

Introduction to Reliability Engineering
Professor Neeraj Kumar Goyal
Subir Chowdhury School of Quality and Reliability
Indian Institute of Technology, Kharagpur
Lecture 03
Introduction to Reliability Engineering (Contd.)

Hello everyone. So we are continuing our lecture series, this is our third lecture. In previous 2 lectures, we discussed about some terms and their definitions, we will continue the discussion on the terms and definitions which are used in reliability engineering. Previous lecture we discussed about the terms which are commonly used for reliability engineering. We will continue our discussion and now, we will discuss about the terms which are used for maintainability and availability and safety.

(Refer Slide Time: 01:00)

The slide is titled "Limitations of Reliability Theory" in yellow text on a dark blue background. It features two bullet points in blue text with red underlines: "It can not predict when a system / component will actually fail ." and "Reliability is 100% only if you do not use the system/component." A small blue circle is positioned below the second bullet point. On the left side, there is a vertical banner with the text "NPTEL ONLINE CERTIFICATION COURSES INTRODUCTION TO RELIABILITY ENGINEERING". At the bottom, there is a video inset of Professor Neeraj Kumar Goyal, a slide number "21", and the text "Dr. Neeraj Kumar Goyal" and "Indian Institute of Technology Kharagpur".

- It can not predict when a system / component will actually fail .
- Reliability is 100% only if you do not use the system/component.

As we discussed in reliability, we want to know the reliability. But the problem is that many times, when it comes to reliability, we are interested in knowing at what time the failure will occur. Unfortunately, we can never determine exactly when a system or component will fail. For example, if I am using a cooler, fridge, AC, or my vehicle, I cannot be sure that it will fail at this moment. Similarly, nobody can predict the exact moment that a person will die.

However, we can assess the probability of failure, meaning the likelihood that a certain system will fail. A higher probability means a higher chance of failure. For instance, if a large population is using a particular device, we can estimate the proportion of the devices that may fail.

Although we cannot predict the exact time of failure, we can estimate the chances of failure. The prediction, however, is limited to the chances of failure and not the exact time to failure. For instance, if I use 100 tube lights in the same room, on average, I can expect to see around 5-6 failures per year. Alternatively, if the tube lights are beyond 2-3 years of use, the failure rate can increase to 30-40%.

Therefore, we cannot claim that any system is risk-free or 100% reliable. There is always a chance of failure or an accident. However, we can work towards improving the reliability of the system to increase the chances of success and minimize the chances of failure and accidents.

(Refer Slide Time: 05:16)

The slide is titled "Maintainability Related Terms" and is part of an NPTEL course on "Introduction to Reliability Engineering". It lists five types of maintenance:

- **Maintenance**
 - The combination of all technical and administrative actions, including supervision actions, intended to retain a product in, or restore it to, a state in which it can perform a required function
- **Corrective Maintenance**
 - The maintenance is carried out after fault recognition and intended to put a product into a state in which it can perform required function.
- **Proactive Maintenance**
 - **Predictive Maintenance**
 - The maintenance is scheduled to be carried out cost effectively using information gathered through condition monitoring technique(s) before equipment performance beyond threshold.
 - **Preventive maintenance**
 - The maintenance carried out at pre-determined intervals or according to criteria and intended to reduce the probability of failure or the deterioration of functioning of an item

Now we will discuss maintainability. In maintainability, maintenance is a combination of all technical and administrative actions. It includes supervision actions and is intended to retain the product in good condition, restore it from a failed state to a good state or to a state where it can perform a required function.

Our intent is that the maintenance intention is the same as the system should be able to perform the required function. The system is designed for certain functions and should be able to perform them. Maintenance is for that purpose, either to ensure that it continues to perform the function without failure or, if it fails, we repair it and bring it to a working condition. Even though it may not be fully restored, it can still perform the required function. Therefore, maintenance is a set of activities aimed to accomplish all these objectives.

There are different types of maintenance. One is corrective maintenance, which was used before World War 2 when dependency on systems was not very high. Whenever a system failed, people could correct it. It was carried out after fault recognition, meaning that once a failure occurred, the fault was identified, and the system was put back into a working state. However, during World War 2, when systems became larger and complex, if a failure happened, people were losing the war because if their equipment did not work, they could lose troops and lives.

