

054402 Design and Analysis



LECTURE 13: HAZARD ANALYSIS (HAZAN)

Daniel R. Lewin
Department of Chemical Engineering
Technion, Haifa, Israel

1

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

OUTLINE

This lecture covers Hazard Analysis (HAZAN) otherwise referred to as Quantitative Risk Assessment (QRA).

HAZAN/QRA is a technique for estimating the probability and consequences of a hazard.

More specifically we shall:

- ☆ Provide motivation for performing a HAZAN on a process.
- ☆ HAZAN: How often ? How big ? So what ?
- ☆ Provide an overview of the tools that are commonly used in HAZAN:
 - Computation of how often hazards can be expected
 - Construction of fault trees to analyze the combination of events leading to hazards

Source: T. Kletz, *HAZOP and HAZAN*, 3rd Ed., IChemE (1992)

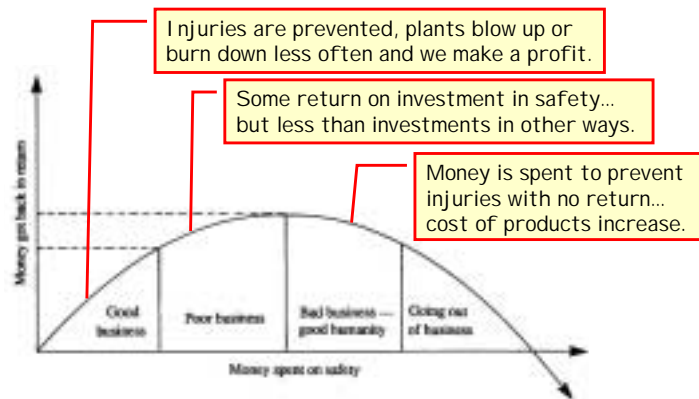
2

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

THE COST OF SAFE MANUFACTURING ?

Clearly, spending money on safety is justified so long as the investment pays for itself in terms of increased profitability and loss prevention.



3

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

STAGES OF HAZAN

Every hazard analysis consists of three steps:

- ❶ Estimating **HOW OFTEN** the incident will occur.
- ❷ Estimating the consequences (**HOW BIG?**) to
 - Employees
 - The public and the environment
 - Plant and profits
- ❸ Comparing the results of ❶ and ❷ with a target or criterion to decide whether or not action to reduce the probability of occurrence or minimize the consequences is desirable, or whether the hazard can be ignored, at least for the time being (**SO WHAT?**).

In this introduction to HAZAN, we will discuss step ❸ first and then learn how to estimate how often hazards occur (❶) in more detail. Estimating ❷ is beyond the scope of this lecture.


4

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

RISKS IN INDUSTRY AND AT LARGE		
Activity	FAR ⁺	Risk per person per year
Oil exploration	82	165×10^{-5}
Construction	67	134×10^{-5}
Coal mining	40	80×10^{-5}
Chemicals	4	8×10^{-5}
Staying at home	3	6×10^{-5}
Car travel	17	34×10^{-5}
Smoking (pack/d)	40	80×10^{-5}
All risks, age 20	50	100×10^{-5}

*FAR - Fatal Accident Rate.
FAR = number of fatalities per 1000 workers in a working lifetime (10^8 hrs)



5

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

SETTING SAFETY TARGETS		
A FAR of 4 implies 0.4 incidents per 10^8 hrs.		
The hazard (or incident) rate is the rate at which dangerous incidents occur. Suppose the person at risk is killed every time the dangerous incident occurs (not typical), then it must occur more often than:		
0.4 incidents in 10^8 working hours or		
once in 2.5×10^8 working hours		
= 30,000 years (i.e. hazard rate, $H = 3 \times 10^{-5}/\text{year}$)		
If a person is killed every 10 th time the incident occurs, the target hazard rate is $H = 3 \times 10^{-4}/\text{year}$.		
<u>Thumb Rules:</u>	Safe	Grey Area
	$H < 10^{-5}/\text{year}$	$10^{-4} < H < 10^{-5}$
		Unsafe
		$H > 10^{-3}/\text{year}$

6

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

COMPUTING THE HAZARD RATE

Some definitions.

