

# Health, Safety and Environmental Management in Petroleum and offshore Engineering

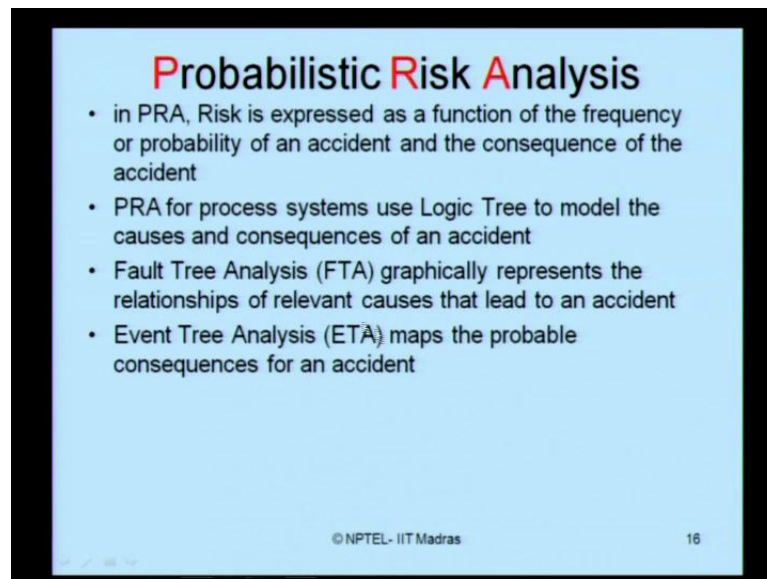
Prof. Dr. Srinivasan Chandrasekaran  
Department of Ocean Engineering  
Indian Institute of Technology, Madras

Module No. # 03

Lecture No. # 11

Probabilistic risk analysis

(Refer Slide Time: 00:15)



**Probabilistic Risk Analysis**

- in PRA, Risk is expressed as a function of the frequency or probability of an accident and the consequence of the accident
- PRA for process systems use Logic Tree to model the causes and consequences of an accident
- Fault Tree Analysis (FTA) graphically represents the relationships of relevant causes that lead to an accident
- Event Tree Analysis (ETA) maps the probable consequences for an accident

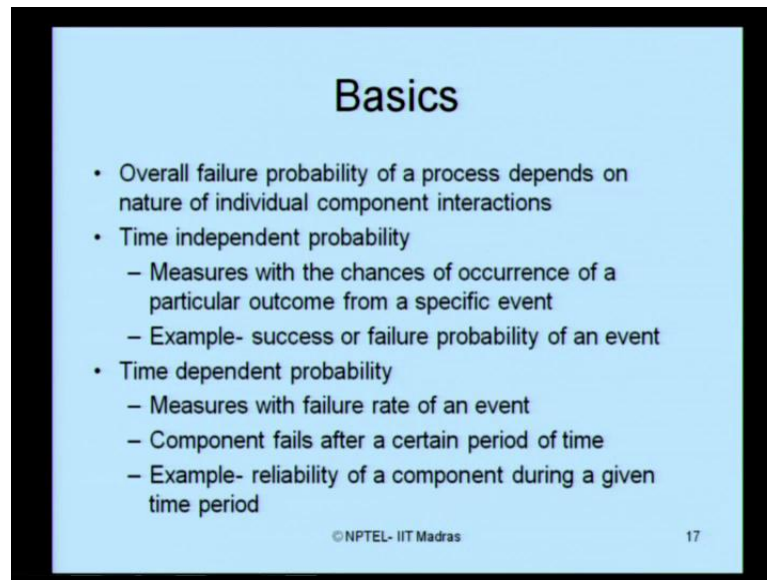
© NPTEL- IIT Madras 16

So, now I am going to discuss about probabilistic risk analysis, what we understand by PRA. In PRA, risk is expressed as a function of frequency or probability, of an accident and the consequence of an accident. PRA for process systems used, what we called as a logic tree to model the causes and consequences. Fault tree analysis – FTA, graphically represents the relationship of relevant causes that lead to an accident. Whereas, event tree analysis what we famously refer as ETA, maps the probable consequences of an accident.

Ladies and gentlemen, in probabilistic risk analysis, mainly people use commonly two type of analysis, what we call as FTA or ETA. FTA represents the relationship of relevant cause that lead to an accident, whereas ETA talks about consequence of an

accident. And we all understand very clearly, what is the difference between cause and consequence. Cause is a reason for an accident, and consequence is an after effect of an accident. So, event tree talks about the after effect, while the fault tree talks about the reason or the cause for such accidents.

