Arthur D Little

Process Safety
Risk Assessment Training

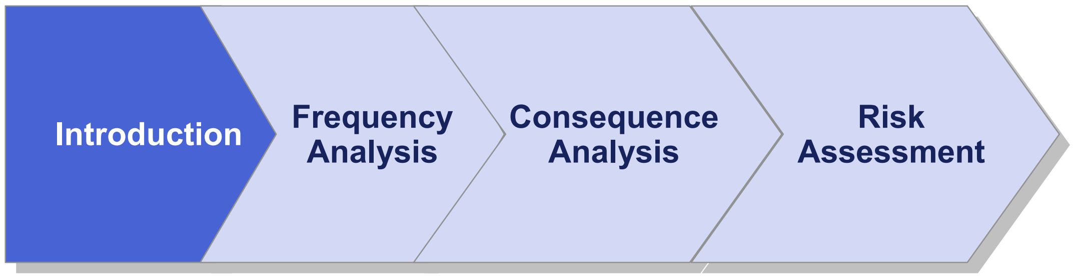
Presentation to

NPC Iran

June 2005

Arthur D. Little Limited
Science Park, Milton Road
Cambridge CB4 0XL
United Kingdom
Telephone +44 (0)1223 392090
Fax +44 (0)1223 420021
www.adlittle.uk.com
Reference 20365

Contents

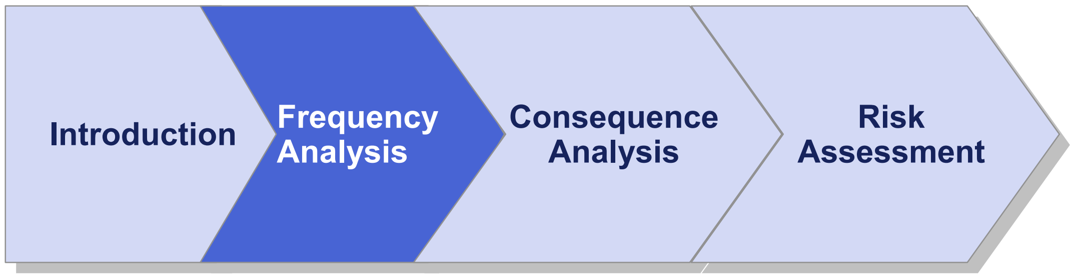


Introduction
Frequency Analysis
Consequence Analysis
Risk Assessment

The same principles and criteria introduced for the Occupational Health and Safety risk assessment can be applied to process safety

- In today's society, the public, customers, in-plant personnel and government regulatory agencies all demand that companies take necessary actions to reduce the possibility of episodic hazardous materials incidents
- The steps to follow for process safety risk assessment are similar to those described for OHS risk assessment:
  - Identify potential hazards
  - Determine who might be harmed and how
  - Evaluate risks and identify control measures
  - Review the risk assessment regularly and when changes occur
- The main techniques adopted for the identification of process hazards were presented during the HAZOP training module
- In this module we focus on techniques and methodologies for frequency analysis, consequence analysis and risk assessment

Contents

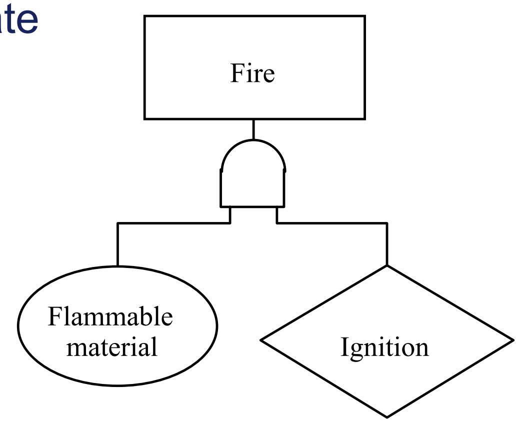

Introduction
Frequency Analysis
Consequence Analysis
Risk Assessment

Fault Tree Analysis is used to identify the ways in which an accident scenario can develop

- The technique starts by identifying a specific hazardous situation which is called the top event
- The technique then works “top down” by breaking the top event into contributing sequences and each sequence is further separated into all of its components which may be initiating or conditional events
- The sequences are presented diagrammatically using a standardised set of symbols which illustrate the logic leading from the combination of initiating events to the top event
- Initiating events are measured as frequencies, typically rates of occurrence per year. Conditional events are measured as probabilities

The Fault Tree Diagram shows the contributing sequences as separate branches where events or sequences are linked through logical gates

- When all of a set of events are necessary for the next higher event the gate is termed an "AND" gate



Top Event

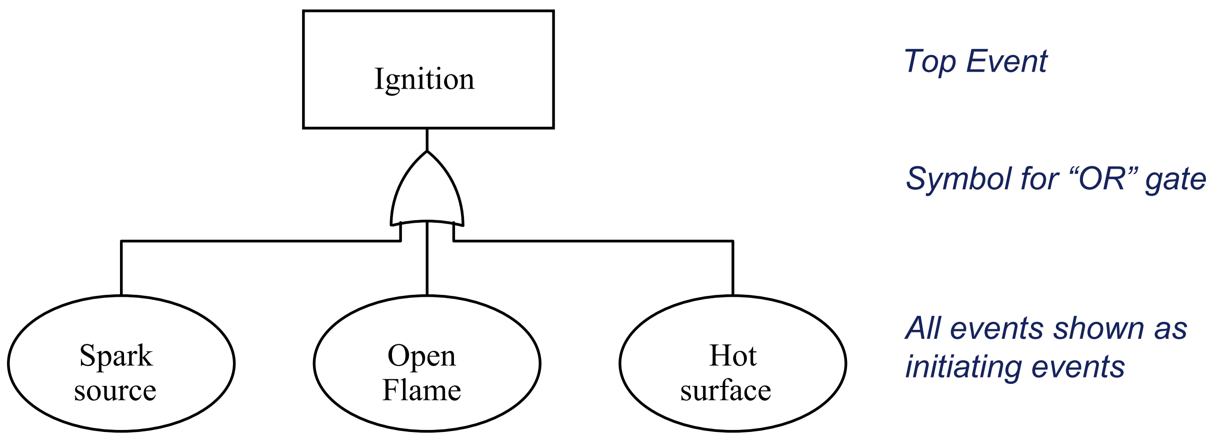
Symbol for "AND" gate

Flammable material shown as an initiating event

Ignition shown as a conditional event

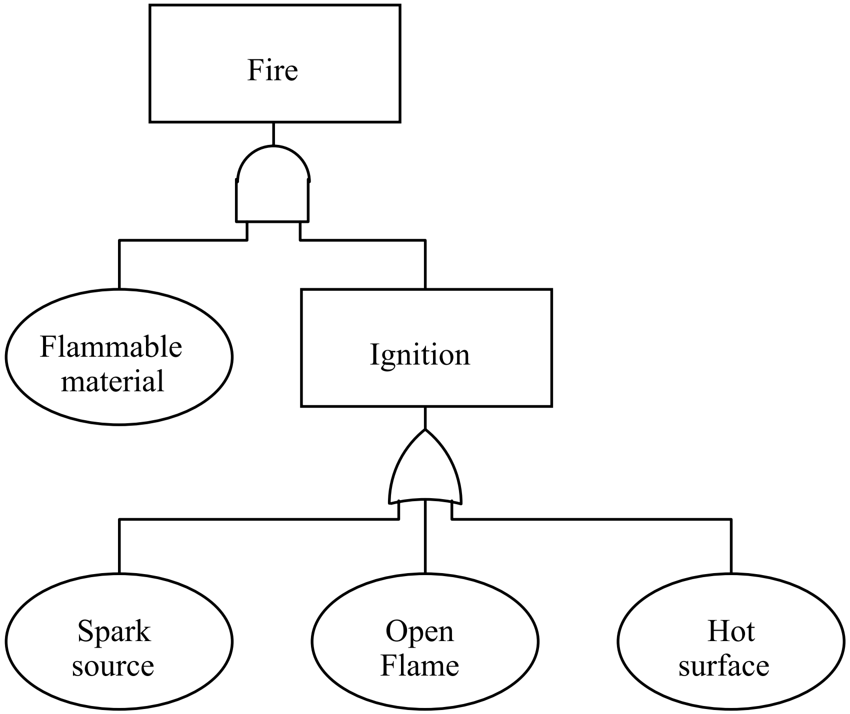
When any one of a set of events are necessary for the next higher event the gate is termed an "OR" gate

- The source of ignition of the fire could be either an open flame, a sufficiently hot surface or a sufficiently energetic spark. Any one of these would be enough to start a fire



"AND" and "OR" gates may be combined to form a tree providing the previously stated rules 1 and 2 are respected

- If the preceding two trees were combined the result would be erroneous



Top event

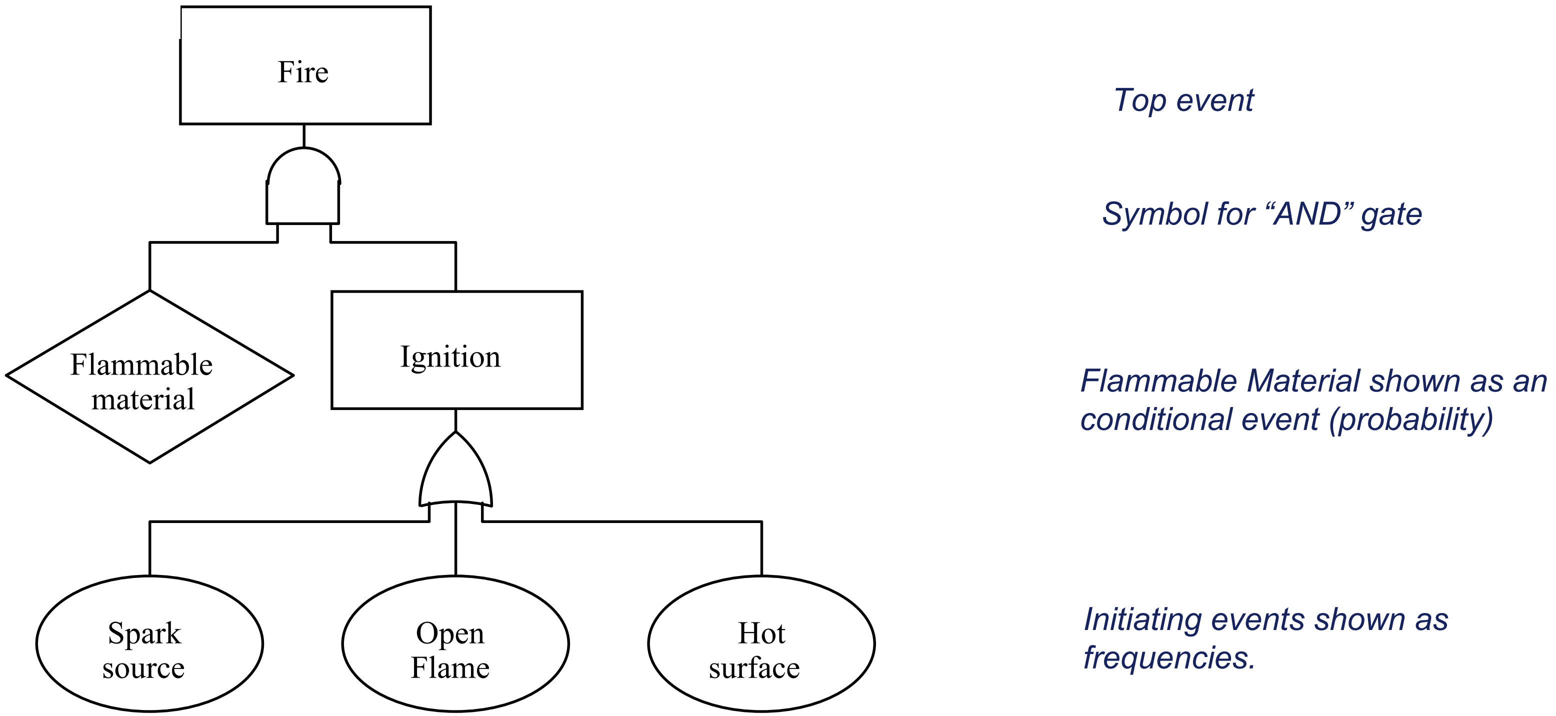
Symbol for "AND" gate

Flammable Material shown as an initiating event (frequency)

