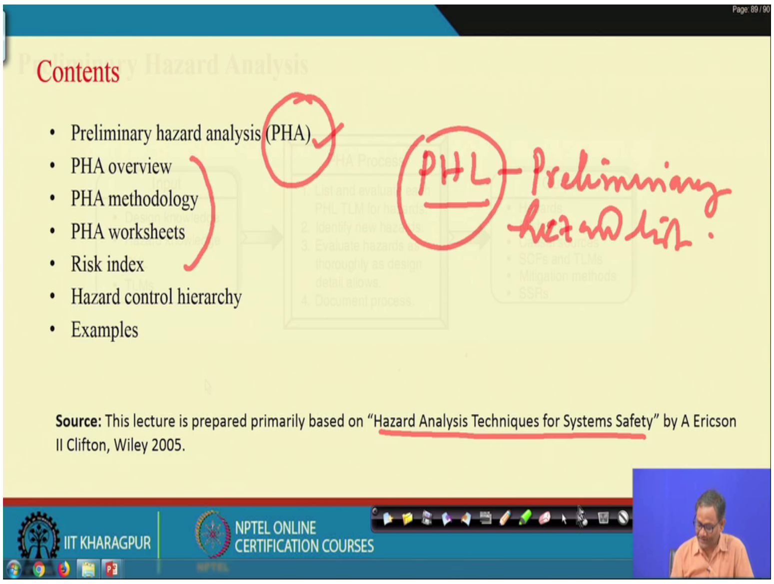
Industrial Safety Engineering
Prof. Jhareswar Maiti
Department of Industrial and Systems Engineering
Indian Institute of Technology, Kharagpur

Lecture – 07
Preliminary Hazard Analysis

Welcome today's lecture Preliminary Hazard Analysis.

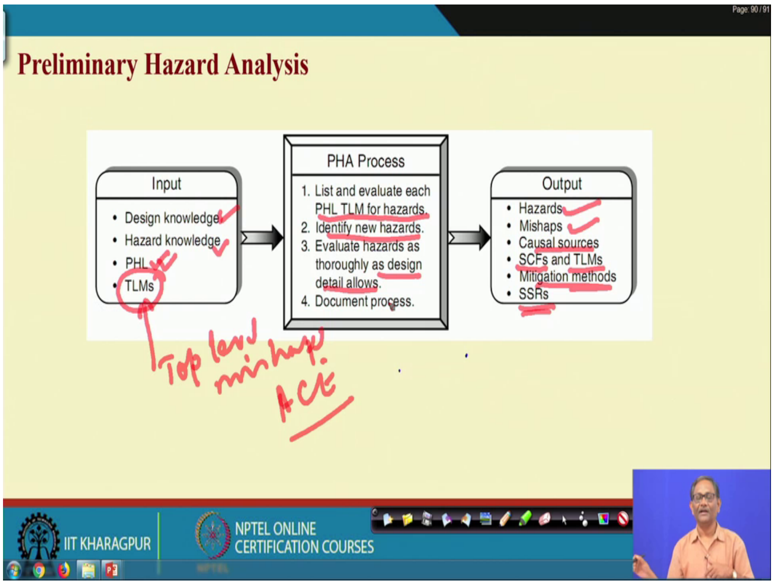
(Refer Slide Time: 00:29)



The content a Preliminary Hazard Analysis; actually we will discuss only PHA Preliminary Hazard Analysis. So, under this, these are the few things which are part of PHA: one is overview, then what is the methodology, the worksheets you require to represent the PHA, document PHA. And then risk index hazard control hierarchy some examples will be given to you obviously the same book hazard analysis techniques for system safety.

Please keep in mind, those who are first going through PHA without PHL without PHL preliminary hazard list, my previous lecture preliminary hazard list you will face problem. So, I request all of you first go through PHL, if not gone through and then understand PHA. This PHL and PHA they are basically very much related thing PHL is the input to PHA.

