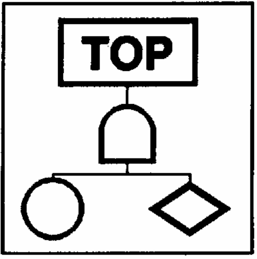
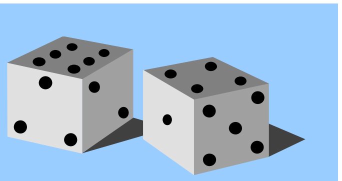




FAULT TREE ANALYSIS

Colin S. ‘Chip’ Howat Ph.D.

Kurata Thermodynamics Laboratory
Department of Chemical & Petroleum Engineering
University of Kansas

Introduction to Fault Tree Analysis
in
Risk Assessment

Lecture: *Three Class Periods*

Title: *Introduction to Fault Tree Analysis*

Thoughts: *It is good to have an end to journey toward; but it is the journey that matters, in the end.*

Ursula K. LeGuin

The journey is the reward.

Chinese Saying

Question: *Congress has considered and will consider again using risk assessment to evaluate the suitability of regulations governing safety and environment. Given what you know about the uncertainties associated with risk evaluation, is this a suitable tool for governing?*

Purpose: *Introduce Fault Tree Analysis*
Continue Scenario Path Development

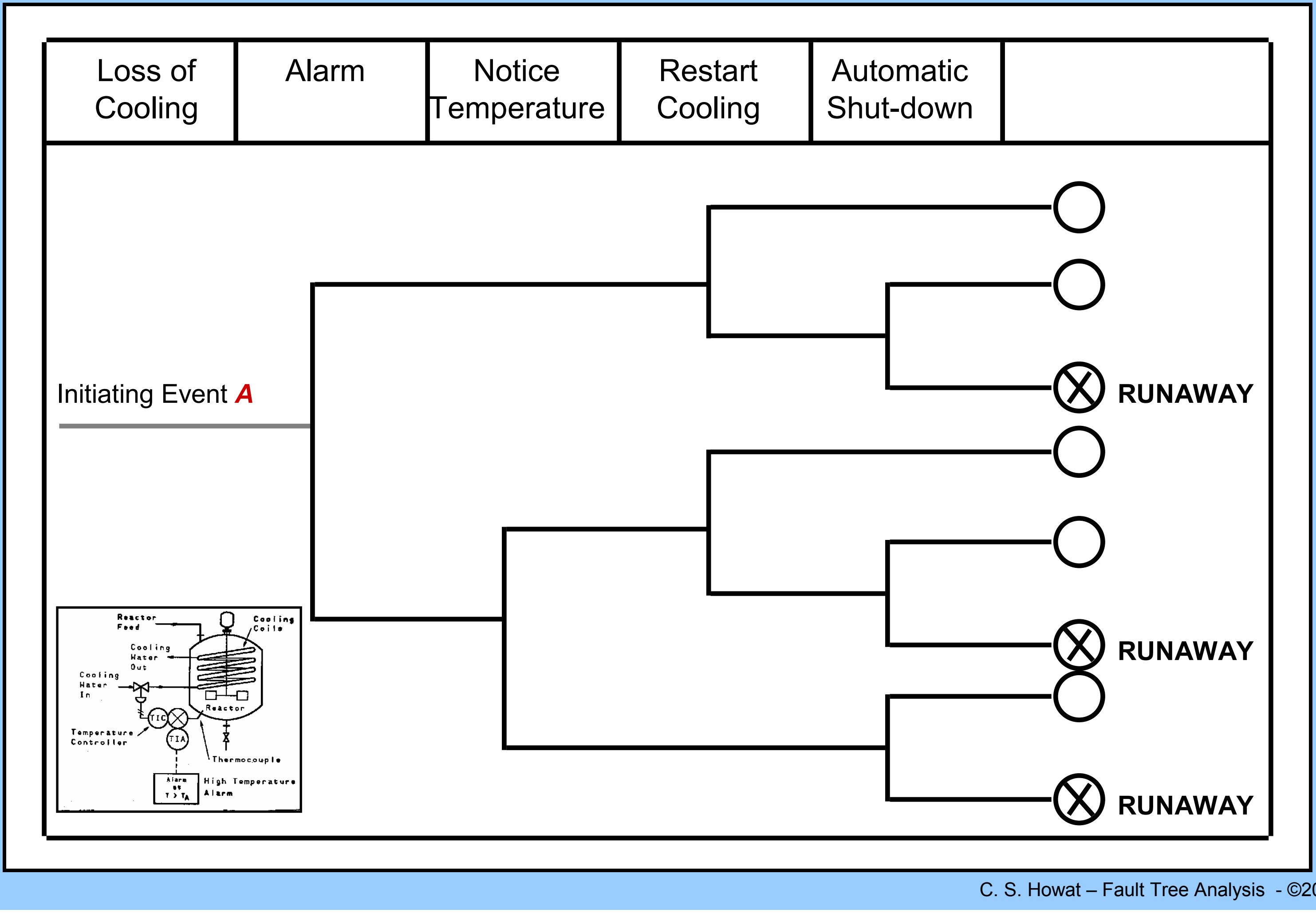
The architects . . . who relied only upon theories and scholarship were obviously hunting the shadow, not the substance.