Initiating events shown as frequencies
BUT RULE 1 states
AND gate can contain only one initiating event

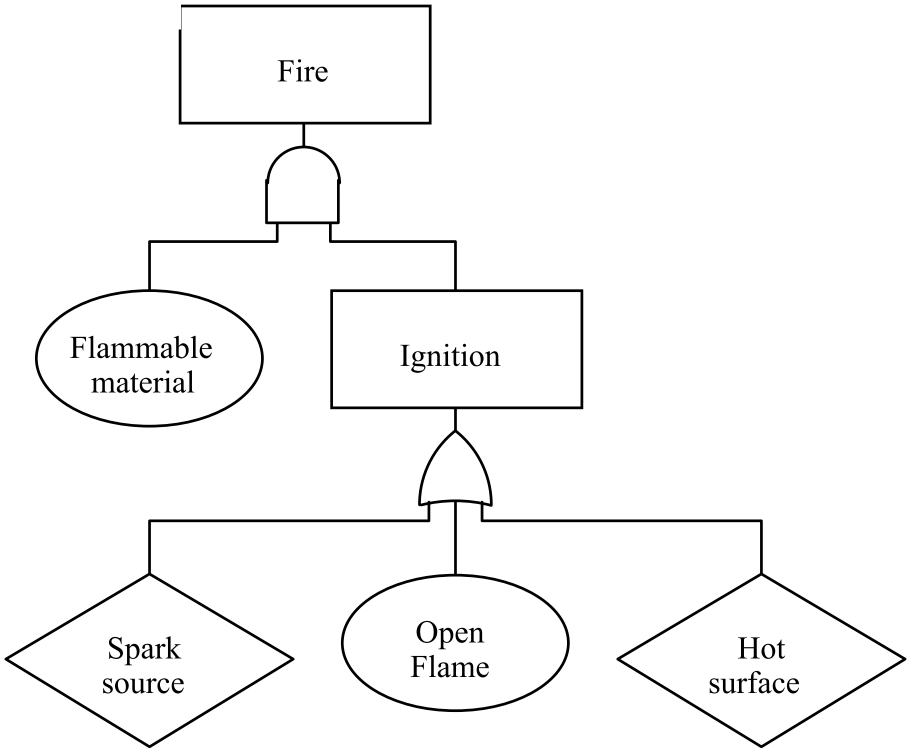
Rule 1 requires there be only one initiating event (frequency) at the "AND" gate

- The following combination is logically acceptable



If the initiating an conditional events were mixed this would violate Rule 2

- The following combination is incorrect



Top event

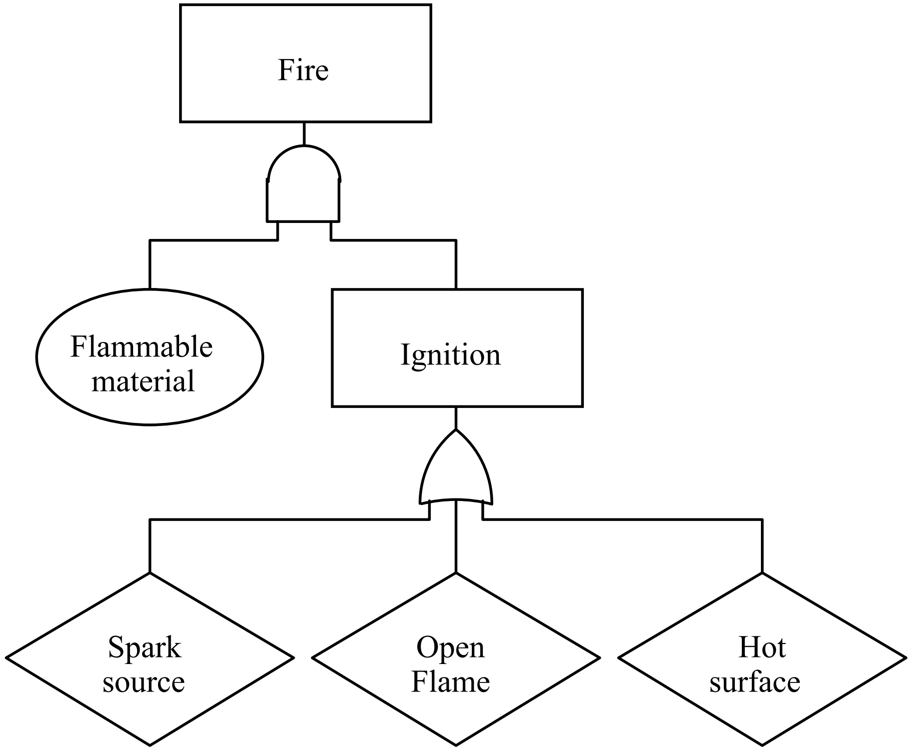
Symbol for "AND" gate

Flammable Material shown as an initiating event (frequency)

Ignition sources mix conditional and initiating events (frequency and probabilities) which infringes **RULE 2.**

But the ignition sources could be treated as all conditional events (probabilities)

- The following combination is acceptable



Top event

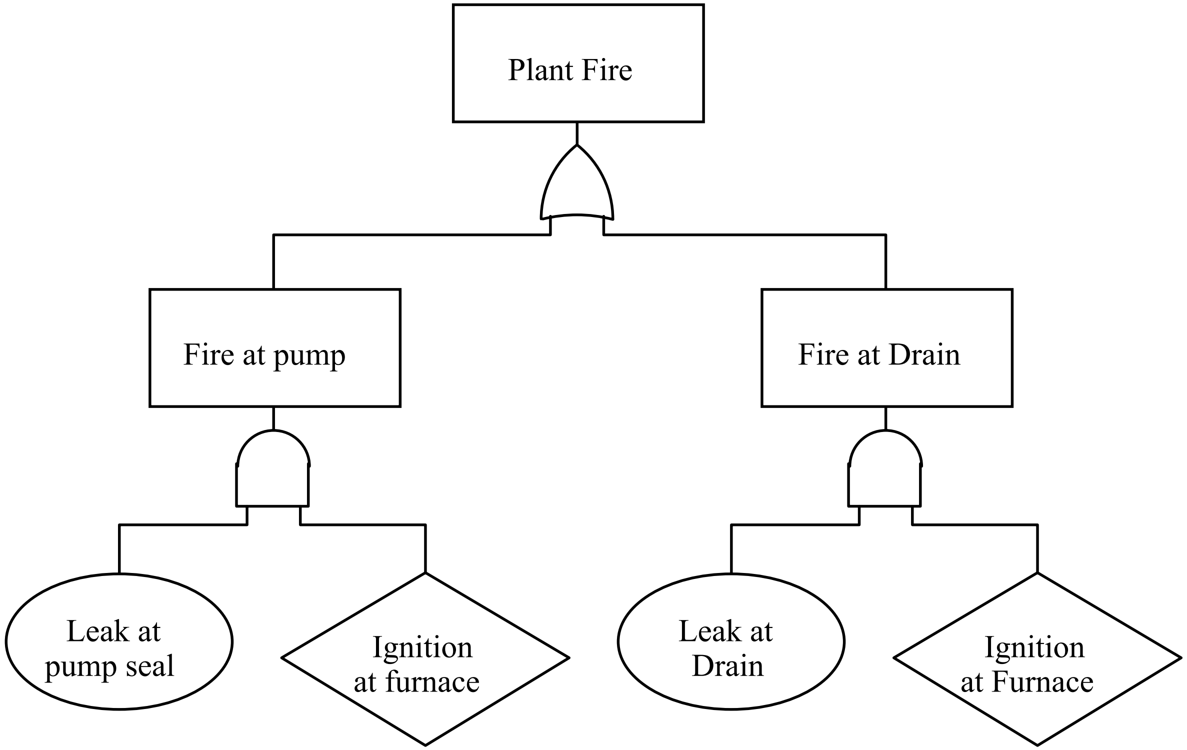
Symbol for "AND" gate

Flammable Material shown as an initiating event (frequency)

Ignition sources are now all conditional events (probabilities)