Similarly, during the Industrial Revolution, when their dependency on machines was higher, if the machine failed, the whole staff would not be able to do any production. Repair costs may not have been high, but repair time was very costly. During downtime, the function could not be performed, and there were high losses, including mission losses. Therefore, a philosophy for proactive maintenance emerged in Second World War and onwards. Preventive maintenance came first. In preventive maintenance, the simpler systems with only a few components, which tended to fail, were assessed to determine how long it generally took to fail. Before the failure occurred, the aged components were replaced with new components. This is applicable only to the components that fail on ageing, such as gears, bearings, moving parts, friction parts, computer screens, etc. Here, predetermined intervals are used from earlier experience and data to identify the safe interval within which there are not many chances of failure. At those intervals after which there is a high probability of failure, the item is replaced with a new one, or it is maintained or repaired using certain procedures so that it becomes as good as new. First, degradation is removed, then the system becomes good, and it continues working. This is called preventive maintenance.

However, preventive maintenance may result in replacing good components and inducing errors during maintenance. Machines that were working fine may start creating problems because of human error or other reasons during maintenance. Therefore, the concept of predictive maintenance was introduced to stop a good running system for maintenance. In predictive maintenance, the system is observed using various sensors, which are used most of the time nowadays. Here, preventive maintenance can be used for frequently checking and inspecting certain parameters, and based on those parameters, it is determined whether a particular component or system is in a healthy or unhealthy state. If the system is healthy, it is

not touched, and we continue with it. However, if the system is found to be developing faults or degradation, those systems are replaced or repaired. This is called predictive maintenance.

"Predictive maintenance helps reduce the replacement of good components or unwanted interactions with the system, thereby preventing unnecessary component replacements. However, predictive maintenance may not always be possible, as the failure must be identifiable in advance. Without a means to identify failure, it may not be feasible. Collectively, these techniques are called proactive maintenance, with proactive maintenance occurring before failure and corrective maintenance taking place after failure. By performing maintenance before failure occurs, we can prevent system failures." (Refer Slide Time: 12:54)

Maintainability Related Terms ...

- **Maintainability**
 - $H(t) = \Pr\{T \leq t\} = \int_0^t h(x) dx$
 - Where T is Time To Repair (TTR) is random variable.
 - $h(x)$ is pdf of TTR
- **Mean Time to Repair (MTTR)**
 - $MTTR = E(T) = \int_0^{\infty} t h(t) dt \Rightarrow \int_0^{\infty} [1 - H(t)] dt$
- **Repair Rate**
 - It provides an instantaneous rate of repair at time t.
 - It is conditional probability of completing repair per unit time in time $(t, t+\Delta t)$.
 - $\mu(t) = \frac{h(t)}{1-H(t)}$

NPTEL ONLINE CERTIFICATION COURSES
INTRODUCTION TO RELIABILITY ENGINEERING

23 Dr. Neeraj Kumar Goyal Indian Institute of Technology Kharagpur


The terms commonly used in maintainability were discussed earlier. Maintenance refers to the procedures, ways, or tools used for upkeep. Maintainability is the probability that the repair time is less than the target time. This means that maintenance should be completed within a certain period of time. For reliability, the time to failure has to be beyond the target time, but for repair, the time to repair should be less than the target time. This is essential for the system to function properly. Maintainability is the probability that the repair time is less than or equal to the target time.

If the probability density function (PDF) of the repair time is $h(x)$, then integrating $h(x)$ from 0 to t will give the maintainability. The mean time to repair can be calculated as 0 to infinity of $h(x)$ multiplied by $t dt$, or 1 minus the cumulative distribution function (CDF) of $h(t)$ from 0 to infinity. Since we are talking about time, the limits are from 0 to infinity.


$$MTTR = E(T) = \int_0^{\infty} th(t)dt$$

The repair rate is the same as the failure rate. It is the instantaneous rate of repair at time t. The concept of failure rate can be applied here as well. The repair rate, μ^*t , has the same PDF as $h(t)$. The survival function of $r(t)$ is 1 minus $h(t)$ because $r(t)$ is 1 minus the CDF (Refer Slide Time: 15:07)

$$\mu(t) = \frac{h(t)}{1 - H(t)}$$



Example 4



- The time to repair a power generator is best described by the following probability density function:

$$h(t) = \frac{t^2}{333} \quad 1 \leq t \leq 10 \text{ hr}$$
- Determine the probability that a repair will be completed in 6 hr. What is the MTTR?
- What is the median time to repair?