(Refer Slide Time: 01:53)



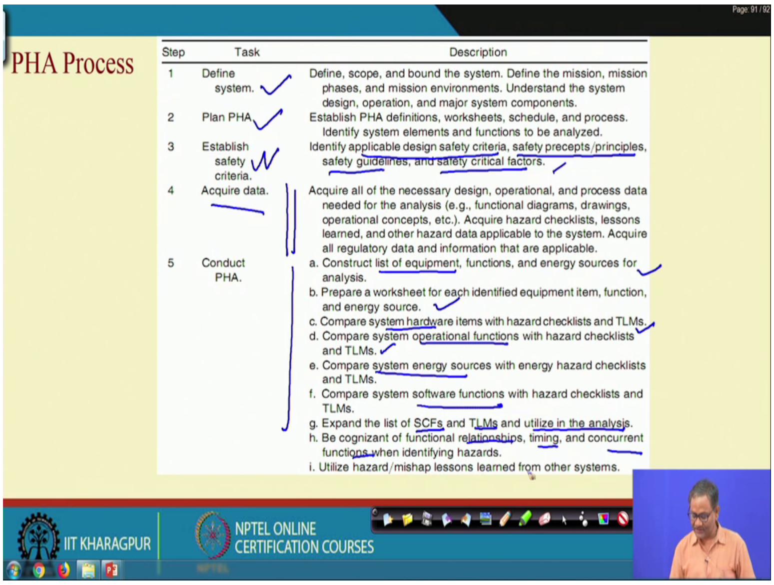
So, let us see that you see I told you if you recall that in PHL also this kind of process diagram I have given. And in PHA also it is given. And in PHL I we are given that design knowledge then hazard knowledge and then listen slot.

But in PHA design knowledge, hazard knowledge, PHL is the input preliminary hazard list and this is top level mishaps; top level mishaps ok. So, if we consider the ace missile system the example what I had given earlier they are one of the stop level measure with missile structure that that crash. So, similarly that is during launch then flight similarly the fire in the ground operation missile structure that fire. So, in the same manner if we go look into the example of pressure tank the top level measured will be pressure take rupture ok.

So, these are basically top level mishaps. So, top level mishaps are inputs to PHA. What are the outputs? Hazards that is I have already also seen in PHL, then accident you have seen in PHL also, causal sources that also you have seen there that safety critical functions and top level mishaps. That is what is basically will put here output here, but we are not discussed that details then mitigation methods and some get safety reviews. So, all those things are the output. And how do you do this PHA process? List and evaluate each PHL PLM for hazards, you have PHL 1, PHL 2 like this in SMS solution there are 50 PHL preliminary hazards.

So, every PHL there will be some top events top level mishaps. So, you have to list all them, then you find out if there is any new hazards then evaluate hazards through thoroughly as design details allows and document the process. So that means, it is intertwined with the PHL the PHL process and PHA process theirs they are they are basically overlapped one, but PHL will help you in doing PHA in a better manner. So, sometimes what happen we do not look PHL we will do PHA starting from the first step of PHL and end of PHL.

(Refer Slide Time: 04:55)



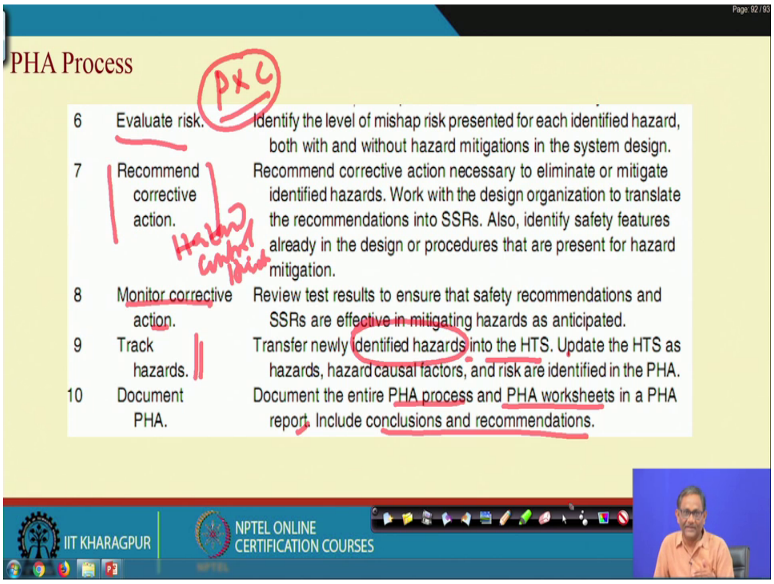
So, you just see the steps define systems you have seen in PHA plan, similar to PHA establish safety criteria it was not there identify acceptable safety design criteria safety pa precepts principle safety guideline and safety critical factors. So, that you have to establish then you acquire data and I have told you what is this acquire data for a ok. Obviously, you are saying that couply safety design criteria like safety factors ok. So, safety perception safety principles; so all different there can be many principles many go companies followed ten to fifteen principles ok. Inspection is one principle, HIRA is another principle like many things there are safety guidelines.