A third rule forbids the use of the same event at different "AND" gates

- The following tree violates rule 3



Top event

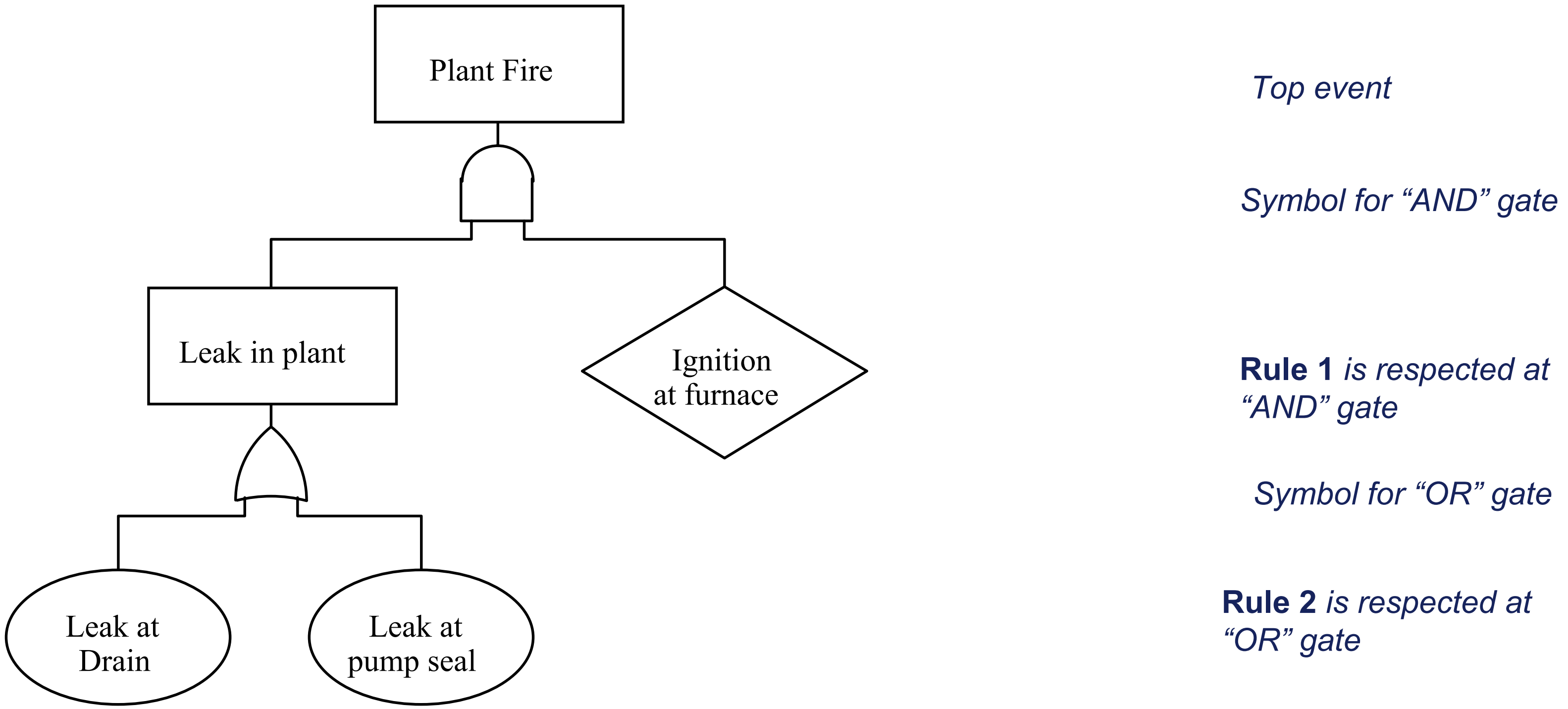
Symbol for "AND" gate

Two fires shown separately

Each AND gate contains the same conditional event infringing **RULE 3**

The tree should be redrawn to group related items like different sources of leakage

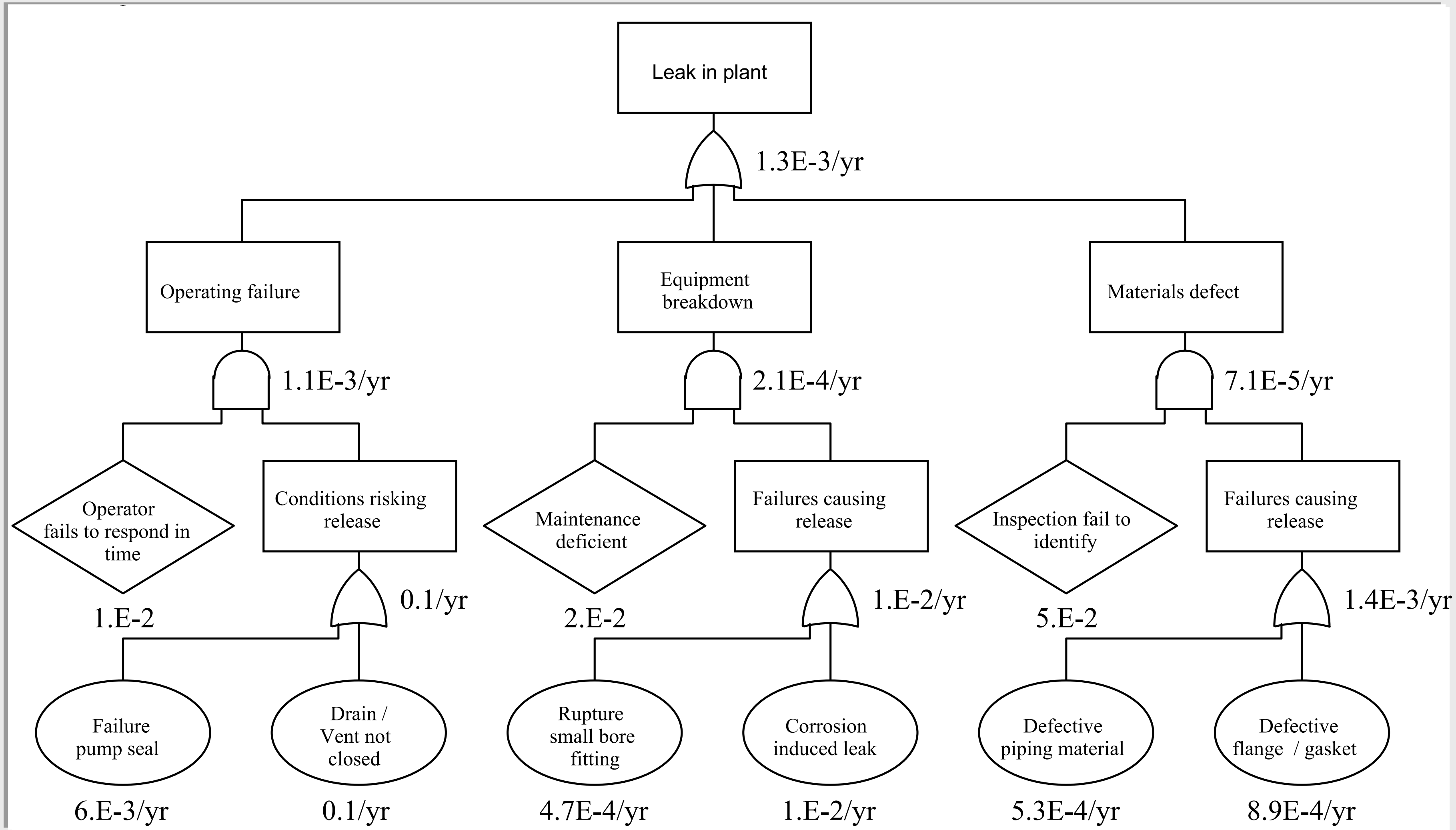
- The following tree complies with all three logical rules



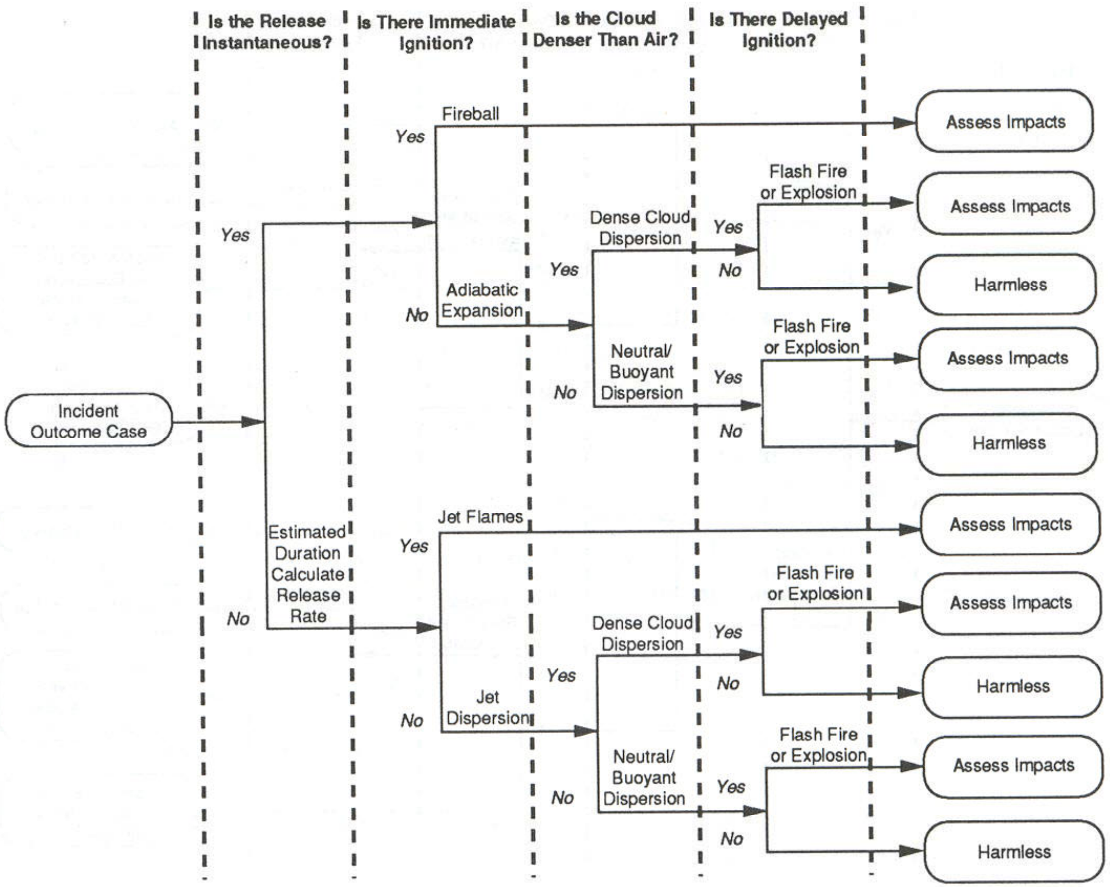
The three logical rules meet the requirements of the Boolean algebra which will be used later to quantify the trees

- The logical rules may be summarised as follows
  - Rule 1 only one frequency at an “AND” gate
  - Rule 2 do not mix frequencies and probabilities at an “OR” gate
  - Rule 3 do not use the same event at different “AND” gates
- In addition other rules are used to guide the development of trees which are helpful and more easily understood
  - Rule 4 Treat normal plant conditions as conditional events and hazardous situations as initiating events
  - Rule 5 Avoid multiple items at an “OR” gate. Instead categorise the events to encourage quick understanding of the tree by the user
  - Rule 6 Try to achieve comparable depth of analysis in different branches using subsidiary trees where greater depth is required

The following example illustrates the quantification of a fault tree



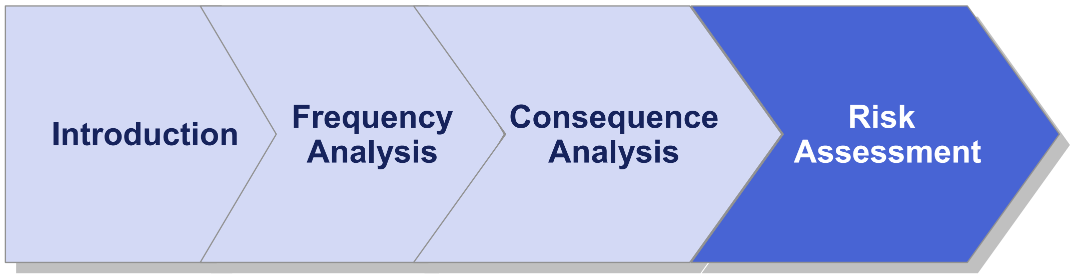
The possible scenarios following the initial event are typically shown as an Event Tree. The frequency of each scenario may be calculated, based on the frequency of the initial event and the probability of subsequent outcomes



