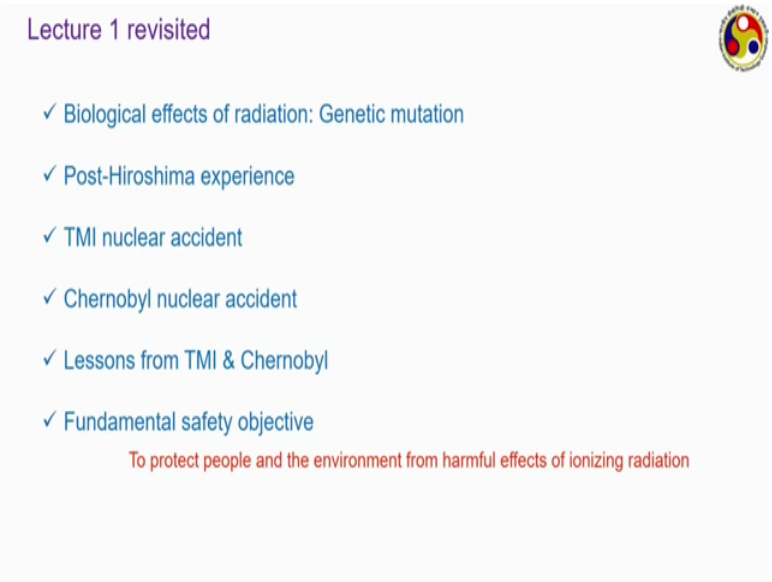
Fundamentals of Nuclear Power Generation
Dr. Dipankar N. Basu
Department of Mechanical Engineering
Indian Institute of Technology, Guwahati

Module – 11
Reactor Safety & Security
Lecture - 02
Defence-in-depth Philosophy

Good afternoon friends, so we are into the second lecture of our week number 11, where we are talking about the reactor safety and security. In the previous lecture of this module we have we are mostly in story telling mode basically, where I just talked about if you major nuclear incident that has happened worldwide like the of course, the Hiroshima incident and then a couple of very important or I should say very significant nuclear accidents that has happened at the three miles islands and Chernobyl. And taking that into account, whatever lessons we learn from this accidents starting from their today we are going to discuss about different kind of safety aspects or safety considerations, which are integrated in the design of a in nuclear power station.

(Refer Slide Time: 01:19)



So, just take quick recap of the previous lecture, we started with the biological effects or radiation which actually was the topic of the previous week, but still I give you a brief summary of that particular is stressing up on the genetic mutation caused by radiation, because the effect of radiation as I have mentioned the effect of any nuclear accident is

not just an instantaneous one, rather can be very very long can have very very long term effect, because the radioactive nuclear it to isotopes, which are released to the environment as a result of a nuclear accident can have very long half life and therefore, they can keep on decaying while emitting beta and gamma raise to the surrounding over a very long period.

Very long may refer to a few years a few 100 years or maybe a few million years. And that is; why the consequences of a nuclear power accident or an accident in a nuclear power plant can be very very power reaching I mean you have to is very mindful about possible consequences. Particularly, the effect the radiation can cause at the prenatal stage, that is to the fetus can be can have power reaching effects and that is why we mentioned about the genetic mutation in the previous lecture.

Then the post Hiroshima experience, what are the experience that we gained nuclemastic gained from that catastrophes, then we discussed about the three mile island nuclear accident which happens in; happened in 1979 in a nuclear power plant at a United States. A much bigger scale accident, which happened in 1986 in Chernobyl of former Soviet Union something which is termed as the biggest man made accident ever to happen, in a power station the Chernobyl accident is regarded as the largest scale level accident that can happen to a nuclear power plant and the; it has very very power reaching implication both on the nuclear industry and also on the corresponding research.

Like we have seen yesterday following the incidents of TMI and particularly Chernobyl there was a huge deep, in the installation of new nuclear power plants actually in United States and also globally hardly any nuclear power plant came up in during the period of 1982 to 2198, 2000 and it was almost in a stalemate kind of situation, as a global nuclear power production capacity remained almost same what the span of 15-20 years, but then with the advent of the generation 3 and generation 4 concepts with much higher level of security aspects newer nuclear plants again have stared come up.

But still the radiation affect, which now it is above we are more than 30 years from the Chernobyl incident and so we have a quite decent level of data to analyze the post effect of Chernobyl like; we have seen the bridge of depth occupied yesterday, it was a small town located just above three mile away from that Chernobyl and power station and, when the accident happened people run to that bridge to see exactly what happened. And

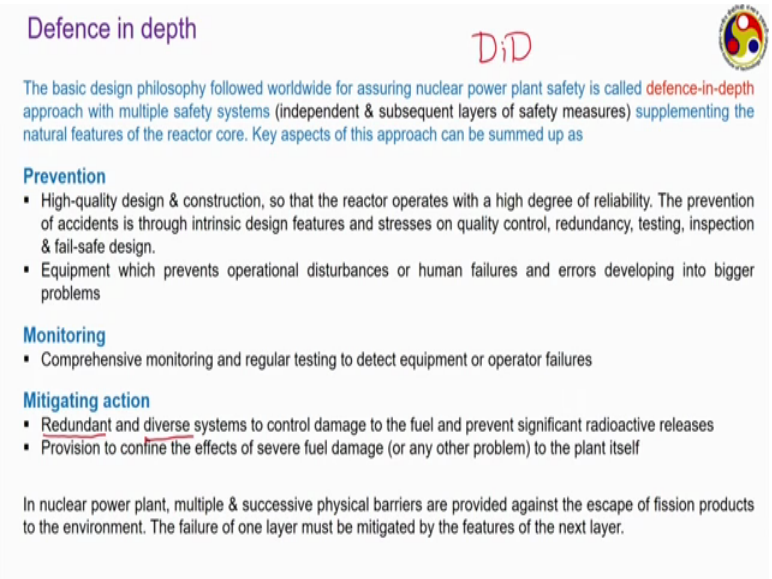
there are lots of peoples standing on the bridge, observing the fire and whatever was happening in that plant and unfortunately they were unaware that they are in the direct path of the radiation that is coming from the plant.

So, lots of them suffer from strong radioactive disease, radioactive syndrome accrued radioactive syndrome something which is called, but there is no proper data about what was the exact affect. At least, but still as we have covered 30 years, we have some more data and though all those informations are regularly getting added to the database their by strengthening the research related to the security aspects.

And by analyzing those lessons from TMI and Chernobyl, and also I must add which I have not discussed yesterday the very recent incident or Hiroshima the Daiichi power station culminating all these experiences, we have got newer safety guidelines and from this is the fundamental safety objective was identified as to protect people and the environment from harmful effects of ionizing radiation.

That is the pioneering objective of this entire module to identify options, which will isolate the find the ionizing radiation coming out of from the fission products particularly from the human being and also to the environment. That is no with is fission products are coming in free contact with the environment of the human, that is what we are trying to ensure.

(Refer Slide Time: 06:15)



And the methodology, that is followed the approach that is followed to at in that objective is known as defence in depth. It is a basic design philosophy just followed globally, different countries have their own methodologies, but the levels or the procedures are more or less similar and all those procedures or the sequence of events which are followed that is what is called the defense in depth. It always refers to multiple safety systems, basically it comprises of several layers of security all those layers are independent and subsequent in nature and the objective is to supplement and natural features of the core.

Key aspects of this approach can be three factors: first is prevention. The high quality design and construction must be ensured; so that the reactor offered to the high degree of reliability. The prevention of accidents is through intrinsic design features as stresses on quality control, redundancy testing inspection and failsafe design. Couple of those trans like this redundancy and failsafe we shall be seeing shortly in this lecture itself. But the meaning of this particular term refers to, we have to ensure high quality design and construction so that all possible types of reactions at sorry (Refer Time: 07:37) accident or incidents at least those which we can for see can be killed at the design level itself.

And also we have to ensure that the equipments; we install equipments, which are capable of preventing operational disturbances or human failures. And also will not allow any kind of small disturbance or small error into a much bigger issue. Before that only can be able to either sub sizes the event or make the authorities aware about, what may happen in; next few minutes to come on in the next period to come.

The second aspect of defence in depth is; defence in depth is monitoring, comprehensive monitoring and regular testing to detect equipment or operator failures particularly as time goes on as the aging effects start has to become dominant, it is very much possible that different parts of the plants may develop newer cracks, newer effects of the wear and tear, so we and also the equipment has they become old many equipements may become less effective, may develop a larger threshold kind of margin and that is why; the operators operator should ensure continuous monitoring in order to avoid any such kind of oversight and it must; they must ensure that all the equipments are in perfect operating condition and are capable of giving the proper signal.

