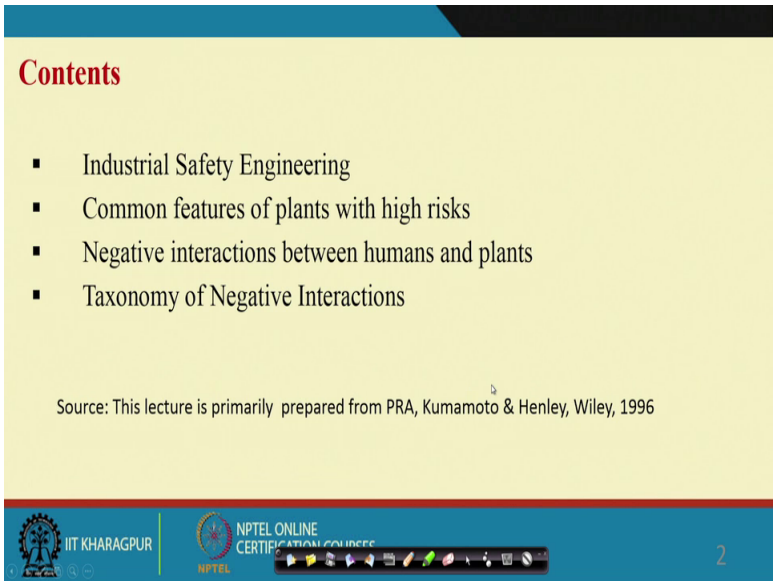
Industrial Safety Engineering
Prof. Jhareswar Maiti
Department of Industrial and Systems Engineering
Indian Institute of Technology, Kharagpur

Lecture – 05
Safety Engineering and Accident Causing Mechanisms

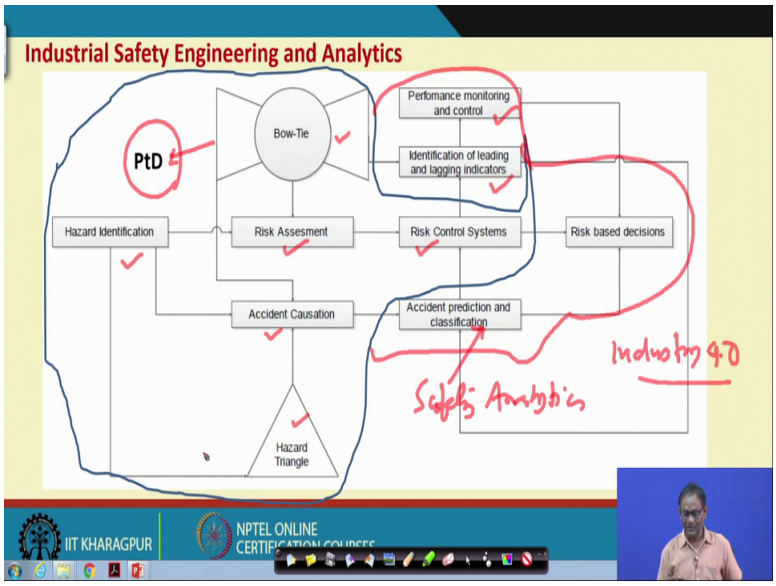
Welcome, today's topic is Safety Engineering and Accident Causing Mechanisms. Today, we will discuss whatever we have conceptualized in the first four lectures and put them under the umbrella of safety engineering and then I will discuss different issues related to accident causing mechanism. In fact, accident causing mechanism is a part of safety engineering; so safety engineering and action causing mechanisms by per set is not that a two distinct topics. Just to tell that today also accident causing mechanisms will be discussed so that since I kept this title.

(Refer Slide Time: 01:16)



So, whatever you have learned so far, we will put under industrial safety engineering. Then common features of plant with high risk, the negative interactions between humans and plants, and taxonomy of negative interactions will be covered in 30 to 40 minutes of time. And I have heavily borrowed all those things from the book written by Kumamoto and Henley which is Probabilistic Risk Assessment for Scientists and Engineering, except the first one industrial safety engineering, the last three items taken from this book.

(Refer Slide Time: 02:07)



So, let us see first what is safety engineering; so you see what is given in the slide, so many things hazard identification, risk assessment, accident causation, hazard triangle, risk control systems, bow-tie all those are coming under PtD - Prevention through Design. So, you know what is PtD, PtD is a lifecycle design concept where the hazards that may occur along the lifecycle of a system or the process or a productive manufacture all you installed. So, the all those hazards to be thought of at the design stage and proper interventions, maybe design, a design of some controls must be put into place.

