Controlling Risks
Safety System Models

Module B

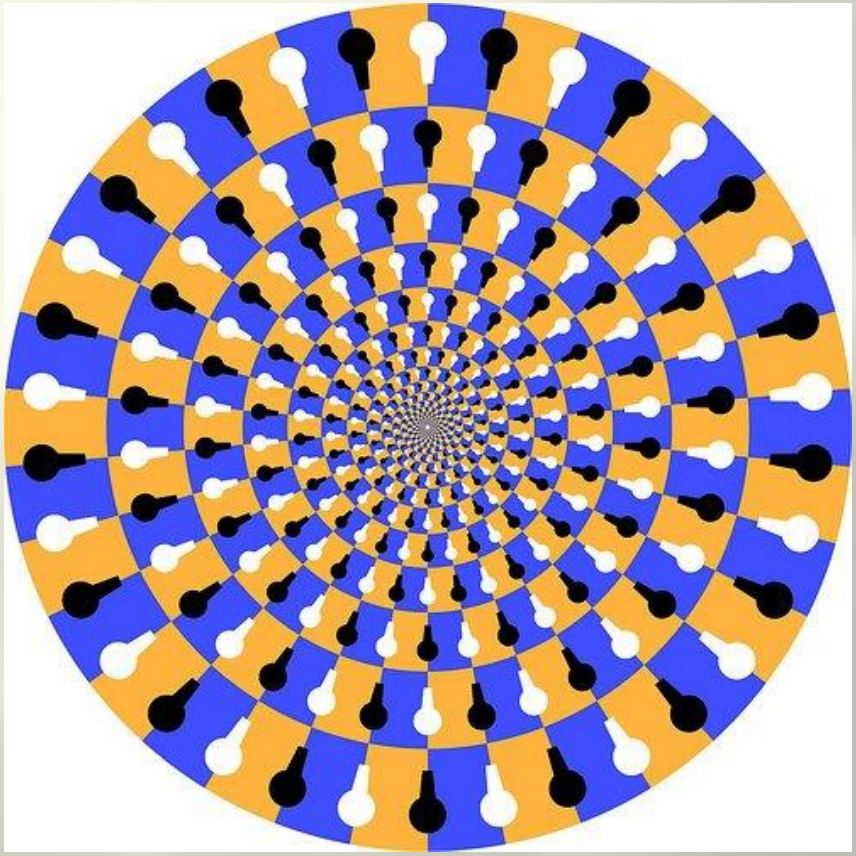
Level of Detail

- The level of detail to be included in a safety and reliability model depends on the objective of the modeling.
- The level of detail affects
  - Effort
  - Cost

Key Issues

- Degree of redundancy
- Common cause failures in redundant systems
- Availability of on-line diagnostics
- Imperfect inspection and repair
- Failure of on-line diagnostics
- Probability of initial equipment failure