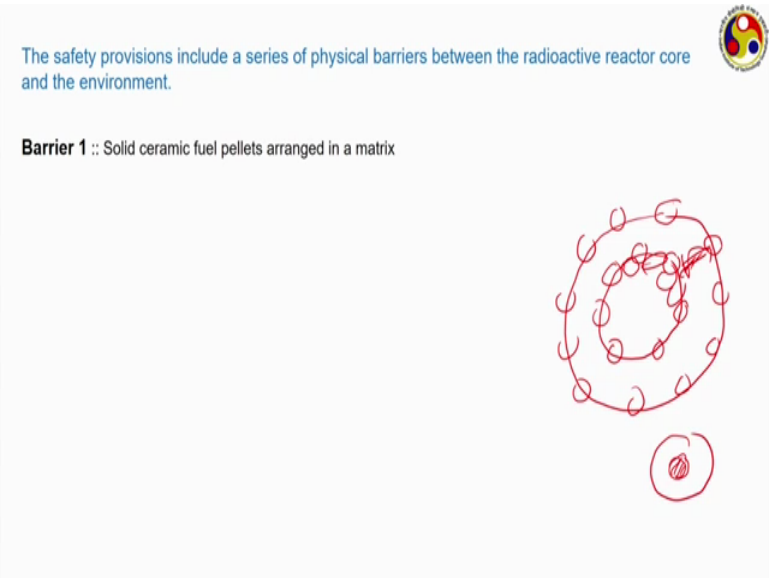
Like, we have seen yesterday, while discussing about the Chernobyl incident; it was a wall which was stuck, but the signal that never reached the operator or rather, when there was a light which was blinking on the main instrumentation panel or on the main control panel, which never indicated that the wall was actually stuck it does not been closed.

So, the operator was not able to discover it immediately, and which led to the following catastrophe at was the 3 mile island. But continuous monitoring is something by virtue of which we can avoid such kind a situtions. And the third aspects of defence in depth in short, this is also quite commonly referred as DiD. So, with the third aspects of this DiD refers to redundant and diverse systems to control damage, to the fuel and prevent subsequent radioactive were releases; this term redundant and diverse we shall discussing, but the; in short it refers to it need to have systems which are able to control damage to the fuel and prevent subsequent radioactive rays and also we must have provision to confine the effect of severe fuel damage or any other problem within the plant itself.

So, these are the three key aspects based on, which this entire philosophy of defence in depth defence in depth are revolves around prevention, monitoring and mitigating action. In nuclear power plant multiple and successive physical barriers are provided as a part of this DiD, which are able to or which theoretically should be able to prevent the leakage of any kind of radioactive effect to the surrounding; and the layers or the subsequent layers of, security of protection and in such that the failure of one layer should be mitigated by the next one by virtue of it is design features itself.

So, each layer has their own design features, and their subsequently strengthen to have; so that each level can serve one specific purpose.

(Refer Slide Time: 11:25)



The safety provisions include series of physical barriers between the radioactive reactor core and the environment. They are generally four levels of barriers in conventional reactor. The first barrier the soiled ceramic fuel pellets itself. Generally, the fuel pellets are arranged in arranged in some kind of matrix.

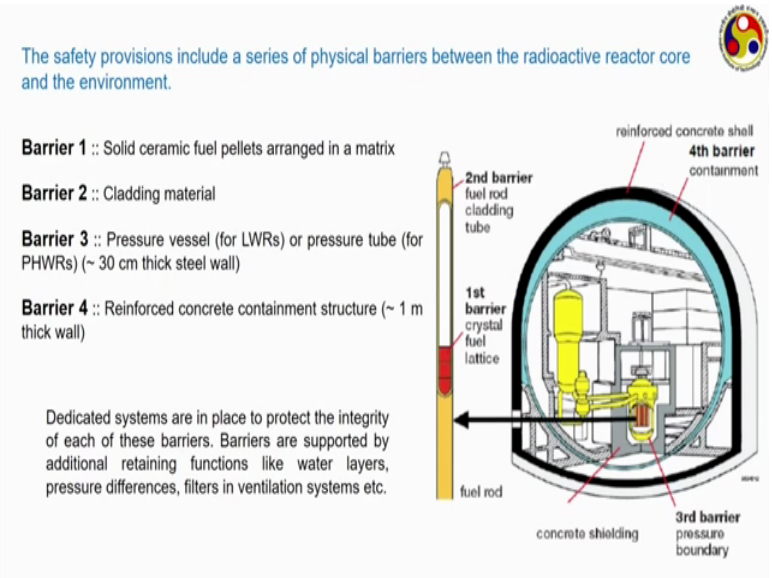
Like, suppose if you are having; sorry, this is in the correct way, if suppose you have thinking about fuel pellets with circular cross sections, you will always find that the fuel pellets are generally arranged in a matrix like this; somewhat like this this is one layer, then we can have several other layers around this number of fuel rods in each layer of course, will vary; so, that we have some fuels rods are arranging one circle, then another set of fuel layers arranged in a another circle, where the center is similar, but the diameter is larger, then you can have generally we generally have three such kind of circles which are and fuel number of fuel rod keeps on increasing as we go to circles of larger radius.

And now once this circles, which are formed of the fissionable fuel as the participate in the radioactive reaction, so it produces fission products and this fuel pallets of this fuel pins are and such that, the radioactive radioactive fission products, they are most likely to be bounded within this intermediate zones only or maybe just get stepped up somewhere here.

So, the first level of barrier is provided by the fuel pallets itself. It may also happen if you are talking about an individual fuel pallet, all the fissionable elements inside this particular fuel pallet or fuel rod are not participating in; fission reaction simultaneously, if may happen only the inner court participation fission reaction and therefore, all the corresponding fission products they get stuck inside this single fission elements or single fuel rod itself.

This is what refers to the as the first barrier, the ceramic fuel rods are the one most important contributor as a part of this first barrier. Next, question is what can be the second barrier, then after the fuel pallet what we have or after the fuel, that is the cladding and while studying the cladding, we have learned one of the functions of cladding is to prevent the release of radioactive fission products to the surrounding or to the cool and streams.

(Refer Slide Time: 13:44)



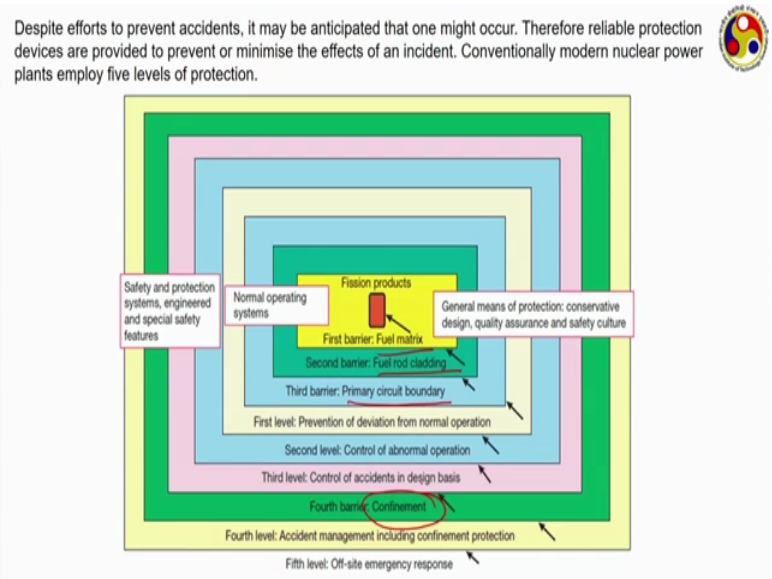
So, cladding provide the second level of barrier. Cladding can be made a zircaloy or magnox or in certain situation maybe or stainless steel. This being a stronger and generally in non permeable kind of metallic sheets, they are able to prevent the leakage of fission fragments quite efficiently. Third refers to the pressure vessel or pressure tube. Pressure vessel is pertinent to light water reactors like PWR or VWR where pressure tube type design, I hope you remember PHWR is something, that is a pressure tube type design and the corresponding walls for this pressure vessel or pressure tube can be very

very thick, like a pressure vessels conventionally have very thick steel wall having thickness of the level of the 30 centimeter.

So, that is the third level of barrier, which prevents the leakage of these fission products. And finally, the containment structure generally made of reinforced concrete which can be as much as 1 meter thickness. This is a typical diagram which shows all this 4 barriers, this is the fuel rod. So, the crystal fuel structure inside the fuel or itself founds the first barrier, then we have the second cladding, which is basically a jacket inside the around the fuel, then we have the third barrier the fuel rods are placed inside the pressure vessel as for this diagram and then this entire containment structure outside this black one, this is the containment structure which is the fourth barrier.

Of course, all these barriers or protection layers have their own dedicated systems to protect the integrity of their this barriers and barriers supported by different retaining functions like, water layer, pressure differences, filters in ventilation systems etcetera. But main objectives are being performed by these barriers.

(Refer Slide Time: 15:50)



Now, despite making all this a efforts, it is very much possible that is it is some fission products may come out of the reactor or because of some other reasons and they are may be accidents. And from whatever experience that we have about the nuclear reactors; now you are in a position to anticipate the types of accidents which may happen in certain power stations. And making use of those knowledge, reliable protection devices

provided to prevent or minimize the effect of any such incident and conventionally modern nuclear power plant implies along with those 4 barriers that we have discuss they also implies 5 layers of protection.

First protection of course, initially on the barriers that we have seen the first if you just go to the center of this particular picture, the first barrier is provided by the fuel matrix, then is the cladding and third is a primary circuit boundary. But before it encounters the fourth one, we can install the first level of protection. And the objective of this first level, which is given by this white line here or this white layer, the objective is just immediate just to protect the release of or protect the reactor against in the kind of accident scenario.

So, the objective of first level as written here is the prevention of deviation from the normal operating conditions. So, the first level tries to retain the reactor in the normal operating condition, which invariably is a critical one. Even whenever there is some changes say in the whenever there is some change in the operating conditions may be small change maybe a large change, this first level should try to get the system back to it is original position.