(Refer Slide Time: 01:44)



## Basics

- Overall failure probability of a process depends on nature of individual component interactions
- Time independent probability
  - Measures with the chances of occurrence of a particular outcome from a specific event
  - Example- success or failure probability of an event
- Time dependent probability
  - Measures with failure rate of an event
  - Component fails after a certain period of time
  - Example- reliability of a component during a given time period

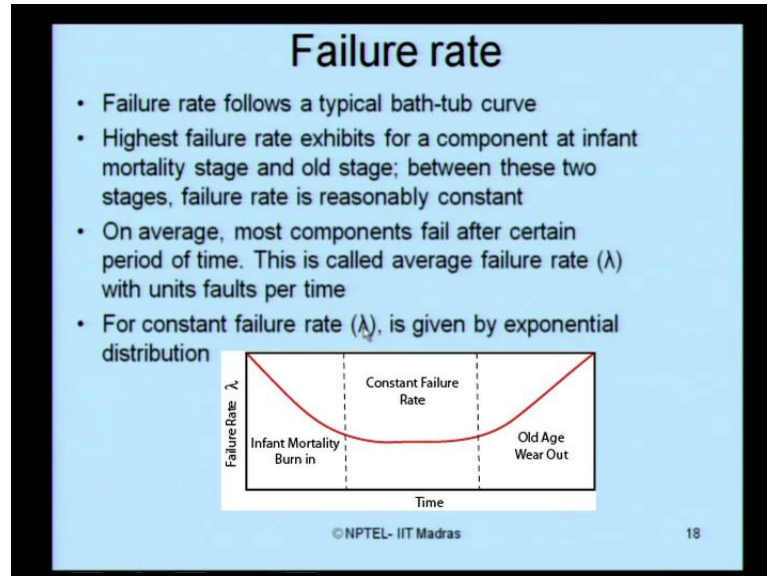
© NPTEL- IIT Madras 17

Before we look into detail, the event tree analysis and fault tree analysis, let us look at too few basics of PRA as such. The overall probability failure of a process actually depends on the nature of individual components interactions. We can express this as a time independent probability; that is the time independent probability basically measures with the chances of occurrence of a particular outcome from a specific event which is independent of time. I can give an example, the success or failure probability of an event. So, it is not calculating or estimating the failure probability within a given time frame. It is time to tell, what is a success or a failure probability rate of any event, which is completely time independent.

We can also express time dependent probability, now such kind of probability failure measures the failure rate of an event. The component fails after a specific period of time. Let us say, for example, the reliability of a component during a given time period is estimated clearly in this kind of study. We have a component; the component is expected to fail after a certain period of time. So, what we look at this kind of probability is that,

what is the reliability of the component or functioning of the component, during any given period of time, so we look for that.

(Refer Slide Time: 03:19)



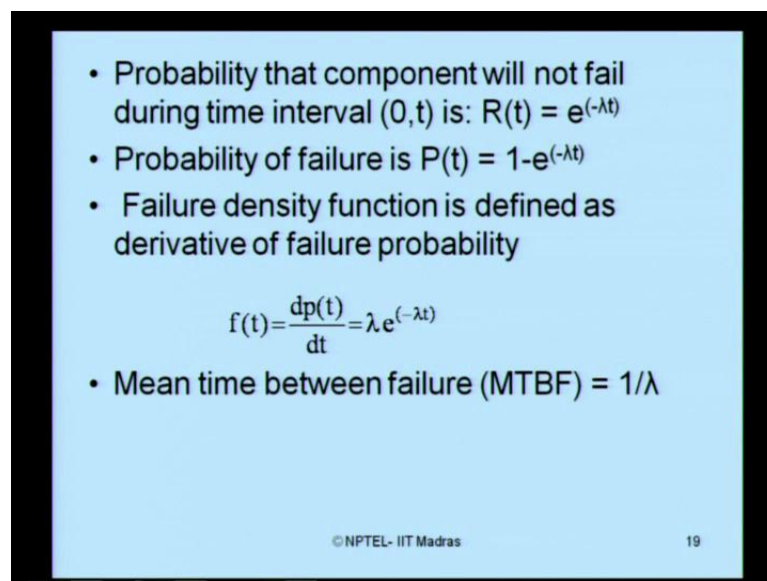
When we look in burn the cases people talk about what we call as a failure rate. The failure rate can be interestingly expressed by what we call as a bath-tub curve. The failure rate  $\lambda$  is given as a bath tub expression in terms of a time scale. Basically, the failure rate actually follows a typical bath-tub curve. The highest failure rate exhibits for a component at infant mortality stage and at the old stage, for example, the component is just new, the highest failure rate is there just before the component is being fixed or introduced in a system. Once the component starts working effectively in due course or passage of time, the failure rate keeps on decreasing. After that, for a specific time of effective functioning of component, the failure rate remains practically constant.

