Safety & Reliability Society Symposium
25th September 1986
Statutory Safety - Meeting the Requirements

THE SAFETY MANAGEMENT FACTOR : AN ANALYSIS OF THE HUMAN ERROR ASPECTS OF THE BHOPAL DISASTER

by

Linda J Bellamy, Technica Ltd., Lynton House, 7/12 Tavistock Square, London WC1H 9LT

1. INTRODUCTION

The aim of this paper is to examine some of the possible human contributions to the Bhopal disaster. The human factors analysis was carried out as part of an investigation by Technica sponsored by the Dutch Government. A group consisting of HAZOP and HAZAN practioners, consequence analysts and a human factors specialist undertook this demonstration exercise in order to illustrate some of the insights achievable through risk analytic techniques.

The team's examination was based on the available literature and the information that was reportedly available to management and to the authorities on which to base planning and operational decisions. As yet, no official report has been released and so there is no authoritative account of the causes of the Bhopal disaster. However, a number of versions of the events leading up to the massive release of methyl isocyanate vapour in the early hours of December 3rd 1984 have now been published (see References). By putting these together, a fairly complete and convincing scenario was obtained by the Technica team. Although undoubtedly not the only possible scenario, it did seem to fit all the features observed and is not contradicted by any of the evidence so far available. The human factors analysis that was carried out was based on this scenario.

2. PLANT SITING

The Bhopal plant, owned by Union Carbide and operated by Union Carbide India Ltd (UCIL), was built to produce a pesticide, Sevin, a DDT substitute.

The plant was located in Madhya Pradesh, said to be part of a policy to bring industry to less developed states. The site, by an old town in a lakeside setting, was initially a quiet suburb but it attracted a large squatter camp. Technica's estimate of the population density at the time of the disaster was 250 persons per hectare (per 10,000 m^2) (from map in Delhi Sceince Forum, 1985).

The release on 3rd December 1984 is said to have caused:

- Over 2,500 fatalities
- Over 200,000 seeking medical treatment
- 70,000 evacuated

The very important issues of disaster planning, management and community response are not dealt with here and warrant further examination.

3. DESIGN FEATURES

From a hazards point of view, the key feature of the design was:

- Provision of storage for up to 180 tonnes of methyl isocyanate (MIC) on site.

Protective systems were needed to ensure that the MIC remained confined. There were two sources of uncontrolled discharge:

- External fire
- Ingress of water leading to an exothermic reaction.

Exclusion of water was achieved by:

- Cathodic protection of tanks against external corrosion.
- Maintenance of tank contents well below a temperature at which attack on tank material would occur.
- Cooling by non-aqueous refrigerant (Freon)
- Use of dry nitrogen for purging and pressure control.
- Ensuring systems requiring water washing are isolated from MIC containing systems by slip plates.

Protection against tank rupture was achieved by:

- Conventional safety relief valves backed up by bursting discs.
- Discharge lines from the relief valves (relief valve vent header) to a containment system, the main feature being a recirculating caustic soda scrubber. This also neutralised "breathing" vents fed in via a separate header (process vent header).
- In the event of a relief discharge exceeding scrubber capacity, the excess flow would automatically be diverted to a flare tower.

From statements made in the Union Carbide (1985) report it is estimated that the scrubber plus flare system was designed for a maximum discharge rate of 10,000 lbs/hr (1.3 kg/s).

This design was based on the assumption that full cooling would be provided by the refrigeration system. Technica's estimated values for the parameters of the MIC release on 3rd December 1984, inferred from the published data, indicated a release rate of 3.5 kg/s over a duration of 2 hrs (about 25 tonnes released) at a temperature of 42°C.

4. ACCIDENT SCENARIO

Figure 1 (taken from Bhushan and Subramaniam, 1985) shows the possible route of ingress of water into tank 610 which is believed to have caused the release (the Union Carbide report estimates about 1 tonne of water). This apparently occurred following washing out operations of another section of the plant. The detailed hypothesis of how the water got in is given in Slater (1986).

The inferred route taken by the water includes a "jumper" line between the vent headers, believed to have been installed by UCIL management around December 1983. The segregation of these headers had been one of the important design features of the water exclusion system.

Although this was a necessary condition for the accident to occur, altogether nine contributory causes were identified as being necessary and sufficient for the accident scenario.

These conditions were:

- MIC in the storage tanks
- Existence of jumper line
- Removal of refrigeration
- Water in pipework with connection to MIC storage tank
- Sufficient quantities of MIC and water
- Insufficient isolation of areas being washed
- Valves in connecting pipework open or ineffective
- Blocked bleeder valves
- Reaction of MIC and water could not be contained by tank design, human action, flare, or vent gas scrubber

At this level of analysis, the immediate causes are apparent but there is no easily discernible pattern of failure. Although recommendations could be given at this level to prevent recurrence of this scale of accident, these are necessarily somewhat specific to Bhopal, and the as yet unidentified root causes may not be addressed. The human factors analysis was aimed at investigating the underlying pattern of failures and the possible causes.

5. HUMAN ERRORS

The most useful definition of human error, from the point of view of evaluating the human contribution to risk, is:

> Any action or failure to act which could cause a system or sub-system to exceed defined limits.

The hypothesised enabling conditions identified above were examined for possible human error causes by analysis of the available report literature. An outline of the way in which failures of the human and equipment components could be related is presented in Table 1. The enabling conditions were subsumed under five major characteristics of plant design and operation, as shown in the first column of the table. Supporting evidence is given for the hypothesised human errors and associated equipment failures.

The analysis suggests a combination of design, decision and procedural errors. Were these related? As large systems typically incorporate relatively independent subsystems, if all the safety systems (engineered and human) fail then it is likely then one or more common factors were at work.

6. POSSIBLE CAUSES OF HUMAN ERROR

6.1 Lack of Design Support Emphasises Human Safety System

One of the areas where the Bhopal plant was criticsed in the literature is in terms of its lack of automatic devices to help maintain the system within tolerable limits (e.g. Bowonder, 1985). It is said that safety systems had to be manually switched on, there was a general lack of automatic warning systems, and safety interlocks were not provided for critical systems. If this is the case then the operator does not appear to have been given much support from the designer.

There is a case to be argued both for and against such automation when considering its effect on human error occurrence. Increased automation can result in increased complexity and interdependence of system components. This in turn increases the likelihood of unanticipated failures or abnormal conditions which are difficult to diagnose.

However, what must be appreciated is that, in the absence or failure of automatic safety devices, the human being is a primary barrier to hazard. Physical, chemical and other forms of containment must be maintained by people; when equipment fails the operator must identify it and put it right; unpredicted process and plant reactions must be diagnosed and cured; adjustments must be made to the process so that conditions remain within efficient and safe limits.

Human beings are therefore not a nuisance. They are an asset. Having said this, it is now easier to put the human causal involvement in the Bhopal tragedy into perspective. That is, there must have been a failure of the human safety system.

6.2 Safety Role Ambiguities

Possible primary candidates with responsibility for safety were identified as:

- Operators
- UCIL supervision and management
- The parent company in the US
- The Madhya Pradesh inspectorate
- The Indian Government

A conclusion was reached that safety roles were probably highly ambiguous (lack of proper specification of safety duties). Potentially independent human safety systems could also fail to "audit" each others decisions and enforce safety. The implications of the report literature were that it could not be clearly established who was responsible for:

- Ensuring that the established procedures of the plant were followed.
- Ensuring that plant management, supervisory and operations personnel had sufficient plant knowledge, training and experience to operate the plant safely.
- Ensuring that the original design of the plant was safe.
- Ensuring that the plant was maintained in a safe condition.
- Defining the safety criteria and ensuring that they were maintained.
- Providing information about risk, such as MIC toxicity, and who should be informed. It should be noted that in the USA there is as yet no requirement to inform the local public of toxicity effects of plants and in the UK this has only recently become a requirement.