Solution:

$$H(6) = \Pr\{T \leq 6\} = \int_1^6 \frac{t^2}{333} dt = \frac{1}{3 \cdot 333} (6^3 - 1) = 0.2152$$

$$MTTR = \int_1^{10} \frac{t^3}{333} dt = \frac{1}{4 \cdot 333} (10^4 - 1) = 7.51 \text{ hr}$$

Handwritten notes on the slide:

- $0.5 = H(t) = \frac{1}{333} (t^3 - 1)$
- $0.5 \times 333 = t^3 - 1$
- $t^3 = 1 + 166.5 = 167.5$
- $t = \sqrt[3]{167.5} \approx 5.5$

Now, let us take one example that time to repair of a power generator is best described by the following distribution. So let us say this is our PDF given for repair time. So my repair time in minimum is 1 hour and maximum is 10 hour, my repair will complete within 1 to 10 hour and within 1 to 10 hour my PDF, that is probability of completing the repair per unit time is $h(t)$. Now, what is the probability that my repair will complete in 6 hours? So that means I am interested in maintainability, maintainability for 6 hours. So maintainability for 6 hours means $H(6)$, I can say $H(t) \leq 6$, probability that is less than equal to 6.

Now, this is on 1, so 0 will be replaced by 1 and maximum limit is up to 6, t is 6, t square by 333 dt . If I take the integration of this, this will become t cube by 3 into triple 3, and if I put the limits 6 and 1, this will become 6 cube minus 1 cube. And this if I solve I get the value 0.2152. This is my probability that my repair will complete in 6 hours. So or I can say this is my maintainability for 6 hours. What is mean time to repair? Mean time to repair as we see this is 0 to infinity, but since this is defined from 1 to 10 only, so 0 will be replaced by 1 and maximum values will be 10.

What is my $R(T)$? I can say $1 - h(t)$ or I can say $\int_0^t f(t)dt$, so $\int_0^t h(t)dt$. So if I multiply t with this, this will become t^3 by triple 3, t^3 by triple 3 dt . If I integrate this, this will become t to the power 4 divided by 4. So t to the power 4 that is 10 to the power 4 minus 1 to the power 4 divided by 4 divided by triple 3, this if I solve this gives me 7.51 hours. So this gives me value that which gives me that is the mean time to repair. So 7.51 hour is expected to be the mean time which is taken for repair.

Next question is what is median time to repair? So median time to repair we can calculate here I have not calculated already. So let us say median time, what is median time? Median time is at that time the probability is CDF value is 0.5 or my maintainability is 0.5 , I can say $1 - \text{maintainability}$ is 0.5 . Let us say maintainability is 0.5 , I want to know the time at which my maintainability is 0.5 , $H(t)$ is 0.5 . So $H(t)$ we have got this here $H(t) = 1 - \frac{1}{9}t^3$. Now, this I can solve, if I solve this then this becomes 0.5 into triple 9 that is equal to $t^3 - 1$. So t^3 will be equal to $1 + \text{triple } 9 \text{ into } 0.5$.

Now, if I take this approximation if I assume this is to be approximately 1000 , then this will become 500 . So $500 + 1$ or even if I calculate this let us say $1 + 499$ point here. So this will become if I add this so this will become 500.5 that is my t^3 . And so my t value will be 500.5 raise to the power $1/3$ which I can calculate using the calculator. I am not using it here this can be done very easily, so I am leaving it here. So, this gives my median time to repair, median time because at this time the probability is 0.5 .

"Now, let us take one example. The time to repair a power generator is best described by the following distribution. So, let us say this is our PDF given for repair time. The minimum time for repair is 1 hour, and the maximum is 10 hours. The repair will complete within 1 to 10 hours, and within this time, the PDF (probability of completing the repair per unit time) is $H(t)$.

