Health, Safety and Environmental Management in Offshore and Petroleum Engineering

Prof. Srinivasan Chandrasekaran
Department of Ocean Engineering
Indian Institute of Technology, Madras

Module – 02
Operational Safety
Lecture – 21
FMEA

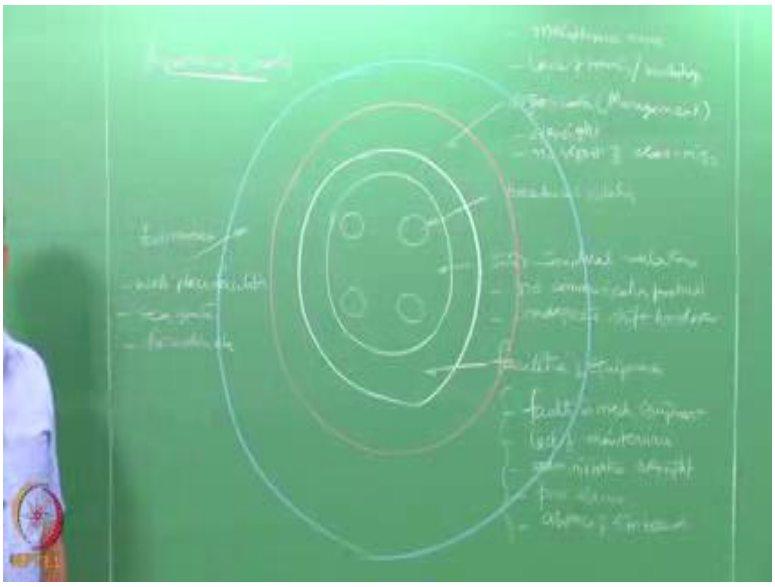
Welcome friends to the online course on HSE practices in Offshore and Petroleum Engineering. We are discussing lectures on module-2, where we have focusing on operational safety.

(Refer Slide Time: 00:20)

This will be the 21st lecture where we are going to focus on FMEA. As we already discussed FMEA abbreviates for failure mode effects analysis, this is one of the interesting tool to study the hazard present in a mechanical models. So, that those hazards can be removed in the design stage itself.

However before looking into the details of an FMEA an applied example on FMEA, let us try to revisit slight to the safety concept more in particular then realize the importance of such analysis in hazard mitigation.

(Refer Slide Time: 01:24)



If you look at importance of safety, interestingly safety violation actually is an alignment of mistakes I could say. Let us say and individually in a group or set of people keep on violating the safety norms, let us say there is a procedural violation being followed by the individual people, let us say individual people procedurally violate certain safety norms working in a work place or industry or on both.

Then they will of course, work in a close group, so the close group will have no consequences seen as inter individual relations. For example, the safety protocols violated be individual is not shared communicated and the consequences or not felt in the group where these individuals are working, and we call as inter individual relationships between the groups or missing in terms of understanding the consequences of safety violation because there are no communication protocols present and there are inadequate shift handovers.

Let say the shift handover is not professionally done there are some lack of communication between the group what we call inter individual relationship and therefore, the safety practices which are violated by the group is not communicated amongst each other to realize the consequences that may arise because of this. Now they work in an environment which contains facilities and equipment there is the environment where we are working and there can be some fault in the mechanical equipments, there can be lack of maintenance there can be even administrative over sight also.

What I mean to say in case of any report made by the near miss events of this people in the group because of the equipments and tools and equipments used in this layout, let us say the administration has over sighted them and they did not focus and there maybe presents of poor alarms, absence of sin boards, etcetera. Let us say these are the possible violations what can happen in the facility level or in the equipment layout level.

Now, this whole unit is working in a sector which is much larger then this group and this sector is organization or even you can call this management. You know at the management level there can be certain oversight, no report of near miss events, let us say lack of training and workshops. There can be also maintenance errors lack of proper schedule of maintenance. All can happen at the organizational level which is now housing the facilities, individual people and the group.

So, you can understand here different tiers, different levels. The first level started with the individual then it started with the group of people, it started with the plants and equipments, it started with the layout of the organization management each level people start violating safety norms by ignorance or by knowing terms let us say, but they do only a small minor deviation from the safety norm.