I told what is hazard, hazard identification and followed by hazard triangle. Then using hazard triangle, I showed you that how accident causation can be done using safety domain ontology. And then I said that there will be risk individual societal risk and risk assessment process. And a we will discuss different hazard identification techniques and analysis techniques. Primarily, under risk assessment you will be discussing about fault tree analysis and event tree analysis. These two collectively gives you another tool called bow-tie and this bow-tie is beautiful tool for implementing PtD. And risk control systems also you have seen, so that mean all those things during design stage you have to identify. And you have to put risk barriers in proper place for proper job for proper activities at proper time primarily at the upstream so that you will get the fruit on your work during the a lifecycle of the I can say the process of the system.

Apart from these, there is accident causation, accident causation leads to accident prediction and classification; this is coming under basically safety analytics. And then you see the risk control system leads to identification of leading and lagging indicators and that also helps in improving the performance of the system by monitoring and control and there are lot of risk based decisions. I intentionally put this under safety engineering, but not under PtD, but there is overlap and one cannot be separated from the other. So, you may be interested to say why not the prevention through design approach will also consider these two, so in this case I cannot say no.

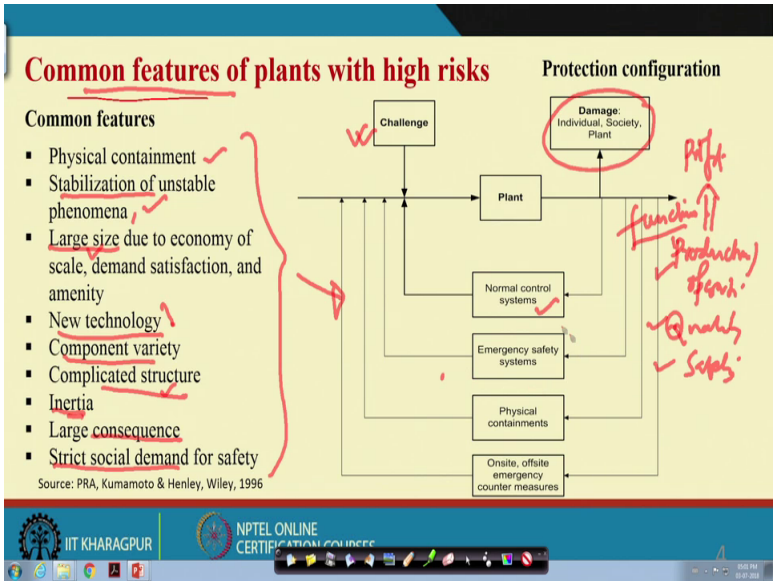
But additionally what PtD will do, PtD will give you that the best design in terms of safety during the design phase only. And these are the things basically leading to leading to monitoring and control of the system. If I know the leading indicators lagging indicators, then definitely it will be easy for the safety to professionals of the safety management team to go for better maintenance of the system or better protection and mitigation approach to be in place, so as such you can say this is also under PtD.

And then why not risk based decisions, risk based decisions, why not there this one all those things. In fact, under industry 4.0, I think all those things are under prevention through design and under safety engineering ok. So, this is what is the core of the safety engineering, but again you see this is in the obstruction level, it subject specific, it context specific issues will be dealt separately. For example, if it is a machine related things, then the definitely the mechanical engineering issues will come in between everywhere; if it is a chemical process, then chemical engineering issues will be governing the things. If it is a software human come process computer interface in the interface design, the computer science engineering electronics engineering all those things into come into consideration.

So, ultimately what I mean to say that this is a subject which is multidisciplinary, interdisciplinary, transdisciplinary whatever we can say fit into everything. So, as a result it is very different to satisfy every discipline people in terms of this contents, but please keep in mind this is basically the road map the blue print that is to be adopted if you are really interested to do safety engineering or rather industrial safety engineering for the process or the facility and to save people at work or during work ok. I hope that it make sense to you that the all the issues what we have discussed so far put into a put into a

frame one under a I can say umbrella ok. So, we will try to give justification to all those things as much as possible.

