European Commission

EUR 19320

Community research

Project report

I-RISK:

A quantified integrated technical and management risk control and monitoring methodology

ENERGY, ENVIRONMENT
AND SUSTAINABLE DEVELOPMENT

EUR 19320

Interested in European research?

RTD info is our quarterly magazine keeping you in touch with the main developments (results, programmes, events, etc.). It is available in English, French and German. A free sample copy or free subscription can be obtained from:

Directorate-General for Research
Communication Unit
European Commission
Rue de la Loi/Wetstraat 200
B-1049 Brussels
Fax (32-2) 29-58220
e-mail: rtd-info@cec.eu.int
http://europa.eu.int/comm/research/rtdinfo.html

EUROPEAN COMMISSION

Directorate-General for Research
Unit D.I.1 — Energy, environment and sustainable development
Contact: Mrs Karen Fabbri – Rue de la Loi/Wetstraat, 200 (SDME 7/23), B-1049 Brussels
Tel: (32-2) 29-95185; Fax (32-2) 29-63024; e-mail: ib.troen@cec.eu.int

European Commission

I-RISK:
A quantified integrated technical and management risk control and monitoring methodology

Ministry of Social Affairs and Employment (SZW), the Netherlands (Coordinator)

Four Elements Ltd, United Kingdom (Secretariat)

Health and Safety Executive, United Kingdom

Ministry of Environment (VROM), the Netherlands

NCSR Demokritos, Greece

National Institute for Health and Environment (RIVM), the Netherlands

Norsk Hydro a.s., Norway

Safety Science Group, Delft University of Technology, the Netherlands

SAVE Consulting Scientists, the Netherlands

Directorate-General for Research

2000

EUR 19320

A great deal of additional information on the European Union is available on the Internet. It can be accessed through the Europa server (http://europa.eu.int).

Cataloguing data can be found at the end of this publication.

Luxembourg: Office for Official Publications of the European Communities, 2000

ISBN 92-828-9483-5

Printed in Italy

PRINTED ON WHITE CHLORINE-FREE PAPER

Contract No: ENVA-CT96-0243

PROJECT i RISK

STEERING COMMITTEE

Chairman

Joy I. H. Oh

Ministerie van Sociale Zaken en Werkgelegenheid (Ministry of Social Affairs and Employment),

Postbus 90801, 2509 LV Den Haag, the Netherlands

Participants June 1996- December 1998

Ben J. M. Ale (RIVM)

Olga N. Aneziris (Demokritos)

Martin Anderson (HSE)

Linda J. Bellamy (SAVE)

Philip G. Brabazon (Four Elements)

WilliNt G. J. Brouwer (SZW)

Jon Arne Grammeltvedt (Norsk Hydro)

Frank W. Guldenmund (TU Delft)

Andrew R. Hale (TU Delft)

Caroline Horbury (HSE)

Nick W. Hurst (HSE)

Jolanda Van der Kamp (SZW)

Mark I. Morris (Four Elements)

Andrð J. Muyselaar (VROM)

Ioannis A. Papazoglou (Demokritos)

Jos G. Post (RIVM)

Unni N. Samdal (Norsk Hydro)

Helen Shannon (Four Elements)

Helen K. Walker (Four Elements)

MAIN REPORT AUTHORS:

Linda J. Bellamy (SAVE)

Ioannis A. Papazoglou (Demokritos)

Andrew R. Hale (TU Delft)

Olga N. Aneziris (Demokritos)

Ben J. M. Ale (RIVM)

Mark I. Morris (Four Elements)

Joy I. H. Oh (SZW)

EDITORS:

Linda J. Bellamy

SAVE Consulting Scientists, Postbus 10466, 7301 GL Apeldoorn, the Netherlands

Karen P. Fabbri

Research DG, European Commission, 200 Rue de la Loi, 1049 Brusels, Belgium

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ALARA	As Low as Reasonably Achievable
AVRIM2	Arbeidsveiligheidsrapport beoordelings- en Inspectiemethodiel 2 (Labour Safety Report Assessment and Inspection Method)
BLEVE	Boiling Liquid Expanding Vapour Explosion
CCDF	Complementary Cumulative Distribution Function
CIMAH	Control of Industrial Major Accidents
EU	European Union
HAZOP	Hazard and Operability (study)
FLL	Feedback and Learning Loop
IE	Initiating Event
I-QRA	Integrated Quantitative Risk Assessment
I-RISK	Integrated (technical and management) Risk
IRMA	Integrated Risk Management Audit
LOC	Loss of Containment
LPG	Liquefied Petroleum Gas
MAPP	Major Accident Prevention Policy
MHMS	Major Hazard Management System
MLD	Master Logic Diagram
PRIMA	Process Risk Management Audit
RCMS	Risk Control and Monitoring System
SADT	Structured Analysis and Design Technique
SHE	Safety, Health and Environment
SMS	Safety Management System

1. INTRODUCTION

1.1 Background

On 3 February 1997 the EU directive 96/82/EC on the control of major-accident hazards, the so-called Seveso II directive entered into force.

The aim of this directive is two-fold:

1) It aims at the prevention of major-accident hazards involving dangerous substances.

2) It aims at the limitation of consequences if major accidents should occur.

These hazards are thus connected to the prevention of loss of containment. This means that the starting point is process safety and installation integrity.

Dangerous substances in this respect are substances that are dangerous for man and/or environment. Furthermore, the directive limits itself to on-site hazardous installations only and does not deal with nuclear safety, offshore, mining activities, or transport.

Apart from all the administrative details, the directive demands that companies should establish and properly implement a so-called major-accident prevention policy (MAPP). To implement this policy properly in a company, a safety management system (SMS) should also be in place. The directive explicitly states what should be in the MAPP and what should be it the SMS. The SMS shall address the following issues which are exactly specified in the directive:

- Organisation and personnel
- Identification and evaluation of major-accident hazards
- Operational control
- Management of change
- Planning for emergencies
- Monitoring performance
- Audit and review

During the development of this directive, which apart from the European Commission involved policy makers from all EU member states, it was recognised that in order to ensure its proper implementation, integration and co-operation of the relevant policy fields was necessary. Not only should internal and external safety policy makers work closely together, but there was also a need for further developing the integration of methods dealing with assessing the technical hazards of installations, and audit methods which deal primarily with safety management systems. The developments around the Seveso II directive were seen as an opportunity to bring the integrated safety approach a step forward.

Previous research for the European Commission's ENVIRONMENT programme has explored a Modification of Risk methodology whereby evaluation of the quality of management by audit was used to modify the generic failure rates of Quantitative Risk Assessment (e.g. Muyselaar and Bellamy 1993, Bellamy and Tinline 1993). The Safety Management System model was derived from analysis of Loss of Containment (LOC) accidents and a control and monitoring loop model used as a standard against which to evaluate a specific installation's SMS. In this respect, the model is directly

linked to process safety and the way that a SMS controls the hazards. This is in contrast with the usual audit systems that are tailor made to a specific company and are based on industry best practice. As such, this model can be applied to every company and focuses totally on the hazards that are involved. The model has been under development since 1985, stimulated by questions from the process industry who wished to have their SMS accounted for in risk evaluation, and subsequently by the regulator requiring tools to investigate a site specific SMS.

So in order to investigate the integration of technical safety and management safety models and the application of such an integrated model a unique team was formed. Unique because it consisted of policy makers that were closely involved in the development of the Seveso II directive, leading research institutions in the fields of quantified risk assessment and safety management systems and representatives of a chemical company with a good (but improvable) safety record. This blend of expertise should also guarantee that a) the research was fundamentally sound, b) it had enough policy and regulatory relevance and c) it was applicable in "real life".

The research was funded under the 'Environment and Climate' stream of the Fourth Framework Programme for RTD (1994-1998) of the European Commission (contract no. ENV4-CT96-0243), the UK Health and Safety Executive and the Dutch ministries of SZW and VROM.

Rather then having an end report that reflects the work as how it progressed during the project a different structure was chosen which reflects the applicability of the study.

This means that after this introduction in which also the objectives and the functional requirements (chapter 1.2) are explained, immediately the methodology is explained via which the I-Risk study is performed. Chapter 2 starts off with descriptions of the three I-Risk model components. In chapter 2.1.2 it is described how one starts building a technical model that is hardware based. It consists of risk assessment aspects that are directly linked to the hardware. Central in technical model is the Master Logic Diagram. In chapter 2.1.3 the management model and IRMA (Integrated Risk Management Audit) are described. This model was developed in such a way that it will fit the technical model and thus indirectly may affect the performance of the hardware. To link the technical and management models, an interface was developed which is described in chapter 2.1.4. Chapters 2.2 to 2.9 deal with a systematic procedure on how to perform the I-Risk study.

Chapter 3 gives a summary of the test results. One desktop exercise was performed and two on-site studies. Chapters 4 and 5 conclude the report with discussion and future developments.

It is the belief of the authors of this report that they succeeded in what was envisaged, which is the development of an integrated (semi) quantified risk model which incorporates hardware and organisation and which also is applicable in "real life". The results and spin-off of this study are very promising for the future.

1.2 Functional Requirements of the Project

1.2.1 Objectives

1.2.1.1 Overall objective

To provide a model for:

- integrating methods for the evaluation and control of risks, and
- integrating assessment of on-site and off-site risks.

1.2.1.2 Sub-Objectives

1. Development of and integrated technical and management risk control and risk monitoring model including on-site and off-site risks and their variation over time, developing the model within the context of the Seveso II Directive.
2. Incorporation of 1 into an Integrated Quantitative Risk Assessment (I-QRA) approach such that risk reduction strategies will be focussed on the system as a whole and on a more realistic representation of risk as something which changes over time rather than as a time based average.
3. Development of management "corrosion" probes to assist in monitoring the state of the risk management system.
4. Testing and application

1.2.1.3 Basis

Integration of risk evaluation and control principles found in:

- engineering risk assessment;
- management systems;
- safety culture concepts;
- organisational structures.

1.2.1.4 Emphasis:

Chemical and petrochemical industry, major hazard installations.

1.2.1.5 Rationale:

To give a basis for controlling the interactions between failures that occur at different levels of the socio-technical system and which have been repeatedly observed in accidents.

1.2.2 Functional Requirements

The functional requirements of the I-Risk project were agreed amongst participants as follows:

1.2.2.1 Integration of LOC Risks

To provide a model to integrate the assessment of the risk of Loss Of Containment (LOC) accidents (sudden releases) of hazardous substances, such that the integrated model can cover the assessment of LOC risk to:

- the environment;
- people working onsite;
- the offsite population,

primarily through integrating the evaluation of LOC failure probabilities for different categories of releases.

1.2.2.2 Technical-Management Integration

To base the integrated model on the two major areas of LOC risk control:

- technical (design plus operators)
- management

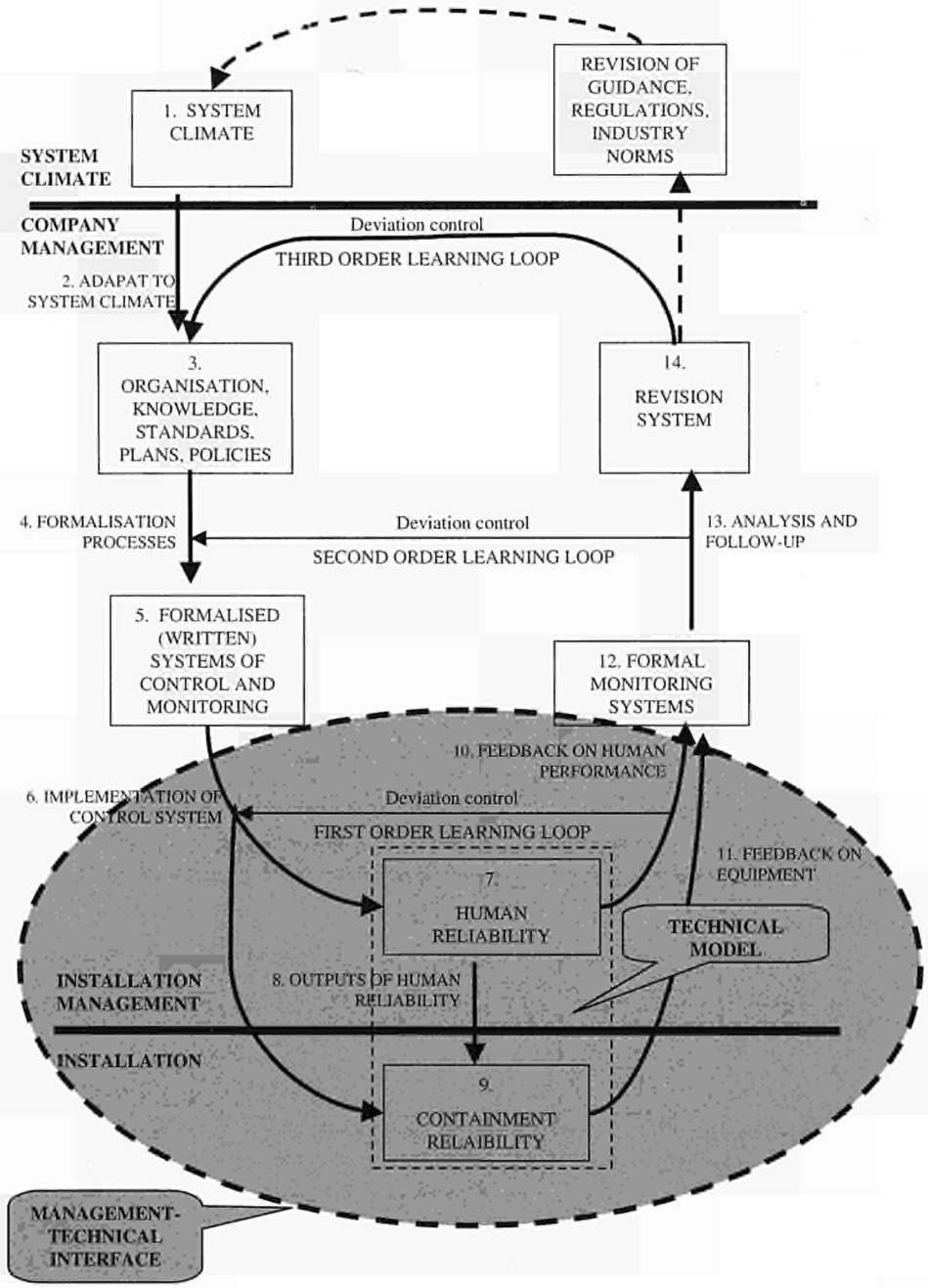
and with the following properties:

- the technical-management interactions must be developed at a point where management exerts a common mode effect;
- the interactions should be modelled in detail;
- the management model should contain components of self monitoring/correcting (continuous and periodic, short term and long term);
- the management model should be able to model time varying components of control/monitoring/correction
- the integrated model should be able to model organisational change (such as changes in manning levels) in terms of effects on failure frequencies.

The starting point for the technical-management interface and the management model was the control and monitoring loop shown in Figure 1-1 (SAVE/SZW 1996).

Figure 1-1

Starting Point for I-Risk Control and Monitoring Loop
(developed from SAVE/SZW 1996)



1.2.2.3 QRA Framework

To develop the integrated model within the framework of Quantitative Risk Assessment (QRA) it should address the following components of the QRA:

1. The plant data collection model.
2. LOC events with the potential to have consequences for:
   - the quality of the environment;
   - the safety of people working onsite;
   - the safety of the offsite population.
3. Parameters of LOC frequency calculation models for releases and their mitigation or escalation.
4. Consequence models insofar as existing models can be used or adapted in the integrated framework (no new models, such as for the environment, will be developed; where models are missing these and the link to the I-QRA will be identifiable).
5. The risk picture:
   - Time varying rather than time averaged; risk projection based on current technical-management status.
   - Show dominant risks so:
     - Risk reduction strategies can be identified.
     - Key performance indicators (management "corrosion monitors") for monitoring risk management effectiveness will be identifiable.
6. It should be possible to investigate the effects of organisational change (such as reduced manning) on risk.

1.2.2.4 Final Products

The final products will be:

1. A suite of models which are the building blocks of the I-Risk methodology of integrated QRA which will include:
   - Technical model
   - Management model
   - Technical-management interface model
   - Time model:
     - Management "corrosion" monitors.
     - Prediction of change in the risk picture over time.

   It should be possible to apply each building block as a stand-alone tool.

2. A field-tested I-Risk QRA procedure, including data collection methods, for site specific application when carrying out such a QRA.

2. METHODOLOGY FOR CARRYING OUT AN I-RISK STUDY

2.1 The I-Risk Model Components

2.1.1 Overview

The objective of the I-Risk project is to quantify the effect of the safety management system (SMS) of an installation on risk, in this case risk of Loss Of Containment (LOC) of hazardous substances. To this effect two general models are developed and quantified:

- A *technical model* incorporating those aspects of risk assessment that are directly affected by the existing hardware along with the associated operating, maintenance and emergency procedures.
- A *management model* incorporating those aspects of the organisation and management of the installation that may affect the performance of people, and indirectly of the hardware.
- In order to couple the management model to the technical model an *interface* was developed between the technical model parameters and the management system components.

The operational procedure for integrating risk is to develop a management model that modifies the various parameters of the technical model. The latter then provides the modified risk measures.

The *technical model*, *management model* and *interface* comprise the key components of the I-Risk model. Section 2.1 further describes these components, then section 2.2 describes the main phases of the I-Risk methodology.

The I-Risk methodology consists of a quantified risk assessment and a management audit. The first step is to establish a base case using generic parameters in the quantification. This quantification includes the establishment of the Master Logic Diagram and the associated fault- and event-trees. Subsequently a management audit is performed. After the management audit has been completed, the following step is to apply the management factors to the parameters that are used in a risk analysis of a chemical plant. This process is explained in detail in section 2.2, while section 3.1 explains the differences with previous models before going on to show how the model is applied in three test cases.

2.1.2 Technical Model

The technical model simulates the performance of hardware and humans in chemical installations. The basic steps of the technical model consist in developing a Master Logic Diagram (MLD) delineating the major immediate causes of Loss of Containment, and Event Tree-Fault Tree Analysis for plant response and assessing the frequency of events. Appropriate management models allow for the quantification of the parameters of the technical model on the basis of the safety management system of the installation.

2.1.2.1 Master Logic Diagram

The basic approach for initiating event identification is the Master Logic Diagram (MLD) technique, as presented by Apostolakis et. al. This is a Logic diagram that resembles a fault tree but without the formal mathematical properties of the latter. It starts with a "Top event" which is the undesired event (like "Loss of Containment")

and it continues decomposing it into simpler contributing events in a way that the events of a certain level will, in some logical combination, cause the events of the level immediately above. The development continues until a level is reached where events directly challenging the various safety functions of the plant are identified. Of interest for chemical installations is the potential for a release of a hazardous substance to the environment. Loss of containment (LOC) means a discontinuity or loss of the pressure boundary between the hazardous substance and the environment, resulting in a release of hazardous substances. A generic MLD for LOC in installations handling hazardous substances is shown in Figure 2-1. This diagram is partly based on the "Generic Fault Trees", presented by van de Mark (1996). There are two major categories of events leading to loss of containment:

- those resulting in a structural failure of the containment, and
- those resulting in containment bypassing because of an inadvertent opening of an engineered discontinuity in the containment.

These major categories are further analysed as shown in Figure 2-1. Most of the events in the last level of development in the tree describe categories of causes that, alone or in some combination, result in a loss of the containment of the hazardous substance. Some of these causes can be further developed into joint events consisting of an initiating event and the failure of one or more safety functions.

2.1.2.2 Event Tree - Fault Tree Analysis

A number of direct causes of LOC can be further analyzed and modeled as a joint event consisting of an "initiating event" and failures of one or more safety functions. Detailed models for these types of direct causes can be built in terms of event-trees and fault trees. For the quantification of the logic models three major categories of parameters must be estimated, namely:

- frequencies of initiating events,
- component unavailabilities, and
- probabilities of human actions,

as presented by Papazoglou et al. (1992).

.1 Frequencies of initiating events

are either estimated directly from historical data or from detailed logic models (e.g. fault trees). This latter approach is necessary when there are dependences among the initiating events and the successful operation of one or more systems.

.2 Components

are distinguished as *continuously monitored* and *non-continuously monitored.*

The state of continuously monitored components is always known and their average unavailability is given as shown in Table 2-1, cases (c) and (d) for non-repairable and repairable components respectively. The state of components that are not continuously monitored can be revealed only through periodic tests. There are four contributions to the unavailability of these components as shown in Table 2-1 case (a). Finally the unavailability of unstable components is given in Table 2-1 case (b).

.3 Human errors

in the logic models are assumed to occur if an operator does not perform an action (foreseen in the operating procedures) and if this error is not detected and recovered by another operator. The probability of this combination equals to:

$H = Q_{01}Q_{02}$

where:

Q_{01} (Probability of not performing the action)

Q_{02} (Probability of not detecting and recovering the error)

2.1.2.3 Accident Sequence Quantification

The next major procedural step of the probabilistic safety assessment includes all the tasks associated with the quantification of accident sequences. This quantification implies the determination in the event trees of the accident sequences to be quantified and their manipulation according to the laws of Boolean algebra. Finally the frequency of the accident sequences is expressed in terms of a number of accident sequences (cut sets) of the form:

$$d = \sum c_i \text{ (rare event approximation)} \quad \text{with} \quad c_i = f_i \cdot \prod_{j=1}^{J} U_j \cdot \prod_{k=1}^{K} H_k$$

Each basic cutset can be expressed in terms of parameters comprising the frequency of initiating event (f_i), a combination of parameters given in Table 2-1 and/or the human error probability of an action (Q_{01}), and the probability of not detecting and recovering the error (Q_{02}).

