Indian Institute of Technology Madras
Present

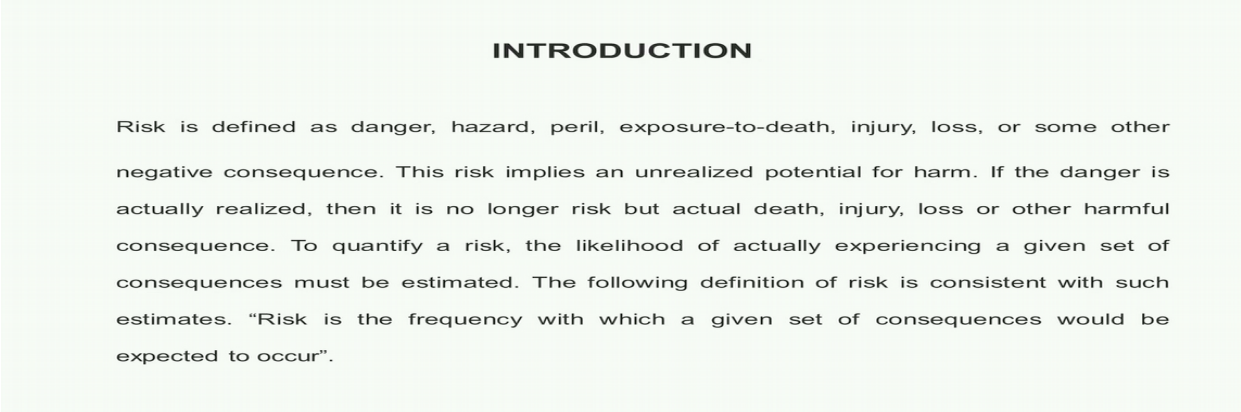
NPTEL
NATIONAL PROGRAMME ON TECHNOLOGY ENHANCED LEARNING

NUCLEAR REACTOR AND SAFETY
AN INTRODUCTORY COURSE
Module 06 Lecture 02
Risk and Probability Safety Analysis (PSA)

Dr. G. Vaidyanathan
School of Mechanical Engineering
SRM University

Good afternoon! In the last lecture, we touched upon the safety analysis, the safety approach, we talked about the deterministic approach, and how do we go about identifying the different events and how do you do a deterministic analysis. In this lecture, I would give you some ideas about the probabilistic safety analysis or sometimes also called as the risk safety analysis.

(Refer Slide Time: 01:04)



Now what is risk? Risk can be defined as a perceived danger, could be a perceived injury, or something of some negative consequence that is risk. So in another word, you can say it is an unrealized potential for harming that is a risk. But if suppose the danger is actually there then there is no question of risk; it's actually when that happens injury or death anything can happen. But we need to quantify the likelihood, the chance. So we tell we or we define risk as a frequency with which given consequences could happen. So that's what we give risk. With reference to risk, I can you give you a very simplest example; traveling on the footboard of a bus, most of our buses are crowded and in the busy office time, you don't get space, you have to hang on. Yes, now what sort of risk? You are hanging, maybe your hand grip might get loose, you might fall down or you might be hit by another bus because your body is protruding away

outside the thing. But it doesn't mean that okay you are going to really, it's going to really happen; it can happen. So what is the probability of this?

(Refer Slide Time: 03:20)

- One can define different measures of risk of accident at nuclear power plants. One measure is the **core damage frequency**, which is the probability per year of reactor operation of experiencing a core damage accident; this evaluation is performed by PSA level 1. Another measure of risk is connected with the **release of fission product into the atmosphere** and is generally given in terms of cumulative frequency (annual frequency of having an activity higher than a given value) of release of different fission products (iodine, Cs); this evaluation is performed by PSA level 2.