Introduction
Frequency Analysis
Consequence Analysis
Risk Assessment

There are various ways to determine and express the consequences of process hazards

- In the event of the release of a hazardous material the first step is to answer the question: “What and how much is coming out of a hole, flange or pump leak, etc.?”. Depending on the nature, pressure and temperature of the substance involved, it could be released as:
  - Liquid
  - Gas or Vapour
  - Two-phase or aerosol
  - Time dependant
- In literature there are numerous models available to determine the flow rate of the material released from vessels, pipes, equipment, etc.
- The next step is to determine the consequences associated with each of the possible outcomes, e.g. hazard distances for flammable or toxic clouds, thermal radiation from fires and overpressure from confined and unconfined explosions
- Finally, various techniques are available to determine the likelihood of fatality or severe injury for people exposed to given levels of thermal radiation, overpressure or concentration of toxic substances


Introduction
Frequency Analysis
Consequence Analysis
Risk Assessment

Risk assessment can be undertaken using a variety of techniques

- Several techniques can be used to evaluate risks, e.g.:

Informed judgement	Risk matrix	Quantified risk assessment (QRA)

Increasing complexity →

- As discussed, these techniques vary in complexity, and each has advantages and disadvantages
- The risk matrix approach is suitable as a first cut assessment, to prioritise the hazards identified, for example, following the HAZOP of a complex process unit
- Following the hazard prioritisation, more detailed frequency and consequence calculations can be carried out, to determine more accurately the risk associated with the top risk scenarios

The first step involves considering the consequences of a hazard in terms of the losses which may occur

- The assessment uses a matrix with five ranges:

1. Assess Consequence

by selecting from consequence matrix ….

The matrix is organised into 5 ranges of financial loss

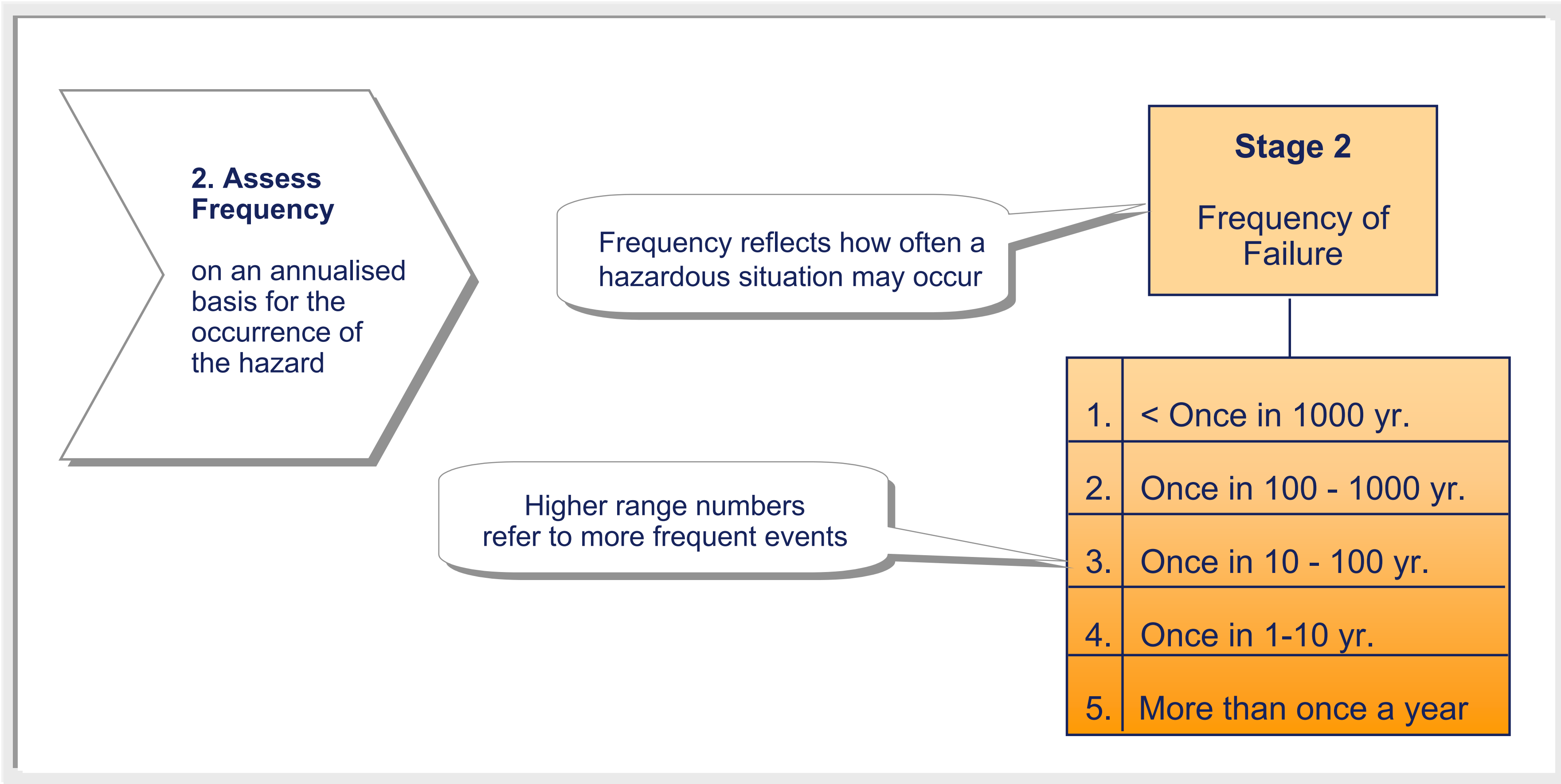
Each range shows the size of the loss eg in millions of Lire

Stage 1

Typical size of Loss

1.	< $50K
2.	$50K to $ 250 K
3.	$250 K - 1 million
4.	$1 - 10 million
5.	> $10 million

The next step requires selecting a range presenting the frequency with which the hazard may occur



The final step is to assess the probability that the loss estimated in the first step will be experienced in practice

3. Assess Probability

of experiencing the loss if the hazard occurs

Probability makes allowance for protective measures which may be in place and which help to avoid or reduce losses should a hazardous situation occur

Stage 3

Probability of Loss

1.	< 1 in 100
2.	1 in 100 to 1 in 20
3.	Between 5% and 25 %
4.	Between 25% and 99%
5.	> 99%

The ranges span from general human error to certainty

Range 5 is used only where a loss is certain

The three matrices are used to assess the risks associated with the process hazards identified, for example, during the HAZOP session

= **Stage 1** Typical size of Loss X **Stage 2** Frequency of Failure X **Stage 3** Probability of Loss

Stage 1 – Typical size of Loss

1.	< $50K
2.	$50K to $ 250 K
3.	$250 K - 1 million
4.	$1 - 10 million
5.	> $10 million

Stage 2 – Frequency of Failure

1.	< Once in 1000 yr.
2.	Once in 100 - 1000 yr.
3.	Once in 10 - 100 yr.
4.	Once in 1-10 yr.
5.	More than once a year

The "top event" which could be derived using a Fault Tree

Stage 3 – Probability of Loss

1.	< 1 in 100
2.	1 in 100 to 1 in 20
3.	Between 5% and 25 %
4.	Between 25% and 99%
5.	> 99%

Probability which could be derived using an event tree

On March 23, 2005 at 1:20 p.m. an explosion and fire occurred at the BP Texas City Refinery's Isomerization unit

The accident is still under investigation

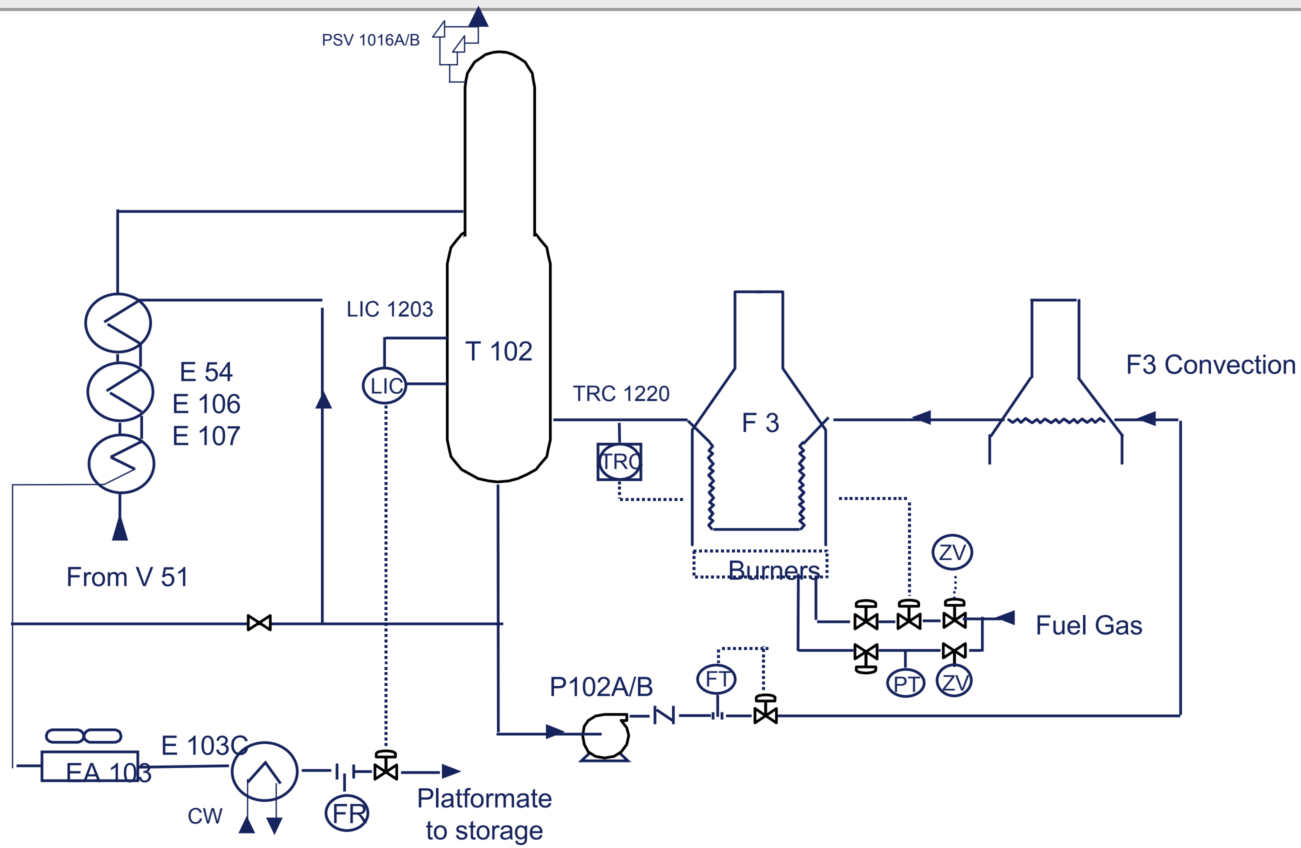
15 people died and between 70 and 100 were injured

