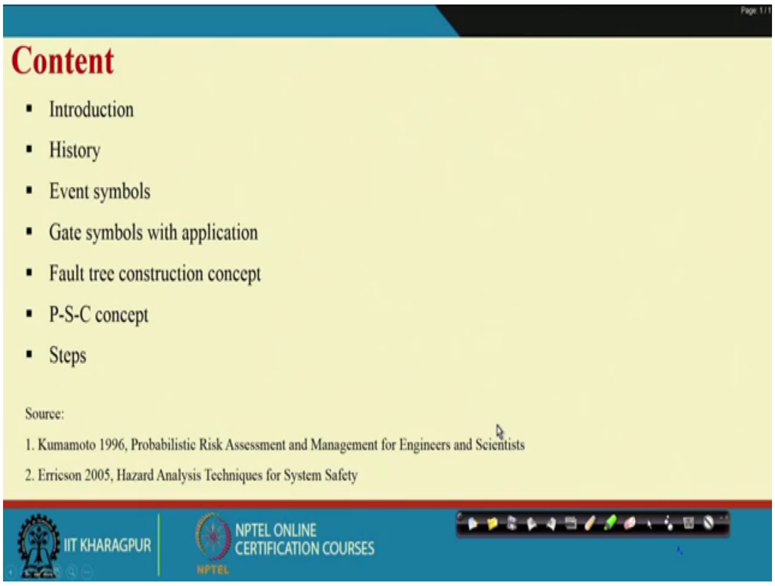
Industrial Safety Engineering
Prof. Jhareswar Maiti
Department of Industrial and Systems Engineering
Indian Institute of Technology, Kharagpur

Lecture - 12
Fault Tree Analysis (FTA) - Construction

(Refer Slide Time: 00:32)



Content

- Introduction
- History
- Event symbols
- Gate symbols with application
- Fault tree construction concept
- P-S-C concept
- Steps

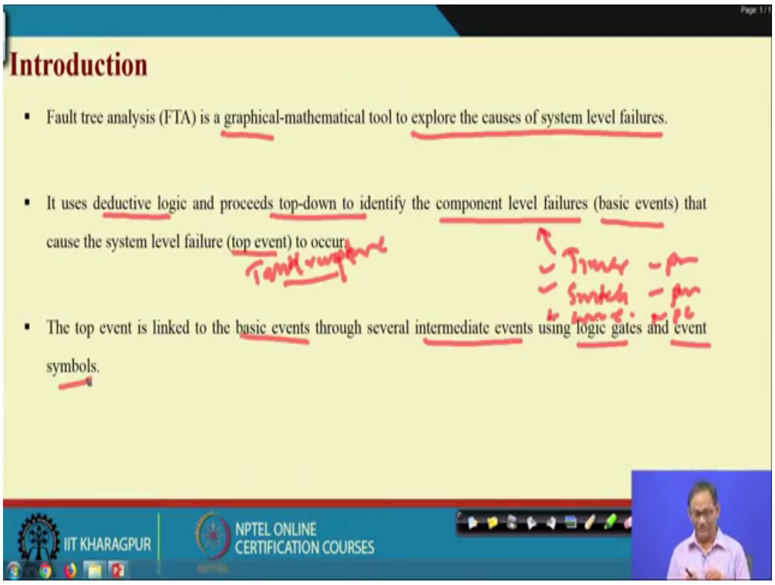
Source:

1. Kumamoto 1996, Probabilistic Risk Assessment and Management for Engineers and Scientists
2. Erricson 2005, Hazard Analysis Techniques for System Safety

IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES

Hello, today we will start Fault Tree Analysis. We will discuss how to construct fault tree in half an hour or 40 minutes of lecture today. The contents we will start with the history. Then the symbols use in fault tree, then the concept of constructing fault tree, and we will describe the P-S-C concept Primary, Secondary and Command concept, and the steps. We will see some example applications. And the source for this particular presentation is Kumamoto book and Ericson 2005; Kumamoto and Henley 1996 and Ericson 2005, 2000, Ericson 2005, Hazard Analysis Techniques for System Safety.

(Refer Slide Time: 01:22)



Introduction

- Fault tree analysis (FTA) is a graphical-mathematical tool to explore the causes of system level failures.
- It uses deductive logic and proceeds top-down to identify the component level failures (basic events) that cause the system level failure (top event) to occur.
- The top event is linked to the basic events through several intermediate events using logic gates and event symbols.

Fault tree analysis is a graphical and mathematical tool. And a purpose is to explore the causes of system level failures. Why it is graphical, because we will be using several symbols in terms of event and gate symbols. And event and gate symbol and all the symbols will be linked; event symbols will be linked with appropriate gate.

And then what happen by this process we will be, we will be getting a graphical tree which ultimately enumerate the causes of system level or top level failure. Why it is mathematical, because the different events from top events to bottom events, including intermediate events, they are linked with some logic symbol like AND gate, OR gate, and similar gate symbols, so which can help us to develop the mathematics of different high level that events. Here the mathematics means the probability of event occurring. It may the top level event, may be the intermediate level event or the basic bottom level event. So, that mean one hand it is a graphical one, another hand it is mathematical one, because these graphical tree structure can be mathematically represented.

So, it uses deductive logic it is basically yy suppose, we start with the system level failure which is known as top event. Then we ask question why that top event has occurred, then immediate answers what you gate the maybe the immediate causes. Then again that immediate event will be answered through another y question and in this manner, you will start from the top to bottom level, so that is why it is a deductive logic. And proceed top-down to identify component level failures.

Now, the component level failures are basic events and system level failure is the top event, we will explain, what is the component level failure. If you recall the system breakdown structure, whatever we have discussed in the earlier lectures, so you have seen that we started with a system. And then subsystems, subsubsystem ultimately we have gone to the component level some time to the part level.

So, in the case of pressure tank, the system is basically to, to store the pressurized gas in the tank. Now, the tank rupture can be the system level failure. Now, if we consider tank rapture is the system level failure, then immediately the question will be why tank rupture then it will be seen that the over pressure is the cause of tank rapture.

So, then what happen you will ask why over pressure, then you will find that pump over run will be the cause. Then you will ask why pump over run, then we will find out the current to that pump is too long. Then in that manner if you was why current to pump too long, you may find out that the timer fail or the operator fail, so many things will be coming. So, so that mean the top level will be may be the tank rupture, component level ultimately you will come to the component level the timer, the then the switch, then the wire, power supply, pump, pressure gauge. So, all component level failure are responsible for the top level failure.

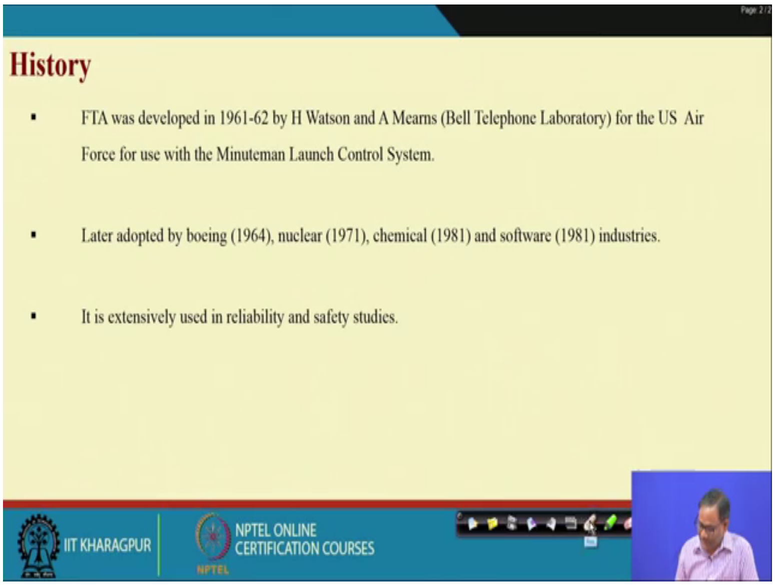
The top event is linked to the basic events. So, when you come to the component level failure, and component level failure is also known as basic event, it is something where you have enough data to know the probability of the failure. So, the stop event is linked to the I mean tank rupture will be linked to this bottom component level failure with reference to pressure tank system with several intermediate events and logic gates and event symbols.

So, for the time being what you have learned here, you have learned that fault tree analysis is a graphical and mathematical tool. Why graphical, it will use several symbols and why mathematical the symbols are event symbols are linked with gate, gate symbol, gate symbol has specific mathematical structure particularly the Boolean algebra related things. And which helps you in quantifying the probability of the top event failure given the bottom, bottom level failure.

