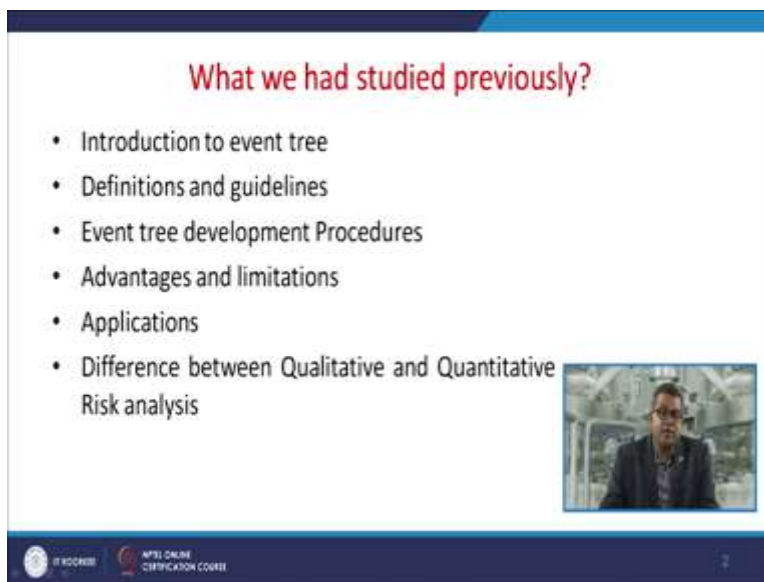


Chemical Process Safety
Professor Shishir Sinha
Department of Chemical Engineering
Indian Institute of Technology, Roorkee
Lecture 43: Fault Tree
Quantitative Risk Analysis

Now welcome to the module pertaining to the Fault Tree Analysis, now this related to the quantitative risk analysis related to the fault tree, so let us have a look about that what we had studied in the previous module.

(Refer Slide Time: 00:38)



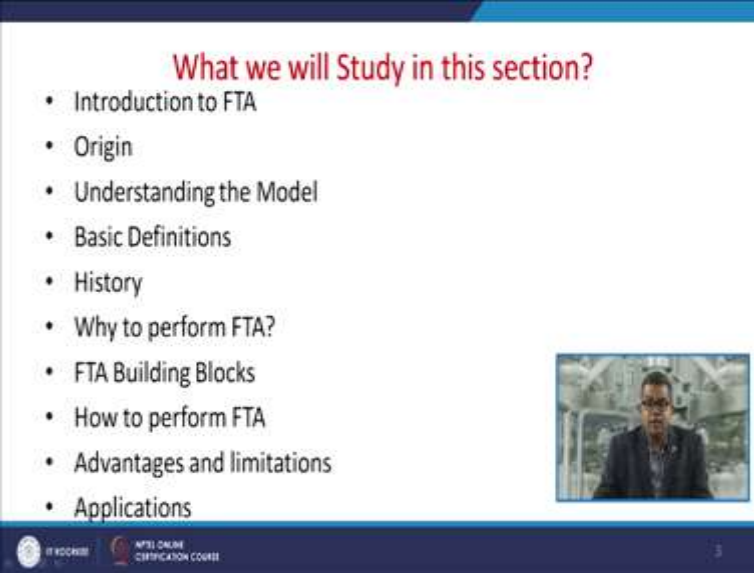
What we had studied previously?

- Introduction to event tree
- Definitions and guidelines
- Event tree development Procedures
- Advantages and limitations
- Applications
- Difference between Qualitative and Quantitative Risk analysis

The slide includes a small video inset of Professor Shishir Sinha in the bottom right corner. At the bottom of the slide, there are logos for IIT Roorkee and NPTEL ONLINE CERTIFICATION COURSE, along with a small number '2'.

We had gone through the basic concept of event tree, we had gone through the definitions and different steps of guidelines related to the event tree, we have discussed about the protocol related to the event tree development, how we can develop the event tree, we have gone through the advantage and disadvantage related to the event tree analysis, discussed about the various applications and above all we have gone through the and we had a discussion about the difference between the qualitative and quantitative risk analysis.

(Refer Slide Time: 01:16)



The slide features a blue header and footer. The main content area is white with a list of topics. A small video inset on the right shows a man in a suit. The footer contains logos for 'BYJU'S' and 'NPTEL ONLINE CERTIFICATION COURSE'.

What we will Study in this section?

- Introduction to FTA
- Origin
- Understanding the Model
- Basic Definitions
- History
- Why to perform FTA?
- FTA Building Blocks
- How to perform FTA
- Advantages and limitations
- Applications



BYJU'S NPTEL ONLINE CERTIFICATION COURSE

Now in this particular module we are going to have an introduction of fault tree analysis, how it originated, we will discuss about the understanding of the model of this fault tree, we will go through the basic definition, history and we will discuss about why we need to perform this fault tree analysis. Now once we will discuss this basic aspect of fault tree perform, then we will discuss about the basic building blocks of fault tree analysis and how they can perform this fault tree analysis. So once we will develop and discuss all these things then we will discuss about the advantages and disadvantages associated with the fault tree analysis with application.

(Refer Slide Time: 02:09)

Introduction

- Industrial operating system consist of a combination of various components club together to form a single unit to perform specific operation.
- It is desirable to analyse the possible failure sequences related to such operations and to perform a probabilistic analysis while developing a production cycle to successfully mitigate the risk associated with it.



NPTEL ONLINE CERTIFICATION COURSE

So let us have an introduction of this fault tree analysis, these industrial operating system, they consist of a combination of various components, they are clubbed together to form a single unit to perform a specific operation, now let us have an example like the production of ammonia. Here it is quite simple that we are having the nitrogen reacting with hydrogen to give you ammonia, but there are several other steps involved, there are several components involved.


The basic component is that what is the appropriate temperature, what are the safety methodology, now if obviously this reaction is an exothermic reaction then how to control the isothermicity of that particular reaction? So there are various components involved in the production of this ammonia, so these components are club together and they form a particular unit for the production of ammonia.



So once we are having the different units so it is desirable to analyze the possible failure sequences those who are related to such operations and we need to perform a probabilistic analysis while developing a production cycle to successful, mitigate any kind of risk there for and associated with that particular thing. So we need to carry out a failure analysis with these six words like Where, When it happens, Why, Who was involved, How it happened and What, so based on these types of sequential questions you may perform these kind of studies.

(Refer Slide Time: 03:56)

Introduction

- This preventive analysis is performed to protect the end user from unidentified and unacceptable consequences.
- Fault tree analysis is one of many tools available to identify potential failures and mechanism associated with them.
- It is a hierarchical representation of various events that directly or indirectly interact with each other, to produce other events and develops a way through which a particular failure can occur.






Now this usually a preventive analysis and this analysis is performed to protect the end user from unidentified and unacceptable consequences, so the fault tree analysis is you can say the one of many tools available to identify the potential failures and mechanism associated with them. So it is a hierarchical representation of various events those are directly or indirectly interact with each other, so you are having different events in a particular plant so they may be either interactive or may be non interactive with each other. So, to produce other events, sometimes if via the interaction and non interaction, they may produce other events and develops a way through which a particular failure can occur.

(Refer Slide Time: 04:51)

Introduction

- Hence proper functioning of the system must be known before performing FTA.
- As FTA produces separate hierarchy for each event, it becomes invaluable for analysing big and complex processes





NTPL ONLINE CERTIFICATION COURSE

So, hence proper functioning of system must be known before performing any kind of fault tree analysis, so as fault tree produces a separate hierarchy for each event it becomes invaluable for analyzing big and complex processes. It is a very important point.

(Refer Slide Time: 05:12)

Origin

- As product and process technology becomes more complex, the visual FTA approach has proven to be invaluable as a stand-alone risk technique or a supplement to Failure Mode and Effects Analysis (FMEA).

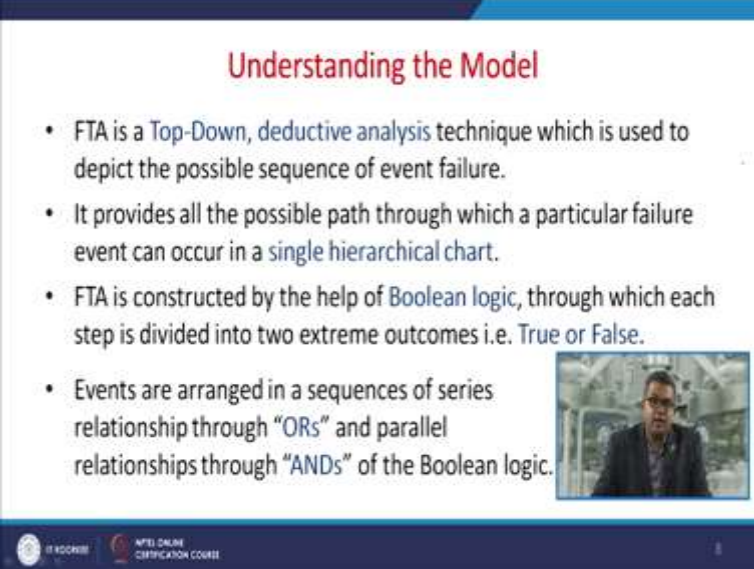


NTPL ONLINE CERTIFICATION COURSE

Now let us discuss about the origin of this one, now as product and process technology becomes more and more complex that we have already discussed with respect to one example of the production of ammonia, the visual fault tree analysis has been proven to be invaluable as standalone risk technique or supplement to the Failure Mode and Effect Analysis.