Now, what is the probability that the repair will complete in 6 hours? This means I am interested in maintainability for 6 hours. Maintainability for 6 hours means $H(6)$, which is the probability that is less than or equal to 6 . On $1, 0$ will be replaced by 1 , and the maximum limit is up to 6 . So, the integral will be t^2 by $333 dt$. If I take the integration of this, it becomes t^3 by 3 into 333 , and if I put the limits 6 and 1 , it becomes $6^3 - 1^3$. Solving this, I get the value 0.2152 . This is the probability that the repair will complete in 6 hours or the maintainability for 6 hours.

What is the mean time to repair? As we see, this is from 0 to infinity, but since this is defined from 1 to 10 only, 0 will be replaced by 1, and the maximum values will be 10. So, my RT can be calculated as 1 minus H(t) or t times the PDF. So, t times H(t) dt. If I multiply t with this, it becomes t cube by 333 dt. If I integrate this, it becomes t to the power 4 divided by 4 into 333. Solving this gives me 7.51 hours, which is the expected mean time for repair.

$$H(t) = \Pr\{T \leq 6\} = \int_1^6 \frac{t^2}{333} dt = \frac{1}{3 * 333} (6^3 - 1) = 0.2152$$

$$MTTR = \int_1^{10} \frac{t^3}{333} dt = \frac{1}{4 * 333} (10^4 - 1) = 7.51 \text{ hr}$$

Next question is, what is the median time to repair? I have not calculated this yet. Let us say, the median time is the time at which the probability is CDF value 0.5 or maintainability is 0.5. So, I can say 1 minus maintainability is 0.5. Let us say, maintainability is 0.5, I want to know the time at which my maintainability is 0.5, H(t) is 0.5. H(t) can be calculated as 1 upon 999t cube minus 1. If I solve this, it becomes 0.5 into 999 is equal to t cube minus 1. So, t cube will be equal to 1 plus 999 into 0.5, which is 500. If I take this approximation, it becomes 500.5, and my t value will be 500.5 raised to the power of 1/3. This gives my median time to repair, as at this time, the probability is 0.5."

(Refer Slide Time: 19:31)

Availability Related Terms

- Average Availability**
 - $A(T) = \frac{1}{T} \int_0^T A(t) dt$ (point availability)
 - For single unit, following exponential failure and repair distributions with parameters λ and μ
 - $A(t) = \frac{\mu}{\mu + \lambda} + \frac{\lambda}{\mu + \lambda} e^{-(\lambda + \mu)t}$
- Interval (mission) Availability**
 - $A_{t_2-t_1} = \frac{1}{t_2-t_1} \int_{t_1}^{t_2} A(t) dt$
- Inherent (Steady State) Availability**
 - $A_{inh} = A_{SS} = \lim_{T \rightarrow \infty} A(T) = \frac{MTBF}{MTBF + MTTR} = \frac{MUT}{MUT + MDT(CM)}$

Handwritten notes include: $\int_{t_1}^{t_2} f(x) dx = \frac{1}{T} \int_0^T f(x) dx$, a graph of $A(t)$ vs t showing an exponential decay curve, and relationships: $\mu = \frac{1}{MTTR}$, $A = \frac{1}{MTTR}$, $A = \frac{1}{MTTR}$, $DN = \frac{MTR}{MTR + MTTR}$.

Next, let us discuss availability. The most commonly used term for availability is "average availability". What is average availability? Average availability is the integral from 0 to t of

$A(t) dt$. How do we take the average of any function? To find the average of function f from 0 to t , we can calculate the integral from 0 to t of $f(x) dx$ divided by the integral from 0 to t of dx . Therefore, it becomes $1/t$ multiplied by the integral of $f(x) dx$ from 0 to t . Here, $f(x)$ is the availability function, also known as point availability or instantaneous availability, which is a function of time.