(Refer Slide Time: 08:53)



Now, this is another very important concept when we talk about accident causing mechanism. So, people must understand this is a very important concept that common features of plants with high risk. You will find out the common features are this. This I have taken from the book written by Kumamoto and Henley; Probabilistic Risk Assessment for this Engineers and Scientists. Physical containment, stabilization of unstable phenomena, large size, new technology, variety of component, complicated structure, inertia, huge consequence, strict social demand for safety. So, all those things are common features if you for any risk plant you think of coal mining, you think of a nuclear plant, you think of oil and gas installation, you think of steel making, you think of construction.

So, wherever there is high risk huge hazard involved, so what will happen you find out that you design consideration will be inclusive of all those things ok. So, these things and particularly from the stabilization of unstable phenomena point of view, we want to explain this. If you are an expert engineer working in a field, then you will be able to find out all those things. If you are a student, then you have to follow some examples and get the concepts. And some case you prepare so that at least you get the meaning of all those things.

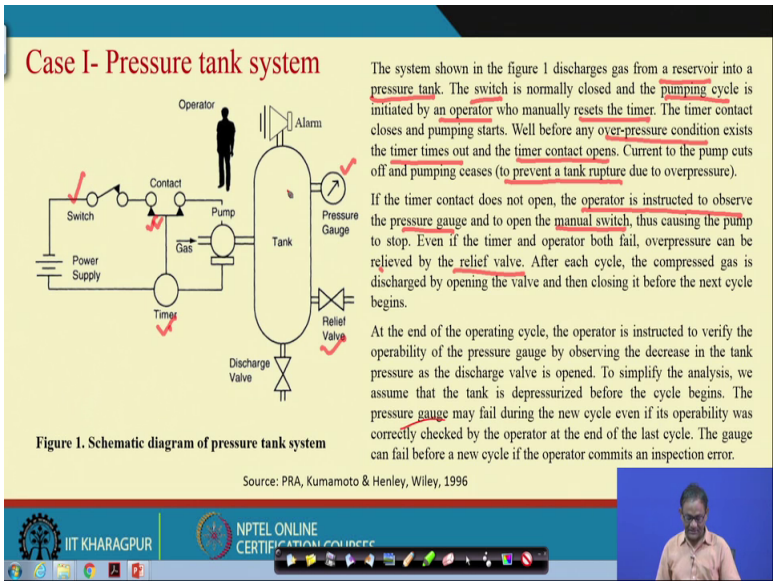
So, if I say that for plant with high risk, there will be two things; one is the challenges; another one is the damages. So, all hazards initiating mechanisms these are basically challenges. And then what will the target and threat, damage to target is the that is what is the what is I can say the threat this is the damage it will create problem. Now, these challenges are inherent to the plant because we deal with hazards. It is a complicated structure; it is a large size; it may be a new technology. It may so happen that you have basically adopted another new technology and inertia is playing role. So, so many things ultimately makes your work very much challenging.

So, then when you see that your system that whether my system is in a position to battle with the risk or the hazards, then and then these are the few process. One is normal control system; to my understanding, normal control system means any system you develop it has few purposes one of this production is very important for less operations.

Then the production definitely quality production then with there will be must be safety. So, there can be more and at the top of the business level, it is basically profit. But whatever we may think we will start with this production or operation that is what I am saying the normal function. So, the system is designed to perform the normal function in such a manner that that is there production or the intended operations can be carried out. So, this is the meaning of requirement for a plant to produce something do some work, all those things are coming under normal control system ok.

So, with reference to a case, you just think of your body, the internal parts, the brain, all those things for what purpose, this is basically you will live healthy; you perform your work ok. So, then in that case, the musculoskeletal and the cardiovascular and other system and the brain system, this we have been the sufficient, but not only this we have protective part also the skin and other things, so that means this will come under safety systems ok.

(Refer Slide Time: 15:22)



But it is better if I go for a example, so before coming to this normal control system again, let me go to sorry the example here. This example I have taken from Kumamoto's book. This is pressure tank system; the system shown in the figure one discharges gas from a reservoir into a pressure tank, the reservoir gas through pump to pressure tank ok. So, reservoir pressure tank. The switch is normally closed; this switch is normally closed. Pumping cycle is initiated pumping cycle initiated by operator, who manually resets the timer, there is the timer. It basically talks about that how long the pump will run.

