Course PI 21

RELIABILITY FOR MANAGEMENT AND PROFESSIONAL STAFF

January, 1990 (R-0)
WP2644uu

January, 1990 (R-0)
WP2644uu

TABLE OF CONTENTS

PI 21.00

INTRODUCTION TO THE COURSE

Audience and Prerequisites

This course is for Management and Professional staff as part of the initial training program. For the most part, these people will be Junior Engineers in Training who have recently graduated from an Engineering or Honors science program at a university. From time to time, there may also be some people who have joined the Nuclear Generation Division in a more advanced position from another division with Ontario Hydro or from an external location.

The prerequisites for this course are:

1. The course introduction to CANDU which outlines the Corporate Objectives.

2. At least one of senior high school math, first year college or university math, or NTC math courses 421, 321 and 221.

Course Content

As you start this course, you should ask yourself "Why am I learning about Reliability?" If you are not sure **why**, then it makes it difficult to see the relevancy of this training. So, let's start by looking at WHY this course exists.

All training should be for one purpose and one purpose alone. That is to improve on-the-job performance. Therefore, this course should help you, someone who will be working as an employee in Ontario Hydro in a technical capacity in a production environment, do your job better.

Reliability is important for a number of reasons that we will be discussing in this course - the main ones being **Safety** and **Cost**. While this course will not be attempting to make expert reliability statisticians out of you, it is intended to give you the tools to do your jobs more efficiently and effectively.

We will be covering some basic calculations, a few definitions and some of the techniques that are used to analyze systems in the operations environment. The table of contents gives you an outline of the topics in this course.

The general aim of the course is to provide you with sufficient background in rudimentary reliability theory so that you will be able to:

a) When designing equipment or systems:

- Recognize that cost and reliability are the two major considerations, the one usually weighing against the other
- Estimate system reliability from component reliabilities
- Estimate component redundancy required to meet target reliability

b) When purchasing equipment:

- Interpret manufacturer's reliability specifications
- Ask for appropriate data if it is not supplied voluntarily

c) When commissioning equipment/systems, devise means of demonstrating equipment/system reliability.

d) When "operating" plant equipment/systems:

- Recognize the importance of collecting accurate data on failures, outages and repairs
- Calculate component and system reliability from failure rate data
- Rationalize the need for and design maintenance schedules (especially for preventative maintenance and/or replacement of components)
- Rationalize the need for and design test schedules for passive safety systems

e) Rationalize the role of station reliability in minimizing cost of electricity and maximizing plant safety.

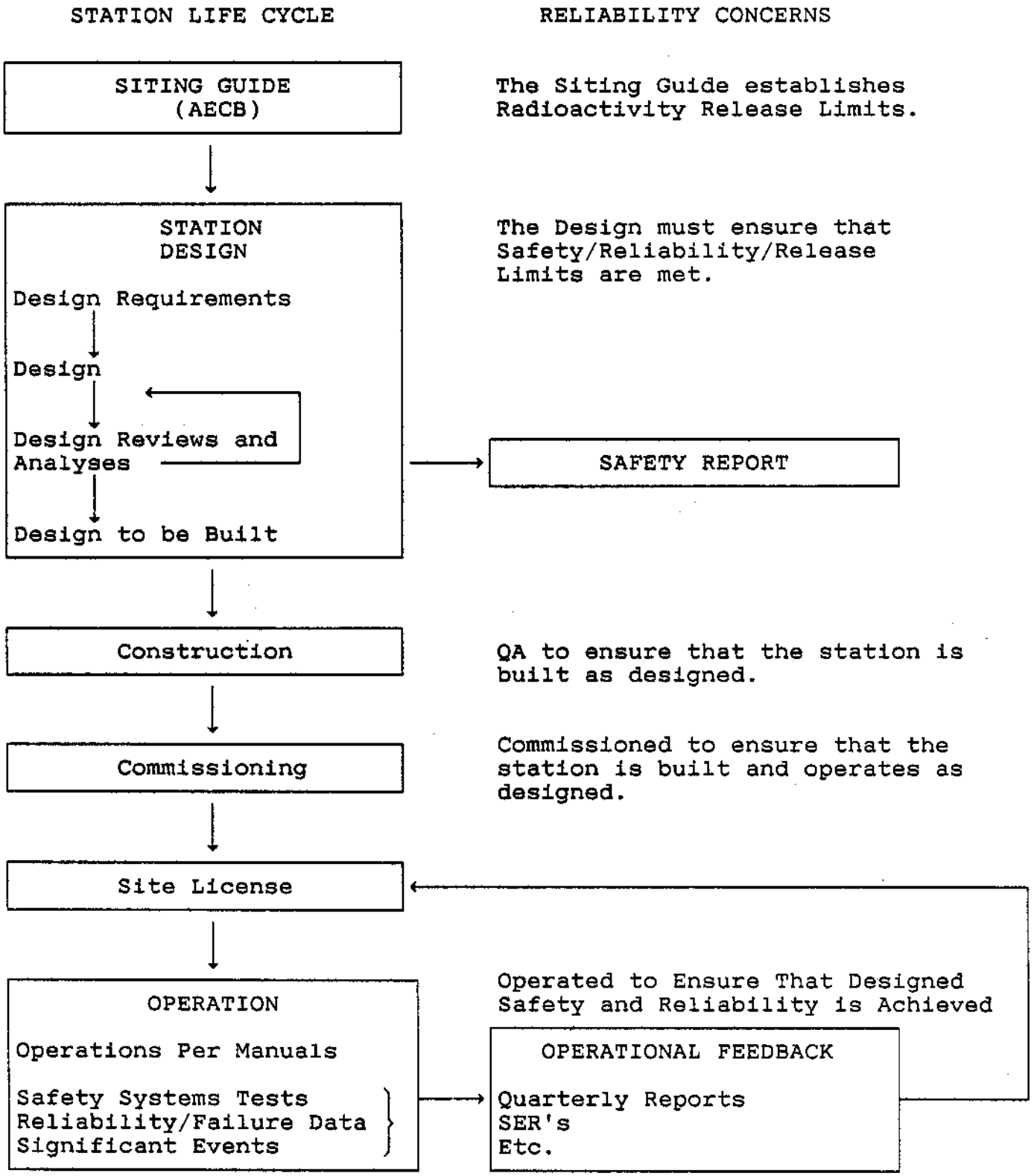
f) Rationalize the existence of reliability departments in Ontario Hydro and interpret reports published by such groups.

The figure on the next page is the Reliability Life Cycle. It shows for each phase in the station's life, the corresponding reliability concerns. For the most part, we will be concentrating on those areas, as shown highlighted, that deal with the **operation** of the station and we will be referring back to this diagram from time to time throughout the notes. However, reliability is a part of every phase of the station's life.

Course Structure

The course is made up of the seven self-contained units of instruction called "modules" as listed in the Table of Contents. Except for this module, all the remaining six modules are divided into two parts:

RELIABILITY LIFE CYCLE



The Objectives

These both specify the content of the module and define the scope of the test you will write at the end of the course. The objectives are based on discussions with staff who are working in the environment that you will be in and have been reviewed by Training and Technical Superintendents to ensure that they are relevant to your job duties.

The Course Notes

To help you meet the objectives and pass the final test, this material contains all the information that you will need. New terms and key concepts are highlighted in the text and are reinforced in a summary at the end of the module. Exercises along the way give you an opportunity to look at the subject material in a little more detail or from a different angle. The summaries are followed by assignment questions based on the objectives to give you an opportunity to practice what you've learned. You can then check your answers by referring back to the relevant parts of the text. If you still aren't sure about the answer, discuss it with the Instructor or your classmates. During reviews in class, you may be called upon to give your answer to some of the questions.

Learning Format

The layout of the course notes makes self-studying a viable option. If you choose to do this, make arrangements to write the final test when you are ready for it. However, the course can also be taught by an Instructor using a balanced mixture of lecturing, self-studying, group-discussions and review sessions. Along with audio-visual aids, this approach can enhance the learning process.

This Module Prepared By: Richard Yun, WNTC

PI 21.01

AN INTRODUCTION TO RELIABILITY

OBJECTIVES

1.1 Explain the implications of station reliability for Ontario Hydro's objectives in the following areas:

a) Worker Safety
b) Public Safety
c) Environmental Protection
d) Reliability of Electrical Supply
e) Cost

1.2 State the working definitions of:

a) Reliability
b) Availability

1.3 State two basic limitations on the applicability of reliability theory.

COURSE NOTES

As far as nuclear reactors go, our CANDU units have historically done quite well when compared to other reactors around the world. This performance is attributable in part to a comprehensive and co-ordinated program of research and development, design, manufacturing, construction and operations. A significant feature of this program, which has been operating since 1942, is feedback of operating experience to researchers, designers and manufacturers.

By 1986, Ontario Hydro had accumulated ≈156 reactor years of operating experience with CANDU units. Right from the start, Nuclear Operations at Ontario Hydro has followed a Management by Objectives approach. This involves setting down objectives that describe where we are going and what we are trying to achieve. The basic objectives fall under the following headings:

- **Worker Safety**
- **Public Safety**
- **Environmental Protection**
- **Reliability of Electrical Supply**
- **Cost**

Numerical indices have been established to quantify performance in each of these five areas, so that performance can be measured, compared to targets and analyzed for trends. The reliability for plant systems is critically important to achieving objectives in all five areas.

How Plant Reliability Affects the Basic Objectives

High reliability of plant systems is crucial to achieving NGD's five basic objectives as explained below.

1. Worker Safety

   The safety of our employees is affected both directly and indirectly. Obviously the more reliable the plant equipment, the less likely we will have equipment failure which can injure or kill someone. Indirectly, if we have reliable equipment, fewer hours are required to maintain equipment which then lessens the exposure of workers to hazards which can cause injury or death.

2. Public Safety

   The risk to public safety is low unless both process and safety systems fail simultaneously. So, the more reliable these systems, the safer the public.

3. Environmental Protection

   The more reliable the plant process and safety systems, the lower the risk of damage to the environment resulting from releases of radiation or chemicals, noise, high temperatures, etc.

4. Reliability of Electrical Supply

   The more reliable the plant systems, the less likely the unit wil suddenly stop producing electrical power.

5. Cost

   The more reliable the plant process systems:

   a) The fewer maintenance personnel and replacement parts which may be required, in other words, lower maintenance costs.

   b) The less time that the unit is unable to produce power, the better the return on plant investment. In the long-term, if equipment is out of service, in need of modification, or requires extra outages to maintain, there will be higher costs in operating it.

It is important to note that although there are five objectives, they are not all equally weighted. The first three objectives dealing with the **safety and protection of the workers, the public and the environment must always have higher priority** than the two objectives dealing with reliability of electrical supply and cost.

However, it is clear that obtaining and maintaining highly reliable plant systems is a common objective to all five of the basic objectives of nuclear operations. Achieving highly reliable plant systems involves virtually every phase of the project: design, purchasing, commissioning, operations and maintenance.

