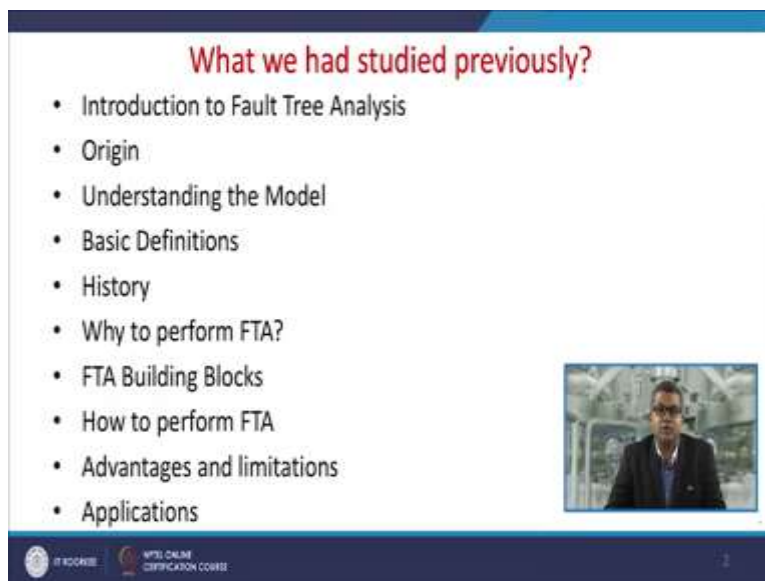


**Chemical Process Safety**  
**Professor Shishir Sinha**  
**Department of Chemical Engineering**  
**Indian Institute of Technology, Roorkee**  
**Lecture 44**

**Cause Consequence Analysis and Layer of Protection Analysis**

Welcome to this module related to the Cause Consequence Analysis and Layer of Protection Analysis sometimes abbreviated as LOPA. Now just we would like to have a brief outlook that what we have studied previously because this particular module is linked with the previous module.

(Refer Slide Time: 01:03)



**What we had studied previously?**

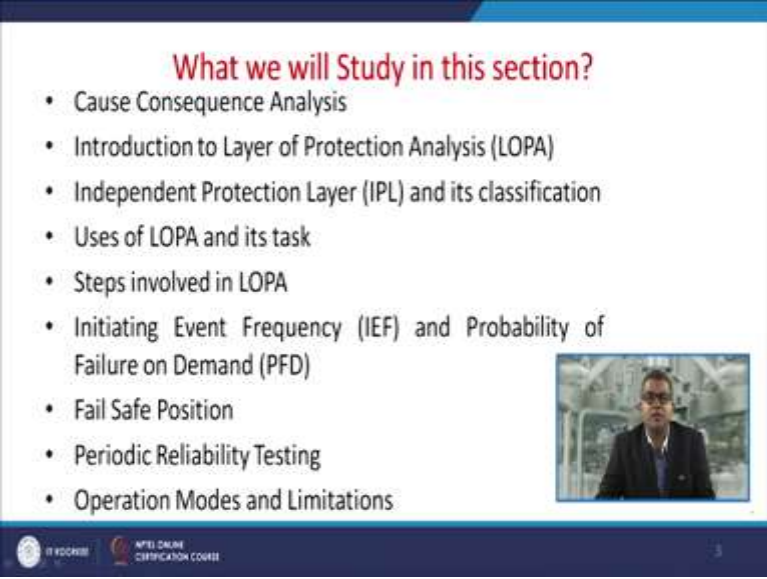
- Introduction to Fault Tree Analysis
- Origin
- Understanding the Model
- Basic Definitions
- History
- Why to perform FTA?
- FTA Building Blocks
- How to perform FTA
- Advantages and limitations
- Applications

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 WPIE ONLINE CERTIFICATION COURSE.

So we had an production about the fault tree analysis and during this analysis we have gone through the origin we had a very good understanding of the model of this fault tree analysis. We were well acquainted with the basic definition and history of this Fault Tree Analysis then we had a brief discussion about that why there is a need to perform fault tree analysis.

And apart from this we had discussion about the various building blocks of fault tree analysis and the basic methodology through which we can perform the fault tree analysis. Apart from this we had a discussion about the advantage and disadvantage or sometimes referred as a limitation of this fault tree analysis. Now in this particular module we are going to study about the cause consequence analysis.

(Refer Slide Time: 01:39)



**What we will Study in this section?**

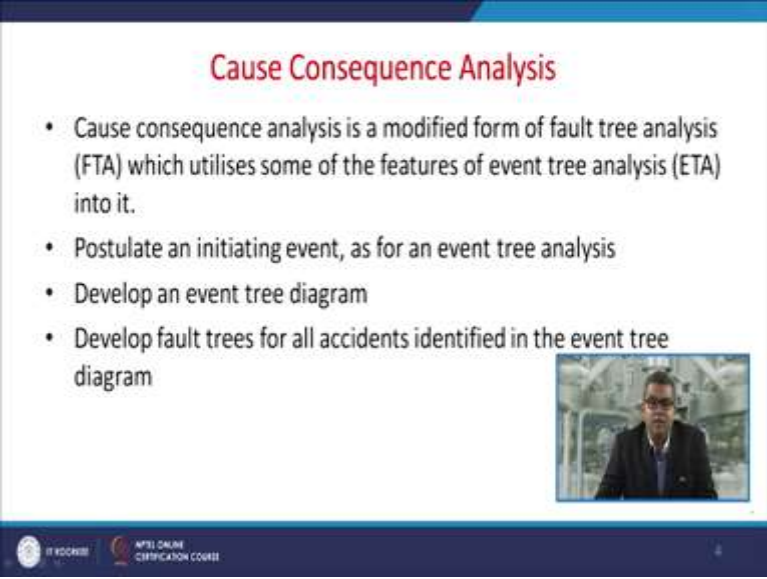
- Cause Consequence Analysis
- Introduction to Layer of Protection Analysis (LOPA)
- Independent Protection Layer (IPL) and its classification
- Uses of LOPA and its task
- Steps involved in LOPA
- Initiating Event Frequency (IEF) and Probability of Failure on Demand (PFD)
- Fail Safe Position
- Periodic Reliability Testing
- Operation Modes and Limitations

The slide includes a small video inset of a presenter in the bottom right corner. The footer contains the logos for 'BYJU'S' and 'NPTEL ONLINE CERTIFICATION COURSE'.

