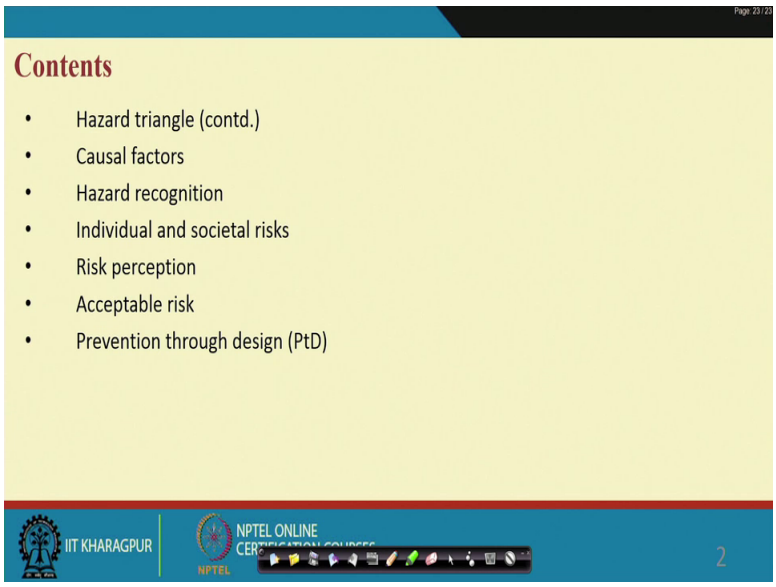
Industrial Safety Engineering
Prof. Jhareswar Maiti
Department of Industrial and Systems Engineering
Indian Institute of Technology, Kharagpur

Lecture – 03
Key Concepts and Terminologies - Safety Domain Ontology

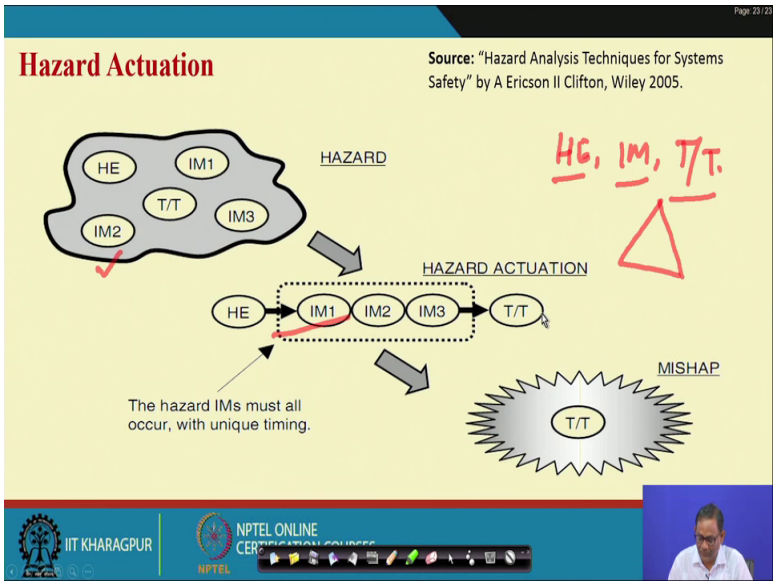
Hello everybody. I am continuing previous topic Key concepts and terminologies. And you have seen in last lecture that I started with the terminologies like safety, risk, accident mishap dead hazard with military standard definitions of hazard and accidents. Then hazard triangle we have elaborately discussed. We will continue with hazard triangle; primarily the hazard theory. And then we will discuss some more topic like causal factors and hazard recognition.

(Refer Slide Time: 01:15)



If you see this slide that hazard triangle, hazard theory, then causal factors, hazard recognition, individual and societal risks, risk perception, acceptable risk, prevention through design. This is the few terms terminologies concepts which are which is very much pertinent to safety engineering.