EXERCISES

1. To minimize the cost of the plant and its operation, why don't we minimize the number of safety devices and systems?

2. Can you give an example of where the first objective given below must take precedence over the second?

   a) *Worker Safety vs Cost*

b) Public Safety vs Reliability of Electrical Supply

3. Explain how improved reliability of the overall station and systems affects:

a) Public Safety

b) Cost

Working Definition of Reliability of a Device

The term "reliability" has been used so far without definition because its technical meaning is similar to its meaning in common usage. However, a definition of reliability as a quantity which can be calculated or measured is required for technical applications. The working definition of reliability is therefore:

> *The probability that the device will perform it purpose adequately for the period of time intended under the operating conditions encountered.*

Note that the reliability is a probability and has a numerical value ranging from 0 for the impossible event, something totally unreliable (cannot succeed) to 1 for the inevitable event, or something totally reliable (always succeeds for the time intended). Note too that this probability usually has a time dependency which can be mathematically modelled. Although more advanced treatments model both degree of performance and variations in operating conditions, this introductory course assumes only two degrees of performance - either the device is fully capable of, or utterly incapable of, performing its intended purpose. The operating conditions are assumed constant.

Working Definition of the Availability of a Device

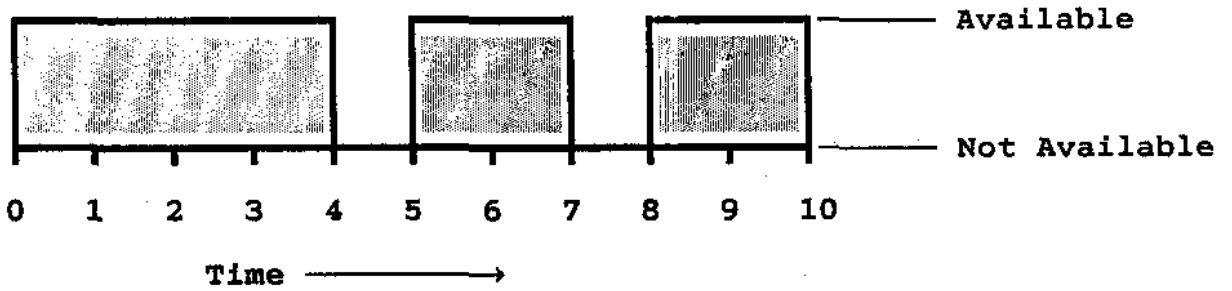
The term **availability** is often used interchangeably with reliability but in fact it has a different meaning.

> *Availability is the fraction of time that a device is available to perform its function if it is called upon to do so.*

This figure is also between 0, meaning that the device is never available and 1, meaning that it is always available. The term availability is often used in describing the devices or systems which are normally not in operation but may be called upon to operate in some circumstances. We also use the term **unavailability**, fraction of time **not available**, when talking about safety systems.

To differentiate between these two terms, let's look at a new pump we are going to put into service. We can estimate the reliability of the pump for, say, the first year of operation, by looking at historical data for pervious pumps of this type. Say this is 0.99. This means that there is a 0.99 (99%) probability that the pump will still be in working order at the end of the year. Or again, a (1 - 0.99) = 0.01 (1%) chance that it will not be. Note that the longer the pump runs, the lower will be its probability of working over the whole period. In other words, the probability of running without failure is higher for one year than for two (assuming, of course, no preventative maintenance). So, you can see how reliability is dependent on the time period being look at.

We usually use the term availability when talking about systems which are poised, ready to operate (e.g., systems needed in an emergency). It is measured by the fraction of time a system is available to perform its function. The following figure shows a system with an availability of 0.8 (this is only for illustration - CANDU systems must be much more available than this!).



Both reliability and availability are unit-less: reliability is a probability and availability is a fraction. Note, however, that for the system shown in the figure above, if you pick a time in the figure at random, the probability that the system will be working at that time is 0.8.

EXERCISES

4. Without looking back, try to fill in the blanks in the following definitions and then check your answers:

   RELIABILITY: The _____ that the device will _____ its _____ adequately for the _____ of _____ intended under the _____ _____ encountered.

   AVAILABILITY: The _____ of _____ that a device is _____ to _____ its _____.

Limitations of Reliability Techniques

Reliability theory is the application of the methods of probability and statistics to predict the system reliability on the basis of operating experience (failure rates). There are two basic limitations on the application of this theory in practice.

1. The validity of reliability theory calculations is based on the assumption of **statistical regularity** in equipment failures due to normal causes. Failure due, for example, to sabotage or to collisions between earth and other celestial bodies or to the construction of an intergalactic bypass do not enter the picture.

2. Reliability theory cannot be used to predict precise events or times thereof, only probabilities and statistical averages. For example one could not calculate the precise time and duration of the next forced outage on Bruce A Unit 3, but one could calculate the expected frequency and average duration of forced outages on Unit 3, or the probability that a forced outage will occur within say, 90 days.

SUMMARY

In this module we have looked at:

- The five major objectives of NGD:

  1. Worker Safety
  2. Public Safety
  3. Environmental Protection
  4. Reliability of Electrical Supply
  5. Cost

  and have seen how station reliability impacts on them. Refer to the notes for a detailed look at these impacts.

- The Working Definition of Reliability is:

  The probability that the device will perform its purpose adequately for the period of time intended under the operating conditions encountered.

- The Working Definition of Availability is:

  The fraction of time that a device is available to perform its function if it is called upon to do so.

- Two limitations on the applicability of reliability theory are:

  1. It assumes normal causes of failures only (statistical regularity).

  2. It is only a statistical average and not a precise prediction.

ASSIGNMENT

1. Which of the following are the five major objectives of NGD?

_____ Environmental Protection	_____ Reliability
_____ Trained Staff	_____ Production of Electricity
_____ Worker Safety	_____ Cost
_____ New Technology	_____ Public Safety

2. What implications does station reliability have on:

a) Worker Safety

b) Cost

3. State the working definition of Availability.

4. What are the two limitations on the applicability of reliability theory?

This Module Prepared By: Richard Yun, WNTC

PI 21.02

RELIABILITY CONCEPTS

OBJECTIVES

2.1 Using block models, calculate the reliability of simple networks which include components in series and parallel.

2.2 Describe (mathematically if applicable) the effects of the following design concepts on the reliability of a system:

a) Redundancy
b) Independence
c) Channelization
d) Two out of Three Logic
e) Odd/Even Components
f) Group 1/Group 2 Systems

COURSE NOTES

As you no doubt remember from the last chapter, reliability is defined as *the probability of success.* So, it is a good idea to pause at this time to go over some basic probability rules which we will be using when analyzing systems and components.

First of all, what is probability anyway? Probability is quite simply the chance or likelihood of something occurring. For example, "There's a 50-50 chance that a coin will come up heads", "...an 85% chance of rain" or "a one in a billion chance of winning the jackpot in the lottery".

We use the format **P(A)** to represent the probability of **A** happening. So, the probability of a coin coming up heads is P(heads) = 1 in 2 or 0.5. Likewise the probability of a particular pump failing to start when called upon to do so might be 1 in 500 or 0.002.

There will also be times when we need to look at the probability of combinations of events. For example "What is the probability of your brakes failing at the same time that you are approaching a stop sign?" Another example would be "What are the chances of a pump and its discharge valve failing?" These two examples describe the combination where one thing happens AND another thing happens.

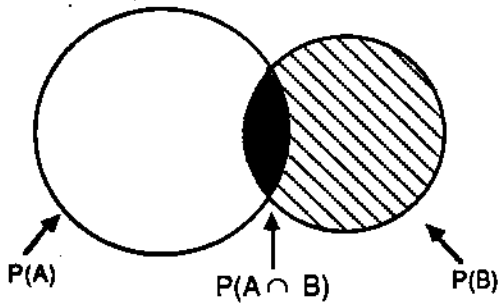
There are also situations where we are interested in the probability of a combination of events where one thing happens OR another thing happens such as "What is the chance of either the Argos winning or the Jays winning?" Since either outcome would result in happy Toronto sports fans, we are only interested in the probability of one OR the other.

The probability rules that cover these scenarios are referred to as **AND** and **OR**. That is to say *"What is the probability of one thing happening AND another thing happening?"* and *"What is the probability of one thing happening OR another thing happening?"* The Venn diagrams below show these two concepts graphically.

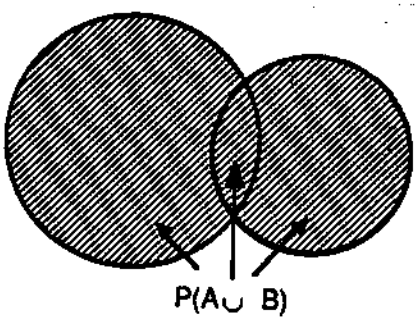
AND (symbol, $\cap$)

$$P(A \cap B) = P(A)\,P(B)$$

The probability of A AND B is equal to the probability of A times the probability of B (for events that are independent of each other).



Let's see an example of how this **equation is used.** If we say A, the probability of a hockey player being Wayne Gretsky, is 1 in 1000 or 0.001 and B, the probability of a player being traded to the L.A. Kings, is 1 in 10 or 0.1, then the probability of a player being traded to the L.A. Kings and that player being Wayne Gretsky is P(A) x P(B) = (0.001) x (0.1) = 0.0001. This is a pretty small number which means that it is not very likely to happen but, of course, we all know that *not very likely* doesn't mean never.



For combinations that involve OR, we use the following equation:

OR (symbol, $\cup$)

$$P(A \cup B)$$

$$= P(A) + P(B) - P(A \cap B)$$
$$= P(A) + P(B) - P(A)\,P(B)$$

The probability of A OR B is equal to the probability of A plus the probability of B minus the probability of A AND B (because this area is counted twice). Again this assumes that the events are independent of each other.

As an example of this, let's look at the Olympics. If the probability of Canadian sprinter Ben Johnson running fast enough to win the gold medal, P(G) is 0.7 and the probability of running fast enough to win the silver medal, P(S) is 0.9, then the probability of running fast enough to win the gold OR the silver medal is:

$$P(G) + P(S) - P(G)\,P(S)$$

$$= (0.7) + (0.9) - (0.7)\,(0.9)$$
$$= 1.6 - 0.63$$
$$= 0.97$$

EXERCISES

1. If the probability of a valve failing is 0.05 and the probability of the pump downstream of the valve failing is 0.07, what is the probability of the valve AND the pump failing?

2. The probability of a severe snow storm in the Winter is one in twenty-five. What is the probability of a snowstorm occurring during the weekend (Saturday and Sunday)?

3. The probability of a weekend social event occurring during Winter is 20%. What is the probability that a snowstorm will occur during a weekend that there is a social event?

We use the letter **R** to represent Reliability, the probability of working, and **Q** to represent Unreliability, the probability of not working. Since we are assuming that a component can only be working or not working, the probability of working plus the probability of not working equals one.

$$R + Q = 1$$

The two equations for calculating the probability of combinations of events and the equation given above, form the basis for the analysis of more complex systems which consist of components operating in series and in parallel. When looking at a system, you have to step back and say to yourself, "How does this system work?" If you take a look at Figure 1, you'll see that this system consists of three 100% pumps. This means that any one of these pumps can handle the flow requirements for the system. So, this system works if Pump A **OR** Pump B **OR** Pump C work.