We will have an introduction about the layer of protection analysis LOPA which is very significant nowadays. We will have a discussion about the Independent Protection Layer sometimes referred as IPL and its classification. We will have a discussion about the use of LOPA that is a layer of protection analysis then discussion about the steps involved in LOPA.


We will have a discussion about the initiating event frequency because it is very crucial while we are discussing ETA that is Event Tree Analysis or a Fault Tree Analysis. Then we will have brief outlook about the Probability of the Failure On Demand PFD, Fail Safe Position will be discussed in the later part of this module and the periodic reliability testing apart from this we will have the discussion about the operation modes and limitations.



(Refer Slide Time: 02:34)



**Cause Consequence Analysis**

- Cause consequence analysis is a modified form of fault tree analysis (FTA) which utilises some of the features of event tree analysis (ETA) into it.
- Postulate an initiating event, as for an event tree analysis
- Develop an event tree diagram
- Develop fault trees for all accidents identified in the event tree diagram



So let us start with the Cause Consequence Analysis. Now this cause consequence analysis is usually a modified form of fault tree analysis now which utilizes some of the features of event tree analysis so you can say that this is an argumentation of the salient feature of both event tree analysis and the fault tree analysis.


Now this postulate an initiating event as far as the event tree analysis is concerned and develop an event tree diagram and this simultaneously this develops the fault tree for all accident identified in the event tree diagram. So you can say that this is the modified version of this ETA and fault tree analysis.

(Refer Slide Time: 03:28)

### Cause Consequence Analysis

- The process can be reversed in that a top event is defined and the fault tree then developed. Then, for each safety function in the fault tree an event tree is developed.
- Some special symbols such as **hexagonal symbol for denoting consequence** and **crescent sign for denoting branch point** is added in this method.

Rest of the part is already discussed in ETA and FTA.




NTPL ONLINE CERTIFICATION COURSE

Now the process this can be reversed in that a top event is defined the fault tree and then developed therefore the for each safety function in the fault tree and event tree is developed. There are some special symbols you will use like hexagonal symbol for denoting the consequences and the crescent sign for denoting the branch point which is which will be used in this particular methodology. Now rest of the part we have already discussed in event tree analysis and the fault tree analysis.

(Refer Slide Time: 04:04)

### Introduction

- While doing HAZOP analysis, various possible process deviation and their probable consequences of potential accidents is assessed. After determining ETA and FTA, possible safeguards are identified to mitigate the risk.
- A list of all supporting safeguards need to be created to understand whether it provides complete or partial mitigation to the process risk.
- Some of the listed safeguards may depend over other safeguards and some may be independent from one another.

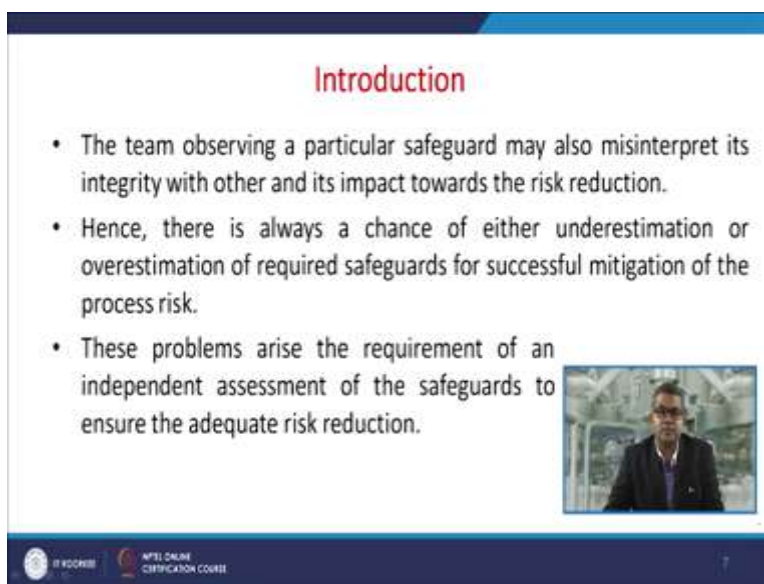


NTPL ONLINE CERTIFICATION COURSE

So let us have an introduction about this things, so while performing any kind of HAZOP analysis various possible process deviation and their probable consequences of potential accident is assessed. Now based on your previous knowledge this assessment is carried out. Now after determining this event tree analysis and a fault tree analysis the possible safeguards are identified to mitigate the risk because ultimately the mitigation of the risk is our prime motto.

So a list of all supporting safeguards need to be created to understand whether it provides complete or partial mitigation to the process risk. So in case if provide the complete then it is of very good use and if provides the partial mitigation then again we need to go for to take the further steps. So some of the listed safeguards may depend over other safeguards and some may be independent from one another.

(Refer Slide Time: 05:09)



The slide is titled "Introduction" in red text. It contains three bullet points:

- The team observing a particular safeguard may also misinterpret its integrity with other and its impact towards the risk reduction.
- Hence, there is always a chance of either underestimation or overestimation of required safeguards for successful mitigation of the process risk.
- These problems arise the requirement of an independent assessment of the safeguards to ensure the adequate risk reduction.

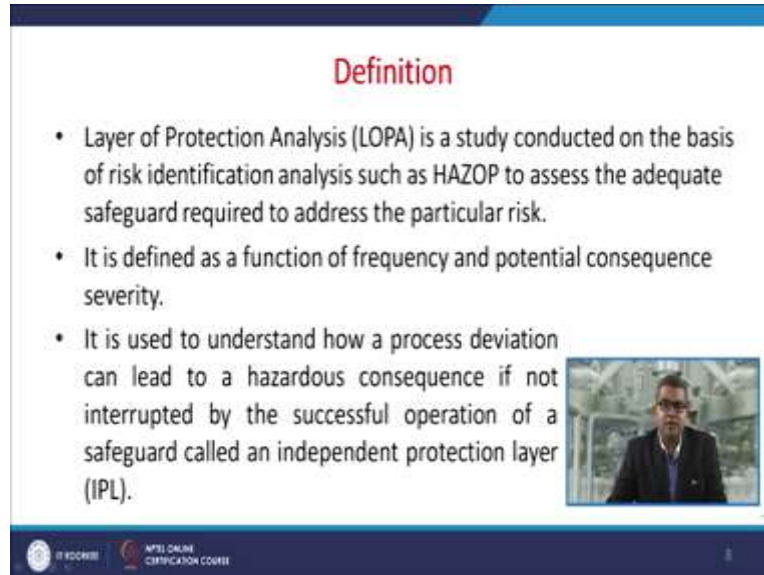
There is a small video inset on the right side of the slide showing a man in a suit. At the bottom of the slide, there are logos for "BYJU'S" and "NPTEL ONLINE CERTIFICATION COURSE".

