Hazard identification based on plant functional modelling

Rasmussen, Birgitte; Whetton, C.

Publication date:
1993

Document Version
Publisher's PDF, also known as Version of record

RISØ

Risø-R-712(EN)

Hazard Identification Based on Plant Functional Modelling

Birgitte Rasmussen, Cris Whetton

Risø National Laboratory, Roskilde, Denmark
October 1993

Hazard Identification Based on Plant Functional Modelling

Risø-R-712(EN)

Birgitte Rasmussen, Cris Whetton*

***The University of Sheffield, United Kingdom**
Risø National Laboratory, Roskilde, Denmark
October 1993

Abstract A major objective of the present work is to provide means for representing a process plant as a socio-technical system, so as to allow hazard identification at a high level. The method includes technical, human and organisational aspects and is intended to be used for plant-level hazard identification so as to identify critical areas and the need for further analysis using existing methods. The first part of the method is the preparation of a plant functional model where a set of plant functions link together hardware, software, operations, work organisation and other safety related aspects of the plant. The basic principle of the functional modelling is that any aspect of the plant can be represented by an object (*in* the sense that this term is used in computer science) based upon an Intent (or goal); associated with each Intent are Methods, by which the Intent is realized, and Constraints, which limit the Intent. The Methods and Constraints can themselves be treated as objects and decomposed into lower-level Intents (hence the procedure is known as functional decomposition) so giving rise to a hierarchical, object-oriented structure. The plant level hazard identification is carried out on the plant functional model using the Concept Hazard Analysis method. In this, users will be supported by checklists and keywords and the analysis is structured by pre-defined worksheets. The preparation of the plant functional model and the performance of the hazard identification can be carried out manually or with computer support.

The present report is the main deliverable of work package 3.1 of the project *An Overall Knowledge-based Methodology for Hazard Identification* sponsored by the CEC STEP programme (contract no. STEP-CT90-0085).

ISBN 87-550-1933-1
ISSN 0106-2840

Grafisk Service, Risø, 1993

Contents

1 Introduction

An important part of a safety analysis of a chemical process plant is the identification of hazards and this can be carried out at either unit or plant level. Methods exist for hazard identification at unit level, e.g. hazard and operability study (HAZOP) and failure mode and effect analysis (FMEA). For large chemical process plants the effort required by these methods can be very extensive and it can be very difficult to establish a total risk survey for the plant. Furthermore, the emphasis of these methods is on identification of hazards closely related to the technical aspects of the plant and less on hazards related to the interaction between the plant equipment, the organisational structure and the management factors.

The present report is part of the project entitled "An Overall Knowledge-based Methodology for Hazard Identification" which is sponsored by the CEC STEP research programme. The working title of the project is: TOMHID. It was initiated in 1991 for a duration of three years. The project is carried out by an international consortium including the following partners: VTT (Technical Research Centre of Finland), The University of Sheffield (United Kingdom), SRD Division of AEA Consulting (United Kingdom), Tecsa (Italy), CIEMAT (Spain), Joint Research Centre (Ispra) and Risø National Laboratory (Denmark).

The basic idea of the TOMHID project is to develop an overall methodology which will provide assistance and guidance to the user for hazard identification purposes and which follows the course of an incident in each stage of the event chain.

One of the major objectives of the project is to provide a comprehensive framework to represent a process plant as a socio-technical system. The methodology is to include technical, human and organisational aspects and is intended to be used as a first stage in the hazard identification process so as to identify critical areas and the need for further analysis using existing methods.

The TOMHID project consists of the following work packages:
- WP1: Review of existing methods and models used for hazard identification.
- WP2: Conceptual study of hazard identification and risk reducing methods.
- WP3.1: Link between the functional model and hazard identification.
- WP3.2: Development of method to investigate management factors related to causes and consequences of specific hazards.
- WP4: Specification of software.
- WP5: Implementation of software.

The object of the TOMHID project is a method which can provide assistance and guidance to the user for high level hazard identification of different kind of chemical process plants (batch reactor plants, continuous plants, mixed reactor plants). The final method will consist of the following main elements:
- a functional description of the plant as a socio-technical system
- high level hazard identification based on the Concept Hazard Analysis method (CHA)
- plant documentation comprising the functional plant model and the plant level hazard identification
- evaluation of the safety impact of management factors on the identified hazards (to be developed in work package 3.2 of the TOMHID project)

- software specification and implementation of the methods developed in work package 3.1 (to be developed in work packages 4 and 5 of the TOMHID project).

The present report has been prepared by The University of Sheffield and Risø National Laboratory and is the main deliverable of work package 3.1. Chapter 3 contains a description of the principles of functional plant decomposition and chapter 4 presents the principles for high level hazard identification based on the Concept Hazard Analysis method (CHA) applied to the functional plant model. In the appendices two examples (a batch reactor plant and a continuous process plant) are presented illustrating the principles of functional plant decomposition and Concept Hazard Analysis.

The present work is based on the following working documents resulting from the first two work packages of the TOMHID project. :
- Users Need Report. February 1992. 18 pp + appendices (WP1).
- Review on Hazard Identification Methods and Software Tools. April 1992. 122 pp (WP1)
- Conceptual Study of Hazard Identification and Risk Reducing Methods. March 1993. 104 pp + appendices (WP2).

2 Overall description of TOMHID

The objective is to carry out a plant level hazard identification analysis based on the plant functional model using Concept Hazard Analysis (CHA) in a structured group session. The users in the group session will be supported by checklists and keywords guiding and structuring the analysis. The analysis will identify critical areas and the need for further analysis where well-established approaches can be applied.

2.1 Overall TOMHID procedure

The overall TOMHID procedure is:

a) Assemble all data, process information, personnel, etc.:
Data requirements and composition of the team are similar to those of an ordinary HAZOP; (Kletz, 1992).

b) Define the scope and objectives of the study:
The objectives will generally be those of TOMHID: identification of plant hazards and areas requiring more detailed study. Scope will usually be that of the entire plant, its management, and environment. However, all requirements may be changed to reflect the needs of the study.

c) Register Information:
This consists of housekeeping activities such as the project name, name of the analyst, and reference documents; it is described in detail (Davies & Whetton, 1993). The most significant procedural decision made here is whether the analysis is to be manual or automated, as this dictates how some of the later software is configured and linked together.

d) Compile Substance List:
This involves compiling a list of those substances present in the system, their quantities, and their locations in terms of vessels, pipes etc. This is described in detail (Anon., section 4, 1993) and (Davies & Whetton, 1993). Regardless of the selected mode, the Substance List will always be available for consultation by the user. This data should be available from process engineering, who would be requested to supply it, and will be used to guide the analyst as to substance properties at each point in the model.

e) Make Functional Model:
The functional model is required in the automated version of TOMHID but is optional in manual mode. A consequence of this is that, in auto mode the model and the forms used for CHA are linked together so that movement through the CHA form is controlled by movement through the model whereas in manual mode the two forms are independent. Construction of the model is described in detail in chapter 2 of this report, while the software functions are detailed in (Davies & Whetton, 1993).

f) Concept Hazard Analysis:
Description of the CHA procedure is presented in chapter 4; however, reference is made to the original description (Anon., section 4, 1993) and to the software description (Davies & Whetton, 1993).

g) Other TOMHID Analyses:
The other analyses are supplementary to CHA and are described in the references as:
- Concept Sociotechnical System Review (CSSR) (Anon . section 4. 1993).
- Preliminary Consequence Analysis (PCA) (Anon.. section 4.3. 1993).
- Short-Cut Risk Assessment (SCRAM) (Anon., Section 4.4. 1993)

h) More Detailed Analyses:
Other analysis methods may be used to explore particular hazards identified by TOMHID (Anon., section 5. 1993).

2.2 Outcome of the TOMHID procedure

The overall outcome of the TOMHID procedure will be a document containing four elements:

a) A plant functional model emphasizing the important parts of the plant with respect to safety. The model will be developed on the basis of the plant documentation and on the principles of functional decomposition.

b) A documented Concept Hazard Analysis comprising analyses and evaluation of the objects contained in the plant model.

c) An identification of the plant units (or parts of plant units) that are critical from a safety point of view. Recommendations concerning further analysis where well-established hazard identification and failure analysis methods can be applied.

d) Suggestion of measures which can reduce the possibilities or limit the consequences of the identified hazards.

3 Principles of functional modelling

3.1 Scope of the functional model

The scope of the functional model is:
- to provide a general framework for representing a chemical process plant as a socio-technical system
- to support the Concept Hazard Analysis which will be the starting point for the subsequent evaluation of the safety impact of the management factors on the identified hazards.

The principles of the functional model are intended to meet the following general requirements:
- Completeness: The functional model shall in principle be able to capture all the safety related information and aspects of the socio-technical system (e.g. equipment, operations, control systems, work organisation).
- Flexibility: It shall be possible to perform the functional modelling and decomposition of the socio-technical system to different degrees of detail or comprehensiveness. The user must be able to decide where the emphasis of the analysis shall be laid.
- Robustness: During functional modelling of the plant the user shall be able to extend the scope or the modelling level of detail without breaking the internal consistency of the plant model. This means that the functional model can be developed incrementally.

In this chapter the basic principles for functional modelling and decomposition are presented and to illustrate these principles two examples of functional modelling have been prepared and can be found in the appendices.

3.2 Functional modelling

The overall goal of the functional modelling and decomposition is to prepare a systematic and comprehensive description of a process plant with reference to hazard identification. The intention is to represent a socio-technical system as a hierarchical, object-oriented structure.

3.2.1 Overall modelling principles

The plant model follows a general framework as indicated in Figure 1. The basic idea is that a set of plant functions link together hardware, software, operations, work organisation and other safety related aspects of the plant. Within this framework it will be possible to integrate information and knowledge about the technical, physical and functional configuration of the plant together with relations and connections to the operations and its management aspects. The basic principle of functional modelling is that any aspect of the plant can be represented by an object based upon an Intent or goal and that associated with each Intent are Methods, by which the Intent is realized, and Constraints, which limit the Intent. The Methods and Constraints can themselves be treated as objects and decomposed into lower-level Intents (hence the procedure is known as functional decomposition), so giving rise to the method's hierarchical structure.