(Refer Slide Time: 01:47)



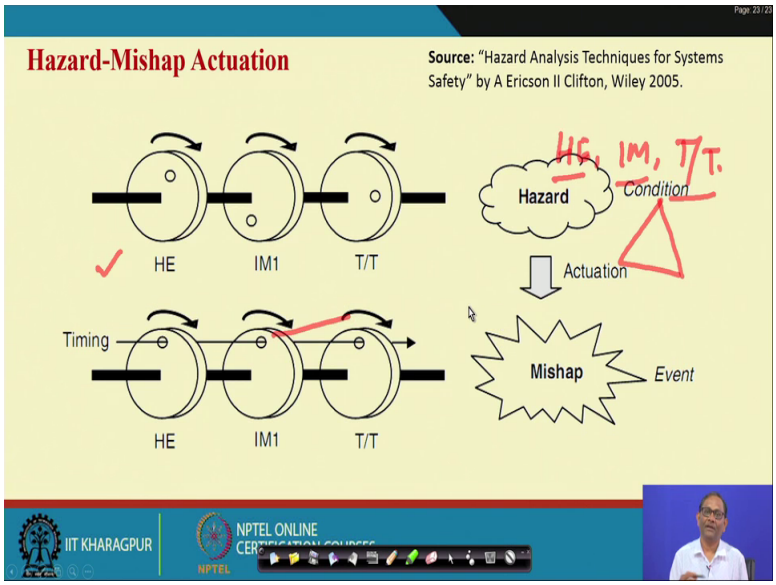
We have already completed a few for example, hazard elements. What are the things I have completed; I can say that hazard element, initiating mechanism, target and threat. And then this hazard triangle part we have completed. And with example we have also seen that how to write a hazard or describe a hazard, where hazard element initially mechanism target threat all will be all will be included and the sequence also will be discussed that is what we have discussed. And I told you that this is nothing but the hazard actuation.

Now, see at when ah um um there is no accident, what is the condition? The condition is like this; that mean when you do some work, any job, any operation, any process, there are hazards, targets, threats, initiating mechanisms; they are basically hidden haphazard not making any chain of events. Now, it is the failure of the safety management to allow these elements to become a chain like this. Hazardous element and then there are three initiative mechanism in sequence form a chain, and then finally accident has taken place with hazardous realized to accidents and then there is a big problem. And the job of safety engineer is the hazard and IM must not occur.

The hazard will be there, IMs may will be there, target threat will be there; but it should not occur means this kind of chain sequence should not occur. Obviously, if there is no hazard, accident is not an issue, no question of accident. If there is no initiating mechanism possible, no question of accident. But please keep in mind that whatever

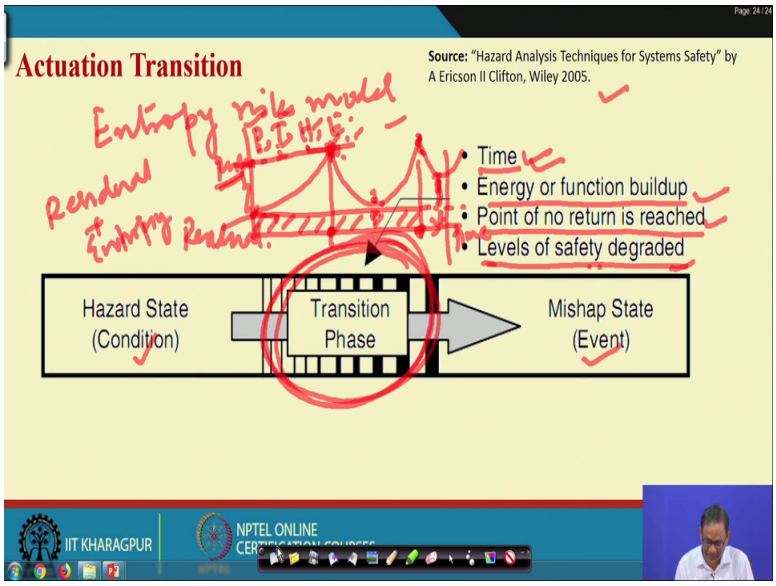
small system you design, by design inevitably there will be all those elements. So, it is the job of safety engineer to understand this and do the needful. This is one thing what in the book of written by hazard analysis um written by Ericson II Clifton that name of the book is Hazard Analysis Techniques for System Safety very, very, very important book.