Vitruvius, Book 1
Ten Books of Architecture

It is not the same to talk of bulls as to be in the bullring.

Spanish Proverb

This is the Event Tree which we developed in class to represent the '**Loss of Cooling**' for the simple reactor system. The question is, is this all possible routes to the runaway reactor event? The Event Tree does not tell us this.



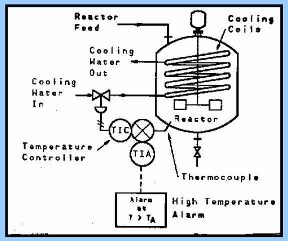
Loss of Cooling	Alarm	Notice Temperature	Restart Cooling	Automatic Shut-down	

Event Tree Analysis

This is an inductive procedure which shows all possible outcomes resulting from an initiating event, e.g. equipment failure or human error.

In the example, the initiating event was the loss of cooling.

What other possibilities are there for arriving at a runaway condition?

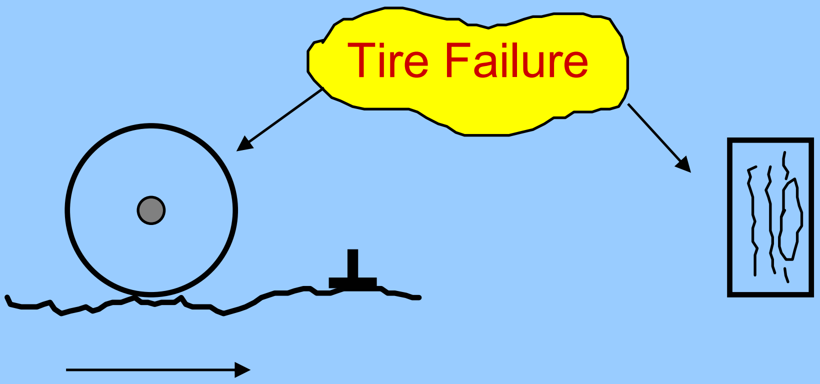


Example

In order to determine the Risk, we need the frequency. For the Simple Reactor Problem, we need to determine the frequency of all runaway situations. For this, we need all possible paths to runaway.

Consider an example of a flat tire. What is the frequency that this will occur?

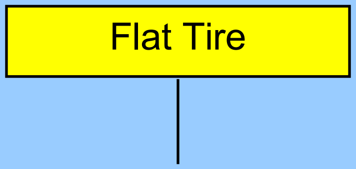
In order to answer this and other questions, we need to recognize that the accident can be a sequence of events, each of which has its own frequency.