HAZARD RATE (H) - The rate (occasions/year) at which hazards occur: e.g., the rate at which the pressure of a vessel exceeds the design pressure.

PROTECTIVE SYSTEM - A device installed to prevent the hazard occurring: e.g., a relief valve or a high level trip.

TEST INTERVAL (T) - The time interval between the testing of a protective system, and its replacement if necessary.

DEMAND RATE (D) - The rate (occasions/year) at which a protective system is called to act.

FAILURE RATE (f) - The rate (occasions/year) at which a protective system develops faults (fail-danger/fail-safe).

7

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

COMPUTING THE HAZARD RATE (Cont'd)

Some definitions (Cont'd).

FRACTIONAL DEAD TIME (F_{DT}) - The fraction of the time that a protective system is inactive: $F_{DT} = 0.5fT$, assuming failure occurs half-way between tests.

A hazard results when a demand occurs during a dead period, hence: $H = D \times F_{DT}$.

If the protective system never fails to operate when required, $H = 0$.

If there is no protective system, $H = D$.

Example 1. Relief valves

Relief valves tests show that fail-danger faults occur at $f = 0.01/\text{year}$ (once in 100 years).

If $T = 1$ year, and say, $D = 1/\text{year}$, then $F_{DT} = 0.5 \times fT = 0.005/\text{year}$ (once in 200 years).

8

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

COMPUTING THE HAZARD RATE (Cont'd)

Example 2. Simple trips

Assume that:

1. Fail-danger faults develop at $f = 0.5/\text{year}$ (once every two years)
2. Test interval $T = 1$ week (0.02 year – rather frequent)
3. $D = 1/\text{year}$ (example)

Compute the hazard rate.

Solution:

Testing once a week: $F_{DT} = 0.5 \times fT = 0.005$

$$H = D \times F_{DT} = 0.005/\text{year} \text{ (1 in 200 years)}$$

Testing once a month: $F_{DT} = 0.02$ (four times the above)

$$H = D \times F_{DT} = 0.02/\text{year} \text{ (1 in 50 years)}$$

Testing once a year: $F_{DT} = 0.25$ (12 times the above)

$$H = D \times F_{DT} = 0.25/\text{year} \text{ (1 in 4 years)}$$

9

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

COMPUTING THE HAZARD RATE (Cont'd)

Example 3. Frequent demands on a trip

Assuming that:

1. Fail-danger faults develop at $f = 0.5/\text{year}$ (once every two years)
2. Test interval $T = 0.1$ year (5 weeks, a typical value)
3. $D = 100/\text{year}$ (much greater than before)

Compute the hazard rate.

Solution:

$$\begin{aligned} \text{Using the formula: } H &= D \times F_{DT} = D \times 0.5fT = 100 \times 0.5 \times 0.5 \times 0.1 \\ &= 2.5/\text{year} \end{aligned}$$

In fact, $H \cong 0.5/\text{year}$, because:

- There will always be a demand in the dead period
- The fault will be disclosed and repaired. 2.5/year would be the right answer if we did not repair the trip after the hazard occurred but left it in a failed state until the next test is due.

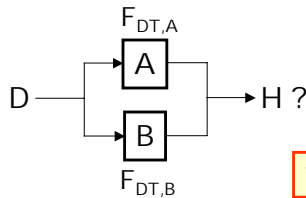
10

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

COMPUTING THE HAZARD RATE (Cont'd)

Two Protective Systems in Parallel.

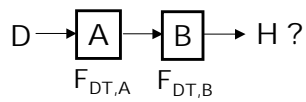


The system fails if both A and B fail.
 Assume that A (arbitrarily) responds first:

- The demand rate on A is D.
- The demand rate on B is $DF_{DT,A}$
- Thus, $H = DF_{DT,A}F_{DT,B}$

Thus, F_{DT} 's MULTIPLY in parallel systems.

Two Protective Systems in Series.