Now coming to the nuclear reactors about which our whole subject of the talks in these different lectures are going to be, we have to -- how do we say, risk of what, risk of damaging the core, but why what happens if the core is damaged. If the core is damaged, the fuel, then the fission products which are already because of the fissions which have already occurred all will come out. So we measure the core damage frequency. So what is that? The probability per year of reactor operation or we say, probability per reactor year of experiencing a core damage accident.

So in the terminology of the probabilistic safety analysis, this is called as level 1 which is most important that the core damage can happen, what is the frequency with which the core damage can happen because only once you know that then you have to start thinking about what will happen, after that what is going to happen, what are the consequences of that.

Now having the core having been damaged, next is these fission products can come to the containment or to the other environment. So the other measure is how much of this fission product will come to the atmosphere, what is the probability, what is the chance, so that is we have the next level so that comes under the PSA level 2. So basically here, we will be worried about the fission products, iodine and cesium. So this is the level.

Just going back, the amount of fission products will be proportional to the power and the integral power, dT that's what will be the cumulative operation. So more, this will be more, if it is less so you take a smaller reactor, there the probabilities or the quantities will come down, probabilities may remain similar.

(Refer Slide Time: 06:13)

- Other measures of risk are defined by their different **impact on the public** (death, cancers, etc.) and are given in term of individual risk (annual frequency of death by cancer) or public risk (annual frequency of having a number of deaths higher than a given value); this evaluation is performed by PSA level 3.
- Although in many countries it is not compulsory to perform a probabilistic safety analysis, in practice it has become common practice for new plants and for existing ones. Moreover, international requirements include that safety analysis reports include a summary of the PSA study of the plant.

Now, some amount of fuel has come out of the core, not all may come, and some has got released to the public, but it may not have total impact; only some impact it may have. And how do we measure this risk. So impact on the public. For example, let us say, how many deaths happened after the Fukushima accident, how many cancers happened after the Fukushima accidents. So they could be measured as frequency of death, annual frequency of depth or annual frequencies of cancer and this we call as the PSA level 3.

Now this probabilistic safety analysis per se even though it does not been compulsory in all countries, nevertheless it has become an accepted practice to have probabilistic safety analysis and the determining safety analysis and at least the first level of PSA, we are able to do and in the following parts of this lecture, we will see what we can get out of PSA.

(Refer Slide Time: 08:07)

A PSA is a complete and well-structured method for identifying accident scenarios and to obtain numerical risk estimates. The question of whether PSAs or probability risk assessments (PRAs) can be used to demonstrate the compliance with numerical safety criteria has been debated at length. However, all those who experienced the probabilistic method, are convinced, at least, of the following positive aspects of it:

- It forces the analyst to examine the complete set of possible sequences of events which may happen on a plant, without excluding any of them beforehand (as is done in the deterministic method). Therefore the risk of forgetting in the analysis some important sequence or situation is lower.

This PSA means you have to know how the scenarios can develop. So if you have to develop the scenarios in this process, you must know how each and every component is going to operate and in which way each component can fail. So this really gives you a good insight, you have to have an insight into the whole plant to do that PSA. Then always we have to compare the risk probability with the risk which we can take. So this is the next step. So basically PSA has made people realize that a set of each sequences may happen or may not, but well beforehand it tells

you that with this sort of a design this can happen. So that sort of what you call input we get in the design.

So we cannot say, some portion we have missed or forgotten in the analysis; you have to know the total plant. So it's a very useful tool. So it really gives a general vision of the plant from the safety point of view and highlights the weak points. For example, let us say, there are two different approaches of providing safety. Let us look at a boiler feed pump. In order that a boiler feed pump, in case it fails, still the flow to the steam generator must be or the boiler must be ensured.

I could have different approaches. I could have two 100% pumps; one in operation, one as a standby. As a redundant approach, I could have both being electrically driven or I could have one turbo driven and one electrical driven, or I could go for a three 50% pump approach where two are normally in operation and if one fails, the third 50% takes over. Here again, I could have a combination of all the three could be electrical or two normally running could be on turbo, the standby could be on electrical.