Now here you are having a FMEA that is the Failure Mode and Effect Analysis, you may start with any one of the function that detect the (failure) various failure mode, go for the severity, then you go for the probability, go for detection and then you perform the risk priority numbers that is R, represented with the multiplication of severity, probability and detection. So this is termed as the failure Mode and Effect Analysis.

(Refer Slide Time: 06:10)



Understanding the Model

- FTA is a **Top-Down, deductive analysis** technique which is used to depict the possible sequence of event failure.
- It provides all the possible path through which a particular failure event can occur in a **single hierarchical chart**.
- FTA is constructed by the help of **Boolean logic**, through which each step is divided into two extreme outcomes i.e. True or False.
- Events are arranged in a sequences of series relationship through **"ORs"** and parallel relationships through **"ANDs"** of the Boolean logic.


© 2020 NPTEL ONLINE CERTIFICATION COURSE

Now let us have understanding of the model that the fault tree analysis is a top down deductive analysis technique which is used to depict the possible consequence or the possible sequence of an event failure, so it provides all the possible path through which a particular failure event can occur in the single hierarchical chart, this FTA is constructed by the help of Boolean logic through which each step is divided into two extreme outcome whether it is true or false. Now these events are arranged in a sequences of a series relationship through O R, ORs or the parallel relationships through AND or AND, the Boolean logic.

(Refer Slide Time: 07:02)

Understanding the Model

- These sequences leads to form a tree-like diagram formed through logic symbols which visualize the dependencies among the events.
- The event can a mechanical components or a software glitch or can be arise from the electronics used while designing the system.
- The failure event of a particular system under study is called the TOP EVENT.
- The event which cannot be subdivided further and hence is the terminating point of the branch of the tree is called a BASIC EVENT.




NPTEL ONLINE CERTIFICATION COURSE

Now these sequences, they lead to form a tree like diagram formed through the logical symbols which visualize the dependencies among the events, now the event can be you can say the mechanical component or a software glitch or can be rise from the electronics used while designing the system. So the failure event of any particular system under the study is called the top event, this one. Now the event which cannot be sub divided further in different branch or sub systems so hence if the terminating group of the branch of the tree that is called the basic event.

(Refer Slide Time: 07:47)

Basic Definitions

- **Fault:** An abnormal undesirable state of a system which can be attributed to implementation of wrong command/ no implementation of command or due to failure of system or component of the system. If the system is interrupted by safety device and has been shut down then it will not be counted as fault.
- **Failure:** Loss of functioning of the system or any component of the system is called failure. Example:
 - Pressure vessel burst - the vessel failure.
 - Cooling coil is not functioning due to corrosion and leaking the coolant - cooling system failure.

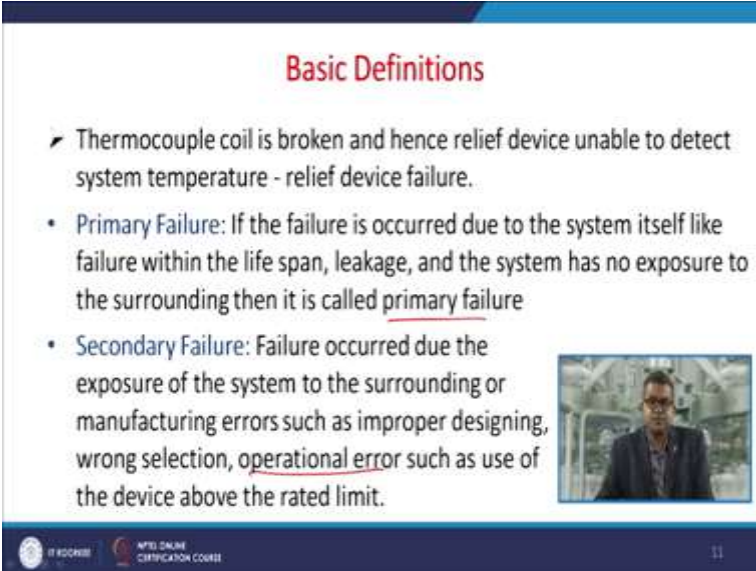


NPTEL ONLINE CERTIFICATION COURSE

Another definition that is the fault, what is the fault, this is an abnormal undesirable state of a system which can be attributed to the implementation of wrong command or sometimes with no implementation of command or due to failure of system or component of the system, so if the system is interrupted by safety device and has been shut down then it will not be counted as a fault because this is the deliberated event.

Now failure that is the loss of functioning of a system or component of the system that is called the failure, for example let us say the Pressure vessel burst, the vessel failure, the cooling coil is not functioning due to the corrosion, sometimes leaking, sometimes lack of pressure, etc. so sometimes the cooling system fails.

(Refer Slide Time: 08:43)



The slide is titled "Basic Definitions" in red text. It contains three bullet points with blue arrows. The first bullet point states: "Thermocouple coil is broken and hence relief device unable to detect system temperature - relief device failure." The second bullet point states: "Primary Failure: If the failure is occurred due to the system itself like failure within the life span, leakage, and the system has no exposure to the surrounding then it is called primary failure". The third bullet point states: "Secondary Failure: Failure occurred due the exposure of the system to the surrounding or manufacturing errors such as improper designing, wrong selection, operational error such as use of the device above the rated limit." To the right of the text is a small video inset showing a man in a suit. At the bottom of the slide, there are logos for "IT EDUCARE" and "NPTEL ONLINE CERTIFICATION COURSE" and the number "11".

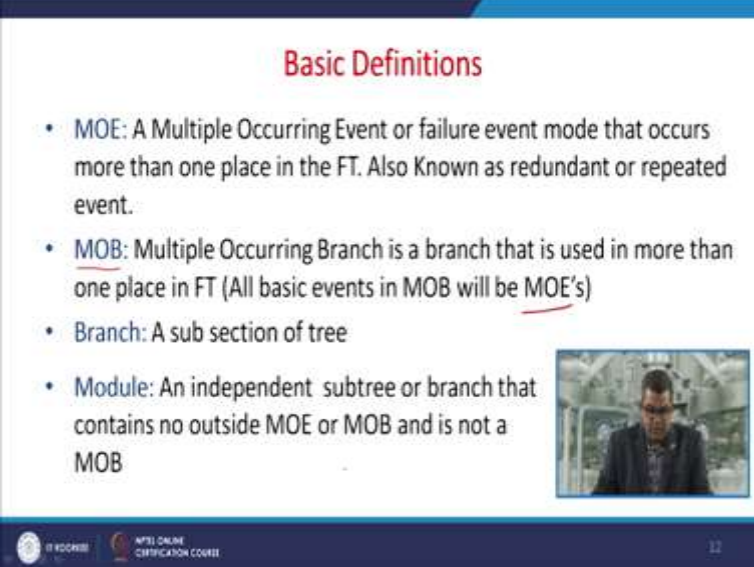
- Thermocouple coil is broken and hence relief device unable to detect system temperature - relief device failure.
- Primary Failure: If the failure is occurred due to the system itself like failure within the life span, leakage, and the system has no exposure to the surrounding then it is called primary failure
- Secondary Failure: Failure occurred due the exposure of the system to the surrounding or manufacturing errors such as improper designing, wrong selection, operational error such as use of the device above the rated limit.

Now sometimes it may happen that thermocouple coil is broken and hence relief device is unable to detect the system temperature so it may be termed as relief device failure, now there is different failures, one is the primary failure, now if the failure is occur due to the system itself like failure within the life span leakage, system has no exposure to the surrounding then it is called the primary failure.

Now the secondary failure, the failure occurred due to the exposure of the system to the surrounding or manufacturing errors such as sometimes improper design may lead to such kind of failure, wrong selection either maybe in terms of a raw material, maybe in terms of process conditions like with respect to the pressure and temperature, sometimes there may be certain

operational errors such as the use of device above the rated limit, etc. So these are termed as the secondary failure.

(Refer Slide Time: 09:53)



Basic Definitions

- **MOE:** A Multiple Occurring Event or failure event mode that occurs more than one place in the FT. Also Known as redundant or repeated event.
- **MOB:** Multiple Occurring Branch is a branch that is used in more than one place in FT (All basic events in MOB will be MOE's)
- **Branch:** A sub section of tree
- **Module:** An independent subtree or branch that contains no outside MOE or MOB and is not a MOB


NPTEL ONLINE CERTIFICATION COURSE


Then there is a concept of multiple occurring event that is called MOE, so MOE or failure event mode that occurs more than one place in the fault tree, this is also known as redundant or repeated event, another is the multiple occurring branch that is referred as MOB. Now this multiple occurring branch is a branch that is used in more than one place of in fault tree analysis, so all basic event in multiple occurring branch will be the multiple occurring events in that particular case, so branch usually are subsection of a tree. The module, an independent subtree or branch that contains no outside multiple occurring event or multiple occurring branch and is not a MOB, that is the multiple occurring branch.