The second level, which is given by this particular layer here; it refers to the control of abnormal operation, if some of the first level fails, then the reactor cants sustain the normal operation, then it will go to the abnormal operation. Deviation prevention of deviation from the normal operation or just ensure that the normal operation is always running is a job performed by the first layer and the second layer accidently, if the nuclear product or has at all been informed, then this second layer ensures the control of abnormal operation and then a very important one, third layer which has first to control the accidents in the design level itself.

Again from our experience, we can for see quite a few different types of nuclear accidents. So, we can provide enough arrangement in the second level so that; even if there is may not be an accident, but even if there is small kind of deviation or the system is trying; system has deviated evict from the normal condition, that can be tackled here.

In the first level it tries to get the system maintain, the normal condition always. Like if there is say system is running is a critical one a critical reactor and now there is small, because of some change in any of the operating conditions the system becomes super critical say is reactivity has become positive by small margin, then the first level ensures

that; the reactivity tries gets back to the normal condition that it gets back to 0 and the reactors continues to operate as the critical one.

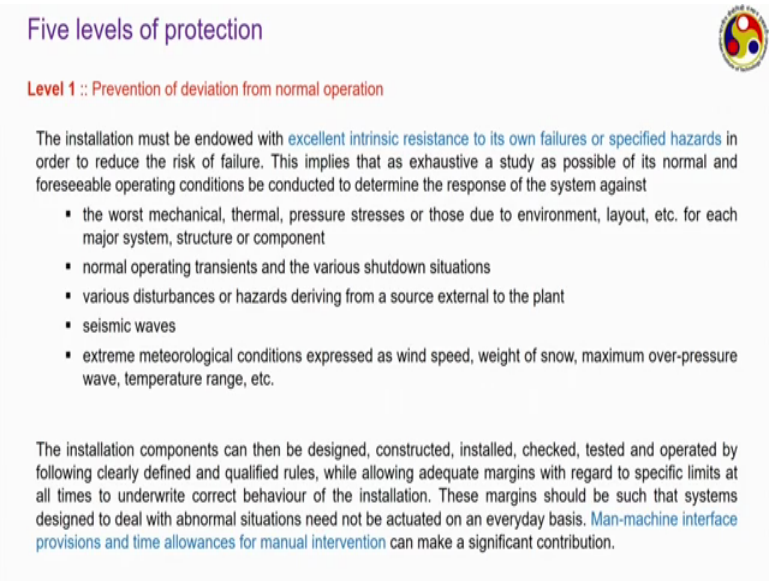
But, if sum of the first level fails, then comes the role of this second level. Now it is normal and abnormal operation it is rather abnormal, because the history will running as a supercritical one; so it has to provide provisions of getting a system back to the normal condition the third level where we have the accidents coming in. From our experience you already have idea what are the different kinds of accidents that we may find in a nuclear power plant. So, when both the first and second level fails it leads to an accident and that is why the third level has a provisions of controlling those accidents and get the system back to the normal condition again or at least get it back to such situations so that the second level can become active again, and then take care of the rest of the situation.

So, in this diagram the four level of barriers or four physical barriers that have talked about you can see this the fuel matrix, then we have the cladding, then the primary circuit boundary and here we have the fourth one, there is a confinement which does not allow the radiation to come out. But after the third level, when the even if the third level also fails, then we have a real accident situation and now we need to go for some kind of accident management technique, that is where the fourth level is, it is the outermost layer of protection in a nuclear power plant, which looks at the active which looks at the accident management including confinement protection.

And finally, the fifth level; which is the which refers to very very severe accident, which where even none of the previous four levels are able to take care of, then oxide emergency response system needs to be activated to prevent just spreading of radio activity for away from the plant itself. Preferably limit that will the plant itself.

So, we conventionally can have 5 layers of protection in defence in depth.

(Refer Slide Time: 21:25)



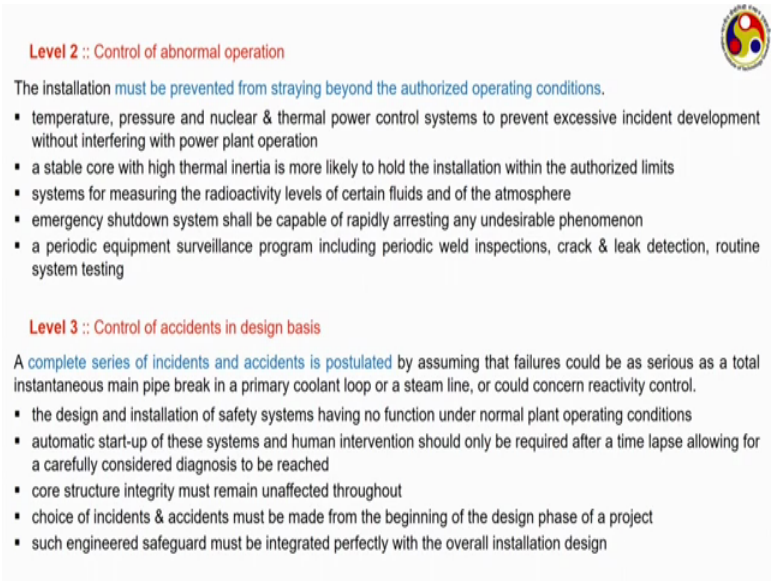
The first layer of protection refers to prevention of deviation from normal operation. The installation must be endowed with excellent intrinsic resistance to it is own failures or specified hazards, in order to reduce the risk of failure. So, in the first level itself, we have to provide options. So, that the system can always get back to small deviation or small amount of failures; this implies that an exhaustive study as possible of it is normal enforceable operating condition we conducted it which of the response of a system against different kind of scenarios; such as the worst mechanical thermal precious resource the system may encounter, because of environmental issues, because of it is layout for each major subsystem structural component.

It also in considers the normal operating transients in the various shutdown situations, various disturbances hazards a deriving from a source external to the plant. The seismic weaves can also in to be considered if that at all we consider relevant to the corresponding location. And the extreme meteorological conditions express as wind speed, weight of snow, maximum over-pressure wave temperature range etcetera.

So, considering all these aspects we design the level one; so that the system is able to continue or maintained it is critical condition or the at least the desire operating condition. The installation components can then we designed, constructed, installed, checked, tested and operated by the by following the clearly define and qualified rules, which while allowing adequate margins it regards to specific limits at all times to

underwent correct behavior of the installation. Adequate margin must be provided to which regard to specific limits at all times undergo contract, undergo correct behavior of the installation. The margins have such that the system design is design to deal with abnormal solutions the actual need not be actuated on over day basis or on a daily basis.

(Refer Slide Time: 23:31)



Man-machine interface provisions and time allowances for mutual; sorry; manual intervention in the second level, it must be prevented from straying beyond the authorized operating condition. The temperature, pressure and nuclear and thermal power control system are installed to prevent excessive incident development without interfering with power plants.

A stable code with high thermal inertia is more likely to hold the installation in the authorized limit, like high thermal inertia refers to which are given heat load the temperature raise of the system will be smaller. And once you can ensure that; then the system can limit is temperature change within it is very very short range and also if the core itself is stable, then resistive will not rush; core itself is a stable in the system a yeah will last and this I will be able to get back to the abnormal condition.

The systems for measuring the radio activity levels for certain fluids and on the atmosphere must also be installed, and emergency shutdown system shall be capable of rapidly arresting any undesirable phenomena. Finally, a periodic equipment surveillance program, like we had in the previous case also in level 1; equipment surveillance

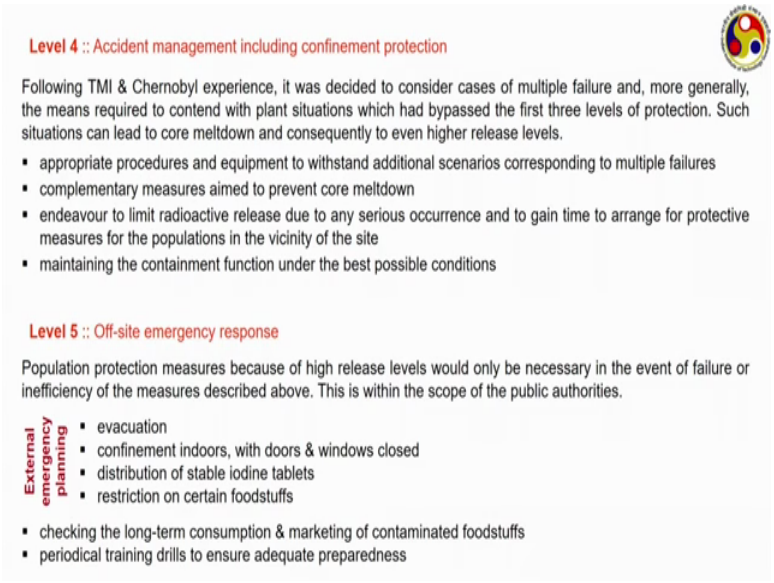
program are including periodic weld inspection, like crack leak detection, routine system testing etcetera.

So, by virtue of by applying these methods, we can control we are we are at least try to control the abnormal operation, but when both level 1 and 2 fails; we come to level 3, which must control the accidents have design level. A complete series of accidents and incidents are postulated while designing a nuclear power plant and taking the corresponding data only the final a designs are drawn.

The design and installation of safety systems having no function under normal operating conditions, that is the safety systems that we are going to install under this level 3; they may not be functioning at all during a normal power operation. Automatic start-up of these systems are essential and human interface should be required after after a time gap, which will allow a careful constitution diagnosis to whether diagnosis should be reached.