- Ensuring that if plant procedures or design were changed they met the safety criteria.
- Identification and notification of unsafe practices or design and whom should be notified.
- Evaluating plant siting and risk to the public.
- Ensuring the enforcement of health and safety legislation.

The execution of these roles represent the primary and back up human safety systems.

6.3 Lack of Knowledge, Rules and Procedures

Operators need to know what the limits of a system are in order to avoid error. Variability in operator behaviour can be controlled by rules and procedures, providing these are followed, but they cannot cater for events that are unanticipated. System knowledge, and sometimes expertise, is also required.

It is possible that operational and/or critical decision making personnel at Bhopal could have lacked sufficient system knowledge. Such knowledge enables the consequences of actions or system state changes to be anticipated during the lifetime of a process plant. It would therefore be important to consider whether operators, supervisors and management at UCIL had sufficient training, experience and formal procedures to enable them to operate the plant safely.

The potential for a serious human error is markedly increased if inadequacy in the engineered safety systems is coupled with insufficient system knowledge.

6.4 Lack of System State Information

Just after washing of the filter RV lines began at 9.15 pm on 2nd December it is reputed that an operator noticed that the bleeder valves were blocked. The situation could have been recovered but, if the reports are correct, the supervisor apparently ordered washing to continue. Another event occurred an hour later. Pressurisation of tanks for transference of MIC to the Sevin plant began but pressure in tank (2 psi) failed to rise.

Fifteen minutes later there was a shift change. This shift was said to have observed leaks of MIC, a pressure rise in tank 610, and ultimately the catastrophic discharge.

A detailed examination of the report literature led to the following questions arising:

1. Was there insufficient communication between shifts? Events that had taken place on the previous shift may not have been recorded. Such information could have included operations carried out, records of indicator readings, and problems encountered. The new shift may have had no way of knowing, for example, whether or not the pressure rise in 610 was due to some previous operation. The earlier shift could have pressurised the tank with nitrogen to transfer MIC to the pesticide plant.

2. Was there a reliable indicator to provide information on the considerable temperature rise from the exothermic reaction in the tank?

3. Were the tank pressure and level indicators working correctly and did operators consider that readings taken from them were reliable?

4. Were sufficient warning information systems available and in operation (temperature, pressure and leak alarms)?

5. Did the operators have sufficient information on MIC toxicity and the behaviour of MIC on contact with water to enable accurate perception of risk?

If the water was not actually turned off until 12.30 am (Badhwar and Trehan 1984) it implies that it took one and a half hours to diagnose that water had entered the tank since the first indication of abnormality at 11 am. Note that the toxic gas alarm was reputedly not switched on until 1 a.m. (Union Carbide, 1985). Why had it been turned off anyway?

Had action been taken immediately the water entered the tank it <u>might</u> have been possible to avert the disaster or at least have provided a longer warning time for the community. This, of course, would have required an immediate diagnosis of the cause, prediction of effects, and identification of the best emergency procedure to deal with it. But even the experts have subsequently had problems in achieving this!

6.5 Economic Pressure

If, as has been reported in the media, pesticides sales in India had been sinking then economic pressures would exist to minimise the costs of pesticides production. Human error in response to pressures of one sort or another is a common contributory factor in major accidents.

If the Bhopal plant was subject to economic or production pressures, one would expect to find certain indicators of this, principally:

- A decrease in production
- Reductions in manning and/or manning costs
- Reductions in downtime and/or attempts to reduce downtime
- Reductions in costly equipment
- Shortcuttings such as reduction in time consuming procedures
- Priorities of production over safety
- Attempts to increase efficiency.

The report literature, if correct would supply supporting evidence for each of these indicators, except the last. For example, the introduction of a jumper line would enable either the process vent header or the relief valve vent header to be used for venting and relief whilst the other was being maintained, without the need for plant shutdown.

It is also estimated that savings from switching off the refrigeration unit would be about $50 a day (World in Action, 1985).

If economic pressures existed at the time that it was decided to have MIC storage, then such pressures may have influenced this decision. Storage has the following advantages:

- Reductions in downtime
- Fluctuations in the process can be evened out
- Ease of operability

7. CONCLUSIONS AND RECOMMENDATIONS

If the report literautre and the analysis summarised here are correct the major lessons from the Bhopal disaster are as follows:

1. Human beings can overcome designs for safety. Redundancy and diversity of safety equipment may protect against equipment failure, but can be prey to a common mode failure, human error. It is therefore important that human error is accounted for in any evaluation of risk if a complete risk picture is to be obtained.

2. Safety is not only dependent upon preventative procedures. It also requires the ability of operators and management to recover errors and equipment failure. When errors or failures are unanticipated, system knowledge and awareness of risks are important in the diagnosis and identification of the correct form of action. Required operator and management knowledge and skills should therefore be identified for high risk plants to ensure that planned safety functions are maintained.

3. The safety of high risk plants should not be allowed to conflict with economic pressures. This should apply from operator to government level.

4. Poorly defined safety roles can lead to violations of safety functions. Responsibilities for safety, and duties related to ensuring safety, should be unequivocally established for plant, company, foreign parent company (if applicable) and government personnel.

8. ACKNOWLEDGEMENTS

The other members of the project team were David Slater, Frank Mitchell, John Fitt and Dilip Chowdhury. I am grateful to them for allowing me to present some of their work, and also to Dr B Ale and the Dutch Government who sponsored this study.

REFERENCES

Badhwar, I., and Trehan, M. (1984) Bhopal: city of death. India Today, 31 Dec. 1984, p.4-25.

Bhushan, B., and Subramaniam, A. (1985) Bhopal: what really happened? Business India, 25 Feb. - 10 Mar. 1985, pp. 102-116.

Bowonder, B., (1985) The Bhopal incident: implications for developing countries. Draft of paper to be published in Environmentalist. 46 pp.

Chemical and Engineering News (1985) Bhopal disaster: Union Carbide explains gas leak. Chemical and Engineering News, 25 Mar., pp. 4-5.

Delhi Science Forum (1985) Bhopal Gas Tragedy. New Delhi: Society for Delhi Science Forum. 47 pp.

European Chemical News (1984) Special Report: Bhopal: key questions raised by the tragedy. European Chemical News, 17 Dec., pp. 28-29.

European Chemical News (1985) Special Report: Firms keep their nerve in Bhopal aftermath. European Chemical News, March 4, pp. 12-13.

FASLI (1984) Bhopal tragedy. Bombay: Directorate-General, Factory Advice Service and Labour Institutes. FASLI News, vol. 1, no.2, Dec. 1984, pp. 2-9.

ICFTU and ICEF (1985) The Trade Union Report on Bhopal. Geneva: International Confederation of Free Trade Unions and International Federation of Chemical, Energy and General Workers' Unions.

Lepkowski, W., (1985) Indians criticise handling of Bhopal tragedy. Chemical and Engineering News, 28 Jan., p.24.

Slater, D.H. (1986) Risk Assessment in Practice - Bhopal. Chemical Engineering in Australia, ChE11(1), 12-16.

Time Magazine (1984) All the world gasped: a tragic gas leak offers a parable of industrial life. Time, 17 Dec. 1984, pp.6-23.

Times of India (1985) Carbide Ignored Safety Rules, 9 April 1985.

Union Carbide (1985) Bhopal Methyl Isocyanate Incident Investigation Team Report. Danbury, Connecticut: Union Carbide Corporation, 20 Mar. 1985. 24 pp.

Union Research Group (1985) The Role of Management Practices in the Bhopal Gas Leak Disaster (A second report by the Union Research Group - June 1985). India, 1985.

World in Action (1985) The Betrayal of Bhopal, Granada Television, 3 June.

