HAZCHECK AND THE DEVELOPMENT OF MAJOR INCIDENTS

G L WELLS and C PHANG (University of Sheffield, Sheffield, UK)

A B REEVES (AEA Technology, Culcheth, UK)

The events which build up into the occurrence of a major incident have been classified and programmed within a small database. This serves as a crude but structured checklist, termed HAZCHECK, which is available for use on an IBM compatible personal computer.

Much effort has been put into the establishing of a consistent nomenclature and the clear distinction between root or basic causes of an incident and the immediate causes which initiate a particular chain of events.

ROOT CAUSE, MAJOR INCIDENTS, AUDITS

THE DEVELOPMENT OF MAJOR INCIDENTS

A major process incident has its origins in root or basic causes and develops by the scenario illustrated in Figure 1.

Such an incident has the potential to cause major distress, hospitalize individuals, cause death to susceptible individuals and damage the environment. Apparently it is initiated by an immediate cause and progresses along the primary event chain summarised in Table 1. This table does not repeat the interconnections noted above. Adherence to rigid definitions of immediate and root causes and avoiding terms such as intermediate cause to define loss of protection leads to a better definition of the accident scenario for investigation purposes, design and the evaluation of risk.

The event chain shows how incidents develop. For general study of the frequency of occurrence of events it is desirable to estimate how often specific deviations and disturbances normally occur. This can be done with confidence only for the main events of each major accident involving a fatality or serious injury. So in the absence of appropriate additional data it is only possible to postulate that something like a million root causes of problems and disturbances might arise for every major incident, as suggested in Figure 3.

Such figures show that it is impractical to eliminate all causes of failures and discharge. They can only be reduced by constant vigilance. It is also clear from plotting the traditional range of hazard identification and evaluation techniques that not one of these covers the range of events particularly well, see Figure 4. Clearly root causes, see figure 2, are not readily identified by top-down studies but must be reduced using a bottom-up strategy and good practice.

TABLE 1 - The Primary Event Chain

DAMAGE OR HARM TO PEOPLE, PLANT, BUSINESS AND ENVIRONMENT
- Harm to environment and people
- Damage to plant and property
- Impact on business
- Incident which is a near-miss

ESCALATING EVENTS AND FAILURE OF MITIGATION
- Inadequate post-accident response
- Inadequate emergency response
- Countermeasures inadequate
- Secondary escalation by explosion, fire or toxic release
- Escalation by toxic release
- Escalation by explosion
- Escalation by fire

UNPLANNED RELEASE OF MATERIAL
- Loss of significant process material
- Rupture on exceeding mechanical design limitations
- Equipment rupture due to defective or deteriorated construction
- Material lost through abnormal opening to atmosphere
- Loss on change in a planned discharge or vent

FAILURE TO CONTROL THE SITUATION
- Emergency control systems fail to control the situation
- Operators fail to control the situation
- Normal control systems fail to control the situation
- Maintenance fails to control the situation

PLANT IN DANGEROUS STATE
- Dangerous trend in operating conditions
- Construction defective or deteriorated in service
- Abnormal opening in equipment
- Change in a planned discharge or vent

IMMEDIATE CAUSES OF FAILURE AND DISCHARGE
- Inadequate action by operator, maintenance or other personnel
- Plant, equipment or facilities inadequate or inoperable
- Control or emergency control inadequate or inoperable
- Defects directly causing loss of plant integrity
- Change from design intent
- Environmental and external cause

ROOT CAUSES OF FAILURE AND DISCHARGE
- Inadequate maintenance
- Inadequate transport of materials
- Inadequate engineering and plant realisation
- Inadequate process design and knowhow
- Use of inappropriate or inadequate procedures
- Inadequate or wrong information, transfer and processing
- Personnel inadequate in task
- Inadequate capabilities of management and organisation
- Change in process requirements and external threats

ROOT CAUSES OF FAILURE AND DISCHARGE

Root causes generally represent conditions, capabilities and practices which fall below standards. They are identified in Table 2 and illustrated in *Figure 2*. *They affect all immediate causes, all actions to control* the situation and all mitigating actions. It is convenient to classify inadequate engineering and plant realisation as a basic cause.