(Refer Slide Time: 04:39)



Now, the same thing graphical representation you see these three components of hazards; in the top figure there are all those loop holes, but they are not aligned. This is hazard. When they are aligned, you see the timing is very important, there is a particular time when all those things aligned and it leads to accident and this is what is the actuation ok. So, this is nothing but another way of explaining the hazard mishap actuation.

(Refer Slide Time: 05:26)



As I told you the safety engineers job I am repeating the word several times in fact ah last class also I repeated it several times that this hazardous condition to mishap; hazardous condition to mishap. This is my hazardous condition; this is mishap; this is the biggest issue. You see what we are write here; it is also taken from this book, the time energy or function build up point of no return is reached, level of safety degraded. So, these things will happen then only hazard will lead to accident.

There is another interesting concept here is known as entropy risk model that we will I I will discuss later in detail, but this entropy risk model is very very important one. What do we mean by design? You create certain amount of risk that is known as residual risk residual which is inherited by the system. Now, what happened over time, this side is time over time, the process, the technology, the human, the environment component of a system; these are the these are the component of a system this will deteriorate, so that deterioration ultimately lead to increase in risk.

So, there will be a threshold risk. So, this one is risk. So, this is the point under time, this is the time using, this is the time when the threshold risk increases to the risk increases, what risk this is known as entropy risk. The deterioration became the system increases from the residual part to up to this threshold part at a particular time, when the accident has taken place. And it is because all those process, technology, human, environment that deteriorates over time. They all this ah decade the decaying not dc orientation ultimately

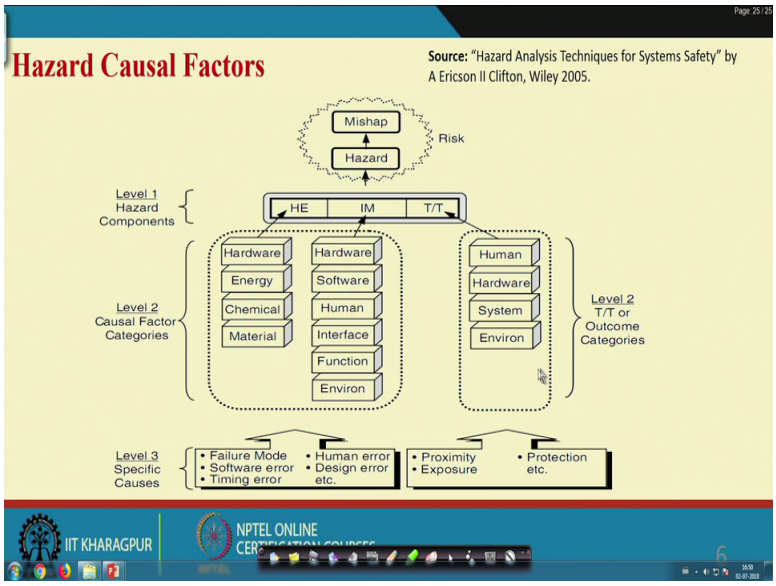
lead to entropy risk. So, that means, when you design a system, you have two component one is residual risk plus entropy risk. So, it is you must who understand that how much risk you are build, you are living with the system and how much risk will be created if the system is not maintained over its lifecycle.

So, these are this is the point where energy buildup to level, point no return is at reached and levels of safety degraded with reference to process, technology, human, environment level of safety degraded. So, what will happen when an accident take place at this point lot of efforts to reduce this risk to a level you will but it is definitely less than threshold risk, but it takes some time to come to this. And again we become complaisant that ok nothing will happen because of this much time nothing will happen and this complacency again raised the risk level to threshold level. And then this is the second time incident first incident has taken place here; this is the second accident that also taken place.

Then again you will find that actually what happened, all those things happened together to system parameters. So, again you start thinking and again the risk will be reduced. But by this process, what happen every time you create certain amount of permanent risk here, and here the you started residually this is by design if it is this much because of poor maintenance, housekeeping, operations everything, so ultimately the residual path or the immediately part it will go on increasing. And at certain time what happen, it will be almost equal to threshold risk and nothing possible you have to dispose the system. This is known as entropy risk model.

