NUCLEAR SAFETY AND RELIABILITY

WEEK 3

TABLE OF CONTENTS - WEEK 1

1. Introduction to Risk Analysis

Quantitative risk analysis is an engineering discipline combining component or subsystem failure probabilities with failure consequence analyses to arrive at a risk profile for any particular technology. The methodology has been developed in some detail over the past 15-20 years for use in nuclear power plant engineering and licensing. Most commonly, a combination of fault trees (using conventional reliability analysis, to be discussed in the following six lectures) and event sequence diagrams are constructed that define a succession of possible accident branches and their probabilities. The accident is described in successive stages:

1. An initiating event (IE) occurs.

2. A sequence of events follows the IE. Each event k has a probability of occurrence p_k and a probability ($1-p_k$) of non-occurrence. Each node in the chain branches to two alternate sub-chains. The branch probabilities may be determined either from fault tree analysis (to be discussed in later lectures) or from accumulated operating experience with the event in question. If no data are available the branch probabilities may be estimated by subjective judgment, made by individuals experienced in the field.

3. The whole of the sequence, initiated by IE and continuing through successive branches to a set of "final states", constitutes the event tree of the chain (or accident sequence). Every final state requires evaluation of (a) its probability of occurrence, and (b) the expected consequence. The formalism can be simplified by partitioning the whole event tree into segments, which can be combined later to yield the overall event tree.

Example

System Considered: A motorist is driving a car down a country road at night.

Initiating Event: A deer steps in front of the car.

1. Given the IE, the first question is: Does the driver notice in time? If NO, does the car hit the deer? (this depends on whether or not the deer evades the car).

2. If YES, the second question is: Does the driver brake in time? If NO, does the car hit the deer? (this again depends on deer evading or not, but the probabilities are different).

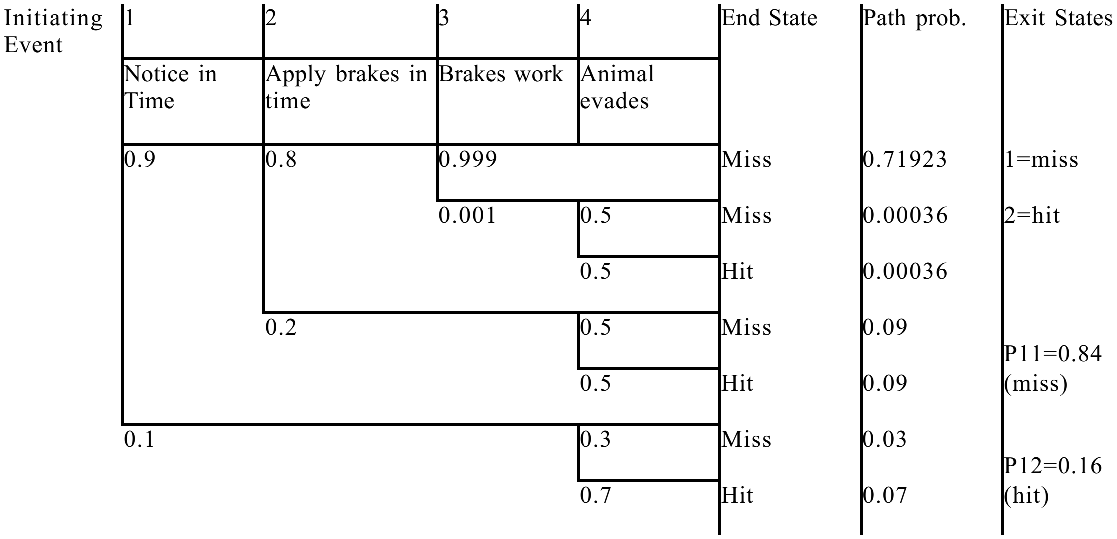
3. If YES, third question: Do the brakes work? If NO, does the car hit the deer? (this also depends on whether or not the deer evades the car).

