2} \Bigg|_0^t \right\}$$

$$\boxed{R_{sys}(t) = e^{-\lambda_1 t} + \left[\frac{\lambda_1 e^{-\lambda_2 t}}{\lambda_1 + \lambda_{ss} + \lambda'_2 - \lambda_2} \right] \left(1 - e^{-(\lambda_1 + \lambda_{ss} + \lambda'_2 - \lambda_2) t}\right)}$$

RBDs: Standby redundant

- **Case II: Perfect switch, no standby failure and iid units with CFR.**
  - This can be reduced to the so-called "***shock model***." In this case, "***shocks***" occur at a constant rate and the system fails after all blocks are failed. Shocks cause failure, the n^{th}shock causes the system to fail.

$$R_s(t) = 1 - \int_0^t \frac{\lambda^n}{\Gamma(n)} x^{n-1} e^{-\lambda x} dx \qquad [i.e., T_{fail} \sim dgamma\left(n, \frac{1}{\lambda}\right)]$$

  - When n is an integer, this becomes:

$$R_s(t) = e^{-\lambda t}\left[1 + \lambda t + \frac{(\lambda t)^2}{2!} + \frac{(\lambda t)^3}{3!} + \cdots + \frac{(\lambda t)^{n-1}}{(n-1)!}\right]$$

$$MTTF_s = \frac{n}{\lambda}$$

  - Recall: The $Gamma(\alpha, \frac{1}{\lambda})$ distribution is the convolution (the sum) of α exponentially (λ) distributed variables.

Example: Standby system

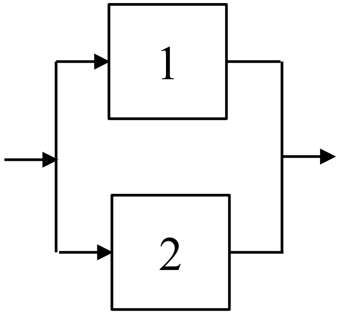
- **Example:** In a two-block standby system with perfect switch and no standby failures, if failure rate of each block is $\lambda = 0.001/hr$, which is the rate of occurrence of shocks, then find the MTTF of the system.

Example: Standby system

- **Solution:** In a two-block standby system with perfect switch and no standby failures, if failure rate of each block is $\lambda_i = 0.001/hr$, which is the rate of occurrence of shocks, then find the MTTF of the system.

$$MTTF_s = \frac{n}{\lambda_i} = \frac{2}{0.001} = 2000\ hours$$

RBDs: Shared load



- **Shared Load System**
  - Initially both items share the load, with identical times to failure distribution being $f_h(t)$. When one item fails, other item operates at a higher stress (i.e., full load) and has increased failure rate, with time to failure distribution $f_f(t)$.

$$R_s(t) = \underbrace{[R_h(t)]^2}_{A} + 2\int_0^t \left\{\underbrace{f_h(t_1)dt_1}_{B} \cdot \underbrace{R_h(t_1)}_{C} \cdot \underbrace{R_f(t-t_1)}_{D}\right\}$$

  - Probability that:
    - A → Both items remain operational in half load until mission time *t*
    - B → One item fails in half load at $t_1, t_1 < t$
    - C → The other item works at half load until $t_1, t_1 < t$
    - D → The other item works at full load after t_1 until mission time *t*

RBDs: Shared load

- Example of Shared Load System
  - If both items have **exponential time-to-failure** model with failure rates:

$\lambda_h \rightarrow$ half load failure rate $\qquad R_h(t) = e^{-\lambda_h t}$

$\lambda_f \rightarrow$ full load failure rate $\qquad R_f(t) = e^{-\lambda_f t}$

$$R_{sys}(t) = e^{-2\lambda_h t} + 2\int_0^t \lambda_h e^{-\lambda_h t_1} e^{-\lambda_h t_1} e^{-\lambda_f (t-t_1)} dt_1$$

$$R_{sys}(t) = e^{-2\lambda_h t} + 2\lambda_h e^{-\lambda_f t} \int_0^t \mathrm{e}^{-(2\lambda_h-\lambda_f)t_1} dt_1$$

$$R_{sys}(t) = e^{-2\lambda_h t} + 2\lambda_h e^{-\lambda_f t} \left\{\frac{\mathrm{e}^{-(2\lambda_h-\lambda_f)t_1}}{-(2\lambda_h-\lambda_f)}\right\}\Bigg|_0^t$$

$$\boxed{R_{sys}(t) = e^{-2\lambda_h t} + \left[\frac{2\lambda_h e^{-\lambda_f t}}{(2\lambda_h-\lambda_f)}\right]\left[1 - e^{-(2\lambda_h-\lambda_f)t}\right]}$$

$$if\ 2\lambda_h - \lambda_f > 0, then\ MTTF = \int_0^\infty R_s(t)dt$$

Example: Shared load

- **Example:** For a two-unit shared load system with $\lambda_h = 0.002, \mathrm{hr}^{-1}$ $\lambda_f = 0.003\ hr^{-1}$
  a) Find the Reliability at t=500 hr
  b) Find $MTTF_s$

Example Shared load: Solution

a) $R_s(t) = e^{-2\lambda_h t} + \left[\frac{2\lambda_h e^{-\lambda_f t}}{(2\lambda_h - \lambda_f)}\right]\left[1 - e^{-(2\lambda_h - \lambda_f)t}\right]$

- With t=500, $\lambda_h = 0.002, \lambda_f = 0.003$: **R(t=500)**=0.135+(.893)(.393)=**0.487**

b) MTTF

- Recall: $R_s(t) = e^{-2\lambda_h t} + \left[\frac{2\lambda_h e^{-\lambda_f t}}{(2\lambda_h - \lambda_f)}\right]\left[1 - e^{-(2\lambda_h - \lambda_f)t}\right]$
- Since $(2\lambda_h - \lambda_f > 0)$, we can use $MTTF = \int_0^\infty R_s(t)dt$:

$$MTTF = \int_0^\infty \left\{ e^{-2\lambda_h t} + \left[\frac{2\lambda_h e^{e^{-\lambda_f t}}}{(2\lambda_h - \lambda_f)}\right]\left[1 - e^{-(2\lambda_h - \lambda_f)t}\right] \right\} dt$$

$$= \frac{-1}{2\lambda_h} e^{-2\lambda_h t} - \frac{2\lambda_h e^{-\lambda_f t}}{\lambda_f(2\lambda_h - \lambda_f)} + \frac{2\lambda_h e^{-2\lambda_h t}}{2\lambda_h(2\lambda_h - \lambda_f)} \Bigg|_0^\infty \quad Since\ e^{-\lambda_f t} e^{-(2\lambda_h - \lambda_f)t} = e^{-2\lambda_h t}$$

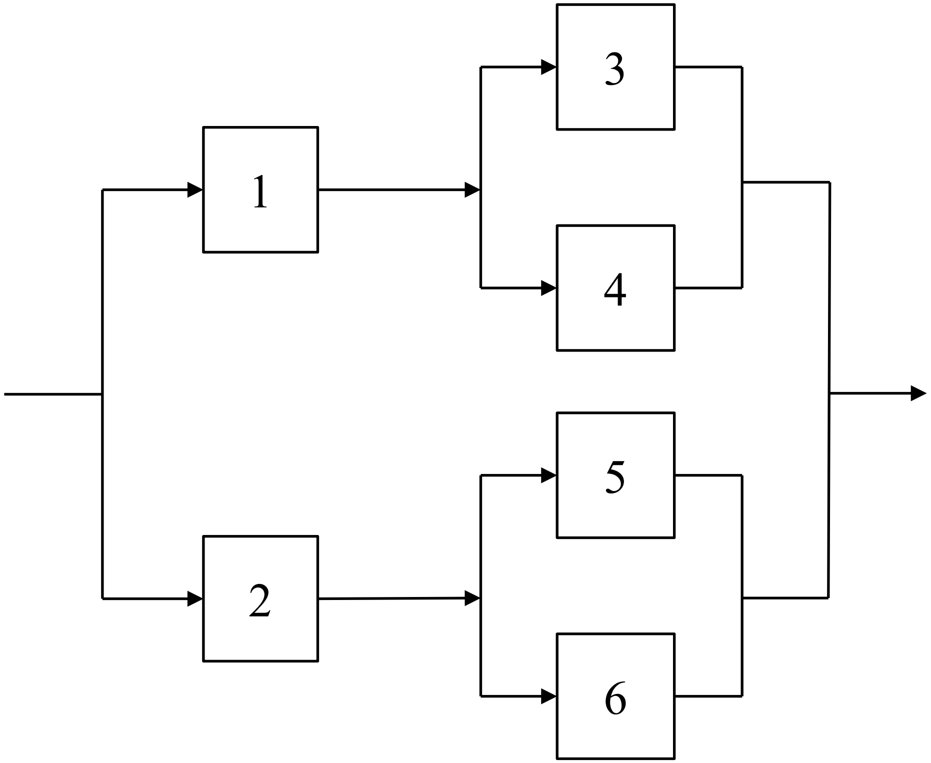
$$= \frac{1}{2\lambda_h} + \frac{2\lambda_h}{\lambda_f(2\lambda_h - \lambda_f)} - \frac{1}{2\lambda_h - \lambda_f}$$

$$MTTF = \frac{1}{2(0.002)} + \frac{2(0.002)}{0.003 + (2(0.002) - 0.003)} - \frac{1}{(2(0.002 - 0.003)}$$

$$= 250 + 1{,}333.33 - 1000 = 583.33\ hrs$$

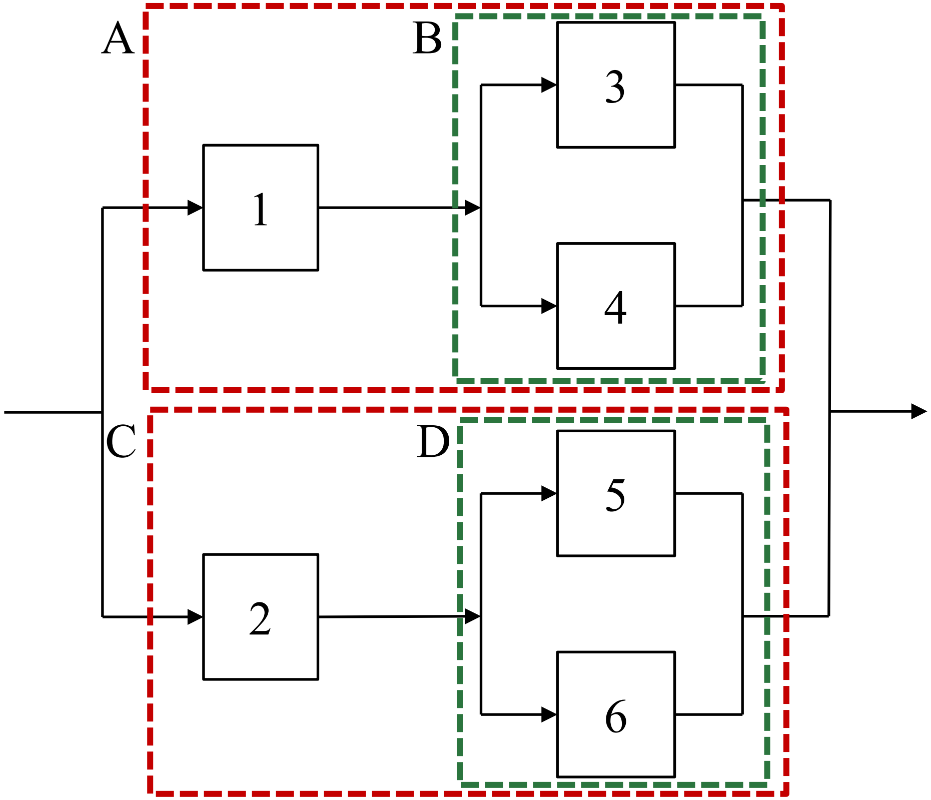
Complex Systems

- Putting it together: Reliability of Parallel-Series Systems.
  - There are some systems which are neither series nor parallel systems, but are some combination of these patterns.



Complex systems: Series, parallel reduction

- **Method 1: Decomposition (Series, parallel reduction)**
  - Decomposing the system into a combination of series, parallel blocks.
  - For the example here: Blocks A, B, C, D.



Complex systems: Series, parallel reduction

- **Example**
  - For the example at right: Blocks are A, B, C, D

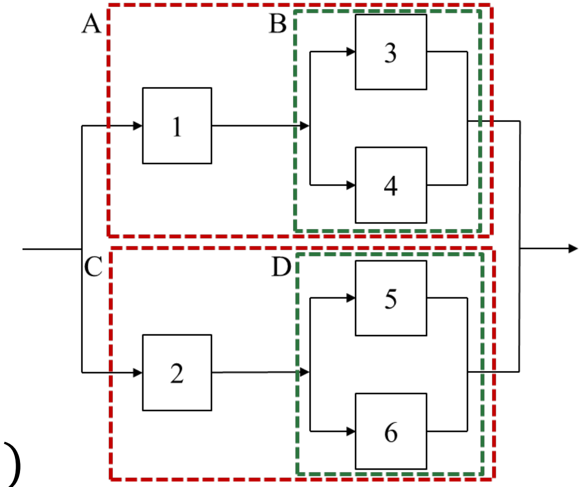
$A \parallel C$

$R_S = 1 - (1 - R_A)(1 - R_C) = R_A + R_C - R_A R_C$

$R_A = R_1 R_B = R_1(R_3 + R_4 - R_3 R_4)$

$R_C = R_2 R_D = R_2(R_5 + R_6 - R_5 R_6)$

$$\boldsymbol{R_S = R_1(R_3 + R_4 - R_3 R_4) + R_2(R_5 + R_6 - R_5 R_6) - R_1 R_2 (R_3 + R_4 - R_3 R_4)(R_5 + R_6 - R_5 R_6)}$$



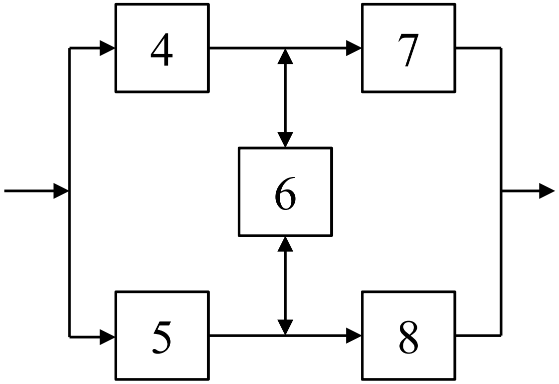
- If $R_i(t) = e^{(-\lambda_i t)}$:

$$R_s(t) = e^{-\lambda_1 t}\left(e^{-\lambda_3 t} + e^{-\lambda_4 t} - e^{-(\lambda_3+\lambda_4)t}\right) + e^{-\lambda_2 t}\left(e^{-\lambda_5 t} + e^{-\lambda_6 t} - e^{-(\lambda_5+\lambda_6)t}\right) - e^{-(\lambda_1+\lambda_2)t}\left[e^{-\lambda_3 t} + e^{-\lambda_4 t} - e^{-(\lambda_3+\lambda_4)t}\right]\left[e^{-\lambda_5 t} + e^{-\lambda_6 t} - e^{-(\lambda_5+\lambda_6)t}\right]$$

$$MTTF = \int_0^\infty R_s(t)dt$$

Complex systems: Decomposition

- **Method 1: Decomposition (Non-Series Parallel Systems)**
  - The system is analyzed by reducing it into parallel-series systems. Conditional probability is used to modify it to parallel-series system.
    - Recall: the law of total probability $\Pr(X) = \Pr(X \cap Y) + \Pr(X \cap \overline{Y})$
    - And the definition: $\Pr(X \cap Y) = \Pr(X|Y)\Pr(Y)$

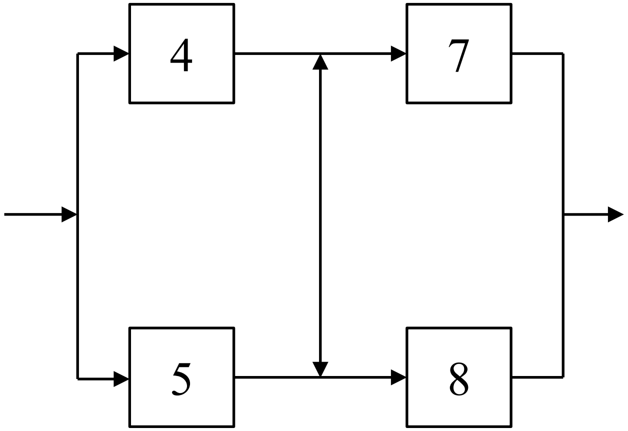


$$R_s(t) = \underbrace{R_s(t|item\ 6\ works)}_{\boldsymbol{A}} \cdot R_6(t) + \underbrace{R_s(t|item\ 6\ fails)}_{\boldsymbol{B}} \cdot [1 - R_6(t)]$$

- Item 6 works => $\overline{6}$ or R_6
- Item 6 fail => 6 or F_6

Decomposition

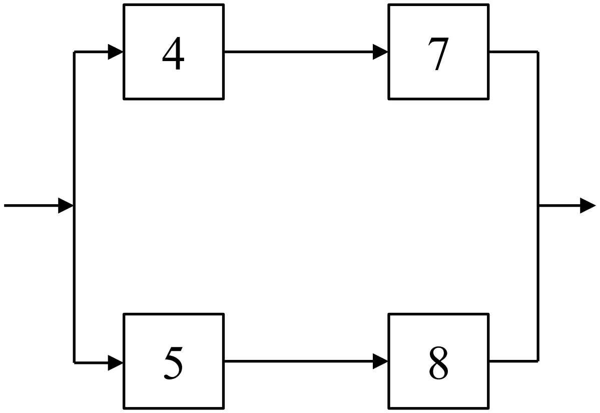
- Quantity A (item 6 works) represents:



- $R_A = R_s(t|\bar{6}) = (R_4 + R_5 - R_4 R_5) \cdot (R_7 + R_8 - R_7 R_8)$

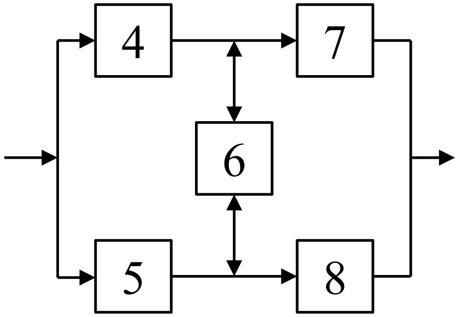
Decomposition (cont.)

