

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

**Lecture -17**

**Bow - Tie**

Let us start another concept, which is known as Bow-Tie. Actually bow-tie is not a new thing, it is basically combination of the fault tree and event tree, but it gives the holistic picture from the basic event failure to the accident scenarios at the end state. So, that is why the in first couple of years this has been very popular and I want to explain this bow-tie concept primarily with examples because, the basic principles underlying the bow-tie is already discussed that fault tree and event tree. Nevertheless let us know that this concept and utility of bow-tie.

(Refer Slide Time: 01:11)

The slide has a yellow background with a blue header. The title 'Content' is in red. Below it is a bulleted list: Introduction, Terminologies, Bowtie tool and management, and Example. There are handwritten notes in blue ink: 'Henley' with an arrow pointing to 'Bowtie tool and management', and 'Modarres' with an arrow pointing to 'Example'. The source text at the bottom reads: 'Source: Kumamoto 1996, Probabilistic Risk Assessment and Management for Engineers and Scientists'. At the bottom of the slide, there is a blue bar with the IIT Kharagpur logo and 'NPTEL ONLINE CERTIFICATION COURSES'. A small video inset in the bottom right corner shows a man in a pink shirt speaking.

**Content**

- Introduction
- Terminologies
- Bowtie tool and management
- Example

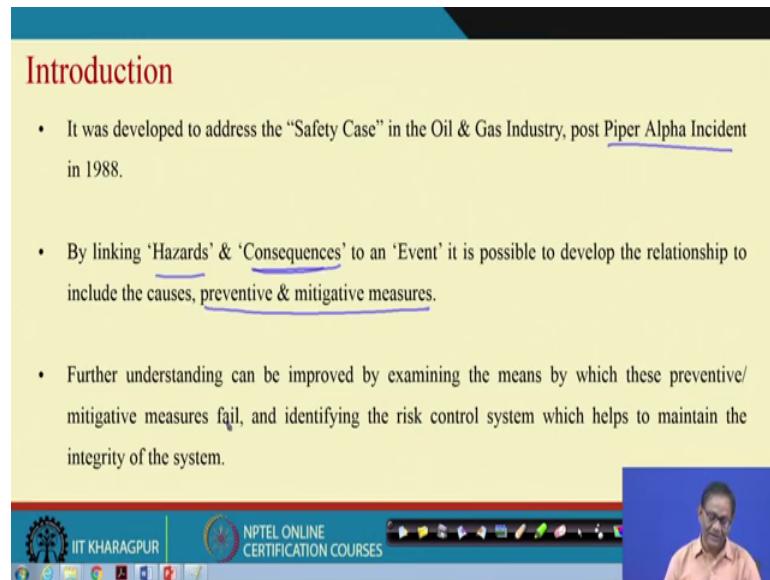
Source: Kumamoto 1996, Probabilistic Risk Assessment and Management for Engineers and Scientists

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So introduction, terminologies, bow-tie tool and management and several examples; so, that is what we will be discussing. And, although I have written here that the book written by Kumamoto and Henley that Henley Kumamoto and Henley so, but there is another book which we have taken into consideration that is by Modarres, so that is also reliability and risk assessment. So, later on I will show you the reference for Modarres also. So, we primarily rely on this two books and the concept of bow-tie and this is what is the discussion for the next 30 minutes of time and you will enjoy it because most of

the things already you know. So, to some extent it will be revise it to fault tree and event tree and another way it is basically the holistic view of for prevention through design also.

(Refer Slide Time: 01:29)



**Introduction**

- It was developed to address the “Safety Case” in the Oil & Gas Industry, post Piper Alpha Incident in 1988.
- By linking ‘Hazards’ & ‘Consequences’ to an ‘Event’ it is possible to develop the relationship to include the causes, preventive & mitigative measures.
- Further understanding can be improved by examining the means by which these preventive/ mitigative measures fail, and identifying the risk control system which helps to maintain the integrity of the system.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, if we go back to the history then it was developed to address the “Safety Case” in the Oil and Gas Industry, Piper Alpha Incident and after piper alpha incident, so far what I know that this bow-tie concept become popular. And in fact, the what I understand from the literature that in first couple of years it is increasingly popular. So, what it does basically as I told you that it basically links the basic event failure to the top event in the fault tree and then linking to event tree and finally, huge path the from basic event to the accident scenarios. So, if the accident scenarios is the ‘Consequences’ and the basic event side that the component level ‘Hazards’.

So, then what we basically say that linking from the Hazards and to Consequences that been the causes of Hazard occurrences and ultimately then, then up to Consequences. So, its relationship, the total relationship and at the another very important one is that it will talk about the preventive and mitigative measures requires for along different accident paths. So, it will also give you the total accident path, but it is very existing one. So, it is possible to develop, may be the, for the entire system.

So, maybe for the safety critical system or safety critical sub system you can go for this. Further understanding can be improved by examining the means by which the preventive

and mitigative measures fails. So, what I mean to say, you have preventive mitigative measures, but it can fail, how it will fail? So, that mean an identifying risk control system which helps to maintain the integrity of the system by integrity means mechanical integrity, operational integrity ok. So, this is what is basically the use of a bow-tie.