Table 2-1 Average unavailability for different types of components

a) Periodically tested components $\overline{U} = \overline{U}_1 + \overline{U}_2 + \overline{U}_3 + \overline{U}_4$	
i) Unavailability owing to hardware failure between tests λ:failure rate T: mean time between tests	$\overline{U}_1 = 1 - \frac{1 - e^{-\lambda T}}{\lambda T}$ if $\lambda T << 1$ $\overline{U}_1 \cong \frac{1}{2}\lambda T$
ii) Unavailability owing to repair of detected failures T_R: duration of the repair	$\overline{U}_2 = \frac{e^{-\lambda(T+T_R)} + \lambda(T+T_R) - 1}{\lambda(T+T_R)} \frac{1}{1+(1-e^{-\lambda T_R})e^{-\lambda T}} + \frac{1-e^{-\lambda T_R}}{e^{\lambda T} + 1 - e^{-\lambda T_R}}$ if $\lambda (T + T_R) << 1$ $\overline{U}_2 \approx \frac{1}{2}\lambda T + \lambda T_R$
iii) unavailability owing to routine maintenance f_m: frequency of maintenance T_m: duration of maintenance	$\overline{U}_3 = \overline{U}_2 \frac{1}{1+f_m T_m} + \frac{f_m T_m}{1+f_m T_m}$ if $f_m T_m << 1$ $\overline{U}_3 = \overline{U}_2 + f_m T_m$
iv) unavailability owing to maintenance Q_{M1}:prob. of committing an error Q_{M2}:prob. of not detecting errors	$\overline{U}_4 = \overline{U}_3(1 - Q_{M1}Q_{M2}) + Q_{M1}Q_{M2}$ $Q_{M1}Q_{M2} << 1$ $\overline{U}_4 = \overline{U}_3 + Q_{M1}Q_{M2}$
b) Untested components λ: failure rate T_p: fault exposure time	$\overline{U} = 1 - \frac{1 - e^{-\lambda T_p}}{\lambda T_p}$
c) non repairable monitored components λ_o: failure rate T_M: duration of maintenance	$\overline{U} = 1 - \exp(\lambda_o T_M)$
d) repairable components λ_o: failure rate μ: repair rate	$\overline{U} = \frac{\lambda_o}{\lambda_o + \mu}$

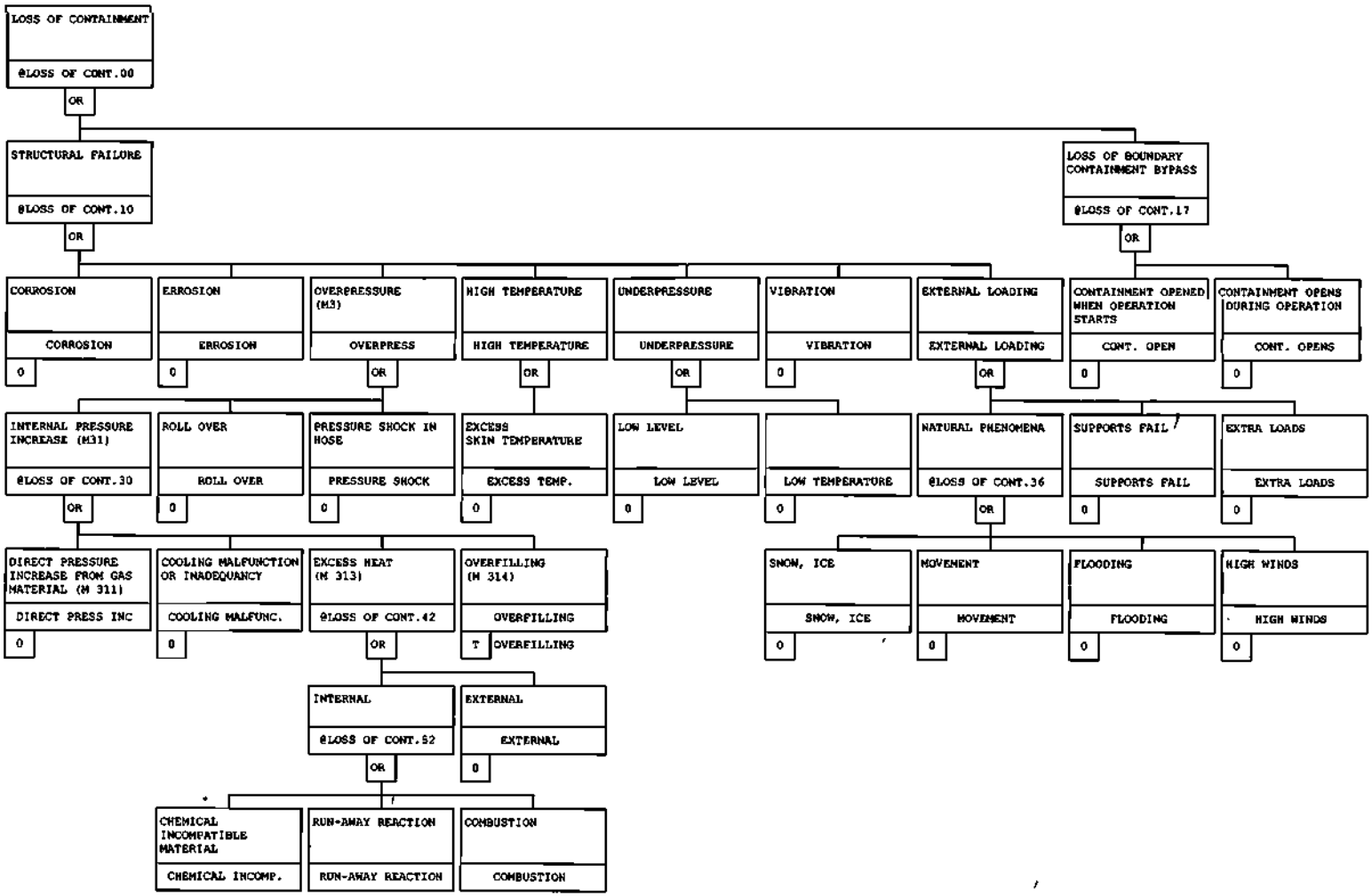


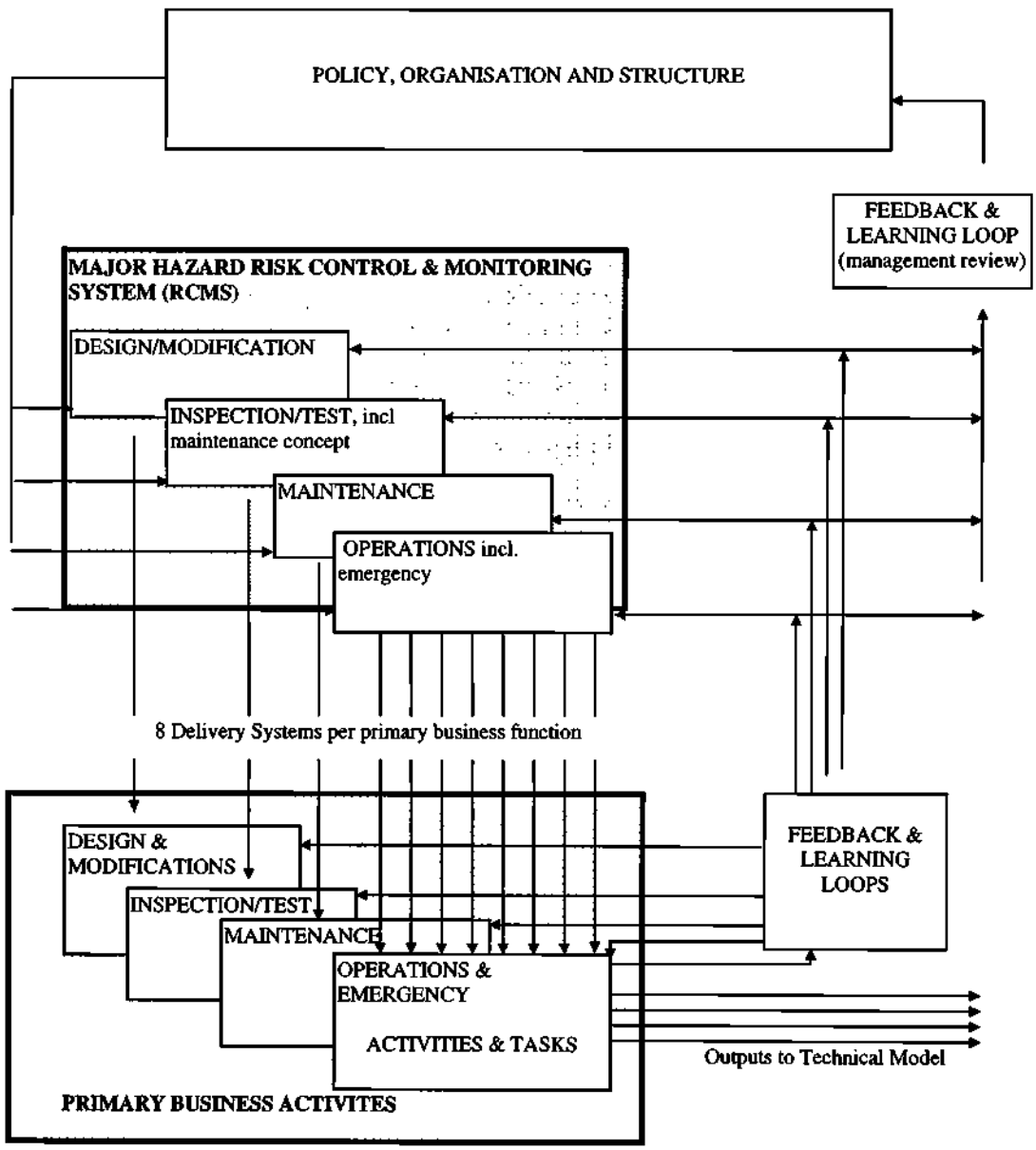
Figure 2-1 Master Logic Diagram for "Loss of Containment" in chemical plants

2.1.3 Management Model

The final management model and audit method developed for the I-Risk project has resulted from a process of development. The model is a combination of the management control and monitoring loops derived from the PRIMA audit (Bellamy et al. 1993, Hurst et al 1996) with the frameworks of the Delft problem solving and SADT (Structured Analysis and Design Technique) models (Hale et al 1997, 1999). Its aim is to focus on the management of major hazards and to distinguish this from the management of other aspects of safety, health and environmental (SHE) management, in order to make very specific links to technical risk modeling. The principles of the management model are generically applicable across the whole area of SHE management, but this application is tailored to major hazards, and specifically loss of containment.

In the model, major hazard safety management is seen as the systematic control and monitoring of the possible scenarios and initiating and base events represented in the risk analysis of the plant as reflected in the technical model. These scenarios and events are a combination of hardware failures and unavailabilities, human errors and miscellaneous initiating events (such as external fires, loss of power, etc.) which are susceptible to a greater or lesser extent to management control. Although this description reflects the I-Risk model structure, management of companies may not see their task quite like this, but in a more holistic way. Hence this description is modified and expanded below. The overall structure of the model is shown in Figure 2-2.

Figure 2-1 Overall Structure of the Management Model



The company exercises control over major hazards by managing a number of primary business functions and activities. For example availability of hardware and, to an extent, its failure rate are controlled by the design and execution of the maintenance regime and function. Failure rates are also influenced by controlling operations, testing and maintenance functions so that the hardware is not taken outside its design envelope and by ensuring that the replacement of parts during maintenance operates on a basis of "like-for-like". Human error, both in omitting necessary control actions and in taking actions which turn out to be incorrect in the circumstances (either through misdiagnosis, mistake or violation of procedures), can be controlled by better management of the activities in which it can occur. The management model therefore centres its attention on the management of the critical parts of these primary business activities as defined by the technical model and its parameters. The link between these two is defined in detail by the tables in the section on the interface (see 2.1.4), in which the management influences per parameter of the technical model are set out.

The primary business functions which the model considers are:

- *operations:* incl. all loading & unloading, supply of power, cooling and all other ancillaries
- *emergency operations*; in which one or more parts of the safety system have been challenged and the situation must be recovered or the damage bemitigated
- *inspection and testing* to assess the condition of hardware, incl. detection of failed stand-by equipment, condition monitoring to decide on preventive maintenance, general detection through walk-around surveys of plant condition and incipient failure
- *maintenance*: covering preventive maintenance and repair
- *modifiactions*:The I-Risk model, in contrast to the PRIMA model, does not include the life cycle phases of design or construction as primary business functions of interest. This is because the technical model represents the plant as built, and hence any shortcomings in the design are reflected in the failure scenarios in the model. However, it is recognised that plants are in a constant state of modification. Constant updating of a technical model would be impracticable.

The primary business functions are controlled proactively by allocating suitable resources to them and by imposing suitable criteria and controls on the way in which they are carried out. The decisions as to what these resources and controls are are taken by the risk control and management system (RCMS). In the case of major hazards this is the system for assessing what the major hazard scenarios are, and for deciding on how they can best be controlled and monitored. It also controls the process of change management. The supply of these resources and controls is governed by secondary management processes, which we have called *delivery systems* in I-Risk. Based on literature review, the modelling experience gained in the project and the systematic logic imposed by the SADT technique, we have grouped these into 8 generic delivery systems, 3 concerned directly with personnel, 2 with hardware and 3 with the way in which the organisation works:

- *Competence*: the knowledge, skills and abilities in the form of first-line and/or back-up personnel who have been selected and trained for the safe execution of the critical primary business functions and activities in the organisation. This system

covers the selection and training function of the company which delivers sufficient staff for overall manpower planning.

- *Availability*: allocating the necessary time (or numbers) of competent people to the safety-critical primary business tasks which have to be carried out. This factor emphasises time-criticality, i.e. people available at the moment (or within the time frame) when the tasks should be carried out. This delivery system singles out the manpower planning aspects, including the planning of work of contractors during major shutdowns and the availability of staff for repair work on critical equipment outside normal work hours, incl. coverage for absence and holidays.
- *Commitment*: the incentives and motivation which personnel have to carry out their tasks and activities with suitable care and alertness, and according to the appropriate safety criteria and procedures specified for the activities by the organisation. This delivery system is fairly closely related to the conflict resolution system (see below), in that it deals with the incentives of individuals carrying out the primary business activities not to choose other criteria above safety, such as ease of working, time saving, social approval, etc. Organisational aspects of conflicts are dealt with there, more personal aspects, such as violation of procedures here.
- *Interface:* The ergonomics of all aspects of the plant which are used/operated by operations, inspection or maintenance. This covers design and layout of control rooms and manually operated equipment, location and design of inspection and test facilities, the maintenance-friendliness of equipment and the ergonomics of the tools used to maintain it. This delivery system covers both the appropriateness of the interface for the activity and the user-friendliness needed to carry out the activities.
- *Spares:* These are the equipment & spares which are installed during maintenance. This delivery system covers both the correctness of the spares for their use (like with like), and the availability of spares when and where needed to carry out the activities.
- *Internal communication and coordination*: Internal communications are those communications which occur implicitly, or explicitly within any primary business activity, i.e. within one task or activity linking to a parameter of the technical model, in order to ensure that the tasks are coordinated and carried out according to the relevant criteria. This delivery system is only relevant if the activity is carried out by more than one person (or group), who have to coordinate or plan joint activities.
- *Conflict resolution*: The mechanisms (such as supervision, monitoring, procedures, learning, group discussion) by which potential and actual conflicts between safety and other criteria in the allocation and use of personnel, hardware and other resources are recognised, avoided or resolved if they occur. This delivery system is closely related to the one concerned with commitment. The issues of violations within tasks at an individual level are covered there. This system covers the organisational mechanisms for resolving conflicts across tasks, between people at operational level and at management level.
- *Procedures, Output goals and Plans:* Rules and procedures are specific performance criteria which specify in detail, usually in written form[1], a formalised "normative" behaviour or method for carrying out an activity (checklist, task list,

[1] In work groups which work intensively together rules and procedures may be unwritten, but known and used by all concerned in every other way as though they were written.

action steps, plan, instruction manual, fault-finding heuristic, form to be completed, etc.). Output goals are performance measures for an activity which specify what the result of the activity should be, but not how the results should be achieved. They are objectives, goals or outputs (e.g. accident/incident targets or trends, exposure of risk levels, ALARA, "safe", numbers of activities carried out, etc.). It is also convenient to regard definitions and criteria for choosing one course of action over another as output criteria. Plans refer to explicit planning of activities in time, either how frequently tasks should be done, or when and by whom they will be done within a particular time period (month, shutdown period, etc.). They include the maintenance regime, maintenance scheduling (including shutdown planning) and testing and inspection activities, which need to link to the parameters of maintenance frequency, test interval and time for maintenance and repair.

These delivery systems are modelled to show how the resources and controls are delivered to the primary business activities, which directly influence the technical risk parameters. The delivery systems themselves also require resources and controls for their correct and efficient functioning, but we do not show these flows in the model, since this would lead us into an infinite regression of delivery systems to delivery systems. The quality of the resources and controls to run each delivery system, e.g. the competence of personnel for all the tasks involved in it, is therefore subsumed within it. Hence, communication between the tasks which are represented in the delivery systems are also not included in the "communications and coordination" delivery system, but are represented by the continuity of the loops for those delivery systems (see below).

Finally, the major hazard management system contains elements which control reactively. These consist of the steps of recording and analysing system performance, including deviations and incidents, and learning from this monitoring to improve control. These feedback and learning loops (FLLs) operate at several levels:

- *correction*: on-line detection of deviation and correction, incl. task checking.
- *local improvement*: adapting the output of one delivery system to make it better suited to controlling hazards in a particular situation
- *delivery system improvement*: modifying any of the delivery systems to function better across a number of situations
- *overall system review and improvement*: reassessment of the whole major hazard RCMS and the structure that it drives, in response to major failure, dissatisfaction or signals that a step change in performance is required. Under this heading falls the change management system.

The policy, RCMS, the 8 delivery systems and the FLLs all consist of a number of management tasks which must be carried out systematically and competently in order to deliver the appropriate control or resource to the appropriate primary business activity at the opportune time, and to learn and improve on that delivery process over time. These tasks are modelled as boxes linked by arrows in loops, as shown in Figure 2-2, which shows the general management loop in summary form.

Where a box has a second outline box behind it, this is intended to indicate that the box is duplicated for all of the 8 delivery systems. Where the box is single, it is

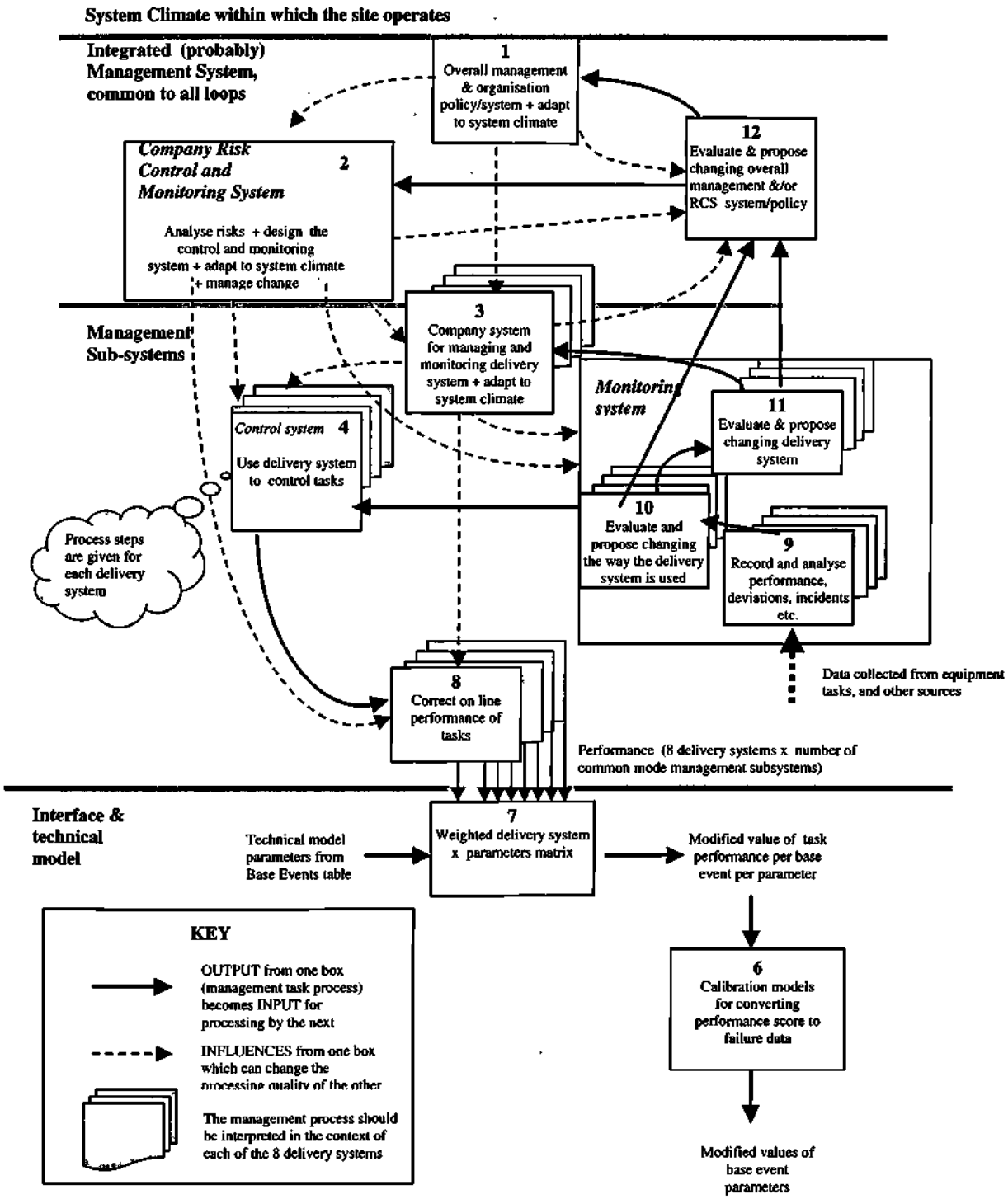
normal to find the activity in most companies operating as one system for all or most of the 8 delivery systems.

The tasks and activities for each box in the model are summarised in the list of topics per box used as prompts during the I-Risk audit .

For the purposes of quantification (see section 2.2.4 and 2.2.5 for further details) a distinction is made in the loops between three different types of relationship between boxes in the loops.

1. One box may provide an output which is used as an *input* to the next box, and which is processed by that box. For example, the control system (box 4) provides resources or controls to be used in the task at hand (box 8 - and 7). The quality of the input partly determines the quality of the output of the next box.
2. One box may have an *influence* on the way another works, by providing it with structure, resources or criteria. For example, the RCMS (box 2) plays a central role in setting up the processes by which the system monitors and learns from experience (boxes 9-12). This influence changes the state of the next box in a more or less permanent way, at least for a period of weeks or months, and so determines the quality with which the box turns inputs into outputs.
3. Finally data about the performance of a box may be used in another box without determining the quality of the output of that box. This is the case with box 9, which collects information from many other boxes in the management system, but whose quality of functioning does not necessarily depend on how well all those other boxes are working.

Figure 2-1: General Management Loop for IRMA (Integrated Risk Management Audit)



These different relationships are shown by different types of line in Figure 2-2. For the purpose of auditing this distinction in types of relationship is not so relevant. The audit concentrates on assessing the boxes and the integrity of the loops connecting them.

Although the general management loop and its elements are relatively straight forward, their application across all of the critical activities to control major hazards leads to a complex and sizeable set of activities (boxes) relevant to the whole safety management system. Each delivery system has its own version of the loop (seeAnnex II, Section 7). Each parameter in the technical model has its own set of 8 delivery system loops influencing the quality of performance of the tasks which manage the parameter. Finally the parameters represent tasks in all of the different life cycle phases represented by the primary business functions (modifications, inspection/testing, maintenance and operations and emergency). In total there are, thus, many hundreds of tasks (and hence boxes) which need to be assessed to get a full picture of the functioning of the major hazard management system of a company. This reflects the reality of major hazard control, which is a process involving almost all the employees of a company and pervading a large part of their work time and activity.

It is the task of the I-Risk audit to reduce this complexity to a manageable degree, so that the management system can be audited sufficiently in a reasonable length of time to be practicable. This reduction is sought in two ways:

1. concentration only on those tasks which are crucial to major hazard control, and not on those relating to other aspects of safety, health and environment.
2. simplifying the model by identifying within the management system of any given site the way in which control tasks for many different hazard scenarios, base events and technical parameters have been grouped together in common management systems. This degree of overlap is referred to in this report as *common mode*. This term has been deliberately chosen to link with the usage in technical risk assessment. In assessing fault trees, common mode is used to describe underlying factors which link separate branches of a fault tree and so breach the rule that such branches should be independent for the purposes of quantification. In that respect it has a negative connotation. In using it in describing the management mode, we give it a positive connotation. Management systems are designed to manage all scenarios and base events in such a way that all will have the lowest practicable probability. This is done by applying the same (excellent) quality of maintenance procedures, operating competence, safety commitment, well designed interface, etc. to all of them. We postulate that an excellent major hazard management system will manage all of its parts, including all of its delivery systems and feedback and learning loops in the same excellent way across all of their applications. If this is the case, it would only be necessary to audit and assess each delivery system and associated feedback loops once for the whole site. That assessment would be valid for all parts of the site. In practice most companies do not have that degree of common mode. Different parts of the company (e.g. the maintenance department as opposed to the operations departments, contractors as opposed to own maintenance staff) are managed in different ways and to different standards. At the other end of the spectrum, a company with no coordinating (major hazard) management system will function very differently in each of its sections and activities, depending on the local quality of staff and provisions. Such a company would need to be audited in detail in all parts to make an assessment of

the management quality for each technical parameter. The audit therefore has to determine, in an early stage, how much common mode there is at a particular company, in order to decide how many times each delivery system and feedback loop has to be assessed in the audit.