- Quantity B (item 6 fails) represents:



- $R_B = R_s(t|6) = R_4R_7 + R_5R_8 - R_4R_5R_7R_8$

Decomposition (cont.)



- Putting it all together:

$$R_s(t) = \underbrace{R_s(t|\bar{6})}_{\boldsymbol{A}} \cdot\ R_6(t) + \underbrace{R_s(t|6)}_{\boldsymbol{B}} \cdot [1 - R_6(t)]$$

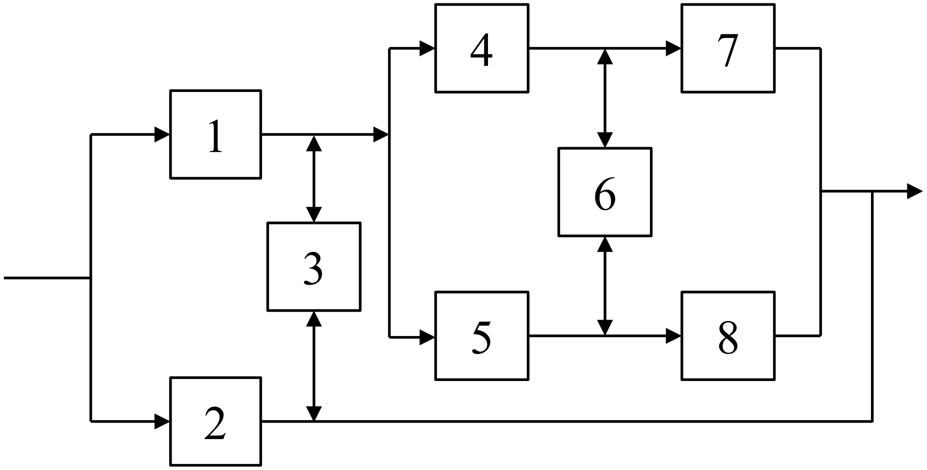
$$\boldsymbol{R_s(t)}$$
$$= (\boldsymbol{R_4} + \boldsymbol{R_5} - \boldsymbol{R_4 R_5})(\boldsymbol{R_7} + \boldsymbol{R_8} - \boldsymbol{R_7 R_8})\boldsymbol{R_6} + (\boldsymbol{R_4 R_7} + \boldsymbol{R_5 R_8} - \boldsymbol{R_4 R_5 R_7 R_8})[\mathbf{1} - \boldsymbol{R_6}]$$

- If all $R_i(t = 50) = 0.9, R_A = 0.9801$ and $R_B = 0.9639$

$$\boldsymbol{R_S(t = 50) = 0.9801 \cdot 0.9 + 0.9639 \cdot 0.1 = 0.9785}$$

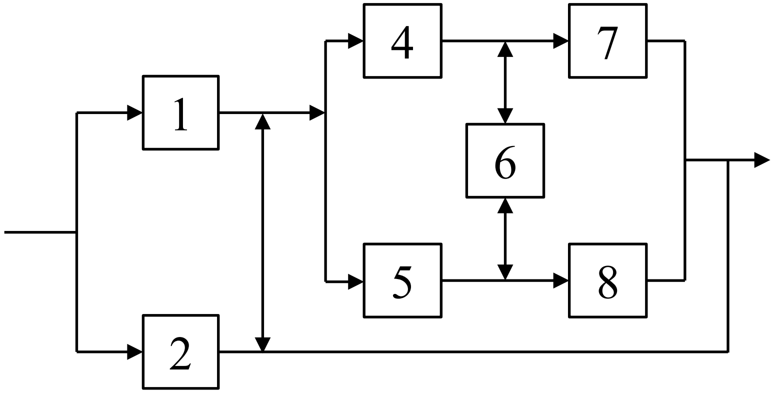
We can do this for increasingly large systems

- **Example (after class):** Conduct decomposition on the RBD below.
  - Hint: Use $R_s(t) = \underbrace{R_s(t|item\ 3\ works)}_{C} \cdot\ R_3(t) + \underbrace{R_s(t|item\ 3\ fails)}_{D} \cdot [1 - R_3(t)]$
  - Hint: Use your solution from our previous example involving 45678

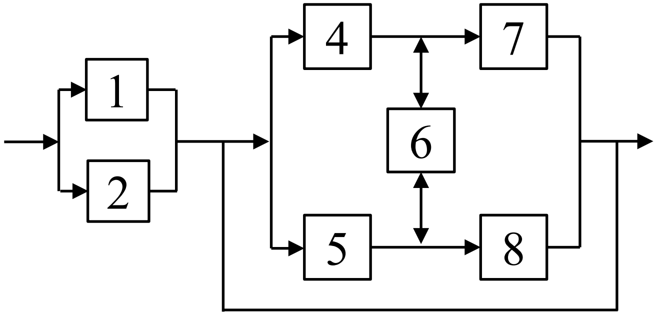


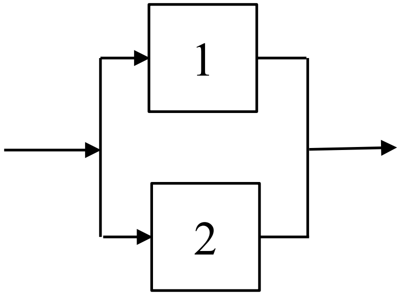
Example Solution: (after class)

- Quantity C (unit 3 good) represents:



- When we redraw, it become evident that this is a simple 2-unit parallel system

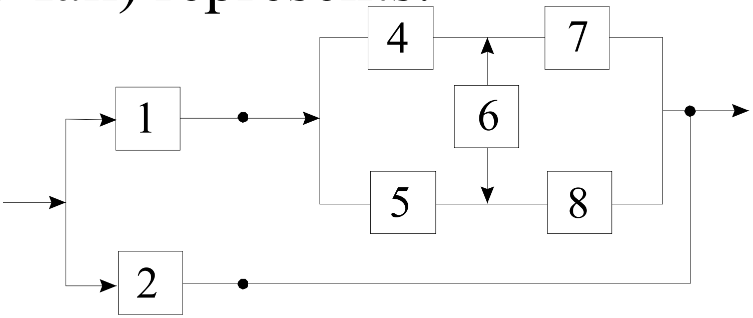




- $R_s(t|\bar{3}) = R_1 + R_2 - R_1 R_2$

Example Solution: (after class)

- Quantity D (item 3 fail) represents:



- We can use the decomposition of S45678 from before.
- Thus, we have:

$$R_D = R_s(t|3) = R_1 R_{s45678} + R_2 - R_1 R_2 R_{s45678}$$

$=R_1((R_4 + R_5 - R_4R_5)(R_7 + R_8 - R_7R_8)R_6 + (R_4R_7 + R_5R_8 - R_4R_5R_7R_8)[1 - R_6]) + R_2 - R_1R_2[(R_4 + R_5 - R_4R_5)(R_7 + R_8 - R_7R_8)R_6 + (R_4R_7 + R_5R_8 - R_4R_5R_7R_8)[1 - R_6]]$

And if we put it all together w/previous slides:

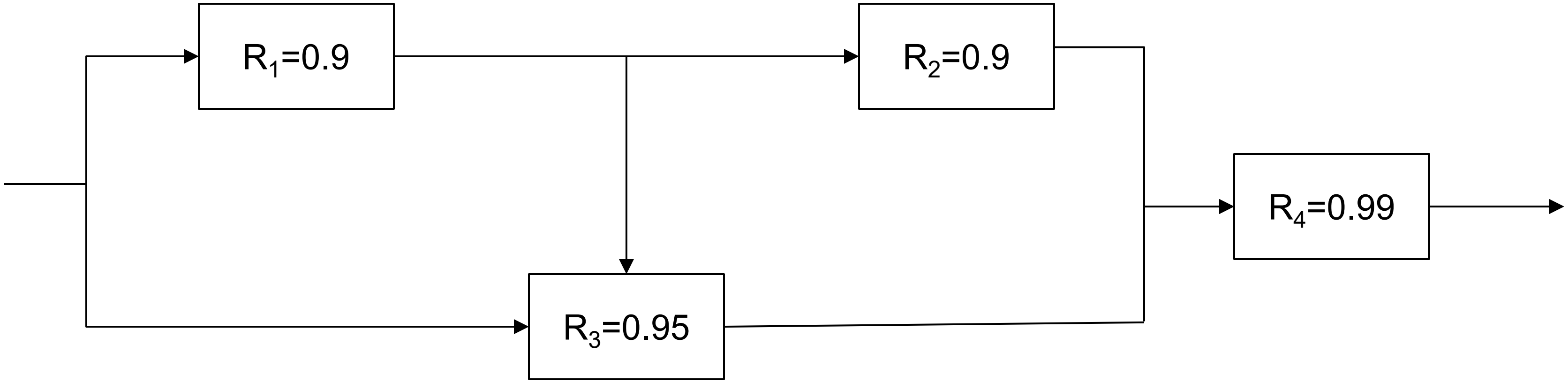
$$\boldsymbol{R_s(t) = [R_1 + R_2 - R_1R_2]R_3 + R_D \cdot [1 - R_3]}$$

Using $R_i(50) = 0.9$ again for all components:

$$\boldsymbol{R_s(50) = 0.99 \cdot 0.9 + (0.9 \cdot 0.9785 + 0.9 - 0.9 \cdot 0.9 \cdot 0.9785) \cdot 0.1 = 0.9899}$$

Extra example (for after class)

- Determine the reliability of the following system using the decomposition method:



Extra example (for after class)

- Solution: Split the system into:
  - $Rs = (R_s | R_3 = 1) * R_3 + (R_s | \bar{R}_3)(1 - R_3).$

$$R_S = R_3 R_4 + (1 - R_3)(R_1)(R_2)(R_4)$$
$$\boldsymbol{R_S = R_3 R_4 + R_1 R_2 R_4 - R_1 R_2 R_3 R_4}$$
$$= 0.9806$$
$$\boldsymbol{R_S = 0.981}$$

- (Another method of solving this is to realize that the link from R_1 to R_3 is essentially irrelevant, and the two parts of the system can be viewed as ($R_1 R_2$ in parallel with R_3) then in series with R_4.

Complex systems: Path sets & cut sets

- **Complex Systems: Methods 2 & 3: Path sets & Cut sets**
  - **Path sets:** The set of paths (successes) that form a connection from input to output—aka guarantee system operation.
  - **Cut sets:** The set of unit (failures) which interrupt all possible connections between input and output—aka guarantee system failure.
  - **Minimal path- or cut-set:** The minimum number to guarantee connection (or disconnection)
  - Be very careful about your notation. When in doubt, define it at the top of your problem.
  - If X denotes component failure, you should have:

$$X \text{ in a cut set, but } \overline{X} \text{ in a path set}$$

Notes on path sets & cut sets

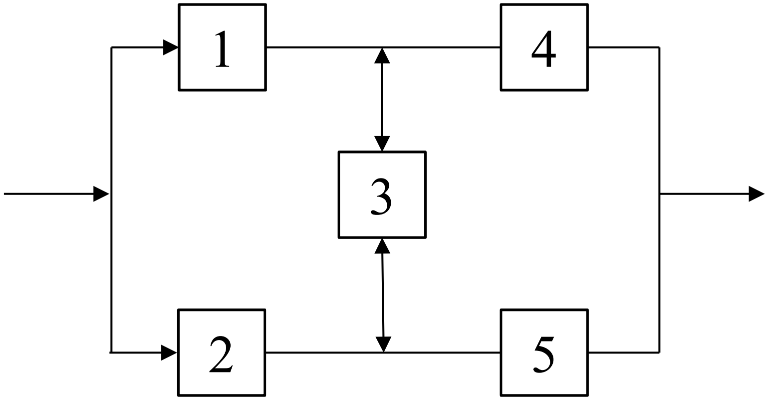
- Quantification with the cut or path sets uses the *minimal* cut sets of *minimal* path sets.
- **The *order* of the sets** denotes how many terms are in that set.
  - E.g., a cut set which contains two elements (A, B) has order 2.
- *A lot of qualitative insights can be gained from the cut sets before you start quantifying – e.g., whether your system has any single point failures (cut sets of order 1), how many cut sets a certain component appears in, etc.*

Example: Path sets & cut sets

- **Complex Systems: Methods 2 & 3: [Minimal] Path sets & Cut sets**

Minimal Path Sets

Minimal Cut Sets



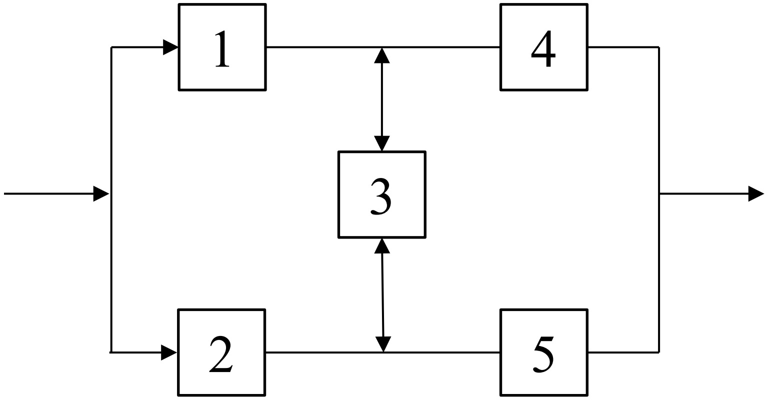
Example: Path sets & cut sets: Solution

- For the system the minimal path sets are:

$$P_1 = \{\overline{1}, \overline{4}\}, P_2 = \{\overline{2}, \overline{5}\}, P_3 = \{\overline{1}, \overline{3}, \overline{5}\}, P_4 = \{\overline{2}, \overline{3}, \overline{4}\}$$

- And the minimal cut sets are:

$$C_1 = \{1,2\}, C_2 = \{4,5\}, C_3 = \{2,3,4\}, C_4 = \{1,3,5\}$$



Path sets: Quantification

- **For path sets**: The system fails when none of the (minimal) path sets, P_i, works.
- Notation:
  - $Pr(\overline{\mathrm{P}_{\mathrm{i}}}) = Pr_F(P_i)$ = Probability that min. path i (P_i) is not successful (not available)
  - $Pr(P_i) = Pr_S(P_i)$= Probability that min. path i (P_i) is successful (available)

$$\boxed{\begin{array}{c} \boldsymbol{R_s = \Pr(P_1 \cup P_2 \cup P_3 \cup \cdots \cup P_m)} \\ R_s = 1 - Pr(\overline{P_1} \cap \overline{P_2} \cap \overline{P_3} \cap \overline{P_4}) \end{array}}$$

  - **If all min. path sets are mutually exclusive (which usually isn't true):**

$$R_s = \Pr(P_1) + \Pr(P_2) + \Pr(P_3) + \Pr(P_4)$$

  - **If they're not, we can treat this as an upper bound on reliability:**

$$R_s \leq \Pr(P_1) + \Pr(P_2) + \Pr(P_3) + \Pr(P_4)$$

  - **If the min. path sets are independent, this becomes:**

$$R_s = 1 - \Pr\left(\overline{P_1}\right)\Pr(\overline{P_2})\Pr(\overline{P_3})\Pr(\overline{P_4})$$

$$R_S = 1 - [1 - \Pr(P_1)][1 - \Pr(P_2)][1 - \Pr(P_3)][1 - \Pr(P_4)]$$

  - **If path sets are not independent, this is an upper bound on reliability.**

Cut sets: Quantification

- **For cut sets**: The system fails if one of the minimal cut sets occurs
- Notation
  - $\Pr(C_i)$ = Probability that min. cut set i (C_i) occurs
  - Therefore,

$$\boxed{\begin{array}{c} F_s(t) = \Pr(C_1 \cup C_2 \cup C_3 \cup C_4) \\ R_s(t) = 1 - \Pr(C_1 \cup C_2 \cup C_3 \cup C_4) \end{array}}$$

  - If the cut sets are mutually exclusive (…not usually true):

$$R_s(t) = 1 - (\Pr(C_1) + \Pr(C_2) + \Pr(C_3) + \Pr(C_4))$$

  - If they're not:

$$R_s(t) \geq 1 - (\Pr(C_1) + \Pr(C_2) + \Pr(C_3) + \Pr(C_4))$$

Rare event approximation

- The **rare event approximation** allows us to eliminate some terms to significantly simplify the math.
- Recall that probability of the union of two events (given by addition law of probability) is:

$$\Pr(A \cup B) = \Pr(A) + \Pr(B) - \Pr(A \cap B)$$

$$\text{If } A \perp B\text{, this becomes} = \Pr(A) + \Pr(B) - \Pr(A)\Pr(B)$$

- Or in compact form: $\Pr(A \cup B) = (1 - [1 - \Pr(A)][1 - \Pr(B)])$
- If we have *rare events*, the term $\Pr(A)\Pr(B)$ is very small.

$$\Pr(A \cup B) = \Pr(A) + \Pr(B) - \underbrace{\Pr(A)\Pr(B)}_{\substack{\text{eliminate this} \\ \text{term for rare} \\ \text{events.}}}$$

$$\boxed{\Pr(A \cup B) \approx \Pr(A) + \Pr(B)}$$

- **General rule for "rare":** $\Pr(E_i) < \frac{1}{50n}$ *where* $n = \#$ *of events*

System reliability analysis (cont.)