Development of the hierarchical structure proceeds as follows: A starting point is chosen (here defined as F0). Usually this will be the top level of the plant - its overall function - but can be the function of a plant section, if so desired. At the next level (level 1) the top function is decomposed into its main constituent elements, say F1, F2, F3. The functional decomposition is continued and refined at the subsequent levels, e.g. F1 into F1.1, F1.2, until an appropriate level of details has been achieved. This principle is illustrated in Figure 1.

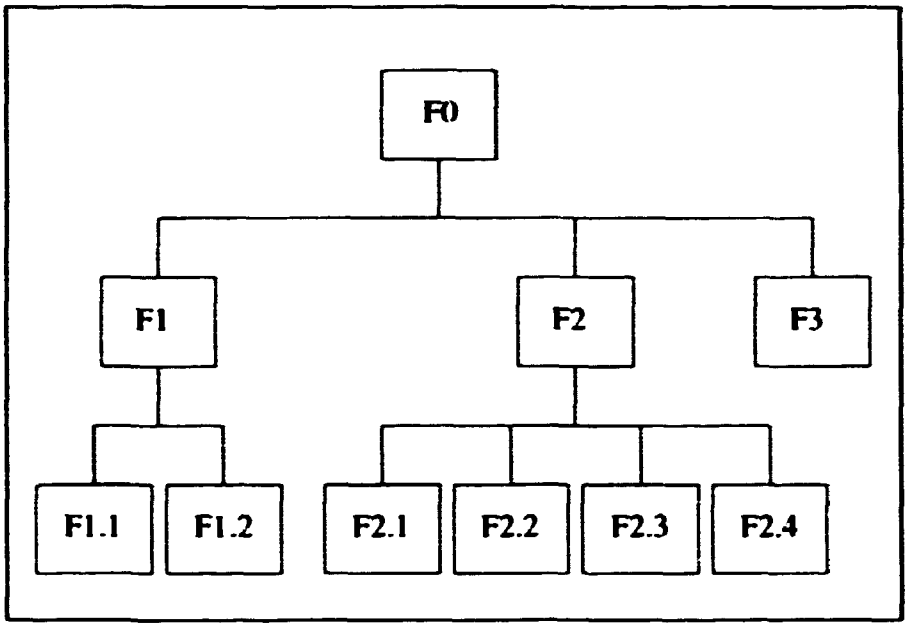


Figure 1. Functional decomposition of a process plant as a hierarchy of functional objects.

3.2.2 Functional description

In the plant functional model, a function is an object comprising an Intent, a list of more than one Methods, which are used to satisfy that Intent, and a list of zero or more Constraints, which impose restrictions upon the Intent. Each element of the lists of Methods and Constraints can itself be treated as an object defining a new Intent with its associated Methods and Constraints. A simple semantic model is shown in Figure 2.

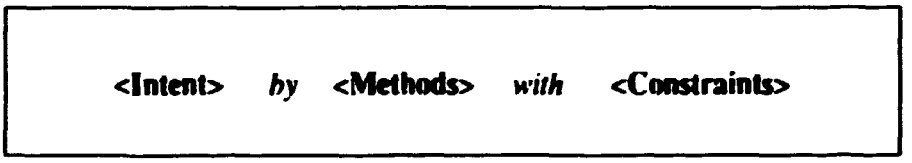


Figure 2. Semantic functional model.

Hence, the plant model contains objects whose elements can be classified as follows:

- Intents representing the functional goals of the specific plant activities in question.
- Methods representing items (hardware, procedures, software, etc.) that are used to carry out the Intent or operations that are carried out using those items.

- Constraints that describe items (physical laws, work organisation, control systems etc.) that exist to supervise or restrict the Intent; Constraints can contain information about the organisational context in which the Intents are fulfilled.

A diagrammatical model is presented in Figure 3 which shows the possibility of including Inputs and Outputs linking together the Intents in the functional plant model. Inputs show the necessary conditions to perform the Intent and the link to the previous Intent. Outputs show the outcome produced by the Intent and the link to the subsequent Intent.

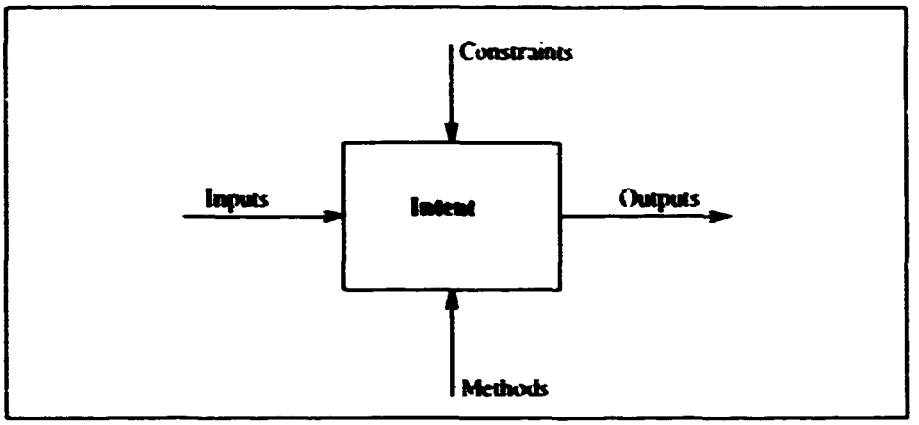


Figure 3. Interrelationships between objects at the same functional level.

Finally, in some cases it may be convenient to divide the functional plant model into environmental or topological zones. These zones are linked to the functional objects and specify where an Intent is carried out and they give information about the local situation.

3.2.3 How to start - where to stop

The modelling principle is a top-down approach which ensures a logic functional model of the process plant. One of the essential parts of the functional decomposition is to determine the starting point of the analysis. To state a general starting point which will be convenient for all kind of hazard identification analyses is not possible, as an appropriate starting point will depend on the specific plant configuration and the objective of the analysis. The usual starting point will be a process flowsheet for the plant and from this the analyst will have information on all the chemical substances and the characteristics of the main process streams. From this starting point, the functional decomposition is performed, ensuring that all relevant activities are considered (processing, maintenance, controls, emergency systems etc.).

The structural decomposition of a process plant may follow the following hierarchy:

1. plant (or section of the plant)
2. unit
3. system
4. subsystem
5. aggregate
6. component
7. piece part

(Note, however, that the analyst may insert intermediate functions which do not correspond to the physical elements if by so doing the clarity of the analysis is enhanced).

For a particular plant, there will be one plant object, one or more unit objects, and as many objects of the lower levels as there are systems, subsystems etc. in the plant. As for the starting point, it is not possible to offer general rules for selection of an appropriate modelling level. The intention is to identify at each level those parts of the plant where further analysis is required; meaning that the degree of detail will differ for the different parts of the plant. Here it is important to keep in mind that the main purpose of the functional model is to provide a frame for a high level hazard identification; consequently the model may be stopped at one of the top levels. Furthermore, it must be remembered that one of the objectives of the high level hazard identification is to identify critical areas and the need for further analysis. At some other stage existing hazard identification and failure analysis methods e.g. Hazard and Operability Studies, Failure Mode and Effects Analysis, Action Error Analysis, will be more suitable for the detailed analysis work.

3.3 Presentation forms

The main objective of the plant functional model is to provide a frame for the overall hazard identification. In the following it is assumed that a Concept Hazard Analysis will be carried out using the worksheets (or variants hereof) presented in chapter 4.

The plant functional model can be developed and presented in two different ways: tabular or graphical form. These two presentation forms can be used separately or they can supplement each other. For each plant or activity the analyst can choose the most convenient way to develop the functional decomposition and present the plant model. Applications of the tabular form and examples of the graphical presentation form can be found in the appendices. However, it must be noted that, with regard to the software specification developed under WP4, the graphical method has not been developed, except so far as it is used in abbreviated form to allow the user to navigate through the model, as described in section 4.2.2 of this document.

3.3.1 Tabular form

Choosing a tabular presentation form will make it easier to develop a frame for the overall hazard identification as the worksheet from the functional model can easily be linked to the worksheet of the Concept Hazard Analysis.

The functional model can be contained in a three column worksheet as shown in Figure 4 where the "Ref" column is used for numerical reference as explained later. The "T" column is used to indicate the type of the object by the letters I for Intent, M for Method and C for Constraint. The "description" column contains an imperative statement which forms the Intent, Method or Constraint.

Function			
Ref	T	Statement	(Concept Hazard Analysis)

Figure 4. Tabular presentation form.

To make the functional model more readable a column for comments or notes can be included in the worksheet. The comments or notes are for explanation only and do not form part of the plant functional model.

As indicated a reference (numbering) system is used to clarify the functional decomposition. A decimal numbering system is proposed, as follows:
- the first Intent of the model is reference 0
- the first list of Methods is numbered sequentially 1...n
- the numbering of the first list of Constraints starts at n+1.

If a Method or Constraint is expanded, then it generates a new Intent which is numbered i.0 which has a new list of Methods numbered from i.1 to i.n and a new list of Constraints starting at i.n+1. This presentation form is unambiguous but can result in lengthy reference numbers (a problem which seems to be unavoidable).

Finally, it is recommended that, in order to keep the clarity of the plant functional model, the numbering of Methods and Constraints follow as much as possible the logical sequential order with respect to the processes and activities at the plant. One way to illustrate the Input/Output relations between the plant objects in the tabular plant functional model is to list the Methods in the same sequential order in which they are performed to fulfil the requirements of the Intent in question. (Note, that activities in parallel can be indicated either by use of a logical OR or by the imposition of a suitable Constraint).

3.3.2 Graphical form

In several cases a graphical presentation form can be useful as a supplement to the tabular documentation. In the graphical presentation form the functional objects of the model follow the general format as illustrated in Figure 3 and which follows the usual conventions of the SADT (Structured Analysis & Design Techniques) method of systems analysis.

The main benefit of using the graphical presentation form is that it is possible in a clear manner to show the main streams and the internal functional relations of the plant. For activities where for instance failure propagation is considered to be an essential safety aspect the preparation of a graphical presentation of the functional decomposition might help to identify the incident course and the critical plant areas.

If a graphical presentation form is chosen the outcome of the functional plant decomposition will differ from the outcome based on the tabular presentation form.

In general the same objects can be found in the two presentation forms but a different structure of the functional model will often be convenient. The graphical form has the advantage that it will almost always be possible in one diagram to contain more than one Intent together with the respective Methods and Constraints.