Tire Failure

Introduction to Fault Tree Analysis

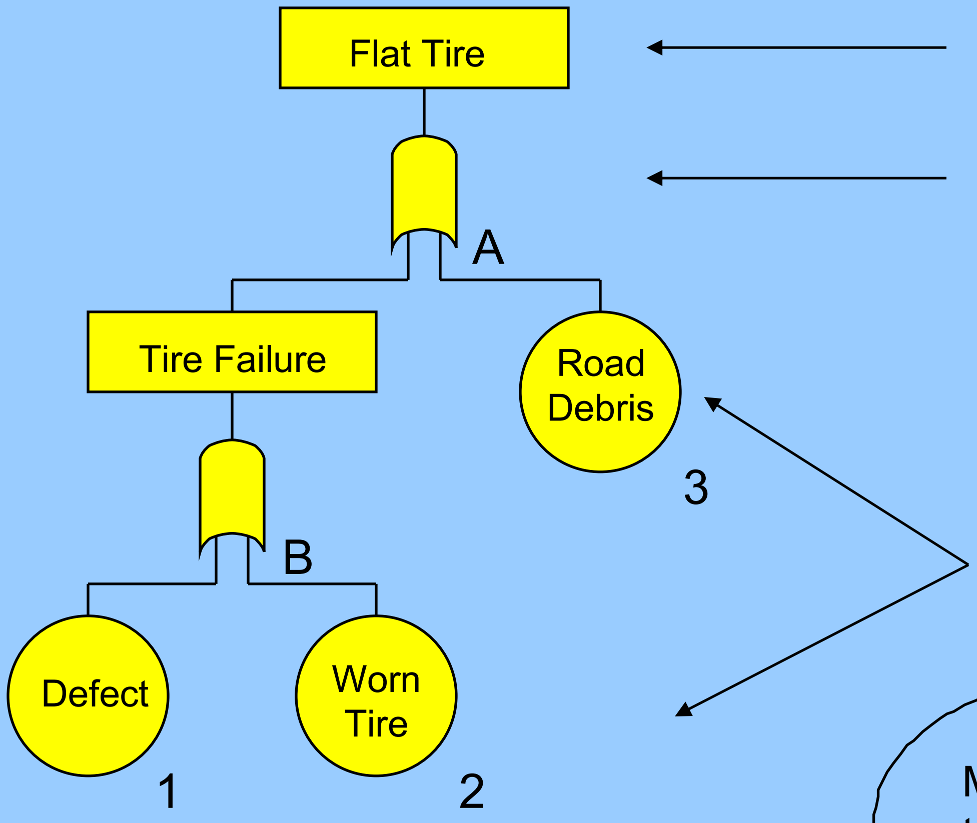
Suppose that the Flat Tire is the terminating (*top?*) event. How might we represent this?



Flat Tire

Fault Tree Analysis is used to find all possible causes of an event.

Fault Tree Representation of Flat Tire



Top Event

Logic Gate

Basic Event

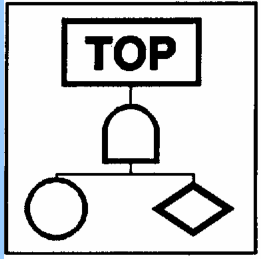
Minimum Cut Sets

~~A~~ 3

~~B~~ 1

2

Minimum Sequence of Steps to Cause Top Event from Basic Events



Fault Tree Analysis

This is a deductive technique focusing on on particular event or consequence.

The purpose is to identify all scenarios, i.e. initiating events that lead to this consequence. In LOPA we call a scenario a cause/consequence pair. A completed fault tree shows many scenarios, all with the same consequence.

HazOp might have been used to discover this event.

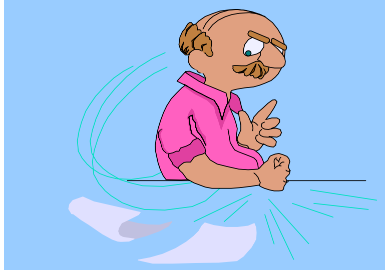
This method uses logic gates to determine the combination of equipment failures and human errors which lead to the event. The minimum number is determined (minimum cut sets).