Simplification of Method



- Account for the important things
- Ignore the rest

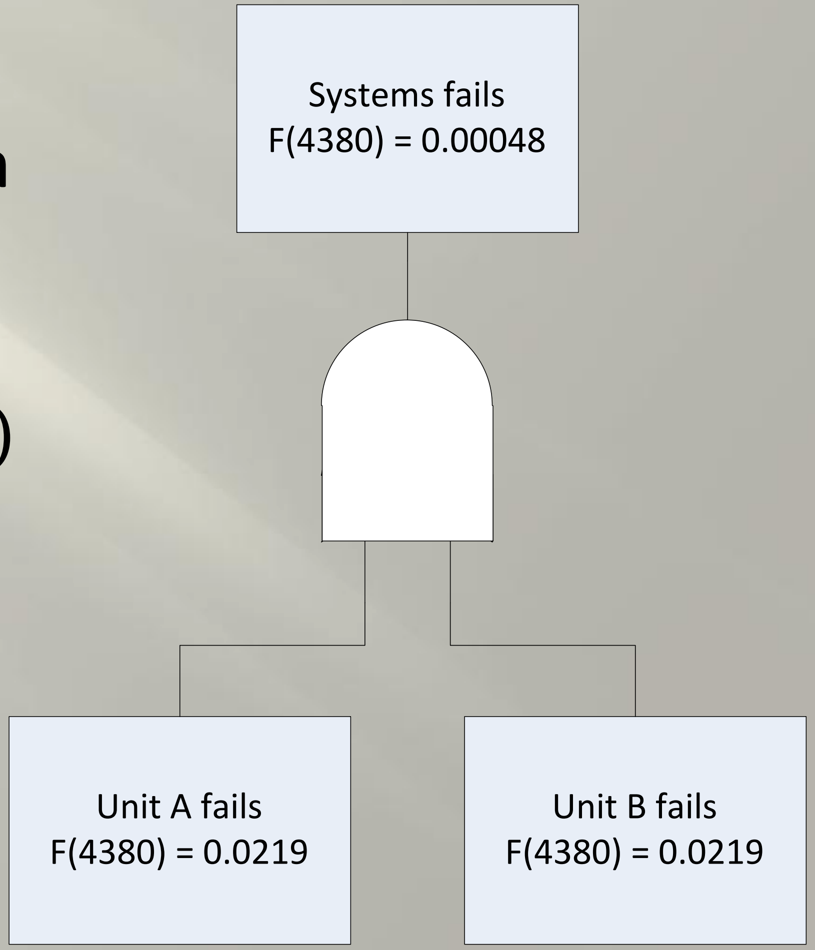
Probability Approximation

- 1oo2 system
- The failure rate is based on the dangerous failure mode

$$PFD = (\lambda_1 * TI) * (\lambda_2 * TI)$$

- If the units have identical failure rates then

$$PFD = (\lambda * TI)^2$$



Example 21-1

- Page 257
  - Constant failure rate for short circuit failures are not manufacturer provided data!

- Historical data about the device or system under consideration should be maintained by the system expert.
- Many organizations maintain internal databases of failure information on the devices or systems that they produce, which can be used to calculate failure rates for those devices or systems.
- For new devices or systems, the historical data for similar devices or systems can serve as a useful estimate.
- Handbooks of failure rate data for various components are available from government and commercial sources.
  - MIL-HDBK-217F, *Reliability Prediction of Electronic Equipment*

PFD Average

- The approximation is not accurate for the use of safety design verification
- The PFD average is calculated by averaging the integrated failure rate over the time interval