And this one this transition phase basically is call this is a process what is happening here. It will be our job to protect though deterioration for process, for technology, for hail human, for environment and so that you will not go to reach to the threshold risk ok. I hope it make sense.

(Refer Slide Time: 11:00)



Now this process, technology, your human, environment, all those things are very very important I told you and these are also that is why these are also termed as causal factor, causal factor sorry this causal factors. What are the causal factors? Causal factors means the factors alone in our combination will ultimately resulted in the transition to complete from hazards to accidents ok.

So, when an accident takes place, immediately you investigate and you find out immediate causes. These are basically related to your physical process, related to your equipment, related to the environment, related to the human, related to their interface, so related to material ok and that can be it can be classified in other way also like different energy. So, all those things leads to accident.

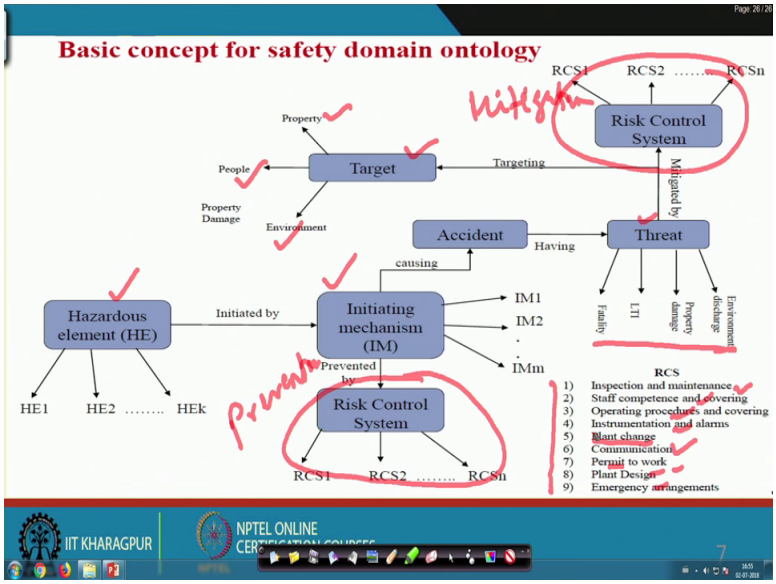
And if you if you go little more or you dig down into further, then you will find out level 3 risk factors, level 3 causes, so like this. So, these are all level 3 causes. If you see this is what is risk factors, causal factors. So what are the causal factors? Causal factors first level causal factor is hazards hazard components. It is given in level 1. Then what is this? When you see the hazard element, these are nothing but the source of the resources of for hazard. So, there is basically the hardware, energy, material, chemical all those things. Then you require initiating mechanisms to happen; these are also related to these hardware, software that interface human error, function, environment all those things. And target threat are all actually the property, people and environment; human is the

people, hardware, system is a property and environment. So, that means, target and threat will be either people property or environment or in combination.

So, when you identify the hazard, you will find out that related different components and they are related level 2 causal factors. If you further dig down, what will happen suppose you are talking about hardware ok; let your motor fail, then you will find out why that because motor fails so then level 3 specific causes you found out like failure modes. For example, pump; pump fails to run, pump ah stop prematurely ok, pump overrun. So, those mean these are the failure mode, so that means, you will like from with reference to energy pressure build up you are not able to control it further.

So, all those things ultimately we will further find out and they are level 3 factors. This level 3 factors, you see failure mode, software error, timing error, human error, design error, there is proximity problem, exposure problem, protection problem ok. So, the amount of amount of protective um system, protective measures that must be there to prevent accident that is not there; all those things we will slowly discuss, but this are the key under key concept and terminologies I am just giving you that please see the complexity, the diversity, the ah multidisciplinary nature of this particular topic.