Now, top event is basically system level failure, whereas the bottom event is the component level failure. So, top event when you ask why top event has occurred. So, you will basically dig down asking why, why question to the bottom level or the component level. Now, the component level is that level where what happened the failure probability is known or it is, it can be quantified that is why the component level failures are known as basic events.

And top level failure is known as top event and top event is connected to basic events through different intermediate events that is why the different event symbols are used. And the connection between the event symbols are through logic gates that is why different logic gates are used. It is a very a well known and very good technique. And it gives useful causes, and identify the path leading from the bottom level or component level failure to top level failure. It is extensively used in safety study reliability studies.

(Refer Slide Time: 08:04)



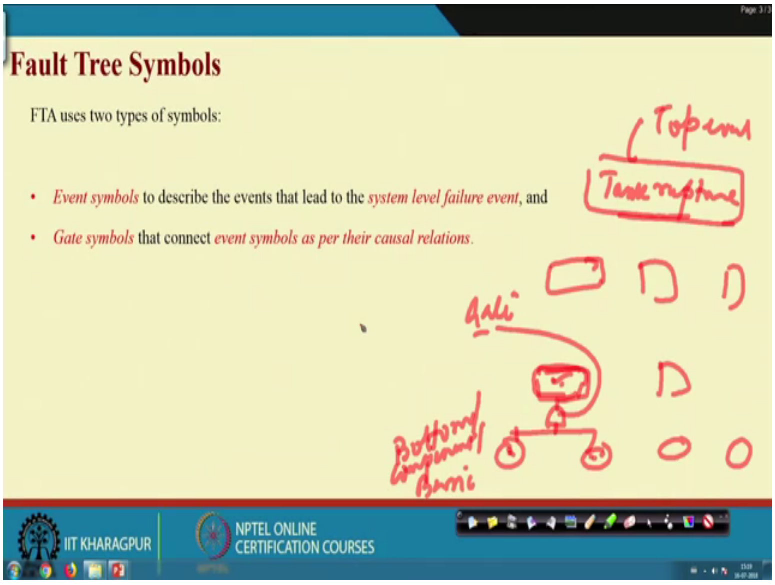
History

- FTA was developed in 1961-62 by H Watson and A Mearns (Bell Telephone Laboratory) for the US Air Force for use with the Minuteman Launch Control System.
- Later adopted by boeing (1964), nuclear (1971), chemical (1981) and software (1981) industries.
- It is extensively used in reliability and safety studies.

So, if we see the history of fault tree, then you see that it was developed in 1961 and 62 by Watson and Mearns in the Bell Laboratory of US Air Force. And it is related to this particular system that is Minuteman Launch Control System. So, later adopted by Boeing, nuclear, chemical, software, so different almost all industries they have accepted this and it is a very good technique, and extensively used in reliability, and safety studies.

In fact, we will see that fault tree is one of the most important techniques for this engineering systems, safety or industrial system safety, industrial safety engineering course. So, we will be dealing it with great depth. And we will spend some time for this fault tree.

(Refer Slide Time: 09:08)



Fault Tree Symbols

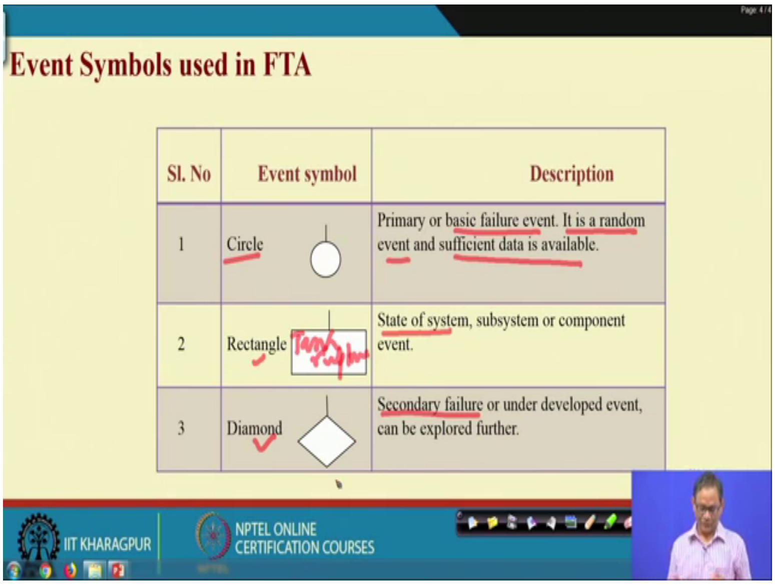
FTA uses two types of symbols:

- *Event symbols* to describe the events that lead to the *system level failure event*, and
- *Gate symbols* that connect *event symbols as per their causal relations.*

So, I this time you, you ok, you have heard that event symbol and gate symbols. I say the event symbol to describe the events that lead to the system level failure and gate symbol are that connect the event symbol as per their causal relations ok. Let me repeat once more. Event symbols described the events that lead to system level failure, system level failure is top event. And with reference to pressure tank, we have seen that tank rupture is the system level failure that is basically top event. And then there will be many intermediate event, so what happened we will put this explanation with box. There will be many intermediate box and finally what will happen there will be many, many other symbols will be coming we will see later on.

So, what I mean to say that this is our top event and these are the basic event or bottom event or component level event, bottom component event or basic event. So, what we are saying that gate symbols are used that connect event symbol to the higher level symbols with causal relation, these are the event, this is event symbol event symbol. Now, suppose I want to link this symbol with this two you can create a gate here like this. So, this is and gate, we will see later on ok. So, gate this is a gate symbol, this is a gate. And now it is obvious that, if I want to see that what why this event has occurred, then definitely these two events are responsible and the relationship is get depicted by this gate we will discuss in detail.

(Refer Slide Time: 11:20)



Event Symbols used in FTA

Sl. No	Event symbol	Description
1	Circle ○	Primary or basic failure event. It is a random event and sufficient data is available.
2	Rectangle □ Tank rupture	State of system, subsystem or component event.
3	Diamond ◇	Secondary failure or under developed event, can be explored further.

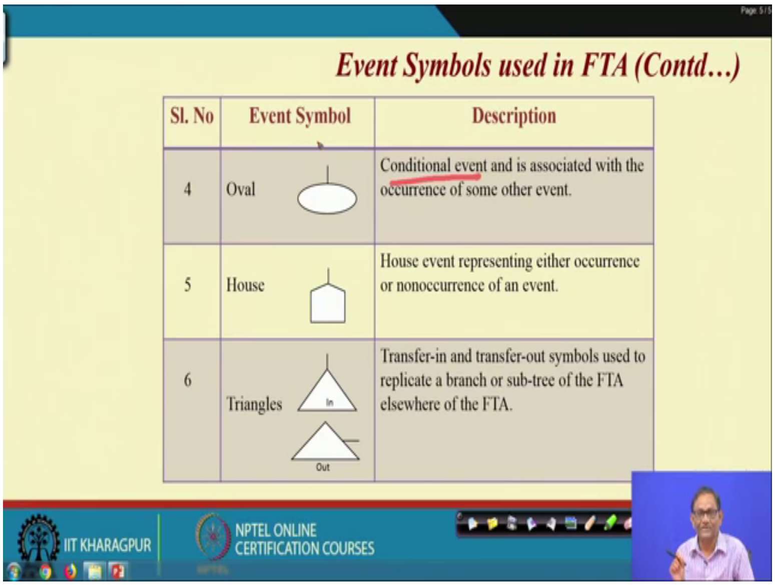
So, let us see some of the symbols then we will go for their application. One is circle. What is circle? Circle determine the primary or basic failure event. What is basic failure event? Basic failure is the component level failure. So, when we put circle we understand that it is a random event and sufficient data is available; that means we know the probability of that event occurrence.

Then another symbol we use rectangle. It basically talks about the state of the system sub system or component event. For example, with reference to pressure tank system, the state of the system is tank rupture or the subsystem may be the pumping system or maybe the that is the storage system like the pressure tank itself store. So, pump overrun or component level event maybe the timer failure may be the operator failure or something like this all such state that whether the tank is in normal condition or in failure condition whether the pumping system is failure condition or in normal of working condition. Whether the component are failure or not all those state of the system will be represented by rectangle.

So, if I say the top event occur tank rupture, then mean the system level failure has occurred this is the state of the system, so you will write tank rupture within a within the rectangle that tank rupture ok. So, then diamond, diamond is a secondary failure under developed event can be explored further. What happened, when you link the top event like the tank rupture to, to the bottom events up to the component level.

