PI 21.05

MODERN RELIABILITY TECHNIQUES

OBJECTIVES

5.1 Describe each of the following reliability assessment techniques by:

i) Stating its purpose.
ii) Giving an example of where it is used.

a) Fault Tree Analysis (FTA)
b) Safety Design Matrix (SDM's)
c) Probabilistic Risk Analysis (PRA)

COURSE NOTES

Going back to the Reliability Life Cycle in Module 0, you will recall that during the design phase there was a need to perform a number of safety analyses and reviews. At this time, there is a requirement to demonstrate to the Atomic Energy Control Board (AECB) that the design will meet the unavailability targets as specified in the Siting Guide. These targets have been developed to ensure safety to the general public.

The analyses however, don't end with the construction of the station. As conditions and requirements change, it is necessary to perform ongoing reliability reviews and analyses. In addition, the reliability models provide a tool that can be used by operations staff to ensure reliability targets continue to be met. In this module, we will be discussing some of the formal reliability studies that have been carried out and are still being done for our Nuclear Generating Stations.

According to "The Darlington Probabilistic Safety Evaluation Summary Report" (Ontario Hydro, 1987):

The assessment of risks associated with the operation of complex industrial undertakings, generally speaking, consists of finding answers to the following questions:

a) What are the undesired events that give rise to risk from the plant?
b) How can such undesired events occur?
c) Given the occurrence of the undesired events, what are their consequences in quantitative terms?

To find the answers to such questions we have used various techniques. In earlier modules, you have done reliability calculations using Block Models. Although they have been used in the past and are a useful tool for understanding how the system works and how its reliability is calculated, there are currently more powerful methods being used. At present, there is often more than one model used. Design Engineers

RISK

Up to this point, our discussion has been focussed on the probability of an event occurring (i.e., its reliability). We haven't yet looked at the consequences of the event if it does occur. For example, we can calculate that the probability of a system of three 50% pumps in parallel failing is 0.005, but what is the consequence if the system fails? Will we lose cooling to a minor system? A major system? The fuel? As you can see, these questions are important ones and must be considered in a discussion of public safety.

When the consequence of an event is considered along with its frequency, we are looking at a term called **risk**. Quantitatively, this is calculated by multiplying the frequency by the consequence.

$$RISK_{(Event)} = FREQUENCY_{(Event)} \times CONSEQUENCE_{(Event)}$$

This means that for an event that has a high frequency (probability of occurrence), along with severe consequences if it does occur, there will be high risk. Likewise for something that has a low frequency and low consequences, the risk is low. As an example, the frequency of failure of the glove compartment door in your car is low and the consequence to your safety is low, so as far as risk to your safety, this is a low risk event. On the other hand, the frequency of your brakes failing is relatively low but its consequence to your safety is high so we have a medium level risk. A high level risk may be mountain climbing where the frequency of falling is fairly high and the consequences are quite severe.

To get the total risk from a particular source, we add up the individual risk for each event.

$$RISK_{(Total)} = \Sigma_{(All\ Events)}\ RISK_{(Event)}$$

A risk management program could be based on risk from individual postulated events or on total plant risk, or, as is used in Ontario Hydro, both.

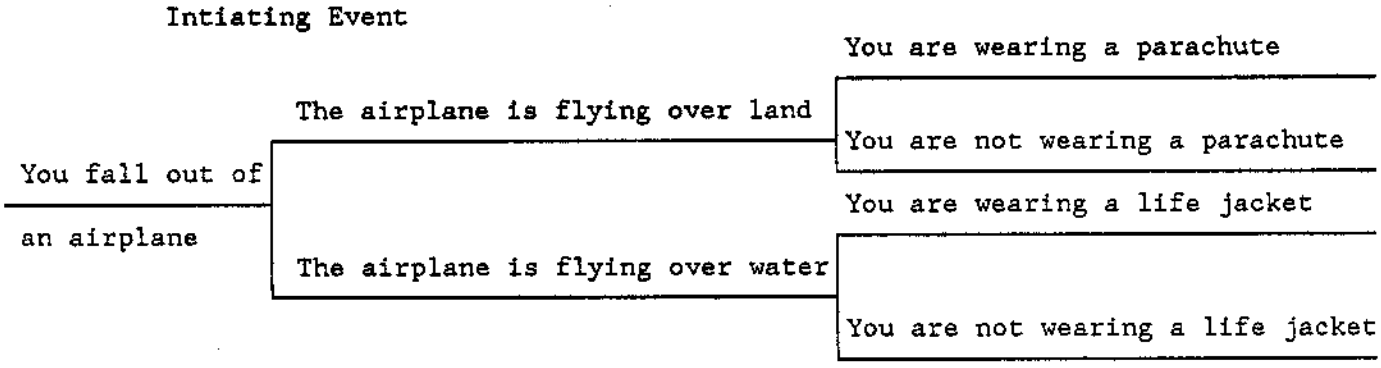
will prepare one during the design stage but it is often not specific enough or readily available to the System Engineers in operations. So they prepare their own models for whatever projects they are working on. Work is now underway so that there will be one reliability model prepared that can be used during the entire reliability life cycle. This model will be computerized to speed up the calculations and kept current with new data so that if you wanted to see the implications of delaying a Safety System Test or removing a piece of equipment from service, you would have a fast and easy way of doing it.

