Indian Institute of Technology Madras

Present

NPTEL

NATIONAL PROGRAMME ON TECHNOLOGY ENHANCED LEARNING

NUCLEAR REACTOR AND SAFETY

AN INTRODUCTORY COURSE

Module 05 Lecture 02

Safety Principles-Cont...

Dr. G. Vaidyanathan

School of Mechanical Engineering

SRM University

Good afternoon students. This morning's lecture I talked to you about the different safety principles which we follow right from the beginning of site selection. Then we moved on to the design. Then we also touched upon the commissioning, then operation, and we also saw how these principles are getting applied and we just saw the enunciation of the principle of defense in depth.

Now in this lecture we will get into more depth. Of course, the more deep and deep we go our knowledge base will improve and will understand better.

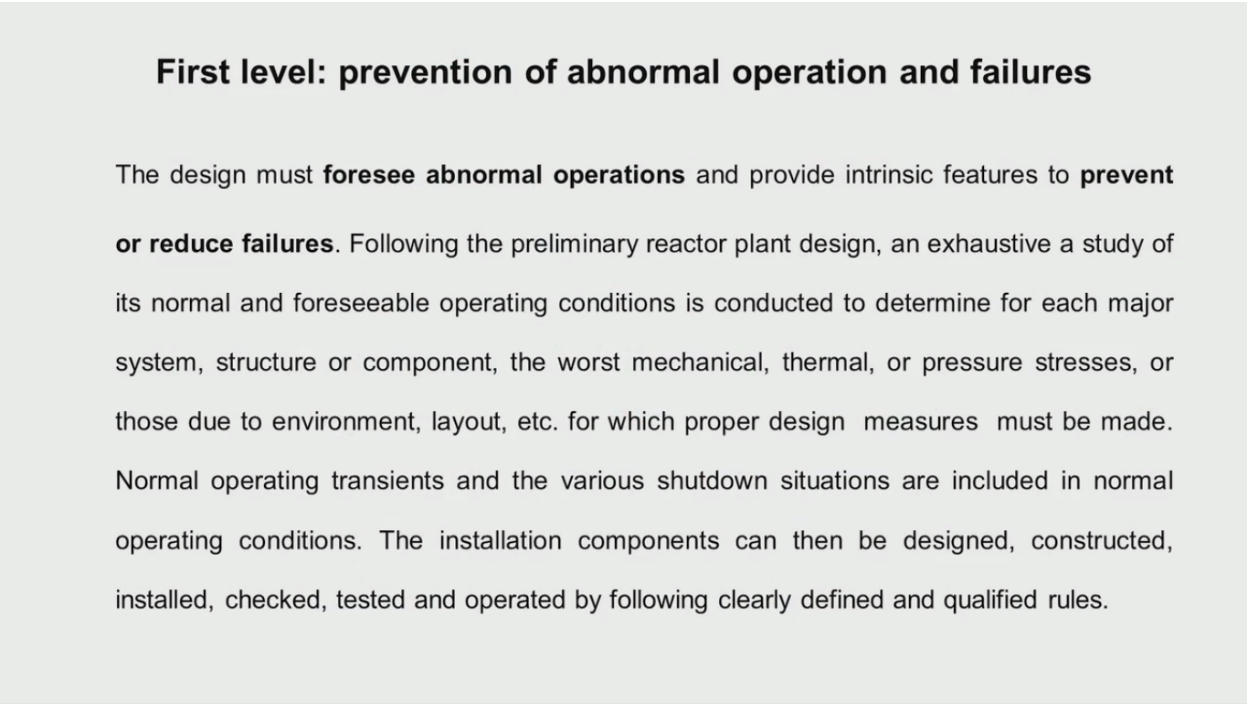
(Refer Slide Time: 00:01:14)

- The defence in depth approach leads us to adopt proven engineering solutions. A **high quality of engineering** is applied to all aspects of the design, construction and operation with adequate **quality assurance**. In the design **adequate safety margins** are used. While giving safety margins sufficient consideration is given to the system **thermal inertia and other intrinsic safety characteristics.** Otherwise the design would be too conservative and costlier. The temperature changes would be slower when the thermal inertia of the system is high. This gives the operators sufficient time to respond in case of any event. Last but not the least, it is a standard practice to provide sufficient **training to the personnel** involved in construction, operation and maintenance of nuclear facilities before putting them on the job.

So here just to recollect the same. The defense approach, depth approach really means good design that means you good high quality of engineering in the design, construction, and operation. How this you can achieve? You assure quality assurance. You assure quality assurance in the design. The design is vetted. The design is validated based on sound testing. So the design is good. Then you provide adequate safety margins in the design so that from what you predict and what really happens you must consider those good safety margins. Another thing if you give too much of a safety margin your design becomes conservative and then your whole plant will become costly. You cannot give too much margin. For example, suppose you expect let us say it is a sodium reactor cooled by sodium and the boiling point of sodium is about 900 degree centigrade. Now let us say you are going to operate the plant such that your clad temperature should not cross 700. okay you can say that okay you will aim it operate – design you may say at 680 or 650 but suppose you say I will only aim at 600 it is too much of a margin. It is not good. It will cost – the plant will cost more. Similarly in the design you must also consider all the intrinsic safety features. One of the features is thermal inertia. Suppose you have a large mass capacity of the coolant then the temperature change will be slow. So these things also need to be very well taken care in the design and allowed otherwise your design should be too much conservative.

Another advantage of this thermal inertia is let us just take a pool type of sodium reacts, sodium cooled fast reactor pool type we saw in the previous lectures. The sodium capacity is huge. So in case there is a loss of flow, the temperature increase slowly because the capacity is high. So this gives sufficient time to the operator to act in case it is needed to be. Then last but not the least training to the personnel involved in all facets of the nuclear is essential before putting them on the job.