Now this entire system is encompassed in a bigger plane. Now, we can call this plane as the environment or the work place let us say. There may be (Refer Time: 07:53) present in the work place facility which may lead to uncomfortable situation hazardous scenarios, may be the sea state, may be rough, may be the situation in terms of operational facilities, may be hazardous etcetera. Now the safety violation happens only when all the mistakes are aligned at one shot when all of them are aligned, when each

one of them are done or happening individually when there is no intra communication between each one of them then there is no accident.

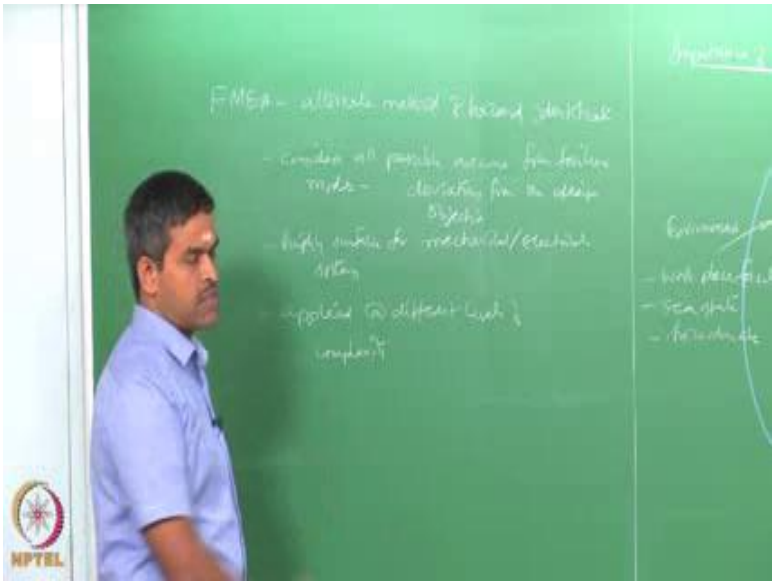
(Refer Slide Time: 07:35)

When all of them are aligned for example, an individual making a mistake is aligned with the group who makes a mistake, which is further aligned with a plants and equipments which is exactly having a maintenance problem which is further aligned with the larger group which is the management over sighting, which is then added to a complication present in the environment it leads to what we call as an accident. Sometimes if the consequences are not very serious it is an incident or an event, if the consequence are very serious we call that has an accident.

Accident is nothing but alignment of mistakes done for an individual level till the environmental support through and through including the management tie as well. So, safety practice or HSE practice in general is actually to break this continuity at different levels safety practices should be implemented. So, that this continuing chain in terms of getting aligned is always attempted to be broken, so that is what we say importance of safety. So, the safety importance is imparted or given at different tiers in the system. So, that at least one violet the other takes care of, if the other also group violets the third system takes care of and so on and so forth.

So, hazard scenario is an identification which is to be done at different tiers maturity of that will become a risk which violate safety norms which is very serious concern because the consequences cost by such incidents or accidents, especially in oil gas industry are very very high. Having said this, let us now discuss an important tool for doing hazard analysis in terms of qualitative methods where I am going to assess the faults in a mechanical system at the design stage.

(Refer Slide Time: 09:31)