(Refer Slide Time: 10:52)

Cut Set Terms

- **Cut Set (CS):** A set of events starting from basic event to the undesirable top event that together cause the top event to occur is called Cut Set
- **Min CS (MCS):** A CS with minimum number of events that can still cause the top event
- **Super Set:** A CS that contains a MCS plus additional events to cause the top undesirable event.
- **Critical Path:** The highest probability CS that drives the top undesired event probability




 NPTEL ONLINE CERTIFICATION COURSE 13


There are certain cut set limits or cut sets, these terms like cut set, this is set of events starting from basic event to the undesirable top event that together cause the top event to occur that is called a cut set, one is the minimum cut set that is sometimes referred as MCS, now this is a cut set with a minimum number of events that can still cause the top event. There is a super set, this is a cut set that contains a minimum cut set plus additional event to cause the top undesirable event, the critical path, this is the highest possibility cut set that drives the top undesirable event probability.

(Refer Slide Time 11:47)

Cut Set Terms


- **Cut Set Order:** The number of elements in a CS
- **Cut Set Truncation:**
Removal of cut sets from consideration during the FT evaluation process.
CS's are truncated when they exceed a specified order and/or probability.



 NPTEL ONLINE CERTIFICATION COURSE 14

Other is the Cut Set Order, the number of elements in a cut set, the cut set truncation, this is the removal of cut set from consideration during the fault tree evaluation process, these cut sets are truncated when they exceed a specified order or probability.

(Refer Slide Time: 12:10)



History

- Fault tree analysis (FTA) was first developed in 1961 for the U.S. Air Force by H. A. Watson at Bell Telephone Laboratories for use with the Minuteman system
- Later adopted and extensively applied by the Boeing Company
 - As system safety analysis tool (1963)
 - Applied to entire Minuteman system for safety (1964-67, 1968-99)

The slide includes the Bell Telephone Laboratories (btl) logo and the Boeing logo, both with red checkmarks next to them. A small video inset shows a man speaking. The footer contains the text 'BY WATSON' and 'NASA ONLINE CERTIFICATION COURSE'.

So let us have a look about the history of this fault tree analysis, so this fault tree analysis was first developed in 1961 for the United States Air force by H. A. Watson at Bell Telephone Laboratories for the use of with the Minuteman system. Now later it was adopted extensively applied by the Boeing Company. So that is why we have used this the trademark of these two, Bell Telephone Laboratories and the Boeing. So the system safety analysis tool, this was developed in 1963 and is applied to the entire Minuteman system for safety in between 1964 to 67 and 1968 to 1999.

(Refer Slide Time: 13:04)

History

- First technical paper presented at the first system safety conference, held in Seattle, June 1965
- Use by Boeing for the design and evaluation of commercial aircraft, (1966)
- Boeing developed 12-phase FTA simulation program on a Colcomp roll plotter
- Further adopted by Nuclear Power industries (1971-80)
- One of many symbolic logic analytical techniques found in the operations research discipline






NTSI ONLINE CERTIFICATION COURSE 16

The first technical paper presented for at the first system safety conference held in Seattle, June 1965 then it was used by Boeing for the design and evaluation of the commercial aircraft and in the year 1966, the Boeing developed the 12 phase fault tree analysis simulating program in the Colcomp roll plotter and further it was adopted by Nuclear Power Industries between 1971 to 1980. One of the many symbolic logic analytical technique found in the operation research discipline.

(Refer Slide Time: 13:46)

History


- Recognized Software codes include:
 - Prepp/Kitt
 - SETS
 - FTAP
 - Importance and COMCAN
- Adopted by chemical industries (1981-90)
- Commercial codes developed that works on PC's (1991-99)
- Adopted by robotics and software industries



NTSI ONLINE CERTIFICATION COURSE 17

So the recognized software codes, they are included with the Prepp Kit, SETS, FTAP, the Importance and COMCAN, they are adopted by the chemical industries in between 1981 to 1990, the commercial code developed that works on various personal computers, it was in the 1991 to 1999 and it was adopted by the robotics and software industry simultaneously.

(Refer Slide Time: 14:15)



The slide features a title in red text, a bulleted list of conditions, and a small video inset of a man speaking. The footer contains logos for NPTEL and NPTEL ONLINE CERTIFICATION COURSE, along with a slide number.

FTA IS BEST APPLIED TO CASES WITH...

- Large, perceived threats of loss,
 - i.e. high risk
- Numerous potential contributors to a mishap
- Complex or multi-element systems or processes.
- Already-identified undesirable events.
 - A must!
- Indiscernible mishap causes,
 - i.e. autopsies


NPTEL ONLINE CERTIFICATION COURSE 18

Now the fault tree analysis is best applied to the cases which are having the large and perceived threats of losses that is for example very high risk, some cases they are the numerals potential contributors to a mishap, sometimes a complex or multi-element systems or processes they may have the fault tree analysis, sometimes already identified undesirable events can be applied, sometimes certain indiscernible mishap causes like autopsies, etc. so in that particular case we may apply this fault tree analysis.

(Refer Slide Time: 14:59)

Cont...

- Provides a traceable, logical, quantitative representation of causes, consequences and event combinations
- Amenable to, but for comprehensive systems, requiring use of software
- Not intuitive, requires training
- Not particularly useful when temporal aspects are important



NPTEL ONLINE CERTIFICATION COURSE 19

This provides a traceable, logical, quantitative representation of causes, consequences and event combinations, this are the amenable to, but for comprehensive system requiring use of softwares, etc. There is intuitive, requires training, not particularly useful when the temporal aspect they are important.

(Refer Slide Time: 15:27)

Why FTA?

Purpose: Identify combinations of equipment failures and human errors that can result in an accident event

When to Use:

Design: FTA can be used in the design phase of the plant to uncover hidden failure modes that result from combinations of equipment failures

Operation: FTA including operator and procedure characteristics can be used to study an operating plant to identify potential combinations of failures, for specific accidents



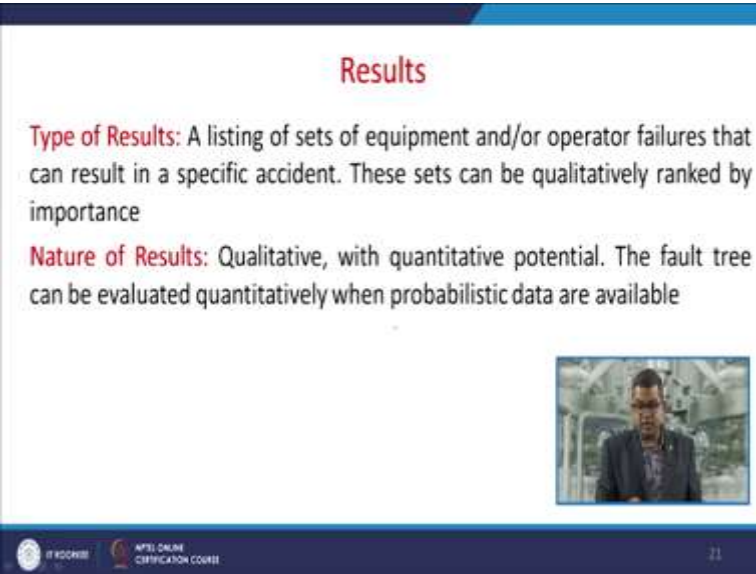
NPTEL ONLINE CERTIFICATION COURSE 20

Now the question arises why fault tree analysis, why we are looking for this fault tree analysis, the basic purpose of this fault tree analysis, is to identify the combination of equipment failure and human error that can result in an accident event, so our predictive mode. Now the question

arises okay we know that why we are using this fault tree analysis, but when to use this fault tree?

So there are couple of options, one is under the design mode that is the fault tree analysis can be used in the design phase of the plant to uncover the hidden failure mode that result from combination of equipment failure another is with respect to the operation, so this fault tree analysis including operator and a procedure characteristics that can be used to study an operating plant to identify the potential combination of failure for specific accidents.


(Refer Slide Time: 16:27)





Results

Type of Results: A listing of sets of equipment and/or operator failures that can result in a specific accident. These sets can be qualitatively ranked by importance

Nature of Results: Qualitative, with quantitative potential. The fault tree can be evaluated quantitatively when probabilistic data are available




  21



Now, let us have a look about the results, there are various types of results, now a listing of sets of equipment or operator failure that can result in the specific accident, so one mode is this one, now these sets can be qualitatively ranked by the importance, the nature of result that is the qualitative with the quantitative potential this fault tree can be evaluated quantitatively when probabilistic data are available so this is the foremost requirement that you must have all these data with you.