(Refer Slide Time: 15:19)



Now, I with the help of hazard triangle, we have made a model. Here you see that there are components like there are components like hazard element compound like initiating mechanism like the target and threat. And also there is a there is there is a path

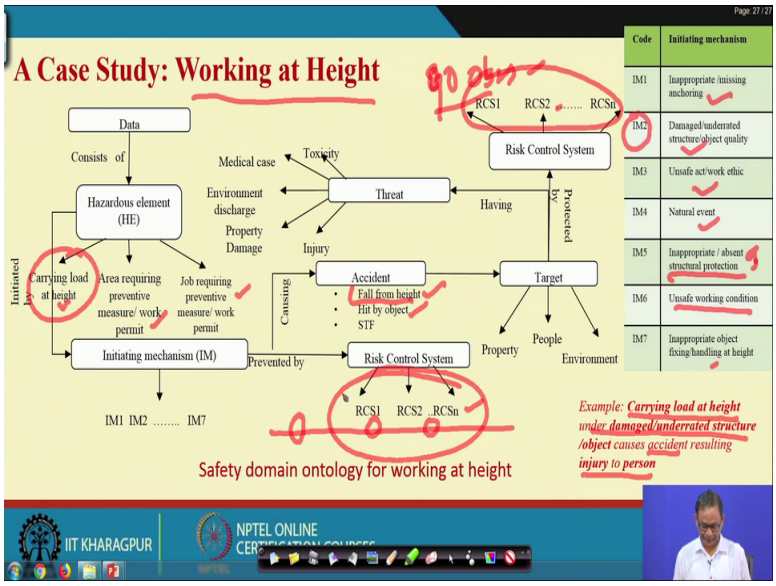
mechanisms target and threat. What way we are developing? A particular hazardous element initiated by initiating different mechanisms cause accident; and this accident have different kind of threats like fatality, loss type injury, property damage environmental discharge and these are targeted to targets like property like people like environment ok.

So, property people environment that means, what is what actually our aim here? Our aim is you have seen that by design there will be hazardous elements, there will be different initiative mechanisms that will occur. And ultimately there will be a time when the system component deteriorates; it may be human, it may be your process, it may be technology, it may be ah I can say that software. So, those things will deteriorate over time, and a threshold risk achieves and accident will take place.

Now, design engineer or other way I can say the safety engineer who are responsible for design a product or process. they must understand this path. The reason is if if I know hazardous element followed by sequence of initiative mechanisms causes accident having threat of different kinds and targeting to either people, property or environment that mean I know the path. Once I know the path, I have to break this path. So, breaking of this path is done by this control system. So, you is your system having sufficient amount of risk control measures to prevent the accident, then this risk control are preventive risk control system. And once accident takes place, there is concept of mitigation.

So, mitigation, this is prevention. There also risk control system will be there. And interestingly most of the control system will be related to like this; either inspection or maintenance problem, or staff competency problem, or operating procedure problem or instrumentation and alarm problem, or there is change plant change, management of change. There may be communication problem, permit to work problem, plant design the design problem, emergency arrangement problem. So, your risk control system will pertaining will be will be one or more of this, but this is not the totality may be, but these are the mostly it will it will cover the enter it. So, now, you understand that when you talk about accident causation that transition that how these things are happening ok. So, now given example you have to understand.

(Refer Slide Time: 19:38)



So, let us see one example. We have taken the case working at height. We have observed for 2 years data for a particular company. And then we found out all the hazardous element from 18, I think around 90 observation 89 to 90 observation, let it be 90 observations we have considered that been 90 working at height related incidents of different at different severity it has occurred, we have that data. And then, when we analyze we found out 90 odd hazard elements; for each case one hazard elements, but many time they are common.

So, the hazardous element when we further classify we found out that carrying load at height, this is the source; area requiring preventive measure or work permit this is another; and job requiring. So, that means, one is basically the area location; another one is basically job requiring preventing and measure of permit; another one is the load that they are carrying not all the case all the times everything is there ok.

