ENGINEERING DEPARTMENT

COURSE

IN

PROCESS HAZARDS ANALYSIS

Engineering Service Division

E. N. (Neil) Helmers, Consultant Manager
L-1352 - 366-2303

R. W. (Dick) Prugh, Senior Consultant
L-1353 - 366-2771

S. B. (Barry) Gibson, Senior Consultant
L-1328 - 366-4509

R. J. (Bob) Gardner - Consultant
L-13W05 - 366-4201

W. R. (Bill) Tilton, Consultant
L-13W30 - 366-4071

R. W. (Bob) Johnson, Technical Services Engineer
L-13W32 - 366-2790

D. G. (Dave) Clark, Technical Services Engineer
L-13W36 - 366-3643

TABLE OF CONTENTS

INTRODUCTION

PROCESS HAZARDS

DEFINITION: "PROCESS HAZARDS" ARE POTENTIAL EXPOSURES TO SERIOUS INJURY OR SUBSTANTIAL PROPERTY DAMAGE INHERENT TO A PROCESS OR OPERATION.

(SAFETY & FIRE PROTECTION DIV. GUIDELINES, SECTION 6.1)

CATEGORIES:

I. BLAST EFFECTS OF EXPLOSIONS
II. HEAT/RADIATION EXPOSURE
III. TOXIC/CORROSIVE CHEMICAL EXPOSURE
IV. MECHANICAL HAZARDS
V. ELECTRICAL HAZARDS

NOTE: MAJOR HAZARDS (WITH POTENTIAL FOR MULTIPLE FATALITIES) USUALLY INVOLVE EXPOSURES WHICH FALL IN CATEGORIES I, II, OR III ABOVE.

PROCESS HAZARDS (CATEGORIES I, II, & III)

I. Blast Effects of Explosions
(Shock waves, missiles, structural damage, bodily displacement)

A. Unconfined vapor cloud explosions (UVCE)

B. Bursting vessel or piping explosions

1. Internal uncontrolled reaction
(deflagration; detonation; runaway reaction with heat and gas evolution)

2. Physical overpressurization
(overfilling; high-pressure feed; thermal expansion; fire exposure; internal flashing)

3. Mechanical failure
(random failure; weakened vessel; external force)

C. Vapor, dust, or mist explosions in confined area

D. Detonation of condensed-phase material
(e.g., high explosives)

E. Rapid phase transition (RPT) explosions; including Boiling-liquid-expanding-vapor explosions (BLEVE's)

II. Thermal/Radiation Exposure

A. Thermal burn hazards
(fire, flammable vapor fireball, flare thermal radiation, steam leak, hot wax leak, etc.)

B. Heat Stress

C. Cryogenic burn hazards

D. Electromagnetic radiation (lasers, microwaves)

E. Nuclear radiation (e.g., radioactive materials)

III. Toxic/Corrosive Chemicals Exposure

1. Acute toxicity effects

2. Chronic or latent toxicity effects

3. Chemical burns/corrosivity

4. Asphyxiation or suffocation

29 Year Summary Of Fatal Injury Causes 1954-1982

PROCESS–RELATED	FATALITIES	INCIDENTS
EXPLOSIONS	60	31
FIRES	12	8
TOXIC MATERIALS	11	11
NON-FIRE BURNS	5	4
SUFFOCATION	3	2
CRUSHING TRAUMA	3	3
	94	59
NOT PROCESS–RELATED	51	50

EXPLOSION TYPE

(INDUSTRIAL RISK INSURERS 1972-1976)

		% OF INCIDENTS	% OF $
COMBUSTION	IN EQUIPMENT	27	12
	OUTSIDE EQUIPMENT IN BUILDING	22	20
	IN OPEN	4	17
	SUBTOTAL	53	49
REACTION	EXPLOSIVE LIQUID OR SOLID	18	14
	RUNAWAY REACTION	16	29
	SUBTOTAL	34	43
METAL FAILURE	CORROSION	1	1
	OVERHEATING	4	1
	ACCIDENTAL OVERPRESSURE	8	6
	SUBTOTAL	13	8

29 Year Process-Related Fatal Injury Causes

(5 Year Groups)

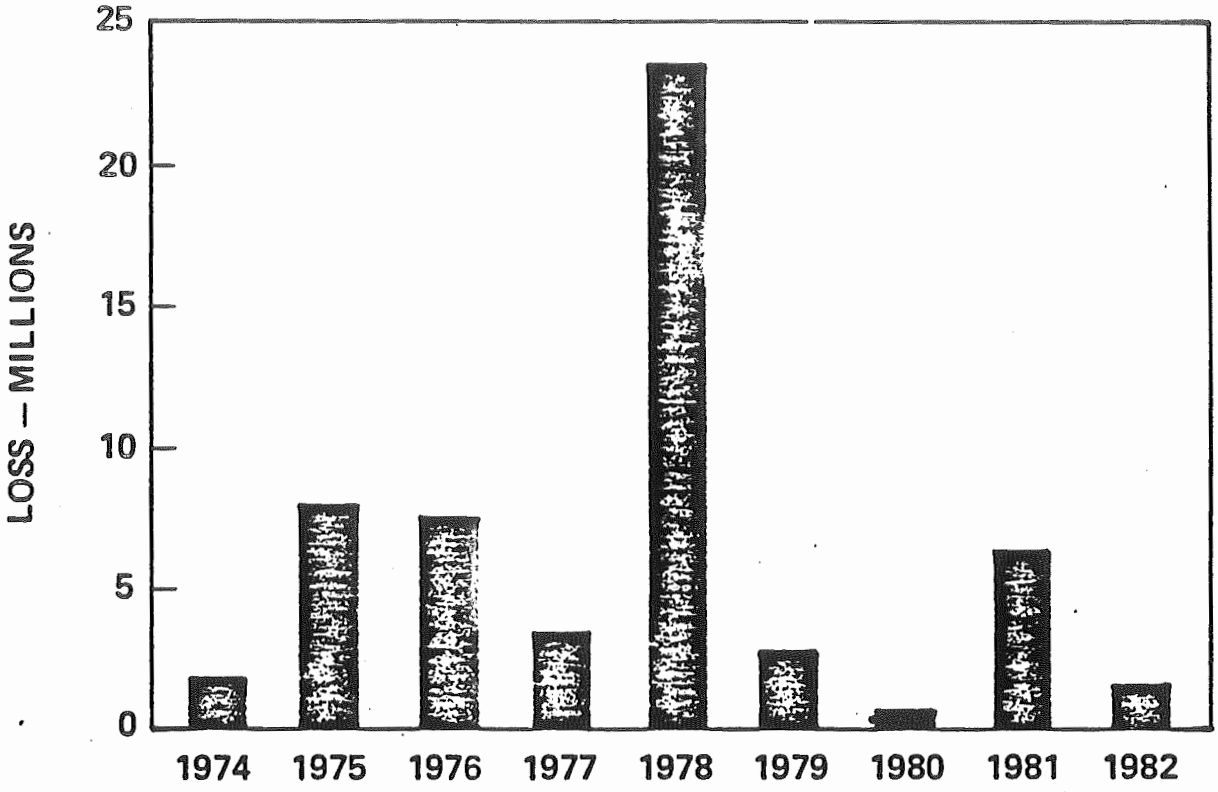
	1954 1958	1959 1963	1964 1968	1969 1973	1974 1978	1979 1982	4 YEARS
EXPLOSIONS	10	4	19	18	7	2	
FIRES	2	2	7	0	1	0	
TOXIC	7	1	1	1	0	1	
TOTAL	22	11	29	19	9	4	

1978 LOSSES EXCEEDING $100M PER INCIDENT

- ISD Fire Nemours Building
- Circleville Freeze-up
- Belle Plant Fire
- Edge Moor Tank Failure
- Carney's Point Explosion
- Houston Plant Explosion
- Chambers Works Explosion & Fire
- Corpus Christi Plant Explosion
- Sabine River Explosion & Fire

Property Damage

FIRE & EXPLOSIONS



CORPORATE POSITION

Following the April 1978 Explosion at Carney's Point, the Executive Committee Recommended a Thorough Review of the Company's Process Hazards Management Procedures. The Key Recommendation Was: Upgrade the Process Hazards Management Program.

- Each Site Responsible To Have Thorough Hazard Reviews on Processes.
- Departmental Process Hazards Coordinators Instituted.
- Engineering Department Implemented Formal Process Hazard Review Procedure.
- Individual Must Accept Responsibility to Improve Safety Performance.

HISTORY
PROCESS HAZARD REVIEWS

- Recommended by Safety & Fire Protection Division Since 1965

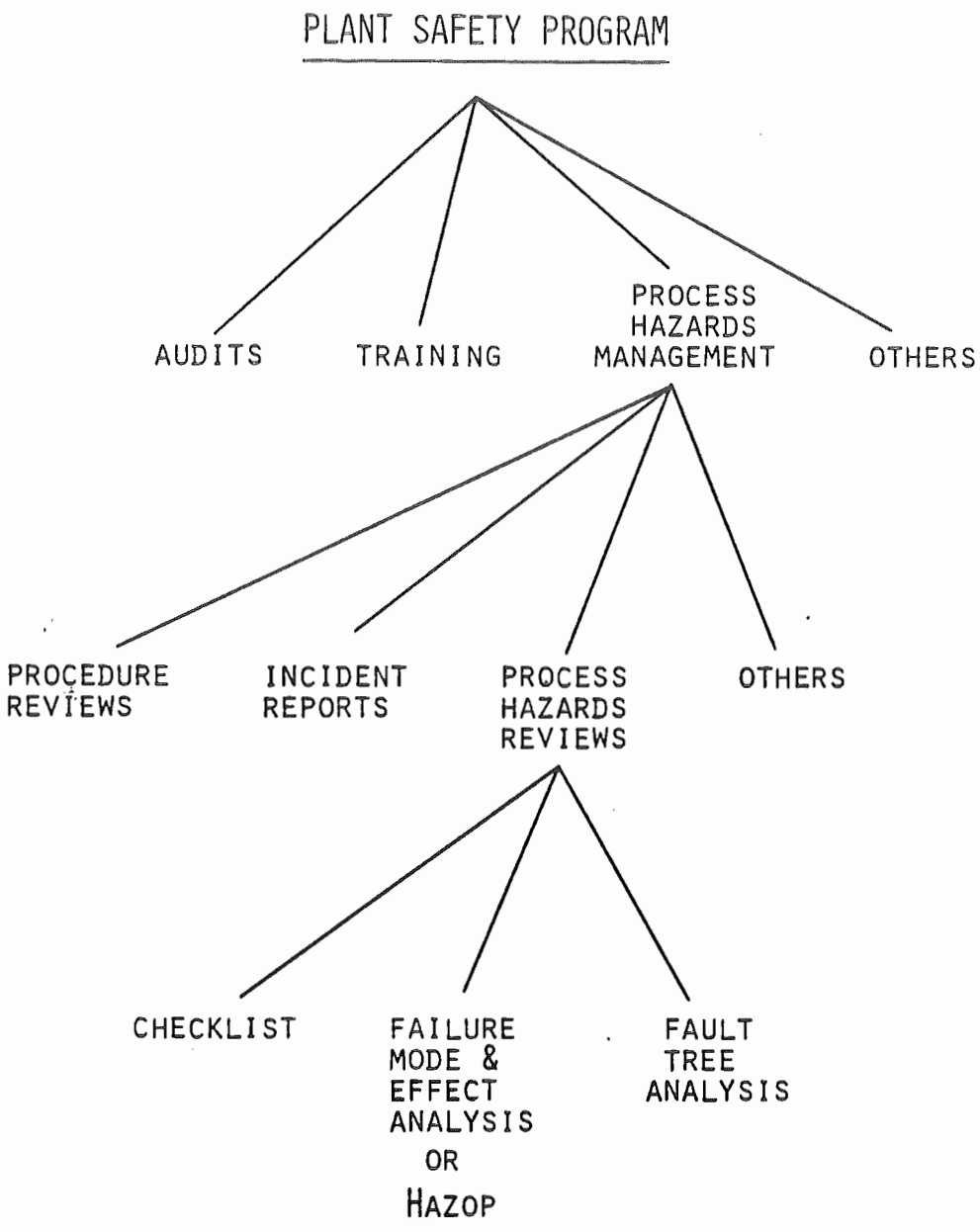
- "Process Hazards Reviews" Bulletin 505 Issued 1973 (Replaced by Section 6.4).

- Upgrade Process Hazards Management Program 1978

  - Departmental Process Hazards Coordinators
  - Indepth Hazard Reviews for Engineering Department New Projects

FREQUENCY OF REVIEWS

HAZARD CLASS AND FREQUENCY	EXAMPLES
HIGH 2-3 YEARS	MANUFACTURING AND OPERATIONS WITH UNSTABLE MATERIALS OR EXPLOSIVES. ACETYLENE COMPRESSION AND PURIFICATION. TFE REACTORS.
MODERATE 3-5 YEARS	OXIDATIONS OR NITRATIONS. ETHYLENE OXIDE PRODUCTION. PROCESSES INVOLVING FLAMMABLE LIQUIDS.
LOW 5-7 YEARS	PROCESSES INVOLVING COMBUSTIBLE MATERIALS. STEAM GENERATION.


