2237

CIRCULATE

~~Greene~~
Barr
Blades
~~Brady~~
Bullock
~~Dutchak~~
Eddinger
~~Friday~~
Handwerk
Ikeda
~~Kemp~~
Ormsby (last)
Repa
Santay
~~Smith~~
Thirion
Wagaman

Air Products

Management Approach to Safety and Hazard Analysi

Safety
Failure Rate
Risk / Benefit

by

F.G. Joyce

M.H. Vogel

~~Address~~ to selected customers of Air Products South ~~Africa~~ (PTY) Limited at a Symposium held at ~~Vanderbijlpark~~, South Africa Tuesday, 2nd February, 1982

Vanderbijlpark

INDEX

INTRODUCTION

We have called this Symposium address "Air Products' Management Approach to Safety and Hazard Analysis." We will tell you how we promote and manage safety worldwide and how we assess and evaluate possible hazards in our industry.

We wish to acknowledge the helpful assistance received from our colleagues in Air Products during the preparation of this paper.

The Importance of Safety in Management

Management has the responsibility for ensuring that production operations are inherently safe or are adequately controlled against inadvertent mis-operation. Its responsibility is to control work - both its human and physical elements - and accidents are caused by failure to control; they are not, as is often believed, the result of straightforward failures of technology; social, organisational and technical problems interact to produce them.

Management must be sure that personnel will not be exposed to hazards which they are unaware of or are unable to control. Ideally, all hazards will be identified during the decision and building stages of a process and appropriate controls will have been incorporated into the process prior to its start-up. However, new hazards may be introduced in response to attempts to improve the efficiency or versatility of a process. Applied research and maintenance of a large complex process may introduce previously unrecognised process hazards.

Complex technology demands high technical competence in controlling risk, but even the highest technical competence will not on its own ensure a consistently safe place of work. There is a great deal more to safety at work than providing the right physical safeguards. There is the whole question of effective and imaginative organisation for safety.

This point was sharply brought out in discussions and enquiries which followed the Three Mile Island nuclear incident in the U.S.A. Popular discussions of nuclear power plants tend to concentrate on questions of equipment safety but as the evidence accumulated it became clear that the fundamental problems were 'people-related problems' and not equipment problems.

This example is not given to show the possible shortcomings of the nuclear energy industry in the U.S.A. but to point out that even in industries where the physical safeguards must be complex and sophisticated, there is an overriding need for a safety organisation which takes into account the way human beings actually behave in the situation in which the advanced technology places them.

Studies by the U.K. Accident Prevention Advisory Unit have shown that only a minority of fatal accidents in, for example, the steel industry are the results of the primary steelmaking process, the majority are associated with activities, such as handling and transportation, which are common to industry in general.

Some of the most recent industrial catastrophes have in the final analysis been found to be unrelated to the fundamental technology of the industry concerned. The primary cause of the incidents have been attributed to failure to follow established procedures, breakdown in craft skills, failure to work to approved or recognised design standards, or introducing design changes without subjecting the proposed change to a thorough hazard review.

Air Products Capabilities

Air Products & Chemicals Incorporated today, founded in 1940, is a $ 1.6 billion multinational Company with 16,000 employees worldwide. In addition to these are about 5,000 temporary employees in our engineering and construction subsidiary, most of whom are construction workers employed locally for a relatively few months during a construction project. In addition to the design and construction of process plants and equipment, we operate industrial gas plants at more than 200 locations and chemical plants at 10 locations. Our plant operations extend to Canada, U.S.A. and South America, the Continent of Europe including the U.K., Belgium, France, Germany Holland, also South Africa and Korea - the list is not all inclusive. We are therefore a truly international company and experienced in dealing with people of all nationalities, their laws, customs and governmental requirements. Our safety programmes are directed to our worldwide team of employees. We operate a fleet of 700 cryogenic liquid road tankers which haul liquid nitrogen, liquid oxygen, liquid hydrogen and liquid argon to 6,000 customers where the cryogenic liquid is stored in vacuum-insulated storage tanks of 500 to 20,000 gallons capacity on the customers premises. In our chemical operations we operate high temperature reformers, high pressure ammonia and methanol synthesis reactors, large high-pressure polymerisation reactors and toluene nitration facilities. At our plant sites we store huge quantities of hazardous materials such as liquid oxygen, liquid ammonia, toluene and many others.

Our safety problems are complex and technology intensive. We face the constant threat that oxygen in the liquid state or in the gaseous state at high pressure might ignite and burn the metal in the tank, or piping that contains it, or in the compressor which is compressing it. Over the years we have learned much of the art and science of avoiding ignition in metal oxygen systems but we just do not have the luxury of being able to keep the metal and the oxygen separated.

Safety as a Management Objective

In Air Products we accept that safety is a management function and the managers safety objectives need to be defined.

The Chief Executive of our Corporation has the overall responsibility for the safety of Air Products employees and for the impact of its operations on our customers, people, plant, premises and the environment. He demands the highest performance, rewards superior performance and refuses to accept mediocrity.

Managers are accountable in production and budgetary terms and are therefore accountable for safety performance in precisely the same manner. Achievement of safety goals is as rewarding as the achievement of sales and net income targets, production targets or any other business objective.

We consider that the distribution and effective use of knowledge is a major management contribution to safety. We endeavour to pursue this course in Air Products.

Our philosophy is based on four simple principles and they are:

All injuries are preventable:
Safety is a line-management responsibility:
Safety is a condition of employment:
Management is responsible for the safety of its employees.

To be a leading company in industrial safety requires a total commitment of the entire organisation to safe designs, and intense design reviews, to safe operation and intense operations reviews, to safety training, motivation and discipline, to putting safety first - no shortcuts, no deviations from the first class way. It requires establishing a system of many checks and balances. It requires diligent investigation of all accidents and near misses, with no tolerance of cover-ups. People do not easily accommodate to these disciplines - they require the strongest kind of leadership from the top.

General Fundamentals for Successful Safety Programme

The need to specify goals and have policy objectives and action plans is a fundamental requirement for a successful safety programme.

The following may be regarded as the minimum standards:

1. Safety Policy

   The preparation in writing and up-dating as necessary of a basic safety policy statement by the Chief Executive which should be communicated to all Managers and Employees and which emphasises:

   a) The commitment of Senior Management to injury reduction and acceptance of accountability.

   b) That safety performance is a line management responsibility and can be managed, reviewed and monitored in the same way as other business functions by setting objectives and planning to meet these objectives.

   c) That all injuries are preventable.

   d) That all accidents, near misses and dang erous occurrences can be regarded as symp toms of management failure and should b investigated.

   e) That production pressures and profits mus not compromise the basic responsibility fc safety.

2. Safety Goals

   Setting worthwhile and understandable goals fc safety at varying levels within an organisatior The strategic goals can be set by the manage ment and the successive operating levels ca identify and promulgate their own aims withi an overall strategy.

   Generalised goals are not satisfactory. The should be graded as appropriate to meet th need and developed from experience.

3. Management Commitment & Example

   Management must demonstrate their continuou commitment to safety by sympathetic involv ment and encouragement, and showing concer end sensitivity to injury. They must obtain b motivation the commitment of all the emplo ees. They must convince each person to accep responsibility for safety insofar as they contr it or need to contribute to group performanc

4. Accident Reporting and Investigation

   All accidents, near misses and dangerous occu rences to be reported and investigated. Lir management to recognise the importance c

   a) Establishing accident reporting and inves igation procedures.

   b) Ensure that accidents and near misses a reported immediately.

   c) Showing concern and responding rapidl

   d) Quick implementation of corrective actio

   e) Internal and external publication as ne essary to avoid repetition.