So, we are saying that this hazardous element in there will be different kind of initiating mechanisms. When we analyze the initiating mechanism, we found out that these are the these are the initiative mechanism inappropriate or missing encoring, damage underrated structure object, unsafe at work ethics, natural event, inappropriate abs or inappropriate or absent of structural protection, and then unsafe working conditions and inappropriate object fixing or handling at height. This is a case specific for a particular plant for a particular period of time with certain inspection, this data generated and we found out.

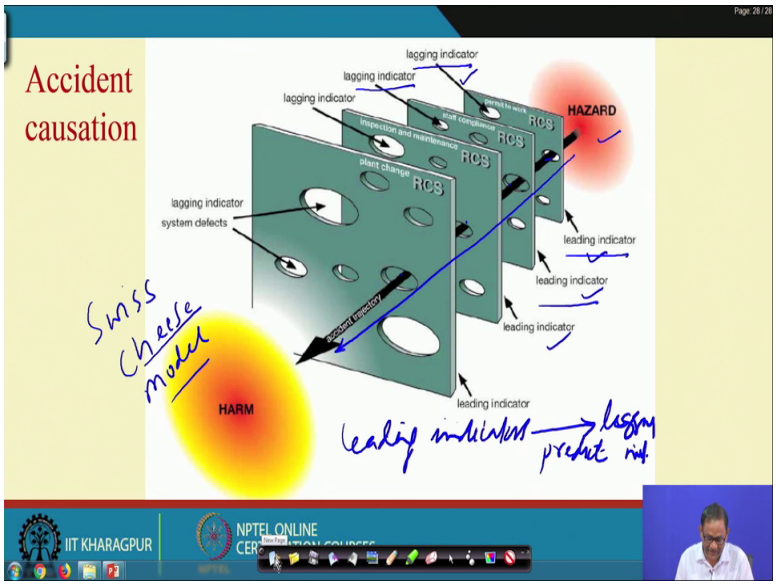
That means, what is happening from a safety engineering point of view? So you are getting a path, hazardous element initiating mechanism like this. Now, if I consider one hazard element with seven initiative mechanism, if possible then seven path is created.

Example, carrying load at height, this is my hazardous element; under damage underrated structure, then damage and under it is IM 2. Causes accident it may be fall off height fall from height or let it be let it be fall from height. Causes fall from height accident resulting injury to person, so that means that hazard triangle is complete; that means, the line is created. One is carrying load; second one is initiating mechanism and target threat, the line. All those 90 odd cases the timing that means, the alignment of those components have been taken place.

My question is that when there are 100 such incidences, why we are not able to prevent those? The reason is we might have lacking there, the re risk control system. When I analyze the data, I found that no information related to risk control system, no information related to responsibility, accountability, due to that mean the complete management is not there. It is there some, but the description not reflecting that ok. This is a interesting model that we have developed with simple very simple hazard triangle concept.

Now, follow these those who are working participants for you have for you it has rate immediate application, because you already have such data. Those who are students graduating for them this is a wonderful model and later on you will see that we will we will build on this model many concepts many many things ok.

(Refer Slide Time: 24:40)



So, as I told you the path is created the path we have seen that hazardous element to target threat, the path created because failure of the risk control system. So, hazard to this., see the holes Swiss Cheese model. Swiss Cheese model, you Google it is Swiss Cheese model I think may be just see the spelling; if it is wrong please check. So, here another interesting concept, you see that lagging indicators, leading indicators. Usually by lagging indicators what do you mean, means we create indicators based on accident already occurred like number of LTI, number of fatalities ok. So, if we go one step further, we will say that which risk control system fails that may be it is because of poor maintenance. These are actually already occur, so they will basically leading indicate, lagging indicators.