The core structure integrity must remain unaffected throughout and the choice of incident and accident must be name from the beginning of their of the design phase of a project. Such engineered safeguard must be integrated perfectly with the overall installation design. So, the equipment, which are installations which comes under this third layer, they should be able to subside all those design level accidents, that is the accidents, which we can for see and therefore, they are concerned effect has been considered while designing the system itself.

(Refer Slide Time: 26:17)



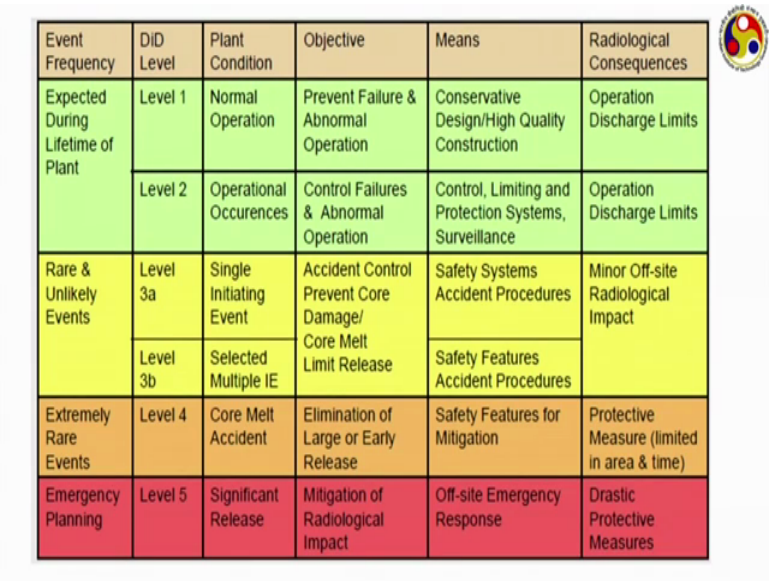
Fourth is accident management including confinement protection, this is a more like the final result or final barrier, which will not allow the release of radioactive surrounding; falling TMI Chernobyl experience it has decided to consider cases of multiple failure and more generally the means required to contained with plant situation, which are bypassed the first three levels of protection. Such situation can lead to core meltdown and consequently to even higher release rate.

So, to counter that we need have a appropriate procedures and equipment to withstand additional scenarios corresponding to multiple failures, complementary measures aimed to prevent core meltdown. Endeavor to limit radioactive release due to any serious occurrence and to gain time to arrange for protective measures for the populations in a vicinity of the site. And of where the role of the authority also comes into play, because it is not possible for the plant authority to evaporated decided to move people from particular location, but only the local governmental authorities or maybe the governmental bodies can only evacuate a particular location.

Maintaining the consignment means function under the best possible condition. And first is off-site emergency response it refers to an all the four levels as failed. So, radioactivity as started to go outside the reaction zone and then we have a role of this level 5, population protection measure; so the public authorities can help in evacuation of the local site, confinement indoors with doors and windows closed, distribution as stable iodine tablets, it can also instruct on the restriction on conservation and selling of certain foodstuffs, which can get radioactive; which can radioactive very very quickly.

These 4 factors that is evacuation, confinement, distribution of iodine tablets and restrictions are together known as external emergency planning, but there can be long term effects as well, or long term planning I should say like checking the long term conversion and marketing of contaminated of foodstuffs and periodical training drills to ensure adequate preparedness.

(Refer Slide Time: 28:30)



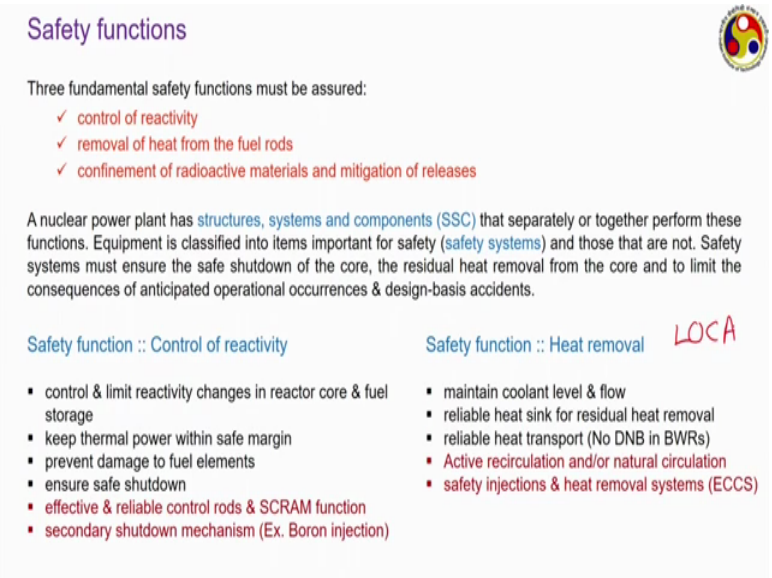
Event Frequency	DiD Level	Plant Condition	Objective	Means	Radiological Consequences
Expected During Lifetime of Plant	Level 1	Normal Operation	Prevent Failure & Abnormal Operation	Conservative Design/High Quality Construction	Operation Discharge Limits
	Level 2	Operational Occurences	Control Failures & Abnormal Operation	Control, Limiting and Protection Systems, Surveillance	Operation Discharge Limits
Rare & Unlikely Events	Level 3a	Single Initiating Event	Accident Control Prevent Core Damage/ Core Melt Limit Release	Safety Systems Accident Procedures	Minor Off-site Radiological Impact
	Level 3b	Selected Multiple IE		Safety Features Accident Procedures	
Extremely Rare Events	Level 4	Core Melt Accident	Elimination of Large or Early Release	Safety Features for Mitigation	Protective Measure (limited in area & time)
Emergency Planning	Level 5	Significant Release	Mitigation of Radiological Impact	Off-site Emergency Response	Drastic Protective Measures

These are the all 5 task put together. Expected during the lifetime of a plant we can we it; those event which are expected to a lifetime of a plant; a it falls under the level 1 category and plant can contribute to normal operation and when it falls during in the faulty zone it comes under level 2 category, which has allows operational contribution. Second that is the third level is very very rare and unlikely event.

It happens to the safety systems or it is mitigated by university safety accident protections extremely rare event the level 4 event, before indicates or results in melting of the co material and frequency of extremely large or early protective measures like, limited in the area and time need to be provided, because these are long term effects falls under level 4; and enough safety features need to be ensured. And finally, the emergency planning which suits the level 5 at least two significant release of radioactivity the surrounding areas and mitigation of radiological; in fact, is generally the objective of this particular level on the drastic protective measures are essential.

Now, the safety functions; all the safety features that we install or insist in a plan, they generally falls under three categories or that generally three measure of feature; one is the control of reactivity. So, whenever there is a change in reactivity the safety features should get it back to the desert level immediately; otherwise are reactor will just because of this multiplication factor, it will immediately grow or decay quick next removal of heat from the fuel roads.

(Refer Slide Time: 30:11)



The rate at which fission heat are getting produced inside the reactor at the same rate heat must be remove, because even if there is some loss in the coolant side results in smaller amount of coolant flow immediately; there will immediately increasing the temperature of the; immediate increase in the temperature level of the coolant, then desert and that can quickly rate to the overheating of the entire reactor core and final the confinement of the radioactive materials and mitigation of releases.

To attain all this fundamental safety fissions, the structure systems and components, which are together known as SSC that separately or together acts with the and accordingly the equipments are classified based on the importance of safety, and or rather I should say the equipments which are required to ensure the safety, that is which has relation with any of this three of safety functions and equipments which are not at all related to safety.

Safety systems must ensure that the safe shutdown of the core residual heat removal from the core and the consequences of anticipated of operational occurrences and design basis accidents taken care of. Here, I would like to quickly mention about this residual heat removal; any amount of heat generation in the reactor that needs to remove, that is true for coal based thermal power plant as well, but there when the coal is bonding have the energy available and the coolant is take that energy, but once the coal has bond, then

there is no energy potential available, but that is not true for the nuclear like, when uranium undergo fission; it releases large amount of energy.

But, the products of the fission they can also be radioactive in nature and therefore, depending upon their respective half lifes it can keep on releasing energy or a very long period of time, that is; that is why the energy that is released, because of the action of prompt neutrons that is definitely important, but from safety point of view the energy release because of the action of the delayed neutrons are much more importance, because that is something which is related to this decay heat or residual heat.

Now, to have the safety function for control of reactivity need to have ensured that the reactivity is limited in the reactor for core and also in the full storage plant, the thermal power kept to the safe margin and the damage to the fuel elements must be prevented. It also ensure safe shutdown of the reactor, whenever that is desired.

So, to attain that we need to provide effective and reliable controllers and SCRAM function; whereas there can be a secondary safety shutdown mechanism also, like injecting boron, if you want to have a very quick shutdown of BWRs, then we can inject large quantity of boron which can because of it is high neutron absorption cross section it can eta all the available neutrons; whereas when you talking about the heat removal, then the coolant level and flow and must be means then inside the reactor because any decreasing the flow rate will just as I mentioned will result in overheating of the plant.

The heat sink for residual heat removal should be very much reliable. The heat transport system should very reliable, that is; particular in boiling water reactor, where there is face change involved during must ensure that the operation is limited in the nuclear boiling zone, the reactor is never able to go in the DNB; that is departure from nuclear boiling or flame boiling zone; which can lead to particularly following the critical it was there will be a subsequent or I should say substantial decrease in the heat transfer coefficient. So, the heat transfer system must be reliable to ensure the absence of this DNB in BWRs.