~Pr(x)

Detailed understanding of how plant functions, detailed process drawings and procedures, knowledge of failure modes and their effects.

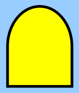
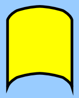
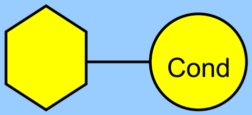
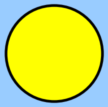
<u>Fault Tree Analysis</u>

Strengths -	Systematic Minimal Cut Sets
Weaknesses -	Complete understanding required Very Large Trees developed Trees not unique

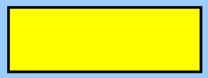


Education research indicates that engineers tend to be inductive. That is, engineers prefer to go from the specific to general. A deductive approach is from the general to specific. The primary weakness of fault tree analysis is that it is <u>deductive</u> in its approach to Hazard Evaluation. The analyst must see the whole picture.

Symbols Used in Fault Tree Analysis

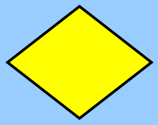
	The resulting output event requires the simultaneous occurrence of all input events.	AND Gate
	The resulting output event requires the occurrence of any individual input event..	OR Gate
	The output event will occur if the input occurs and inhibit event occurs.	INHIBIT Event
	A fault event that needs no further definition.	BASIC Event

Symbols Used in Fault Tree Analysis (cont.)



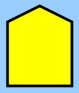
An event that results due to the interaction of a number of other events.

INTERMEDIATE Event



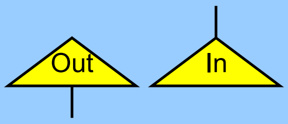
An event that cannot be developed further due to lack of suitable information.

UNDEVELOPED Event



An event that is a boundary condition to the fault tree.

EXTERNAL Event



Use to transfer the fault tree in and out of a sheet of paper.

TRANSFER Symbol

Fault Tree Rules

1. State what, where, when fault is.

    Define Top Event.
    Define Existing Events.
    Define Unallowed Events.
    Define the Physical Bounds of the Analysis.
    Define the Equipment Configurations.
    Define the Level of Resolution.

    Critical!

2. Ask whether this fault can be caused by equipment failure.

3. No miracles are allowed.

    If Normal Operation propagates a fault, then assume Normal Operation.

4. Complete the gate.

    All inputs to a Gate must be defined before going to the next Gate.

5. No Gate to Gate connections are allowed.

    Input to gates should be a fault.

Fault Tree Resolution *(Determining Minimum Cut Sets)*

1. Uniquely Identify Gates and Basic Events.

   Gates are identified with letters.
   Basic Events are identified with numbers.

2. Resolve all Gates into Basic Events.

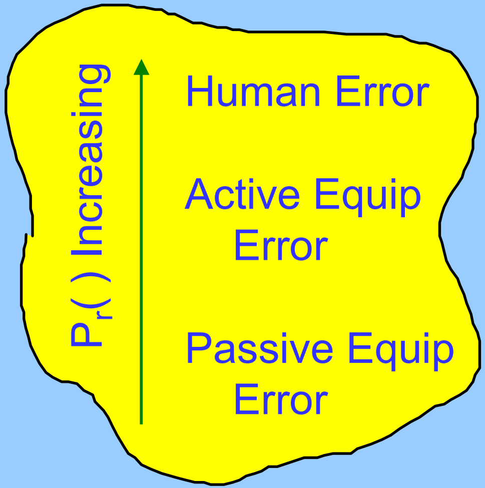
3. Remove duplicate Events within a set.

4. Delete all supersets.

Or Gate forms new line in development. And Gate forms a new column. The resolution is complete when outcome is defined by Basic Events. See Flat Tire analysis for a simple example.

Estimating the Probability

Qualitative Probabilities can be used as an initial estimate of each sequence of events.



