# CE 400 / CE 500

## Process Safety Management

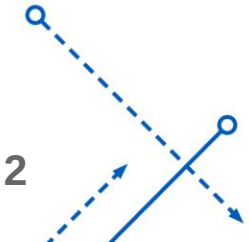
## Lecture 24 Determining Frequency of Events

## Instructor: David Courtemanche

University at Buffalo
Department of Chemical and Biological Engineering
School of Engineering and Applied Sciences

# Frequency Calculations in Hazards Analysis

- What-If/HAZOP/FMEA studies do not usually get into probability calculations
  - Team judgment is usually sufficient for less serious consequences
- For the highest Consequence Levels one needs to demonstrate extremely low frequencies
- When an Interlock is used as a safeguard calculations are required to demonstrate that the interlock has a sufficient reliability to achieve the desired Risk Level



# Reliability and Probability of Failure

- When looking at various incidents it is often the case that the initiating event is the failure of particular component of equipment
- In the last lecture we were introduced to the Poisson Distribution
  - We were looking at it as expressed in discrete events
  - Today we will look at it as a continuous function
- **Reliability** – $\boldsymbol{R(t)}$ is the probability that the component will NOT failure during the time interval between time $\mathbf{0}$ through time $\boldsymbol{t}$

$$\boldsymbol{R(t) = e^{-\mu t}}$$

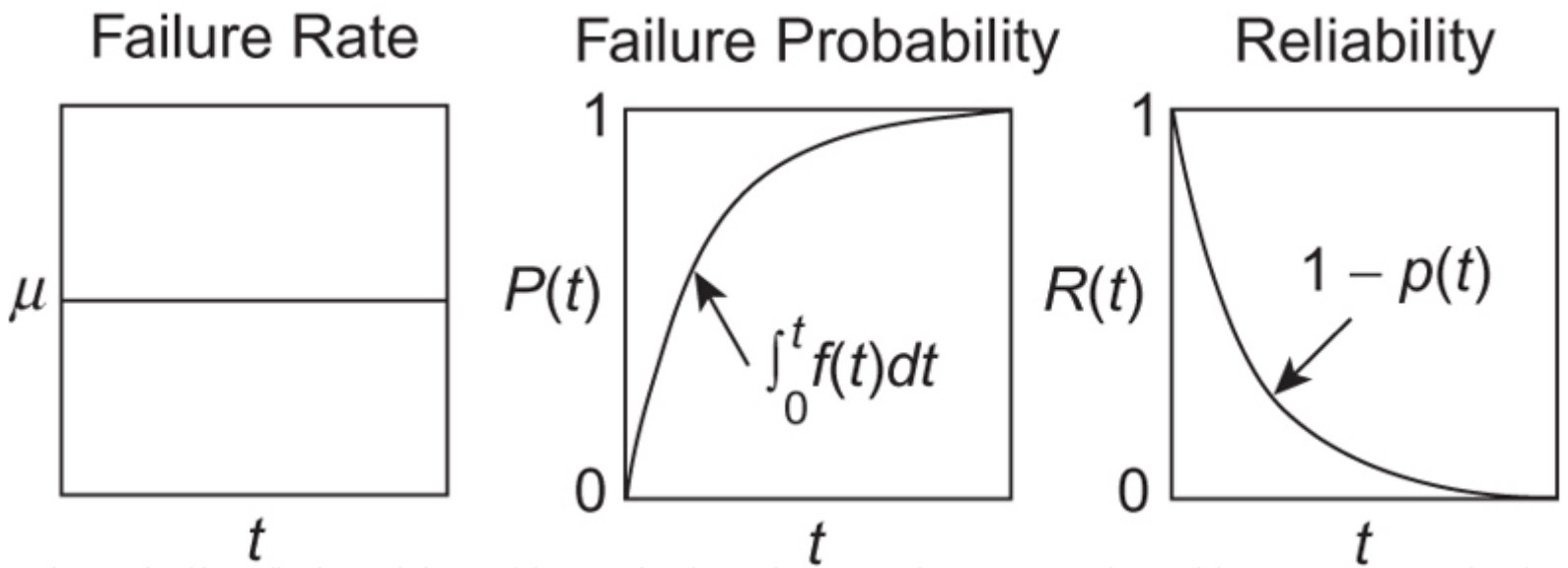
- where $\boldsymbol{\mu}$ is average failure rate for that component with units of faults/time
- As $\boldsymbol{t \to \infty}$, $\boldsymbol{R(t) \to 0}$, indicating that eventually everything fails