(Refer Slide Time: 00:04:02)



Normally we have the licensing of the operation and maintenance people who are working on the job basically in the nuclear installations. We will come to the depth of the first level, first level of defense in depth. Now let us look at the first level or defense in depth. So it is to prevent abnormal operations and failures. So abnormal operations what do you mean by abnormal operations? Those operations which you are not foreseen it can happen. For example, if there is a switch meant for starting up or shutting down the motor maybe somebody could indolently put off the switch or something so let us say it is unsafe to put on a switch when it is in off condition. Then I have to prevent this failure. So what I have to do? I have to have a mechanism by which even if he is puts on the switch the container operation will not happen without some other condition being fulfilled. So there is a need to build in intrinsic features in the design to see that abnormal operations do not happen, but should they happen then you have to see how to take care of it. But here in the first level we find out all the operating conditions, normal, low power, high power, low flow, high flow, then conditions of different conditions of operation, what are the stresses on these structures. It could be a thermal stress because of temperature changes, it could be a pressure stress or it could be your cycling because a component may undergo some cycles because of there is a flow oscillation, the temperature oscillations could be there and in all such conditions the operating transients as we call them should be considered in this level. So in this level the normal operating transients, the shutdown, start up, all are going to be faced by the plant. So the components installation, components installation need to be designed considering clear-cut defined rules so that the prevention of abnormal operation is there and failures are not there. So first level is what is this.

(Refer Slide Time:00:07:06)

Site selection should consider:

- seismic level, meteorological conditions, weight of snow, maximum over-pressure wave, etc.
- Sets of **rules and codes** (ASTM standards, ASME codes) define the conditions for design, supply, manufacture, erection, testing, operation and maintenance of all safety related equipment and structures in the plant. The selection of appropriate staff for each stage, their appropriate training, the overall organization, the sharing of responsibilities contribute to the prevention of failures throughout plant life.

So here how do we say that things site selection. We choose a site such that the seismic level is not, such that it cannot cause a very large earthquake to the plant. So we choose a site which is having a lower seismic level. Then the meteorological conditions like tsunami, flooding should not be there. If it is a very cold country snow, weight of snow, weight of snow itself you might have heard recently in Kashmir in the month of February there are very heavy fall of snow. Some of the houseboats with the weight of snow they've got into the Dal Lake. Then what is the in case they are going to see a pressure wave. So all these conditions are going to be seen during the site selection. And in the design we have to follow the rules, design rules for example the ASME codes and the ASTM standards for the different materials so that we can define the specifications for design specifications, the manufacturing specifications, the testing specifications, and the operating specifications of each and every equipment. The selection of appropriate manpower or appropriate staff to deal at every stage, their training, etcetera. again is one which can minimize the failure.

(Refer Slide Time:00:08:41)

Second level: control of abnormal operation and detection of failures

- The installation must be prevented from crossing the authorized operating limits and sufficiently reliable regulation, **control and protection systems** must be designed, to inhibit any abnormal development before equipment is loaded beyond its rated operating conditions. Temperature, pressure and nuclear and thermal power control systems shall be installed to prevent excessive incident development without interfering with power plant operation. With a stable core and high thermal inertia, it is easier to hold the installation within the authorized limits. Systems for measuring the radioactivity levels of certain fluids and of the atmosphere in various facilities shall be monitored continuously to check the **effectiveness of the various barriers**.

Now the second level, what is it, control of abnormal operation and detection of failures. So if you are able to detect the failure you might be able to see that the system does not get into a bad situation. So how do you do? You have proper control and protection systems which must be in-built into the design so that you do not take the plant to an abnormal operating conditions. For example, you have temperature control systems means if the temperature rises you increase the coolant flow so that the temperature is maintained. In case there is a steam pressure raises beyond a limit your safety valves open and releases, or the nuclear power, the power of the reactor control all such systems put in the plant will prevent any excessive rise of the parameters which can interfere with the plant operation. And you must have a stable core. Stable core in the sense that any change in the neutrons should not lead the core to a higher power and good thermal inertia.

Now in this way if we are able to do we can keep the plant operating within the limits. Also we must in the – as we are talking about the plant we must also monitor continuously the different barriers of to radioactivity release which we discuss some time back. So to see that they are effective that means you monitor the radiation at every, after every barrier and see that things are nothing much is moving out.

(Refer Slide Time: 00:10:57)

- Malfunctions should be sensed and alarms sounded in the control room so that it can be better dealt with by the operators without undue delay. Finally, the protection systems, the most important of which is the **emergency shutdown system**, but also including, for example, safety valves, shall be capable of rapidly arresting any undesirable phenomenon, even if this entails shutting down the reactor.
- Furthermore, a **periodic equipment surveillance** program enables any abnormal developments in major equipment to be spotted. Such developments would otherwise be likely to lead to failures over a period of time. Periodic weld inspections, crack and leak detection, routine system testing pertains to these preventive surveillance activities.

So what this leads to the sensing by the monitoring system. So good monitoring system, good instrumentation and then alarms in the control room so that the operator is well warned about any situation that is going to develop later, and finally the protection system. In case things are going fast it must shut down the reactor. So what we call as emergency shut down system or sometimes the word scram is used. Scram the control rods. So the reactor is scarmed we say, or as I mentioned in the case of pressure some safety valves which can release the pressure so that the pressure is brought down.

Then periodic equipment surveillance so that you can find out before the real development of any abnormal situation. For example, it could be a weld which is periodically inspected. It could be a walk around the plant to see if any where any high temperatures are existing or high activity is existing from time to time. In fact the surveillance program is well made in the beginning itself before the start of operation. There are some areas surveillance every week, some surveillance every day, some surveillance every fortnight, some surveillance every month and once in six months like that. All things are very clearly drawn up and followed scrupulously.

(Refer Slide Time: 00:12:50)

Third level: control of accidents within the design basis

- The first two levels of defense in depth, prevention and keeping the reactor within the authorized limits, are designed to eliminate, with a high degree of reliability, the risk of plant failure. However, despite the care, a complete series of incidents and accidents is postulated by assuming that failures could be as serious as a total instantaneous main pipe break in a primary coolant loop or a steam line, or could concern reactivity control. This places us in a deterministic context, which is one of the essential elements of the safety approach.
- Systems are to be designed to limit the effects of these accidents to acceptable levels. These are the **engineered safeguard systems** (e.g. Shutdown and decay heat removal systems).

