AVRIM2: A holistic assessment tool for use within the context of the EU Seveso II directive

Joy I.H. Oh, Ministry of Social Affairs, the Netherlands [1]
Linda J. Bellamy, SAVE Consulting Scientists for Industrial Safety[2]

A presentation for the Seveso 2000 conference 22-23 June, Bordeaux, France

Abstract

In this paper a holistic method is described based on the concept of scenarios and lines of defence by which the safety management system of a company can be assessed for its robustness in relation to controling the hazards of loss of containment of dangerous substances.

Introduction

The Seveso II directive places requirements on both operators and regulators. The operator has to demonstrate via the safety report that a major accident prevention policy and a safety management system for implementing it has been put into effect. Furthermore the operator has to demonstrate that major accident hazards have been identified and that the necessary measures have been taken to prevent such accidents and to limit their consequences for man and the environment (article 9.1). The regulator has to organize a system of inspections for a systematic examination of the systems being employed at the establishment, whether of a technical or organisational nature to ensure that the operator has fulfilled his obligations (article 18.1).
For both the operator and the regulator the problem lies with the amount and detail of the information provided in the safety report so that the regulator can properly assess that a) the operator knows the major-accident hazards on his site, b) he has taken the necessary technical measures and c) has the appropriate safety management system to manage those measures.

Holistic approach towards major hazard safety

In figure 1 a presentation is given of all the hazards in relation to the technical and management systems. In the centre of this diagram are all the hazards on the site. Only a small portion of those hazards are linked to loss of containment and are major hazards. All these hazards are controlled by a hazard control system which is

[1] po box 90801 2509 LV Den Haag, the Netherlands, e-mail: joh@minszw.nl
[2] po box 10466, 7301 GL Apeldoorn, the Netherlands, e-mail: save@save.nl

technical and is in essence systems of lines of defences. Only a small portion of these are there to prevent the major hazards from occurring. Around this technical system there is the layer of the safety management system, designed to manage the technical system. Again only a small portion of this system is there specifically to manage the major hazard aspects. The aspects of the hazard control system and the safety management system that are linked to the major hazards have been grouped together in the slice which says "AVRIM2". The challenge for both operator and regulator lies within the identification of all the relevant major hazard parts of this slice and to ensure that all these aspects are linked together in the right way. This can only be achieved if a holistic approach is being used and both description and assessment are tailor made to the specific situation.

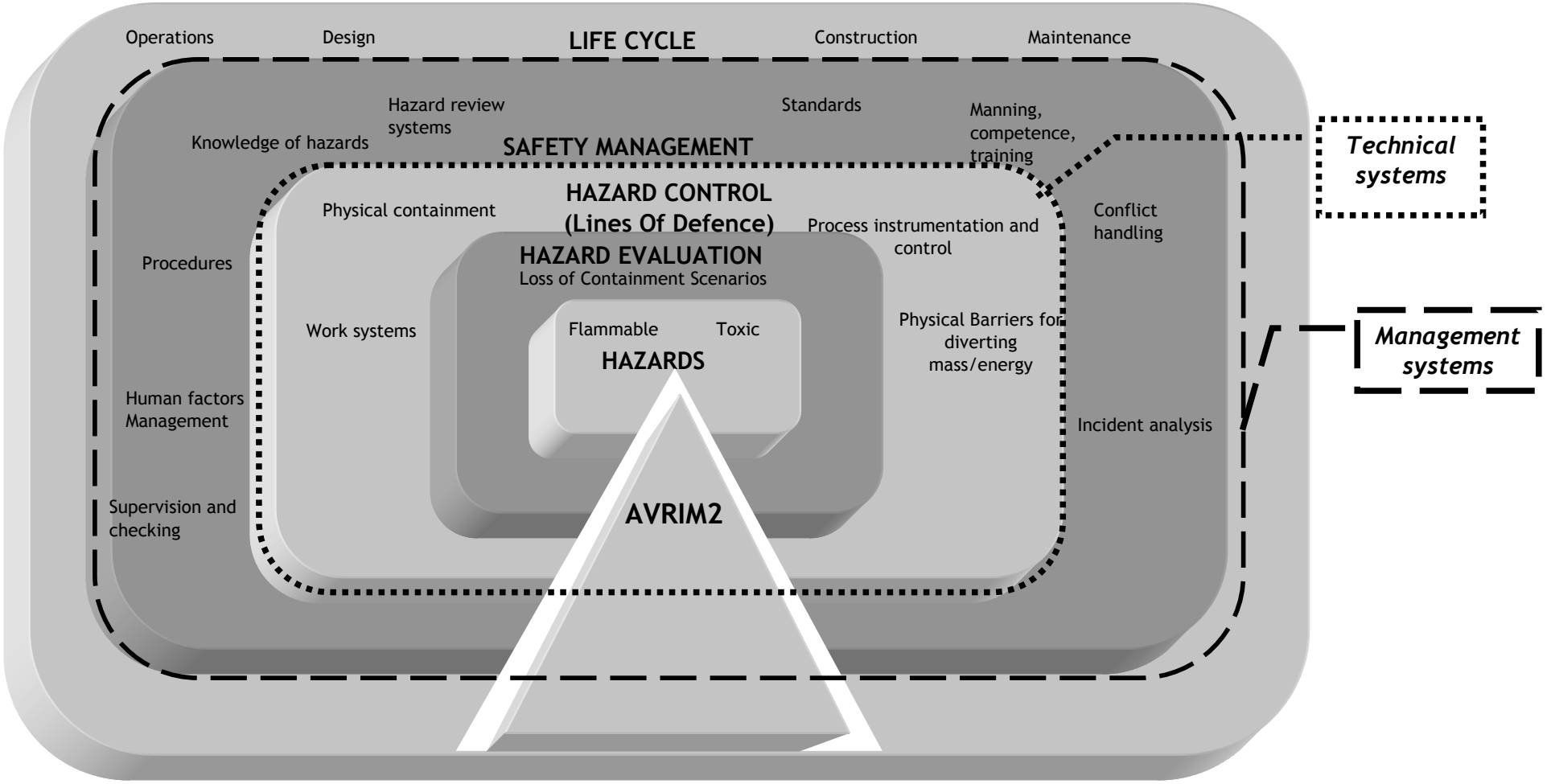
Operations
Design
LIFE CYCLE
Construction
Maintenance
Hazard review systems
Standards
Manning, competence, training
Knowledge of hazards
SAFETY MANAGEMENT
Technical systems
HAZARD CONTROL (Lines Of Defence)
Physical containment
Process instrumentation and control
Conflict handling
HAZARD EVALUATION
Loss of Containment Scenarios
Procedures
Work systems
Flammable
Toxic
HAZARDS
Physical Barriers for diverting mass/energy
Management systems
Human factors Management
Incident analysis
Supervision and checking
AVRIM2