5. Analyse Safety Performance

   Review and analyse the last five years of ac dent records to establish major problem are which may be either operational, behavioural technical. Use results to decide priority f action.

6. Safety Committees

   Establish the following committees:

   a) Executive Management Safety Policy Co mittee.

b) Division or Group Safety Committee as appropriate.

c) A Safety Committee at each Company location (senior member to be chairman).

7. Working Rules

Establish for each Company location a set of working rules outlining the basic standards with which employees must comply, e.g.

Housekeeping
No smoking areas
Safety control procedures
Use of protective clothing and equipment
Code of personal conduct
Emergency plan.

8. First Aid

Encourage operatives to qualify in first aid. Evidence exists that the higher the number of first aiders in worker groups the lower the accident rate.

9. Safety Audits

Establish procedures for regular audits of Company locations by line management. Audits may be conducted to monitor one or more of the following:

a) Behaviour of personnel regarding compliance with safety rules.

b) Training needs.

c) Compliance with statutory regulations and company standards.

d) Opportunity for injury i.e. general hazards.

e) Hazards of process equipment for either new or existing facilities.

Management when visiting locations should hold 'safety walk' with Manager and Supervisors.

10. Performance Measurement

Establish programme for measuring performance of individuals. The setting of individual performance standards and the regular monitoring and evaluation of progress. Appropriate approval or disapproval of the standard of safety achieved at the workplace should be made.

11. Performance Recognition

Management to recognise good safety performance by groups or individuals in the form of awards which should be of a non-monetary variety. Participate in all established award programmes.

12. Action Plans

Develop action plans and objectives on both an longer term objectives for statistical injury performance, to be monitored frequently and reviewed each year.

13. Safety Information

Ensure that adequate information on safety matters is available to employees in the form of safety manuals, safety bulletins, data sheets, etc.

14. Training

Comprehensive training programmes should be in a form to ensure that employees are instructed and informed how to carry out their job properly and safely.

Refresher courses and a requalification of certain trade skills essential in maintaining high standards.

15. Safety Organisation

Safety is primarily the responsibility of management and cannot be delegated. There is a need for specialists to provide advice on specific topics and general strategy.

16. Emergency Procedures

Each Company location should have well conceived and adequate procedures to deal with emergencies such as:

- Fire
- Explosion
- Major releases of potentially harmful substances
- Threat of harm or damage, sabotage, etc.

17. Progress Reports

Senior management should arrange to receive regular progress reports on safety programmes and action plans and encourage employees to seek management involvement in major issues on Safety and Health.

18. Maintenance

Maintenance procedures to be subject to central review and direction of its scope and frequency.

19. Compliance with Statutory Regulations

Ensure compliance with the statutory regulations and that these and our Company standards are widely accepted and applied as good working practices.

How to Measure Safety Progress and Performance

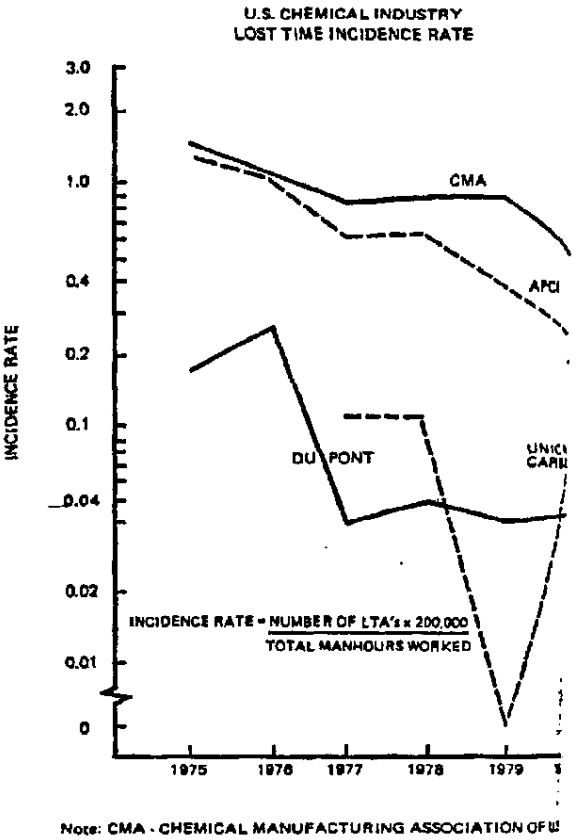
Air Products aims to be recognised as a safe company by its employees, by the public at large and by industry. We seek to be among the leaders in safety and to be on par with the top two or three worldwide corporations in the area of lost time accident frequency, recordable injury frequency and injury

of disabling injury and of fatalities. We believe that the statistical results truly reflect performance and we set statistical goals for worker groups both for the short and long term.

We have made considerable progress worldwide towards this statistical goal in the last five years. We have seen a parallel reduction in our product liability costs and in our costs due to damage to plant and equipment. We have seen better morale, improved productivity and higher product quality. We remain convinced that a first-class approach to safety management is a necessary ingredient of a first-class management system. We have still some way to go to match the best, but we are worldwide totally dedicated to getting there.

The first of the following charts illustrates the progress made in statistical terms within our Worldwide Corporation. During the period 1975 to 1981 (Fig.1.) there has been an overall fourfold improvement in the Corporation's performance. The improvement in performance by some sections of the Corporation has been extremely dramatic. We, as a Corporation, find it beneficial to compare our performance and progress with that of Du Pont and Union Carbide, (Fig.2.) both multinational companies recognised as leaders in all fields of industrial and worker safety. In Fig.2. the average performance of the Chemical Manufacturing Association of America is also included. Air Products in Europe is a member of an industrial gas manufacturers association and in Fig.3. our European performance is compared with the average for the European gas industry. While Air Products in Europe is not the leading group in the Corporation on performance, we have seen a twelve-fold improvement in our safety performance during the past six years.

Fig. 2.



Note: CMA - CHEMICAL MANUFACTURING ASSOCIATION OF U

Fig. 1.

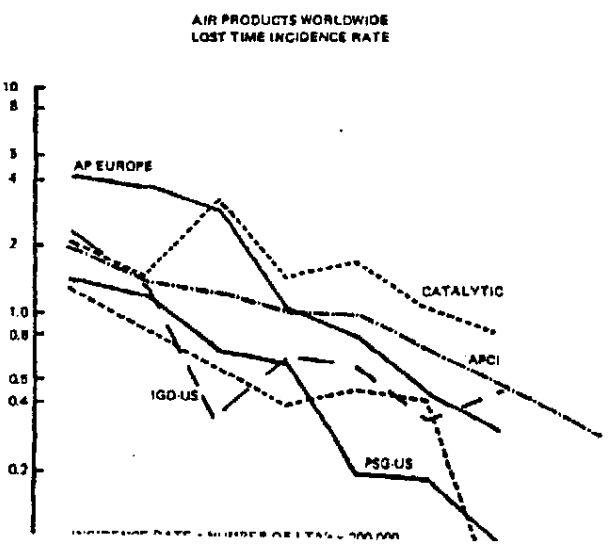
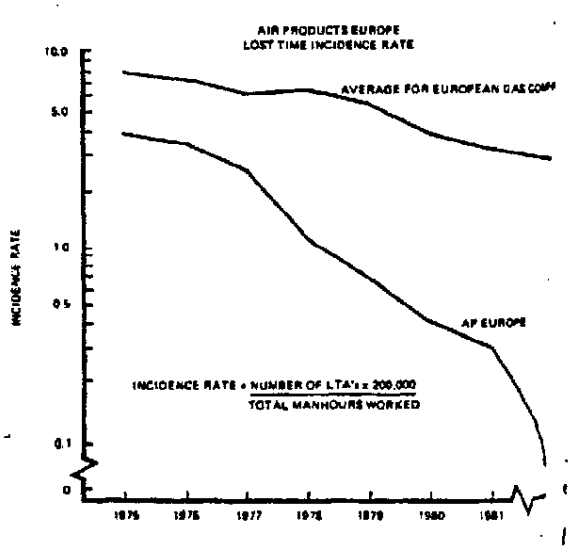


Fig. 3.