(Refer Slide Time: 04:55)

**Bow tie terminologies**

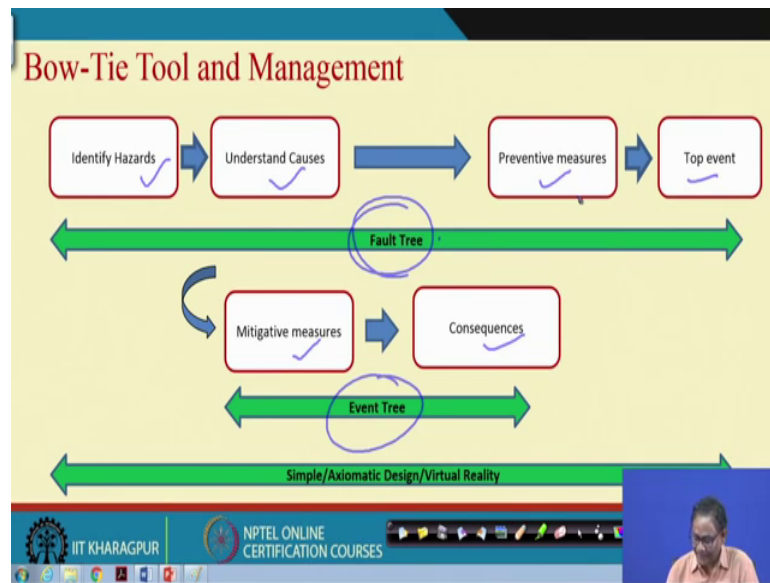
- **Hazard:** Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment (MIL-STD-882D).
- **Top event:** Most critical event when hazard is actuated
- **Basic Event:** What could cause the top event to occur ?
- **Consequences:** What could happen if the top event occurs?
- **Preventive measures:** What prevents the likelihood of cause?
- **Mitigative measures:** What prevents, minimize or helps recovery from consequence?

The slide is part of an NPTEL online certification course from IIT Kharagpur. A video inset in the bottom right corner shows a male speaker. The slide has a yellow background with a blue header and footer. The footer includes the IIT Kharagpur logo and the text 'NPTEL ONLINE CERTIFICATION COURSES'.

So, terminologies are very much known to you hazard you know top event, basic event, consequences, preventive measures, mitigative measures. So, what I mean by preventive measures; that means, actually when you talk about an any accident. So, the top event then whatever you do to so that the top event will not occur. So, that is basically nothing, but the cause will not occur.

So, similarly mitigative measure is the what you will do that the impact of an accident will be minimize it is nothing, but that you will basically minimize the impact or recovery from the consequences in one way or other way, these are the explanations. So, many a times I have explain all these things, so I do not think that you require further explanation here.

(Refer Slide Time: 05:49)

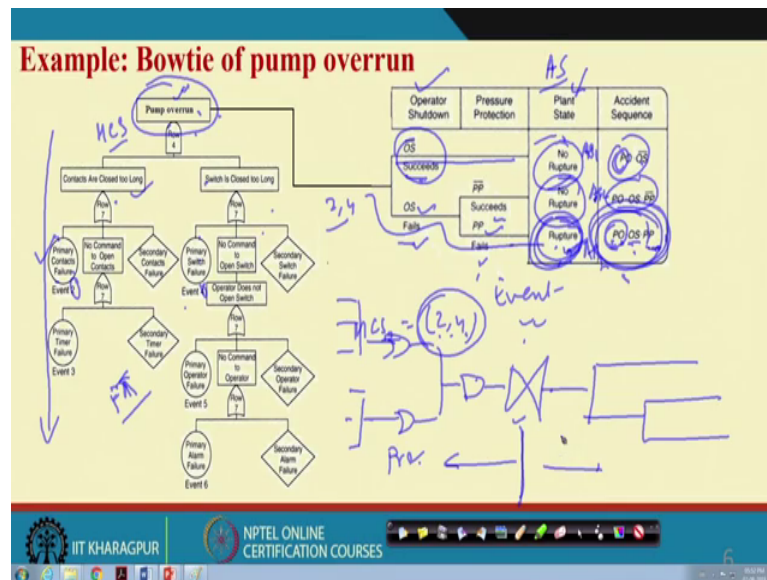


So, as I told you that particularly this bow-tie tool so; that means, it is from the hazard, then causes, then preventive measures, top event, mitigative measure, consequence. So, there the sequence and you see we are saying the top event with reference to probability when we are talking about consequence we are bringing the event tree. So, that mean fault tree and event tree will be linked and there are simple design axiomatic design virtual reality many things that can be added to their analytics.

So, all will ultimately leads to either identifying hazards or underlying the safety critical factors or under underlying the factors that contributes towards the hazard occurrence initiating mechanism all those things, then what kind of preventive measures, mitigative measures those things will be required. And, ultimately the risk control system and how risk control systems will be made operational, will be monitored and control.

All those things can be put together under bow-tie tool and management. So, that aspect bow-tie tool and management we will not be discussed in this particular lecture, but later on if will try, but I am not sure that we will go up to that bow-tie tool management part. And definitely you will be able to do it the reason is because, you have enough time after going through this course you practice this.

(Refer Slide Time: 07:27)



So, here we are again relying back to the system that is basically pressure tank system. Here intentionally I am created the top event as pump overrun because we think that the tank rupture is the basically the accident state. So, it is better you, you work on pump overrun because if pump overrun can be minimized important or can be eliminated that over pressure condition can be eliminated rupture will at least because of that deviation over pressure it will not happen. So, these part you have seen in my last lecture also that why pump overrun takes place because the current to motor too long because why current to motor too long because the contact the circuit is close too long.

And then contactor close too long, switch is closed too long. This way we have developed and then what I am saying that e pump overrun is my top event then what happened the overpressure condition will arise and in order to, in order to adjust the overpressure or fight against the overpressure condition or bringing back the overpressure situation to the normal c. So, there are different protection measures are there. So, like alarm is there alarm should work then operator should work. So, anyhow alarm is a signal only. So, we are not using alarm here that mean what I am straight way going that that will be under pump overrun situation the operator should work.