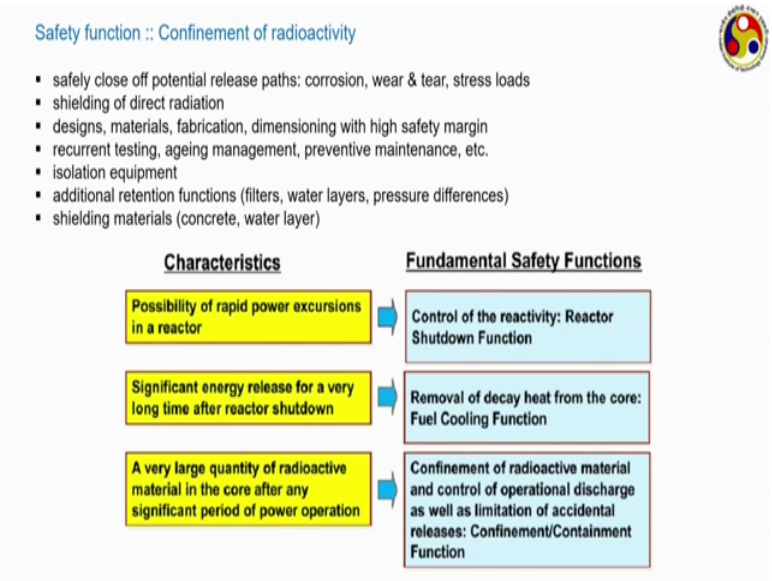
The this functions can be achieved by actively recirculation and the natural circulation, safety injections and heat removal systems, like in this particular contexts; I would like to mention about what happened in this Fukoshima power station. Fukoshima power station of course, it has their it is own the Daiichi power station basically; it has it is own

issues it was a very old planned running for more than 40 years and therefore, all the safety measures were not the most advanced one, but still that accident that happened that was a result of some kind of misfortune for them; because you know that the tsunami has struck that time; just before the accident happened Japan was (Refer Time: 34:39) Tsunami.

And because of that tsunami power grid that failed; so there was no power available in the reactor or I should say in the nuclear power plant and, because there is no power available. So, the coolant circulation pump coolant recirculation that stopped working. And so there was no coolant that was flowing. So, the reactor core and hence, but the reactor core despite all the effort it tried it controls to produce fission it and they were not able to provide me and arrange for any additional power. They had some kind of backup generator, diesel generators; unfortunately, because of the tsunami those also went under water and they are not able to start the pump.

As they did not had any kind of natural circulation kind of background such kind of acid mechanism that did not had so the that lead to LOCA, that is loss of coolant accident; no coolant were there in the plant and hence it led to the meltdown of the entire reactor core, that is why the newer generation; three generation three onwards they are ensuring this passive recirculation system employing natural circulation; of where even in the absence of any kind of prime mover any kind of electrical sources the fluid will always be flowing using the buoyancy force.

(Refer Slide Time: 35:58)

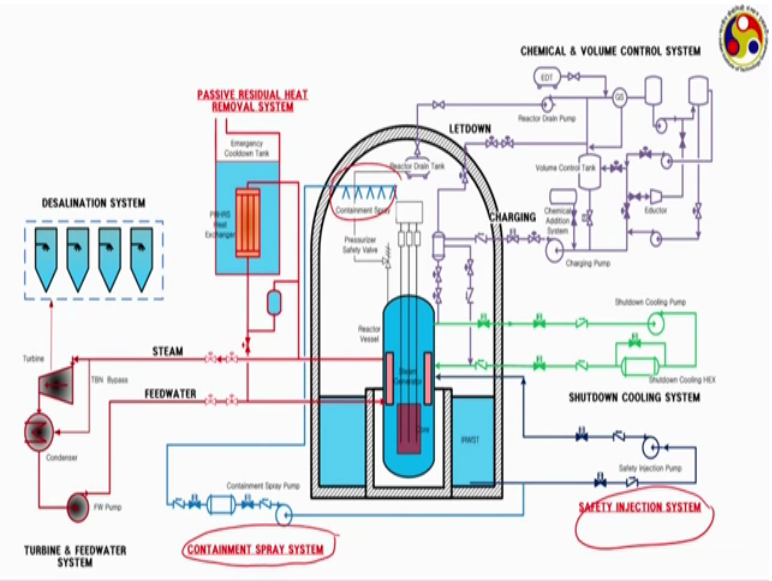


So, the confinement of radioactive, generally refers to first we have to close the all potential release path like, corrosion wear and tear the against kind of stress load, shield must be providing direct radiation, designs, material, fabrication, dimensioning with high safety margin and any kind of all kind of recurrent testing, ageing management, preventive maintenance, etcetera should be done; And finally, isolation equipment ok.

We also can have additional attention functions like filters, water layers, etcetera which can lead to the rate confinement of reactivity. And shielding material of course has to be there. There are several levels of shields which are provided inside the around the reactor like made of concrete, we can have water layers you know water is has a reasonably high neutron absorption cross section, it can absorb neutron thereby avoiding or providing a way of reducing reactivity inside the core.

This are the fundamental three characters that I mentioned. First and the three aspects of DiD, possibility of a rapid power excursion in a core, it should be control; we should have control of the reactivity and reactor shutdown functions, and other two corresponds to the other functions that I have just mention.

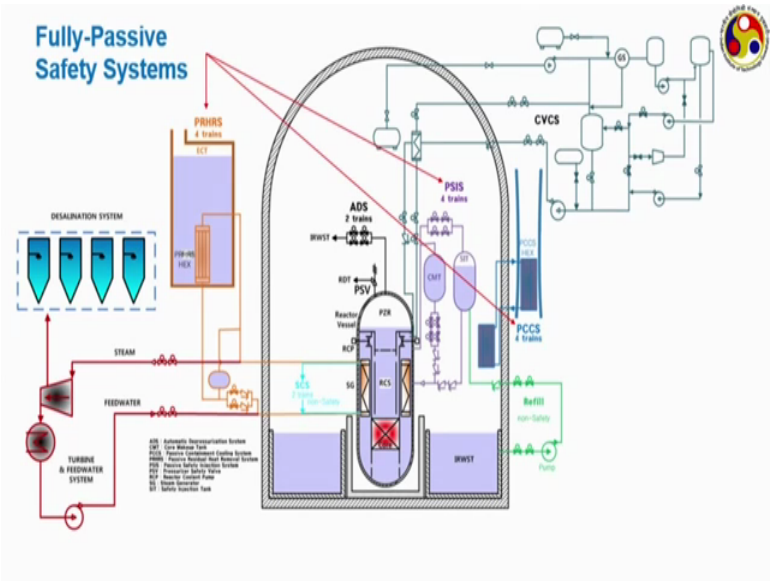
(Refer Slide Time: 37:14)



This is the schematic view of one power station; power station of where, we have a several passive safety systems are installed.

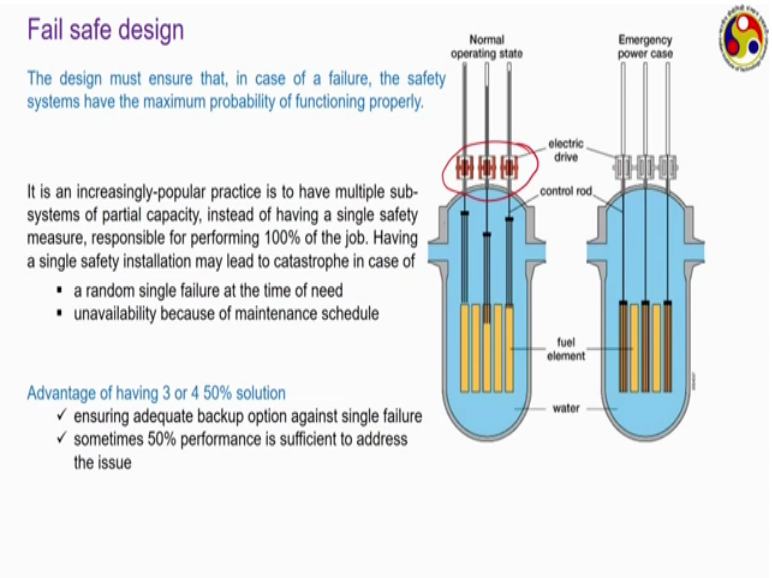
Like we have the safety injection system, then we have this confinement spray system, these are additional system. This is also a confinement spray here, which is coming from the specific heat removal system. So, using this spray and some other means; I can fight other means the safety these 5 layers are safety and ensured.

(Refer Slide Time: 37:46)



You can see this is another diagram, which has implemented fully passive safety systems, it was a natural circulation and also their quite of you others fully passive safety systems.

(Refer Slide Time: 37:57)



Next is the fail safe design the strong came earlier; so fail safe refers to fill the instrument that you are providing for safety for ensuring safety; in case of failure the system must act or it has a maximum possibility of functioning properly.

It should not fail, otherwise I will be catastrophic because of we are dependent on this kind of safety equipments to ensure the maximum probability of functioning. Like you can see this diagram this for control rods, these are a normal operating condition, control rods are nearly taken out of the reactor, there completely removed and their hold in this position using some kind of to be electrical right.