The once the operator received the timer, the timer's contact gets closed, timer's contact closes and pumping starts means electricity or power to this pump will be initiated and ultimately the pumping start here. So, now, when pumping start what happen this gas will be fed to this tank. Well, before any over pressure condition exist that timer times out, well before over pressure condition exist, so over pressure condition timer will times out before the designed that maximum pressure. Timer times out and timer contact opens, timer contact opens power gate disconnected pump stop.

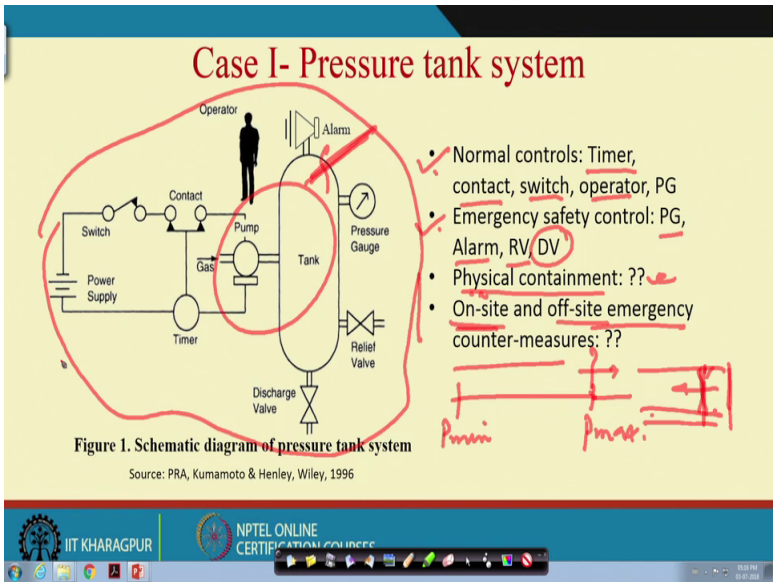
So, current to the pump cuts off and pumping ceases to prevent tank rupture due to over pressure, this is the safety issue tank rupture due to over pressure. If the timer contact does not open, by chance timer this time is elapsed, contact does not open the operator is instructed to observe the pressure gauge. There is an alarm, if the pressure is beyond the

certain limit, alarm will activate and operator will know and it will he or she will come and see the pressure gauges also.

So, the operator is instructed to observe the pressure gauge and open the manual switch thus causing the pump to stop. Even if the timer and operator both fail, suppose this contact fail, operator also fail, over pressure can be relieved by relief value. There is relief value relieved. After each cycle the over compressed gas is discharged by opening the value and then closing it before the next cycle begins ok. So, once it is completely filled up as per the design pressure, then what will happen the discharge valve will open and every valve and everything all gases will be discharged, then again new cycle will start. At the end of the operating cycle, the operator is instructed to verify the operability of the pressure gauge observing and the decrease in the time pressure as the discharge valve is opened.

To simplify the analysis, we assume that the tank is depressurized before the cycle begin. The pressure gauge may fail due to during the new cycle even if the operability was correctly checked by the operator at the end of the last cycle. The gauge can fail before a new cycle if the operator content inspection error ok. If the purpose is just to feed the feed the gas to this tank, then you see what is require a connect a power connection here, pump will start and then gas will come here. And so what happen timer then and the pump switch these things are so required minimum requirement ok.

(Refer Slide Time: 19:44)



So, if this is the case, now we want to understand what are the normal conditions controls here, the normal controls timer, contact, switch, operator; timer, contact, switch of the operator; basically pump will be there; pump related controls are also there. Now, what happened if normal means so long the pressure suppose the design pressure is this, this is the min P min and this is P max. So, long it is within this particularly from safety point of view this one P max. So, learning this fine this is under normal, but there because the pump is getting common from many things. So, there can be failure of so many components of there.

So, what will happen there will be a case when the your pressure may exceed to this site. So that means, what happen some emergency safety system should work. So, for this simple system, emergency safety we are writing the pressure gauge, alarm, relief value, sometimes discharge valve also. All though discharge valve basically discharges the gas to the utility equipment, but under situation it can be used also ok. So, that is what we are saying that that when you go for any system and you definitely find out these things normal controls, emergency controls.

And what will happen if you think this in much bigger scale, lot of pipe, gas and all other things are there, so what will happen these two are not sufficient you require to go for some other things also ok. So, from normal control means the designed parameters, they must work within the design range, the system must have the facility to do this purpose. So, long the so long the system parameters are within this design range, this is normal control. And you must know that what are the components, what are the subsystems sub system and up to component level those are require to work fully for the function of the for proper functioning of the system. But as you have seen that every activity hazard as soon as such any system is basically having lot of risk. And there are some plants or some system which are very high risk. So, particularly for those high risk systems, the layer of protection will be much more.