Then what is the third level of defense in depth? Control of the accidents within the design basis. See in the first level we saw how to prevent the reactor crossing the authorized limits, high degree of reliability we design so that failure should not happen. We then started monitoring the thing so that and protecting but in spite of all that there could be a failure such as a pipe break, your main pipe break. Instantaneous pipe break. Normally instantaneous pipe breaks do not happen. Any material has got slowly development of a crack, then a leak, growth of the crack. Nevertheless you can just assume a heavy weight falling and then a pipe breaks. You cannot say no but the probability is very very less. Of course we do prevent. Take enough measures to prevent such failure. Nevertheless, this can happen and this could cause you know a concern to the safety of the establishment. So here we have to design such that the effect of any accidents are within the acceptable levels. That is where we bring in the engineered safeguard system, the shutdown, and the decay heat removal systems. Decay heat removal is essential even after shutdown. So both these go together.

(Refer Slide Time:00:14:48)

- Startup of these systems must be automatic and human intervention should only be required after a time lapse (15 to 30 min) allowing sufficient time for a carefully considered diagnosis to be reached. In the postulated situations, the correct operation of these systems ensures that core structure integrity will be unaffected, which means that it can subsequently be cooled. Release to the environment will consequently be limited.
- The choice of incidents and accidents must be made from the beginning of the design phase of a project so that those systems required for limiting the consequences of incidents or accidents integrate perfectly with the overall installation design. This choice must be made with the greatest care as it is very difficult to insert major systems in a completed construction at a later date.

And start up of this surround systems or the decay heat removal system should be automatic and we always do not take credit for any manual or human actions for about 15 to 30 minutes after it is decided that the plant needs to be shut down. Why? See when there is an event happening in the plant which has crossed some of the limits there are going to too many alarms in the control room and too many signals. Operator does take certain time to really get a picture and take some action. So we always in the spirit of 15 to 30 minutes from the instant we always say it should be automatic. Beyond 30 minutes maybe we can consider some operational actions. Now the correct operation of these systems is required and so that any release of activity to the environment should be limited. So the operator has to do things with a cool mind so that is why the it is called the grace period.

Then the choice of the events, events could be incidents or accidents and at all stages of the plant from design phase have to be integrated perfectly with the overall design so that any changes, any major changes are not required after the construction of the plant. So you must for see as many events, as many incidents as possible right at the design stage.

(Refer Slide Time: 00:16:59)

Fourth level: control of severe plant conditions

- Considering plant failure, such as the accident which occurred at Three Mile Island in 1979, the means required to contend with plant situations which had bypassed the first three levels of the defense in depth strategy needs to be studied. Such situations can lead to core meltdown and consequently to even higher release levels. The concern here is to reduce the probability of such situations by preparing appropriate procedures and equipment to withstand additional scenarios corresponding to multiple failures. This then gives the requirement of **the containment** around the reactor, which needs to be designed suitably for the expected conditions of core melt down. It is then essential that the containment function be maintained under the best possible conditions.

Then the fourth level is control of severe plant conditions. Okay we did all, still we assume that okay a condition has happened which we are not forcing. Then what happens the activity will come out of the reactor. Now this is what happened in the Three Mile accident wherein there was a core meltdown. Then there was release of the activity and efficient products into the reactor building but it didn't get into the environment because of the fact that there was a containment, concrete containment structure around the reactor which prevented the activity from going out. In fact there was no evacuation in the case of the Three Mile Island. However, in the case of the Chernobyl the containment structure was absent. So and in the case of Fukushima there is a breach of the containment. So here if you see containment plays the role of the fourth level of defense in depth.

(Refer Slide Time: 00:18:38)

Fifth level: mitigation of radiological consequences

- Population protection measures because of high release levels (evacuation, confinement indoors, with doors and windows closed, distribution of stable iodine tablets, restrictions on certain foodstuffs, etc.) would only be necessary in the event of failure or inefficiency of the measures described above. The conditions of this evacuation or confinement are supplemented by the preparation of long or short term measures for checking the consumption or marketing of contaminated foodstuffs. Such measures are included in the external emergency plans. Periodical emergency training drills will also be necessary in this area to ensure adequate efficiency of the resources and linkups provided.

Okay we now take Fukushima, the containment failed and we have gone. Now we have to mitigate the radiological consequences. So what are the mitigation measures? Evacuation. People are who are in the path of the plume of radioactive particles which you can assess by knowing the weather conditions then we need to evacuate that area first. For all these purposes softwares have been developed and validated from time to time, integrated with the weather satellites data and today we have got a very good picture at any moment we can tell which direction, in case the accident happens, which direction the radioactive plume will go. So evacuation needs to be done. Then confinement. Confinement indoors one of the ways suppose a person is within a house, best way would be for him to stay indoors and maybe close his nose with a handkerchief that would be sufficient. Then the other measures like distribution of stable iodine tablets wherein the iodine is given to the people who are supposed to have had some exposure. These iodine tablets will go into the thyroid. The reason is once this iodine is in thyroid the radioactive iodine which is coming out from the radioactive plume will not be able to get into the person thyroid, already thyroid saturated with iron. And this evacuation and then confinement all these need to be decided very well. There is also may need to see the contamination of the footsteps. Footsteps which are being sold in the market but that is a later stage, but all these things are included in emergency plans and the emergency drills are conducted very regularly so that the people are aware what they should do in case of an emergency.