# Probability of Failure

- Failure Probability is the complement of Reliability
  - If an article has not failed, then it is still reliable
  - Therefore, the Probability of Failure is:

$$P(t) = 1 - R(t) = 1 - e^{-\mu t}$$

- Wait long enough and Probability of Failure goes to 1
- The question is – What is the time frame?



# Failure Rates

- The equations and graphs on the previous slide presume that $\mu$ is a constant value
- That is not always the case

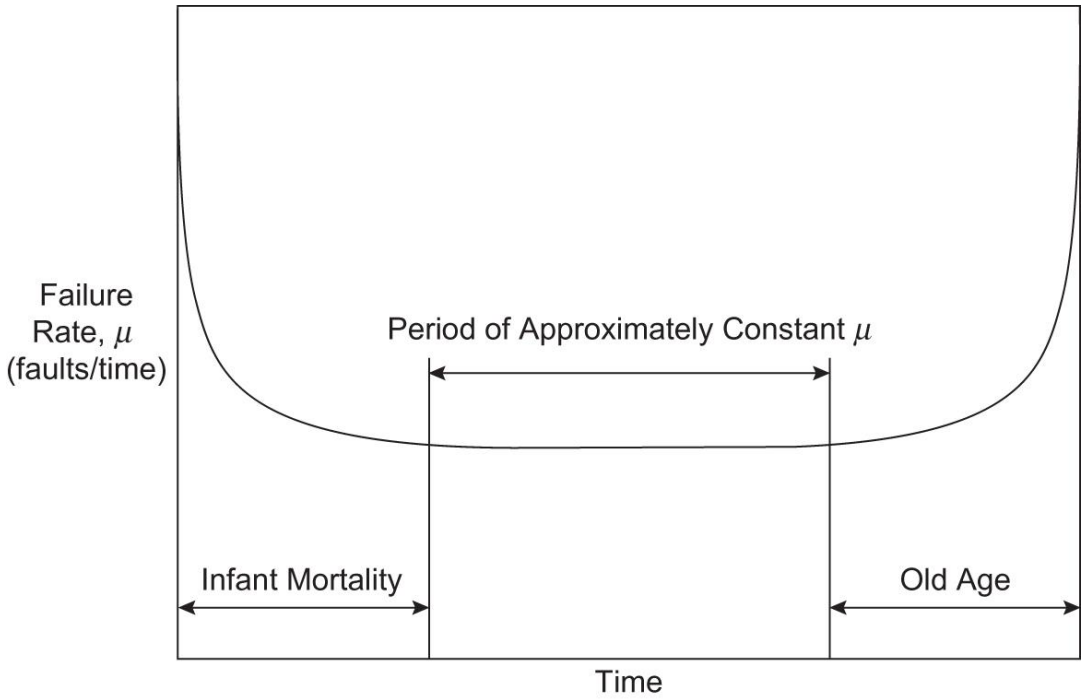



Figure 12-2 A typical bathtub failure rate curve for process hardware. The failure rate is approximately constant over the midlife of the component.