For example, if we talk about that the gas then when over pressure condition occurs after certain pressure tank rupture may take place. Now, depending on the amount involved here, it will create (Refer Time: 23:13). So, there if there is a tank rupture, there will be gas coming out. Suppose, if there are another one, there are lot of valves, pipes, joints, so everywhere there is a possibility that that gas will come out. So, when gas comes out, I

do have a; do have a system which ultimately that comes out gas coming out gas or the or the undesirable one that the hazard that can be physically contain somewhere ok.

Maybe you have very high chimney at the end; and there is a flayer it will be burn and going to the upper atmosphere, that may no may ultimately not make the people or property and the environment immediate environment getting affected then this is coming under physical containment, for example, nuclear power plant. A nuclear waste this is a very hazardous material. So, what you require to do, the waste material to be stored much beneath the earth crust much lower. So, that even that the nuclear that raise another things, they will generated that will be there only it will not be exposed to the society to the environment to the near nearby people, they will not be affected.

Another example for physical containment will be may be that fire sealing in mines. Suppose, you are when you are dealing with underground mines, so may be with (Refer Time: 24:57) methods means the root will come down. So, there will be exposed coal which when mixed with oxygen catches fire and then if you make a fire sealing because the caved out area is basically of no zone no work zone area because they are coal meant you have already extracted; means something like this. You are going, some way you are going, and then you are here you are coming back and this particular top portion it is kept and collapsed. Here suppose your fire take place. If you can put (Refer Time: 25:40) brick wall here, so that fire will not with sufficient strength and the dimension it will not come out ok, so that is basically fire sealing. So, this is fire physical containment ok.

Now, if you think of a big steel plant that co carbon gas coming through pipe, suppose there is there must be some way to the discharge some of the gases in such a manner that it will ultimately will not affect the environment. Obviously not the people and property surrounded, this is what is physical containment. So, when you go for any high risk system, you will find out that normal condition, emergency control, normal control, physical containment may be there, this two must this may be there.

Now, on-site, and off-site counter measures is another issue which is very important. What is on-site and off-site counter measures? On-site and off-site counter measures mean suppose you just think of suppose this is my plant. There are many people working here. If any anything happen here, then what are the measures when the accident has taken place tank rupture is taken place. So, what are the measures you have so that you

will save the people, save the property? So, those measures are on-site means where the accident has taken place ok.

For example, two go, two passenger trains collision that the effect will be on-site effect only because the two train, where they collide the two train gets damaged people will be injured, death all those things. So, that means, there are certain hazards which if occurs their effect will be localized to that place where accident has taken place. So, for that what are the on-site may counter measures you have persons fall from height, so the there must be emergence that is ambulance or emergence ambulance system so that immediately the person will be taken hospital; or person working at heights, suddenly his medical fitness deteriorated, he must he your system he will be he will be brought to the ground level and then again emergency will system will be there, on-site measures will be there, so that he will be quickly shifted to doctor the hospital. For example that can be many more.

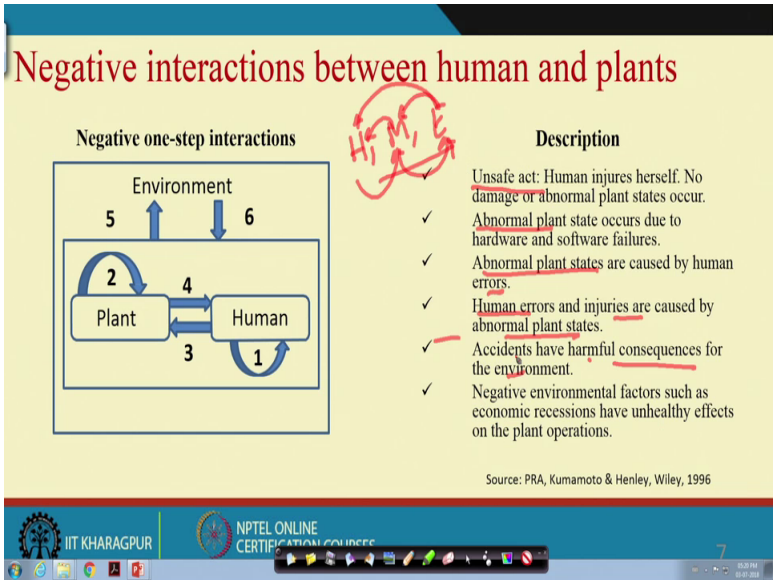
Now, now if here what is off-site counter-measure? Suppose, there is a rupture, now this gas is a toxic gas. And the rupture the hole is bigger one, huge volume amount of is coming. So, in that case what happen, locality will be affected. If it is the gas is carbon monoxide in some case, even that small volume will come out that will basically create (Refer Time: 28:58) to the people.