So all sorts of combinations and if I take the failure data of a turbo driven pump and electrical and then compare, I can get which is better. Both have a certain probability of failure, but which has a lesser probability or lesser probability means it has got a lesser risk. So this PSA is really a very, very useful tool even at the design stage.

(Refer Slide Time: 12:38)

- It affords a general vision of the plant from the safety point of view, highlighting specific weak points and, therefore, in particular during the design phase, allowing a well-balanced plant to be conceived.
- The method gives an idea of the global risk and, notwithstanding its possible imprecision, is useful for comparative considerations between different plants and, therefore, it contributes to the creation of a homogeneous reactor overview from the point of view of risk.

So it gives you a comparative consideration between different solutions and really it gives you your real homogeneous reactor overview. We have talked about the reliability of the equipments, so we said okay, depending on the reliability of the equipment, you have failure; if the reliability is not good, you can have more frequent failures. All these malfunctions could be caused because of the component failure or equipment failure, it could also be human errors.

So human reliability also needs to be looked into then you analyze the probabilistic safety. So one of the most important things we look in the human or the man-machine interaction that any set of rules or procedures need to consider how the human can approach, let us say, the panel,

whether the switches he can operate are easy to operate or for a certain of important operations he doesn't have to move from one panel to the other, all sorts of things had to be thought of to make the errors less in case of human beings. But here again, the human behavior, individual human behavior differs. We do give training so that how the operator has to react in different situations, but then there is always an uncertainty.

(Refer Slide Time: 14:52)

- Usually, for the sake of conservatism, focus is placed on the probability of operator error (omission, commission and, more difficult to analyze, diagnosis errors). In the real world, however, the role of operators in an accident sequence is not limited to committing or not committing mistakes in the implementation of operational procedures. In fact, as many events indicate the operators may react to an unexpected situation with creative and resolving interventions. For the present moment, however, except for specific cases, the possibility is taken into account only that the operator makes mistakes in the implementation of emergency procedures, even in the field of the management of severe accidents.

So in the safety analysis, we do consider operator errors, but as I've mentioned some time back, we have seen that in many events the operator has acted in a way which is really commendable, understanding the reactor operations, reactor design, and have been able to prevent many accidents. So even though the human error is there, so in all the designs we do take credit for at least for 30 minutes for human intervention.

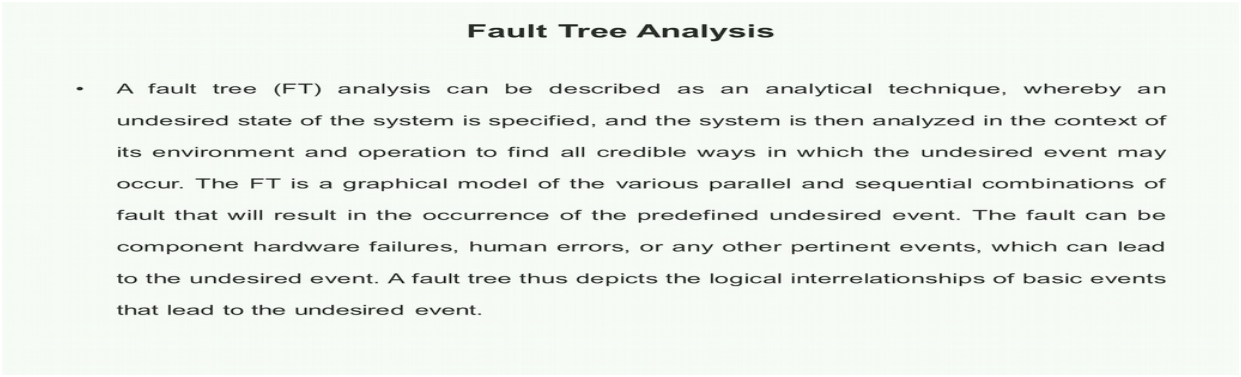
(Refer Slide Time: 15:42)

PROBABILISTIC ANALYSIS

- The probabilistic analysis of a plant is usually performed by the construction of event trees, for any single group of similar initiating events, and of fault trees, for any single system or component whose fault probability is important for the study of the various accident sequences.