And obviously, safety critical factors related to human error software hardware and the interface all those things will take place here. Acquire data fine that you understand and conduct PHA see construct list of equipment function it is like PHA, PPR worksheet for each identified equipment item like PHL. Compare hardware with hazard checklist TLM, PHL compare system operational function with work hazard checklist TLM. So, operational function, hardware, energy sources then software function all you compare these already you have seen in PHL.

But suppose you have not gone though PHL you want to do generally. So, then all those steps you have to follow. And I request all of you to first see my PHL lecture preliminary hazard list lecture then follow this one.

Expand the list of safety critical factors or TLM and utilize in analysis in PHL you found out the safety cal critical factors and top level mishap, what here you expand the list. The cognizant of functional relationship timing, concurrent, function I have already told you that dependency between components, it is one layer to another layer now utilizing hazard and mishap relations learnt from other systems.

(Refer Slide Time: 07:26)



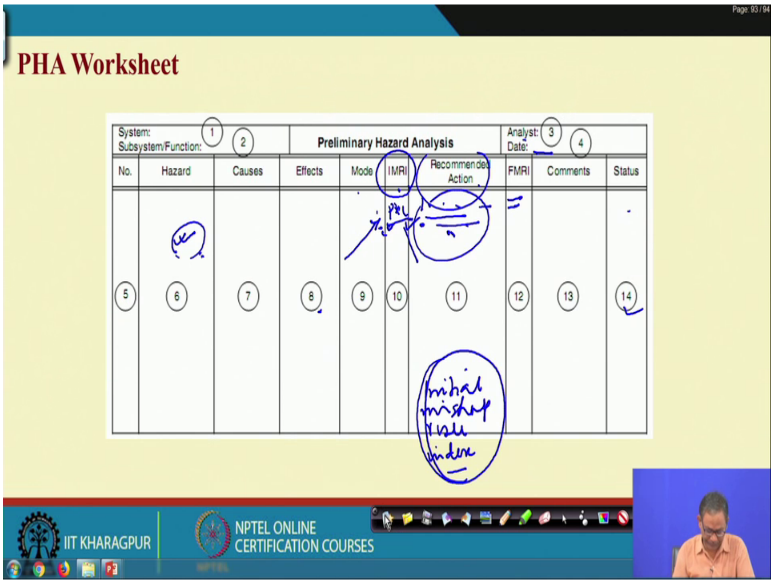
Then few things which are basically new, what is not there is PHL evaluate risk. I told you risk I told you risk is probability times consequence, these principle will be used in here for every PHL every hazard then recommend corrective actions. So, what do you want you want to you want to do something, so that the risk will be minimized.

So, they are that is why I have kept one concept in the lecture that is hazard control hierarchy, hazard control hierarchy. So, you have to once you evaluate reason if it is unacceptable suppose whatever may be the level of risk you want to reduce it, then you require to give some actions to take some actions to give some suggestions. So, some control measures, so using hazard control hierarchy you can get some control measures.

Then monitor corrective actions, review test results and ensure that the safety recommendation and SSR are effective in mitigating hazards as anticipated which basically once you improve it must be monitored and maintained, then track hazards. Whether the hazards are still occurring or not transfer newly identified hazard into the HTS update the hazard top and ok. So, what I mean to say that that if you have any identify new identified hazard you just feed into the list. Then document the entire PHA process and PHA worksheets in the PHA report include conclusions and recommendations.

So, these are these are guidelines, so how to do PHA. So, what I told obviously, these are descriptive. So, once you read further you will know that what things are there, but please follow this steps that is what is the issue here.

(Refer Slide Time: 09:53)



Then when you try to document the documentation is having how many components, 14 components first is system subsystem function [FL] what is the system what subsystem, then who is the analyst, who is date they are the minimum basics. Then number it will come from 1, 2, 3 the post system number, then suppose hardware number item one what are the different hazards.

Hazard one what are the causes of that hazard one? Then what are the effects of hazard one? What mode means, when it has occurred may be is it during the operation or during the maintenance or may be during in case of SMS case during flight during ground operation where it is. Or in case of the material handling system in a in a steel plant where it has occurred during when the torpedo on the track going to ladle or basically it is the (Refer Time: 10:59) shown in the ladle.