The site management audit collects information about the quality of the company management of the overall major hazard management system, and in particular of the delivery of critical controls and resources to the specific parts of the primary business processes relevant to the parameters involved in the scenarios of loss of containment which the technical model has identified as being possible for that site. This information enables the auditing team to make an assessment of the quality of each of the boxes in the various delivery system loops in the management model. These scores are used to assess the management of each technical parameter. How that is done is described in detail in section 2.2.

In summary, the scores for the boxes in each delivery system for each relevant primary business activity per technical parameter are combined to give a score for the quality of that control or resource for that technical parameter. The scores of the 8 different delivery systems for that technical parameter are then combined to give an assessment of the quality of the management of that parameter compared to an average company. These scores are then used to select a figure for the probabilities or frequencies of the errors or failures or for the equipment unavailabilities associated with each base and initiating event. This is chosen from the range around the default generic figures deriving from industry wide databases.

2.1.4 Management-Technical Interface

The effect of management on the technical system that controls the major hazards is the primary concern of the I-Risk Interface model. This effect is modelled through the chance component of the risk equation (where risk = Σ chance x consequence). In risk analysis the chance component may be based on historical data, manufacturer's data, actual site specific data, or judgement in order to make predictions for a specific case.

The effects of management may increase or decrease the chance of an event compared to the generic data. In an integrated risk assessment the idea is to take the assessed state of the management system into account in the calculation of the frequencies of LOC which are usually based on generic data. While this was a consideration in the PRIMA audit (EU Contract Research Report (1995)), there was no interface between the management system and the technical system which would allow the tasks of the management system to be directly linked to aspects of the technical system which they control. The purpose of the I-Risk interface is to link the relevant aspects of an integrated (usually) risk management system to a model of the risks that are being managed.

2.1.4.1 Linking between output quality of the management system deliveries and the base event parameters

For the case of major hazards, which we are dealing with in this project, the management system has been linked to the 10 parameters of the model of the technical system which are used to quantify the Loss of Containment risks (Table 2-2). This linking process actually determines the specific content of the aspects of the Risk Control and Monitoring system in which we are interested. The idea that was

agreed upon was to assess the quality of the management system for each of the parameters of the base events of fault trees constructed in the technical model. In the process of making the link certain factors had to be considered such as:

1. The Management Team must understand the parameters and equations provided by the Technical Team because that is crucial to understanding how and whether the technical parameters can be linked to the Management Model (see section 2.1.2.3 and Table 2-1). For example, the team had to understand that lambda represented a reciprocal of the mean time between failure with only two conditions – failed and not failed. In this respect, the management team could not consider management control behaviour, which examined intermediate states of the component. In cases where the management system was known to carry out safety related tasks that could not be linked to the technical model, this gave rise to new developments on the Technical Model side
2. The nature of the quantitative data for defining the parameter must be known. For example, if a site has site-specific data (such as for frequency of maintenance) then it is a question of whether management keeps to the specified data. The management model could determine whether the company is likely to be good at meeting its own targets for the frequency of maintenance, and whether it is good at defining its own maintenance policy in such a way that it learns to improve the target frequencies. If the data is historical, as with the failure rate (λ), then we need to consider how management may increase the failure rate (such as by replacement with a poorer component) or decrease it (such as by improved components.
3. If management is good, it must always have a positive effect on the risk through the parameter. This means that, for example, safe behaviour cannot be considered to increase unavailability (e.g. the time consuming part of making a system safe).
4. The base events generated by the Technical Model should be displayed in a matrix indicating all their relevant parameters and grouped as far as possible into organisationally rational groups (such as 'electrical'). See, for example, Table 2-1 which also shows organisational groups of Company A which were linked to the base events. Together with a base event table, the Management Team need to know what the Scenarios are (combinations of base events) and possible consequences. This structure helps both with applications of scenario specific audit questions, and with considerations of possible common modes .

Table 2-1 Example of a base event table (Test Case A). Continued

NAME	DESCRIPTION	ORGANISATION	EQUATION	FAILURE RATE (λ)	FREQUENCY (fi)	Qo1	Qo2	T	fm	Tm	T_r	QM1	QM2
	A) HUMAN ERRORS												
AIRLINE NOT ENGAGED	AIRLINE NOT ENGAGED	Company A Operating Team = Operators, supervisor, shift manager	3.13			x	x						
CHOCKS NOT USED	CHOCKS HAVE NOT BEEN USED	Company A Operating Team	3.13			x	x						
DRIVER DOESN'T STOP	DRIVER DOESN'T STOP THE MOVEMENT OF THE TANKER	Tanker Driver	3.13			x	x						
OP. FAILS TO DIAG.	OPERATOR FAILS TO DIAGNOSE TANKER MOVEMENT	Company A Operating Team	3.13			x	x						
OPERATOR DISCONECS	OPERATOR DISCONNECTS WHILE LOADING	Company A Operating Team	3.13			x	x						
OPERATOR ERROR (B)	BARRIER IS UP, OWING TO OPERATOR ERROR	Company A Operating Team	3.13			x	x						
OPERATOR ERROR CON	OPERATOR ERROR IN CONNECTING THE HOSE	Tanker Driver	3.13			x	x						
OPERATOR FAIL M	OPERATOR FAILS TO CLOSE MANUAL VALVE ON TANKER	Tanker Driver	3.13			x	x						
OPERATOR FAILS	OPERATOR FAILS TO CLOSE ACTUATED VALVE	Company A Operating Team	3.13			x	x						

Table 2-1 Example of a base event table (Test Case A). Continued

NAME	DESCRIPTION	ORGANISATION	EQUATION	FAILURE RATE (λ)	FREQUENCY (fi)	Qo1	Qo2	T	fm	Tm	T_r	QM1	QM2
	B) STANDBY COMPONENTS												
	I) VALVES												
RELIEF IN V. FAILS	RELIEF SYSTEM IN VESSEL FAILURE(*)	Company A Plant Engineer + Maintenance Team = Maintenance supervisor and fitters	3.9	x				x	-	-	-	x	x
RELIEF PRESSURE F.	RELIEF SYSTEM IN TANKER FAILURE (*)	Tanker Company	3.9	x				x	-	-	-	x	x
ROSOV FAILURE	ROSOV FAIL TO CLOSE (*)	Tanker Company	3.9	x				x	-	-	-	x	x
VALVE FAILS TO CLD	ACTUATED VALVE ON TANKER FAILS TO CLOSE	Tanker Company	3.9	x				x	-	-	-	x	x
VALVE ON TANK FAIL	MANUAL VALVE ON TANKER FAILS TO CLOSE	Tanker Company	3.9	x				x	-	-	-	x	x
MANUAL VALVE F.	MANUAL VALVE ON TANKER FAILS TO CLOSE	Tanker Company	3.9	x				x	-	-	-	x	x
	II) MECHANICAL COMPONENTS												
COUPLING FAILURE	COUPLING MECHANICAL FAILURE	Company A Plant Engineer + Maintenance Team	3.9	x				x	-	-	-	x	x
CHOCKS INADEQUATE	CHOCKS CANNOT STOP TANK MOVEMENT	Company A Operating Team	3.9	x				x	-	-	-	x	x
BARRIER FAILURE	BARRIER IN FRONT OF THE TANKER HAS FAILED IN UP POSITION	Company A Operating Team + Maintenance Team	3.9	x				x	-	-	-	x	x

Table 2-1 Example of a base event table (Test Case A). Continued

NAME	DESCRIPTION	ORGANISATION	EQUATION	FAILURE RATE (λ)	FREQUENCY (fi)	Qo1	Qo2	T	fm	Tm	T_t	QM1	QM2
	iii) INSTRUMENTATION												
DETECTOR FAILURE	MOVEMENT DETECTOR HAS FAILED	Company A Maintenance Team	3.9	x				x	?	?	?	x	x
OVERFILLING SAFETY	OVERFILLING SAFETY SYSTEM FAILURE(*)	Company A Operating Team + Maintenance Team	3.9	x				x	?	?	?	x	x
PUSH BUTTON FAIL.	PUSH BUTTON (FOR ESD) FAILURE	Company A Maintenance Team	3.9	x				x	-	-	-	x	x
AIR SYS WRONG SIGS	AIR SYSTEM SENDS WRONG SIGNAL TO ESD	Company A Maintenance Team	3.9	x				x	-	-	-	x	x
INTERLOCK BRAKING	INTERLOCK IN TANKER BRAKING SYSTEM HAS FAILED	Tanker Company	3.9	x				x	-	-	-	x	x
	iv) OTHER COMPONENTS												
AGEING OF HOSE	HOSE UNABLE TO MAINTAIN PRESSURE BOUNDARY INTEGRITY OWING TO CORROSION	Company A Operations Team + Company A Maintenance Team	3.9	x				x	0	0	0	x	x

Table 2-2: Basic Event Parameters of the Technical Model

f_i:	Frequency of initiating events (not human errors)
λ_s, λ_O :	Failure rate of unmonitored (standby) or monitored components
T:	Time between testing
Q_{M1}:	Error in test and repair
Q_{M2}:	Failure to detect and recover previous error in test and repair
f_M:	Frequency of routine maintenance
T_M:	Duration of routine maintenance
T_R:	Duration of repair
Q_{O1}:	Probability of error in operations or emergency
Q_{O2}:	Probability of not detecting and recovering error

It is important to understand that the management model as developed (see Figure 2-2) could be applied to the management of any risk control system, not just major hazards. By creating an interface between the management and the technical system, we constrain our consideration of the management system to those factors of interest in controlling and monitoring the specific risks under consideration, in this case major hazards in chemical manufacturing which impact on safety and environment (this is the focus of the Seveso II Directive). With the management model that we have developed, it would also be possible to make an interface with other risks (project risks, financial risks, health risks, environmental risks etc.) providing those risks have a defined calculation model. The general procedure and principles are basically the same.

In the PRIMA (EU Contract Research Report, 1995) and AVRIM2 (SAVE/SZW 1996) management models, the technical system was linked to the management system through the output of human actions at the 'workface' (designers, construction workers, operators, maintenance technicians), as shown in Figure 1-1. In PRIMA, the modification of risk in the technical model was at the level of generic failure rates for top events (such as pipe rupture) based on an overall qualitative assessment of the quality of the management loop.

The output of the I-Risk management system into the interface is the result of a series of management processes that are assessed and quantified for each *delivery system.* The final output of the management system emerges from local feedback and adjustment processes in task execution made at the workface (Figure 2-2). These final outputs are connect in the interface to the parameters of the technical model at the level of the base events of the fault trees. Figure 2-1 illustrates this principles of the I-Risk interface (where I=Input, O=Output, and fm and fi are examples of base event parameters). A, B, C and D represent common mode (common quality) organisational groups of the management system (such as electrical maintenance as opposed to mechanical, say). The single output from each of these qualitatively

different management systems is linked to base event parameters (such as frequency of maintenance, fm) in such a way that parameters common across base events (such as fm) are grouped together when they have a common mode management system. In this respect, if the management system has a common quality across all its managed functions then all maintenance frequency values, for example, will be subject to a common modifying factor. This is a basic principle of the I-Risk interface.

For each of the 10 parameters shown in Table 2-2 the basis of the technical model data was clearly defined, for example whether it was generic (such as for 8) or plant specific (such as for T). The relevant management aspects were identified, for example whether the maintenance frequency specified by the plant is kept to or whether management increase or decrease it.

It follows, logically, that if the parameters of the technical model are used to model the major hazard risks, and if these parameters are going to be affected in some way by the quality of the management system, then the content of the connections flowing to the management system form a basis for the demands and constraints on what is looked at in the management system.

There are a number of things that a management system controls in relation to the different values that a parameter can take. These parameter-influencing factors were considered at a detailed level for each parameter using a method of categorising the components of the parameters. For example for time for repair this could include:

1 Waiting Time Prior To Repair

1.1 Waiting for the "making safe" activity to begin
1.2 Waiting for people who can get access to the component and/or do the repair job
1.3 Waiting for access equipment and/or spares and/or tools
1.4 Waiting for turn in the access/repair schedule
1.5 Waiting for diagnosis of what component has failed

2 Accessing and Replacing Time

2.1 Time to make safe dependent on the design for isolation
2.2 Time for constructing access to item to be repaired (and removing it if this has to be done before item can be brought back into service)
2.3 Time to remove/replace item
2.4 Time to transfer to repair shop and return it to location, before and after repair

3 Time To Do The Repair

3.1 Time for problem diagnosis
3.2 Time required for the repair/replace procedure, including use of equipment and type of repair/replacement done
3.3 Dead time due to shift hand-over

3.4 Dead time due to other jobs taking priority/interfering (rescheduling)

4 Time For Return To Service
4.1 Time to carry out testing, which is dependent on the design for testing
4.2 Time to return to service, which is dependent on the design for returning to service
4.3 Waiting for turn in the schedule
4.4 Waiting for people/equipment for returning it to service

The associated management tasks (which are mainly concerned with Box 4 processes in Figure 2-2) were identified and grouped according to the relevant management delivery systems. This is shown in detail in Annex III. For example, for the routine maintenance frequency, fm, the *Communications* delivery system influences included: communication of schedules, of priorities, and unambiguous instructions on scheduling.

These parameter-influencing factors were different for each parameter and the number of factors varied between delivery systems for each parameter. Counting the number of parameter influencing factors for each parameter, and then expressing the number for each delivery system as a proportion, enabled every delivery system to be weighted in importance for each parameter. This was a very rough and ready calculation which provided us with default values for our model, quite simply based on the number of things thought of by the experts. There is a need for more work here to establish a sounder basis for the weightings (such as expert judgement methods being applied by the TU Delft Safety Science group).

The result giving the default weightings is shown in Table 2-3 and provides a conversion table for apportioning the quantified outputs of the management system deliveries to the parameters.

The basic principles involved in building an I-Risk interface can be summarised as:

1. Identifying the relevant parameters in the technical model that determine the quantification of the probability or frequency of events.
2. Specifying the nature (underlying assumptions) of the technical parameter data so that the management aspects to which the data are sensitive can be identified. In other words, what aspects of the data specification are modifiable and what not. For example, generic equipment repair times that are found in databases do not include the waiting time for spare parts. Or, the generic failure rate of a component does not include consideration of changes in assumed internal conditions.
3. Specifying how the use of management delivery systems can affect the parameters of the technical model.
4. Quantifying the relative importance of the delivery systems in terms of the effects on the parameters.

Figure 2-1 Management- Technical Interface Model (see text)

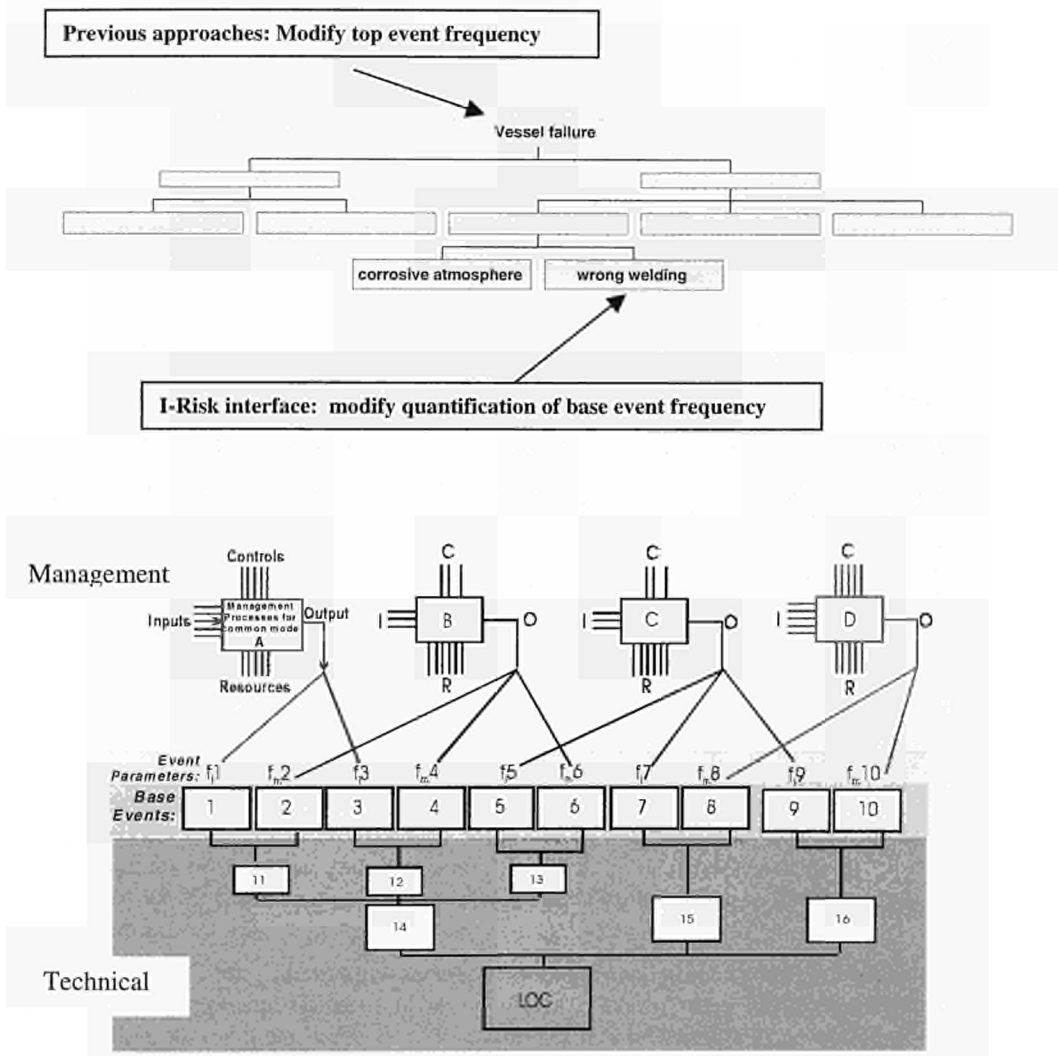


Table 2-3 Delivery systems that affect basic event parameters of a common mode management system (the values shown are the default proportional importance weightings of each delivery system per component)

Delivery systems	Basic event parameters										
	Qo1	*Qo2*	*Qm1*	*Qm2*	*fi*	λ	*T*	*fm*	*Tr*	*Tm*	*Total*
Availability	0,06	0,05	0,08	0,05	0,1	0,08	0,05	0,05	0,12	0,12	0,76
Commitment	0,15	0,14	0,19	0,13	0,2	0,12	0,24	0,21	0,07	0,08	1,53
Communication	0,07	0,05	0,06	0,05	0,1	0,12	0,14	0,16	0,21	0,21	1,17
Competence	0,16	0,21	0,14	0,22	0,1	0,08	0	0	0,09	0,08	1,08
Conflict resolution	0,18	0,21	0,14	0,18	0,1	0,08	0,28	0,32	0,10	0,12	1,71
Interface	0,20	0,20	0,08	0,18	0	0,08	0,05	0,05	0,19	0,17	1,2
Procedures	0,18	0,14	0,17	0,15	0,4	0,16	0,19	0,16	0,10	0,08	1,73
Spares & tools	0	0	0,14	0,04	0	0,28	0,05	0,05	0,12	0,14	0,82

2.2 Overview Of Step by Step Procedure

The methodology and procedures to be followed for the quantification of integrated risk from installations handling toxic or flammable substances can be distinguished into four major phases:

1. Assessment of Plant Damage States and their Frequency of occurrence.
2. Assessment of the Safety Management System (SMS) of an installation
3. Modification of the frequencies of plant damage states, according to the characteristics of the safety management system.
4. Assessment of Consequences of Toxic or Flammable Substances Release.
5. Risk Integration.

2.3 Phase 1: Assessment of Plant-Damage States and their Frequency of Occurrence

The first phase of an integrated risk assessment consists in analysing the installation to identify potential accident initiators, assess the response of the plant to these initiators and establish end damage states of the plant resulting in the release of a dangerous substance in the environment. Furthermore, the frequency with which the identified plant damage states are expected to occur is estimated.

This phase can be distinguished in the following five procedural tasks:

a) Hazard source identification

The main sources of potential hazardous-substance releases are identified and the initiating events that can cause such releases are determined.

b) Accident Sequence Determination

A logic model for the installation is developed in this step. The model includes each and every initiator of potential accidents and the response to the installation to these initiators. Specific accident sequences are defined (in models called event trees) which consist of an initiating event, specific system failures or successes and their timing, and human responses. Accident sequences result in plant damage states that involve release of the hazardous substance.

System failures are in turn modelled (in models called fault trees) in terms of basic component failures and human errors to identify their basic causes and to allow for the quantification of the system failure probabilities and accident sequence frequencies.

c) Plant Damage State Definition

A plant damage state uniquely characterises the installation-dependent conditions of release of the hazardous substance. Accident sequences resulting in the same conditions of release are formed into groups each corresponding to a particular plant damage state.

d) Parameter Assessment

Parameters which must be estimated include the frequencies of the initiating events, (external events, human errors, component failures) component unavailability and probabilities of human actions. Estimation of these parameters is based on generic values.

e) Accident Sequence and Plant Damage State Quantification

This task quantifies the accident sequences and the plant damage states that is, calculates their frequency of occurrence. In particular, the plant model built in the second step is quantified using the parameter values estimated in the fourth task. Accident sequences to be quantified in the event trees are specified and manipulated according to the laws of Boolean algebra in order to be put in a form suitable for quantification. The results of this task is the calculation of the frequency of occurrence of each accident sequence and consequently of each plant damage state. This last step is repeated again with the modified values of the parameters as described in the third major phase.

Details on these procedural tasks are given in steps I.1 to I.16.

Once the plant damage states and their frequencies are established, the consequences to the public and worker's health must be established. It is not necessary to estimate consequences for each and every plant-damage state. A screening procedure can be followed where only those plant damage states with significant frequency (e.g. $\geq 10^{-9}$/years) will be retained. Caution must be exercised, however, to avoid excluding states with extremely severe consequences. Alternatively, some people prefer to calculate consequences for all identified plant damage states prior to the frequency estimation. Then, frequency calculations are performed only for those states with non-negligible consequences.

These alternative approaches are depicted in Figure 2-1 where frequency estimation and consequence assessment are shown in parallel paths in the flowchart format of the procedural steps.