You can add alarm no problem, but for the time being I am saying that the operator should shutdown the system. If operator fail to operator shutdown may be may succeed, may not succeed. If operator succeeds what will happen then pressure protection that is

not applicable here because not required. So, they know that mean the relief valve case it is not required maybe because it is pump overrun operator shutdown, so that may not be required. So, then what happened no rupture situation will be there this is my plant state what the other way this is the accident scenarios, but if operator shutdown fails then what will happen over pressure that condition this will increase more gas will be filled then ultimate the relief valve should work. And, then if relief valve succeeds again there is no rupture again, although there will be minimum loss of that gas, but if relief valve fails the rupture will take place.

So, then I can tell you that if I know the MCS CR for the for the pump overrun the minimum cut state then every MCS leads to this and then the path is that pump overrun this takes place and this one is this one ways going to this, what you have done here you created bow-tie y one hand this fault tree fault tree another an event tree. This fault tree talks about y pump overrun event tree talks about if pump overrun takes place how your system behave against pump overrun to make to restore the normal c. If your that system protection measure fails then finally, the rupture situation accident situation will take place.

So, it is a beautiful way of looking into the problem. You may say I start with these and then ultimately one big fault tree will be there. So, that we have seen earlier, other way you can say no because tank rupture if it is the top; that means, everything has happened and a your preventive and mitigative measures are not that much differentiated, but here if I know that pump overrun to be adjusted. So, in order to adjust pump overrun what I will do that are mitigation that are basically mitigating the effect of pump overrun and then what is the accident path here.

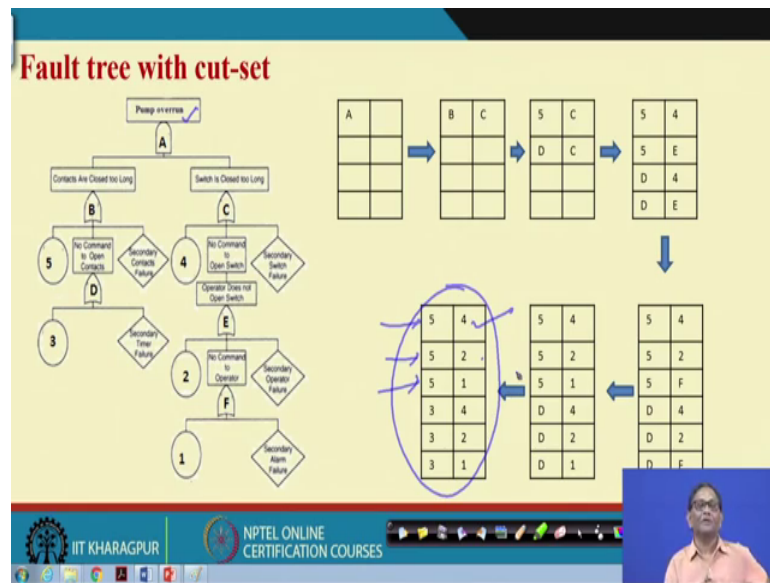
So, accident path will be suppose let us this event 2 occurs, this is row, this is and then one more event should occur here suppose event 2 occur. So, 2 and 4 will be the one of the MCS. So, MCS suppose this is 2 MSC 2 this is nothing, but 2 and 4. So, when 2 and 4, so, these 2 together along with this path will lead to no rupture, 2 and 4 happen here along with this path. So, 2 and 4 along with this path it will be rupture. So, 2 4 occurs here operator shutdown occurs operator shutdown fails means operator fail to shutdown and protection measure relief valve also fail then rupture condition will take place.

So, that mean 2 4 ways PP that 2 4 combiningly this is PO pump overrun, OS and PP they are all independent event. So, they are multiplied and this is: what is the accidents sequence and if you know the probability of this PO probability of OS and probability of PP I can know the probability of these accidents sequence ok. So, that mean this is accident sequence 1 sequence as 2 and as 3, but fortunately these two sequence are same no rupture condition. So, no rupture condition probability will be probability of these probability plus probability of these whereas, rupture condition probability will be this, so this is what is our bow-tie.

So, bow-tie what and this side event tree and this side if I just rotate this one with end gate what will happen you are getting 2 side here this and this then or gate here also OR gate, OR gate then 1, 2, 3. So, 1, 2, 3 again 1, 2, 3 these are all. So, this so ultimately what happen it looks like a bow-tie. It is a tie this is the tie. If I say this is my top event this bow-tie this top event then this side is basically why this event occur and this side what will happen if that event occur is this the, if I say that we want to prevent the pump overrun and then these whatever we do here, what you do if you can one casted this is 2 and 4 primary contact failure primary switch failure this is should not simultaneously occur.