Note the following:

A. We have not yet questioned the driver's state (he may be sleepy) or the speed of the car. All probabilities will in fact depend on "entry state" characterizing the driving conditions.

B. We have only tried to answer, up to this point, <u>one</u> ultimate question: Does the car hit the deer or not? We have yet to evaluate the consequences.

Notwithstanding A and B, we can construct an event tree for this portion of the overall chain of events. The basic event tree is shown as:



Initiating Event	1 Notice in Time	2 Apply brakes in time	3 Brakes work	4 Animal evades	End State	Path prob.	Exit States
	0.9	0.8	0.999		Miss	0.71923	1=miss
			0.001	0.5	Miss	0.00036	2=hit
				0.5	Hit	0.00036	
		0.2		0.5	Miss	0.09	P11=0.84 (miss)
				0.5	Hit	0.09	
	0.1			0.3	Miss	0.03	P12=0.16 (hit)
				0.7	Hit	0.07	

The event probabilities for the reference driving conditions are given as: probability of noticing in time = 0.9, probability of timely braking = 0.8. Two alternate entry states can be defined:

Entry state 2 - Sleepy driver, probability of noticing = 0.5
Then P21 = 0.60 (Miss)
P22 = 0.40 (Hit)

Entry state 3 - Speeding, probability of timely braking = 0.4
Then P31 = 0.66
P32 = 0.34

Summarizing in matrix form,

$$M_1 = \begin{pmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \\ P_{31} & P_{32} \end{pmatrix} \mathrm{P_{IJ}} = \text{probability of exit state J for given entry state I}$$

The consequence tree for this event sequence is analyzed independently. There are only two entry states: MISS, or exit state 1 from the previous tree and HIT, or exit state 2 from the previous tree. The exit states of the consequence tree are concerned with consequences to the deer, to the car, and to the driver's insurance policy. It is assumed that the animal dies if it is hit and damage to the car is sustained - in reality, degrees of consequence might be considered here as well. The consequence tree may be drawn as:

	- 5 -	- 6 -	EXIT STATE			
	Degree of Damage	Insurance Status	Number	Animal	Car damage	Insurance
Miss			1	Alive	None	OK
Hit	0		1	Alive	None	OK
	0.2		2	Dead	Minor	OK
	0.6		3	Dead	Moderate	OK
	0.2	0.5	4	Dead	Major	OK
		0.5	5	Dead	Major	Canceled

Or, in matrix form:

$$M_2 = \begin{vmatrix} P_{11} & P_{12} & P_{13} & P_{14} & P_{15} \\ P_{21} & P_{22} & P_{23} & P_{24} & P_{25} \end{vmatrix} = \begin{vmatrix} 1.0 & 0 & 0 & 0 & 0 \\ 0.0 & 0.2 & 0.6 & 0.1 & 0.1 \end{vmatrix}$$

Where P_{ij}= probability of consequence j given entry state i.

These event trees (now expressed as probability matrices) can be combined to give a probability matrix describing the probability distribution of various consequences (end states) for each of the defined input driving conditions (entry states). Let the probability of consequence j from driving condition i be Pij; then

$$P_{ij} = P_{i1}P_{1j} + P_{i2}P_{2j} = \underset{k=1}{\overset{2}{S}} P_{ik}P_{kj}$$

or, in matrix form: $M_3 = \left[P_{ij}\right] = M_1 \cdot M_2$

Numerically, the result is:

$$M_1 \cdot M_2 = \begin{vmatrix} 0.84 & 0.16 \\ 0.60 & 0.40 \\ 0.66 & 0.34 \end{vmatrix} \cdot \begin{vmatrix} 1.0 & 0 & 0 & 0 & 0 \\ 0.0 & 0.2 & 0.6 & 0.1 & 0.1 \end{vmatrix}$$

$$M_3 = \begin{vmatrix} 0.84 & 0.032 & 0.096 & 0.016 & 0.016 \\ 0.60 & 0.08 & 0.24 & 0.04 & 0.04 \\ 0.66 & 0.068 & 0.204 & 0.034 & 0.034 \end{vmatrix}$$