$$A(T) = \frac{1}{T} \int_0^T A(t) dt$$

As we can see here, $A(t)$ becomes $1/t$ multiplied by the integral from 0 to t of $A(t) dt$ when we take the average for an interval. If we have the exponential failure rate and exponential repair rate with parameters λ and μ , we can obtain the availability function. We will discuss this later, maybe around the eighth or seventh week. If we have the failure distribution, which is exponential with repair, and a failure rate λ , and if we have the repair rate μ for the repair distribution, which is also exponential, then we can get the availability function, which is $\mu/(\mu+\lambda) * (\lambda/(\mu+\lambda)) * e^{-(\lambda+\mu)t}$.

$$A(t) = \frac{\mu}{\mu + \lambda} + \frac{\lambda}{\mu + \lambda} e^{-(\lambda + \mu)t}$$

If we plot t versus $A(t)$, it will look something like this. If we put t equal to infinity, then $A(t)$ becomes 0 because exponential minus infinity equals 0. Therefore, it terminates at $\mu/(\mu+\lambda)$, which means it will never be below $\mu/(\mu+\lambda)$. At the start, when t equals 0, $A(t)$ becomes $\mu+\lambda/(\mu+\lambda)$, which means availability starts from 1 and decreases. Generally, this is our instantaneous or point availability, which varies for one device that has the exponential distribution for repair and failure.

If we want the interval or mission availability, we need to integrate from t_1 to t_2 using the same formula. The result will be $(1/(t_2-t_1))$ multiplied by the integral from t_1 to t_2 of $A(t) dt$. As we see, this availability, which is a time function, becomes almost constant after a certain period of time, and this value that we get is called inherent or steady state availability. This value is not changing even though time is changing. It is independent of time because repair and failure have happened too many times. This is known as the inherent or steady state availability.

$$A_{t_2-t_1} = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} A(t) dt$$

The limit t tending to infinity of $A(t)$ is the inherent or steady state availability, which is $\mu/(\mu+\lambda)$. What is μ ? μ is $1/MTTR$, and λ is $1/MTTF$. Therefore, if we apply this here, it becomes $1/MTTR$ divided by $1/MTTR+1/MTTF$. If we simplify this, it becomes $MTTF/(MTTR+MTTF)$, which is the same as the previous result.

$$A_{inh} = A_{SS} = \lim_{T \rightarrow \infty} A(T) = \frac{MTBF}{MTBF + MTTR} = \frac{MUT}{MUT + MDT_{CM}}$$

This has some different notations. We can say that if we use the uptime and downtime basis, the mean uptime divided by the mean uptime plus mean downtime is the inherent or steady state availability. Here, downtime is only considered due to corrective maintenance, which means the downtime that occurs only due to repair after failure. We are not counting the downtime that occurs due to preventive or predictive maintenance.

(Refer Slide Time: 25:15)

Availability Related Terms ...

- Achieved Availability**
 - $A_a = \frac{MTBM}{MTBM + \bar{M}} = \frac{MUT}{MUT + MDT_{CM} + MDT_{PM}}$
 - where, MTBM is mean time between maintenance (all types) and
 - \bar{M} is mean system downtime considering all maintenance downtimes.
- Operational Availability**
 - $A_o = \frac{MTBM}{MTBM + \bar{M} + MDT} = \frac{MUT}{MUT + MDT_{CM} + MDT_{PM} + MDT_{adm}}$
 - Where, MDT is mean delay time due to maintenance and supply time (including administrative delays)
- Which of the above availability decreases to achieve reliability?

28 Dr. Neeraj Kumar Goyal Indian Institute of Technology Kharagpur

Then we could include the downtime due to the predictive maintenance and preventive maintenance that is our proactive maintenance, then we call it as achieved availability. So mean uptime divided by mean uptime, then downtime due to both causes either due to the failures whatever repair time is taken after the failure or whatever is the repair time which is there due to the preventive maintenance actions, both downtime will be combined here, then we will call it achieved availability.