PLANT SAFETY PROGRAM
AUDITS
TRAINING
PROCESS HAZARDS MANAGEMENT
OTHERS
PROCEDURE REVIEWS
INCIDENT REPORTS
PROCESS HAZARDS REVIEWS
OTHERS
CHECKLIST
FAILURE MODE & EFFECT ANALYSIS OR HAZOP
FAULT TREE ANALYSIS

PROCESS HAZARDS REVIEW PROCEDURE

STEP 1 - REVIEW TEAM SELECTION AND
REVIEW SCOPE ESTABLISHMENT

STEP 2 - PROCESS DESCRIPTION AND DIVISION

STEP 3 - HAZARDS IDENTIFICATION

STEP 4 - DECISION TREE FOR REVIEW METHOD SELECTION

STEP 5 - HAZARDS ANALYSES
("HOW OFTEN?"; "HOW BIG?")

STEP 6 - RECOMMENDATIONS ("SO WHAT?")

STEP 7 - DOCUMENTATION, WITH RESPONSIBILITIES
AND TIMING ON ALL RECOMMENDATIONS

PHR COMMITTEES

CHAIRMAN

- Assures Comprehensive and Intensive Review
- Documentation and Communication
- Arranges for Process Description

PARTICIPANTS

- Operations - Procedures, Past Incidents
- Technical - Process Basis and Limits
- Maintenance - Inspections, Equipment problems
- Consultants - Instruments, Special Systems

HAZARDS IDENTIFICATION

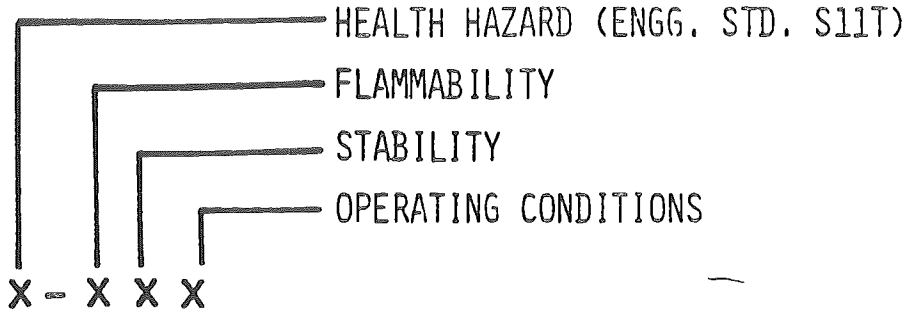
AN ATTEMPT SHOULD BE MADE TO IDENTIFY ALL PROCESS HAZARDS IN THE INITIAL STAGES OF THE HAZARDS REVIEW.

OCCASIONALLY, ADDITIONAL HAZARDS ARE UNCOVERED DURING LATER STAGES IN THE REVIEW.

INITIAL ASSESSMENT TECHNIQUES

- PROCESS HAZARDS CLASSIFICATION SYSTEM (4-DIGIT SUMMARY OF MATERIAL SAFETY DATA)
- CHEMICAL INTERACTION MATRIX
- SERIOUS INCIDENT REVIEW
- PREVIOUS ANALYSES AND REPORTS
- EXPERIENCE; CONSULTANTS

PROCESS HAZARD CLASSIFICATION



EACH CATEGORY RATED 0 TO 4 (LOWEST 0, HIGHEST 4)

- HEALTH SCORE - BASED ON ANALYSIS OF 8 FACTORS:

1. TOXIC ROUTE - ROUTE OF ENTRY INTO BODY
2. ACUTE - SHORT TERM EXPOSURE - IMMEDIATE EFFECTS
3. CHRONIC - LONG TERM EXPOSURE - EVENTUAL EFFECTS
4. WARNING - ABILITY TO DETECT BEFORE OVEREXPOSURE
5. PHYSICAL - CONDITION OF CHEMICAL AT OP. COND. (SOLID, LIQ., VAPOR)
6. AMOUNT - LB/YR CHEMICAL HANDLED
7. EXPOSURE - NUMBER OF EMPLOYEES EXPOSED
8. DEGREE - NUMBER OF EMPLOYEES EXPOSED

- FLAMMABILITY - FLASH PT. (LIQUIDS); DP/DT (DUSTS)
- STABILITY - DEGREE OF SELF-REACTION
- OPERATING CONDITIONS - STORAGE; PROCESSING; REACTION

TABLE I
PROCESS HAZARD CLASSIFICATION

Hazard Class***	Health	Flammability	Stability	Operating Conditions
	Highest Chemical Hazard Score*			
0	8-13	Materials that will not burn (at 1500°F for 5 min)	Not capable of self-reaction	Storage at ambient conditions
1	14-19	Materials with Fl. Pt. $\geq$ 200°F; dust with $\frac{dp}{dt}$** < 1000 psi/sec	Normally stable; unstable only at temperature >300°C above normal temperature	Physical Processing (mixing, pumping, distilling), storage at >15 psig or >60°C
2	20-25	Liquid with: 100° $\leq$ Fl. Pt. < 200°F dust with: 1000 $\leq \frac{dp}{dt}$ < 2000 psi/sec	Subject to decomposition or exothermic self-reaction and not capable of detonation	Chemical reaction near boiling point
3	26-35	Combustible liquid above Fl. Pt.; liquid with Fl. Pt. < 100°F: or flammable gas $\leq$50 psig; dust with: 2000 $\leq \frac{dp}{dt}$ < 4000 psi/sec	Capable of detonation or explosive reaction with strong confinement or initiation	Exothermic reaction with $\geq$50M lbs inventory or $\geq$25M pph throughput, or at $\geq$100 psig, or $\geq$B. Pt.
4	36-64	Combustible liquid above B. Pt.; liquid with Fl. Pt. < 0°C; or operation above autoignition temp. or near explo. range; or flam. gas > 50 psig; dust with $\frac{dp}{dt} \geq$ 4000 psi/sec	Readily capable of detonation or explosive reaction at ambient conditions	Exothermic reaction with $\geq$50M lbs inventory or $\geq$25M pph throughput and at $\geq$100 psig, and $\geq$B. Pt. or any hazardous reaction difficult to control

References: * Refer to Table II
NFPA 704M, "Identification of the Fire Hazards of Materials"
Design Standard DE1D, "Environmental Classification for Electrical Installations"
U.S. Bureau of Mines Report of Investigations No. 5971 "Explosibility of Dusts Used in the Plastics Industry" (1962).

** Dust $\frac{dp}{dt}$ based on tests in 1.23 L Hartman bomb using the finest 25 percent (by weight) portion of the sample.

*** The complete Process Hazard Classification would be in the form "HFSO" (for example: "4421" for storage of 25 tons of hydrogen cyanide).

3/31/82
3642W:dlm

TABLE II
HEALTH HAZARD[1]

Score is Total of the Eight Categories
Low Toxicity Materials Scoring 1 in Categories 2 and 3 are Health Hazard Class 0

CATEGORIES	1	2	4	8
1. Toxic Route	Eye or mouth	Skin	Lung	Lung and skin
2. Acute Toxicity[2] (Human or animal)				
Oral LD50[3]	>500	50-500	5-50	<5
Inhalation LC50[4]	>1000	100-1000	10-100	<10
Skin LD50[3]	>5000	200-5000	10-200	<10
Subjective: Conc. > STEL, < 0.1 LC50 or Dose < 0.1 LD50	Minor injury, readily reversible	Severe, reversible irritation or skin sensitizer	Life-threatening or permanent injury	Rapidly fatal
3. Chronic toxicity[2] Repeated exposures: Conc. > TLV, < STEL; or Dose < 0.01 LD50	Minor reversible injury	Serious reversible injury	Permanent or cumulative injury	Fatal; carcinogens; embryotoxins
4. Warning properties: odor, irritation, color, or taste	< TLV or < 1/10 STEL; or < 1/100 LD50	> TLV and < STEL; or > 1/100 LD50 and < 1/10 LD50	> STEL and < LC50; or > 1/10 LD50 and < LD50	> LC50; or > LD50
5. Physical factor (leak or spill)	Non-dusty solid Non-volatile liquid	Low-volatility liq. pp 0.3-10 mm at 25°C	Volatile liquid pp 10-300 mm Hg	Gas, aerosol, dust, or liquid pp > 300 at 25°C
6. Amount used (lbs/yr)	<100	100-10,000	10,000-1,000,000	>1,000,000
7. Number of employees[5]	1-4	5-24	25-125	>125
8. Degree of exposure	Enclosed process good ventilation; few spills	Enclosed process; fair leak/spill performance	Frequent opening of equipment; high potential for leaks	Open process, manual handling

1. Ref: Engineering Standard S11T (TLV: Threshold Limit Value; STEL: Short Term Exposure Limit)
2. When these scores are selected by comparison with a structurally similar chemical, the next higher score is used.
3. mg/kg (LD50: Dose lethal to 50 percent of those exposed; LC50: Concentration lethal to 50 percent of those exposed.)
4. ppm by volume, for a 4-hour exposure (for shorter exposures, use LC50 (t) = (4)(LC 50)/t
5. Employees regularly assigned to the area who are likely to be exposed to the chemical.

INTERACTION MATRIX

DOES X REACT WITH Y TO CAUSE A PROBLEM

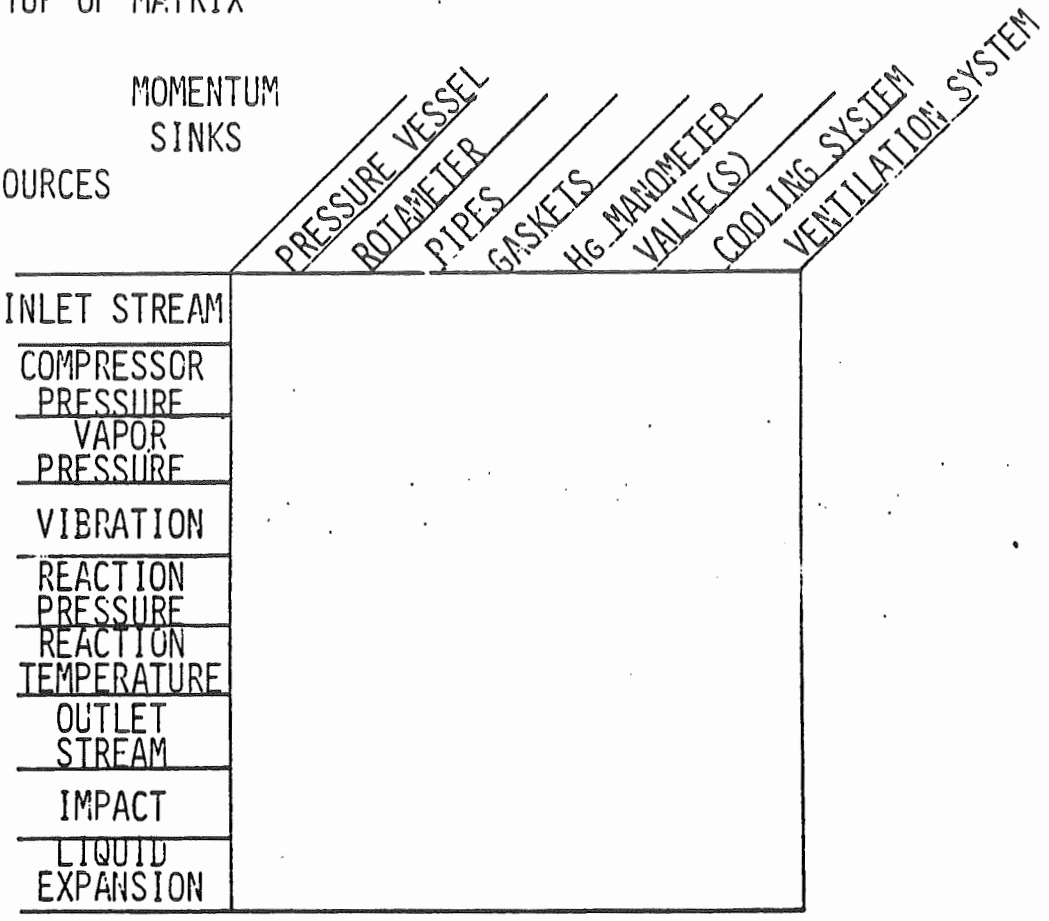
Y \ X	Cl_2	BUTADIENE	HCl	AIR	PEROXIDE	LUBE OIL	STEEL
Cl_2	N	Y	N	N	Y	Y	Y
BUTADIENE		Y	Y	Y	?	?	N
HCl			N	N	Y	Y	Y
AIR				N	Y	N	N
PEROXIDE					Y	Y	?
LUBE OIL						N	N
STEEL							N

Y = YES N = NO ? = DON'T KNOW

- LIST SHOULD INCLUDE ALL MATERIALS, INCLUDING KNOWN IMPURITIES.
- FOR EACH "Y", THE TYPE OF REACTION - AND THE CONDITIONS NECESSARY, SHOULD BE DETERMINED.

ANTICIPATION OF HAZARDS
MOMENTUM SOURCES AND SINKS MATRIX

GENERAL SETUP OF MATRIX



EXAMPLE: Compare "Impact" to "Hg Manometer" and ask questions such as "Will the manometer be exposed to impact? How much impact? What has been done to avoid this impact? What happens if it occurs?" (Consider normal and abnormal conditions, as well as start-up and shutdown.)

PROCESS HAZARDS TECHNIQUES

CHECKLIST

- Tabulated "What if . . .?"
- Identify obvious hazards in the least time for large areas
- Limited depth

FAILURE MODE & EFFECT

- Component ⟶ Consequences
- Approximate ranking of hazards - probability and severity
- Nonquantitative
- Limited consideration of human failures and missing components

HAZOP

- Failure ⟵ Intent ⟶ Consequence
- Tabulated "What if"
- Key words
- Non Quantitative

FAULT TREE ANALYSIS

- Consequence ⟶ Component
- Quantitative risk analysis
- Human failures
- Common modes and multiple failures
- Cost/Benefit evaluation

CHECKLIST

(WHAT IF . . .?)