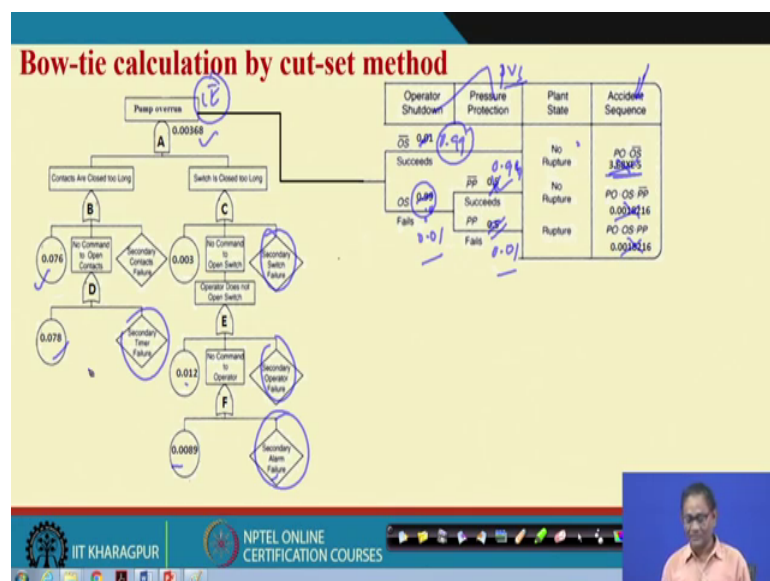
So, you put a prevention, so this should not occur then this prevention to this similarly there are several cut-sets. So, all cut-sets if does not occur then this will not occur. Now, question is that the preventive measures whatever you will put that also will fail. So, ultimately there is a possibility of (Refer Time: 15:01) of this then your protection system operator shutdown other things would occur. So, that pump overrun will not take place. So, this is nut shell what is mean by bow-tie.

(Refer Slide Time: 15:16)



Now, I will just repeat the case the cut sheet case for this. These are the cut-set earlier we have discussed how to develop cut-sets. I am not going into why not going into that detail of cut-sets. So, you say that there are 6 cut-sets two any this occurs this will occur this occur this will occur. So, what will be your preventive measures here you do something. So, that this two simultaneously these two simultaneously, this two simultaneously this should not occur ok.

(Refer Slide Time: 15:49)

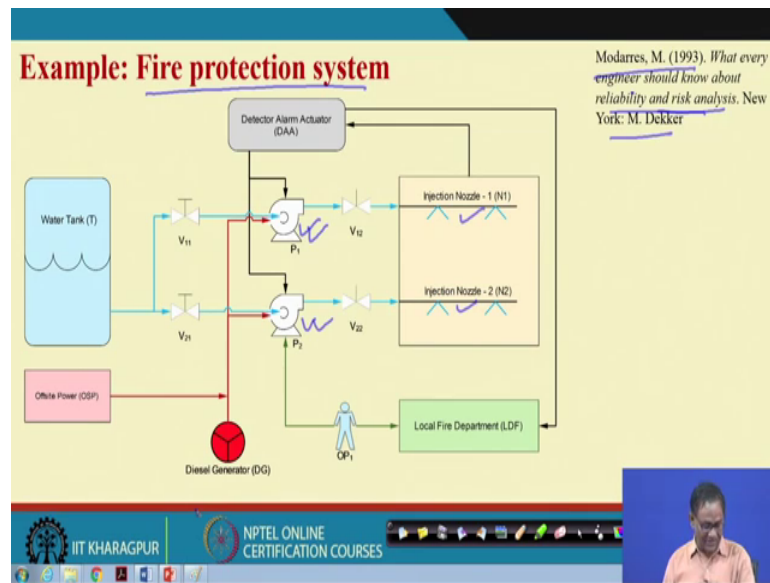


Now, what happened you may be interested to know that I want to know the probability of the accident sequence then you have the bow-tie. So, you first find out the probability of these then you know that what is the success of these and this one fails it should be it should be reverse success should be 0.99 and failure should be 0.01 and in this case, in this case 0.5 and 0.5, let means under over pressure condition, but these are these are very hypothetical value given, but it is better always this is very poor design is it also may be 0.99 and the fail 0.01, then what will happen 0.00368 multiplied by this will give you the probability of this.

So, you just change this one I am not sure this way the this value, but purpose was just to demonstrate, but the demonstration should be also practically significant because operators are do not suit succeed maximum the time. So, other way you can say; that means, you I want to give you, other way this can be integrated like this. If you give a here more probability that it will fail that we have not understand the system or the system is actually this is this is meaningless should not be there. So, similarly the protection measure this should work for the maximum number of situation V.

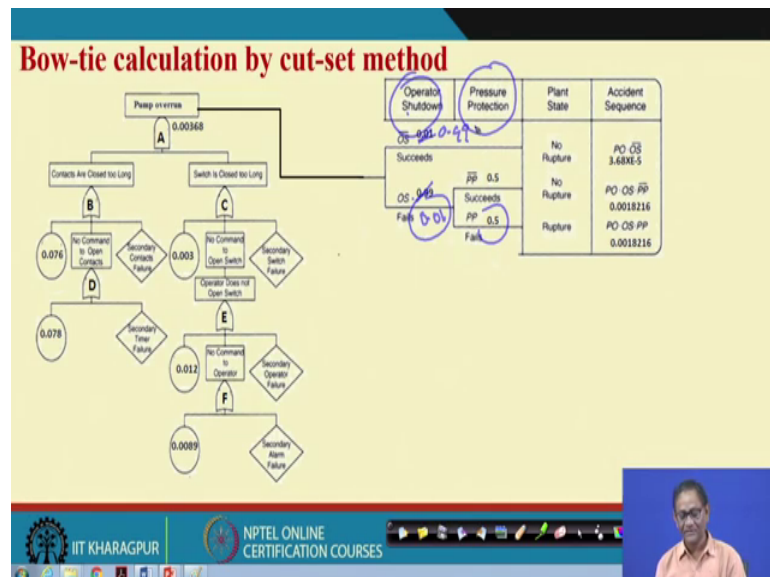
So, this is again is the clue. So, if you put more probability of failures, more probability of protection fail, this second fails this is not a good one. So, accordingly you change this one and as I told you this is the initiating event from event tree point of view and these are the pivotal events and these are the basic events, these are the secondary events secondary event means which are not known, so far the causes are underdeveloped.