Then subsequently due to malfunctioning of the component after large elapse of time maybe one year, maybe two years depending upon what component we are looking at, the failure rate keeps on increasing with increase in time. So, this is what we call as old age wear out failure rate. This is what we call as infant mortality. You can also understand this in relationship to a human life chain. Child can also die as an infant, because of some basic premature failure during birth, but generally people take care to avoid that kind of death by giving medicines to the mother. Therefore, the failure rate

with passage of time has been decreased. And of course, once the child is born by immunizing and giving some medicines then the child can have a very constant failure rate.

As the person grows older and older, some of his body organism may get wearied out what I should say, therefore then after the specific period the failure rate increases. So, it is a very common phenomenon, which can also be discussed with human life chain, but still we are interested in addressing the probabilistic risk analysis failure rate using what we call as a bath-tub curve. On an average, ladies and gentlemen most components fail only after a certain period of time, because the components are designed initially to be a very **robastic** and rugged as the time passes with passage of time most of the components fail after certain period of time. This is what we call as average failure rate lambda with units' faults per time that is what we measure lambda as.

(Refer Slide Time: 06:15)



- Probability that component will not fail during time interval (0,t) is:  $R(t) = e^{-\lambda t}$
- Probability of failure is  $P(t) = 1 - e^{-\lambda t}$
- Failure density function is defined as derivative of failure probability

$$f(t) = \frac{dp(t)}{dt} = \lambda e^{-\lambda t}$$

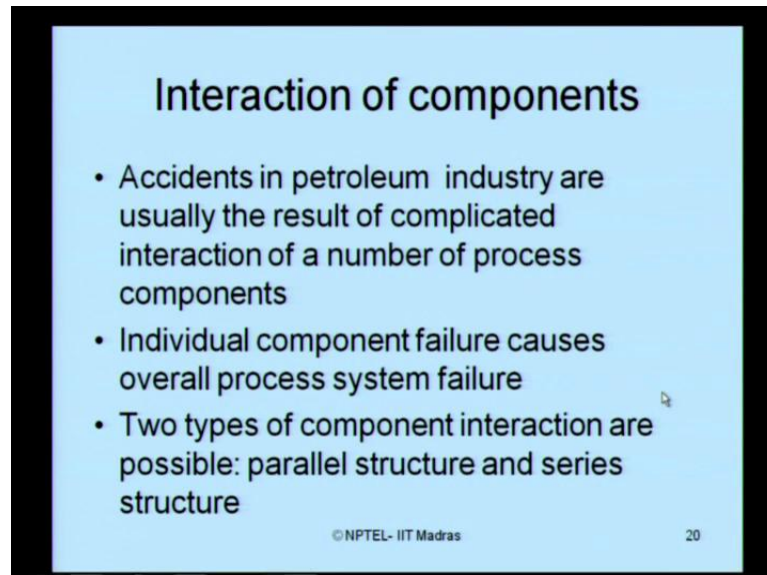
- Mean time between failure (MTBF) =  $1/\lambda$

© NPTEL- IIT Madras 19

For constant failure rate, then it follows an exponential distribution which is given by this equation. The probability that component will not fail during time interval (0, t) is what we call as R of t which is e to the power of minus lambda t, of course the probability of failure which will be P of t is nothing but 1 minus R or t. The failure density function is then defined as, the derivative of the failure probability as given by this expression which is dp(t) by dt. One can also estimate, what you call as mean time

between failure for example, you have got one failure, you will have the other failure what is the mean time between such failures is nothing but  $1/\lambda$ .