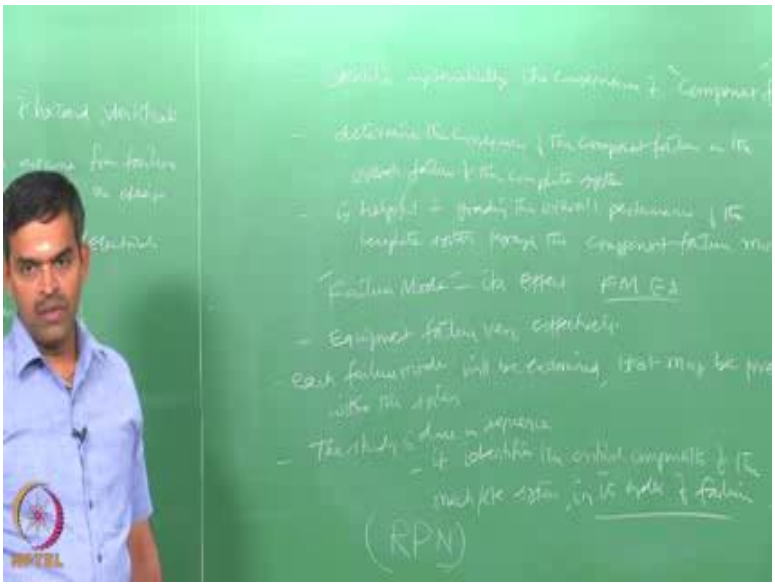


FMEA is actually an alternate method of hazard assessment or hazard identification we should say. This method considers all possible outcomes from failure modes. Then the question is what are failure modes. Failure modes are nothing but deviation from the design objective which is also common in case of an hazop study. This study is highly suitable for mechanical systems and electrical systems, possibly it is one of the most powerful tool which can do hazard analysis for mechanical and electrical systems compared to any other existing methods available in the literature as we saw hazard study is available for chemical process.

Similarly, this method is also a hazard identification method which can be very comfortably applied to mechanical in electrical systems. This can be applied a different

level of complexity that is starting from the design to that of the end final product release you can apply this kind of study to any level a different levels of complexity.

(Refer Slide Time: 11:23)



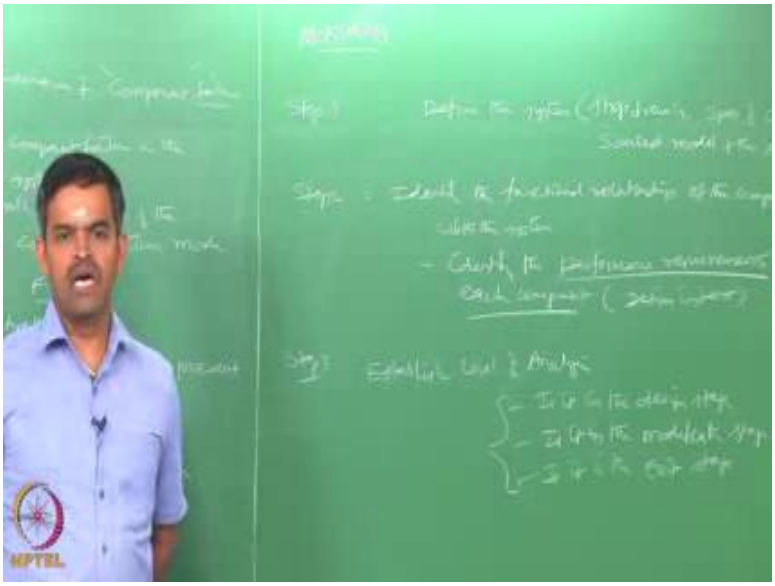
FMEA actually identifies systematically the consequences of component failure, please understand this method does not explicitly bring out the product failure or the whole system failure, it tells you in breakup the failure of each components present in the system. So, it determines the consequence of the component failure on the overall failure of the complete system. Most importantly the system is helpful in grading the overall performance of the complete system through the component failure mode that is why, the study is called failure mode which is happening at the component level and its effect that is way it is FMEA.

This can identify equipment failure very effectively. In this study each failure mode will be examined that may be present within the system then, effect of this failure modes on the overall performance of the system will be assessed. So, it will be done in stages in sequence the study is done in sequence and it actually identifies the critical components of the mechanical electrical systems in its order of failure that is very very important. The component which is highest critical or most critical let us say will be identified and

that component can be focused in the design, either to replace the component or to redesign the system with the different component and so on and so forth.

So, will give you an order of failure, ultimately FMEA gives you what we call as an risk priority number which tells me the hierarchy of failure in terms of its consequences and the chain effect of one failure on the other. So, it will also help me to understand the cascading effect of failure of components on the overall failure of the system. Let us say the methodology what are the steps involved in carrying out FMEA.