A disadvantage with the graphical presentation is that the development of the functional diagrams can be rather time consuming and they can be more troublesome to update and correct. A good software editor will reduce this problem. Furthermore, to carry out the hazard identification it is necessary to transfer the objects of the diagram onto a tabular form to which the CHA worksheet can be connected. For these reasons, it is proposed that the computerised version of TOMHID will incorporate a graphical representation that shows only the model structure, content being given in the tabular displays.

3.4 Plant functional objects

The technical configuration of chemical process plants clearly differs from plant to plant making it rather difficult to formulate explicit rules for carrying out functional decomposition. It must be stressed, that the decomposition of a plant or unit into its functional elements is not a well-defined exercise with only one outcome - it can be done in different ways depending on the experience and choices of the analyst.

On the other hand, examples and guidelines may be useful and it is to some extent possible to exemplify the kind of information that is intended to be represented at the different functional levels. Examples of functional objects can be found in the following sections. Furthermore, some problems which may arise during a functional decomposition of a process plant are discussed. Detailed examples and application of the principles of functional decomposition can be found in the appendices.

It must be stressed that the basic idea is to develop a procedure which can structure and support plant level hazard identification by use of the functional decomposition principles. It has not been the intention to develop a real taxonomy for representation of functional objects in a plant model.

3.4.1 Establish the Intents of the plant

One question is how the different functional objects are to be characterised. If, as an example, we consider a chemical batch reactor equipped with a temperature alarm, the question is whether the temperature alarm should be characterised as a Method (equipment used to realize the Intent) or as a Constraint (equipment used to control the Intent). Since the reason for making the plant functional model is eventually to perform a plant level hazard identification, the important point is not how the object is characterised, but that all objects important to safety appear in the functional model of the plant. The basic principle of the functional modelling in which any aspect of the plant can be represented as *Intent by Methods with Constraints* is a valuable way of thinking to ensure that all safety aspects have been considered. It cannot be over-emphasised that it is more important to ensure that all those objects which affect safety are included, than to be concerned as to whether or not they are included exactly in the right place. In each case it must be considered whether the choice of function and the way in which it is expressed

will influence the performance and result of the subsequent plant level hazard identification.

Determining the Intent of a plant and distinguishing the Intent from Constraints (and sometimes Methods) is a matter of some judgement as the following examples show:

Intent: *Make liquid oxygen.* This is clearly an Intent and nothing but.
Intent: *Make liquid oxygen by liquefaction of air.* Here, the Intent has been mixed with the Method "by liquefaction of air".
Intent: *Make liquid oxygen at a cost lower than £10/tonne.* Here the Intent has been mixed up with the cost Constraint.
Intent: *Make liquid oxygen with noble gasses as a by-product.* This is a valid Intent which can be split into two subsidiary Methods "Make liquid oxygen" and "Extract noble gases as by-products".

The best way to decide whether an Intent is correct is to examine each clause of the sentence and see if it is a Method or a Constraint. If is either, then the clause is removed from the Intent statement and replaced in the category it belongs. As a general principle, the top Intent should be kept as simple as possible, while still capturing the essence of the plant.

Another aspect related to the determination of plant Intents is the identification of those production units and activities which will be the principal parts of the plant functional model. The logical starting point for the functional decomposition will often be the specific Intent of the plant. Here it is important to keep in mind that this choice will often lead to a fragmented structure for auxiliary operations highly integrated in several Intents e.g. the control system, maintenance operations, quality assurance system, procedures for handling chemicals, emergency system. These auxiliary systems will appear at those points in the functional model where they are considered to be important from a safety point of view, while the structure of the entire systems may not appear clearly any where. If the tasks of the auxiliary systems are separated and only included in the functional model where relevant it must be considered how to ensure a complete analysis covering all relevant tasks of the auxiliary systems. Consequently, there may be occasions when it is desirably to decompose the system starting from the auxiliary system Intent. E.g. the safety of maintenance operations could be examined by starting from *Maintain the plant* as the top Intent.

3.4.2 Establish the Methods and Constraints of the plant

"Methods" and "Constraints" are objects related to a specific Intent at a specific plant level. "Constraints" comprise activities, installation or systems that restrict or control the Intent. Generally speaking "Constraints" can be equipment, supervision and/or management. "Methods" comprise hardware (i.e. equipment and chemicals) used and procedures or operations carried out to realize the Intent.

Having established a valid Intent for the plant the next step/task is to decide the Methods available to implement the Intent and the conditions which restrict the Intent. It is impossible to prepare a complete list of Methods and Constraints relevant to the plant functional model, but Tables 1 and 2 contain some high level standard Methods and Constraints, respectively, which it is recommended always to consider during the development of the plant functional model.

Table 1. Standard Methods.

Method	Suggestions for expending the Method
Manage the operation	Feedstock loading; Intermediates; Plant coordination; Production activities; Product unloading; Safety culture.
Support the operation	Catalyst loading; Cleaning; Construction; Control process; Deployment; Firefighting; Loading; Maintenance; Manage emergencies; Modification; Painting; Quality control; Security; Shutdown; Start-up; Storage; Testing; Training; Transport; Unloading; Waste disposal.

Table 2. Standard Constraints.

Constraint	Suggestions for decomposition of the Constraint
Protect environment from damage by plant	Avoid accidental releases Contain process fluids Control effluent disposal Minimize acoustic emissions Minimize planned releases
Protect plant from damage by environment	Protect against incidents in adjacent plant Protect against man-made disasters Protect against natural disasters Protect against unauthorized access to plant

The first standard Method "manage the operation" presented in Table 1 refers to production activities while the second "support the operation" covers everything else. Supporting tasks are often not covered sufficiently in hazard analyses. Including these Methods at a high level ensures an appropriate integration of these aspects in the analysis. Supporting tasks should be examined at each stage of the functional decomposition to see whether a particular Method is appropriate for inclusion.

Currently, two standard Constraints have been identified for inclusion at level 0 in the plant functional model (Table 2): "Protect environment from damage by plant" and "Protect plant from damage by environment". These are clearly complementary and it should be noted that personnel are included in the concept of Environment. The lists of Table 2 suggest some Methods into which these Constraints can be decomposed.

3.4.3 Systems and items with multiple functions

It can sometimes be difficult to decide where an object belongs, as the following two small examples show:

- Heat exchanger: is the primary purpose to heat stream A or cool stream B ?
- Pump: is the primary purpose to empty tank A or fill tank B ?

These examples are trivial, but they do illustrate an important point: where a hardware item has multiple functions, these functions may appear separately in the appropriate parts of the model. The modelling problem is bipartite:

- A multiple function will appear frequently. Indicating all relations to and impact on other functions can easily diminish the clarity of a functional model.

- If the tasks of a multiple function are separated and only included in the functional model where relevant it must be considered how to ensure a complete analysis covering all relevant tasks of the multiple functions.

In general this presents no great problem; however, if a clearer relationship between function and equipment/hardware hierarchy is required then means must be found to accomplish this.

3.4.4 Dynamic aspects of processes

The principles for decomposition of the plant functional model have been developed for application to batch processes as well as continuous processes. In some cases the dynamics of the system can be a critical safety factor: e.g. an important dynamic factor for batch processes can be time and for continuous processes flow.

In general it is important to assess the impact on plant safety of the dynamic behaviour of a system. Relevant dynamic factors can e.g. be: time, flow, temperature.

3.5 Operations and management issues

3.5.1 Operations issues

"Methods" and "Constraints" identified as operations can be difficult to decompose in a clear and logical manner. In Table 3 a general list of operations is presented which can support the functional decomposition. The idea is to write down a broad sample of actions that may appear at a process plant. In the content of functional modelling, the intention is that operations are related to a specific Intent where it is considered important from a safety point of view.

Observation and manipulation cover the physical interaction with plant and equipment, while evaluation is a mental task. Communication includes telephone calls, reading production schedules etc. Control is reserved for terms that refer to higher level manipulation or special control concepts such as set points. The three first categories may be seen to form an observe - evaluate - manipulate loop, modelling the central operator actions, with the next two categories serving as tool families. Plants with high degrees of automation have a central control system operating the whole plant with the operator merely monitoring the needs of the control system. Plant maintenance, which is an important but often overlooked aspect of system safety, also involves the functions of observe, evaluate etc. and is also included as one of the standard Methods of Table 1.

Table 3 attempts to present the tasks of an "operator" according to the basic verbal meanings and the lists are not reduced to minimum sets representing the necessary operator tasks. The list is presented here as a rough sketch of possible input parameters to error lists and to suggest a background for wording the functional model at the lower plant levels.

Table 3. A general list of operator actions.

observe	read (instrument, label, sign scheme, text); listen; feel (temperature, movement); smell; measure (weight, count); check; inspect; look after; measure if
evaluate	compare (with reference, target value, scale, plan); review (observation, data, experience); judge; decide; choose plan, strategy or procedure
manipulate objects (goods, bodies, substance)	take; carry; return; load/unload object; fill/empty container; add/remove; add substance; treat substance; move; lift/lower; turn; position; secure; lock/loosen
manipulate equipment	establish; connect/disconnect; assemble/dissemble; install; adjust; reset; activate; deactivate; open/close; select; fill/empty; clean
manipulate tools and instruments	press; push; turn; draw; modify/work on; vibrate; measure; connect/disconnect remove; exchange; reset
communicate	ask; answer; inform; contact; record; log; write
control	initialize; prepare; observe state; check state; change state; increase attention; reset; steer

3.5.2 Management issues

As mentioned, one of the main objectives of the functional model is to represent a process plant as a socio-technical system. One of the important elements in this connection is representation and integration of management issues and work organisation in the functional plant model.

In this part of the project the analysis of management factors is limited to an identification and integration in the plant model of the management factors. In work package 3.2 methods to investigate the impact of management factors on plant safety will be further developed.

Management issues will usually be developed from standard Methods (Table 1) or standard Constraints (Table 2). If this approach is followed, then the functional sub-model of the management issues may not correspond to that of the rest of the plant - especially to that of its physical sub-structure. Within the functional model, there is no requirement for the structure of one sub-model to correspond with that of another. However, the lack of structural correspondence may cause confusion. One solution to this problem is to integrate management issues into the model by means of a bottom-up approach. In this case, the starting point for functional decomposition is the low-level function and the management issues are only integrated into the functional model if they are considered to be important from the point of view of safety. Table 4 contains some examples of management issues which can support the functional model.