Figure 1: Presentation of the hazards in relation to the technical and mangement systems

The AVRIM2 tool

AVRIM2 is a methodology and software program for supporting the assessment of the Safety Report and the carrying out of major hazard site inspections. 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. The concept requires that:

- 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 developed in detail over the period 1996-1999. This project provided links between technical and management systems for major hazard chemical plant, where:

- the description of the ways in which the hazards might be realised is based on "scenarios" - the individual or combinations of failures in the technical (equipment + procedural) system for keeping the dangerous substances contained;
- the management system is linked to "lines of defence" (LODs) which prevent and protect against the occurrence of scenarios.

The fundamental work for the scenario-management links project led to the idea that the scenarios to be described in the Safety Report should not only be representative of the hazards but should also be chosen in such a way as to demonstrate all the technical and organisational measures employed for controlling major accidents. The principal is shown in figure 2 where the complete management system can be reflected in the way a limited number of technical elements are managed. That is, the basic management principles that 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.

The basic scheme for making these scenario descriptions is shown in the "loss of containment bowtie" in figure 3 where the idea is that the complete system of lines of defence and their management should be demonstrated through the choice of cause and effect scenarios.

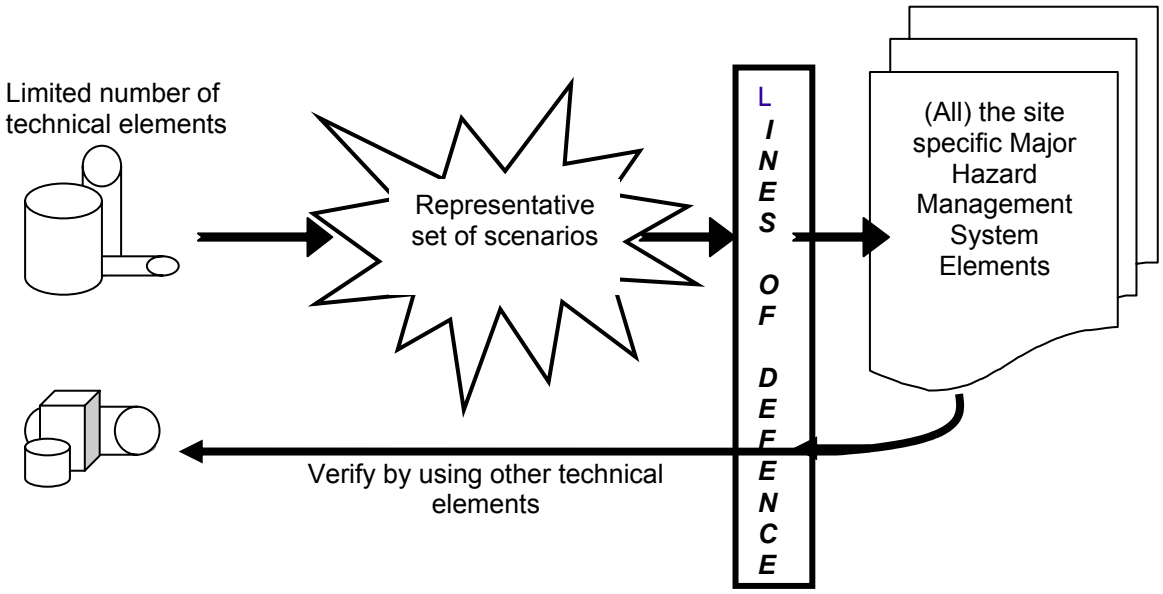

Figure 2: Overview of the components of AVRIM2

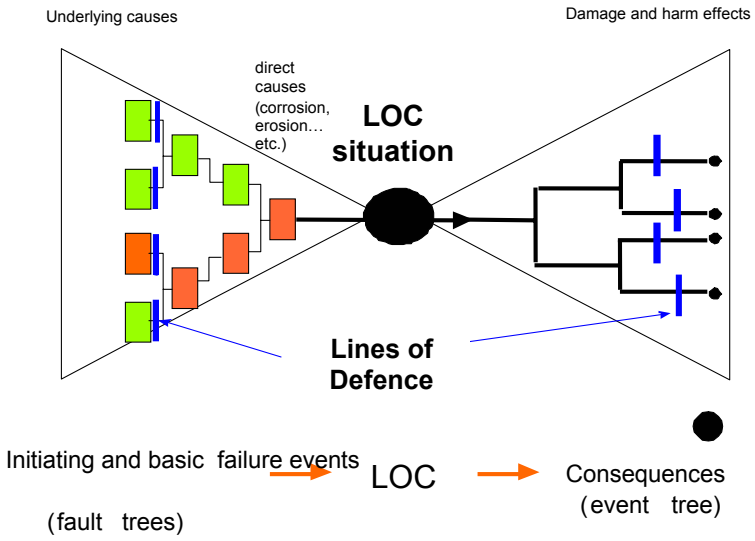

Figure 3: Overview of the scenarios leading up to Loss Of Containment (LOC) and effect scenarios (LOC bowtie)

Risk matrix

The next stage is for the company to evaluate the risk of occurrence of the scenarios. Under Seveso II in the Netherlands Quantified Risk Assessment is a requirement.

However this only looks at scenarios with offsite consequences. In addition, attention is very much directed towards mitigation of consequences rather than identifying and reducing causes of failure. Generic historical failure data is used to identify the likelihood of releases and mitigation evaluation focussed on *protective* Lines of Defence.

The aim of getting companies to evaluate the risks of occurrence of scenarios is to get them to focus on reliabilities of Lines Of Defence systems and possible 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. It also requires 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.
