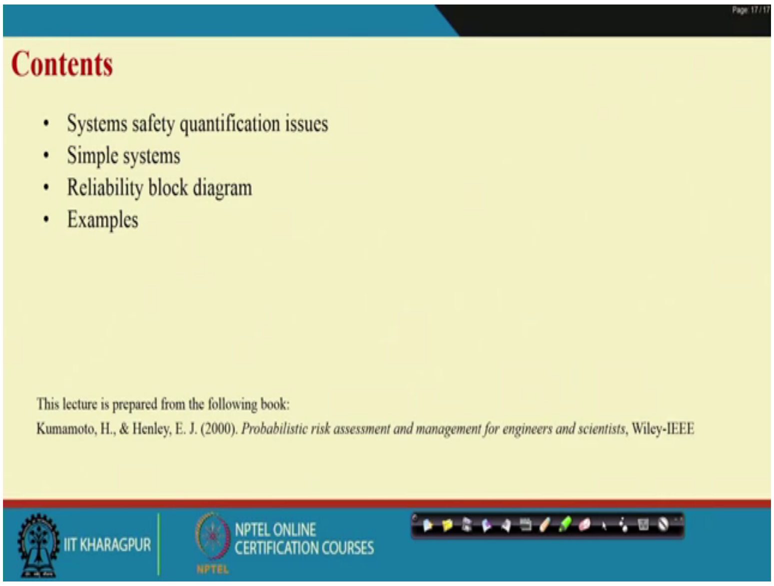
Industrial Safety Engineering
Prof. Jhareswar Maiti
Department of Industrial and Systems Engineering
Indian Institute of Technology, Kharagpur

Lecture – 36
Systems Safety Quantification: Truth Table Approach

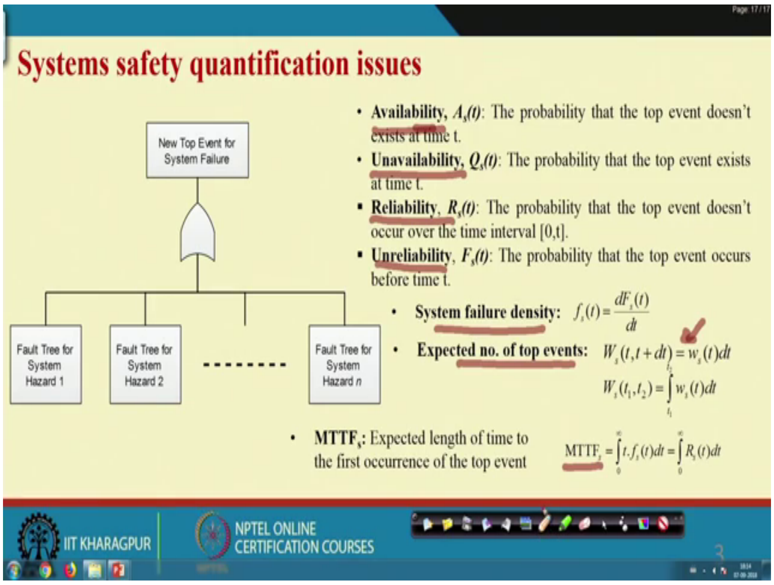
Hello everybody, last class I have completed the quantification issues related to basic events. Today we will start system level quantification and today's topic is the basics of quantification of system safety and one of the method for system safety quantification that is liability block diagram.

(Refer Slide Time: 00:47)



So we will see, what are the issues related to system safety quantification, then we will see first the simple systems and their quantification and then we will describe reliability block diagram and finally, some examples we have seen and I hope that 35 minutes of time, we will be able to complete it and this is this lecture is also taken from the book written by Kumamoto Henley, probabilistic risk assessment and management for engineer and scientist published by Wiley.

(Refer Slide Time: 01:23)



Now, let us spend some time here, that what are the issues that is important for system safety quantification. So, if you recall the fault tree and finally, the cut sets for fault tree or different kinds of hazards, that alone or in combination with different events lead to the top event.

So here, the top event is the issue. So, top event is basically system level event, if top event occurs means system level failure occurs there could be more than one top events.

So in that case, the collectively the quantification will be different, but we are assuming one top event at a time and that sense we are quantifying the system safety. So like, component quantification component will safety quantification or component level, basic event level quantification. So, in the system level quantification also the parameters are more or less same. So, the parameters of interests are availability, unavailability, reliability, unreliability system failure density, then your expected number of top events and also unconditional failure intensity for the system and also a mean time to failure for the system ok.

So, you know all those definitions from component failure point of view. Now what is the unavailability? Unavailability at the system level is there the probability that let us start with availability, availability the probability that the top event does not exist at time t; at time t system is available, unavailability at time t system is unavailable; that means, the probability that the top event exist at time t.

Now, what is the top event? It can be, for the pressure tense system, it can be the tank rupture some system can be fire, can some system, it may be simple the break down machines and it all it all depends, what are the top events you are interested with. Then what is the reliability? Reliability that the probability that the top event does not occur over the time interval 0 to t and then, unreliability that probability that the top event occurs before time t.

