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".

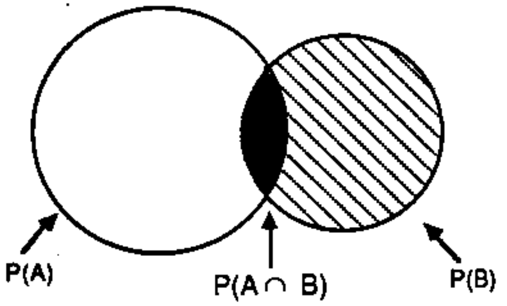
We use the format **P(A)** to represent the probability of **A** happening. So, the probability of a coin coming up heads is P(heads) = 1 in 2 or 0.5. Likewise the probability of a particular pump failing to start when called upon to do so might be 1 in 500 or 0.002.

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.

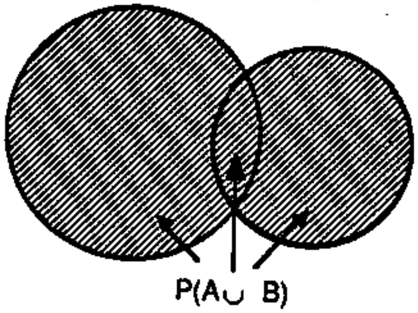
The probability rules that cover these scenarios are referred to as **AND** and **OR**. That is to say *"What is the probability of one thing happening AND another thing happening?"* and *"What is the probability of one thing happening OR another thing happening?"* The Venn diagrams below show these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

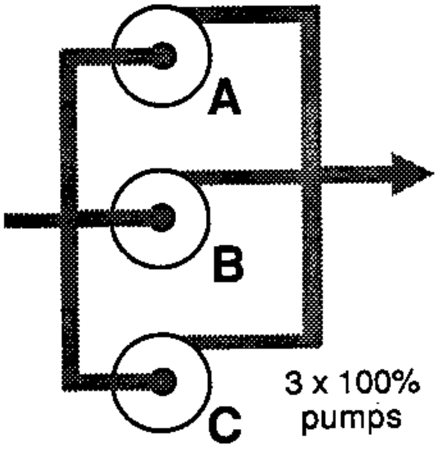


Figure 1

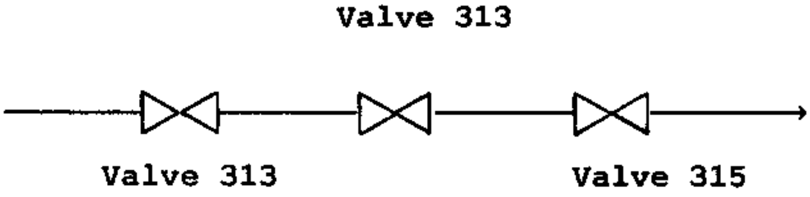
So, the probability of the system working is determined as follows:

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

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.



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

$$
\begin{aligned}
R &= \text{probability of working} \\
R(311 \cap 313 \cap 315) &= R(311)\ R(313)\ R(315)
\end{aligned}
$$

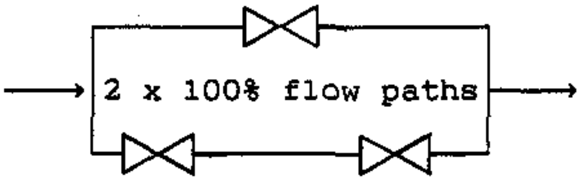
Again, there is another way of looking at this. The system will not work if Valve 311 **OR** Valve 313 **OR** Valve 315 doesn't work. The equation for that is given as:

$$
\begin{aligned}
Q &= \text{probability of not working} \\
Q(311 \cup 313 \cup 315) &= Q[311 \cup 313) \cup 315] \\
&= Q[(Q(311) + Q(313) - Q(313)) \cup 315] \\
&= [Q(311) + Q(313) - Q(311)\ Q(313)] + Q(315) \\
&\quad - [Q(311) + Q(313) - Q(311)\ Q(313)]\ Q(315)
\end{aligned}
$$