So, what happen there will be several intermediate events, but you may find out that some of the intermediate events are such that you are they are under developed means, you are not able to have the full information, and you require to explore it further. And at present when you are developing the fault tree that time your knowledge base is not that sufficient to explore it, then this is this will be put under diamond symbol. Then we say this is the secondary failure. It cannot be explored, now but it required to be explored further, but if it is to it you can explore it further, so you explore it dig down to the bottom level, so do not put diamond.

(Refer Slide Time: 14:16)



Event Symbols used in FTA (Contd...)

Sl. No	Event Symbol	Description
4	Oval	Conditional event and is associated with the occurrence of some other event.
5	House	House event representing either occurrence or nonoccurrence of an event.
6	Triangles	Transfer-in and transfer-out symbols used to replicate a branch or sub-tree of the FTA elsewhere of the FTA.

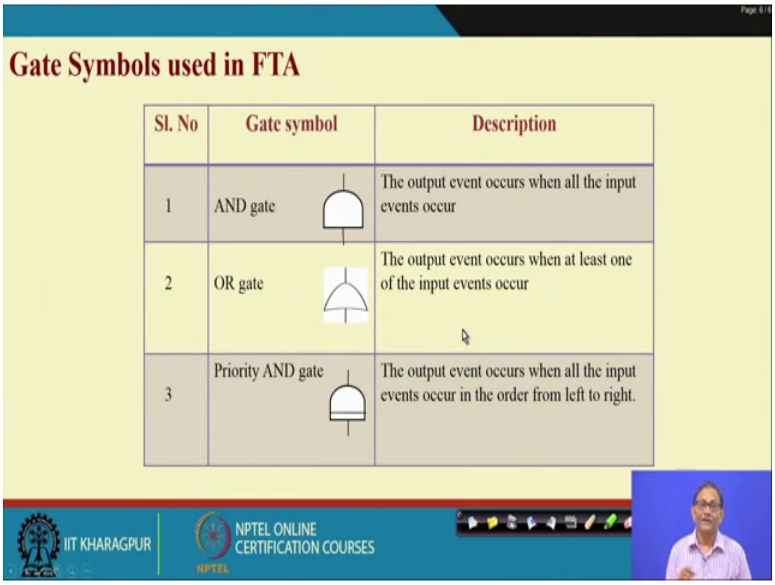
Then what happen oval; oval symbol is basically conditional event. So, if something happened with the in reference to these, then only these top event will occur. For example, that alarm sounds like in the pressure tank system, you will see in that there is a alarm, alarm sound under what pressure condition. And if alarm sounds at the time operator need to check the pressure gauge, and then he should remove the, the contact ok.

So, now what happened suppose alarm sound and operator taken wrong action then what happen top event will occur over pressure condition will occur and finally, rupture will take place. So, here operator pushes wrong switch is the conditional event. So, such things will be put under oval. What is house? House represent either occurrence and non-occurrence of an event. There may be a situation, when the both occurrence and non-occurrence as consequence has causal implication to the system. So, then what happened under such situation you will use this it is occurrence and as well as non-occurrence such consequent not only occurrence non-occurrence. So, when you go for bigger fault tree may be house event and other things will come.

Now, the triangles in and out two triangles are use that is transfer in and transfer out symbol used to replicate a branch of a sub tree of a fault tree elsewhere of the fault tree. So, when you develop system level fault tree, you may find out that the tree will be very, very big. And may it may so happen when you come to the subsystem levels. So, there may be some of the sub subsystem which are basically applicable in other part of the tree, so that is why, what happen the if you develop a fault tree for a particular sub subsystem, and then you should not require to develop it further in the other part. You just put in and out symbol, out symbol in the first case another place you right in and that will basically reduce the size of the tree qualitative that tree the size of the tree.

So, these two symbols, these two symbols very special symbol, so they will be or commonly small tree it is not used, but for the big tree particularly for big tree this is used. And this is a symbol which basically you may not get all the times such kind of examples, but sometimes it may happen that whether it is occurred or not occurred that has some implications ok. So, that mean how many there are 6 event symbols these are just to represent the represents basically what is happening there, when you develop the fault tree.

(Refer Slide Time: 17:41)



Gate Symbols used in FTA

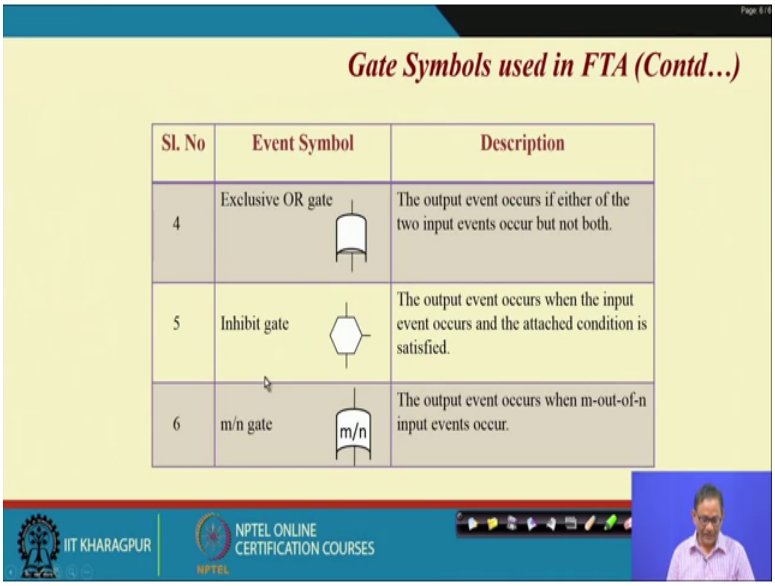
Sl. No	Gate symbol	Description
1	AND gate	The output event occurs when all the input events occur
2	OR gate	The output event occurs when at least one of the input events occur
3	Priority AND gate	The output event occurs when all the input events occur in the order from left to right.

IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

Then there will be several gate symbols. Gate symbols are used in between event symbols to logically link the parent and child that events parent event to the children events ok.

(Refer Slide Time: 18:08)



Gate Symbols used in FTA (Contd…)

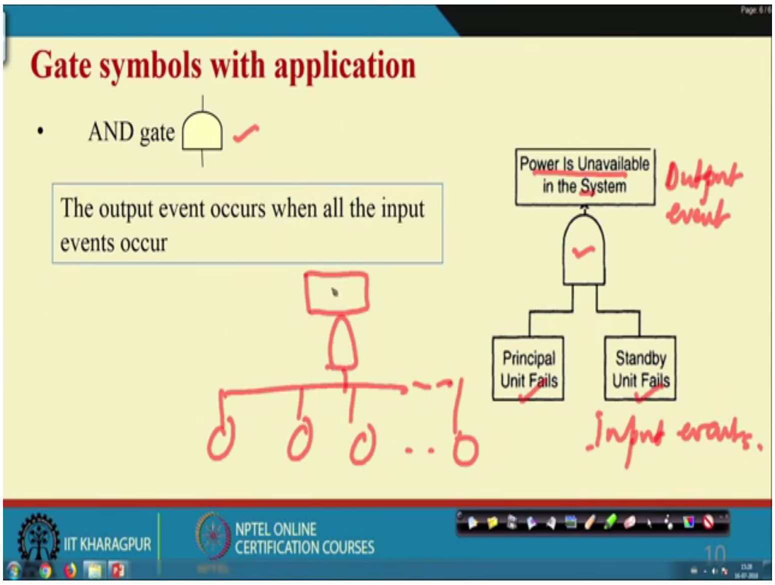
Sl. No	Event Symbol	Description
4	Exclusive OR gate	The output event occurs if either of the two input events occur but not both.
5	Inhibit gate	The output event occurs when the input event occurs and the attached condition is satisfied.
6	m/n gate	The output event occurs when m-out-of-n input events occur.

IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES

So, there will be AND gate. There will be AND gate, OR gate, priority AND gate. And then Exclusive OR gate inhibit gate this boating gate, so 6 gates I am showing here. So, I will explain all those gate with example ok.

