SEVESO 2000: European Conference Risk Management in the European Union of 2000:The Challenge of Implementing Council Directive 'Seveso II' Chamber of Commerce and Industry of Athens, Athens, Greece, November 10 - 12, 1999

Major Hazard Management: Technical-Management Links and the AVRIM2 Method

dr. Linda J. Bellamy and ir. Jaap van der Schaaf

SAVE Consulting Scientists, PO Box 10466, 7301 GL Apeldoorn, The Netherlands

In the Netherlands the legislation and guidance for implementing Seveso II uses, amongst other things, concepts from AVRIM2[1] in order to develop specific requirements for companies to describe scenarios, and for these scenarios to be used by companies as a basis for demonstrating that the major hazard management system works. One of the features of the approach to be taken by both the Labour Inspectorate and by the companies is the use of a limited part of the technical system of a major hazard site to examine the entire major hazard management system in depth. Another aspect is to target potential weak spots in the management system by first considering site specific scenarios. The AVRIM2 software tool supports this approach by providing direct links (in the form of checklists) between lines of defence (LODs) against loss of containment (LOC) scenarios on the one hand and relevant components of the management system across the four life cycle phases (design, construction, operations and maintenance) on the other. This paper explains the approach and gives examples of links as used in AVRIM2.

1. INTRODUCTION TO THE AVRIM2 CONCEPT AND THE RESULTS OF THE LINKS PROJECT

AVRIM2 is a methodology and software program for supporting the assessment of the Safety Report and the carrying out of major hazard site inspections [1], [2], [3], [4]. One of the foundation stones of AVRIM2 is the concept that a Safety Management System should be tailor made for the technical system and its associated risks. This concept is derived from the hands-on experience and observations of the policy makers and the Labour Inspectorate of the Ministry of Social Affairs and Employment in the Netherlands [7]. The concept requires that:

[1] the labour safety report (**a**rbeids**v**eiligheids**r**apport) assessment and **i**nspection **m**ethod version 2

- the regulator must first assess the technical system safety before examining the safety management system.
- the company must show how prevention of the accident scenarios of the technical system is managed by the safety management system.

Seveso II does not explicitly require a company to make a link between the technical system descriptions in the safety report, and the demonstration of the working of the management system in the context of major hazard control. However, the company has to be able to show that it is effectively managing the major hazards.

To make this process as efficient as possible, the “lines of defence” concept of AVRIM2 was further developed in a project which began in 1996 and ended this year [4], [5]. This project provided links between technical and management systems for major hazard (dangerous substances) chemical plant, where:

- the description of the ways in which the hazards might be realised is based on “scenarios” – individual or combinations of failures in the technical (equipment + humans) system for keeping the dangerous substances contained [8].
- the management system is linked to “lines of defence” (LODs) which prevent and protect against scenarios.

The fundamental work for the scenario-management links project led to the idea of the so-called “deep scenarios” or “scenarios at site level” [6] to be described in the Safety Report. The principal is shown in Figure 1 where the complete management system can be reflected in the way a limited number of technical elements are managed [4]. The basic management principles which apply to one part of the technical system can be expected to be found amongst the other parts, and only that much of the technical system has to be analysed to demonstrate these principles.