$$PFDavg(t) = \frac{1}{t}\int_0^t (\lambda^D t')^2 dt'$$

Solve the Integration

- Substitute t = TI

$$PFDavg(TI) = \frac{1}{TI}\int_0^{TI} (\lambda^D t')^2 dt'$$

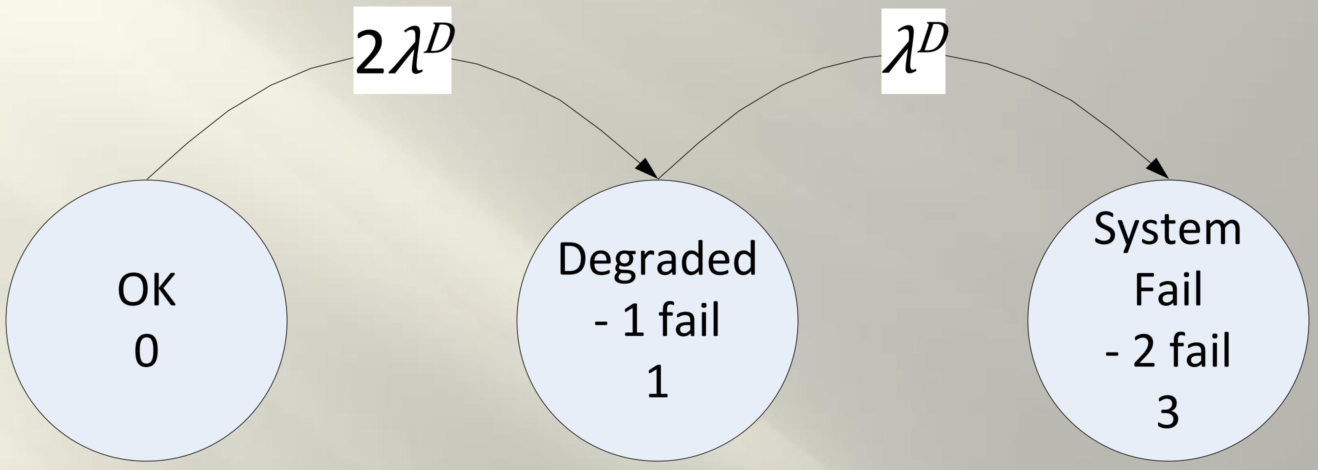
Integrate

$$PFDavg(TI) = \frac{1}{TI}[(\lambda^D)^2 \frac{t^3}{3}] \text{ from 0 to TI}$$

$$PFDavg(TI) = \frac{1}{TI}[(\lambda^D)^2 \frac{TI^3}{3}]$$

$$PFDavg(TI) = (\lambda^D)^2 \frac{TI^2}{3}$$

Markov Model

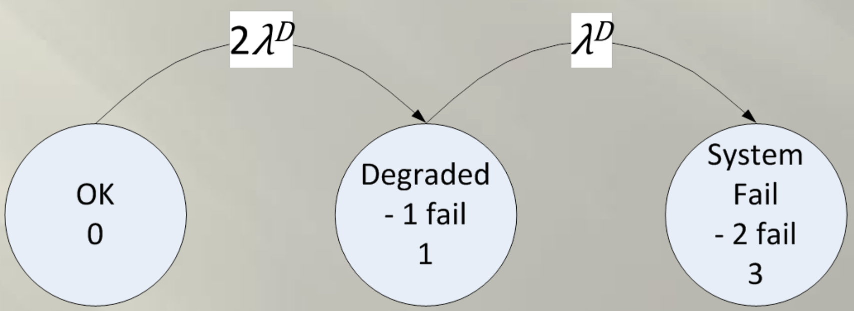


- The Markov model for the 1oo2 system shows 3 states
  - The initial state
  - One component failure
  - Both components failed
- The edges represent the probability of state changes

Markov Matrix

$$P = \begin{bmatrix} 1-2\lambda^D & 2\lambda^D & 0 \\ 0 & 1-\lambda^D & \lambda^D \\ 0 & 0 & 1 \end{bmatrix}$$

- The system of equations is the state change probability for the model
- Each row adds to 1 (or 100% probability)



Solve the Matrix

$$P = \begin{bmatrix} 1-2\lambda^D & 2\lambda^D & 0 \\ 0 & 1-\lambda^D & \lambda^D \\ 0 & 0 & 1 \end{bmatrix}$$

$$S = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$$

$$\lambda^D = 5 * 10^{-6}$$

- Put the data into a spreadsheet and solve the P*S matrix
- Pull the data down 4380 cells then average column 3 of the P*S matrix.

Comparison of PFDavg

$$PFDavg(TI) = (\lambda^D)^2\ \frac{TI^2}{3}$$

$$PFDavg(4380) = (.000005)^2\ \frac{4380^2}{3}$$

$$PFDavg(4380) = 0.00015987$$

Matrix solution = 0.00015716

Mechanical Lifetime

- MTBF is an attempt to predict the life expectancy of a device in hours.
- Reliability for electromechanical devices are rated in Mean Cycles Between Failures.
- MCBF may be calculated using the predetermined number of unit cycles called out on a data sheet and dividing that by the number of cycles/hour.