So how do we consider the probabilistic or how do we go about the probabilistic analysis? Here we talk about event trees and fault trees. Now what is an event tree? For a similar type of faults or initiating events, we see what is the consequence on the plant or what is the core damage frequency and in the fault tree, for a single system to fail, what is the probability that single system can fail. So that is the fault tree. So you know what is the event which will happen and a set of events lead to the event tree, finally the core damage frequency.

(Refer Slide Time: 16:45)

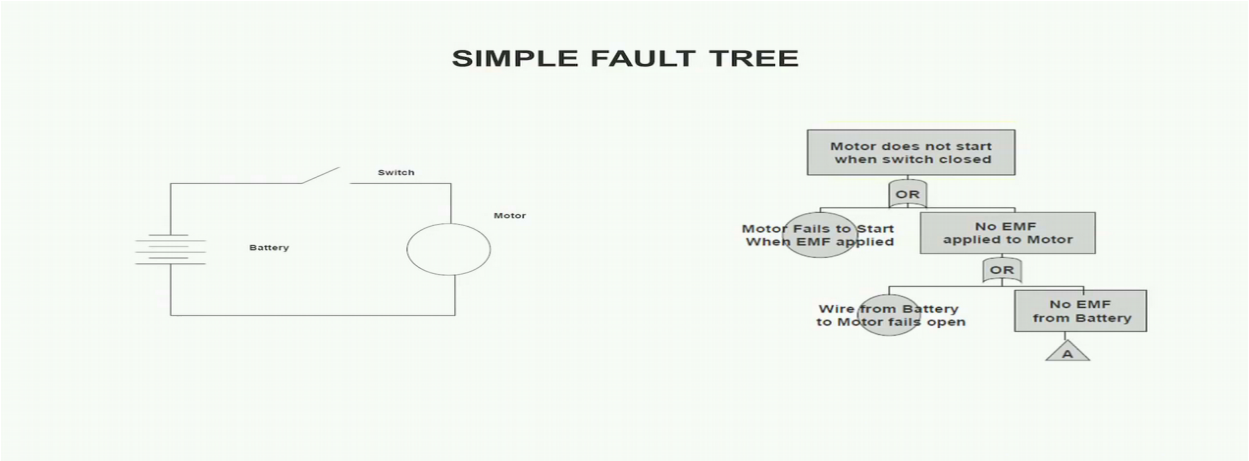


So let us look at first at the fault tree. If I have to define fault tree, it gives an analytical technique where an undesired state of the system is specified and the system is analyzed to find out all credible ways in which that undesirable state can happen or undesirable event may happen. In this case of reactor, let us say, a trip of a reactor pump so in all ways, in which always it can happen. So it is something like a graphical approach, we make the sequential combinations or different things which both can happen mean two sorts of events, combination of events, all sorts of things, combination of failures which can happen which can lead to the particular event.

So the fault can be a component failure or a human error or anything. So this is actually a logical interrelationship between the different component functions and human actions. So effectively, it is a backward-looking; you have put the pump trip at the end, it can happen because power is not there or the pump bearing is not working. So if the pump bearing is not working, okay maybe the oil is not there for the cooling or some other problem. If the power supply is not there, maybe the switch is not closed or there is a power supply.

So like this, we develop the backward sort of. So the end result is the analysis starting point and we go down, traced back and of course, we have logic symbols because to the faults happening together can lead or each individual fault this or that also can lead. So we have logic gates; OR gate, AND gate, and things like that.