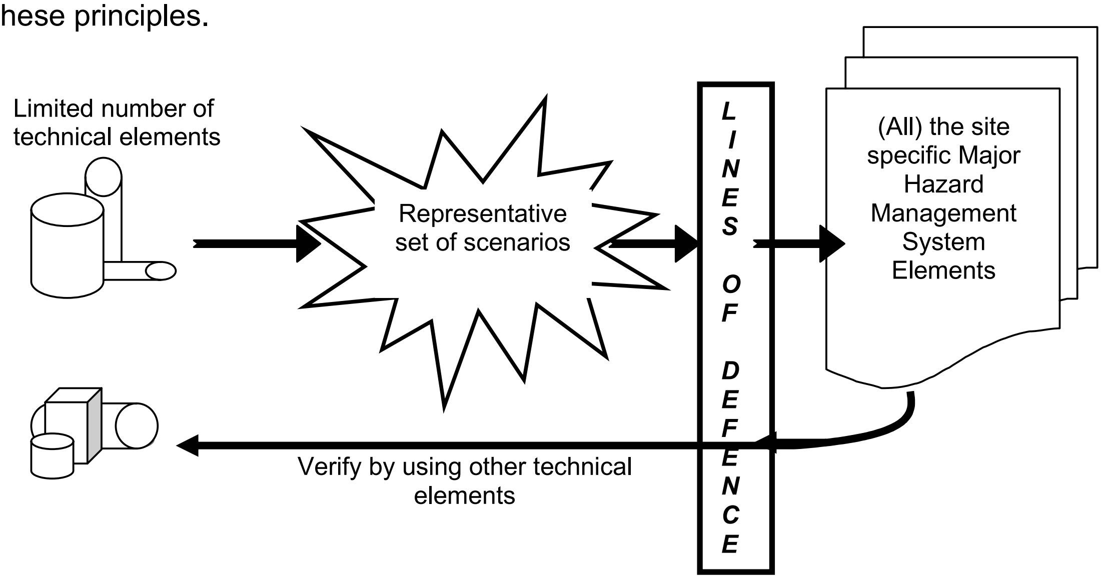

Limited number of technical elements
Representative set of scenarios
LINES OF DEFENCE
(All) the site specific Major Hazard Management System Elements
Verify by using other technical elements

Figure 1: Technical-Management-Technical Connections

The basic scheme for making these scenario descriptions is shown in the "loss of containment bowtie" in figure 2 where the idea is that for 1-3 LOC situations a full working out of causes and effects and lines of defence should be provided:

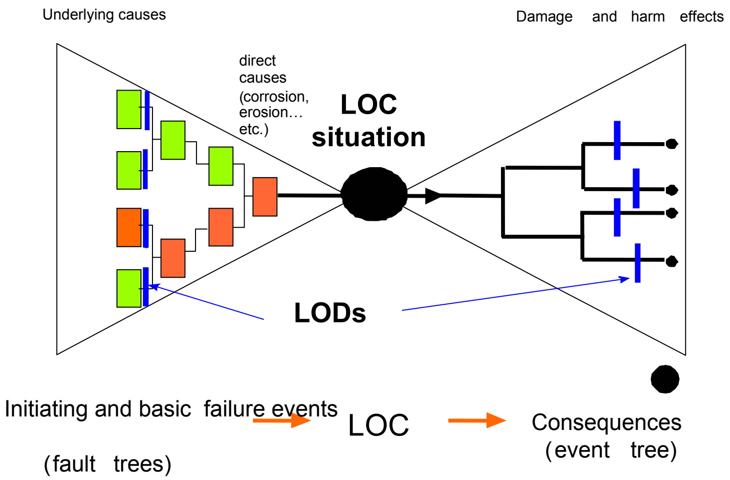


Figure 2: Schematic representation for detailed scenario descriptions ("bowtie"), where LOC=Loss Of Containment and LOD=Line of Defence

2. INCORPORATING LINKS INTO AVRIM2: CHECKLIST LINES OF DEFENCE

Through the links project, support was provided for the AVRIM2 method in the software by making a generically complete set of links between the generic scenarios model (11 generic fault trees with a total of 139 basic failure events and 125 scenarios) and the management system (4 life cycles, 9 management themes per cycle) through a set of lines of defence types (4 types). For every one of the 139 base events, which represent the whole system of generic failures, a number of links to the management system were made based on informed judgement (actual causes of accidents, engineering practice, logical links etc.). The set of links for any particular base event was called "Checklist Lines of Defence".

A "Checklist Lines of Defence" is made from the following components:

Basic Event

This is the starting point for generating the checklist. The basic event is a failure in the technical system which alone or in combination with other events gives the failure scenario. For example, “substance introduced in wrong form” is one of the basic events in the scenario “runaway reaction”.

Type of Line Of Defence

Four types of LOD were defined (see below). A basic event could have one or more types of LOD. For example, “failure to shut off feed in time” can have both process instrumentation and control LODs and work system LODs.