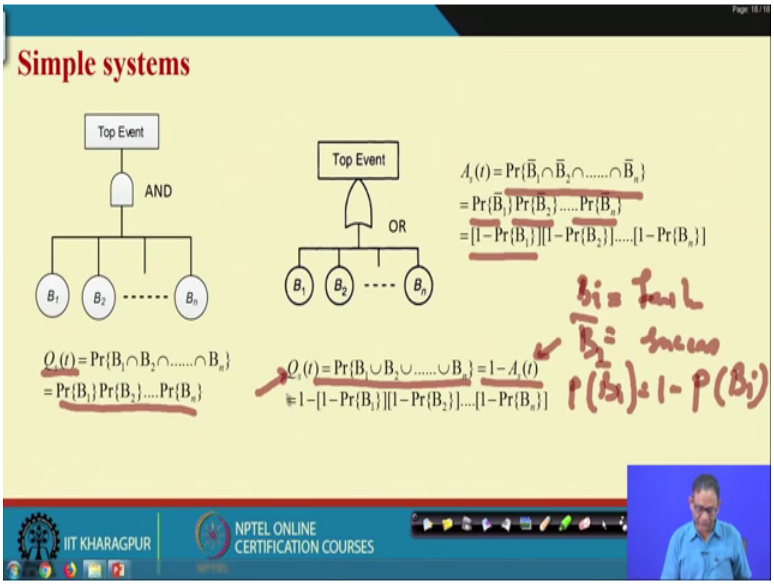
So, I am not stressing more today, because these are the definitions that we have already discussed while we have discussed the quantification of basic events. Then what is the system failure density? It is basically, the derivative reference took time for the reliability then, expected number of top events. So, if you know the unconditional failure intensity for the at the system level, then this is the formula and we in between t and t plus delta t in such a manner that within the small amount of time, only one even can take place.

And if you are interested to know, the expected number of failures within t 1 and t 2, then this is the formula and what is the mean 10 to failure here for that the system level? Expected length of time to the first occurrence of the top event, so, then this is the formula ok.

So, we are using s everywhere to denote that the parameter at the system level or the distribution or the system level ok. For component, we have not used anything only for availability; we are use At, for unavailability Qt, but at system level Ast, Qst, Rst, Fst like this ok.

So, these are the issues, these are the things you require to quantify at the system level.

(Refer Slide Time: 06:16)



Simple system, simple system means, the system can be represented using AND or OR gate or maybe and our combinations ok. So, if the top event is linked with the bottom basic events, with AND gate you all know what is the probability of the top event occurrence, if top event occur at time t, then it is basically system is unavailable.

So as a result, we are able to write here Qst, which is probability of that joint probability, I can say the intersection between all the basic event probabilities ok. So then, this is basically multiplication, assuming that the basic events are independent events and in the at OR gate case, what will happen? We will, start with if you say, the unavailability then unavailability means any one of the basic events, if occur lead to the top event occur, the top that will be unavailable. So, union ok.

So, union is important. So, how do we compute this? So, then Qst will be 1 minus Ast, where Ast is the availability. Now availability means that if Bi is, Bi stands for that failure, then the complement Bi bar is success ok. So that mean all those, basic event that should not occur as basic events, we started with failure events. So, then all the success require. So, that is why our probability intersection of all those, then probability of B 1 bar into probability B 2 bar probability in Bn bar as we have assumed that all the events are independent.

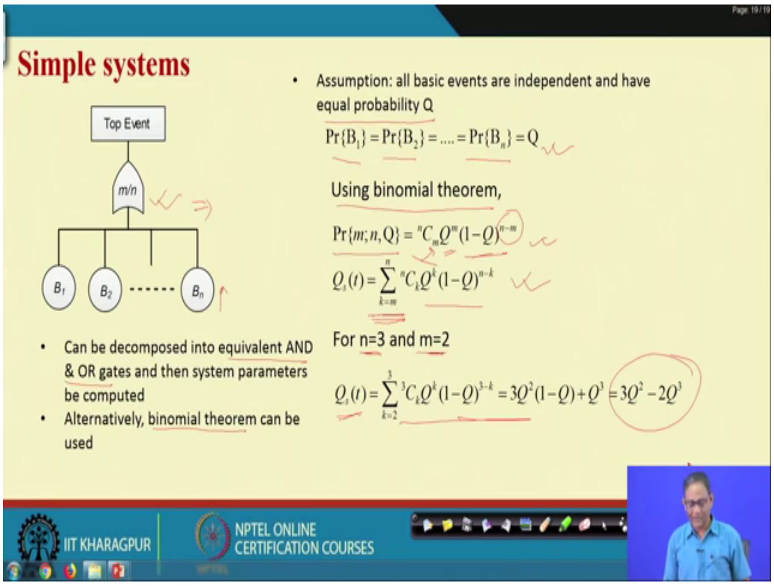
So, their probability will be multiplied for the intersectional gen probability and then, what is PB 1 bar? This is nothing, but 1 minus PB 1. So, PB bar, if I say P Bi bar this is nothing, but 1 minus probability.

Student: (Refer Time: 08:54).