Now the team which who is carrying out all this aspect the team observing a particular safeguard may also miss interpret its integrity with other because sometimes the system may say that this is a foreign body so they may not be the system may not be in a position to interpret properly that particular safeguard tool. So that is why it may miss interpret its integrity and its impact towards the risk reduction.

So there is always a chance of either underestimation or overestimation of required safeguard for the successful mitigation of the process risk. So both the conditions either underestimation or overestimation is always undesirable. So you must have a proper optimization so these problems

may arise the requirement of an independent assessment of the safeguard to ensure the adequate risk reduction.

(Refer Slide Time: 06:11)




### Definition

- Layer of Protection Analysis (LOPA) is a study conducted on the basis of risk identification analysis such as HAZOP to assess the adequate safeguard required to address the particular risk.
- It is defined as a function of frequency and potential consequence severity.
- It is used to understand how a process deviation can lead to a hazardous consequence if not interrupted by the successful operation of a safeguard called an independent protection layer (IPL).

So let us have a some of the definition related to this particular aspect. The layer protection analysis LOPA is study conducted on the basis of risk identification analysis such as HAZOP to assess the adequate safeguard required to address the particular risk. So nowadays it is an upcoming field so therefore because it gives you an optimized level of safeguard tools so it is defined as frequency and the potential consequence severity so it is used to understand how a process deviation can laid to a hazardous consequence and if not interpret by the successful operation of a safeguard and sometimes this particular aspect. Is referred as independent protection layer or IPL.

(Refer Slide Time: 07:08)

- It is to be noted that these countermeasures (IPL) as per the name suggests, must be independent to each other to be effective.
- This is a semi-quantitative approach which generally applied to the system and their protective safeguards already in place.
- The term semi-quantitative represents that LOPA utilizes both qualitative (characterized by methods such as HAZOP and What-if analysis) as well as quantitative (characterized by methods such as ETA and FTA) approach to decide the adequacy of existing or proposed system.




NPTEL ONLINE CERTIFICATION COURSE

So it is to be noted that these countermeasures like IPL as per the name suggest must be independent to each other to be very effective. Now this is semi-quantitative approach which generally applied to the system and their protective safeguard which is already in place. So the term semi-quantitative this represent that LOPA utilize this both qualitative that is characterized by method such as HAZOP and What-if analysis or as well as the quantitative usually they are characterized by the method such as Event Tree Analysis and Fault Tree Analysis so the quantitative approach to decide the adequacy of existing or proposed system.

(Refer Slide Time: 08:02)

- LOPA **does not** suggests which additional safeguards are required, but it assures that the potential risk to the process system is successfully mitigated to an acceptable limit.
- LOPA is limited to a single cause-consequence pair as a scenario.



NPTEL ONLINE CERTIFICATION COURSE

Now remember the LOPA does not suggest which additional safeguards are required but it assures that the potential risk to the process system is successfully mitigated to an acceptable limit. Now this LOPA is limited to a single cause consequence pair as a scenario.

(Refer Slide Time: 08:26)



**Independent Protection Layer (IPL)**

- IPLs are intrinsic safety system as an independent series of elements related to the process design and maintenance.

Features of IPL

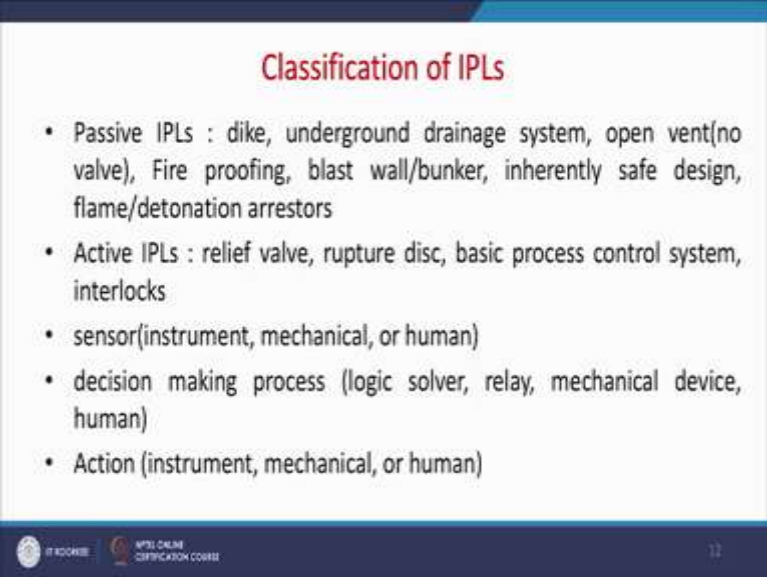
- Criteria : Specificity, Independence, Dependability, Auditability
- 3D : Detect, Decide, Deflect
- 3E : Fast Enough, Strong Enough, Big Enough
- Big I : Independent
- All IPLs are safeguards, but not all safeguards are IPLs.

IT RECORDS NPTI ONLINE CERTIFICATION COURSE 11

So let us have a look about the independent protection layer that is referred as IPL now this independent protection layer IPL is they are intrinsic safety system as an independent series of element those are related to the process design and maintenance. So let us have a look about the salient features of this independent protection layer. First thing is that criteria now this is having the very specific aspect it is Independence, Dependability and Auditability.

Now there are three D's which we need to remember Detect, Decide, and Deflect. Similarly we are having three E's that is referred as Fats Enough, Strong Enough, and Big Enough so Enough is there. Then there is one big I that is Independent so all IPL's they are safeguards but not all safeguards are IPL so this thing must be remembered in all the aspects. Now let us have a look about the classification of IPL's.

(Refer Slide Time: 09:58)



The slide is titled "Classification of IPLs" in red text. It contains a bulleted list of safety measures categorized into passive and active IPLs. The footer includes the IIT Kharagpur logo, the text "IIT KHARAGPUR", and "NPTEL ONLINE CERTIFICATION COURSE". The slide number "12" is in the bottom right corner.