- When **rare event approximation** is applied (or if we assume the error from assuming mutual exclusivity of sets is small):

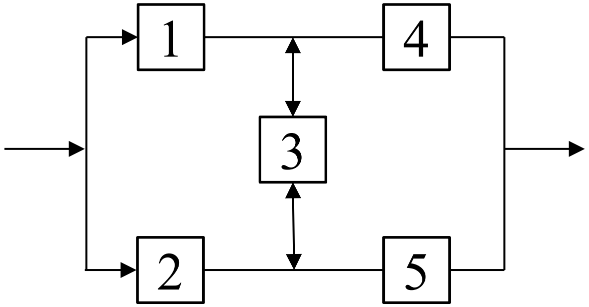
$$R_s^{cutset} < R_s < R_s^{pathset}$$

- Therefore, cut sets give the lower bound of reliability, whereas path sets give the upper bound of reliability.

Example Part 2: Path sets and cut sets

- **Example:** Use both the cut set and path set methods to find the upper and lower bounds for reliability for the system at time *t*, for the system with minimal path sets $P_1 = \{\overline{1}, \overline{4}\}, P_2 = \{\overline{2}, \overline{5}\}, P_3 = \{\overline{1}, \overline{3}, \overline{5}\}, P_4 = \{\overline{2}, \overline{3}, \overline{4}\}$ and minimal cut sets $C_1 = \{1, 2\}, C_2 = \{4, 5\}, C_3 = \{2, 3, 4\}, C_4 = \{1, 3, 5\}$

Assume the units are independent of each other, $1 \perp 2 \perp 3 \perp 4 \perp 5$



Example Part 2: Path sets and cut sets

- **Solution:** Using the cut sets $C_1 = \{1, 2\}, C_2 = \{4, 5\}, C_3 = \{2, 3, 4\}, C_4 = \{1, 3, 5\}$

$$R_s(t) = 1 - \Pr(C_1 \cup C_2 \cup C_3 \cup C_4)$$

$$R_s(t) \geq 1 - \left[\underbrace{Pr_f(C_1)}_{(1-R_1)(1-R_2)}\right] + \left[\underbrace{Pr_f(C_2)}_{(1-R_4)(1-R_5)}\right] + \left[\underbrace{Pr_f(C_3)}_{(1-R_2)(1-R_3)(1-R_4)}\right] + \left[\underbrace{Pr_f(C_4)}_{(1-R_1)(1-R_3)(1-R_5)}\right]$$

$$R_s(t) \geq 1 - \begin{bmatrix} (1-R_1)(1-R_2) + \\ (1-R_4)(1-R_5) + \\ (1-R_2)(1-R_3)(1-R_4) + \\ (1-R_1)(1-R_3)(1-R_5) \end{bmatrix}$$

Example Part 2: Path sets & cut sets

- **Solution:** Using the path sets$P_1 = \{\overline{1}, \overline{4}\}, P_2 = \{\overline{2}, \overline{5}\},\ \ P_3 = \{\overline{1}, \overline{3}, \overline{5}\}, P_4 = \{\overline{2}, \overline{3}, \overline{4}\}$

$$R_s \leq 1 - Pr_f\left(\overline{P_1}\right)Pr_f\left(\overline{P_2}\right)Pr_f\left(\overline{P_3}\right)Pr_f\left(\overline{P_4}\right)$$

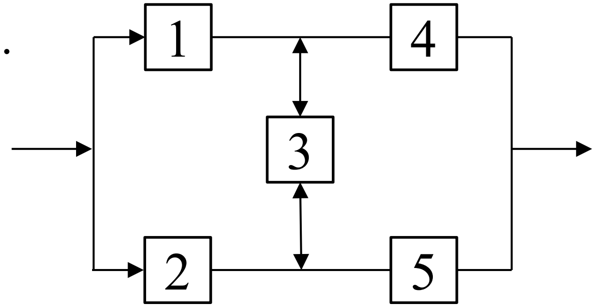
$$R_s \leq 1 - [1 - Pr_s(P_1)][1 - Pr_s(P_2)][1 - Pr_s(P_3)][1 - Pr_s(P_4)]$$

$$\boldsymbol{R_s(t) \leq 1 - [1 - R_1(t)R_4(t)][1 - R_2(t)R_5(t)][1 - R_1(t)R_3(t)R_5(t)]}$$
$$\boldsymbol{[1 - R_2(t)R_3(t)R_4(t)]}$$

Truth Tables

Method 4:

- List every possible combination of component states & system failures.
  - **Pros:** Mutually exclusive!
  - **Cons:** This gets long. 2^n combinations for a system with n components and binary (2) states.
- A truth table for our example is shown at right with $\Pr(F_i) = 0.01$ for all components.



Seq. Number	1	2	3	4	5	Combination	System Operation	Probability
1	S	S	S	S	S	$R_1R_2R_3R_4R_5$	S	0.59019
2	F	S	S	S	S	$F_1R_2R_3R_4R_5$	S	0.06531
3	S	F	S	S	S	$R_1F_2R_3R_4R_5$	S	0.06561
4	S	S	F	S	S	$R_1R_2F_3R_4R_5$	S	0.06561
5	S	S	S	F	S	$R_1R_2R_3F_4R_5$	S	0.06561
6	S	S	S	S	F	$R_1R_2R_3R_4F_5$	S	0.06561
7	F	F	S	S	S	$F_1F_2R_3R_4R_5$	F	0.00729
8	F	S	F	S	S	$F_1R_2F_3R_4R_5$	S	0.00729
9	F	S	S	F	S	$F_1R_2R_3F_4R_5$	S	0.00729
10	F	S	S	S	F	$F_1R_2R_3R_4F_5$	S	0.00729
11	S	F	F	S	S	$R_1F_2F_3R_4R_5$	S	0.00729
12	S	F	S	F	S	$R_1F_2R_3F_4R_5$	S	0.00729
13	S	F	S	S	F	$R_1F_2R_3R_4F_5$	S	0.00729
14	S	S	F	F	S	$R_1R_2F_3F_4R_5$	S	0.00729
15	S	S	F	S	F	$R_1R_2F_3R_4F_5$	S	0.00729
16	S	S	S	F	F	$R_1R_2R_3F_4F_5$	F	0.00729
17	F	F	F	S	S	$F_1F_2F_3R_4R_5$	F	8.10E-04
18	F	F	S	F	S	$F_1F_2R_3F_4R_5$	F	8.10E-04
19	F	F	S	S	F	$F_1F_2R_3R_4F_5$	F	8.10E-04
20	F	S	F	F	S	$F_1R_2F_3F_4R_5$	S	8.10E-04
21	F	S	F	S	F	$F_1R_2F_3R_4F_5$	F	8.10E-04
22	F	S	S	F	F	$F_1R_2R_3F_4F_5$	F	8.10E-04
23	S	F	F	F	S	$R_1F_2F_3F_4R_5$	F	8.10E-04
24	S	F	F	S	F	$R_1F_2F_3R_4F_5$	S	8.10E-04
25	S	F	S	F	F	$R_1F_2R_3F_4F_5$	F	8.10E-04
26	S	S	F	F	F	$R_1R_2F_3F_4F_5$	F	8.10E-04
27	F	F	F	F	S	$F_1F_2F_3F_4R_5$	F	9.00E-05
28	F	F	F	S	F	$F_1F_2F_3R_4F_5$	F	9.00E-05
29	F	F	S	F	F	$F_1F_2R_3F_4F_5$	F	9.00E-05
30	F	S	F	F	F	$F_1R_2F_3F_4F_5$	F	9.00E-05
31	S	F	F	F	F	$R_1F_2F_3F_4F_5$	F	9.00E-05
32	F	F	F	F	F	$F_1F_2F_3F_4F_5$	F	1.00E-05

$$\sum Pr = \Pr(S) + \Pr(F) = 1.00$$

$$\Pr(F) = 2.15 \times 10^{-2}$$

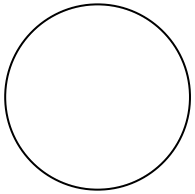
Logic trees

- **Fault Trees (FT) & Success Trees, Event Trees (ET)**
  - RBDs become very complex to use when number of units increases; this motivates the use of other types of models like FTs and ETs.
  - FT Analysis (FTA) is a deductive method – deducing how component failures contribute to a top event.
  - Approach: Top-down decomposition of the logic of a system (failure or success)
    - Many equivalent trees are possible
  - Only includes important events – not all postulated failures included.
    - What is important is a function of industry procedures and assumptions, system design, available data, analysis choices…
  - The FT is a qualitative model of the system logic, but we use quantitative algorithms to evaluate it (e.g., cut set method).

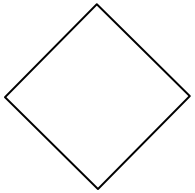
Fault tree analysis steps

1. Define the system to be analyzed & its boundaries
2. Define the top event
3. Construct the fault tree
4. Perform qualitative evaluation of fault tree (logic evaluation)
5. Perform quantitative evaluation of the FT (compute probability of top event)

Logic trees: event symbols

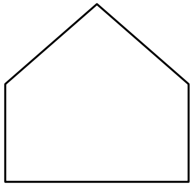


Basic Event



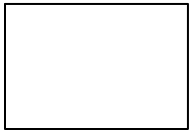
Undeveloped Event

Not developed further because it is of insufficient consequence, or because information is not available.



External Event

External but normally expected to occur.



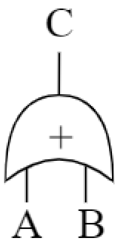
Intermediate Event

Provided for explanation only.

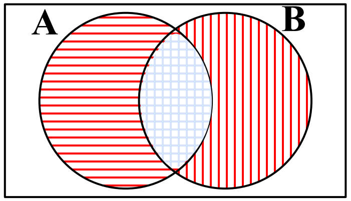
Logic tree analysis: Gates (1)

- Top-down deductive decomposition of a failure into basic causes of failure using Boolean Logic

Gates (Logic Representation) in Logic Trees



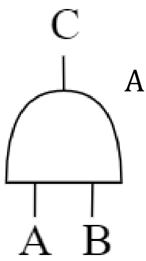
OR gate



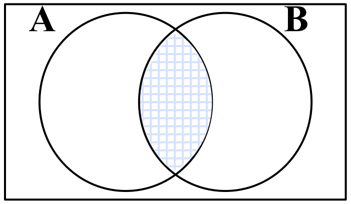
Union Operation

$C = A \cup B$

$C = A + B$



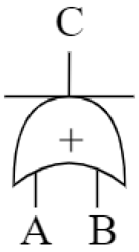
AND gate



Intersection Operation

$C = A \cap B$

$C = A \cdot B$

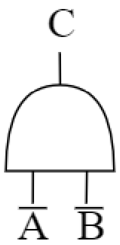


NOT OR gate
NOR

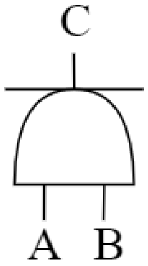
$C = \overline{A \cup B}$

$C = \bar{A} \cap \bar{B}$

$C = \bar{A} \cdot \bar{B}$



Input 1	Input 2	Output
		1
	1	
1		
1	1	

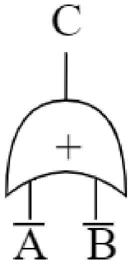


NOT AND gate
NAND

$C = \overline{A \cap B}$

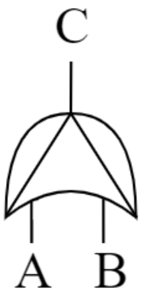
$C = \bar{A} \cup \bar{B}$

$C = \bar{A} + \bar{B}$

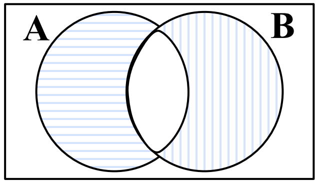


Input 1	Input 2	Output
		1
	1	1
1		1
1	1	

Logic tree analysis: Gates (2)

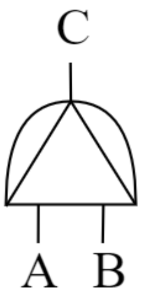


Exclusive OR gate



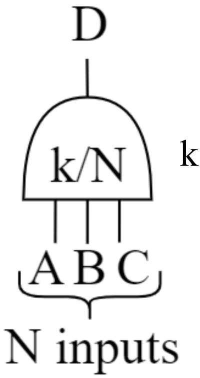
$$C = (A \cap \bar{B}) \cup (\bar{A} \cap B)$$
$$C = (A \cdot \bar{B}) + (\bar{A} \cdot B)$$

Input 1	Input 2	Output
	1	1
1		1
1	1	



Priority AND gate

Output C occurs if all of the inputs occur in a specific order (the order usually indicated by a conditioning event): A occurs first, and then B occur



k-out-of-N gate

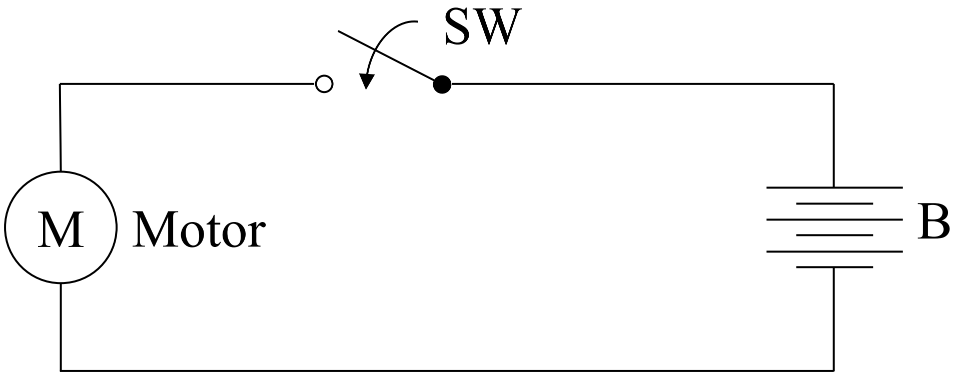
If any k combination of the inputs occur, then the output will occur

For a k=2, N=3 2-out-of-3 gate:

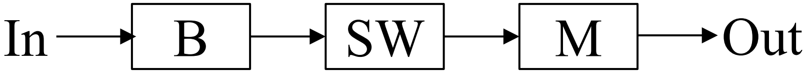
$$D = (A \cap B) \cup (A \cap C) \cup (B \cap C)$$
$$D = (A \cdot B) + (A \cdot C) + (B \cdot C)$$

Example: Fault tree analysis

- **Example**: A motor system, wherein a motor is powered by a battery, connected by a switch. Assume independence of the components.