The following example from a HAZOP at another site illustrates the analysis of the hazard

The principal safety issues raised by the case include the design of the un-flared blow-down system

Use the following Safeguarding Flow Diagram to suggest a fault tree leading to flood of the column T 102 and lift of the PSV 1016 A/B

- Consider which control has to fail to fill the column
- Consider which alarms would occur and the operator would need to ignore

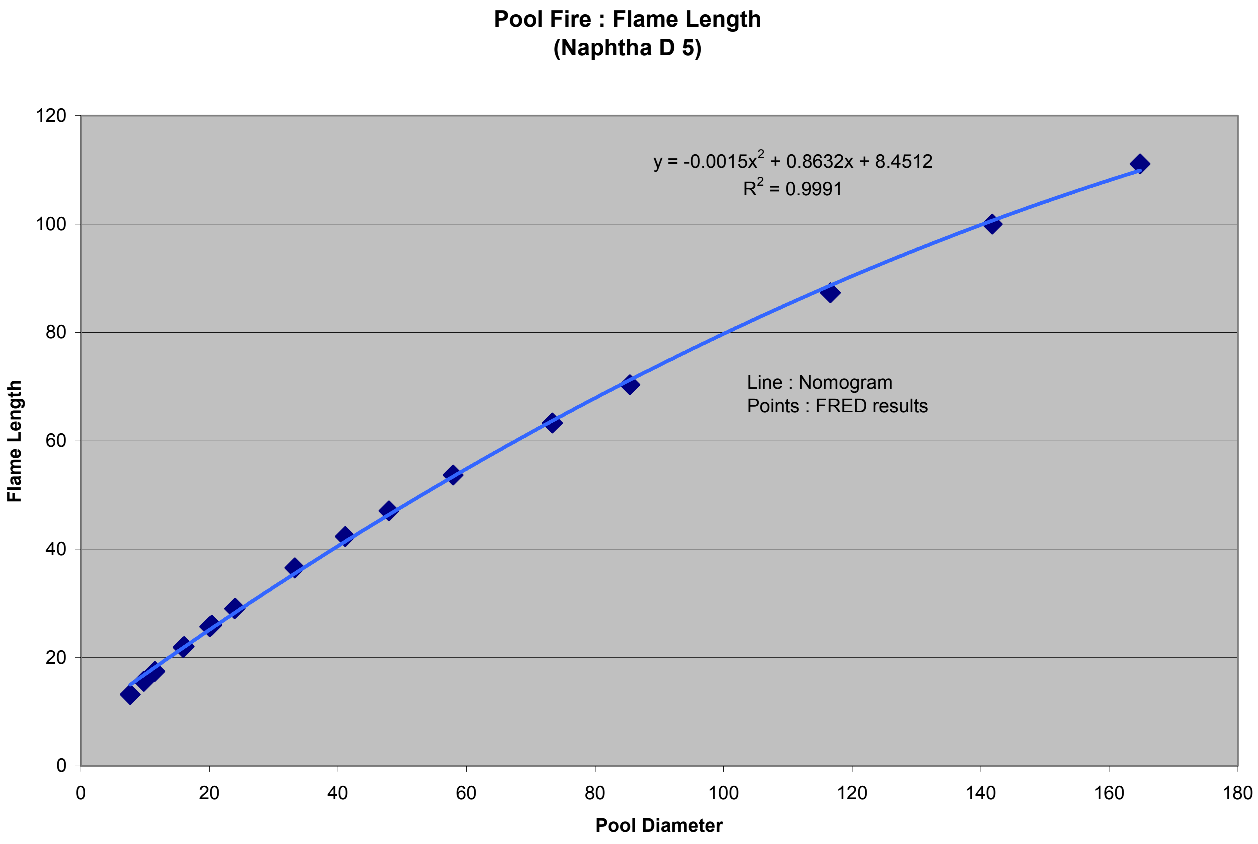


Liquid released from PSV 1016A/B which is not connected to the blowdown and flare system could escape as a hot naphtha liquid spray some of which would fall down the column to form a pool

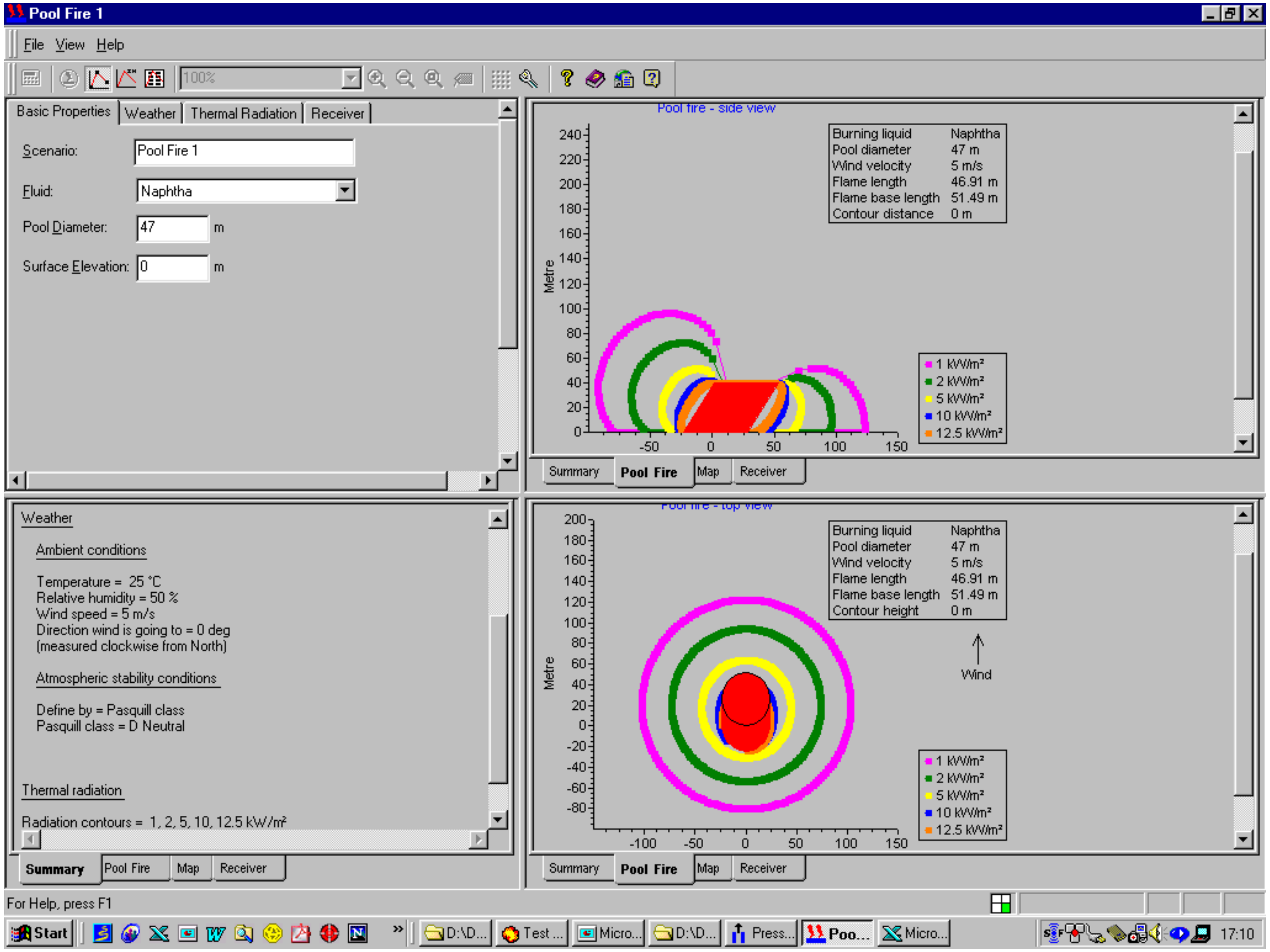
The modelling indicates formation of a pool of up to 47 m diameter in a congested process area and may be ignited if it encounters a suitable source.

Use the nomogram to estimate the flame length if the pool ignited

Use the matrix to estimate frequency, probability and consequence



Exercises in risk assessment : Accident Scenario 1 Model output



Answers : The following Risk Register entry describes scenario 1

ID Number	Issue	Revision	G						
23	33	Date	22-Apr-99						
Issue		Discharge from PSV							
Cause		PSV on debutaniser not connected to blowdown. If failure of level control liquid could be released							
		6 HAZOP items eg 952.5							
Consequence		Potential for ignition of falling liquid and development of large fire							
Recommendation		Connect PSV on debutaniser to flare This is considered an intolerable risk							
Implementation					Action Summary				
Asigned to			Date Due						
			Date Done						
Verified by			Date Verified						
Assessment Notes		Frequency 1 in 100 years - requires loss of level control							
		Probability low -operator likely to detect problem							
		Consequence could be catastrophic in crowded process area							
Before/After Implement		Frequency	Probability	Consequence	Frequency	Probability	Consequence	Plant Benefit	Industry Benefit
Human Safety		1	3	4	1	1	4	1287541.675	540767503.4
Property Loss		3	3	5	3	3	1	96823465.62	40665855561
Business Interruption		3	3	5	3	3	1	95845260.38	40255009359
Catalyst life								0	0
Energy								0	0
Product Losses								0	0
Plant Utilisation								0	0
Plant Maintenance								0	0
Publicity									
Environmental Impact									
Cost of implementation		Total Benefit	Benefit/Cost	Total Saving					
3	50000000	193956267.7	3.88	143956267.7					