Table 4. Examples of management issues.

system climate	technical adsorption; legislation; regulations; political climate; economic climate; business factors; public relations
organisation structure	corporate mission and philosophy; resource provision; decision-making hierarchy; safety policy; corporate culture; interaction with other socio-technical system
management structure	resource allocation; level of staffing; competence; quality control; command structure; activity monitoring; setting and maintaining standards; supervision; third parties relations (contractors); response to change; safety responsibilities; accident/incident investigation
information	data processing; availability; interfaces; operating procedure/manual; task specification; quality assurance manual; emergency procedures
communication	channels; emphasis; interface/exchange media; incident reporting; emergency back-up

3.6 Procedure for functional decomposition of a process plant

The functional model approach proposed has the advantage that it offers the possibility of representing all facets of the plant description (activities, hardware, operations, work organisation) in an integrated and consistent way. The procedure proposed to carry out the functional decomposition of the plant is the following:

a) Discuss the overall goal of the functional model.
b) For large complex plants it might be necessary to perform the functional modelling of the plant activities by subdividing the plant into systems, subsystems etc. and perform a functional decomposition for each part.
c) Determine the principal parts of the plant and the starting point for the functional model.
d) Choose the documentation form for the functional model and the hazard identification. If performing a manual decomposition, then choose a format such as that shown in Figure 4 or the graphical form discussed in section 3.3.2. Otherwise, the computer-assisted TOMHID tool can be used, as described in section 4.2.
e) Establish the top Intent of the plant.
f) Link the Intent with the Methods that are used in carrying out the Intent.
g) Identify Constraints and link them to the Intent.
h) List the Methods and Constraints; if possible, in a logical sequential order with respect to plant design and the operations carried out.
i) Discuss the identified Methods and Constraints and identify those which are going to be further decomposed.
j) Prepare the new list of Intents and proceed from point d.
k) The functional decomposition is finalized when an appropriate level of detail has been achieved.

4 Principles of CHA applied with functional modelling

The previous section described how a process plant may be modelled by the functional method; this section describes how a Concept Hazard Analysis (CHA) may be performed on that model.

4.1 CHA on a plant functional model

A general method for CHA is described in (Anon, section 4, 1993), primarily in connection with the manual version of TOMHID and without reference to the functional model. Figure 5 shows the CHA procedure which is identical for automated and manual modes, the only difference being the linkage between the analysis form and the functional model, as described in section 2.1.

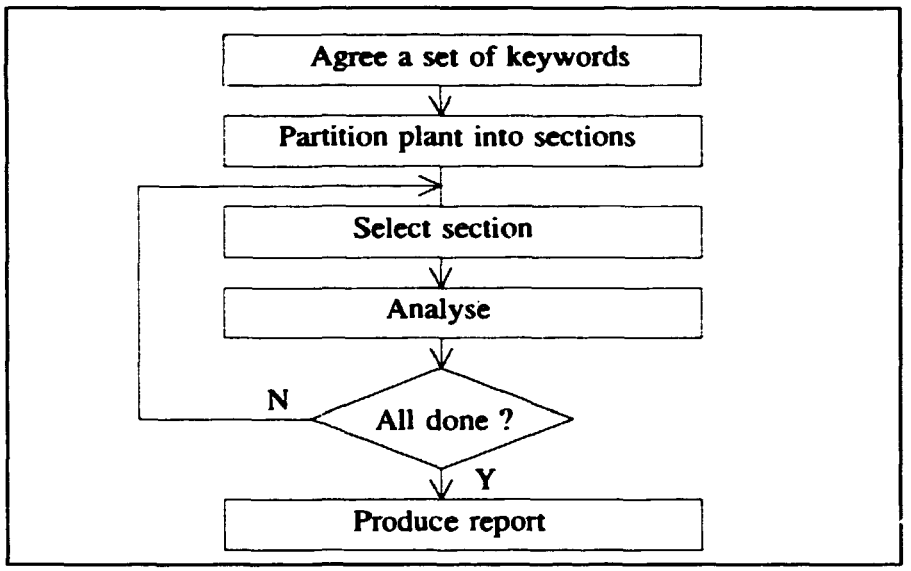


Figure 5. Overall CHA procedure.

4.1.1 Agree on a set of CHA keywords

A Task-specific CHA Keyword Database (CKD) must be assembled for each analysis, in accordance with the procedure shown in Figure 6.

A programme module **Edit CKD** is used to add (and, deliberately with some difficulty, to delete) keywords to a file known as the **Core CKD**. This file will contain keywords which are applicable to a variety of industries and situations and from these a database, **Task CKD**, must be assembled, using the **Abstract** tool, containing only keywords applicable to the analysis (examples of keywords can be found in the appendices and in (Wells, Wardman & Whetton, 1993)). The details of this database (location, filename, etc.) are added to the registration data. Typically, ten to twenty keywords will be abstracted from the Core CKD to the Task CKD. Once the Task CKD has been created, the user has access to it via a **Browse** facility which displays one or more keywords and allows the user to

move back and forth in the file at will; keywords can be copied from the Task CKD into the appropriate slot of the analysis form, using the usual Windows copy and paste commands.

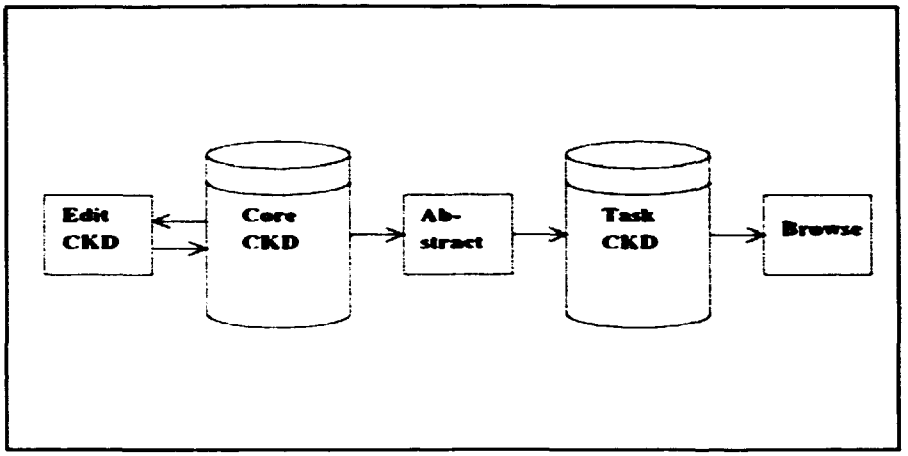


Figure 6. Assembling keywords.

4.1.2 Partition the plant into sections

The details of this action vary according to which operating mode has been selected; there are, in fact, three possibilities:

a) Automated mode. Here, creation of the plant functional model has in effect partitioned the plant into sections. The first level of decomposition will usually provide sufficient partitioning; however, if this proves to be too broad or coarse, functions can be selected from the next level of decomposition. Partitions can be selected from any mix of levels of decomposition of the model, provided that it is ensured that the full breadth of the model is covered. E.g. in Figure 7(a), the selected functions provide full coverage, whereas in Figure 7(b) they do not.

b) Manual mode, using a functional model. Here, partitioning is again provided by the functional decomposition and this may be used if so desired.

c) Manual mode, not using a functional model. In this case, no help or guidance is available from the model and the user must partition the plant according to the team's needs. In general, partitions should be such as to be comprehensible and to allow a reasonable amount of time for the team to discuss.

Note that is not recommended that any mixture of manual and model-based partitioning be used as this is a sure recipe for confusion.

Once the plant has been partitioned, analysis proceeds section by section until all have been covered. Forms for the documentation of substance properties and the CHA are given in (Anon. section 4, 1993); modified CHA forms, derived with the objective of a computer based system, are given in the following sections of this document and demonstrated in the appendices.

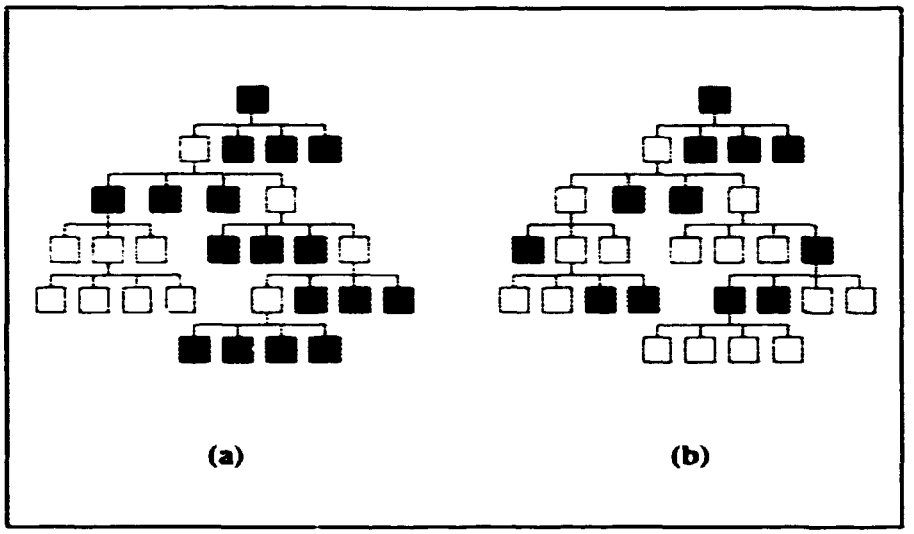


Figure 7. (a) Valid partitioning. (b) Invalid partitioning.

4.2 Performing the CHA

Several formats are proposed for the analysis; Figure 8 shows that suggested for a purely manual analysis, without computer support, and may be adapted to a word processor or to a printed form.

Function								
Ref	T	Statement	k	Keyword	Main variance	Conse-quences	Mitigation	Notes

Figure 8. Simple CHA form.

For the TOMHID software, two forms are proposed: one for the plant functional model and the other for the analysis. Figure 9 shows the format proposed for the functional model.