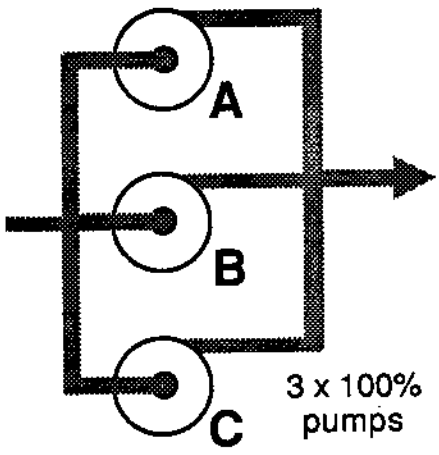


Figure 1

So, the probability of the system working is determined as follows:

R = probability of working

$$\begin{aligned} R(A \cup B \cup C) &= R[(A \cup B) \cup C] \\ &= R[(R(A) + R(B) - R(A)\,R(B)) \cup C] \\ &= [R(A) + R(B) - R(A)\,R(B)] + R(C) \\ &\quad - [R(A) + R(B) - R(A)\,R(B)]\,R(C) \end{aligned}$$

Another way of looking at it is that the system *doesn't* work if Pump A **AND** Pump B **AND** Pump C don't work. So, the probability of it not working is determined as follows:

Q = probability of not working

$$Q(A \cap B \cap C) = Q(A)\,Q(B)\,Q(C)$$

As another example, we can look at the valve arrangement below. Here we see that for flow to go through the pipe (probability of the system working), we need Valve 311 **AND** Valve 313 **AND** Valve 315 to work.

Valve 313

Valve 313 **Valve 315**

This means that the probability of the system working (provided a valve does not fail open) is determined as follows:

R = probability of working

$$R(311 \cap 313 \cap 315) = R(311)\ R(313)\ R(315)$$

Again, there is another way of looking at this. The system will **not** work if Valve 311 **OR** Valve 313 **OR** Valve 315 doesn't work. The equation for that is given as:

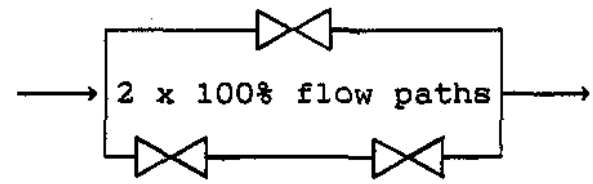
Q = probability of not working

$$\begin{aligned} Q(311 \cup 313 \cup 315) &= Q[311 \cup 313) \cup 315] \\ &= Q[(Q(311) + Q(313) - Q(313)) \cup 315] \\ &= [Q(311) + Q(313) - Q(311)\ Q(313)] + Q(315) \\ &\quad - [Q(311) + Q(313) - Q(311)\ Q(313)]\ Q(315) \end{aligned}$$

Using these two equations for probabilities and with a bit of mathematical manipulation, it is possible to determine the reliabilities and unreliabilities for almost any configuration. Keep in mind that although we've been using symbols to represent reliability, in actual calculations, these are numerical values. On the next few pages, there are some other examples showing the use of these equations.

EXAMPLE ONE

In the valving arrangement shown on the right, there are two flow paths each capable of handling 100% of the flow. The valves are all identical and have a reliability of 0.95, calculate the reliability of the arrangement.



Looking at the setup, we can see that for the arrangement to work, either the top path OR the bottom path must work. So, the reliability of the arrangement, being the probability of it working, is given by:

R(total) = R(top) + R(bottom) - R(top) x R(bottom)

For the top flowpath to work, the valve in that path must work (we will assume that the piping is 100% reliable). So, the reliability of the top path is simply the reliability of the valve. However, for the bottom flow path to work, both the first valve **AND** the second valve have to work. So, the reliability for the bottom flow path is:

R(bottom) = R(valve 1) x R(valve 2)
R(top) = R(top valve)

Therefore,

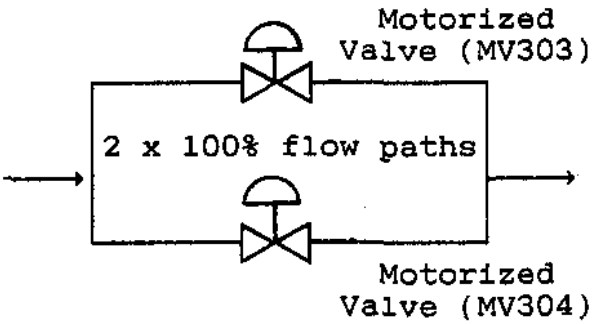
R(total) = R(top valve) + [R(valve 1) x R(valve 2)]
- R(top valve) x [R(valve 1) x R(valve 2)]

Since all the valves are identical then their reliabilities are all 0.95. Substituting these figures into the equation, we get:

R(total) = 0.95 + [0.95 x 0.95] - 0.95 x [0.95 x 0.95]
= ***0.9951***

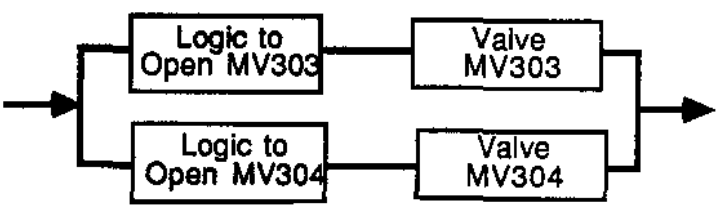
So, you can see the overall reliability is higher than for the individual valves.

EXAMPLE TWO



This valve arrangement is part of the High Pressure Emergency Coolant Injection System at Bruce B and is very similar to the arrangement used in the first example except that we now have two motorized valves in parallel. This means that the valve is opened and closed using a motorized actuator which can be controlled either locally or remotely. From a reliability calculation point of view, the difference is that now the reliability of the valves also depends on the logic which opens and closes the valves. To show this we need to draw a **Reliability Block Diagram.**

This type of diagram helps to visually show the interrelations of the various components in the network. Components which are related in an AND arrangement, where the reliability of the combination depends on one AND the other working, are shown in series whereas components which are related in an OR the other working, are shown in parallel. The Reliability Block Diagram for the above arrangement is shown



Note that although the block diagram resembles the actual physical layout of the system, it is not an exact physical representation. For instance, we know that the actual fluid flow in the real system doesn't go through the logic of the motorized valve. The flows shown on a block diagram indicate logic flows.

Now to continue with the example, given that the reliability of the valves are the same as for the last example, R(valve) = 0.95 and that the reliability of the logic to operate the valve, R(logic) is 0.99, calculate the reliability of the system.

$$R(\text{total}) = R(303) + R(304) - R(303) \times R(304)$$

$$R(304) = R(\text{valve}) \times R(\text{logic})$$
$$R(303) = R(\text{valve}) \times R(\text{logic})$$

Therefore,

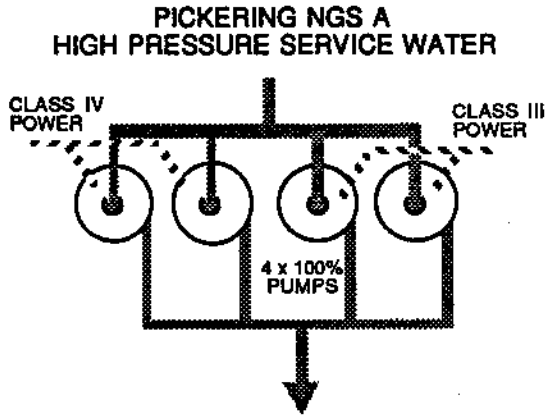
$$R(total) = [R(valve) \times R(logic) + [R(valve) \times R(logic)] - [R(valve) \times R(logic)] \times [R(valve) \times R(logic)]$$

Substituting the appropriate figures into the equation, we get:

$$R(total) = [0.95 \times 0.99] + [0.95 \times 0.99] - \{[0.95 \times 0.99] \times [0.95 \times 0.99]\}$$
$$= \mathbf{0.9966}$$

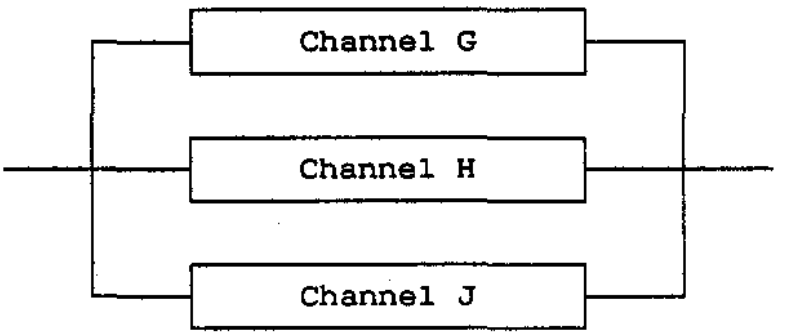
EXERCISES

3. Draw a **Reliability Block Diagram for the following system:**



4. If the reliability of the Class III pumps is 0.96, the reliability of the Class IV pumps is 0.91, the reliability of the Class III power supply is 0.99 and the reliability of the Class IV power supply is 0.97, what is the reliability of the system in Exercise 3?

5. The system shown below requires two out of the three channels to operate for the system to operate. Fill in the chart to show the eight different combinations of channel success or failure and for each indicate whether the system as a whole will operate successfully. The first one is done for you.



Channel G	Channel H	Channel J	Overall System
✓	✓	X	✓

Key: ✓ = operates successfully, X = fails

DESIGN PRINCIPLES WHICH IMPROVE RELIABILITY

Many of the considerations that go into making a reliable system or station involve the physical layout of the equipment itself. These aspects of reliability are designed into the station. The design principles described below ensure a high degree of reliability for essential systems. Although you are not likely to "un-design" these systems during the operation and maintenance of the station, there are many times that an Engineering Change Notice (ECN) will be initiated which requires changes to the design of systems. These ECN's may require your input and/or

review. It is for these reasons that it is important for people like yourselves who are working in Operations to understand why the systems are designed the way they are.

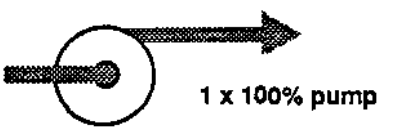
Redundancy

If we have a system where there is only one pump which must be working for the system to work and we wanted the system to work 99.9% of the time, there would be a lot riding on that pump working. If it fails or needs to be repaired, the entire system would be out of service. This problem can be eliminated if there were two or more pumps which were capable of the job. This redundancy generally gives the system greater reliability.

Mathematically we can compare the reliability of a system with one 100% capacity pump versus one that has two 100% capacity pumps in parallel.

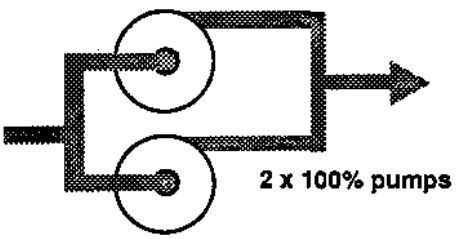
Assuming a pump reliability of 0.95,

Scenario 1 - Single Pump



$$Rs = 0.95$$

Scenario 2 - Redundant Pumps



$$Rs = 0.95 + 0.95 - (0.95) \times (0.95)$$
$$= 0.9975$$

So you can see the difference one redundant component makes. Many of our essential systems have even greater redundancy. For example, there are two identical digital control computers (DCC's) which run concurrently to monitor and regulate the reactor. If either one should fail, the other takes over and continues to run the reactor.