(Refer Slide Time: 15:23)

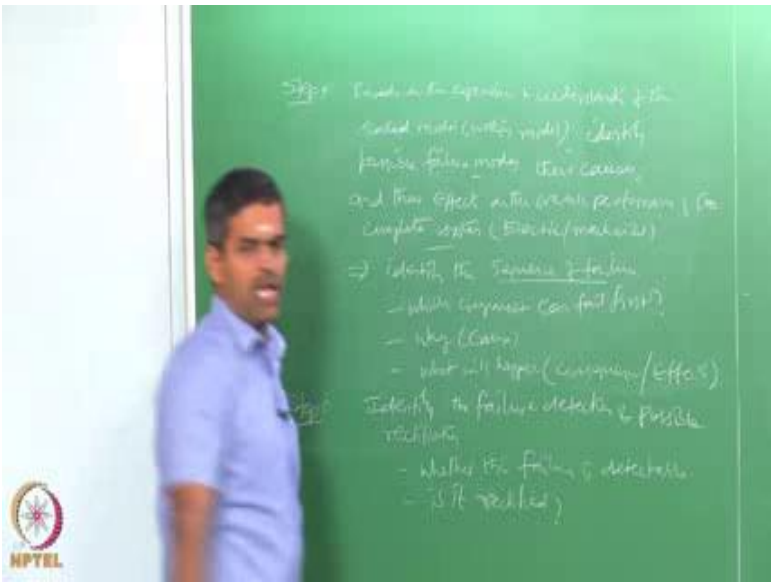


First step define the system, define the system includes have a shop drawing, specification of components, if possible a scaled model of the system. So, we have to define the system first in detail.

Second step, identify the functional relationship of the components with the system. Also identify the performance requirements of each component that is what we call as design intent what are the performance requirements of each component should be identified in the beginning. Step number three, establish the level of analysis is the component or the product is in the design stage, is it in the modification stage, is it in the exit stage, I mean you do not want this product any more to be used, you want to disconnect the product

because of its risk involved in the whole process line. So, at what level you are doing FMEA is also prefixed before the study starts.

(Refer Slide Time: 17:53)



Step number four, based on the experience and understanding of the scaled model which is possibly a working model, identify possible failure modes. Now it is very interesting, the model is a scaled model it is in the working condition, therefore the model is not going to have any failure mode at all because the model is perfectly working.

You have to perceive this you have to assume, if a specific component is going to fail what will happen to overall performance of the complete model. So, one has got to perceive those failure modes, so identify this failure modes. The reasons for the failure that is what we call as the causes and their consequences that is what we call as effects on the overall performance of the complete system; system I refer here is electric or mechanic systems not a chemical or process system; mechanical systems that is what we mean here.

So, in step number four, you have to also identify the sequence of failure that is very very important. I mean you should identify which component can fail first. Why, that is what

the cause; if it fails what will happen that is what the consequence what we call as effects. So, you study the sequence of failure that is very important step number four.

In step number five, you identify the failure detection and rectification. What does it mean is if the system is going to fail because of failure of any specific component which perceive in this step. Then identify whether this failure is detectable, can we physically see this failure? For example, an arm may break in a shaft your (Refer Time: 21:14) may get disconnected in an electric cable or a lay out. So, can we physically detect this kind of failure? Is it detectable? If it is detectable then, can it be rectified, can it be corrected.

(Refer Slide Time: 21:37)

In step number six, identify the design changes that are required for those critical components, also identify the operating provisions that can be recommended to avoid the failure of components.

Based on this, in step number seven, prepare a list of recommendations or actions and summarize. So, one can see here there are various steps which are involved in an total FMEA methodology, some of the steps are qualitative, some of them are quantitative. Let us quickly see which are qualitative. Defining a system is a qualitative step because you are going to describe the system in terms of its operational features, in the design idea,

shop drawing etcetera you will not associate any number, any numeric value at this level of analysis.

The step number two you are identifying the functional relationship, again this is qualitative because again you are not going to assign a number to this case, you are going to only identify the performance requirements or design intends. In the third stage, I going to prefix the level of analysis what you want to do, is it in operational stage, is it in modification stage, design stage etcetera this is also qualitative.

We move to step number four we are going to identify the sequence of failure. The sequence of failure cannot be identified unless you attach an associate number which can ascend or descend the order of failure, therefore, this is quantitative. Now where quantitative if it is coming in to play here you are going to assign a specific number to the failure identification, detection and rectification. So, on a 10 point scale we can always identify a number to each one of these components in terms of identification of failure, detectability, occurrence of failure, and can it be rectified.