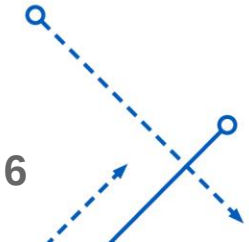
# Mean Time Between Failures

# MTBF

- The time interval between two failures is

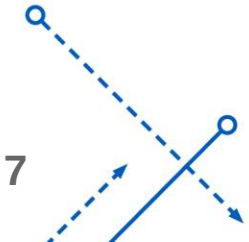
$$MTBF = \frac{1}{\mu}$$

- Where $\boldsymbol{\mu}$ is the failure rate and is a constant value



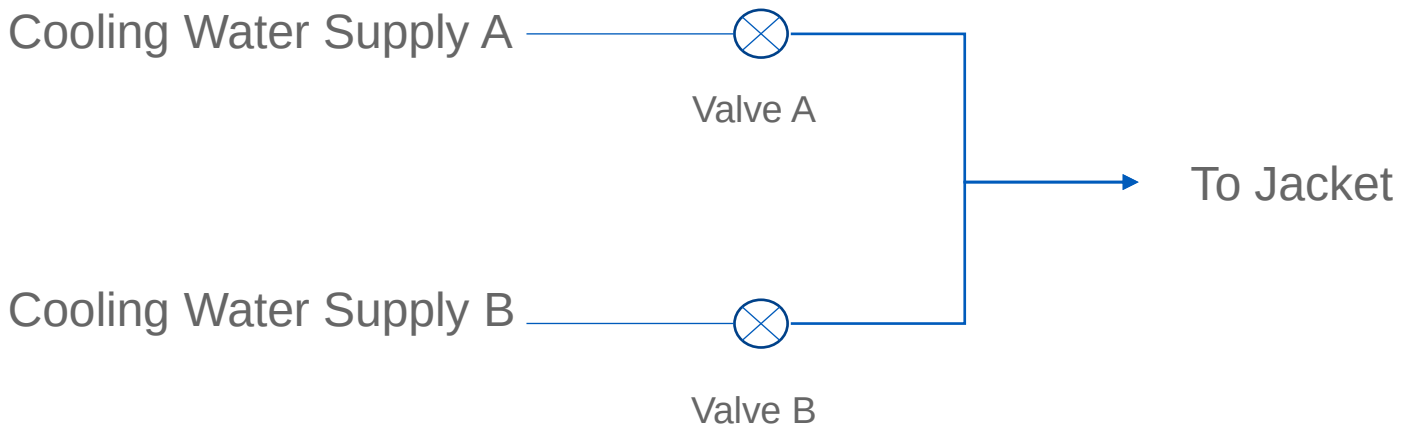
# Multiple Failures Required

- As we can see from the previous slides, one has to assume that a given component will fail at some point
- If the consequence of that failure is low then we may choose to live with the fact that it will happen with some relatively high frequency
- If the consequence of that failure is higher then we will need to design our process such that a single failure does not lead to any catastrophic events
  - For example we may have our process set up so that loss of some chemical flow will not lead to dangerous conditions as long as we have the designed cooling water flow rate
  - Now there are two failure modes required to lead to an unacceptable consequence



# Interactions Between Process Units – Parallel Interaction

- A well designed process won't suffer high consequence events unless there are multiple failures – if any of them work as designed, the event will not occur
- In this case simultaneous failures must occur – all $n$ components must fail for the event to occur
- This is represented by the Intersection of the two (or more) events




- Both Valve A ***and*** Valve B must be closed (failure) to prevent flow (undesired event)
- If ***either*** of them are open we will have flow (desired condition)

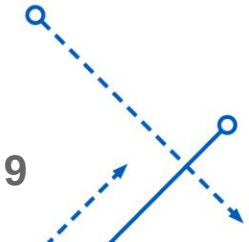
# Interactions Between Process Units – Parallel Interaction

- The parallel structure is represented by the logical **AND** function
- The probability of the undesired event is given by multiplying the probability of the required simultaneous failures (assuming the various failures are independent of one another)

$$P = \prod_{i=1}^{n} P_i$$

- The reliability (i.e. how likely it is that the undesired event does NOT happen) is expressed as:

$$R = 1 - \prod_{i=1}^{n} (1 - R_i)$$



# Interactions Between Process Units – Series Interaction

- Some parts of a design rely on ALL components performing in order for the system to work
  - There are two flows and if we lose either one then the undesired consequence occurs
- In this case a failure of ANY of the $n$ components causes the event to occur
- Put another way: ALL $n$ components must work in order to avoid the event
- This is represented by the Union of the two (or more) events


- If ***either*** valve is closed (failure) we lose flow (undesired event)
- Both valves must be open to have flow (desired condition)