Probabilistic Risk Assessment and Safety Design Matrices are large studies which involve modelling the system, performing the calculations and documenting the results. They will be discussed in greater detail later on in this module. First we will look at Fault Tee Analysis, a technique similar to the reliability block diagram, that is used to

perform the calculations of probability, reliability and unavailability.

Event Trees

Event trees trace the logic connections that show the various possible outcomes of a given event called in Initiating Event. For example:



EVENT TREE

Fault Tree Analysis

Fault tree analysis (FTA) was developed in the early 1960's and was used in the aerospace industry principally for system safety analysis. It is a deductive top down approach to reliability prediction meaning that it considers an accident situation and then looks at the possible causes. It then examines the origins of those causes. At the same time, the probability of those causes is calculated.

Using our example above, we would now look at one part of the Event Tree (say, "You are not wearing a parachute") and investigate the possible causes of this - there wasn't one in the plane; you weren't told that you needed to wear one; you thought parachutes were for wimps, etc.

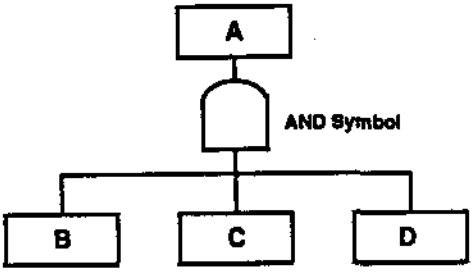
One of the most serious accidents which can occur at a nuclear generating station is the loss of coolant to the fuel. If this were to occur, there could be fuel failures and damage to the reactor itself. If we look at this accident, a loss of coolant, we can then examine what could cause it. The obvious cause would be if there was a major pipe break which allowed the water to leak out of the system. Taking it another step further, we could say, "what could cause the pipe to break?" We could then trace this all the way back to some root cause. This forms the basis of Fault Tree analysis.

FTA is used to trace the interactions between various components of a system in an organized and systematic manner. It also serves as a graphical display to show how basic component failures can lead to a pre-determined system failure state and, as a result, used to determine the different ways of failing and the likelihood of failure in the

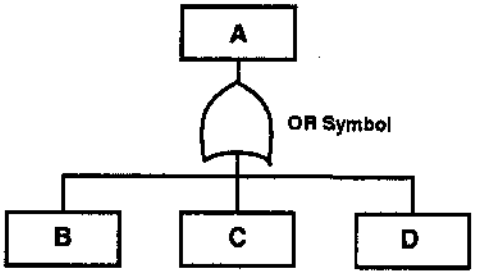
various systems identified in the event tree paths. This graphical display is similar to the reliability block diagrams used in the previous modules and is shown in the figures on the next page.

Explanation of Symbols

Unlike the reliability block diagrams, where logical relationships are shown by either drawing components in series or parallel, special symbols are used as part of the fault tree diagram to show logical AND's and logical OR's.



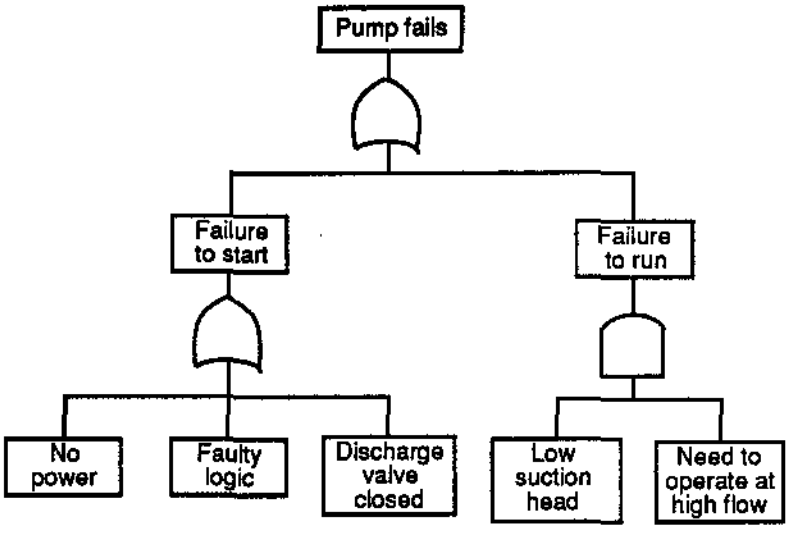
The diagram on the left shows that for event **A** to occur, **B** AND **C** AND **D** all have to occur.



The diagram on the right shows that for event **A** to occur, one of **B** OR **C** or **D** has to occur.