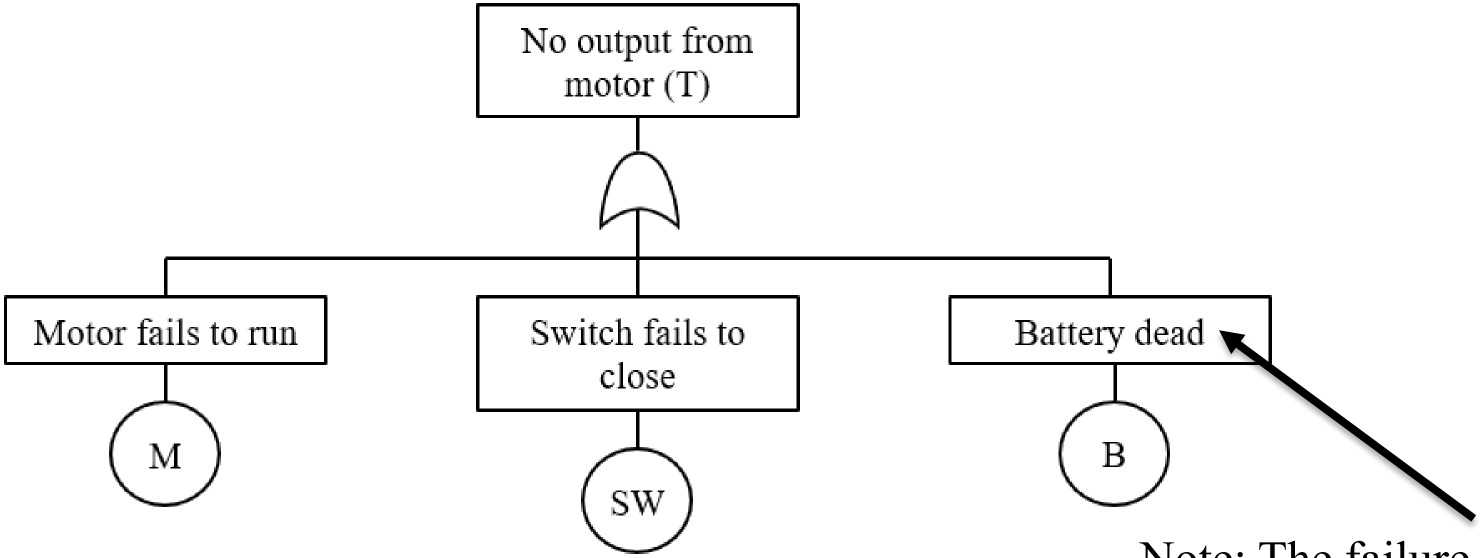
The system can be represented as a series model in a block diagram form



- **Part 1:** Draw a fault tree for the event “No output from motor system.”
- **Part 2:** Use the successive substitution method to get the cut sets. Use both the exact method and the cut set method (with rare event approximation) to determine the expression for the top event probability.

Example: Fault tree analysis

- **Solution (1)**:
  A fault tree for the event "No output from motor system" will be:



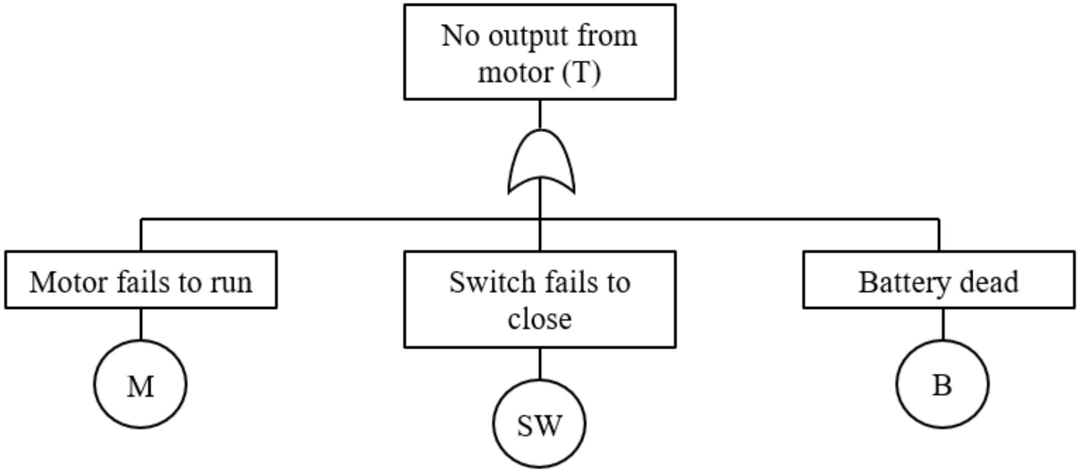
Note: The failure modes matter here!

FT successive substitution

- **Successive Substitution Method**: Boolean Reduction Process of a FT.
  - Reminder: Boolean reduction table on page 31.
  - **Step 1:** Top-down Boolean substitution of the gates.
  - **Step 2:** Boolean reduction of the final expression to reach minimal cut sets.
  - **Step 3:** Quantification.

FTA example (cont.): Qualitative solution

- **Solution (2):** Now we can evaluate the logic of this tree using Boolean substitution:



$$System\ failure\ logic, F_s = T = B \cup M \cup SW$$

Note: This Boolean expression represents the cut sets of the fault tree.

FTA example: Quantitative evaluation

- **Solution (3):** Next, we focus on the quantification aspects of this FT:

$$For\ T: B \cup M \cup SW$$

$$\boldsymbol{Unreliability, F_s} = \mathbf{Pr}(\boldsymbol{T}) = \mathbf{Pr}(\boldsymbol{B} \cup \boldsymbol{M} \cup \boldsymbol{SW})$$

To calculate this probability, we use one of the methods discussed previously: cut sets, exact expression, truth table, etc.

FTA example: Quantitative evaluation

- **Solution (4):**

$$F_S = \Pr(T) = \Pr(B \cup M \cup SW)$$

- **The exact calculation is:**

$$\Pr(T) \\ = \Pr(B) + \Pr(M) + \Pr(SW) - \Pr(B, M) - \Pr(B, SW) - \Pr(M, SW) \\ + \Pr(B, M, SW)$$

- **Since the components are independent this becomes:**

$$\Pr(T) \\ = \Pr(B) + \Pr(M) + \Pr(SW) - \Pr(B)\Pr(M) - \Pr(B)\Pr(SW) \\ - \Pr(M)\Pr(Sw) + \Pr(M)\Pr(B)\Pr(Sw)\,.$$

Or, written in more compact form:

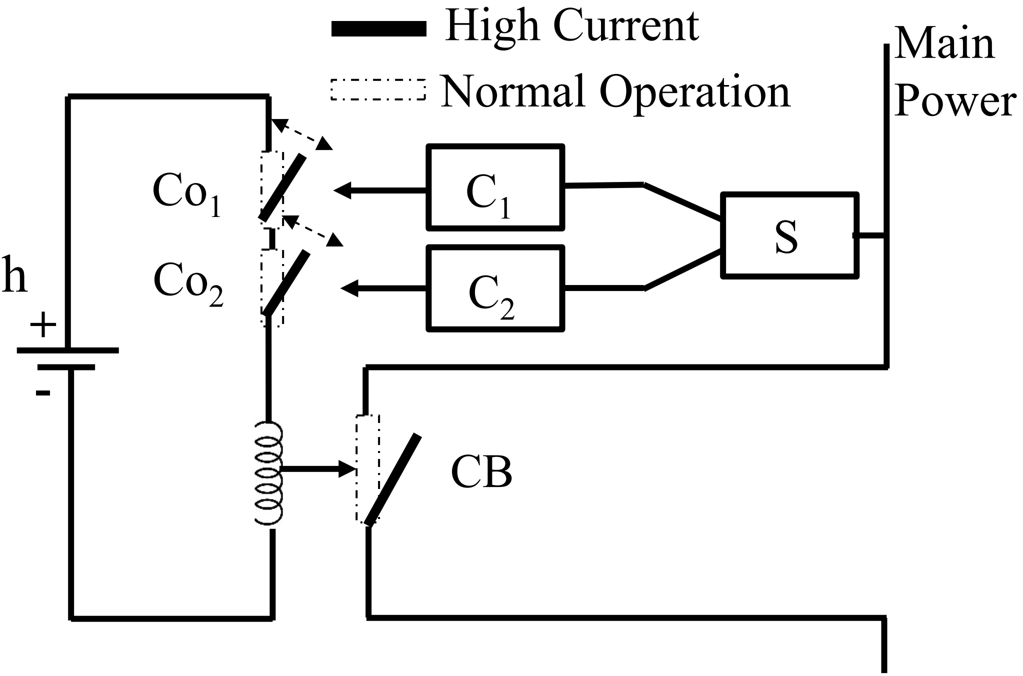
$$\Pr(T) = 1 - (1 - \Pr(B))(1 - \Pr(M))(1 - \Pr(SW))$$

Or, an approximation can be obtained with the cut set method with the rare event approximation:

$$\mathbf{Pr}(\boldsymbol{T}) \cong \mathbf{Pr}(\boldsymbol{B}) + \mathbf{Pr}(\boldsymbol{M}) + \mathbf{Pr}(\boldsymbol{SW})$$

FTA: CB system example

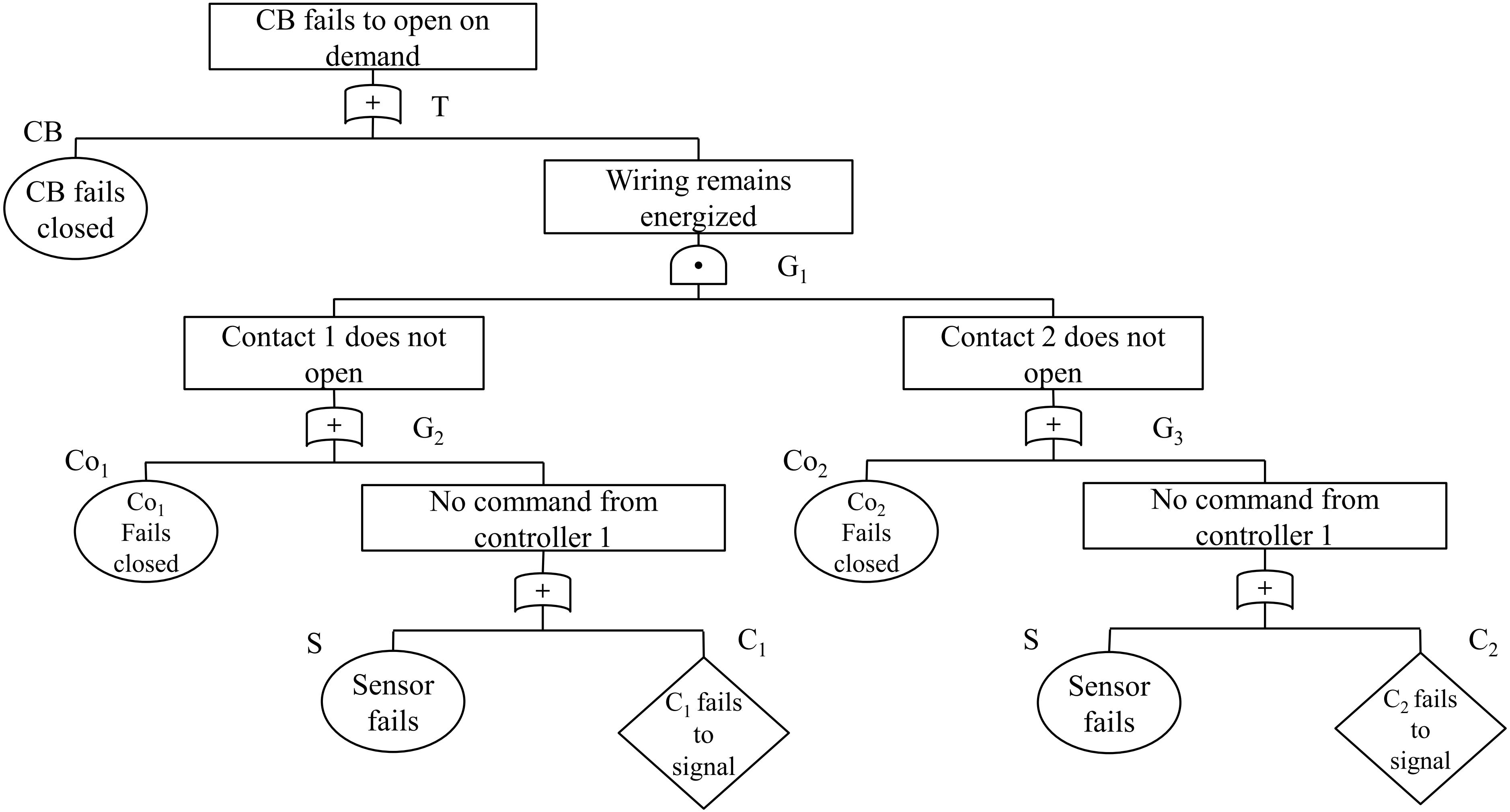
- **Example:** Circuit breaker System
  - C_1 and C_2 = Controller
  - S = Sensor
  - Co_1 and Co_2 = Contacts
  - CB = Circuit Breaker Switch



- **Functions:**
  - If the current gets too high in the main power line, the circuit breaker switch (CB) should open to prevent a short circuit.
  - Sensor S detects high current. If S indicates high current, the controllers issue a command to open contacts (Co_1, Co_2). If any contact is open, the power to the coil is removed and CB opens.

CB system example

- **CB Fault tree**



CB system example (cont.)

- Boolean Substitution Process:

$$T = CB \cup G_1 = CB + G_1$$

$$G_1 = G_2 \cdot G_3$$

$$G_2 = S + Co_1 + C_1$$

$$G_3 = S + Co_2 + C_2$$

$$G_1 = (S + Co_1 + C_1) \cdot (S + Co_2 + C_2)$$

$$T = \mathrm{CB} + \underset{\mathrm{S}}{(\mathrm{S} \cdot \mathrm{S})} + \mathrm{S} \cdot \mathrm{Co}_2 + \mathrm{S} \cdot \mathrm{C}_2 + \mathrm{Co}_1 \cdot \mathrm{S} + \mathrm{Co}_1 \cdot \mathrm{Co}_2 + \mathrm{Co}_1 \cdot \mathrm{C}_2 + \mathrm{C}_1 \cdot \mathrm{S} + \mathrm{C}_1 \cdot \mathrm{Co}_2 + \mathrm{C}_1 \cdot \mathrm{C}_2$$

- Applying Boolean reduction on this expression gives the minimal cut sets:

$$T = \mathrm{CB} + \underset{\mathrm{S}}{(\mathrm{S} \cdot \mathrm{S})} + \cancel{\mathrm{S} \cdot \mathrm{Co}_2} + \cancel{\mathrm{S} \cdot \mathrm{C}_2} + \cancel{\mathrm{Co}_1 \cdot \mathrm{S}} + \mathrm{Co}_1 \cdot \mathrm{Co}_2 + \mathrm{Co}_1 \cdot \mathrm{C}_2 + \cancel{\mathrm{C}_1 \cdot \mathrm{S}} + \mathrm{C}_1 \cdot \mathrm{Co}_2 + \mathrm{C}_1 \cdot \mathrm{C}_2$$

$$\mathbf{T = CB + S + Co_1 \cdot Co_2 + Co_1 \cdot C_2 + C_1 \cdot Co_2 + C_1 \cdot C_2}$$

Fault tree analysis (cont.)