(Refer Slide Time: 17:06)

Staff Requirements

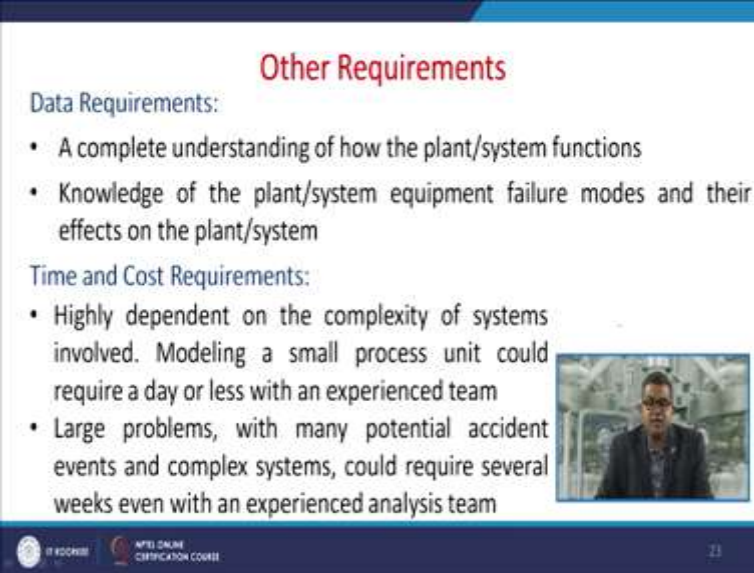
- One analyst should be responsible for a single fault tree, with frequent consultation with the engineers, operators, and other personnel who have experience with the systems/equipment that are included in the analysis
- A team approach is desirable if multiple fault trees are needed, with each team member concentrating on one individual fault tree.
- Interactions between team members and other experienced personnel are necessary for completeness in the analysis process



  22

The other requirements may include the staff requirement so under the staff requirement one analyst should be responsible for a single fault tree so with frequent consultation with the engineers, operators and other persons who have experience with the system or any kind of equipment those involve that particular equipment, involve in the process that are included in the analysis. The next is the a team approaches always desirable if multiple fault trees are needed so with each team member concentrating on one individual fault tree, there must be interaction between the team members and other experienced person, it is always necessary for completeness of this analysis process.

(Refer Slide Time: 18:04)



Other Requirements

Data Requirements:

- A complete understanding of how the plant/system functions
- Knowledge of the plant/system equipment failure modes and their effects on the plant/system

Time and Cost Requirements:

- Highly dependent on the complexity of systems involved. Modeling a small process unit could require a day or less with an experienced team
- Large problems, with many potential accident events and complex systems, could require several weeks even with an experienced analysis team


The slide includes a small video inset on the right side showing a man in a suit speaking. At the bottom, there are logos for 'OF KECORSE' and 'NTEL ONLINE CERTIFICATION COUNCIL' along with the number '21'.

The data requirement, a complete understanding how the plant system functions that is the upmost requirement for this system, the knowledge of the plant, system equipment failure mode and their effect on the plant or system, it is quite essential under the head of the data requirement. The time and cost requirements, they are highly dependent on the complexity of the system involved, modeling a small process unit could require a day or less with an experienced team. The large problem with the many potential accidents or accident event and the complex system could require several weeks even with an experienced analysis team, so that is I mean in terms of a variable.

(Refer Slide Time: 18:56)

Applying Fault Tree Analysis

- Postulate top event (fault)
- Branch down listing faults in the system that must occur for the top event to occur
- Consider sequential and parallel or combinations of faults
- Use Boolean algebra to quantify fault tree with event probabilities
- Determine probability of top event




NPTEL ONLINE CERTIFICATION COURSE 24

Now while considering the (applic) applying the fault tree analysis you must postulate the top event that is the fault then branch down the listing fault in the system that must occur for the top event to occur, must consider the sequential and parallel or combination of the fault, use Boolean algebra to quantify the fault tree with event probabilities you need to determine the probability of the top event that is once you have postulated the top event that is fault.

(Refer Slide Time: 19:34)

Fault Tree Logic

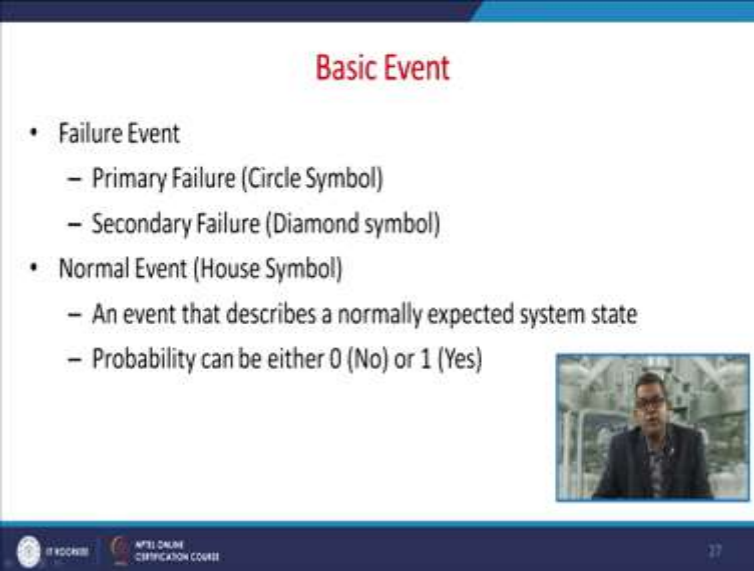
- Use logic gates to show how top event occurs
- Higher gates are the outputs from lower gates in the tree
- Top event is output of all the input faults or events that occur



NPTEL ONLINE CERTIFICATION COURSE 25

Then adopt for the (free) fault tree logic, now use this logic gate to show how top event occurs, higher gates are outputs from the lower gate in the tree, the top event is output of all the input fault or events that occur.

(Refer Slide Time: 19:56)



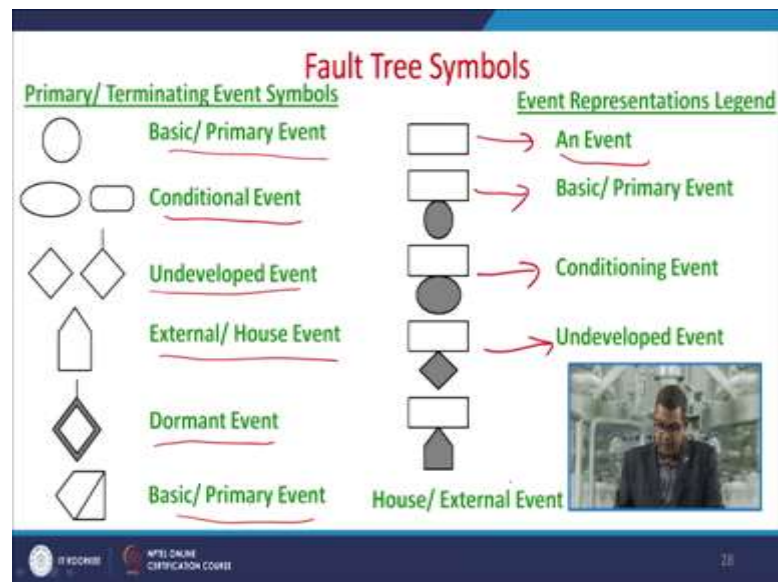
The slide is titled "Basic Event" in red text. It contains a bulleted list of event types:

- Failure Event
 - Primary Failure (Circle Symbol)
 - Secondary Failure (Diamond symbol)
- Normal Event (House Symbol)
 - An event that describes a normally expected system state
 - Probability can be either 0 (No) or 1 (Yes)

In the bottom right corner of the slide, there is a small video inset showing a man in a suit speaking. The slide footer includes the logos of "IIT Kharagpur" and "NPTEL ONLINE CERTIFICATION COURSE" on the left, and the number "27" on the right.

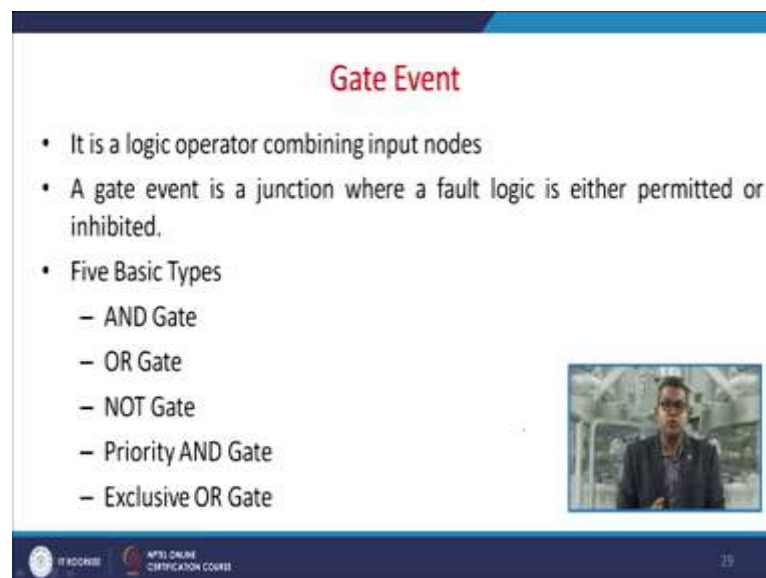
Now there are certain, let us have a discussion about the fault tree building blocks, so you can divide into the four different groups, basic event, gate event, conditional event or the transfer event. So let us have a look about the basic event that is the failure event, that is the primary failure or a (cir) usually denoted by the circle symbol, the secondary failure that is represented by the diamond symbol. The next is the normal event and usually it is denoted by the house symbol, this is an event that describes a normally expected system state, now the probability can be either 0, that is no or 1 that is yes.