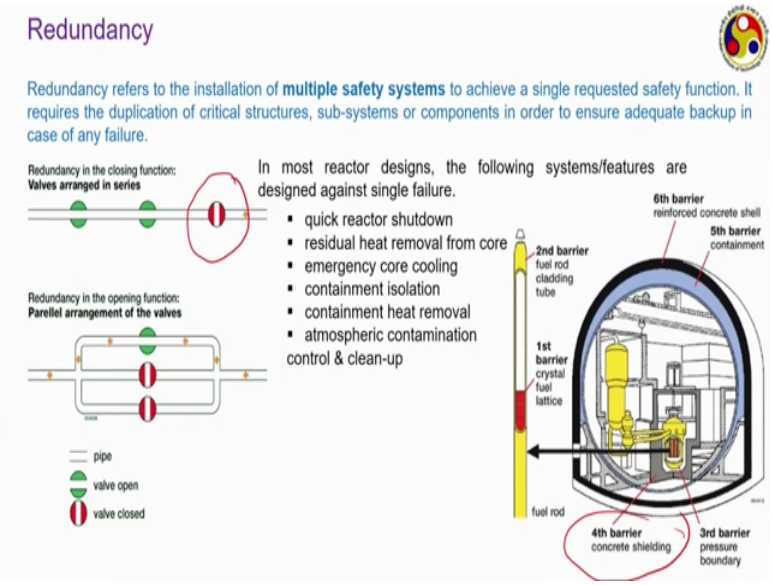
Now, if there is some kind of SCRAM situation that we have to suddenly close this reactor core, then you have to deactivate this electrical drive and then only the using some kind of other means; we can get this control we can completely using various scram, we can insert the control rods using this electrical drives, but also we can make use of the gravitational force; like in this design controllers are located at the upper position of this reactor shell. And therefore, if you just allow them under gravity they will fall down till the maximum lowest possible fission there by allowing the scram.

So, we are making use of a natural phenomenon disgravity, and hence that is some kind of failsafe design. The recirculation using natural circulation is also a failsafe mode of operation. It is an increasingly-popular practices to have multiple sub-systems of partial capacity, instead of having just a single equipment like if you are providing a single equipment we was protection complete protection against something.

So, instead of having one equipment, which is capable of providing complete solution or a complete protection; nowadays the reactors are having 2 or 3 or 4 smaller systems each having say 50 percent capacity or like that and having just a single system may lead to catastrophic event, because it may happen in the time of need the system fails as it may be required to operate very very rarely; so there may not be proper maintenance and the equipment failed at the time of the need.

Secondly, unavailability because of maintenance schedule. So, under situation; so to avoid that we can have multiple subsistence, like having if we are having 3 or 4, 5 a systems with 5 percent solution, then we are ensuring that adequate backup options are there again single failure and also some cases we were 50 percent performance is sufficient to address the issue.

(Refer Slide Time: 40:36)



So, is no point for all the control rods to get activated then comes around redundancy; it refers to installation of multiple safety system to achieve a single objective; that is to have perform one kind of safety features, we are installing multiple devices just to ensure

this is something that released redundancy like, if our objective is to close this valve; sorry close this pipeline using the valve this gives and greens are the normal valves here you can see instead of 1, we have put 3 valve; so that at least one of them will operate.

So, this is the valve in a closed position. So, if all three operates that is fine, but even if the drive mechanism for the first one and also for the second one fails, we still have a third one this third valve will operate or we have to operate this third valve protect the system ok. When you are looking to have the valves in open situation, then we can put the valve; we can have line open situation to have the floor we can put these valves in parallel and even if at least one of the valve is open there will be flow through this circuit.

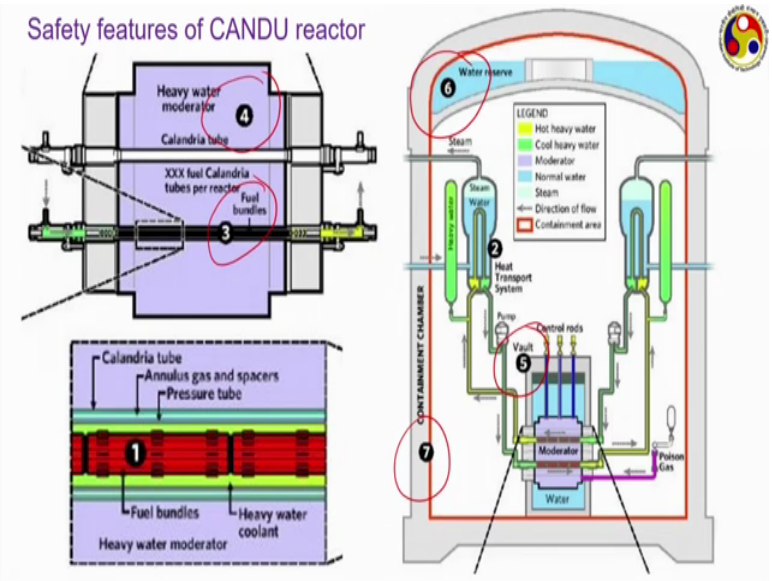
So, this is what you call redundancy in both this cases just the function that would have been done by the single valve we have putting three valve just to ensure that at least one is operating.

The same is referred by the redundancy. In most reacted designs, the several systems are used against the like, the quick reactor shutdown system of from very fast shutdown system, residual heat removal from core, emergency core cooling, continental isolation, containment heat removal, atmospheric contamination control and clean up all this for all this possibilities we have several equipments in the plant I a.

Like you can see in this diagram, these are similar diagram that is I shown out or earlier about the physical barriers here instead of 4, you having 6 barriers; like 1, 2 and 3 remains the same, but now I have a concrete shielding around this lattice structure of fuel and then we have the reinforce concrete shell outside and then this contamination barrier, which was always there.

So, we have refer; we reformist or reinforce rather concrete shell, which has been provided to provide what case additional barrier for safety.

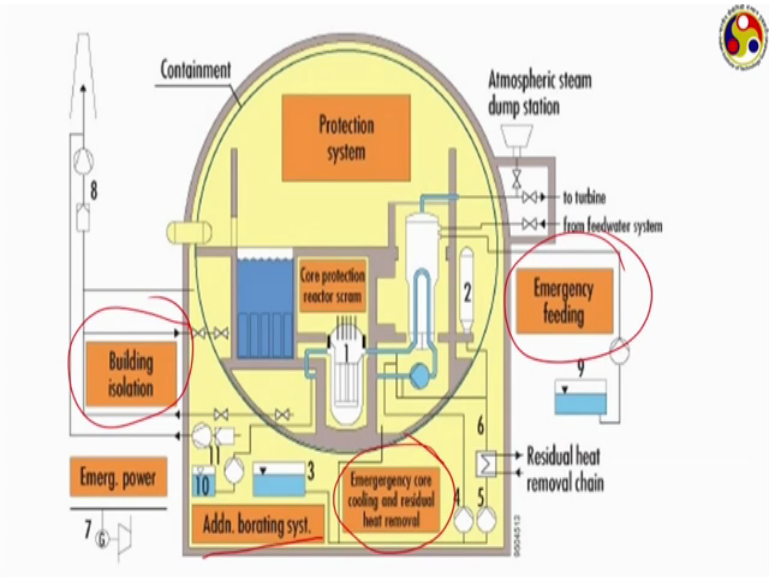
(Refer Slide Time: 43:00)



CANDU features reactor I hope you remember the name Canadian deuterium uranium, which is also the most of the PHW words in India of CANDU time. So, the CANDU reactor has several essential design features of safety features; like this heat transport system is a safety features under any situation this heat transport system will provide heat thereby it can also remove the decay heat if required, then this is zoom view of this particular portion.

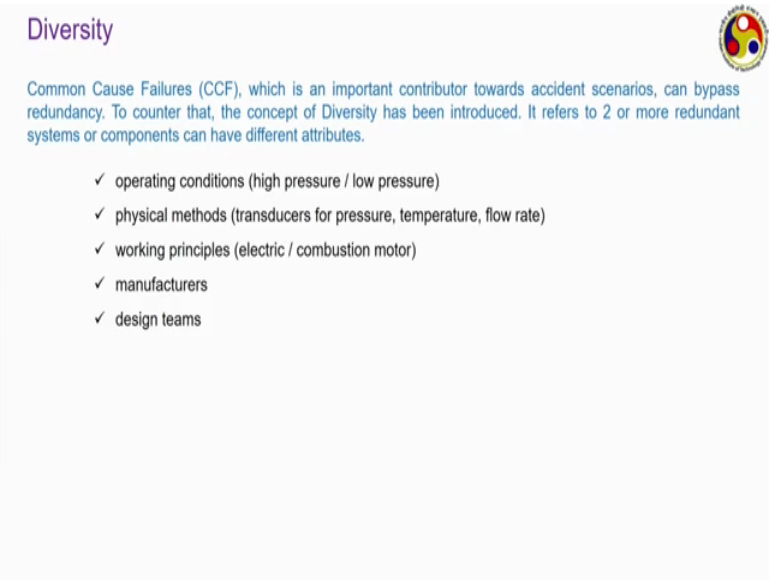
Here, we have this fuel road bundles fuel not able to core fuel rod bundles which are able to restrict the or will not able to not allow the fission products to go outside, then this a moderator in the calendrial large volume of moderator kept so that can always absorb huge amount of heat, then this number 5, there is a valved; a concrete valved around this calendria, then we have a water reserve here which can always be used if some additional heat load is present and finally, the containment chamber. And this is the modified view of this fuel bundles here the, this is the fuel pallet, which provide the first layer of barrier.