EXERCISES

6. How does redundancy help make a system more reliable?

_____

_____

_____

_____

_____

_____

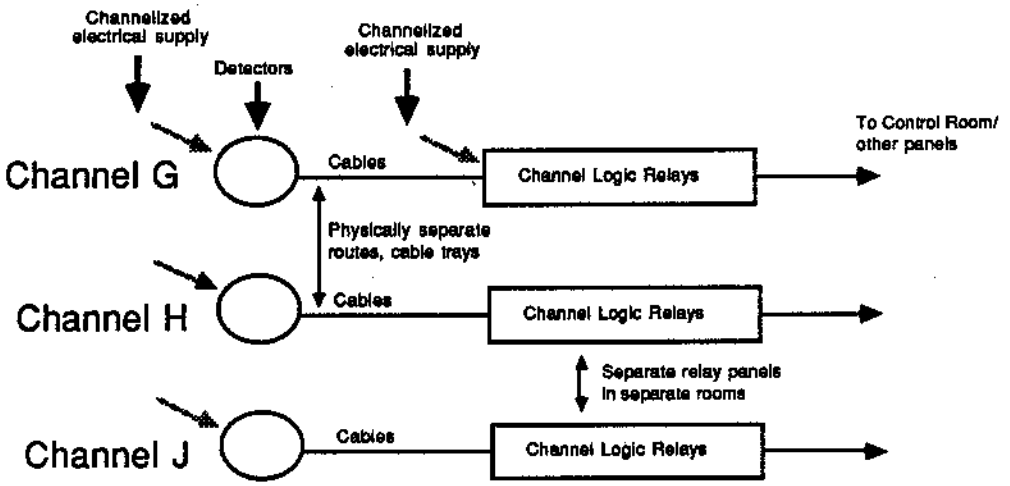
_____

Independence

So far, in our consideration of failures, we have looked at individual failures such as a pump quitting or a valve not working or a shutoff rod sticking. But what about failures such as a fire which affects a lot of instrumentation lines or a steam line break where the escaping steam causes widespread electrical faults or flooding which shorts out all those redundant pumps we've been talking about? These failures are referred to as *common cause failures*, where a single failure can cause other failures which share a common location or connection.

Independence is the separation of systems or parts to minimize the occurrence of common cause failures so that if one system doesn't work, it doesn't incapacitate the redundant system. In other words, it is a method of ensuring redundancy is maintained. This can be achieved in a number of ways.

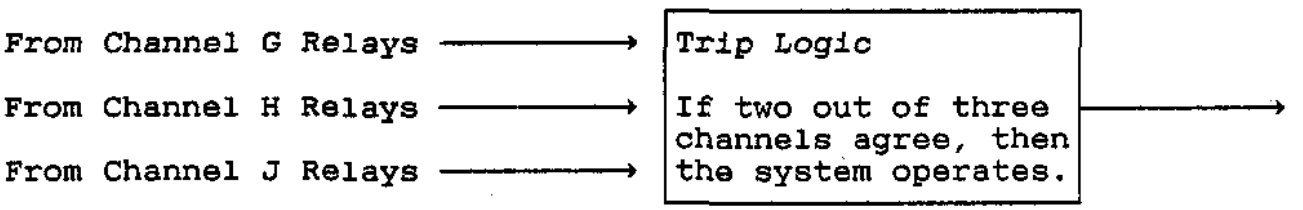
All critical systems, such as those which are required to shutdown the reactor in case of an emergency, have redundant monitoring, controlling and annunciating equipment. **Channelization** involves running the separate instrumentation, wiring, piping, etc., so that a failure on one channel does not affect the other channels. This means physically separate pathways through the station so that the signals for each channel go between the field and the Control Room via a different route.



Independent Redundant Channels

Channelization provides two other features besides that of improved reliability. They involve the fourth and fifth NGD objectives, namely Reliability of Electrical Supply and Product Cost. To meet these objectives, it is necessary to avoid shutting down the reactor when it doesn't need to be, for example, a faulty instrument reading, or testing a reactor trip circuit. If this were to happen, it would mean that Ontario Hydro would have to generate electricity by some other method. Since it is usually by burning coal and since fuel costs for coal fired stations are higher than that of nuclear stations, this means an overall increase in the cost of electricity. As you can see, while we want to ensure that we can reliably shutdown the reactor in the event of an emergency, it is also important that we avoid unnecessarily shutting down the reactor.

Channelization usually involves three channels labelled and colour coded (where practical) uniquely. Operation of a triplicated system requires the operation of two out of the three channels, hence the term *two out of three logic* which refers to the instrumentation logic for this setup. At Darlington and Pickering, some systems are quadrupled and use three out of four logic.



Two Out of Three Logic

By having three separate sets of equipment and requiring two of them to operate before the system operates, it means that if there was a malfunction in one of the channels, it would not activate the system (this is called a spurious trip). The Instrumentation and Control course will go into detail discussing the logic associated with this set up.

The third feature of channelization concerns being able to test systems. The systems which are channelized are, for the most part, systems which normally remain poised, i.e., ready to operate in the event of an emergency (usually to shutdown the reactor, keep the fuel cooled and contain any releases of radiation). So, how are we going to know if they work?

Looking at another example, if an ambulance or fire truck normally sits ready to go when needed, how would you assure yourself that they in fact, are going to work? Right, we test them. But surely we don't want to activate the system and shutdown the reactor every time we test it. We can make use of the two out of three logic to allow us to test one channel at a time without activating the system.

Another designed-in safety feature is that of **Odd and Even** designation. One of the biggest potential common failures is that of the loss of an electrical supply. This would mean that all the equipment that receives its power from that supply would be lost. To address this, there are many redundant electrical supplies which are designated as ODD or EVEN. Redundant equipment receives power from either an odd supply or an even one usually depending on its own nomenclature. Pump 1, Valve 3 or any other component with an odd numbered designation would usually receive power from an ODD supply. Likewise, Shutoff Rod 4 and Inverter 2 usually receive power from an EVEN power supply. The designation carries

on to the actual components themselves so that a pump which receives power from an ODD electrical supply is referred to as an ODD pump. For example, if we have two 100% pumps (that is two "redundant" pumps), generally one will be fed from the ODD supply and one from the EVEN supply.

To provide defence against common mode failures, such as fires, flooding, etc., the plant systems are separated into two groups, **Group One and Group Two.** According to the Pickering B Safety Report,

"Each group provides the following capabilities:

1. Ability to shutdown the reactor.

2. Ability to maintain the shutdown status.

3. Ability to remove decay heat and thus prevent subsequent process failures.

4. Ability to remove decay heat and thus prevent subsequent process failures.

5. Ability to monitor the status of the nuclear steam supply system."

This separation means that a large scale failure in one group does not cause a failure in the other group. At Pickering B and Darlington, the Group Two systems are seismically qualified (to ensure their operation in the event of an earthquake) and have their own seismically qualified water and power supplies. The Group Two systems also can be operated from a remote location (Unit Emergency Control Centres or Secondary Control Areas) should the Main Control Room become uninhabitable, say, due to a fire.

Examples of Group One and Two Systems

Group One	Group Two
Reactor Regulating System (RRS)	Shutdown System Two
Channels A,B,C	*Channels G,H,J*
Shutdown System One	These systems are seismically qualified at the later stations, with separate water and power supplies and controls
Channels D,E,F	
ECI	Containment

Each channels has its own separate cables, routes, instruments, etc.

Diversity/Functional Independence

To further improve the reliability of critical systems, redundant functions are accomplished using functionally different system designs. At the Bruce Nuclear Generating Stations, Shutdown System One (SDS1) uses gravity to insert shutoff rods into the reactor whereas Shutdown System Two (SDS2) uses a difference in pressure to inject a neutron absorbing substance into the reactor. Therefore, if for some reason the shutoff rods could not enter the core (due to damage to the reactivity deck for example), forces due to differences in pressure would still cause the reactor to shutdown. SDS1 is oriented vertically from above the reactor and SDS2 is horizontally located on the north side of the reactor. The detectors for the two different systems are made by different manufacturers to avoid any potential generic design problems.

All these differences serve to ensure that the two systems are indeed redundant and that no single failure can cause both systems to fail.

Fail Safe

Many components are operated remotely. Two examples of this are valves which are controlled by instrument air and reactor shutoff rods which are suspended above the reactor by electromagnetic clutches. If the controlling power or air to these devices is lost, we still want them to operate. There will be failures of control power from time to time but when that happens fail safe

devices will fail in such a way as to minimize the consequences. Valves that supply cooling water fail open thereby ensuring a heat sink for the process systems. On the other hand, if power is lost to the shutoff rods, they will drop into the reactor and shut it down. Again, the details of fail safe logic are discussed in the Instrumentation and Control course. Note, however, that not all components can be designed to be fail safe.

EXERCISE

7. How can you make a reliable system out of less than 100% reliable parts?

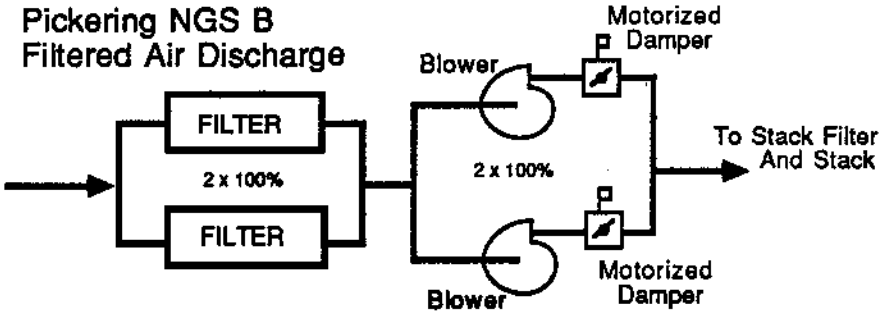
SUMMARY

In this module, the following topics have been discussed:

- The basic probability rules
  - AND (symbol, $\cap$), $P(A \cap B) = P(A)\ P(B)$
  - OR (symbol, $\cup$), $P(A \cup B) = P(A) + P(B) - P(A \cap B)$
- Redundancy involves having two or more components each capable of performing the intended function, connected in parallel.
- Independence is the separation of systems or parts of systems so that a single fault will not disable components which are meant to be redundant.
  - Channelization - separate detectors, wiring and alarm units are provided so that failure on any one channel does not impair the other channels.
  - Two out of three logic requires that two channels of a triplicated system operate for the system to operate. This allows testing of a single channel without operating the system and reduces the chance of a malfunction causing a spurious operation of the system.
  - Odd/Even is a system which ensures redundant components are fed from independent power supplies.
  - Group 1/Group 2 separation ensures that each group of systems has the capability to shutdown the reactor, keep the fuel cool and contain radiation in the event of a larger scale failure which affects a number of systems.
  - Diversity/Functional Independence is achieved by designing systems so that they function differently and use different kinds of equipment to avoid any coincident failure due to a generic design.