(Refer Slide Time: 18:12)



So, now I will tell you another one. So, as I told you that bow-tie uses fault tree and event tree. Here we will I will show you that how fault tree is used inside the event tree because the protection configuration also may fail and then how do you find the failure probability of those. For example let me explain here.

(Refer Slide Time: 18:47)



Here what happen we are saying operators shutdown and we are writing that operator shutdown fails with 0.01 and succeeds 0.99 ok. So, now, how do you get this probability? So, that mean there maybe or pressure protection it suppose fails 50 percent

of the time. It should not be able, let it be like this, then how do you know this is 0.5. So, that means you can have a fault tree of these you can have another fault tree of these, provided these are there for those fault tree will be relevant and significant fault tree, otherwise if it is trivial then we do not do. So, that is what I want to discuss here. Here for this particular thing we have taken from Modarres 1993.

That what every engineer should know about reliability and risk analysis near. So, there he has given this particular system it is basically fire protection system that means fire already taken place now what should you do. So, that we will see protect your system from fire ok. So, see that there are different components like nozzle 1, nozzle 2 where injection nozzle which basically injects the water to the fire. So, that will be activated through that pump must be there which will supply water then pump 2, there are different valves, more important and importantly the water tank is there from where the pumps are basically sucking water and then providing to injection nozzle and injection nozzle will basically suppress the fire.

So, it is a kind of standby system. Basically if this does not work this will work or if both fail then ultimately the operator will call the fire department and ultimately there, there are offset fire source this fire source will not work then this DG system is there and; obviously, there is detection alarm actuator which basically helps in and doing the work. Now, let us read the operation details and so that so that what will happen you will understand how the system will work.

(Refer Slide Time: 21:07)

**System description**

Modarres, M. (1993). *What every engineer should know about reliability and risk analysis*. New York: M. Dekker

This system is designed to extinguish all possible fires in a plant with toxic chemicals. Two physical independent water extinguishing nozzles are designed such that each is capable of controlling all types of fire in the plant. Extinguishing nozzle 1 is the primary method of injection. Upon receiving a signal from the detector/ alarm/ actuator device, pump 1 starts automatically, drawing water from the reservoir tank and injecting it into the fire area in the plant. If this pump injection path is not actuated, pump operator can start a second injection path manually. If the second path is not available, the operator will call for help from the local fire department. However due to delay in the arrival of the local fire department, the magnitude of damage would be higher than it would be if the local fire extinguishing nozzles were available to extinguish the fire. Under all condition, if the normal offsite power is not available due to the fire or other reason, local generator would provide electrical power to the pump. The power to the detector/ alarm/ actuator system is provided through the batteries, which is constantly charged by the offsite power. Even if the AC power is not available, the DC power provided through the battery is expected to be available at all times. The manual valves on the two sides of pump 1 and pump 2 are normally opened, and only remain closed when they are being repaired. The entire fire system and generator are located outside of the reactor compartment, are therefore not affected by an internal fire.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

The study you see the system is designed to extinguish all possible fires in a plant with toxic chemicals I am taken it from this particular refer book. So, it is nd two the 2 physical independent water extinguishing nozzle that sorry, 2 physical independent water extinguishing nozzles are designed such that each one is capable of controlling all types of fire in the plant means nozzle 1 is capable of extinguishing the fire, nozzle 2 also extinguish takes place extinguishing nozzle 1 is the primary method of injection. So, whenever in fire situation nozzle 1 will work primarily. Upon receiving a signal from the detector alarm actuated device pump 1 start automatically.

So, the detection device is there it, it will detect that fire occurs may they move is the starting point. So, then immediately what will happen the nozzle 1 after may be the starting point. So, then you meet open the nozzle 1 the pump 1 will activate and pumping start. And nozzle through nozzle 1 the extinguishing will start. So, what way pump 1 start drawing water from the reservoir tank and injecting it into the fire into the fire area in the plant if this if this pump injection [FL] ok. Now what will happen if these pump injection path is not activated, pump operator can start a second injection path manually this is a manual 1.

If the second part is not available then the operator will call for help from the local fire department. So, there are 3, 1 is injection, 1 it is it basically get signal from the alarm detector start working if that that does not work then injection system 2 2 is there, which

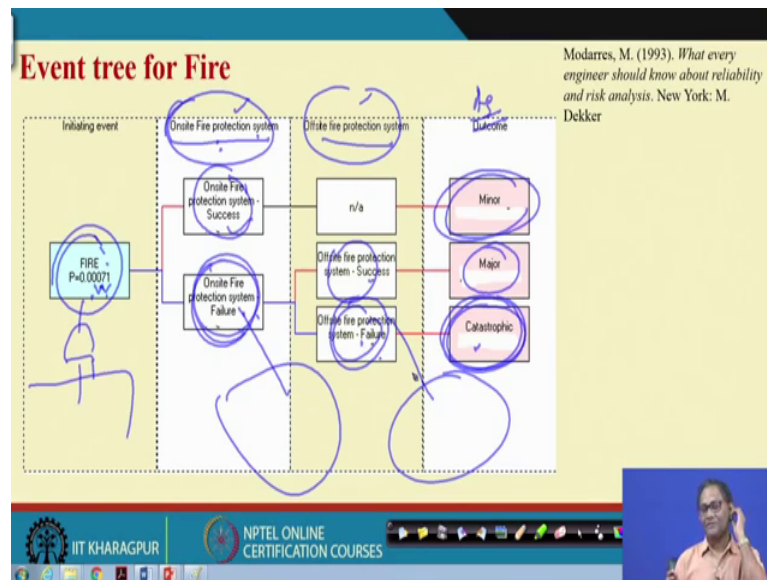
will be which will be operated manually by the operator. Suppose both the things fail then operator call the local fire department. However, due to delay in the arrival of the local fire department the magnitude of damage would be higher then it would be if the local fire extinguisher nozzles were available to extinguish the fire that mean if nozzle 1, nozzle 2, or nozzle 2 they can extinguish the fire the damage will be less compared to calling the fire department when these 2 system fails.