(Refer Slide Time: 20:42)



So these are the various symbols which are used in the fault tree analysis, this is the circle, the basic and primary event, the conditional event, the undeveloped event, the external house event, the dormant event, the basic primary event, now these events they are represented by the legends, they are event, this one represents the event, this one is the basic and a primary event, this one is the conditional event, this is the underdeveloped event and this is the house or external event.

(Refer Slide Time: 21:18)




Now let us have a look about the gate event this is the logic operator combining the input nodes so gate event is a junction where a fault logic is either permitted or inhibited so there are only

two options, now there are five basic type of gate events, AND gate, OR gate, NOT gate, Priority AND gate and Exclusive OR gate.

(Refer Slide Time: 21:46)

Condition Event

- It develops a condition that is required for the occurrence of the gate event.
- These conditions are symbolically attached to gate event
- Types:
 - Inhibit
 - Priority AND
 - Exclusive OR





NPTEL ONLINE CERTIFICATION COURSE

Now there are certain condition events so it develops a condition that is required for the occurrence of the gate event, so these two are interlinked. Now these conditions are symbolically attached to the gate event, now there are three types of condition event, Inhibit, Priority AND, Exclusive OR.

(Refer Slide Time: 22:08)

Transfer Event

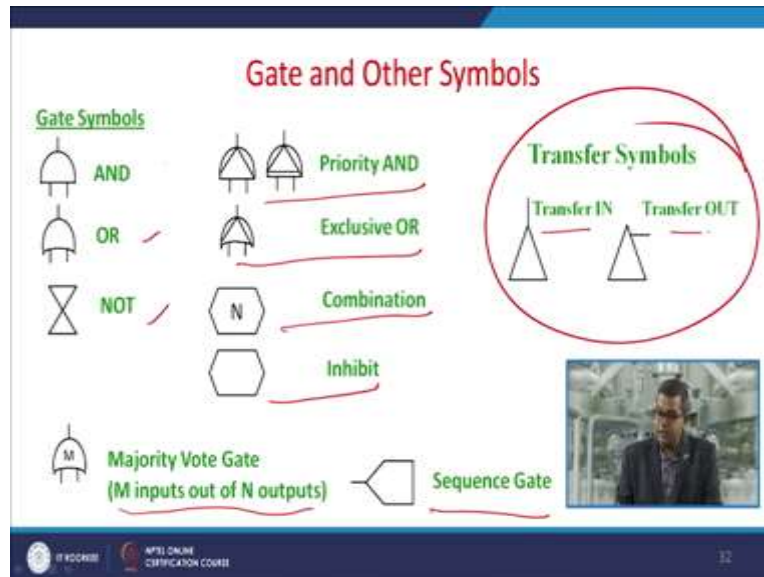
- A pointer used to a tree branch 
- Indicates a subtree branch that is used elsewhere in the tree. It is represented by a triangle symbol.
- Can be used for several purpose:
 - Start a new page of plots
 - It indicates where a branch is used numerous places in the same tree, but is not repeatedly drawn (internal transfer)
 - It indicates an input module from a separate analysis (External Transfer)



NPTEL ONLINE CERTIFICATION COURSE

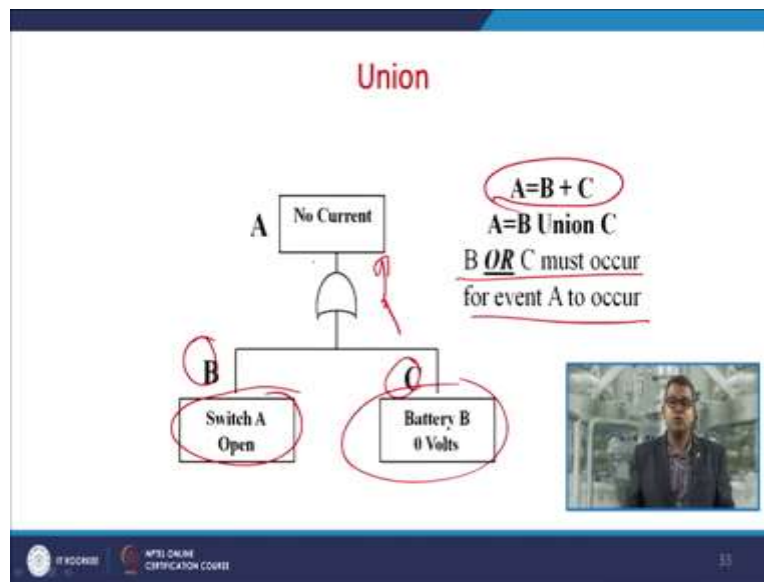
There are transfer event, this is a pointer used to tree branch like this, now it indicates a sub tree branch that is used elsewhere in the tree and it is represented by a triangle symbol, now it can be used for several purposes, now it may start a new page of plot, it indicates where a branch is used, numerous places in the same tree but is not repeatedly drawn, that is the internal transfer. Now it indicates an input module from a separate analysis that is called the external transfer.

(Refer Slide Time: 22:50)



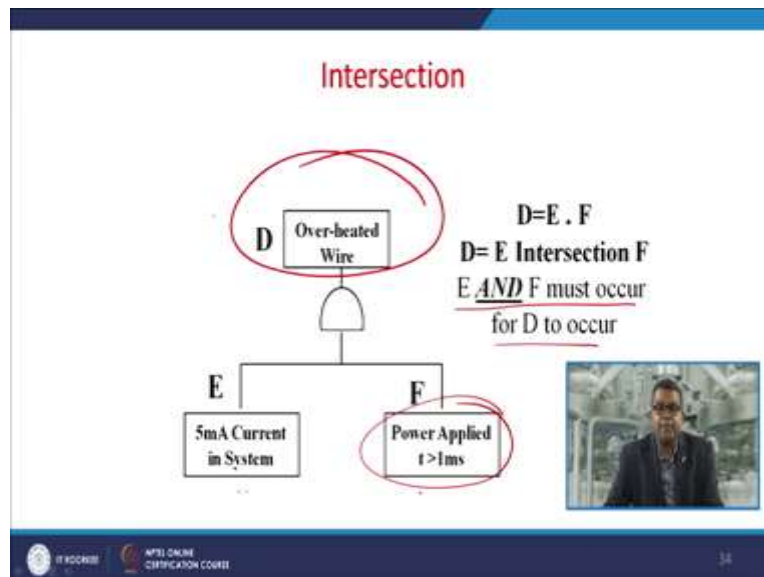
So these are the (gates) gate and other symbol, AND gate, OR, NOT, that is the Priority one, exclusive OR, this is the combination, this is the inhibit and this is the Majority Vote Gate, that is M input out of (N input) N output, now this is the sequence gate and these are the transfer symbols, this is the transfer IN and this is the transfer OUT.

(Refer Slide Time: 23:19)



Now, let us have a look about the union, now here there are two events, either B or C, so if this switch is open then definitely there would be no current and if the battery is at 0 volt then definitely there would be no current so A is the result of B plus C and B or C must occur for any kind of event that needs to occur with respect to A.

(Refer Slide Time: 23:43)



Now whereas in intersection you are having the two system E and F, these are simultaneously they need to be occur like this is the 5 milli ampere current in a system and power applied should

be greater than 1 millisecond so these two needs to be occur, so E and F must occur for any kind of this process to be happen.

(Refer Slide Time: 24:12)



Guidelines for developing a Fault tree

- Replace an abstract event by a less abstract event.
- Classify an event into more elementary events.
- Identify distinct causes for an event.
- Couple trigger event with 'no protective action'.
- Find co-operative causes for an event
- Pinpoint a component failure event.

The slide features a small video inset in the bottom right corner showing a man in a suit and glasses speaking. The bottom of the slide has a dark blue footer with the IIT Kharagpur logo, the text 'IIT KHARAGPUR', 'NPTEL ONLINE CERTIFICATION COURSE', and the slide number '35'.


So there are guidelines for the developing fault tree analysis, you must replace an abstract by a less abstract, to classify the event into the more elementary events, you need to identify the distinct causes for an event and the couple trigger event with no protective action, you need to find the co-operative causes for an event and pin point a component failure event, so these are the certain guidelines for the development of a fault tree.