Typical Data Sheet

Contact specification				
Contact configuration		2 CO (DPDT)	3 CO (3PDT)	4 CO (4PDT)
Rated current/Maximum peak current	A	10/20	10/20	7/15
Rated voltage/Maximum switching voltage	V AC	250/400	250/400	250/250
Rated load AC1	VA	2,500	2,500	1,750
Rated load AC15 (230 V AC)	VA	500	500	350
Single phase motor rating (230 V AC)	kW	0.37	0.37	0.125
Breaking capacity DC1: 30/110/220	VA	10/0.25/0.12	10/0.25/0.12	7/0.25/0.12
Minimum switching load	mW (V/mA)	300 (5/5)	300 (5/5)	300 (5/5)
Standard contact material		AgNi	AgNi	AgNi
Coil specification				
Nominal voltage (U_N)	V AC (50/60 Hz)	6 · 12 · 24 · 48 · 60 · 110 · 120 · 230 · 240		
	V DC	6 · 12 · 24 · 48 · 60 · 110 -125 · 220		
Rated power AC/DC	VA (50 Hz)/W	1.5/1	1.5/1	1.5/1
Operating range	AC	$(0.8\ldots1.1)U_N$	$(0.8\ldots1.1)U_N$	$(0.8\ldots1.1)U_N$
	DC	$(0.8\ldots1.1)U_N$	$(0.8\ldots1.1)U_N$	$(0.8\ldots1.1)U_N$
Holding voltage	AC/DC	$0.8\ U_N/0.5\ U_N$	$0.8\ U_N/0.5\ U_N$	$0.8\ U_N/0.5\ U_N$
Must drop-out voltage	AC/DC	$0.2\ U_N/0.1\ U_N$	$0.2\ U_N/0.1\ U_N$	$0.2\ U_N/0.1\ U_N$
Technical data				
Mechanical life AC/DC	cycles	$20 \cdot 10^6/50 \cdot 10^6$	$20 \cdot 10^6/50 \cdot 10^6$	$20 \cdot 10^6/50 \cdot 10^6$
Electrical life at rated load AC1	cycles	$200 \cdot 10^3$	$200 \cdot 10^3$	$150 \cdot 10^3$
Operate/release time	ms	9/3	9/3	9/3
Insulation between coil and contacts (1.2/50 µs)	kV	3.6	3.6	3.6
Dielectric strength between open contacts	V AC	1,000	1,000	1,000
Ambient temperature range	°C	–40…+85	–40…+85	–40…+85
Environmental protection		RT I	RT I	RT I
Approvals (according to type)		IRAM		

Example

- Rated mechanical lifetime
  - 1,000,000 operations
- Estimated number of accesses to enclosure
  - 100
- Number of days enclosure is open for access
  - 30
- Hours in a year
  - 8760