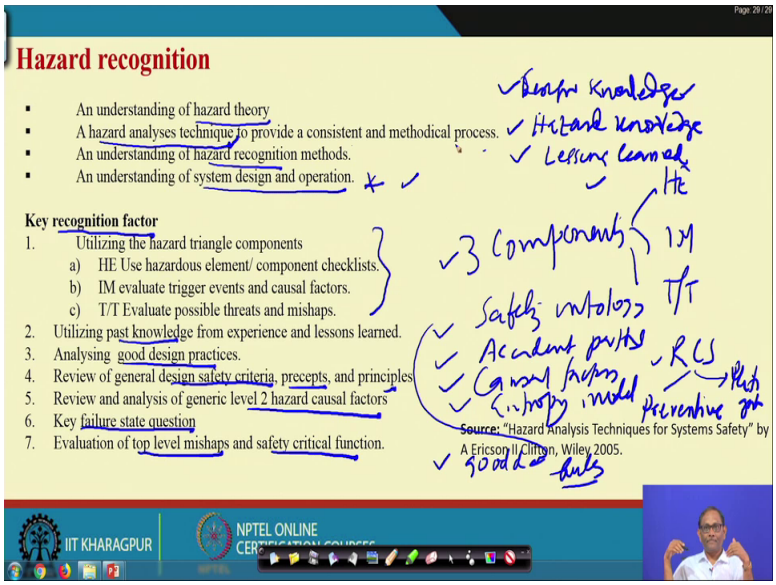
Lagging means after event indicators. What is after event here? It may be accident of large like top level accident or it may be a first state or near means or it may be while inspecting may find that some of the maintenance operations and other issues, design issues all those things are there. So, failure of the risk control systems ultimately those events we will talk about lagging indicators.

Now in order to maintain the health of this risk control systems, what you will do that gives you leading indicators. So, leading indicator leads to or predicts can predict lagging indicator ok. So, my question here is you have to create case for this. I am giving you the concept, when we will be discussing in detail the living leading and lagging indicators,

we will discuss one or more cases. But it cannot be possible to tell you several cases under this because of time constant, but those who are listening to me please understand it is applicable to safety in all domain, all context. We have to we have to ah use it is.

And if I know the leading indicators, I am telling you prevention is very much easy. It is basically we do not know what are the leading indicators of safety; industry, academia, everywhere that the problem is that we have not come to this, and we are not matured in this level. It is a it is a hot topic that is why today for high risk or event low risk plants also that how to find out the leading indicators and then using leading indicator, predict the lagging indicator, I hope that it make sense.

(Refer Slide Time: 28:22)



Now finally, I will talk about hazard recognition. So, before telling this, let me repeat what we have learned so far. So, you have learned that 3 elements or 3 components of of a hazard; 3 components - hazard element, initiating mechanism and target and threat. You have understand that safety ontology, causal accident path, and causal factors and you will you find out that the causal factors can be related to system components, entropy model. Then I also talk about this control systems which are of two types; preventive, preventive means the control measures to prevent accident to happen. And then mitigative, mitigative mean even the accident has taken place the severity can be minimized mitigative.

Then one case with or 90 odd data, 90 odd data how the safety ontology will give you rules different rules ok. So, all those things and apart from last class so many terminologies, we have discussed all those thing if you really do definitely safety engineering will be in place ok and you will understand hazard, you will recognize hazard. Here some of the key issues further described what is hazard recognition? Understanding of hazard theory, I hope you understand now.

A hazard analysis techniques to provide consistent and methodical process, generalization technique we have not discussed; understanding of hazard recognition methods not discussed. Understanding of system design and operation, it will not be discussed; it is expected that an engineer from every operations every discipline. They must know their system when if you do not know have the system knowledge, you cannot do so that is why here very very important is your design knowledge this is very important design knowledge, then your hazard knowledge, then your um lessons learned, lessons learned very, very important.

Now, what are the key recognition factors? Utilizing hazard triangle you have understood now, utilizing past knowledge I told you already, analyzing good design practices this knowledge is important, review of general design safety criteria percepts principles from engineering design it will it should come, review of analysis of generally level 2 causal factors level 2 means all the system related factors, key failure state questions and evaluates in a top level accidents and safety critical functions.

We will see some of the things you have understood; now some of the things it will come we will follow. So, I hope that the concepts ah coming ah are being recognized by you and I will take ah I think one more lecture on these terminologies in the concepts. And a and then actually we will build on these concepts and theories later on by the identification techniques, risk assessment, then different probability models and then finally, safety function deployment, accident, other causations theories or so many things are there when prevents and through design and so forth.

Thank you very much.