(Refer Slide Time: 24:52)

How to Perform Fault Tree Analysis (FTA)

The 5 basic steps to perform a Fault Tree Analysis are as follows:

- Identify the Hazard
- Obtain Understanding of the System Being Analyzed ↗
- Create the Fault Tree
- Identify the Cut Sets ↗
- Mitigate the Risk



NPTEL ONLINE CERTIFICATION COURSE 36

Now question arises how to perform the fault tree analysis, there are five basic steps to perform the fault tree analysis, these are, you need to identify the hazards, you need to obtain the understanding of the system which you need to analyze then you create a fault tree then based on your knowledge you identify the cut sets, so once you identify the cut sets then you try to attempt to mitigate the risk whatever being identified through this particular analysis.


(Refer Slide Time: 25:26)

Performing FTA

Step 1: Define the Undesired Event (Top Event)

Usually several different, but equivalent, fault trees can be constructed for a given system. Also, different top events led to different fault trees. It should be defined as precisely as possible:

- How much impact does the top event pose to system?
- What will be the duration of the top event?
- What is the consequence of happening i.e. safety impact?
- What is the environmental impact?
- What is the regulatory impact?




NPTEL ONLINE CERTIFICATION COURSE 37

So let us take the first step that is defining the undesired event and that is obviously is having the top event so usually several different but equivalent fault trees can be constructed for a given

system so also different top events they left to the different fault trees, so it should be defined that as precisely as possible, so you need to ask or frame several questions that how much impact does the top event pose to the system, what will be the duration of that particular top event, what are the (consequence of) consequences of happening, that is the safety impact. What is the environmental impact, what is the regulatory impact, so you need to frame all these questions and you need to answer all these questions.

(Refer Slide Time: 26:22)



Performing FTA

Step 1: Define the Undesired Event (Top Event)

Identify all the Immediate, Necessary and Sufficient events to the the Top Event

Immediate Event: Collection of past events, previous experiences (always include in FT)

Necessary Event: Always try to include only those events which are actually necessary. Inclusion of small faults (events) leads to a complicated visualization.

Sufficient Event: Do not include more than minimum necessary

NPTEL ONLINE CERTIFICATION COURSE


Then identify all the immediate necessary and sufficient events to the top event, now those immediate event they are the collection of past event, previous experience, they should be always included in fault tree, then necessary event, always try to include only those events which are actually necessary. Now inclusion of small faults event lead to the complication and complicated visualization of the scenario, there are sufficient event, so usually do not include more than the minimum necessary.

(Refer Slide Time: 27:01)

Performing FTA

Step 2: Obtain Understanding of the System

- Create or acquire appropriate support information:
 - List of components involved in the system
 - Boundary Diagram
 - Schematic
 - Code Requirements (Safety Codes associated to the system)
 - Engineering Noises and Environments
 - Examples of similar products or failures
 - Previous FTA data (If Available)




NPTEL ONLINE CERTIFICATION COURSE

Now the second step is to obtain the understanding of the system, this create or acquire the appropriate support in formation, this includes the list of the components involved in the system, boundary diagrams, schematic diagrams, code requirements, that is safety code associated to the system, engineering noises and environments, example of similar product or failures and in case if you have any previous fault tree analysis data it should be included.

(Refer Slide Time: 27:37)

Performing FTA

- Starting from top event, list the potential causes of hazard in accordance with the level (Top Event, Level 1, Level 2... Basic Event). The development of FT should be focused on completion single level first and then proceed to the next level.
- Always try to include the past experiences of the design engineers, who have good physical, thermodynamic and chemical knowledge of that system.
- This knowledge is very important for cause selection.

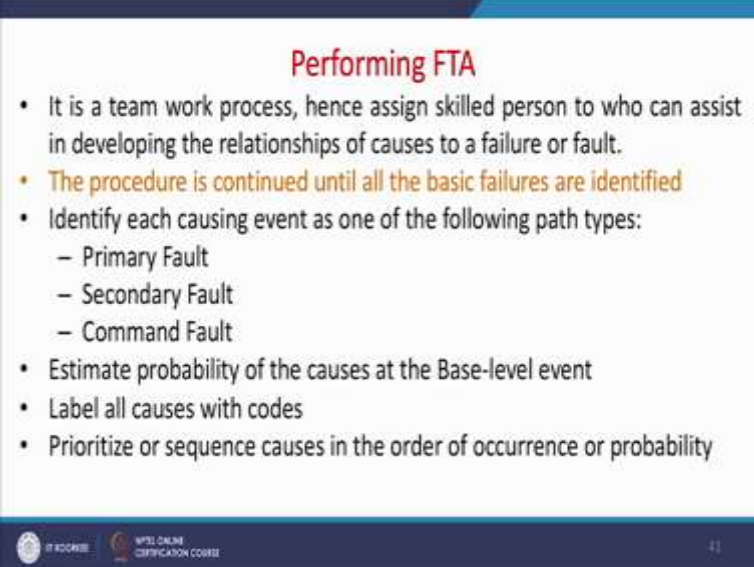


NPTEL ONLINE CERTIFICATION COURSE

Then starting from the top event, list the potential causes of hazard in accordance with the level that is the top level, level 1, 2, 3 to the basic event. The development of fault tree should be

focused on completion of single level first and then proceed to the next level. So always try to include the past experience in the design engineers who have good physical thermodynamic or chemical engineering knowledge of that particular system. Now this knowledge is very crucial for cause selection.

(Refer Slide Time: 28:14)



Performing FTA

- It is a team work process, hence assign skilled person to who can assist in developing the relationships of causes to a failure or fault.
- The procedure is continued until all the basic failures are identified
- Identify each causing event as one of the following path types:
 - Primary Fault
 - Secondary Fault
 - Command Fault
- Estimate probability of the causes at the Base-level event
- Label all causes with codes
- Prioritize or sequence causes in the order of occurrence or probability

WPI ONLINE CERTIFICATION COURSE 41


Now it is usually team work this process, hence assign to who can assists in developing the relationship of the cause to failure or fault, now the procedure is continued until the basic failures are identified. So identify each causing event as one of the following path like primary fault, secondary fault, command fault, etc. Then you need to estimate the probability of the cause at the base level event, now label all (cause) causes with codes and prioritize or sequence cause in order of occurrence or probability.

(Refer Slide Time: 28:58)

Performing FTA

Step 3: Construct the Fault Tree

- The set of events that are all required to produce an event of interest are connected to AND gates
- The set of events that can individually produce an event of interest are connected to OR gates
- It is a complete analysis of system including mechanical, software as well as the electronics used in the system.
- The risks may be prevented through engineering choices or controlled through Quality Control.



NPTEL ONLINE CERTIFICATION COURSE 42

Now the next step is the construction of fault tree, the set of events that all required to produce an event of interest are connected to an AND gate then the set of events that can individually produce an event of interest are connected to OR gate, it is a complete analysis of system including mechanical, software as well as the electronics used in the system. Now this risk may be prevented through engineering choices or control through quality control.

(Refer Slide Time: 29:34)

Performing FTA

- The Basic event (depicted as a circle or oval) is the point at which the team can address the risk. It is typically color coded as follows:
 - Red: Critical Risk
 - Orange: High Risk
 - Yellow: Minor Risk
 - Green: Acceptable / Very Low Risk

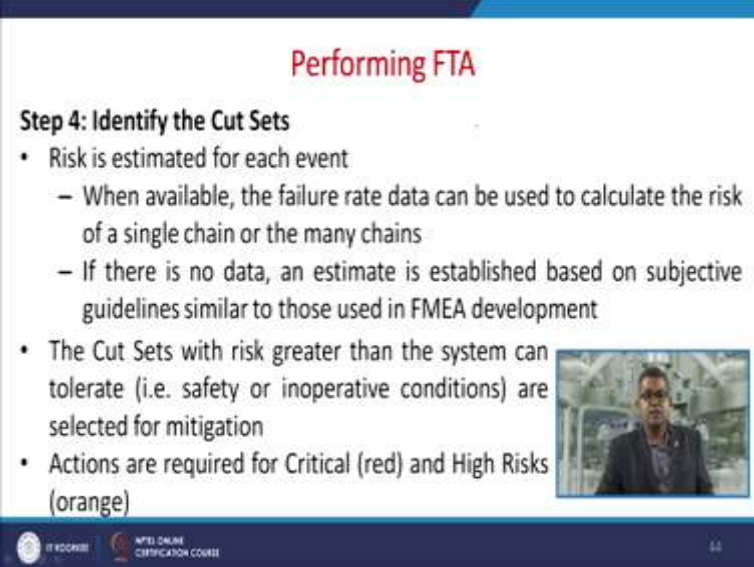


NPTEL ONLINE CERTIFICATION COURSE 43

Now the basic event depicted usually as a circle or oval, now this the basic event is the point at which the team can address the risk, now usually typically they are color coded, usually red that

is the critical risk, orange that is the high risk, yellow minor risk and a green that is acceptable or very low risk.