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 measures 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.

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 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. 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 assessment criterion is 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. This means that, where there are major hazards, there is always some level of risk.

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 higher the acceptable level of reliability 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.

Figure 4: Example of Risk Based Criteria

Likelihood of loss of containment	Consequence severity				
	Negligible	Minor	Serious	Major	Severe
Very high	O	X	X	X	X
High	O	O	X	X	X
Average	-	O	O	X	X
Low	-	-	O	O	X
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 risk. No further action required

Figure 5: Example of Likelihood - Consequence Scale

	Likelihood scale:		**Consequence scale:**[3]
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

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

Scenario Management links

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 that 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 can have more than one type 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 thickness 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.

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 that 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

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.

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). What is interesting is that it is now possible to backtrack from a management theme to a connected set of scenarios. The ability to backtrack leads to interesting possibilities for beginning an evaluation in the safety management system and frees inspectors from having to begin with scenarios. This is also useful for investigating Major Accident Prevention Policy sites where a technical evaluation by the company is not required under Seveso II.

Conclusion

In this paper a method is described to assess the safety management system from a Seveso II company in a holistic way, meaning that apart from the safety management system itself it takes into account the major hazards, the technical hazard control system and assesses their links. To be able to use AVRIM2 the company has to provide specific information in the safety report. Scenarios that

can lead to loss of containment are an essential part of this. The technical requirements for these descriptions have been put into the regulations. First results are very promising; the method has given leading companies insight into weaknesses in their major hazard control system. For the regulator it has given a uniform procedure by which the top tier Seveso II sites can be assessed.