- **Physical LODs** which prevent failure of the physical containment itself, such as thicknesss of metal, physical protection against internal and external conditions.
- **Process instrumentation and control LODs** which prevent failure of the measurement and/or control of the process, which includes process instruments/control loops, pumps, filters etc. (in effect, any equipment or instrument that affects the parameters of the process conditions).
- **Barrier LODs** which prevent failure of the containment through a protective device or system which diverts material or energy when there is a demand on the containment system, such as pressure relief, or a barrier to prevent impact from vehicles.
- **Work-system LODs** which prevent events that may place demands on physical systems and include plans, procedures, instructions and other support systems (like the ergonomics of information displays or operational controls) which help to prevent human error or omission.

Life Cycle

For each LOD there are relevant life cycles in which the LOD is introduced and preserved, such as the Design phase for determining the correct protection specifications against corrosion. There can be more than one possible life cycle for each LOD. For example, failure in equipment supports can cause physical loading conditions. These support failures might arise due to the supports being poorly installed. This could happen in the Construction phase, or because of Maintenance.

The life cycles are:

- Design (and modifications)
- Construction
- Operations
- Maintenance, Inspection and Testing

Management Theme per life cycle

This is the point at which the technical system is connected to the management system. In effect, the life cycles in which the LODs are introduced and preserved are considered in terms of the key management tasks or “themes” involved in introducing and preserving them. A list of one or more management themes under each life cycle is the concluding part of the Checklist LOD.

The themes are derived from AVRIM2's management model. For every life cycle there is a management model, the Control and Monitoring loop, which has a number of components of control and monitoring linked together as a self regulating, self improving control system. For each of the 15 loop components of the system there are common themes which run through them. Attention points for auditing this system are grouped under 9 themes, which recur under each of the 15 loop components. These themes are more or less common across all life cycles. Selections of a limited number of themes make it possible to carry out a restricted audit of the control and monitoring loop. These management themes appear in every life cycle:

- Knowledge of hazards/risks
- Use of standards
- Control of safety-production conflicts
- Formal safety studies
- Safe procedures
- Manning levels, competence, training
- Human factors in error management
- Supervision and checking
- Capturing experience, incident/near miss analysis

3. TECHNICAL-MANAGEMENT LINKS IN AVRIM2 SOFTWARE

Figure 3 gives a hypothetical case of an 'LOC situation' using AVRIM2 software. The hypothetical case is a C-CAP transfer pipework leak. Figure 3 shows the set of generic fault trees connected to this LOC situation. AVRIM2 software always automatically connects all the generic trees to a named LOC situation (Note: the effect tree part of the bowtie in figure 2 has not been connected yet). In Figure 3 on the right hand side of the screen, one of the generic fault trees has been expanded. It is possible to do this with any selected tree. Numbered events in the expanded tree are the basic failure events. In the example in figure 3 the failure event is 'not replaced like with like'.

Every basic event in every tree has an associated "Checklist Lines Of Defence" This is a suggested list of the components of a lines of defence system against the occurrence of the basic failure event. For example, for the event 'not replaced like with like' the checklist is as follows:

Not replaced like with like

LOD Type*:* Systems of Work
Life cycle*:* Maintenance, Inspection and Testing (MIT)
Management themes in MIT life cycle*:* -Standards for maintenance, inspection and testing -Control of conflicts between safety and production - Human factors in error management of MIT- Supervision and checking of MIT tasks.