- Quantifying via minimal cut set approach (and assuming indep.) gives:

$$\mathbf{Pr(T)} \approx \mathbf{Pr(CB)} + \mathbf{Pr(S)} + \mathbf{Pr}(\mathbf{Co_1}) \cdot \mathbf{Pr}(\mathbf{Co_2}) + \mathbf{Pr}(\mathbf{Co_1}) \cdot \mathbf{Pr}(\mathbf{C_2}) + \mathbf{Pr}(\mathbf{C_1}) \cdot \mathbf{Pr}(\mathbf{Co_2}) + \mathbf{Pr}(\mathbf{C_1}) \cdot \mathbf{Pr}(\mathbf{C_2})$$

- If we assume that unreliability for each component is 0.01, then:

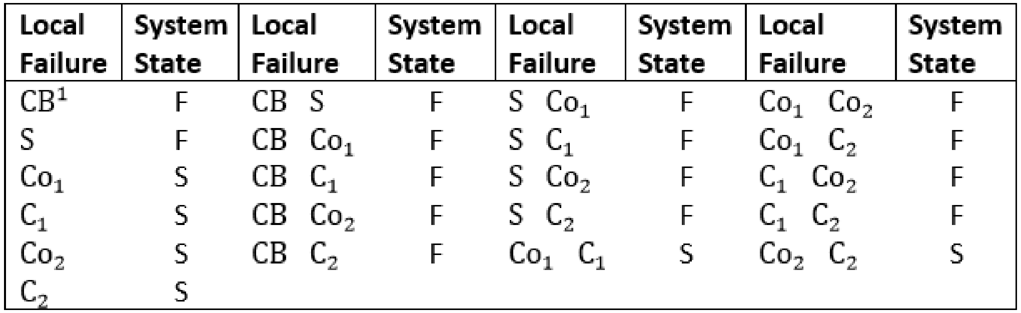
$$\mathbf{Pr(T)} \approx \mathbf{2 \times .01 + 4 \times (.01 \times .01) \approx 0.0204}$$

Combinatorial approach (aka Truth Table) for the same FT

- A more accurate quantification approach
- Finds all combinations (mutually exclusive) that cause top event to occur
  - 2^6 combinations exist = 64

$$C_1^6 + C_2^6 + C_3^6 + C_4^6 + C_5^6 + C_6^6 = 2^6$$

- Each of these elements are the (non-minimal) cut sets of the Systems (you can test to verify)



Local Failure	System State	Local Failure	System State	Local Failure	System State	Local Failure	System State
CB^1	F	CB S	F	S Co_1	F	Co_1 Co_2	F
S	F	CB Co_1	F	S C_1	F	Co_1 C_2	F
Co_1	S	CB C_1	F	S Co_2	F	C_1 Co_2	F
C_1	S	CB Co_2	F	S C_2	F	C_1 C_2	F
Co_2	S	CB C_2	F	Co_1 C_1	S	Co_2 C_2	S
C_2	S						

$$CB^1 = CB \cdot \overline{S} \cdot \overline{Co_1} \cdot \overline{Co_2} \cdot \overline{C_1} \cdot \overline{C_2}$$

$$\Pr(Mutually\ Exclusive\ Set\ 1) = \Pr(CB) \cdot \Pr(\overline{S}) \cdot \Pr(\overline{Co_1}) \cdot \Pr(\overline{Co_2}) \cdot \Pr(\overline{C_1}) \cdot \Pr(\overline{C_2})$$

$$= 0.01 \times 0.99^5\ (if\ all\ failure\ probabilities\ are\ 0.01)$$

$$= 0.0095099$$

- Accounting for all 64 rows, you should get a value of: $\Pr(F_S) = 0.020292$

FT vs. BDD vs. Truth Table

- All methods list combinations of events that cause system failure.

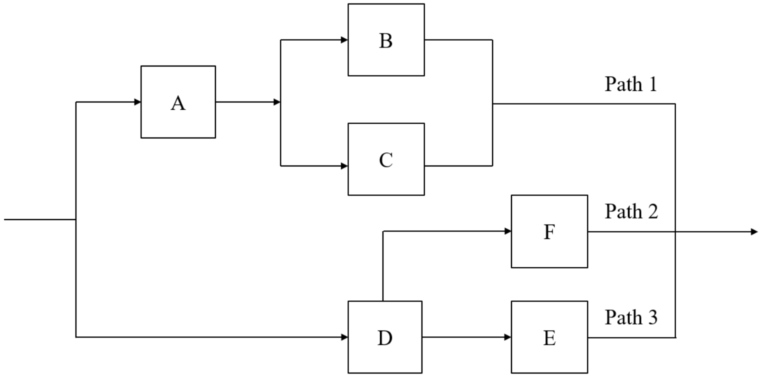
FT Boolean reduction	BDD	Truth Table
AD, BCD, AEF, BCEF	$AD,$ $\bar{A}BCD,$ $A\bar{D}EF,$ $\bar{A}\bar{D}BCEF$	$A\bar{B}\bar{C}D\bar{E}\bar{F}, AB\bar{C}D\bar{E}\bar{F}, A\bar{B}CD\bar{E}\bar{F}, A\bar{B}\bar{C}DE\bar{F}, A\bar{B}\bar{C}D\bar{E}F,$ $A\bar{B}\bar{C}\bar{D}EF, \bar{A}BCD\bar{E}\bar{F}, ABCD\bar{E}\bar{F}, AB\bar{C}DE\bar{F},$ $A\bar{B}CDE\bar{F}, \bar{A}BCDE\bar{F}, AB\bar{C}D\bar{E}F, A\bar{B}CD\bar{E}F,$ $\bar{A}BCD\bar{E}F, AB\bar{C}\bar{D}EF, A\bar{B}C\bar{D}EF, \bar{A}BC\bar{D}EF, A\bar{B}\bar{C}DEF,$ $ABCDE\bar{F}, ABCD\bar{E}F, ABC\bar{D}EF, AB\bar{C}DEF,$ $A\bar{B}CDEF, \bar{A}BCDEF, ABCDEF$

Minimal cut sets

Mutually exclusive minimal cut sets

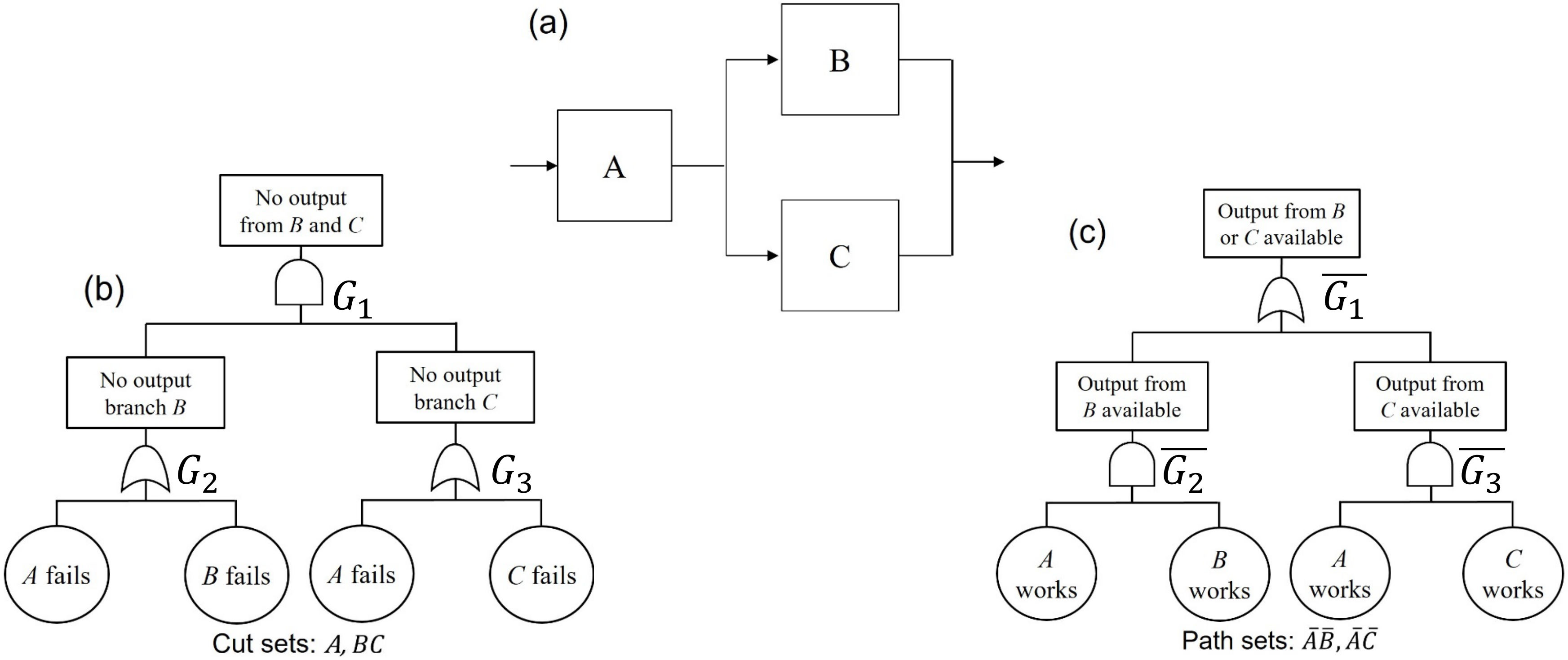
All cut sets (mutually exclusive)

Results correspond to RBD at right



Comparison of success trees and fault trees

- Consider the system:



i. Fault tree, cut sets are:

$$T = G_1 = G_2 \cdot G_3$$

$$T = (A + B) \cdot (A + C)$$

$$= A + B \cdot C$$

ii. For equivalent Success tree, path sets are:

$$\bar{T} = \overline{G_1} = \overline{G_2} + \overline{G_3}$$

$$\bar{T} = \overline{A + B} + \overline{A + C} = \bar{A} \cdot \bar{B} + \bar{A} \cdot \bar{C}$$

$$= \bar{A} \cdot \bar{B} + \bar{A} \cdot \bar{C}$$

Comparison of success tree and fault tree (cont.)

- You can use Boolean Laws to find path sets of the Success Tree from cut sets of Fault Tree:

$$\bar{T} = \left(\overline{A + B \cdot C}\right) = \bar{A} \cdot \overline{B \cdot C} = \bar{A} \cdot (\bar{B} + \bar{C})$$

$$\bar{T} = \bar{A} \cdot \bar{B} + \bar{A} \cdot \bar{C} \text{ same as (ii)}$$

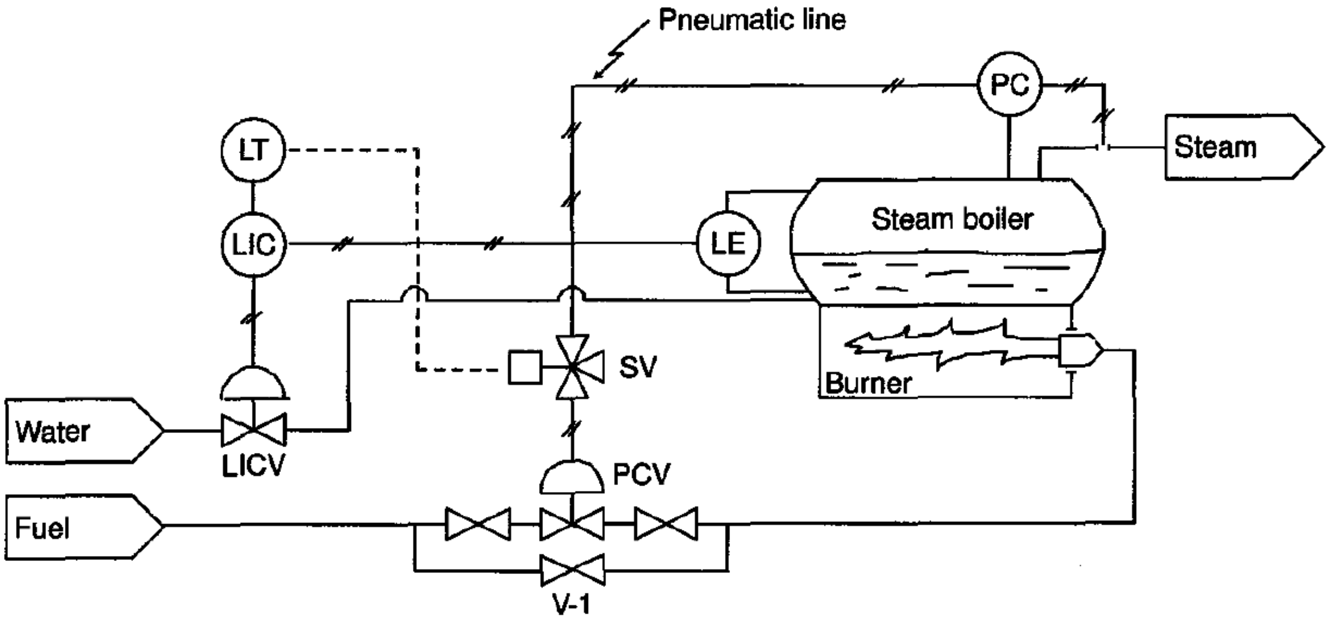
- So success trees are the complement (logical inverse) of fault trees (in most of the cases).

$$fault\ tree \rightarrow success\ tree$$
$$OR\ gate \rightarrow AND\ gate$$
$$AND\ gate \rightarrow OR\ gate$$
$$\overline{A} \cdot B + \overline{B} \cdot A \rightarrow A \cdot B + \overline{A} \cdot \overline{B}$$

(exclusive or)

Boiler example (page 1 of 3)

- This steam boiler system supplies steam to a process system at a specified pressure.



- A critical situation occurs if the boiler is boiled dry. In this case the pressure in the vessel will increase very rapidly and the vessel may explode

a. Construct a fault tree where the Top event is the critical situation mentioned above. (Only use components given a variable name on next 2 pages – but annotate tree with the relevant failure mode)

b. Determine all minimal cut sets in the fault tree.

Boiler example (page 2 of 3)

- **Description of system provided to you by boiler engineer (2 slides)**

Water from a feedwater system (W) is led to the boiler through pipe with a regulator valve called a level indicator controller valve (LICV). Fuel is led to the burner chamber through a pipe with a regulator valve called a pressure controller valve (PCV). The valve PCV is installed in parallel with a bypass valve (V-1) together with two isolation valves to facilitate inspection and maintenance of the PCV during normal operation.

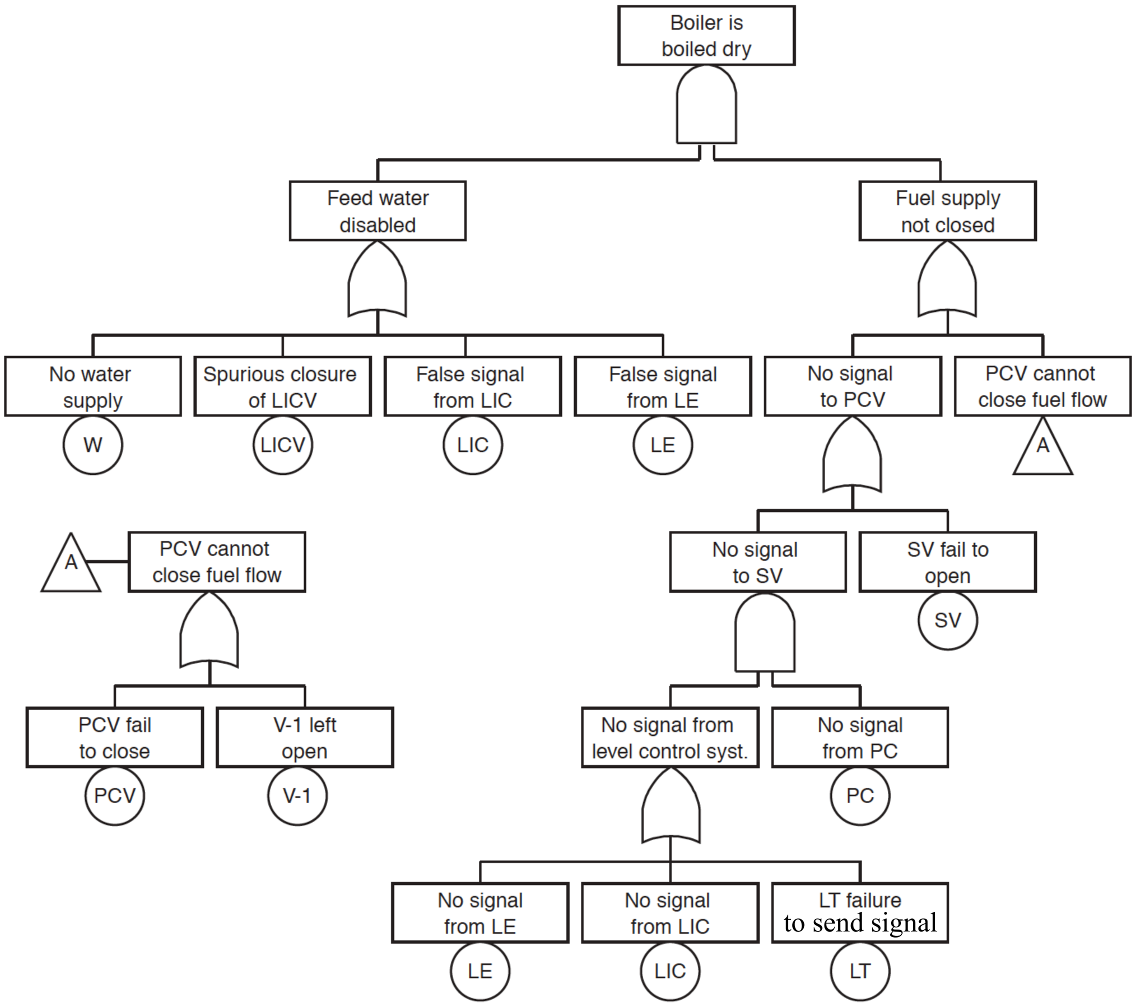
The level of the water in the boiler is monitored by a level emitter (LE). The water level is maintained in an interval between a specified low level and a specified high level by a pneumatic control circuit connected to the water regulator valve LICV. The level indicator controller (LIC) translates the pneumatic "signal" from LE to a pneumatic "signal" controlling the valve LICV.