Bi ok. So, then Ast is computed, now you can put here you can find out the Qst.

Student: (Refer Time: 09:06).

(Refer Slide Time: 09:16)



Now let us talk about voting gate, which is basically gate m out of n gate. So in that case, what way you will find out, the system unavailability system level, unavailability we have discussed that when finding out the cut set and that time also, we have discussed and in some other classes well quantification get by get method and we have discuss that, it can be the voting gate can be decomposed into equivalent and then or gate and then using gate by gate method, you can find out the, what is the probability of the top event? Top event is nothing, but failure of failure bend and then this is the unavailability of the top event.

So all here, we will be show another approach basically, using binomial theorem. So, in order to use the binomial theorem, we will assume that, all the basic events are independent that and equal probability all have equal probability Q. That mean probability of B 1 equality of probability of B 2 equality to probability of Bn equal to Q, where Q is basically the component level unavailability ok.

So then, then using binomial theorem, we can write this one that, what is required for the top event to occur out of n inputs? m must occur then top event will occur or m or more getting me, it m out of n, n basic events if m or more basic events occur then, top event will occur minimum m basic event must occur, then if using binomial theorem, you know that the probability that that out of m, m number of m events can occur. This is nothing, but n choice, n choose m out of n basic event, choose m number of basic events into Q to the power m and 1 minus Q to the power n minus m, this is what is coming from binomial theorem.

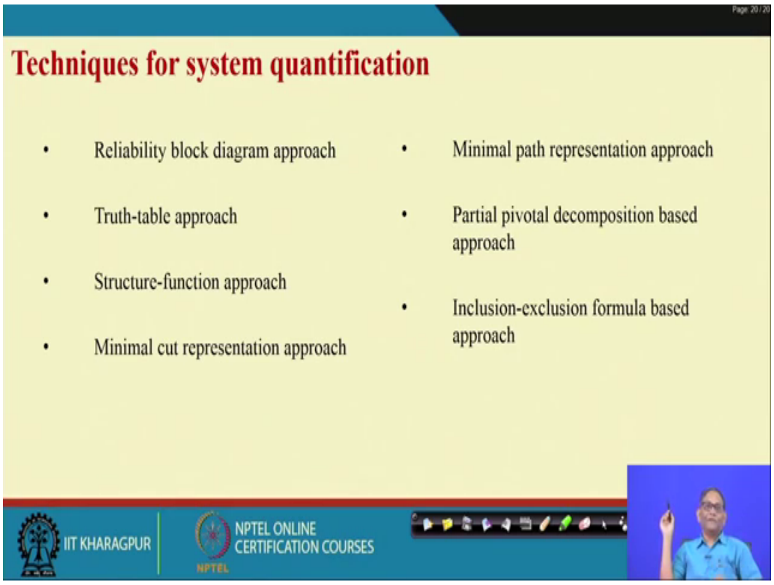
So, what did that mean? This is the combination part n Cm, how many combinations possible? That mean, how many ways you can choose m components out of n give in? Then what is Q? Q is basically the probability that the component is unavailable component is a failed state. So that, to the power m and then compo and then there is another probability, that is basically success probability which is basically, 1 minus Q. So the rest will be under success. So, 1 minus Q to the power n minus m.

Now, what will happen for the system level unavailability? System level unavailability that means, either m or m plus 1 or m plus 2, means m or more number of basic events should occur as a result the summation is coming here. So, Qst is k equal to m to n nCk Q to the power k 1 minus k to the power n minus k. So, this one summed over k equal to 1 2 n, all the probabilities have summed.

So, that is what is our probability for the in the voting gate, when m out of n combinations lead to the top event to occur, the unavailability of the system can be computed using this equation provided. All the basic event have equal probability of occurring and the basic events are independent in nature. For example, if we choose n equal to 3 and m equal to 2, then the Qst will be, just putting the k equal to 2 to 3 in this equation, you will this equation you will be getting this value, 3 Q square minus 2 Q 3.

Now you know, what is the Q value, if Q is 0.5, you can put here 0.5, then you will get the system unavailability ok.

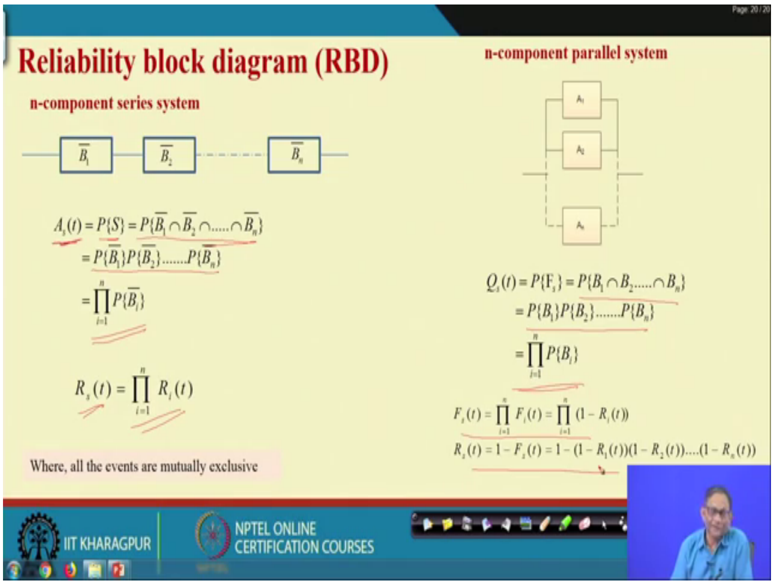
(Refer Slide Time: 13:56)



So now, let us see that what are the different methods that are techniques that are available to quantify the system level failures or system level unavailability, availability and other system level parameters? So, there are quite a number of approaches available. For example, reliability block diagram, truth table, structure function, minimal cut representation, minimal path representation, partial pivotal, decomposition or inclusion, exclusion formula approach.