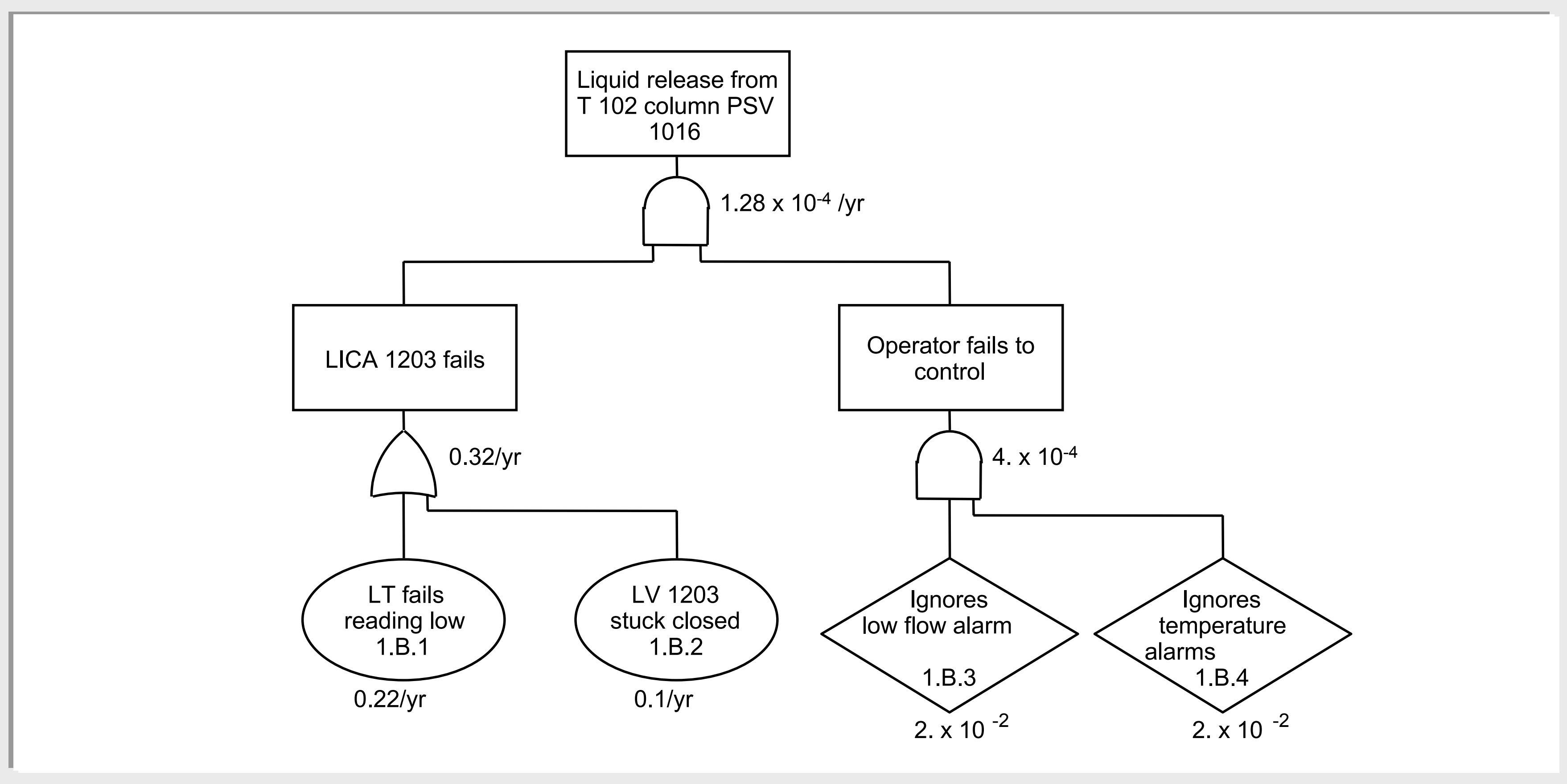
Quantify your Fault tree for liquid release using the following data

Release Case Case 1B : Liquid release from PSV 1016

Selected values

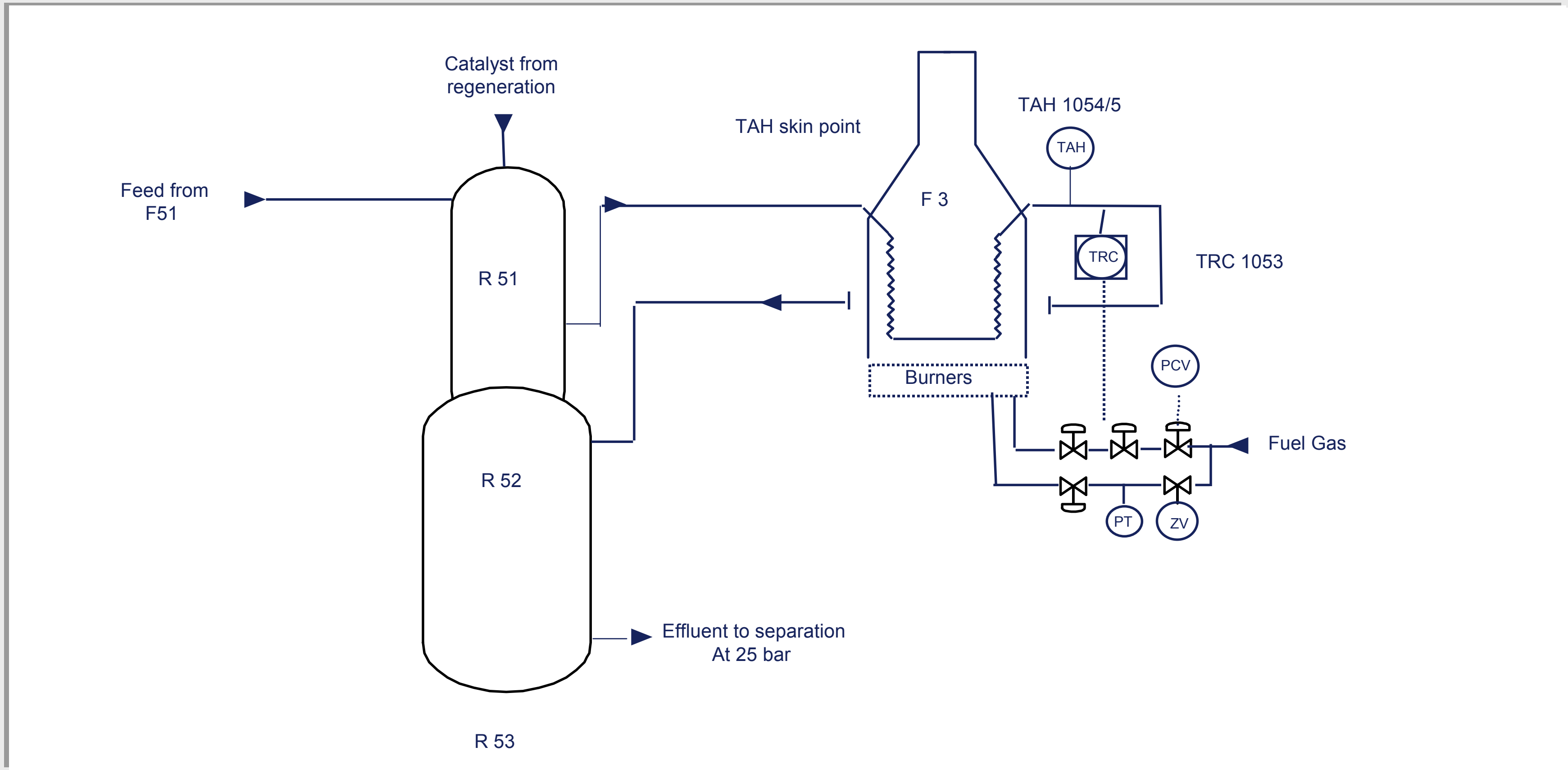
Fault Tree Reference	Event	Frequency	Probability	Data Source
1B.1	LT fails reading low	0.22		Process Equipment Reliability Data, Centre for Chemical process safety AICE 1989, ISBN 0-8169-0422-7
1B.2	LV 1203 stuck closed	0.10		Risk Analysis Report to the Rijnmond Public Authority, D.Reidel Publishing Co., 1981 ISBN 90-277-1393-6
1B.3	Ignores low flow alarm FR 1192		0.02	HEART generic task E
1B.4	Ignore temperature alarms TI 107/8		0.02	HEART generic task E

Answers : Suggested Fault tree for liquid release



This emergency was initiated by a furnace tube rupture in a fired reboiler

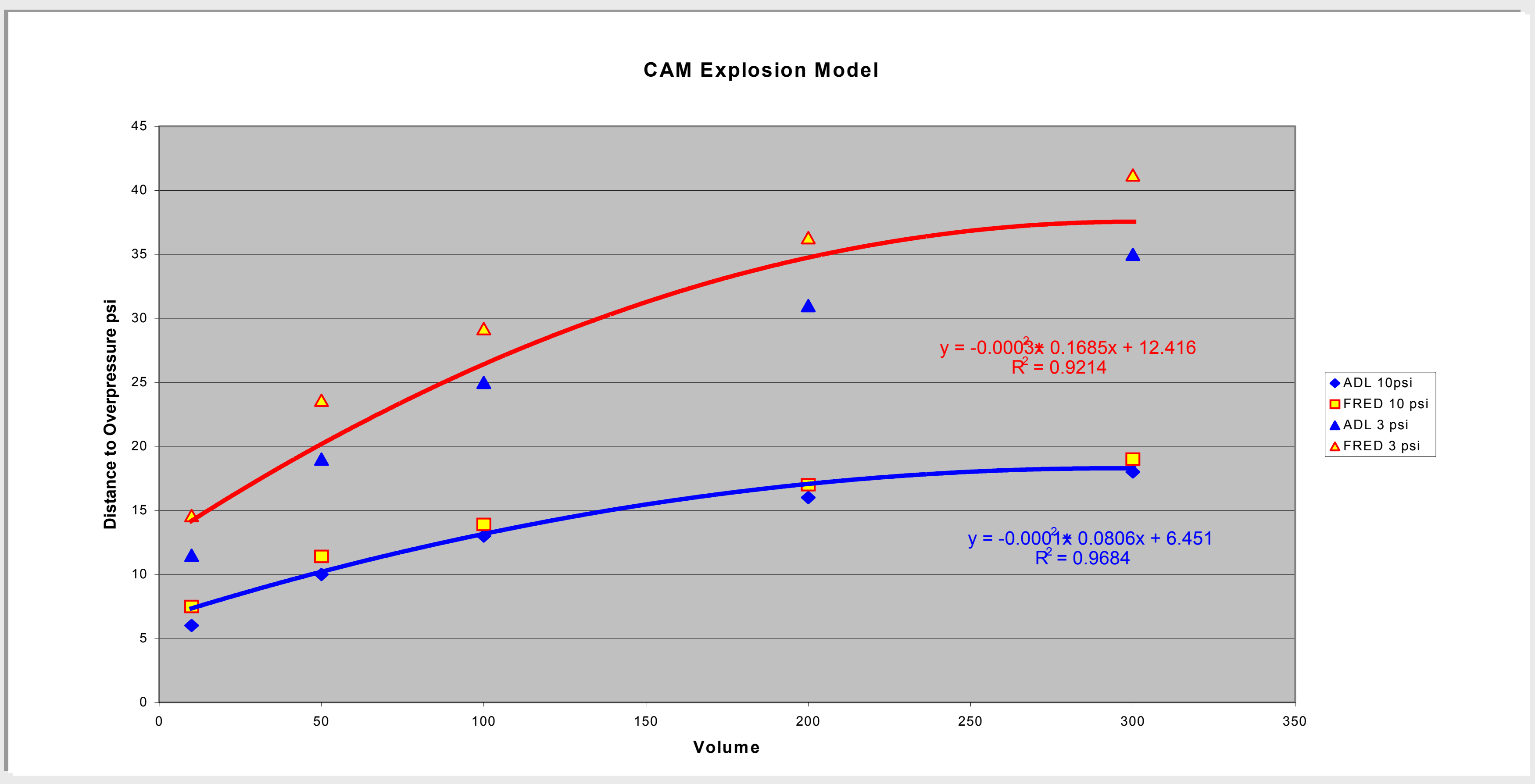
Consider tube rupture using the following Safeguarding Flow Diagram for the furnace F3