Under all condition if the normal offsite fire is not available, offsite fire normal supplied may be through the through the local grid. So, not available due to fire or other reasons local generator route provide electrical fire to the pump. So, there is standby generator set the fire to the detector alarm actuator system is provided through batteries. So, detected system will work whether it is fire is there or not, but these 2 batteries which is constantly charged by offsite powder.

Even if AC fire is not available the DC fire provided through the battery is expected to be available at all times. The manual valves on the 2 sides of the pump 1 and pump 2 are normally opened, only remain closed when they are being repaired, the entire fire system and generator are located outside the reactor compartment, so therefore, not affected by internal fire. So, now, I go back to this again. So, see this is the primary, primary system for fire extinguishing this when this one this one actuates after getting signal from the detector, if this fails the second one this one will work this one will be basically pump will be activated by operator, if both fails local department will be called.

And you see that the pump 1 and pump 2 takes water from water tank there is always offsite fire available, in case offset fire not available, diesel generator will basically provide supply fire and the battery to this systems are always basically recharged and it is available even if the electric fire is not available. So, my your work is basically. So, you want to know that how good your system is to, to protect the fire, to extinguish the fire from greater damage. So, it is basically see the fire occur mean accident has already occurred. So, that mean it is basically a we are talking about when an accident takes place how your system behaves. So, this is basically event tree issue initially.

(Refer Slide Time: 26:12)



So, what we will do? We will first prepare event tree. So, let us hope that the fire how it occurs that fault tree is known and the very small probability that fire will occur in the system. Now there are two things, one is onsite fire protection system and offside fire protection system you have seen that onsite and offsite fire protection system because nozzle 1, nozzle 2 onsite and otherwise local fire department will come. If onsite fire protection system is successful then offsite is not declared. So, outcome or accident scenario will be that minor damage.

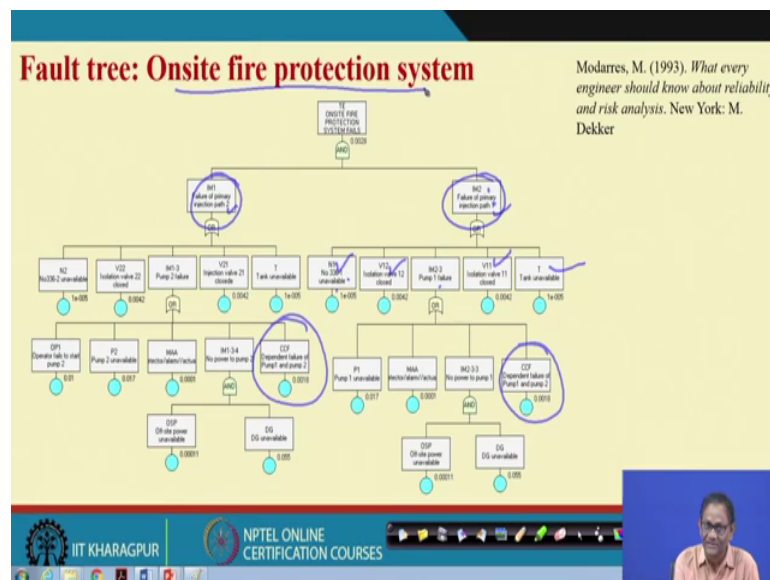
If onsite 1 is failure offsite fire protection system may be successful, may be failure. If it is successful major damage will be there, if this also are successful catastrophic things will happen. So, this is my accident scenarios. Now, here in this example I want to show you that that how the success of these or failure of these also an issue because this is basically protection measure there is success and failure. Now, you can use fault tree here, you can is fault tree here then you can find out success and failures.

So, 1 fault tree you constructing here for the system while how fire will when fire will take place what is the probability of fire occurring then if fire occurs whether onsite protection measure works what is the probability that it will not work what is the probability that it will work. Similarly, if onsite fails whether the local fire department will and extinguish or not probability of being a failure, so that mean this probability

times this probability times this probability will give you the probability of catastrophic in nature ok.

So, that is also that is ok. Now, in the you have the entire bow-tie for this one may be another fault tree is there and this side also now here for this for, this here another fault tree for this fault tree. So, I mean fault tree and event tree in combination you are in able to find out all possible routes of failure the preventive measures mitigative measures, all those things are very possible ok. So, I will what I will do I will show you that the this these 2. Suppose the onsite protection measures fail, so, that mean this one fault tree that they 2 will fail. So, this is this one.

(Refer Slide Time: 28:58)



The onsite protection measure fails, failure of primary one, failure of second one, primary injection path 2 primary injection path 1. So, path 1 mean the nozzle 1 you see that these are the things this failure that nozzle failure, valve failure, another inlet valve outlet valve, tank not available. So, all those things lead to failure of these and pump failure also lead to failure of these, but pump failure depend on many other things and similarly here your, but these both the pump are identical.