TABLE 1 POSSIBLE HUMAN ERRORS AND RELATED FAILURES THAT COULD HAVE CONTRIBUTED TO THE BHOPAL DISASTER

DESIGN OR OPERATIONAL CHARACTERISTIC	POSSIBLE HUMAN ERRORS	POSSIBLE ASSOCIATED FAILURES	RELATED COMMENTS FROM SOURCES
1. MIC in storage tanks.	- Decision error: Decision to have storage of large quantities of MIC without adequate safety provisions. - Error recovery failure: Fail to heed warnings.	- Potential for massive release of MIC from storage	Bhushan and Subramaniam (1985) state that Edward Munoz, former managing director of UCIL maintained that "only token storage was necessary, preferably in small quantities based on both economic and and safety considerations." (p.109) ICFTU and ICEF (1985) claim that this recommendation on behalf of UCIL "was overruled by the parent corporation, which insisted on a design similar to UCC's Institute, West Virginia plant .... in fact, Union Carbide could have produced Sevin in Bhopal without any MIC storage." (p.8)
	- Procedural error: MIC not removed from storage during washing activities.	- Simultaneous presence of large quantities of MIC and water	It would have been good engineering practice to remove MIC from storage during shutdown. (Internal engineering opinion).
2. Existence of jumper line	- Design error: Installation of jumper line. - Error recovery failure: Design not examined for possible consequences.	- Process and relief vent headers connected; potential route for water to enter storage tank established	Bhushan and Subramaniam (1985) state that "had it not been for the jumper line water could not have leaked in." (p.104) The Union Carbide (1985) report says that one of the provisions for the prevention of contamination is that: "Storage tanks and associated process lines are dedicated to MIC service and no other materials are permitted in this equipment." (p.6) There are no indications from any of the sources as to whether the jumper line installation was approved by UCC or whether it was solely a management decision at UCIL although Bhushan and Subramaniam (1985) say that "as this was a major design modification, UCIL had sought prior permission from the parent company - Union Carbide Corporation." (p.103)

Continued/

TABLE 1 Continued

DESIGN OR OPERATIONAL CHARACTERISTIC	POSSIBLE HUMAN ERRORS	POSSIBLE ASSOCIATED FAILURES	RELATED COMMENTS FROM SOURCES
3. Removal of refrigeration	- Decision error: Decision to remove refrigeration while MIC still being stored.	- MIC no longer cooled - Insufficient time available for operators to be able to handle the reaction.	The Union Carbide (1985) report states that in the event of contamination the refrigeration system would "maintain the stored material at low temperatures which retard reaction rates and allows time for reprocessing or destruction in the case of contamination." (p.9) They also say that, during reaction in tank 610: "The increase in temperature was not signalled by the tank high temperature alarm since it had not been reset to a temperature above the storage temperature." Many sources, including Union Carbide (1985), agree that the refrigeration system had either been switched off, or the Freon inventory removed (eg. Badhwar & Trehan, 1984; Delhi Science Forum, 1985; Bhushan & Subramaniam, 1985).
4. Insufficient isolation of areas being washed	Procedural errors: - Failure to use slip blinds - Failure to ensure status of relevant valves - Equipment associated with isolation not adequately maintained	- No slip blinding - Malfunctioning/ leaking/ incorrect status valves	Union Carbide (1985) reports that: "Procedures exist to positively isolate lines using slip blinds when any work is done on lines or equipment used for or in conjunction with hazardous material. In addition, safety procedures require that operations and/or maintenance supervision give written approval before activities can be initiated or equipment can be returned to service." The Union Research Group (1985) report documents the initial procedural steps that appear in the company's manual as: "(1) Isolate the equipment by closing the relevant valves. (2) Evacuate the equipment with steam eductors. (3) Put slip blinds and positively isolate. (4) Carry out washing, cleaning etc."

Continued/

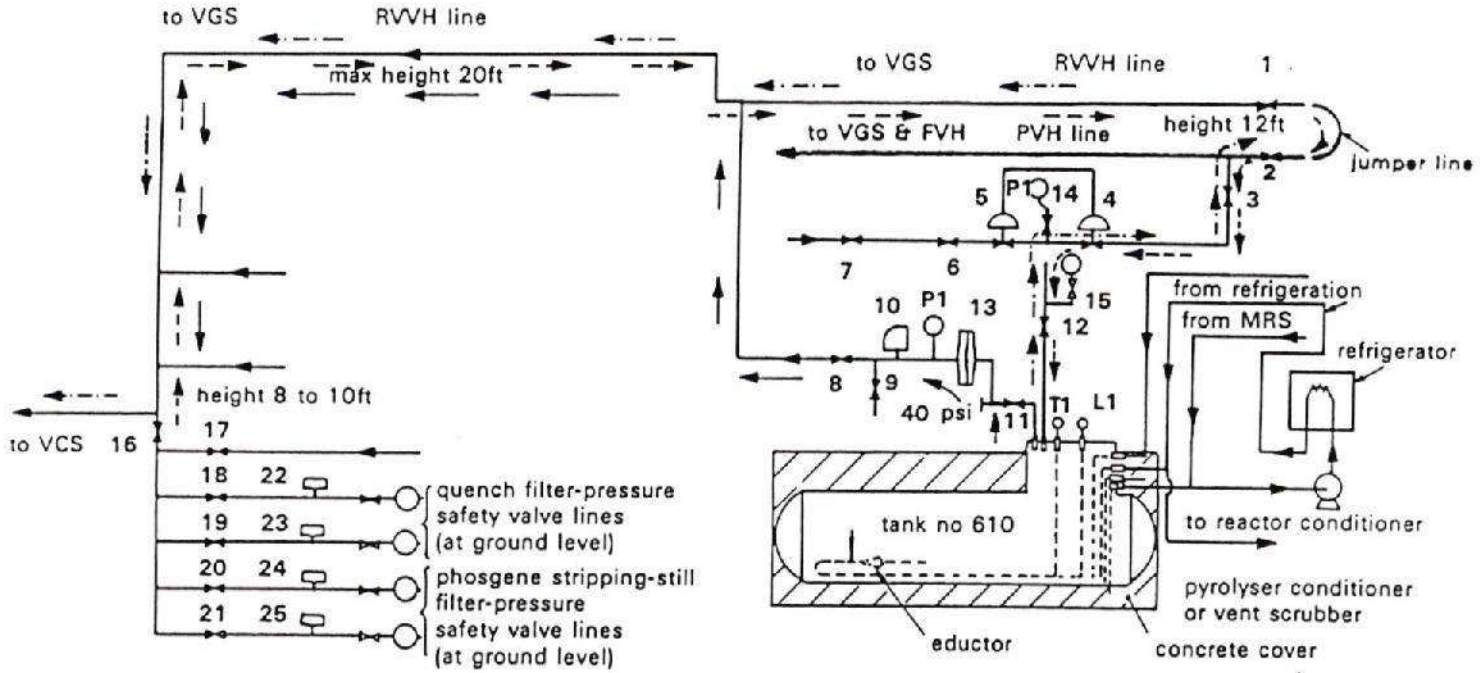
TABLE 1 Continued

DESIGN OR OPERATIONAL CHARACTERISTIC	POSSIBLE HUMAN ERRORS	POSSIBLE ASSOCIATED FAILURES	RELATED COMMENTS FROM SOURCES
			Many sources suggest that there was poor maintenance: "Many valves, vent lines, feed lines etc. are in poor condition: items which should have been replaced every six months have been over used for two years." (Delhi Science Forum 1985) The Union Research Group (1985) report supports the view that there was insufficient maintenance as part of what they call "The regime of short cuts." (p.2) On the use of slipblinds: "Sources believe the slip blind was not inserted when the operator connected the water hosepipes to the tubes he was required to wash." (Badhwar & Trehan 1984).
5. Design of system unable to contain reaction.	Design errors: - Failure to have redundant safety systems - Safety systems inadequate for large releases	- Safety systems out of action without back up. - Absence of a safety system able to contain large releases	The Union Carbide (1985) report mentions only the following for handling contamination: - A refrigeration system - A reject line so that contaminated material can be reprocessed or destroyed in the VGS - An emergency tank - Versatile arrangements of piping for material transfer - Safety relief system for relieving tank pressure above 40 psig to the RVVH No other systems available for this purpose are mentioned other than the human operator system. Several sources mention the VGS. For example: "....the unit had actually been shutdown for maintenance. As it happens, even when it is under maintenance the scrubber can be turned on, but its effectiveness is reduced. Under emergency conditions, the scrubber could have neutralized over four tonnes of liquid MIC in the first 30 minutes and then .... a little less than one tonne every subsequent half hour period." (Badhwar & Trehan (1984).

