ELSEVIER

Journal of Hazardous Materials 65 (1999) 191–210

Journal of Hazardous Materials

AVRIM2, a Dutch major hazard assessment and inspection tool [1]

Linda J. Bellamy [a], Williët G.J. Brouwer [b,*]

[a] *SAVE Consulting Scientists for Industrial Safety, P.O. Box 10466, 7301 GL Apeldoorn, Netherlands*
[b] *Ministry of Social Affairs and Employment (SZW), ARBO / AIS, P.O. Box 90801, 2509 LV's Gravenhage, Netherlands*

Abstract

The development of and experiences with AVRIM2, a major hazard assessment and inspection tool, are described. AVRIM2 is a modular inspection and assessment 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 AVRs, which are the safety reports addressing the internal (with respect to the workforce) safety of

* Corresponding author. Tel.: +31-70-333-5431; fax: +31-70-333-4026; e-mail: w.g.l.brouwer@minszw.nl

[1] This article is a personal contribution and does not necessarily reflect the opinion of the Ministry.

0304-3894/99/$ - see front matter
PII: S0304-3894(98)00263-5

major hazard installations. [2] 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 which means Occupational Safety Report (Assessment and) Inspection Method version 2. It is the successor of an earlier inspection tool, AVRIM [3].

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

[2] '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.

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—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 replaced by 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; and

-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 [8]. 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 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 Fig. 1.

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 focused 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.

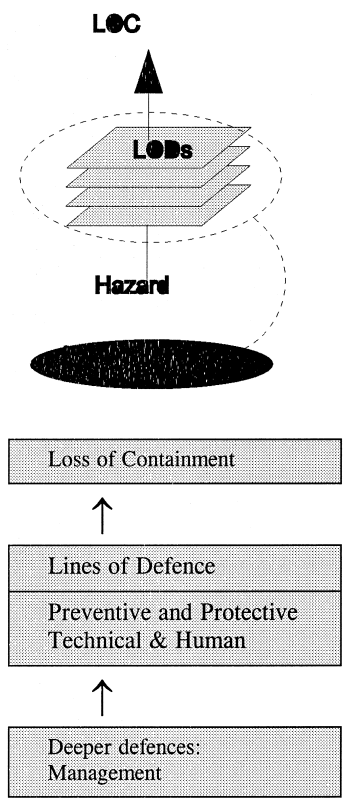

Fig. 1. The Lines of Defence Concept.

3. AVRIM2 components

3.1. Overview

AVRIM2 is a modular inspection and assessment 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; and

(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; and

(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 (Fig. 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, and 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.

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, and Wrong Equipment/Location. In addition, there was a Generic Fault Tree for Exceeds Containment Limit, because it recurred in most of the other trees. Fig. 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).

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

INITIATING EVENT MATRIX		DIRECT CAUSES OF LOC								
Activities	CONTAINMENT (Release Points)	Corrosion	Erosion	External Loading	Impact	Pressure (High/Low)	Vibration	Temperature (High/Low)	Wrong Equipment/location	Operator Error (contain-ment bypass)
Storage										
	Atmospheric tanks									
	Pressurised vessels									
Transfer										
	Pumps									
	Compressors									
	Pipework									
	Ductwork									
Sampling										
	Sampling points									
	Sample container									
Processing										
	Pumps									
	Compressors									
	Heat Exchangers									
	Pipework									
	Pressure Vessels									
	Atmospheric Tanks									

Fig. 2. Initiating Event Matrix.

	Ship									
	Barge									
	Atmospheric Tanks on									
	Rail car									
	Road Tanker									
	Ship									
	Barge									
	Loading arms									
	Hoses									
	Pipework									
	Pumps									
	Compressors									
Designed Release Points										
	Relief valves									
	Explosion Panels									
	Drain points									
	Bursting discs									
	Vents									
Special Cases										
	Domino (other sites)									
	Aircraft impact									
	Terrorism/vandalism									
General										
	Flanges									
	Instruments									
	Valve									
	Gaskets									
	Bellows									
	Expansion Joints									
	Coolant Systems									
	Heating Systems									
	Inert Systems									
	Air Systems									
	Water Systems									

Fig. 2 (continued).

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 as 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 is required. In other cases, combinations of events must occur before there is a loss of containment.