TABLE 2 - Root Causes

Inadequate Engineering, Plant Realisation and Maintenance

- Inadequate maintenance
- Inadequate commissioning and realisation
- Inadequate construction
- Inadequate manufacture/assembly
- Inadequate safety reviews and plans
- Inadequate site and plant layout
- Inadequate transport of materials
- Inadequate detailed engineering
- Inadequate engineering standards and specifications

Use of Inappropriate or Inadequate Procedures

- Inadequate or faulty procedures
- Inadequate working practices
- Procedures difficult to follow
- Inadequate specification of task
- Absence or inadequate introduction of procedure
- Adverse extrinsic task factors
- Adverse intrinsic task factors

Personnel Inadequate in Task

- Improper and inadvertent actions
- Adverse physiological state
- Inadequate quality and character
- Task overload of personnel
- Personnel absent or incapacitated
- Inadequate training and rehearsal
- Inadequate man-machine interface
- Inadequate operating environment

Change in Process Requirements and external threats

- Change from specified process use
- Operational change
- Failure to manage change
- Disturbance from other systems
- Extreme environmental and external causes including sabotage

Inadequate Process Design

- Inadequate operating instructions
- Inadequate contingency measures
- Inadequate emergency control systems
- Inadequate control/operability
- Inadequate preliminary evaluation
- Lack of consideration of states
- Excessive process discharges
- Excessive inventory and severe operating conditions
- Inadequate development and design
- Inadequate process knowhow

Inadequate Information, Transfer and Information Processing

- Inadequate or wrong information
- Inadequate information processing
- Faulty problem solving, decision-making and risk-taking
- Incorrect response to information
- Loss of meaning on communication
- Inadequate channels of communication
- Inadequate information transfer

Inadequate Capabilities of Management and Organisation

- Inadequate management abilities
- Failure to direct and coordinate
- Inadequate safety leadership
- Inadequate corporate management
- Inadequate technological experience
- Inadequate supervision & management
- Inadequate provision of resources
- Inadequate human resource management
- Inadequate facilities and site
- Inadequate procedures and standards
- Adverse organisational factors and corporate culture
- Inadequate response to change
- Failure to identify or monitor the capabilities of the firm
- Inadequate corporate strategies and tactics

IMMEDIATE CAUSES OF FAILURE AND DISCHARGE

The immediate causes of incidents are seen as the initiating events. They are given in Table 3. Inadequate action by personnel can be broken down according to the conventional job descriptions of operators, etc. Human failure or error is normally used in such a context but all too readily is inferred as to imply blame. The root cause of the incident is wherein blame probably lies. Change from the design intent is a helpful term with its link to inadequate management and organisational capabilities. Environmental and external cause are often significant only because of faults in the engineering design although obviously deliberate sabotage can be hard to prevent.

TABLE 3 - *Immediate Causes*

Inadequate Action by Operator Maintenance or Other Personnel

Failure to process information check or report
Action based on inadequate or incorrect information
Action not stimulated, not taken or omitted
Action or check generating inadequate information or response

Process, Equipment, or Other Facilities Inadequate or Inoperable

Sudden failure of equipment
Gradual or partial failure incipient failure
Use of facilities ignored
Faulty information, transfer or processing
Design functional deficiencies
Inadequate installation
Failure unavailable for use

Control System Inadequate or Inoperable

Control system inadequate or defective
Control system cannot be used when required
Control system used incorrectly by operator
Design functional deficiencies
Inadequate installation of system
Monitoring system faulty or inadequate

Defects Directly Causing Loss of Integrity

Defective or missing components
Inadequate inspection
Failure to detect defects prior to start-up
Failure to support plant correctly
Incorrect construction/installation
Construction causes stresses/cracks
Defective manufacture or assembly
Incorrect or flawed joints, welds seals, packing, etc
Incorrect or flawed materials

Change From Design Intent

Use of equipment for purposes and conditions outside those specified
Incorrect modification from design intent during plant realisation
Incorrect modification or other change particularly during maintenance
Incorrect supply of raw materials and services

Environmental and External Cause

Normal environmental extremes
Act of god and natural causes
General accidental impact damage
External energetic and toxic events
External interference causing loosening
Force majeure, sabotage, theft, hooliganism
Effect of environmental and external cause on personnel

PLANT IN DANGEROUS STATE

The deviation and disturbances noted under this heading in Table 4 are expanded to identify specific cause within the HAZCHECK program. Other systems do much the same. Indeed the methodology of HAZOP is primarily directed at the identification of dangerous trends in operating conditions or a change in a planned discharge, and there is much value in having a terminology which readily focuses on possible disturbances. Study of the incident chain places a higher priority on identifying causes of overpressure and overtemperature than changes in flow. A breakdown of the usual causes of deviations is helpful as it reduces the reliance on the memory of the team or individual effecting the study.