(Refer Slide Time: 00:20:59)

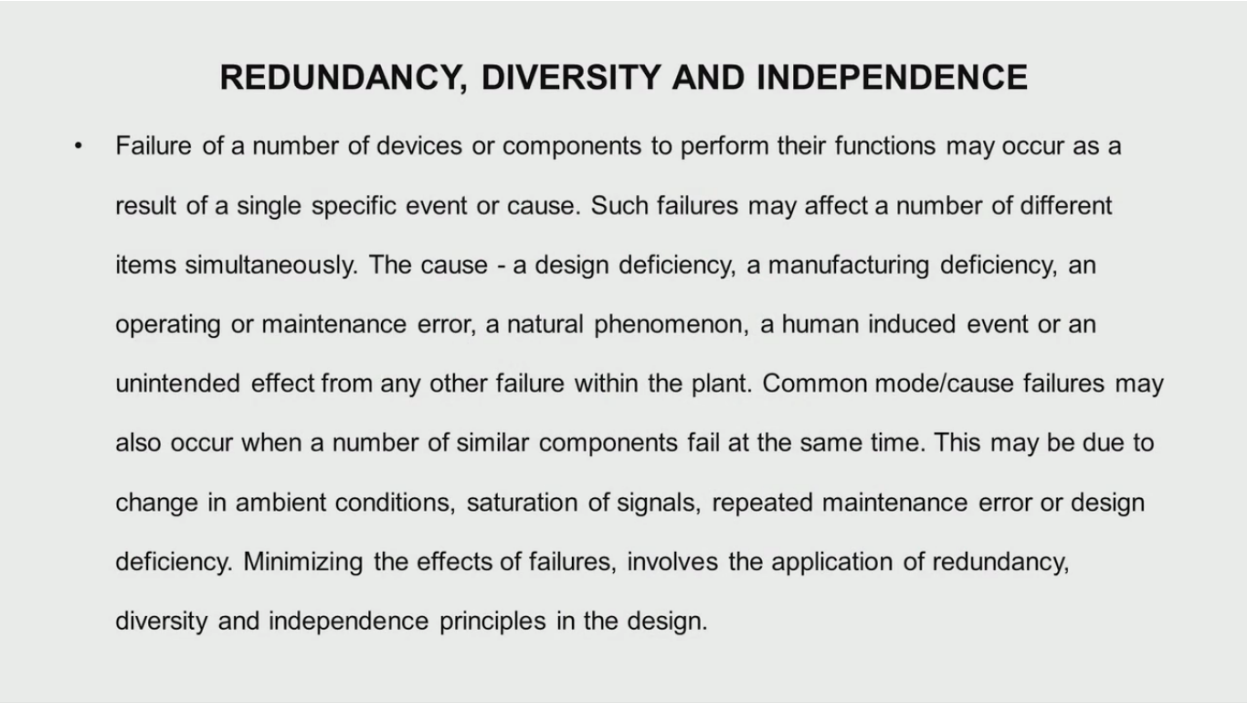
Essential objectives of accident management, including both preventive and protective measures, are:

- monitoring of the principal characteristics of the plant state;
- controlling the core sub-criticality;
- restoring the core cooling and ensuring longtime cooling;
- protecting the containment integrity (including its leak-proof characteristics) ensuring the removal of heat and preventing loads and dangerous effects on containment;
- Regaining the control of the plant in order to avoid further damage.

So if you look at the essential objectives of the accident management is monitoring first. Monitoring the state of the plant. Next, control the cores of criticality means the core should be in a controllable state. You should be able to shut it down and shut down the fission reaction. That is the third. Second. Then, third one is you must be able to provide cooling to the core not

only short-term, long-term. Then next one to protect the containment integrity. In fact, containment does not only the as a barrier to radioactivity to the amount of heat. So it is very essential that the containment be kept cool so that the concrete does not fail. Finally, having the accident has happened we have to see how to regain control of the plant so that we can avoid any further damage.

(Refer Slide Time:00:22:18)



Now I mentioned something about providing more than one equipment. That is we consider a single failure in any system or plant should not give rise to a safety issue. I used about three words; redundancy, diversity, independence. Now why we are thinking as I said a single failure should not cause a safety problem. The problem could be your design deficiency because of which the failure, single failure can happen. It could be a manufacturing failure. Manufacturing deficiency, not properly manufactured. The weld may not have been properly done, or could be an operator error, or it could be a man induced event due to human. Then there is other type that there could be common mode or common cause failures, let us say cause of fire, or an earthquake, or a tsunami. All such things may lead to failure of all these redundant systems. So minimizing the effects of failures if you follow the redundancy, diversity, and independence principles we can bring down the failures or the effects of these failures to a very large extent.

(Refer Slide Time: 00:24:01)

REDUNDANCY

Redundancy is the use of more than the minimum number of sets of equipment to fulfill a given safety function. Safety functions must remain effective even if a single failure occurs independently of an initiating event, and also if a component is not available due to maintenance or repair. Such separate single failures include the random failure of a component that results in its incapacity to perform its intended safety function. Subsequent failures arising from such random failures are also regarded as part of the original single failure. Redundancy enables failure or unavailability of at least one set of equipment to be tolerated without loss of the function.

Let us look at redundancy. It is very simple as I mentioned. It is the use of more than minimum number of equipments required to fulfill a given function. As I said if one pump is sufficient you provide two pumps. If one pump fails other pump will take over automatically or you can say both the pumps are running and if one pump fails other pump can still supply you 50% of the flow. If you need one thermocouple if it fails you provide two or three. So safety functions will still or will be able to have in case the flow comes down the temperature will be monitored and the plant actions will be taken, and this I am explaining at every stage this redundancy we will have to maintain. When it goes to the shutdown again redundant. Redundant control rods. If to control rods are sufficient you provide four control rods or six control rods. Now thus the redundancy enables the unavailability to be minimal. So our unavailability is tolerated without any loss of the safety function.

(Refer Slide Time: 00:25:23)

- Two full capacity pumps so that in the event of failure of one the other pump would supply coolant to the core.
- Provision of two or more similar instruments for measurement of plant parameters like flow, temperature, flow, and reactor power etc., so that even if one instrument fails the other would be able to monitor the health of the plant and initiate automatic safety actions, when the thresholds are crossed.
- Provision of many control rods of a similar design, though few are sufficient for shutting down the reactor.

This is just to reinforce to full capacity pumps provision of two or more instruments for measurement of flow, temperature, reactor power and as I said provision of many control rods even though few may be sufficient for shutting down the reactor.

(Refer Slide Time:00:25:46)

DIVERSITY

- The reliability of some systems can be enhanced by using the principle of diversity to reduce the potential for certain Common Cause Failures (CCF). Diversity is applied to redundant systems or components that perform the same safety function by incorporating different attributes into the systems or components. A CCF is a dependent failure event where approximately simultaneous multiple failures result from a single shared cause (e.g. fire, flooding). A Common Mode Failure (CMF) is a common cause event where the multiple equipment items fail in the same mode (e.g. failure to reset pumps following maintenance, design failures).