P_r( ) Increasing

Human Error

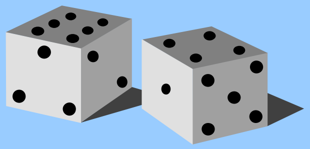
Active Equip Error

Passive Equip Error

Notes on Probability Estimation

$P_r(A \text{ and } B) = P_r(A)\ P_r(B)$

$P_r(A \text{ or } B) = P_r(A) + P_r(B) - P_r(A)\ P_r(B)$

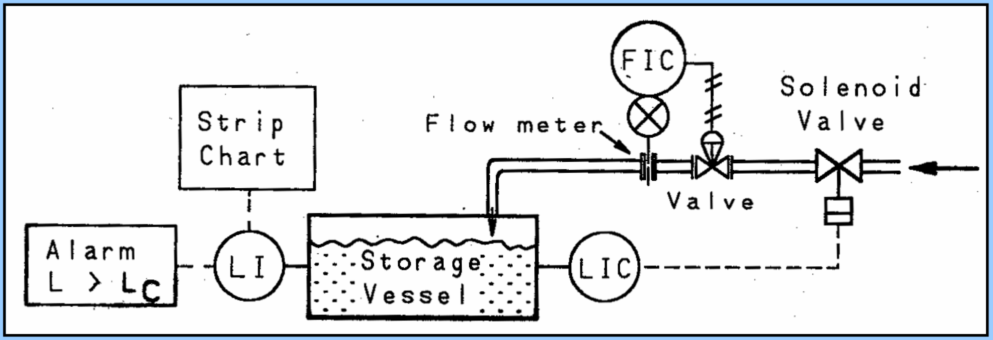


Of course, we know more probabilities than implied on this slide since we have covered LOPA and Event Tree.

Steps

Define	Top Event Existing Event Unallowed Events Physical Bounds Equipment Configurations Level of Resolution

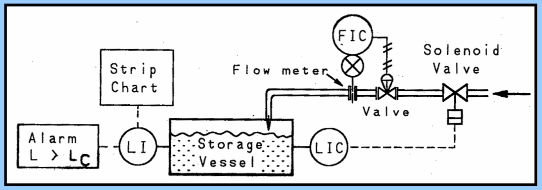
Example



Top Event:

Storage Tank Overflows

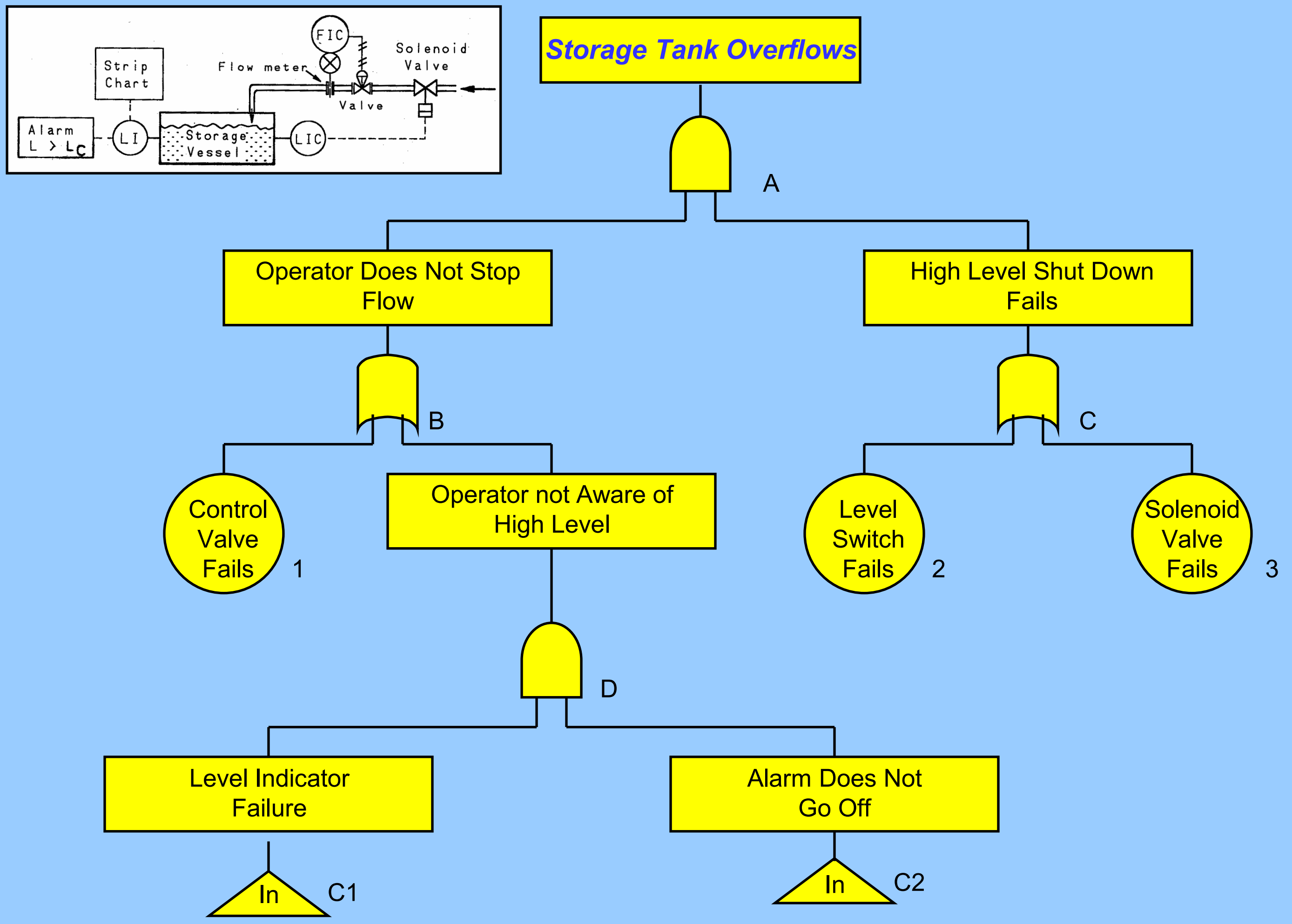
Introduction to Fault Tree Analysis



Storage Tank Overflows

What Next?

Introduction to Fault Tree Analysis



Storage Tank Overflows

Operator Does Not Stop Flow

High Level Shut Down Fails

Control Valve Fails

Operator not Aware of High Level

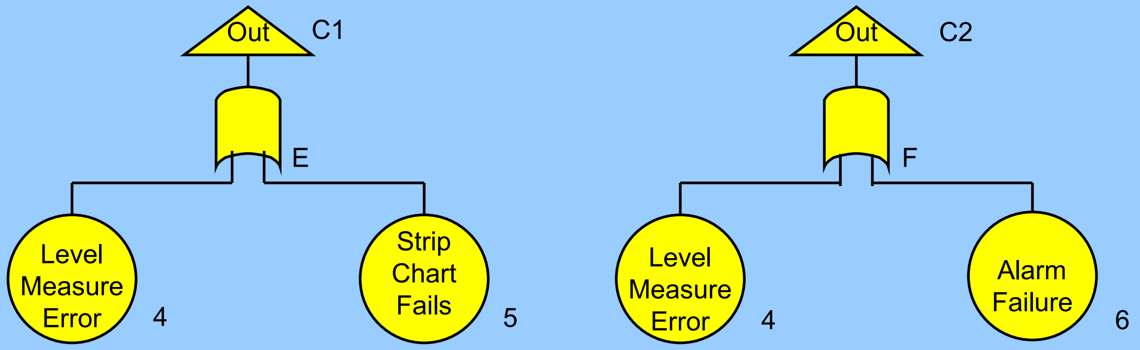
Level Switch Fails

Solenoid Valve Fails

Level Indicator Failure

Alarm Does Not Go Off

Introduction to Fault Tree Analysis



This completes the fault tree for the event of *storage tank overfills*.