(Refer Slide Time: 19:10)

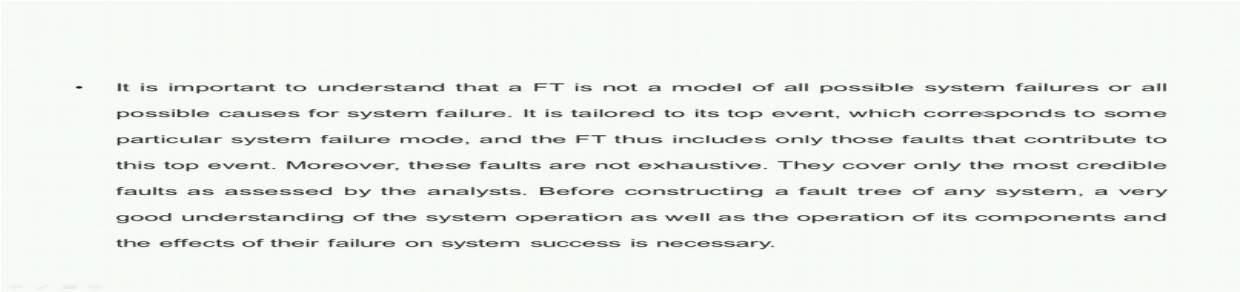


We will look at a simple fault tree for this. This is a motor which is running on a battery and this is a switch and our event is, we want to start the motor, we have closed the switch, but motor is not started. So if the motor starts, there is no event; motor does not start is an event. So the motor may not start because of two reasons; one, the EMF has come, but the motor does not start. EMF is there, motor does not start. Another case could be no EMF, either of these two can happen. If this is happening means there is a problem internal to the motor whereas if it is no EMF means there is the problem is external to the motor.

Okay, when the motor will not get EMF, there could be two situations; the battery is not charged so there is no EMF in the battery or the wire from the battery to the motor is open, but connection is not there. So now let us come, if the connections you can't do, there is no going below.

Coming to the no EMF from battery, it can happen under two conditions; the battery is not having EMF and no charge is coming to the battery, because the battery would be charged by some other source. So no. Then why it is not charging? Maybe the wire from the switch of the battery has failed; it is open or no EMF from the charging source and no EMF of the charging source can happen if the switch is not connected or again the wire. So like this, we develop and we look at combination of these or that and things can happen by which it leads to the final fault.

(Refer Slide Time: 21:38)



One thing we should keep in mind that fault tree is not a model for all possible system failures; it is tailored to the top event. You postulate an event and find out in what way it can happen. So you have to postulate certain events. So it very much depends on your ingenuity how do you postulate. So it's a very, very endless list. So you need to have the knowledge of the plant, you need to have the knowledge of the experience which the other plants have had, and it also needs to know what sort of failures can take place. So when you are talking, we are talking about the credible faults most likely happen. So we need to have a very good understanding of the system and its operation and also the operation of the components.

(Refer Slide Time: 22:35)

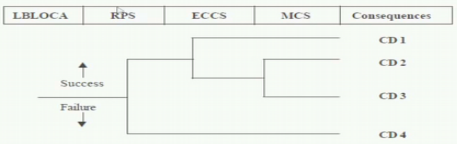
Event Tree Analysis

Event trees (ET) are graphic models that order and reflect event sequences. A typical accident sequence consists of a PIE group, specific system failures and successes, and their timings and human responses. An event sequence can lead either to a successful state or to core damage. Every accident sequence that does not lead to successful end state (safe reactor shutdown state as defined in the plant design and technical specifications for plant operation) is assumed to lead to core damage.

Let us come to the event as now we have seen which faults have led to the event and which set of events can lead to a core damage. So this is an accident sequence consisting of different events and the failure or the success of every step will tell you whether the core will get damaged or what is the probability with which the core will get damaged.