Mean, here we use the term MTBM, MTBM is the mean time between maintenance sections. So maintenance sections here can be either due to the repair on failure or it can be maintenance action can be taken to avoid the failure that is our preventive maintenance section. And \bar{M} is the mean system downtime which is considering all maintenance downtime, corrective maintenance also and preventive maintenance also. Then comes operational availability that actually how much time it is available for operation in that case, we are including additional downtime, which is due to the administrative reason, this administrative reason is mostly like decision making, there can be the downtime due to the spare parts like.

$$A_u = \frac{MTBM}{MTBM + \bar{M}} = \frac{MUT}{MUT + MDT_{CM} + MDT_{PM}}$$

So sometimes what happens our devices fail, but we do not have a spare available. Then there is a maintenance time, maintenance in terms of here this is for crew availability. So what can happen that the specific person or the specific technicians are required that may not be available, so all these types of downtime when we combine it becomes operational availability that actually this becomes very close to the practical experience, where we are counting the downtime due to the corrective maintenance, preventive maintenance as well as the delays, various delays, maintenance delays, logistic delays, all delays are counted here.

$$A_o = \frac{MTBM}{MTBM + \bar{M} + MDT} = \frac{MUT}{MUT + MDT_{CM} + MDT_{PM} + MDT_{adm}}$$

Supply delay time, supply delay time is the spare part and maintenance delay time maintenance is due to the crew availability or the equipment which is required for repair. So generally, if we want to achieve high reliability, what will happen? To achieve high reliability we have to do the preventive maintenance. So to achieve high reliability many times we have to put more time here. So this may decrease achieved availability, this may decrease our operational availability.

So we have to look into that how much but most of the time we have to achieve high reliability the reason being that there is a high losses whenever there is a failure. So we may have to invest some time here that may reduce availability sometime not always because there is a gain here also. So there is a increase in uptime expected but generally that is not there because generally that uptime may also be a little bit reduced because we are doing

maintenance early, earlier than that life is fully consumed. So overall it is generally tending to give you the lower availability when you are doing the preventive maintenance.

(Refer Slide Time: 28:45)

Availability and Downtime

- Expected downtime in a year can be calculated as:
 - $MDT = (1 - A_{ss}) \times 365 \times 24 \times 60 \text{ min/yr}$
- For most of railway projects, availability requirements of signalling system are at least 99.99%.
- If signalling system is demanded for 99.99% availability, but vendor has provided 99.95% availability. How much is the difference in downtime? $A = 0.9999$, $A = 0.9995$, $A - 0.0004 = 10^{-4}$

Availability (%)	Downtime (%)	Downtime (in Hrs)	Downtime (in Min)
90%	10%	876 hrs.	52560 Min.
99%	1%	87.6 hrs.	5256 min.
99.9%	0.1%	8.76 hrs.	525.6 min.
99.99%	0.01%	0.876 hrs.	52.56 min.
99.999%	0.001%	0.0876 hrs.	5.256 min.

If we consider our main interest, it is mostly in downtime, such as for railways or other facilities that are highly costly and time-based. Mean downtime can be calculated as unavailability. What is unavailability? Unavailability is 1 minus steady-state availability multiplied by 365 days, 24 hours, and 60 minutes. There are 60 minutes in each hour and 24 hours in each day, so there are 365 days in a year. Therefore, we can calculate the downtime in terms of minutes per year.

$$MDT = (1 - A_{ss}) \times 365 \times 24 \times 60 \text{ min / yr}$$

For example, if our availability requirement is 99.99 percent, that means our unavailability is 0.01, or 99.9 percent, which is 99.99 divided by 100. This gives us an availability of 0.9999. The unavailability is then 1 minus availability, which equals 0.0001, or 10 to the power of minus 4. We can use this value to calculate the mean downtime.

In the table provided, we can see that when the availability is 90 percent, the downtime is 10 percent. This means that in a year, we are spending 876 hours or 52,560 minutes on downtime. If we aim for 99 percent availability, the downtime is 87.6 hours or 5,256 minutes per year. If we aim for 99.9 percent availability, the downtime allowed is only 0.1 percent, which is equivalent to 8.76 hours of downtime per year. We can obtain other figures in a similar manner.

As we can see, these figures need to be determined based on our requirements, and the target is set accordingly to allow for the desired level of downtime.

(Refer Slide Time: 31:07)

Safety Related Terms

- System safety definition as per MIL-STD-882D
 - The application of engineering and management principles, criteria and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time and cost, throughout all phases of system life cycle.
- Accident
 - An unintended event or series of events resulting in loss of human health or life, damage to property or environmental damage
- Hazard
 - A condition that could lead to an accident

Handwritten annotations: $10^{-6}/\text{year}$ next to System safety definition; a diagram showing 'Hazard' leading to 'Accident' and 'Mishap'.