PROS

- IDENTIFY OBVIOUS HAZARDS IN THE LEAST TIME FOR LARGE AREAS
- ASSESS "FAIL SAFETY" OF POWERED EQUIPMENT
- IDENTIFY TYPES OF POTENTIAL SERIOUS INCIDENTS
- USEFUL IN LATER REVIEWS

CONS

- LIMITED DEPTH
- INADEQUATE INVESTIGATION OF HUMAN FAILURES AND PROCESS CHEMISTRY

FAILURE MODE AND EFFECT

PROS

- Identify Component Failure Modes and Evaluate Consequences
- Approximate Ranking of Hazards Using Probability and Severity
- Provide a Basis to Substantiate Recommendations and Establish Priorities for Corrections

CONS

- Nonquantitative
- Limited Consideration of Human Failures and Missing Components

HAZARD AND OPERABILITY STUDIES (HAZOPS)

HAZOP

PROS

- Identifies Failures Leading to Hazardous Consequences
- Considers Human Failures

CONS

- Nonquantitative
- Limited Consideration of Common Mode Failures

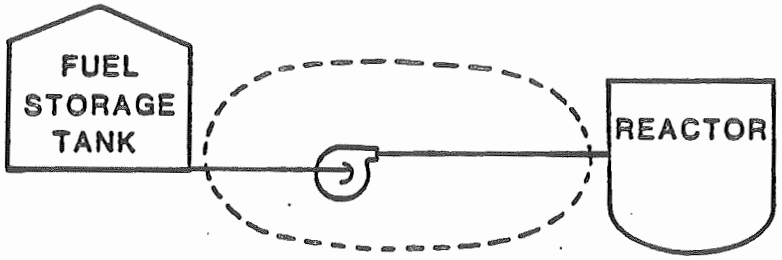
PRINCIPLES OF HAZOPS

GUIDE WORDS*
NONE
MORE OF
LESS OF
PART OF
MORE THAN
OTHER

CAUSE ➸ DEVIATION (From standard condition) ➸ CONSEQUENCES (Trivial, important, catastrophic)

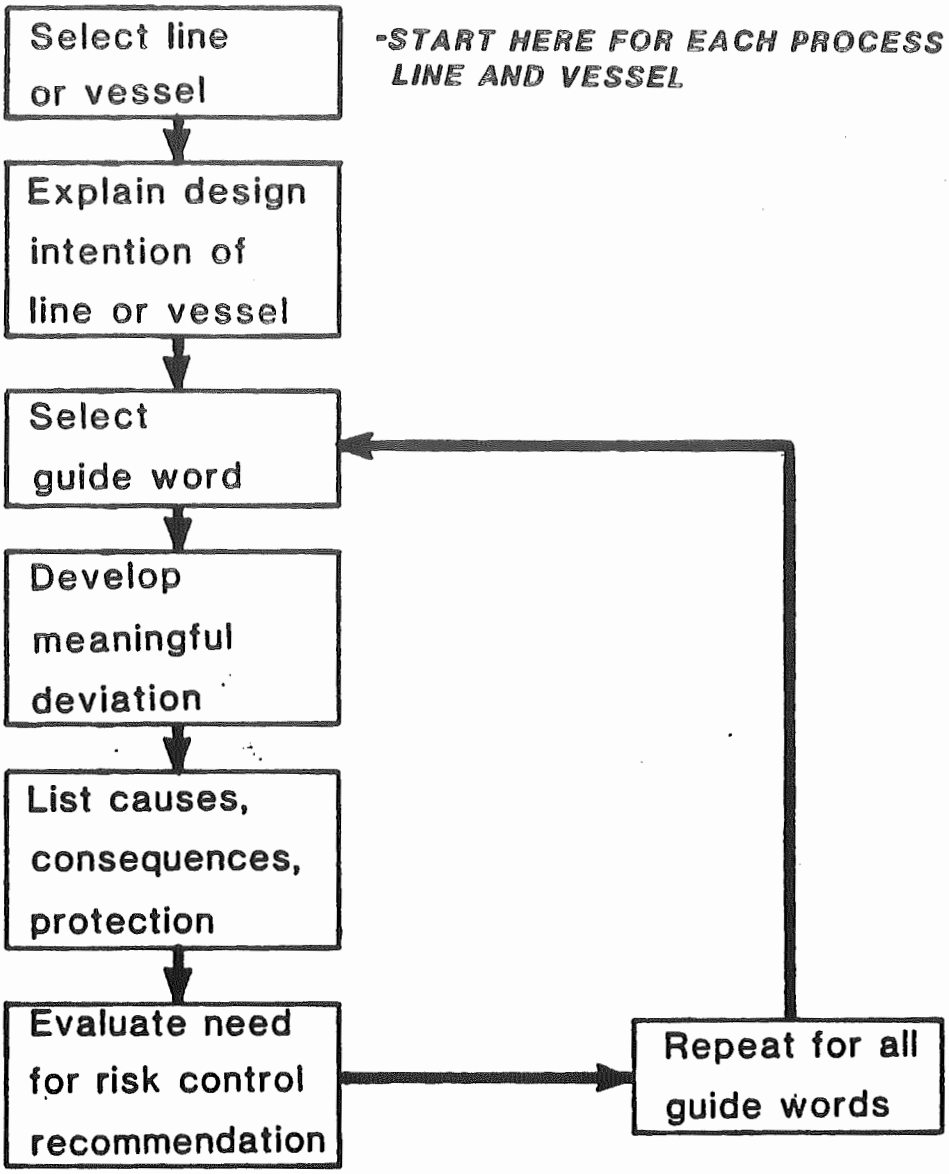
*COVERING EVERY PARAMETER RELEVANT TO THE SYSTEM UNDER REVIEW:
i.e. Flow Rate, Flow Quantity, Pressure, Temperature, Viscosity, Components

DESIGN INTENTION EXAMPLE



FUEL LINE: TRANSFER FUEL FROM STORAGE TANK TO REACTOR

HAZOPS PROCEDURE



Note: Apply all guide words to each process line; apply only the guide word "other" to vessels

MEANING OF GUIDE WORDS USED TO DERIVE PROCESS DEVIATIONS

NONE: No forward flow when there should be i.e. no flow, reverse flow

MORE OF: More of any relevant physical parameter than there should be i.e. more flow (rate, quantity), more pressure or dP, more temperature, more viscosity etc.

LESS OF: Opposite to "more of"

PART OF: System composition different from what it should be

MORE THAN: More things present than should be e.g. extra phases, impurities

OTHER: What needs to happen other than normal operation e.g. start up, shut down, maintenance, provision for services failures, spare equipment needed, omitted equipment or instrumentation

HAZOPS

Guide Word Sequence

1) No flow

2) Reverse flow

3) Less flow (rate; quantity)

4) More flow (rate; quantity)

5) More pressure

6) Less pressure

7) More temperature

8) Less temperature

9) More of/ Less of (any other relevant physical parameter)

10) Composition differences ("part of")

11) Extra things present ("more than")

12) Other

DECISION ON NEED FOR ACTION

Need for action (Process or procedure changes) is based on level of risk for each deviation cause:

$$\text{"RISK"} = \frac{\boxed{\text{Frequency of occurrence}} \times \boxed{\text{Seriousness of consequences}}}{\boxed{\text{Effectiveness of existing protective systems}}}$$

-Major risk decisions may need to be assessed quantitatively (e. g. by Fault Tree Analysis)

-For less important risks, need for action can be based on experience and judgment

RISK REDUCTION

Risks can be reduced by one or more of the following:

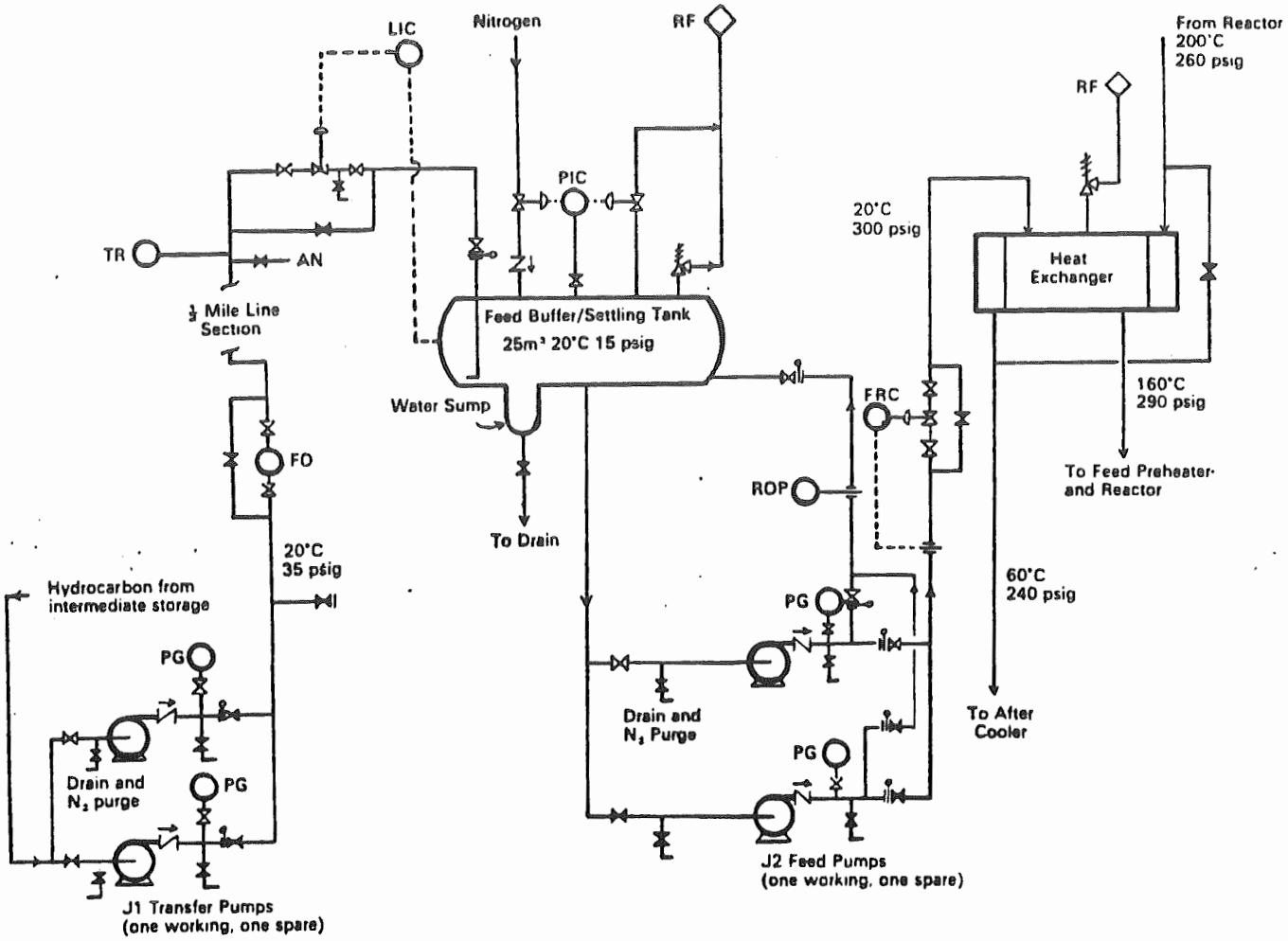
1) Reduce frequency of occurrence of process deviation cause

2) Reduce seriousness of consequences of uncontrolled deviation

3) Increase effectiveness of protection against uncontrolled deviation

HAZOPS EXAMPLE

FEED SECTION OF PROPOSED OLEFIN DIMERISATION PLANT



HAZOPS EXAMPLE

OPERABILITY STUDY OF PROPOSED OLEFIN DIMERISATION UNITS: RESULTS OF LINE SECTION FROM INTERMEDIATE STORAGE TO BUFFER/SETTLING TANK

The guide words are applied to the design intention which states what the equipment is expected to DO.