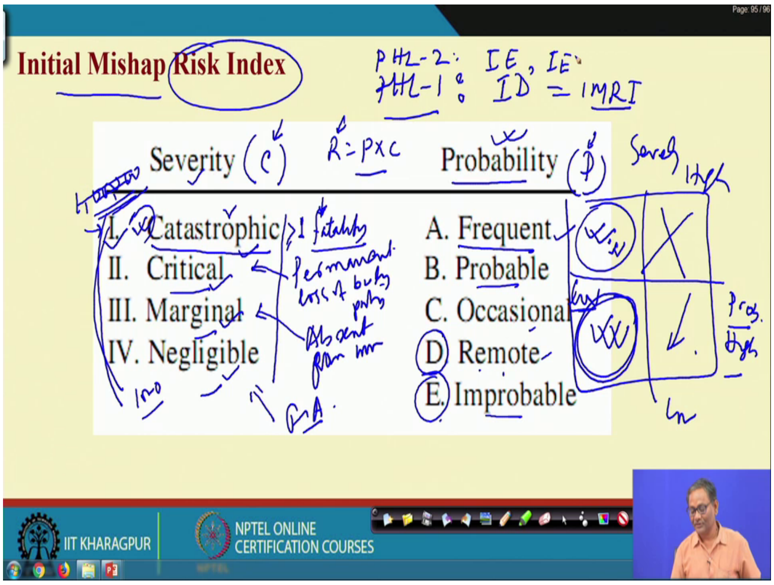
So, where it is show that since IMRI, IMRI stands for initial mishap risk index. So, that mean you have to know the hazard; what is the probability occurring, and what is this consequence, then that multiplication of this P and C will give you initial hazard mishap risk index.

Then what happened here you want to reduce this risk then either you reduce the probability of occurring or consequence of that event or both. Then that recommendation may be related to prevention related to mitigation, when you are you are basically giving recommendation to reduce the probability, then the hazard will not hazard will not occur the probability of reducing hazard occurrences that is the prevention.

When you are thinking hazard occur, but it is consequence can be mitigated then it is basically mitigation. So, it can both, so then you find out the preventive measures, mitigating measures then you put here, and then what will happen if both preventive and mitigating measures found out then this both P and C value here it will be reduced.

I will show you with one example how this done, and then you have to give the comment. Comment means whether that is implemented, recommendation implemented or not or what is the feasibility cost component of those things you can write and under status you write the implementation status. If it is implemented closed if it is not implemented open under comment you can write many things whatever you fit find relevant. So, in PHL we have given a very small documentation item I think 5 6, but in PHA 14 items to per hazard you have to write down 4, I 4 items are common 5 to 14 10 hazard specific information you have to give.

(Refer Slide Time: 13:29)



So, now the issue is that how do I find out the initial mispah risk index or risk index there are many ways to find out risk index, but here a subjective or qualitative way of risk index calculation is there. Severity is the part of consequence probability P probably as we have told that risk equal to P into C. Now, finally, that can be this can be come once you know the probability in the quantitative term and consequence or severity in the quantitative term, then risk will also be in the quantitative term. So, that is quantified risk which is basically objective in nature then it is quantitative risk assessment.

This scheme adopted in PHA is usually qualitative risk assessment not quantitative risk assessment, because quantitative risk assessment requires data of probability and consequence values. And that too for every top level accidents or every hazard you have to find out it will be huge task. And at PHA is done usually at the system level, but in comprising all the component system subsystem to get an idea first that what is the hazards la hazard level, then what are the different kinds of hazards available in the system.

So, that a existive list of hazard can be found out. So, then they are index risk value maybe given in a qualitative term. By qualitative term what do we mean is given here, severity can be have can have four different categories, catastrophic, critical, marginal, negligible.

For example we may say if there is a fatality suppose one or more fatality that may be catastrophic. Or sometimes people say it may it is catastrophic even not one more than one fatality is a, but fatality is a big issue. Critical we can say from human safety point of view from human safety point of view critical may be permanent, permanent loss of body parts. If deterioration may be your eye or something like this marginal which is which may not be leading to any kind of um the disability, but it making maybe absent from work, absent from work negligible means maybe first aid kind of thing first aid.

So, but you may say that no my system is such that it is not the human safety only it is a loss control point of view that human property environment all will be important. Then what you have to do? You have to you may find out the equivalent, equivalent that law quantification or loss in terms of money ok. So, maybe human's loss then your property loss, environment loss or loss in com compute and then find out your categorization of catastrophe critical marginal like this.

For example if a accident can cause suppose rupees 1 lakh or more, 1 lakh or more um, 1 lakh means basically or a or if you say one million Indian rupees then it may say it is catastrophic, but negligible if it is the ultimate loss is 1000 rupees Indian rupees. So, that conversion is also possible. But if you can make in terms of money then it is quantitative. So, what I mean to say qualitative means you have you must have an idea that you loss value beyond certain level is catastrophic within certain level is critical, within certain level is marginal, within certain is negligible. Usually from severity in terms of human safety is considered. So that means this is a four point four point scale for severity.