(Refer Slide Time: 07:02)



**Interaction of components**

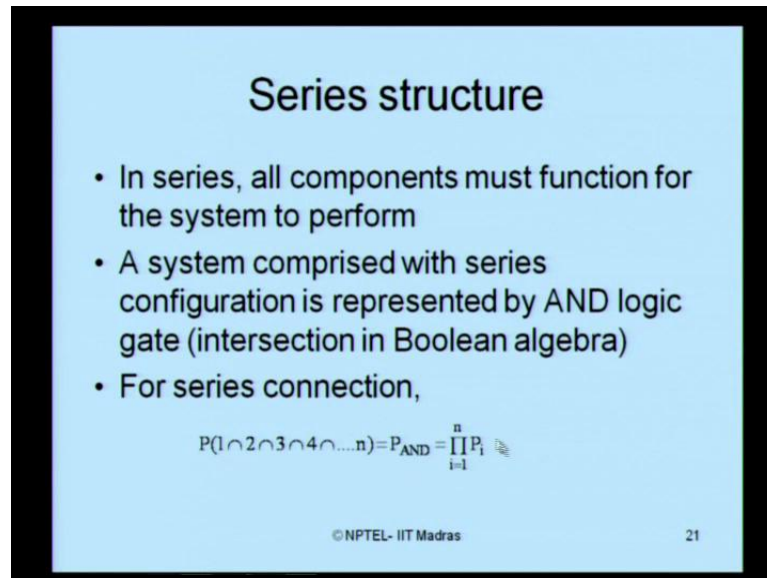
- Accidents in petroleum industry are usually the result of complicated interaction of a number of process components
- Individual component failure causes overall process system failure
- Two types of component interaction are possible: parallel structure and series structure

© NPTEL- IIT Madras 20

Let us look at interaction of the components. Accidents in petroleum industry are usually the result of complicated interaction of number of process components. The accident is not initiated by just only one process component, it may also basically come from interaction of different process components which are very, very common phenomenon for in petroleum industry which results actually in accident in petroleum industry.

The individual component failure actually causes an overall process system failure. There are two types of component interaction which are possible. One is what we call as a parallel structure and other is what we call as a series structure.

(Refer Slide Time: 07:45)



**Series structure**

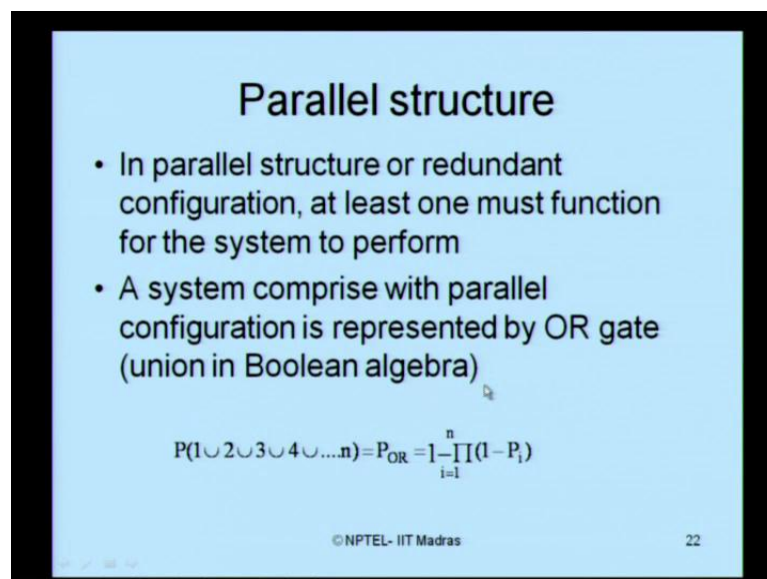
- In series, all components must function for the system to perform
- A system comprised with series configuration is represented by AND logic gate (intersection in Boolean algebra)
- For series connection,

$$P(1 \cap 2 \cap 3 \cap 4 \cap \dots \cap n) = P_{\text{AND}} = \prod_{i=1}^n P_i$$

© NPTEL- IIT Madras 21

What is a series structure? In series, all components must function for the system to perform. A system comprised with series configuration, is represented usually by AND logic gate that is intersection symbol in Boolean algebra. So, for series connection p of 1 and 2 and 3 and 4 and so on there are n components are present, then I can say, in series, structure, all components must function for the system to perform Therefore, the probability can be expressed as given equation  $\prod_{i=1}^n P_i$  of varying from 1 to n i simply say  $P_i$ .