Guide Word	Deviation	Possible Causes	Consequences	Action Required
NONE	NO FLOW	(1) No hydrocarbon available at intermediate storage	Loss of feed to reaction section and reduced output. Polymer formed in heat exchanger under no flow conditions	(a) Ensure good communications with intermediate storage operator (b) Install low level alarm on settling tank LIC
		(2) J1 pump fails (motor fault, loss of drive, impeller corroded away, etc.)	As for (1)	Covered by (b)
		(3) Line blockage, isolation valve closed in error, or LCV fails shut	As for (1) J1 pump overheats	Covered by (b) (c) Install kickback on J1 pumps (d) Check design of J1 pump strainers
		(4) Line fracture	As for (1) Hydrocarbon discharged into area adjacent to public highway	Covered by (b). (e) Institute regular patrolling and inspection of transfer line
MORE OF	MORE FLOW	(5) LCV fails open or LCV bypass open in error	Settling tank overfills	(f) Install high level alarm on LIC and check sizing of relief opposite liquid over-filling (g) Institute locking off procedure for LCV bypass when not in use
			Incomplete separation of water phase in tank leading to problems on reaction section	(h) Extend J2 pump suction line to 12 in above tank base
	MORE PRESSURE	(6) Isolation valve closed in error or LCV closes, with J1 pump running	Transfer line subjected to full pump delivery or surge pressure	(j) Covered by (c) except when kickback blocked or isolated. Check line, FQ and flange ratings, and reduce stroking speed of LCV if necessary. Install a PG upstream of LCV and an independent PG on settling tank

(continued)

Guide Word	Deviation	Possible Causes	Consequences	Action Required
		(7) Thermal expansion in an isolated valved section due to fire or strong sunlight	Line fracture or flange leak	(k) Install thermal expansion relief on valved section (relief discharge route to be decided later in study)
MORE OF (cont'd.)	MORE TEMPERATURE	(8) High intermediate storage temperature	Higher pressure in transfer line and settling tank	(l) Check whether there is adequate warning of high temperature at intermediate storage. If not, install
LESS OF	LESS FLOW	(9) Leaking flange or valve stub not blanked and leaking	Material loss adjacent to public highway	Covered by (e) and the checks in (j)
	LESS TEMPERATURE	(10) Winter conditions	Water sump and drain line freeze up	(m) Lag water sump down to drain valve, and steam trace drain valve and drain line downstream
MORE THAN	ORGANIC ACIDS PRESENT	(11) Disturbance on distillation columns upstream of intermediate storage	Increased rate of corrosion of tank base, sump and drain line	(n) Check suitability of materials of construction
PART OF	HIGH WATER CONCENTRATION IN STREAM	(12) High water level in intermediate storage tanks	Water sump fills up more quickly. Increased chance water phase passing to reaction section	(p) Arrange for frequent draining off of water from intermediate storage tank. Install high interface level alarm on sump
	HIGH CONCENTRATION OF LOWER ALKANES OR ALKENES IN STREAM	(13) Disturbance on distillation columns upstream of intermediate storage	Higher system pressure	(q) Check that the design of settling tank and associated pipework, including relief valve sizing, will cope with sudden ingress of more volatile hydrocarbons
OTHER	MAINTENANCE	(14) Equipment failure flange leak, etc.	Line cannot be completely drained or purged	(r) Install low-point drain and N_2 purge point downstream of LCV. Also N_2 vent on settling tank

NB No hazards were evident from consideration of REVERSE or LESS PRESSURE.

NOTE: This example does not include a column to document existing protective systems.

ZOP PROCESS HAZARD STUDIES
OJECT ____ - _____ WORKS
_____ MANUFACTURING FACILITIES

TE: _____ REVIEW TEAM _____

OCESS & INSTRUMENT DIAGRAM W-_____ TITLE: _____ REVIEW HOURS: _____

NUMBER / PIPE LINE NO.: _____ DESCRIPTION: _____

SIGN INTENTION: _____

IDE	DEVIATION	CAUSE	CONSEQUENCES	PROTECTION	RECOMMENDED ACTION
NE					
RE OF					
SS OF					

PART OF	
MORE THAN	
OTHER	

Line or Vessel: _____ Page _____

Design Intention: _____

HAZOP STUDY

Guide	Deviation	Cause	Consequences	Protection	Recommended Action

FAULT TREE ANALYSIS

OBJECTIVE

TO REDUCE THE LIKELIHOOD OF A SELECTED UNDESIRED EVENT. TO IDENTIFY DESIGN AND OPERATING DEFICIENCIES BY MODELING BASIC FAILURE EVENTS AND QUANTITATIVELY ANALYZING FAILURE OCCURRENCES.

PROS

- QUANTITATIVE EVALUATION FOR DECISION MAKING AND COMPARISON WITH SAFETY GUIDELINES
- MODELS HUMAN FAILURES AND PROCESS CHEMISTRY
- HANDLES COMMON-MODE FAILURES

CONS

- TIME CONSUMING
- LIMITED SCOPE
- DIFFICULT

DECISION TREE

REVIEW METHOD SELECTION

FACTORS TO BE CONSIDERED:

- HAZARD SEVERITY (FATALITIES, INJURIES, $ LOSS)
- OFF-SITE EXPOSURE OR DAMAGE (RISK TO PUBLIC)
- HAZARD TYPE (EXPLOSION, TOXIC RELEASE, FIRE,...)
- PROCESS MATERIALS (INSTABILITY, TOXICITY, REACTIVITY,...)
- PROCESS EXPERIENCE (SITE, COMPANY, INDUSTRY)
- RATE OF TECHNOLOGY CHANGE (DYNAMIC VS STABLE)
- PREVIOUS HAZARDS ANALYSES (ADEQUACY; APPLICABILITY)
- HAZARD CONTROL BY STANDARD PROTECTION EQUIPMENT (EG, EMERGENCY RELIEF SYSTEMS)
- COMPLEXITY OF PROCESS CONTROL (INSTRUMENTATION)
- MANAGEMENT STRATEGIES ("BIG EVENT" FIRST; CREDIBILITY OF METHOD; ETC)

PROCESS HAZARDS REVIEW

DECISION TREE FOR REVIEW METHOD SELECTION

Purpose - When a process hazard review is started, one of the initial decisions is selection of review methods capable of identifying process safety deficiencies with minimum effort. The Decision Tree provides guidelines for selecting the minimum appropriate review methods based on several process and risk criteria. Factors combined in the Decision Tree include hazard severity, hazard type, and process complexity. Hazard review methods selected by the Decision Tree are:

Fault Tree Analysis (FTA) - This is the most complex technique, and it is for analyzing a specific hazard event. When the process hazards review is being done for a process area rather than an event, an FMEA or Checklist will also be required as indicated by the Decision Tree.

Failure Mode and Effect Analysis (FMEA) - This is a moderately complex technique which is frequently indicated for chemical process areas. The HAZOP technique can be used as a substitute for FMEA (see S&F Guideline, Section 6.4).

Checklist - This is the minimum requirement for all process hazard reviews.

Procedure

1. A committee consisting of people familiar with the process equipment, chemistry, and operating procedures should divide the process into major steps or operations (polymerization, absorption, distillation, etc).

2. The committee should then list the significant hazardous events associated with the process divisions identified in Step 1. Examples of hazardous events include toxic releases, vapor cloud explosions, vessel ruptures, and fires. (Usually processes have more than one hazard associated with them.)

3. The committee should then use the Decision Tree to determine the most appropriate analysis technique for each hazardous event, based on the type of hazard and the process characteristics.

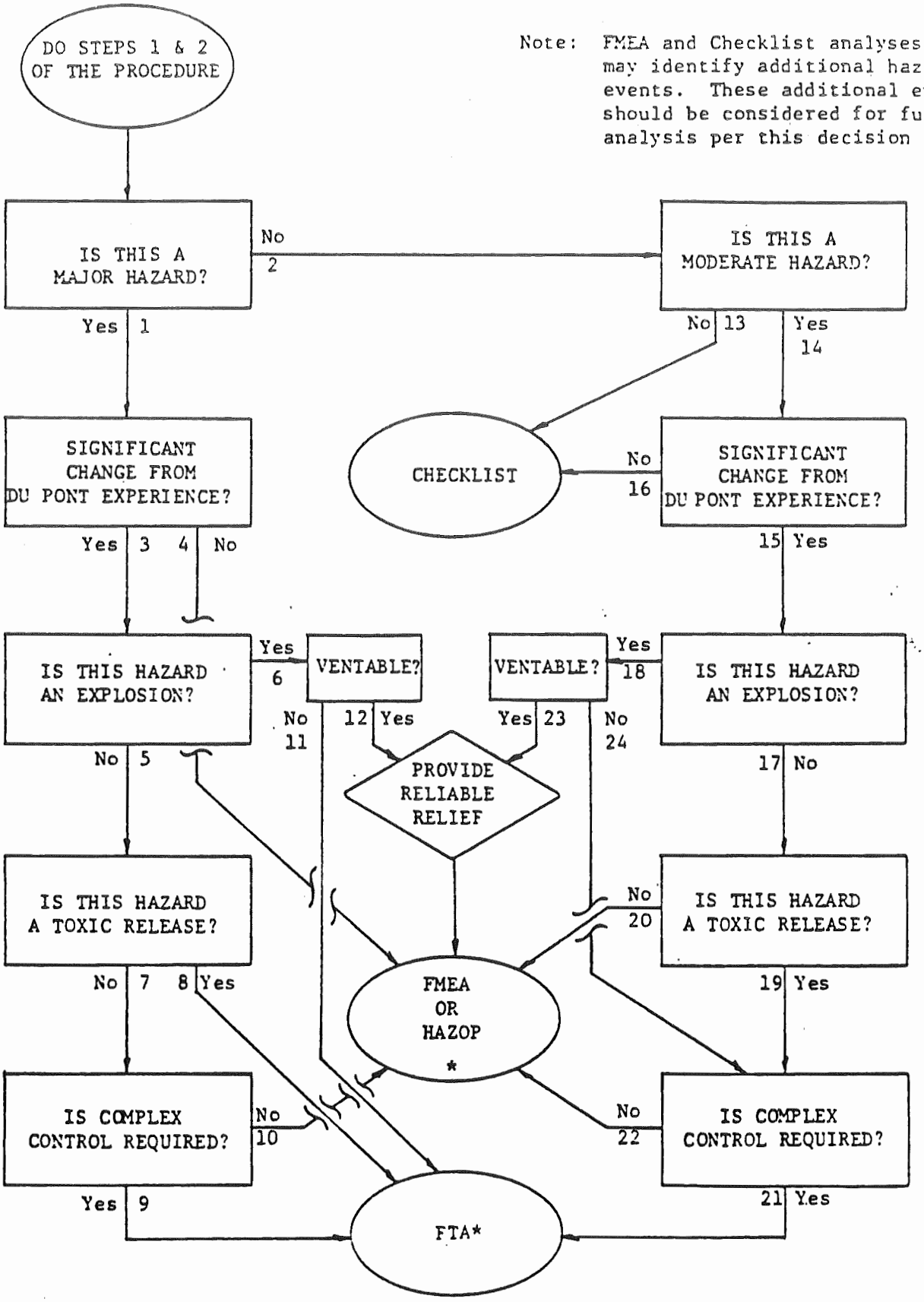
4. When a specific hazardous event is to be evaluated by Fault Tree Analysis, additional review techniques (Checklist and FMEA) are usually necessary to provide a complete process hazard review. FTA is merely an event review, so it fails to evaluate other equipment or process failures that may contribute to other hazards. Checklist and FMEA studies are area reviews and thereby can incorporate all equipment pieces and procedures associated with a process.

5. The final authority as to which hazard review techniques will be used rests with the Hazard Review Committee. The Decision Tree is only an aid. Various hazard review objectives or process characteristics may make, for instance, a Fault Tree Analysis more appropriate, even though the Decision Tree indicates a Failure Mode and Effect analysis.

6. The use of the Decision Tree should be documented (recording the numbered routes) for the benefit of future reviews.

DECISION TREE

FOR REVIEW METHOD SELECTION



*ALSO USE CRITICAL ITEMS CHECKLIST

DEFINITIONS

MAJOR HAZARD: An event with reasonable potential for

1) multiple fatalities, or

2) hazardous exposures outside the plant, or

3) property plus business-interruption loss of $2MM or more.

Note: Evaluation of "reasonable potential" should include considerations such as normal occupancy in the vicinity of the hazard, area fire portection facilities, and probability of escape from the hazard.

MODERATE HAZARD: An event with reasonable potential for

1) a single fatality, or

2) multiple serious injuries, or

3) property plus business-interruption loss of $100M to $2MM

SIGNIFICANT CHANGE FROM DU PONT EXPERIENCE: A process and its associated equipment is considered a significant change from Du Pont experience if any of the following criteria is not met:

1) The Company has several operating years of experience with identical or similar process chemistry, equipment, and operating procedures, and

2) the experience has been good (safe) experience, and

3) an adequate hazard analysis has been done

Note: The significance of a process change must be evaluated relative to a specific hazardous event. As an example, consider a reactor process being modified for operation at a higher temperature. Two hazardous events have been identified: "explosion in the reactor" and "external fire - small leak." The higher operating temperature is a significant change relative to the explosion hazard. But protection against leaks/fires will rely on prior experience in the design of seals and fittings for specific environments. Thus, increased temperature does not create a significant change relative to a leak hazard.

Examples of changes include reduced temperature margins between normal and runaway conditions, reduced pressure margins between normal and vessel rating, new type of catalyst, new feed ratios, increased heat input, new cooling method, and different accessory equipment configuration.

VENTABLE EXPLOSION: Any pressure-generating event where the pressure can be vented reliably and safely using standard overpressure protection equipment. If the process will impair the vent's reliability through plugging or corrosion, the explosion is not considered a ventable explosion.

HIGHLY TOXIC MATERIAL: A material with a score of 29 or greater per Engineering Standard S11T.

COMPLEX CONTROL: Instrumentation where proper operation of automatic controls and interlocks is necessary to insure safety, ie, the process is not intrinsically safe. "Complex Control" also applies to complex control systems and to systems where small departures in operating conditions lead to hazardous incidents.

RELIABLE RELIEF: Rupture disks, relief valves, or explosion panels with adequate vent area (as determined from appropriate data, tests, or experience). The discharge piping should vent materials safely to prevent exposing people to excessive concentrations of toxic materials, thermal radiation, blasts from vapor cloud explosions, or noise. Also the discharge piping should be adequately supported against reaction forces.

CHECKLIST FOR CRITICAL PROCESS SAFETY ITEMS

(With Engineering Standards References)

(To be done before a Failure Mode and Effect or Fault Tree Analysis.)