So, on a 10 point scale you assign a number then you will be able to get a step number five what we call risk priority number therefore, this is again quantitative because here you get a numeric index, here also you will get a numeric index. Ultimately I am converting a qualitative study of performance of a specific item or object or a product into a quantified risk analysis.

So, I am connecting qualitative analysis and understanding and interpreting the damages anticipated in the design through a quantified number. Friends wherever you are looking for a final summary of risk analysis it should be always indicated in terms of a number. This number can even probabilistic terms or in deterministic terms, but anything which is qualitative cannot be really ranked is very difficult, you will not be able to relatively compare them and say which is better than the other because the parameters which are used for qualitatively indexing them may not be common to all those items which you are trying to compare.

However, when you convert them into a numeric value or quantify them in risk analysis modes then you can ascend or descend these to identify the most critical component that is how the FMEA converts the qualitative observations into quantitative system. And ultimately in step number six, depending upon the highest RPN number you are going to identify and recommend the changes therefore, this step anyway is quantitative and of course, this step is only a summary which gives me the recommendation so therefore, this has to be qualitative there is no doubt, but however, this is depending upon the number or the numeric figure. We are going to derive the recommendations and give the actions according to suggested by the committee.

So, let us quickly see what would be the system definition means. We all know as the process of oil exploitation, production, storage (Refer Time: 26:58) is highly complex. FMEA generally done in small steps, as we also understood hazop study is not done for the entire plant, it is done on segment of the plant and we already learnt how the segmental hazop studies can be integrated for the entire unit in terms of simple software which helps you to connect the data base from that of the recommendation made in the first segment of the plant to that of the nth segment of the plant by simply identifying these numbers from the existing data base.

Similarly, here also one can do FMEA in small steps then integrated to the complete extend of the system and one can analysis the system as failure of different modes or failure of difference components of the whole system. So, here the idea is not to analyze the system as a whole, but system as a whole through parts of the system or components of system. Therefore, one can say FMEA is component level analysis. So, it is very important to know the interaction between the components, before we look in to the consequence of the failure of these components on the overall performance of the system.

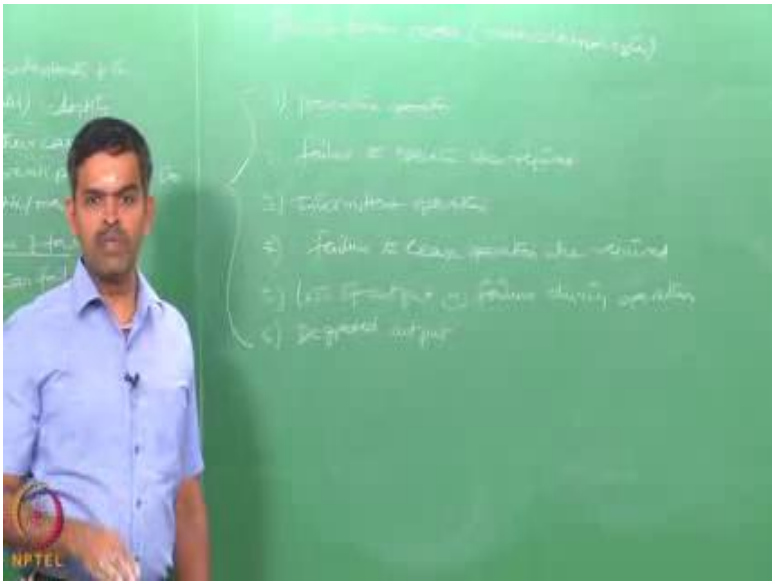
So, when you define the system be very clear in defining the interaction of components that is very important then only you will know, will your component failure lead to cascading effect of the whole system. What we saw in the beginning about orientation mistakes is nothing but accident or incidents. So, that what we are insisting hear as well.

So, if you look at the level of analysis as I said in step number three. The level of analysis depends upon what kind of functional or structural system you are discussing for FMEA. It is not about the physical component system at all, it is about the functional structure of the system. So, it is the failure mode which is insisted not the physical system which we are looking at. So, the primary function of a system should be identified then any deviation from the primary function of the system should be identifying through deviations of the components of failure of the system which can be a sub system as well. So, one can look for a primary function of a system, one can then identify the secondary function of the system then, if you feel the deviations between the primary and secondary functions system is going to be affected by the failure of components of the system then keep on identifying them and ranking them as the most critical component that is what we call as level of analysis.