$$\frac{cycles}{h} = 2 * access * \frac{days\ per\ year}{hours\ per\ year}$$

$$MTBF = \frac{rated\ operations}{cycles\ per\ hour}$$

Result

$$\frac{cycles}{h} = 2 * 100 * \frac{30}{8760} = 0.684931507$$

$$MTBF = \frac{1 * 10^6}{0.684931507} = 1460000$$

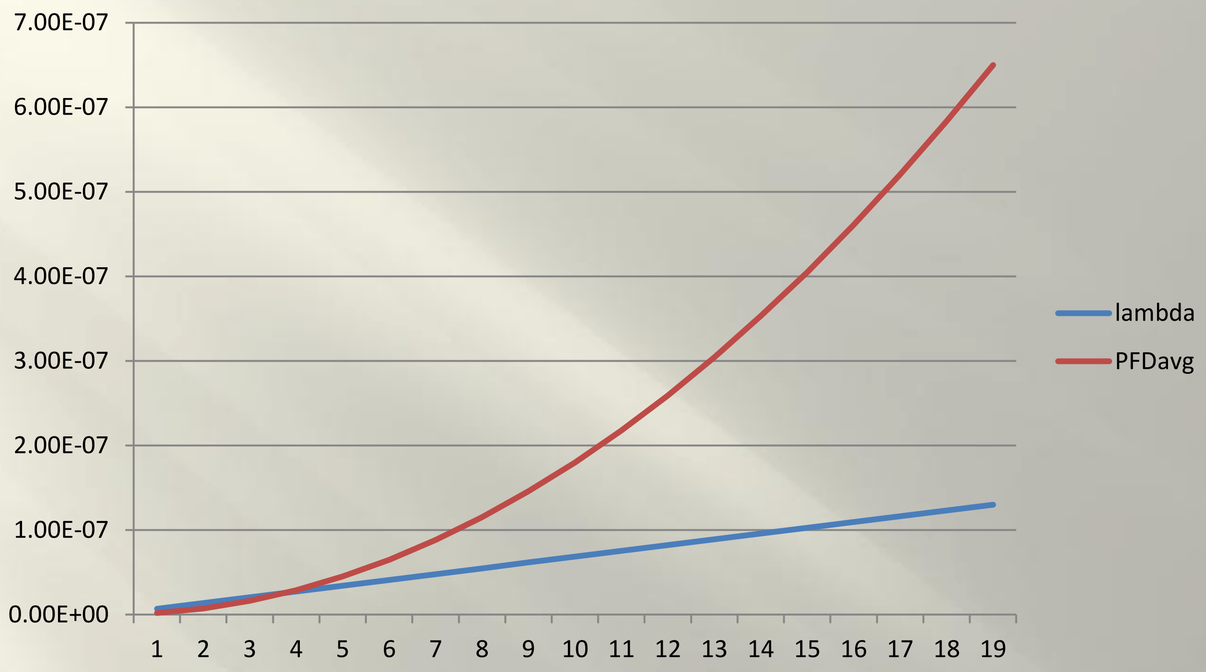
$$\lambda = \frac{1}{MTBF} = \frac{1}{1460000} = 685 * 10^{-9}$$

PFDavg

- 685 E-9 is the failure rate for all failures/hour.
- Using this failure rate may result in a erroneous estimate of dangerous failures.
- The dangerous failure estimate of mechanical devices working within rated tolerances should be calculated using known failure data from your facility.
- Using 10%

$$\lambda^D = 0.1 * 685 * 10^{-9} = 68.5 * 10^{-9}$$

PFDavg



- Calculating PFDavg over 1 to 19 percent of dangerous failures shows how PFDavg diverges
- The limit occurs at 100% dangerous failures

Common Cause

- Failures are divided into normal failures and common cause failures
- A beta factor is used to calculate failures due to common cause
- A typical beta factor for this calculation is 10%