PROCESS _____ DATE _____

"Last-Resort" Emergency-Control Features

Condition

1. Relief Valves (or Rupture Disks)
   a. Protection of every closed vessel - from fire exposure, process overpressure, overfilling, etc. (F2G, F13G, F3K)
   b. Proper installation to avoid pinching shut or breaking off from reaction forces or thermal shock.
   c. Discharge of vented materials in a safe direction and height. (S17G, K9R)
2. Drainage or Dikes
   a. Provided wherever flammable liquids are handled, where combustible materials which do not freeze or congeal at ambient temperature are handled above their flash points, or wherever sprinkler protection is installed. (F16G)
   b. Cable and instrument trays not severely exposed to fire in drainage systems or diked areas.
3. Emergency Shutoff Devices
   a. Local shutoff switches or valves for powered equipment.
   b. Shutoff devices for heating media, fuels, hazardous raw materials, etc., sufficiently remote from the process to be accessible in an emergency and adequately labeled.
4. Propagation Prevention
   a. Fire walls, barricades, or distance commensurate with process "energy." (F24B, F1K)
   b. Isolation of continuous ignition sources (flares, burners, etc.) from the process, by inerting or arresters. (F4J)

Condition

5. Adequate Knowledge of Process Materials

   a. Toxicity (S2T)

   b. Stability (autodecomposition; unstable intermediates)

6. Procedures

   a. Operating and emergency procedures up-to-date and readily available.

   b. Analysis of raw materials prior to use.

   c. Test procedures for relief devices and interlocks. (SG6T, SG7T, R113J)

   d. Conformance with electrical classifications. (DE1D)

7. Proper Materials of Construction - To avoid sudden, unpredictable equipment failure.

8. Guard Devices for Fatality Prevention

   a. Protection from falling from elevated locations. (S1A)

   b. Protection from falling into equipment. (S1M)

9. Adequate Exit Facilities and Safe Rally Spots (S1C)

10. Protection from Vehicles

11. Pressure Vessel Procedure and Adequate Compliance (SG5T)

CHECKLISTS

APPENDIX A
CHECKLISTS FOR COMMITTEE MEMBERS

1. INTRODUCTION

The following checklists for committee members were derived from "what-if" questions and attempt to cover all important aspects of a production operation. The words or phrases in the lists should serve to stimulate questions concerning the subject.

2. EXAMPLE

The phrase "Materials of Construction" should lead to such questions as:

- "Have suitable materials been used in vessels, piping, instruments, instrument connections, agitators, dip tubes, valves, valve packing, vessel supports, flange bolts, expansion joints, etc?"
- "Are corrosion tests needed or desirable?"
- "Where plastic pipe linings or equipment is used, are the temperatures and pressures low enough or adequately controlled?"

PROCESS HAZARDS CHECKLIST

Plant _____

Process _____

CATEGORY	SUBJECTS TO BE INVESTIGATED		OPERATIONS	ENGINEERING	TECHNICAL	DATE COMPLETED
STORAGE OF RAW MATERIALS, PRODUCTS, INTERMEDIATES	Storage Tanks	Design, Separation, Inerting	☐☐			____
	Dikes	Capacity, Drainage	☐☐			____
	Emergency Valves	Remote Control – Hazardous Mat'ls.	☐			____
	Inspections	Flash Arrestors, Relief Devices		☐		____
	Procedures	Contamination Prevention, Analysis			☐	____
	Specifications	Chemical, Physical, Quality, Stability			☐	____
	Limitations	Temperature, Time, Quantity			☐	____
MATERIALS HANDLING	Pumps	Relief, Reverse Rotation, Identification	☐			____
	Ducts	Explosion Relief, Fire Protection, Support	☐☐			____
	Conveyors, Mills	Stop Devices, Coasting, Guards	☐☐			____
	Procedures	Spills, Leaks, Decontamination	☐			____
	Piping	Ratings, Codes, Cross-Connections			☐	____
PROCESS EQUIPMENT, FACILITIES, AND PROCEDURES	Procedures	Startup, Normal, Shutdown, Emergency	☐			____
	Conformance	Job Audits, Shortcuts, Suggestions	☐☐			____
	Loss of Utilities	Elect., Heating, Coolant, Air, Inerts, Agitation	☐☐			____
	Vessels	Design, Materials, Codes, Access	☐☐			____
	Identification	Vessels, Piping, Switches, Valves	☐☐			____
	Relief Devices	Reactors, Exchangers, Glassware	☐☐			____
	Review of Incidents	Plant, Company, Industry	☐			____
	Inspections, Tests	Vessels, Relief Devices, Corrosion		☐		____

PROCESS HAZARDS CHECKLIST (continued)

CATEGORY	SUBJECTS TO BE INVESTIGATED		OPERATIONS	ENGINEERING	TECHNICAL	DATE COMPLETED
PROCESS EQUIPMENT, FACILITIES, AND PROCEDURES (CONT'D)	Electrical	Area Classification, Conformance, Purging		☐		
	Process	Description, Test Authorizations			☐	
	Operating Ranges	Temp., Press., Flows, Ratios, Concentrations, Densities, Levels, Time, Sequence			☐	
	Ignition Sources	Peroxides, Acetylides, Friction, Fouling, Compressors, Static Elect., Valves, Heaters			☐	
	Compatibility	Heating Media, Lubricants, Flushes, Packing			☐	
	Safety Margins	Cooling, Contamination			☐	
PERSONNEL PROTECTION	Protection	Barricades, Personal, Shower, Escape Aids	☐			
	Ventilation	General, Local, Air Intakes, Rate	☐			
	Exposures	Other Processes, Public Environment	☐			
	Utilities	Isolation: Air, Water, Inerts, Steam		☐		
	Hazards Manual	Toxicity, Flammability, Reactivity, Corrosion, Symptoms, First Aid			☐	
	Environment	Sampling, Vapors, Dusts, Noise, Radiation			☐	
CONTROLS AND EMERGENCY DEVICES	Controls	Ranges, Redundancy, Fail-safe	☐			
	Calibration, Inspection	Frequency, Adequacy	☐			
	Alarms	Adequacy, Limits, Fire, Fume	☐			
	Interlocks	Tests, Bypass Procedures	☐			
	Relief Devices	Adequacy, Vent Size, Discharge, Drain, Support	☐			
	Emergencies	Dump, Drown, Inhibit, Dilute	☐			
	Process Isolation	Block Valves, Fire-safe Valves, Purging	☐			
	Instruments	Air Quality, Time Lag, Reset Windup		☐		
	Hazards	Hang-fires, Runaways			☐	
WASTE DISPOSAL	Ditches	Flame Traps, Reactions, Exposures, Solids	☐			
	Vents	Discharge, Dispersion, Radiation, Mists	☐			
	Characteristics	Sludges, Residues, Fouling Materials			☐	
SAMPLING FACILITIES	Sampling Points	Accessibility, Ventilation, Valving	☐			
	Procedures	Pluggage, Purging	☐			
	Samples	Containers, Storage, Disposal			☐	
	Analysis	Procedures, Records, Feed-back			☐	
MAINTENANCE	Decontamination	Solutions, Equipment, Procedures	☐			
	Vessel Openings	Size, Obstructions, Access		☐		
	Procedures	Vessel Entry, Welding, Lockout		☐		
FIRE PROTECTION	Fixed Protection	Sprinklers, Deluge, Monitors: Adequacy	☐			
	Extinguishers	Type, Location, Training	☐			
	Fire Walls	Adequacy, Condition, Doors, Ducts	☐			
	Drainage	Slope, Drain Rate	☐			

PROCESS HAZARDS REVIEW CHECKLIST

The following checklist is to be used as the standard with "Checklist" type Process Hazard reviews at the Dordrecht site. This list is intended to cover the most important aspects of all possible questions with all operations.

The questions listed should be used to stimulate the identification of potential hazards and should not be simply answered by a "Yes or "No". Obviously not all questions will be applicable to the review of a given production operation.

I. PROCESS CHECKLIST

NOTE: Consider the checklist in terms not only of steady-state operation but also start-up, shutdown, and upsets of all conceivable types.

A. Materials

- Have materials been defined as "hazardous" or "non-hazardous" (ingredients as well as final and by products).
- What process materials are unstable or spontaneously ignitable?
  - What evaluation has been made of impact sensitivity?
  - Has an evaluation of possible uncontrolled reaction or decomposition been made?
- What precautions are necessary to meet environmental requirements and health of personnel?
- What data is available on amount and rate of heat evolution during decompositions of any material in the process?
- What precautions are necessary for flammable materials?
- What flammable dust hazards exist?
- What materials are highly toxic?
- What has been done to assure that materials of construction are compatible with the chemical process materials that are involved?
- What maintenance control is necessary to assure replacement of proper materials, e.g., to avoid excessive corrosion, to avoid producing hazardous compounds with reactants?

- What changes have occurred in composition of raw materials and what resulting changes in process?
- What is done to assure sufficient control of raw material identification and quality?
- What hazards can occur as a result of loss of gas for purging, blanketing, or inerting? How certain is gas supply quality?
- What precautions need to be considered relative to stability of all materials in storage?
- What fire extinguishing agents are compatible with process material?
- What fire emergency equipment and procedures are being provided?

B. Reactions

- How are potentially hazardous reactions isolated?
- What process variables could, or do, approach limiting conditions for hazard?
- What unwanted hazardous reactions can be developed through unlikely flow or process conditions or through contamination?
- What combustible mixtures can occur within equipment?
- What are process margins of safety for all reactants and intermediates? What are the consequences of missing ingrediants or wrong proportion of reactants?
- What reaction-rate data are available on the normal, or abnormally possible, reactions?
- How thoroughly is chemistry of the process and any undesired reaction known? (See NFPA "Manual of Hazardous Chemical Reaction").
- What foreign materials can contaminate the process and create hazards?
- What provision is made for rapid disposal of reactants if required by plant emergency?
- What provisions are made for handling impending run-aways and for short-stopping and existing runaway?
- What hazardous reactions could develop as a result of mechanical equipment (pump, agitator, etc.) failure?

- What hazardous process conditions can result from gradual or sudden blockage in equipment?
- What raw materials or process materials can be adversely affected by extreme weather conditions?
- What process changes have been made since the previous process safety review?

C. Equipment

- In view of process changes since the last process safety review, how was adequate size of equipment assured?
- Are any venting systems manifolded and, if so, what hazards can result?
- What procedure is there for assuring adequate liquid level in liquid seals?
- What is the potential for external fire which may create hazardous internal process conditions?
- Is explosion suppression equipment needed to stop an explosions once started?
- Where are flame arresters and detonation arresters needed?
- In confined areas, how is open-fired equipment protected from spills?
- What safety control is maintained over storage areas?
- In the case of equipment made of glass or other fragile material, can a more durable material be used? If not, is the fragile material adequately protected to minimize breakage? What is the hazard resulting from breakage?
- Are sight glasses on reactors provided only where positively needed? On pressure or toxic reactors, are special sight glasses provided which have a capability to withstand high pressure?
- What emergency valves and switches cannot be reached readily and safely?
- When was pertinent equipment, especially process vessels, last checked for pressure rating?
- What hazards are introduced by failure of agitators?
- What plugging of lines can occur and what are the hazards?

- What provisions are needed for complete drainage of equipment for safety in maintenance?
- How was adequecy of ventilation determined?
- What provisions have been made for dissipation of static electricity to avoid sparking?
- What requirements are there for concrete bulkheads, or barricades to isolate highly sensitive equipment and protect adjacent areas from disruption of operations?
- What provisions have been made for relieving explosions in building or operating areas?
- Do all pressure vessels conform to state and local requirements?
- Are the vessels registered in compliance with state or local code requirements?
- When were pressure vessels inspected visually, calipered, radiographed, hydrostatically tested, etc.?
- Has the use history of all vessels been competely reviewed?

D. Instrumentation Control

- What hazards will develop if all types of motive power used in instrumentation should fail nearly simultaneously?
- If all instruments fail simultaneously, is the collective operation still fail-safe?
- What provision is made for process safety when an instrument, operating in process safety as well as in process control, is taken out of service for maintenance; when such an instrument goes through a dead time period for standardization or when, for some other reason, the instrument reading is not available?
- What has been done to minimize response time lag in instruments directly or indirectly significant to process safety? Is every significant instrument or control device backed up by an independent instrument or control operating in an entirely different manner? In critical processes, are these first two methods of control backed up by a third ultimate safety shutdown?

- Has the process safety function of instrumentation been considered integrally with the process control function throughout plant design?

- What are effects of extremes of atmospheric humidity and temperature on instrumentation?

- What gauges, meters, recorders cannot be read easily? What modifications are being made to cope with this problem?

- Is the system completely free of sight glasses or direct reading liquid level gauges or other devices which, if broken, could allow escape of materials in the system?

- How has the area National Electrical Code classification been established and hardware and techniques selected?

  - What process details affect the classification, group and division?

  - What "UL approved" hardware is unavailable for this job? Does this require testing?

  - Are any new techniques being applied on this job?

- Is the electrical system simple in schematic and physical layout so that it can be operated in a straight-forward manner? (This minimizes human error in switching for isolation and load transfer.)

- What electrical equipment can be taken out of service for preventive maintenance without interrupting production? How?

- How is the electrical system instrumented so that equipment operation can be monitored? Will this eliminate downtime due to equipment failures caused by unknown overloading?

- What are the overload and short circuit protective devices?

  - Are they located in circuits for optium isolation of faults?

  - What is the interrupting capacity?

  - How are they coordinated?

  - What instructions are furnished for field testing during the life of equipment?

- What bonding and grounding is provided?
  - Does it protect against static buildup?
  - Does it provide lightning protection?
  - Does it provide for personnel protection from power system faults?
- Check Lighting.
  - Adequacy for safe normal operation?
  - Adequacy for normal running maintenance?
  - Adequacy for escape lighting during power failure?
- Is tankage grounding coordinated with cathodic protection?
- What is being done to verify that instrument packages are properly installed? Grounded? Properly designed for the environment?
- What procedures have been established for testing and proving instrument functions?
- What periodic testing to check performance and potential malfunction is scheduled?