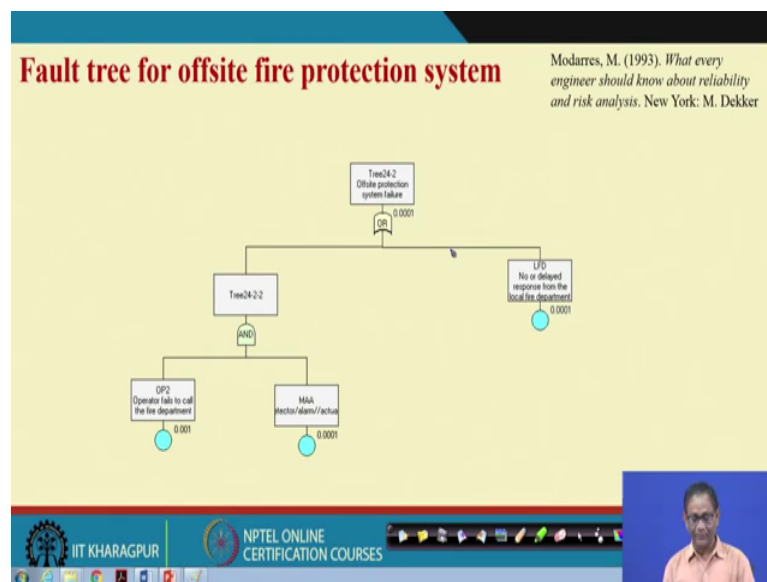
So, that mean the pump failure what will happen you will find out that that there will be common cause let it be there will be common cause of failure because pump failure there will be common cause of failure. So, that is why what happened it may be a situation

when there are certain causes which cause pump 1 2 fail as well as pump 2 2 fail that situation will has to be taken care of here.

So, here one additional thing you are learning that all the basic events it not that it is basically to going to do something separate top events or intermediate events. There are certain things which ultimately maybe applicable to a different intermediate or finally, leading to top event. For example and those things to be looked into matter you have to see that those common causes should not be should not be eliminated maybe in one side of the fault tree you use it in other side you have not use it that should not taken place.

So, now see we have we have given a common cause failure that dependent failure of pump one pump 2 in this side also and in this side also. So, there are there are method how to find out the common cause failure and you have to do it, but for the for the sake of simplicity we have not added here this common cause how this common cause that dependent failures are quantified we have not given to you here ok. So, what I mean to say this is basically onsite protection system in that fails this is given like this. So, that mean fault tree again you are using fault tree within the event tree.

(Refer Slide Time: 31:34)



Now, you can find out the offsite on the also that will fail um. So, in a similar manner you find out the fault tree for this event tree for this. So, that mean what i mean to say what I have shown you here not only fault tree here, fault tree here fault tree for this, fault tree for this also because otherwise how do know it is working the pivotal events

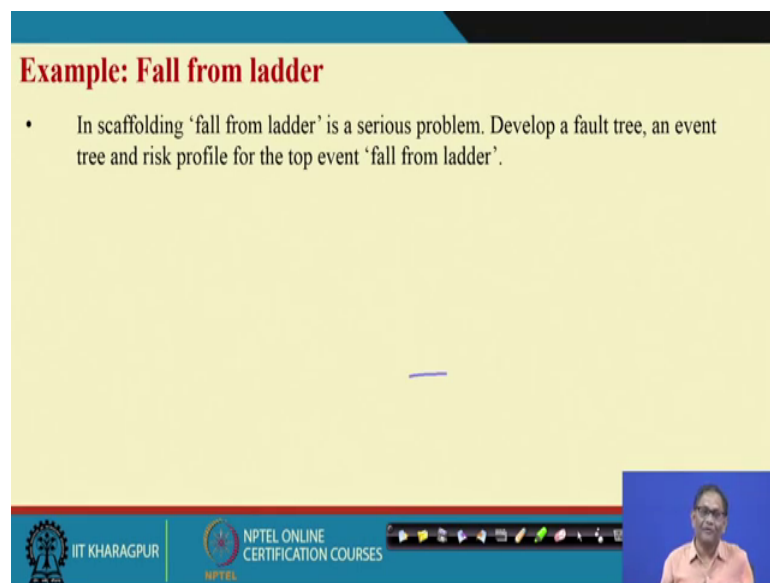
are working or not. Suppose you say we have onsite protection measure then you must know when onset protection measure fails how do know it you will know from this.

Now, you have to develop the cut-set for this and then you will know what are the events that if occur will lead top event to occur those events should not occur simultaneously ok.

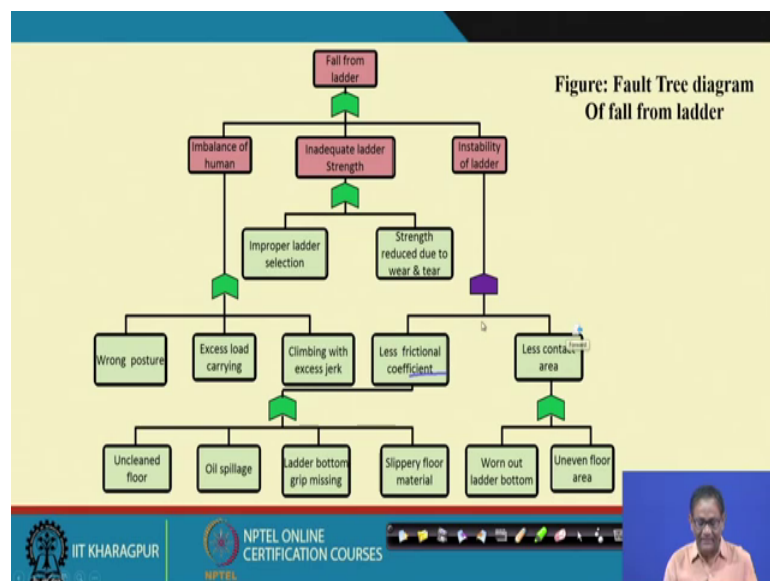
(Refer Slide Time: 32:28)