(Refer Slide Time: 23:20)

- Events or 'headings' of an event tree can be any or combination of safety function, safety systems, basic events and operator actions. The event tree headings are normally arranged in either chronological order. Chronological ordering means that events are considered in the chronological order in which they are expected to occur in an accident as depicted in (deterministic) safety analysis.



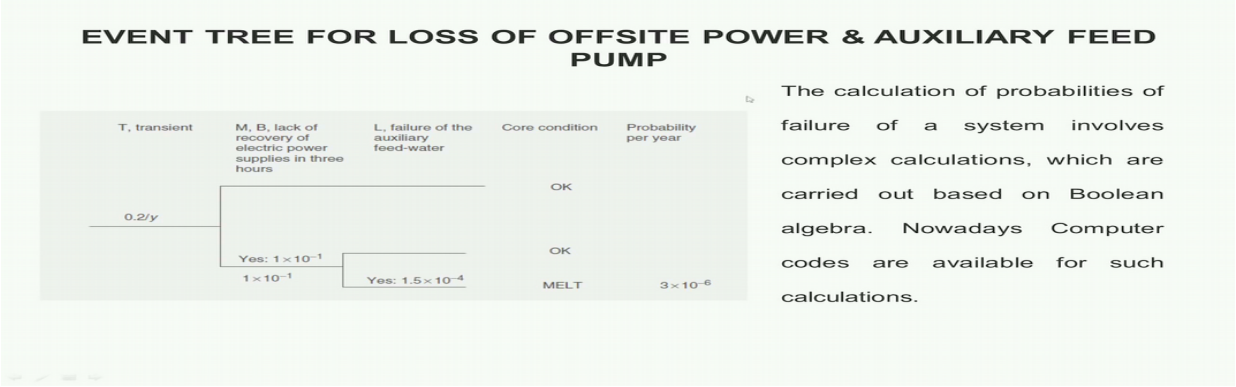
LBLOCA: Large break LOCA, **RPS**: Reactor protection system. **ECCS**: Emergency core cooling system, **MCS**: Moderator circulation system. **CD1**: Core damage category 1,

Let us look here, this is an event related to a large break LOCA, loss-of-coolant-accident that means there's a big break so a large amount of coolant is getting lost. Then what is the safety function? You must have the reactor protection system which must shut down. Okay, let us say, the reactor operation shuts down. Then the coolant is getting lost from the core so you need to

provide emergency core cooling. Let us say, emergency core cooling comes then the core may not get damaged. Okay, so there is a certain core damage probability for this, the core may not get damaged. But suppose here, the emergency core cooling system doesn't come. We have provided the design that the moderator will cool. So if that is there, again the probability with this can happen will be different because this includes the probability of a ECCS failing on demand.

In case your failure is there of the MCS then it will lead to a certain frequency of core damage. If the reactor protection system fails then you have a certain event, certain frequency of core damage. So this way depending on the failure probability of each and every system which is following in sequence, we will find out the core damage frequency. So basically here it is very important, chronological order of the safety function, the safety systems, and operator actions if any need to be brought in, then we find out the core damage frequency.

(Refer Slide Time: 25:48)



Another event tree involves a loss of offsite power. Offsite power is the power which you get outside the site, any power plant whether it's a conventional thermal power plant or a nuclear power plant always is connected to the grid, power grid through different lines so that always in case you don't generate, you will get power from outside to maintain the state of the plant or in case connection would be able, you can be able to send power to the grid through different lines.