Background to the introduction of Process Hazards Analysis

During the last ten years, the chemical industry has been involved in explosions unprecedented in industrial history. As chemical facilities become larger and technically more complicated, our risks become larger and our safety margin less secure. Air Products, and much of the chemical industry, turned toward the same sound technological base which was responsible for the industry's growth for the answers to the safety and loss prevention problem. The result has been the development of the philosophies and methodologies of process hazards analysis. It is through comprehensive, detailed reviews of process operating conditions and instructions that we may assure ourselves that our facilities pose a minimal hazard to our employees, our neighbours (third parties) and our capital.

It is our intent to provide our employees with this technology to properly exercise their safety responsibility. All employees whether in design, construction, or operation of a facility are responsible for the safety of their area of responsibility.

Explosions, energy releases, fires, vessel ruptures are all terms which we read in the various engineering journals every week, and feel fortunate that it wasn't our plant or our design. The Flixborough caprolactam plant explosion is the accident we all remember when the term explosion is used. This incident resulted in twenty-eight people killed, thirty-six injured and over $ 150 million dollars in property damage, The effects of the shock wave were felt eight miles from the facility. The explosive force was equivalent to fifteen tons of TNT.

This particular incident resulted from a failure to properly review a design change in the field. Sure, a pipe collapsed and released fifty (50) tons of cyclohexane; but the real cause was that the man who made the change did not think it through; he did not review the safety of his work.

In 1968, a hot oil-water emulsion broke in a slop oil tank in the Shell Nederlands refinery in Pernis, The Netherlands. The world's second largest refinery suffered over $ 28MM of damage over thirty (30) acres of the refinery. Improper review of the compatability of materials was the culprit here. Are we always sure of the reactivity of the materials we combine in vent headers or sumps or recycle systems?

Sometimes even the fluids we run through heat exchangers can cause problems. In Dow Chemicals' Plaquemine, Louisiana facility, a leak between the shell and tubes of a heat exchanger allowed air into the heat transfer system. This time a four-hour fire cost Dow $ 12,000,000

Mechanical failure is not a necessary part of an accident; sometimes we just place too much faith in our own engineering. The controls are foolproof! The process is the best! The operators can handle anything! Have we really examined all the environmental factors, all the numerous assumptions we make? In Tokuyama, Japan, Idemitsu Chemical had an interruption in their instrument air system; it cost them their ethylene plant. The fire which followed the exothermic reaction caused $ 14.8MM in damage.

Air Products has not been immune to such incidents. The inoperability of a single check valve after a leak occurred in a heat exchanger resulted in a $ 1,000,000 loss at our Escambia nitric-acid plant. The inability to properly relieve an overpressure within a TDA check tank resulted in a $ 1.5MM loss.

In August 1977, a reactor involved in the decomposition of ammonium nitrate to nitrous oxide exploded, leaving four men dead, including the plant manager. The replaceable damage was over $ 2,000,000. The loss of life to employees was irreplaceable.

The rate at which we hear of these incidents has been increasing as has been the magnitude of the loss. Inflation has taken its toll, but other factors more actively influenced this trend. Our plants are becoming larger and larger. The term 'world-scale' changes from year to year. They are single train; pipes are larger, flow rates are faster and chemical hold-up massive. Any hole in the armour can release tons of flammable liquid into the atmosphere.

Our customers are requiring more assurance that their product will be continued in the event of plant problems and this necessitates large quantities of storage; both raw materials and products. Tank failures, vessel overfills and 'suck-ins' are all common failures in the industry which have led to disaster.

While inflation has not been a major item leading to increased risk in our plants, its impact has been felt in the layout of our facilities. In order to reduce costs, we tend to shorten piperuns and construct a more compact unit. This tendency leads to a higher dollar density in a given area. Thus, a fire in a 200' square block will damage more equipment than a comparable fire ten years ago.

Although certain spacing requirements exist by law (OSHA), by industry consensus (NFPA) and by internal agreement (Group/Division and Corporate Standards), there is room for trade-offs among separation distance; fire protection and equipment; and process central instrumentation. Who must make these trade-off decisions? In the long run, we all make these type decisions in our daily activities. Whether it's a change in instruments, a bypass on a control or a change in a project layout, there is an impact on plant safety. It is the purpose of this seminar to discuss methods of analyzing these changes and determining their effect on plant safety.

Hazards Identification

The typical practice in the majority of chemical engineering companies for controlling the engineering development of a project from initial design right through to construction, revolves around the use of the Process and Instrumentation Flowhseet (P. & I.D.) at all stages of the project.

Usually a Project Manager is responsible for overall control of the P. & I.D. (issuing all flowsheet revisions to the necessary departments, calling meetings, etc.).

The P. & I.D. Coordinator (usually a senior piping engineer) is responsible for ensuring the requirements of all key departments are incorporated into subsequent issues of the P. & I.D.

Most projects have a minimum of five complete revisions; (e.g. at A.P.L:-)

Preliminary
Revision 0
Revision 1
For Design
For Construction

Late design changes, e.g. during commissioning, have to be circulated to all sections for approval using a 'P. & I.D. Change Note' before they can be implemented.

At all stages of review, each key department can make use of a P. & I.D. checklist in searching the proposed flowsheet for safety related inadequacies. Company engineering standards also give guidance in this respect.

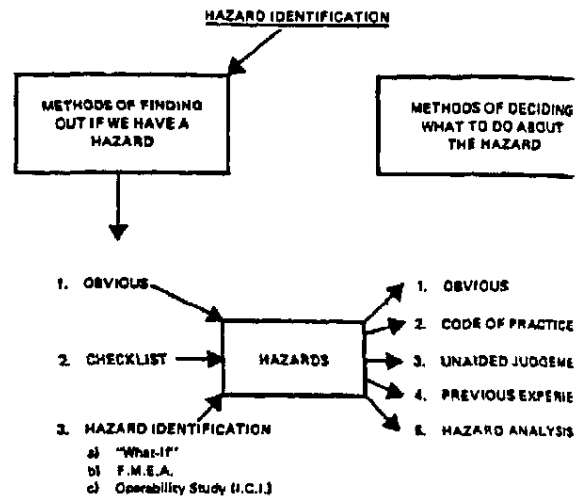
Until recently, the above mentioned type of procedure has proved adequate for examining a project for inadequacies. However, its structure inevitably means that attention is focused primarily on aspects with which each department is most knowledgeable. While this approach is acceptable for very simple systems involving conventional well established processes and plant, it is likely to be far from adequate if the proposal is at all complicated or novel.

For such projects a much more rigorous, systematic and process-orientated examination is required. The most commonly used methods of systematic hazards identification are; (Fig.4.)

a) "What-If" Analysis
b) Failure Mode and Effects Analysis (FMEA)
c) Operability Study (I.C.I.)