E. Operations

- When was the written operating procedure last reviewed and revised?
- How are new operating personnel trained on initial operations and experienced operating personnel kept up-to-date on plant operating procedures, especially for start-up, shutdown, upsets and emergencies.
- What plant revisions have been made since the last process safety review?
- What special clean-up requirements are there before start-up and how are these checked?
- What emergency valves and switches cannot be reached readily? What procedures are there to cope with these situations?
- What safety precautions are needed in loading liquids into, or withdrawing them from tanks? Has possibility of static electricity creation been adequately taken care of?

- What process hazards are introduced by routine maintenance procedures?
- What evaluations has been made of the hazards of sewered materials during normal and abnormal operation?
- How dependable are supplies of inerting gas and how easily can supplies to individual units be interrupted?
- What safety margins have been narrowed by revisions of design or construction in efforts to de-bottleneck operations, reduce cost, increase capacity, or improve quality?
- What provisions does the operating manual have for coverage of start-up, shutdown, upsets and emergencies?
- What economic evaluation has dictated the choice between a batch process and a continuous one?

F. Malfunctions

- What hazards are created by the loss of each feed, and by simultaneous loss of two more feeds?
- What hazards result from loss of each utility, and from simultaneous loss of two or more utilities?
- What is the severest credible incident, i.e., the worst conceivable combination of reasonable malfunctions, which can occur?
- What is the potential for spills and what hazards would result from them?

G. Location and Plot Plan

- Has equipment been adequately spaced and located to permit anticipated maintenance during operation without danger to the process?
- In the event of the foreseeable types of spills, what dangers will there be to the community?
- What hazards are there from materials dumped into sewers of neighboring areas?
- What public liability risks from spray, fumes, mists, noise, etc. exist, and how have they been controlled or minimized?

II. ELECTRIC CHECKLIST

A. Design

- How completely does the electrical system parallel the process?
  - What faults in one part of the plant will affect operation of other independent parts of the plant?
  - How are instruments for a plant protected from faults or other voltage disturbances?
- Are interlocks and shutdown devices made fail-safe?
  - What is the need for each interlock and shutdown used?
  - Are interactions and complications minimized?
  - Is continued use of protective devices insured?
  - What requirements or standards were used for the hardware that has been selected?
- What is the probability of accessibility during mishaps of power disconnects, starters, etc.?
- Is communication provided to operate a complex safely? (Telephones, radios, signals, alarms, etc.?)
- Are spacings and clearances furnished for normal traffic maintenance, and for fire fighting?
- Is there a schedule for checking operability of interlocks?
- Where sequency controllers are used, is there an automatic check, together with alarms, at key steps after the controller has called for a change, and is there a check together with alarms at key steps before the next sequence changes?

III. BOILER AND MACHINERY CHECKLIST

A. Boilers

- Safety Valves
  - Are long and large vent lines supported?
  - What drain connections are provided?
  - Is first drum valve set to relieve boiler working pressure?

- Is last drum valve set to pop at or below 103% of boiler working pressure?

- Blow-off Piping

  - Is piping used for boiler pressure of next higher gauge steel than required? Are sharp radius elbows avoided? Lines sloped? Low points drained?

- Feedwater Piping

  - Is the bypass around feedwater regulator accessible from the operating level and located where the drum level gauge glass can be seen? Are electrically-driven feedwater pumps duplicated by steam-driven pumps?

- Steam Outlet Piping

  - Are there separate non-return and header stop valves where one or more boilers discharge into the same piping system?

  - Is there a visible free blow and drain in piping between non-return and header stop valves?

  - Are there condensate drain provisions for all sections of piping?

  - Is there adequate piping expansion flexibility? How is piping supported?

- Drum Water Level--Attended Operation

  - Is there both high and low water alarms?

  - Is there a low water cut-off of gas or oil burners? (If drop of loss of plant steam pressure does not jeopardize process safety).

  - Is gauge glass visible from feedwater regulator bypass valve?

  - Is remote drum level gauge independent of drum level controls?

- Drum Water Level--Unattended Operation

  - Are high and low boiler water levels monitored?

  - Are two independent low water level switches interlocked with gas or oil burner safety shut-off valves?

- Gas Burner Control and Piping--General

  - Are plug cocks provided for manual shut-off service?

- Is there in-line strainer in gas line ahead of of all regulating and safety shut-off valves?

- Is there provision for stable gas pressure regulation at all loads? This may require a small regulator in parallel with the full-sized regulator for start-up or low fire service.

- Is there a double safety shut-off and vent valve arrangement? What type of reset is there for each valve?

- What type of automatic fuel-air ratio control is used?

- Is there separate pressure regulation of pilot gas?

- Is safety control circuit DC, or 120v AC with the safety controls in the ungrounded circuit?

- Do you insure positive, tamper-proof time period to provide minumim of 6 air changes in combustion chamber before light-off? Air flow rate during purge should be at least 70% of maximum capacity.

- Are controls or interlocks installed to prevent burner firing rate from being reduced below minimum stable flame?

- Are controls or interlocks installed to prevent burner light-off when insufficient combustion air flow is present?

- What interlock is there to assure low-fire burner light-off?

• Additional gas burner controls and interlocks for unattended operation:

- Is main burner flame monitored?

- Are following interlocks for safety shutdown furnished:
  (1) High gas pressure?
  (2) Low gas pressure?
  (3) Low combustion air flame?
  (4) Low boiler water (double switches)?

- Is there flame scanner response line of 2-4 seconds?

- Is there tamper-proof programmed light-off sequence to purge, light and prove pilot; light and prove main flame; post purge?

- How have you set up positioning fuel-air ratio controls?

- Is there a self-checking feature for flame scanner and flame scanner relay circuitry?

- Are provisions made in the oil burner controls and piping for each of the following items?
  - Oil line strainer
  - Oil pressure control
  - Heater for heavy oil
  - Single safety shut-off valve
  - Start-up recirculating line for heavy oil
  - Positive fuel-air ratio control
  - Low oil pressure alarm or interlock
  - Low oil temperature alarm or interlock for heavy oil
  - Low atomizing steam pressure alarm or interlock
  - Positive purge cycle and low fire start controls
  - Interrupted pilot

- Additional oil burner controls and interlocks for unattended operation:

  - Are interrupted and proved pilot and monitoring of main oil burner flame with interlock to close safety shut-off valve during flames failure provided?

  - Are the following interlocks in use for safety shut-down of burners?
    (1) Low oil temperature--for heavy oils?
    (2) Low oil pressure?
    (3) Low combustion air flow?
    (4) Low atomizing steam pressure?
    (5) Low boiler water (double switches)?

  - Is a tamper-proof programmed light-off sequence provided?

  - Are positioning fuel-air ratio controls used?

B. Piping and Valves

- Were piping systems analyzed for stresses and movement due to thermal expansion?

- Are piping systems adequately supported and guided?

- Are piping systems provided for anti-freezing protection, particularly cold water lines, instrument connections and lines in dead-end service such as piping at standby pumps?

- Are provisions made for flushing out all piping during start-up?

- Are cast iron valves avoided in strain piping?
- Are non-rising stem valves being avoided?
- Are double block and bleed valves used on emergency interconnections where possible cross-contamination is undesirable?
- Are controllers and control valves readily accessible for maintenance?
- Are bypass valves readily reached for operation? Are they so arranged that opening of valves will not result in an unsafe condition?
- Are any mechanical spray steam de-superheaters used?
- Are all control valves reviewed for safe action in event of power or instrument air failure?
- Are means provided for testing and maintaining primary elements of alarm and interlock instrumentation without shutting down procecces?
- What provisions for draining and trapping steam piping are provided?

C. Pressure and Vacuum Relief

- What provisions are there for removal, inspection, and replacement of relief valves and rupture discs, and what scheduling procedure?
- What need is there for emergency relief devices: breather vents relief valves, rupture discs, and liquid seals? What are the bases for sizing these?
- Where rupture discs are used to prevent explosion damage, how are they sized relative to vessel capacity and design?
- Where rupture discs have delivery lines to or from the discs, what has been done to assure adequate line size relative to desired relieving dynamics? To prevent whipping of discharge end of line?
- Are discharges from vents, relief valves, rupture discs, and flares located to avoid hazard to equipment and personnel?
- What equipment, operation under pressure or capable of having internal pressures developed by process malfunction, is not protected by relief devices and why not?

- Is discharge piping of relief valves independently supported? Make piping as short as possible and with minimum changes in direction.

- Are drain connections provided in discharge piping of relief valves where condensate could collect?

- Are relief valves provided on discharge side of positive displacement pumps; between positive displacement compressor and block valves; between back-pressure turbine exhaust flames and block valves?

- Where rupture discs are in series with relief valves to prevent corrosion on valves or leakage of toxic material, install rupture disc next to the vessel and monitor section of pipe between disc and relief valve with pressure gauge and pressure bleed-off line. Have any rupture discs been installed on discharge side of relief valve?

- What provisions are made for keeping piping to relief valves and vacuum breakers at proper temperature to prevent accumulation of solids from interfering with action of safety device?

D. Machinery

- Are adequate piping supports and flexibility provided to keep forces on machinery due to thermal expansion of piping within acceptable limits?

- What is separation of critical and operating speeds?

- Are check valves adequate and fast acting to prevent reverse flow and reverse rotation of pumps, compressors and drivers?

- Are adequate service factors on speed changing gears in shock services provided?

- Are there Full-flow filters in lube-oil systems serving aluminum bearings?

- Are there provisions for draining and trapping steam turbine inlet and exhaust lines?

- Are there separate visible-flow drain lines from all steam turbine points?

- Are driven machines capable of withstanding tripping speed of turbine drivers?

- Are non-lubricated construction or non-flammable synthetic lubricants used for air compressors with discharge pressures of greater than 75 psig to guard against explosion?

- What provisions are made for spare machines or critical spare parts for critical machines?

- Are there provisions for operation or safe shutdown during power failures?

- Are vibration switches on alarm or on interlock for cooling tower fans provided? Is sprinkler protection for the fan deck on induced draft combustion cooling towers provided?

IV. FIRE PROTECTION CHECKLIST

- If the building has enclosed walls and the construction or occupancy has combustibles, what kind of automatic sprinklers (wet or dry pipe system) are provided?

- If the building has open walls and the construction or occupancy has combustibles, how much water spray protection (HAD's, pilot head heat actuating or other systems) has been provided?

- What existing hydrants serve the area or project? What additional ones are to be provided?

- What fixed or portable monitor nozzles (on hydrants or separate) are provided for coverage of manufacturing facilities or storage facilities in open area (not within open or closed wall buildings)?

- Have the underground fire mains been extended or looped to supply additional sprinkler systems, hydrants and monitor nozzles? Dead ends should be avoided. What sectional control valves have been provided?

- Are small hose standpipes provided inside of buildings?

- What type, size, location and number of fire extinguishers are needed?

- What flammable liquid storage tank protection has been provided? Foam? Dikes with drain valves outside the dike?

- Where have total flooding or local-application carbon dioxide systems been provided?

- Is load-bearing stuctural steel exposed to potential flammable liquid or gas fires fire-proofed to a sufficient height above ground level to protect the steel? (This height varies from 30' - 35' depending on additional fire protection features).

- Has adequate drainage been provided to carry spilled flammable liquids and water used for fire fighting away from buildings, storage tanks, and process equipment?

- What protection has been provided for dust hazards?

- What is the capacity of fire water supplies? What is the maximum fire water demand?

- How long will supplies meet this maximum demand?

- What is the estimated maximum probable loss?

- What is the approximate "hold-up" of flammable liquids in the manufacturing equipment broken down by flash points? Are "hold-up" amounts kept to a minimum?

- What attention has been given to protection of process equipment from external fire?

- Are liquid inventory tanks near or under the ground instead of elevated?

- Is the area pad or flooring designed to conduct spill liquid away from process equipment? What facilities are provided for drainage?

- How have major storage tanks or vessels been located to minimize hazard to process equipment in the event of rupture or burning?

- Are all structures made of non-combustible materials and fire walls, partitions or barricades provided to separate important property damage values, high hazard operations and units important for continuity of production?

- Are operating units spaced to minimize potential damage from fires or explosions in adjacent units and to allow room for fire fighting activities?

- Have suitable locations been designed for fire alarms?

- Has key data been developed and additional protection planned for high piled storage areas?

FAILURE MODE AND EFFECT ANALYSIS

FAILURE MODE AND EFFECT ANALYSIS

FMEA is a methodical study of component failures. First, each component is listed on a FMEA tabulation sheet. For each component, the analyst asks the question, "How could this component fail?" and "How does this failure affect the system?" Ratings are then assigned to each failure which reflect the severity and probability of these risks. These numerical results are used for evaluating which failure modes should be given further attention by the hazards committee. Although FMEA involves some numerical analysis, it is primarily a qualitative method. The final decision regarding adequacy of process safeguards are a collective judgment by the review committee.

FMEA Objectives

- Evaluation of the adequacy of process safeguards and recommendations to correct inadequacies.
- Identification of component failures which could cause or contribute to hazardous events.

- Identification of failures which could have multiple effects on the system (common mode failures).

- Identification of hazards which require a Fault Tree Analysis. Occasionally these hazards may not have been recognized at the "Decision Tree" stage.

- Documentation to assure continuity for future review teams.

Analysis Procedure

An FMEA team of three to six participants is recommended, with one individual designated as study leader. Whenever possible, at least one team member with previous experience should be included. Using the FMEA form, the leader tabulates information about each system component as described in steps one through six below. These partially completed forms should be distributed to the study team for review. The team then meets to complete the tabulation forms and develop recommendations.