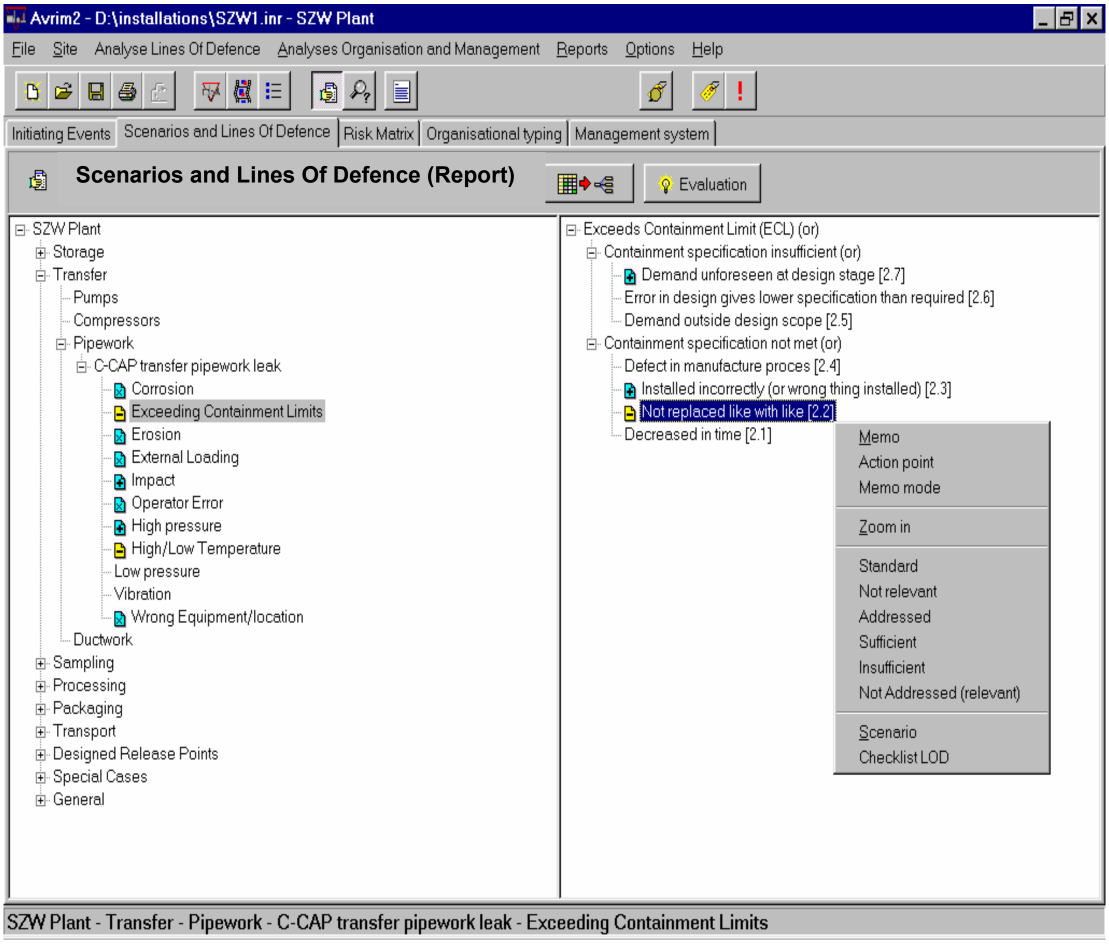
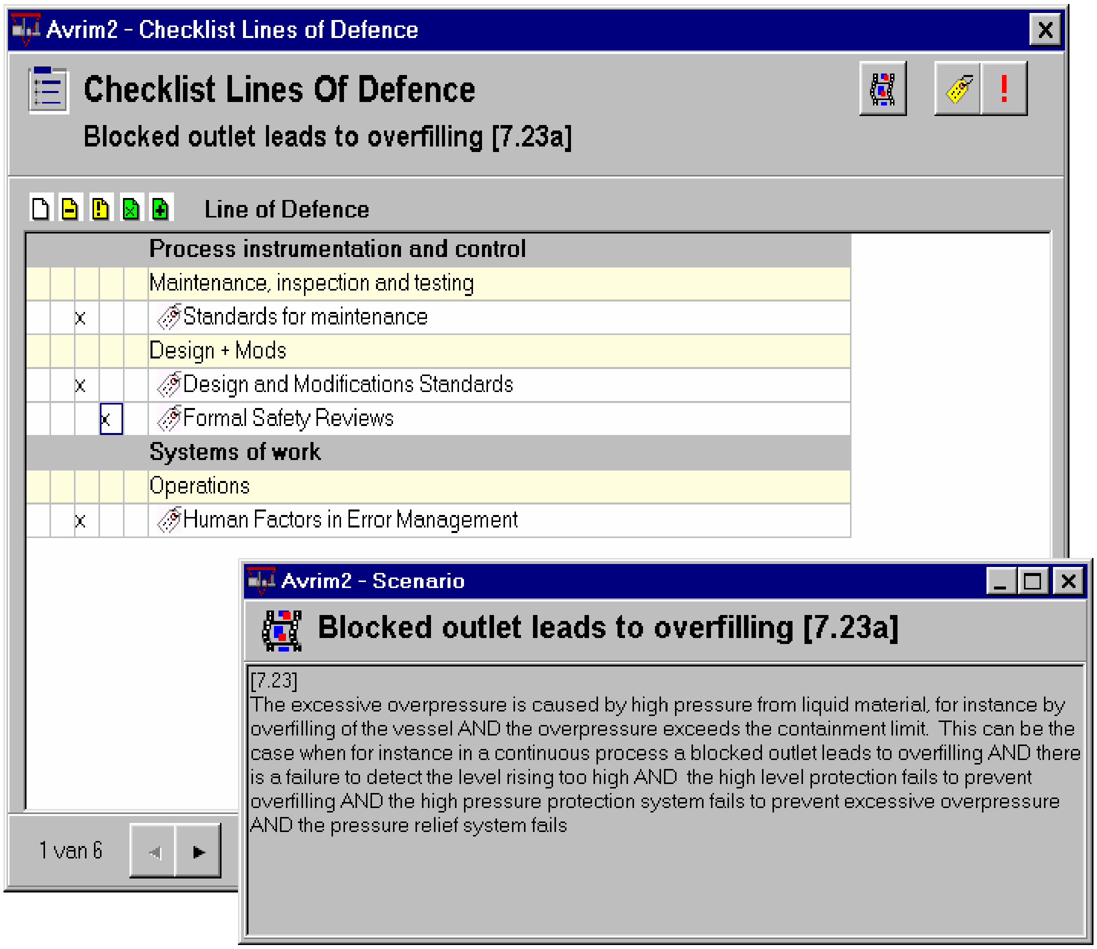