(Note: The above methods will only be very briefly discussed. Interested readers wishing to know further details of the application of either of the methods should consult the literature).

FIG.4.



A. 'What If' Analysis

Perhaps the most successful technique in evaluatir an idea is to have a co-worker take the position of t devil's advocate. By questioning the basic assum tions for the idea, the reliability of the equipmen and the safety precautions utilized, one hopes tc unearth any hidden flaws in the design.

The simpfest and easiest-to-use hazards analysis tec nique, 'What If' Analysis, is based on this metho ology. 'What If' aims at forecasting scenarios and de ermining the hazard of their consequences. It is straight-forward tool and does not require a great de of time or sophistication. All employees should b using this basic tool as they perform their respectiv job functions. The 'What If' technique is also quite useful in performing Preliminary Hazards Analyses o in reviewing a facility's operating procedures.

The procedure is to: (1) define the system under study, (2) determine the underlying assumptions, (3) state the hazards in the system, (4) define the orde of the review, (5) systematically ask 'What If' questions of the system and its components, (6) generate recommendations, and (7) issue report to management.

'What If' questions can relate to:

- a state of nature - 'What if lightning strikes?'
- an assumed condition - 'What if the wrong material is delivered?'
- the reliability of an instrument or piece of equipment - 'What if the valve sticks open?'
- a human reaction - 'What if the operator opens the wrong valve?', or
- combinations of events - 'What if the level indicator is broken and we unload a trailer into the tank?'

B. Failure Mode and Effect Analysis Method

The Failure Mode and Effect Analysis (FMEA) method is used to evaluate systems in a manner which its name implies. That is, a particular item in a process is analyzed in its failure mode for its effect on other components and on the entire system. By definition, the FMEA method will evaluate aspects of an operation and determine the destructive potential of each hazard and of related hazards. This method is equipment-oriented, and as such, it may not put enough emphasis on the operator's or operating procedures' role in running a process. The 'What If' Method, or, as will be discussed later, the fault tree analysis is more conducive to analyzing operating errors.

C. The Operability Study

Philosophy:

The Operability Study is based upon the principle that a problem can only arise when there is a deviation from what is normally expected.

Basic Procedure:

Search the proposed scheme systematically for every conceivable DEVIATION and then look backwards for CAUSES and forwards for possible CONSEQUENCES.

The scheme is examined line by line looking for inadequacies in design. A check list of guide words is applied to each stage of the process in turn, thereby generating DEVIATIONS opposite all possible eventualities.

Aspects considered are normal plant operation, start up and shut down, suitability of plant materials, equipment and instrumentation, provision for failure of plant services, provision of maintenance, safety.

Before examining each section, make sure you understand the function of the section, including normal process conditions and specifications if available.

Keywords are applied only to lines joining pieces of equipment or to off-sites and not directly to the equipment itself. This is because any problem that could arise in a piece of equipment should show up as a cause or consequence of a deviation in a line leading to that piece of equipment. However the guide word 'OTHER' which has special significance for aspects other than normal operation, must be applied to the items of equipment as well as the lines.

Guidewords and their Meaning:

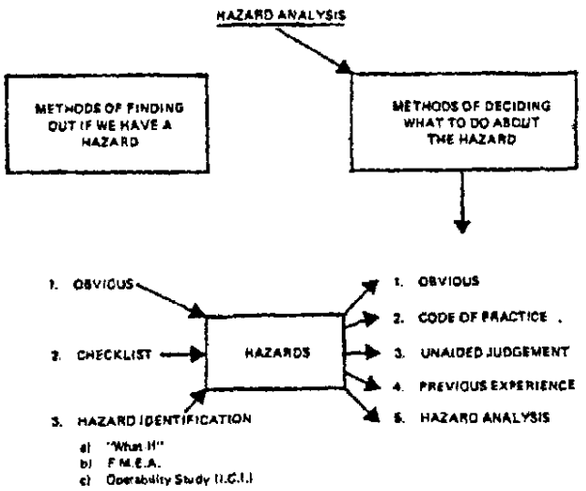
WORD	MEANING
NONE	— No flow, reverse flow
MORE OF	— Higher flow, temperature, pressure, viscosity, etc.
PART OF	— Change in stream composition
MORE THAN	— Impurities present, e.g. ingress of air, water. Extra phase present, e.g. vapour, liquid.
OTHER	— What else apart from normal operation can happen? e.g. start up, shut down, maintenance, catalyst or absorbent change, failure of plant services, safety.

(Note: Implementation of an Operability Study through use of the above guideword system is illustrated in the example of a proposed olefin dimerization unit in a paper by H.G. LAWLEY, I.C.I. Chemical Engineering Progress, April 1974).

Hazard Analysis (Fig.5.)

Having carried out the identification of hazards on a proposed or existing plant design and having identified the existence of certain serious hazards, we may then wish to ask the question, 'How often will this hazard occur?'. The Hazard Analysis answers this question by relating logically the circumstances necessary for the development of the potentially dangerous situation (the hazard) and subsequently estimating the probability that the hazard will occur (the hazard rate). The most commonly used method of hazard analysis logic is Fault Tree Analysis.

FIG. 5



The method was orginated by Bell Telephone in 1961, and further developed by the Boeing Company during the 1960's. Fault trees were initially limited to the aerospace field, but have since emerged within the chemicals industry. Fault tree analysis defines basic causes and their relationships in leading to a single, undesired event. The procedure for applying this method is as follows:

a) Define the Undesired Event

The fault tree is a logical sequence of events which could result in the undesired event, such as a vessel rupture or chemical spill. The undesired event will have been identified by use of the Operability Study, previous experience or other methods. The undesired event is placed at the top of the fault tree schematic. The main objective in using this method is to determine how failures or actions, equipment, maintenance and personnel could result in an undesired event.

b) Construct Fault Tree

Having selected the undesired event, construct the fault tree using logic symbols to relate all possible event sequences to the undesired event. The undesired event is placed at the top of the fault tree schematic. Then follows generation of possible causes of this event, called sub-events, in descending order of occurrence, building on the "stump" of the tree. Each sub-event forms a branch of the tree and is developed independantly of the other branches. The cause should be direct and immediate and reflect its fail state only on the sub-event to which it is connected.

Sub-events can be related to one another through the use of "AND" or "OR" gates. A single sub-event will cause the next higher event to occur if the two events are connected by an "OR" gate. The "AND" gate is used when the next higher event is the result of all sub-events happening simultaneously. Construction of the tree continues until all possible causes for each sub-event have been considered and the basic causes for each branch of the tree developed.

Applying the fault tree method to calculate the hazard rate for a given undesired event is demonstrated in the following example. (Figure 6.)

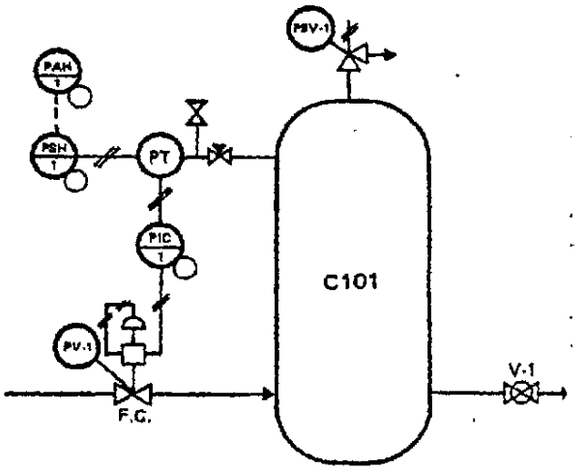


Figure 6. Example of Hazard Rate Calculation

System Description
The system consists of a vessel (C101) fed by a high pressure gas source (limited to 8 bars.g.). Pressure in C101 is controlled by a pressure control loop acting on an inlet control valve (PV–1). The vessel is protected by the relief valve PSV–1. An operator in the control room has C101 pressure indication via PIC–1 and warning of high vessel pressure via alarm PAH–1. (C101 design pressure is 1.0 bars.g.).