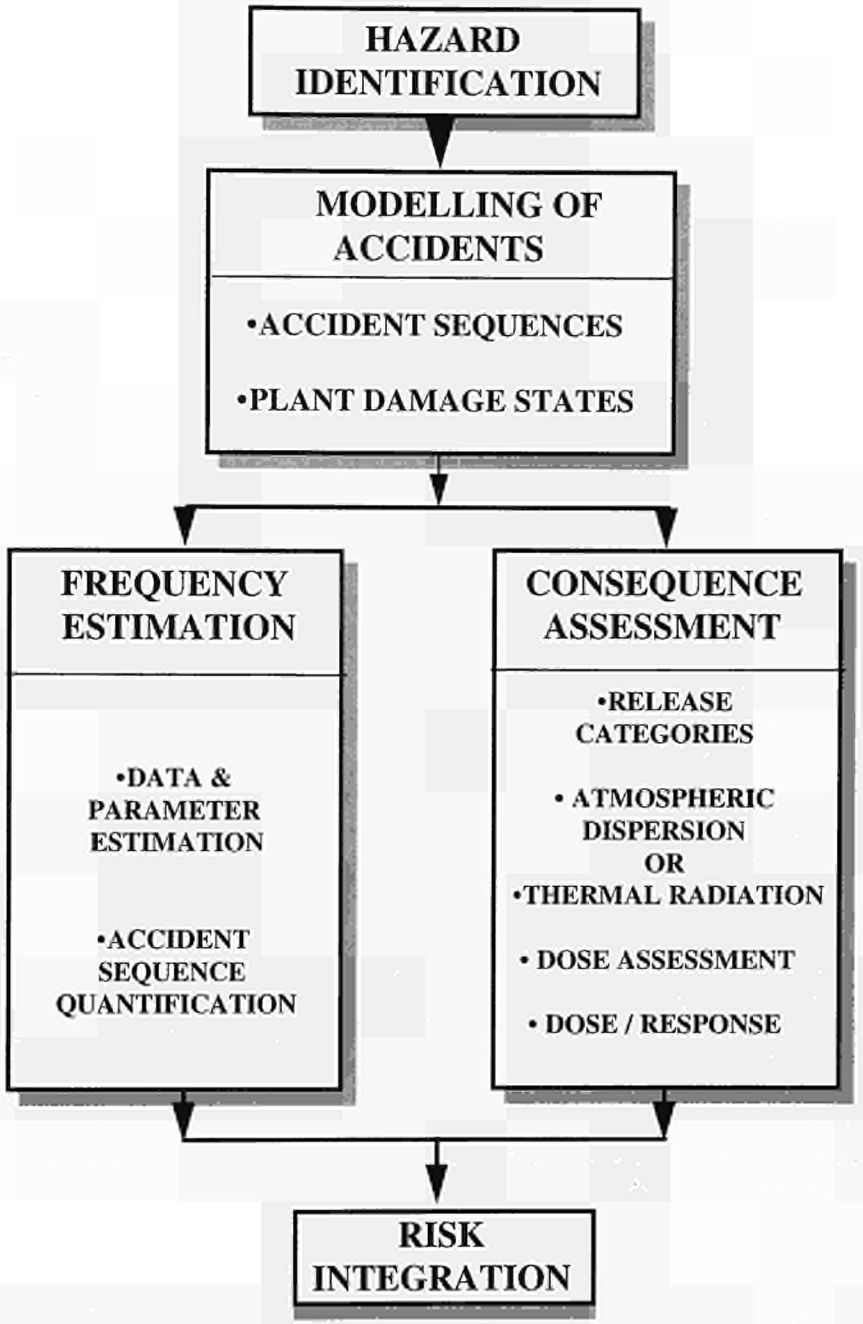


Figure 2-1 Procedural Steps for Risk Assessment in Chemical Installation

2.3.1 Hazard source Identification

The main objective of this task is to identify the release sources in the installation and the initiating events that can lead to these releases of this ammonia to the environment. The methodological task of hazard identification, which is of major importance to the chemical industries owing to the large number and variety of the chemical processes, can be distinguished in the following nine steps:

2.3.1.1 Step I.1 Plant Familiarisation and Information Gathering

This step involves the familiarisation of the analysts with the plant design and operation. This includes a study of the plant documentation supplied by the plant and an installation visit and communication with the appropriate personnel.

2.3.1.2 Step I.2 Identification of Release Sources of Concern

The aim here is to identify all possible sources of release (within the boundary of the study). To this end, the installation is divided into subcompartments, each representing a possible release source.

2.3.1.3 Step I.3 Identification of Plant Operating States of Concern

Consideration of all operating states of the facility is necessary since it affects the possible release sources, release mode, as well as the amount of the released substance.

2.3.1.4 Step I.4 Initiating Event Selection

The possible events, which create a disturbance in the installation and have the potential to lead to the release of toxic or flammable gas are identified and listed. The aim is to make this list as complete as possible, including events beyond the design basis of the plant. Three different approaches, namely the Master Logic Diagrams, the use of check lists and the HAZOP analysis, may be followed for the identification of the initiating events. The application of the Generic Master Logic Diagram for Loss of containment presented by Papazoglou and Aneziris(1998), results in the identification of a list of initiating events.

2.3.1.5 Step I.5 Safety Functions

For each initiating event listed in the previous task the safety functions which are required to prevent the occurrence of toxic or flammable gas release are identified. This step is actually performed interactively with the construction of the Master Logic Diagram, which requires the definition of the safety functions.

2.3.1.6 Step I.6 Function - System Relationship

The **frontline** systems, i.e. the systems that directly serve each safety function (e.g. Refrigeration system, fire fighting system, pressure control system etc) are identified along with their **support** systems, i.e. systems on which the frontline systems depend for proper function (e.g. AC power, DC power, cooling water, lube oil etc). Functional dependencies among frontline systems through common support systems are identified.

2.3.1.7 Step I.7 Plant System Requirements

This task assesses the performance requirements (success criteria) imposed on the various frontline systems by each initiating event (e.g. two out of three compressors working). In addition, it determines any special conditions which the initiating events create for support systems, on the symptoms displayed to the operator, etc.

2.3.1.8 Step I.8 Grouping of Initiating Events

The initiating events are grouped in such a way that the members of each group impose the same success criteria on the front line systems and similar special conditions on the rest of the plant.

2.3.1.9 Step I.9 Screening of Initiating Events

Groups of initiating events are screened for further analysis. Two criteria are used in general, namely the frequency and the magnitude of possible consequences. If the frequency of a group of initiating events is too low then they are excluded from further consideration. The same is done if the possible consequences (assuming the initiating event has indeed occurred) are of negligible magnitude.

2.3.2 Accident Sequence Determination

In this procedural task, a model is constructed which defines the initiators of potential accidents, the response of the plant to these initiators, and the spectrum of the resulting plant-damage states. Specific accident sequences are defined which consist of an initiating event group, specific system failures and successes and their timings and human responses, which then produce a plant damage state. The system failures are in turn modeled in terms of basic component failures and human errors in order to identify their basic causes and allow for the quantification of the system failure probabilities and accident sequence frequencies. The methodological task of Accident Sequence Modeling can be distinguished in the following four steps:

2.3.2.1 Step I.10 Event Sequence Modeling

This step determines the response of the plant to each and every group of initiating events. The response includes the systems that are called upon to respond and the corresponding required actions, human actions, etc. The combinations of the initiating event with successful or failed system and human responses are assessed,

producing event sequences. These sequences lead to either a successful control or mitigation of the initiating event, or to an abnormal event (release of ammonia). In the latter case the event sequences are called accident sequences and are depicted through the construction of the appropriate Event Tree (see NUREG/CR-2815 (1984), PSA (1985), IAEA(1995)).

2.3.2.2 Step I.11 System Modeling

This step develops the models defining the various ways the systems can fail or succeed which produces the events identified in the event sequence modelling. Fault tree techniques are used for system modelling for this phase of the work. Corrosion is the only direct cause of loss of containment that is not amenable to a treatment via the Fault Tree Analysis. A multistate Markov model is used for quantification of this event (see Papazoglou and Aneziris(1998)).

2.3.2.3 Step I.12 Human Performance Analysis

The human response to the initiating events and to subsequent system responses are analysed in this step. Pre- and Post-accident human actions are considered and decisions are made on the human actions to be included in the event trees - as being important for the course of the accident - or in the fault trees - because they affect the accident sequence only through their effect on the operability of the system.

2.3.2.4 Step I.13 Classification of Accident Sequences into Plant Damage States

Accident sequences that cause similar damages into the installation are grouped into plant-damage states. The similarity refers to the failure mode of the installation as it affects the release of the hazardous substance.

In general there might be at least three damage states in a plant with toxic substances either in liquid or in gas phase:

- Tank failure, partial or catastrophic
- Pipe failure connected to a tank, partial or catastrophic
- Pipe failure connected to a pump, partial or catastrophic

The possible plant damage states for flammable substances are the following:

- Break of a tank with flammable liquid, partial or catastrophic
- Break of a pipe with flammable liquid
- BLEVE of a tank with liquefied gas under pressure
- Break of a tank with liquefied gas
- Break of a pipe with liquefied gas
- Break of a tank with pressurized gas
- Break of a pipe with pressurized gas

2.3.2.5 *Step I.14 Parameter assessment*

For the quantification of the logic models described above major categories of parameters must be estimated, namely frequencies of initiating events, component unavailabilities and probabilities of human actions.

2.3.2.6 *Initiating events*

Initiating events might be either external events, or human errors, or components failures. Frequencies of external initiating events can be estimated from generic data. If there are dependencies among the initiating events and the successful operation of one or more front-line systems, or simpler events (e.g. component failures) contribute both to the occurrence of the initiating event and the failure of the front-line system, the frequency of the initiating events can be estimated from detailed logic models (e.g. fault trees).

2.3.2.7 *Component unavailabilities*

Components are distinguished as continuously monitored and unmonitored. The state of continuously monitored components is always known and their average unavailability is a function of their failure repair rates and duration of repair. The state of components that are not continuously monitored can be revealed through periodic tests. Their unavailability is a function of their failure rate, repair rate, frequency and duration of routine maintenance, test period, probability of error during maintenance and probability of not detecting and recovering the error during maintenance (see Papazoglou and Aneziris(1998)). These parameters (see Table 2-1) are estimated from generic data, such as those presented by OREDA (1987).

2.3.2.8 *Human error probabilities*

Most of the human actions incorporated in the logic models are of the "cognitive" type according to the definition given by Hannaman et. al. (1985). This means that they consist of actions not routinely performed, but actions required as a response to events not included in normal operation. The probability of failing to perform an action is a function of the available thinking time and the level of stress affected by the severity of the incident. These probabilities are estimated from generic data.

All the basic event parameters which are estimated in this step from generic data (see Table 2-1) will be modified in step III.3, according to the safety management system of an installation.

Table 2-1 Basic event parameters

f_i:	Frequency of external events
λ_s, λ_O :	Failure rate of unmonitored (standby) or monitored components
T:	Time between testing
Q_{M1}:	Error in test and repair
Q_{M2}:	Failure to detect and recover previous error in test and repair
f_M:	Frequency of routine maintenance
T_M:	Duration of routine maintenance
T_R:	Duration of repair
Q_{O1}:	Probability of error in operations or emergency
Q_{O2}:	Probability of not detecting and recovering error

2.3.3 Accident Sequence Quantification

The fifth major procedural task of the probabilistic safety assessment includes all the steps associated with the quantification of accident sequences. This quantification implies the determination in the event trees of the accident sequences to be quantified and their manipulation according to the laws of Boolean algebra. In case of corrosion the following steps I.15 and I.16 are not required.

2.3.3.1 Step I.15. Determination of accident sequences to be quantified

Each accident sequence consists of an initiating event followed by a number of system failures and sometimes system successes. If all these events, i.e. initiating event, system failures and system successes, were independent, then the quantification of an accident sequence would consist of simple multiplication of the corresponding frequency and probabilities. This situation is rarely true, however, owing to existing dependencies among the events which constitute the accident sequence. To take into account these dependencies, the events comprising the accident sequence must be treated according to the laws of Boolean Algebra to produce an equivalent Boolean equation which can then be used in the quantification.

2.3.3.2 Step I.16. Boolean reduction

Boolean reduction is the code name for the following manipulation of the system models. An accident sequence fault tree is generated consisting of an AND gate having as inputs the system failures that are included in the accident sequence. The system fault trees that have been developed for these failures then replace the system failures, and the large accident sequence fault tree is Boolean reduced to a number of cutsets. These cutsets provide combinations of simple events that cause the accident sequence to occur.

Two important points warrant special mention. The first has to do with the initiating event. If the frequency of this event is estimated from generic data and if it is known that no failures that might contribute to its occurrence are shared with other system failures, then this event is represented by a simple basic event in the accident sequence fault tree and basically it multiplies the cutsets of the remaining system failures. On the other hand, if a fault tree has been developed for the initiating event, then this tree must be linked with other trees in the sequence, and care must be taken so that the cut sets of this tree when quantified provide the frequency of their occurrence, while the cutsets of the rest of the trees provide their unavailability on demand.

The second important point has to do with the treatment of the system successes in the accident sequences. In certain instances it is important to explicitly consider the success of these systems in the Boolean reduction of the accident sequence to avoid an overestimation of its frequency. Such a situation arises in certain accident sequences identified in this study, since the fault trees developed for the frontline systems include the support systems. In these situations the success of a frontline system implies the success of its support systems, which cannot be then considered as contributing to the failure of a different frontline system in the same accident sequence. Exact treatment of this problem would require linking to the accident sequence tree the success trees for those systems assumed operating. Success trees are the trees resulting when the top event is replaced by its negation. This approach results, however, in large non-coherent fault trees which were difficult to treat with most of today's available computer codes.

The following approximate approach to face this problem is followed in this quantification:

a) An accident sequence fault tree is developed. This tree consisted of an AND gate having as inputs the initiating events and the top gates of the fault trees for the system failures in the accident sequence.
b) The minimal cutsets of the accident sequence fault tree are determined (List # 1).
c) The fault trees of the systems assumed successful in the accident sequence are linked under an OR gate.
d) The minimal cutsets of this second large tree are generated (List #2). This is actually a merging of the cutsets of each system assumed successful in the sequence.
e) The two lists are compared and cutsets in List #1 which imply a cut set in List #2 are eliminated.
f) The remaining cutsets in List #1 are those which form the accident sequence.

2.4 Phase 2: Audit and Assessment of the major hazard safety management system (SMS) of an installation

2.4.1 Purpose and strategy of the Integrated Risk Management Audit (IRMA)

2.4.1.1 Step II.1: Estimation of the management delivery systems

According to the methodology developed by the management team the safety management system has eight management delivery systems: availability, competence, commitment, communication, conflict resolution, interface, plans and procedures and spares and parts. In this step each delivery system (i) is assessed and graded (K_i) according to the procedure described in this section..

The purpose of the site audit within the I-Risk model is twofold:

- The audit should assess the quality of management systems pertaining to technical parameters and/or human errors which are critical to major hazard control within the technical model.
- The audit should assess the time trends or time dependency of the quality of the relevant (parts of the) management systems, i.e. should assess whether these systems are, on the whole, deteriorating, stable or improving.

The strategy of the I-Risk site audit can be outlined as follows.

1. To map the site's major hazard management system (MHMS) onto the general I-Risk model for major hazard management (and draw conclusions from that).
2. To link the quantitative risk analysis model to the company business process (and draw conclusions from that).
3. To produce a custom made audit and interview plan based on the above
4. Using this, to assess the quality of management of the relevant parts of the company's MHMS.

2.4.2 Overview of I-Risk Audit Procedure

1. Introduction of I-Risk audit
   A. Site introduction
   B. Requirements of the management audit team from the technical model
2. Choice of audit team
3. Preparation of audit plan
   A. Inventory of company MHMS
   B. Mapping of company MHMS onto I-Risk model and grouping of areas to be covered based on estimates of common mode
   C. Allocate scenarios, initiating and base events and technical parameter clusters to interviews
   D. Plan on-site audit interviews and verification checks
4. Conduct of audit
   A. Interviewing
   B. Verification
   C. Recording data and adapting audit plan
5. Evaluation of management tasks and activities and reporting
6. Calculation of management influences

2.4.2.1 *Introduction*

2.4.2.2 *Site introduction*

Description

The audit has to be introduced at the company that will be assessed, before either the technical or management modelling and assessment can begin. This should be done by representatives of the full audit team, including both the technical as well as the management modellers. An overview of the audit approach will be given and a description of its deliverables as well as a detailed description of its phases. The scope of the audit will be agreed (part or whole of plant). This should result in full understanding on both sides of what is and can be expected. The focus of the audit on major hazards should be explained and the boundaries of the part of the site to be audited should be agreed upon. This introduction should be at a suitable time before the audit so that the necessary information for the modelling (both technical and management) can be provided by the company. For the auditors the information under 3.A) (below) is needed at least three weeks before the audit, so that the audit team can do the preliminary mapping and planning.

Purpose

- Familiarise the company with the audit
- Outline requirements and expectations
- Request preliminary management system information
- Establish time frame

Deliverables

- Agreements with company on scope and focus of audit
- Overview of requirements on both sides
- Timeframe

2.4.2.3 *Requirements of management audit from technical model*

Description

The technical model defines and drives the management audit. Information is needed about all the ways in which it is considered that the plant can fail and produce a loss of containment, and which system components contribute to each of these scenarios. The scenarios are derived from the generic failure types, whereby a number are considered always to be credible, notably human errors by operators and/or maintenance staff leading to by-passing of the containment. A number of failure types will be credible only sometimes, notably earthquake, flooding. The short scenario descriptions and event trees given to the auditors also indicate the arguments why scenarios are considered credible (and why excluded scenarios are regarded as incredible).

The table given to the auditors contains base events and initiating events broken down to a level of detail that enables each to be linked to defined parts of the management system and to management influences in it. Where human errors are defined, the information indicates what type of person (e.g. operator, inspector, maintenance fitter, etc.) could make the error and broadly what type of error it is (notably whether

committed during routine, abnormal or emergency conditions, and whether it is an error of omission from a proceduralised routine, or error of commission, or other type). The table also contains the generic (or site specific) probability or frequency value to be used in quantification, so that it is clear what assumptions about failure are being made and whether the site audit needs to produce a modifying factor for the generic figures. The information is needed for two purposes:

1. To enable the base and initiating events and technical parameters to be grouped into clusters which are likely to be influenced by common management influences, and so to plan the interviews and questioning during the site audit.
2. To give to the auditors the full range of scenarios which can lead to loss of containment, so that they can be used selectively during interviews to test the completeness and understanding of the major hazard scenarios at the various levels in the organisation.

The draft of the scenarios and table of base is discussed between the technical modellers and the auditors (preferably in a face-to-face meeting) before the audit begins to arrive at agreement. This shares the expertise of all parties in respect of credible failure mechanisms and provides an essential opportunity for the auditors to be briefed on the technical model. It is essential that the set of scenarios is complete for the (part of the) plant to be audited, since one test of how good the plant Risk Control and Monitoring System (RCMS) is is whether it has identified all the scenarios in the I-Risk model.

The link between each of the technical parameters and its management influences is defined in Table 2-3. These indicate that all parameters are influenced by all eight of the delivery system loops (management influences) to a greater or lesser extent. Hence the site audit must collect information about all of these management influences related to each of the events in the technical model table. In this project the issue of the relative weighting of the different management influences on each of the parameters has been resolved by using the procedure described in section 2.1.4. In a small scale pilot a systematic expert judgement method has been tried out to resolve this issue more scientifically. Such a method can result in a reduction in the need to collect data, since the influence of some management delivery systems on some parameters is considered so marginal relative to others, that it is not worth wasting audit time on assessing them. Until that point is reached, however, all delivery systems are assessed for all parameters, i.e. all business activities.

To make this process manageable the events need to be clustered into as few groups as possible on the basis of the fact that all members of a group are influenced by the same management influences. The classificatory information collected in this stage lays the foundations for this step, which is completed in step 3C.

Purpose

- Define scenarios leading to loss of containment
- Define links with management influences
- Provide basis for interviews about major hazard scenarios

Deliverables

- An agreed list of scenarios indicating the ways in which the containment can fail or be by-passed
- An agreed table of base and initiating events and technical parameters with default data which forms the basis for management factor modification

- Preliminary classifications of events to be used in step 3.C. for clustering.

2.4.2.4 Choice of audit team

Description

The audit team should consist of at least two people, so that interviews can be efficiently planned and recorded (see 4.A below), who should have between them the following skills and knowledge. If two auditors cannot encompass all these skills, then the team should be expanded to a third member.

- Experience with the I-Risk audit technique and underlying management model
- Training and experience as (lead) auditor
- Technical knowledge of the technology to be audited
- Thorough understanding of the technical model of the plant
- Skills in interviewing, recording and interpreting information from interviews and verification checks

The audit team should agree in advance their method of working, role allocation and responsibilities.

Purpose

- Define audit team

Deliverables

- Agreed audit team and task allocation

2.4.2.5 Audit preparation

This is the most vital part of the audit, upon which its success depends. Time spent in planning will be recouped many times over in the conduct and evaluation stages. The preparation stage combines preliminary information from the company with the technical model and the I-Risk generic management model to produce a tailored set of topics for guiding the interviews, a plan of the interviews and the scenarios, base events and parameters which will be considered in each.

2.4.2.6 Inventory of company MHMS

Description

The I-Risk management model is described in section 2.1.3. It consists of a number of management loops which manage the setting up, running and improvement of the MHMS, and in particular the provision of a number of generic resources and controls to the primary business processes of operations, emergency control, maintenance (and plant modification).

In the planning stage the audit team has to see to it that it gets all the information it needs from the company that will be assessed in order to map the company MHMS onto these generic loops. "Mapping" is used here to describe the process of indicating who in the company carries out each of the tasks represented by each of the sets of

boxes in the loops in the model. This stage must indicate which person in the company should be interviewed about each part of each of the loops.

To do this the company needs to provide summary information about how it organises its MHMS; who has what responsibilities; what work is out-sourced, and what carried out by the company's own staff; what parts of the company MHMS are managed as one common mode, and what are decentralised or managed separately.

This question list and document list can be sent to the company to help it to gather information to be sent or made available for this stage. This information may also be collected in a preliminary visit by one of the auditors to the site for a discussion of a half to one day with senior safety staff in the company.

Purpose

- Collect site specific information on how company MHMS is organised

Requirements

- Generic question set for collecting information on allocation of responsibilities and common mode
- Generic list of relevant documentation

Deliverables

- Structured information from company on its MHMS and the business process(es)/plant(s) to be audited

2.4.2.7 Mapping the company MHMS and deciding common mode

Description

The information provided is mapped onto the management loops, allocating named company staff or company functions to all parts of all the loops. The aim of this mapping is to get a picture of the assessed company's MHMS which is as complete as possible, to determine who is responsible for what and to make a preliminary formulation of the audit plan and questions based on issues which arise during the mapping process. The mapping process should also shed light onto the matter of 'common mode', i.e. the extent to which the company runs different parts of its MHMS in the same systematic way, for example whether procedures for all activities are written following the same method, whether selection and training is centrally or decentrally organised and run, and, in the latter case, whether to a central detailed policy.

This exercise must determine how many times each of the generic management loops should be assessed, based on the degree of common mode.

Purpose

- Define size of audit by assessing degree of system (common mode) in the company MHMS
- Define persons to be interviewed about different aspects of the MHMS

Requirements

- Company information on responsibilities and broad structure of the MHMS
- I-Risk model loops
- Default common mode list and criteria

Deliverables

- Preliminary mapping of company's MHMS on overview sheets (management loops)
- Preliminary allocation of parts of the audit to particular interviews (by name or function).
- First insight into the strengths and weaknesses of the company's MHMS

2.4.2.8 Allocate scenarios to interviews

Description

When the first, top-down mapping has taken place, the scenarios, technical parameters and human errors resulting from the technical model can be linked to the MHMS. This information directly connects the audit to the business processes - operations, maintenance and emergency response - in that it highlights the critical activities in those and therefore will narrow the focus of the audit. Major hazard scenarios, their critical hardware parameters, initiating events and human errors are mapped onto the preliminary interview schedules from 3.B. on the basis of the understanding of allocation of responsibilities for the activities. This helps to refine the decisions about what is/is not common mode. For example, at this stage, human errors can be clustered according to the likely type of person who may commit them and the stages and situations in the different business processes in which the errors are considered to occur. Hardware can be clustered with reference to who maintains it; contractors or own staff, and within those groups, possible sub-groups of maintenance staff reporting to differently managed sections or contracting companies .

These clusters are then allocated to the responsible functions both at management and execution levels, to provide the auditor with examples of scenarios, events and parameters to use in the appropriate interviews. This annotation helps to keep the interviews focused on major hazard issues. It can be recorded on the prompt lists for the various delivery systems and interviews (see below).

Where a whole site is to be audited, with a very large table of base events, choices will have to be made of which business activities, scenarios, events and parameters will be sampled to arrive at assessments.

Purpose

- Further refinement of audit plan
- Annotation of interview schedules with major hazard focus for each interviewee.

Requirements

- Base events table suitably classified into types of errors and specification of hardware, with initiating events broken down to the level that specific parts of the MHMS can be linked to them.
- Preliminary interview schedules and mapping of company MHMS onto management loops.