So today, in the rest of the time, we will discuss the reliability block diagram. In the next class, truth table structure function or minimal cut and path presentation approach will be discussed. The sole purpose is to find out the top limit top event occurrence, which is basically, unavailability of the system and then resulting availability and other failure parameters quantification.

(Refer Slide Time: 15:19)



So, let us see what is the reliability block diagram?

Now here, we will define 2 kinds of system, one is in component series system and n component parallel system, what does it mean n component series system? That mean for example, you just think of any machine and which you have created in such a manner that the component, one of the component fails mean the system will fail. So then, what happened this can be said that, it is in the series one like this.

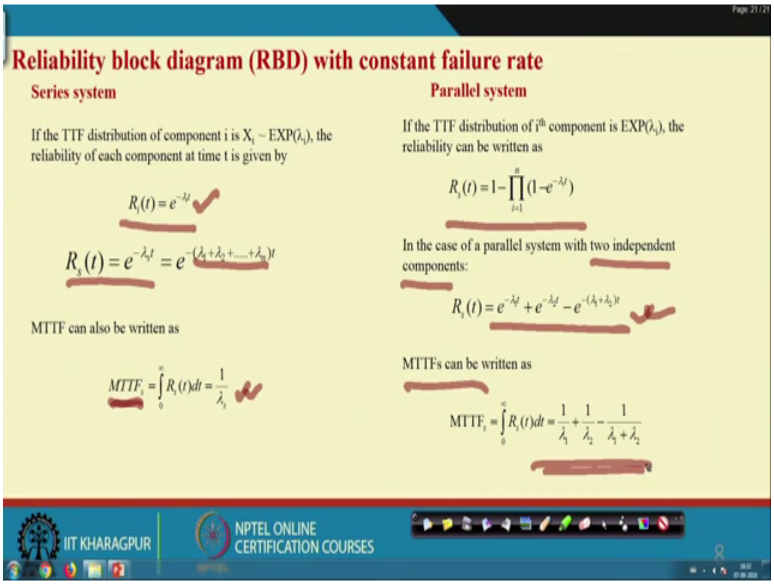
So, under this situation, what will be the availability of the system? Availability of the system is that, when all the components are available then only the system is available, if any one of the component is unavailable system is unavailable. So, that is why you calculate the availability of the system at time t, which is basically probability of that success of the system, which is basically joint probability, but all the components are successful.

If Bi is the probability of failure for the ith component, Bi bar will be the probability of success. So in that sense, this one can be written like this as B 1 to Bn, all events are independent, we are multiplying their probable corresponding probabilities and which in this manner can be written and then what will be the reliability of the system? Reliability of the system is individual component reliability multiplic, multiplied Rst i equal to 1 2 n Rit, where Rit is the component level reliability ok.

When it is n parallel component, in that case what happens? In that case the system will be unavailable, if all the components these are simultaneously unavailable. Here, what happen? If any one component is unavailable system is unavailable, here if all are unavailable then only system is unavailable. So, as a result the system level failure, is basically intersection of all the component, unavailability and this can be written like this and finally, you are writing like this.

So, then correspondingly Fst, Rst you can call calculate using these equations. Essentially, these are simple and easy to understand also I do not think that, you will face any problem just and you will not be lost within these notations ok.

(Refer Slide Time: 18:35)



So, let us see some more related to this. Now, what will happen, if the components are having constant failure rate? So; that means, the time to failure is exponentially distributed under this situation, what will be the reliability? Reliability will be for component, reliability will be this, where lambda i is the distribution parameter exponential that distribution parameter for the ith component.

Then Rst will also be e to the power will be exponentially distributed, it could minus lambda St, where lambda s nothing, but the sum of the individual component failure parameter lambda. And then obviously, that mean time to failure system level will be 1 by this.