Boiler example (page 3 of 3)

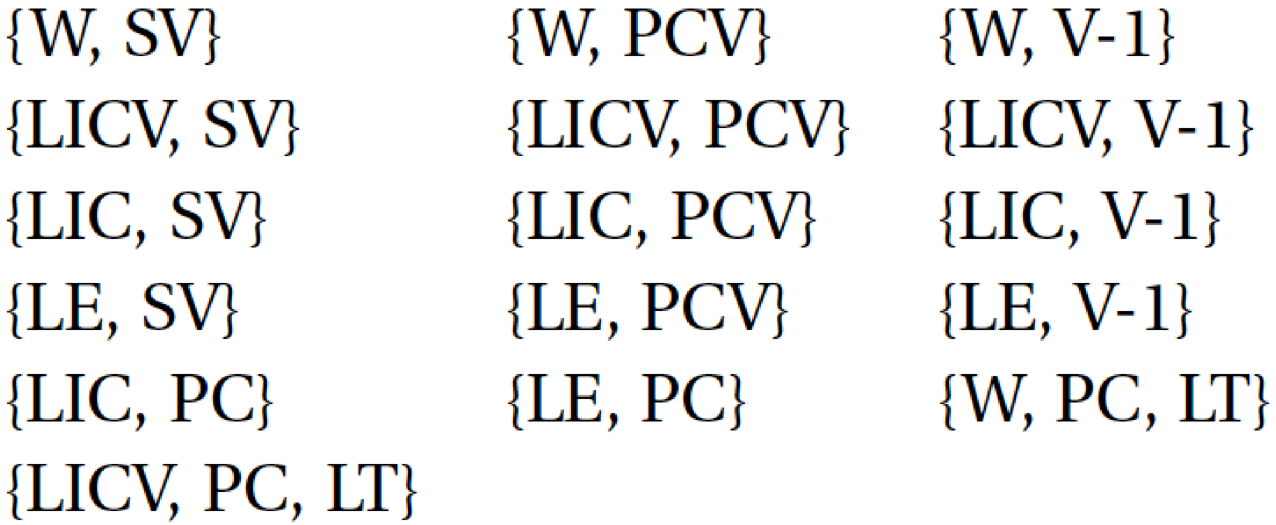
It is very important that the water level does not fall below the specified low level. When the water level approaches the low level, a pneumatic "signal" is passed from the level indicator controller LIC to the level transmitter (LT). The LT translates the pneumatic signal into an electrical signal which is sent to the solenoid valve (SV). The solenoid valve again controls the valve PCV on the fuel inlet pipeline. This circuit is thus installed to cut off the fuel supply in case the water level comes below the specified low level.

The pressure in the boiler and in the steam outlet pipeline is monitored by a pressure controller PC which is connected to the solenoid valve SV, and thereby to the valve PCV on the fuel inlet pipeline. This circuit is thus installed to cut off the fuel supply in case the pressure in the boiler increases above a specified high pressure

Boiler example: Solution (page 1 of 2)



Boiler example: Solution (page 2 of 2)



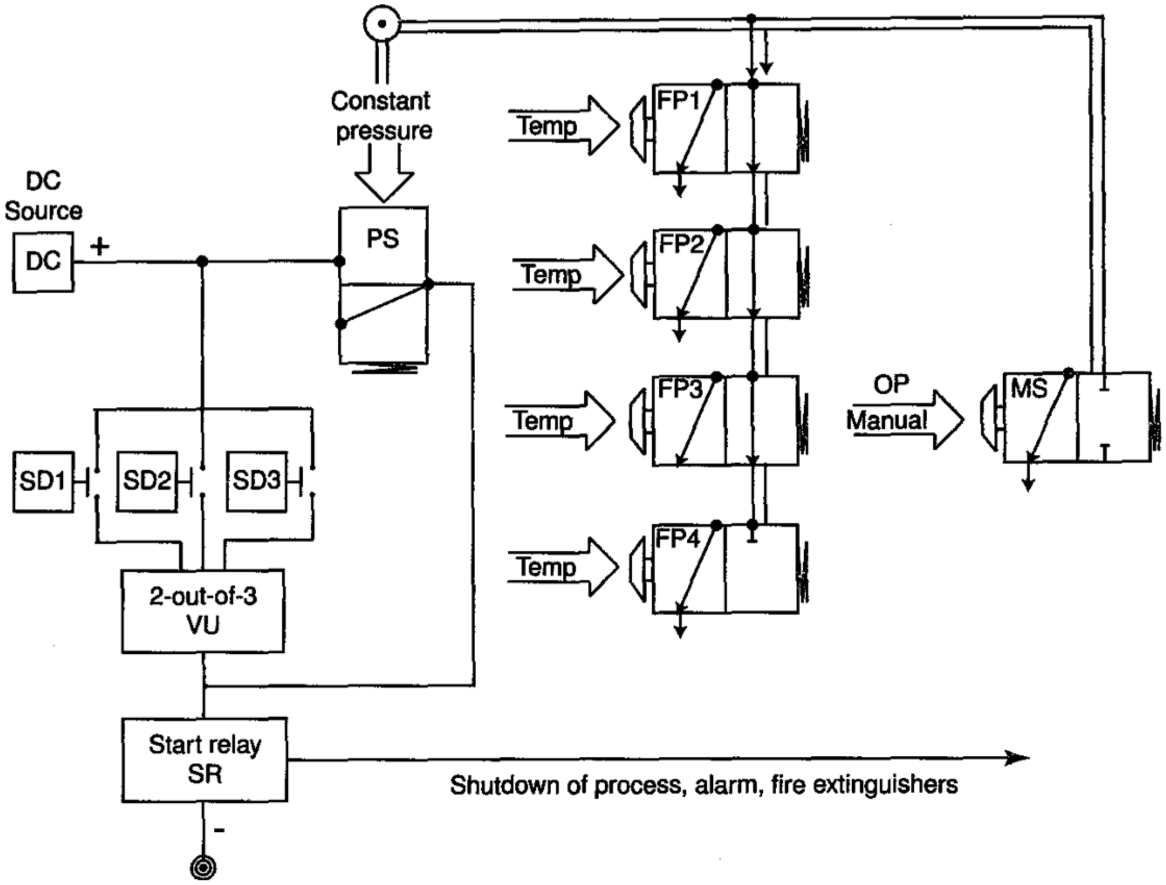
{W, SV}
{LICV, SV}
{LIC, SV}
{LE, SV}
{LIC, PC}
{LICV, PC, LT}

{W, PCV}
{LICV, PCV}
{LIC, PCV}
{LE, PCV}
{LE, PC}

{W, V-1}
{LICV, V-1}
{LIC, V-1}
{LE, V-1}
{W, PC, LT}

Another example* (SKIP slides 82-88/do after class)

- Consider the following fire detector system:



*Source: System Relıabılıty Theory: Models, Statıstıcal Methods, and Applıcatıons, Second Edıtıon, Wıley, 2004, M. Rausand, A. Hoyland

Another example

- The fire detector system is divided into two parts, heat detection and smoke detection. In addition, there is an alarm button that can be operated manually.
- *Heat Detection*:

In the production room there is a closed, pneumatic pipe circuit with four identical fuse plugs, FP_1, FP_2, FP_3, and FP_4. These plugs let air out of the circuit if they are exposed to temperatures higher than 72C. The pneumatic system has a pressure of 3 bars and is connected to a pressure switch PS. If one or more of the plugs are activated, the switch will be activated and give an electrical signal to the start relay for the alarm and shutdown system. In order to have an electrical signal, the direct current (DC) source must be intact.

Another example

- *Smoke Detection*:

The smoke detection system consists of three optical smoke detectors, SD_1, SD_2, and SD_3; all are independent and have their own batteries. These detectors are very sensitive and can give warning of fire at an early stage. In order to avoid false alarms, the three smoke detectors are connected via a logical 2-out-of-3 voting unit, VU.

This means that at least two detectors must give fire signal before the fire alarm is activated. If at least two of the three detectors are activated, the 2-out-of-3 voting unit will give an electric signal to the start relay, SR, for the alarm and shutdown system. Again the DC voltage source must be intact to obtain an electrical signal.

Another example

- *Manual Activation*:

Together with the pneumatic pipe circuit with the four fuse plugs, there is also a manual switch, MS, that can be turned to relieve the pressure in the pipe circuit. If the operator, OP, who should be continually present, notices a fire, he can activate this switch. When the switch is activated, the pressure in the pipe circuit is relieved and the pressure switch, PS, is activated and gives an electric signal to the start relay, SR. Again the DC source must be intact.

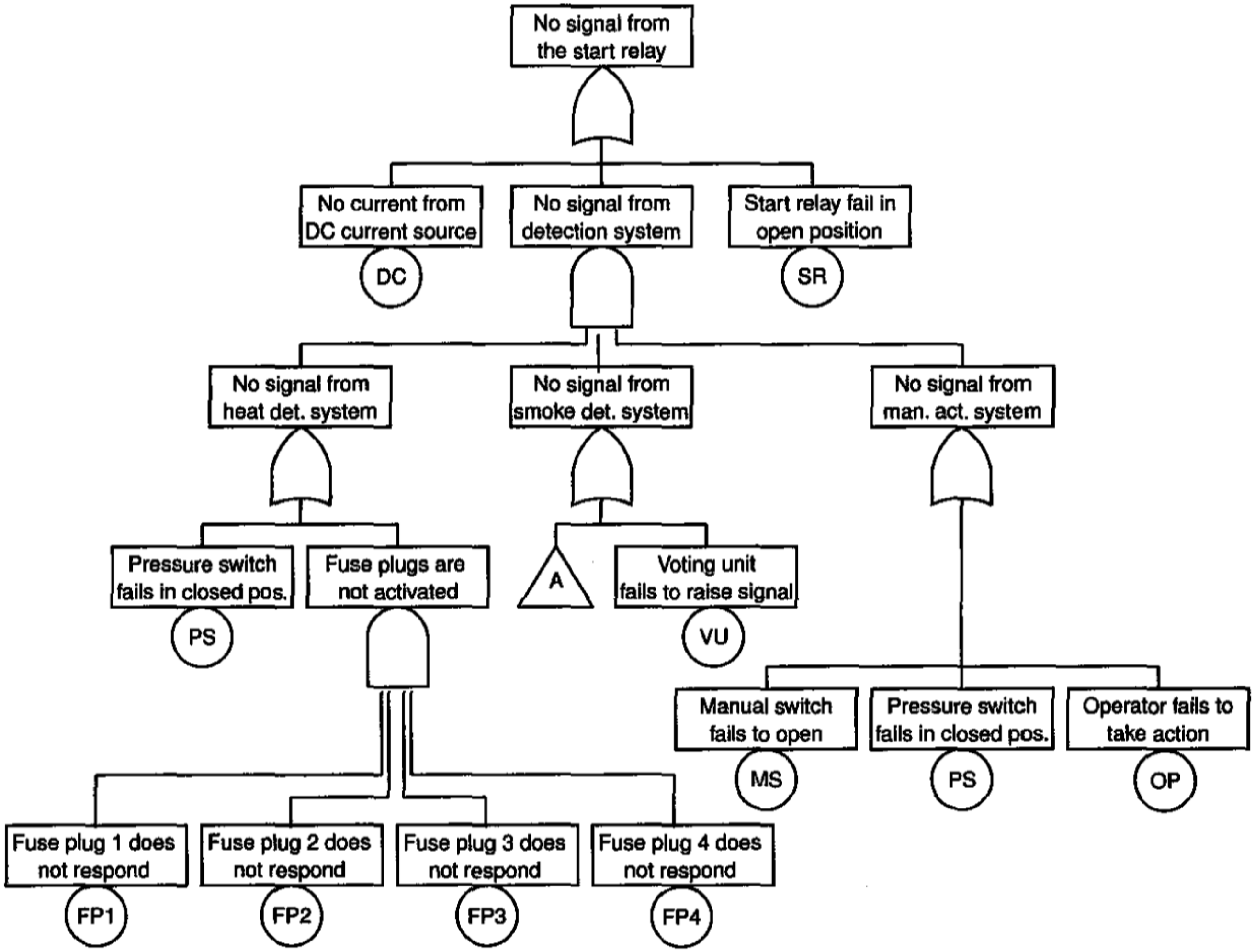
- *The Start Relay*:

When the start relay, SR, receives an electrical signal from the detection systems, it is activated and gives a signal to (i) Shut down the process, and (ii) Activate the alarm and the fire extinguishers.

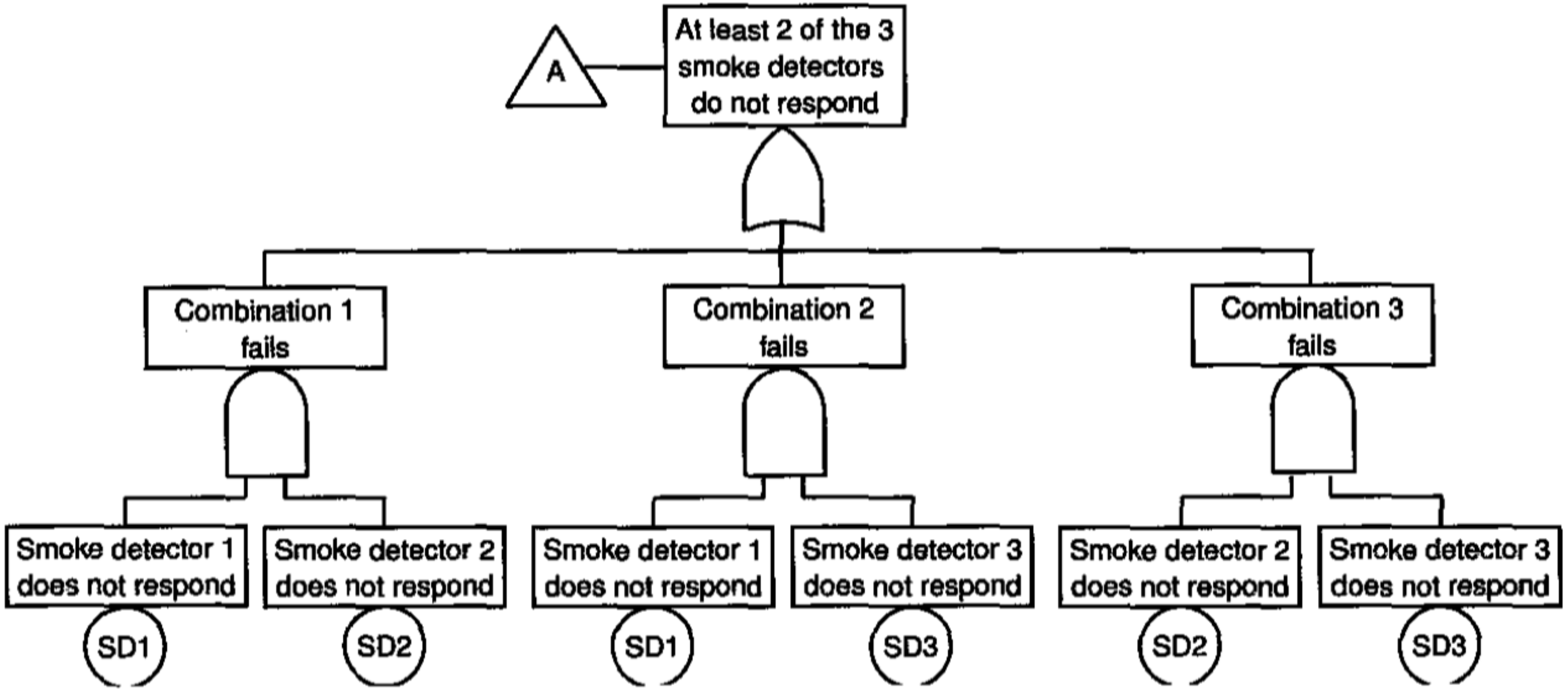
Another example

- Assume now that a fire starts
- The fire detector system should detect and give warning about the fire
- Let the TOP event be: *no signals from the start relay SR when a fire condition is present*
- Develop the fault tree and find the cut sets

Another example: Fault tree


No signal from the start relay
No current from DC current source
DC
No signal from detection system
Start relay fail in open position
SR
No signal from heat det. system
No signal from smoke det. system
No signal from man. act. system
Pressure switch fails in closed pos.
PS
Fuse plugs are not activated
A
Voting unit fails to raise signal
VU
Manual switch fails to open
MS
Pressure switch fails in closed pos.
PS
Operator fails to take action
OP
Fuse plug 1 does not respond
FP1
Fuse plug 2 does not respond
FP2
Fuse plug 3 does not respond
FP3
Fuse plug 4 does not respond
FP4

Another example: Fault tree



A
At least 2 of the 3 smoke detectors do not respond
Combination 1 fails
Combination 2 fails
Combination 3 fails
Smoke detector 1 does not respond
Smoke detector 2 does not respond
Smoke detector 1 does not respond
Smoke detector 3 does not respond
Smoke detector 2 does not respond
Smoke detector 3 does not respond
SD1
SD2
SD1
SD3
SD2
SD3