(Refer Slide Time: 08:29)



**Parallel structure**

- In parallel structure or redundant configuration, at least one must function for the system to perform
- A system comprise with parallel configuration is represented by OR gate (union in Boolean algebra)

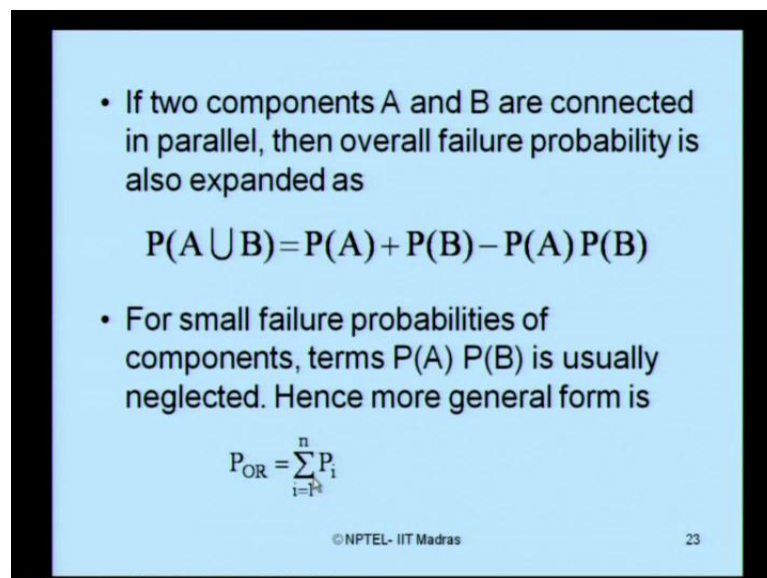
$$P(1 \cup 2 \cup 3 \cup 4 \cup \dots \cup n) = P_{\text{OR}} = 1 - \prod_{i=1}^n (1 - P_i)$$

© NPTEL- IIT Madras 22

If you look at on the other hand the parallel structure. In parallel structure or what we call as a redundant configuration, at least one must function for the system to perform. Contrarily in the serial structure or series structure, all have to function for the system to perform. In parallel structure, at least one must function. This is generally expressed with OR gate which is indicated as union symbol in Boolean algebra.

So, if you want to express the probability of failure then I can say probability of 1, OR 2, OR 3, OR 4 and so on, because I must at least have one of these components in the functional order for the system to perform which is I call as probability of or function which is given by a simple expression.

(Refer Slide Time: 09:23)



• If two components A and B are connected in parallel, then overall failure probability is also expanded as

$$P(A \cup B) = P(A) + P(B) - P(A)P(B)$$

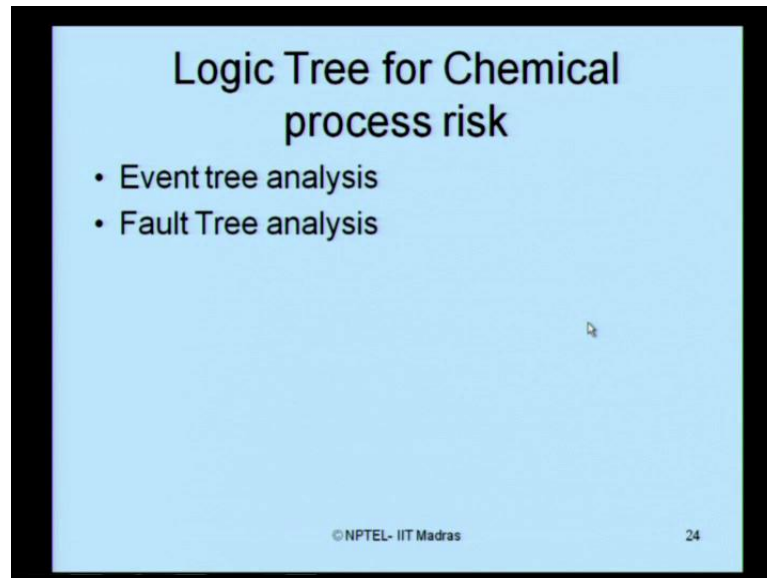
• For small failure probabilities of components, terms  $P(A)P(B)$  is usually neglected. Hence more general form is