With the scheme of Figure 9, References would be assigned automatically; one grid is assigned to the Intent statement (of which there can only be one) and an unlimited number of grids each are assigned to the Methods and Constraints, though only three are displayed. Movement amongst the Methods and Constraints, when there are more than three, is controlled by the scroll-bars, shown to the right of each block. Movement amongst the functions is controlled either by horizontal and vertical scroll bars (not shown in the Figure) or by the model navigator (similar to Figure 7(a)), which is the preferred method.

As noted above, in the automated mode the analysis form is linked to the model display so that whatever functional statement is highlighted on the model, the

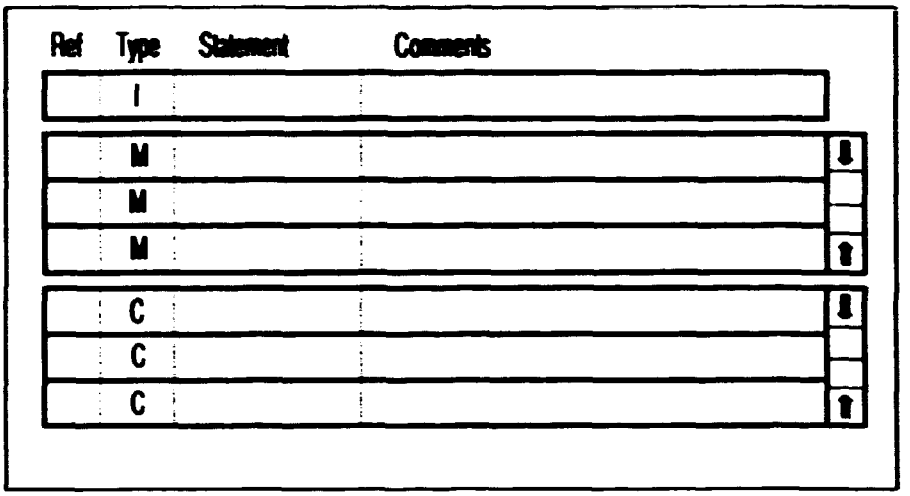


Figure 9. The Function window.

analysis form shows the corresponding analysis. In this case, the Ref. field of the model form provides the primary reference to the analysis, a second reference being provided by the keyword, since more than one keyword can be applied to a functional statement. However, in the manual mode, this linkage does not exist and reference numbers are supplied by the user. This requires a composite format to accommodate the two modes; Figure 10 shows the format proposed.

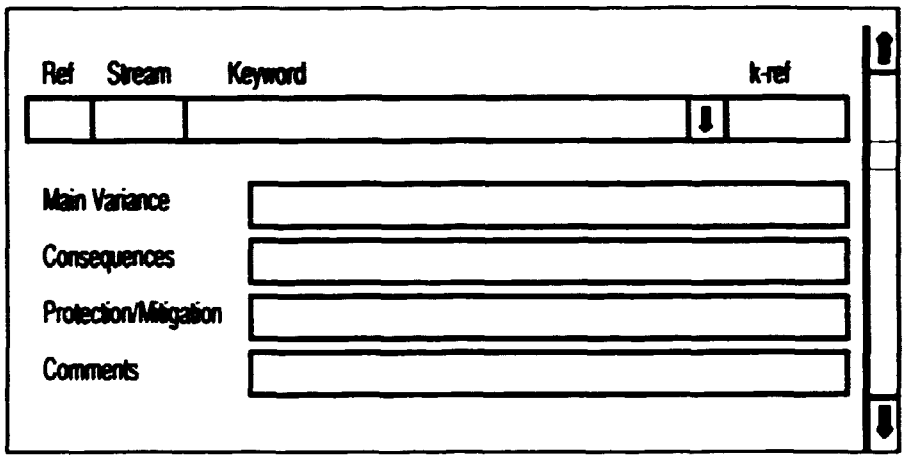


Figure 10. The CHA window.

In the automatic mode, the Ref field merely mimics what is already displayed in the Ref field of the model and the vertical scroll bar (right) is greyed-out. In manual mode, the Ref field is automatically incremented whenever a new stream is selected and the vertical scroll bar is activated and used to move up and down amongst the records, which are organised sequentially. Since multiple keywords are allowed, this field is provided with a drop-down box, so that the keywords can be seen and selected. The fields of the three formats are summarised as follows:

- Ref field provides a reference to the record. In the functional model, references are allocated automatically, using the scheme as explained in paragraph 3.3.1 of this document. Alternatively, in manual mode, the same scheme is applied to the model (if used) but the Ref. field of the analysis is numbered sequentially as records are added.

- T. An entry in this field indicates the Type of the following statement, with the convention: I→Intent; M→Method; and C→Constraint. If using the form of Figure 8, this is supplied by the user; otherwise, it is allocated automatically since separate fields are allocated to Intents, Methods, and Constraints.

- Stream, this has been included in the computer-based method as an option; it need not be used but it is felt that it can be useful to have a cross reference to the substance list.

- Statement describes the Intent, Method, or Constraint to which it refers. Since no operations are actually performed on the statements, their format and content is unlimited, though users will be encouraged to be brief and to phrase their statements in certain standardised ways. To facilitate this, statements can be collected and assigned to a function dictionary where they can be examined and re-used so as to promote a consistent style.

- k or k-ref is an index to the keyword, within the functional statement reference. There may be multiple keywords applied to the statement; these are referenced by letters a, b, c...z.

- Keyword, this is the keyword, selected from the task CHA keyword database as described in 3.2.1, above. Applying the What if...? principle by negation of Intents and Constraints as described in (Anon., section 6.2, 1993) suggests that the first keyword in these two categories should always be the word 'NOT'.

- Main variance, this details the main effects inferred from applying the keyword to the function statement.

- Consequences, the major consequences which could arise from the main variance.

- Mitigation, any factors which exist to mitigate the identified consequences. If factors are identified which should exist (but are absent) these should also be recorded.

- Notes and Comments, any comments entered during construction of the model are carried forward into this section. Further notes are added as required.

With the forms and tools described above, several options are available for performing the actual CHA.

4.2.1 CHA without computer support

a) Keywords are taken from a prepared list and applied to each selected plant section in turn. By discussion amongst the team, this is used to generate a Main Variance on the analysis form.

b) Each item of equipment is checked against the Equipment Data Base (EDB) for known hazards. Using the item name as keyword, variances are recorded from the database.

c) Identify the consequences of each main variance.

d) Determine if the hazard can be designed-out or if the hazard can be otherwise reduced or eliminated.

e) Determine any controls or mitigation.

f) Determine any comments and actions.

4.2.2 CHA with computer support and with the plant functional model

a) Perform a What if..? analysis by negating each Intent, Method, and Constraint of the model. I.e. by asking: What if this Intent (Method or Constraint) is not satisfied? In describing the manual method, (Anon., section 4, 1993) suggests that a What if..? analysis can be performed at this time. Adapting this idea to the features offered by the functional model, a similar effect can obtained by negating the verb in the Intent and Constraints statements. See (Anon., section 6.2, 1993). Use the results of this step to generate a Main Variance on the analysis form. (Note that to indicate that this step has been applied, the word 'NOT' should be inserted in the Keyword column).

b) Apply the CHA keywords to each Intent, Method, and Constraint in the model. Keywords are taken from the Task-CKD and applied to each statement in turn. This is also used to generate a Main Variance on the analysis form.

c) Check each item of equipment against the Equipment Data Base for known hazards. Using the item name as keyword, record any variances.

d) Identify the Consequences each Main Variance.

e) Determine if the hazard can be designed-out or if the hazard can be otherwise reduced or eliminated.

f) Determine any controls or mitigation.

g) Determine any comments and actions. (Note that if any comments were generated during the construction of the functional model, these will be brought forward into the final report form though during the analysis they will be displayed at their point of origin.)

4.3 Supporting databases

In the following the databases required for a TOMHID CHA - along with the functions supported - is presented. These functions are detailed in (Davies & Whetton, 1993) and the software will be further developed in WP4 and WP5 and therefore, the discussion here is limited to the usage and contents of the databases. Databases listed in regular type are required for a TOMHID CHA, those in italic type are optional.

- Core Key Words: The Core Keyword Database (CKDB) will consist of primary and secondary keywords. An initial set of keywords is given in the report on WP2, (Anon.,1993) and other keywords will no doubt be added as the project progresses. In rough, round figures, storage will be provided for a maximum of 1,000 primary keywords, with an average of 5 secondary keywords and a maximum of 20 secondary keywords per primary. I.e. 5,000 records total. These

keywords are used to generate the Task Keyword Database; consequently it has been decided that material cannot be deleted from this database without great difficulty, though keywords can be added at any time. Thus, with use, the database will become ever richer.

- Task Key Words: The Task Keyword Database (TKDB) will always be a subset of the LKDB. As such, it seems unlikely that a TKDB would ever contain more than 100 keywords; therefore a typical TKDB will have, as a maximum, 500 records. These keywords are used directly in the analysis and, although it is possible to have up to a hundred such keywords, it is unlikely that a typical analysis will use more than twenty.

- Equipment: The equipment database contains details of common process equipment, including application diagrams and known characteristics and hazards. It is planned that this database will contain a mixture of text and graphics but that only hazard information in text form can be pasted to the Main Variance and Consequences fields of the analysis form.

- Operations: This optional facility would be a database of basic operations such as fill, empty, lift, observe, etc. as described in section 3.5.1.

- Management Issues: This optional facility would be a database of management issues such as system climate, organisational structure, etc. as described in section 3.5.2.

- *Functions*: Eventually, as one of the benefits of the functional method, a database of functions would be developed. This would consist of functional models containing the generic portions of models which had previously been created.

- *Scenario*: This is envisaged as being similar to the database of functions, but concentrating on generic portions of management and operational models.

- *Method Dictionary*: From the functions database, a dictionary of standard methods can be extracted and then used to promote greater consistency in the analyses.

- *Constraint dictionary*: From the functions database, a dictionary of standard constraints can be extracted and then used to promote greater consistency in the analyses.

4.4 Supporting analyses

Three supporting analyses are planned for TOMHID : Concept Sociotechnical System Review (CSSR), Preliminary Consequence Analysis (PCA), and Short-Cut Risk Assessment Method (SCRAM); these are outlined in the following paragraphs, further details being given in Ref. (Anon., 1993).