TABLE 4 - Plant In Dangerous State

Dangerous Trend in Operating Conditions

Underpressure, excessive vacuum
Overpressure resulting from explosion
Overpressure from connected pressure source
Thermal expansion of process material
High temperature from direct source
High temperature from increase in heating or decrease in cooling
High temperature from change in mixing
High temperature from unexpected exothermic reaction at any location
Low temperature of wall, usually extremely cold
Dangerous trend (see change in a planned discharge)

Change in a Planned Discharge or vent

Change of composition or concentration
Change in phase, fraction of phase or additional phase
Change of rate, velocity, direction or quantity of flow
Change in size or other physical properties of process materials
Change in a periodic or fugitive discharge or normal vent
Change in dispersion of a discharge

Construction Defective or Deteriorated in Service

Loosening or disconnecting by personnel
Loosening by vibration
Corrosion, stress corrosion or erosion
Distortion or aging due to chemical attack or thermal expansion
Creep and fatigue
Variations in loadings
Water hammer or other change causing thermal stress, pressure waves or transient flows
Impact and changes due to excessive stress or force
Out-of-tolerance faults: changes due to wear, friction, rubbing, thinning, weakening, etc.
Deterioration due to external attack
Defect or its propogation prior to failure

Abnormal opening in equipment

Incorrect status of equipment valve or safety system
Failure of isolation device to air
Discharge of safety device
Construction defective (leave open)
Abnormal opening for entry or discharge

FURTHER DEVELOPMENT OF THE INCIDENT

Tables 5-7 follow the development of the incident. Clearly many of the activities relating to control of the situation by corrective or mitigating action take place at the same time. It is particularly important to stress the role of the operator in resolving many of the problems without the need for intervention by the emergency control systems. Maintenance is vital to preventing the release of material within the design mechanical limitations of equipment. At the same time the loosening of equipment by maintenance personnel is a major cause of the release of material. .

Table 6 is useful as it emphasises the way in which release occurs given the plant in a dangerous state and the failure to control the situation. The loss of material may in itself be at a significant rate or it may accumulate. Explosion can initiate the release of material or cause secondary escalation. The spurious failure of a relief system can initiate the hazardous situation. However for purposes of analysis it is convenient to follow the sequence given here.

The frequency at which incidents might occur should be assessed together with the consequences of their occurrence. This can then be used to evaluate the hazard category of incidents.

TABLE 5 - Failure to Control the Situation

Emergency Control System Fail to Correct the Situation

Incorrect use of emergency control
Defect of emergency control system causes or increases danger
Emergency control systems inadequate or failed
Emergency control systems not provided, installed or available

Operators Fail to Control the Situation

Action of operators causes or increases hazards
Contingency action by operators fails to reduce trend
Incorrect discharge of the system through an available opening
Action of operators causes or increases hazard
Inadequate action by operators
Failure to take action by operators

Normal Control System Fails to Correct the Situation

Defect of control system causes or increases hazard
Control system inadequate or failed
Reading or indication is invalid
Incorrect use of control system
Control system not provided disabled or isolated

Maintenance Fails to Control the Situation

Malufunction cuses or increases the hazard
Malfunction of maintenance causes or increases hazard
Inadequate action taken by maintenance
Failure to take action by maintenance

TABLE 6 - Unplanned Release of Material

Loss of Significant Process Material

Release detected but not isolated or attenuated before significant loss
Release not detected or reduced befor significant

Release of Material by Rupture or Discharge

Mechanical design limitations exceeded
Rupture due to defective or deteriorated construction
Loss through abnormal opening to atmosphere
Change in a planned discharge, emergency discharge or vent

TABLE 7 - Escalating Events and Failure of Mitigation

Inadequate Post-accident Response

Inadequate post-accident action
Inadequate health control

Countermeasures Inadequate

Inadequate segregation of people plant and external threats
Inadequate protection of plant personnel and environment
Inadequate countermeasures for vapour and gas emission
Failure of secondary containment or avoiding vaporisation
Inadequate response of people
Release fails to disperse
Inadequate detection and activation of response
Failure to attenuate loss
Inadequate detection and warnings