Human error could be added if it were allowed. The addition point would be before the gate D, wouldn't it? What would the addition of Human Error look like?

Resolution of the Fault Tree Example

The resolution of the Fault Tree is to determine the most probable event leading to the top event.

A				
~~A~~	B	C		
	1	C		
	D	C		
	~~D~~	C	E	F
		C	4	F
		C	5	F
		C	4	4
		C	4	6
		C	5	4
		C	5	6
	1	2		
	1	3		
		2	4	4
		2	4	6
		2	5	4
		2	5	6
		3	4	4
		3	4	6
		3	5	4
		3	5	6

This process continues adding a new column for each ‘and’ gate. A new row is added for each ‘or’ gate.

This process continues until all gates are resolved into basic events.

Resolution of the Fault Tree Example

Can you prove that the minimum cut sets are:

1,2

1,3

2,4

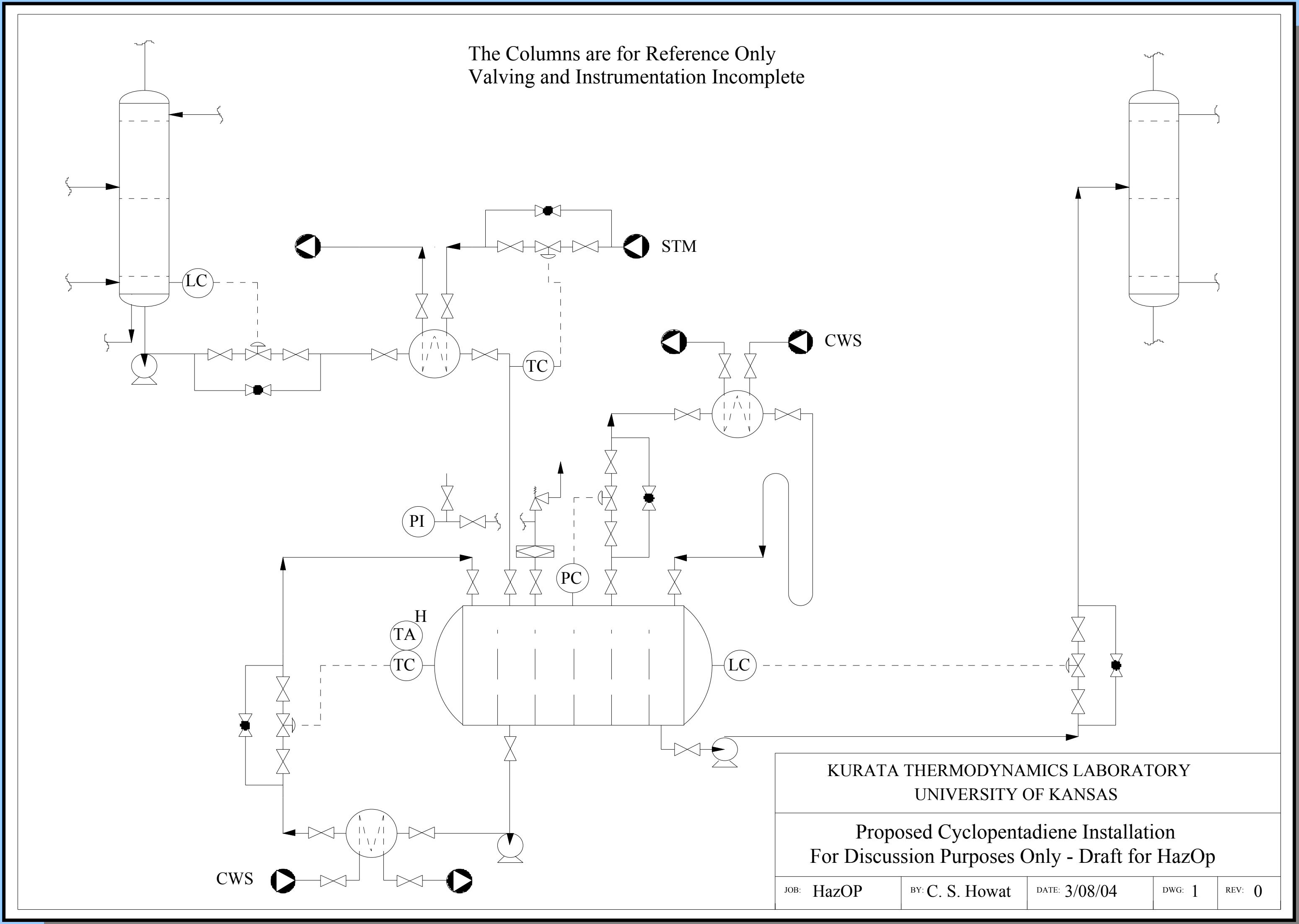
3,4

2,5,6

3,5,6

This is accomplished by removing all duplicate steps and by recognizing which sets contain supersets. That is those multiple steps which have as part of them some other minimum set.

Introduction to Fault Tree Analysis



The Columns are for Reference Only
Valving and Instrumentation Incomplete

KURATA THERMODYNAMICS LABORATORY
UNIVERSITY OF KANSAS