EXERCISE

1. What combinations of events could cause the pump in the following diagram to fail?



Once the diagram is constructed, failure data can be assigned to the component level of the tree. This means putting in numbers such as the failure rate, test frequency, repair times maintenance outages, etc. Then using the same probability rules we used in Module Two, it is possible to calculate reliability figures for systems and groups of systems all the way up to the top event in the Fault Tree.

Advantages of Fault Tree Analysis

Using a Fault Tree Analysis can help in many ways. It can:

1. Help make the analysis more objective.

2. Point out system aspects which are important with respect to the failure of interest.

3. Provide a graphical aid which can improve visualization of system interdependencies.

4. Provide the option for both Qualitative and Quantitative system reliability analyses.

Application of Fault Tree Analysis

Fault Tree Analysis can be done as a stand alone exercise to assess the reliability of a system or can be used as a part of a more detailed analysis. It forms part of the total package that makes up the reliability review.

EXERCISES

2. What is a Fault Tree Analysis used for?

3. Where is it used?

SAFETY DESIGN MATRIX AND PROBABILISTIC RISK ASSESSMENT

The next two techniques will be discussed together due to their similarity. In general terms, these techniques follow the following steps.

I Identity the Hazard

What are we concerned about? For example, "The release of radioactivity from a nuclear power plant leading to injury to members of the public".

II Determine How These Hazards Can Occur

What events could cause the consequences that have been identified in Step I. To identify these events, we use Event Trees and Fault Trees.

III Prepare Event Trees

This involves first identifying Initiating Events which, in the case of our nuclear stations, are those malfunctions which can, either by themselves or in a combination with other events, lead to fuel failures. Table 1 gives a list of some of these Initiating Events that were used at Darlington. The Event Tree Analysis then identifies those functions whose failure following the occurrence of an initiating event would lead to fuel damage. In other words, what systems should prevent fuel failure but wouldn't if they didn't work?

TABLE 1

Some of the initiating events used for the Darlington Study:

- 25 different LOCAs classified according to size and location
- PHT Pump Trip
- Loss of Pressure Control in solid mode due to loss of controller (high)
- Global Neutron Overpower
- Feedwater Line Break
- Total Loss of Low Pressure Service Water
- Loss of Instrument Air
- 26 different Loss of Power scenarios

IV Use Fault Trees to Perform Detailed Analyses

By this time, you have progressed down to the component level and can use reliability data to actually put some numbers into the model.

Safety Design Matrix

The Safety Design Matrix (SDM) is the precursor to the somewhat more powerful Probabilistic Risk Assessment technique of reliability assessment. It was used to a limited extent for Bruce A and extensively at Bruce B and Pickering B. Although similar to the Probabilistic Risk Assessment technique, it is not as thorough in that it considers fewer initiating events and only a limited number of system interdependencies.

Probabilistic Risk Assessment

In 1987, Ontario Hydro notified the AECB that it would not undertake to update the SDM, opting instead to perform full Probabilistic Risk Assessments on all its nuclear stations. This change has occurred to make use of the most current risk assessment methodology and to use techniques which have been accepted internationally as the standard way of doing these studies. Darlington was the first to undergo this type of analysis and the study known as the Darlington Probabilistic Safety Evaluation (DPSE) was completed in 1987 and consists of 20 volumes of data and calculations. It is expected that this type of analysis will be done for all our other stations.

As stated earlier, the PRA considers many more initiating events and system interdependencies. The DPSE also expanded the number of systems covered to include the Fuelling Machine, End Shield Cooling, Class IV, III, II and I Power, Emergency Power and Low Pressure Water among others.

SUMMARY

Fault Tree Analysis

- A graphical method used to examine how basic component failures can lead to system failures.
- Primarily used as part of a reliability model to trace the interactions among various sub-systems/components of a system in an organized and systematic manner.
- Currently used as the system level analysis part of larger reliability assessments.

Probabilistic Risk Assessment

- A large scale analysis of a complex set of systems which takes into account a large number of system interdependencies.
- The resultant reliability model can be used during the operations phase of the station life cycle.

Darlington Probabilistic Safety Evaluation is currently the only one that is completed as of September 1988, but this type of analysis is planned for the other stations.

ASSIGNMENT

1. For each of the following statements, place the appropriate acronym in the space to match the correct analysis.

   FTA - Fault Tree Analysis
   SDM - Safety Design Matrix
   PRA - Probabilistic Risk Assessment

   _____ A limited version of PRA which considers fewer initiating events and systems.

   _____ A large scale analysis which includes analysis of Standby Electrical Power, Instrument Air and Service Water.

   _____ A graphical technique used to analyze interactions between various sub-systems and components.

   _____ The first one was done for the Darlington Nuclear Generating Station.

   _____ Done at the Pickering B and Bruce B stations but being phased out.

This Module Prepared By: Richard Yun, WNTC