Similarly, probability it can be quantitative can be qualitative, qualitative mean frequent. Suppose the work has been done 100 times, 10 times it has that incident is occurring very frequent. Probable may be if I say that four times only 4 to 5 times probable out of hundred occasional may be 2 to 3 and remote may be 1 2 improbable less than 1. So, something like this, but at the qualitatively you please understand that there is no in qualitative risk assessment for the severity scale as well as probability scale there is there is no reference point ok.

It is basically used for ranking purpose, so for my own system, but considering hazards if I stick to this. Then when I compare first risk all with the second hazard risk then what will happen it will the difference ultimately is significant not the individual value difference will be significant therefore, for improving the for ranking.

But from improvement point if view, if catastrophic severity is there it is to be reduced definitely, otherwise do not do this work. But that means, if your this thing cannot be reduced then it should be E improbable the P principle is like this if I say this is my probability and this is my severity. Then if I say this is high and this is low when this is high and this is low and high probability high severity high probability high severity means catastrophic and frequent impossible this quadrant big 0, it is impossible.

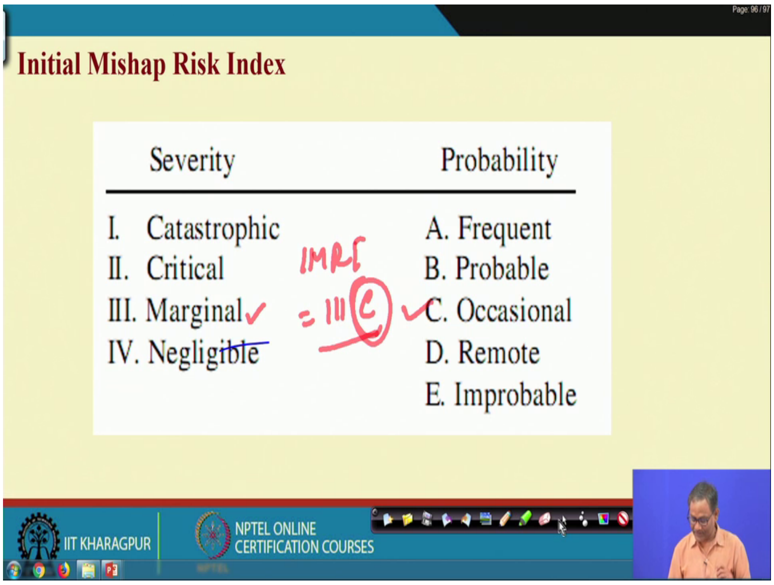
If your system is having this that means, this is not a working cannot people cannot work there then here probability is low severity is high it may be there. So that means what happened probability low severity high. So, your severity must be reduced your prevention measure will be severity oriented here.

Now, probability severity both low this is the most desirable one and you find out that in ee in general or day to day all activities will fall under this. And here probability high and severity low that must be there, here what happened you reduce the probability. So, action here I think it is inoperable system action here reduce them catastrophic nature or the severity, action here reduce the probability action here I think it is the risk level here fall under acceptable job.

So, that means, what happen for every hazard suppose PHL 1 you know what is the hazard, now you have to see that what is the probability that it will happen. So, you may say it is remote then probability value is D, if it happen what is the consequence you say this catastrophic then it is 1 D. This is my initial, initial risk index in this manner in PHA risk index is written, for the second hazard suppose PHL 2. So, you may say for example, have PHL 1 the missile body that that crash be catastrophic, but it may be remote possibility.