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,

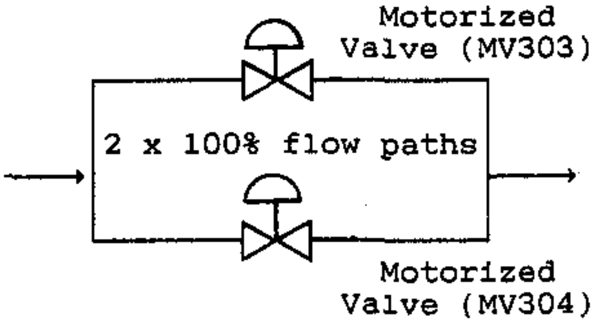
R(total) = R(top valve) + [R(valve 1) x R(valve 2)]
- R(top valve) x [R(valve 1) x R(valve 2)]

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***

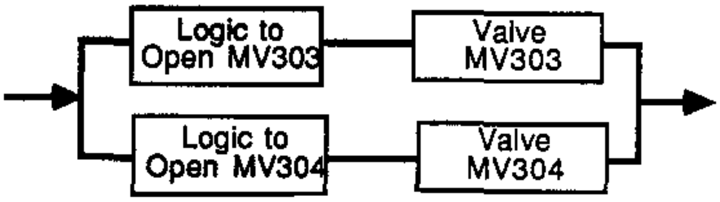
So, you can see the overall reliability is higher than for the individual valves.

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,

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

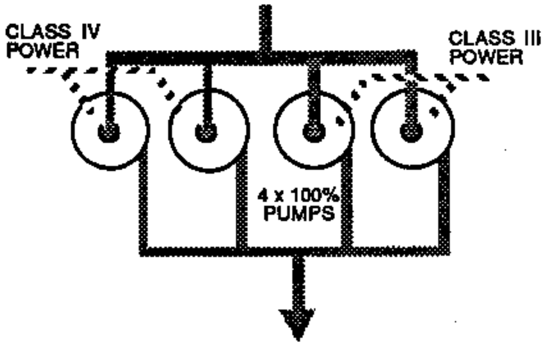
Substituting the appropriate figures into the equation, we get:

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

EXERCISES

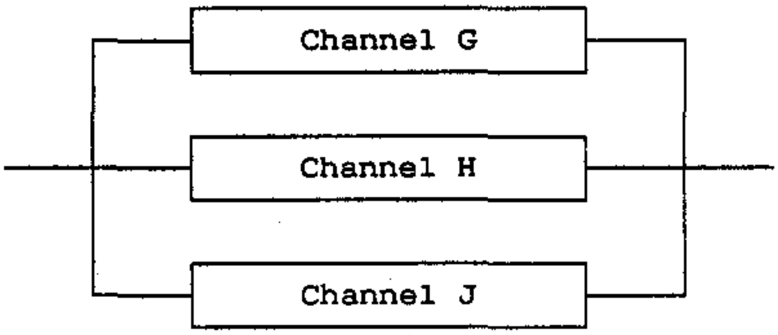
3. **Draw a Reliability Block Diagram for the following system:**

PICKERING NGS A
HIGH PRESSURE SERVICE WATER



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

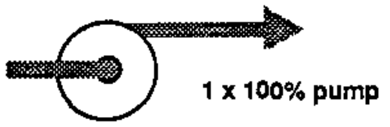
If we have a system where there is only one pump which must be working for the system to work and we wanted the system to work 99.9% of the time, there would be a lot riding on that pump working.. If it fails or needs to be repaired, the entire system would be out of service. This problem can be eliminated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

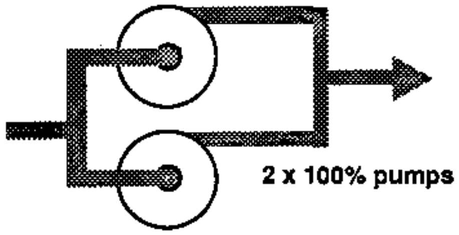
Mathematically we can compare the reliability of a system with one 100% capacity pump versus one that has two 100% capacity pumps in parallel.