$$P_{OR} = \sum_{i=1}^n P_i$$

© NPTEL- IIT Madras 23

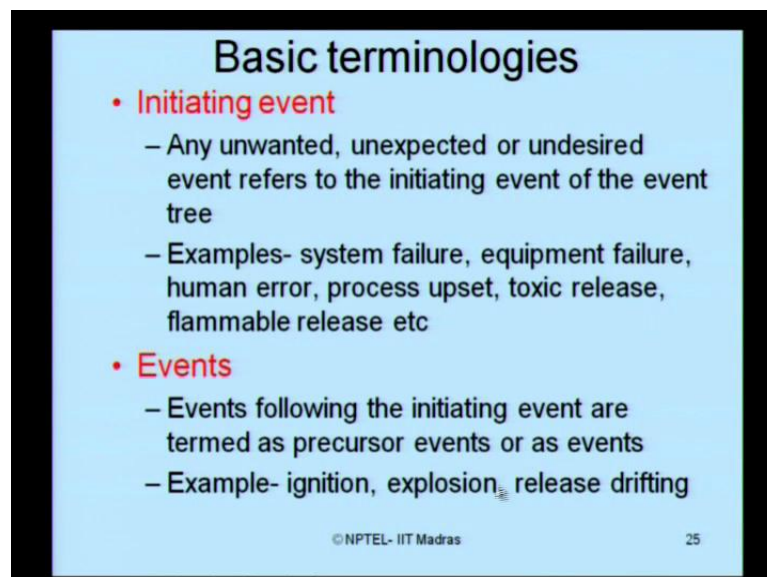
If two components are A and B are connected in parallel, then the overall failure probability is then expanded as simply A union B which is simply P of A, there is probability of failure of A alone plus probability of failure B alone minus probability of joint failure of A and B as well. For small failure, probabilities of components, P (A) product P (B) is usually neglected. Hence, in the more general form, I can say P OR is given by simply this equation which you saw in the previous slide as well.

(Refer Slide Time: 10:00)



Now, let us look at expressing the failure phenomena for chemical process risk. If you want to do a probabilistic risk analysis, expression for chemical process risk, then generally we go what we call as logic tree. Let us see what is a logic tree? Logic tree can be of two types, one is what you call as event tree analysis; other is what we call as fault tree analysis.

(Refer Slide Time: 10:29)



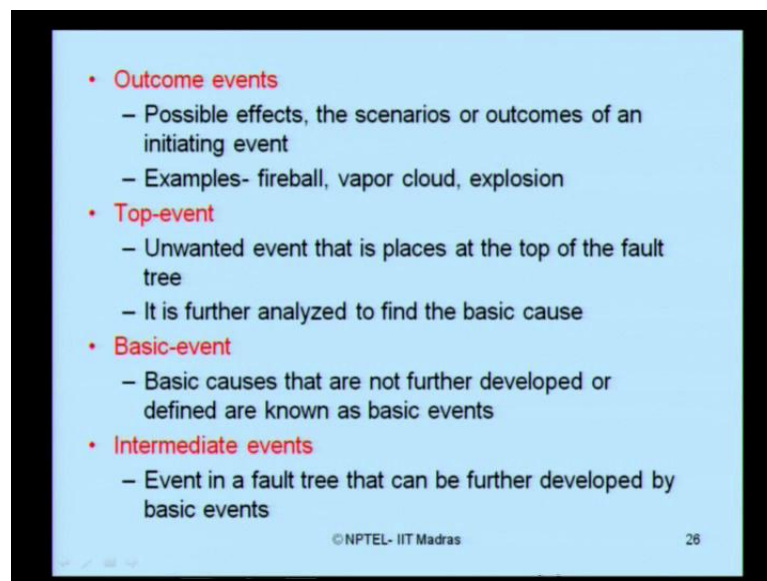
Before we look at the event tree and fault tree analysis in detail with some examples. Let us first try to understand some basic terminologies in logic tree analysis. What do we



understand by an initiating event? An initiating event is any unwanted, unexpected or undesired event in the event tree. There are many examples system failure is undesired; equipment failure is unwanted, but it can be unexpected. Human error is undesired, but it can become unexpected, process upset, there could be a toxic release, there could be a flammable release. All these are what we call as initiating event, because they are either unwanted; they are either unexpected or undesired in any given event tree.

So, then what is an event? Events following the initiating event are termed as precursor events or simply as events. Initiating event is that first event which is generally considered as unwanted, unexpected or undesired. All events which is following these event are simply called as precursor events or simply as events. I can give some examples, ignition, explosion, chemical release, drifting etcetera.

(Refer Slide Time: 12:02)



What do we understand by outcome events? These are nothing but the possible effects, the scenarios or outcomes of an initiating event. Initiating event is that event which is undesired which is unexpected, unwanted. However, if such events are present, then they will give an outcome; there will be on possibly effect on the scenario of an initiating event. That possible outcome is what we call as an outcome, for example, there could be a fireball; there could be a vapor cloud; there could be an explosion. All these are what we call as outcome events, which are results effects of initiating event present in the scenario.