Every direct cause Generic Fault Tree will have several scenarios, because there are several pathways within the fault tree that could lead to a loss of containment. The

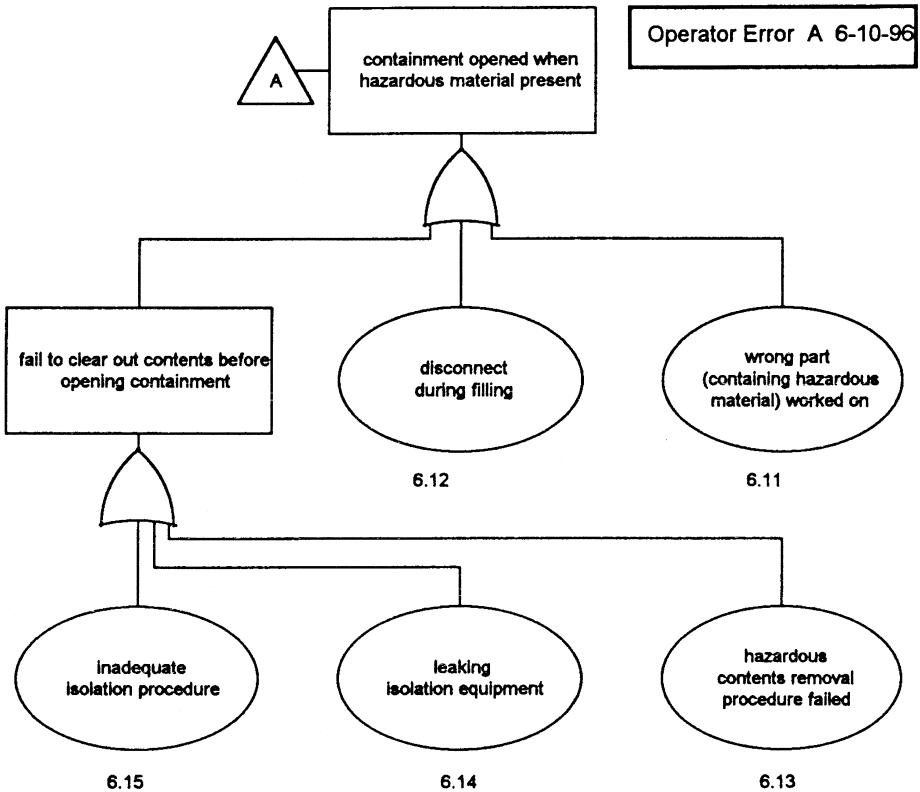

Fig. 3. Branch of Generic Fault Tree: Operator Error (containment bypass).

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], as in the following 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 LODs 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 LODs, called scenario-management links, are being 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 relevant 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; and

-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 relevant 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; and
- 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 off-site 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 developed 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.

$$\text{Risk} = \text{Likelihood of failure of a lines of defence system (against a particular scenario)} \times \text{Consequences of failure}$$

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 Lines 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 into 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 Fig. 4. The principle used is that the more severe the consequences, the lower the acceptable level of likelihood of failure of the Lines 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 Fig. 4 are benchmarked in Fig. 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.

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,

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

Fig. 4. Risk Matrix.

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.

	Likelihood scale:		Consequence scale:
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

Fig. 5. Example of likelihood–consequence scale. Costs are in Dutch guilders (f.)

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 Fig. 6).

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.