ASSIGNMENT

1) **Calculate the reliability of the following system:**



2) Briefly describe the following design concepts and state how they apply to reliability.

a) Redundancy

b) Independence

c) Group 1 and Group 2 Systems

This Module Prepared By: Richard Yun, WNTC

PI 21.03

PROCESS SYSTEMS

OBJECTIVES

3.1 Define and give examples of a process system in an NGS.

3.2 Define [or illustrate using a diagram for a) to c)], as related to the lifetime of a device:

a) Infant mortality/burn in period
b) Useful life
c) Wear out region
d) Mean time to failure

3.3 State and graphically illustrate the General Reliability Function.

3.4 Define and give an example of a Type A process system failure.

COURSE NOTES

Nuclear Plant systems can be classified into two major categories - Process Systems, which we will be discussing in this module and Safety Systems, which are those systems which are usually in a standby mode ready to act in the event of an emergency.

Process Systems

Process systems are active in the normal functioning of the plant, i.e., all the systems involved in the "process" of converting fission heat to electrical energy. Some examples are:

The Heat Transport System
Steam and Feedwater Systems
Turbine Lube Oil System
Heat Transport Pressure Control System
Reactor Regulating System

As an analogy, if you were driving down the road in your car, the systems associated with keeping the car running would all be process systems. These would include, the fuel pump, the distributor, the steering mechanism and the drive shaft. Systems that wouldn't be process systems would be things like the hand brake and the horn.

Since process systems are normally active, that is to say operating, it is relatively easy to determine that they have failed. If the Heat Transport pump motors decided to stop or the steering mechanism in your car failed, it would be quite noticeable. In this module, we will be looking at the reliability of process systems because as you can see if the process systems work well, there is less dependence on the Safety Systems.

EXERCISES

1. Give three examples of Process Systems.

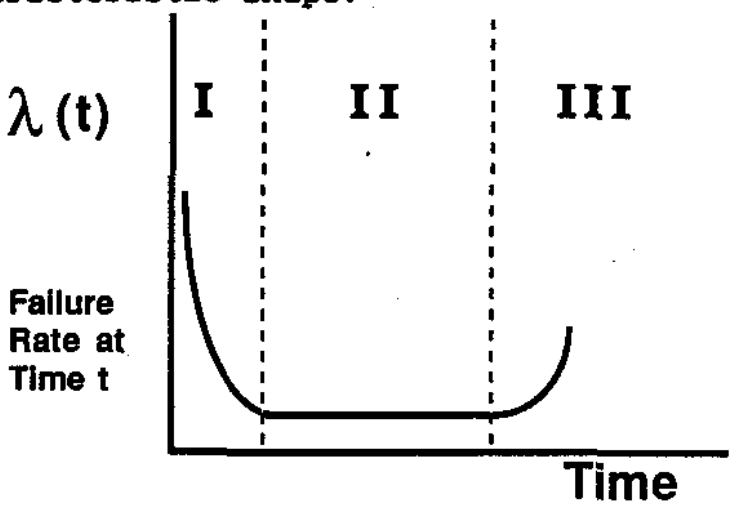
   a) _____

   b) _____

   c) _____

Variation of Equipment Failure Rate With Time

The **Failure Rate** (λ), as applied to process equipment, is defined as the number of failures per unit time (e.g., 5 failures per year). Failure rate normally varies with time in service in a typical manner as shown in the **Bathtub Curve** which is shown below. Its name comes from its characteristic shape.



The curve is divided into three regions which are as follows:

I - **Burn In or Infant Mortality Period**

Failures due to manufacturing defects are most common early in equipment service life resulting in an initially high failure which decreases as time in service increases. You probably recognize this phenomenon as the "Getting the bugs worked out" part of the life cycle of a new car. It's always a good idea to ensure your warranty covers this stage.

II - **Useful Life Period**

After the manufacturing defects stage, the failure rate drops to it's minimum level and remains fairly constant. The failures that do occur during this stage are random in nature. If possible, we would like to operate all our equipment during this portion of it's service life. The failure rate is low and being constant makes it easier to predict failures.

III - **Wear Out Period**

As the component gets older, parts wear out and the failure rate goes up.

From this discussion, you can see that it would be advantageous if we could always operate during the useful life phase. This brings us to the golden rule of reliability which states:

> *Replace components as they fail within their useful lives and replace components preventatively, even if they haven't failed, no later than by the end of their useful lives.*

For an individual component, this means that we test it to detect any manufacturing defects prior to putting it into service. If it fails we replace it and as we approach the wear out region where we know the failure rate will increase, we should replace it. (Note that when we say replace, it may mean that we just replace those parts which fail or have worn out. It is not necessary to replace an entire piece of equipment simply because one part has failed or is worn out.) This philosophy manifests itself in our preventative maintenance programs. For example, during a turbine outage, many components are checked and replaced even if they haven't failed yet, simply because it is detrimental to station reliability to leave components in service which are approaching or are in the wear out period of their service life.

EXERCISES

2. In certain locations where the fluorescent light fixtures are located high off the ground and are rather inaccessible, there are programs in place that require someone to change the fluorescent tubes on a regular basis. This is done whether or not the tube has actually burnt out. Why is such a program in place?

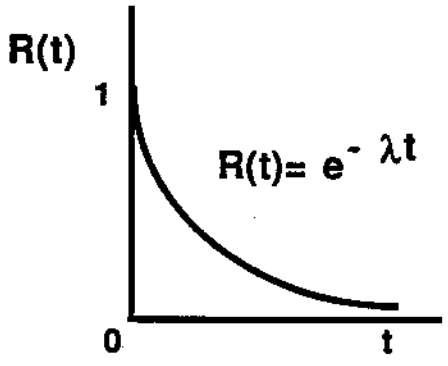
While the bathtub curve shows failure rate with respect to time, the reliability of the component (that is, the probability of it surviving to time t) is given by the general reliability function which is:

For operation in the useful life region, where the failure rate is constant,

$$R(t) = e^{-\int_{\cdot}^{t} \lambda(t)\,dt}$$

the equation simplifies to:

$$R(t) = e^{-\lambda \int_{\cdot}^{t} dt}$$
$$= e^{-\lambda t}$$



This function describes the reliability of a component for a mission time, t, after it is put into service. So, although up to now we have used examples where the numerical value of the reliability is given, in actual fact it is calculated from historical data. This data is usually in the form of an expression call Mean Time to Failure (MTTF)*.

* MTTF is often confused with MTBF (Mean Time Between Failures). When something is repairable, the time between failures is the time to failure plus the time to repair (i.e., MTTF = MTBF + MTTR). If the repair time is small when compared to the time to failure, then the MTTF is approximately equal to the MTBF.

The definition of MTTF is given as: The average time a component would operate under useful life conditions, before failing. The units are in time per failure. To convert this to something we can use, take the reciprocal which gives us failure per time which as you know is the failure rate.

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

Given a MTTF, you can now calculate a failure rate. If you know how long the equipment has been in service, you can then calculate the reliability using the equation given.

Note that the MTTF is defined for operation in the useful life period of the bathtub curve where the failure rate is constant. There is no mathematical relationship between the length of the useful life period and the MTTF. In practical terms, this means that if you see a manufacturer's claim that its product has a MTTF of 10,000 hours, it doesn't mean that it will have a long useful life. All it tells you is that during the useful life period, the failure rate is low. The following bathtub curves show how it is possible to have a long useful life with a short MTTF and vice versa.

The curve on the left illustrates a short useful life but a long MTTF (since the failure rate during the useful life region is small, the reciprocal, which is the MTTF, is large). On the right, we have the opposite scenario where there is a long useful life but a short MTTF.

Some examples which may help in understanding this idea are people and tires. First the people - for a human in the prime of life, the failure rate may be in the order of 10^{-3}, corresponding to a MTTF of 1000 years. This would mean that people would live an average of 1000 years if they could "operate" continuously under "useful life" conditions. In reality, of course, an individual enters the "wear out region" long before the 1000 years are up and failure then is due to aging rather than random statistical failure (accidents, disease, etc.) characteristic of prime life operation.

Now the tires - for your average car tires, the useful life failure rate might be in the order of 2.5×10^{-6} per km, corresponding to a MTTF of 400,000 km. In reality, of course, the tire goes bald due to wear rather than due to the random statistical failures such as puncture and overheating.

As for people with spare tires around their middles, we don't have much data yet, but we're working on it.

EXAMPLE ONE

A component has an MTTF equal to 10,000 hours and a useful life of 1,000 hours. Find the reliability for a 10 hour mission time.

Solution

The equation for reliability is:

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

λ can be found from MTTF,

$$\lambda = \frac{1}{10,000} = 1 \times 10^{-4} \ h^{-1}$$

So for a mission time of 10 hours,

$$R(10) = e^{-(1 \times 10^{-4})(10)}$$

$$= e^{-1 \times 10^{-3}}$$

$$= 0.9990$$

Process System Faults

In this module we've been discussing process system failures. Although most people think of safety systems when talking about reliability and public safety, environmental protection, worker safety, etc., it is important to note that, if we have very reliable process systems, then our safety systems don't need to operate as often. A rupture of the Primary Heat Transport System, which is a process system, can result in loss of cooling to the fuel and do a lot of damage if the safety systems aren't working. So you can see that a Process System fault can be very important.

To make it easier to document and analyze these faults, it is necessary to categorize them as to their severity - specifically in terms of how they affect fuel temperature. Since 99% of the radioactive fission products formed in our reactors is trapped inside the ceramic fuel pellet, it is of paramount importance that the fuel does not overheat

and allow fission products to escape. The categories of process system failures are named from Type A, being the most serious, to Type E, the least serious, and are fully defined in station technical reports. The following definition of a Type A Process system fault is taken from the Bruce B Technical reports and is the same as that used at other nuclear stations.

"A Type A fault is one that raised fuel temperature and significant fuel failures would have occurred in the absence of action on the part of a safety system. The term "serious process failure" is synonymous with a Type A fault."

SUMMARY

In this module, the following topics have been discussed:

- Process Systems are those systems which are directly involved in the "process" of converting fission heat to electricity. Refer back to the notes for examples of these.
- The "bathtub" curve is a graphical illustration of how failure rate varies with time.
  - During Stage One (burn in period) of the curve, the failure rate is high but decreases with time. These failures are due to manufacturing defects.
  - During Stage Two (useful life period), the failure rate is low and constant. These failures are due to random failures.
  - During Stage Three (wear out period), the failure rate begins to increase again. These failures are due to wearing out of the component or fatigue.
- Mean Time To Failure is a common expression which arithmetically is equal to the reciprocal of the failure rate during the useful life period of a component's lifetime.
- The General Reliability Function simplifies to the form:

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

  where R(t) gives the reliability of a component with a failure rate of λ for a mission time, t.

- Process system faults may be categorized depending on the severity of the resultant accident had there been no safety systems available. Type A failures are the most severe, in which significant fuel failures are possible.

ASSIGNMENT

1) Draw the "bathtub" curve and label each of the three stages.