System Hazard
The hazard in the above system has been identified as vessel rupture. In order to quantify the hazard, it will be first necessary to draw up the fault tree for this hazard (See figure 7.). Quantification can then proceed subject to component failure rate data being available.

Risk
Calc
haza
rate
arm

System Data
Key failure rate data for this system is as follows:

		Faults/ year
a)	Pressure controller	0.20
b)	Control Valve	0.15
c)	Pressure transmitter	0.20
d)	Impulse line	0.10
e)	Relief valve (overhauled every 2 years)	0.005
f)	Operator	

Assume the operator will fail to intervene successfully after a high pressure alarm with a probability of 0.1. If the alarm does not operate the probability will be only 0.5.

Risk Criteria

Calculation of a hazard rate is the first step in any hazards analysis. However, unless there is a hazard rate goal there is no way to assess whether or not the amount of safety protection built into the process is

ICI has been a leader in developing quantitative risk criteria for the chemical industry which they have applied and which has been widely published. The basis of their criteria is the fatal accident frequency rate (FAFR). The FAFR is the number of fatalities per 100 million (10^8) worker hours. This is roughly equivalent to the number of fatalities in a group of 1000 men over their working lifetimes.

Typical FAFR's for various occupations calculated by Trevor Kletz of ICI are shown in Table I[1] while FAFR's for non-occupational activities are shown in Table II[1].

Bulloch of ICI[2] produced an interesting histogram (Figure 8) of the FAFR of various activities in daily life.

Approximately half of the FAFR of 4 for the chemical industry, which is considered good, is due to process related accidents (e.g. explosions, fires, etc.) while the other half is attributable to non-process related accidents (e.g. falling off a ladder). Kletz[1] has argued that in a given plant no hazardous event should contribute more than 10% or 0.4 FAFR to the total FAFR.

Table I

FAFR FOR VARIOUS INDUSTRIES

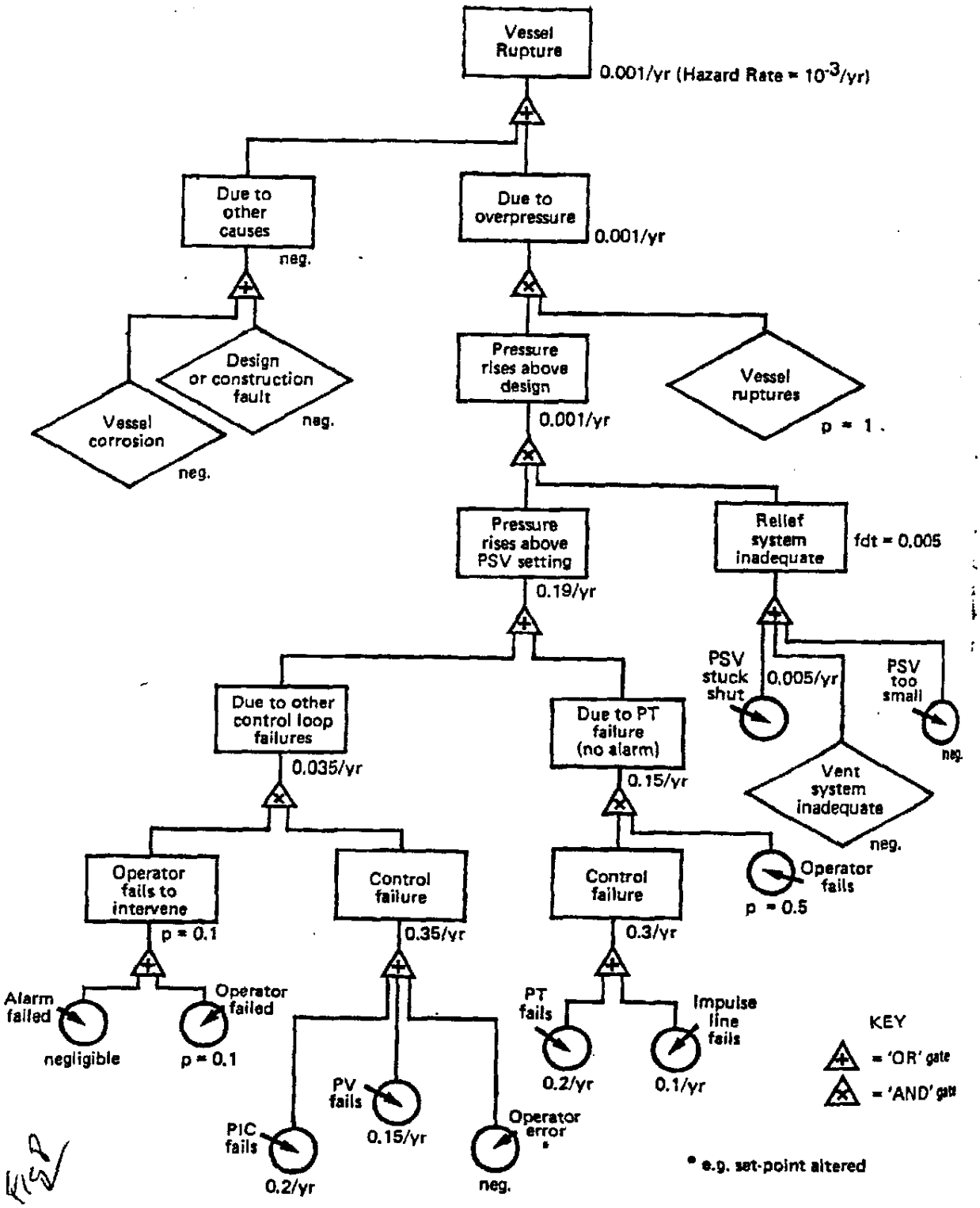
Chemical Industry	3.5
British Industry	4
Steel Industry	8
Fishing	35
Coal Mining	40
Railway Shunters	45
Construction Workers	67
Air Crew	250
Professional Boxers	7,000
Jockeys (Flat racing)	50,000

Table II

FAFR FOR NON-OCCUPATIONAL ACTIVITIES

Staying at home	3
Travelling by bus	3
Travelling by train	5
Travelling by car	57
Pedal cycling	96
Travelling by air	240
Moped riding	260
Motor scooter driving	310
Motor cycling	660
Canoeing	1,000
Rock climbing	4,000

An FAFR of 0.4 is equivalent to an average hazard rate of 3.5×10^{-5} events/year. If this criteria is used