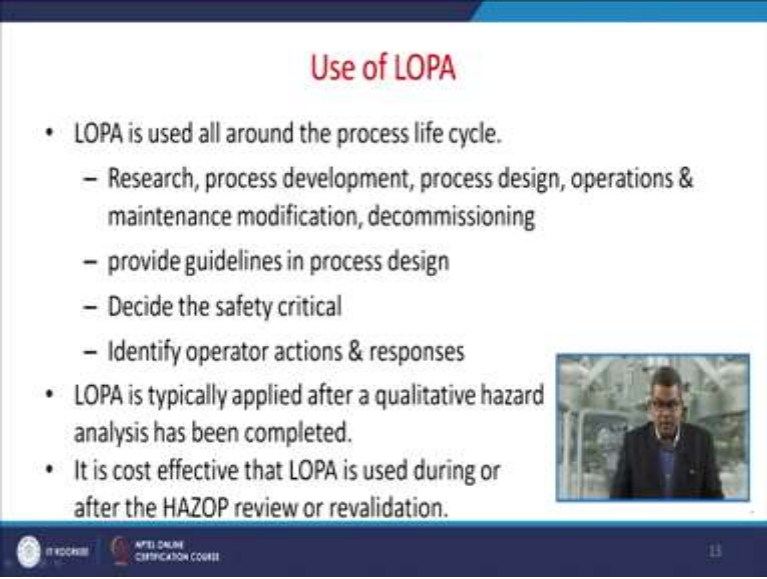
### Classification of IPLs

- Passive IPLs : dike, underground drainage system, open vent(no valve), Fire proofing, blast wall/bunker, inherently safe design, flame/detonation arrestors
- Active IPLs : relief valve, rupture disc, basic process control system, interlocks
- sensor(instrument, mechanical, or human)
- decision making process (logic solver, relay, mechanical device, human)
- Action (instrument, mechanical, or human)

IIT KHARAGPUR NPTEL ONLINE CERTIFICATION COURSE 12


Basically there are two ways to classify it one is on the basis of the passive and active approach so the passive IPL dike, underground drainage system, open vent then then there is no valve etc, fire proofing, blast wall or bunker, inherently safe design, flame or detonation arrestors etc and then active IPL they are having relief valves, rupture disc, basic process control systems, safety valves etc then interlocks. There may are certain sensors like instruments, mechanical may maybe or human then decision making process with the help of logics solver, relay, sometimes human etc then various actions like instruments maybe attributed to the mechanical or a human aspects etc.



(Refer Slide Time: 10:47)



### Use of LOPA

- LOPA is used all around the process life cycle.
  - Research, process development, process design, operations & maintenance modification, decommissioning
  - provide guidelines in process design
  - Decide the safety critical
  - Identify operator actions & responses
- LOPA is typically applied after a qualitative hazard analysis has been completed.
- It is cost effective that LOPA is used during or after the HAZOP review or revalidation.





13


Now let us discuss about the use of LOPA so LOPA is used all around the process lifecycle, this includes the research, the process development because sometime research may lead for the process development then after process development the process designed place so process design then operator and maintenance modification schemes and then decommissioning. So it covers the entire process lifecycle.

This provide guidelines in process design it also decides the safety the critical aspect of various safety measures it identifies the operator action and responses. So LOPA is typically applied after it qualitative hazard analysis has been completed. Now it is a cost effective that LOPA is used during or after the HAZOP review or revalidation. So you can cut down the cost the entire designing or process lifecycle cost.

(Refer Slide Time: 11:56)

### Task of LOPA

- 3Q's
  - Q: How safe is safe enough?
  - Q: How many protection layers are needed?
  - Q: How much risk reduction should each layer provide?
- Providing rational, semi-quantitative, risk-based answers
- Reducing emotionalism
- Providing clarity and consistency
- Documenting the basis of the decision




NPTEL ONLINE CERTIFICATION COURSE 14

There are various tasks associated with the LOPA one foremost task is 3 Q's, what are those? The Q's first question is that how safe is safe enough? Then second Q is that how many protection layers are needed? Because ultimately it decides the cost the third Q is that how much risk reduction should each layer provide? So the providing rational semi-quantitative risk based answers and sometimes another task is the to reducing the emotionalism and provide the clarity and consistency and sometimes the major task of LOPA is the documenting the basis of decision because sometimes it maybe referred for future study or future consequence analysis.

(Refer Slide Time: 12:49)

### The steps to the LOPA process

- Step 1: Identify the consequence to screen the scenario
- Step 2 : Select an accident scenario
- Step 3 : Identify the initiating event & determine the initiating event frequency
- Step 4 : Identify the IPLs & estimate PFD of each IPL
- Step 5 : Estimate the risk
- Step 6 : Evaluate the risk



NPTEL ONLINE CERTIFICATION COURSE 15

Now there are various steps associated with the LOPA process we have enlisted all those process the step 1 that need to identify the consequence to screen the scenario because there may be several consequences then you need to shortlist or screen the scenario then the step 2 that is the select and accident scenario so you will have a different scenarios then you need to pick the accident scenario because there may be certain process related scenarios there maybe certain safety related scenarios, there may be certain environmental related scenarios so you need to select and accident scenario.

Then the third step is identify the initiating event and determine the initiating event frequency, so that you can properly design this particular process a priory then step 4that is you need to identify the IPLs and estimate the PFD of each IPL so that you can narrow down or zero down the process then step 5 that you estimate the risk and step 6 is that you evaluate on the basis of your estimation you evaluate the risk.

(Refer Slide Time: 14:01)

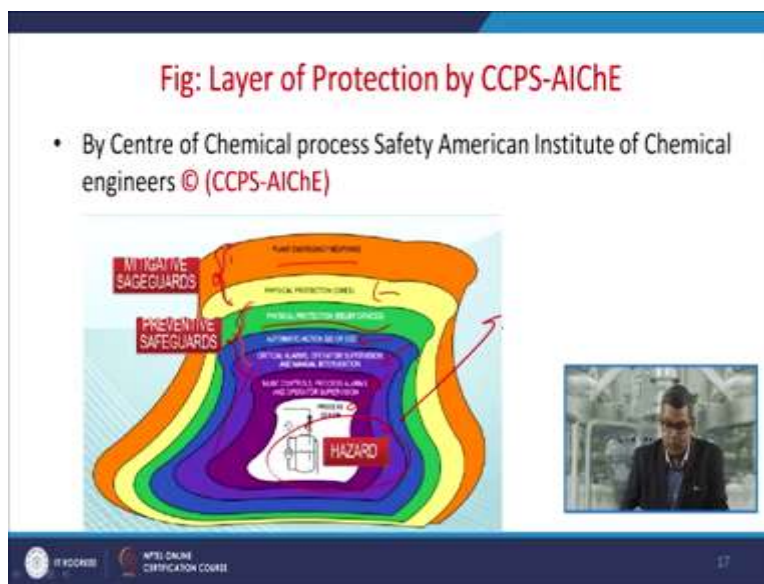
**Benefits of LOPA**

- LOPA takes less time than quantitative risk analysis.
- LOPA provides better risk decision basis.
- LOPA is more defensible for more rigorous documentation and specific value than qualitative method.
- LOPA identifies operations and practices.