Inadequate Emergency Response

Inadequate preparedness
Failure of information interface
Inadequate protection environment, personnel and plant
Inadequate service arrangements
Inadequate on-site response
Inadequate response to leak
Failure to limit people on-site
Inadequate off-site response
Inadequate segregation

Escalation by Toxic Loss

Further spread of release
Further loss of toxic material due to explosion or evaporation
Failure to prevent reactions
Failure of emergency relief treatment
Failure to dilute material
Release fails to disperse

Escalation by Explosion

Secondary escalation by explosion
Explosion of external vapour cloud
Explosion and BLEVE
Dust explosion
Confined explosion prior to release
Physical or condensed-phase explosion
Runaway reaction of explosive force
Failure to avoid primary explosion
Electical explosion

Escalation by Fire

Further release of material following fire
Ignition of fire previously extinguished
Further spread of fire
Failure to extinguish fire
Flammables ignited on release
Failure of ignition source control
Significant flammable mixture
Fire prior to release

HAZCHECK

HAZCHECK has been developed to provide an aid for the identification of factors affecting the development of an incident. HAZCHECK gives guidance; for example on contingency measures and emergency control systems. The structure of HAZCHECK follows that given in Figure 1 and Tables 2-7.

HAZCHECK runs on an IBM Compatible PC. The program contains extensive further notes on each topic so that, for example, overpressure from vaporisation can be subdivided into specific causes. In this way it is possible to use the expertise put into the programme as a means of generating causes for a specific plant incident. A window system is used to access the information. Thus the root cause 'Personnel inadequate in task' expands as follows:

```
Personnal inadequate task
     Improper and inadvertant actions
     Inadequate quality and innate characteristics
     Inadequate task training and appraisal
     Inadequate safety training and rehearsal
     Task overload of personnel
     Inadequate operating environment
```

and 'Inadequate task training and appraisal' is then developed under the following headings

```
Inadequate task training and appraisal
     Inadequate experience in task or process
     Inadequate training
     Inadequate appraisal
     Inadequate opportunities for worker suggestions
     Disturbance caused by monitoring performance
```

HAZCHECK is a simple data base which may be used as a rough checklist. The process engineer can use it within any general strategy for implementing risk control. It is applied not solely at the design stage of plant but throughout the life of a plant, including its dismantling and disposal. Brief notes on applications to some recent incidents are noted in Table 8.

It would be helpful to be able to claim that a study of incidents justifies the breakdown and to give details of the contribution of each root cause. However this is frustrated by the lack of detail in incident reports. For example it is rare that reference is made to the adequacy of corrective and protective actions, and the identification of root cause is almost entirely ignored. Occasionally mention is made of lack of information or training and the capabilities of management may be criticized. But all too often a report might emphasise an immediate cause such as human error when inadequate human action due to specified root causes and failure of emergency control systems would be more appropriate. Indeed the root causes of the incident may not be defined even when blame is apportioned by the courts.