Then diversity. Now diversity is basically diverse as the name says it diverse. Let me take up -- let us take I have a motor supplied by company A. I require only one motor. I provide, let us say, three pumps are operating I put three pump with motors of company A. should there be your design deficiency under certain conditions of operation all the three may come off. It may fail. So what we call as a common mode. Then we have the common cause where multiple failures can happen from a single cause that is a flooding, or a fire. So we need to take care of this. So how do we do it? We have to do it through two approaches.

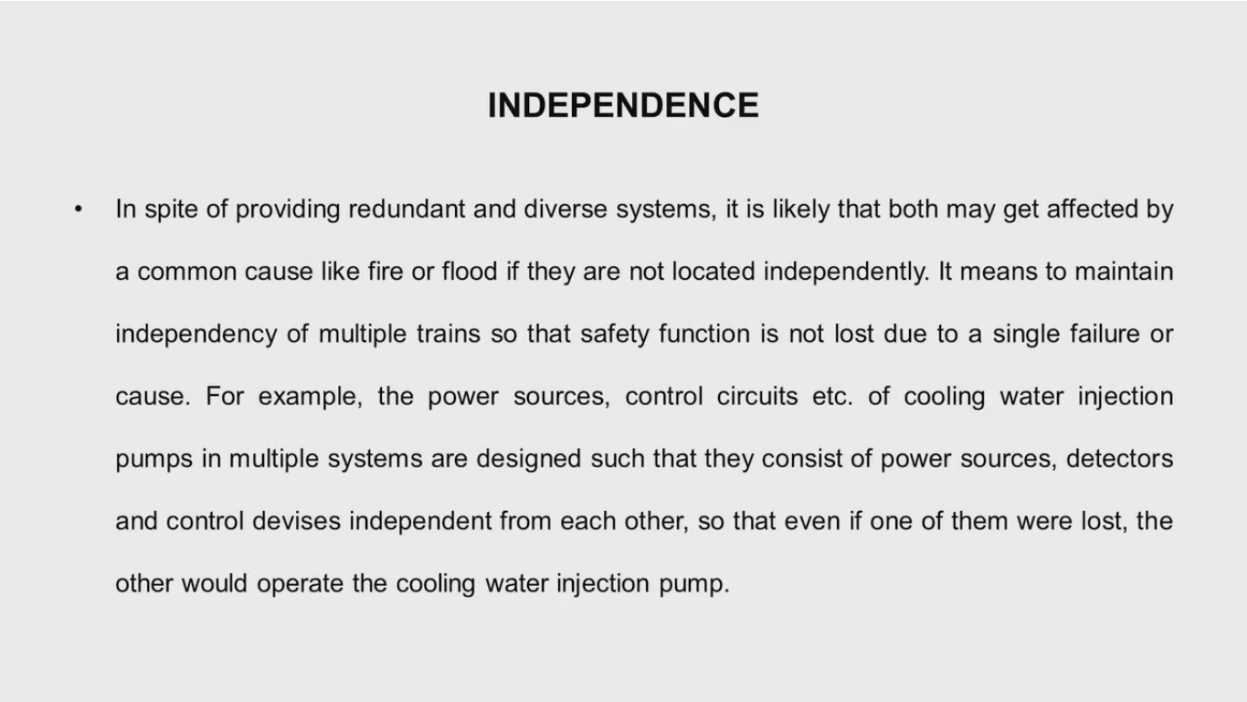
(Refer Slide Time: 00:27:01)

- Diversity can be achieved by having different principles of operation, different physical variables, different conditions of operation, or production by different manufacturers. Care should be exercised to ensure that any diversity used, actually achieves the desired increase in reliability. For example, to reduce the potential for common cause failures the designer should examine the application of diversity for any similarity in **materials**, **components and manufacturing processes**. Use of diverse components has the disadvantages of extra complication in operational, maintenance and test procedures, besides spare inventory and maintenance.

We try to have equipment from different manufactures. Manufacturer A, manufacturer B, manufacture C. So sure they won't fail in the same time. Then I can also have diversity in the materials, material choice I can have different materials not of the same material but both the materials maybe good. Then diversity let us say I apply in the case of a flow decrease in the reactor. When the flow decreases in the reactor the flow measure can tell you whether the flow has decreased or temperature increase can tell you whether the temperatures of the flow has decreased. So these are diverse methods of knowing the malfunction. So this way we are able to provide additional information that is additionally we are trying to reduce the chance of failures, common mode or common cause, common mode failures. Of course, when you have diverse equipment it does lead to difficulties in your spares inventory and maintenance. You have got keep spares for all types of motors but that is the price you have to pay.

Now as I said a common cause like fire. I may have redundant equipment. I may have diverse equipment but if all are there in the same area location they will be subjected to the fire and they won't conk off. They won't work.

(Refer Slide Time: 00:29:00)



So in providing this redundant and diverse system we need to see that they are independent trains. For example your diverse motor maybe get a supply but the supply routing of that line should be different from the supply routing of the other motors. All the motor should not get supply from the same power, what you call, the same circuit breaker. So by keeping independence then only we can achieve and many cases the layout of the plant at the layout stage this needs to be very much looked into that all my redundant and drivers channels or is independence is also being satisfied. So you must have different diversity in power sources. Many of you may if you go to any power station, any nuclear power station or nuclear station, normally they are connected to the grid through many lines; not one line alone is not put. They have got many lines so that even if the possession power link with one the grid is lost in one direction the other thing will still be able to give you power in case there is no power generation in the plant.

(Refer Slide Time: 00:30:25)

Independence is accomplished in the design of systems by using functional isolation and physical separation:

- **Functional isolation**: Functional isolation should be used to reduce the likelihood of adverse interaction between equipment and components of redundant or connected systems resulting from normal or abnormal operation or failure of any component in the systems.
- **Physical separation and layout of plant components**: System layout and design should use physical separation as far as practicable to increase assurance that independence will be achieved, particularly in relation to certain common cause failures.

So how do you achieve independence? Two ways; functional isolation and the physical separation. So functionally you isolate the components so that interaction between the components is reduced and also the failure of one will not affect the failure of the other. Then the physical separation which as I mentioned needs to be done in the layout.