Assuming a pump reliability of 0.95,

Scenario 1 - Single Pump

Rs = 0.95





Scenario 2 - Redundant Pumps

$$
\begin{aligned}
Rs &= 0.95 + 0.95 - (0.95) \times (0.95) \\
&= 0.9975
\end{aligned}
$$

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

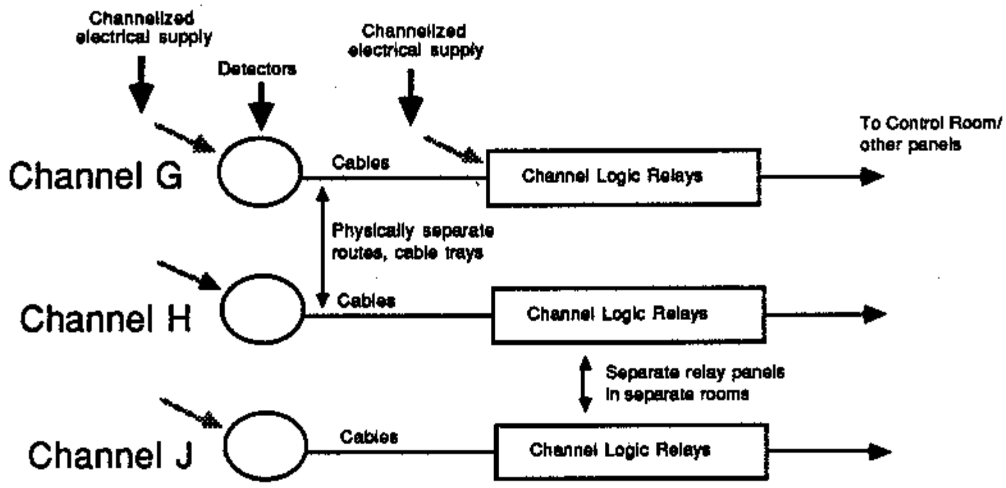
6. How does redundancy help make a system more reliable?

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.

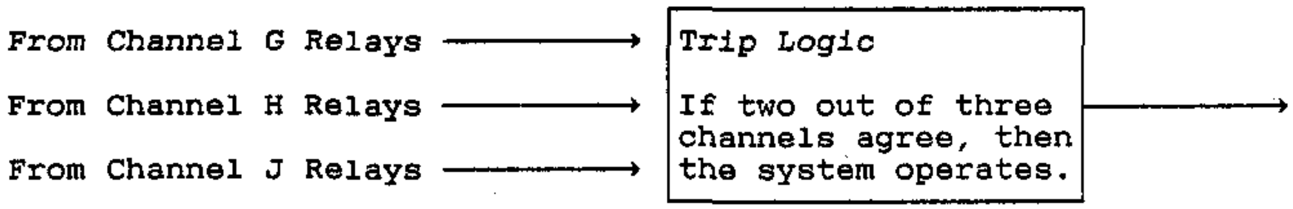
All critical systems, such as those which are required to shutdown the reactor in case of an emergency, have redundant monitoring, controlling and annunciating equipment. **Channelization** involves running the separate instrumentation, wiring, piping, etc., so that a failure on one channel does not 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.


Channelized electrical supply
Detectors
Channelized electrical supply
To Control Room/ other panels
Channel G
Cables
Channel Logic Relays
Physically separate routes, cable trays
Channel H
Cables
Channel Logic Relays
Separate relay panels in separate rooms
Channel J
Cables
Channel Logic Relays

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) Channels A,B,C	Shutdown System Two Channels G,H,J
Shutdown System One Channels D,E,F	These systems are seismically qualified at the later stations, with separate water and power supplies and controls
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?

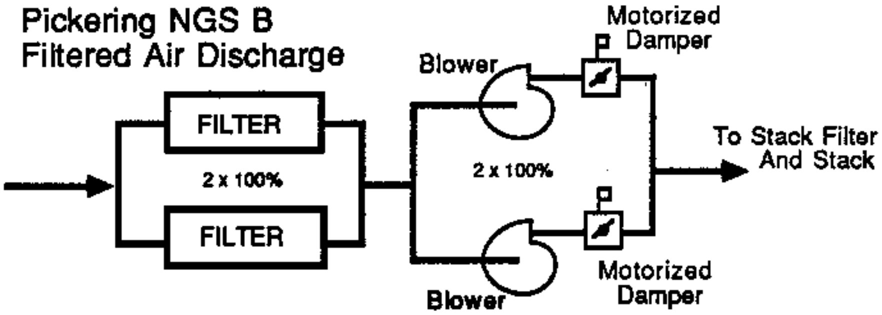
SUMMARY

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