2) For each stage labeled above, state the typical causes of failures in that region.

3) Define the term "Mean Time To Failure".

4) A Type A process failure is one which:

a) Results in a rise in fuel temperature but no significant fuel failures

b) Would have raised fuel temperature and caused significant fuel failures if special safety systems were not available

c) Causes the unit to shutdown and remain out of service for greater than 40 hours

d) Results in a release of radioactivity to the environment

e) Would have resulted in injury or death to the public

This Module Prepared By: Richard Yun, WNTC

PI 21.04

AVAILABILITY OF SAFETY SYSTEMS

OBJECTIVES

4.1 Define and give an example of the following terms:

a) A Safety Related System
b) A Poised System
c) A Standby Safety Support System
d) A Special Safety System
e) An Active System

4.2 a) Describe in words, or mathematically, the relationship among failure rate, test interval and unavailability.

b) Explain how the availability of a passive system can be increased without any physical changes to the system.

4.3 Calculate the unavailability of a tested component.

4.4 a) List and explain four reasons for testing safety systems.

b) List and explain four reasons for limiting testing of safety systems.

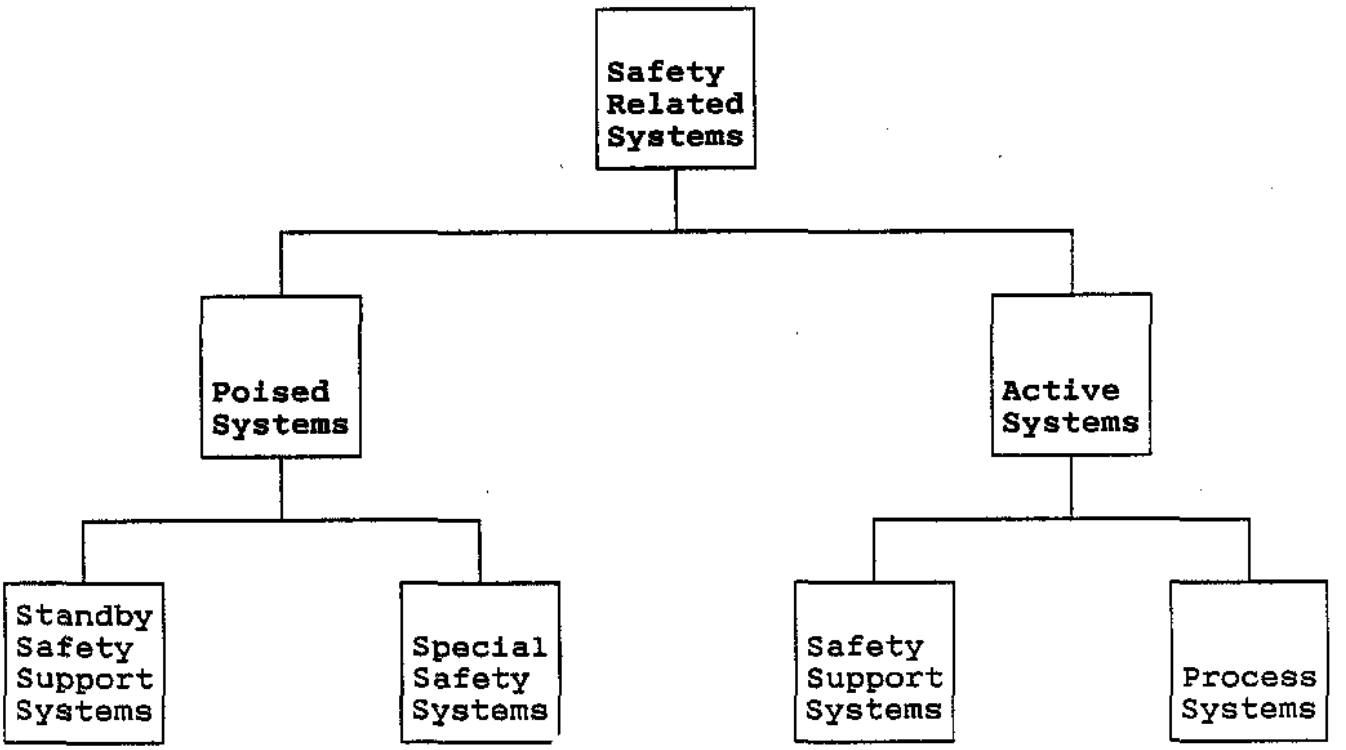
4.5 Calculate the probability of single and dual failures involving process and safety systems.

4.6 Describe and give an example of a Level I impairment of a Safety System.

COURSE NOTES

In this module, we will be looking at the reliability of Safety Systems, so it is important to take a few minutes up front to go over some of the terminology used when describing them. There are many definitions of the various classifications of systems but the ones given here are those generally used in station technical reports.

For the purpose of assessing failures which could lead to the escape of radioactivity, station systems which provide a safety function are classified as **Safety Related Systems.** They are then subdivided into the classifications shown on the next page.



Safety Related Systems

Those systems which are intended to:

a) Control

Regulate the reactor under all normal plant and anticipated transient conditions and to maintain the reactor core in a safe state for an extended period.

b) Cool

Cool the reactor core under all normal plant and anticipated transient conditions and to maintain the reactor core cooling for an extended shutdown period under such conditions.

c) Contain

Limit the release of radioactive materials to meet the criteria established by the licensing authority, with respect to radiation exposure.

Poised Systems

The term poised is applied to those systems which usually play no part in the normal production process but remain available, ready to operate to minimize the consequences of a process system failure. All special safety systems and standby safety support systems are classified as poised.

Component failures on poised systems tend not to be revealed immediately and routine testing is the principal method of fault detection.

Examples of poised systems are Emergency Power System, the dousing water system and the auxiliary boiler feed system.

Standby Safety Support Systems

A standby safety support system is a poised system which will prevent the occurrence, or mitigate the consequences, of a serious process failure. However, it may perform other normal operating functions in addition to its safety support role.

Examples of standby safety systems are Instrument Air System, service water, Emergency Power System and emergency air.

Special Safety Systems

A system designed specifically to prevent significant releases of radioactivity to the public in the event of a serious process failure. There are three types of special safety systems.

a) Shutdown Systems
b) Emergency Coolant Injection Systems
c) Containment Systems

A Special Safety System has no purpose other than to Control the reactor, Cool the fuel and Contain any releases of radioactive material. It is not used in day-to-day operation and usually has its own detectors, trip logic and equipment so that it is independent of any failures of normal process systems.

Active Systems

A term applied to those safety-related systems which are an integral part of the normal production process. Component failure on active systems tends to be revealed immediately. The impact of the failure is usually immediately obvious and the Operator can initiate prompt corrective action.

Active safety-related systems are broken down into two groups, Safety Support Systems and Process Systems.

Safety Support Systems

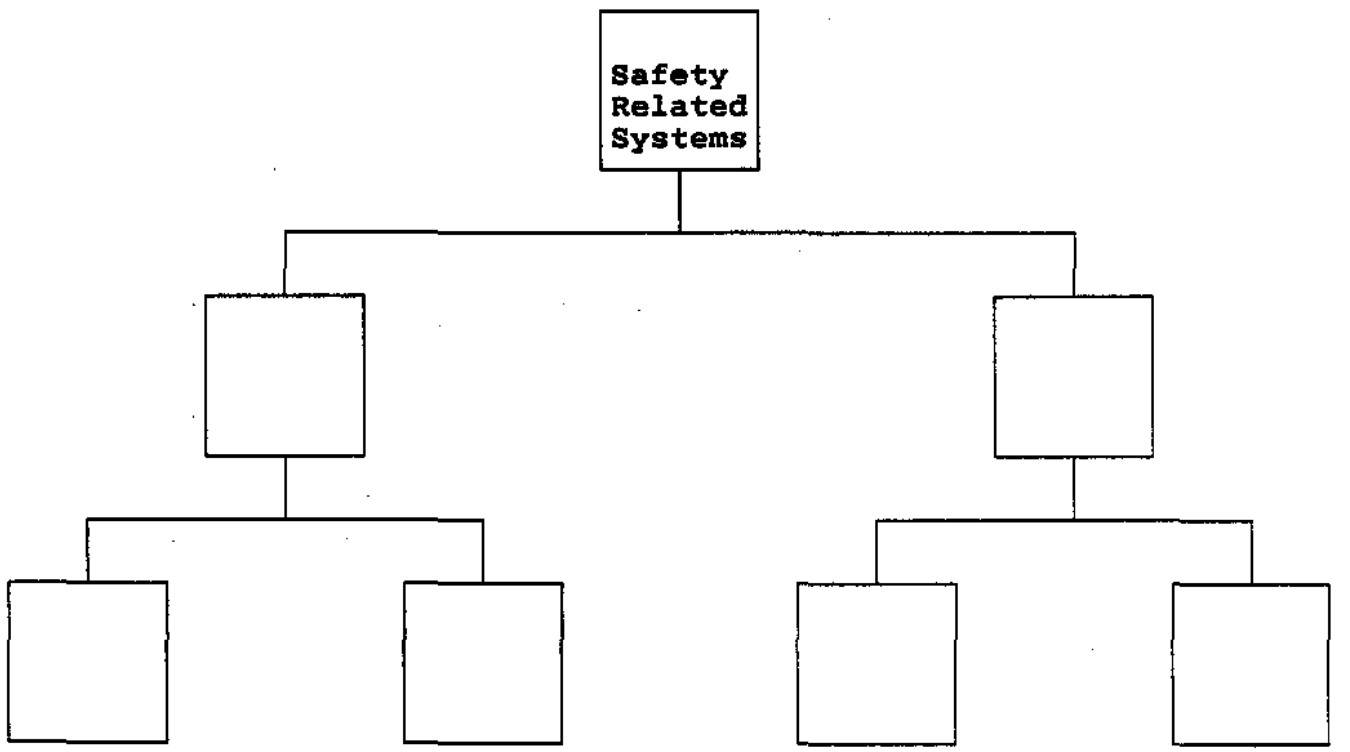
These are those systems which are active and support or are a part of the Special Safety systems described earlier. Examples of this type of system are the Low Pressure Service Water System (which provides cooling water to many heat exchangers) and the Instrument Air System (which is used to open and close valves).

Process Systems

In Module 3, we looked at process systems as those systems which are involved in the "process" of the conversion of fission heat to electricity. Some of these systems, although normally active and used in normal operation also can play a safety-related role in the event of an accident. This can be by acting as a heat sink (service water for example) or a heat transfer medium (primary heat transport coolant) or by providing control to instruments and equipment (Class II electrical power, instrument air).

EXERCISE

1. **Fill in the following diagram showing the subdivisions of safety related systems:**



Unavailability

As you with great memories no doubt recall, in Module 1 we gave a definition of Availability. For those whose memories are good but just short, we'll review it here. The availability of a component is that fraction of time that it is able to perform its intended purpose. It then follows that unavailability (Q) is that fraction of time that a component is not able to perform its intended purpose. This is equal to the probability that a component is unavailable at any randomly chosen instant.