Deliverables

- Linking of technical model with management model, through clusters of base events and parameters
- Annotated interview schedule indicating major hazard focus for each interview
- Modification to audit plan related to common modes

2.4.2.9 Produce final interview schedule and topic list per interview

Description

Based on the bottom-up and top-down processes described above, the audit team should have a rather complete view of the formal functioning of the company's MHMS, or at least how the company sees and projects it. Also, the critical activities within the business processes for major hazard control should be identified. Additionally, the audit team should have a clear picture of those who are responsible for the relevant activities which can give rise to loss of containment, or keep that risk under control through the control of the scenarios, initiating and base events and their technical parameters. On this basis the final decisions can be made about who should be interviewed during the audit, both to obtain preliminary assessments of the quality of different parts of the MHMS and to check those assessments (at the execution level). This amounts to allocating to one or more interviews each box on each of the management loops, as applied to each of the separate parts of the company management system defined after use of the common mode list.

As a general guideline, every box in every loop and delivery system should be allocated to more than one interviewee, in order to provide the opportunity for double checking of the information, and to avoid bias. Such an overlap can be achieved by allocating the same box to two adjacent levels in the hierarchy (boss and subordinate), or by cross-checking with two persons at the same level, or by verification between interview and documentation or observation. 100% cross-checking may lengthen the audit time unacceptably; in which case auditors need to use their judgement to cut out what they regard as unnecessary duplication during the course of the audit.

Each box has a prompt list of topics associated with it.

These prompts can therefore be allocated to each of the interviews. This is done by a process of annotating the standard interview recording forms with the name of the person from whom the information will be collected and by annotating the interview sheets with the list of scenarios, events and parameters which can be used as focus during the interviews. The auditors are provided with a cross-reference table , so that the correct sheets can be assembled before each interview.

This process produces the final list of required interviews which can be sent to the company for them to arrange the interviews. It also indicates the length of the interview (based on the number of boxes and topics to be explored). The experience of the trial site audits indicated that the order of interviews needs to controlled to

some extent. A progression from top management down to execution levels is a good way to proceed, since it gives the auditor a broad view of how the MHMS works and then allows zooming in to focus on specific aspects within this frame. Grouping of interviews by business function (operations, maintenance, safety, personnel & training, change management, etc.) is desirable, so that the auditors do not have to jump about all over the place in the MHMS and its application to the major hazard influences. Interviews should be planned with suitable short gaps in-between so that the results can be mapped onto the master diagrams and the auditors can discuss findings, modifications to the audit plan and tactics for the following step.

At the same time as the interview plan, preliminary lists can be made of the verification checks which will be needed and the stage at which they should take place, either during interviews, or as a separate exercise of observation or checking of documents.

Purpose

- Design of final audit plan - interviews with whom, about what and in what (rough) order.

Requirements

- Deliverables from previous steps

Deliverables

- Audit plan and prompt list of topics and scenarios/parameters/events per interview
- List of interviewees/auditees and schedule of interviews to be sent to the company for making arrangements

2.4.2.10 Conduct of the audit (Interview, verification, recording)

Description

It is the objective that all of the above steps will take place before the team gets to the audit site. Some steps may require telephone or e-mail contact with the company (or between audit team members if these are geographically separated) to check information. In non-ideal cases the final planning steps may need to be done at the site after a preliminary discussion with the senior manager or safety department to verify who is responsible for what. The final interview schedule will also be subject to change dependent on availability of people. The objective is, however, that the audit team starts with a clear idea of how the MHMS maps onto the I-Risk model and can concentrate fully in this phase on assessing the quality of the various parts of the MHMS.

The overall strategy for the audit will have two focuses:

1. Evaluation of the quality at the present moment of the major hazard risk control system(s) and the delivery systems and feedback loops managing the business processes identified. The strategy here is strongly guided by the search for the quality and integrity of the loops involved in these systems. It is guided by the prompt lists and the overviews of the management loops.Verification on a sample basis provides direct checking of the business process activities which have, as outputs, the parameters for the technical model, in order to confirm how these are planned, resourced and controlled.

2. Collection of information about the periodicity with which the MHMS feedback and improvement loops are carried out. This information provides an indication of the degree to which the management loops will detect and correct shortcomings, respond to changes in the system by adapting to them, and improve itself based on learning from feedback internally, or best practice and changing situations outside itself.

The information collected will be mapped onto the overview diagrams so far as possible during the interviews, but if not at regular intervals between them, to build the final picture. This will enable the audit plan and questions to be modified as information emerges, curtailing questioning in areas where sufficient information is available to make judgements and expanding it in areas which throw up unexpected shortcomings.

During the interviews further information may emerge which leads the auditors to modify their assessment of the degree of common mode in a part of the organisation. If this occurs, the interview schedule may need to be modified either by arranging extra interviews or verification visits or by dropping some.

The prompt lists provide the framework for the interview. The auditors select the sheets appropriate to each interview beforehand, using the cross-reference plan .

They agree the rough order of conduct of the interview and the major hazard scenarios, base or initiating events to be used in it. The prompt lists are not formulated as specific questions, since it is never possible to conduct an audit with such a rigid list. The interviewee always strays outside such a straitjacket and the interviewer must be able to respond flexibly. The lists are there as reminders of topics to be covered, and can serve during and at the end of the interview as a checklist of what still has to be covered. Experience suggests that two auditors should be present at as many of the interviews as possible, so that one can record information and keep the structure and flow of questioning under control, whilst the other poses the questions. In long interviews an agreed swap of these two roles during the interview is advisable. For some of the more straightforward areas of questioning, particularly with shop floor or supporting staff (e.g. personnel, stores), and for the verification process of checking documents and making observations, the two auditors can operate in parallel to save time.

Verification may enable a very direct assessment of the quality of the output of some delivery systems, and hence a very direct assessment of the quality of influence on a specific technical parameter.

If this is the case, theoretically there is no need, for that delivery system, to assess the other boxes in the loop. However such direct quality assessments will only be possible for a very small sample of the parameters from the technical model, and in any case will give no indication as to how the quality of the influence will alter with time, because of the quality of the whole loop. Therefore these direct assessments of the box should be used as cross checks.

The aim of the audit is that all information is recorded as directly as possible onto the evaluation forms. This saves a very large transcription task after the audit. It also allows the auditors to see how the evidence they have collected is building up, and whether they feel they have enough to make an evaluation of a given box on a given loop. Care should be taken not to stop with the collection of evidence too soon, since this may result in missing more subtle problems. The auditors should also refrain from

making premature evaluations of the boxes, since these will be likely to lead to attempts (albeit unconscious) to steer the further audit towards confirmation of the preliminary evaluation. It is better to separate the data collection and evaluation steps and postpone the latter until after the audit is over. However, the cumulation of the evidence on the forms can give sufficient indication to the auditors of gaps needing still to be filled, or areas where there is a great deal of information and planned questions can be curtailed. In this way the audit plan can be adapted as it progresses.

Purpose

- Collect all information needed to evaluate the MHMS in all its ramifications relevant to the technical parameters in the I-Risk technical model

Requirements

- Cross reference schedule of interviewees and topic areas to be covered.
- Generic overview diagrams and prompt lists duplicated the appropriate number of times to reflect the degree of common mode, or lack of it, in the company (for guiding questioning and recording data)
- Scenario descriptions and technical model base event table for reference

Deliverables

- Recorded information on the quality of all the relevant parts of the MHMS, presence of loops, etc.
- Recorded information on the periodicity with which the feedback and learning loops operate.

2.4.2.11 Evaluate management influences and produce modification factors

Description

Based on the recorded information two actions will follow:

1. Immediate feedback to the company on the strengths and weaknesses of the MHMS either at the end of the site visit, and/or in a later report to the company
2. Decisions on the quality assessment of each of the management processes (boxes) which will be used to calculate the quantitative output of the management system to be applied to the parameters for the technical model

For the first, the overview diagrams of the MHMS will be the main inputs and the comments will be qualitative and relative. The feedback will normally be presented verbally on the last day of the audit and confirmed in a written report.

For the second the process of decision making must be more considered, transparent and quantitative and final decisions do not have to be made on site. Some interaction with the technical team is expected in this process, since one of the results of the management assessments will be to emphasise common modes between base events which were regarded as independent up to that point. This may mean that certain quality assessments will become much more critical than others and will need to be reviewed in more detail.

In the first instance the two auditors should go through the recorded information for each box, for each application and, where necessary, clarify and discuss it. They should then make a rating of each box, preferably independently in order to check on the inter-rater reliability of the audit instrument. In the trial audits a 10-point scale has

been used for these ratings. In one audit ratings were made by putting a mark on a 10cm line continuous scale; in another to the nearest half a point score on the scale. The two auditors should agree in advance to what level of accuracy they will rate.

After initial independent rating, the auditors should compare the ratings given and identify differences. Where the ratings differ significantly (more than one point difference can be considered significant in all cases; smaller differences may be significant depending on sensitivity analysis), the auditors should discuss these differences and try to resolve them. This process reveals differences in interpretation of the prompt lists and rating scales, which can often be resolved easily. Where this is not the case and auditors have different assessments of the quality of the same activity, it may be necessary to collect more data. In all cases of difference the final ratings of the two auditors should be averaged to arrive at the final score.

Purpose

- Produce agreed evaluations of all parts of the MHMS to feed into the process of modifying the technical parameters.

Requirements

- Completed overview diagram of MHMS
- Audit notes
- Discussion

Deliverables

- Reasoned quantitative assessment, agreed between the auditors of the quality of each box in each application of the management loops, as input to the modification process of the technical parameters.
- Feedback to the company on strengths and weaknesses of the MHMS

2.4.2.12 6. Calculation of management influences

As a result of the audit procedure the quality of each box has been quantified. As mentioned earlier the ultimate objective of the management model is to quantify its influence on the technical parameters. This influence is manifested through the output of each box 8 of each of the eight management delivery systems. The output of each of the box-8 is influenced by the rest of the management system. As a result the quality of its output depends on the quality of the various elements of the management system.

It is assumed that each that each box (i) is represented by its state x_i and its output y_i. The state of a box is representing the quality of the corresponding management procedure and it is quantified through the audit procedure. The output of the box represents everything that comes out of this particular management function (product, procedure, action, e.t.c.) and contributes an input to another management function (or box). This the output of a box is and input to one or more other box. Each box has one output and it can receive several inputs.

The model further assumes that the quality of an output y_i is a function of the quality of the state of that box (x_i) and of the quality of all the inputs it receives. So,

$$y_i = k_{ii}x_i + (1-K_{ii})\sum_{j=i}^{12} c_{ij}y_j$$

This equation can be written in matrix form as:

$$\mathbf{y} = \mathbf{Kx} + (\mathbf{I}-\mathbf{K})\cdot\mathbf{C}\cdot\mathbf{y}$$

And solved to provide,

$$\mathbf{y} = [\mathbf{I} - (\mathbf{I}-\mathbf{K})\cdot\mathbf{C}]^{-1}\cdot\mathbf{K}\cdot\mathbf{x}$$

The elements of matrices **K** and **C** provide the relative importance the state and inputs in the determination of the quality of the output and represent the subjective judgement of the team assessing the management system. It should be noted, however, that **K** and **C** are not considered plant specific, but they are supposed to generic. From this last equation the values of the outputs of boxes 8 (y_8) of the various management delivery systems are obtained as a function of the qualities x_i's of the various boxes.

2.5 Phase 3: Modification of the frequencies of the plant damage states according to the Major Hazard Management System

The third phase of integrated risk assessment aims at the modification of the frequencies of the plant damage states, according to the assessment of the major hazard management system of an installation. This is achieved first via the modification of all the basic event parameters (see Table 2-1) according to the assessment of the MHMS.

The steps to be followed for this modification are the following:

2.5.1.1 Step III.1: Grouping of the parameters according to the common management systems: operation, maintenance and emergency

The basic events of the system are either component failures or human errors, as already discussed in step I.14. These might occur, either during normal operation of the installation, or during maintenance, or event during an emergency situation. All basic events and their parameters are first grouped into these three broad categories but can be further divided into subcategories. For example maintenance may be divided into mechanical, electrical or instrumentation maintenance.

2.5.1.2 Step III.2: Estimation of the delivery systems which affect each basic event parameter

In this step the weighting factor, with which delivery systems affect basic event parameters are estimated. This is performed for all subcategories (common mode

management system) of step III.1 (see section 2.1.4 and Table 2-1). The specific weighting factors w_{ij} with which a delivery system i (i=1,8) affects a basic event parameter j are estimated. This is repeated for all parameters and for all different subcategories.

Table 2-1 Delivery systems which affect basic event parameters of a subcategory

Delivery systems	Basic event parameters										
	Qo1	*Qo2*	*Qm1*	*Qm2*	*fi*	λ	*T*	*fm*	*Tr*	*Tm*	*Total*
Availability	0,06	0,05	0,08	0,05	0,1	0,08	0,05	0,05	0,12	0,12	0,76
Commitment	0,15	0,14	0,19	0,13	0,2	0,12	0,24	0,21	0,07	0,08	1,53
Communication	0,07	0,05	0,06	0,05	0,1	0,12	0,14	0,16	0,21	0,21	1,17
Competence	0,16	0,21	0,14	0,22	0,1	0,08	0	0	0,09	0,08	1,08
Conflict resolution	0,18	0,21	0,14	0,18	0,1	0,08	0,28	0,32	0,10	0,12	1,71
Interface	0,20	0,20	0,08	0,18	0	0,08	0,05	0,05	0,19	0,17	1,2
Procedures	0,18	0,14	0,17	0,15	0,4	0,16	0,19	0,16	0,10	0,08	1,73
Spares & tools	0	0	0,14	0,04	0	0,28	0,05	0,05	0,12	0,14	0,82

2.5.1.3 Step III.3: Estimation of the upper (f_u) and lower (f_l) value of each basic event parameter

Each basic event parameter may take a lower f_l value, when the safety management system of the installation is the poorest in the industry or an upper value f_u when it is the best in the industry. These two values are estimated for all the basic event parameters.

2.5.1.4 Step III.4: Estimation of the modification factor (m_j) of each basic event parameter.

The modification factor (m_j) of each basic event parameter (which belongs to a specific subcategory) is estimated from the following equation:

$$m_j = \sum_{i=1}^{8} y_{8i} w_{ij} \qquad (1)$$

y_{8i}: grading value for each delivery system of a specific subcategory (output of box 8) i=1,...8...(estimated in step 6 of the management audit)

w_{ij}: weighting factor for each basic event parameter j, affected by delivery system i... of a specific subcategory (estimated in step III.2)

2.5.1.5 Step III.5: Modification of the basic event parameters

Basic event parameters are modified according to the following function:

$$\ln f = \ln f_l + \frac{(\ln f_u - \ln f_l)}{10} m_j \qquad (2)$$

f: modified value of specific parameter

f_l: lower value of each parameter (estimated in step III.3)

f_u: upper value of each parameter (estimated in step III.3)

m_j: modification factor (estimated in step III.4)

Finally steps 15 and 16 of accident quantification are repeated with the modified basic event parameters, so as to calculate the modified frequencies of the plant damage states.

2.6 Phase 4: Consequences of toxic or flammable substance releases

The fourth phase of the integrated risk assessment aim at the establishment of the consequences of the released hazardous substances. In case of toxic substances steps IV.1-IV.4 should be followed, while in case of flammable substance steps IV.5-IV.8.

2.6.1 Toxic Substances

For toxic substances the assessment of the consequences involves the following steps:

2.6.1.1 Step IV.1: Determination of Release Categories for Toxic Materials.

For toxic substances to be dispersed in the atmosphere, this step comprises the determination of all the conditions (installation dependent and environmental) that affect atmospheric dispersion. This includes quantity and physical conditions of the substance released from its containment (outflow models), evaporation rate (if released in liquid form), temperature, other weather conditions, and so on.

Plant Damage States usually are associated with one release category. It is possible, however, that a plant damage state can lead to one of several release categories depending on various uncertain parameters and conditions.

2.6.1.2 Step IV.2: Atmospheric Dispersion of Toxic Materials.

In this step a model simulating dispersion of a toxic substance is established. The model estimates the concentration of the toxic substance as a function of time and space. Each release category leads to a specific concentration level for each point of time and space.

2.6.1.3 Step IV.3: Dose Assessment.

Given the concentration of the toxic substance an individual in the general area of the installation will receive a certain dose (inhalation) of the toxic substance. This depends also on the particular emergency response plan, implemented, in each case.

2.6.1.4 Step IV.4: Consequence Assessment.

A dose/response model receives as input the dose calculated by the dose model and calculates the probability of fatality for the individual receiving the dose.

2.6.2 Flammable Substances.

A parallel set of steps can be distinguished for the assessment of the consequences of released flammable substances.

2.6.2.1 Step IV.5: Determination of Release categories of Flammable Material.

A release category for a flammable material uniquely determines the type of the physical phenomenon that could result in fatalities or injuries. For example, in the case of the LPG, it is established whether a BLEVE will take place or whether an explosion or deflagration will result following atmospheric dispersion of the gas. The type of fire that might result from other flammable materials is another example.

2.6.2.2 Step IV.6: Estimation of Heat Radiation and Peak Overpressure.

In this step, a model for simulating the heat radiation or the peak overpressure resulting from the released flammable material and the associated physical phenomenon is established.

2.6.2.3 Step IV.7: Dose Assessment.

The integrated, over time, exposure of an individual to the extreme phenomenon generated by the flammable material is calculated. This defines the "dose" an individual receives.

2.6.2.4 Step IV.8: Consequence Assessment

Appropriate dose/response models receiving as input the dose of heat radiation or overpressure calculate the probability of fatality or injury of the individual receiving the dose.

2.7 Phase 5: Risk Integration.

In this last phase integration of the results obtained so far, that is combining the frequencies of the various accidents with the corresponding consequences, results in the quantification of risk. Two risk measures are usually used to quantify risk.

1. Individual fatality risk at a location
2. Group fatality risk in a given area

2.7.1.1 Step V.1: Individual Risk

Individual fatality risk is defined as the "frequency (probability per unit of time) that an individual at a specific location (x,y) relative to the installation(s) will die as a result of an accident in the installation", (see AIChE/CCPS (1989), HSE (1989), VROM(1990)).

Individual fatality risk is usually expressed per unit of time (e.g. per year) of installation operation. Individual fatality risk is calculated as follows:

Let

i: be an index, spanning the space of the initiating events. That is, of those events that have the potential to initiate an accident sequence.

(i = 1, . . ., I)

k: be an index spanning the space of the possible plant damage states of an installation.

(k = 1, . . ., K)

r: be an index spanning the space of the possible release categories of a toxic or flammable substance. It is reminded that the space of release categories includes all possible combinations of installation - related, weather, and any other parameters that determine the intensity of the adverse effect. (concentration, thermal radiation e.t.c.).

(r = 1, . . ., R)

f_i: be the frequency of the i^{th} initiating event.

p_{ki}: be the conditional probability that the i^{th} initiating event will lead to the k^{th} plant damage state.

f_k: be the frequency of the k^{th} plant damage state.

It follows that :

$$f_k = \sum_{i=1}^{I} f_i p_{ki} \qquad (3)$$

Examples for calculating frequencies f_k s are given by IAEA (1993) and Papazoglou et al. (1992).

Furthermore, let

f_r: be the frequency of the r^{th} release category, and

p_{rk}: be the conditional probability that the k^{th} plant damage state will lead to the r^{th} release category with $\sum_{r=1}^{R} p_{rk} = 1$

It follows that:

$$f_r = \sum_{k=1}^{K} f_k \, p_{rk} = \sum_{k=1}^{K} p_{rk} \sum_{i=1}^{I} f_i \, p_{ki} \qquad (4)$$

Let

$c_r(x,y,t)$: be the intensity of the adverse effect (e.g. concentration of toxic material, heat radiation, overpressure) at point (x,y) and instant of time t given that release category r has occurred.

$d_r(x,y)$: be the level of adverse exposure that is, the integrated over time exposure to the adverse effect. This quantity is commonly referred to as "dose" and it is calculated by:

$$d_r(x,y) = \int_0^T f\{c_r(x,y,t)\} \, dt \qquad (5)$$

where $f\{c_r\}$ is a substance dependent function.

p_d: be the conditional probability of fatality <u>given</u> that one individual is exposed to a level {d} of the adverse effect of the hazardous material.

Probability p_d is usually calculated through the so called "probit functions" (see AIChE/CCPS (1989), Lecs (1996), TNO (1989)).

It follows that the quantity $p_r(x,y)$ where:

$p_r(x,y)$: is the conditional probability of fatality for an individual at location (x,y) given release category r.

can be calculated form the doses as follows:

release category r $\xrightarrow{\text{Dispersion}} c_r(x,y,t) \xrightarrow{\text{Dose}} d_r(x,y) \xrightarrow{\text{Probit}} p_r(x,y)$ (6)

If now

R(x,y): is the frequency of fatality for an individual at location (x,y). (individual risk),

It follows that:

$$R(x,y) = \sum_{r=1}^{R} p_r(x,y)\, f_r \qquad (7)$$

or $$R(x,y) = \sum_{r=1}^{R} p_r(x,y) \sum_{k=1}^{K} p_{rk} \sum_{i=1}^{I} p_{ki}\, f_i \qquad (8)$$

Frequencies f_i, conditional probabilities p_{ki}, and frequencies f_k are calculated in the first phase of the analysis.

Frequencies f_r include all possible uncertainties in the parameters that determine the level of an adverse effect at a location (x,y) and at time t; consequences $c_r(x,y,t)$, doses $d_r(x,y)$, and probability $p_r(x,y)$ are calculated during the consequences estimation phase.

Usually individual risk is expressed in terms of *isorisk curves*, that is the loci of points with the same level of individual risk.

2.7.1.2 Step V.2: Group Risk

Group fatality risk proceeds one step further than individual risk by taking into consideration the population size and distribution around the site of the installation. Group risk is expressed in terms of the so called (F, N) curves and gives the frequency with which it is expected that the number of fatalities which exceed N, (see AIChE/CCPS (1989), Lecs (1996), TNO (1989)).

Group risk is calculated as follows:

Let

w(x,y): be the population density at location (x,y) of an area A.

N_r: be the total number of people that will die in area A given the release category r.

It follows that :

$$N_r = \sum_A p_r(x,y)\, w(x,y) \qquad (9)$$

This process results in R numbers of N_r fatalities, each one associated with one release category. There are two types of group risk measures that can be calculated. One *conditional* on a particular plant damage state k, and one *unconditional* on the plant damage state.

Given a plant damage state k, each release category r may occur with probability p_{rk}. As a result, the N_r (r=1,....,R) number of fatalities are each associated with probabilities p_{rk} (r=1,....,R). Out of the R doublets (N_r,p_{rk}) a Complementary Cumulative Distribution Function (CCDF) can be constructed, $F_k(N)$, which gives the probability that *given a plant damage state* k, there will be more than N fatalities.

Out of the K conditional CCDFs an unconditional on the plant damage state CCDF can be constructed according to the relationship

$$F(N) = \sum_{k=1}^{K} f_k\, F_k(N) \qquad (10)$$

where now F(N) gives the frequency (probability per unit time) with which an accident causing more than N fatalities is expected.

2.8 Phase 6: Modification of frequencies of plant damage states over time

In this phase the time-dependent behavior of the management effect on the frequencies of accidents is examined .

The influences of the management model are distinguished into:

1. Direct influences affecting the day-to-day operation of the plant and having a direct affect on the various activities determining the values of the technical parameters.
2. Indirect influences that actually describe the state of the various management activities and can cause a change overtime on the management system and in turn cause a temporal change to the direct influences.

Denoting by **y** the direct influences and by **x** the indirect influences the model assumes that:

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{y}$$

and $$\mathbf{y} = \mathbf{K}\mathbf{x} + (\mathbf{I} - \mathbf{K}) \cdot \mathbf{C}\mathbf{y}$$

Matrices **A**, **B** determine the rate of change of the indirect influences caused by the present state of the indirect and direct influences, respectively.