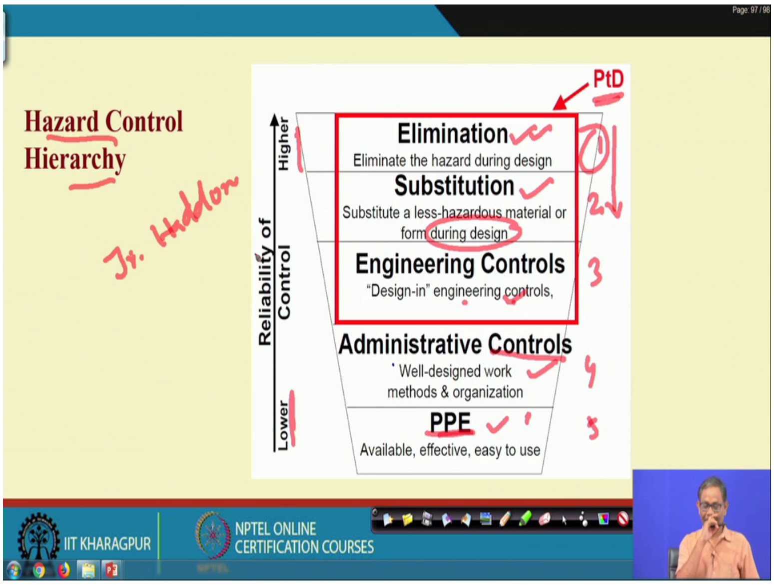
Suppose the second one that the when I can say the tank rupture that also will be catastrophic, but this probability is again remote or improbable, men maybe the when the material handling the torpedo is going. So, if there is there is the there is a fracture rupture in the torpedo what will happen it will again it may again lead to catastrophic and, but it can it may be improbable ok. Suppose you just think of that somebody is carrying something. So, there is a possibility of slip and fall it may be occasional it maybe occasional.

(Refer Slide Time: 22:45)



So, slip frequent fall that may be see occasional, but if you go by the consequence it is mini marginal. So, then the IMRI is three C, here you may be interested to reduce this one ok. In this manner initial risk index is complicated once you have the risk index then what is the next.

(Refer Slide Time: 23:12)



Next is how to reduce the risk, so here is the concept called hazard control hierarchy, hazard control hierarchy. So, for I know Junior Haddon, Haddon has given this that means that elimination, substitution, engineering, control then administrative control, personal control this is the five stags. Elimination means eliminate the hazard during design that is the concept of PT.

That during design before designing then at the design group if you understand if you have done PHA, then all the hazards are known consider one hazard and then see that whether this hazard can be removed at the design stage if it is remove it. Now that is what we say that elimination for example, working at height. If the work can be done at the ground floor the flow did it done there, even though you know working at height if you do at the height it will be better from the efficiency point of view, but from safety point of view it is not.

So, elimination is there if you cannot eliminate substitute a less hazardous material or form during design please keep in mind during design ok. It is now elimination not possible working at height cannot be eliminated totally some case it will be there, but please understand that. Suppose the maintenance percent is equate to carry certain material, so can it be eliminated, so the load part can be eliminated.

So that means, that little less that is substitution for example, the pressure tank system you are suppose the instead of gas you are using toxic gas, now toxic gas is the hazard. Now if the for the operation point of view for the pneumatic control machines what the gas will be used, who will be used whenever the gas will be used here it requires ordinary gas tank. Then what happened instead of toxic gas you are using ordinary gas, but you are using toxic gas we get toxics may be available which is produced by your system. For example, a in steel plant what happens co carbon gas, LD gas blast furnace gas they are all toxic gases particular co carbon gases.

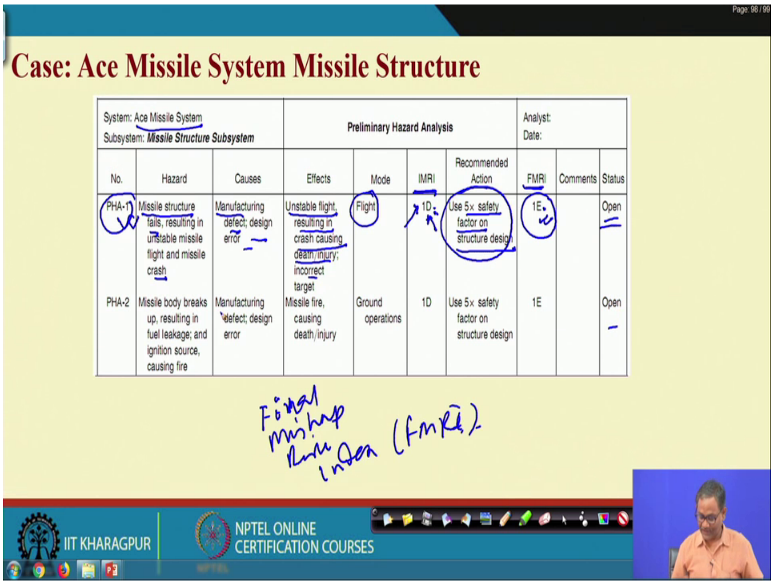
So, these are these are ka plenty of such gases available. So, in another place where you want to suppose pressure something in those gas, but please keep in mind if instead of that coke gas co carbon gas some other less toxic gas or no toxic gas available it is better to use this is the case of substitution. Then engineering control design in engineering control, engineering control basically what do you mean here you are you are not able to eliminate the hazard or substitute the hazard you have to work with the hazard.