Avrim2 - D:\installations\SZW1.inr - SZW Plant
File
Site
Analyse Lines Of Defence
Analyses Organisation and Management
Reports
Options
Help
Initiating Events
Scenarios and Lines Of Defence
Risk Matrix
Organisational typing
Management system
Scenarios and Lines Of Defence (Report)
Evaluation
SZW Plant
Storage
Transfer
Pumps
Compressors
Pipework
C-CAP transfer pipework leak
Corrosion
Exceeding Containment Limits
Erosion
External Loading
Impact
Operator Error
High pressure
High/Low Temperature
Low pressure
Vibration
Wrong Equipment/location
Ductwork
Sampling
Processing
Packaging
Transport
Designed Release Points
Special Cases
General
Exceeds Containment Limit (ECL) (or)
Containment specification insufficient (or)
Demand unforeseen at design stage [2.7]
Error in design gives lower specification than required [2.6]
Demand outside design scope [2.5]
Containment specification not met (or)
Defect in manufacture proces [2.4]
Installed incorrectly (or wrong thing installed) [2.3]
Not replaced like with like [2.2]
Decreased in time [2.1]
Memo
Action point
Memo mode
Zoom in
Standard
Not relevant
Addressed
Sufficient
Insufficient
Not Addressed (relevant)
Scenario
Checklist LOD
SZW Plant - Transfer - Pipework - C-CAP transfer pipework leak - Exceeding Containment Limits

Figure 3: AVRIM2 software showing LOC situation and connected direct causes (left) and base events of one of the generic fault trees (right). Base event for scenario 2.2 is highlighted. At the bottom of the menu for this base event is "Checklist LOD"
(Note: this particular tree 'Exceeds Containment Limits' always occurs in combination with one of the others).

The checklist tells the inspector to consider whether there are indications given by the company that the chance of not replacing like with like is defended against in the systems of working in Maintenance. Are there, for example, maintenance standards available which make clear what "like" is, for example, and do the standard procedures cover this issue; are there factors for minimising error in selecting a wrong part, for example, and does someone supervise or check the replacement task. The checklist is a sort of first pass, which the inspector or company uses to connect the specific scenarios to key elements in the management system.