The event tree also can be segmented or decomposed into a succession of simpler event trees, each one containing only the relevant <u>conditional</u> probabilities (C.P.). For example,

Conditional Probability Matrices for Each Step of Event Tree

Question	Entry States	Exit States	Conditional Probability Matrix
Timely notice?	(3) 1-normal 2-sleepy 3-speeding	(4) 1-no sp, timely not. 2-no sp, late not. 3-speed, timely not. 4-speed, late not.	$M_1 = \begin{matrix} 0.9 & 0.1 & 0 & 0 \\ 0.5 & 0.5 & 0 & 0 \\ 0 & 0 & 0.9 & 0.1 \end{matrix}$
Timely braking?		(3) 1-timely braking 2-late braking 3-no braking	$M_2 = \begin{matrix} 0.8 & 0.2 & 0 \\ 0 & 0 & 1.0 \\ 0.4 & 0.6 & 0 \\ 0 & 0 & 1.0 \end{matrix}$
Brakes working?		(4) 1-timely, brakes ok 2-timely, brakes fail 3-late braking 4-no braking	$M_3 = \begin{matrix} .999 & .001 & 0 & 0 \\ 0 & 0 & 1.0 & 0 \\ 0 & 0 & 0 & 1.0 \end{matrix}$
Animal evades?		(2) 1-miss 2-hit	$M_4 = \begin{matrix} 1.0 & 0 \\ 0.5 & 0.5 \\ 0.5 & 0.5 \\ 0.3 & 0.7 \end{matrix}$
Degree of damage?		(4) 1-none 2-minor 3-moderate 4-major	$M_5 = \begin{matrix} 1.0 & 0 & 0 & 0 \\ 0 & 0.2 & 0.6 & 0.2 \end{matrix}$
FINAL STATE		(5) 1-miss, no conseq. 2-hit, minor damage 3-hit, mod. Damage 4-hit, major, ins.ON 5-hit, major, ins OFF	$M_6 = \begin{matrix} 1.0 & 0 & 0 & 0 & 0 \\ 0 & 1.0 & 0 & 0 & 0 \\ 0 & 0 & 1.0 & 0 & 0 \\ 0 & 0 & 0 & 0.5 & 0.5 \end{matrix}$

The arrows indicate that the exit states of the previous event tree segment are applied as entry states for the next segment.

Application to Reactor Systems

The methodology outlined in the above example can be applied at any level of complexity desired by the designer/analyst. The algebra quickly becomes difficult, so computer codes are written to relieve the drudgery. In general, the sequence contains the following steps.

A. PLANT event tree (from initiating event [IE] to a set of post-accident plant states).

Plant matrix M = [m_{kj}] , where m_{kj} is the probability that initiating event i_k leads to plant state y_j.

B. CONTAINMENT event tree (from plant states to radioactive releases).

Containment matrix C = [c_{kj}], where c_{kj} is the probability that plant state y_k will lead to release r_j.

C. SITE event tree (from releases to a set of consequences).

Site Matrix S = [s_{kj}], where s_{kj} is the probability that release r_k
will lead to consequence x_j.

Now define a set of probability vectors (row vectors):

- Of occurrence of IE:$\left[f^i\right]=\left[f_1^i, f_2^i, f_3^i, \ldots\right]$
- Of occurrence of plant state y_i:$\left[f^y\right]=\left[f_1^y, f_2^y, f_3^y, \ldots\right]$
- Of occurrence of radioactive release r_k:$\left[f^r\right]=\left[f_k^r\right]$
- Of occurrence of damage x_ℓ:$\left[f^x\right]=\left[f_\ell^x\right]$

Then, $\left[f^y\right]=\left[f^i\right]\cdot M$

And likewise, $\left[f^r\right]=\left[f^y\right]\cdot C$
$\left[f^x\right]=\left[f^r\right]\cdot S$