The level of analysis also means, you are bisecting the whole system into various levels of components and diagnosing each component level to find out the consequence of that failure on the overall system, do you understand.

So, all possible failure modes should be identifying. Now the question is what are the possible failure modes in a given analysis of a mechanical electrical system.

(Refer Slide Time: 30:14)



Possible failure modes of a mechanical or electrical system, the component can have a premature operation, what do you mean by premature operation? Let us take for example, the wall. The wall we suppose to open only when the pressure exceeds let us say 10 bar, but the wall by mistake has opened even when the pressure is reached 9 bar.

So, premature operation the wall we suppose to open only when the pressure exceeds a certain threshold value, but because of a mall functioning of the wall, the wall was already opened a prior to the pressure reaching the threshold value is called premature operation. The second could be failure to operate when required, what you mean by this statement? Let us say, I need to have a wall which should be opened automatically when the pressure reaches 10 bar.

So, in the process line the pressure has reached 10 bar, but the wall has not opened or it is not operated, it is failure to operate when require to operate. The third could be intermittent operation, what does it mean is the wall or the component operates at a spurious manner sometimes it operates, sometime does not operate. But the operational conditions are continuously same, but the mechanical fault is there in the component which prevents the operational the component in the continuous mode.

The fourth could be failure to cease operation when required. That is again take an example of a wall, the wall should close when the pressure drops below 10 bar; the wall should remain open only when the pressure is equal to or greater than 10 bar in the given process line. So, when the pressure exceeds 10 bar the wall opened then the pressure was controlled by some mechanism or some mechanical means. The pressure dropped down to let us say 9.59 bar at that incidents the wall should close because the wall should remain open only when the pressure remains at 10 bar or higher. So, in this case the wall does not close even though the pressure drops down below the threshold value where the wall should remain operatable. So, failure to cease operation when require.

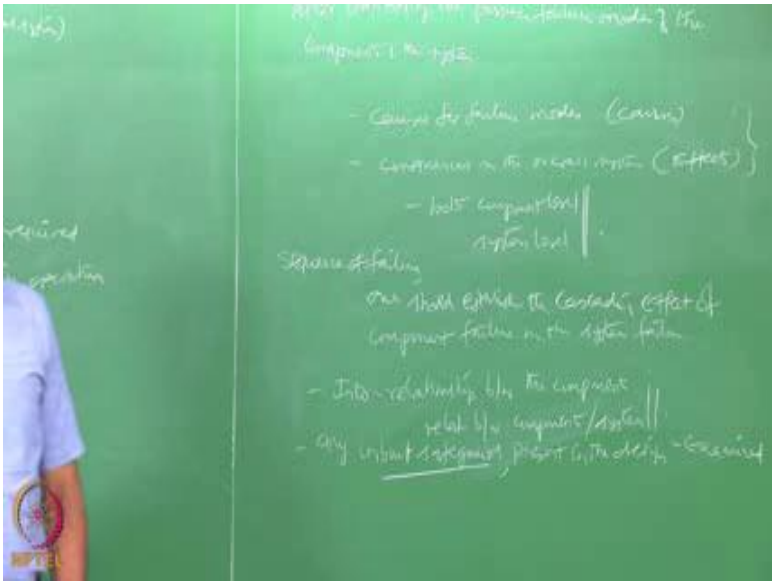
Loss of output or failure during operation, let us say I have a sensor which should glow or we should raise an alarm when the temperature in a given system exceeds may be 100 degree Celsius. So, the temperature sensor records a temperature if the temperature exceeds 100 degree Celsius in a given system, it should raise an alarm. But the sensor

records a temperature does not trigger of the alarm system and the alarm does not work even though the temperature is exceeding 100 degree Celsius. Loss of output from the sensor or failure during operation is again a case of failure.