An example of a Checklist LOD in AVRIM2 software is shown below in figure 4 for one base event from the Overpressure tree. This base event 'blocked outlet leads to overfilling' is one event in a scenario which comprises 6 base events (the scenario definition is also shown in the figure). The basic structure of the checklist is to specify the relevant life cycle management themes under each LOD. So, for example, the blocked outlet is considered to have potential defences of the process instrumentation and control type for which standards for doing maintenance, standards of design, and a safety study in the design phase are all considered relevant. In addition, a blocked outlet is considered to have possible defences of the systems of work type for which management of the human factors aspect of error (such as minimising the chance of a monitoring failure for blockages, for example) during operation of the system are considered relevant.



Checklist Lines Of Defence

Blocked outlet leads to overfilling [7.23a]

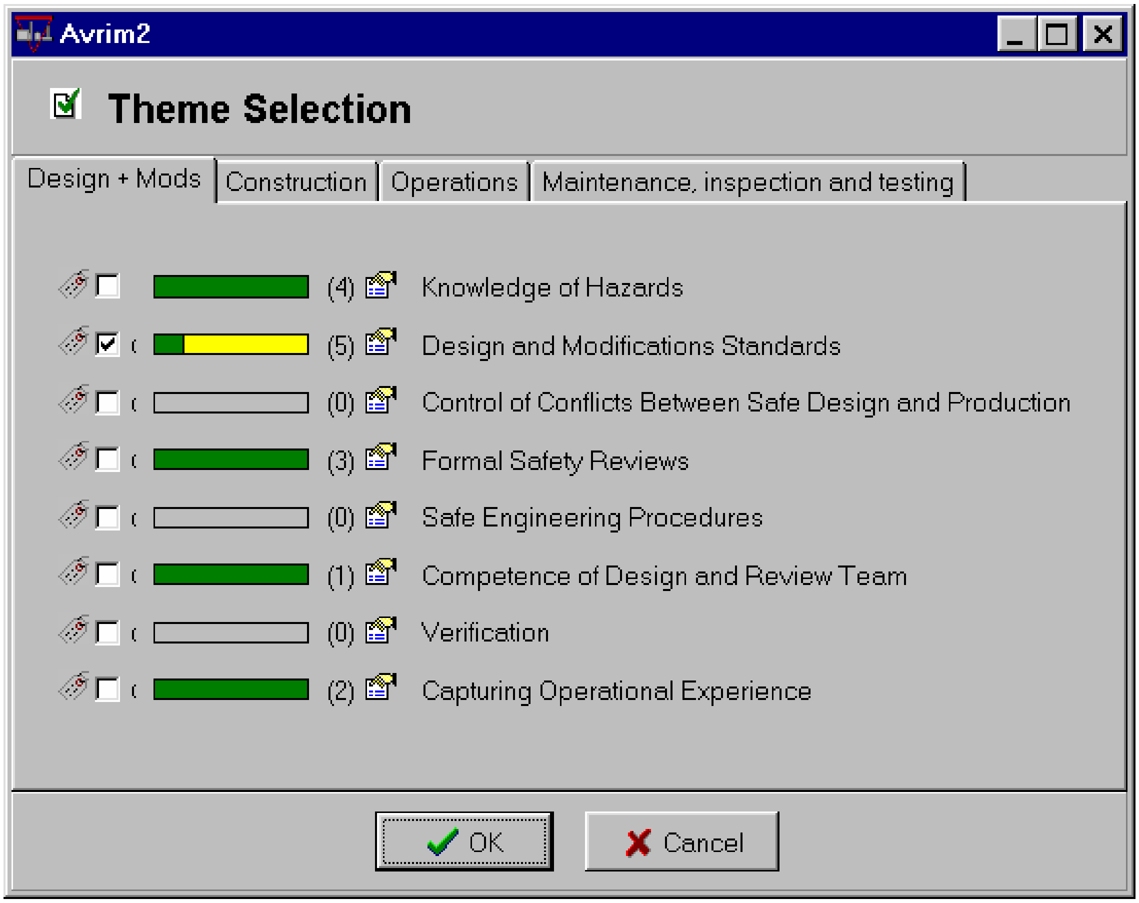
					Line of Defence
					Process instrumentation and control
					Maintenance, inspection and testing
		x			Standards for maintenance
					Design + Mods
		x			Design and Modifications Standards
			x		Formal Safety Reviews
					Systems of work
					Operations
		x			Human Factors in Error Management