Matrices **A**, **B**, **K** and **C** are provided by the analyst.

Solution of these equations provides the indirect influences **y**(t) as a function of time.

For each instant of time the corresponding frequencies of LOC can be calculated by repeating the steps phase 3 (Section 2.5).

2.9 Phase 7: Specification of the important management influences on risk whose performance should be monitored

The relative importance of the various management influences on risk can be determined through the mathematical relationship of the various risk indices and these influences.

They are repeated here for convenience.

Let f_{LOC} be one of the risk indices of interest namely the frequency of the loss of containment. The technical model through the various logic models provides this index as a function of a number of basic events (b_i). For each basic event there is a probability of occurrence expressed in terms of the 10 fundamental technical parameters .

Mathematically these expressions can be written as:

$$f_{LOC} = g(\mathbf{b})$$

and $$\mathbf{b} = u(\mathbf{q})$$

where, **b** : vector of basic events of the technical model.

Q : vector of technical parameters.

g(**b**) : logic function providing the frequency of LOC as a function of the basic events **b**.

u(**q**) : function connecting the basic event probabilities with the technical parameters; this function is practically one of the equations (3.6)-(3.12).

In general there are at least as many basic events as components in the system and of course more than that technical parameters.

A technical parameter q is calculated from the quality factor q*. If q*=10 (best) then q takes the best possible values q_u, while if q*=0 (worse) then q takes the worse possible value q_l (see § 2.5 of main report). In compact form this can be written as:

$$\mathbf{q}=w(\mathbf{q}^*)$$

The quality factors for the technical parameters q* are obtained from the outputs y_8 of the various delivery loops of the management model, as follows:

$$\mathbf{q}^*=\mathbf{M}\cdot\mathbf{y}_8$$

where $\mathbf{y}_8$ is the vector of output #8 from each of the eight delivery loops and every management common mode system. If there are n_j technical parameters for the basic event corresponding to components managed by the j^{th} management subsystem (j^{th} common-mode) then, $\mathbf{M}_j$ is an n_jx8 matrix, each row of which provides the relative weights of each of the eight fundamental delivery systems into forming the corresponding q*.

If more than on management subsystems are affecting a particular set of components and a corresponding parameter then the previous equation is written as

$$\mathbf{q}^*=\sum_j \mathbf{M}^j\cdot\mathbf{y}_8^j$$

where the summation extends over the management subsystems that are affecting the particular group of components.

Management model outputs $\mathbf{y}_8^j$ are given as a function of time by

$$\mathbf{y}_8(n)=\mathbf{H}\cdot\mathbf{x}(n)$$

$$\mathbf{y}(n)=[\mathbf{I}-(\mathbf{I}-\mathbf{K})\cdot\mathbf{C}]^{-1}\cdot\mathbf{K}\cdot\mathbf{x}(n)$$

where $t_n=n\cdot t$,

Matrix **H** is an 8x51 matrix consisting of those rows of $[\mathbf{I}-(\mathbf{I}-\mathbf{K})\cdot\mathbf{C}]^{-1}\cdot\mathbf{K}$ corresponding to the y_8's. Furthermore the dependence on the j^{th} management subsystem has been dropped to facilitate notation. Finally **x**(n) can be written as

$$\mathbf{x}(n+1)=\mathbf{D}(n)\mathbf{x}(n)$$

Where $\mathbf{D}(n)=\mathbf{I}+\mathbf{F}(n)[\mathbf{A}+\mathbf{B}\cdot[\mathbf{I}-(\mathbf{I}-\mathbf{K})\cdot\mathbf{C}]^{-1}\cdot\mathbf{K}]\bullet t$

The procedure for calculating the effect of the management on the frequency of LOC (or any other risk index) is to solve the equations above in reverse order.

- Develop management model, perform audit and assess $\mathbf{x}(0)$ for n=0, 1, 2,...
- Obtain $\mathbf{y}_s(n)$
- Obtain quality factors $\mathbf{q}^*(n)$
- Obtain technical parameters $\mathbf{q}(n)$
- Calculate Basic Event probabilities $\mathbf{b}(n)$
- Calculate the Technical model and quantify $f_{LOC}(n)$

Risk index f_{LOC} is a function of the initial states of the management system $\mathbf{x}(0)$, the management structure and evolution parameters (**A**, **B**, **C**, **K**), the effect of the management on the technical model parameters [**M**, w(·)] and the technical model [u(·) and g(·)].

One measure of the relative importance that is of the contribution of each box-state at time zero (time of the assessment) to the risk index is the derivative of this index with respect a particular box state at time zero. In general three measures of importance can be calculated:

Elasticity: $$\text{å} = \frac{\partial \ln f}{\partial \ln x_i(0)} \Rightarrow \text{å} = \frac{\partial f_{LOC}}{\partial x_i(0)} \cdot \frac{x_i(0)}{f_{LOC}}$$

Risk Worth: $R_W=f(x_i(0)=1)$

Risk Degradation: $R_D=f(x_i(0)=0)$

Elasticity provides the % change of the risk index per 1% of change of variable $x_i(0)$ from its present value.

Risk Worth provides how much risk index f_{LOC} is improved if box i could become perfect.

Risk Degradation gives the reduction of the risk index if box I was at its worse state ($x_i(0)=0$).

It is noteworthy that all three measures provide relative importance of each and every initial state of the management boxes provided that all other boxes have their values fixed at the assessed initial conditions.

3. SUMMARY OF THE TEST RESULTS

3.1 Introduction

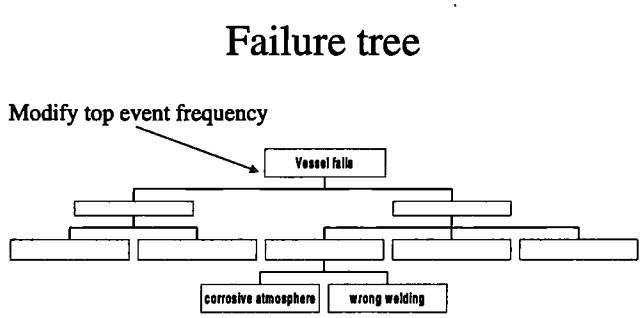
In this chapter the I-Risk process is illustrated using three examples. These examples were the test cases used in the investigation .

Besides the illustration, they also show that the I-Risk approach is feasible in practice and produces meaningful results.

In a risk analysis of a chemical plant, the frequency of the base events of the event-trees, usually loss of containment events (LOCs) are taken from a database or from some list of standard values or set by expert judgement. Only rarely is a fault-tree with such a LOC as the top event used to develop the frequency of a LOC from initiating events. It is not customary to take management factors into account in such a quantified risk analysis. If it is done at all, it is done by multiplication of the frequency of the top event by a constant number.

In the past, several attempts were made to include in QRA the effects of organisational and managerial factors. Modification of the frequency of releases based on judgement was the usual way of doing this. This judgement could be based on the results of audits of the safety management systems (SMS) of an installation, as, for example, as presented by Pitblado et al. (1990). This reduces or increases the frequency of all LOCs by the same amount. (Figure 3-1)

Figure 3-1 Traditional way of introducing management influences

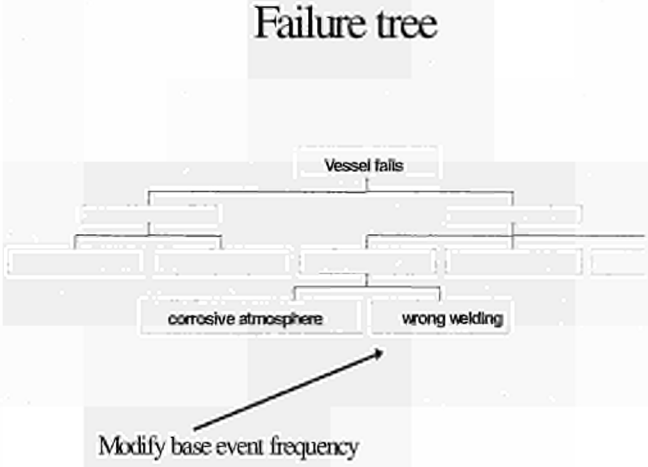


In the I-Risk project, the frequency of releases is calculated from detailed "technical" models. These models have parameters that characterise the stochastic aspects of performance of hardware and humans. In addition, "organisational" models describing the characteristics of the management systems are employed. These are used to quantify the effect of these systems on the parameters of the technical model with the objective of giving a better description of these influences than the straight modification of the frequency of release. The I-Risk approach allows the different tasks of management to influence only those parts of a fault-tree to which the particular management task pertains. (Figure 3.2). This in theory results in a better estimate of the influence of management on the frequency of LOC and it allows

identifying the vulnerability of the system as a whole: management and hardware together.

Figure 3.2: I-Risk way of incorporating management effects

The I-Risk approach was applied to three test cases: a chlorine loading facility , a refinery, and an ammonia storage facility. For each of these plants a preliminary risk analysis was performed in which the generic parameters were not modified to take account of management factors specific to the plant under study. In addition, a more



detailed Hazard and Operability study (HAZOP) was used where appropriate. These studies in part formed the basis for shaping the audit. They also provided the base data with which a later "modified" analysis could be compared.

From this comparison conclusions could be drawn, amongst others, on the importance of the various tasks and functions for the overall safety of the plant. This was done by calculation of the derivative of the failure frequency with respect to the various scores. This gives the amount of change of the frequency when the score of an aspect of management quality changes one unit on the scale. The higher this importance, the more can be gained by improving this factor and the more important it is not to let this factor deteriorate. There are several mechanisms in the audit to assess such a change of management over time. These mechanisms are also referred to as "management corrosion" monitors.

The chlorine example, although a real, existing plant, was merely a paper test. The other two involved real plants, real sites, real site visits and audits. The results of these test cases are summarised in the next sections.

In this chapter these cases are described in summary. Some details are given where appropriate only to illustrate a point.

3.2 Chlorine loading facility test results

The Chlorine loading facility investigated in this test case, also called plant A, consists of a storage vessel holding the chlorine, a loading hose and a chlorine road tanker. The storage tank itself is not part of the system other than being in principal an unlimited supply of chlorine. (fig 3.3). The system under consideration thus consists of a chlorine tank and a loading hose. The operator in a CIMAH report published earlier described the details of the system.

3.2.1 Safety systems

There are a number of systems installed to prevent an accidental release of chlorine.

There is a pressure relief system fitted on the tank.

There are pneumatically actuated valves on either end of the loading hose. There also is a manually actuated valve on the tanker.

There is a system that prevents the truck from moving while it is loaded. This system consists of a barrier and chocks on the wheels. In addition, the brakes are interlocked with the loading system.

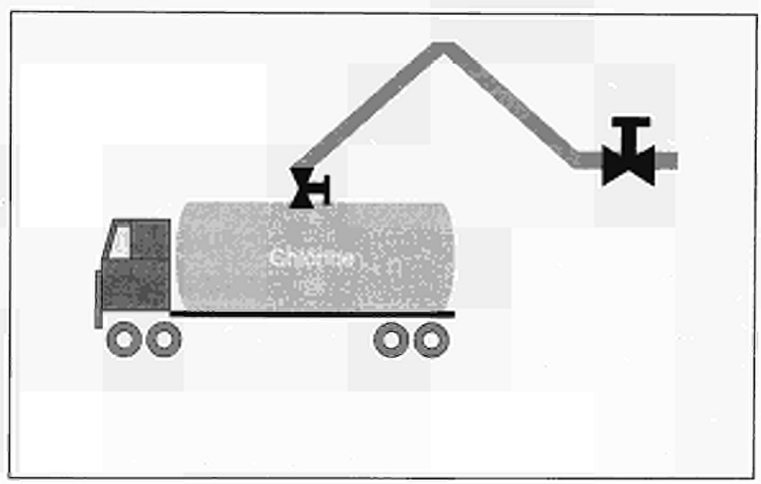


Figure 3-3: Chlorine loading facility

3.2.2 Loss of containment accidents

The LOCs relevant for this system, are a leakage or a break in the loading hose and a leakage or break of the tank. These and most of the primary causes were taken from a risk analysis performed by HSE previously.

A leakage or break of the loading hose can be initiated by corrosion or brittle failure. The hose might still be open after repair. The hose can break because the tanker moves. A pressure shock may occur as a result of a sudden closure of a valve. An existing overpressure in the tank or the supply vessel may be transferred to the hose because of a failure of the pressure protection system. An earthquake may occur and finally the operator may not notice an improper connection before starting the loading operation.

Every one of these causes may be decomposed in associated underlying hardware problems and operator errors. Then the link between these and the management system can be established. For this purpose the Master Logic Diagrams (MLDs) whose principles are described in the previous chapter were established.

These MLDs led to a number of questions that related to both the technical system and to the management system that would have to be answered in the audit.

3.2.3 The audit

The audit of the chlorine loading system took place early in the development of I-Risk It was considered inappropriate to perform the audit in this stage at the site of the plant. It therefore was decided to simulate the audit, by auditing the information available on paper, with the help of some members of the project team who were familiar with the actual plant.

The auditing method and the associated question set at this stage was wholly based on a description of the management system based on the SADT model structure .

Although the quantified risk analysis provided sufficient information on the LOCs for consideration, some key information proved to be lacking. This was, in particular, information on how operators could cause a LOC by direct action and other types of human errors possible once the initiating events occurs.

However, the question set used to gather the information and diagnose deficiencies proved to be too complicated to be used in a test involving personnel of a real plant.

The audit resulted in a number of recommendations for the further development of the I-Risk methodology. These included:

- To define the requirements put by the audit team on the preliminary QRA, and the requirements put on the technical team by demands from the audit team.
- To allow interaction between the technical and the management auditors during the audit.
- To perform both the technical modelling and the management auditing in stages, to allow modifications of the original plan according to the findings.

3.2.4 The results

The results of the first audit can be distinguished between those pertaining to the plant under study and those pertaining to the I-Risk method itself.

As far as the plant was concerned, no major deficiencies in the plant's safety management system was detected. Nevertheless some instances were found were the written and sound procedures were not followed. These included that the drivers of the trucks were not always adequately informed about the emergency procedures in case of a release and that inspections are left to the individual supervisors, resulting in widely varying levels.

With respect to the model structure and the associated questions set several observations and conclusions were drawn.

The SADT model did not link with the technical model and the associated HAZOP sufficiently. A better definition of the interface between the technical model of the plant, for instance, the fault-tree, the master logic diagram and the quantified risk

analysis, and the output of the management model was needed. This resulted in a further development of the interface described in the previous chapter.

The actual audit needs extensive preparation if undue lengthy interaction with the plant and its personnel is to be avoided.

The poor linkage between the management and the technical model prevented an actual modification of the quantified risk analysis. However a revised interface system was developed. This was used in the following two tests.

3.3 Refinery

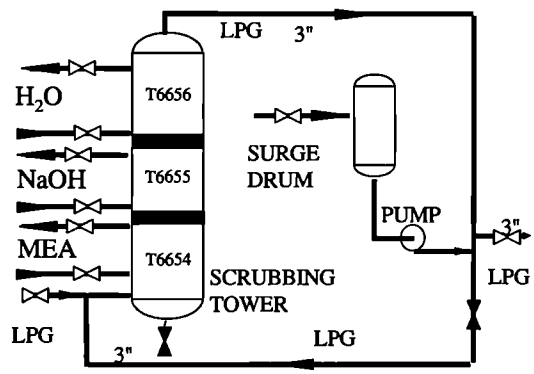
The second test, plant B, involved a part of a refinery. This was the first test in which a more practicable interface between the management model and the technical model could be used. This model is described in detail in Chapter 2.

3.3.1 Description of the Installation

The installation analysed is a scrubber section typically found in refinery installations.

The installation analysed is depicted in figure 3.4.

Figure 3-4: Diagram of installation



Its purpose it to remove traces of Hydrogen Sulphide (H_2S) from an intermediate: LPG. To this end the LPG is passed through a tower and washed in three stages with MonoEthanolAmine (MEA), Caustic and water. Another stream of LPG is merged through a surge drum. The recirculation line is closed during normal operation. The washing tower is about 24 m high and 1.4 m in diameter. The surge drum is 4 m high and 1 m in diameter. The normal flow through the tower is 3.8 kg/s at a pressure of 23 bar and a temperature of 43C. The relevant lines are 3" in diameter. The H_2S content is only 0.6%, so that significant releases of H_2S are not to be expected. Only the risk of the release of LPG therefore is considered in the analysis.

3.3.2 The audit

In this case the audit was performed on site by interviewing plant personnel, and inspecting the technical state of the plant. The audit was performed in two sessions.

The purpose of the first session was to inspect the technical state of the plant and to establish the distribution of responsibilities among the plant personnel. In addition relevant documents were assembled, which enabled a thorough preparation of the second session.

In preparation for the second session, the personnel and their responsibilities were mapped onto the I-Risk schematic. It was determined in which boxes of the management system each member of personnel had functions. This helped in restricting the amount of questions to the necessary minimum. Even so, the second session needed to be cut to an acceptable compromise between the details wanted by the audit team and the time available on the plant. Nevertheless, the preparatory phase proved of enormous value in the second session.

The audit was performed in duplicate, by two separate auditors. They agreed fairly well in their judgements, which indicates that a well constructed approach has a harmonising effect on the audit. However, this exercise and the following one did not provide sufficient material to draw definitive conclusions on the level of preparation needed for auditors who were not previously involved in the investigation.

3.3.3 Master Logic Diagram of the Tower

Following the MLD methodology the following direct causes for LOC have been identified:

- Failure of Tower owing to material ageing
- Tower failure from overpressure caused by pressure increase caused by heat flux from external heat source.
- Tower failure from overpressure owing to overfilling.
- Tower failure owing to freezing.
- Extra loads owing to a road accident

Each "direct cause of LOC" in the Master Logic Diagram can be considered as a joint event, which consists of one initiating event and the failure of one or more safety functions that are served by either systems (hardware) and/ or operator procedures. In certain circumstances there are no safety functions present and hence the direct cause of LOC of the MLD will be the initiating event itself.

Direct Causes "Tower failure owing to material ageing" and "Tower failure owing to freezing" lead to Tower failure since the safety function in this case is the structural strength of the tower material, which by definition is exceeded by stress.

Direct Causes "Tower failure from overpressure caused by pressure increase caused by heat flux from external heat source" and "Tower failure from overpressure owing to overfilling" are considered as joint events consisting of one initiating event and failure of one or more safety systems. These two events are further analysed in order to identify all the initiating events of this system, which are presented in Table 3.1. The safety systems required to prevent the occurrence of LPG release, for all initiating events, are presented in Table 3.2.

Table 3.1. List of initiating events

1. Operating conditions off specifications
2. External fire
3. High inlet of MEA owing to valve failure
4. No outlet of MEA
5. High inlet of caustic (NAOH)
6. No outlet of caustic (NAOH)
7. High inlet of water owing to valve failure
8. No outlet of water
9. High inlet of LPG
10. No outlet of LPG

Table 3.2. List of safety systems

1. Pressure detection system
2. Fire suppression system
3. Pressure safety valves
4. Low level protection system in Tower T6654
5. High Level protection System in Tower T6654
6. Low level protection system in Tower T6655
7. High level protection system in Tower T6655
8. Low level protection system in Tower T6656
9. High level protection system in Tower T6656
10. Tower integrity

Next, event trees are constructed for all initiating events (IEs) presented in Table 3.1, defining the response of the plant and the spectrum of the resulting damage states. A typical event tree constructed for the initiating event "High inlet of MEA owing to valve failure" is presented in Figure 3.4. The first two tree paths (#1, #2) lead to a safe state and the third one leads to tower rupture owing to overpressure. A total of 10 event trees corresponding to 10 IEs have been developed.

Failures of systems have been modelled through the Fault Tree technique. Nine Fault Trees have been constructed for the first nine safety systems presented in Table 3.2. This results in the frequency of LOC in any of the three scrubbing towers being expressed in terms of 41 basic events. From an audit of the safety management system it was determined that all these events are affected by a single management system.

Figure 3.4. Event Tree with initiating event "High Inlet of MEA owing to valve failure"

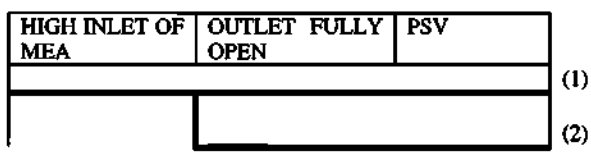


Table 3.3. Modification factors of technical parameters

Technical Parameter	Modification factor
Q_{o1}	9.1
Q_{o2}	9.0
Q_{M1}	9.3
Q_{M2}	9.0
f_l	9.5
Λ	9.3
T	9.4
f_m	9.3
T_R	9.1
T_M	9.2

Therefore, there were only eight management delivery systems to be assessed and quantified. Details of the audit procedure and the resulting quantification are reported elsewhere. The qualities of the eight outputs y_i (i=1,...,8) when combined with the weighting factors w_{ij} from the model provide the modification factors given in Table 3.3.

3.3.4 Risk quantification.

Using the numbers derived from the previously described procedure, the risk of the installation for its surroundings was quantified, by evaluating the frequency and the consequences of failures of the three parts of the scrubbing tower.

Three large Fault Trees with top events 'Tower T6654 Failure", "Tower T6655 Failure" and "Tower T6656 Failure" have been created, each consisting of an OR gate

Table 3.4: Frequencies of failure (per year)

Section of scrubber	T6654	T6655	T6656
Best possible case	1×10^{-7}/hr	1.1×10^{-6}/hr	1.0×10^{-7}/hr
Worst possible case	6.4×10^{-1}/hr	9.0×10^{-1}/hr	9.3×10^{-1}/hr
Plant as analysed	4.1×10^{-6}/hr	4.8×10^{-6}/hr	3.4×10^{-6}/hr

with inputs to the accident sequences leading to the corresponding top event.

Each accident sequence has then been developed in terms of an AND gate with inputs system failures and the initiating event of each accident sequence. Quantification has been performed for three cases according to the specific management system of the installation: a) using the values of the parameters corresponding to the best management system, b) using the values of the parameters corresponding to the worst management system and c) using the modified values of the parameters according to the quality of the management system and the values of Table 3.3. The three sets of calculations are given in Table 3.4.

The three sections of the scrubber, T6654, T6655 and T6656, contain flammable LPG, which will be released to the environment in case of a LOC. The sizes of the release will be 2700kg, 1200kg and 800 kg respectively. If LPG is ignited immediately, a fireball will occur. Otherwise LPG will disperse to the atmosphere as a dense cloud and either a flash fire or an explosion will occur. It is assumed that in case of delayed ignition there is a probability of 1/3 for flash fire and 2/3 for explosion. These values differ from values used in other contexts, such as the Dutch guidelines for quantitative risk analysis of chemical plants (Ale 1999, IPO 1994), so comparison of these results with results obtained with other methods, should be performed with care. In all cases, individual risk of death does not exceed 10^{-4} at a distance of 300m away from the towers.

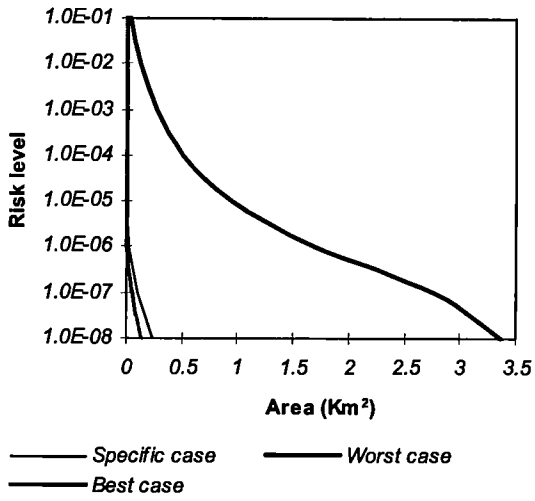
3.3.5 Management influence

In order to depict the sensitivity of the results for management influences the area inside risk contours was calculated depending on the quality of the management system. Three levels of quality of management systems are evaluated namely the specific system of this installation, the best and the worst which might occur. The area versus risk levels is presented in Figure 3.5.