(Refer Slide Time: 30:04)



Performing FTA

Step 4: Identify the Cut Sets

- Risk is estimated for each event
 - When available, the failure rate data can be used to calculate the risk of a single chain or the many chains
 - If there is no data, an estimate is established based on subjective guidelines similar to those used in FMEA development
- The Cut Sets with risk greater than the system can tolerate (i.e. safety or inoperative conditions) are selected for mitigation
- Actions are required for Critical (red) and High Risks (orange)


NPTEL ONLINE CERTIFICATION COURSE

The fourth step is to identify the cut sets, now risk is estimated for each event so when available the failure rate data can be used to calculate the risk of a single chain or many chain. Now if there is no data, an estimate is established based on subjective guidelines similar to those used in FMEA development, failure mode analysis. Now the cut set with the risk greater than the system can tolerate that is the safety or in operative conditions are selected for mitigation, so the actions are required for the critical, that is the red one and high risk which we have already discussed with respect to the orange color.

(Refer Slide Time: 30:49)

Minimal Cut Set Theory

- The fault tree consists of many levels of basic and intermediate events linked Together by AND and OR gates. Some basic events may appear in different places of the fault tree.
- The minimal cut set analysis provides a new fault tree, logically equivalent to the original, with an OR gate beneath the top event, whose inputs (bottom) are minimal cut sets.
- Each minimal cut set is an AND gate with a set of basic event input necessary and sufficient to cause the top event




NPTEL ONLINE CERTIFICATION COURSE 45

Now the minimal cut set theory says that the fault tree consists of many level of basic and intermediate events linked together (and or) AND OR gates, some basic events may appear in different places on the fault tree, the minimal cut set analysis provides a new fault tree logical equivalent to the original with an OR gate beneath the top event whose inputs sometimes in the bottom are minimal cut sets. Now each minimal cut set is an AND gate with a set of basic event input necessary and sufficient to cause the top event.

(Refer Slide Time: 31:32)

Perform corrections and make decisions

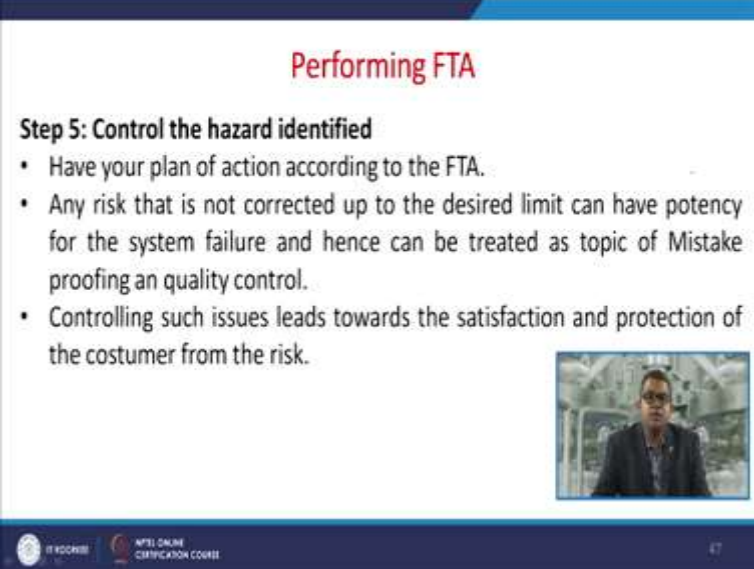
- Application of Boolean Algebra and minimal cut set theory will result in identifying the basic events (A) and combination events (B.C.D.) that have major influence on the top event
- This will give clear insight on what needs to be attended and where resources has to be put for problem solving



NPTEL ONLINE CERTIFICATION COURSE 46

Then you will have a performance correction and then make decision so the application of Boolean algebra and minimal cut set theory will result in identifying the basic events that is A and the combination event BCD that have the major influence on the top events, so this will give the clear insight on what needs to be attended and where the resources has to be put for the problem solving.


(Refer Slide Time: 32:03)





Performing FTA

Step 5: Control the hazard identified

- Have your plan of action according to the FTA.
- Any risk that is not corrected up to the desired limit can have potency for the system failure and hence can be treated as topic of Mistake proofing and quality control.
- Controlling such issues leads towards the satisfaction and protection of the customer from the risk.



  67

The last step that is the step 5 that is the control of hazard identified, now have your plan of action according to the fault tree analysis, now any risk that is not corrected up to the desired limit can have a potency for the system failure and hence can be treated as topic of mistake proofing and quality control. Now controlling such issues they may lead towards the satisfaction and protection of customer from the risk.

(Refer Slide Time: 32:42)

Examples of Mitigation Strategies

When a risk is unacceptable the team may have several options available. The following are a few examples of the options available:

- Design change
- Selection of a component with a higher reliability to replace the Base-level event component
 - ✓ This is often expensive unless identified early in Product Development




NTU ONLINE CERTIFICATION COURSE 48

The examples of mitigation strategy is so when risk is unacceptable for the team may have several options available, there are few example of the options available like you may have option to change the design, you may have a selection of component with higher reliability to replace the base level event component, now this is often expensive unless identified early in product development.

(Refer Slide Time: 33:07)

Examples of Mitigation Strategies

- Physical Redundancy of the Component
 - This option places the redundant component in parallel to the other. Both must fail simultaneously for the hazard to be experienced. If a safety issue exists, this option may require non-identical components.
- Software Redundancy
 - The addition of a sensing circuit, which can change the state of the product, often reduces the severity of the event by protecting components through duty cycle changes and reducing input stresses when identified.

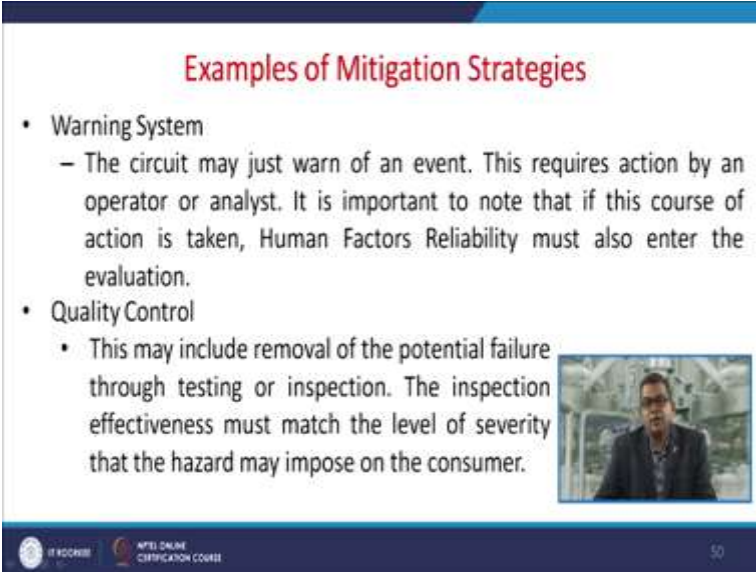


NTU ONLINE CERTIFICATION COURSE 49

Then the physical redundancy of the component, now this option usually places the redundant component in parallel to the other one so the both must fail simultaneously for hazard to be

experienced and that is very unprecedented, so if a safety issue exists the option may require non-identical components. Then the software redundancy, the addition of sensing circuit which can change the state of the product often reduces the severity of the event by protecting component through duty cycle changes and reducing input stresses when identified.

(Refer Slide Time: 33:55)



Examples of Mitigation Strategies

- Warning System
 - The circuit may just warn of an event. This requires action by an operator or analyst. It is important to note that if this course of action is taken, Human Factors Reliability must also enter the evaluation.
- Quality Control
 - This may include removal of the potential failure through testing or inspection. The inspection effectiveness must match the level of severity that the hazard may impose on the consumer.

© 2020 IEEE. ALL RIGHTS RESERVED. NPTEL ONLINE CERTIFICATION COURSE


50

There are certain warnings systems, so the circuit may just warn off an event, now this requires action by an operator or analyst so it is important to note that if this course of action is taken the human factor reliability, they must also enter into evaluation, so this particular aspect is important. Another one is the quality control, so this may include the removal of potential failure through testing or inspection, now the inspection effectiveness must match the level of severity that the hazard may impose on the consumer.

(Refer Slide Time: 34:40)

Things to Remember while doing FTA

- Always try to omit inputs with small probabilities
- Always remember the difference between active and passive components
- Ask Yourself: Does quantified tree make sense?
- Don't fault tree everything
- Careful with Boolean expressions
- Independent Vs dependent failure modes
- Ensure top event is high priority




NTPL ONLINE CERTIFICATION COURSE 51

There are certain things you need to remember while performing the fault tree analysis like always try to omit inputs with a small probabilities, always remember the difference between the active and passive components, sometimes you may need to ask yourself does the quantified tree makes sense, do not fault tree everything, be careful with the Boolean expressions, you must have independent verses dependent failure modes, ensure the top event is having the high priority.