(Refer Slide Time: 18:16)



Gate symbols with application

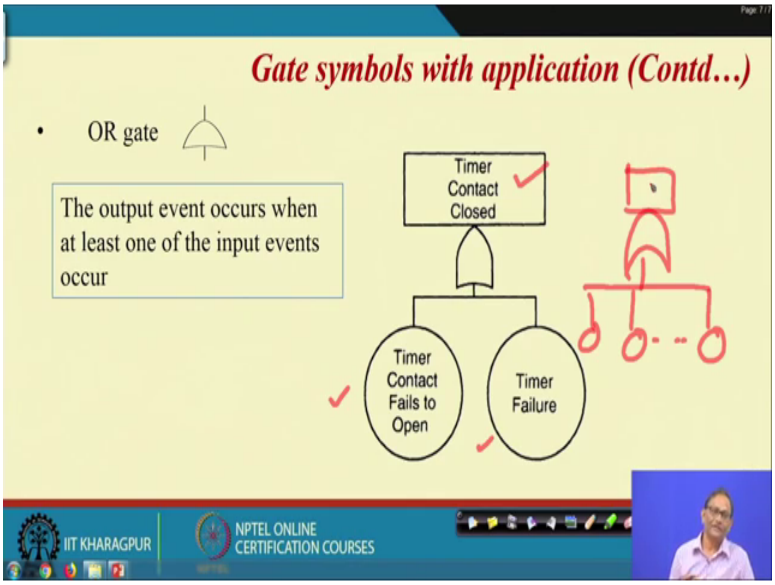
- AND gate

The output event occurs when all the input events occur

Now, first is AND gate. What does it mean the output event occurs when all the input event occurs this is a AND gate. What is the output event power is unavailable in the system what are the input event principal unit fails standby unit fails, you think of two situation where the principal unit is there standby generator is also there. So, now, there is no power, no electricity in the system when principal unit fail so there may that the standby unit will work automatically with the help of a switch controller.

Now, let us a situation is there principal unit fails and then also standby units fails. So, much before repair, replacement or repairment of the principal unit, what will happen power is unavailable. So, I mean both principal you need as well as standby unit should fail then only this situation will occur. So, here this is my output event and these two are input event input event need not be there will be only two inputs. So, there can be many more inputs here. Suppose, there are k inputs with AND gate and one output obviously, so in that case this output will occur only when all the k inputs occur. If all the k inputs does not occur output will not occur that is what is AND gate.

(Refer Slide Time: 20:16)



Gate symbols with application (Contd…)

- OR gate

The output event occurs when at least one of the input events occur

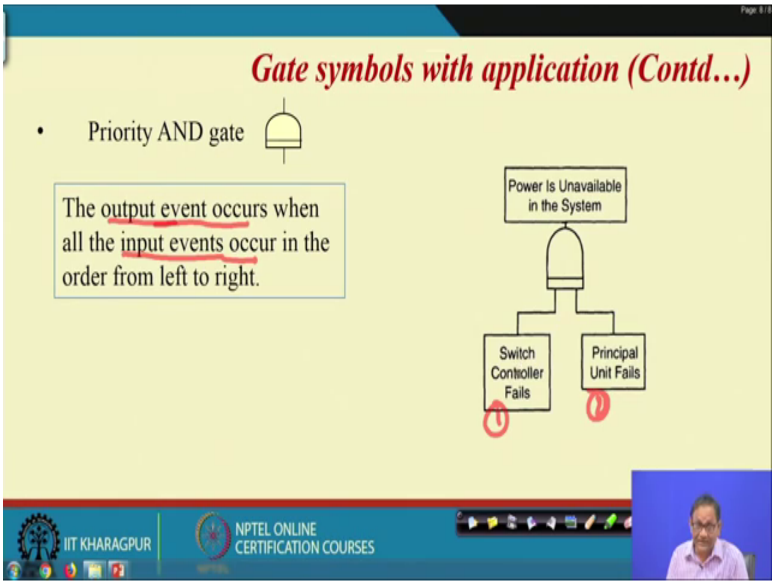
Timer Contact Closed
Timer Contact Fails to Open
Timer Failure
IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES

Then OR gate; OR gate with it is basically again in terms OR gate there will be output event, there will be input events ok. Now, you just see the pressure tank example what we have already explained. So, what happen timer contact closed, so when timer contact will be closed, timer contact fails to open and timer failure.

So, over pressure condition occurs when timers contact closed more than the set time. The setting will be done by timer. Now, if there is a timer failure, then what will happen this one this contact will be closed, if it we think that it is first closed and it is running, then and then otherwise what will happen the timer contact itself is fails to open. So, this is failure mode of timer contact and timer also is fail it is as failed, it is not working. If either of the two are happen, then timer contact will be closed.

So, this kind of situation that output event occurs when at least one of the input events occur. So, need not be again here there will be only one input, there will be many inputs. What does it mean any one of the input event if occurs output event will occur, so that is your OR gate.

(Refer Slide Time: 22:17)



Gate symbols with application (Contd...)

- Priority AND gate

The output event occurs when all the input events occur in the order from left to right.

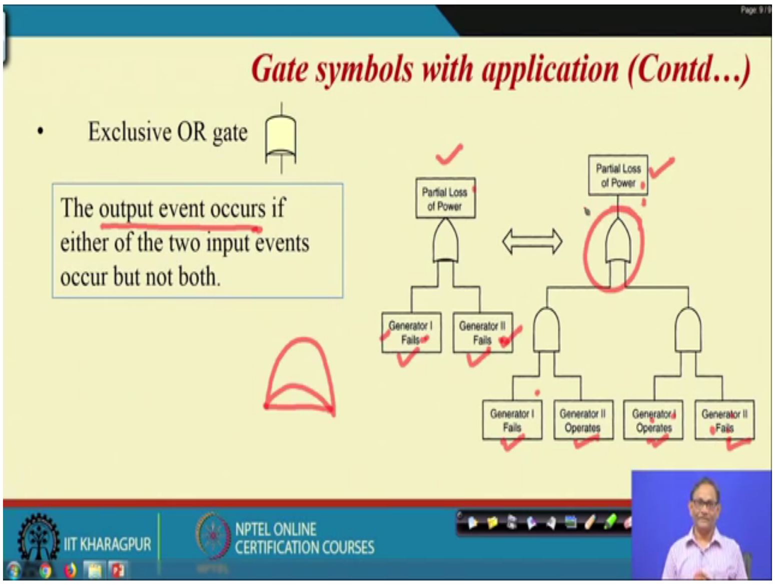
Power Is Unavailable in the System
Switch Controller Fails
Principal Unit Fails
IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES

Then priority AND gate; what is priority AND gate, priority AND gate is the output event occurs, when all the input event occurs in the order from left to right or right to left. Actually there is a sequence of occurrence that is then you use priority AND gate. For example there is a standby suppose that is main system fails, then the standby system will be automatically operational through a switch controller, switch controller connect the standby units.

So, what will happen, when principal unit fails, then switch controller job starts; it basically makes the standby unit operational, but unfortunately what happens switch controller first fails and maybe after that principal unit fails, and it was not notice the switch controller fails not repair. So, when principal control unit fail, so switch controller as already fail it will not make the standby unit operation.

So, here the standby unit will not work and as a result the power will be unavailable provided first switch controller followed by principal unit fails. So, that is what is the order; that is the first then the second but both the things must happen, it should happen in this order. What will happen, if switch controller is successful principal unit fails there automatically standby unit will start working. So, power will be available in that case ok. This is known as priority AND gate.

(Refer Slide Time: 24:21)



Gate symbols with application (Contd...)

- Exclusive OR gate

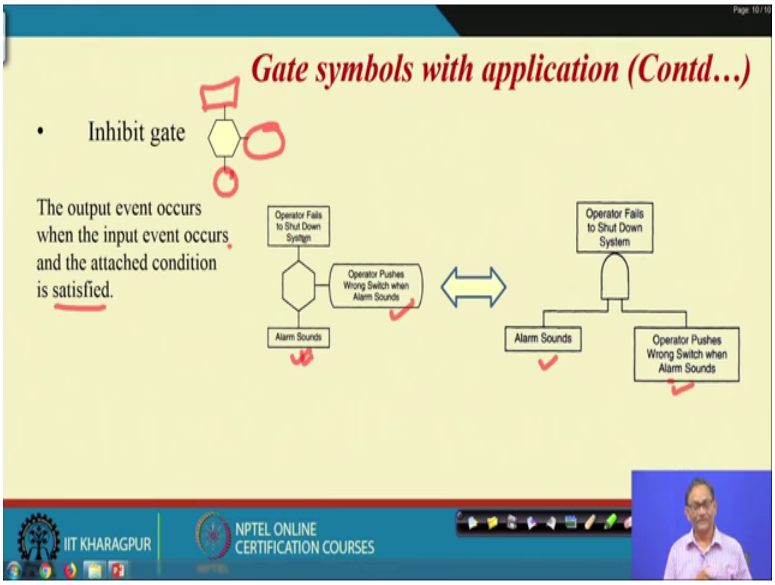
The output event occurs if either of the two input events occur but not both.

Then another gate, it is Exclusive OR gate. What is Exclusive OR gate exclusive output event occurs, output event occurs, if either of the two input event occurs, but not both. So, you have generator I and generator II. So, we are talking about my output event is partial loss of power.