Minimal cut-sets for this example are (14 in total):
DC + SR+PSVU+PSSD1SD3+PSSD2SD3+PSSD1SD2+FP1FP2FP3FP4MSVU+
FP1FP2FP3FP4OPVU+FP1FP2FP3FP4MSSD1SD2+FP1FP2FP3FP4MSSD2SD3+
FP1FP2FP3FP4MSSD1SD3+FP1FP2FP3FP4OPSD1SD2+FP1FP2FP3FP4OPSD1SD3+
FP1FP2FP3FP4OPSD2SD3

Event tree method

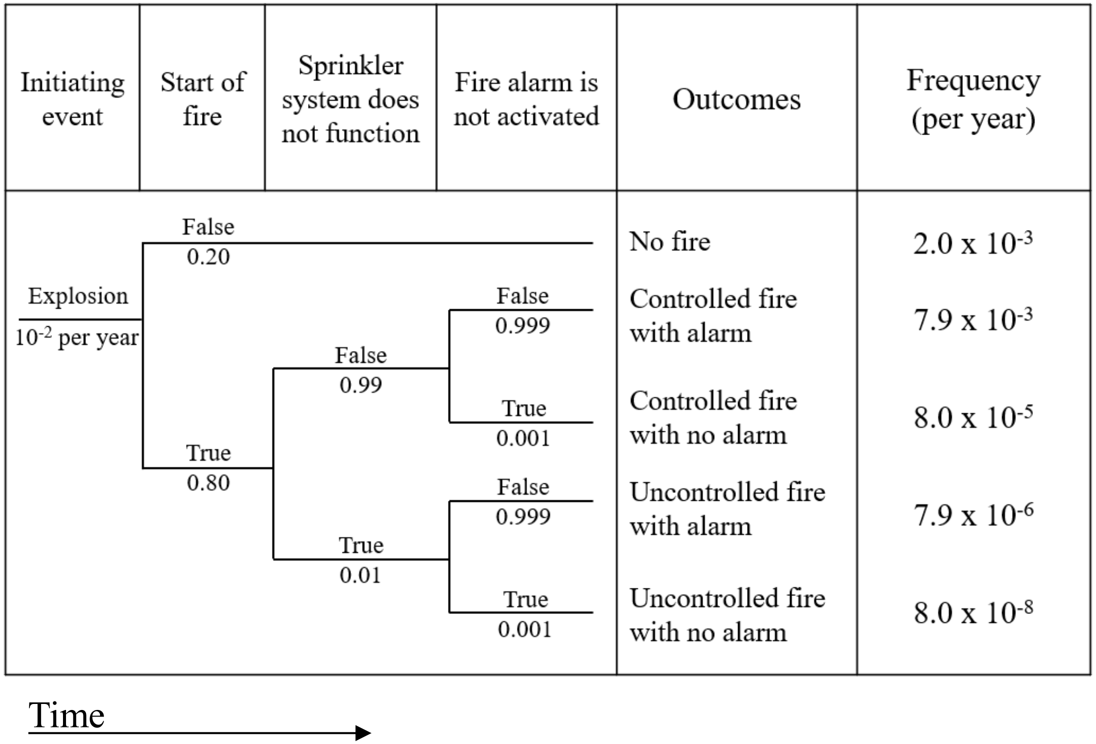
If successful operation of a system depends on an ***approximately*** chronological but discrete operation of some of its units or subsystems, then an event tree is a useful logical model for the system.

Key Features

- Sequence of events
- Initiating event (with frequency)
- Up/down branching
  - In this class:
  - Up = Success
  - Down = Failure
- (Conditional) probabilities

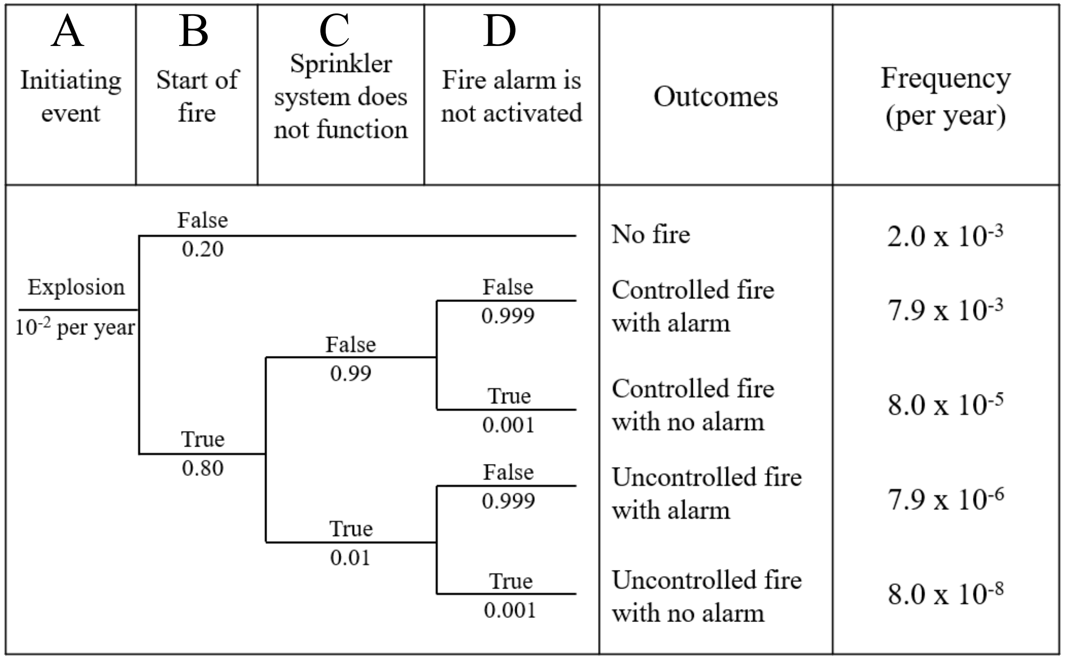
or independent events

- Mutually exclusive sequences
- End state descriptions



Outcomes	Frequency (per year)
No fire	2.0×10^{-3}
Controlled fire with alarm	7.9×10^{-3}
Controlled fire with no alarm	8.0×10^{-5}
Uncontrolled fire with alarm	7.9×10^{-6}
Uncontrolled fire with no alarm	8.0×10^{-8}

Event tree quantification



A Initiating event	B Start of fire	C Sprinkler system does not function	D Fire alarm is not activated	Outcomes	Frequency (per year)
Explosion 10^{-2} per year	False 0.20			No fire	2.0 x 10^{-3}
	True 0.80	False 0.99	False 0.999	Controlled fire with alarm	7.9 x 10^{-3}
			True 0.001	Controlled fire with no alarm	8.0 x 10^{-5}
		True 0.01	False 0.999	Uncontrolled fire with alarm	7.9 x 10^{-6}
			True 0.001	Uncontrolled fire with no alarm	8.0 x 10^{-8}

$$\boldsymbol{\Sigma = 0.01}$$

- Note: typically written with marginal notation but should be interpreted as conditional when needed!

$$= f(A)\Pr(\bar{B}|A)$$

$$= f(A)\Pr(B|A)\Pr\left(\bar{C}\middle|B,A\right)\Pr\left(\bar{D}\middle|\bar{C},B,A\right)$$

$$= f(A)\Pr(B|A)\Pr\left(\bar{C}\middle|B,A\right)\Pr\left(D\middle|\bar{C},\ B,A\right)$$

$$= f(A)\Pr(B|A)\Pr(C|B,A)\Pr\left(\bar{D}\middle|C,B,A\right)$$

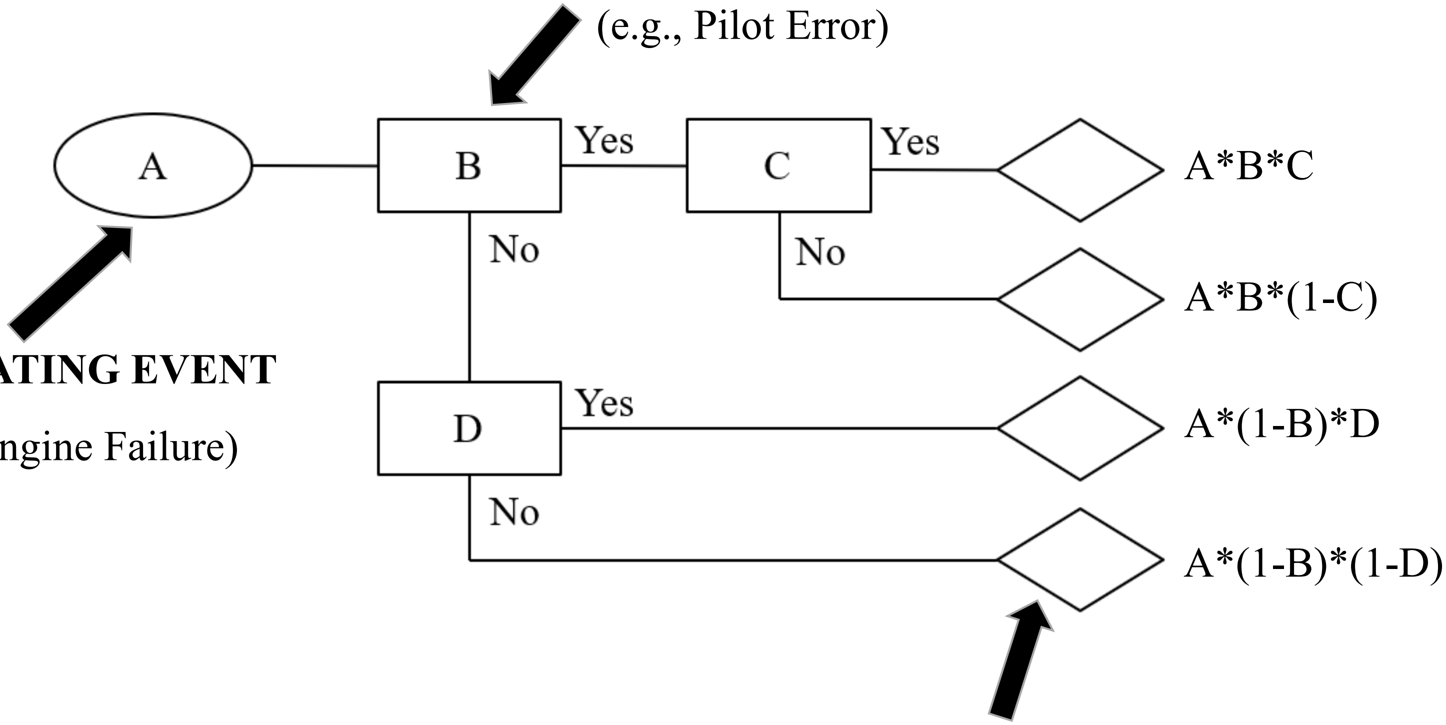
$$= f(A)\Pr(B|A)\Pr(C|B,A)\Pr(D|C,B,A)$$

Adapted from: M. Rausand, A. Hoyland, *System Reliability Theory: Models, Statistical Methods, and Applications*, Second Edition, Wiley, 2004.

Event sequence diagram/event tree

PIVOTAL EVENT

(e.g., Pilot Error)



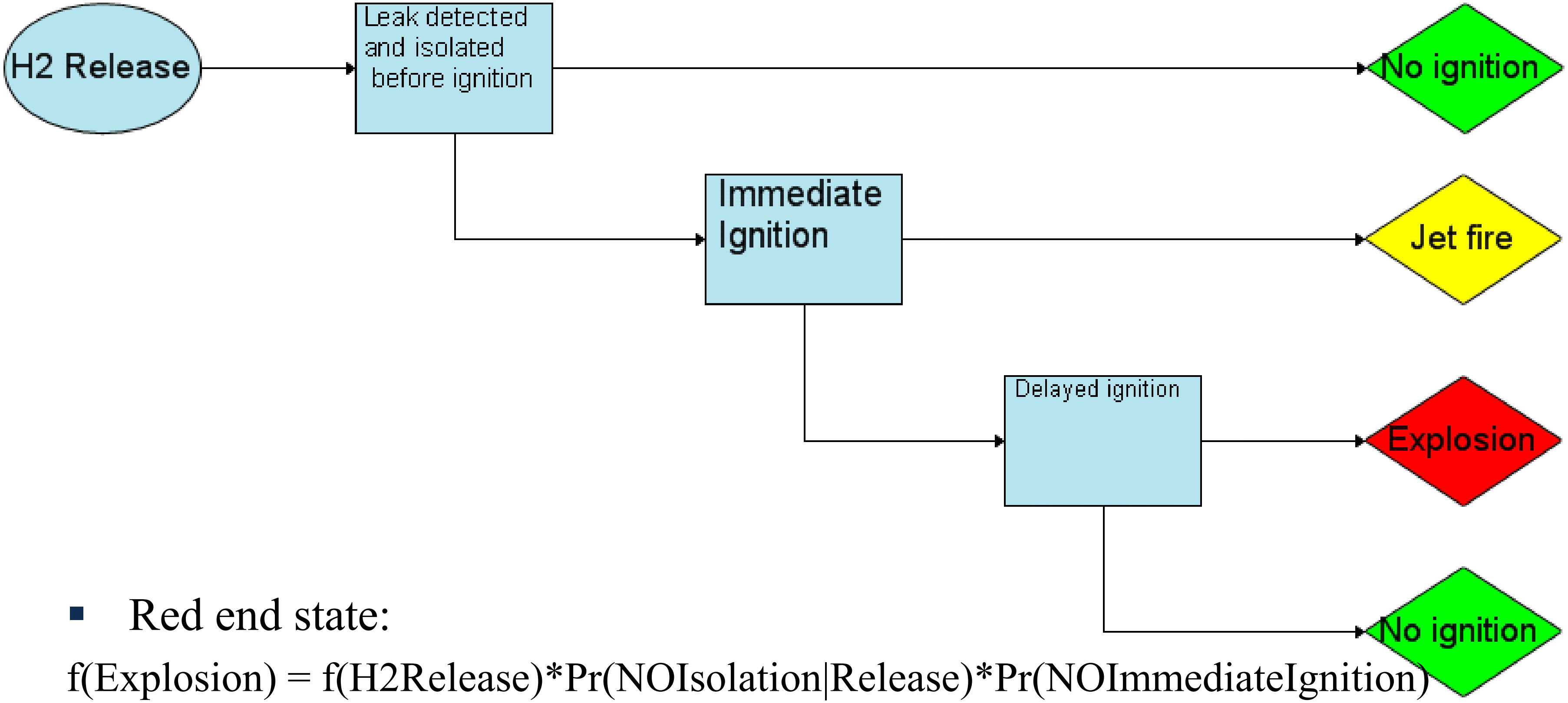
INITIATING EVENT

(e.g., Engine Failure)

END STATE (Consequence)

(e.g., Ground Collision)

ESD: Hydrogen release from H2 dispenser

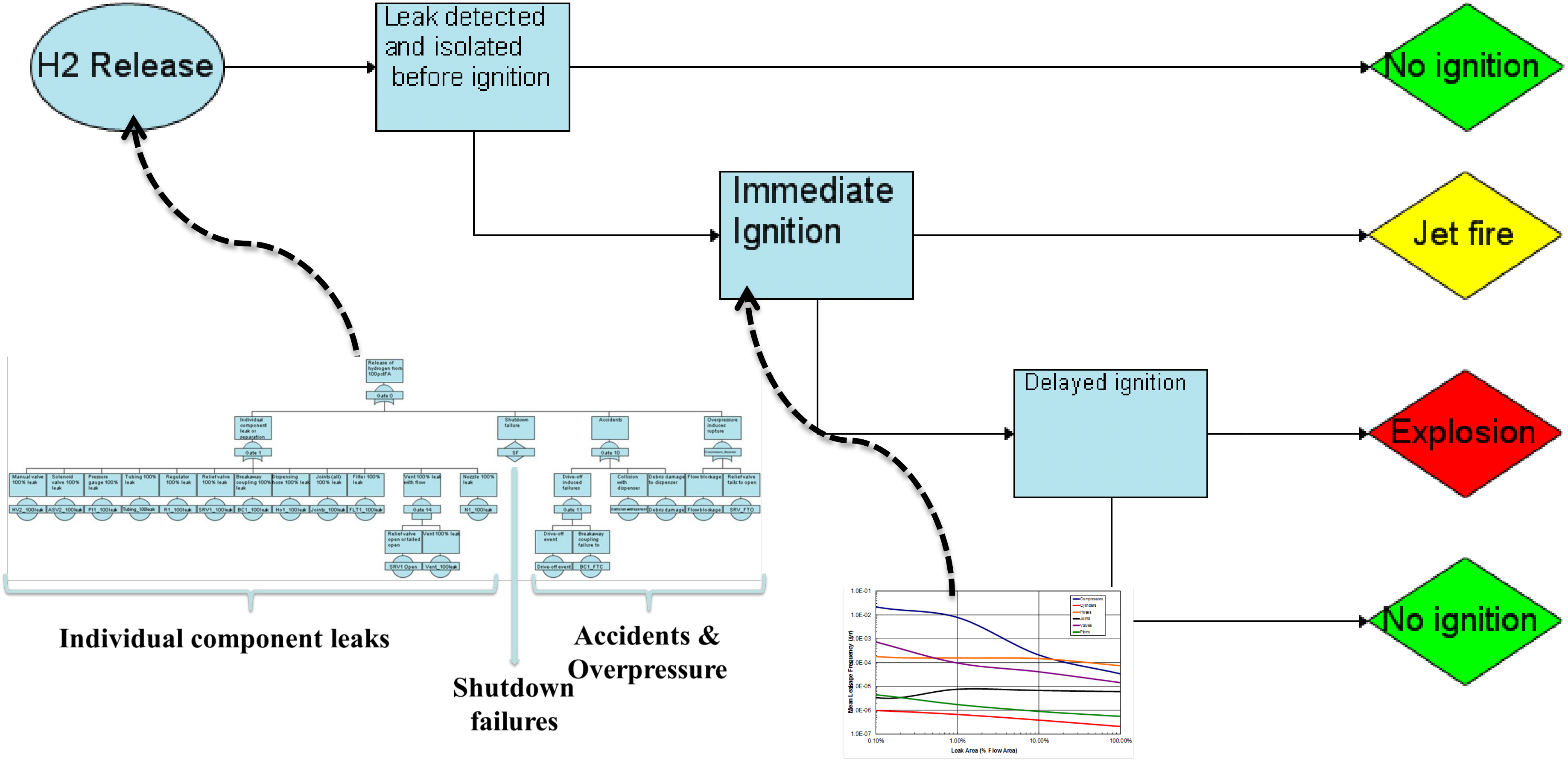


- Red end state:

f(Explosion) = f(H2Release)*Pr(NOIsolation|Release)*Pr(NOImmediateIgnition) *Pr(Delayedignition)

Adapted from: Groth, Katrina M., and Ethan S. Hecht. 2017. “HyRAM: A Methodology and Toolkit for Quantitative Risk Assessment of Hydrogen Systems.” *International Journal of Hydrogen Energy*, International Journal of Hydrogen Energy, 42 (11): 7485–7493. doi:10.1016/j.ijhydene.2016.07.002.