1. Select a System - Choosing the correct scope of analysis is important. The smallest portion of a process which is reasonably independent of other parts, particularly with respect to control systems, is a good choice. For example, in analyzing a plant power supply system, a FMEA study of the boiler and controls could be appropriate based on explosion potential. But the associated fuel storage and supply system is a separate process step which could require only a checklist study because hazards are less significant. If FMEA was used throughout, the study might become excessively large. The decision tree is useful in making these judgments.

2. Describe the System - A complete sketch of the system being analyzed is needed. All components must be shown and labeled. Process and Instrument drawings are excellent for this purpose if they are available and current at the time of the study.

3. Tabulate Item Number and Component Descriptions - Each component in the system (ie, valve, transmitter, sensor, etc) is listed on the FMEA form. Numbers are assigned to each component so they may be referenced at other places in the study. Some situations will be described later in which control or interlock loops may be listed as a single component. But, in general, each loop component is listed separately.

4. List Failure or Error Modes - Most components can fail in more than one way (ie, valve fails open or closed). List each failure mode separately, even though some or all failures appear to be safe.

5. List Effects on Other Components - These are local effects directly caused by the failure mode being considered. "Valve closes" when a sensor fails or "steam jacket temperature increases" when the steam valve fails open are examples. No other failures are considered in this listing.

6. List Effects on the Whole System - These are the potential "worst case" result of the failure. "Process cools - reaction stops" or "vessel overpressure-rupture" are examples. Usually, other protective systems (relief valve, interlocks, etc) must also fail in order to cause the worst-case event involving the failure mode being considered. For this listing, those failures are assumed. The other protective

systems will be considered later in the "compensating provisions" and "discussion" portions of the study.

7. Determine a "Hazard Severity Rating" Associated with Each Failure Mode - Table I defines four levels of hazard severity. Ratings are assigned to each on a scale of 0 to 3. These ratings should be applied to the "worst case" events identified in step 6 (whole system effects). Note that ratings of 3 and 2 correspond to the definitions of "major" and "moderate" hazards used in the "Decision Tree".

8. Determine the Failure Probability and Assign a Probability Rating - This rating relates to the failure mode being considered. It depends on the frequency of failure and the duration of the failed state. The probability rating is assigned using Figure I. This subject is discussed further in the section on Failure Probability.

9. Calculate "Criticality" - This is the sum of the "Hazard Severity" and "Failure Probability" Ratings. Thus, "Criticality" is an evaluation of both the probability of a failure and the severity of a "worst case" result.

10. List Failure Detection Methods - Failures may be detected in several ways including formal inspections and operating observations. Thus, a failed pressure transmitter might be detected either by an unusual chart recording or by a formal quarterly interlock check. Failure detection methods usually determine the duration of component failure (see section on Failure Probability).

11. List Compensating Provisions and Remarks - Compensating provisions include other interlocks, alarms and operator

actions that can still protect the system when the failure occurs. "Operator closes manual shutdown valve" may be a compensating provision for "automatic valve (interlocked for emergency shutdown) fails open".

The remarks column may also include time considerations such as whether an operator has several minutes or several hours to react to a given failure.

12. Review All Events with a "Hazard Severity Rating" of 2 or 3 (Regardless of "Criticality") - Where these events recognized earlier when the decision tree was used? If not, evaluate these events using the Decision Tree. Occasionally, this may result in a recommendation to conduct Fault Tree Analysis on one or more hazardous events.

13. Consider High "Criticality" Events - All events with a "Criticality" of -3 or greater (algebraically) should be considered further. Determine whether these failure modes are adequately safeguarded by interlocks, alarms or other protective devices. These determinations are arrived at by judgment. The "Criticality Rating" is a rough ranking of events by component reliability and severity of consequences, but it does not account for redundancy in interlocks, common mode failures or time available to make corrections. Thus, "Criticality" is only one of several factors to be considered in evaluating process safety.

The final hazards review report should contain adequate discussion of this evaluation step so that future review teams will be able to understand and build on this study with minimum effort. And a procedure for following up on recommendations should be implemented.

Probability of Failure

Two types of events are usually involved in a serious process incident. One type "initiates" or causes a problem while the second type "enables" or allows a hazardous condition to proceed. The probabilities assigned to these two types of events are different. Thus, it is necessary to identify initiators and enablers prior to assigning probabilities. These events are further defined as follows:

Initiator - An event which triggers a hazardous condition. Initiator events must be promptly corrected by process safeguards or operator action to avoid serious consequences. A steam valve failing wide open is an initiator event when this could lead to vessel rupture. Since duration of failure is not significant for initiator events, failure "probability" is a function of failure frequency alone (or its reciprocal, interval between failures).

Enabler - An event which allows a hazardous condition to proceed or continue but does not cause the hazard directly. Generally, enabler events can remain failed for extended periods of time without serious consequences until "tested" by an initiator event. Failed alarm loops, incapacitated relief valves and interlock systems are typical enabler events. Failure probability for enablers is a function of both failure frequency and duration of failure.

To detemine failure probabilities, a failure interval must be assigned to each component. Enablers must also be assigned a failure duration. Failure intervals are assigned using published

tables or by using plant experience. Failure durations depend on maintenance and inspection schedules as well as less formal inspections by process operators.

Consider the example of a pressure switch used in an emergency trip system. Failure of the switch would result in loss of process protection. Note that this failure is an enabler event because it does not trigger a hazardous event and the switch could remain failed for a considerable period of time. One source of failure rate information is Appendix C of the Du Pont Safety and Fire Protection Division Guidelines Section 6.2, "Guide for Fault Tree Analysis Vol. II". In that reference under "Switches, Pressure", a number of sources cite failure intervals of about 1 to 18 years. A suggested value of 7 years is marked by an asterisk. Plant experience should also be considered, particularly where process conditions may be more severe than average. Exact numbers are not required as will be shown later. So on the FMEA form under failure probability, enter the number "7" under the subheading "Interval".

Duration of failure depends on inspection frequency. Assume for this example that the trip system is inspected once a year. Failure could occur either just before or just after the scheduled inspection. In those situations, duration could be either a few minutes or a full year. On the average, though, the failure duration will be half the inspection period. In the switch example then, failure duration is 6 months or about 4400 hours. This number in hours should be inserted under "duration" on the FMEA form.

For the switch example, there is now enough information to determine a "failure probability rating". The Failure Probability Graph, shown in Figure I, is provided for this purpose. First

locate 7 years along the "Interval" axis. Follow that line vertically until the duration of 4400 hours is reached. Note that this point falls in a band on the graph with the failure probability of 1×10^{-1}. Only the exponent, or -1, is used as the rating on the FMEA form. Thus, a -1 should be placed in the "Probability of Failure-Rating" column. Note also that at the given duration, failure intervals of 1 to 10 years would all give the same probability rating. Usually, examining the limits of the interval band at the known duration simplify the choice of failure interval.

Initiating events are handled in a similar manner except that since initiators "trigger" an event, no duration is associated with them. Probability of failure for an initiator can be determined by reading along the baseline of the graph in Figure I. This represents a difference in assigning probabilities for initiators and enablers. It should not be implied that initiators have a 1 hour failure duration although they are read that way on the graph. Initiators are identified by an * in the duration column of the example problem in Appendix I.

Hazard Rating for Enablers

According to the definitions for Hazards Ratings, enablers would appear to rate a zero since these events never initiate damage or injury. However, one purpose of the FMEA is to identify unreliable protective devices associated with high hazard events. To accomplish this end, hazard ratings are assigned to enablers based on the most serious hazard against which they protect. Thus, a temperature sensor in a critical interlock circuit could receive a maximum rating (3).

Common Mode Failures

Common Mode failures have two or more effects on the system which contribute to the same hazardous event. A typical example is the use of Hi level alarm/Hi-Hi level interlock instrumentation. Although it might appear that these are separate protective systems, there are usually several components such as a sensor and transmitter which are common to both. Thus, a single failure could disable both systems. Such designs are not always undesirable, since they give an operator time to respond before shutting a process down. But the analyst should not consider the design equivalent to two separate forms of protection.

When common modes exist in an instrument loop, it is important to recognize these multiple effects. These multiple effects are easiest to identify when each component is analyzed separately (ie, sensor, transmitter, etc). Conversely, when an instrument loop has a single effect, it is adequate and certainly easier to consider the whole loop as one component. For purposes of this analysis, it is adequate to assume a "failure probability" for such a loop as 1×10^{-1}. Thus, a -1 may be entered in the rating column. When using this approach, the device which is actuated (ie, a valve) should be listed separately from the "loop". The actuated component failure may represent a common mode failure even when the loop does not.

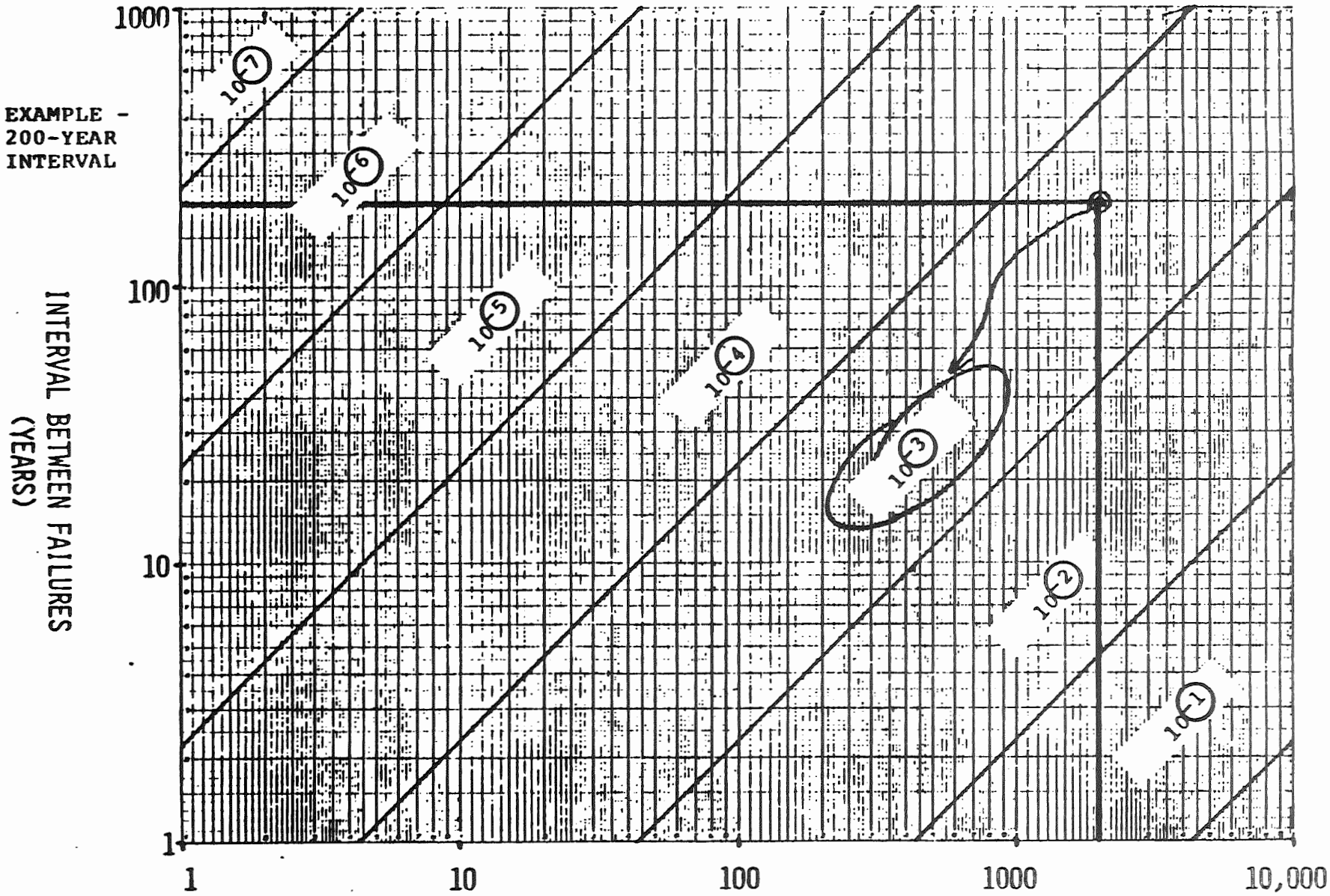
TABLE 1 - HAZARD SEVERITY

HAZARD DEFINITION	HAZARD RATING
A. Reasonable potential for multiple fatalities from toxicity or chemical/thermal energies involved in a process, for property plus business-interruption loss of $2MM or more, or for hazardous exposures outside the plant.	3
B. Reasonable potential for a single fatality, for multiple serious injuries, or for property plus business-interruption loss of $100,000 to $2MM.	2
C. Reasonable potential for a single serious injury or for property plus business interruption loss under $100,000	1
D. System fails safe or has only inconsequential results.	0