IIT Kharagpur NPTEL ONLINE CERTIFICATION COURSE 15

Now, there are benefits of LOPA this these benefits are enlisted in this slide this LOPA takes less time than the quantitative risk analysis the reason is that you have already shortlisted the various scenarios so the time devoted to those unnecessary is less or curtailed compare to the quantitative risk analysis. Now this LOPA provides the better risk decision basis because you have already zero down your process now LOPA is more defensible for more rigorous documentation and specific value than qualitative methods. Now this LOPA identifies the operation and practices so it is more practical compare to the tools available.

(Refer Slide Time: 14:51)




Now, let us have a discussion about the layer of protection by CCPS-AICHE now the CCPS stands for Chemical Process Safety and it is a branch of American (chemical) American Institute of Chemical engineers this is the foremost body of chemical engineers across globe. So you can have a look that there is a hazard present over here then you need to take the process decision then there are certain basic controls process alarms and operator supervision then the critical alarms and operator.

The super vision and manual intervention, this is the another layer, then the automatic actions or SIS for various system then the physical protection of the relief devices so these are the preventive safeguards. So once they fail then the physical protection like dikes and the plant emergency responders so they are the mitigating safeguards so that it cannot propagate further.

(Refer Slide Time: 15:58)

In this figure, safety protection is broken down into several layers (By Mannan, S, 2005)

- Layer 1: Process Design (e.g. inherently safer designs)
- Layer 2: Basic controls, process alarms, and operator supervision
- Layer 3: critical alarms, operator supervision, and manual intervention
- Layer 4: Automatic action such as safety instrumented system (SIS) or emergency shutdown
- Layer 5: Physical protection such as pressure relief devices
- Layer 6: Physical protection such as blast walls and dikes)
- Layer 7: Plant emergency response; and not shown
- Layer 8: Community emergency response



18


Now in this figure the safety protection is broken by several layers the layer 1 this particular layer is the process design then we have discussed the basic control process alarms etc. so you can see that there different layers.

(Refer Slide Time: 16:25)

- It is to be noted that these layers described are not exhaustive layers of protection and not to considered as complete.
- The development of layer of protection (LOP) depends upon the type of the case. Additionally, no layer can be said perfectly effective and hence additional layers must be provided to perfectly mitigate the risk.
- Frequency of Consequence ( $f_i^c$ ) can be calculated through frequency of initiating event (IEF<sub>i</sub>) and probability of failure on demand of IPL (PFD<sub>ij</sub>) as (from reference No.2)

$$f_i^c = IEF_i \times \prod PFD_{ij}$$

$\prod PFD_{ij}$  represents product of all PFDs



19

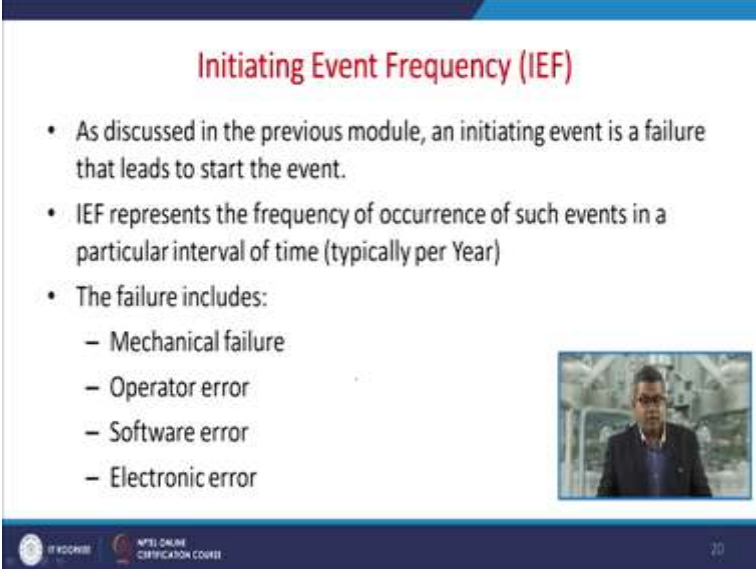
Now on the basis of these different layers you can respond to various accidents if any take place so it is to be noted that these layers describe not the exhaustive layers of protection and not to consider as a complete one because some unforcing circumstances may take place. So the development of layer of protection depends upon the type of case additionally no layer can be set

perfectly effective and additional layer must be provided to perfectly mitigate the risk. So let us have a look about the frequency of consequences that is sometimes referred as  $f_i^c$  this can be calculated through the frequency of initiating event that is ( $IEF_i$ ) and probability of the failure on demand of IPL that is ( $PFD_{ij}$ ) they are two events so this can be calculated through this particular mathematical relation that is

$$f_i^c = IEF_i \times \prod PFD_{ij}$$

$F_i$  is equal to  $IEF_i$  into  $PFD_{ij}$  now this represents the product of all PFDs.

(Refer Slide Time: 17:36)



**Initiating Event Frequency (IEF)**

- As discussed in the previous module, an initiating event is a failure that leads to start the event.
- IEF represents the frequency of occurrence of such events in a particular interval of time (typically per Year)
- The failure includes:
  - Mechanical failure
  - Operator error
  - Software error
  - Electronic error


20

Now, let us have a look initiating event frequency IEF so in the previous module we have discussed about various initiating event in failure so that leads to start the event. So IEF that is initiating event frequency this represents the frequency of occurrence of such event in a particular interval of time typically you can say the per year. Now this failure includes various kind of mechanical failures sometimes error attributed to the operator sometimes maybe because of some bug etc the software error sometimes any kind of electronic instrument or instrumentation panel may fail so it is attributed to electronic error.