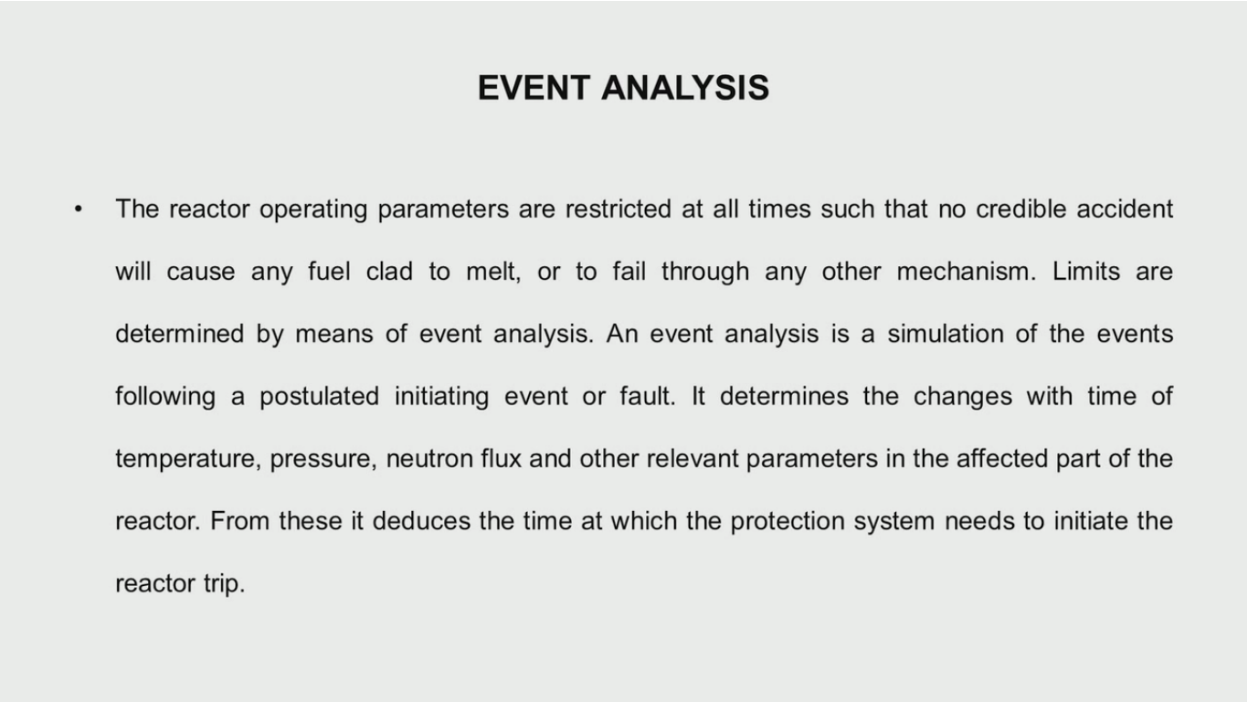
(Refer Slide Time:00:31:02)

Physical separation includes:

- separation by geometry (such as distance or orientation);
- separation by barriers or by a combination of these.
- The choice of means of separation will depend on the postulated initiating events (PIEs) considered, such as effects of fire, chemical explosion, aircraft crash, missile impact, flooding etc.
- Certain areas of the plant tend to be natural centres of convergence for equipment or wiring of various levels of importance to safety. Examples are containment penetrations, motor control centres, cable spreading rooms, equipment rooms, the control rooms etc.

So how do you do the physical separation? By geometry, by putting barriers. Let us say there could be a wall. There be a fire barrier between two pumps or motors and this will depend upon whether you are postulating a fire, you are postulating a chemical act or a flooding; all these things needs to be kept in mind. Now surely most in all cases there are some areas which are very important to safety. They are basically the cable rooms, motor control centers, the control rooms, containment penetration, etc. here is where the separation is very much needed so that there need not be a common cause failure.

(Refer Slide Time: 00:31:56)



Okay. Having done the redundancy, diversity, and independence having implemented to the maximum extent we need to do an analysis of the plant under different events what will happen; is there a chance for the fuel to clad to melt or fuel clad to fail. So when should I actuate the automatically the protection system, at what -- up to what could be the threshold at which I should set so that the production system can act and if required the reactor trip may be acted upon.

(Refer Slide Time:00:32:51)

- Allowing for **the time delays in the electronics and control rod drive mechanisms** and the time for the control rods to fall under gravity, it calculates the peak temperature in the hottest fuel pin. It then adds appropriate **allowances for random variations and uncertainties in the data**, and compares the resulting temperature with the melt temperature of the can. It repeats this process for a range of reactor operating conditions, thereby establishing which reactor conditions are safe with respect to that particular accident. The analysis is carried out by **computer codes, which are licensed by the regulatory authorities.**

Here we have to consider in this analysis that any action for example let us say you measure a temperature. There is a time constant of the measuring instrument, may be four seconds, five seconds, depending on this has to be considered even at the design stage itself. Suppose I want something to happen, action to be done very fast I must have an instrument with a very low response time. For example, in sodium systems even we have a thermovalve but we also have a fast response thermocouple which is without a thermovalve so that extreme cases that can act as a act to give a signal to trip the reactor. Then next step is the electronics delay, delays in the electronics that need to be considered and even though you might have given the trip signal there is a certain time which it takes for the control rods to drop into the core. You have to consider that. So all these time delays need to be considered. Then you have to give allowances for variations and uncertainties in the data. For example you might be measuring a temperature, let us say 500 degree centigrade when it could be 5 not 495 because there is the error of the instrument. This also needs to be considered while fixing the thresholds.

So this process has to be repeated for all the operating conditions and then you have to come to a common threshold for the plant at which your protective action should be actuated and all these safety analysis is done by computer codes which are again licensed by the regulatory authorities.