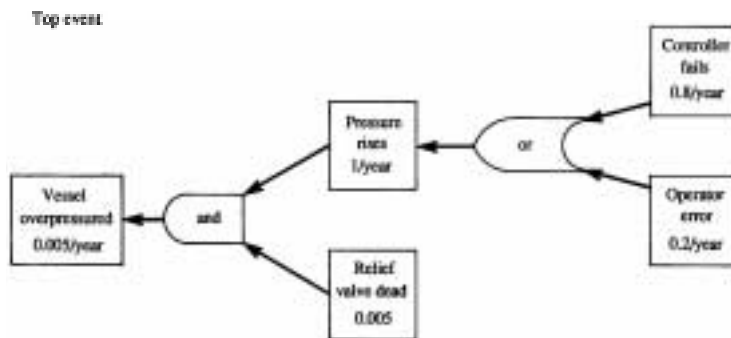
The system fails if either A or B fail.

- The hazard rate for this case is:
 $H = D(F_{DT,A} + F_{DT,B})$

Thus, F_{DT} 's ADD in series systems.

FAULT TREES

These are widely used in hazard analysis to investigate the combinations of events that lead to hazards. They assist in estimating the probability that the hazard event occurs.



FAULT TREES - CLASS EXERCISE

As an exercise, draw a fault tree to describe the failure of a car to start.

```
graph TD; A[Car fails to start] --- B{or}; B --- C[Fault in car]; B --- D[Incorrect procedure];
```

13

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

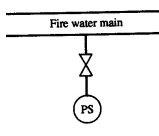
FAULT TREES - CLASS EXERCISE

14

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

PROTECTION SYSTEM REDUNDANCY



$$D \rightarrow A \rightarrow B \rightarrow H$$

$$D = 10, f_A = 0.6, f_B = 0.2, T = 0.1$$

$$F_{DT,A} = 0.5 \times 0.6 \times 0.1 = 0.03$$

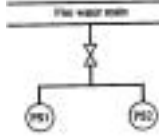
$$F_{DT,B} = 0.5 \times 0.2 \times 0.1 = 0.01$$

$$H = D(F_{DT,A} + F_{DT,B})$$

$$= 10 \times (0.03 + 0.01)$$

$$= 0.4/\text{year}$$

$$= \text{Once}/2.5 \text{ years}$$



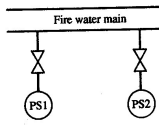
$$D \rightarrow A \rightarrow \begin{matrix} B \\ B \end{matrix} \rightarrow H$$

$$H = D(F_{DT,A} + (F_{DT,B})^2)$$

$$= 10 \times (0.03 + 0.0001)$$

$$= 0.30/\text{year}$$

$$= \text{Once}/3.3 \text{ years}$$



$$D \rightarrow \begin{matrix} A \\ A \end{matrix} \rightarrow \begin{matrix} B \\ B \end{matrix} \rightarrow H$$

$$H = D((F_{DT,A} + F_{DT,B})^2)$$

$$= 10 \times (0.03 + 0.01)^2$$

$$= 0.016/\text{year}$$

$$= \text{Once}/62 \text{ years}$$

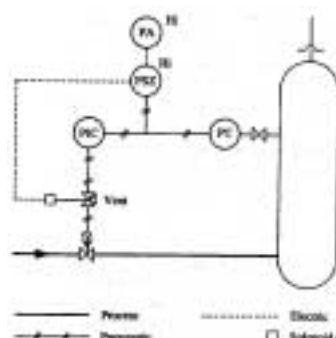
15

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

WHAT IS WRONG WITH THIS TRIP SYSTEM?

The pressure in the vessel is measured by a PT and controlled by a PIC, which adjusts the motor valve setting. If the PIC fails and the pressure rises above the set point, the PSZ^{Hi} operates to close the motor valve. At the same time, the PA^{Hi} operates.



The trip system is almost useless. The most likely causes of high pressure are:

- ❶ Failure of the PT or a blockage of the line.
- ❷ Motor valve sticks open.
- ❸ Failure of the PIC. In this case the trip will work.

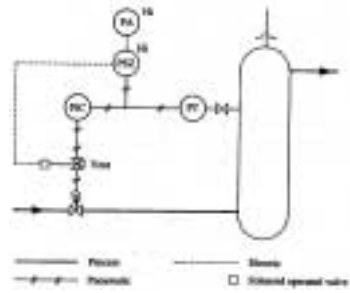
❸ is less likely than ❶ or ❷. At best the system will work in a third of the cases.