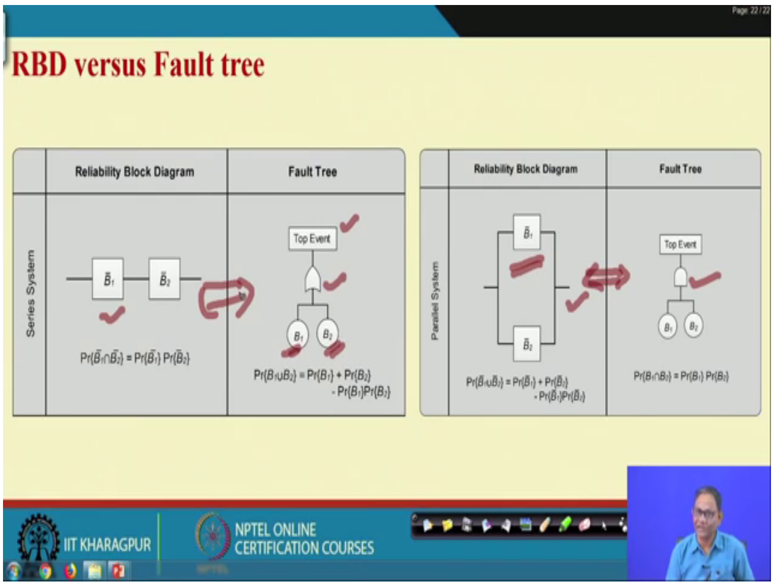
Now, if the same thing which applied many same exponential distribution applied to a parallel system, where the components failure probability is exponentially distributed with ith component exponential parameter lambda i then, we have seen earlier that this is the equation.

And now for for only 2 2 independent components, we have defined this. So, i equal to 1 and i equal to 2. So, one minus i equal to one means one minus e to the power minus lambda i and when it is i equal to 2. So that in lambda, lambda, lambda 2 so, that since it is to be understood ok.

So from here, putting i equal to 1 and i equal and i equal to 2 and multiplying the 2 basically, this is a multiplication you will be getting this value and MTTF will be this one. So, MTTF is basically system level, if you know the system level that will your parameter, which is lambda, I think we have defined earlier, what is lambda? Lambda Dt is basically probability, that the component will fail within time t delta t, when it was as good as new at when it was normal at time t and as good as new at time t equal to 0.

So, those derivations and all those things, already given to you in earlier lectures, I hope that you will not face any problem.

(Refer Slide Time: 21:30)



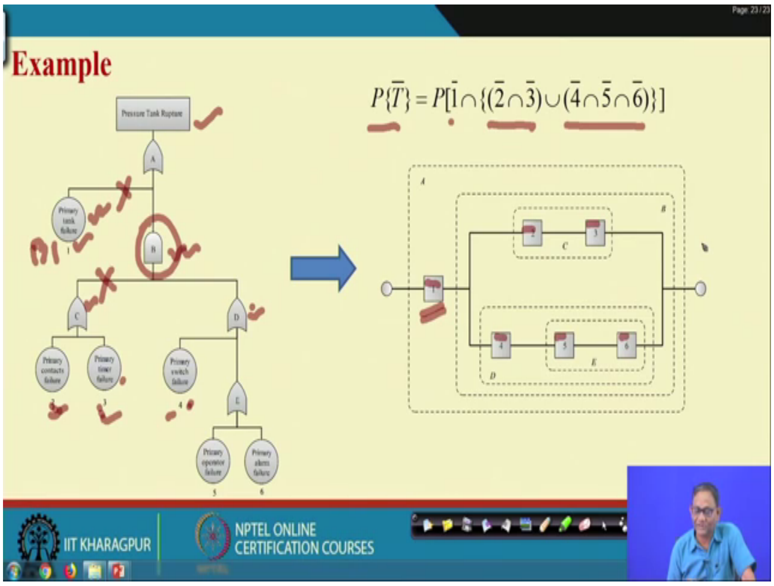
Now we will see that the difference between reliability board block diagram and fault tree. Impact 1 is one can be constructed from the other, if you reliably block diagram, if it is a series system so; that means, the success of the system will depend on both the system both the component success, this is successful, this is successful then only system will be successful.

So if one of the component fails, then the system is failed. So, that is represented in fault tree using OR gate. If B 1 takes place top event will occur be to toast x plus top event will occur, but when we are, what is the difference? When use reliability block diagram. We use the success probability, when you use fault tree, we use the failure probability. So, that mean this series system be AN, OR gate series system in RBD and OR gate in fault free, they are synonyms or once that 2 sides of the coin basically.

Now, if it is a parallel system for reliability block diagram and that means, any one of the cysts of the component if it is successful the system is successful. So, that we took in order to make the system failure both the component should fail. So, both the components should fail means AND gate. So that way, you can you any RBD can be converted to a fault tree and any fault tree can be converted to a RBD, where are RBD talks about success path and fault tree talk about failure path.

That is why, we will see later on using RBD, we will calculate path set, which is basically success path and using fault tree, you have already seen we have computed cut set on minimal cut sets.

(Refer Slide Time: 23:52)



So one example, this is the pressure tank example, several times we have discussed, what is this pressure tank. Our issue is pressure tank rupture and considering only the primary failures or the basic events and ignoring the your secondary events, the poultry is simplified to this part, this kind of poultry.

So here, we have 6 basic events 1, 2, 3, 4, 5, 6. So, we have denoted by 1, 2, 3, 4, 5, 6 but, someone can say B 1 and B 1 to B 6 no problem right. So, then if this is the fault tree, then what is the corresponding reliability block diagram? You see, what will happen? What do you, what it in fault tree you see that if the one for B 1 takes place top event will take place mean failure takes place, but because of AND gate here.