(Refer Slide Time: 18:27)

### Probability of Failure upon Demand (PFD)

- Failure on demand is a case when a safety system fails to react when an initiating event happens. For example,  
If a relief device is assigned to address the pressure relief in case of reaction runaway, and if runaway occurs then it is considered as a demand.  
In a testing experiment of relief device or through previous plant history, if it is observed that:  
the relief device opens in 98 times out of 100 demands then,  
PFD will be calculated as  $(100-98)/100 = 0.02$




21

Now the probability of a failure upon demand that is PFD this failure on demand is a case when a safety system fails to react when an initiating event happens. So let us take an example that if a relief device is assigned to address the pressure relief in case of reaction runaway and if runaway occurs then it is considered as a demand the reason is that without this pressure release system you cannot control the process. So in a testing experiment a relief device or through previous say plant history now if it is observed that the relief device opens in 98 times out of 100 demand then the PFD will be calculated as 100 minus 98 because this 100 the demand and 98 is the success. So it is 0.02. So the PFD would be 0.02.

(Refer Slide Time: 19:32)

### Fail Safe Position

- Consider a case of electricity failure in the plant.
- What will happen if the safety layer designed depends upon the electricity?
- It may also be possible that more than one safety layer depends on electricity (in this case both of the layers will not be considered as independent, as they depend upon one cause)
- This type of situation leads the safety engineer to evaluate the fail safe position of the control device.



NTPL ONLINE CERTIFICATION COURSE


22

Now, there is a Fail Safe Position so let us consider a case of electricity failure in the plant so what will happen if the safety layer designed depend upon this electricity then definitely it could not be in a position to work so it may also be possible more than one safety layer which we have already discuss depends on the electricity in this particular case both of the layer will not be considered as independent as they depend upon one cause. So this type of situation leads the safety engineer to evaluate the fail safe position of the control device.

(Refer Slide Time: 20:12)

### Fail Safe Position

- The fail safe position of a safety device (e.g. pressure relief valve) is how it should operate when there is a loss of power or signal.
- Proper functioning of safety device must be know to assess this position. In case of pressure relief device, it should be noted that majority of these devices are pneumatic, means it depends on the air pressure to function.
- The functioning of relief system is already discussed in the previous lectures.
- Air has to be added or released to function a relief device.



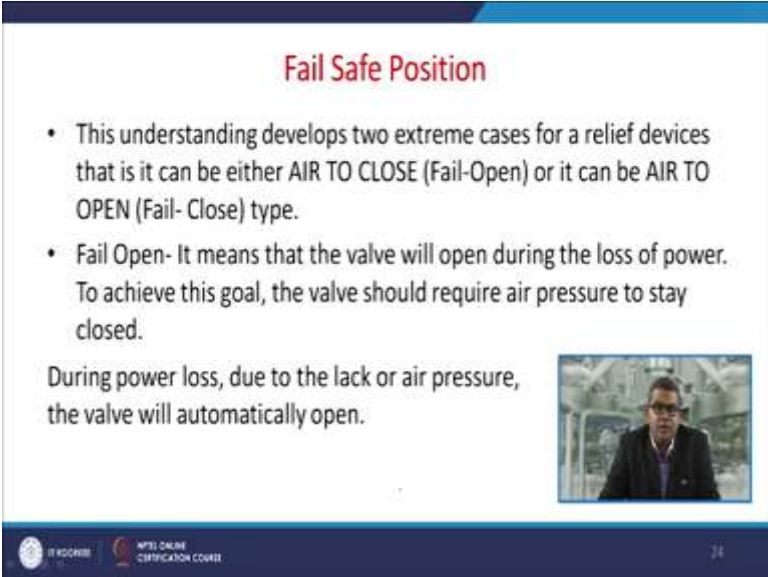
NTPL ONLINE CERTIFICATION COURSE

23

Now the Fail Safe Position of a safety device sometimes like example of the pressure relief valve is how it should operate? It should operate when there is a loss of power or signal because there may be certain relief devices those who are actuated with the power or electricity and some of the safety devices they do not require any kind of supply of power so let us discuss the previous case.

Now the proper functioning of the safety device must be known to assess this position. In this in the case of pressure relief device it should be noted that majority of this devices are pneumatic that means it depends on the air pressure to function. So the functioning of the relief system already discussed we have already discussed the relief segment of the various modules so air has to be added to release to function a relieve device.

(Refer Slide Time: 21:16)



**Fail Safe Position**

- This understanding develops two extreme cases for a relief devices that is it can be either AIR TO CLOSE (Fail-Open) or it can be AIR TO OPEN (Fail- Close) type.
- Fail Open- It means that the valve will open during the loss of power. To achieve this goal, the valve should require air pressure to stay closed.

During power loss, due to the lack of air pressure, the valve will automatically open.

NPTEL ONLINE CERTIFICATION COURSE

24

Now this understanding develops two extreme cases for a relief device that is can be either AIR to CLOSE that is Fail-Open or it can be AIR to OPEN Fail-Close type system. So fail-open it means that the valve will open during the loss of power now to achieve this goal the wall should require air pressure to stay close so during the power loss due to the lack of air pressure the wall will automatically open. So this is the fail-safe position.

(Refer Slide Time: 21:53)


### Example of Fail-Open Scenario

Let us consider a case where a pressure relief device is mounted with the inlet water line of a cooling system. This cooling system is provide to cool down the vessel during reaction runaway.

Assume, suddenly an electricity failure occurs, which leads to loss of control to the pressure relief device.

Now two possibilities arise:

1. Runaway does not occur
2. Runaway occur



NPTEL ONLINE CERTIFICATION COURSE 25

So let us have an example of fail-open scenario, so let us consider a case where the pressure relief device is mounted with the inlet of water line of a cooling system now this cooling system is provide to cool down the vessel during the reaction runaway. So let us assume that suddenly an electricity failure occurs which led to the loss of control to the pressure relief device. Now there are two possibilities, one is that runaway does not occur and second is that runaway occurs.


(Refer Slide Time: 22:30)

### Example of Fail-Open (FO) Scenario

For case one when runaway reaction does not occur, their will be no need of cooling system and the process continues.

But due to the installation of FO relief device, suddenly cooling water will start flowing which leads to lower down the reaction temperature and may interrupt the process, which may leads to loss of product quality for that batch.