**Example: Fall from ladder**

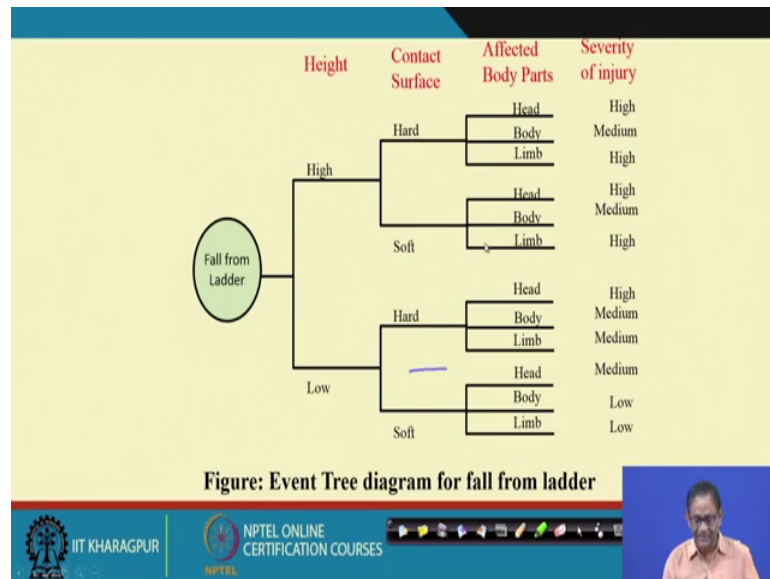
- In scaffolding 'fall from ladder' is a serious problem. Develop a fault tree, an event tree and risk profile for the top event 'fall from ladder'.



(Refer Slide Time: 32:33)



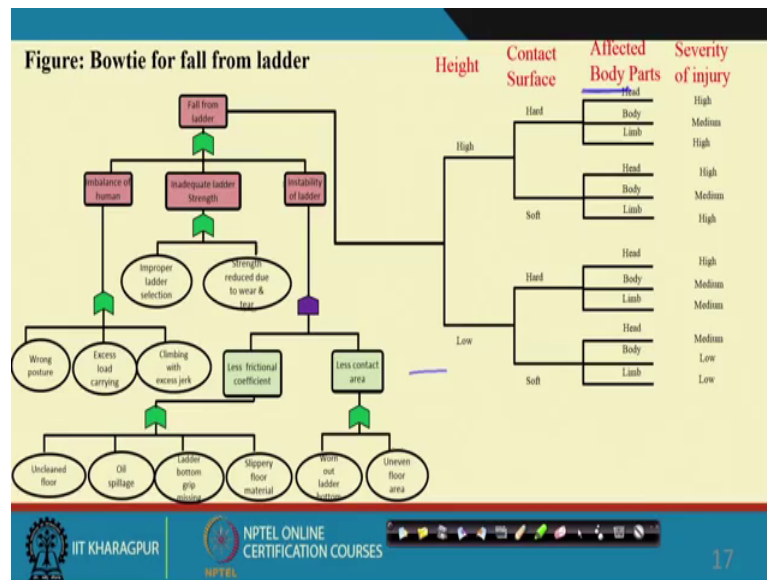
(Refer Slide Time: 32:37)



So, many a times we give this example fall from ladder. So, you see that fall from ladder, why fall from ladder, this fault tree, and that this I have explained earlier also then fall from ladder what will happen depending on the conditions. Here actually not protection configuration, here basically under what condition this event can take place whether from which site what is the contact surface and all those things and then which body at very effective then accordingly the severity or the consequence has been different it is primary basically related to injury severity ok.

So, that mean in not necessarily that you will use only for the high more technology oriented situation the bow-tie. It is not this is an example that which basically can be used also in a manual job or semi mechanized kind of job also this bow-tie can be applied, so this that is why this application I have kept.

(Refer Slide Time: 33:29)



So, now these two when you combine together this is nothing, but bow-tie for fall from ladder. So, my ultimate aim of showing; so, many bow-tie just to tell you that bow-tie can be developed for almost every system for to understand the accident scenarios. Understanding accident scenarios means knowing the path from hazards to accident and when you have safety critical system it is better to use bow-tie, bow-tie in the sense fault tree and event tree together.

By saying fault tree and event tree together, it is another simplification of bow-tie, it does not mean that bow-tie always requires fault tree and event tree. The issue is that bow-tie basically links the preventive site and mitigating site preventive measures and mitigation measures. So, you may not apply may not develop also fault tree and event tree, you may adopt some other techniques to identify the causes of the accident and to identify that how the system behaves when accident takes place absolutely no harm. So, that since bow-tie is more versatile. So, here the cut-sets we have developed and this part you know and then finally, the quantification part this is again the repetition so, but the repetition for the for the benefit of you not benefit of anybody else.

So, thank you very much. So, in nutshell I said that bow-tie is an important tool for safety engineering particularly if you are interested in prevention through design, because from the cause to consequence and for the safety critical system, it is a wonderful tool. So, I recommend all of you understand fault tree and event tree take

safety critical system develop the thing and all and generate all the all the accident spots understand cut-set from the bow-tie fault tree point of view, then understand cut-set from the accident scenario point of view I will be discussing the cut-set for accident scenario in the next class. So, be careful attentive in the next class.

Thank you for listening to me, thank you very much.