So, what we mean that your system has certain hazards which not only cause on-site effect, but it may cause off-site effect, out of your plant effect. If your on-site is this one, this is your target area the neighboring departments will be off-site. But if on-site if you consider plant as a whole, then society at large is off-site. So, you must know that as you are working with hazardous system, you must know that this hazard should not affect the locality, the society. So, you must have sufficient protection measures, these are off-site emergency counter measures ok.

Suppose your plant produce lot of gasses for example. So, having the periphery of the plant must have the detection system, gas detection system. Whenever you find out some gas is detected, immediately evacuation of the people who are going to be affected, so many issues are important. We cannot forget the effect of that union carbide, Bhopal gas tragedy, till now people are suffering.

So, it is a very big thing to happen. And just by saying few lines is not saving the people, it you have to be you have to design it in such a manner that this can be possible, accidents are predictable, so it can be it is also preventable ok. So, these are the few things, because suppose you are asked to the redesign your system for safety improvement, then first thing is that you understand the system in detail and find out that all the controls are there or not. If something is missing, you have to immediately install that one and redesign in this manner. It is a good concept this will help you in design and redesign.

(Refer Slide Time: 31:29)



Then I will come to the negative interactions between human and plants. Here the basic concept is that any plant any system you consider, there will be three things at least three things human, machine environment. And human affect machine, machine may affect environment, environment may affect machine, environment may affect human, environment a machine also can affect human; so that means, there is interactions between all the components. So, those interactions can be positive and negative also and it is required. Suppose, a crane operator pushing some button where the load will be transformed from one place to another that it means interacting with the control there, this is a positive interaction, so done.

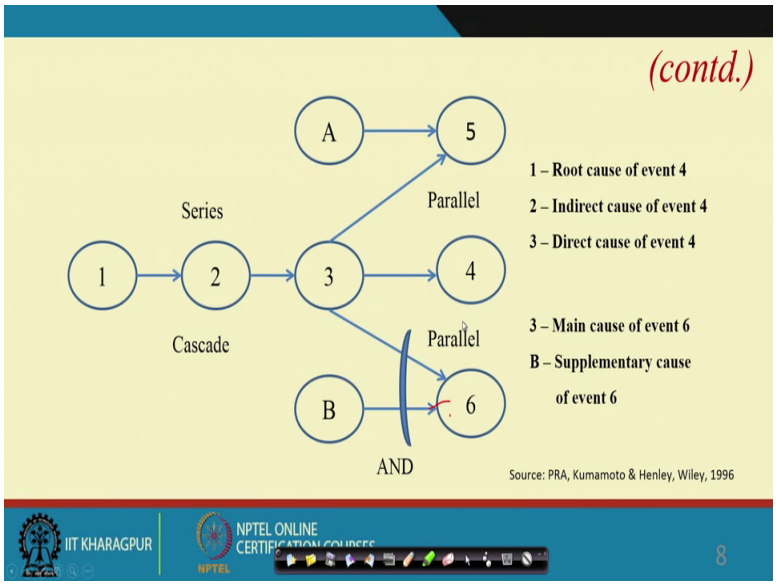
But independently if you push a separate button which is not basically transferring may be it is basically lifting it further which is undesirable and may be somebody will be heat

then it is negative interaction. So, similarly the machine should display that what is the status of it if it display wrongly the operator may take a action. So, now, when you are working in a hot and human environment, so your body must be acclimatized to that environment; and that you cannot work under heat risk for several hours, so that mean the environment effect on body. And in saw a in return what will happen if that means, you will negatively interact with the machine and at collectively there will be problem in the sense lot of in undesired incidents will take place.