(Refer Slide Time: 00:34:47)

CORE INVENTORY-RADIONUCLIDES

- The unique hazard associated with a nuclear reactor is the inventory of radioactive material that accumulates in the core after power operation. The basic purpose is to protect the plant workers, members of the public, and the environment from harmful effects of radiation. The radioactive material is primarily from the accumulation of radioactive fission products. Another source is neutron activation of various structural materials in the core. The approach is to ensure that the core inventory of radioactive material is contained by the barriers (fuel, clad, primary system boundary, containment), and that shielding is provided within the plant to protect against penetrating radiation. Calculation of the inventory of radio-nuclides is complex, involving considerations of generation of radio-nuclides through fission and neutron activation, decay of the radio-nuclides, and transmutation by neutron absorption.

This radionuclides which will come out in the case of any accident and we say we have to protect the public. So effectively it depends upon how much of fuel you have put into the core. If you have a small reactor the fuel inventory would be small and it's, in case of an accident the amount of fissile material coming out also will be small. In fact this sort of approach has been promulgated by many people saying that let us go for small reactors so that even if an accident happens the chances of any radioactive or the amount of radioactive material coming out is less but you know if you make smaller and smaller components or smaller plants the cost goes up. So this we have to keep in the mind because nobody is going to accept electricity from you it is very costly.

So now fission you have to protect not only from the radioactive material which you can come out the fission products which can come out. So the fission products we saw on the fuel is contained by the fuel, the clad, then your primary vessel and the containment. Of course shielding is provided within the plant so that you do not have radiation during normal operation. Then how do you calculate the activity which can come to the public? It is not only due to the fuel. It is also as I said due to the fission products and the structural material which will get activated because of the radioactivity. So that is additional. So they also can give you activity if you come in very close to that. So we need to consider all these aspects when we say how much of activity is going to come out.

(Refer Slide Time:00:37:01)

MITIGATION OF RADIOLOGICAL CONSEQUENCES

The fifth level of defense is mitigation of radiological consequences. Mitigation measures include on-site emergency plans, aimed at providing protection to the plant workers and assuring that vital control functions can be maintained, and off-site emergency plans, aimed at protection of the public and the environment. On-site and remote emergency control centers are provided for coordination of emergency response and decision making.

So when we want to reduce or mitigate this this is what we talked the -- we have got on site emergency plants and off-site emergency plants. In case the plant as a case of Three Mile Island we had only on-site emergency because the whole containment was there. Nothing came out. There was no much consequence outside. so on-site emergency plants were implemented. Then if it goes to outside you have the off-site emergency plants as in the case of Chernobyl. It was very nicely implemented.

(Refer Slide Time:00:37:48)

On-site emergency response

A well organized and tested on-site emergency response plan must be in place. Elements of this plan may include such items as:

- Definition of the decision-making process and the people responsible for making emergency decisions;
- Criteria for declaring various levels of alert or an emergency situation;
- Notification of appropriate company, local, state, and national authorities of the occurrence, depending on the severity of the situation;
- Activation of an on-site or near-site emergency control centre, with appropriate staff, communications, and support, including public communications personnel;

What is the on-site emergence response? What we should do? So first and foremost is your decision making process, that is people have to be there who are responsible to take the decision A. I declare on-site emergency. So there must be authority which is able to decide and he must be given the criteria he must be well aware of the criteria, how to decide emergency situation. Then how to notify because the communication must go to the different people, the local area, the state, the national level. So all – so in case of a disaster what sort of things should do because you require support from all areas. So that is one. Then there needs to be a control center, suppose something has happened in the plant that there needs to be a place from which all these activities need to be communicated and all. So you require a communication or control center and also public communication so that you keep the public informed of what is happening so that it is in a transparent way things are known to the public and you take them into confidence.

(Refer Slide Time: 00:39:07)

- Activation of emergency response teams as required by the nature of the situation;
- If necessary, activation of control room habitability features or a remote reactor control room;
- Evacuation of non-essential personnel from the site.
- The on-site emergency response organization must have access to sufficient information about the event to assess the need for activation of off-site emergency plans. Local, state, and national regulatory and emergency organizations will also require information, and appropriate communications arrangements must be in the emergency plan.

Then habitability of the control room. When you many choose the emergency control room you must choose it away, not very much away from the normal control room. So you must have a remote control room from where you can operate the reactor. Similarly a control center which is going to be that it has to be away from the reactor. It can't be very close to the reactor. Then first and foremost the non-essential personnel who are not directly involved in the reactor they are shifted out. Then the – so the on-site emergency response needs to have the data of people, how many people are there etcetera. All those things are planned well. Again I repeat there is not need to act very fast. There are some few hours between the time the incident happens and the effect is felt outside.

(Refer Slide Time:00:40:09)

Off-site emergency response

- **Sheltering**- means requiring the population to remain indoors, with doors and windows closed, until a release has ended and the plume of radionuclide has dispersed. Sheltering is the minimum level of protective action for the public.
- **Chemical protection**: A significant contribution to risk from a radioactive release is uptake of radioactive iodine into the thyroid which can put children at risk of developing thyroid cancer. A possible measure is to supply normal iodine pills to persons within the emergency planning zone. In this way, radioiodine will be prevented from concentrating in the thyroid, affording a measure of protection.