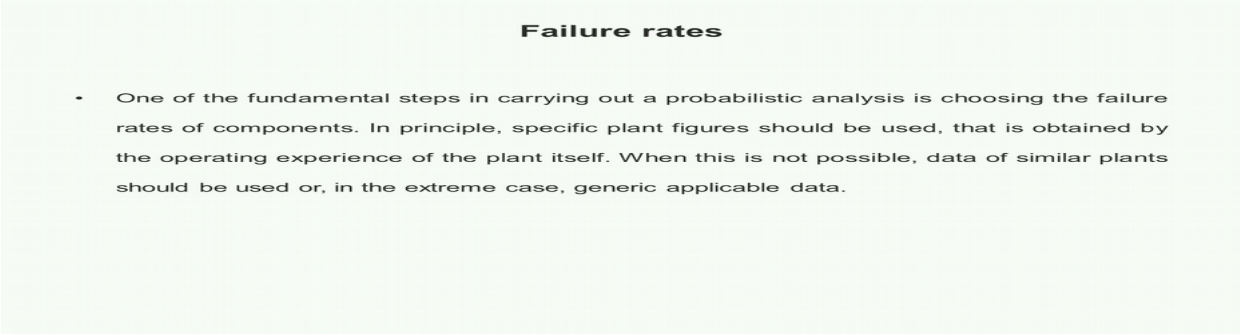
In case there is a loss of offsite power, normally in case, even though in spite of multiple things, you have a loss of offsite power, you then go for the onsite power, onsite power is your diesel generator and this diesel generator will not have a very large capacity. So it will not be in a position to run them main pumps because that requires a higher voltage and the higher power. So we try to shut down the plant and then try to give, feed water through the auxiliary pumps.

So here we consider the case of loss of offsite power. Let us say, the power supply doesn't come. If it comes, well and good, no probability, it comes back, cooling is assured, no problem. Let us say it fails with a certain probability, so the next step is auxiliary feed water has to come. If it comes, okay, no problem, core is safe, but then if the auxiliary thing doesn't feed water doesn't

come, your cooling of the core will not be possible then you have the core melting. So here what is the probability of this core melting happening based on the transient occurring as 0.2 per year and 10^{-1} for the failure of non-resumption of the power or getting it from the diesels then the failure of the auxiliary feed pump, all those things together can lead to this probability.

Now all these calculations are done by Boolean algebra and you do have computer codes, in fact, prepared or developed by different countries and also now distributed freely by the International Atomic Energy Agencies, they train you. So there is something like a cooperation.

(Refer Slide Time: 28:48)



Actually nuclear arena is one where there's very good cooperation among the countries and we have a forum for cooperation unlike many other industries and energy sources. Now when we look at the fault tree and the event tree, we are trying to calculate the probability with which it can happen. So the probability of the individual failures is a very, very important data. Now, let us say, I use a company A motor, then I must use the data of the company A motor that failure data. We will see if it is available or generate that data by running the component in some rigs we can generate or we can see where that component has been used and find out what was the failure rate.

In case, it is not available, something of a similar design, we can see, so we get starting point. Now getting this data will surely be better than not using any data and these data are generally available for us.

(Refer Slide Time: 30:20)

Component	Failure Rate
Transient loss of DC bus	$5x\ 10^{-3}/y$
Transient Loss of AC bus	$5x\ 10^{-3}$
Transient loss of Offsite Power	0.1/y
Spurious opening of relief Valve	$1x10^{-4}/y$
Solenoid valve failure to operate	$1x\ 10^{-3}/d$ on demand
Non return valve failure to close	$1x\ 10^{-3}/d$ on demand
Electric Motor Pumps-Failure to start	$3x\ 10^{-3}/d$ on demand
Failure to operate	$3x\ 10^{-5}/h$ on demand
Turbine driven Pump Failure to start	$3x\ 10^{-3}/d$ on demand
Failure to operate	$5x\ 10^{-3}/h$ on demand
Diesel Engine Pump Failure to start	$1x\ 10^{-3}/d$ on demand
Failure to operate	$8x\ 10^{-4}/h$ on demand
Emergency Diesel Gen Failure to start	$3x\ 10^{-2}/d$ on demand
Failure to operate	$2x\ 10^{-3}/h$ on demand

Here I am just giving you a very long list of some of the data which are available like transient loss of DC bus, transient loss of AC bus is $5x10^{-3}$ per year. Transient loss of offsite power is about 0.1 per year. Then sudden or unexpected opening of a relief valve could be 10^{-4} per year. Then emergency diesel failed to start and there are different. Failed to start on demand then failure to operate on demand; there are two things, it may start but may not operate. So these are different types of frequencies data is available.