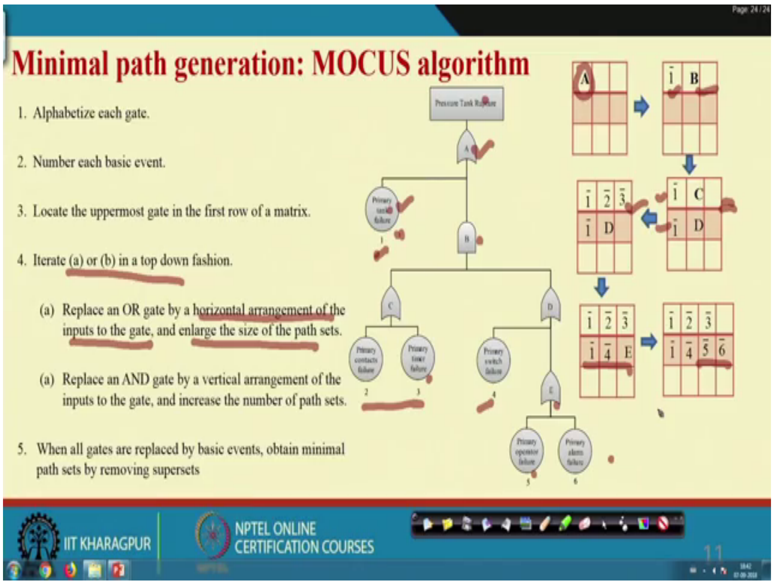
So, at least from this side and one from this side means, either 2 and 4 or 2 and 5 or 2 and 6 or 3 4, 3 5, 3 6 must occur then only, then only what will happen? This side this AND gate condition will be satisfied and this will occur.

Now, what do you want using path C 8 path or RBD, we want that the pressure tank rupture, will not take place. Now see the condition, now if we if 1, in this one, and then 2 and 3. 1, 2 and 3, this will not occur failure will not occur like this one, this and this. If this one, 1 will not occur when 1 is a primary tank is successfully running, then what will happen? And also 2 and 3 are successfully running, that mean this condition will not be satisfied. If this is successfully running this OR gate, this side is over that path 1 is successfully running forget.

So, we have to satisfy this AND gate part ok. Now if we say that both 2 and 3 are successfully running. So, what will happen? This side will be blocked. So, whatever even know, all those things fails this AND gate will not be satisfied. So, this is one success path, this is another success path for bar 6 path, ok.

So now, what we are basically, one to do you want to find out the probability of this tank rupture. Now using these you can find out that probability is 1, intersection these 2, intersection 3 union, 4 all this 3 and ultimately, we will be able to get that success, success mean there are 2 paths one this side, another this side. So, both the path probability will ultimately give you the success probability.

(Refer Slide Time: 27:37)



So now, we want to generate the path set. So earlier, you have generated the cut set means failure path, now we want to know the success path. So success path here, the difference will be in case of cut set, we say all other things same alphabetic each gate number, each basic event, then go in this manner that is what in the mucus algorithm in cut set computation, you were seen.

The difference starts here, in cut set we say that OR gate actually increases the number of cut set and AND gate increases the number of elements in a cut set, but in case of path set or in case of RB RBD, when you go for path set computation any OR gate, what will happen? It gate by horizontal arrangement, increase that actually replace OR gate by a horizontal arrangement of the inputs to the gate, enlarge the size of the path sets and AND gate, what it will do is increases the number of path set.

So, if there are and more and get more path sets will be created. So, as a result that is what we are doing here? So from here to fault, RBD also you can find out from fault tree. First gate is this you write this one, then what is this gate? This is OR gate. So, what it will do? It increase the number of elements, in the path set, what is this element? This element is 1 bar. So, this is B.

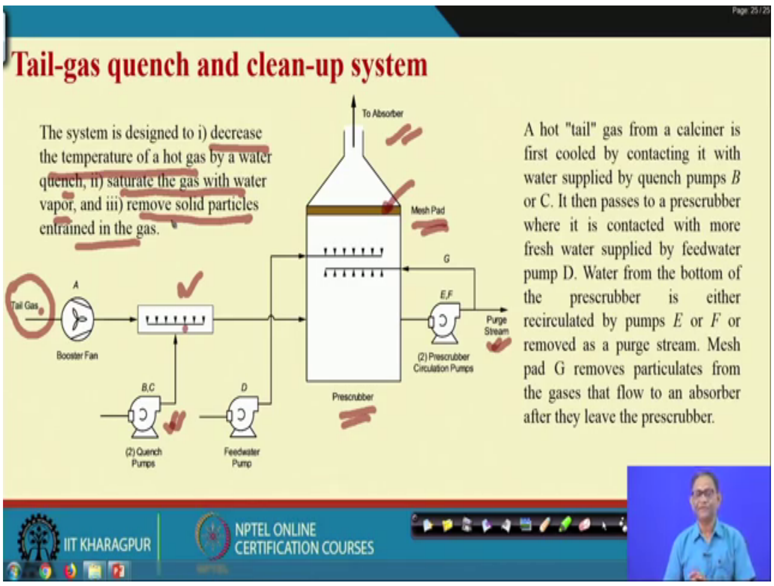
Now, B is OR gate, B is AND gate, if it is and gate from path set point of view, it will increase the part number of paths sets. So, that is why 1 bar, because of the basic event say, basic success events means the success of the basic component level. So, that remain as you teach, now B will be split, but B again you see B is AND gate. So, C and D is coming so; that means, because of AND gate, it is increasing the path set.