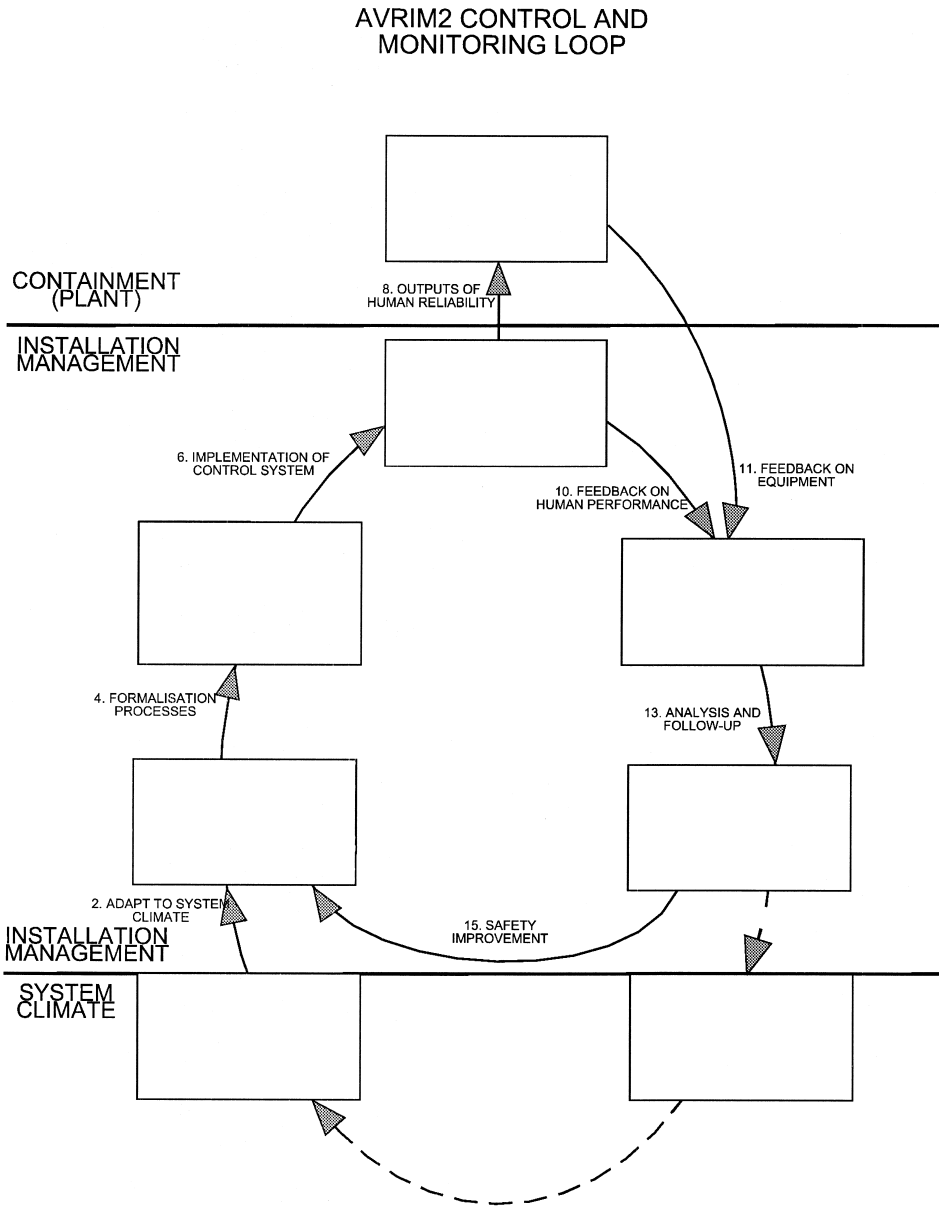

Fig. 6. Control and Monitoring Loop.

The management system is shown represented as the *middle block of components* in Fig. 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.

- 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 from the following.

- 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 Fig. 7. These areas cover the whole of the management system in terms of possible sources of failure leading to loss of containment.

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 Fig. 6 are explained.

(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, and 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,

	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

Fig. 7. Summary of Management Areas Considered in AVRIM2 (LOD = Line of Defence).

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, and 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 nonconformances, 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; and

-subsequent periodic safety inspections of major hazard installations.

As a consequence of the use of AVRIM2 with regards to the assessment 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-Risk, 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, until 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 must demonstrate their approach. 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 focusing rules are needed. Focusing 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 address all issues that are necessary for assessing the quality of the major hazard control systems of companies without being prescriptive.

Acknowledgements

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, Assessment 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] J.I.H. Oh, 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] L.J. Bellamy, T.A.W. Geyer, J.A. Astley, 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] L.J. Bellamy, T.A.W. Geyer, Organisational, management and human factors in quantified risk assessment, Report 1, HSE Contract Research Report 33/92, HMSO, 1992.
[7] M. Wright, G. Tinline, Further development of an audit technique for the evaluation and management of risks, Report C2278, Four Elements, London, 1993.

[8] J. Rasmussen, Risk management, adaptation and design for safety, in: B. Brehmer, N.E. Sahlin (Eds.), Future Risks and Risk Management, Kluwer, Dordrecht, 1994.
[9] R. Van der Mark, 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] L.J. Bellamy, B. Leathley, H. Gibson, Organisational Factors and Safety In the Process Industry, Den Haag, Ministerie van Sociale Zaken en Werkgelegenheid, 1995.