Consider an accident involving full bore rupture of a furnace tube in F3

- Three main causes were identified with the potential of leading to this scenario:
  - Mechanical failure of furnace coil
  - Low flow due to control failure or fouling/coking
  - Over-firing of furnace
- Draw a fault tree for the furnace tube rupture including how the rupture occurs and operator actions to control situation
- The modelling indicates that the escaping liquid naphtha immediately vaporises. Depending on operator actions the scenario might lead to a semi-confined explosion in the furnace (estimated 280 m3)
- Use the matrix to estimate frequency, probability and consequence

Use the following nomogram to estimate the distance to 10 psi overpressure caused by the explosion



Answers : The following Risk Register entry describes scenario 2

ID Number	Issue	Revision	G
35	47	Date	22-Apr-99

Issue	Protection against tube rupture
Cause	Uneven firing causes one tube to overheat 8 HAZOP items eg 954.1
Incident	Furnace tube rupture
Recommendation	FCV or TSHH trip on each pass
Implementation	Action Summary

Asigned to		Date Due	
		Date Done	
Verified by		Date Verified	

Assessment Notes	Frequency between 1 in 100 and 1 in 10 years Probability low because of operator care and other alarms Consequence severe

Before/After Implement	Frequency	Probability	Consequence	Frequency	Probability	Consequence	Plant Benefit	Industry Benefit
Human Safety							L. 0	L. 0
Property Loss	3	2	3	3	1	3	L. 678,766	L. 285,081,727
Business Interruption	3	2	4	3	1	4	L. 3,291,840	L. 1,382,572,898
Catalyst life							L. 0	L. 0
Energy							L. 0	L. 0
Product Losses							L. 0	L. 0
Plant Utilisation							L. 0	L. 0
Plant Maintenance							L. 0	L. 0
Publicity								
Environmental Impact								

Cost of implementation		Total Benefit	Benefit/Cost	Total Saving
2	L. 11,180,340	L. 3,970,606	0.36	

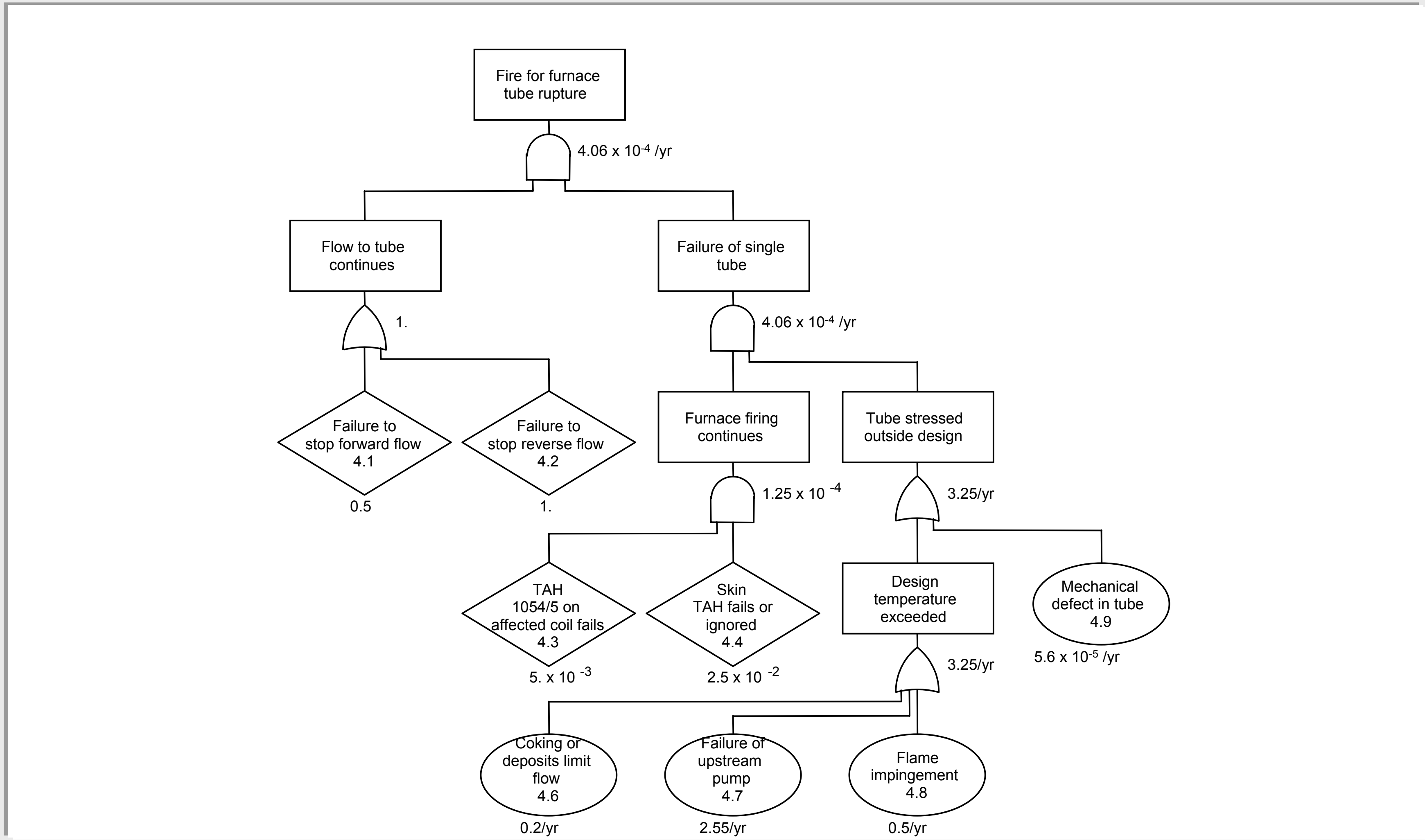
Quantify your Fault tree for tube rupture using the following data

Release Case Case 4 : Fire for furnace tube rupture

Selected values

Fault Tree Reference	Event	Frequency	Probability	Data Source
4.1	Failure to stop forward flow		0.50	
4.2	Failure to stop reverse flow		1	No means to act in time
4.3	TAH 1054/5 on affected coil fails		0.005	Reliability and Maintainability in perspective 3rd edition D.J.Smith 1988 ISBN 0-33-46205-X assuming 50% fail to danger and 12 month test interval
4.4	Skin TAH fails or ignored		0.025	Reliability and Maintainability in perspective 3rd edition D.J.Smith 1988 ISBN 0-33-46205-X assuming 50% fail to danger and 12 month test interval plus HEART generic task E
4.5 (Figure 4B only)	TSHH fails		0.01	Reliability and Maintainability in perspective 3rd edition D.J.Smith 1988 ISBN 0-33-46205-X assuming 1005 fail to danger and 12 month test interval
4.6	Coking of deposits limit flow	0.2		Estimate
4.7	Failure of upstream pump	2.55		Process Equipment Reliability Data, Centre for Chemical process safety AICE 1989, ISBN 0-8169-0422-7
4.8	Flame impingement	0.5		Estimate
4.9	Mechanical defect in tube	5.60E-05		Process Equipment Reliability Data, Centre for Chemical process safety AICE 1989, ISBN 0-8169-0422-7 for 4 tubes

Answers: Fault Tree for rupture of furnace tube



The third accident involves seal leak at a pump which could be very difficult to isolate if there were immediate ignition

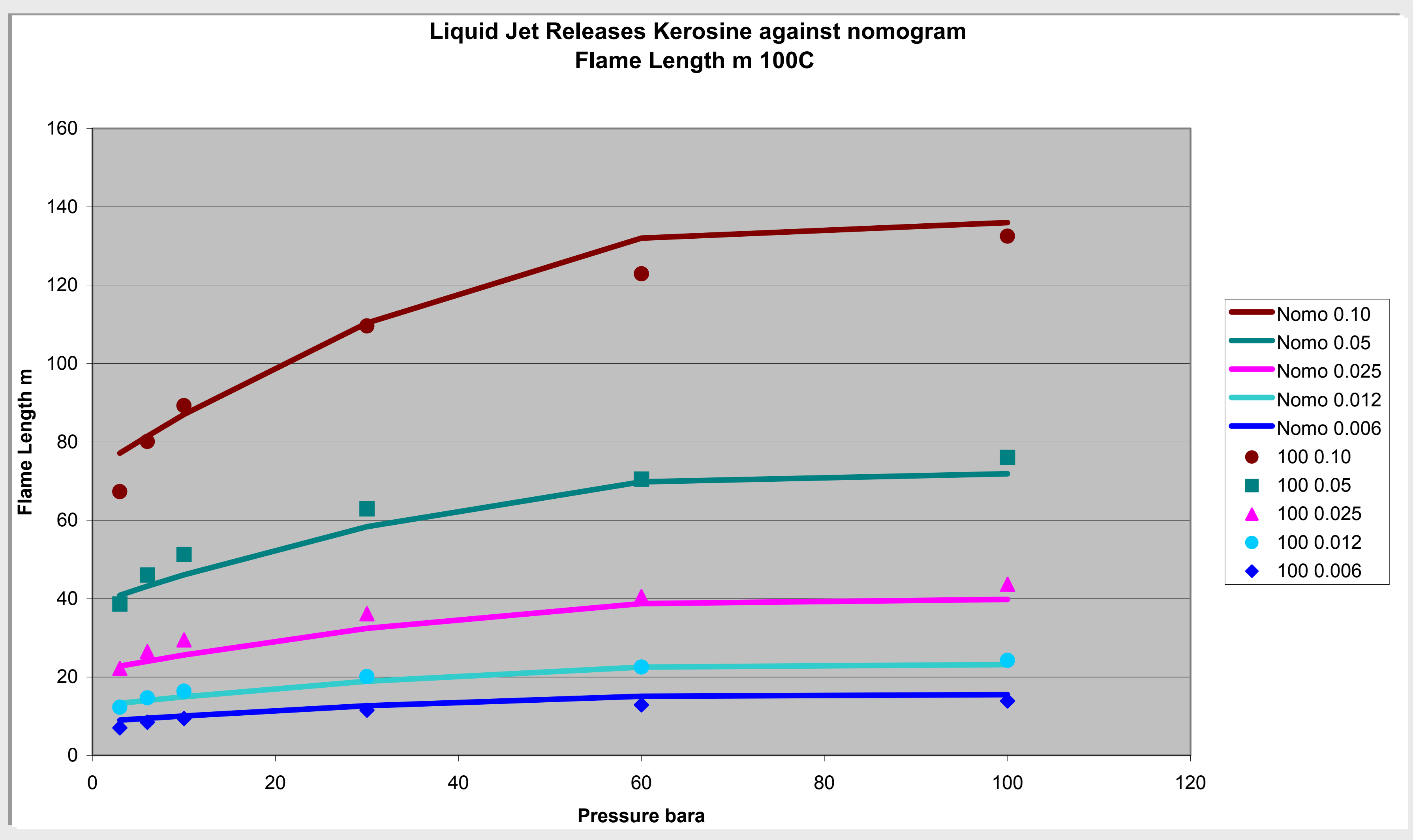
The prefractionator section of the plant was shut down when upgrading investment was made.