So, let the both generator I and generator II should operate to have the full loss of power at full power. So, if both the fail a generator fails that will be full loss of power. Now, partial loss of power is a situation when any one of the generator we will work you can extend to more inputs, but for the two inhibits level. So, this is the case suppose output event occurs, if either of the two event not both if both will occur suppose these fail and these fail there will be no power. These fail this does not fail or this fail, second one fail first one does not fail, then it is partial loss. And as a result we are using this symbol that exclusive or symbol is like this. So, we are using this symbol.

Its equivalent AND and OR gates you see; partial loss of power is possible, when generator I fails, generator II operates; or generator I operates, generator II fails. If this condition occur; that means, here no supply of power here generator one operates and generator two fails. Then here what will be this condition simultaneously occur partial loss of power will be there or this condition occur partial loss for power will be there as a result you are putting the OR gate.

(Refer Slide Time: 26:33)



Gate symbols with application (Contd…)

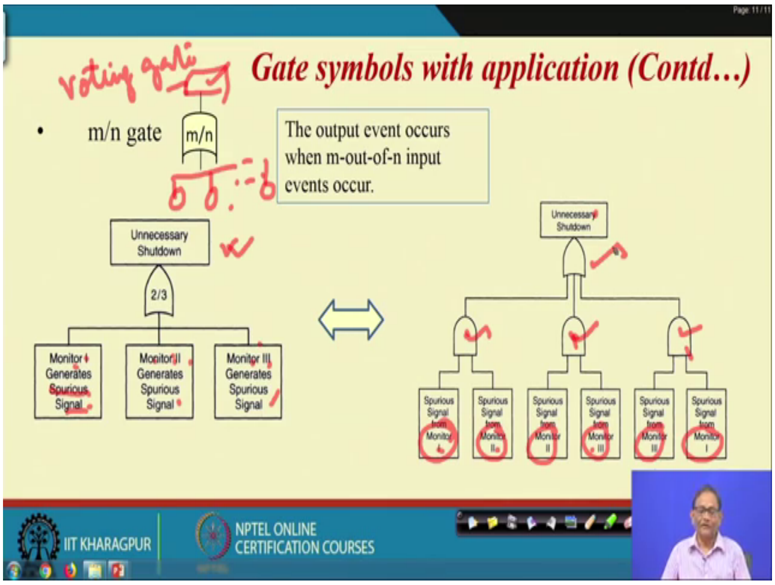
- Inhibit gate

The output event occurs when the input event occurs and the attached condition is satisfied.

Operator Fails to Shut Down System
Operator Pushes Wrong Switch when Alarm Sounds
Alarm Sounds
Operator Fails to Shut Down System
Alarm Sounds
Operator Pushes Wrong Switch when Alarm Sounds
IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES

Now, inhibit gate. What is inhibit gate the output event occurs when the input event occurs and the attach condition is satisfied. This is the case, so this is input, there will be output, this is the attach condition exactly it is written here. As I explained this one that. Alarm sounds operator pushes wrong switch, when alarm sounds operator fails to shutdown the system. So, this is basically this is the situation inhibited immediate its equivalent is this alarm sound operator pushes wrong switch when alarm sounds. So, it is a AND gate. But this is a conditional one, so that is why this inhibit gate is 0. If this happens, then this will be and ultimately operator fails to shutdown this. Now, this is what is inhibit gate.

(Refer Slide Time: 27:34)



Gate symbols with application (Contd...)

- m/n gate

The output event occurs when m-out-of-n input events occur.

Page 11/11
voting gate
m/n
Unnecessary Shutdown
2/3
Monitor I Generates Spurious Signal
Monitor II Generates Spurious Signal
Monitor III Generates Spurious Signal
Unnecessary Shutdown
Spurious Signal from Monitor I
Spurious Signal from Monitor II
Spurious Signal from Monitor II
Spurious Signal from Monitor III
Spurious Signal from Monitor III
Spurious Signal from Monitor I
IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES

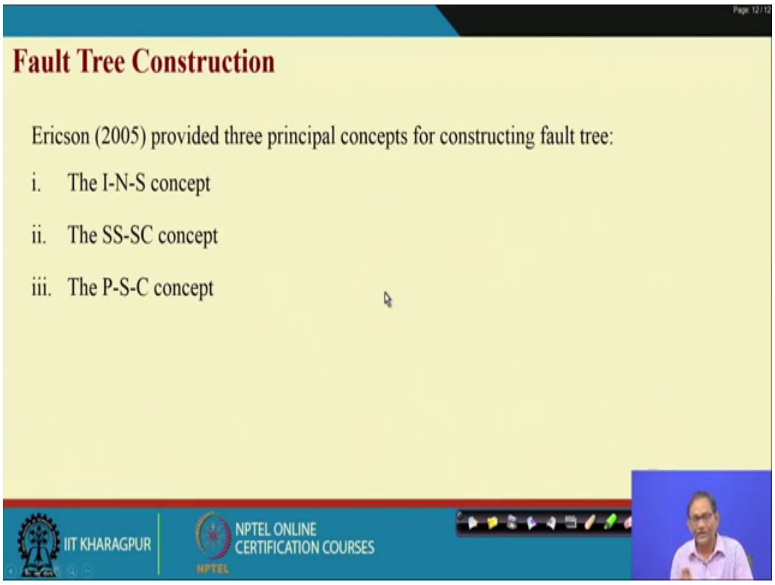
Then last gate symbol important symbol is m by n gate which is also known as voting gate. So, it is basically output we will occur when m of n input events occur it need not be that all requires. You require at least m input events out of n small n input events should occur then top event will occur.

Example is, example is here suppose you have automatic system and then for shutdown. There are three monitors and you say that if monitor at least two of the three monitors signal shut down, you go for shutdown. But monitor is monitor it can be it, it can also fail or it can generate spurious signal also. If monitor I generates spurious signal and monitor II generates spurious signal, and monitor III also generates spurious signals; obviously, there is a shutdown. But as you say that, if two of the three, if two give some signal, you will, you will make shutdown.

So, if monitor I, monitor II or monitor I monitor III, or monitor II monitor III, if this combination any of the combination shows you that we are signal for shutting down so, shutdown will take place. Here top event is unnecessary shutdown. You have three monitors, if two of the three monitors give signal for shutdown, you will shutdown, so but these are spurious signal no problem, but this is what is the concept.

So, its equivalent representation is this one a at least what happened monitor I monitor II, or monitor II monitor III, or monitor III monitor I gives spurious signal that means, these conditions simultaneously this must be satisfy that is why. And these two must be satisfy that is why and these two must be satisfy that is AND gate AND gate; but this will occur, if this condition, this condition or this condition satisfy that is why OR gate so, this is what is voting gate. So, we are explained you the symbol AND gate I can say event symbol AND gate symbol.

(Refer Slide Time: 30:14)



Fault Tree Construction

Ericson (2005) provided three principal concepts for constructing fault tree:

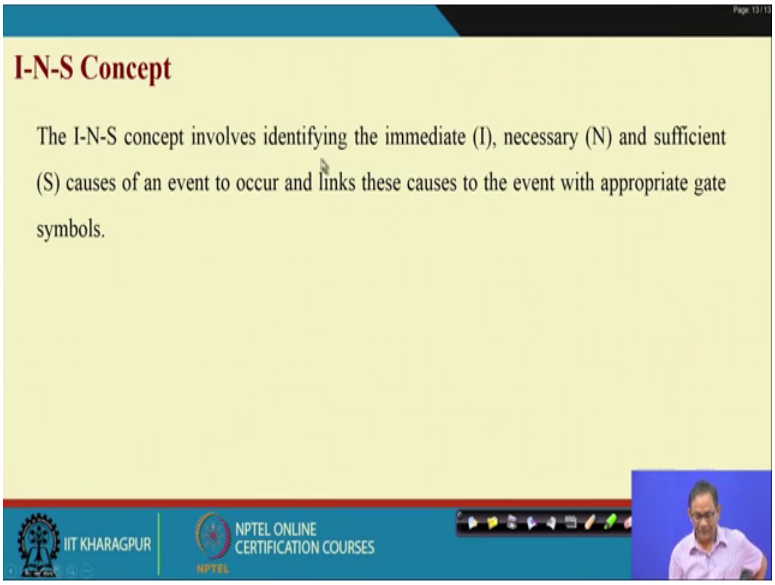
i. The I-N-S concept

ii. The SS-SC concept

iii. The P-S-C concept

Then what happen using those symbols you have to develop or construct the fault tree. So, Ericson has given three concepts actually talk that there will be I-N-S, I-N-S concept SS-SC concept and P-S-C concept. We will discuss what are those I concept first two I will just give you the definition from Ericson book and last one we will discuss at length.