Now, from energy control point of view air quit the hazard means suppose the pressure tank the pressure gas you will be using. So, that mean you must have some control, so that the over pressure condition will not occur ok. So, overpressure condition will not occur provided some mechanisms are put let there be you have seen already pressure gauge is there alarm is there, so relief valve is there they are basically for what purpose to avoid the overpressure condition. So, these are all engineering controls.

Now, elimination substitution or engineering control later on we will be discussing in detail when we discussed that safety function deployment, I will discuss in detail how it will be done. So, for the time you understand these three are basically you consider the PTD prevention through design. Whatever PTD you adopt all administrative control is also a must. So, for every hazard what you identify, for some may be PTD related solution somewhere administrative solution is also related, so those you will find out. So, well designed work methods and organization in administrative control say SOP must be available, SOP must be adequate, SOP must be followed all those things how do you know it is a administrative control only can do it.

Then last, but not the least PPE is also important because occurrence of hazard is a probabilistic event, whatever you do there is a chance. So, PPE must be used it is basically least effective, but it is a must. So, reliability of control if you see the elimination is the best method PPE is the worst method, but this lower reliability to higher reliability. So, your order of execution should be rank 1, rank 2, rank 3, rank 4, rank 5, your execution order will be like this first this is reliability effected by (Refer Time: 28:44) I hope that make this make sense.

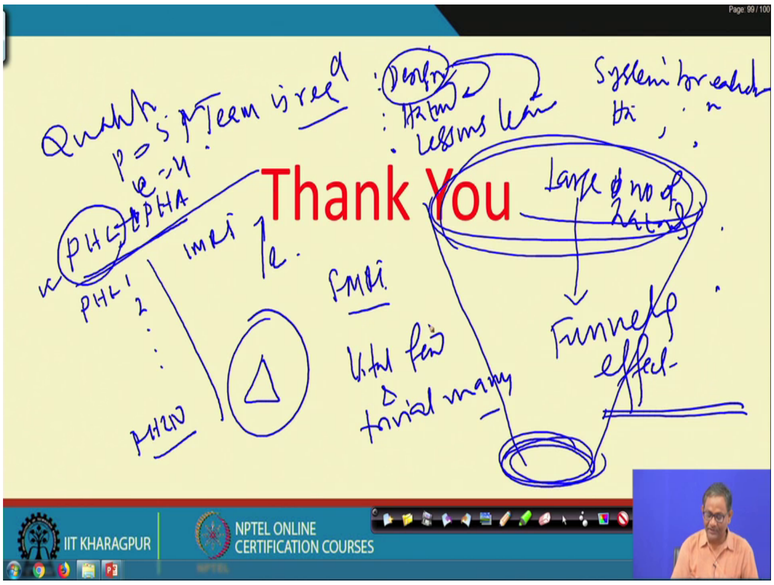
(Refer Slide Time: 28:49)



Now, let us see that the documentation part with an example, what is a, or example ace missile system then PHA 1. We have already seen that missile structure fails resulting in unstable missile flight and missile crash, causes manufacturing defect design error effect unstable flight resulting in crash during the death like this. This is basically this hazard and effects and initiating mechanism this is the total hazard list this is the first hazard, and this is the hazard triangle cycle. Then where which mode it is in the flight mode what is the initiative a initial mishap index catastrophic in nature remote occurrence. So, what is the recommendation action use five times safety factor on structural design?

Then what will happen D will be converted to E. So, D is probability E is also probability in probable it is remote. So that means, prevention it is a prevention comment basically this action if you take then what will happen probability final risk may have risk in this FMRI, final mishap risk index open means it is not yet done similarly other one ok.

(Refer Slide Time: 30:38)



So, what is you learn then we have learnt there that PHL and PHA one actually PHL, PHL over left PHL is the input to PHA. So, when you do PHA you must have PHL the list must be available.

So, and the process is given to you second thing is that in the hazard list you will find out so many so many hazards PHL 1 2. So, like this there will be PHL n, so many hazards are there. So, the format is given in that format you have to write down the causes the hazard the causes the effects initial risk index then recommended action then final risk index and so forth ok. So, I had given you only that s missile example here.

But the material, what material transfer case also similar things we have prepared your pressure tank system, you can prepare you have your own system there also you can prepare. So, in between some cases will be discussed there also you will see further development. So, inertial PHA which is which includes PHL also is a very effective hazard identification technique, which can be used at the design stage ok.