So, those interactions are classified under unsafe act. Human injured himself; abnormal plant state or unsafe condition; abnormal plant states are caused by human errors; human errors and injuries are caused by plant; accidents and are have harmful consequences to the environment; negative environmental factors like this. So, if you investigate any of the any accident if you find out the victim himself is responsible that may be unsafe act. The condition is responsible unsafe condition abnormal plant state. It may so happen that abnormal plant state is caused by the human errors, human error is very important one that I have not talked about under safety engineering that concept, but please keep in mind human errors is also very important one ok.

So; that means, you have to find out that what are the different ways those negative interactions can take place and those in negative interactions should not happen. One is the hazard initiative mechanism, then accident, and negative interaction. Initiative mechanism which leading to your bad state here accident, there are the interfaces are also responsible so that needs to be considered ok.

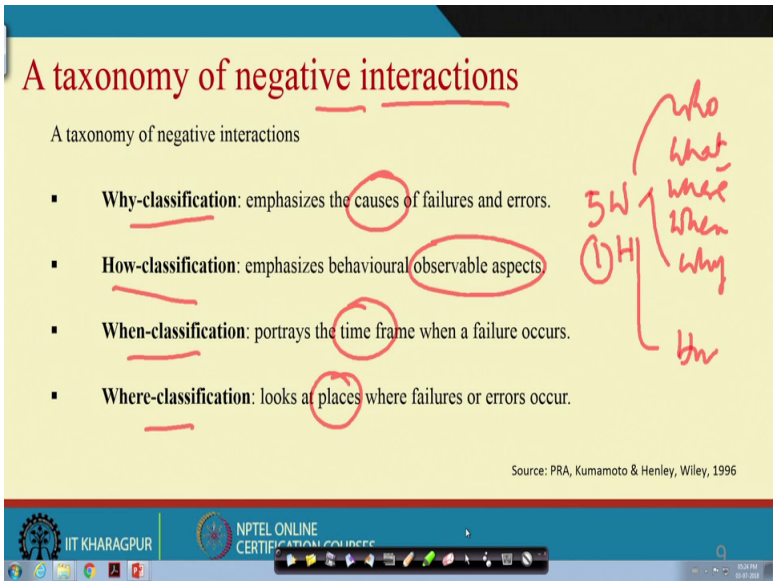
(Refer Slide Time: 35:18)



So, some classifications are given. So, what we will see that how those negative interactions can take place that basically this is one example where we are basically trying to say something happens then followed by something happen followed by something happened, then finally, end result will take place. But there are many way that parallel and series conditions will happen.

Here basically 1 is the root cause that is you require to understand, 2 indirect cause of event 4; 3 direct cause of event 4; 3 main cause of event 6. And B and A, they are supplementary; suppose B is supplementary cause of event 6. So, so you have to find out all those things because if you understand the ontology part there, I think that will help you in developing these also.

(Refer Slide Time: 36:21)



Now, how to do it? So, Kumamoto and Henley book has given you that there will be why-classification, there can be how-classification, why-classification, when-classification, where-classification. Actually there are 5 W and 1 H, what, where, when, why, and how is there. So, how, when, where, why, what, and who, another one is who. So, who what-happened, who are involved, where it has happened, when it has happened, why it has happened, how it has happened, all those things you have to understand from negative interaction point.

Once you know the negative interactions, you have to ask all those questions that is why classification that emphasizes at the cause. How emphasizes primarily observational facts. When actually basically talk about the time; and where the places locations ok. And then who I can do the responsible person. And what actually happened what happened negative interaction happened. There are many ways that any accident situations can be can be analyzed so it is a analysts game.

So, what we what will do therefore, we will give you some important tools and techniques, some important examples, some important cases all through the through the lectures and some tutorial some kind of mathematics also will there, so that it will be a it will be descriptive and mathematical combination. And you will one way you will understand the concept, the qualitative things; other way you will understand the quantitative part. So, both mix in together will give you much better understanding.

So, I hope that you have understood the concept key concepts, the different terms and terminologies, the issues, safety engineering overall gamut of safety engineering and all those things. So, this is what is the end of our introductory lecture that is the first week lecture that just knowing the totality of the say of this particular industrial safety engineering course, but not in depth in (Refer Time: 39:31) ok. Hence, next lecture onwards what will happen we will go to specific tools and techniques will give you the what is this, and how it is to be done with cases and this subject being a complicated subject. And also it varies from discipline to discipline from understanding point of view from implementation from point of view. So, you have to be very careful ok.

Thank you very much.