Continued/

TABLE 1 Continued

DESIGN OR OPERATIONAL CHARACTERISTIC	POSSIBLE HUMAN ERRORS	POSSIBLE ASSOCIATED FAILURES	RELATED COMMENTS FROM SOURCES
			Bhushan & Subramaniam (1985) suggest that: ".... MIC was perhaps coming into the scrubber at a rate more than two hundred times its rate capacity and at a temperature of nearly 400°C .... And the minimum pressure at which the MIC will escape the storage tank is at 165 times higher than the VGS's 15 psi capacity (the rupture disc gives way only at 40 psi)." (p.105) Union Carbide (1985) estimate that 90,000 lbs (23 tonnes) were released and Technica estimate 25 tonnes Regarding the flare, many sources say it was inoperational. For example: "The line connecting the VGS and the flare tower .... was also master-carded (blanked off) for repairs: this line has suffered extensive corrosion due to neglect." (Delhi Science Forum p. 23) Bhushan & Subramaniam (1985) claim that: ".... because of faulty design, both the VGS and flare tower together also could not have prevented the MIC from escaping into the atmosphere." (p.105) It is not clear whether operators could have contained the reaction by transferring material to other tanks. ICFTU and ICEF (1985) say that: "If either tank 611 and 619 had been empty, it could have been used as a surge tank to contain some of the reacting MIC .... thus giving operators more time to regain control of the reaction. In fact, operators were not even sure how much MIC was in in tanks 611 and 619 .... As a result workers were afraid to open the line to tanks 611 and 619." (p.8) Badhwar & Trehan (1985) claim that: "In the confusion, the valves weren't opened." (p.9)



Key:

1. Interconnection RVVH isolation valve
2. Interconnection PVH isolation valve
3. PVH isolation valve
4. Blow down DMV
5. Make up DMV
6. Check valve for nitrogen line
7. Nitrogen header isolation valve
8. RVVH isolation valve
9. RVVH bleeder valve
10. relief valve for MIC tank
11. First RVVH isolation valve MIC tank
12. First PVH isolation valve for MIC tank
13. Rupture disc
14. PIC isolation valve
15. PI isolation valve
16. RVVH isolation valve
17. Valve from which water for flushing was let in
18, 19, 20, 21. Isolation valves
22, 23, 24, 25. Bleeder valves

MRS – MIC reactor side
RVVH – relief valve vent header
PVH – process valve vent header
VGS – vent gas scrubber
FVH – flare vent header

---→ route of water ingress
-·-→ route of gas leakage before 0030 hours
——→ route of gas leakage after 0030 hours

PROBABLE ROUTE OF INGRESS OF WATER INTO TANK 610 (AFTER BHUSHAN & SUBRAMANIAM, 1985) FIGURE 1

AVRIM2, A DUTCH MAJOR HAZARD ASSESSMENT AND INSPECTION TOOL

Linda J. Bellamy, SAVE Consulting Scientists for Industrial Safety, P.O. box 10466, 7301 GL Apeldoorn, The Netherlands

Williët G.J. Brouwer[1],[2], Ministry of Social Affairs and Employment (SZW), ARBO/AIS, P.O. box 90801, 2509 LV 's Gravenhage, The Netherlands

Abstract

The development of and experiences with AVRIM2, major hazard assessment and inspection tool, are described. AVRIM2 is a modular inspection and assesment tool. It is composed of a number of building blocks that home in on the technical aspects of the installation and on the quality of the management system. Together these make a complete assessment of the quality of the major hazard control system of the company possible.

The components of AVRIM2 are: an Initiating Event Matrix, Generic Fault Trees for direct causes of failure, a benchmark Risk Matrix, a Management Control and Monitoring Loop and an Organisational Typing Tool.

The central concept of AVRIM2 is Lines of Defence: the safety controls which a company has in place to prevent Loss Of Containment of hazardous materials, and the systems by which a company monitors and improves the effectiveness of those controls.

Keywords: Loss of containment, Inspection tool, Risk, Major Hazard Control

1. Introduction

This paper describes the development of and experiences with a major hazard assessment and inspection tool, AVRIM2 [1]. This tool is currently in use by the dutch Labour Inspectorate for the assessment of Arbeidsveiligheidsrapporten, or AVR's, which are the safety reports addressing the internal (with respect to the workforce) safety of major hazard installations.[3] These reports are obligatory for major hazard installations in the Netherlands. The company has to describe in the AVR the hazards, operations, and the technical and organisational/managerial systems it has in place to prevent major accidents [2]. The task of the Labour Inspector is then to assess the completeness and accuracy of the report and to assess and inspect the safety of the installations. For the safety assessment and inspection tasks the Inspector uses AVRIM2. AVRIM2 is a Dutch acronym with means Occupational Safety Report (Assessment and) Inspection Method version 2. It is the succesor of an earlier inspection tool, AVRIM [3].

---

1 Corresponding author, Tel: +31 70 333 5431, Fax: +31 70 333 4026, e-mail W.G.L.BROUWER@MINSZW.NL

2 This article is a personal contribution and does not necessarily reflect the opinion of the Ministry

3 'Arbeidsveiligheidsrapport' translates into english as 'Occupational Safety Report', but the term 'occupational' is misleading because the focus is on major hazard loss of containment accidents. The term 'internal' is more accurate. In the current regime in The Netherlands, companies also have to produce an Extern VeiligheidsRapport, or EVR, which addresses external safety.

Once Seveso II is implemented in Dutch law, AVRIM2 will be used to assess Safety Reports which will combine the internal and external safety reporting for a site, as well as for the inspection of Seveso II sites, both low tier and top tier sites.

In this paper, the background and aims of the tool are described. A description of the central concept of AVRIM2 and an overview of the tool is given. The components of AVRIM2 are presented next. Finally, the practical experiences with the tool and remaining work to be done are discussed.

2. Background and aims

2.1 Aims

The development of AVRIM2 started in July 1995 with a research project which resulted in the basic AVRIM2 concept: the *"Lines of Defence"* approach. During the course of the project a number of aspects were taken into account and were incorporated into AVRIM2 as follows:

1. Seveso II The EU Directive Seveso II was coming into force, requiring companies to produce a newly defined site safety report. AVRIM2 was developed to be workable within the current AVR framework and in the new Seveso II approach as far as possible.

2. Burden of proof The earlier approach placed too much burden on the inspectors. For this reason, AVRIM2 puts much more emphasis on companies to provide a demonstration of their level of safety, but providing inspectors with tools to check this, including sets of evaluation criteria.

3. Risk-based AVRIM2 is focused on prevention of loss of containment accidents for major hazard installations. At the start of the project the then current concept of a criterion of zero accidents was discussed in relation to what is "safe". This criterion is replaced with an approach developed for AVRIM2 that is risk-based. Such an approach requires risk based criteria (for likelihood and consequences of the occurrence of accident scenarios) with the burden on the companies to provide their own criteria and assessments. Benchmark criteria are provided for the inspectors.