$$\lambda^{DN} = (1 - \beta)\lambda^{D}$$

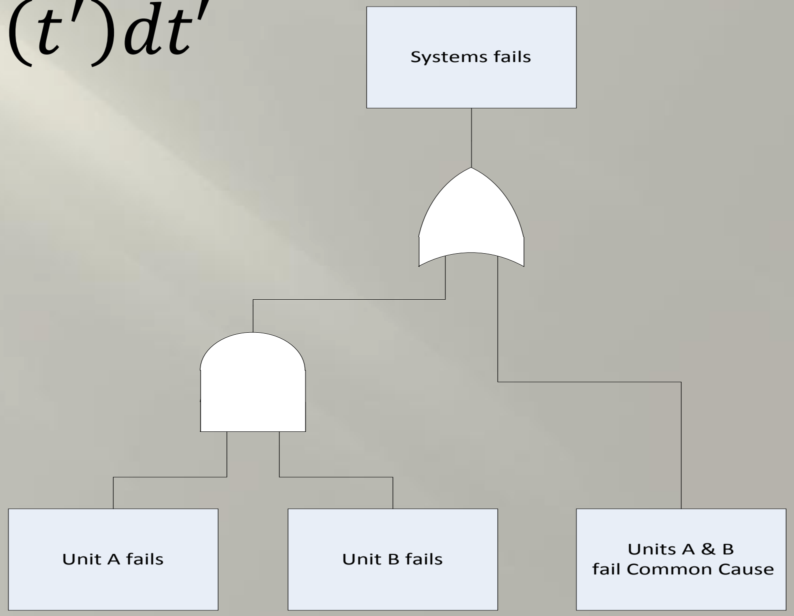
$$\lambda^{DC} = \beta\lambda^{D}$$

Common Cause Calculation

$$PFD = (\lambda^{DN})^2 * TI^2 + \lambda^{DC} * TI$$

$$PFDavg(TI) = \frac{1}{TI}\int_0^{TI} PDF(t')dt'$$

Eq. 12-7 in the text



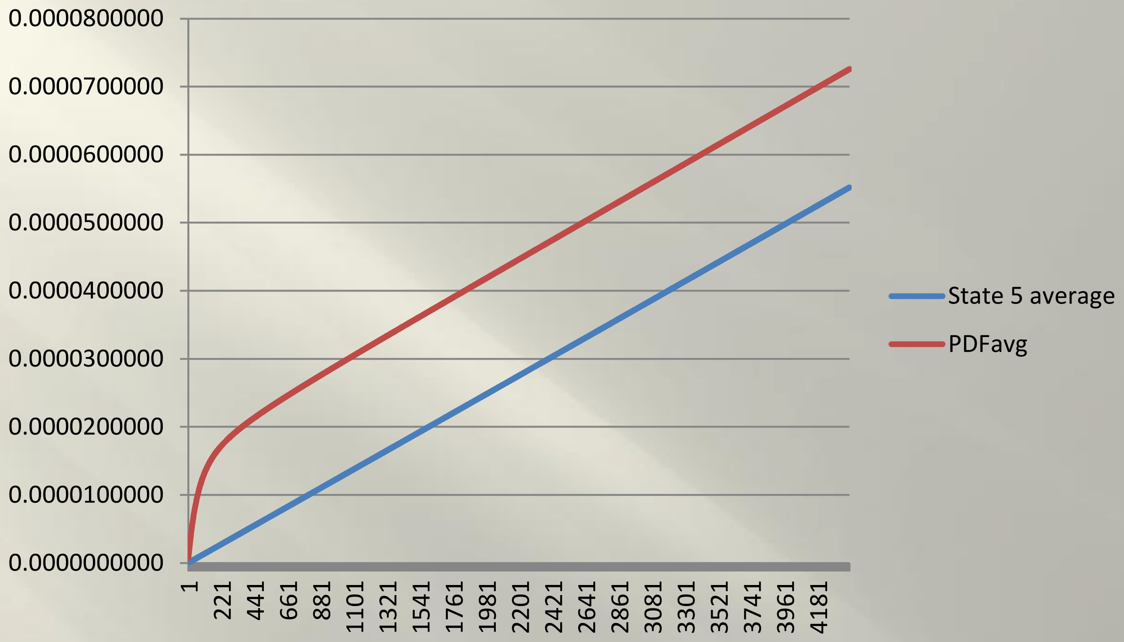
Example 12-10, page 273

- The data may be calculated using a spreadsheet
- When using =MMULT
  - Lock the cells using an
    - Locks an alpha numerical cell
  - Note that =MMULT contains an error that selects a sliding array1

=MMULT(array1,array2)