# Interactions Between Process Units – Series Interaction


- The series structure is represented by the logical **OR** function
- The probability of AVOIDING the undesired event is given by multiplying the reliability of the required components (assuming the various failures are independent of one another)

$$R = \prod_{i=1}^{n} R_i$$

- The probability of the undesired event is given as:

$$P = 1 - \prod_{i=1}^{n} (1 - P_i)$$

# Interactions Between Process Units – Series Interaction


- The probability of the undesired event is given as:

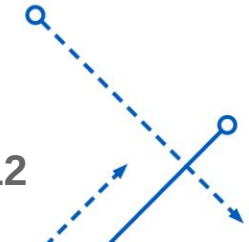
$$P = 1 - \prod_{i=A}^{B}(1 - P_i) = 1 - [(1 - P_A) * (1 - P_B)] = P_A + P_B - P_A * P_B$$

- The term $P_A * P_B$ is the term for cases where both valves have failed or the intersection term, $P(E1 \cap E2)$ from our last lecture.
  - We don't fail any worse for the case where both valves are closed…
- If the probabilities are small then the term $P_A * P_B$ is negliglible and the probability reduces to:

$$P = P_A + P_B$$

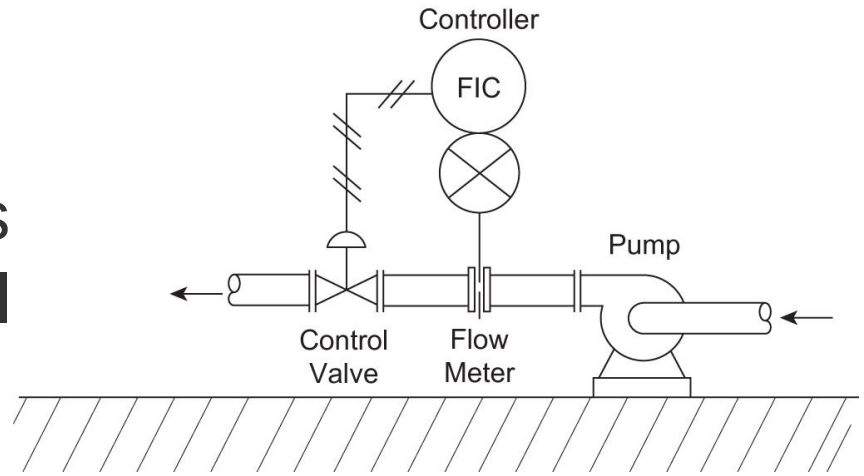
- This result is generalized to the following:

$$P = \sum_{i=1}^{n} P_i$$



## Series Example

- Flow Control System
  - Flow is measured by flow meter
  - Controller receives signal and calculates what output is appropriate for the control valve
  - Control valve throttles the flow to the desired flow rate
- If any of these components fail, the control system fails – Series Linkage




| Component | Failure rate $\mu$ (faults/yr) | Reliability $R = e^{-\mu t}$ | Failure probability $P = 1 - R$ |
|---|---|---|---|
| Control valve | 0.60 | 0.55 | 0.45 |
| Controller | 0.29 | 0.75 | 0.25 |
| DP cell | 1.41 | 0.24 | 0.76 |

# Series Example

- The reliability of this control system is given by $\boldsymbol{R = \prod_{i=1}^{n} R_i = 0.55 * 0.75 * 0.24 = 0.10}$
- The failure probability is $\boldsymbol{P = 1 - R = 1 - 0.10 = 0.90}$.
  - 90% chance of a failure in one year of operation
- Overall Failure Rate can be computed using the following definition:

$$\boldsymbol{R(t) = e^{-\mu t}}$$
$$\boldsymbol{0.10 = e^{-\mu * 1}}$$
$$\boldsymbol{\ln 0.10 = -\mu}$$