4. Lines of Defence There needs to be a way of homing in on key safety weaknesses in the technical aspects of the design that can then lead to consideration of the relevant management aspects. The solving of this problem is the central focus of AVRIM2, namely the development of the concept of Lines of Defence. In requiring companies to go through a process of identifying their lines of defence against causes of loss of containment, and of demonstrating how they manage these defences, the idea is that inspectors can pick up on any weaknesses in these Lines Of Defence systems with the help of the tools in AVRIM2.

5. Management Control and Monitoring Loop The management system model of AVRIM2 is based on the control and monitoring loop concept of the PRIMA audit approach which was developed by Four Elements and investigated as part of the EC project Auditing and Safety Management for Safe Operation and Land Use Planning CEC Environment Project EV5V-CT92-0068 [4]. In AVRIM2 the PRIMA audit was redeveloped into four control and monitoring loops, one for each life cycle phase (Design, Construction, Operations, and Maintenance) [5-7]. Evaluation criteria are provided for each element of the loop. The loops were redefined for AVRIM2 and each link

and component has common themes running throughout which make it easier to select questions on specific topics of interest. The original PRIMA questions were simplified into a set of briefer points of attention.

A final requirement for AVRIM2 was that it should enable inspectors to use a more uniform approach to the assessment of the safety of major hazard installations

2.2. The Central Concept of Lines Of Defence

AVRIM2 applies to assessment and inspection of the safety controls which a company has in place to prevent *Loss Of Containment* of hazardous materials, and to the assessment and inspection of the systems by which a company monitors and improves the effectiveness of those controls. In AVRIM2 these safety controls are called *"Lines of Defence"*.

The emphasis is on:

- The *Risks of Failure of Lines of Defence* in the design and operation of the installation
- The *Safety Management System* which manages the *Lines of Defence*

Typically, in low risk operation of high hazard systems, systems are designed with a 'defence-in-depth' philosophy such that even when several technical faults or human errors occur, a release of the potential hazard can be prevented. The protection strategy is based on several last Lines of Defence such as:

1. Redundant and diversity of equipment is introduced such that if one fails, another can take over
2. If control of energy or mass accumulations fails in spite of 1., it can be detected by monitoring critical parameters such as increasing temperature or pressure and the process can be shut down by automatic emergency actions
3. If 2. also fails, energy or mass can be retained by containment, or..
4. Diverted by barriers etc.

Only a coincidence of errors and faults violating all LODs will release a full scale accident and, therefore, hazard control is is directed toward maintaining the barriers intact.

One such source of coincidence is poor management. The relationship between management, lines of defence and loss of containment is illustrated in figure 1.

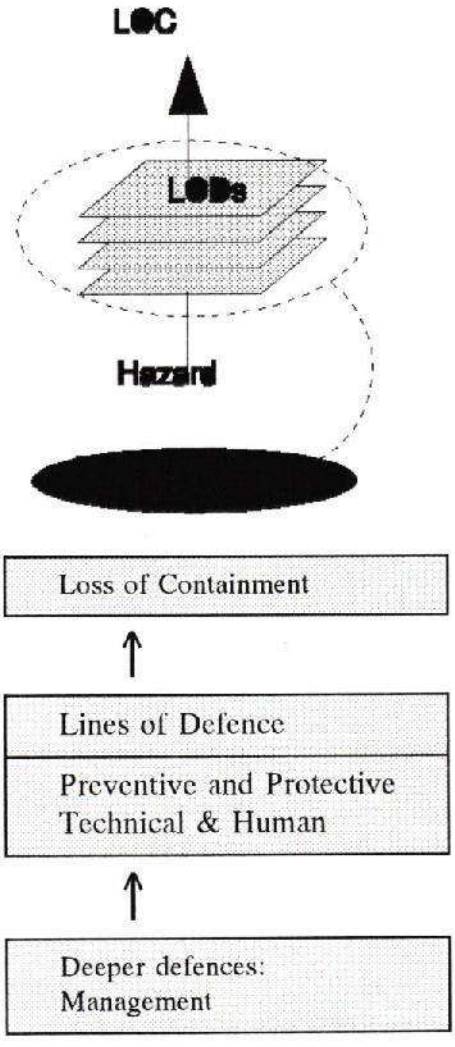


Figure 1 Lines Of Defence Concept

For some hazards the accident frequency is high enough to base the design of LODs on analysis of past accidents. However, where this is not the case, risks must be predicted using available techniques such as Quantitative Risk Assessment, for example. Safety management should then be focussed on controlling and monitoring the lines of defence, not on prescriptive rules of conduct based on controlling the causes of past accidents [8]. It is this latter approach to safety management that is used in AVRIM2.

The burden of proof in the AVRIM2 tool is on the company which must demonstrate it has identified all possible causes of loss of containment and has sufficient lines of defence in place to prevent and protect against these possible causes.

3. AVRIM2 Components

3.1. *Overview*

AVRIM2 is a modular inspection and assesment tool. It is composed of a number of building blocks that home in on the technical aspects of the installation. There are also building blocks that home in on the possible organisational strengths and weaknesses and the quality of the management system. Together these make a complete assessment of the quality of the major hazard control system of the company possible.

The tools developed for AVRIM2 for evaluating the technical aspects of the design are:

i An Initiating Event Matrix in order to support an overview of a company's coverage of possible activities and equipment from which Loss Of Containment could arise and possible direct causes of failure.

ii Generic Fault Trees for direct causes of failure giving a very general level of global coverage to all possible failure pathways (scenarios), for which lines of defence were needed.

iii A benchmark Risk Matrix.

Tools for reviewing the organisation's ability of maintaining the Lines of Defence are:

iv A Management Control and Monitoring Loop addressing each life cycle phase and which has attention points for assessing the completeness and quality of the management's control and monitoring of lines of defence systems;

V An Organisational Typing Tool which can be used to home in systematically on potential organisational weaknesses in the evaluation of the management system.

All the components are described in the next paragraphs.

3.2. *The Initiating Event Matrix*

The Initiating Event Matrix of AVRIM2 (Figure 2) identifies, in a generic way, every single possible initiating event on an installation. An initiating event leads immediately to a loss of containment. An initiating event is a combination of a direct cause and a piece of containment equipment.

In AVRIM2, *Direct Causes* of Loss Of Containment (LOC) have been defined. The set of causes covers *all possibilities of failure* of containment and are mutually exclusive. Definitions and statistics on these Direct Causes were derived from earlier studies.

In AVRIM2, the combination of a direct cause and a containment or activity is called an *Initiating Event*. For example: Corrosion of pipe; erosion of loading arm; external loading on pipe; impact on railcar; overpressure of vessel; vibration of hose; thermal stress on vessel, frozen valve; wrong valve installed/wrongly located; operator error with pump.

The only containments of interest are those where major hazard substances are involved (according to the Seveso II classification). For each installation, *all the possible types of containment* combined with *all the possible types of direct causes of a release* determine the set of potential Initiating Events for that installation. When filled in with major hazard events which a company itself has identified, the Initiating Event Matrix provides an overview of the safety window through which the company looks at major hazards.

Figure 2 Initiating Event Matrix.

3.3. Generic Fault Trees, Scenarios and Lines Of Defence

Based on the possible causes of loss of containment of the initiating event matrix, Generic Fault Trees were developed for every direct cause: Corrosion, Erosion, External Loading, Impact, Operator Error (containment bypass), Overpressure, Temperature, Underpressure, Vibration, Wrong equipment/Location. In addition there was a Generic Fault Tree for Exceeds Containment Limit, because it recurred in most of the other trees. Figure 3 shows an example of a generic fault tree, the one for the direct cause Operator Error (containment bypass, no structural failure). Branch a is developed further in a separate tree (not shown).