Now, what do you require to do? You have further decompose, you require to decompose C and D C and D both are OR gate, it will just increase the number of that success events in the path set. So, if you break C C 2 and 3 is their 2 bar 3 bar for D again, what happened D is having 4 bar and e. So 4 bar, any you writing again E is another OR gate. So, it will increase the number. So, that mean 5 and input is 5 and 6, 5 by 6 bar

So then, how many path sets? 1 bar, 2 bar, 3 bar, 1 bar, 2 bar, 3 bar, 1 bar, 4 bar, 5 bar, 6 bar. So, if this one is successful and these 2 successful, this will not that system will be successful or this is successful and this 3 successful system will be successful ok.

So that is what is our and what will happen ultimately, in this way you decompose and finally, you may find out the situation, where you have to you have to actually go for minimal path sets by removing supersets, the way we have removed the super sets in terms of cut sets finding to find out the minimal cut set.

(Refer Slide Time: 31:28)



So, I I hope that we have given enough explanation to RBD and then fault, fault tree and RBD linking here, I am just giving another example, which we have taken from the Kumamoto book. This is a system, where basically some hot tail gas is coming from calciner and it is basically through booster pen, it is coming to this quenching system.

So, were basically water is supplied using 2 coins pumps B or C and then it then passes through a [pres/prescriber] prescriber and this prescriber is basically here, there is one another pump which basically again further for water there.

So, water from the bottom of the prescriber, this is ok. This dish and water from the bottom of the prescriber is either recirculated by pump E and F. So, as Paul using pump the water is poured here. So, at the bottom there will be water that will be recirculated either pump E or F or other way there is a their they will be removed to the power stream. Now there is a Mesh, Mesh pad this is basically to remove the particulates in the gas and finally, after removal of these the gases flow to the absorber.

So, what is there then hot gas is coming. So, going through that quenching system then another water quenching then finally, it is basically going through mess pad for particulates removal and going to absorber and the whatever item following the water it is basically accumulated here, this is either recirculated by this one of the 2 pumps or it is basically taken out by spar stream.

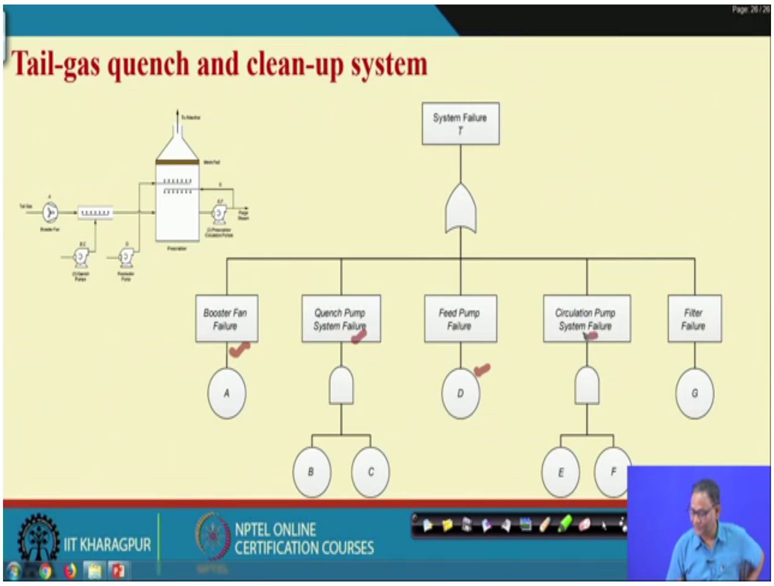
So, what is the system level objective here? The system is designed to decrease the temperature of the hot gas by water quench. So, because this gas is hot by quarter quenching, you want to decrease the temperature. So, here you are doing as well as here, you are doing then saturate the gas with water vapor. So, inside gas will be saturated using water vapor, then remove solid particles entrained in the gas, this Mesh pad, you doing this purpose.

Now, if I want to say what is the system will success then, all those, the 3 objectives must be fulfilled then it is system is successful, anyone abducting if you not your fulfill them system is a failure. So now, you can develop fault free for this. So, what is the system failure? If any one of the objectives this is not fulfilled that is failure. So, the mean booster fan does not work that also lead to failure, because tail gas will not come here and if the quench either of the quenching pub will not work then, temperature will not be cooled.

It feed water pump does not work, vapor that whatever the situation will not be vapor saturation will not take place, if the either of the pump will not work then this water will not be taken out for from this prescriber and recirculated, if the purge system will not work then also what is happening? That water is not going out. Now, if the Mesh pad will not work particulates will not be removed.

So, all those things ultimately means this is not working one of the two is not working, this is not working one of the two not working, this mesh pad is not working, all those things finally, lead to system failure.