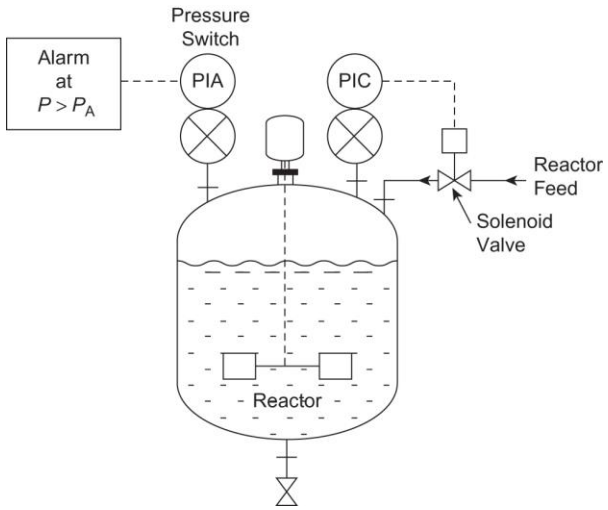
$\boldsymbol{\mu = 2.30}$ failures per year

- The mean time between failures is:
  - $\boldsymbol{MTBF = \frac{1}{\mu} = \frac{1}{2.30\ per\ year} = 0.43\ year}$

| Component | Failure rate $\mu$ (faults/yr) | Reliability $R = e^{-\mu t}$ | Failure probability $P = 1 - R$ |
|---|---|---|---|
| Control valve | 0.60 | 0.55 | 0.45 |
| Controller | 0.29 | 0.75 | 0.25 |
| DP cell | 1.41 | 0.24 | 0.76 |

# Parallel Example

- Reactor System with parallel pressure safety systems
- System 1 has a pressure switch which turns on an alarm light
  - This analysis assumes that operators will respond successfully to shut off the reactor
- System 2 has a pressure switch which shuts off a solenoid valve
  - The valve shuts off feed of the reactant to the reactor
- Data for the components are given in table




| Component | Failure rate $\mu$ (faults/yr) | Reliability $R = e^{-\mu t}$ | Failure probability $P = 1 - R$ |
|---|---|---|---|
| 1. Pressure switch 1 | 0.14 | 0.87 | 0.13 |
| 2. Alarm indicator | 0.044 | 0.96 | 0.04 |
| 3. Pressure switch 2 | 0.14 | 0.87 | 0.13 |
| 4. Solenoid valve | 0.42 | 0.66 | 0.34 |

Figure 12-5 A chemical reactor with an alarm and an inlet feed solenoid valve. The alarm and feed shutdown systems are linked in parallel.

# Parallel Example

- Both systems have components in series (i.e. all of the components must function in order for the system to be successful)
- The two systems work in parallel (i.e. as long as one or the other is successful we will avoid overpressurizing the reactor)
- System 1
  - The pressure switch and alarm light must both work in series
  - The reliability of this control system is given by $\boldsymbol{R = \prod_{i=1}^{n} R_i = 0.87 * 0.96 = 0.835}$
  - The failure probability is $\boldsymbol{P_1 = 1 - R = 1 - 0.835 = 0.165}$.
- System 2
  - The pressure switch and solenoid valve must both work in series
  - The reliability of this control system is given by $\boldsymbol{R = \prod_{i=1}^{n} R_i = 0.87 * 0.66 = 0.574}$
  - The failure probability is $\boldsymbol{P_2 = 1 - R = 1 - 0.574 = 0.426}$.

# Parallel Example

- The two systems work in parallel, so the following analysis applies:
  - Probability of Failure in one year -

$$P = \prod_{i=1}^{2} P_i = P_1 * P_2 = 0.165 * 0.426 = 0.070$$

  - Reliability for one year of operation -

$$R = 1 - P = 1 - 0.070 = 0.930$$

  - Overall Railure Rate –

$$\mu = -\ln R = -ln\, 0.930 = 0.073 \text{ faults in one year}$$

  - Mean Time Between Failure –

$$MTBF = \frac{1}{\mu} = \frac{1}{0.073} = 13.7 \text{ years}$$

- The parallel nature of the using two separate systems greatly improves the reliability
- Note that these figures are for the safety systems themselves
  - The systems may not be challenged and the actual probability of overpressuring reactor is likely to be much smaller