So how do we find out the fraction of time that a component is unavailable? Well, it's definitely unavailable when it's broken and while it's being fixed, so we get: Q = [number of times it is broken] x [how long it is unavailable each time it is broken]. For systems which are active, it is easy to determine these figures because when something fails, you know about it right away. For systems which are poised, the only way we can find out about failures in some components is by testing.

Now suppose that we've been testing something once a week and the last time we checked, it was working fine. However, this week when we test it, we find that it has failed. How long has it been unavailable? It could be anything from the entire time since the last test to just a few moments before we tested it this week. For our calculations we take the average and assume that it has been in a failed mode for one half of the time since the last test. This then gives us the equation for the calculation of unavailability of tested components or systems:

$$Q = \lambda\left(\frac{T}{2} + r\right)$$

Where T is the test interval or time between tests in years
r is the repair time in years
λ is the failure rate in failures per component year

If the repair time is small compared to the test interval, we can simplify the equation to:

$$Q = \lambda\left(\frac{T}{2}\right)$$

The following examples illustrate how this is used.

EXAMPLE ONE

For a component which is tested weekly, it was discovered that there were 5 failures in the last 7 years of operation. What was the unavailability of the component during this time?

Solution

Using the equation, we have a test interval of one week or 1/52 years, a failure rate of 5/7 failures per year. If we assume that the repair time is negligible, then the unavailability is:

$$Q = 5 \frac{\text{failures}}{7 \text{ years}} \times \left(\frac{\frac{1}{52} \text{ years}}{2}\right)$$

$$= 7.0 \times 10^{-3} \text{ years/year}$$

EXAMPLE TWO

Calculate the unavailability of the protective system of a reactor if 22 failures have been detected during 4 years of operation. Failures are detected and corrected at the beginning of each 12 hour shift.

Solution

$$Q = \lambda \frac{T}{2}$$

$$= \frac{22 \text{ failures}}{4 \text{ years}} \times \frac{\left(\frac{12}{24} \times \frac{1}{365}\right) \text{years}}{2}$$

$$= 4.5 \times 10^{-3} \text{ years/year}$$

NOTE: The units of Unavailability have been expressed as years per year here but can also be and often are, expressed as hours per year, days per year or some other units of time per time.

For the Special Safety Systems, the target unavailability is 10^{-3} years per year or about 8 hours per year.

EXERCISES

2. Why are poised safety-related systems tested?

3. In 12 years of operation of 30 pressure detection instrument lines in the containment system, 5 failures were detected. The instrumentation is tested semi-annually. What is the unavailability of a pressure detection line?

Looking at the equation for calculating unavailability, a little algebraic examination will tell you that the unavailability of a component or system can be altered by merely changing the test frequency.

$$Q = \lambda\left(\frac{T}{2}\right)$$

Although this may seem like lying with statistics, it actually is quite legitimate. If you test something more often, you have a better idea of whether or not it is working. Taken to the extreme, if we keep the component in operation continuously, you can be sure that it is always available. In fact, we do this with the standby generators when we want to ensure that we have backup power available in situations where some of the units in a station are shutdown or otherwise unable to supply backup power to a unit that is running.

Testing of Safety Systems

So, you can see from the above discussions that it is important to test safety systems. Specifically there are a number of reasons that this should be done. These are:

1) To discover failed components so that they can be repaired or replaced.

2) To maintain system unavailability below a specified maximum value (proactive). In other words, reduce the time that the system is unavailable.

3) To check whether or not unavailability targets are being met (reactive), so that corrective action such as upgrading the system and/or more frequent testing can be taken if the targets are not met. This also satisfies the conditions of the AECB operating license.

4) To build up a data bank of component failure rates for use by designers in either modifying existing systems or designing future systems.

However, in spite of all these reasons for testing safety systems, there are a few good reasons for limiting the frequency of testing.

1) Excessive testing can cause excessive wear on the system or components.

2) The testing process itself can contribute to system unavailability. Some tests involve removing the component from service which means that for the duration of the test, it is unavailable.

3) The more human intervention, the greater the risk of inadvertently leaving the system in a downgraded state.

4) If the systems are tested too often, it can increase the risk of unplanned outages. If during a test, human error or random failures results in shutting down the reactor when it doesn't need to be shut down, there is an economic penalty.

Combinations of Failures

Up to now, we have been looking at failures of Process Systems in Module 3 and Safety Systems in this module. Back in Module 2, we looked at the probability of combinations of events, which are applicable in situations where we are interested in the probability of one thing happening AND/OR another thing happening. In the discussion of unavailability, we often need to consider those combinations of events. For example "what is the probability of the Reactor Regulating System failing and the Shutdown Systems being unavailable?" "What is the probability of a Shutdown System and the Containment System being unavailable at the same time?" The answer to these and other questions are usually calculated using some of the same techniques that you have used up to now.

There's really nothing too difficult about these calculations. In most cases, it is simply the AND relationship which means that we multiply the probabilities together. So, if we want the probability that the Regulating System will fail **AND** the Shutdown System will be unavailable, we simply multiply the failure rate of the Regulating System by the Unavailability of the Shutdown System. This type of failure is referred to as a Dual failure where a Process System fails along with the Safety System required to act in that event. The following example will illustrate how these are done. Warning: Do not attempt to do this at home. These examples have been done by trained professionals (and after this, you'll be trained professionals)!

EXAMPLE THREE

Assume that the Reactor Regulating System for a large nuclear unit has failed 3 times in 7 years of operation. The shutdown system, which is tested once per shift, has had 16 failures in the same 7 years. These failures were detected and corrected very quickly at the beginning of each 12 hour shift. What is the probability of the regulating system failing at the same time that the shutdown system is unavailable?

Solution

Probability of Dual Failure = Probability of Regulating System Failure **AND** Shutdown System being unavailable

$$= \lambda_{Reg} \times Q_{Shutdown}$$

$$= \lambda_{Reg} \times (\lambda_{Reg} \times \frac{T}{2})$$

$$= \frac{3 \text{ failures}}{7 \text{ years}} \times (\frac{16 \text{ failures}}{7 \text{ years}} \times \frac{(\frac{12}{24} \times \frac{1}{365})}{2})$$

$$= 6.7 \times 10^{-4} \text{ failures/year}$$

Safety System Impairments

At times, it is possible for safety systems to be impaired (no, this doesn't mean that someone put alcohol in the poison injection tanks). It means that the system cannot perform its function totally as intended. The seriousness of this is classified according to Impairment Levels which provide Operator action guidelines and objectives for a variety of safety system faults. The levels range from the most serious, Level 0, to the least serious, Level 3.

Level 0: The system is totally incapacitated such that it would not have provided any protection under any circumstances.

Level 1: The system effectiveness is significantly reduced such that it would have been of little or no benefit if any possible process system failure had occurred which required that system. The system is not effective in keeping releases below allowable limits for either the worst case or lesser events.

Level 2: The system effectiveness is marginally reduced to below the design intent. The system is effective for keeping releases below allowable limits for lesser events but not the worst case.

Level 3: There is a reduction in system redundancy or margin of safety (however, design intent can still be fulfilled).

SUMMARY

In this module, we have discussed:

- Definitions and examples of:
  - A Poised System
  - An Active System
  - A Safety Related System
  - A Special Safety System
  - A Standby Safety System
- The relationship among failure rate, test interval and unavailability.
- Calculations of unavailability.
- Reasons for testing Safety Systems and reasons for limiting the amount of testing.
- Calculations of dual and triple failures.
- Impairments of Safety Systems.
- Significant Events as they pertain to an NGS.

ASSIGNMENT

1) For the following examples of systems, identify whether they are:

A - An Active Safety Related System
B - A Special Safety System, or
C - A Standby Safety Support System

_____ i) Shutdown System One

_____ ii) The Reactor Regulating System which is used during normal operation

_____ iii) Emergency Boiler Cooling

_____ iv) Containment System

_____ v) Emergency Water System

_____ vi) Standby Generators

2) How is the unavailability of a tested component determined?

3) Give four reasons for testing Safety Systems.

i)

ii)

iii)

iv) _____

4) Give four reasons for limiting the testing of Safety Systems.

i) _____

ii) _____

iii) _____

iv) _____

5) In five years of operation, there were two faults on the Reactor Regulating System which would have allowed the reactor power to increase uncontrolled if the Shutdown Systems were not available. During this same time, the Shutdown System was tested daily and two faults were discovered. In all cases, the failures were repaired in a very short time. Based on this data, what is the probability of the regulating system failing at the same time that the Shutdown System is unavailable?

This Module Prepared By: Richard Yun, WNTC

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.

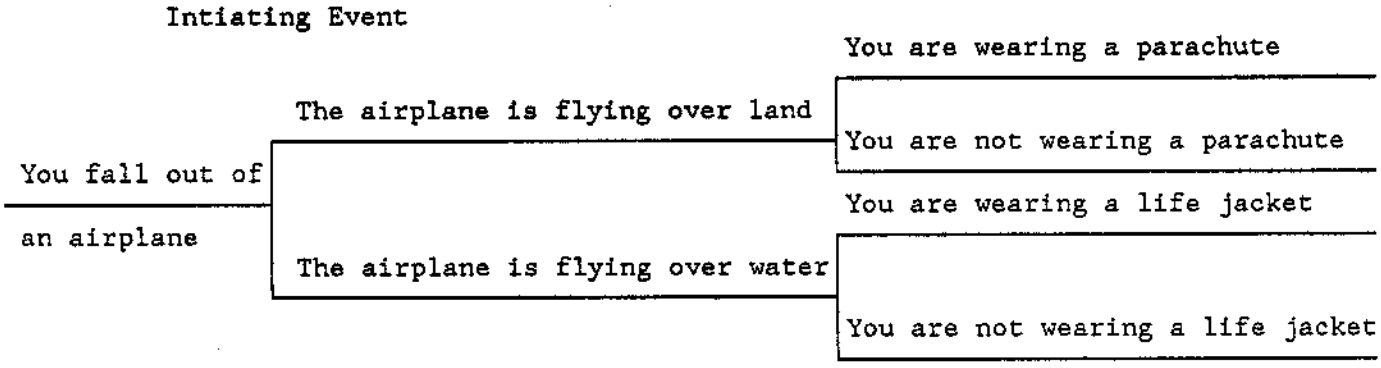
will prepare one during the design stage but it is often not specific enough or readily available to the System Engineers in operations. So they prepare their own models for whatever projects they are working on. Work is now underway so that there will be one reliability model prepared that can be used 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.

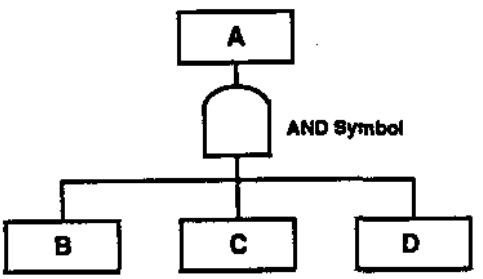
One of the most serious accidents which can occur at a nuclear generating station is the loss of coolant to the fuel. If this were to occur, there could be fuel failures and damage to the reactor itself. If we look at this accident, a loss of coolant, we can then examine what could cause it. The obvious 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

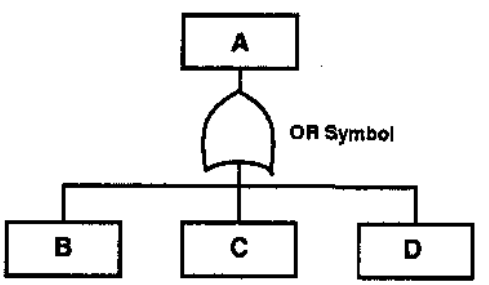
various systems identified in the event tree paths. This graphical display is similar to the reliability block diagrams used in the previous modules and is shown in the figures on the next page.