(Refer Slide Time: 35:23)

Fault Tree Quantification

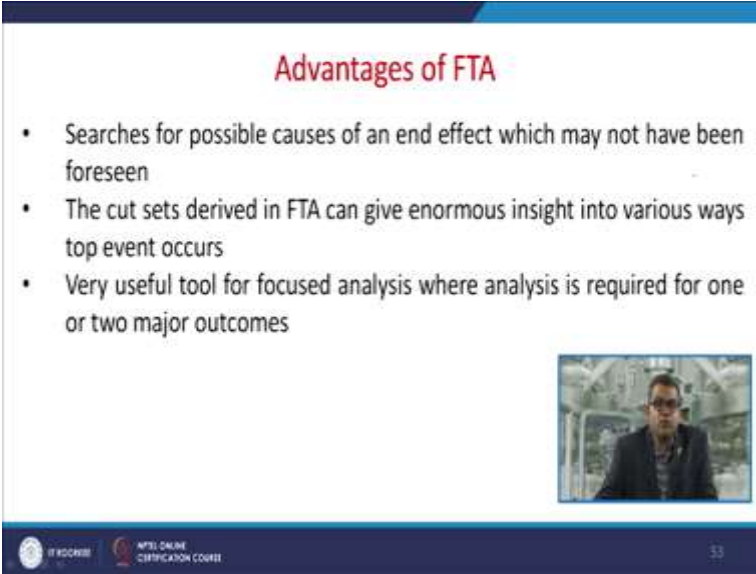
- Fault tree analysis - is not a quantitative analysis but can be quantified
- How to
 - Draw fault tree and derive Boolean equations
 - Generate probability estimates
 - Assign estimates to events
 - Combine probabilities to determine top event



NTPL ONLINE CERTIFICATION COURSE 52

Now the fault tree quantification, this analysis is not quantitative analysis but can be quantified so the question arises how to quantify this one, so draw fault tree and derive the Boolean equations, generate the probability estimates, assign estimates to events and then combine the probabilities to determine the top event, so this the user protocol for this quantification.

(Refer Slide Time: 35:52)



Advantages of FTA

- Searches for possible causes of an end effect which may not have been foreseen
- The cut sets derived in FTA can give enormous insight into various ways top event occurs
- Very useful tool for focused analysis where analysis is required for one or two major outcomes

The slide features a small video inset in the bottom right corner showing a man in a suit and glasses speaking. At the bottom of the slide, there are logos for 'NPTEL ONLINE CERTIFICATION COURSE' and a page number '33'.

Now let us have a look about the advantages of fault tree analysis, this searches for the possible causes of an end effect which may not have been foreseen, the cut sets derived in cut set analysis can derived in fault tree analysis can give enormous insight into various ways the top event occurs, it is very useful tool for focused analysis where analysis is required for one or two major outcomes.

(Refer Slide Time: 36:19)

Advantages of FTA

- Graphical representation of FTA helps understanding the logic.
- Starting from top event, convenient selection of the point of interest to find the root cause of problem.
- Monitoring and control and optimization of the safety performance of a complex system is possible.
- Easy compatibility towards system safety and aid towards the reliability of system.
- Deals well with parallel, redundant or alternative fault paths
- It Provides framework for thorough qualitative and quantitative analyses of system.




NPTEL ONLINE CERTIFICATION COURSE 54

The graphical representation of fault tree analysis help understanding the logic, the starting from top event, convenient selection of the point of interest to find the root cause of the problem, the monitoring and control optimization of the safety performance of a complex system is usually possible under the head of this fault tree analysis, now easy compatibility towards the system and towards the reliability of the system. Now it deals well with the parallel, redundant or alternative fault paths, usually it provides the framework for thorough qualitative and quantitative analysis of the system.

(Refer Slide Time: 37:07)

Advantages of FTA


- Cut set method can be deployed to give enormous insight into various ways unwanted top event may occurs.
- Creating the list of precarious equipment, parts and various events, the results can directly rank the contributors leading to top event.
- Using mathematical modeling, a number of modes could be arrived at; repairable, non-repairable, and stand-by modes.
- There could be consideration of sensitivity cases for modifications to system components, architecture, and component testing intervals.



NPTEL ONLINE CERTIFICATION COURSE 55

The cut set method can be developed to give the enormous insight into various ways unwanted top event may occur, now creating the list of precarious equipment, part or a various event, the result can directly rank the (contribution) contributors leading to the top event, now one may use the mathematical model, a number of modes could be arrived at reparable one, non-repairable one or standby modes. So there could be consideration of sensitivity of cases for modification to system component, architecture and component testing intervals.

(Refer Slide Time: 37:51)



Limitations of FTA

- Requires a separate fault tree for each top event and makes it difficult to analyze complex systems
- Fault trees developed by different individuals are usually different in structure, producing different cut set elements and results
- The same event may appear in different parts of the tree, leading to some initial confusion


The slide features a small video inset in the bottom right corner showing a man in a suit. At the bottom of the slide, there are logos for 'APRIE ONLINE CERTIFICATION COURSE' and a page number '56'.


So we have discussed a lot of the advantage of this fault tree analysis, so let us have a look about the limitation of fault tree analysis, they require a separate fault tree for each top event and makes it difficult to analyze the complex system. Now the fault trees they developed by the different individual, they are usually different because they depend on their own perception, so they usually different in structure, producing different cut set limits and results. So the same event may appear in different parts of the trees leading to some initial confusion, so this is the disadvantage of this fault tree analysis.

(Refer Slide Time: 38:33)

Limitations of FTA

- It is very time consuming analysis and requires large efforts for a complex system.
- Possibility of omissions failure event probability.
- No existences of Partial failure.
- For calculating error probability of top event, probability of all basic events are necessary, which are not always possible to obtain.



 NPTEL ONLINE CERTIFICATION COURSE

Apart from this, it is very time consuming analysis and requires a large efforts for a complex system, sometimes the possibility of omissions may occur then the failure event probability may increase, there is no existence of any kind of partial failure and sometimes it is an integral part or a process, for calculating the error probability of top event, probability of all basic events are necessary which are not always possible to obtain because it may lead to cumbersome process so this is again one of the disadvantage of fault tree analysis.

(Refer Slide Time: 39:13)

Applications of FTA

- Used in the field of Safety Engineering and reliability engineering to determine the probability of a safety accident or a particular system level failure
- To monitor the performance of the system
- To assist in designing a system as per the safety and regulatory concern
- To analyze the effect of medication in the present system.
- Used as a Diagnostic tool to identify and correct causes of the top event
- Use to understand the impact of changing environment or change in duty cycle for same design

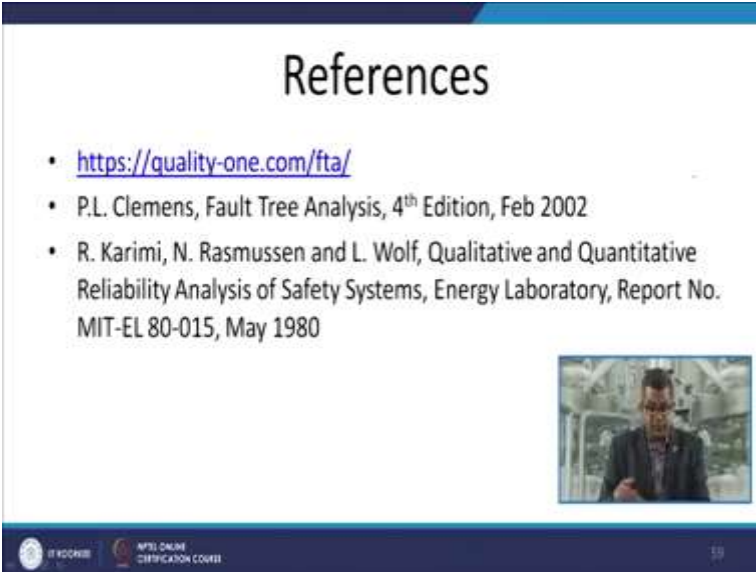


 NPTEL ONLINE CERTIFICATION COURSE

Let us have look about the application of fault tree analysis, they are used in the field of safety Engineering and reliability engineering to determine the probability of safety, accident or a particular system level failure. Now they are used to monitor the performance of the system, they are used to assist in designing a system as per the safety and regulatory concerned, sometimes they are used to analyze the effect of medication in the present system.


They are used as a diagnostic tool to identify and correct causes of the top event, they are used to understand the impact of changing environment or change in the duty cycle of the same design. So in this particular module we have discussed about the various aspects of fault tree analysis, different guidelines, limitations, advantages of the fault tree analysis, how do we constrict this fault tree and we had a small discussion about the application of the fault tree analysis.

(Refer Slide Time: 40:21)



References

- <https://quality-one.com/fta/>
- P.L. Clemens, Fault Tree Analysis, 4th Edition, Feb 2002
- R. Karimi, N. Rasmussen and L. Wolf, Qualitative and Quantitative Reliability Analysis of Safety Systems, Energy Laboratory, Report No. MIT-EL 80-015, May 1980



BY RECORDING MPH ONLINE CERTIFICATION COURSE 59

For further (ref) studies you may have a look of the references listed in this particular slide, thank you very much.