Six could be degraded output, you want a specific level of output but you are getting the output, but the output is not satisfactory as level to the performance function of the system. So, these are the possible failure modes which can very commonly occur in an electro mechanical systems which are not very common in case of chemical process systems. So, these are the analysis of failures which are very commonly used successfully in FMEA studies.

Now, once identifying, after identifying all the possible failure modes in a given mechanical electrical system then one should also look at what are the possible causes, the reasons for these kinds of failure modes to happen and if they happen what would be the effects or the consequences on the overall system?

(Refer Slide Time: 35:01)



After identifying the possible failures modes of the components of the system then one would should look for what are the causes for such failures modes, and if they fail what

would be the consequences on the overall system what we call as effects. So, this is what we call as causes.

So, one should now look at the possible causes and consequences. Now the causes and consequences should be looked at both - component level and system level. So, this will help you to really find out the sequence of failure. So, if you really wanted to find the sequence of failure one should establish the cascading effect of component failure on the system failure. To understand this, one must know very clearly the inter relationship between the components as well as the relationship between the components and the system the both should be understood very thoroughly.

Suppose, in the prose of identifying the causes and consequences if the system has got an inbuilt safeguard then that should also be examined. So, any inbuilt safeguard present in the system should also be examined, now this will be helpful to really identify any component where inbuilt safeguard is present then that component will not be in the priority of failure. For example, let us say there are some electrical components where the working of the component will cut off when the temperature rises beyond a specific value, when the input voltage rises beyond a specific value etcetera.

There is auto cut off facility may be available as an input in the design itself. So, if such safeguards are present in the component level one should also account for those safeguards present in the system because that will prevent the cascading effect of the failure of the whole system. So, if really wanted to identify their sequence of failure one should look at the inter relationship between the components and the safeguards present in the component which may or may not lead to the cascading effect of the failure of the overall system. So, that is what the analyze of failure means.

Once you have identified the consequence then the sequence of failure and so on, one has got a report the whole document in a standard format. So, let us now talk about Reporting.

(Refer Slide Time: 38:52)

One has to identify the most significant failure in the given system, identify also the existing safeguards and the detection devices are adequate. So, one has got to identify essentially the weak link in the system that is what we are interested in. So, the report should focus on bringing out explicitly the weak link.

What do we mean by the weak link? Weak link is that one - is one which has the highest rank of failure this will be the most critical component in the overall system. Please understand friends, the criticality of the component is not because is one of the most expensive components in the given system. The criticality will come only when the component failure will lead to a largest possible cascading effect which will lead to the system failure.

So, one has to go to identify the highest rank of the failure in a given system mathematically, quantitatively whichever component gets the highest rank of failure that is what we call as weakest link in the entire system. So, in that case for the weakest link one has to do detail analysis further, may be the system has to be redesign, material specification may change, component size may be different, etcetera. So, one has to do a further detail analysis.

Friends please understand FMEA only detects the weakest link. FMEA does not analysis the weakest link in detail for a design. So, FMEA prompts in a given system which is the most critical vulnerable component. So, it is for the designer to pick up that component, reexamine the design, re-change the design and then replace it with a new component and then do a FMEA analysis. So, one may also think of redesigning the whole system if the cascading effect is so serious about the design.

So, FMEA is available in a specific format like hazard report.

(Refer Slide Time: 41:23)

So, the format of FMEA is given like this. You have to say which component you are talking about, what failure mode you are going to discuss and what would be the failure effect the component will have and what is the comment or recommendation or action you are going to give. So, that is the simple format which is used for FMEA report. However, in this format where are we going to convert is the qualitative statements into quantitative statements by giving numbers in terms of the order of priority. We will talk about this in detail in the next lecture. By then we will illustrate this by couple of examples, make you to comfortably understand how to prepare an FMEA for a mechanical system which is having a perceived fault.

In this lecture, friends I hope you have understood one of the important tool which can be used for hazard indexing or identification for electro mechanical systems. So, what are the requirements for doing an FMEA, how an FMEA need to be carried out, what are the different levels where you got of focus, what is the most important item in an FMEA output as we have seen in the identification or risk indexing. The FMEA should identify explicitly the weakest link so that the component can be redesigned or the whole system can be rethought of by replacing this component by better component in terms. So, we will look into the more details of FMEA in the next lecture.

Thank you very much.