Finally, $\left[f^x\right]=\left[f^i\right]\cdot M\cdot C\cdot S$

Hypothetically, the full risk spectrum of the plant can be described in this way. In practice, the method is limited by the need to consider only a relatively small set of initiating events IE, and by the uncertainty associated with the completeness question: Are all possible initiating events encompassed by those chosen? Additionally, are all potential failure branches included in the event trees? By their nature, these questions cannot be answered precisely. Nevertheless, the systematic analysis of any engineered system that is inherent in this methodology makes it by preferable to the only apparent alternative, which is trial and error.

2. Laws of Probability

These concepts are well described in Section 2-1 in Chapter 2 of McCormick.

3. The Bayes Equation

A simple development is given in Section 2-2 of McCormick. Example 2.2 is of particular interest; further details are given in Kaplan and Garrick, "On the Use of Bayesian Reasoning in Safety and Reliability - Three Examples", Nuclear Technology 44, 231 (1979). The following example is based directly on CANDU operating experience.

The Frequency of Serious Process Failures in CANDU Stations

The AECB Siting Guide combines probabilistic and deterministic rules that have been developed over the past 25 years. One of the fundamental precepts is that "serious process failures" will occur which require response by special safety systems in order to prevent the release of radioactive materials from exceeding amounts which could lead to radiation doses above prescribed limits. The assumed frequency of such serious process failures ("serious" being defined as failures in which safety systems must intervene to prevent significant fuel failures) is one per three operating years.

The Guide provides that, at a frequency of once per three years, it is acceptable that the station release an amount of radioactive material off-site which would result in a whole-body dose to the hypothetical "most exposed individual" of 5 mSv. Consider a subset of serious process failures that could produce consequences of this magnitude. Historically, it is known that such a large release has never occurred. In fact, only minuscule amounts of radioactive material have been released from these stations under either normal or accident conditions.

The Bayesian question posed is "Given the observation of more than 160 reactor-years of CANDU operation with zero radioactive material release as a result of serious process failures (to the end of 1989), what is the probability of the alternate postulates that the occurrence frequency of this failure subset is one per 3 years, one per 30 years, etc.?" The calculation can be done on a hand calculator in about ten minutes; the result is shown in the following Table.

The Bayesian statistical argument relies on complete independence between each "event". In this case the event is one reactor year of operation without a serious process failure having off-site consequences. It seems fair to assume that one year's experience is independent of the next. The other data needed are the assigned prior (before the observation) probabilities of each postulated event frequency. The Uniform Prior Distribution says that we didn't know what to expect for the frequency of serious process failures with consequences. Added information from the observation "none in 160 years" reduces the probability that the real frequency of occurrence is one in three years to about 10^{-20}, and the probability that the real frequency is one in thirty years to 0.3 percent. The observation cannot distinguish between postulates 3,4, or 5.

Frequency of Serious Process Failures with Offsite Consequences in CANDU Reactors

	Postulate Number				
	1	2	3	4	5
Postulated frequency	$3x10^{-1}$	$3x10^{-2}$	$3x10^{-3}$	$3x10^{-4}$	$3x10^{-5}$
probability of zero events in 160 reactor years*	0	.008	.618	.953	.995
A.Uniform Prior	0.2	0.2	0.2	0.2	0.2
Distribution	0	.003	.24	.37	.38
Probability of Postulate					
Probability of postulate given zero events					
B.Estimated prior	0	.05	.50	.40	.05
distribution	0	.0005	.41	.50	.07
Probability of postulate					
Probability of postulate given zero events					