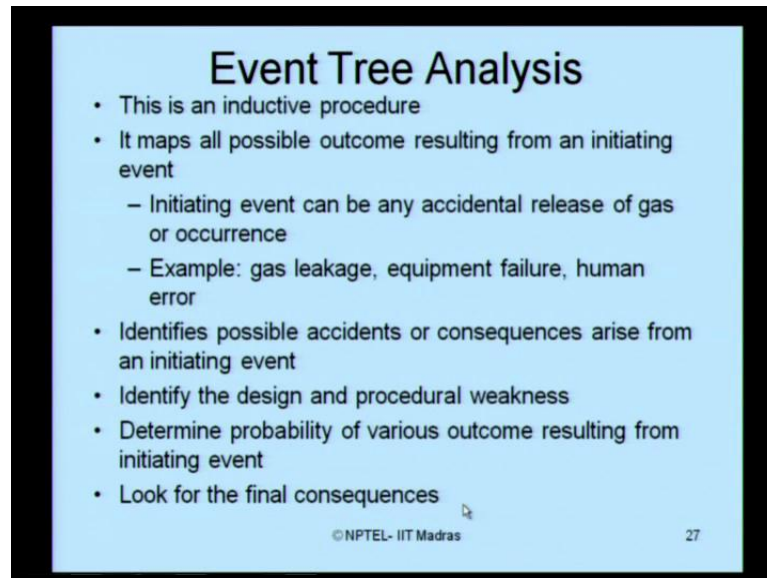
What do we call as a top-event? Top-event is that unwanted event which is placed at the top of the fault tree. What is the significance of this event? The significance is this event should be further analyzed to find the basic cause for making this event as a top-event. So, top-events on the other hand can be considered as most critical events which should be further analyzed in detail to basically know, what is the fundamental reason for such kind of initiating event to be present in the system? Or expected to be present in a given system?

What do we understand by the term basic-event? The basic causes that are not further developed are what we call as basic events. Of course, these are events which follow the initiating event, but they are not further developed actually. Such events are what we called as basic events.

There can be something called intermediate event. There is nothing but event in the fault tree, which can be further developed to form some basic events. So, ladies and gentlemen initiating event is the first event which is undesired, in that initiating events there can be many, then we can identify what we call as a top-event which is the most unwanted event. In that case, we must pay critical attention to that event to really find out the reason for that event to be qualified as a top-event.

Basic-event is, of course, an event following the initiating event, but they need not be or generally they are not further developed for detail analysis. Intermediate events are in between the top and the basic-event, which can be slightly enhanced, explored for further development to form basically some of the basic events.

(Refer Slide Time: 14:54)



**Event Tree Analysis**

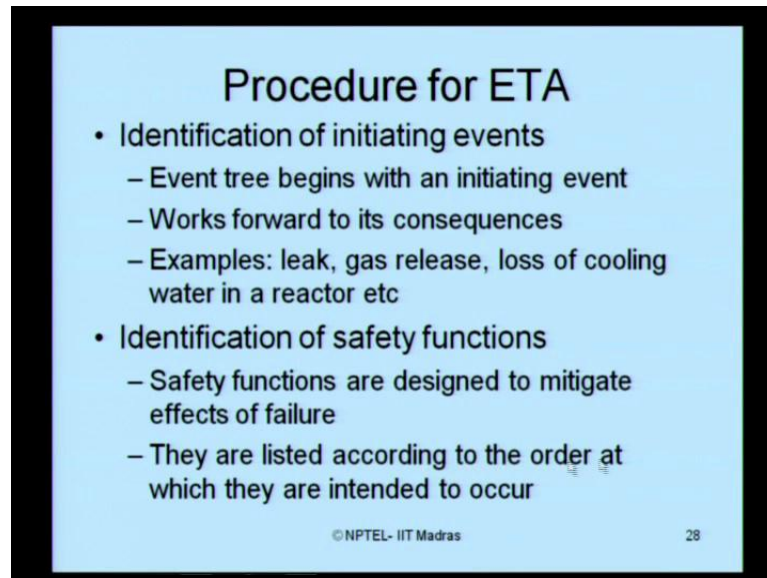
- This is an inductive procedure
- It maps all possible outcome resulting from an initiating event
  - Initiating event can be any accidental release of gas or occurrence
  - Example: gas leakage, equipment failure, human error
- Identifies possible accidents or consequences arise from an initiating event
- Identify the design and procedural weakness
- Determine probability of various outcome resulting from initiating event
- Look for the final consequences

© NPTEL- IIT Madras 27

When we look at the even tree analysis, there are some important steps which I want to tell you before exactly we do an event tree analysis. This is actually inductive procedure; it maps all possible outcomes resulting from an initiating event. The initiating event can be any accidental release of gas or occurrence of any event, for example, it could be a gas leakage, it could be an equipment failure, it could be a human error.