Using event tree + fault tree for system reliability


H2 Release

Leak detected and isolated before ignition

Immediate Ignition

Delayed ignition

No ignition

Jet fire

Explosion

No ignition

Individual component leaks

Shutdown failures

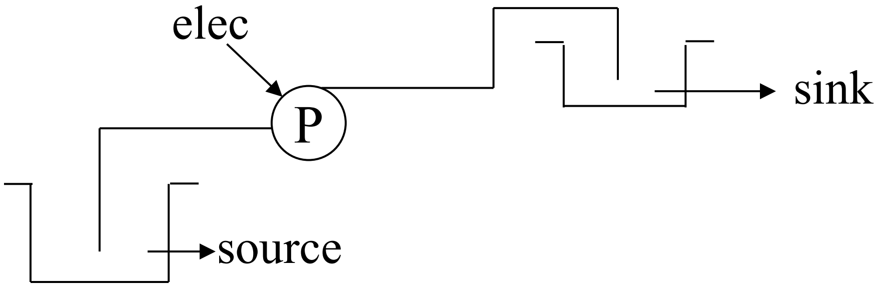
Accidents & Overpressure

Connected to FT(s) (Or BNs)…

Or Direct use of data

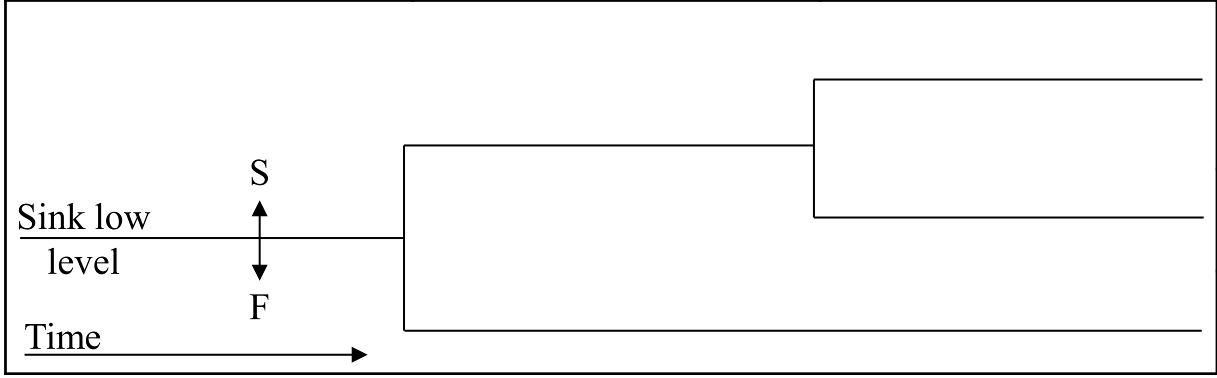
Event tree for pumping system reliability

- **Example: Pumping system designed to fill a sink from a source tank.**



I = frequency of "sink low" event
Elec = Electric power fails off
P = Pump fails off

If the sink is low, the system should pump water from the source. An ET for this would be:

I (Sink Low)	Elec Power (Elec)	Pump (P)	End State
			$I \cdot \overline{Elec} \cdot \overline{P}$: System Functions (S1)
			$I \cdot \overline{Elec} \cdot P$: System Fails (F1)
			$I \cdot Elec$: System Fails (F2)

Event tree for pumping system reliability

- Since the event tree sequences are mutually exclusive, we can calculate probability of system failure as:

$$\begin{aligned}\Pr(system\ failure) &= \Pr(F_1 + F_2)\\ &= \Pr\left(I \cdot \overline{Elec} \cdot P + I \cdot Elec\right)\\ &= \Pr\left(I \cdot \overline{Elec} \cdot P\right) + \Pr(I \cdot Elec)\end{aligned}$$

If *I* happens with a frequency 10 times/mo, *Elec* power fails off with probability 0.1, and *P* fails off with probability 0.05,

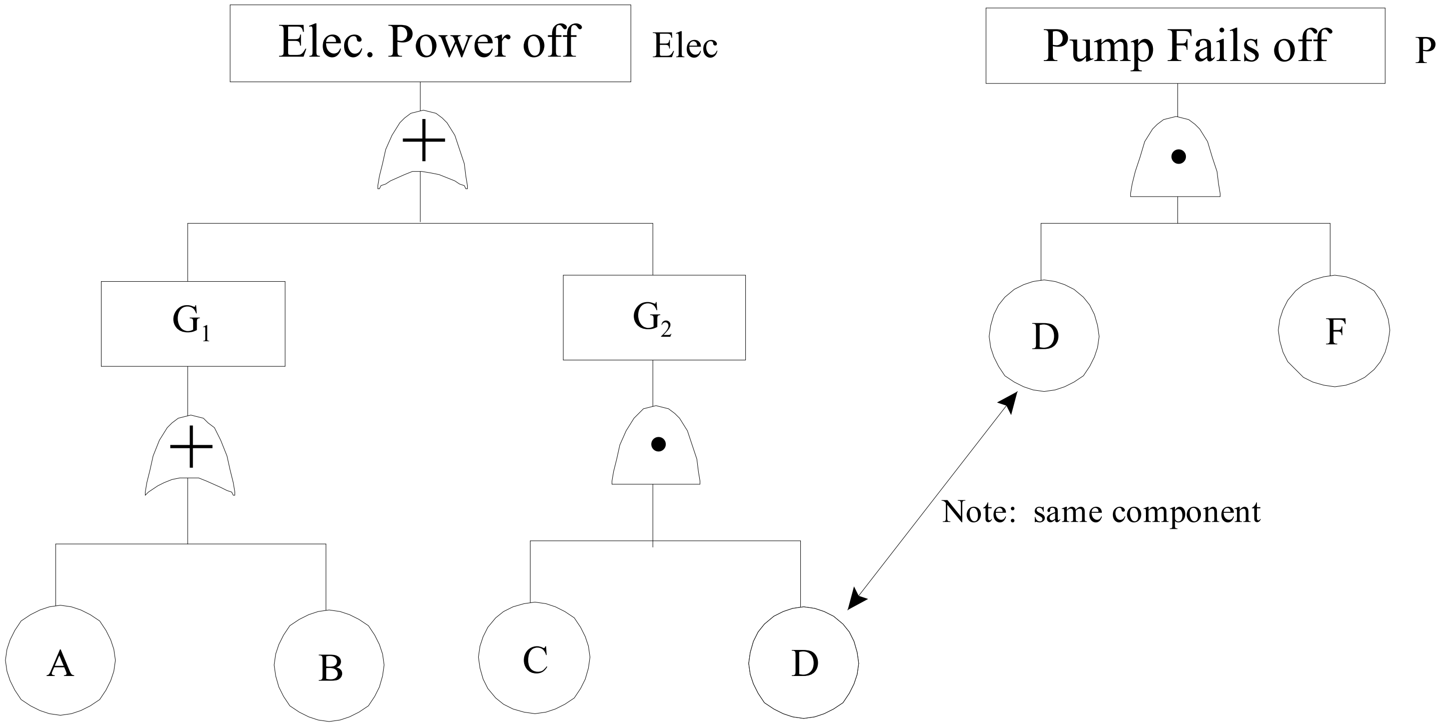
f(S1)=8.55/month

f(F1)=0.45/month

f(F2)=1.0/month

Event tree + fault tree method

- Now, assume *Elec* and *P* can be represented by a set of fault trees showing how they could fail:



Event tree + fault tree method

- First start by solving the FTs

$$Elec = G_1 + G_2$$

$$G_1 = A + B, \qquad G_2 = C \cdot D$$

$$\boldsymbol{Elec = A + B + C \cdot D}$$

$$\overline{Elec} = \overline{A + B + C \cdot D} = \left(\overline{A} \cdot \overline{B}\right) \cdot \left(\overline{C \cdot D}\right) = \overline{A} \cdot \overline{B} \cdot \left(\overline{C} + \overline{D}\right)$$

$$\boldsymbol{\overline{Elec} = \overline{A} \cdot \overline{B} \cdot \overline{C} + \overline{A} \cdot \overline{B} \cdot \overline{D}}$$

$$\boldsymbol{P = D \cdot F}$$

$$\boldsymbol{\overline{P} = \overline{D} + \overline{F}}$$

Event tree + fault tree method

- To find the ET sequence F_1, which is $I \cdot \overline{Elec} \cdot P,$ start inserting the logic from your FTs

$$I \cdot \overline{Elec} \cdot P = I \cdot \left(\bar{A} \cdot \bar{B} \cdot \bar{C} + \bar{A} \cdot \bar{B} \cdot \bar{D}\right) \cdot D \cdot F$$

$$= I \cdot \bar{A} \cdot \bar{B} \cdot \bar{C} \cdot D \cdot F + I \cdot \bar{A} \cdot \bar{B} \cdot \bar{D} \cdot D \cdot F$$

- Since $D \cdot \bar{D}$ is a null set:

$$\boldsymbol{I \cdot \overline{Elec} \cdot P = I \cdot \bar{A} \cdot \bar{B} \cdot \bar{C} \cdot D \cdot F}$$

Event tree + fault tree method

- In the same way, we find the expression for the bottom ET sequence, F_2 :

$$\boldsymbol{I \cdot Elec = I \cdot A + I \cdot B + I \cdot C \cdot D}$$

- And the final ET sequence, S_1 (the one representing system success).

$$I \cdot \overline{Elec} \cdot \overline{P} = I \cdot \left(\overline{A} \cdot \overline{B} \cdot \overline{C} + \overline{A} \cdot \overline{B} \cdot \overline{D}\right) \cdot \left(\overline{D} + \overline{F}\right)$$

$$= I \cdot \overline{A} \cdot \overline{B} \cdot \overline{C} \cdot \overline{D} + I \cdot \overline{A} \cdot \overline{B} \cdot \overline{C} \cdot \overline{F} + I \cdot \overline{A} \cdot \overline{B} \cdot \overline{D} + I \cdot \overline{A} \cdot \overline{B} \cdot \overline{D} \cdot \overline{F}$$

$$= \boldsymbol{I \cdot \overline{A} \cdot \overline{B} \cdot \overline{C} \cdot \overline{F} + I \cdot \overline{A} \cdot \overline{B} \cdot \overline{D}}$$

Event tree + fault tree method

- Assume the following probabilities $\Pr(\bullet)$ and frequency $f(I)$, and independent events, find system failure probability (use the rare event approximation on the FT cut sets)

Event	**Failure Probability or Freq.**	**Success Probability**	**Event**	**Failure Probability or Frequ.**	**Success Probability**
I	10 per month		C	0.02	0.98
A	0.01	0.99	D	0.05	0.95
B	0.01	0.99	F	0.01	0.99

- Since the event tree sequences are mutually exclusive:

$$\Pr(system\ failure) = \Pr(I \cdot Elec) + \Pr(I \cdot \overline{Elec} \cdot P)$$

$$= \underbrace{f(I)\Pr(A) + f(I)\Pr(B) + f(I)\Pr(C)\Pr(D)}_{Not\ mutually\ exclusive\ items, but\ rare\ event\ applies} + \underbrace{f(I)\Pr(\overline{A})\Pr(\overline{B})\Pr(\overline{C})\Pr(D)\Pr(F)}_{Rare\ event\ doesn't\ apply}$$

Event tree + fault tree method

- Frequency of System Failure with rare event approximation is:

$F_1 + F_2$

$= 10(0.01) + 10(0.01) + 10(0.02)(0.05) + 10(0.99)(0.99)(0.98)(0.05)(0.01)$

$= 10(0.021 + 0.00048) = \mathbf{0.2148}\ \boldsymbol{failures/month}$

- The Frequency of System Failure without rare event approximation uses the addition law of probability:

$= f(I)\{(1 - (1 - P(A))(1 - P(B))(1 - P(CD))) + P(\overline{ABC}DF)\}$

$= 10\ \{(1 - (1 - .01)(1 - .01)(1 - .02 * .05) + (0.048)\}$

$=10\ \{(1 - (.99)(.99)(.999)) + (0.00048)\}$

=10(0.02088+0.00048)

$= \mathbf{0.2136}\ \boldsymbol{failures/month}$

Event tree + fault tree method

- Frequency of System Success is:

$$I \cdot \overline{elec} \cdot \overline{P} = I \cdot \left(\overline{A} \cdot \overline{B} \cdot \overline{C} + \overline{A} \cdot \overline{B} \cdot \overline{D}\right) \cdot \left(\overline{D} + \overline{F}\right)$$

$$= I \cdot \overline{A} \cdot \overline{B} \cdot \overline{C} \cdot \overline{D} + I \cdot \overline{A} \cdot \overline{B} \cdot \overline{C} \cdot \overline{F} + I \cdot \overline{A} \cdot \overline{B} \cdot \overline{D} + I \cdot \overline{A} \cdot \overline{B} \cdot \overline{D} \cdot \overline{F}$$

$$= I \cdot \overline{A} \cdot \overline{B} \cdot \overline{C} \cdot \overline{F} + I \cdot \overline{A} \cdot \overline{B} \cdot \overline{D}$$

For success quantification, the rare event approximation doesn't apply because the probabilities are too high. The two cut sets for this sequence aren't mutually exclusive, either. So, we calculate it using the addition law of probability:

$$R_s = 1 - \prod (1 - R_i)$$

So, assuming independence between the two parts of the sequence:

$$= 10\{1 - [(1 - 0.99 \times 0.99 \times 0.98 \times 0.99)(1 - 0.99 \times 0.99 \times 0.95)]\} \cong 9.9662$$

$$= 10\{1 - [(1 - 0.9508)(1 - 0.931095)]\}$$

$$= 10\{1 - [(0.0491)(0.0689)]\} = 10 \cdot 9.9662 \cong 9.9662$$

Event tree + fault tree method

- Exact calculation for frequency of System Success is:

$$I \cdot \overline{elec} \cdot \overline{P} = I \cdot \overline{A} \cdot \overline{B} \cdot \overline{C} \cdot \overline{F} + I \cdot \overline{A} \cdot \overline{B} \cdot \overline{D}$$

It should be noted that these two parts of the sequence aren't independent (even though the units A, B, C, D are independent of each other) – this is because of the element D which appears in both FTs), so the exact answer would be:

$$\mathrm{I} \cdot (\Pr(\bar{A}, \bar{B}, \bar{C}, \bar{F}) + \Pr(\bar{A}, \bar{B}, \bar{D}) \; - \Pr(\bar{A}, \bar{B}, \bar{C}, \bar{D}, \bar{F}))$$

$$= 10((.99 \times .98 \times .99 \times .99) + (.99 \times .99 \times .95) - (.99 \times .99 \times .98 \times .95 \times .99))$$

$= 10((0.9509) + (.9311) - (.9037))$=**9.786**