It is applicable to the entire system and the primary purpose is here to find out all permissible whatever the different level of hazards available there ok. So may be PHL can give you a very big list of hazards ok. So, then what happened through risk analysis and other measures you may finally come down to a few risk or hazards which require may be further analysis.

So, this is known as this can be underst in 6 sigma terminology this is funneling effect to we have large number of hazards, and then we want to find out very few significant one. So that mean, there may be vital few hazards and trivial many. So, what happened, but PHL ultimately work at this level we are going to find out more because it is basically the system level, current level, department level it can be done.

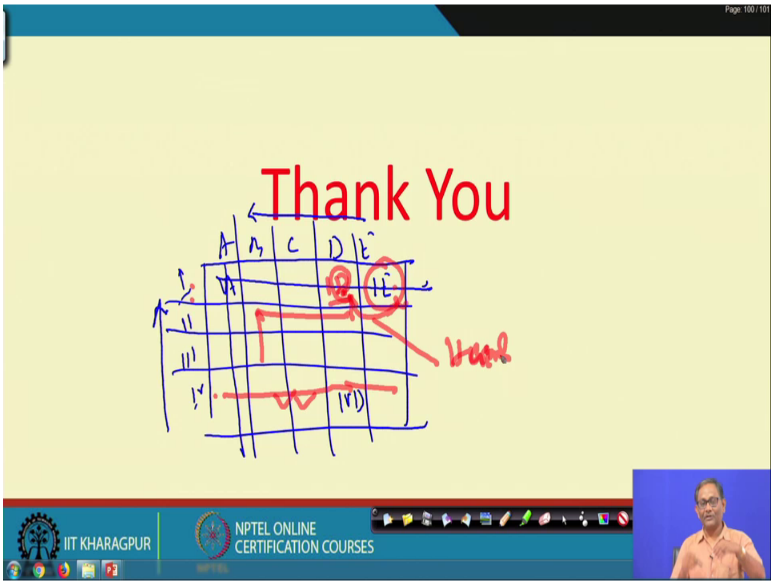
But whatever you do you please keep in mind that a team is required, team is required your design noted system knowledge, the design knowledge, hazard knowledge and lessons learnt these are very very important. The design knowledge will be compared with hazard knowledge design will be compared relation then the design gap will be identified and new hazards will be identified also.

Second is that the system breakdown structure, system breakdown which I have disused in PHL lecture. So that means, system there will be hardware, there will human ware, there will be software and system can be broken down to subsystem sub subsystem to component level. So, you can at the component level, that mean the hardware item every item you have to find out.

Then the energy sources and hazardous process events you have to understand and accordingly you have to find out the what can hazard can be there ma in the conceptual lectures I have talked about hazard triangle it is nothing but PHL will give you many hazard triangle and PHA will give you how many hazard triangle are when what is the amount risk and what kind of actions can be taken, so that risk can be minimized.

We have we have discussed in the qualitative way the risk qualitative risk that mean P in four may be 5 point and in C in 4 points.

(Refer Slide Time: 35:14)



So, you have in total that mean you have in total that A B C D and E and 1 2 3 4. So, how many risk value, so that mean you in your case there will be put twenty risk values. So, this one is 1 A and this one is 1 E similarly this one is 4 D. So, the higher this is this is the higher the consequence and the higher the probability that is that is the worst thing. So that means, in the first few coordinate like this all those things these are very very serious one maybe here also this should not be this should not be there which we must avoid this.

Severely maybe you will find out the two this and this maybe you know maybe only four this fourth case this may be acceptable case. So, if you original risk is falling here that 1 1 E. So, you please see that the it may be acceptable, but if it is 1 D it may not be acceptable in that case thus D must be combated to E, and your recommended actions will E how to convert this probability of occurrence reduce this from D to E that there the hazard control hierarchy, so you play a role.

But please keep in mind here hazard controlling all those things we are talking at the very abstraction level. Then integrate detail if I say elimination of hazard or substitution of hazard or engineering control, we are give we are giving you here in broad base engineering control not the specific engineering control. The specificity comes when you actually designing a design and you have the design knowledge everything. Then automatically because of your the teams knowledge this concept once you will apply the specific items you will find out from hazard control point of view. So, wonderful technique very easy and easy to understand a very difficult to do in reality, because domain knowledge, hazard knowledge, design knowledge lessons all those things are prerequisite for doing PHA ok.

I hope that you have understood it and you will definitely be able to develop case because what will happen? When you give when we give you the assignment we will be looking for such case specific assignment from your side also ok.

Thank you very much.