16

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

HAZARD ANALYSIS OF TRIP SYSTEM 1



$D \rightarrow [V] \rightarrow [PT] \rightarrow \begin{cases} [PSZ] \\ [PIC] \end{cases} \rightarrow [MV] \rightarrow H$

$f_V = 0.5, f_{PT} = 0.1, f_{PSZ} = 0.1, f_{PIC} = 0.3,$
 $f_{MV} = 0.5, T = 0.1, D = 10.$

$F_{DT,V} = 0.5 \times 0.5 \times 0.1 = 0.025$
 $F_{DT,PT} = 0.5 \times 0.1 \times 0.1 = 0.005$
 $F_{DT,PSZ} = 0.5 \times 0.1 \times 0.1 = 0.005$
 $F_{DT,PIC} = 0.5 \times 0.3 \times 0.1 = 0.015$
 $F_{DT,MV} = 0.5 \times 0.5 \times 0.1 = 0.025$

$H = D(F_{DT,V} + F_{DT,PT} + F_{DT,PSZ} + F_{DT,PIC} + F_{DT,MV})$
 $= 0.55/\text{year or once}/1.8 \text{ years}$

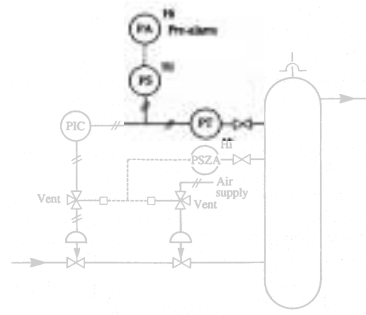
17

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

MODIFIED TRIP SYSTEM

The modified system is much more reliable:

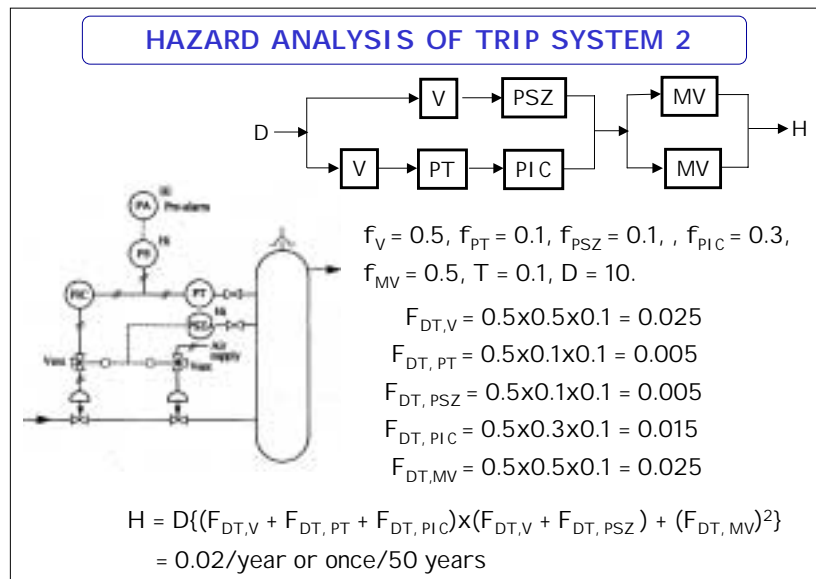


- ❶ The PSZA^{Hi} has an independent connection to the vessel, and operates a separate motor valve.
- ❷ A cross-connection to the control valve allows for a back-up.
- ❸ A PS^{Hi} and pre-alarm PA^{Hi} warn the operator in advance of the trip.

18

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN



19

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN

SUMMARY

After completing this part of the course, you should:

- ☆ Be able to describe the main purpose of HAZAN to a layman
 - How often?
 - How big?
 - So what?
- ☆ Be able to construct a fault tree that describes how a specific hazard can occur.
- ☆ Be able to compute the hazard rate, given information about the reliability of the components of a protective system, the demand rate and the testing frequency.
- ☆ Be able to do a "reality check" on the above calculation.
- ☆ Be able to suggest ways of increasing the reliability of protective systems to meet a target safety level.

20

DESIGN AND ANALYSIS - (c) Daniel R. Lewin

13 - HAZAN