(Refer Slide Time: 44:26)



This is another diagram for another reactor you can see there are additional borating system, we can provide additional boron to reduce the reactivity inside the core, we have this emergency core cooling system and residual building we have the building has been isolated or building isolated system require the building can be isolated; the emergency feeding system these are all part of different layers of protection. And these are all mostly to meet those three objectives, that is restricting the reactivity, removing the heat and containing the radioactivity.

(Refer Slide Time: 45:06)



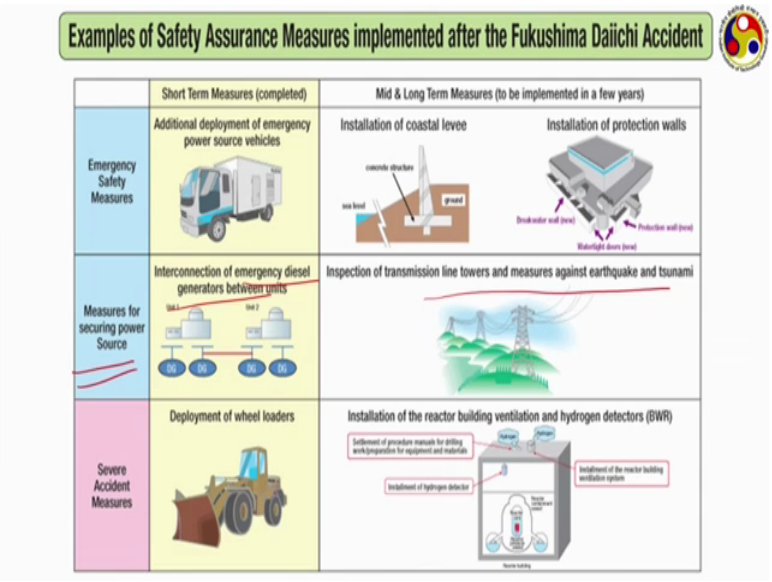
Next is diversity it is possible that, if all those components used under redundancy of similar kind, then for the same reason all of them a or a particular kind of failure may

bypass all of them who is something if it is a common cause failures which is an important contributor to our accident.

So, it is for the if all corresponding equipments are of similar type, then none of the may be able to detect this kind of equipment, that is; why you need to use diversity, that is; different equipment under the for serving the same purpose can be of different kinds may have different attributes such as different operating pressures can have different physical methods of operation like, transducer based or mechanical based. The working principle electrical, combustion motor based, manufacturers can be different for the same equipments because each manufacturer would be provides their own features.

So, while the equipment broadly is the same actual there can be quite major differences. Similarly the design teams also the same equipment same system design by two teams will be having different attributes and different features, thereby ensuring the diversity. This is a one schematic or one picture, which shows the different kind of action that has been ensured in this and Daiichi power station which falls under both redundancy and diversity.

(Refer Slide Time: 46:31)

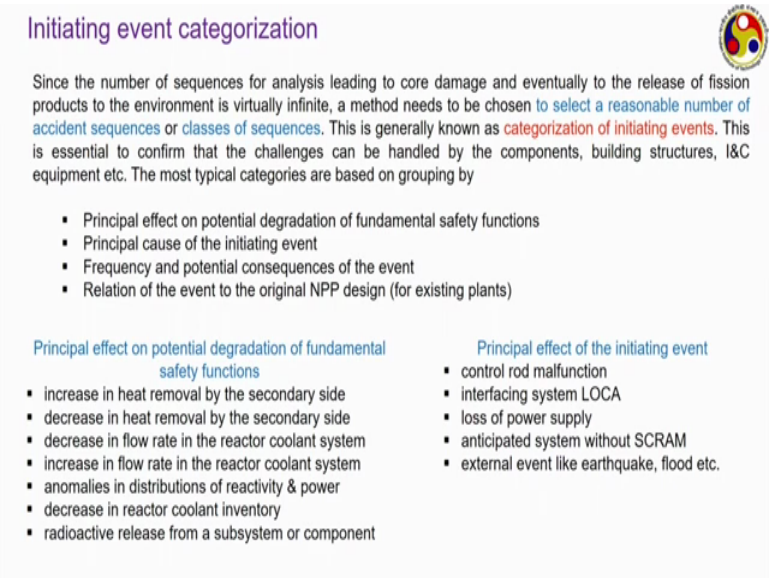


Like the emergency for emergency safety measure the short term and option additional deployment of emergency power source vehicle; like what the; it a loss the power so they are providing additional power source vehicles also they are providing coastal areas, which long term objective and is special protection valves. The in order to secure the

power source, they are using the interconnected emergency diesel generator between units, and also inspecting the transmission line towers in measuring earthquake and tsunami; which is a long term objectives.

The severe accident measures deployment of fuel loaders can be an option, but installation of the reactor buildings, ventilation, hydrogen, detectors or detectors can be particular in BWR type can be another option. So, for serving the same purpose; we are using defined or we can use different kinds of mechanism, which falls under this diversity.

(Refer Slide Time: 47:35)

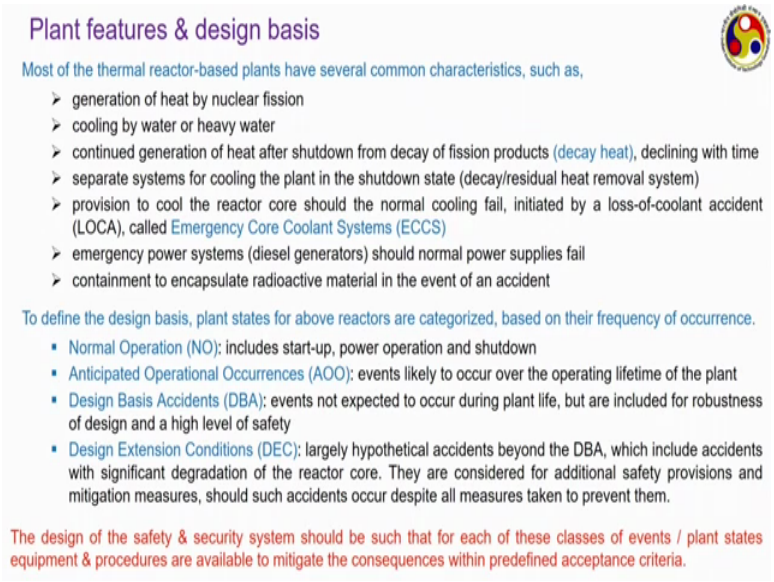


Then initiating event characterization; the reason for which this entire series of events during accident that happens; it is important to categorize those initiating events as well. Because, the challenges that can be handle by what kind of challenges that we are going to face and how that can be handled by using which kind of component or equipment that is; then accordingly the depending upon the initiating event or most typical categories are like principle effect on potential degradation of fundamental safety functions, which can be increase in heat removal by the secondary site, decrease in heat removal by the secondary site.

Similarly increase or decrease in the flow rate in the coolant system anomalies in distribution of reactivity and power, decrease in reactor coolant inventory and reactive release from a subsistence or components.

Another principle type can be based upon the initiating event. The control rod malfunction we can have initiated by interfacing LOCA; loss of power supply can be another reason, anticipate system without SCRAM external events like earthquake and flood all these are going to have different kinds of effects. Finally, come to the planned features and design basis; it has been found that all those plants which are based up on thermal reactor like the PWRs, BWRs, PHWRs they have several common features.

(Refer Slide Time: 48:57)



Both from normal operation and safety point of view; like their source of energy comes from nuclear fissions, then they are cooled by some kind of liquid, which is water or heavy water they continued to generate heat even after shutdown, because of the decay heat which of course, keeps on declining which time separate system for cooling the plant in the shutdown state to remove the decay heat.

Provisions to cool the reactor core should be normal should the normal cooling fail, we must have as backup as emergency core cooling system and the emergency power systems like diesel generator kind of options so, if the there is failure of the normal power. So, these are the features that you will find in all the plants; like also confinement incomplete radioactive material in the event of an accident.

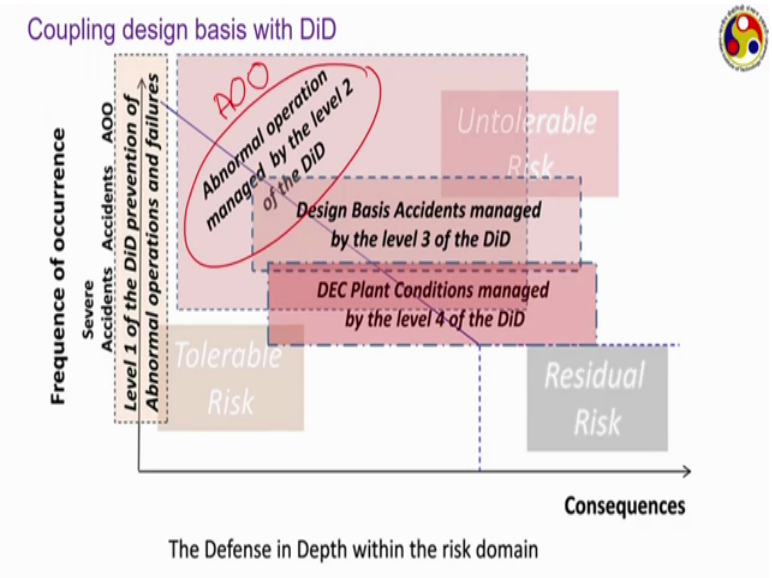
And so, as their design features are quite similar from safety point of view so, we can treat all of them as just a single group and then, we go to the design basis to define the design basis the different states of a plant needs to be categorized based upon their

frequency of occurrences; first is NO normal operation, which is the normal startup operation and shutdown. Next is anticipated operational occurrences AOO; in this refers to the events which are very likely to occur during the lifetime of the reactor.