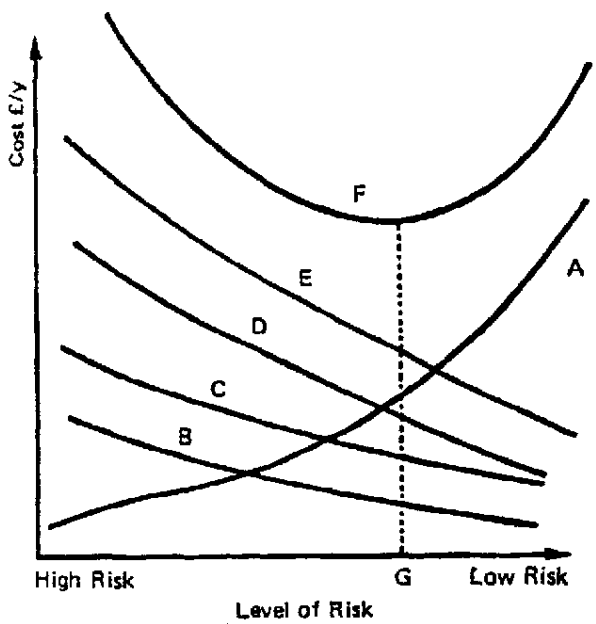

Vessel Rupture
0.001/yr (Hazard Rate = 10^{-3}/yr)
Due to other causes
neg.
Due to overpressure
0.001/yr
Design or construction fault
neg.
Vessel corrosion
neg.
Pressure rises above design
0.001/yr
Vessel ruptures
p = 1.
Pressure rises above PSV setting
0.19/yr
Relief system inadequate
fdt = 0.005
PSV stuck shut
0.005/yr
PSV too small
neg.
Vent system inadequate
neg.
Due to other control loop failures
0.035/yr
Due to PT failure (no alarm)
0.15/yr
Operator fails to intervene
p = 0.1
Control failure
0.35/yr
Control failure
0.3/yr
Operator fails
p = 0.5
Alarm failed
negligible
Operator failed
p = 0.1
PIC fails
0.2/yr
PV fails
0.15/yr
Operator error *
neg.
PT fails
0.2/yr
Impulse line fails
0.1/yr
KEY
= 'OR' gate
= 'AND' gate
* e.g. set-point altered

to reduce the risk of significant in-plant hazards then the average FAFR should decrease over time. However, what appears to be a reasonable FAFR criteria in the chemical industry may be very unrealistic for another (.eg. mining) industry. Even though criteria are used to establish the appropriate level of safety there may arise instances when it is impractical to reach the hazard rate goal. Gibson[3] provides a possible way of analyzing this problem via a cost-benefit approach. The chart in Figure 9 explains this technique.

However, a major problem occurs in trying to establish the number of people exposed. Society may be willing to accept a particular frequency for a single fatality but very unwilling to accept that same frequency for multiple deaths.

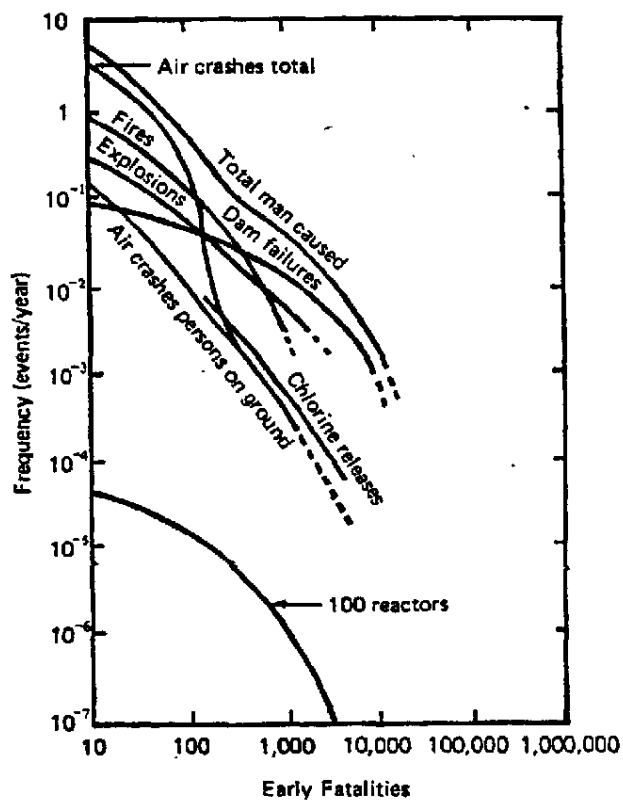
Risk analysis can be used to calculate this potential exposure. Figure 10 is an example from the Wash 1400 study to illustrate the risk to the public from exposure to 100 nuclear reactors.

FIGURE 9
COST-BENEFIT ANALYSIS[3]



A - Cost of Prevention
B - Material Damage Costs
C - Loss of Profit
D - Costs or Measures Taken After the Incident
E - Loss of Life
F - Total Cost

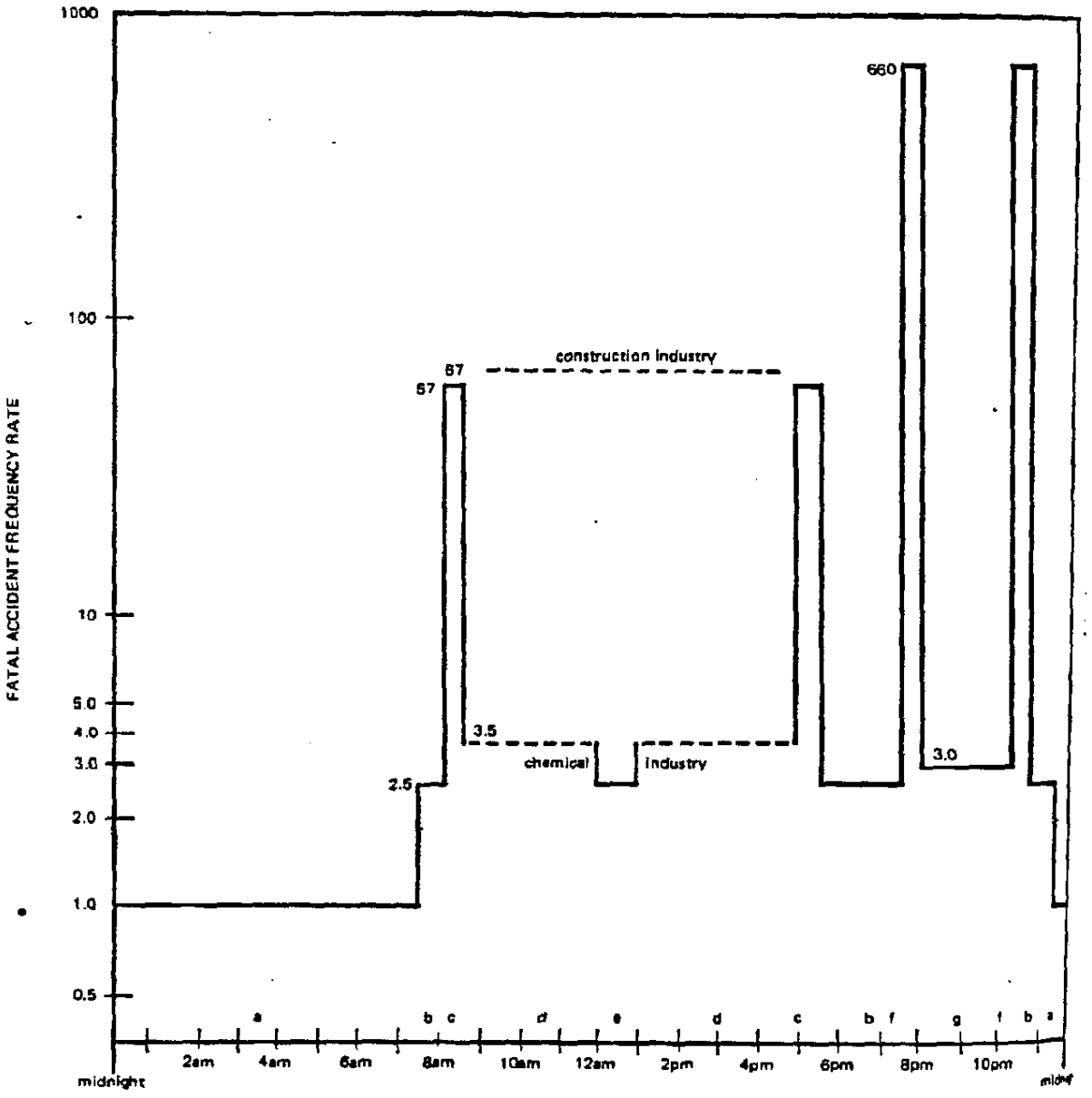
FIGURE 10
FREQUENCY VS. EARLY FATALITIES



Risks to the population at large pose a more difficult problem. It has been suggested[3] that a risk of death of 10^{-7} per person per year (FAFR = 0.001) may be acceptable as this level approaches a number of involuntary event frequencies which the public has accepted without complaint (Table III).