(Refer Slide Time: 30:47)

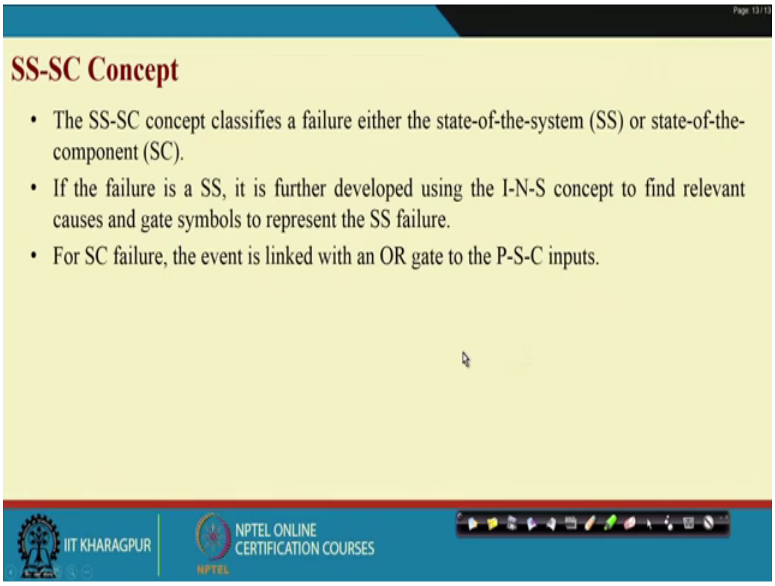


I-N-S Concept

The I-N-S concept involves identifying the immediate (I), necessary (N) and sufficient (S) causes of an event to occur and links these causes to the event with appropriate gate symbols.

I-N-S concept involves identifying immediate necessary and sufficient causes, immediate necessary and sufficient causes of an event to occur and link these causes to the top event with appropriate gate symbol. Suppose you are talking about a system level failure. So, immediately what you require you, you will just find out what are the possible causes so and those causes must be necessary and sufficient to have the top event occurs ok.

(Refer Slide Time: 31:20)

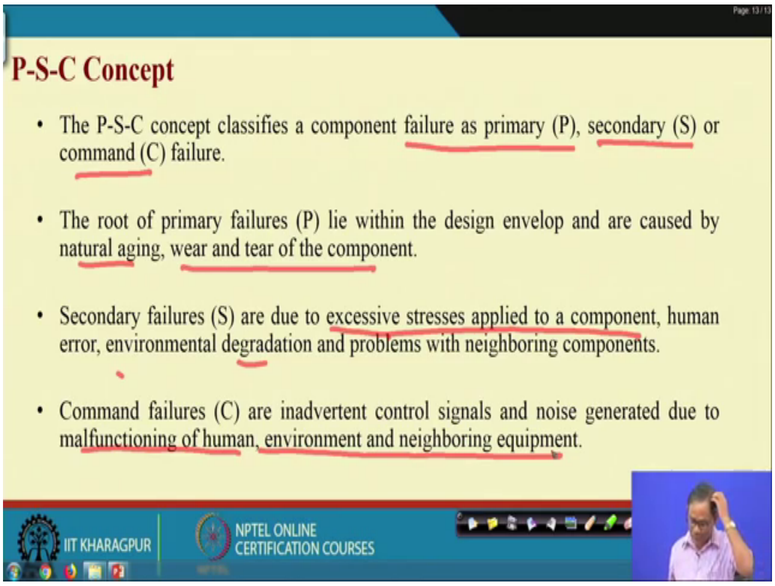


SS-SC Concept

- The SS-SC concept classifies a failure either the state-of-the-system (SS) or state-of-the-component (SC).
- If the failure is a SS, it is further developed using the I-N-S concept to find relevant causes and gate symbols to represent the SS failure.
- For SC failure, the event is linked with an OR gate to the P-S-C inputs.

So, and then second one is SS-SC concept SS-SC concept classifies a failure either state of the system it is a system level failure or component level failure. If the failure is system level, then you use I-N-S concept to further broken down. And if it is a system component level failure, then you use P-S-C, P-S-C, concept and P-S-C concept will be discussed later.

(Refer Slide Time: 31:54)



P-S-C Concept

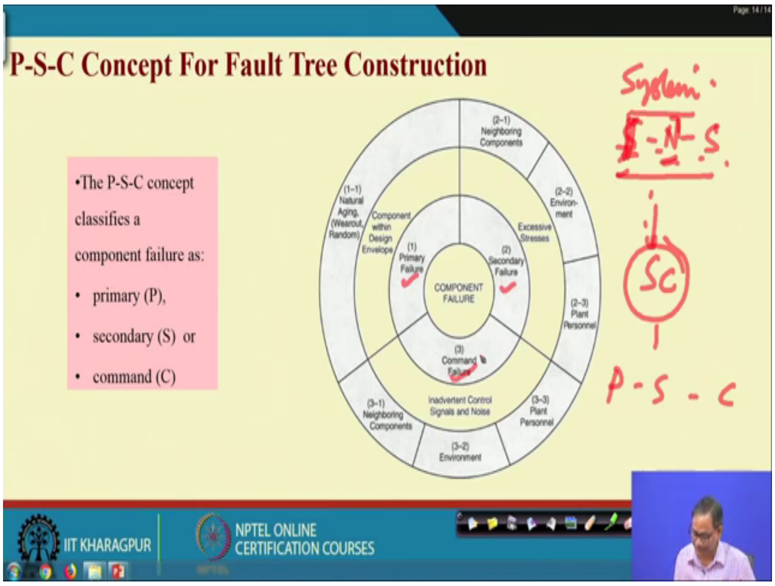
- The P-S-C concept classifies a component failure as primary (P), secondary (S) or command (C) failure.
- The root of primary failures (P) lie within the design envelop and are caused by natural aging, wear and tear of the component.
- Secondary failures (S) are due to excessive stresses applied to a component, human error, environmental degradation and problems with neighboring components.
- Command failures (C) are inadvertent control signals and noise generated due to malfunctioning of human, environment and neighboring equipment.

So, then what is P-S-C concept? P-S-C concept P stands for primary, S stands for secondary, C stands for command failure ok. So, the route of the primary failure lie within the design envelop and are caused by natural ageing, wear and tear. So, primary failure see P-S-C concept is use at the component level. Primary failure means the component itself fails because of it is within design and build up, because of wear and tear.

Secondary failure here with reference to this component failure due to excessive stresses applied to the component human error environment other things. So, it is not the not, because of the design problem it is because of the that mean over use of the things means excessive stress on it. Suppose bulb can run continuously for 20 hours so, if you use it more than 20 hour, suppose 30 hours, there is chance that bulb will fail. So, it is not, because of the wear and tear is, because of excessive load on it.

What are the command failure anything, suppose any component that will work given certain command from neighbouring components ok, or someone give some component. For example, a bulb will glow only, when you put on the switch and the wire connected to the bulb switch and power supply that should work. Suppose, thus you have not put on the switch bulb will not glow. The wire is broken it will not carry currents. So, these type of things; that means, proper signal not comes to the component and that is the situation when we say command failure has taken place. So, command failure are inadvertent control signals and noise generated due to malfunction of human environment and neighbouring components ok.

(Refer Slide Time: 34:11)



P-S-C Concept For Fault Tree Construction

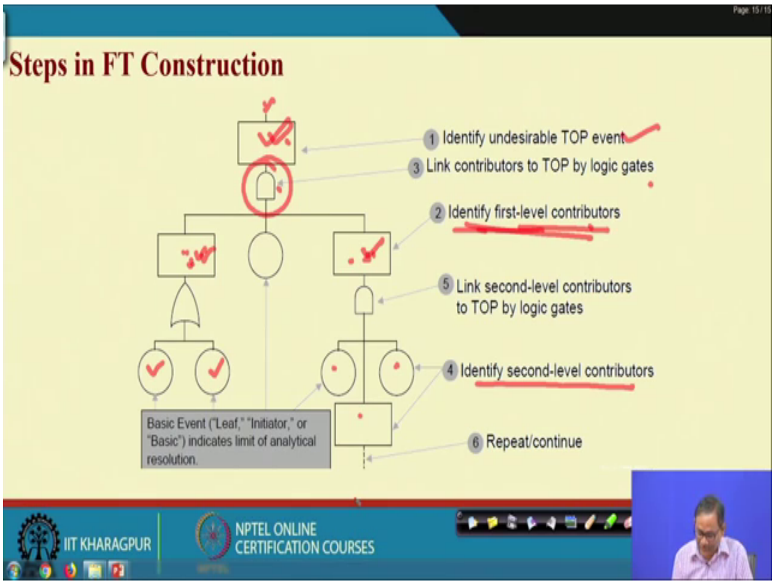
- The P-S-C concept classifies a component failure as:
  - primary (P),
  - secondary (S) or
  - command (C)

So, what happened then we say we say that for fault tree construction, suppose when you start with system level failure, so use S your immediate I-N-S concept immediate for initially your top level failure you will find out the immediate causes write down. And see that they are necessary, and they are sufficient to have this.