(Refer Slide Time: 31:20)

SUMMARY

- This chapter has focused on identifying the different events that can occur in a nuclear plant and classifying them based on frequency and consequences. Ideas on the deterministic and probabilistic safety approaches have been brought out with typical examples. The advantages of probabilistic approach by the step by step approach of fault tree and event tree and its help in quantifying risk have been explained.

Now I can tell you, this failure data has been collected over a large number of reactors and many countries have established data banks. Right from the beginning, as I mentioned, all these are available on record, how many times the pump has failed. Everything is recorded in the nuclear systems and shared with the Atomic Energy Agency and we know how many times it has happened, every event. For example, let me take the case of the prototype fast breeder reactor, 500 megawatt electrical prototype fast breeder reactor which is coming up at Kalpakkam in India. We identified the different design basis events, we took the failure data of different plants.

In fact, we could get how many sort of event trips have happened in different reactors. We also had experience of our own fast beta test reactor plant, we had the experience of the nuclear heavy water reactors. So based on this we could arrive at a very, very important input for the design; how many events of each type, type of event which can happen and how many such events can happen in the lifetime of the plant.

Mind you, the number of times it can happen is very important to me for the design of a component. Let us take a mechanical structure. From shut down, I go to operation, it goes from a low temperature to a high temperature, it goes from a low pressure to a high pressure. Then I shut down, it comes down again to the low value, again you start up, it goes up, it comes down. There is a transient, there is a variation of temperature.

Every time these temperatures and pressures change, the structure is getting loaded in a cyclic fashion. Sometimes there is a tensile stress, sometimes there is a compressive stress and there is a fatigue life of the structure; more the number of cycles your life can come down for a particular or you must use a material which can withstand the required number of fatigue cycles. So mind you, this is a very, very important input for the design. I repeat even though the failure data or the component failure data which leads to the event frequency may not be very, very accurate, nevertheless it tells you the direction in which you need to go about and the deterministic analysis combined with the probabilistic safety analysis yields a very good insight into the reactor systems and gives you on what basis you can make it more safe.

Let me now summarize what all we have talked in these two lectures. We identified the PIEs, we identified the different design basis events, then we classified them based on the frequency, we looked at a deterministic safety analysis. Then we looked at what a probabilistic safety analysis looks like. I was able to give you some simple examples of an event tree or a fault tree how it is developed and how we can quantify the risk is what is explained to you and I hope you have seen what are the safety principles and in the safety approach, how we take care of that. Thank you.

Online Video Editing /Post Production
K.R.Mahendra Babu
Soju Francis
S.Pradeepa
S.Subash

Camera
Selvam
Robert Joseph
Karthikeyan
Ram Kumar
Ramganesh
Sathiaraj

Studio Assistants
Krishankumar
Linuselvan
Saranraj

Animations

Anushree Santhosh
Pradeep Valan .S.L

NPTEL Web &Faculty Assistance Team

Allen Jacob Dinesh
Bharathi Balaji
Deepa Venkatraman
Dianis Bertin
Gayathri
Gurumoorthi
Jason Prasad
Jayanthi
Kamala Ramakrishnan
Lakshmi Priya
Malarvizhi
Manikandasivam
Mohana Sundari
Muthu Kumaran
Naveen Kumar
Palani
Salomi
Senthil
Sridharan
Suriyakumari

Administrative Assistant

Janakiraman.K.S

Video Producers

K.R. Ravindranath
Kannan Krishnamurty

IIT Madras Production

Funded By

Department of Higher Education
Ministry of Human Resource Development
Government of India

www.nptel.ac.in