Figure 3 Operator error fault tree

A fault tree is a graphical representation of the logical relations between an undesired event (the top event), in this case a Loss of Containment, and its primary cause events. The top event is broken down into all the possible logical causes until further breakdown is considered unnecessary. The rationale for the Generic Fault Trees in AVRIM2 was that the graphical representation, and relative

simplicity in the generic descriptions, would provide the inspector with a broad overview and starting point for considering whether a company had considered all the possible routes to failure for containments with hazardous materials. In the development of the AVRIM2 trees, a team from the Ministry of Social Affairs (SZW) with expertise in major hazards were coordinated by a student from TU Delft, whose resulting thesis became the basis for the 11 Generic Fault Trees [9].

Within the generic fault trees, scenarios can be identified. In AVRIM2 a scenario is a unique combination of generic failure events from the base of a tree (events which are not further broken down) which are necessary and sufficient to lead to Loss of Containment. In some cases, only one base event event is required. In other cases combinations of events must occur before there is a LOC. Every direct cause Generic Fault Tree will have several scenarios, because there a several pathways within the fault tree that could lead to a loss of containment. The Operator Error tree, which is tree number 6, contains 15 scenarios. Each scenario is identified by a number, 6.1, 6.2, 6.3.....6.15.

Every scenario in the Generic Fault Trees is described [1]. For example:

Scenario 6.3: During sampling or draining from the containment the operator fails to stop the flow correctly, for instance by not operating the device in time. This can be the case when a liquid is drained from a containment and the valve is not closed in time and the outflowing product makes it impossible to close the valve in a later stage.

Or, taking an example from the Overpressure tree:

Scenario 7.8 The excessive overpressure is caused by high pressure from liquid material, for instance roll-over causes the high pressure AND the overpressure exceeds the containment limit. For a roll-over to occur there has to be stratification potential in the liquid phase of the product in the containment AND there is no mixing in the containment AND there is a difference in temperature between the layers *which can for instance be caused during filling of the containment* AND the pressure relief system fails to prevent the overpressure.

In total there are 125 scenarios in the Generic Fault Trees.

The scenarios form a basis for identifying where a company should have Lines of Defence in place. The Generic Fault Trees are intended to trigger the investigation as to what installation specific scenarios are possible, whether these scenarios have been identified, and whether there are preventive and protective Lines of Defence systems in place which minimise the likelihood of occurrence of a failure.

The approach taken in AVRIM2 starts with the risk model through identification of scenarios to loss of containment and identifying company specific Lines of Defence Systems. This order is a safeguard that all possible scenarios have been identified. This is also the order in which the AVRIM2

research project has evolved.

An approach which works the other way around is possible too: starting with the management system and generic Lines of Defence Systems, asking the company to identify possible scenarios on site. These generic LOD's can be derived from expert judgement. This second approach makes it difficult to be comprehensive in identifying the scenarios. On the other hand it makes it easier to identify weak spots in management systems in a more generic way. At the moment these generic LOD's, called scenario management links, are been added to the AVRIM2 software.

Lines of Defence come "below" the base failure events in the fault trees, as systems which are intended to prevent a failure occurring. For example, scenario 5.3 (from LOC by Impact) includes base events:

(a) Collision with transport vehicles.

AND

(b) Exceeds containment Limit.

The Lines of Defence which should be in place are those which are intended to prevent: (a) Collision with transport vehicles, and (b), should collision occur, prevent that the impact causes a Loss of Containment. For (a), Lines of Defence might relate to traffic control systems (speed limits), height bars, crash barriers, and the layout distance between roads or the height of a vehicle and equipment carrying hazardous materials. For (b) it might be that it was not possible to design the containment such that it withstands the impact of a moving vehicle (no LOD).

In such a case, the LODs for (a) are even more important.

A Lines of Defence system should have all the relevent preventive and protective components of a defence in depth system:

- physical containment
- automatic shutdown/shut-off for deviations
- physical barriers for diverting mass/energy so containment limits not exceeded
- systems of work, including response procedures should a deviation occur
- protection of personnel against exposure
- emergency preparedness should hazard control fail

The order of priority for Lines of Defence Systems are as follows:

a. Remove hazard altogether (highest preference)
b. Reduce hazard to low level
c. Contain/control hazard by physical means
d. Contain/control by systems of work
e. Protect personnel against exposure:

1. Personnel not present within the effect distance
2. Measures which protect a group
3. Measures which protect an individual

f. Emergency preparedness should hazard control fail

The inspector is required to carry out a completeness check of the information provided by the company. It should be checked that:

- All relevant scenarios have been identified and their lines of defence specified.
- The lines of defence systems prevent and protect against all the failure events in the scenario.
- A line of defence system has all the relevent preventive and protective components of a defence in depth system
- Missing lines of defence have been identified by the company.
- Any inconsistencies across defence systems have been identified by the company.
- There is a plan for dealing with identified weaknesses.

3.4. Risk matrix

The next stage is for the company to evaluate the risk of occurrence of the scenarios. Risk assessment is already a requirement for the External Safety Report (EVR) but this only looks at scenarios with offsite consequences. Generic historical failure data are used to identify the likelihood of releases, and attention directed toward mitigation of consequences.

Since the EVR and AVR are going to be merged into one safety report it makes sense to concentrate in AVRIM2 on those aspects of risk which are not dealt with in the EVR but which are relevant to internal safety. The AVR-EVR balance is primarily one of Prevention-Mitigation.

The aim of getting companies to evaluate the risks of occurrence of scenarios is to get them to focus on chances of failure of Lines Of Defence systems and possible on-site consequences should they fail. This will provide the information which enables the inspector to carry out a quality check on the lines of defence. For this purpose, benchmark risk criteria were devloped to enable comparison with companies own criteria.

The intention is that companies should specify their own criteria for evaluating whether the possible failure scenarios are adequately defended against in terms of reliability of lines of defence. The reliability of the system should be commensurate with the severity of the consequences should the system fail. This approach replaces the previously held view relating to internal safety that "Safe" means zero loss of containment. Such a view is unrealistic since there is always a finite probability that the hazard will be realised. The previous approach also required that companies demonstrate that accidents can never happen, when in fact the best they can do is demonstrate an acceptably low level of chance of failure.

Risk is a function of both the *likelihood* and the *consequences* of failure. In AVRIM2 the consequences of interest are impact on personnel on the site.

Risk = Likelihood of failure of a lines of defence system (against a particular scenario) X Consequences of failure

There is a difference between a risk management system which prescribes rules of conduct based on controlling the causes of past accidents, and a risk management system which controls and monitors its lines of defence. The first type of management only works if the accident frequency is high enough to provide enough data for analysis and rule prescription. The second type depends upon knowing the effectiveness of the lines of defence systems and taking action when the risk of failure is unacceptable. It is this latter type of system which AVRIM2 is based on.

Wherever there is a line of defence it can fail. Companies cannot say, for example, that because there is a pressure relief valve a vessel cannot be overpressured. The pressure relief valve can fail. It can be subject to pressures beyond the design specification. A piece of equipment with the wrong pressure rating might have been installed.

So, whatever the line of defence, there is always a chance, however small, that it will fail.

For this reason, the reliability of the line of defence system against each possible scenario should be considered by the company and the consequences of failure identified.

A semi-quantitative approach is recommended where the calculation of likelihoods and consequences can be fitted ito a number of categories. The company should provide an evaluation of the likelihood and consequences of each installation specific scenario or group of scenarios associated with a Loss of containment. They should assess these scenario risks against criteria. The criteria should be developed by the company and show what is and is not an acceptable risk.