So, then what happened first level breakup is over. Then you will you may find out the immediate causes related to a subsystem. Then again you may use I-N-S concept. And in this manner what happen, you will come to the component, level when you come to the component level that time you use P-S-C concept to understand why that component fails.

So, I-N-S and then ultimately S-C finally we lead to S-C component, then in the component P-S-C. So system level to system component level and then at the component level use P-S-C and as I told you P-S-C primary failure, secondary failure, command failure. And we have given you I have given you already that what is primary, secondary all those things.

(Refer Slide Time: 35:42)



Steps in FT Construction

1 Identify undesirable TOP event

3 Link contributors to TOP by logic gates

2 Identify first-level contributors

5 Link second-level contributors to TOP by logic gates

4 Identify second-level contributors

6 Repeat/continue

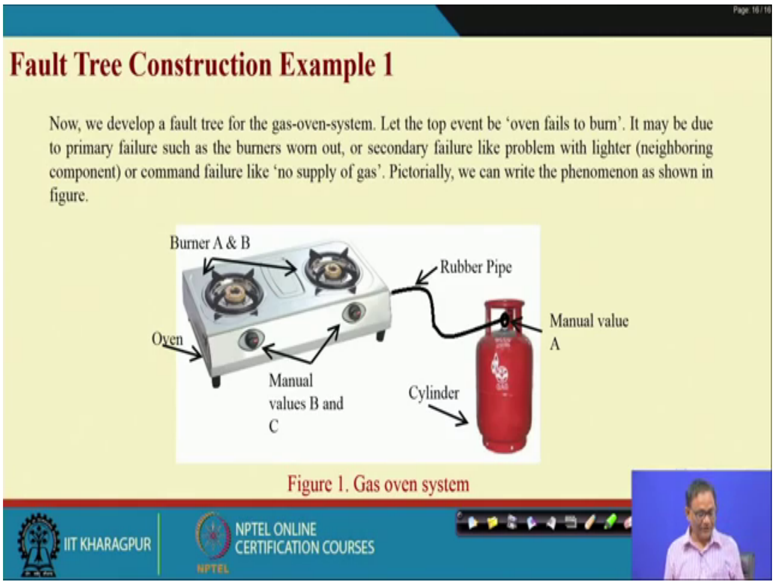
Basic Event ("Leaf," "Initiator," or "Basic") indicates limit of analytical resolution.

So, your this is the system level failure, then what happen these two you see first level contributor they are the immediate causes, then immediate causes are linked with the top or system level failure by some gate. Now, what happened here as it is immediate causes; it may be a subsystem level 1 or maybe a component level 1. Then what you required to do, you required to find out the bottom level again, so find out this when you are putting circles, this is the component level failure; circle means component level. So, will have you are not putting circle it is not component.

So, what are the then steps; identify undesirable top event, link contributor to top by logic gates that is a step 3, step 3, step 2 is identify first level contributor once you got these come here. Then you know the proper logic put AND gate, OR gate or whatever other gate is applicable.

Then what will happen, immediately the first level contributor again, you just see after 3, then 4 identify the second level contributor, this is the first level contributor. Then you find out the second level contributor these, these and this. Out of these three second level contributor two are basic events, because they are component level failure, but this one is not basic event, because they may be subsystem level failure, it required to further broken down and you repeat this process, so that is the steps. I will quickly show you one example and then we will finish this lecture.

(Refer Slide Time: 37:22)



Fault Tree Construction Example 1

Now, we develop a fault tree for the gas-oven-system. Let the top event be 'oven fails to burn'. It may be due to primary failure such as the burners worn out, or secondary failure like problem with lighter (neighboring component) or command failure like 'no supply of gas'. Pictorially, we can write the phenomenon as shown in figure.

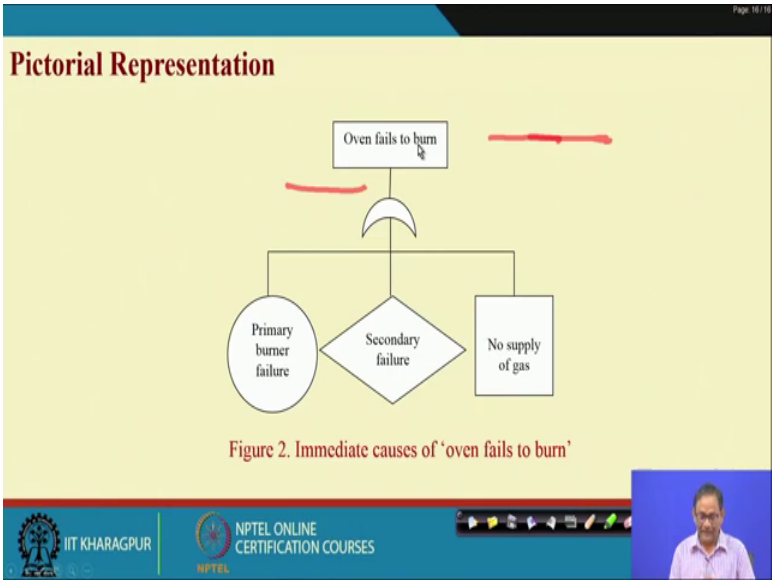
Figure 1. Gas oven system

This is what everybody knows this; this is the kitchen gas oven. Now, what happen suppose we want to develop a fault tree, what is our top failure the top event is oven fails to burn, it may be due to primary failure such as the burner maybe problematic one, secondary failure may be the lighter is neighbouring component not working or command failure like no supply of gas.

So, the oven fails to burn that mean the burner itself may fails. So, this burner system level failure. So, burner may fail, then your I am giving in terms of P-S-C concept here the burner may fail, so then it is the primary then or what will happen the burner is working. But the in you are using lighter, lighter is not working, but you are not able to understand that one may be some reasons it is not working.

So, or what will happen it gas is not coming. So, when gas is not coming that is a subsystem level, because supply of gas is a issue. So, if I consider system and subsystem here, the this oven is one system, another one is supply of gas is another system; so that burner is fails to burn, so immediately what happened we got the primary that the component of the burners. So, we are using P-S-C concept here; so burner fails means burner itself fails or burner is not getting the supply of gas. So, why burner is not getting the supply of gas means this is the subsystem level fail. So, why burner is not getting the gas, then you may find out that there will command failure. Command failure why, because that may be the component are not able to supply gas ok.

(Refer Slide Time: 39:21)



Pictorial Representation

Figure 2. Immediate causes of 'oven fails to burn'

So, then using this P-S-C concept here what we will finally found out, oven fails to burn, primary burner failure, secondary failure may not be known and no supply of gas this is the command failure. So, no supply of gas is the command failure.

So here when we talk, when you put like this rectangle symbol these are all command case basically command failures. And they may be intermediate failure and finally they may be component level failure. So, when you come down to component level failure put circle.

(Refer Slide Time: 39:58)

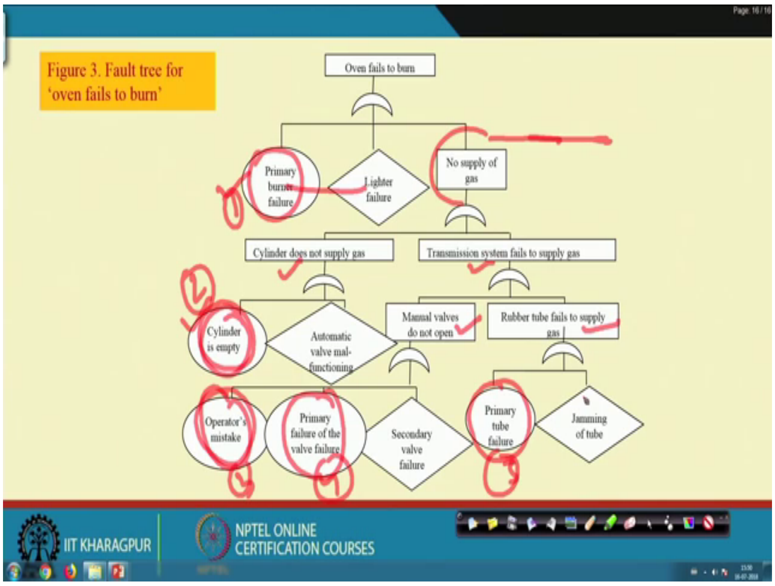


Figure 3. Fault tree for 'oven fails to burn'

Oven fails to burn
Primary burner failure
Lighter failure
No supply of gas
Cylinder does not supply gas
Transmission system fails to supply gas
Cylinder is empty
Automatic valve mal-functioning
Manual valves do not open
Rubber tube fails to supply gas
Operator's mistake
Primary failure of the valve failure
Secondary valve failure
Primary tube failure
Jamming of tube
1
2
3
4
5
IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES

So, then what happened finally no supply of gas, no supply of gas cylinder does not supply gas transmission system fails to supply gas. Then why cylinder not supply, cylinder is a component; cylinder is empty automatic valve malfunctioning, you are putting diamond, because you do not know why it is malfunctioning at that point in time.