TABLE 8 - Some recent incidents

INCIDENT	IMMEDIATE CAUSE	FAILURE TO CONTROL THE SITUATION	MAIN ROOT CAUSES
Kings Cross 1987 *Fire on escalator*	Flammable material accumulated in *escalator area*	Failure to remove material. *Absence of ignition* control. Inadequate emergency response.	Change from design intent(lack of cleaning) Inadequate procedures (inspection, ignition) *Inadequate emergency planning* Inadequate fire protection Inadequate resources for maintenance workload Inadequate learning from previous incidents Inadequate safety objectives
Zeebrugge 6 March 1987 Capsize of ferry	Bow doors open on departure	No protection as doors open at critical speed/ sea conditions. Ship poorly trimmed	Inadequate procedures/communication Inadequate design of protection systems Inadequate training Change from design intent (doors open) Inadequate job supervision.
Camelford 6 July 1988 Pollution of public water supply	Aluminium sulphate unloaded into wrong tank	Failure to monitor water quality. Inadequate emergency response.	Inadequate procedures Inadequate emergency plan Inadequate task supervision Inadequate communication of requirements to driver.
Bhopal 3 Dec.1985 Toxic gas release	Water incorrectly mixed with MIC and and reaction due to wrong routing or *sabotage*	Protection systems shutdown. Inadequate emergency response.	Inadequate design: pipework, spray size Inadequate procedures Inadequate emergency plan Inadequatemaintenance of protective equipment *Inadequate job supervision* Possible sabotage Inadequate capabilities of management
BP Grange-mouth 13 March '87 Fire in Flare system	Loosening of flange when equipment not effectively isolated	Failure to cease work when leak noted. Failure of ignition control. Inadequate personal protection. Failure to shut-down *downstream plants.*	Inadequate procedures for maintenance and isolation Inadequate design (valve and layout) Inadequate job supervision Inadequate use of available information Inadequate training Inadequate communication at several levels *Inadequate planning of task*
Piper Alpha North Sea 6 July '88 Fire on Oil platform	Valve removed but replaced by cap that was not leak-proof. Start-up of pump after shift change	Explosion prevented emergency isolation and destroyed fire-wall. Incoming gas pipeline ruptured and gas burns as torch. Large pool fire on further escalation	Inadequate permit to work procedures Inadequate physical locking off/tagging of isolation valves. Inadequate communication on shift change Excessive inventory of flammables Inadequate location of emergency isolation valves Inadequate layout of rig Inadequate protection *Inadequacy in fire and explosion of key* equipment and emergency plan

GENERAL CONCLUSIONS

The analysis of incidents and the incident chain suggests that there is a need to apply four basic approaches within any structured programme of risk control. These are as follows:

a) **Give attention to process design and inherent safety** with particular consideration of process route, equipment needed, inventory and operating conditions. All feasible reactions must be identified allowing for impurities being present.

b) **Improve the engineering and operability of the system**, including all protective measures, with an emphasis on the use of the highest standards of engineering, plant realisation and maintenance, with effective monitoring which fully considers the role of the production and maintenance personnel, and having adequate safeguards to control any situation both on and off the site.

c) **Control external threats and unplanned changes** by adopting a strategy that assumes a plant is under constant threat, particularly from human interference and the environment.

d) **Implement total quality management in company and plant** to maintain constant vigilance to eliminate disturbances and faults. Monitor the frequency with which they occur, carry out regular safety audits and root-out problems at their inception.

HAZCHECK can help in all these tasks. It is being extended to permit of short-cut quantified risk analysis. This includes factors for the quality of the maintenance and the loss prevention programmes, the quality of engineering design and realisation and construction, the capabilities of the management and organisation, and the experience on-site for a specific process. Quantification of risk also helps in highlighting the immediate reduction of safety stemming from any removal or degradation of a clearly identifiable defence against incidents. Such degradation as arose at *Bhopal can be analysed so as to suggest the likely frequency of a major* incident as increasing from 10^{-4} per year to 10^{-1} per year or less.

The basic list also is being adapted to use a questioning approach for application in conjunction with conventional auditing methods. This is directed towards root cause analysis, the identification of performance indicators and the need for the two safeguard approach to protection against loss of control of the situation.

GENERAL REFERENCES

1. Crosby P B, Quality without Tears, McGrawhill, 1984.

2. Reeves A B, Davies J, Wells G L, Foster J, GOFA, Int.Conf. on Quality Management in the Nuclear Industry, IMechE, 17-18 Oct, London, 1990.