Because the measure of risk is a combination of the likelihood of a loss of containment event and its consequences, assessment criteria have to address both. The criteria are that the risks of loss of containment of hazardous substances should be acceptably low. If a hazard is present, the only way to achieve zero risk is to remove it.

AVRIM2 provides a set of risk criteria which can be used as guidance to compare against a company's own criteria. These are shown in Figure 4. The principle used is that the more severe the consequences, the lower the acceptable level of likelihood of failure of the line of defence system. Any possible failure scenario would have a position in the matrix, showing its relationship with respect to the criteria. The action requirements, depending on the position of a scenario, are shown in the key to the figure.

The values shown in Figure 4 are benchmarked in Figure 5. These benchmark data have been amalgamated from two major company sources. Since consequence severity depends on a number of

parameters, the benchmark includes more than simply impact on personnel. Estimates of consequence severity made by a company should therefore also consider these other factors.

Likelihood of loss of containment	Consequence severity				
	5 Severe	4 Major	3 Serious	2 Minor	1 Negligible
5 Very High	X	X	X	X	O
4 High	X	X	X	O	O
3 Average	X	X	O	O	=
2 Low	X	O	O	=	=
1 Very Low	O	O	=	=	=

KEY	
X	Unacceptably high risk. Company should reduce by prevention/protection.
O	High risk. Company should address cost-benefits of further risk reduction. Inspector should verify that procedures and controls in place.
=	Acceptable. No action required

Figure 4 Risk Matrix

	Likelihood scale:		Consequence scale:[4]
1	Very low Failure never heard of in the industry. Almost impossible on the installation. $< 10^{-4}$ per year.	1	Negligible Minor impact on personnel, no loss of production time, < f. 10.000 cost
2	Low Failure heard of in the industry. Remote, but possible on the installation $< 10^{-3}$ per year	2	Minor Medical treatment for personnel, minor damage, short loss of production time, < f. 100.000 cost
3	Average Failure has occurred in the company as a whole. Occasional, could occur some time on the installation. $< 10^{-2}$ per year	3	Serious Serious injury to personnel (LTI), limited damage, partial shutdown, < f. 500,000 cost
4	High Failure happens several times a year in the whole company. Possibility of isolated incidents on the installation. $< 10^{-1}$ per year	4	Major Permanent injury/health effect, major damage, production stop, < f. 1.000.000 cost
5	Very high Failure happens several times a year at the installation Could be repeated incidents on installation. $> 10^{-1}$ per year	5	Severe One or more fatalities, large scale damage, long term production stop, > f. 1.000.000 cost

Figure 5 Example of Likelihood - Consequence Scale

[4] Costs are in dutch guilders (f.)

3.5. Organisational factors

A tool has been developed to enable the organisational profile of a company to be specified. From this profile a prediction of the possible strengths and weaknesses of the risk management of a particular company and installation can be generated. This tool, called the Organisational Typing Tool, has been incorporated into AVRIM2 in the form of a computer program.

The development of this tool has been well documented [10]. It originated from a structured investigation of inspectors' knowledge and perceptions of companies in the Netherlands which have to provide an AVR. The investigation provided correlations between factors in an organisation's profile and possible strengths and weaknesses with respect to safety.

Use of the Organisational Typing Tool can be made prior to investigation of the management system. From a specification of the profile of the organisation, the computer program makes a calculation which provides the inspector with suggestions of areas of strength and weakness likely to be found in each component and link of the control and monitoring loop.

3.6. The Management Control and Monitoring Loop

Much of the analysis surrounding the previous sections can point the way to the relevant components in the management system which should be examined in the assessment. The Control and Monitoring Loop described here provides inspectors with support for evaluating an installation's management system.

In the context of AVRIM2, *the management system has a common mode effect on the lines of defence against failure*. Therefore, the effects of management could be to increase the likelihood of scenarios, and so generate an unacceptable risk.

- *Absence* of a proper management system would result in *increased risks* of loss of containment across *all* lines of defence systems.
- A *weak* management system would result in *increased risks* of loss of containment for the lines of defence in those *areas of weakness*.

The model underlying this principle is the Control and Monitoring Loop (see Figure 6).

Figure 6 Control and Monitoring Loop

The aim of the Control and Monitoring Loop is to provide inspectors with support for assessing whether all the safety components of a management system are present and functioning adequately.

The management system is shown represented as the *middle block of components* in Figure 6 of the Control and Monitoring Loop. Its relationship with lines of defence is as follows:

- the left hand CONTROL side of the loop: the control of human decisions and actions which have an effect on these defences, and

- the right hand MONITORING side of the loop: the monitoring and correcting of deviations from required standards in the control of lines of defence, and the improvement of those standards.

Analysis of loss of containment accidents shows that management could have prevented or corrected deviations which originated in:

- Design
- Construction
- Operation
- Maintenance

These management prevention or recovery measures can be grouped into four key areas:

- Hazard review
- Checking and supervision of tasks
- Routine inspection and testing
- Human Factors review

The combination of these measures with the life cycle phases above gives the following areas for consideration, shown in Figure 7. These areas cover the whole of the management system in terms of possible sources of failure leading to loss of containment.

	HAZARD REVIEW	CHECKING AND SUPERVISION	ROUTINE INSPECTION AND TESTING	HUMAN FACTORS REVIEW
DESIGN	Design and mods standards, codes, hazard analysis/safety studies and follow-up			
CONSTRUCTION		Checking and supervision that construction of LODs is to spec.		
MAINTENANCE	Evaluation of maintenance errors in the hazard analysis/safety study	The supervision of maintenance tasks and checking of completed activities to ensure safe/correct for relevant LOD related tasks	Routine testing and inspection of LOD equipment to determine if OK, and maintenance follow-up as required	Identification that possibilities for maintenance error are minimised in maintaining LODs through appropriate ergonomics, task design and training
OPERATION	Evaluation of operational errors in the hazard analysis/safety study	Supervision and checking of operational tasks for relevant LODs		Identification that possibilities for operational error are minimised in maintaining LODs through appropriate ergonomics, task design and training

Figure 7: Areas Of Importance In Management Of Major Hazards
Note: LOD= Lines of Defence)

In AVRIM2 the eight areas are, for simplicity of application, combined into four key loops of Design, Construction, Operation and Maintenance. Each component and link of the loop shown in Figure 6 can be explained as follows:

1. **System Climate**: A company should be aware of the climate which it operates in. This includes the climate of regulation, economic pressures, know-how, availability of resources, and special requirements dependent upon the type of business it is involved in. The safety management system should be tailor made for the specific technical safety aspects of the installation and process.

2. **Adaptation to System Climate**: A company needs access to information and resources from the system climate they operate in. They need to adapt to changing requirements, knowledge and experience, and economic pressures.

3. **Organisation, knowledge, standards, plans, policies**: The company must establish a management organisation which will determine and implement safety policy. It must have knowledge about safety which enables it to set safety standards against which the safety of its operations will be measured and adjusted. There is a commitment to implementing the policies and plans, with designated personnel with specific roles for implementing and coordinating policy and plans.

4. **Formalisation processes**: The processes by which policies, standards and plans are formalised will determine what gets written down and how that information is organised. It is necessary that the formalisation process captures what is necessary in the Safety Management System, and organises that information such that it is accessible and understandable.

5. **Formalised (written) Systems of Control and Monitoring**: These are all the documented systems which play a part in the control and monitoring of people and equipment. They include policies, plans, procedures, minutes of safety meetings, drawings, work orders, material safety data, safety reviews, checklists, safety manual, job descriptions, and so on. The documentation system should capture the knowledge of the company about how to do things safely, demonstrate that it has been subject to safety review and been accepted by the responsible persons. It must be available and understandable to those who use it.