The management group of the research team performed an audit that resulted in an assessment of the state of most management tasks that can be characterised as almost optimal. However, the feedback elements of each delivery system are those that could be further improved. Of the delivery systems themselves, the system on hardware,

control, plant interface, etc., is the one in which there is the most room for improvement. These are nevertheless qualitative results and do not provide further guidance on how important the potential improvements are, which to attempt first and, furthermore, how important is the maintenance of this level of excellence. The ability to integrate these management aspects into risk quantification provides some guidance on answering these questions. First, it is shown that the level of excellence implied by the quality assessment of the management audit is also supported by the QRA.

Figure 3-5 Area above certain risk levels (10^{-1}- 10^{-8}/yr)



For example, the frequency of LOC for Tower T6654 varies from $1.2x10^{-4}$/hr in the worst case to 10^{-10}/hr in the best case spanning a range of six orders of magnitude. The corresponding frequency of the plant has been assessed at $4.7x10^{-10}$/hr, approximately four times larger than the best possible value. This result indicates that it is much more important to try to maintain the present level of management quality rather than to try to improve it. More insight can be obtained through a sensitivity analysis. The derivatives of the frequency of LOC for tower T6654 with respect to the quality of the state of each managerial task have been calculated. It follows that this frequency is mostly sensitive to the performance of tasks by front line personnel:

- producing the right types of spares and on time for maintenance,
- the existence of appropriate procedures for various tasks,
- provisions for resolving conflicts between safety and non safety tasks, and
- providing the right incentives for personnel commitment.

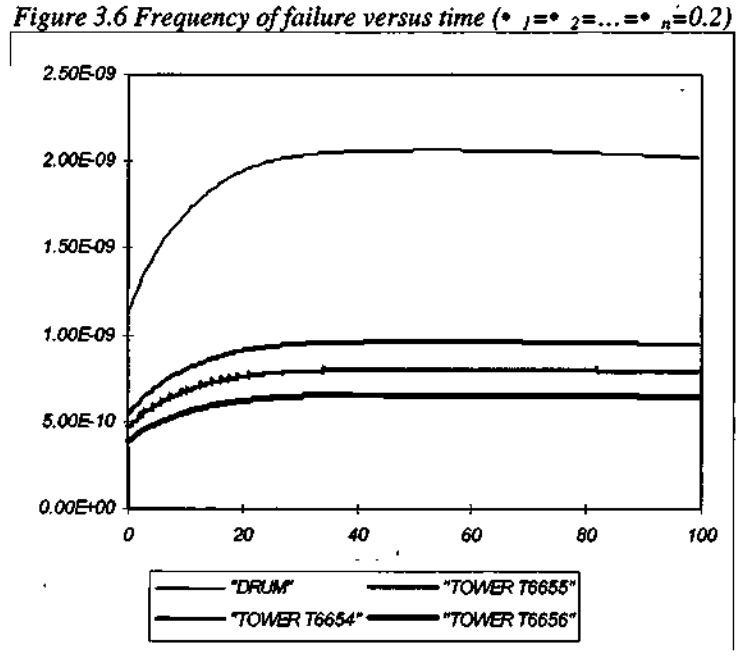
These tasks include the possibility for online correction of any deviation from desired or specified performance standards. Given the assessed values of the present quality, the area of conflict resolution could provide the largest reduction (among the four most important) in risk, since by changing from 9.1-10 it can reduce the frequency of LOC from $4.7x10^{-10}$/hr down to $3.2x10^{-10}$/hr.

It is noteworthy to remark that zero importance of a task, i.e. the derivative of the failure frequencies with respect to the quality of the task, indicates that such a task is not playing a role in the present performance of the system. These tasks are however instrumental in the time-dependent analysis of the future performance of the SMS that is, in keeping the system at its present level, improving it or letting it deteriorate.

3.3.6 Development over time

In this case it was also possible to calculate the development of the parameters of the technical model with time. As these parameters determine the frequency of failure, the development of the risks of the plant over time given the present quality of the management system can be predicted. When this works towards the negative, i.e. when the safety management deteriorates, it is also called management corrosion. In fig 3.6 the development of these parameters is depicted.

Figure 3.6 Frequency of failure versus time ($\bullet_1=\bullet_2=\ldots=\bullet_n=0.2$)



It can be seen that the present state is unstable and not in equilibrium. Over time a stable state will be reached.

3.3.7 Findings

Also for the refinery case, conclusions were drawn with respect to the management of the installation and with respect to the usefulness of the I-Risk system.

As far as the plant is concerned, the evaluation shows that the best course of action would be to maintain current management levels. However, conflict resolution at front line activities is a potential area of concern, which warrants further attention.

The I-RISK methodology with the modified interface between the management and the technical model proved to perform well. From the application to the scrubbing tower it has been demonstrated that the combination of qualitative evaluation and quantitative analysis gives valuable insights in worthwhile courses of action to maintain and improve the safety performance of an installation.

3.4 Ammonia storage

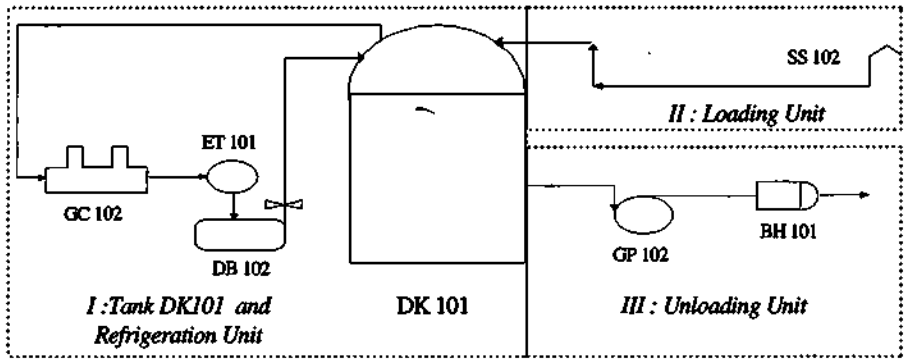
The application of the I-Risk system to the third and last example case, plant C, was the most developed and the most extensive. In this case all the management subsystems were considered separately. Only the time dependent behaviour of management systems could not be modelled. The ranges of values used in the interface between the technical and the management model were different from those used in the previous example as these were considered more appropriate by the actual analysts.

The installation has been subject of extensive studies before. A complete quantified risk analysis and an earlier safety audit performed under the PRIMA project were available.

3.4.1 The plant

The installation under consideration consists of a storage tank holding 15000 tons of refrigerated ammonia. The tank is fitted with a refrigeration unit consisting of compressors, condensers and separation units. The tank is connected to a loading unit were ammonia is transferred from a ship to the tank. Ammonia is pumped from the tank to two adjacent fertilizer plants by way of three discharge pumps. (see figure 3.7)

Figure 3-7: Diagram of the ammonia cryogenic storage facility



Refrigeration Unit	DK 101 : refrigeration tank
GC 102: compressors	GP 102 unloading pumps
ET 101: condensers	BH 101: heating unit
DB 102 :separation drum	SS 102: loading arms

In this plant three locations could be identified where a release of ammonia could take place: The storage vessel itself with its refrigeration unit, the loading and the transfer section.

3.4.2 Events and causes considered

In this case as in the previous example there is a wide range of possible failures. However, only a limited number is considered worth following up with a deeper analysis.

Loss of containment in the storage tank obviously is a major contributor to the risk. Of the potential causes an internal pressure increase, internal under-pressure and excessive external loading are considered.

Three pathways for loss of containment in the loading section are considered: corrosion of the pipe-work, pressure shock and excessive external loading.

Of the possible causes of loss of containment in the unloading section only internal pressure increase is considered.

For each of these pathways Master Logic Diagrams were produced similar to those for the other examples.

3.4.3 The audit

The audit was conducted in much the same way as in the refinery case. Some other members of the project team were involved. This led to some additional points that

needed to be clarified. Especially, the translation of the findings on the individual auditors into the parametric values of the management model still caused difficulties. The correlation between the results of the various auditors varied widely. From subsequent evaluation of the differences it appears that consensus between the auditors can be achieved. However, a discussion between the auditors obviously leads to the loss of the independent check on the ratings.

A serious problem in the audit was that not all the documentation was in a language all members of the team could understand. In part this was compensated because older, existing documentation was extensive. Nevertheless it is preferred to have all documentation in a common language.

The audit went much more smoothly than in case B, indicating that the changes indeed were improvements.

In terms of quality of management, this plant did not score as well as plant B, which scored almost top of the scale. This translates into the resulting failure frequencies as described in the next section.

3.4.4 Results

For this case the sensitivity of the results for the various parts of the management system were evaluated. In this case, just as in test-case B, the tasks of the frontline personnel for providing the right type of spares in good time are critical for the ultimate frequency of failure. For a number of specific scenario's the frequencies for the current management system are given together with the best and worst possible cases in table 3.5

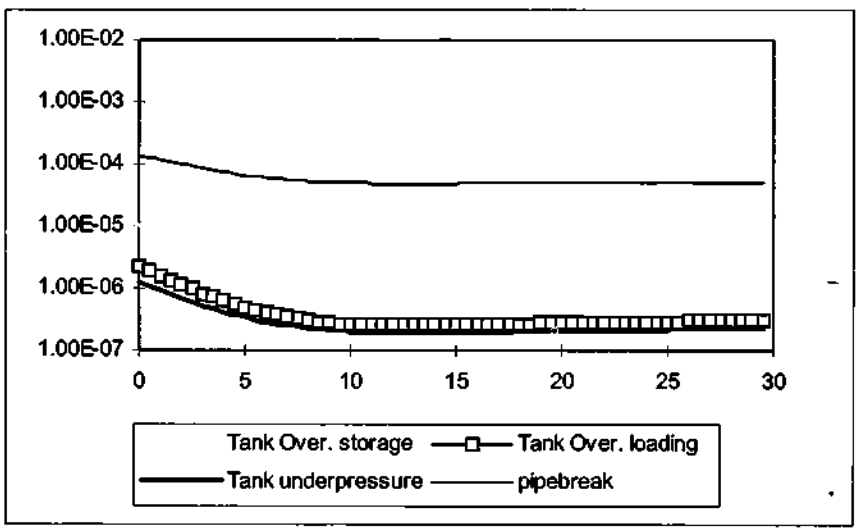
Table 3-5 Current, best and worse case frequencies

Management mode	Frequency of failure/hr			
	Overpressure of tank during storage	Overpressure of tank during loading	Underpressure of tank	Pipebreak from ship to tank
Current state	$1.1\ 10^{-5}$	$2.2\ 10^{-6}$	$1.2\ 10^{-6}$	$1.4\ 10^{-4}$
Worst case	$6.1\ 10^{-3}$	$8.7\ 10^{-2}$	$5.5\ 10^{-4}$	$5.0\ 10^{-2}$
Best case	$2.9\ 10^{-10}$	$4.3\ 10^{-10}$	$1.9\ 10^{-10}$	$5.5\ 10^{-6}$

This plant is much further away from the best possible state than the plant in example B. There is thus more room for improvement.

However, for the development in time of the frequency, that is the rate and direction at which the safety performance of the plant evolves over time, the company's risk control management system is the dominant factor. Also here the initial state is unstable. Over time the safety situation of the plant will settle in a stable equilibrium. (Figure 3.8). Just as in case B the final state will be one with a better safety performance than the current state, provided the management systems as currently in place will keep existing.

Figure 3-8: Development of the performance scores over time



3.5 Conclusion

In conclusion it can be stated that the three tests were material in the development of the methodology. The first test led to the construction of a working interface between the technical and the management model. The second test led to a better structure of the auditing process.

The methodology gives a good insight into the quality of the management and consistent results with respect to the influence of management on the safety of a plant.

The audit can be performed more efficiently by tightening the planning process, sharpening the focus on specific major hazard scenarios and improving the support for recording information and arriving at a well-calibrated evaluation. These improvements will grow over time as the methodology is applied in more and more cases.

The audit process is greatly helped when the audit team has available the Master Logic Diagrams and the reasoning behind it. Especially those scenarios which from a technical point of view merit close scrutiny should be know to the management auditors in advance.

Priority items for the management audit are tasks that are common to many activities in the plant and thus may constitute a common mode for either failure or success.

It is possible to predict the future development of the safety situation in a plant. This is of potential of great value in practice. Management changes will not have immediately noticeable effects. The I-Risk methodology can help to establish whether a company is on the right track and will meet its goals in the near future. The quantitative results produced in this study warrant a further investigation into the transient behaviour with special attention for potential numerical effects in the results.

It should be borne in mind that the installations in the examples have been small and relatively simple. Further work is needed to make the I-Risk method feasible for large installations with many possibilities of Loss of Containment.

In all, the primary objectives of this study were achieved. A practicable audit system was developed, together with an interface between the technical and the management model which made it feasible to do something not possible in a rigorous way before: to incorporate site specific information on the quality of the management in a quantified risk assessment.

4. DISCUSSION

4.1 Were the objectives met?

For the purpose of clarifying the success of the project in meeting the various objective and functional requirements that were agreed at the beginning of the project (and which are set out in Section 1 of this report), the requirements have been broadly grouped into the following eight components:

1. General
2. Technical model: loss of containment
3. Technical model: consequences (on site, off site and environment)
4. Management model
5. Technical-management interface model
6. Time model
7. Risk picture
8. I-QRA method.

The project objectives relating to each of these components is summarised in Table 4.1, together with an indication of whether the objectives have been met, and in that case where in the report the relevant work is described. Where the requirements have not been met, or have only been partially met, some comment is given on the scope or reason for the shortfall.

Table 4.1: Were the project objectives met?

Component	Objectives	Achieved ?	Cross Reference: Main Text	Cross Reference: Annex	Comment
1. General	The model will be developed within the context of the Seveso II Directive	Yes	Section 1.1		
2. Technical model: loss of containment	The integrated model will address the following components of the QRA:				
	- Plant data collection model	Yes		1 & 4.1	
	- Parameters of LOC frequency calculation models for releases their mitigation or escalation	Yes	Section 2.1.2	2 & 3	
3. Technical model: consequences (on site, off site and environment)	Consequence models will be made use of and where missing will be identified	Partial	Section 2.6		Environmental models not included
4. Management model	The management model should contain components of self monitoring/correcting (continuous and periodic short term and long term)	Yes	Section 2.1.3	2	
5. Technical-management interface model	The technical management interactions must be developed to a point where	Yes	Section 2.1.4	3	
	management exerts a common mode effect	Yes	Section 2.1.4	3	
	Should be modelled in detail				
6. Time model	The management model should be able to model time varying component of	Yes	Section 2.1.3	4.4 & 4.5	
	control/monitoring/correction	Yes	Section 2.1.3	4.4 & 4.5	
	Time varied rather than time averaged, risk projection based on current technical management status				
7. Risk picture	Show dominant risks so that:				
	- risk reduction strategies can	Yes	Section 2.8	4.1 & 4.4	
	be identified	Yes	Section 2.9	4.1 & 4.4	
	- key performance indicators (management corrosion monitors) will be identified	No			Too ambitious at this stage in the development of the model
	Investigate the effects of organisational change (such as reduced manning) on risk				
8. I-QRA method	A field tested I-Risk QRA procedure, including data collection methods, for site specific application when carrying out such a QRA	Yes	Sections 2 & 3	5	

4.2 The project development process

The project team began with the idea that on the one hand there is Quantitative Risk Assessment, on the other hand there are safety management audits, and that it would be valuable to integrate the two to address major hazard management.

The two integrated aspects were to be:

1) A technical model, different from that used in the Netherlands or UK;
2) An audit model different from PRIMA (EU Contract Research Report 1995) because it had to be adapted to a technical model.

Developing a technical model appeared to be a much more straightforward process than the management model development which was more difficult and took considerably more time than had been envisaged. Although separate teams developed the models, there was a continuous process of interfacing the two. In ensuring a good fit, the need for cross-disciplinary understanding was critical and the Steering Committee meetings were vital for the discussions and question and answer sessions that enabled modifications and further developments to each model to be made.

Amongst other things, this process resulted in a whole new way of auditing organisations. With a classic audit one goes on site with topics and questions and, based on the results, the auditors decide if the company is stronger or weaker in certain parts. But if quantification is required as in I-Risk, the state of completeness of the management system for the relevant major hazard related tasks has to be dealt with, otherwise the numbers cannot be depicted. Tackling this problem involved a detailed confrontation between the mathematical modelling, the technical modelling and the management modelling. The technical modellers had to find a logical structure for the quantification of the IRMA model that was acceptable to both teams. This process forced the management auditors to come off the fence and say clearly what they were judging. In addition, the model started to become dynamic with questions about the (quantification) effects of one management process box of the IRMA model on another. This had never been done before and revealed a serious absence of data and observation on which to base hypotheses. Unfortunately at this point time and resources were running out.

Looking back, was enough time spent scrutinising the model?

The technical model is very robust. With the exception of the Master Logic Diagram and the corrosion model the rest was a rearrangement of what had already existed. The question as to whether it was a good technical model for the test sites includes considering whether the level of detail gives some additional insight.

There were new insights into the management system when integrating at a detailed technical level, particularly the clearer focus on the relevant management processes and content for major hazards. However, a full-scale site I-QRA at this level of detail is not currently practical

The demands on the resources of the I-Risk team and on the site personnel were considerable in the test cases for both the technical and management modelling. . One very important lesson was that the team could not build an I-Risk technical model away from the site because of the required level detail. With the management model there was not a rigid audit question set. The questions had to be formulated in a way that adapted to the management and technical specifics of the installation. This is different from previous audit methods. However, the question generation process

was a difficult problem to solve and I-Risk still requires auditors to follow a procedure to generate them. This necessitates an understanding of the I-Risk model and its procedures that currently puts an exceptional demand on the auditors and on audit preparation.

In the beginning, the technical group and the management group were two groups, but by the end of the project they were operating as one. This was quite an achievement. Despite the enormous demands of the complexity of what the team set out to do, and the practical difficulties, the authors of the I-Risk method believe that the paradigm shift was worthwhile. The main problem that remains is how to communicate the new viewpoint.

4.3 Advantages of the method

Before discussing the advantages of the method, a few disadvantages have to be mentioned. In its present state, applying I-Risk takes a multifunctional team of at least a technical risk analyst and an expert in safety management auditing. Apart from that they also have to speak and understand each others vocabularies. As such, the method is highly specialised and its dissemination in its present state, in the sense of having this method broadly applied within industry and among regulators, will be very hard.

However there are many advantages to the method.

It was feared that building the technical model would be extremely time consuming and building a technical model for a refinery, for example, would cost man-months if not man-years. The first test results show that this may not be necessarily true. A technical model built out of a few vessels and equipment gave sufficient input for the IRMA model to ultimately generate generic results for a whole refinery. Of course, this is under the condition that the safety management system and all the codes and standards on that particular site are coherent and used in the same way for every installation.

From an inspection/auditing point of view, roughly speaking the method consists of a reliability engineering driven safety management audit. The advantage is that for the first time in the history of this type of audit it is possible to solely investigate all the parts of the management system that are relevant to major hazards, the latter being defined as hazards that are connected to loss of containment and the release of dangerous substances. As such, it was possible to link every question in the audit and every topic that was discussed to a very specific part of the installation or even part of the equipment. This gives a safety management audit a tremendous focus and impact. Also it proved possible to make the results of the audit generic, meaning that generic statements could be made on the improvement of certain aspects in the safety management system, all having to do with major hazards.

From a reliability point of view, using and studying the method will make it clear which parameters used in reliability engineering can or will be influenced by the safety management system. It will therefore be easier in decision making to prioritise the relevant reliability issues not only purely on the numbers but also on relevance to the safety management system. With this method the first step towards a truly integrated quantified risk assessment methodology was made.

Regarding the time simulation of management quality, the model that is used is promising. With the different orders of loops and their cycle times it seems to be possible to actually measure and predict improvement and or detoriation of certain

management system aspects. As such, the application of this concept has broader implications than major hazard safety itself. The possibility to build the model in software will create a powerful tool with which, after further research and validation, it will be possible to study the behaviour of management models over time.

5. FUTURE DEVELOPMENTS

Both the purpose and achievement of the project was to make a risk assessment that can include the effects of management. However, the fruits of the integrated multidisciplinary approach are in the future, particularly with the mathematical modelling providing the dialogue mechanism between the multi-disciplines.

When the I-Risk model has been applied several more times (currently there have been only 2 full test cases), using the structure and procedures which determine the I-Risk assessment process, changes in the details may be made, but the fundamentals should stay the same. The danger is that we may be overconfident in the use of the system as it is now so we know that a few cases of experience are needed.

Although the modelling process has changed the way the project team think about risk assessment and management, the weakness of the I-Risk model is that it is very difficult to grasp and so some way of making it more accessible should be found. The important thing is not to treat it like a black box. This I-Risk report and its annexes specify what is in the I-Risk "box", even if it is only a mathematical content; it is not magic. The model has been derived from a multidisciplinary team. Although it is not often that there is an opportunity to get these disciplines together, in order to apply the I-Risk model, in the beginning one needs people from both the technical and the management disciplines.

However, further developments could make this unnecessary. At this stage the I-Risk "box" is not rigorous enough that we can say that what is in it is perfectly satisfactory and that we can determine what we can get out based on what we throw in. However, if I-Risk can be shown to produce consistent results, then the user can throw audit scores into the system, say, and out will come the result. Until that state is reached it will be necessary to have people evaluate (judge) management system quality. If that state could be reached, however, it would be a great advantage for the technical disciplines that do not understand about management systems and hence cannot make those judgements.

It is considered possible that in the future an I-Risk type approach is the way governments will look at companies with major hazards which means that this is how companies will look at themselves. In addition, I-Risk deals with the time element associated with change in management quality. This may make integrating management assessment with QRA more attractive than in any previous system such as PRIMA where there was a risk model and a management factor that did not change (Hurst et al, 1996). The time questions such as "how long does change take?", "what data are relevant management quality monitors?", and "how frequently should data be sampled and reviewed?" can now be fitted into a model structure that targets the important risk issues. There is the capability for identifying the sequencing of improvements in the management system processes because of being able to specify what makes a bigger difference to the risk. This is a prime motivation for doing an I-Risk assessment. Also, the sort of reaction from the companies is to ask whether I-Risk is a way to see more clearly what they are doing in risk management.

Perhaps I-Risk could be made less detailed for achieving the same result, and so give greater opportunity to apply it. For example, revising the management audit process to be a verification of a company's filling in of a standard preliminary questionnaire sent and returned before site visit would considerably reduce the need for time and resources.

Looking to the future, integration is an important topic in the EU. Application of an I-Risk approach to other kinds of risks (besides major hazards in chemical manufacturing) is achievable. Development of a risk management simulator is a real possibility, which could provide the basis for specifying risk management performance indicators for a company.

On the other hand, the I-Risk report may be put on the shelf, never looked at again, and the opportunity for developing the model further lost. The authors are confident that this will not happen.

6. REFERENCES

6.1 Bibliography of Publications Used in the Project

AIChE/CCPS (1989). "Guidelines for Chemical Process Quantitative Risk Analysis", 345 East 47th Street, New York, NY 10017 (ISBN 0-8169-0402-2).

Ale, B.J.M., P. Uijt de Haag, (1999) Guideline for Quantitative Risk Assessment, RIVM, april 1999.

Apostolakis G., Kaplam S., Garrick B.J., Bley D., Woodard D., "Methodology for Probabilistic Risk Assessment of Nuclear Power Plants", Pickard, Lowe and Garrick, Inc, PLG -0209.