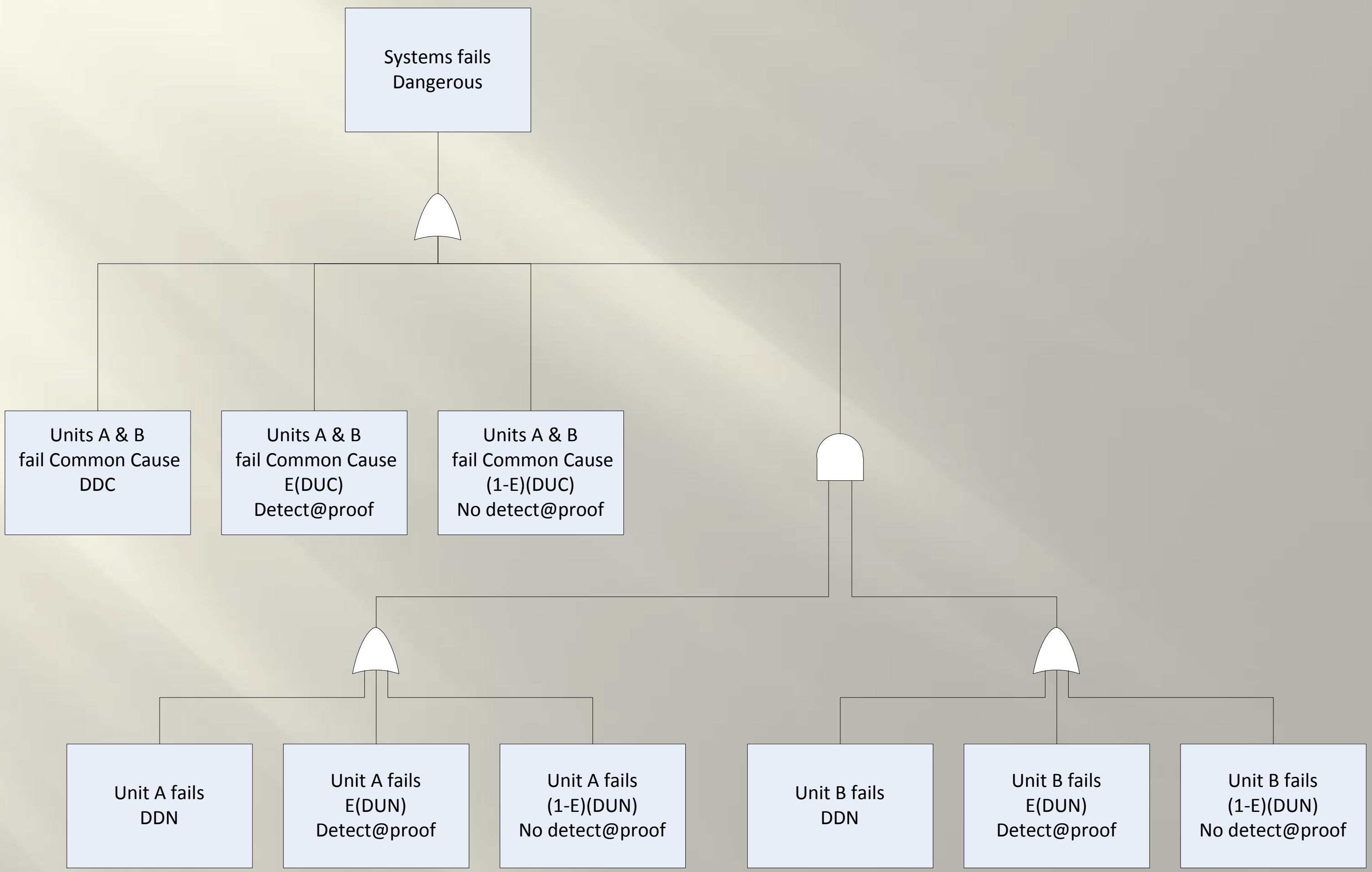
=MMULT(B34:G34,$B$26:$B$31)