Blocked outlet leads to overfilling [7.23a]

[7.23]
The excessive overpressure is caused by high pressure from liquid material, for instance by overfilling of the vessel AND the overpressure exceeds the containment limit. This can be the case when for instance in a continuous process a blocked outlet leads to overfilling AND there is a failure to detect the level rising too high AND the high level protection fails to prevent overfilling AND the high pressure protection system fails to prevent excessive overpressure AND the pressure relief system fails

Figure 4: Checklist Lines Of Defence for one of the basic events in Scenario 7.23, together with a description of the complete scenario. Each of the basic events in the scenario has its own checklist.

Whenever a management theme is marked up in a Checklist LOD, this is reported back in the software in the Management module as shown in Figure 5. The thermometer scales on the left indicate the proportion of LODs marked positively or negatively (darker portion of the strip indicates positive), and the number is the total number of basic events assessed.



□ (4) Knowledge of Hazards

☑ (5) Design and Modifications Standards

□ (0) Control of Conflicts Between Safe Design and Production

□ (3) Formal Safety Reviews

□ (0) Safe Engineering Procedures

□ (1) Competence of Design and Review Team

□ (0) Verification

□ (2) Capturing Operational Experience

Figure 5: The scoring of management themes in the Checklists LODs reappears in the management module to give guidance on what themes are strong or weak with respect to management of site specific scenarios. The theme "Design and Modification Standards" has been selected for further analysis in an audit of the management system.

4. SUMMARY

The connection of failure scenarios to the management system in AVRIM2 enables a management system to be addressed in a site specific way in terms of the specific major hazard scenarios (technical system failures). 46 technical-management connections (Checklists Lines Of Defence) have been made across the AVRIM2 system.

What is interesting is that it is now possible to backtrack from a management theme to a connected set of scenarios. For example, taking the theme of: ‘conflicts between safety and production’ in the operations and maintenance phases, this is linked to the following types of scenarios:

- erosion,
- failure to detect accelerated corrosion or deterioration in quaility of materials, corroded (not maintained/inspected) equipment, unrepaired damage to corrosion protection,
- operating outside the design safety limits,
- various types of blockage in pipework and associated equipment resulting in overpressures,
- runaway reactions,
- wrong spec equipment due to incorrectly installed equipment including due to not having the right parts available and maintenance being carried out at the wrong place, not replacing like with like,
- overfilling, failure in automatic stop devices due to lack of maintenance,
- removing and not replacing equipment supports after maintenance
- starting up an operation with open equipment,
- failing to properly clear out hazardous contents before maintenance.

The ability to backtrack leads to interesting possibilities for beginning an evaluation in the safety management system as shown in Figure 6. This is particularly useful for investigating Major Accident Prevention Policy sites where a technical evaluation by the company is not required under Seveso II.