But the good news is **No Accident Happen!**

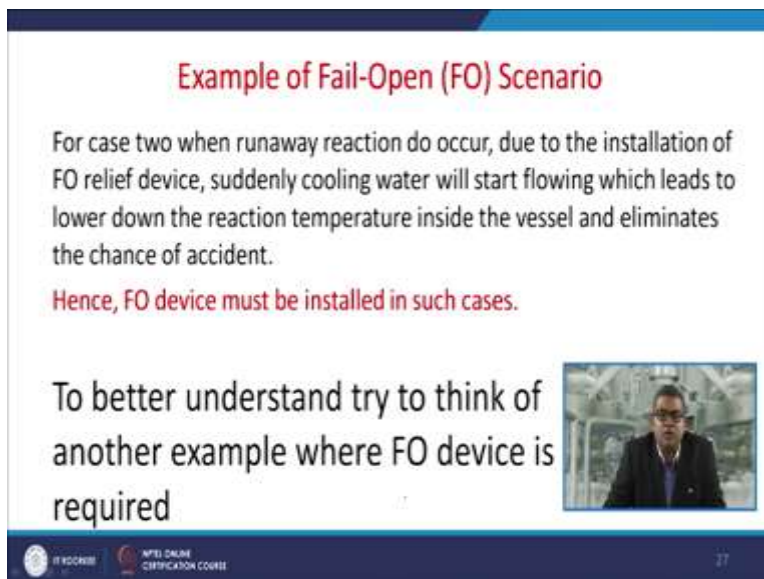


NPTEL ONLINE CERTIFICATION COURSE 26

So for case when the runaway reaction does not occur now there will be no need of any kind of cooling system and the process will continue but due to the installation of fail-open relief device

suddenly cooling water will start flowing which leads to lower down the reaction temperature and it may interrupt the process. So this may lead to the loss of product quality for the batch and sometimes it may lead to economic losses but the good news is that no accident happens but ultimately there is a loss in the product quality and there maybe a chances of the process shutdown so economic loss may occur.

(Refer Slide Time: 23:20)




**Example of Fail-Open (FO) Scenario**

For case two when runaway reaction do occur, due to the installation of FO relief device, suddenly cooling water will start flowing which leads to lower down the reaction temperature inside the vessel and eliminates the chance of accident.

Hence, FO device must be installed in such cases.

To better understand try to think of another example where FO device is required



NPTEL ONLINE CERTIFICATION COURSE 27


For the case number 2 when the runaway reaction do occur now due to the installation of this fail-open relief device suddenly cooling water will start flowing which leads to lower down the reaction temperature inside the vessel and eliminates the chance of accident hence the fail-open device must be installed in such a cases. So to better understand try to think of another example where fail-open device is required.

(Refer Slide Time: 23:44)

### Fail-Close

- Fail Open- It means that the valve will close during the loss of power. To achieve this goal, the valve should require air pressure to remain open.

During power loss, due to the lack of air pressure, the valve will automatically close.



NPTEL ONLINE CERTIFICATION COURSE 28

Now another thing is that the fail close, the fail-open it means that the valve will close during the loss of power now to achieve this goal the valve should require air pressure to remain open so during the power loss due to the lack of air pressure the valve will automatically close.


(Refer Slide Time: 24:06)

### Example of Fail-Close (FC) Scenario

Consider a case where a control valve is installed at the inlet of the feed of a reaction vessel, and a controlled supply of the feed is required to eliminate the chances of reaction runaway.

If power fails then due to the lack of air supply, the control valve automatically close and the feed will stop entering the reactor and the product formation will gradually stop or may be the quality will be compromised for that batch.

But the reaction vessel will remains safe.



NPTEL ONLINE CERTIFICATION COURSE 29

So let us have an example of fail-close scenario so consider a case where a control is installed at the inlet of the feed of reaction vessel and a control supply of feed is required to eliminate the chances of any reaction runaway. So if power fails then due to the lack of air supply the control valve automatically close and the feed will stop entering into the reactor. The product formation

will gradually stop and maybe the quality will be compromised or a challenged for that particular batch but the reaction vessel will remain safe so this is the plus point of this particular thing. Now let us have a look about that either fail-open or a fail-close scenario.

(Refer Slide Time: 25:06)

**FO or FC!**

**Let us assume if FO device was installed in case of FC!**

Then during power failure the inlet will remain open and results to the reaction runaway and the safeguard is said to be failed.

In other words, safeguard (FO device) for this case is called as dependent (on electricity) event. Hence it cannot be considered as IPL.

**From the above discussed examples it is clear that:**

Safety instrument system SIS (Layer 4) must be independent of basic controls, process alarms, and operator supervision (Layer 2)

10

So let us assume that if fail-open device was installed in case of a fail-close then during the power failure the inlet will remain open and that would result to the reaction runaway and the safeguard is set to be failed. So in other words the safeguard or fail-open device for this case is called the dependent on electricity hence it cannot be considered as an IPL scenario. So from the above discussed example it is obvious that if safety instrument system that is SIS sometimes if we recall the layering of AICHE diagram the layer 4 must be independent of basic control and the process alarm and the operator supervision which are clubbed in the layer 2 of that particular diagram.

(Refer Slide Time: 26:03)

### Periodic Reliability Testing

Each layer of safety protection system must be audited periodically.


The period of testing depend upon the type of safeguard

**Big Relief Valves – 3 to 5 years cycle**

**Sensors (fire, toxicity and other) – Monthly**

The time period of testing can be estimated through probability of failure (PFD); higher the PFD shorter the time period of testing.

It is required to maintain the reliability of the IPL.



NPTEL ONLINE CERTIFICATION COURSE 11


Now there are certain things related to the Periodic Reliability Testing, so each layer of safety protection system it must be audited periodically. Now the period of testing depend upon the type of safeguard like big relief valves are in question then 3 to 4 years cycle if sensor this sensor maybe attributed to the fire, toxicity, and others maybe monthly. So the time period of the testing can be estimated through the probability of failure PFDs higher the PFD shorter the time period of the testing it requires to maintain the reliability of the IPL. So this ultimately this is the governing factor.

(Refer Slide Time: 26:56)

### SIS Operation Modes

- Low Demand Mode: The mode of operation where the IEF is not greater than 1/year. The IPL is not challenged more than once per year.
- High Demand Mode: The mode of operation where the IEF is greater than 1/year. The IPL is challenged more than once per year.
- Continuous Mode: the mode of operation where the process must be retained in a safe state as part of normal operation.