Calculation Errors

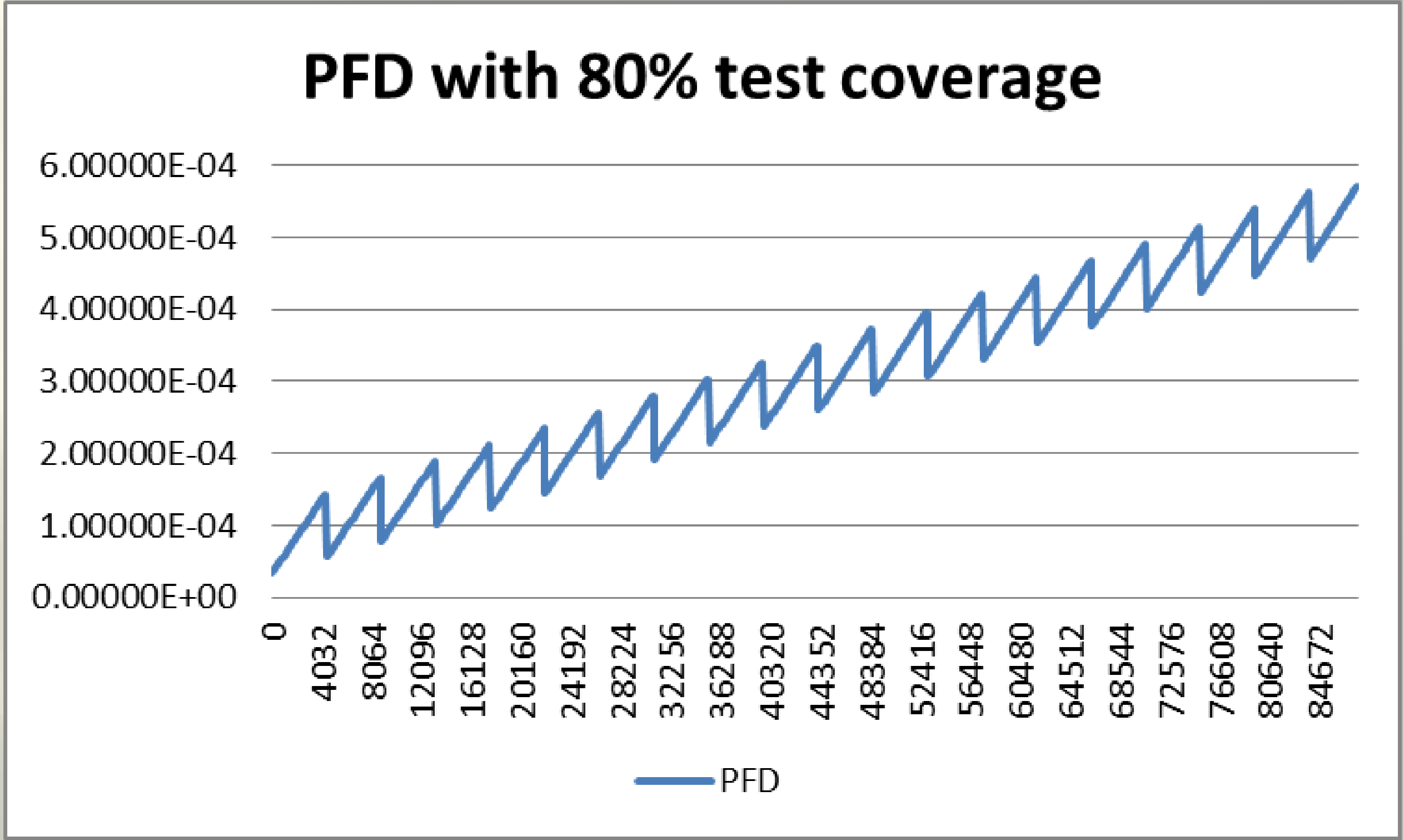


- An incorrect result occurs if you average only the data from state 5 in the S*P matrix.
- You must account for all the fail states
  - Column 3, 4 and 5

1oo2 Fault Tree w/ Proof Test



Risk is Increasing



Always Integrate

- The solution for the 1oo2 Fault Tree w/ Diagnostics, Common Cause and Proof Test is the PFD
- The PFDavg is the result needed for safety system evaluation
- The PFD must be integrated over time to find the solution
- A spread sheet may also be used, then average the PFD as a function of operating intervals

Story Time

- Here's your chance to discuss the topic
  - Safety System Models