3. Wells G L, Safety in Process Plant Design, Godwin, 1979.

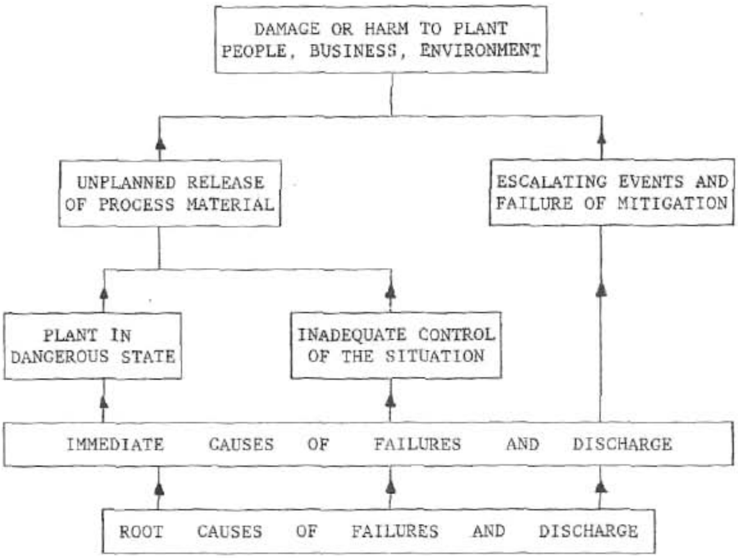


Figure 1 Development of an incident

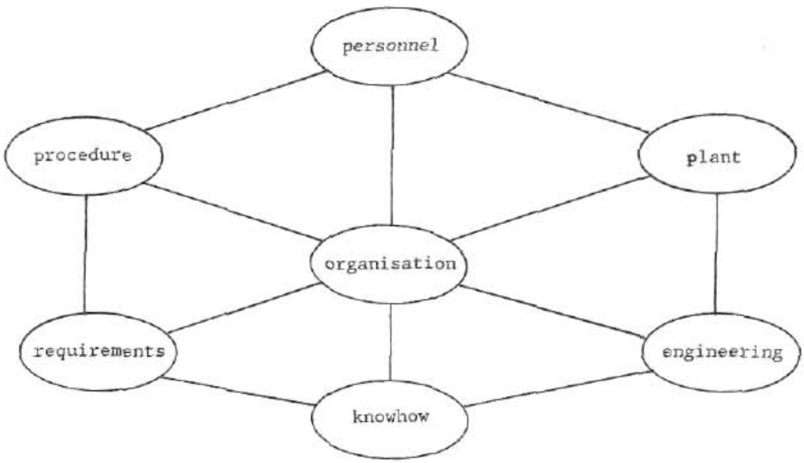


Figure 2 Simplified representation of root causes

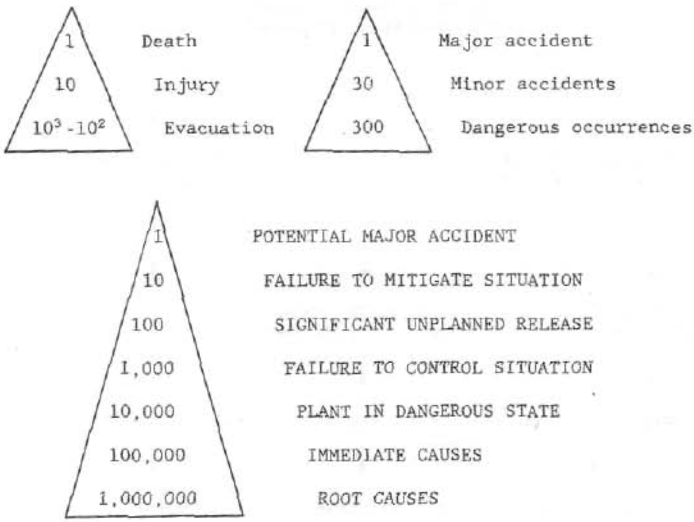
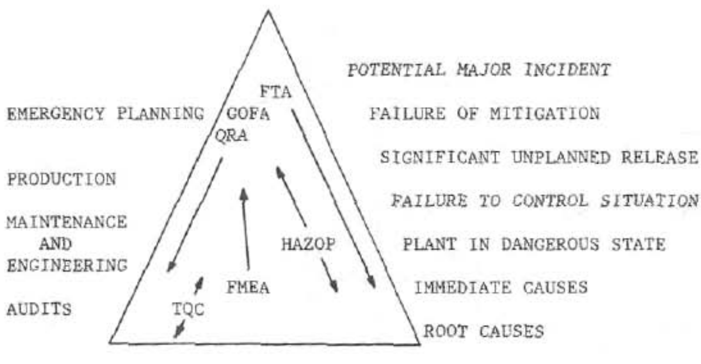


Figure 3 Suggested Relative Frequency of Events



KEY:

GOFA Goal Orientated Failure Analysis	FTA Fault Tree Analysis
FMEA Fault Mode and Effect Analysis	QRA Quantified Risk Analysis
HAZOP Hazard and Operability Studies	TQC Total Quality Control

See General References for further information.

Figure 4 Activities and Analysis with Each Event