Event tree analysis identifies all possible accidents or consequences arise from initiating event. It identifies the design and procedural weakness. It determines the probability of various out coming resulting from the initiating event. It looks for the final consequences of such analysis.

(Refer Slide Time: 15:44)



**Procedure for ETA**

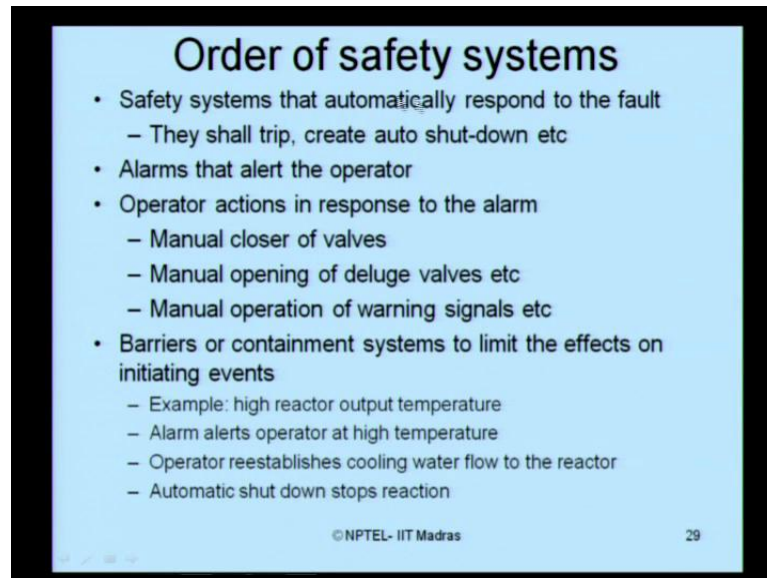
- Identification of initiating events
  - Event tree begins with an initiating event
  - Works forward to its consequences
  - Examples: leak, gas release, loss of cooling water in a reactor etc
- Identification of safety functions
  - Safety functions are designed to mitigate effects of failure
  - They are listed according to the order at which they are intended to occur

© NPTEL- IIT Madras 28

Let me discuss very briefly in few minutes the procedure for event tree analysis. The first step is, identify the initiating event. Event tree actually begins within initiating event. The work is forwarded to its consequences, for example, the initiating event can be a leak, a gas release, a loss of cooling water in a reactor. Followed by that is identify the safety functions.

What are safety functions? Safety functions are those functions which are generally designed to mitigate the effects of failure. Generally if there are many safety functions present in board, how do you prioritize them? How to list them? They are listed according to the orders at which are intended to occur.

(Refer Slide Time: 16:37)



**Order of safety systems**

- Safety systems that automatically respond to the fault
  - They shall trip, create auto shut-down etc
- Alarms that alert the operator
- Operator actions in response to the alarm
  - Manual closer of valves
  - Manual opening of deluge valves etc
  - Manual operation of warning signals etc
- Barriers or containment systems to limit the effects on initiating events
  - Example: high reactor output temperature
  - Alarm alerts operator at high temperature
  - Operator reestablishes cooling water flow to the reactor
  - Automatic shut down stops reaction

© NPTEL- IIT Madras 29

For example, what is the order of a safety system, which we must consider in ETA. A safety system, that automatically respond to the fault will be considered first, for example, a system can have a trip valve it can create an auto shut down facility. So, these are all safety systems which automatically respond to the fault, therefore they are prioritized and kept or considered first. Followed by that is alarm, which can alert the operator. Followed by that, is the operator action in response to the alarm, the operator can initiate a manual closer of a valve, you can initiate manual opening of a deluge valves for spring less systems to be activated. The manual operation of warning signals can also be initiated by the operator as a response to the alarm which is received.

So, safety systems can be multi tier, you can arrange them in such a way that which one has automatic response is considered to be the first in your ETA; the one which is manual is considered to be the last.

In addition, you can also consider what we called as containment systems, because if such barriers or containment systems exist which can limit the effects of initiating event then you can consider them also as a safety system. Because they can also help in mitigating or controlling the accidents, for example, high reactor output temperature can be there alarms alert operators at high temperature, the operator reestablishes the cooling water flow to the reactor and automatic shutdown stops the reaction. So, this can be a

barrier or a containment system which can also be considered as one of the safety system.

Thank you.