Proposed Cyclopentadiene Installation
For Discussion Purposes Only - Draft for HazOp

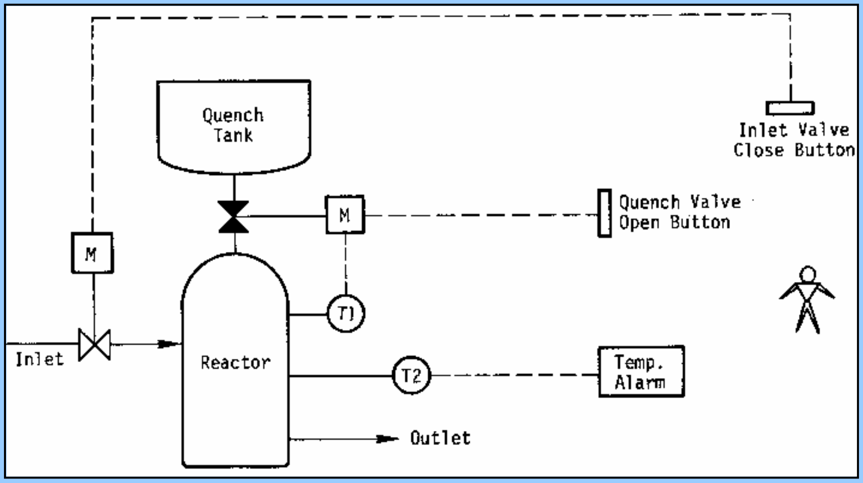
JOB: HazOP	BY: C. S. Howat	DATE: 3/08/04	DWG: 1	REV: 0

Fault Tree Example

Stable Condition reached if Quench Valve Opens adding material to reactor and Inlet Valve Closes

Top Event

Damage due to High Process Temperature



Top Event?

Existing Event?

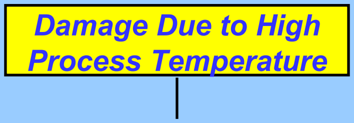
Unallowed Events?

Physical Bounds?

Equipment Considerations?

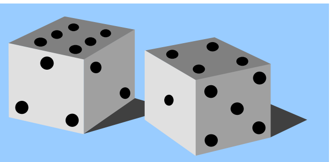
Level of Resolution?

Introduction to Fault Tree Analysis



Damage Due to High Process Temperature

What Next?



Conclusions

Fault Tree Analysis -- Deductive Approach to resolve Top Events into all possible initiating events. It is used to test the most probable sequence of events which lead to the undesirable top event. Probabilities of undesirable outcomes can be calculated with most probable outcome identified.

Five Rules to Fault Tree Analysis

1) Identify what, when, where fault occurs.

2) Ask whether fault can be caused by equipment failure.

3) No miracles are allowed.

4) Complete each gate.

5) No gate-to-gate connections are allowed.