4.4.1 Concept Socio-technical System Review (CSSR)

The Concept Safety Review needs to consider both the Sociotechnical System of which the plant is to be a part and the hazards presented by the plant. Suggested keywords for use during the initial stage of this socio-technical system review

which are specifically directed at safety factors are listed in the Tables of (Anon., section 4.2, 1993).

It is emphasised that this is a review stage and consequently it is important not to get involved in detailed discussion but to highlight possible problem areas. The aim is to *generate major variances* caused by the new plant at a particular location for further study. If the review is to be carried out for an expansion of an existing plant it may be a good time to highlight areas giving problems possibly with the aim of getting the topic accepted for the Company's Safety Improvement Programme.

4.4.2 Preliminary Consequence Analysis (PCA)

A Preliminary Consequence Analysis of Major Incidents examines the impact of what might occur on a particular process plant. It is usually carried out as soon as a description of the process flow diagram is available. If the site is to be selected it may be done very early and such a study may well only consider pipe breaks and common leaks. The analysis can be carried out following Critical Examination before a decision is made to proceed with more extensive design. Although here the emphasis is on plant it is necessary to do similar studies on the transport of raw materials and products.

In order to ascertain the problems, it is necessary to identify the proposed site and effect an approximate layout of the plant. The basic information required is listed in (Anon., section 4.3, 1993) and some of this information is subsequently transmitted to Regulatory and Planning Authorities when required. The Preliminary Consequence Analysis of Major Hazards will not give an accurate assessment of the frequency of any incident nor the measures used to control or avoid the release. It should however consider ways of dealing with the resulting emergency and instigating the emergency response.

The report should at this stage concentrate on the response to the emergency rather than countermeasures to a specific release. However due attention must be given to the possible escalation of the incident, including escalation as a result of mitigating efforts such as fighting fires.

4.4.3 Short-Cut Risk Assessment Method (SCRAM)

Risk is here defined as the Likelihood, L, of a specific undesired event occurring within a given period or in particular circumstances. The likelihood is measured as a frequency per year. The Severity, S, is a measure of the expected consequence of an incident outcome. The *Target Risk* is defined by the equation

$$\text{TARGET RISK} = \log_{10}10^{L} + \log_{10}10^{S} = L + S$$

where L is the exponent of likelihood as measured by frequency (a negative value) and S is the severity ranking. *The target risk is only acceptable when its value is equal to or less than zero.*

To reduce the risk, take measures to:

a) reduce the likelihood of occurrence, which is a measure of the expected probability or frequency of occurrence of an event.

or

b) ameliorate the severity of the consequences of its occurrence by appropriate measures, for example the exposure of an individual to a hazardous substance which may not be eliminated by other means might involve measures aimed at prevention of exposure, reduction of emission or exposure and provision of means for dealing with residual risk.

5 Conclusions

From the theoretical work and the two case studies some specific and general experiences and recommendations can be drawn which are summarized below. In this connection it must be remembered that the TOMHID project continues until 1. August 1994 and that the method will be further improved during the work packages 3.2, 4 and 5.

5.1 Arising from the batch case study

From the case study of the batch reactor plant (appendix A) the following points can be noted:

- Functional decomposition: "Methods" and "Constraints" identified as hardware (equipment, chemicals, etc.) are much easier to decompose in a cogent way than objects identified as software (operations, management etc.). Especially "6.0 Manage the operation" and "7.0 Support the operation" cause trouble with respect to selection of an appropriate modelling structure. The structure chosen is to a large extent close to the organisational working structure at the plant and the hierarchical structure of the quality assurance system. (The impact of management and organisational factors on plant safety will be further investigated in work package 3.2).

- Graphical form: Two examples ("1.5.0: Provide MTI" and "7.3.0: Cleaning of MTI/MCF feedsystem") have been worked out to illustrate the application of the graphical form. The numbers in the two forms correspond to the same numbers in the tabular forms. With respect to the graphical presentation form it is important to notice that these forms provide the possibility of clearly showing the interrelations between the different Methods and Constraints related to a specific Intent.

- Level of detail: The batch reactor plant selected as test case is a rather small chemical process plant what concerns the size of the plant, the quantity of chemical substances handled and the number of operators directly involved in the production. In the plant functional model the level of detail is high and probably too high for a plant level hazard identification purpose. Therefore it is expected that the degree of detail of plant functional models will be less extensive for other and bigger chemical process plants.

5.2 Arising from the continuous case study

Several useful conclusions can be drawn from this exercise (appendix B); they are summarized below, according to subject.

- Overall efficacity: Producing the model, top-down, to the required level of detail and then performing the hazard analysis in bottom-up fashion worked as intended. No great difficulties were encountered and the results seem comparable to a HAZOP to the same level of detail. In fact, hazards such as those associated with security and catalyst handling would probably not have been identified by other methods at this level.

-Keywords: In general, the existing keywords performed well. However, it is clear that keywords such as EXTREME_WEATHER may be too general to guarantee meaningful results without extra imagination on the part of the analysis. Consideration must therefore be given to expanding some of the existing keywords into sub-categories.

Similarly, as noted for Functions 3.1.5, 3.1.7 and 3.1.8, in the example, new keywords are likely to be required to cope with some situations, especially those that concern functions such as maintenance and transport which are outside the immediate domain of the process. It is worth stressing that the development of keywords appropriate to these areas is most important; existing methods of hazard identification do not adequately address these areas and TOMHID offers an opportunity to improve upon this situation.

Standard Methods and Constraints: The existing standard Methods and Constraints performed well, allowing identification of problems which existing methods might not have focused upon so readily. However, some revision is clearly necessary, in particular the need to distinguish clearly between Methods such as *Protect from man-made disasters* and *Protect from incidents in adjacent plant.*

Duplicate hazard statements: Performing the hazard analysis 'bottom-up' allowed a more rational treatment of duplicate hazards than when it is performed 'top-down' and is clearly the preferable procedure. Two general types of duplicate statement have been identified: hazards which are repetitive across functions; and those which are repetitive within a function.

As already noted in WP4 (Davies & Whetton, 1993), the use of a Hazard Library, stating hazards in a standard form, would allow duplicates to be readily identified by the software so that, where duplicates occur within a function, they can be collected and moved up to the function's Intent and where duplicates occur across functions, they can be tied to the most appropriate place and then cross-referenced at the other places where they occur. Developing from this is the concept of a Specific Hazard Dictionary, a data-base which would be specific to the analysis and would list the identified hazards against where they occur in the analysis. The opposite concept, collecting hazard statements and moving them up to the higher levels, was demonstrated in Functions 5 and 6 of the example, where it appears to be adequate but inconvenient; the proposed solution of a Specific Hazard Dictionary may well have advantages.

Substances list: Although a substance list was not prepared as part of this exercise, it became apparent that in preparing such a list consideration must be given to the 'before and after' states of materials such as catalysts. Other work (Whetton, 1993), (Whetton & Armstrong) suggests that materials of construction should also be added to the substances list.

5.3 General

- Tabular form: The tabular presentation form in which the Concept Hazard Analysis is linked to the plant functional model gives a good overview of the hazards and safety aspects of the different parts of the chemical process plant.

- Standard Methods and Constraints: The use of standard Methods and standard Constraints at a high plant functional level ensures that these important safety aspects are considered and integrated in the analysis. However, experience

shows that further development of these concepts is required, before they can be reliably used as generic TOMHID objects. Work is under development to improve the model for maintenance and this will be reported shortly; further refinements will follow.

- Duplicate hazard statements: The functional based Concept Hazard Analysis has a tendency to throw up the same problems several times in different places. While such redundancy is not detrimental, some means will have to be found to keep this problem within bounds. In appendix B, two possible approaches to the problem have been demonstrated: collecting hazards to a higher level and recording them only at the lowest levels. Neither method seems satisfactory on its own and it seems probable that ad-hoc use of both methods is preferable.

Acknowledgements

The authors wish to thank the work performed in the frame of the TOMHID project by our partners at VTT (Technical Research Centre of Finland), Tecsa (Italy), Joint Research Centre (Ispra), SRD Division of AEA Consulting (United Kingdom) and CIEMAT (Spain).

Furthermore, we wish to acknowledge the CEC programme *Major Industrial Hazards* for sponsoring the TOMHID project.

References

Anon. (1993). *Conceptual Study of Hazard Identification and Risk Reducing Methods.* Final WP2 report. CIEMAT, JRC, Risø, SRD, Sheffield University (editor) & VTT (deliverer). 284 pp.

Davies, J. & Whetton C.P. (1993). *TOMHID Software Design Document: Software Specification.* 22 pp.

Kletz, T.A. (1992). *Hazop and Hazan.* Rugby, IChemE, ISBN 0-85295-285-6.

Malmén, Y., Nissilä, M, Rasmussen, B. & Rouhiainen, V. (1992). *Nordic Experiences and Future Trends for the Preparation of Safety Reports.* Nordic Council of Ministers. Nord 1992:46. 180 pp.

Wells, G., Wardman, M. & Whetton, C.P. (1993). *Preliminary safety analysis.* J.Loss Prev. Process Ind., **6**, 47-60.

Whetton, C.P. (1993). *Sneak Analysis of Process Systems.* Trans IChemE, Vol 71, Part B, August 1993. pp 169-179.

Whetton, C.P., and W. Armstrong. *Sneak Analysis Applied to Batch Processes.* Journal of Hazardous Materials. Publication details to be announced.

A Case study of a batch reactor plant

A.1 Introduction

This appendix contains one batch reactor example performed on the principles of the TOMHID tool described in the main report. The intention is to illustrate and discuss how the concept and the principles can work in practice. First, the technical plant configuration is shortly described together with remarks and results on the practical implementation of the functional modelling principles and the Concept Hazard Analysis on the batch reactor plant. Second, enclosed to the appendix the tabular forms and a few graphical examples can be found containing the functional plant decomposition and the hazard identification. The main conclusions and recommendations from this example are summarized in chapter 5 of the main report together with the corresponding results from the continuous process plant example.

A.2 Short description of the batch reactor plant

The selected batch reactor example is the previous production of the herbicide PMP (Phenmedipham) at the Danish company Kemisk Værk Køge A/S (KVK). The production of PMP at KVK was abandoned in 1989, the consequence of a production reorganisation at KVK. *Thus, due to this reorganisation is must be emphasized that the activities at KVK no longer involve quantities of hazardous substances which according to the Seveso Directive may lead to major-accident hazards.*

The following plant description is very short. A more detailed and comprehensive safety report can be found in Malmén et al (1992).