6. **Implementation of Control System**: It is not enough to simply capture the Safety Management System on paper. Policy and procedures must be implemented through the management structure down to the front line through communication and instruction and provision of resources (people, equipment, tools, controls and displays). For example, identification of safety critical tasks will have indicated priorities for supervision or special safety checks, and it is up to management to ensure that such supervision is provided and carried out.

7. **Human Reliability**: This is the function which ultimately affects the reliability of containment through the way it is designed, constructed, maintained and operated.

Human reliability will be dependent upon the support which is provided in terms of information, training, man-machine interface, task design and workload, working environment. It will also be dependent upon the effectiveness with which safety is controlled through implementation of standards and procedures

8. **Outputs of Human Reliability**: The decision making processes which determine actions, such as the resolution of conflicts between production pressures and safety, determine outcomes. How disciplined the company is in terms of the enforcement of rules, such as the carrying out of hazard reviews, safety checks, the wearing of personal protective equipment, following the correct procedure, ensuring proper and safe maintenance etc. will influence the effect of people on the safety of the plant. The occurrence of non-conformances, incidents and near misses will be an indicator of how well the system is performing.

9. **Containment Reliability**. Containment means the vessels, pipework, hoses and other plant components which contain the hazardous materials, and all the associated systems in the design of plant and chemical process which prevent and protect against exceeding containment limits. Human decisions and actions occurring at different points in the installation's life cycle will affect the integrity of the containment systems. Loss of containment could result in damage, injury or loss of life.

10, 11 **Feedback.**. The implementation of safety is monitored by measurement, observation, review, audits, safety review meetings, and front line personnel communicating problems to higher management. Ultimately safety monitoring information gets back to the highest level of management through regular safety performance reports.

12. **Formal Monitoring Systems**. The capturing of monitored safety information will be highly dependent upon the formal requirements for monitoring safety, and the existence of personnel with specialist safety monitoring roles, such as an internal audit team who are trained in auditing and the use of a formalised audit system. The formal monitoring systems will relate to the standards which have been set up and implemented on the control side of the loop. It will include capture of data on incidents and near misses.

13. **Analysis and Follow-Up**. Captured data about the performance of the safety management system will need to be analysed in order to provide meaningful information which can be learnt from. It is important to analyse not just the statistics of monitored events but also the underlying reasons as to why there was a deviation from safety performance standards, what controls had failed or were not in place.

14. **Revision System**. The analysis process allows control failures or lack of controls to be identified. It is then necessary to revise or reinforce the control process by which safety is implemented. In this way the whole system is self adjusting.

15. **Safety Improvement.** The follow up to identifying the need to revise the SMS has to be implemented in order for safety to at least be maintained at the specified standards,

or to be improved where those standards are already being met. When the loop is whole, continuous safety improvement will be achieved, and there will be evidence of this through the formalisation of safety improvement plans.

The aim is to establish whether there is a management system in place by examining whether the loop is complete, and if not, where the areas of weakness lie. The four loops provide sets of attention points which are effectively "Performance Indicators" of a safety system which is preventing the incubation of accidents. The use of the term "system" means that all the components of the organisation and management have a relationship with one another within a clearly defined structure.

4. Use of AVRIM2

AVRIM2 is to be used for:

- Examination of the information that Seveso II establishments must provide to the authorities, in particular the Safety Report and the Major Accident Prevention Policy ;
- Verification that the safety systems specified by the companies for Major Hazard sites are actually applied in relation to the design, construction, operations and maintenance;
- Subsequent periodic safety inspections of Major Hazard installations.

As a consequence of the use of AVRIM2 with regards to the assesment of the Safety Report, there will be a demand for extending the possible use of the tool to other fields of interest, like the environment and emergency response and planning. At the moment AVRIM2 only regards possible routes to loss of containment. It does not take account of consequences. In the future effect trees will be added. This could make an integration with the quantitative risk assessment approach taken by our Dutch environmental colleagues more feasible.

Further research in combining the safety management systems approach for internal safety with the quantitative risk assessment approach for external safety is ongoing with the EC project I-Risks, Development of an integrated technical and management risk control and monitoring methodology for managing and quantifying on-site and off-site risks (Contract ENVA-CT96-0243). The basic concepts of AVRIM2 have been integrated in this research project.

Once Seveso II is implemented in Dutch law the aim is to ask companies to use a more AVRIM2 like approach in the Safety Report. Many companies use scenarios and risk matrices, but untill now it was not asked of them to give this information to the authorities. Under the new legislation they will be encouraged to use this information in the dialogue with the authorities in which they nust demontrate their appoach. This will make the task of the inspectors more appropriate to the role envisaged for them in AVRIM2.

A company is expected to provide evidence that it has identified its lines of defence against failure, their chances of failure, the consequences of failure, and that the management system is complete in addressing all the Control and Monitoring Loop components. However, even with the burden placed on the companies to demonstrate safety, the assessment of completeness and adequacy of the risk control and management system is still an extensive task, and so focussing rules are needed. Focussing rules are needed for systematisation of approach in an area where

comprehensiveness is an impossibility. In theory, this could be achieved by technical and organisational typing whereby potential weaknesses of a particular technical or organisational system are predicted beforehand. As far as possible within the scope of the current AVRIM2 project, schemes for reducing the size of the inspectors' tasks have been developed but this is one very important area where further developments are needed and are in progress.

AVRIM2 is a tool which is one of the few true major hazard technical review and audit methods linking the technical and management systems. It is considered to adress all issues that are necessary for assessing the quality of the major hazard control systems of companies without being prescriptive.

Aknowledgements

AVRIM2 was developed with the assistance of colleagues from the Ministry of VROM, the Provincie Zeeland, DCMR, TU Delft and the Arbeidsinspectie. Their help is greatly appreciated.
Testing of the tool and discussions about changes are ongoing with the Process Safety Specialists of the Arbeidsinspectie. We value their contribution. Especially we would like to thank Ad van der Staak and Joy Oh from the Ministry of SZW.

References

[1] AVRIM2 Assesment and Inspection Methodiek Handboek, Version 1.0, Ministerie van Sociale Zaken en Werkgelegenheid, 1996

[2] P172-2E, Occupational Safety Report, Guideline for compilation, Publication of the Dutch Labour Inspectorate, 1990

[3] Oh, J.I.H., The AVRIM safety inspection method, Loss Prevention symposium, Antwerp, 1994

[4] Auditing and Safety Management for Safe Operation and Land Use Planning: A Cross National Comparison and Validation Exercise" CEC Environment Project EV5V-CT92-0068 1993-1994

[5] Bellamy, L.J., Geyer, T.A.W., Astley, J.A. "Evaluation of the human contribution to pipework and in-line equipment failure frequencies", Health and Safety Executive, Bootle: HSE, ISBN 0717603245. HSE Contract Research Report 15/1989, 1989

[6] Bellamy, L.J. and Geyer, T.A.W. "Organisational, Management and Human Factors in Quantified Risk Assessment - Report 1" - HSE Contract Research Report 33/92, HMSO, 1992

[7] Wright, M. and Tinline, G. "Further Development of an Audit Technique for the Evaluation and Management of Risks." London: Four Elements, Report C2278, 1993

[8] Rasmussen, J. "Risk management, adaptation and design for safety" in Sahlin, N.E. and Brehmer, B. (Eds) Future Risks and Risk Management. Dordrecht: Kluwer, 1994

[9] Van der Mark, R. "Generic Fault Trees and the Modelling of Management and Organisation". Delft University of Technology (Technische Universiteit Delft),Department of Statistics, Probability and Operations Research, Faculty of Technical Mathematics and Computer Science/ Department of Safety Science, Faculty of Technology and Society, August 25, 1996

[10] Bellamy, L.J., Leathley, and Gibson Organisational Factors and Safety In the Process Industry. Den Haag, Ministerie van Sociale Zaken en Werkgelegenheid, 1995