Bellamy, L.J. and Tinline G (1993) Development of a Safety Management System Audit which addresses Loss of Containment Risks on Major Hazard Installations" Paper presented at 3ASI Conference, Milan, Italy, 23 November 1993.

Bellamy J.L.& Wright S. M., Hurst W. (1993) History and development of a safety management system audit for incorporation into quantitative risk assessment. International process safety management Conference and Workshop San Francisco California Part II. September 1993.

EU Contract Research Report (1995) Auditing and Safety Managemnt for Safe Operations and Land Use Planning. Contract EV5V-CT92-0068.

Hale A.R., Heming B. Carthey J., & Kirwan B. 1997. Modelling of safety management systems. Safety Science 26 (1/2) 121-140.

Hale A.R., Kirwan B., & Guldenmund F. (1999). Capturing the river: multi-level modelling of safety management. In Misumi J, Wilpert B. & Miller R. (eds.) Nuclear safety: a human factors perspective. Taylor & Francis. London.

Hannaman, G.W., Spurgin, A.J. & Lukic, Y.(1985). "Model for assessment human cognitive reliability in PRA studies", IEEE third conf. on factors and nuclear power plants, Monterey, CA.

HSE (1989). "Risk criteria for land-use planning in the vicinity of major industrial hazards" ISBN. 0 - 11-885491-7, London.

Hurst N.W., Young S., Donald I., Gibson H & Muyselaar A. 1996. Measures of safety management performance and attitudes to safety at major hazard sites. J. of Loss Prevention in the Process Industry. 9(2). 161-172.

IAEA(1995). "Guidelines for Integrated Risk Assessment and Management in Large Industrial Areas", IAEA-TECDOX-XXX,Vienna, Austria.

IAEA (1993). "Manual for the classification and prioritization of risks due to major accidents in process and related industries", IAEA-TECDOC-727, Vienna.

IPO (1994), Handleiding voor het opstellen en beoordelen van een extern veilgheidsrapport, INFO transfer, the Netherlands.

Lees, Frank P., (1980) Loss Prevention in the Process Industries, Volume 1 chapter 9

Lees, F.P. (1996). "Loss Prevention in the Process Industries", Butterworth & Co Ltd, London, Second edition (ISBN 09506 1547 8).

Muyselaar, A.J. and Bellamy, L.J.(1994) "An Audit Technique for the Evaluation and Management of Risks". Paper presented at the CEC DGXI workshop on Safety Management in the Process Industry, October 7-8, 1993, Ravello, Italy. pp. 175-192 in "Safety Management Systems in the Process Industry" Ed. P.C. Cacciabue et al, Report EUR 15743 EN, European Commission, 1994.

N.K.A. (1985). "PSA Uses and Techniques: a Nordic perspective"

NUREG (1984). "Probabilistic Safety Analysis Procedures Guide", NUREG/ CR-2815, US Nuclear Regulatory Commission, Washington, DC 20555.

OREDA-97 (1997) " Offshore Reliability Data", 3rd Edition, Det Norske Veritas, Norway, (ISBN 82-14-00438-1).

Papazoglou, I.A., and Aneziris, O.N. (1998). "QRA Technical models Workpackage 2: Report D.5", Athens.

Papazoglou, I.A., Nivolianitou Z.,Aneziris O.,Christou M. (1992). "Probabilistic safety analysis in chemical installations", Journal of Loss Prevention in the Process Industries, 5,3,181-191.

Pitblado, R., J.C. Williams, D.H. Slater, (1990). "Quantitative Assessment of Process Safety Programs". Plant/Operations Progress,Vol. 9, No 3, 169-175.

SAVE/SZW (1996) AVRIM2 manual version 1.0: The internal safety report (AVR) assessment and inspection method. Produced by SAVE Consulting Scientists for the Ministry of Social Affairs and Employment (SZW), The Hague, The Netherlands

TNO (1989) "Methods for determination of possible damage to people and objects resulting from releases of hazardous materials" (Green Book), Voorburg.

Van de Mark R., 1996, "Generic Fault trees and the modeling of management and organization". Final year report Dept. of Statistics, Probability and Operations Research. TU Delft.

VROM (1990). "Dutch National Environmental Policy Plan - Premises for Risk Management: Risk Limits in the Context of Environmental Policy". Annex to the Dutch National Environmental Policy

Plan. "Kiezen of Verliezen". Second Chapter of the States General, 1988-89, session, 21137, nos. 1-2, VROM 00197/4-90, The Hague.

6.2 I-Risk Publications

Ale, B.J.M, J.G.Post, L.J. Bellamy, (1998) "The interface between the technical and the managment model for use in quantified risk assesment", in A. Mosleh and R.A. Bari (eds) Probablistic Safety Analysis and Managment 4, Springer 1998

Alme, I. A. (1998) A safety audit approach for quantifying management control of risk. Graduation Report. Safety Science Group. Delft University of Technology.

Bellamy L., J.I.H. Oh, A.R. Hale, I.A. Papazoglou, B.J.M. Ale., M. Morris, O. Aneziris, J.G. Post, H. Walker, W.G.J. Brouwer, A.J. Muyselaar, (1999). "IRISK Development of an integrated technical and management risk control and monitoring methodology for managing and quantifying on-site and off-site risks"

Bellamy L., Ale, B.J.M., Post J.G., Hale, A.R., Guldenmund, F., Papazoglou, I.A., & Aneziris, O. (1999) Integrated risk assessment: The interface between management and technical modelling. , Risk and Crisis Management, 2nd International Conference at Liege, May 1999.

Costa M.A.F. (1998) Relative weight of maintenance management influences on technical risk parameters. Graduation report. Safety Science Group. Delft University of Technology & University of Minho

Hale A.R., Bellamy L.J., Guldenmund F., Heming B.H.J. and Kirwan B., (1997). Dynamic modelling of safety management in Guedes Soares C. (ed.) Advances in Safety & Reliability. Pergamon. Oxford. 63-70.

Hale A.R., Costa M.A.F., Goossens L.H.J & Smit K. (1999) Relative importance of maintenance management influences on equipment failure and availability in relation to major hazards. Paper to ESREL conference 1999 Munich

Hale A.R.& Guldenmund F. (1997) Insights into safety management and culture based on formal representational methods. Proceedings of the International Ergonomics Association Conference. Tampere.

Hale A.R., F. Guldenmund, L. Bellamy, (1998)."An Audit Method for the Modification of Technical Risk Assessment with Management Weighting Factors", Proceedings of the 4th International Conference on Probabilistic Safety Assessment and Management, Edited by A. Mosleh and R.A. Bari., Vol 3, pp2093, N.Y.

Hale A.R., Guldenmund F., & Bellamy L. (1998b). An audit method for the modification of technical risk assessment with management weighting factors. in Mosleh A. & Bari R.A. (eds.) Probabilistic Safety Assessment and Management. Springer. London. 2093-2098

Hale A.R., Guldenmund F, Bellamy L. & Wilson C., (1999). IRMA: Integrated Risk Management Audit for major hazard sites. Paper to ESREL conference 1999 Munich

Hale A.R., Guldenmund F., Smit K. Bellamy L. (1998a). Modification of technical risk assessment with management weighting factors in Lydersen S., Hansen G.K. & Sandtorv H.A. (eds.) Safety & Reliability. Springer. London. 115-120

Hale A.R., Kirwan B., & Guldenmund F. (1999). Capturing the river: multi-level modeling of safety management. In Misumi J., Wilpert B., & Miller R. (Eds.) Nuclear safety: a human factors perspective. London. Taylor & Francis. Pp 161-182.

Oh J.I.H., Brouwer W.G.J., Bellamy L.J., Hale A.R., Ale B.J.M. & Papazoglou I.A. (1998) The I-Risk project: development of an integrated technical and management risk control and monitoring methodology for managing and quantifying on-site and off-site risks. in Mosleh A. & Bari R.A. (eds.) Probabilistic Safety Assessment and Management. Springer. London. 2485-249

Papazoglou I. A., O. Aneziris, (1998a). "System Performance Modeling for Quantification of Organizational Factors in Chemical Installations", Proceedings of the 4th International Conference on Probabilistic Safety Assessment and Management, 13-18 September, New York, Edited by A. Mosleh and R.A. Bari, Vol 3, pp2081-6, N.Y.

Papazoglou I. A., O. Aneziris, (1998b). "QRA Technical Models", IRISK Report, NCSR "DEMOKRITOS", Athens, Greece.

Papazoglou I. A., and Aneziris O.N. (1999), Integrating Management Effects into the Quanntified Risk Assessment of an LPG Scrubbing Tower, accepted for ESREL 99, Munich, September 1999.

Papazoglou I. A., and Aneziris O.N., Ale B., Bellamy L (1999), Effects of the management system of a chemical installation to risk assessment, Risk and Crisis Management, 2nd International Conference at Liege, May 1999.

European Commission

EUR 19320 — I RISK: A quantified integrated technical and management risk control and monitoring methodology

Luxembourg: Office for Official Publications of the European Communities

2000 — 94 pp. — 17.6 x 25 cm

ISBN 92-828-9483-5

Price (excluding VAT) in Luxembourg: EUR 14.50

Venta • Salg • Verkauf • Πωλήσεις • Sales • Vente • Vendita • Verkoop • Venda • Myynti • Försäljning
http://eur-op.eu.int/general/en/s-ad.htm

BELGIQUE/BELGIË

Jean De Lannoy
Avenue du Roi 202/Koningslaan 202
B-1190 Bruxelles/Brussel
Tél. (32-2) 538 43 08
Fax (32-2) 538 08 41
E-mail: jean.de.lannoy@infoboard.be
URL: http://www.jean-de-lannoy.be

La librairie européenne/ De Europese Boekhandel
Rue de la Loi 244/Wetstraat 244
B-1040 Bruxelles/Brussel
Tél. (32-2) 295 26 39
Fax (32-2) 735 08 60
E-mail: mail@libeurop.be
URL: http://www.libeurop.be

Moniteur belge/Belgisch Staatsblad
Rue de Louvain 40-42/Leuvenseweg 40-42
B-1000 Bruxelles/Brussel
Tél. (32-2) 552 22 11
Fax (32-2) 511 01 84
E-mail: ousales@just.fgov.be

DANMARK

J. H. Schultz Information A/S
Herstedvang 12
DK-2620 Albertslund
Tlf. (45) 43 63 23 00
Fax (45) 43 63 19 69
E-mail: schultz@schultz.dk
URL: http://www.schultz.dk

DEUTSCHLAND

Bundesanzeiger Verlag GmbH
Vertriebsabteilung
Amsterdamer Straße 192
D-50735 Köln
Tel. (49-221) 97 66 80
Fax (49-221) 97 66 82 78
E-Mail: vertrieb@bundesanzeiger.de
URL: http://www.bundesanzeiger.de

ΕΛΛΑΔΑ/GREECE

G. C. Eleftheroudakis SA
International Bookstore
Panepistimiou 17
GR-10564 Athina
Tel. (30-1) 331 41 80/1/2/3/4/5
Fax (30-1) 323 98 21
E-mail: elebooks@netor.gr

ESPAÑA

Boletín Oficial del Estado
Trafalgar, 27
E-28071 Madrid
Tel. (34) 915 38 21 11 (libros),
913 84 17 15 (suscripción)
Fax (34) 915 38 21 21 (libros),
913 84 17 14 (suscripción)
E-mail: clientes@com.boe.es
URL: http://www.boe.es

Mundi Prensa Libros, SA
Castelló, 37
E-28001 Madrid
Tel. (34) 914 36 37 00
Fax (34) 915 75 39 98
E-mail: libreria@mundiprensa.es
URL: http://www.mundiprensa.com

FRANCE

Journal officiel
Service des publications des CE
26, rue Desaix
F-75727 Paris Cedex 15
Tél. (33) 140 58 77 31
Fax (33) 140 58 77 00
E-mail: europublications@journal-officiel.gouv.fr
URL: http://www.journal-officiel.gouv.fr

IRELAND

Alan Hanna's Bookshop
270 LR Rathmines Road
Dublin 6
Tel. (353-1) 496 73 98
Fax (353-1) 496 02 28
E-mail: hannas@iol.ie

ITALIA

Licosa SpA
Via Duca di Calabria, 1/1
Casella postale 552
I-50125 Firenze
Tel. (39) 055 64 83 1
Fax (39) 055 64 12 57
E-mail: licosa@licosa.com
URL: http://www.licosa.com

LUXEMBOURG

Messageries du livre SARL
5, rue Raiffeisen
L-2411 Luxembourg
Tél. (352) 40 10 20
Fax (352) 49 06 61
E-mail: mail@mdl.lu
URL: http://www.mdl.lu

NEDERLAND

SDU Servicecentrum Uitgevers
Christoffel Plantijnstraat 2
Postbus 20014
2500 EA Den Haag
Tel. (31-70) 378 98 80
Fax (31-70) 378 97 83
E-mail: sdu@sdu.nl
URL: http://www.sdu.nl

ÖSTERREICH

Manz'sche Verlags- und Universitätsbuchhandlung GmbH
Kohlmarkt 16
A-1014 Wien
Tel. (43-1) 53 16 11 00
Fax (43-1) 53 16 11 67
E-Mail: manz@schwinge.at
URL: http://www.manz.at

PORTUGAL

Distribuidora de Livros Bertrand Ld.ª
Grupo Bertrand, SA
Rua das Terras dos Vales, 4-A
Apartado 60037
P-2700 Amadora
Tel. (351) 214 95 87 87
Fax (351) 214 96 02 55
E-mail: dlb@ip.pt

Imprensa Nacional-Casa da Moeda, SA
Sector de Publicações Oficiais
Rua da Escola Politécnica, 135
P-1250-100 Lisboa Codex
Tel. (351) 213 94 57 00
Fax (351) 213 94 57 50
E-mail: spoce@incm.pt
URL: http://www.incm.pt

SUOMI/FINLAND

Akateeminen Kirjakauppa/ Akademiska Bokhandeln
Keskuskatu 1/Centralgatan 1
PL/PB 128
FIN-00101 Helsinki/Helsingfors
P./tfn (358-9) 121 44 18
F./fax (358-9) 121 44 35
Sähköposti: sps@akateeminen.com
URL: http://www.akateeminen.com

SVERIGE

BTJ AB
Traktorvägen 11-13
S-221 82 Lund
Tfl. (46-46) 18 00 00
Fax (46-46) 30 79 47
E-post: btjeu-pub@btj.se
URL: http://www.btj.se

UNITED KINGDOM

The Stationery Office Ltd
Customer Services
PO Box 29
Norwich NR3 1GN
Tel. (44) 870 60 05-522
Fax (44) 870 60 05-533
E-mail: book.orders@theso.co.uk
URL: http://www.itsofficial.net

ÍSLAND

Bokabud Larusar Blöndal
Skólavördustig, 2
IS-101 Reykjavik
Tel. (354) 552 55 40
Fax (354) 552 55 60
E-mail: bokabud@simnet.is

NORGE

Swets Blackwell AS
Østenjoveien 18
Boks 6512 Etterstad
N-0606 Oslo
Tel. (47-22) 97 45 00
Fax (47-22) 97 45 45
E-mail: info@no.swetsblackwell.com

SCHWEIZ/SUISSE/SVIZZERA

Euro Info Center Schweiz
c/o OSEC
Stampfenbachstraße 85
PF 492
CH-8035 Zürich
Tel. (41-1) 365 53 15
Fax (41-1) 365 54 11
E-mail: eics@osec.ch
URL: http://www.osec.ch/eics

BĂLGARIJA

Europress Euromedia Ltd
59, blvd Vitosha
BG-1000 Sofia
Tel. (359-2) 980 37 66
Fax (359-2) 980 42 30
E-mail: Milena@mbox.cit.bg

ČESKÁ REPUBLIKA

ÚSIS
odd. Publikací
Havelkova 22
CZ-130 00 Praha 3
Tel. (420-2) 24 23 14 66
Fax (420-2) 24 23 11 14
E-mail: publikace@usiscr.cz
URL: http://www.usiscr.cz

CYPRUS

Cyprus Chamber of Commerce and Industry
PO Box 21455
CY-1509 Nicosia
Tel. (35
Fax (35
E-mail

EESTI

Eesti Kaubandus-Tööstuskoda
(Estonian Chamber of Commerce and Industry)
Toom-Kooli 17
EE-0001 Tallinn
Tel. (372) 646 02 44
Fax (372) 646 02 45
E-mail: einfo@koda.ee
URL: http://www.koda.ee

HRVATSKA

Mediatrade Ltd
Pavla Hatza 1
HR-10000 Zagreb
Tel. (385-1) 481 94 11
Fax (385-1) 481 94 11

MAGYARORSZÁG

Euro Info Service
Expo tér 1
Hungexpo Európa Központ
PO Box 44
H-1101 Budapest
Tel. (36-1) 264 82 70
Fax (36-1) 264 82 75
E-mail: euroinfo@euroinfo.hu
URL: http://www.euroinfo.hu

MALTA

Miller Distributors Ltd
Malta International Airport
PO Box 25
Luqa LQA 05
Tel. (356) 66 44 88
Fax (356) 67 67 99
E-mail: gwirth@usa.net

POLSKA

Ars Polona
Krakowskie Przedmiescie 7
Skr. pocztowa 1001
PL-00-950 Warszawa
Tel. (48-22) 826 12 01
Fax (48-22) 826 62 40
E-mail: books119@arspolona.com.pl

ROMÂNIA

Euromedia
Str.Dr. Marcovici, 9, sector 1
RO-70749 Bucuresti
Tel. (40-1) 315 44 03
Fax (40-1) 315 44 03
E-mail: euromedia@mailcity.com

ROSSIYA

CCEC
60-letiya Oktyabrya Av. 9
117312 Moscow
Tel. (7-095) 135 52 27
Fax (7-095) 135 52 27

SLOVAKIA

Centrum VTI SR
Nám. Slobody, 19
SK-81223 Bratislava
Tel. (421-7) 54 41 83 64
Fax (421-7) 54 41 83 64
E-mail: europ@tbb1.sltk.stuba.sk
URL: http://www.sltk.stuba.sk

SLOVENIJA

Gospodarski Vestnik
Dunajska cesta 5
SLO-1000 Ljubljana
Tel. (386) 613 09 16 40
Fax (386) 613 09 16 45
E-mail: europ@gvestnik.si
URL: http://www.gvestnik.si

TÜRKIYE

Dünya Infotel AS
100, Yil Mahallessi 34440
TR-80050 Bagcilar-Istanbul
Tel. (90-212) 629 46 99
Fax (90-212) 629 46 27
E-mail: infotel@dunya-gazete.com.tr

ARGENTINA

World Publications SA
Av. Cordoba 1877
C1120 AAA Buenos Aires
Tel. (54-11) 48 15 81 56
Fax (54-11) 48 15 81 56
E-mail: wpbooks@infovia.com.ar
URL: http://www.wpbooks.com.ar

AUSTRALIA

Hunter Publications
PO Box 404
3067 Abbotsford, Victoria
Tel. (61-3) 94 17 53 61
Fax (61-3) 94 19 71 54
E-mail: jpdavies@ozemail.com.au

CANADA

Les éditions La Liberté Inc.
3020, chemin Sainte-Foy
G1X 3V6 Sainte-Foy, Québec
Tel. (1-418) 658 37 63
Fax (1-800) 567 54 49
E-mail: liberte@mediom.qc.ca

Renouf Publishing Co. Ltd
5369 Chemin Canotek Road Unit 1
K1J 9J3 Ottawa, Ontario
Tel. (1-613) 745 26 65
Fax (1-613) 745 76 60
E-mail: order.dept@renoufbooks.com

EGYPT

The Middle East Observer
41 Sherif Street
Cairo
Tel. (20-2) 392 69 19
Fax (20-2) 393 97 32
E-mail: inquiry@meobserver.com
URL: http://www.meobserver.com.eg

INDIA

EBIC India
3rd Floor, Y. B. Chavan Centre
Gen. J. Bhosale Marg.
400 021 Mumbai
Tel. (91-22) 282 60 64
Fax (91-22) 285 45 64
E-mail: ebic@giasbm01.vsnl.net.in
URL: http://www.ebicindia.com

JAPAN

PSI-Japan
Asahi Sanbancho Plaza #206
7-1 Sanbancho, Chiyoda-ku
Tokyo 102
Tel. (81-3) 32 34 69 21
Fax (81-3) 32 34 69 15
E-mail: books@psi-japan.co.jp
URL: http://www.psi-japan.co.jp

MALAYSIA

EBIC Malaysia
Suite 45.02, Level 45
Plaza MBI (Letter Box 45)
8 Jalan Yap Kwan Seng
50450 Kuala Lumpur
Tel. (60-3) 21 62 62 98
Fax (60-3) 21 62 61 98
E-mail: ebic-kl@mol.net.my

MÉXICO

Mundi Prensa México, SA de CV
Río Pánuco, 141
Colonia Cuauhtémoc
MX-06500 México, DF
Tel. (52-5) 533 56 58
Fax (52-5) 514 67 99
E-mail: 101545.2361@compuserve.com

PHILIPPINES

EBIC Philippines
19th Floor, PS Bank Tower
Sen. Gil J. Puyat Ave. cor. Tindalo St.
Makati City
Metro Manila
Tel. (63-2) 759 66 80
Fax (63-2) 759 66 90
E-mail: eccpcom@globe.com.ph
URL: http://www.eccp.com

SOUTH AFRICA

Eurochamber of Commerce in South Africa
PO Box 781738
2146 Sandton
Tel. (27-11) 884 39 52
Fax (27-11) 883 55 73
E-mail: info@eurochamber.co.za

SOUTH KOREA

The European Union Chamber of Commerce in Korea
5th Fl, The Shilla Hotel
202, Jangchung-dong 2 Ga, Chung-ku
100-392 Seoul
Tel. (82-2) 22 53-5631/4
Fax (82-2) 22 53-5635/6
E-mail: eucck@eucck.org
URL: http://www.eucck.org

SRI LANKA

EBIC Sri Lanka
Trans Asia Hotel
115 Sir chittampalam
A. Gardiner Mawatha
Colombo 2
Tel. (94-1) 074 71 50 78
Fax (94-1) 44 87 79
E-mail: ebicsl@lmin.com

UNITED STATES OF AMERICA

Beman Associates
4611-F Assembly Drive
Lanham MD20706
Tel. (1-800) 274 44 47 (toll free telephone)
Fax (1-800) 865 34 50 (toll free fax)
E-mail: query@beman.com
URL: http://www.beman.com

ANDERE LÄNDER/OTHER COUNTRIES/ AUTRES PAYS

Bitte wenden Sie sich an ein Büro Ihrer Wahl/Please contact the sales office of your choice/Veuillez vous adresser au bureau de vente de votre choix

Office for Official Publications of the European Communities
2, rue Mercier
L-2985 Luxembourg
Tel. (352) 29 29-42455
Fax (352) 29 29-42758
E-mail: info.info@cec.eu.int
URL: http://eur-op.eu.int

9/2000

The I-RISK project was funded under the European Commission's 'Environment and climate' programme of the fourth framework programme for research and technological development (1994–98). The objective of I-RISK was to design a methodology to quantify the effect of safety management systems (SMS) of industrial installations at risk of loss of containment (LOC) of hazardous substances. The I-RISK methodology, inspired by the Seveso II directive, consists of a quantified risk assessment and a management audit. The I-RISK approach was applied to three test cases: a chlorine loading facility, a refinery and an ammonia storage facility. The I-RISK methodology can help to establish whether an industrial installation is on the right track and whether it can meet its safety goals in the near future.

16 14 KI-NA-19320-EN-C

Price (excluding VAT) in Luxembourg: EUR 14.50

ISBN 92-828-9483-5

OFFICE FOR OFFICIAL PUBLICATIONS
OF THE EUROPEAN COMMUNITIES

L-2985 Luxembourg

9 789282 894835