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.



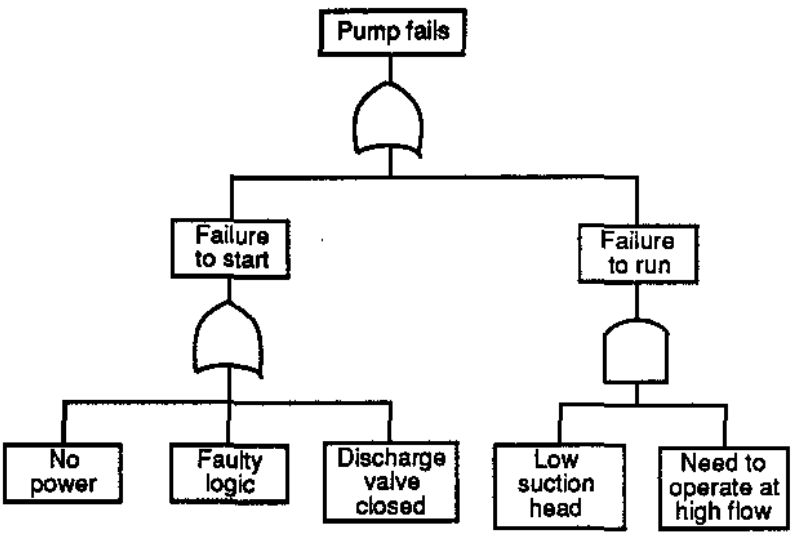
The diagram on the left shows that for event **A** to occur, **B** AND **C** AND **D** all have to occur.



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

PI 21.06

REPORTING AND ADMINISTRATION

OBJECTIVES

6.1 State who generates the following documents and what reliability information is available in them.

a) Station Safety Report
b) Station Quarterly Technical Report
c) NGD-9, CANDU Operating Experience

6.2* Identify the reliability related responsibilities of the following groups:

a) Design Division (Nuclear Studies and Safety, Quality Engineering)
b) Nuclear Operating Standards Department
c) Central Production Services Division
d) Station Reliability Unit

* Currently not required.

COURSE NOTES

In this module, we will be looking at some of the reports that you will come across while working in the Technical Section. These reports document our performance in the reliability areas that we've been discussing. For instance, how well we've kept to the availability targets, the number of significant events that we've had and the overall performance of the units.

We will also be examining the various groups in the corporation who deal with reliability issues. This will help to familiarize you with who does what and how they can be of assistance to your job in the field.

The Siting Guide

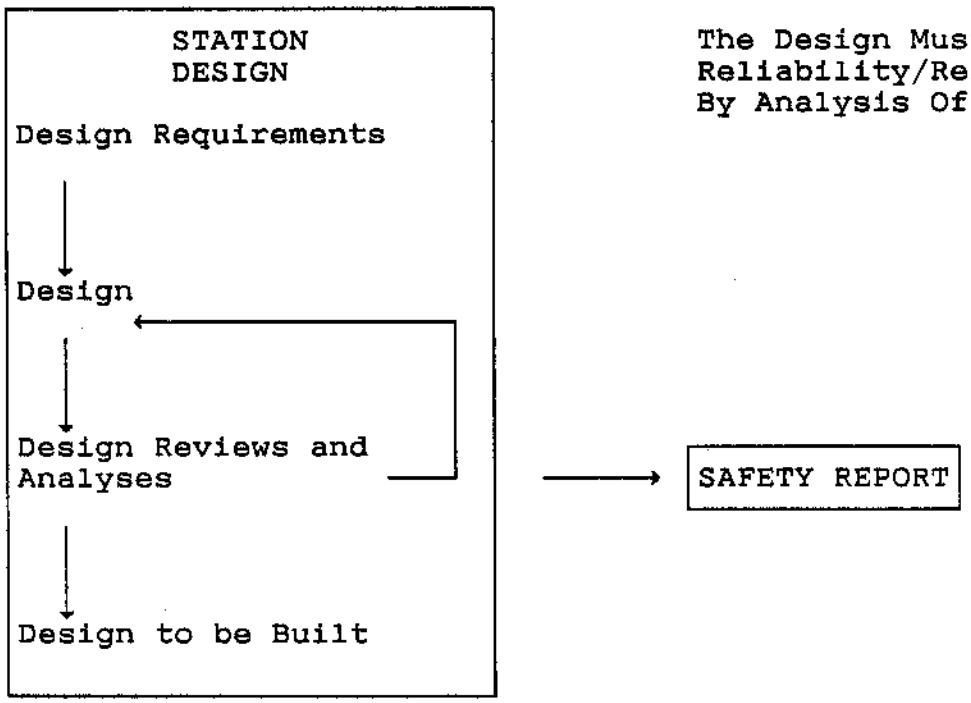
To ensure that the public and environment are kept safe, the Atomic Energy Control Board prepared a set of ground rules that described the radiation dose limits allowable for the general population. These limits then are the specifications that the designers have to ensure are not exceeded in the event of single and dual failures. The Siting Guide originated as a document issued in

STATION LIFE CYCLE	RELIABILITY CONCERNS
SITING GUIDE (AECB)	The Siting Guide Establishes Radioactivity Release Limits And Allowable Frequency

1964 with later revisions until the version which was presented as a paper ("Reactor Licensing and Safety Requirements") at a conference in 1972. This version is the one to which most of our stations have been designed.

Station Safety Report

This document is prepared by the designers of the station and submitted to the Atomic Energy Control Board prior to the construction of the station. It is to assure the AECB, as representatives of the public, that the conditions of the Siting Guide are met. The Safety Report



describes the design features that contribute to the safety of the public, the environment and the employees. In other words, to ensure that the first three main objectives of Ontario Hydro, as outlined in Module 1, are met.

Contents of the Safety Report include:

- Basic Safety Philosophy

- Factors Affecting Releases

- Emission Limits

- Design Criteria for the various systems including the structures, instrumentation, electrical supplies as well as the reactor and associated systems

- Radioactive Waste Management

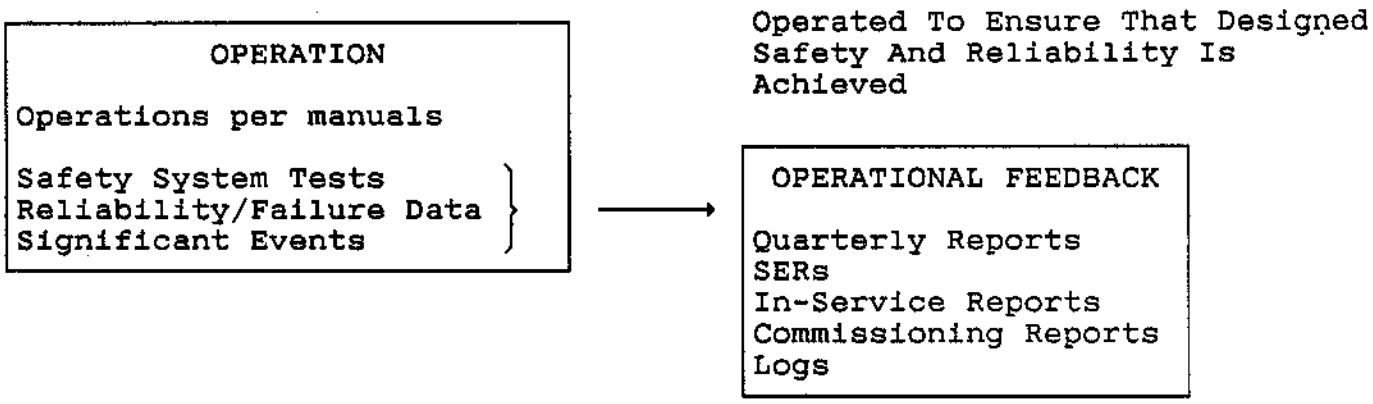
- Radiation Protection

- Safety Assessment/Accident Analysis

Significant Event Reports (SERs)

In the operation of Nuclear Generating Stations, abnormal and unexpected events can occur which cause or have the potential to cause reduced protection for the health and safety of personnel, lost production or a major economic loss. These events are described as Significant Events. Examples include Loss of Regulation, Impairment of Safety Systems, Reactor Trips and accidents of a conventional nature (falls, electrical shocks, etc.).

Because they have important implications and because we don't wish to see them repeated, these events are documented and distributed within NGD. The Significant Event Report describes the background and occurrence of the event as well as comments by the staff as to what went wrong. The report is reviewed by more senior staff and a recommendation is made by the Station Manager as to how to avoid such an event in the future, for example, by changes to the Operating Procedures. A copy of this is sent to the AECB for their information.



Station Quarterly Technical Report

To monitor the performance of our units, technical staff at each station produce monthly and quarterly reports which document any upsets or abnormalities, as well as reliability statistics such as capacity factors, the number of times that a unit was out of service for maintenance, the number of spurious trips and unavailability figures.

Contents of the Quarterly Technical Reports include:

- Station Performance
- Review of Major Systems
- Staff Details

- Radiation Control
- Radiation Emergency Procedures
- Reactor Safety Reliability Assessment
- Summary of Lifetime Fault Data

The section on Reliability reports the actual unavailabilities of the safety systems as they were found in the station. It also records the number and type of any process or safety system faults as well as a summary of any Significant Events.

An appendix provides a glossary of terms used in the report. These terms include some of the ones we've discussed in this course and some others which you will be covering in other courses. These reports are located at their respective stations and centrally in the NGD Records Centre.

NGD-9, CANDU Operating Experience

Once a year, usually in May or June, a division wide report is prepared by the Central Production Services Group located at Head Office and reporting to the Director of the Nuclear Generation Division, which summarizes the performance of all of the nuclear stations in the corporation for the previous year. This report documents how successful we were at meeting our targets in the five major objectives: Employee Safety, Public Safety, Environmental Protection, Reliability of Electrical Supply and Production Cost. There is also a document, NGD-12, which gives the standings of our units in the world ranking. Both these documents are available by contacting the NGD Records Centre.

SUMMARY

In this module, we have looked at:

- The Siting Guide prepared by the AECB which defines the ground rules for the design of nuclear reactors as well as the radiation release limits.
- The Safety Report that is prepared by the designers to ensure that the proposed design meets the requirements set out in the Siting Guide.
- Significant Event Reports document events that have an important impact on the main objectives.
- Station Technical Reports record the actual reliability data.
- NGD-9, CANDU Operating Experience, reports on how well the targets in the five major objective areas have been met.

ASSIGNMENT

1. What reliability information do the following documents contain?

   a) NGD-9, CANDU Operating Experience

   b) Station Technical Reports

This Module Prepared By: Richard Yun, WNTC