Because of this the column has not be raised to the standard of other plant sections. In particular single seals are retained on pumps and there was no emergency shutdown valve installed to isolate the upstream inventory.

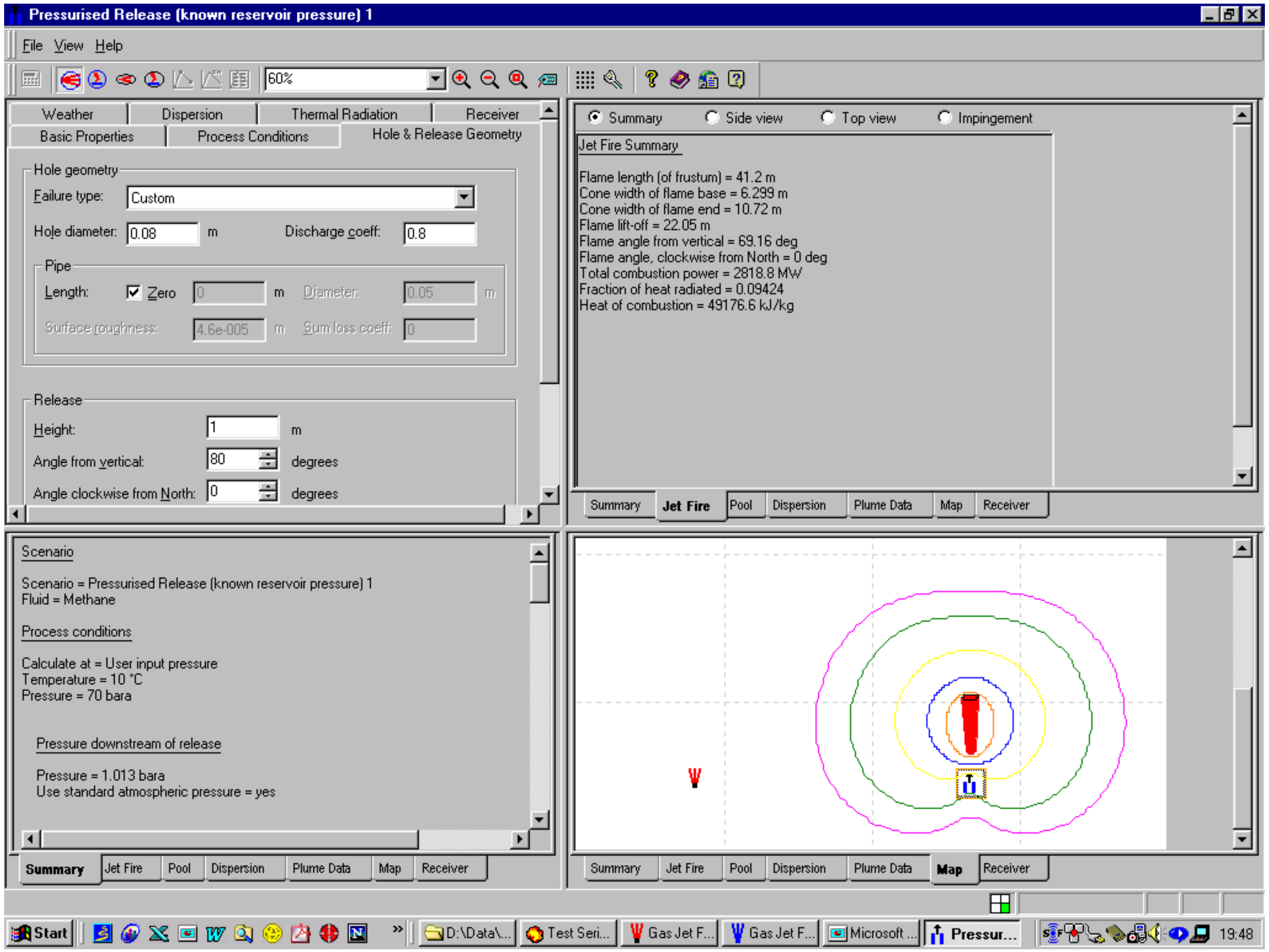
Failure of the seal followed by immediate ignition lead to a fire which affected other units because there was no rapid isolation

Suggest a fault tree for the event and use the risk matrix to assess F,P,C

Use the following nomogram to estimate the flame length for a 12 mm hole at 30 bar



Example of a pressurised release model



Answers : The following Risk Register entry describes scenario 3

ID Number	HAZOP Items	Revision	3(Draft Report)
37	R 677.3	Date	12-Dec-00

Incident Description	Pumps
Cause	Protection against seal rupture
Consequence	Rupture of single mechanical seal caused by maloperation of pump (loss upsteam level or outlet blocked in operation) Rupture leads to leak which ignites but upstream inventory cannot be isolated leading to escalating fire worse if under fin fan
Recommendation	Install double seal with fluid reservoir protecteced by LAL and PAH giving common alarm in DCS
Implementation	
Asigned to	Date Due: Date Done:
Verified by	Date Verified:
Assessment Notes	

Before/After Implement	Frequency	Probability	Consequence	Frequency	Probability	Consequence	Plant Benefit	Industry Benefit
Human Safety	3	2	2	2	1	1	L. 161,273	L. 15,482,205
Property Loss	3	2	2	2	1	1	L. 158,111	L. 15,178,629
Business Interruption	3	3	3	3	1	3	L. 3,824,032	L. 367,107,040
Catalyst life							L. 0	L. 0
Energy							L. 0	L. 0
Product Losses							L. 0	L. 0
Plant Utilisation							L. 0	L. 0
Plant Maintenance							L. 0	L. 0
Publicity								
Cost of implementation 1 L. 2,236,068	Total Benefit L. 4,143,415	Benefit/Cost 1.85	Total Saving L. 1,907,347					

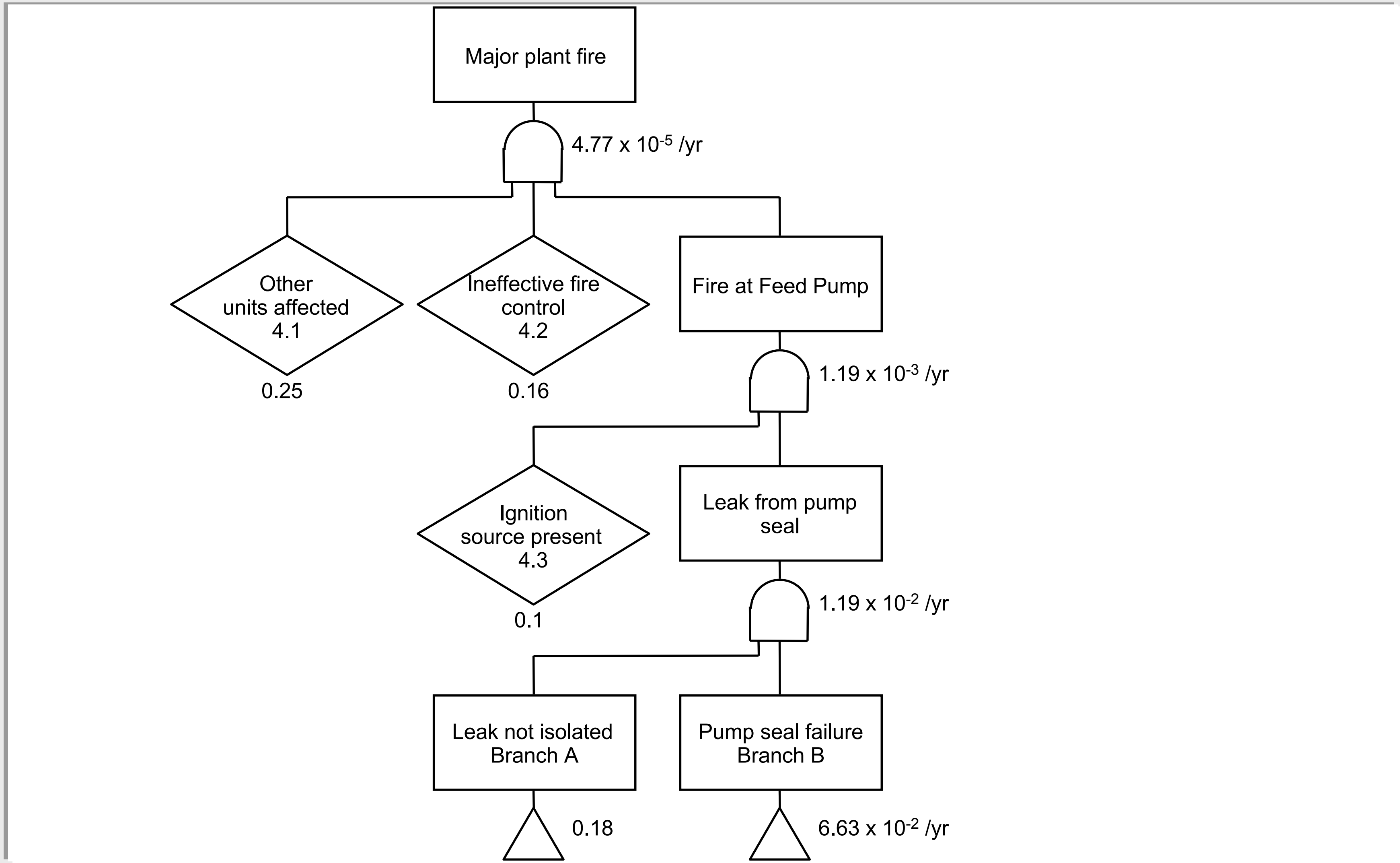
Quantify your Fault Tree for leak from a single seal pump

Release Case Case 4 : Pump seal Leak

Selected values

Fault Tree Reference	Event	Frequency	Probability	Data Source
4.1	Other units affected		0.25	Estimate for compact plant
4.2	Ineffective fire control		0.16	HEART generic task C
4.3	Ignition		0.1	Estimate used in previous work
	Branch A			
4A.1	Leak not detected		0.02	HEART generic task E
4A.2	Operator fails to reach valve		0.16	HEART generic task C
4A.3	Valve fails to seal tight		2.74E-04	Probability derived from Risk Analysis Report to the Rijnmond Public Authority, D.Reidel Publishing Co., 1981 ISBN 90-277-1393-6 assuming 8 hours to repair
	Branch B			
4B.1	Mechanical seal failure	5.6E-02		Data from ICI Mond for various pump types
4B.2	Failure pump utilities	1.0E-02		Estimate
4B.3	Seal fails for low flow		0.1	Estimate used in previous ADL work
4B.4	LAL fails or ignored		0.1	Sum of alarm failure (0.07) Reliability and Maintainability in Perspective, 3rd Edition, D.J. Smith, 1988 ISBN 0-333-46205-X and operator ignores alarm (0.03 Lees)
4B.5	LCV fails open	3.00E-01		Risk Analysis Report to the Rijnmond Public Authority, D.Reidel Publishing Co., 1981 ISBN 90-277-1393-6

Answers : Fault Tree for Major fire following leak from a single seal pump



Fault Trees for failure to isolate leak and failure of single seal