FIGURE 8

HISTOGRAM OF FATAL ACCIDENTS RISKS



a. represents sleeping time
b. representing eating, washing, dressing etc. at home
c. represents driving to or from work by car
d. represents the day's work
e. represents the lunch break
f. represents motor-cycling
g. represents communal entertainment, e.g. pub

Table III

VOLUNTARY AND INVOLUNTARY RISKS COMPARED[3]

Voluntary		Involuntary	
Activity	Risk of Death Per Person Per Year	Activity	Risk of Death Per Person Per Year
Smoking (20 cigarettes/day)	500×10^{-6}	Run over by road vehicle (USA)	500×10^{-7}
Drinking (1 bottle wine/day)	75×10^{-6}	Run over by road vehicle (UK)	600×10^{-7}
Football	4×10^{-6}	Floods (USA)	22×10^{-7}
Car racing	120×10^{-6}	Earthquake (California)	17×10^{-7}
Rock climbing	4×10^{-6}	Tornadoes (Mid-West USA)	22×10^{-7}
Car driving	17×10^{-6}	Storms (US)	8×10^{-7}
Motorcycling	200×10^{-6}	Lightning (UK)	1×10^{-7}
Taking contraceptive pills	2×10^{-6}	Falling aircraft (USA)	1×10^{-7}
		Falling aircraft (UK)	0.2×10^{-7}
		Explosion of pressure Vessel (USA)	0.5×10^{-7}
		Release from atomic power station -	
		(at site boundary) (USA)	1×10^{-7}
		(at 1 km) (UK)	1×10^{-7}
		Flooding of dikes (Holland)	1×10^{-7}
		Bites of venomous creatures (UK)	2×10^{-7}
		Transport of petro & chemicals (USA)	0.5×10^{-7}
		Transport of petro & chemicals (UK)	0.2×10^{-7}
		Leukemia	800×10^{-7}
		Influenza	2000×10^{-7}
		Meteorite	6×10^{-11}
		Cosmic rays from explosion of supernovae	$10^{-6} - 10^{-11}$

Failure Rate Data

A. Sources of Data

In order to use reliability engineering methods, a source of data on equipment failure and repair, various peripheral events, and human resources are required.

This necessary data can be obtained from three major sources:

1. Data Banks

One of the principal data banks used by the chemical industry is that provided in the U.K. by the United Kingdom Atomic Energy Authority called the System Reliability Service (SRS).

Normally, the facilities of the data banks are available to organisations through a subscription service.

There are also many published sources of failure rate data in the literature. A great deal of this data has been incorporated into existing data banks. Selected data from Anyakora, Engel and Lees[4] is presented at the end of this section (Table VIII) for general reference.

2. Plant Experience

Plant Experience can provide good failure data. A benefit is that environmental factors can automatically become part of the data. However, there is a tremendous amount of effort involved in the collection of meaningful data. It is very difficult to get operations people to record the amount of data required and unless there is a large sample with many failures, then the confidence limits on the data will be extremely large.

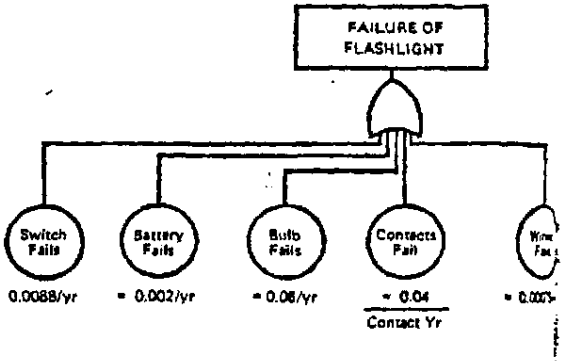
Event data can sometimes be obtained which can prove useful. For example, the number of times a particular relief valve has lifted can provide the demand rate directly for that relief valve. If the unit has had a large number of operating years experience, questioning the plant personnel or reviewing plant records can prove beneficial and supplement a fault tree analysis.

3. Prediction

Prediction really means to apply failure rate data for the elemental parts to produce the failure rate of the instrument. Elemental parts include components such as contacts, relays, springs, connections, etc. (See figure 12.).

Figure 12.

An example of the the technique of prediction is illustrated below which pred the failure rate of a common flashlight:



Failure Rate of Flashlight = 0.00088 + 0.002 + 0.06 + 4 (0.04) + 0.0001

= 0.22/yr

Lees[5] has summarized, observed and predicte instrument failure rate data shown in Table from various sources and there is generally w good agreement.

Table IV

Observed and Predicted Instrument Failure Rate

Instrument	Failure Rate (Observed Faults/y)	(Predic Faults
Control Valve[a]	0.25	0.19
Differential Pressure Transmitter[a]	0.76	0.4
Variable Area Flowmeter Transmitter[a]	0.68	0.7
Temperature Trip Amplifier:		
Type A	2.6	2.8
Type B	1.7	2.1
Controller	0.38	0.8
Pressure Switch	0.14	0.1
Gas Analyzer	2.5	3.3
Relay[a]	0.17	0.2

(a)

8. Instrument Failures

There are many factors which can influence instrument failure. Some of these are:

1. System Definition:

   Display/Control
   Accuracy/Precision
   Response

2. Installation

3. Environmental Factors - Internal

   Material (Gas, Liquid, Solid)
   Cleanliness
   Temperature
   Pressure
   Corrosion
   Erosion

4. Environmental Factors - External

   Control Room/Plant
   Temperature
   Humidity
   Dust
   Frost
   Vibration
   Impact

5. Operation

   Cycling

6. Maintenance

1. Environmental Factors

It is generally felt that environmental factors, in particular the types of materials that the instrument is in contact with (both internal and external), have the greatest impact on failure rate. From the same paper by Anyakora Engel and Lees[4] are the results of comparing similar instruments in clean and dirty fluids (Table V).

It is possible to assign correction factors for instrument failure rates in particularly dirty service if thought necessary. The instrument failure data at the end of this section in Table V include an environmental factor. To obtain a base failure rate divide the failure rate given by the environmental factor. Note also that the failure rate of the impulse lines should be added to the failure rate of the instrument itself to obtain the total instrument failure rate.