* probability = (1.0-postulated frequency)^{160}

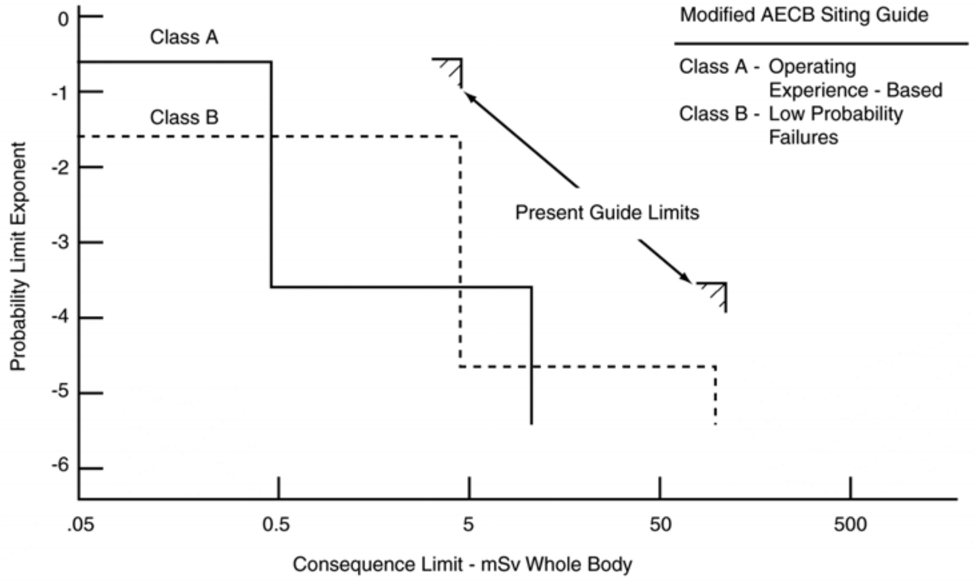
Now, if we use our best judgment about the real frequency of occurrence to estimate the prior distribution and then redo the calculation, the result of the observation skews the distribution even further toward the improbable end as seen in the Table under Estimated Prior Distribution. There is a diminishing return here because, with the prior distribution estimate, one is biasing the results. But at least we can eliminate postulate 1 from the list and can conclude that the probability of the recurrence frequency being as large as one in thirty years is quite small. As operating experience accumulates, now at a rate of 20 operating years per calendar year, these probabilities will become more firmly established.

The conclusion of this exercise can be expressed as follows: "As a result of direct operating experience with CANDU reactors, it has been found that the actual probability of occurrence of accidental radioactive releases is at least a factor of ten less than expected when the Canadian safety regulations were drawn up. This record is a credit to the diligence and care of the Utility operations staff, regulatory staff of the AECB, and finally AECL and Ontario Hydro designers. It is a record of which Canada can be proud." Such a statement should bring a lump to the throat of folks in the nuclear business and have a positive effect on public opinion of our enterprise. It might even reduce the pressure for making licensing regulations ever tighter.

This is an example of the direct use of real operating experience to slowly adapt the licensing system so that it more closely represents a true picture of plants risks. (Bayesian statistical reasoning can be applied to a large number of reliability and safety questions.).

The Siting Guide could be modified by introducing a second pair of steps in the graphical illustration, as shown in Figure 3.1. There would then be a new class of process failures with the old frequency limit of 1 per 3 years, but with a consequence limit of 0.5 mSv. The corresponding dual failure limit would be 1 per 3000 years at a consequence of 25 mSv whole body. The second class of process failures would have a limit of 1 per 30 years with the old consequence of 5 mSv; the dual failure component would have limit of 1 per 30,000 years at a consequence of 250 mSv whole body. Further years of reactor operating experience might reveal justification for even greater reductions.

Figure 3.1 – Risk-Limiting Regulation



4. Probability Distribution Functions

This topic is summarized in McCormick Section 2-3. It is covered in more detail in Chapter 3.

5. Probability Concepts for Failure Analysis

This subject is covered adequately in McCormick Section 2-4.

6. Probability Distributions

This topic is covered in Chapter 3 of McCormick. Knowledge of only a subset of this information is expected.

7. Data Manipulation, Failure Data

This material is covered in Chapters 4 and 5 of McCormick. Only general familiarity with these Chapters is expected.