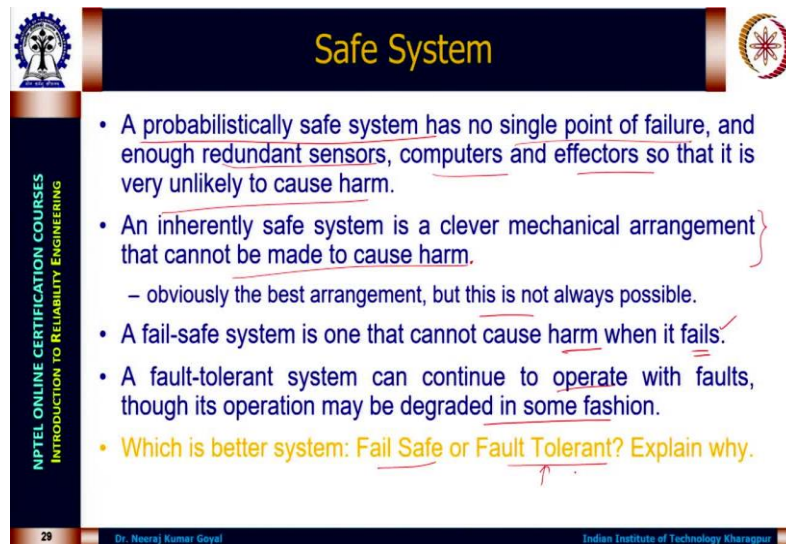
There are safety-related terms, such as system safety definition. This involves the application of engineering management principles, criteria, and techniques to achieve an acceptable level of mishap risk. As we discussed earlier, risk cannot be reduced to zero, but we can aim for a risk level of, let's say, 10 to the power of minus 6 failure probability per year. This means that out of 1 million devices, one device may fail or there is a 1 in a million chance of failure per year. While this is a low risk, it cannot be reduced to zero, and an acceptable level of risk must be determined. System safety aims to achieve a low and acceptable level of risk by using engineering and management approaches.

However, there are operational effectiveness and suitability constraints that must be considered. We cannot assume that everything is possible; we must consider practical factors such as time and cost. Things cannot be too expensive to the point of being unusable or less helpful throughout the system's lifecycle phases. The second term is accident, which refers to a series of accidents resulting in loss of human life, damage to property, or environmental damage.

What is a hazard? A hazard is a potential condition that can lead to something bad happening. However, for that condition to cause harm, certain accidents must occur or certain things must go wrong. Therefore, a hazard is a condition that exists in the system. An accident turns

the system into a mishap. While a hazard is a deterministic quantity that may or may not be possible, an accident makes it probabilistic because the accidental event may happen at any moment. As a result, the probability of a mishap happening will be determined by the risk, which is a probabilistic term that combines hazard and accident.

(Refer Slide Time: 33:36)



The slide is titled "Safe System" and features a list of definitions and a question. The text is as follows:

- A probabilistically safe system has no single point of failure, and enough redundant sensors, computers and effectors so that it is very unlikely to cause harm.
- An inherently safe system is a clever mechanical arrangement that cannot be made to cause harm.
 - obviously the best arrangement, but this is not always possible.
- A fail-safe system is one that cannot cause harm when it fails.
- A fault-tolerant system can continue to operate with faults, though its operation may be degraded in some fashion.
- Which is better system: Fail Safe or Fault Tolerant? Explain why.

What is a safe system? A safe system is a probabilistic system that ensures there is no single point of failure leading to disasters. Therefore, redundancy in terms of sensors, computers, and effectors is implemented to minimize the likelihood of harm. At least 2-3 accidents or failures should occur before something bad happens; a single failure can happen at any moment due to any reason.

An inherently safe system is a clever mechanism arrangement that cannot cause harm. However, every arrangement can fail, and when they do, they may lead to harm. Therefore, a probabilistic concept may also come into play, although it is not always possible.

A failsafe system is one that will not cause harm on failure. So even if it fails, it fails in a condition that will not result in harmful consequences.