Then what happened and it and this one transmission system fails to supply gas, manual bulbs do not open, rubber tube fails to supply gas; so rubber tube failure is a primary these are all, these are all circles, these are all circles ok. So, here also primary failure; so that mean this is one circle, this is another circle, this is another circle. So 1, 2 then 3 then 4 then 5 so, these are the 5 circle in 5 component level failure.

Jamming of tube, then why jamming of tube you have not explore it further, so that is why you are putting under secondary failure. Secondary failure means something which to be explored further, in this manner the fault tree will be constructed ok.

(Refer Slide Time: 41:18)

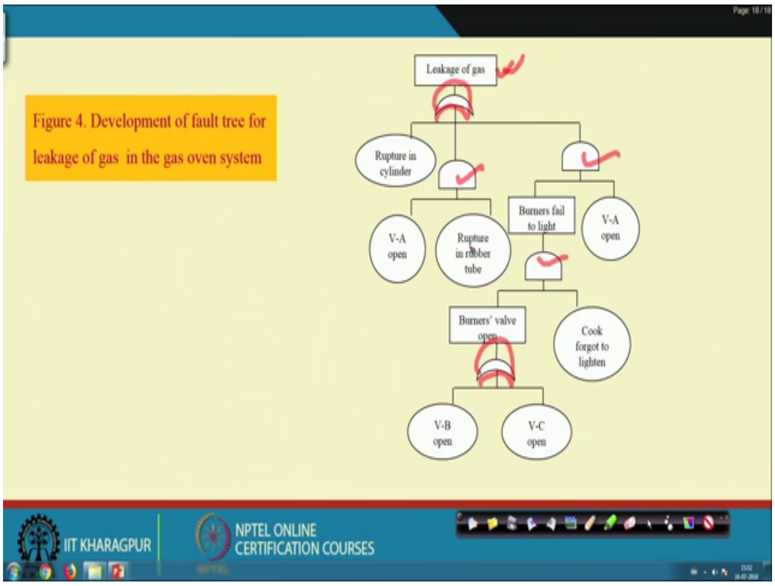


Figure 4. Development of fault tree for leakage of gas in the gas oven system

For the same thing you develop the case the leakage of gas. What happen if you see here, we are using only all these are basically worse these are, these are this symbols are OR gate, but just from drawing point of view there is some these are all OR gates, these are all OR gates ok.

(Refer Slide Time: 41:36)

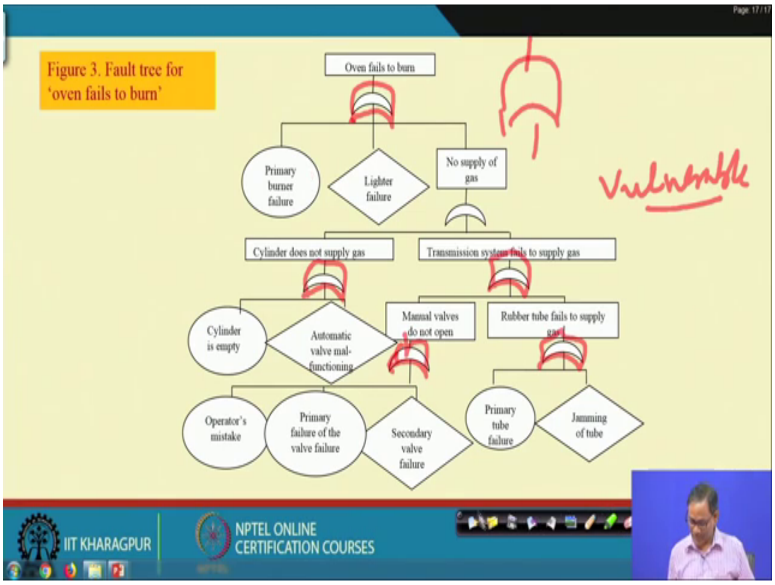


Figure 3. Fault tree for 'oven fails to burn'

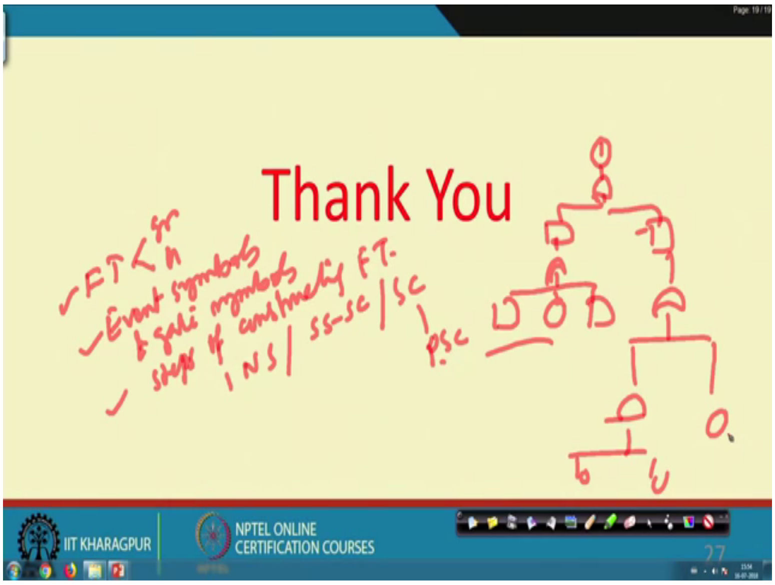
Page 17 / 17
Oven fails to burn
Primary burner failure
Lighter failure
No supply of gas
Cylinder does not supply gas
Transmission system fails to supply gas
Cylinder is empty
Automatic valve mal-functioning
Manual valves do not open
Rubber tube fails to supply gas
Operator's mistake
Primary failure of the valve failure
Secondary valve failure
Primary tube failure
Jamming of tube
Vulnerable
IIT KHARAGPUR
NPTEL ONLINE CERTIFICATION COURSES

So, the more the OR gate that mean what happen anything any basic event occurs, it will lead to the top event. So, it is a vulnerable system, vulnerable system top event may happen occur ok. So, I will show you another one, leakage of gas here for the same kitchen system oven system leakage of gas, so this is my OR gate cylinder rapture, then there is AND gate, AND gate, AND gate, AND gate another OR gate.

So, when AND gate is there; that means, some kind of standby so your system is better in terms of, because our ultimate in safety studies, top event is the undesired event. So, there are more AND gate means it, it basically prohibit to the undesired event to occur more and this is basically reduce the probably, this is the region is the probability of event.

So, by constructing fault tree of a top event, you can find out that what is the system level vulnerability ok. When there are more AND gates as we are talking about the undesired event it is better system configuration, if more OR gates or all OR gates, then it is a problematic one ok. So what I have shown, then we have basically seen that we have basically seen that the gate symbol.

(Refer Slide Time: 43:36)



Thank You

So, let me tell you what I say, we say that fault tree; it is a graphical and mathematical tool, graphical and mathematical. It uses event symbols, gate symbols ok. Then what happened we have given all example, we have seen that the meaning of event symbol, gate symbol with examples. Then the steps of construction, steps of constructing fault tree, constructing fault tree, what are the steps, so you may go for I-N-S concept and then SS-SC concept at the S C level, you will use P-S-C concept ok.

So, in general, this is the process, but P-S-C concept or you may not use P-S-C concept, you can develop if you have you are expert, so you can develop. But please keep in mind initially you start with identifying top event, then first level contributors, then second level contributors and you have to use appropriate logic in between ok. So, logic will be there; as I told you, if you and with using AND and OR gate, you can construct fault tree. Other gates are required to use also you may find out example or cases in your system, where other gates can be used.

So, but my first level suggestion is that you use AND and OR gate only. And it this definitely gives you the full idea, but it will be the there will be may be the longer one, but your knowledge will be clear. And the second thing is that once you become expert you use other gates and other symbols.

Thank you very much.