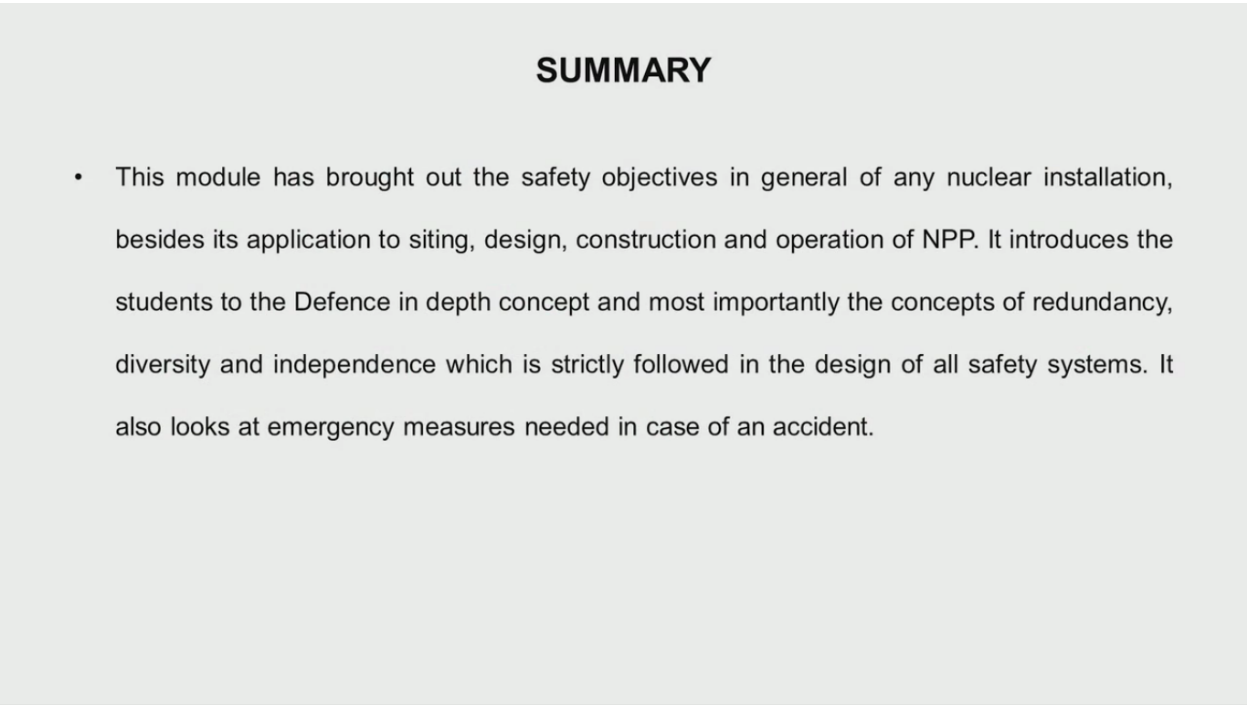
Off-site emergency response as I mentioned to remain indoors. So we call it the sheltering so that the plume of radionuclide once it has dispersed then maybe you can come out. This is a very very minimal way of protecting the public. Then other one is likelihood of taking the radioactive iodine which is released from the fission gases so you have to have a measure or means to supply iodine tablets the people and this needs to be so the off-site emergency organization needs to consider this.

(Refer Slide Time:00:40:59)

- **Evacuation:** The most extreme measure to mitigate off-site radiological consequences is evacuation of the population. Evacuation involves significant risk due to transportation accidents, and disruption to the lives of the population. Evacuation was considered at the time of the TMI-2 accident, but rejected except for voluntary evacuation of particularly vulnerable people. Large-scale, permanent evacuation followed the Chernobyl and Fukushima accidents. Planning for evacuation involves consideration of transportation means, mapping routes, traffic control, and establishment of reception facilities for evacuees. Evacuation must be decided after careful considerations as it has been seen after the Chernobyl and Fukushima accidents that psychological effects of fear of getting affected by radiation was more than actual effect.

Then evacuation. As I mentioned some time back in the case of Three Mile Island evacuation was considered but they found it is not very much necessary. Of course for the Chernobyl and Fukushima evacuation was done. So in fact, when you locate a site right in the beginning we consider whether there are sufficient evacuation routes, multiple evacuation routes so that in case of any calamity on one route, the people could be taken by some other route away so that they can be sent to safer places. So the routes, the traffic control in those areas when these people are being evacuated; all these are part of the emergency planning. And in fact, I can tell you having lived at Kalpakkam for 40 years I have seen many exercises, emergency exercises both on-site and off-site. Things have been able to move. The central, the state government, the district authorities all are able to come in a very very cohesive manner and all this is possible only if the drills are being done regularly. It does not mean that okay it may happen once in a while but we have to be prepared. I can tell you it is fortunate that we have such drills for nuclear situations. Unfortunately it is not so. Do you have a chemical emergency plan. I do not know. It is not so it is a very very well thought of program of emergency planning which is there right in the beginning because we are worried about ourselves and the public as a whole.

(Refer Slide Time: 00:42:53)



In summary I can only tell that safety objectives for any nuclear installation we apply the principles of the defense in depth right from design, construction, commissioning, operation. At every state we try to see, avoid the happening of events and should they happen how to protect the plant and in case the plant failure happens to the plant there is a breach of the barrier, still we would like to see that the activity does not come out and mitigate and in case it comes out after breaching the barriers, what I should do in a case of an emergency to protect the people from the effects of radioactivity.

So in brief I can only tell you or reinforce that the safety thing is built into our approach in all nuclear installations, and it is being regulated by the Atomic Energy Regulatory Authority.

(Refer Slide Time: 00:44:11)

BIBLIOGRAPHY

1. IAEA SAFETY STANDARDS SERIES No. SF-1, Fundamental Safety Principles-Safety Fundamentals, IAEA, Vienna (2006).
2. Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants Safety Guide Series No. NS-G-1.11, IAEA, Vienna,(2004).
3. IAEA, Safety Fundamentals: The Safety of Nuclear Installations, Safety Series No. 110 (1993)
4. LIBMANN, J., Elements of Nuclear Safety, EDP, France (1996).
5. IAEA, Defence in Depth in nuclear safety, INSAG-10, (1996).

Just small bibliography which you can have a look. Most of them are from IAEA. There is also a book by Libmann of France which gives very nicely the elements of nuclear safety which is followed in France. And on defense in depth there are some manuals of the IAEA which you can see.

(Refer Slide Time: 00:44:36)

ASSIGNMENTS

1. What are the basic objectives in the safe design of nuclear reactors.
2. What is the concept of Defence in depth? Please explain with an example.
3. What are the different levels of defence in depth?
4. What are the methods of achieving design safety in practice?
5. Clarify the terms Redundancy, Diversity and independence with reference to a nuclear reactor.

And the effect of any understanding can be really felt only if you can able to answer certain questions. So some certain basic questions which i have put which if you could answer okay, you know that the lecture has been well taken. Thank you.

Online Video Editing /Post Production/camera

R. Selvam

S Subash

F Soju

S Pradeepa

M Karthikeyan

T Ramkumar

R Sathiaraj

Video Producers

K R Ravindranath

Kannan Krishnamurty

IIT Madras Production

Funded By

Department of Higher Education

Ministry of Human Resource Development

Government of India