2. Failure Modes

There are normally a number of modes of failure for a given instrument. Lees[5] lists various fault modes for a control valve which are presented in

Table V

EFFECT OF PROCESS FLUID CONDITIONS ON FAILURE RATES[4]

Instrument	No. At Risk	No. of Faults	Failure Rate (Faults/Y)
Control Valve:			
Clean Fluid	214	17	0.17
Dirty Fluids	167	71	0.89
Differential Pressure Transmitter:			
Clean Fluids	27	5	0.39
Dirty Fluids	90	82	1.91

Table VI

FAILURE MODES OF A CONTROL VALVE[5]

CONTROL VALVE	NO. OF FAULTS
Leakage	54
Failure to Move Freely	
Sticking (But Moving)	28
Siezed Up	7
Not Opening	5
Not Seating	3
Blockage	27
Failure to Shut Off Flow	14
Glands Repacked/Tightened	12
Diaphragm Fault	6
Valve Greased	5
General Faults	27

It is important to know exactly what type of failure will be causing a potentially dangerous situation. Some of these modes are fail safe while others are fail dangerous and some occur over a period of time (slow) while others are instantaneous (sudden). In most applications, the sudden dangerous failure is the most serious. However, the failure data will normally not be sufficiently detailed to assess this failure rate for a dangerous mode. A rough rule of thumb is to consider that dangerous failures represent 25-50% of total failures and sudden dangerous failures 10-25% of the total failures.

3. Problems of Data Collection

Some of the problems in trying to collect plant failure data have been previously alluded to.

Below is a more comprehensive list of items that must be considered when attempting to collect

- Application of the Equipment
  Environment (External)
  Failure Mode
  Preventive Maintenance
  Operating Time
  Physical and Chemical Properties of the System and the Process Medium
  Repair Time
  Total Plant Population

The above list represents a vast information requirement. Who will collect the data (e.g. a special staff?, maintenance personnel?) and how will it be stored and accessed (e.g. computer?) are all difficult problems to address. There is a balance necessary between the level of data collection and the perceived benefit.

Few individual companies have elected to collect their own data.

C. Human Error

Human Error is an extremely complex subject. The actions of a human being are much more difficult to analyze because of variable factors such as:

- The work environment - control room, plant layout
- Management attitudes
- Stress level of immediate situation
- Physical and mental state of operator
- Recovery factor

The basic approach has been to examine human error on a failures per demand basis. For example, an operator may forget to close a valve after routine maintenance one out of every 100 times he is asked to perform that function. The probability of failure per demand is then 0.01.

Below are estimates on human error based on the complexity of the task and the stress level. (Table VII).

TABLE VII

HUMAN ERROR ESTIMATES
FRACTION OF TIME ERROR PER OPERATION OCCURS

COMPLEXITY OF TASK / LEVEL OF STRESS	SIMPLEST	ROUTINE AND SIMPLE	ROUTINE REQUIRES CARE	COMPLICATED, NON ROUTINE OTHER DUTIES REQUIRED
NONE	1×10^{-4}	5×10^{-3}	1×10^{-2}	0.1
MODERATE	1×10^{-3}	5×10^{-2}	5×10^{-2}	0.3
EMERGENCY HIGH STRESS	1×10^{-2})	0.5)	0.25)	1.0

Table VIII

INSTRUMENT FAILURE RATE DATA, ANYAKORA ENGEL AND LEES[4]

Instrument	No. At Risk	Instrument Years	Environment Factor	No. of Faults	Failure Rate (Faults/y)
Control Valve	1531	747	2	447	0.60
Power Cylinder	98	39.9	2	31	0.78
Valve Positioner	334	158	1	69	0.44
Solenoid Valve	252	113	1	48	0.42
Current/Pressure Transducer	200	87.3	1	43	0.49
Pressure Measurement	233	87.9	3	124	1.41
Flow Measurement (Fluids):	1942	943	3	1069	1.14
Differential Pressure Transducer	636	324	3	559	1.73
Transmitting Variable Area Flowmeter	100	47.7	3	48	1.01
Indicating Variable Area Flowmeter	857	409	3	137	0.34
Magnetic Flowmeter	15	5.98	4	13	2.18
Flow Measurement (Solids):					
Load Cell	45	17.9		67	3.75
Belt Speed Measurement & Control	19	7.58		116	15.3
Level Measurement (Liquids):	421	193	4	327	1.70
Differential Pressure Transducer	130	62	4	106	1.71
Float-Type Level Transducer	158	75.3	4	124	1.64
Capacitance-Type Level Transducer	28	13.4	4	3	0.22
Electrical Conductivity Probes	100	39.8	4	94	2.36
Level Measurement (Solids)	11	4.38	–	30	6.86
Temperature Measurement (excluding Pyrometers)	2579	1225	3	425	0.35
Thermocouple	772	369	3	191	0.52
Resistance Thermometer	479	227	3	92	0.41
Mercury-in-steel Thermometer	1001	477	2	13	0.027
Vapour Pressure Bulb	27	10.7	4	4	0.37
Temperature Transducer	300	142	3	124	0.88
Radiation Pyrometer	43	30.9	4	67	2.17
Optical Pyrometer	4	3.4	4	33	9.70
Controller	1192	575	1	164	0.29
Pressure Switch	549	259	2	87	0.34
Flow Switch	9	3.59	–	4	1.12
Speed Switch	6	2.39	–	0	–
Monitor Switch	16	6.38	–	0	–
Flame Failure Detector	45	21.3	3	36	1.69

CONCLUSION

As stated in the Introduction, this Symposium address has dealt with Air Products' Management Approach to Safety and Hazard Analysis.

Often it is wrongly assumed that one can separate the more traditional "Safety Management" concepts from the more novel "Hazard Analysis" techniques. It should now be obvious from the presentation that hazard analysis is necessary to fully understand and hence control possible hazards and in this respect is an extension of Safety Management.

However, what must be emphasized is that the correct application of hazard analysis depends on there being effective Safety Management. This point was spelt out in a recent paper by Trevor Kletz:[7]

> "It is an unwritten assumption when applying Hazard Analysis that the plant is designed, operated and maintained according to good engineering and management standards. If this is not true, hazard analysis is a waste of time. It is no use calculating the probability of unlikely events if serious incidents are probable as a result of a poor permit-to-work system, lack of instructions, "Heath Robinson" methods of maintenance and so on. Hazard analysis is a sophisticated technique for good organisations who wish to allocate their resources sensibly and improve their standards. It should not be used until the basic management is satisfactory."

References

1. Kletz, T.A., "Hazard Analysis -- A Quantitative Approach to Safety", IChE Symposium Series No. 34, Institution of Chemical Engineers, London, 1971.
2. Bulloch, B.C., "The Development and Application of Quantitative Risk Criteria for Chemical Processes", IChE Symposium Series No. 39a, Institution of Chemical Engineers, London, 1974.
3. Gibson, S.B., "Risk Criteria in Hazard Analysis", CEP, Vol 72, No. 2, Feb 1976.
4. Anyakora, S.N., Engel, G.F.M., Lees, F.P., "Some Data on the Reliability of Instrument in the Chemical Environment" The Chemical Engineer, Nov. 1971.
5. Lees, F.P., Loss Prevention in the Chemical Process Industries, Vol I, Butterworth, 1980.
6. U.S. Atomic Energy Commission, "Reactor Safety Study An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400, Washington, D.C. 1974.
7. Kletz, T.A. "Hazard Analysis - The Manager and the Expert". Reliability Engineering 2 (1981) 35-43.

Other References of Risk Criteria

Farmer, F.R., "Experience in the Reduction of Risk", IChE Symposium Series No. 34, Institution of Chemical Engineers, London, 1970.
Kletz, T.A., "The Application of Hazard Analysis to Risks to the Public at Large", World Congress of Chemical Engineering, Amsterdam, July 1976.