Then design basis accident DBA events, which are not expected to occur during the lifetime, but are included for robustness of design and a high level of safety and are if design extension of conditions, this is refers to the large scale accident quite severe accidents these are generally hypothetical accidents designed beyond the DBA which include accidents with significant degradation of the reactor core.

The design of the safety and security system should be such that; they all these classes of a plants states can be taken care of by the equipment and procedures within and the plant operation should remain within the predefined acceptance criteria.

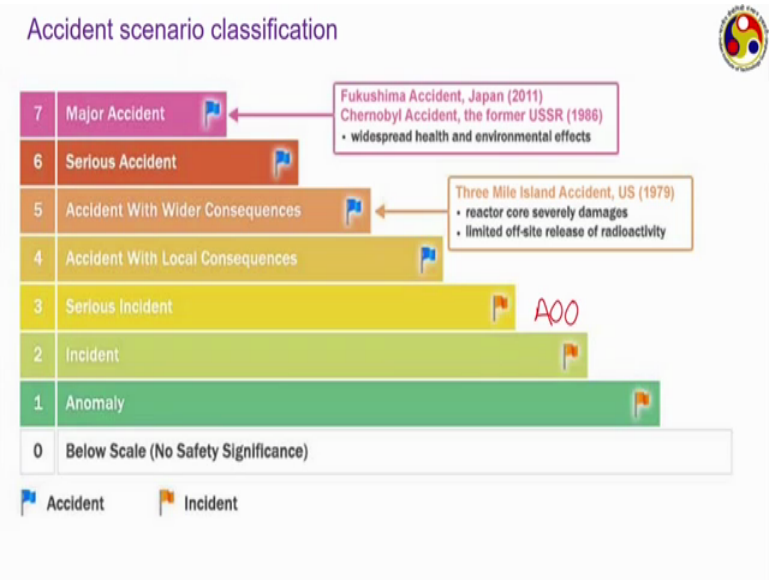
(Refer Slide Time: 51:08)



If we coupled this design basis with the design in depth, then you will find the label one is for abnormal operation and failures. The abnormal operation is generally manages by level 2 abnormal operation means here will able to by AOO. AOO refers to only minor version from normal operating conditions, which are always expected during life of the plant and near general taken care of by the level 2 (Refer Time: 51:36) NO the normal operation is not an accident conditions we do not need any kind of protective layer for that, but the second one AOO is taken care of by the second layer second level.

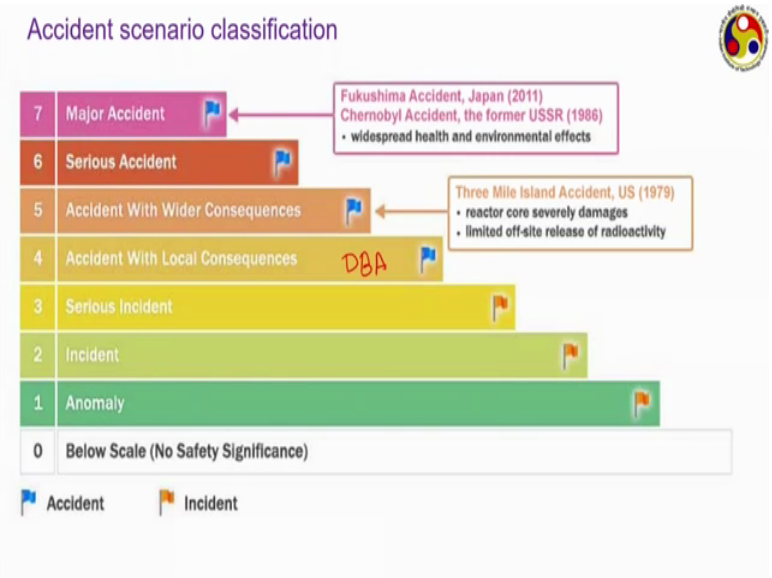
Then DBA are taken care of by level 3, where as if DEC at all happens very unlikely; this refers to only very very severe situations like in Chernobyl, then we have the level 4 and level 5 if required. Of course, as the level of this accident that goes on a there is from AOO to the DBA to DEC the amount of consequences that keeps on increasing and in certain situations it becomes un tolerable.

(Refer Slide Time: 52:16)



And in this like; just I mention this accidents; or this different kind of scenarios in nuclear power plant can also be put in this classifications of accidents scenario Here a 1 refers to very minor normally something which actually is taken care of by level 1 even level; in the second one this scale two incident you also can be taken care of by level 1; level 3 refers to serious incident with something in the range of AOO, which can be taken care of by the third layer and rather which falls under this scale 3; so, the scale 0 to 3; they falls under this category of incidents; we do not call them accident in this, but once it is above 3, then that is very much and accident like a 4; 4 is an accident with only local consequences.

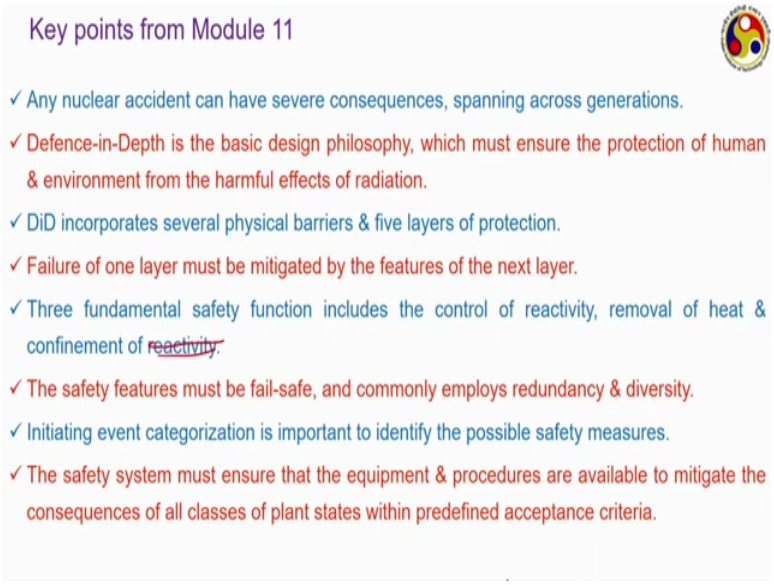
(Refer Slide Time: 53:08)



So, this is where DBA starts to come into picture 5 is accident is much bigger consequences three mile island accident is an example of this level 5, where the reactor core possibly damaged and radioactivity was also released, but that was limited level 6 is must serious accident and level 7 is extremely severe accident such as in Chernobyl or in fukushima power stations. In fact, these are the only two examples of level 7, nuclear accident and three mile island is only major incident to fall under level 5 level 7 refers to something kind of accident which relates to widespread health and environmental effects.

So, depending upon what kind of I should say when we are in this category these are level 4 and level 5 designs of DiD are generally for this for as level one is capable of taking care of this one itself. This is generally for level 2; level 3 can take care of this kind of situation and level 4 and 5 or for larger layers like level 4 and 5 can take up from this particular point onwards. So, depending upon what kind of accidents happening and several other factors as we have seen today we can we need to have different kind of safety arrangements and all those can be defined under those five layers of protection this takes as source the to the end of this particular module.

(Refer Slide Time: 54:40)



So, in module 11 we have seen that any nuclear accident, can a several consequences spanning across generations.

Because of the genetic mutation which may lead to the DiD is the basic design philosophy, which must ensure the protection of human and environment from the harmful effect of radiation commonly DiD incorporate 4 layers of physical barriers and 5 layers of protection; number of physical barrier can be even more it can be is 5 or 6 also starting from the fuel pallet to the outer containment structure failure of one layer of protection must be mitigated by the features of the next layer three fundamental safety function includes, the control of reactivity removal of heat and confinement of reactivity it is wrong confinement of radioactivity should be safety features multi failsafe and commonly employees redundancy and diversity you have to increase the stability of this security system.

Passive safety features should also come under this category initiating event characterization is important to identify the possible safety measures and finally, the safety system must ensure that the equipment and procedures are available to mitigate the consequences of all classes of plant states within predefined acceptance criteria.

So, this takes us to the end of module number 11; here we have seen different philosophies of reactor safety modern reactor safety general design in depth is the main philosophy it which provides or which in covers 5 layers of protection we generally

would like to receive the plant up to layer 2 or in the worst case layer 3, layer 4 is something that corresponds to very very severe experience in the level of Chernobyl. There are different ways we can relate the design to this DiD concept like, I categorizing the initiating effect categorizing the accident and several other kinds of situation.

Several other kinds of situation categorization as well, but overall a plant must strictly ad where to this design philosophies in order to ensure the utmost protection of human being and also the environment against any kind of ionizing radiation. So, thank you very much for your protection keep posting your comments; I would shall be very very happy to respond to your queries and you have just one more week to go in this particular course. So, see you in the next week bye.