FAILURE RATE

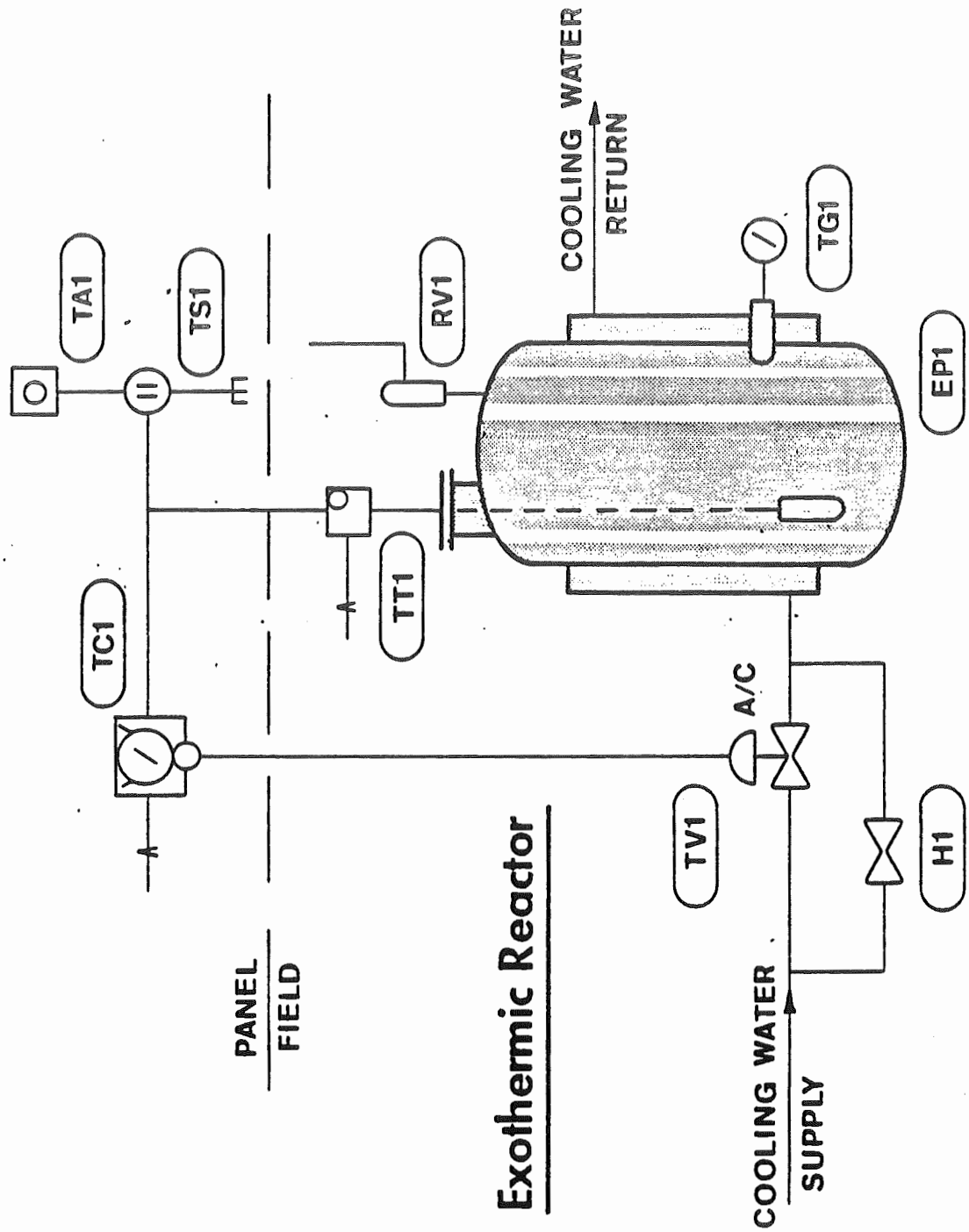
COMPONENT	AVERAGE
INSTRUMENTATION	
CONTROL LOOP	2.5×10^{-4} (5M) 9.9×10^{-5} (14M) 2.6×10^{-5} (4)
PNEUMATIC CONNECTIONS	1.6×10^{-6} (70)
SQUARE ROOT CONVERTER	1.6×10^{-5} (7)
SUMMER	2×10^{-5} (6)
TRANSMITTER (AMPLIFIERS)	8.9×10^{-6} (13)
TRIPS (ONE PRESSURE SWITCH AND SINGLE MOTOR VALVE)	7.6×10^{-5} (18M)

FAILURE PROBABILITY AND RATING



NOTE:

$$\frac{\text{Duration (hrs)}}{\text{Interval (yrs)} \times 8766} = \text{FAILURE PROBABILITY}$$



Exothermic Reactor

m t. e	Component Description	Failure or Error Mode	Effects On: Other Components	Effects On: Whole System	HAZARD	SEVERITY	RANKING	Prob. of Failure INT. YRS.	Prob. of Failure DUR. HRS	RATING	Criticality	Failure Detection Method(s)	Compensating Provisions and Remarks
	TV1 Valve	Fails Shut	Lose Vessel Cooling	Vessel Rupture	2			20	*	-5	-3	TA1, TG1, TC1	Manual Bypass, Relief Valve
		Fails Open	Vessel Cooled	Slowed Reaction	0								
2	H1 Manual Bypass Valve	Fails Closed	Lose Over-Heat Prot.	Reduced Rupture Protection	2			50	4000	-2	0	Annual Inspection	Relief Valve
		Leaks or Opened by Operator	Vessel Cooled	Slowed Reaction	0								
3	TC1 Temp Controller	Fails Low Output	TV1 Opened	Slowed Reaction	0								
		Fails High Output	TV1 Closed	Vessel Rupture	2			20	*	-5	-3	TA1, TG1	Manual Bypass Relief Valve
4	TT1-Temp Sensor/ Transmit	Fails Low Output	TV1 Closed Lose Alarm	Vessel Rupture	2			10	*	-5	-3	TG1	Relief Valve
		Fails High Output	TV1 Opened Alarm Sounds	Slowed Reaction *	0								
5	TS1 Pressure Switch	Fails Open	Alarm Sounds	Operator Confusion	0								
		Fails Closed	Lose Alarm	Reduced Rupture Protection	2			10	4000	-1	+1	Annual Inspection	Relief Valve
6	TA1 Alarm	Fails	None	Reduced Rupture Protection	2			25	10	-5	-3	Daily Inspection	Relief Valve
7	TG1 Temperature Gage	Fails Low	Lose One Temperature Indication	Reduced Rupture Protection	2			100	2	-6	-4	Operator Checks 4 Hrs	Relief Valve Alarm
		Fails High	Operator Confusion	None	0								
8	RV1 Relief Valve	Opens Below Set Point	Possible Release To Vent	Pressure Loss Through Vent	0								

Component Description	Failure or Error Mode	Effects On: Other Components	Effects On: Whole System	Hazard Severity	Prob. of Failure: INT. YRS.	Prob. of Failure: DUR. HRS	Rating	Criticality	Failure Detection Method(s)	Compensating Provisions and Remarks
RV1 Relief valve (cont'd)	Fails Closed	Inadequate Venting	Reduced Rupture Protection	2	1000	4000	-3	-1	Annual Inspection	None - see (A) Below
Cooling Water	Supply Loss	TV1 Opens Vessel Heats	Vessel Rupture	2	25	*	-6	-4	TC1, TA1 TG1	Relief Valve Stop Reactants?
	Water Temp Increases	TV1 Opens Vessel Heats	Vessel Rupture	2	15	*	-5	-3	TC1, TA1 TG1	Slower Runaway Same as Above
Instrument Air	Lose Pressure	TV1 Opens	Slowed Reaction	0						
EP1 Vessel	Leak	Possible Cooling Effect	Fire Hazard	1	50	*	-6	-5	Area Patrol	Diked Area; Class I Div. 2
	Rupture	---	Explosion Hazard	2	10M	8	-8	-6	Audible	Annual Corrosion Inspection

DISCUSSION

1A TV1 VALVE STICKS/FAILS SHUT (-3)

Loss of cooling results. Operator alerted by high temperature alarm, then uses manual bypass. Relief valve is sized for overpressure and provides a second backup.

Comments: Control room should be manned continually to ensure prompt response to alarm.

2A H1 MANUAL VALVE FAILS CLOSED (0)

One mode of protection is lost for situations involving failures of the temperature control loop. The relief valve is the only remaining protection.

Comments: In most processes, the operator will have an alternative means of emergency shutdown (stop feeds, ditch batch, etc). However, if opening the cooling water bypass is the only possible action, a second source of cooling water with a separate manual valve should be considered.

3B TC1 TEMPERATURE CONTROLLER FAILED HIGH (-3)

This includes set point errors by operators as well as controller failures. Valve TV1 closes, causing overheating in the reactor. The operator is alerted by the alarm. He can open H1, adjust TC1 (for set point error), or possibly shut off reactants. The relief valve provides a second backup.

4A TT1 TEMPERATURE SENSOR/TRANSMITTER FAILS LOW (-3)

Cooling water is shut off causing overheating. And the alarm will not sound to alert the operator. The relief valve is the only backup.

Comments: Since readings on TG1 are made hourly, there is a high probability of missing a temperature excursion. Consider adding an independent high temperature interlock loop to accomplish an emergency shutdown (eg, stop feeds, ditch batch, etc).

5B TS1 SWITCH FAILS CLOSED (+1)

Operator is not alerted in the event of overtemperature. The relief valve is the only backup.

Comments: The independent interlock loop discussed under 4A would improve system safety.

6 ALARM TA1 FAILED (-3)

See Comments under 5B

8B RV1 RELIEF VALVE FAILS CLOSED (-1)

Loss of significant protection mode against overpressure.

Comments: The relief valve provides a final backup for a number of failures leading toward vessel rupture. However, the recommendations listed under 2A and 4A ensure that the relief valve is only required after two or more other failures have occurred. Thus, backup relief protection is not recommended.

9 COOLING WATER HIGH TEMPERATURE (-3)

Operator should be alerted to high temperature by TA1, TG1, and TC1. TV1 opening fully may supply sufficient cooling to prevent a runaway. The relief valve is a backup.

Comments: Additional protection discussed in 4A would improve system safety.

FAILURE MODE AND EFFECT TABULATION SHEET

Item Ident. Code	Component Description	Failure or Error Mode	Effects On:		HAZARD RATING	Prob. of Failure		RATING	Criticality	Failure Detection Method(s)	Compensating Provisions and Remarks
			Other Components	Whole System		INT. YRS.	DUR. HRS				

Area_____ Process _____ Date _____ By _____ Sheet ____ Of ___

PROCESS SAFETY PUBLICATIONS

DU PONT PROCESS SAFETY PUBLICATIONS

Title	Order As
Safety & Fire Protection Guidelines	ER-8750
Safety & Fire Protection Guidelines - Process Hazards Manual	ER-8751
Safety & Fire Protection Guidelines - Occupational Health	ER-8752

Contact Safety & Fire Protection Division (774-6291) for these publications.

HAZARDS ANALYSIS
BIBLIOGRAPHY

METHODS

What If...?

Safety and Fire Protection Division, "Guide for Process Hazards Reviews," Guidelines Section 6.4 (1981).

Checklist

Safety and Fire Protection Division, "Guide for Process Hazards Reviews," Guidelines Section 6.4, App. A (1981).

Failure Mode and Effect

Recht, J. L., "Systems Safety Analysis," National Safety News, 93(2):24 (Feb. 1966).

Lambert, H., "System Modeling for Reliability and Safety Evaluation," UCRL-76186, Paper 26C at AIChE 67th Annual Meeting, Wash., DC (1974).

Amer. Nat. Stds. Inst., "General Principles of Reliability Analysis," ANSI N41.4/IEEE Std. 352; 4.1 (1976).

Safety and Fire Protection Division, "Guide for Process Hazards Reviews," Guideline Section 6.4, App. B (1981).

Applied Technology Division, "Process Hazards Reviews-Seminar Manual," Section 5 (1976).

Hazard and Operability Studies

Chemical Industries Assoc. Ltd., "A Guide to Hazard and Operability Studies," 1st Ed. (1977).

Safety and Fire Protection Division, "Guide for Process Hazards Reviews," Guidelines Section 6.4, App. E (1981).

Fault Tree Analysis

Recht, J. L., "Systems Safety Analysis," National Safety News, 93(4): 37 (April 1966).

Lambert, H., "System Modeling for Reliability and Safety Evaluation," UCRL-76186, Paper 26C at AIChE 67th Annual Meeting, Wash., DC (1974).

Powers, G. J., and F. C. Tompkins, "A Synthesis Strategy for Fault Trees," AIChE Loss Prevention, 8:91 (1974).

Safety and Fire Protection Division, "Guide for Process Hazards Reviews," Guidelines Section 6.4, App. C (1981). "Guide for Fault Tree Analysis," Guidelines Sections 6.2 and 6.3 (1978 and 1980).

Bibliography (Cont'd)

Fault Tree Analysis (cont.)

Prugh, R. W., "Application of Fault Tree Analysis," Chem. Eng. Prog., 76(7):59 (July 1980); AIChE Loss Prevention, 14:1 (1981).

Applied Technology Division, "Process Hazards Reviews - Seminar Manual, Section 6 (1976).

ACCEPTABILITY

Gibson, S. B., "Hazard Analysis and Risk Criteria," Chem. Eng. Prog., 76 (11):46 (Nov. 1980); AIChE Loss Prevention, 14: 11 (1981).

Lees, F. P., "Accident Fatality Number - A Supplementary Criterion," Loss Prevention in the Process Industries, 3rd Symp.:426 (Sept. 1980).

Cox, R. A., "Improving Risk Assessment Methods," J. of Haz. Materials, 6(3):249 (May 1982).

Prugh, R. W., "Use of Calculated Process Risks in Hazards Management," Eng. Dept. Report No. 15895 (Dec. 1981); AIChE Plant/Operations Progress, 1(3):190 (July 1982).

APPLICATIONS

Prugh, R. W., "Evaluation of Toxic Vapor Cloud Hazards," Eng. Dept. Report No. 16557 (Aug. 1982).

Prugh, R. W., "Evaluation of Vapor Cloud Explosion Hazards," Eng. Dept. Report (to be issued).