Information about the involved chemical substances and their combustion products

For the production in question the final product is Herbaphene. The chemical composition of Herbaphene is PMP and auxiliary substances dissolved in isophoron. In the production the following chemical substances are involved: *m*-aminophenol (MAP), methyl chloroformate (MCF), *m*-tolyl isocyanate (MTI), 28% NaOH solution and 30% HCl solution. The formulation process further involves isophoron and for cleaning of equipment solvesso (trimethylbenzene) and varsol (solvent naphtha) are used.

From a safety point of view the most essential chemical substances are:

- MCF: (Formula: $ClCOOCH_3$). Colourless or light yellow volatile liquid (b.p. 71°C and high vapour pressure at 20°C) with vapours extremely irritating to eyes. MCF is classified as "poisonous" (TLV: 0.2 mg/m^3). Even relatively low concentrations of MCF can be highly toxic to human beings upon inhalation (pulmonary edema). MCF is inflammable and explosion hazards arise when MCF vapours are mixed with air. Vapours may travel to a source of ignition and flash back. Water and humid air can hydrolyse MCF under the formation of toxic and corrosive fumes. MCF is very dangerous when exposed to heat sour-

ces, sparks, flames or oxidizers. Combustion products: Phosgene ($COCl_3$) and toxic fumes of Cl^-.

- MTI: (Formula: $OCN.C_6H_4.CH_3$). Colourless or light yellow and flammable liquid with a characteristic smell. MTI has a relatively high boiling point, 189°C. MTI vapours have a high density, 3.7. MTI is classified as "extremely poisonous" (TLV: 0.035 mg/m^3) and it is irritating to eyes, skin and respiratory organs. Combustion products: Oxides of nitrogen (NO_x).
- MAP: (Formula: $HO.C_6H_4.NH_2$). MAP is a solid substance which smells like phenol (b.p. 164°C, m.p. 121-122°C). MAP is soluble in water. MAP is classified as "injurious to health". Combustion products: Oxides of nitrogen (NO_x).
- PMP: (Formula: $C_{16}H_{16}N_2O_4$). Pure PMP forms colourless crystals (m.p. 140-144°C). No fire or explosions hazards exist. PMP is not classified. Combustion products: Fumes are injurious to health.

Quantities of chemical substances involved in the different activities

The PMP synthesis is carried out as a batch process. The process time is 8 hours per batch and the capacity is 590 kg PMP per batch. MCF and MTI are stored in 200 litre drums inside covered by a plastic coating. The maximum storage size is limited to 6 tons of each substance. Isophoron is stored in a 20 tons container. MAP is stored in sacks and the average size of the MAP storage is 5 tons.

Information about processes and chemical reactions

The PMP plant consists of two stirred batch reactors (tank A and B). The raw materials MCF and MTI are automatically added to tank A through a special piping installation. A thin layer evaporator is installed between tank A and B. A holding tank for the final product (tank C) is connected to tank B. Furthermore, there is a tank for collection of waste water (tank D). The Herbaphene manufacturing can be divided into four steps:

- PMP synthesis: Initially water and MAP are mixed. MCF is added and the intermediate product methyl-N-(3-hydroxyphenyl)-carbamate (MHPC) is formed. This step of the synthesis is carried out at fixed pH and by addition of ice the temperature is kept at a fixed level. This reaction step is exothermic and if the addition of ice is omitted a temperature increase of 16°C will appear. In the second step PMP is formed by a reaction between MTI and MHPC. In the second step pH is fixed while the temperature will increase slowly. MCF and MTI are added through the special piping installation from the storage drums placed in a small room separated from the rest of the plant. The chemical reactions are:

$$\underset{(MCF)}{CH_3OCOCl} + \underset{(MAP)}{C_6H_4(OH)\text{-}NH_2} \longrightarrow \underset{(MHPC)}{C_6H_4(OH)\text{-}NHCOOCH_3}$$

$$\underset{(MHPC)}{C_6H_4(OH)\text{-}NHCOOCH_3} + \underset{(MTI)}{C_6H_4(CH_3)\text{-}NCO} \longrightarrow \underset{(PMP)}{C_6H_4(CH_3)\text{-}NHCOO\text{-}C_6H_4\text{-}NHCOOCH_3}$$

- Isophoron formulation: When the synthesis is finalized pH is lowered and PMP is dissolved in isophoron.
- Drying of the isophoron phase: The isophoron is pumped through the thin layer evaporator and by contact with hot air the water content of the isophoron phase is lowered.

- Addition of auxiliary substances: Auxiliary substances are added to the isophoron solution and isophoron is added adjusting the mixture to the Herbaphene requirements. Finally, the Herbaphene drums are filled with the product.

The overall structure of the PMP plant

The overall structure of the PMP is presented in table A1 and in figure A1 the flow diagram of the PMP production can be found.

Table A1. Overall structure of the PMP plant

Provide raw materials	• Provide MAP, MCF, HCl, NaOH, MTI, isophoron, NaCl, auxiliary substances
Pre treatment	• The batch reactor is filled with water. • Addition of MAP. • Conditioning of pH (HCl); conditioning of temperature (ice).
Reacting	• Addition of MCF. • Reacting MAP and MCF to MHPC in water; conditioning of pH (NaOH); conditioning of temperature (ice). • Increase of pH (NaOH). • Addition of MTI. • Reacting MTI and MHPC to PMP in water; conditioning of pH (HCl, NaOH).
Post treatment	• Decrease of pH (HCl). • Addition of isophoron and NaCl. • Separation of water and isophoron phases. • Drying of the isophoron phase (thin layer evaporator). • Addition of auxiliary substances (xylene, emulsifiers, dispersants); adjustment of product to Herbaphene requirements.
Storage	• Packing and storage of the product Herbaphene.
Auxiliary activities	• Maintenance, repair and cleaning of process equipment. • Treatment of solid waste, waste water and exhausted air. • PMP control systems (including sequence control, alarm systems etc.). • PMP emergency system.

Information relating to the organisation and the management

The organisation of the PMP activities at KVK is split up into three levels.

Strategic level:
- *Managing director* responsible for performance of the primary safety and quality goals for the enterprise.
- *Technical director* responsible for performance of the safety and quality goals for the PMP production.
- *Head of quality assurance department* responsible for:
  * development and implementation of the quality assurance system
  * performance of quality assurance tests
  * analysis of deviations from expected quality
  * information to the board of directors about the implementation of the quality assurance programme.

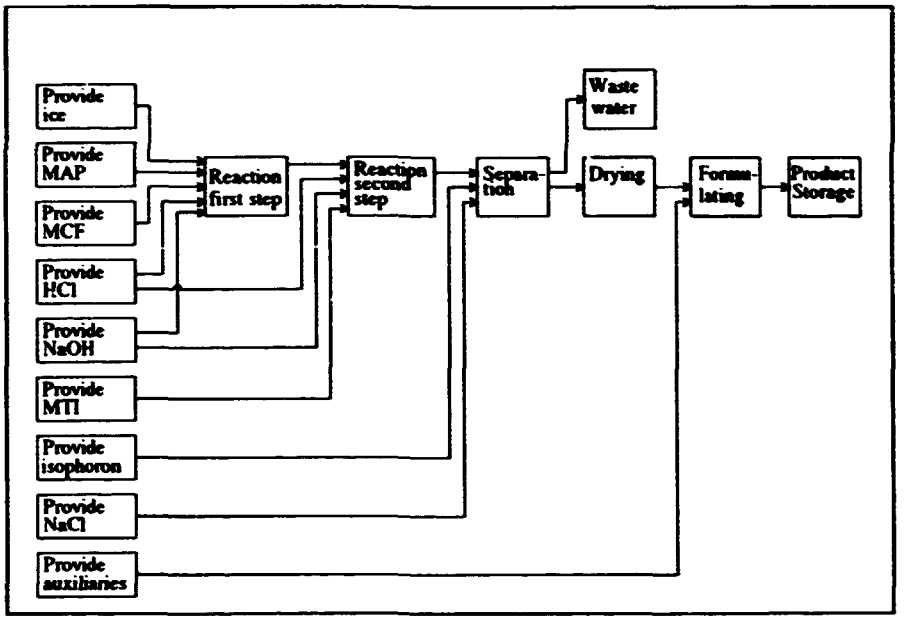


Figure A1. Flow diagram - PMP production.

- *Safety officer* responsible for promoting safety at KVK. The safety organisation comprises:
  * the safety officer
  * a safety, health and welfare committee with 5 members
  * 33 safety groups.

  Furthermore, an industrial doctor is employed.

Tactical level:
At the tactical level there are three managers: Head of production, head of maintenance and an engineer responsible for the electrical installations. Each of these is responsible for working out procedures, instructions and manuals necessary to meet the safety and quality goals in accordance with the principles laid down in the strategic plan.

Operational level:
For each of the three working areas (production, maintenance and electrical facilities) 2 managing engineers are responsible for:
- that all employees in his group are informed about instructions and procedures
- that manuals and instructions are obeyed
- that the necessary revisions of technical and administrative instructions and information are initiated and implemented
- that all employees possess sufficient training and experience
- that the activities in his area are coordinated with the other activities at KVK
- that tests initiated by the quality assurance department are accomplished.

Quality assurance system

A quality assurance system has been developed in relation to the PMP production. The QA handbook contains a description of the primary principles for quality assurance at KVK. Routines for construction, control, operation, maintenance, repair, emergency etc. are described in manuals. Finally, series of instructions contain detailed descriptions of the specific job functions.

Emergency plan for hazardous releases and large fires at KVK

Incidents involving MCF or MTI have been integrated in the general emergency programme of KVK. It must be stressed that the general emergency plan comprises incidents and accidents that might occur in connection with other KVK activities. The following incidents and alarms are covered by the emergency plan:

1. Local emergency: Minor incidents limited to a production unit.
2. Internal emergency: Major incidents causing inconveniences outside a production area but without effects outside the area of KVK.
3. External emergency: Major hazards.

A.3 PMP plant functional model

As mentioned earlier the functional modelling of the PMP plant has been carried out by use of the tabular form. To illustrate the application of the graphical form two examples have been prepared.