(Refer Slide Time: 35:41)



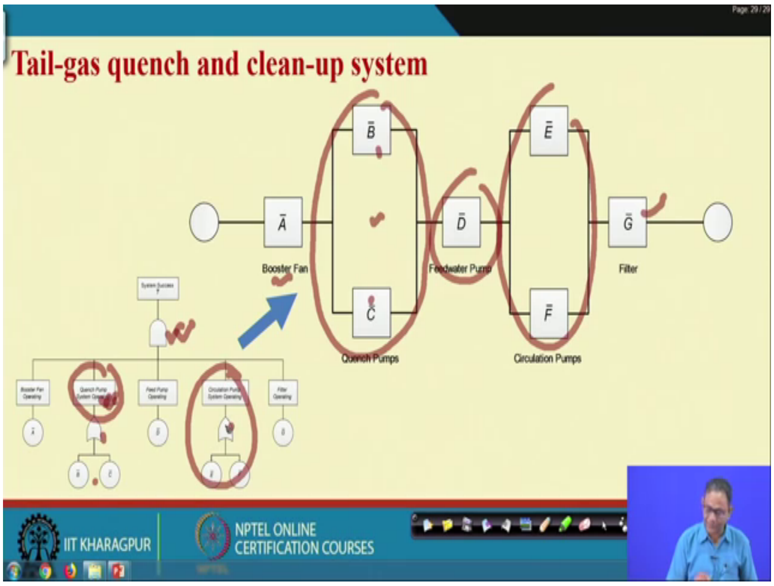
So, then what will be the fault tree? The whatever, I told in verbally your, in description that is what we have written in fault tree, you just see.

System failure this T, booster fan failure, quench pump failure, if both the quench pump does not work then, quench pump failure, feed pump failure, if both this circulation pump does not work then, this failure, filter failure that mesh pad failure. So, if these things happens only the top event will work, now if we want to see the your successful path or this is basic, this gives us the once you use the mucus algorithm, you will get the cut straight from this then what will be the success one? Success one, we can write like this system success T bar you see here, here we have used, when we are talking about system failure, we have used OR gate here and AND gate here.

When we are going for success or replaced by AND gate and AND gates are replaced by OR gate. So, that is the different regional success tree that was the fault tree. So, here basic even success, but basic even success is the basic event and probability of success should be computed in fault tree, probability of failure will be computed.

If you use this fault tree and use mucus algorithm, you will get the cut set path sets, if you used other fault tree that sorry, if you use this success tree, you will get the path sets if you use the fault tree, you will get the cut sets.

(Refer Slide Time: 37:29)



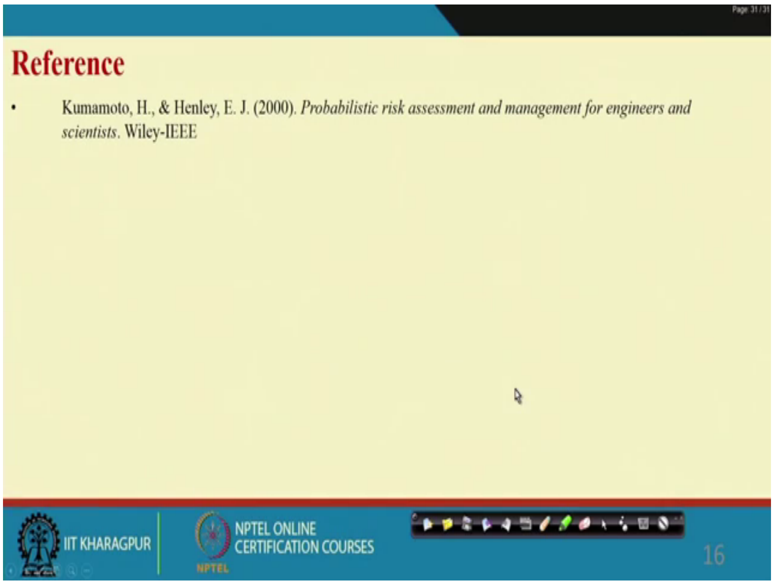
Now, this one can be equivalently represented by reliability block diagram ok. So, that is what is written here a booster fan, there is or gate parallel system, then and this one is basically with AND gate, in the series another or gate parallel this is with AND gates series.

So, here series and parallel systems are combined. So, this is a combined system. So, wherever if this is the AND gate. So, series issues are coming. So, if I consider this is together and these in series to these, series to these, series to this, series to this.

Now, this one related to this bomb because of OR gate, they are in parallel, if any one of the two is successful then what will happen? This that that quench spring pump is successful. Similarly, any of the circulation pump is successful, then this is successful. So, that is why in the parallel system ok.

Now, using this you can find out the probability, unavailability, reliability, MTTR and all those things the way, we have discussed so far ok.

(Refer Slide Time: 38:52)



So, I hope that you understood on this one and I as I told in the beginning, we have taken the lecture material from the book written by Kumamoto and Henley. Please go through this chapter, system safety issues quantification of system safety and go through the video lecture if and also participate in the discussion forum.

Thank you very much.