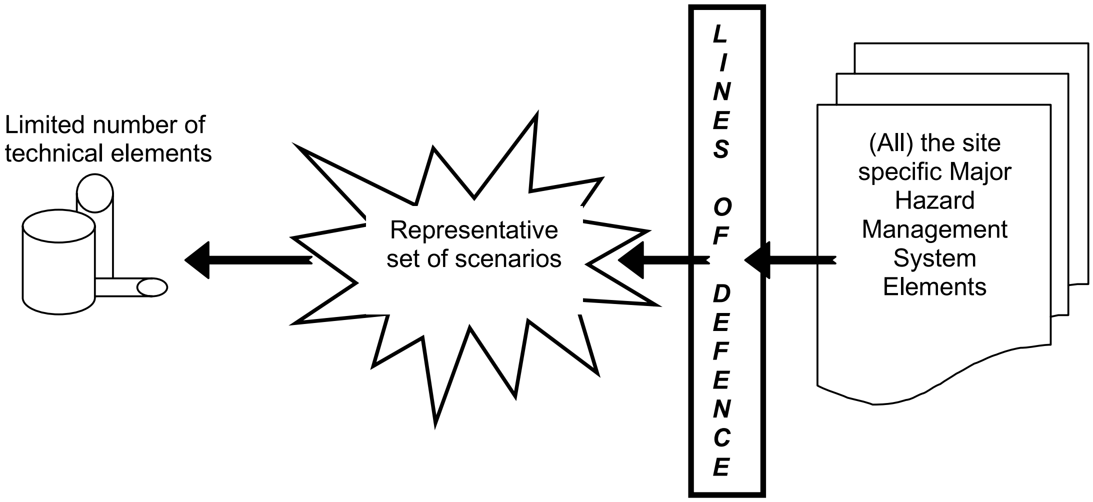

Limited number of technical elements
Representative set of scenarios
LINES OF DEFENCE
(All) the site specific Major Hazard Management System Elements

Figure 6: Scenario-Management Links study enables investigations to begin in the management system and link to the potential technical system weaknesses.

REFERENCES

1. SAVE/SZW (1996, 1999) AVRIM2 Assessment and Inspection Method Handbook, Version 1.0, 1996; AVRIM2 Software, Version 1.19, 1999. Produced by SAVE consulting scientists, Apeldoorn, the Netherlands, for the Dutch Ministry of Social Affairs and Employment (Ministerie van Sociale Zaken en Werkgelegenheid, Den Haag).
2. Bellamy, L.J. and Brouwer, W.G.J (1999) AVRIM2, a dutch major hazard assessment and inspection tool. Journal of Hazardous Materials, 65 (1999) 191-210.
3. Oh, J.I.H. and Bellamy, L.J. (1998) "AVRIM2: Safety Report Assessment and Inspection Method for Major Hazard Installations and their Safety Management Systems Within the context of the EU Seveso II Directive." Proceedings of Inspection Systems and Examination of the Safety Report, Rome, September 1998. Special Publication No.I.98.90 of the European Commission Joint Research Centre, 21020 Ispra (VA) Italy.
3. Bellamy, L.J. and Oh, J.I.H. (1998) "AVRIM2: Safety Report Assessment and Inspection Method for Major Hazard Installations and their Safety Management Systems Within the context of the EU Seveso II Directive." pp. 163-174 in Proceedings of the 9th International Symposium Loss Prevention and Safety Promotion in the Process Industries, 4-7 May, 1998, Barcelona, Spain.
4. Bellamy, L.J. (1998) "A Case Study in the Use of AVRIM2 Scenarios." Proceedings of Inspection Systems and Examination of the Safety Report, Rome, September 1998. Special Publication No.I.98.90 of the European Commission Joint Research Centre, 21020 Ispra (VA) Italy.
5. SAVE (1999) Scenario-management links. Ingenieurs/adviesbureau SAVE report 991752-A41, prepared for the Dutch Ministry of Social Affairs and Employment (Ministerie van Sociale Zaken en Werkgelegenheid, Den Haag).
6. RIB: **R**apport **I**nformatie-eisen **B**RZO '99 (*Safety report information demands according to the Decree on the Risks of Major Accidents 1999*) Drawn up by ingenieurs/adviesbureau SAVE, Apeldoorn, the Netherlands under assignment from the Ministries of VROM (Environment), SZW (Social Affairs) and BZK (Internal affairs). SAVE report 991188-C78, june 1999 [officially published as CPR 20, 1999].
7. Bellamy, L.J., Leathley, B., and Gibson, H. (1995) Organisational Factors and Safety In the Process Industry. Ministerie van Sociale Zaken en Werkgelegenheid, Den Haag, The Netherlands. ISBN 90-5250-976-X
8. Van de Mark, R. (1996) "Generic Fault trees and the modelling of management and organisation". Final year report Dept. of Statistics, Probability and Operations Research, TU Delft, The Netherlands.