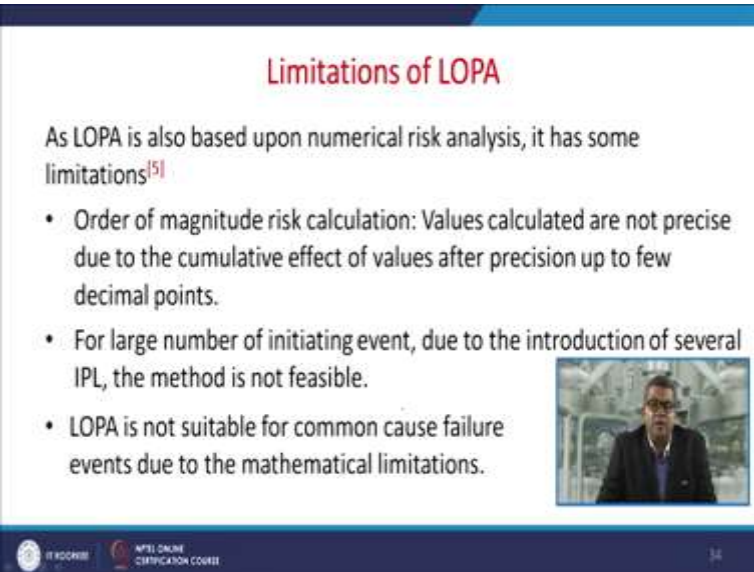
**IF an IPL is working in a high/ continuous mode, then efforts should me made to make improved design and maintenance, such that IPL are able to operate in low demand.**



NPTEL ONLINE CERTIFICATION COURSE 12

Now SIS operation modes so the lower demand mode the mode of operation where the IEF is not greater than one per year so the IPL is not challenged more than once per year. Now there is another high demand mode now the mode of operation where IEF is greater than one per year the IPL is challenged more than once per year. There is another mode that is called the continuous mode now this mode of operation where the process must be retained in a safe state as part of normal operation. So if an IPL is working in high or continuous mode then efforts should be made to make improved design and maintenance such that IPLs they are able to operate in low demand.

(Refer Slide Time: 27:56)



**Limitations of LOPA**

As LOPA is also based upon numerical risk analysis, it has some limitations<sup>[5]</sup>

- Order of magnitude risk calculation: Values calculated are not precise due to the cumulative effect of values after precision up to few decimal points.
- For large number of initiating event, due to the introduction of several IPL, the method is not feasible.
- LOPA is not suitable for common cause failure events due to the mathematical limitations.


The slide includes a small video inset showing a man in a suit speaking. At the bottom, there are logos for 'NPTEL ONLINE CERTIFICATION COURSE' and the number '34'.

Now there are certain limitations they are attributed to LOPA now LOPA is also based on the numerical risk analysis so it has some limitations. Now in the order of magnitude risk calculation this is the first limitations the value calculated are not precise due to the cumulative effect of values after precision up to few decimal point. Now for large number of initiating event due to the introduction of several IPLs the method is not feasible and LOPA is not suitable for common cause failure event due to the mathematical limitation so be particular about using LOPA for various scenarios.

(Refer Slide Time: 28:48)

**Discussion**

- LOPA is a methodology for hazard evaluation and risk assessment, and lies between simple qualitative and more elaborate quantitative analysis techniques.
- In decision-making process, LOPA helps to decide the propriety of protection layers that exist or are suggested to prevent accidents, so ideally matches the risk-decision criteria of the company.
- LOPA is a recognized technique that can establish a proper safety integrity level (SIL) of the process.




NPTEL ONLINE CERTIFICATION COURSE 35

Now LOPA is the methodology for hazard evaluation and risk assessment and it lies between the simple qualitative and more elaborative quantitative analysis technique and in decision making process the LOPA helps to decide the propriety of protection layer that exist are suggested to prevent the accidents so ideally matches the risk decision criteria of the particular unit or a company whatever you would like to say. Now this LOPA is recognized technique that can establish a proper safety integrity between level SIL of that particular process.

(Refer Slide Time: 29:30)

**Discussion**

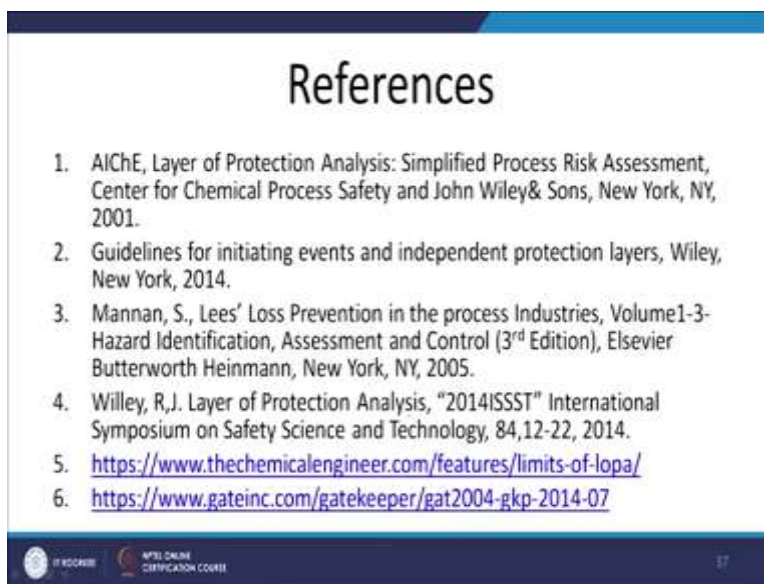
- Using LOPA, we need to set up proper protection layers that evaluate, analyse, and decrease the risk in chemical process.



NPTEL ONLINE CERTIFICATION COURSE 36

So using LOPA we need to set up proper protection layers that evaluate analysis that evaluate analyze and decrease the risk in chemical process. So in particular module we had discussion about the cause consequences and LOPA and this are the you can say the elaborative work of your event tree and fault tree analysis.

(Refer Slide Time: 30:04)



## References

1. AIChE, Layer of Protection Analysis: Simplified Process Risk Assessment, Center for Chemical Process Safety and John Wiley& Sons, New York, NY, 2001.
2. Guidelines for initiating events and independent protection layers, Wiley, New York, 2014.
3. Mannan, S., Lees' Loss Prevention in the process Industries, Volume1-3- Hazard Identification, Assessment and Control (3<sup>rd</sup> Edition), Elsevier Butterworth Heinmann, New York, NY, 2005.
4. Willey, R.J. Layer of Protection Analysis, "2014ISSST" International Symposium on Safety Science and Technology, 84,12-22, 2014.
5. <https://www.thechemicalengineer.com/features/limits-of-lop/>
6. <https://www.gateinc.com/gatekeeper/gat2004-gkp-2014-07>

At the bottom of the slide, there are logos for 'IT RECORDS' and 'NPTEL ONLINE CERTIFICATION COURSE' on the left, and the number '37' on the right.

So if you wish you to have further discussion or further study then you can have a look of these references which are enlisted over here, thank you very much.