A fault-tolerant system can continue to operate despite faults, although its operation may be degraded. Fault-tolerance means that even though there is a fault, the system can still continue to operate without causing problems.

So which is better, failsafe or fault-tolerant? While we would prefer a failsafe system, it is not always achievable. Therefore, we often have to settle for a fault-tolerant system, where the system is tolerant of faults and does not cause problems.

(Refer Slide Time: 35:20)

The slide is titled "Risk Related Terms" and features the NPTEL logo on the left and the IIT Kharagpur logo on the right. The main content is as follows:

- Risk**
 - It is the probability that a particular adverse event occur during a stated period of time or results from a particular challenge.
 - An adverse event is an occurrence that produces harm, which is loss to human being or population of human being.
- Linear Risk**
 - Formula: $R = \sum_{i=1}^n p_i C_i$
 - Handwritten notes: "10 deaths/yr = 10 Accidents / 1 death", "10 death/acc → 1 Acc/def / 10 death"
- Non linear Risk**
 - Formula: $R = \sum_{i=1}^n p_i C_i^2$
 - Handwritten notes: "10 x P = 10", "1 x 10^2 = 100"


At the bottom of the slide, it says "30 Dr. Neeraj Kumar Goyal Indian Institute of Technology Kharagpur".

Whenever we discuss the concept of risk, the concept of probability comes into play. Probability refers to the likelihood of a particular adverse event occurring during a specified period or resulting from a particular challenge, such as a threat or failure. When such an adverse event occurs, we want to know what the probability of that event is. An adverse event is an occurrence that produces harm or loss to humans, populations, or the environment.


Risk is calculated by adding up the probabilities of all possible events and their consequences. The consequence (C_i) refers to the amount of loss, and the probability (p_i) refers to the likelihood of that consequence occurring. If we sum up the probabilities for all events and their consequences, we get the total risk. This is the formula for linear risk. However, there is also nonlinear risk, which occurs when high-consequence events are perceived to have a higher risk than low-consequence events.

For example, there may be 10 motorbike accidents resulting in 1 death each, and 1 bus accident resulting in 10 deaths. Both cases have the same linear risk of 10 deaths per year. However, in the second case, the consequence is higher (10 deaths), so the risk is perceived to be higher. To account for this, we may use a nonlinear factor (such as 2) to adjust the risk calculation. This formula is used only in specific conditions when specified.

(Refer Slide Time: 38:11)




Risk Related Terms




NPTEL ONLINE CERTIFICATION COURSES
 INTRODUCTION TO RELIABILITY ENGINEERING


- Residual Risk
 - Risk remaining once risk control measures have been taken
- Risk Analysis ✓
 - Systematic use of all available information to identify hazards and to estimate the risk
- Risk based approach ✓ *Probabilistic Risk Assessment*
 - In relation to safety, the risk based approach is a procedure for ensuring the safety of products, processes and systems through consideration of the hazards and their consequent risks



31
Dr. Neeraj Kumar Goyal
Indian Institute of Technology Kharagpur




References



NPTEL ONLINE CERTIFICATION COURSES
 INTRODUCTION TO RELIABILITY ENGINEERING

- Charles E. Ebeling (2019) “An Introduction to Reliability and Maintainability Engineering”, 3rd edition, Publisher: McGraw Hill Education.
- Technical Committee CENELEC TC9X, electrical and electronic applications in railways, “EN 50126-1: Generic RAMS process”, 2019, CENLEC



32
Dr. Neeraj Kumar Goyal
Indian Institute of Technology Kharagpur

There can be residual risk when designing a system. We develop control measures to reduce the risk, and this residual risk becomes the factor by which we decide whether the system will continue to run. In risk analysis, we use all available information to identify hazards and estimate risks, and then we use the analysis results to determine whether the system should be allowed to run.

Risk-based approaches are used in various contexts, including for economic purposes. In terms of safety, we use risk-based approaches to ensure that products, processes, and systems are safe, considering all hazards and associated risks. This complete process is called probabilistic risk assessment, which includes various subjects. More details can be found by following this approach.

In future lectures, we will discuss reliability, availability, and maintainability, with a focus on reliability. We have used the following references in preparing these lectures. Thank you.