The overall plant Intent has been defined as Produce PMP. The Methods and Constraints related to the overall Intent has been defined on basis of the overall plant structure (table A1) and the lists of standard methods and standard constraints (table 1 and 2 of the main report). This has resulted in the following first level objects in the functional model of the PMP plant:

Intent	Produce PMP
by	
Method	Provide raw materials
Method	Pre-treatment
Method	Reacting
Method	Post-treatment
Method	Store final product
Method	Manage the operation
Method	Support the operation
with	
Constraint	Protect the environment from the plant
Constraint	Protect the plant from the environment

Each of these Methods or Constraints have been further decomposed until an appropriate level of details has been achieved. During the functional modelling it is important to keep in mind that the main reason for carrying out the functional modelling is the subsequent hazard identification and therefore the functional modelling has to end up with methods and constraints suitable for the keywords of the Concept Hazard Analysis.

A.4 Concept Hazard Analysis

The relevant keywords considered in relation to the PMP plant are listed below. These keywords have been selected on basis of our knowledge about the technical configuration of the PMP plant and the general list of keywords (Wells, Wardman & Whetton, 1992) and (Anon. 1993).

The Concept Hazard Analysis of the batch reactor plant has been carried out as described in section 4.2.1; i.e. CHA without computer support.

Selected keywords:
- flammables: ignition; fire
- chemicals: toxic; highly toxic; extremely poisonous; corrosion
- health hazards: chemical contact; exposure
- reactions: mildly exothermic
- process conditions: temperature; pH
- equipment problems: capacity; pipelines; below; drum; feedsystem; pump; separator; evaporator; formulation
- mode of operation: test and maintenance;
- operator performance: working discipline; supervision and support; qualifications and education; emergency exercises and training
- procedures: working practice
- system climate: corporate culture; public relations
- organisation: decision-making hierarchy
- management system: safety responsibilities; handling emergencies
- communication: incident reporting and investigations; information quality

A.5 Results

Identified potential hazards

The most essential hazard is dispersion and combustion of the extremely poisonous substance MTI. Health hazards may also exist in relation to other chemical substances and here special emphasis must be laid on dispersion and combustion of MCF.

Identified sources of hazards and the conditions under which an accident could occur

During handling or internal transport drums containing the toxic chemical substances may be damaged, and this may cause a leak of a toxic chemical. Toxic chemicals may be released during repair, maintenance and cleaning, e.g. if a drum is not fully emptied or the feed system is drained insufficiently. A fire in one of the chemical storages may be initiated if highly inflammable substances are erroneously placed in the storage. Furthermore, releases and spills during processing may be considered caused by ruptures, leakages and overfilling.

Assessment of accident consequences

This may include dose/concentration assessment covering the following scenarios:
- evaporation of toxic gases from a pool
- emission of toxic fumes from a pool fire
- emission of toxic fumes from a large fire in a chemical storage.

Safety measures

The safety level at the PMP plant is high, both technically and organisationally. Several safety measures have been implemented and installed, thus reducing the incident frequencies and the incident consequences. The precautions cover all ac-

tivities where MTI and MCF are involved, i.e. handling, storage, transport and processing. The most important safety measures are:
- implementation of the quality assurance system
- implementation of the PMP emergency plan.

The implementation of the emergency plan has resulted in very good possibilities and conditions for efficient prevention and handling of incidents. The established alarm system is considered to be sufficient to ensure that neighbours are warned efficiently in case of a major accident hazard at the enterprise.

FUNCTION			HAZARDOUS PROCESS CHARACTERISTICS - PMP PLANT					
REF	T	DESCRIPTION	k	KEYWORD	MAIN VARIANCE	CONSEQUENCES	MITIGATION	NOTES
0	I	Produce PMP						
1	M	Provide raw materials		See 1.0				
2	M	Pre-treatment		See 2.0				
3	M	Reacting		See 3.0				
4	M	Post-treatment		See 4.0				
5	M	Store final product		See 5.0				
6	M	Manage the operation		See 6.0				
7	M	Support the operation		See 7.0				
8	C	Protect the environment from the plant		See 8.0				
9	C	Protect the plant from the environment		See 9.0				
1.0	I	Provide raw materials						
1.1	M	Provide MAP	a	Chemicals: Toxic	Release → ignition	Emission of NO_x, MAP	Handling and storage procedures	Check health effects
1.2	M	Provide MCF	a	Flammables	Release → fire	Emission of $COCl_2$, Cl^-, MCF	Handling/cleaning/storage procedures Emergency system QA-system	Check health effects
			b	Chemicals: Highly toxic	Release → evaporation	Emission of MCF		
1.3	M	Provide HCl	a	Chemicals: Corrosion	Release	Corrosion	Handling and storage procedures	
1.4	M	Provide NaOH	a	Chemicals: Corrosion	Release	Corrosion	Handling and storage procedures	
1.5	M	Provide MTI	a	Chemicals: Extremely poisonous	Release → ignition	Emission of MTI, NO_x	Handling/cleaning/storage procedures Emergency system QA-system	Check entrainment of MTI in case of fire Check health effects
1.6	M	Provide isophoron	a	Flammables	Release → fire	Fire, domino effects	Segregation by distance	Fire hazard moderate

FUNCTION			HAZARDOUS PROCESS CHARACTERISTICS - PMP PLANT						
REF	T	DESCRIPTION	k	KEYWORD	MAIN VARIANCE	CONSEQUENCES	MITIGATION	NOTES
1.7	M	Provide NaCl	a	No hazards				
1.8	M	Provide xylene	a	Flammables	Release → ignition or explosion	Fire, domino effects	Segregation by distance Xylene gas detector	Xylene ignition source
1.1.0	I	Provide MAP						
1.1.1	M	Warehouse operations	a	Chemicals: Toxic	Release during storage	Emission of NO_x, MAP	Regular inspection of storage	
1.1.2	M	Load MAP drum onto truck	a		Release during handling		Handling procedures	
1.1.3	M	Transport by truck to local storage	a		Release during transport		Transportation procedures	
1.1.4	M	Unload from truck into local storage	a		Release during handling		Handling procedures	
1.1.5	C	Operation manual	a	Working practice	Procedures not followed			
1.2.0	I	Provide MCF						
1.2.1	M	Warehouse operations	a	Flammables	Release during storage	Emission of MCF, Cl', $COCl_2$	Regular inspection of storage, logbook HCl gas alarm system	To be investigated
			b	Chemicals: Highly toxic				
1.2.2	M	Load MCF onto truck	a	Flammables	Release during handling		Handling procedures See 1.2.7; 1.2.8; 1.2.10	To be investigated
			b	Chemicals: Highly toxic				
1.2.3	M	Transport by truck to local storage	a	Flammables	Release during transport		Transportation procedures See 1.2.6; 1.2.7; 1.2.8; 1.2.10; 1.2.11	To be investigated
			b	Chemicals: Highly toxic				
1.2.4	M	Unload from truck into local storage	a	Flammables	Release during handling		Handling procedures See 1.2.7; 1.2.8	To be investigated
			b	Chemicals: Highly toxic				
1.2.5	C	Procedures for MCF handling	a	Working practice	Procedures not followed			To be investigated

FUNCTION			HAZARDOUS PROCESS CHARACTERISTICS - PMP PLANT					
REF	T	DESCRIPTION	k	KEYWORD	MAIN VARIANCE	CONSEQUENCES	MITIGATION	NOTES
1.2.6	C	Establish restricted route for transport of MCF	a	Working discipline	Route not established properly			To be investigated
1.2.7	C	Close supervision of all movements of MCF is required	a	Supervision and support	Not performed properly			To be investigated
1.2.8	C	Radiotelephone must be available during the MCF transport	a	Supervision and support	Not performed properly			To be investigated
1.2.9	C	HCl gas alarm system in central storage	a	Test and maintenance	Malfunction of alarm system	Undetected fire or release		Check maintenance procedures
1.2-.10	C	Absorbing material, slaked lime and extinguisher available at central storage	a	Availability	Not available	Escalation of consequences in case of an accident		Check routine inspection of accident protective measures
1.2-.11	C	Fire alarm and gas alarm system at local storage (PMP control system)	a	Test and maintenance	Malfunction of alarm systems	Undetected fire or release		Check maintenance procedures
1.3.0	I	Provide HCl						
1.3.1	M	Warehouse operations	a	Chemicals: Corrosion	Release during storage	Chemical exposure, corrosion	Regular inspection of storage	
1.3.2	M	Load HCl drum onto truck	a		Release during handling		Handling procedures	
1.3.3	M	Transport by truck to local storage	a		Release during transport		Transportation procedures	
1.3.4	M	Unload from truck into local storage	a		Release during handling		Handling procedures	
1.3.5	C	Operation manual	a	Working practice	Procedures not followed			
1.4.0	I	Provide NaOH	a					
1.4.1	M	Warehouse operations	a	Chemicals: Corrosion	Release during storage	Chemical exposure, corrosion	Regular inspection of storage	
1.4.2	M	Load NaOH drum onto truck	a		Release during transport		Handling procedures	
1.4.3	M	Transport by truck to local storage	a		Release during handling		Transportation procedures	

FUNCTION			HAZARDOUS PROCESS CHARACTERISTICS - PMP PLANT					
REF	T	DESCRIPTION	k	KEYWORD	MAIN VARIANCE	CONSEQUENCES	MITIGATION	NOTES
1.4.4	M	Unload from truck into local storage	a		Release during handling		Handling procedures	
1.4.5	C	Operation manual	a	Working practice	Procedures not followed			
1.5.0	**I**	**Provide MTI**						
1.5.1	M	Warehouse operations	a	Chemicals: Extremely poisonous	Release during storage	Emission of NO_x, MTI	Regular inspection of storage, logbook	To be investigated
1.5.2	M	Load MTI onto truck	a		Release during handling		Handling procedures See 1.5.7 - 1.5.9	To be investigated
1.5.3	M	Transport by truck to local storage	a		Release during transport		Transportation procedures See 1.5.6 - 1.5.10	To be investigated
1.5.4	M	Unload from truck into local storage	a		Release during handling		Handling procedures See 1.5.7; 1.5.8	To be investigated
1.5.5	C	Procedures for MTI handling	a	Working practice	Procedures not followed			To be investigated
1.5.6	C	Establish restricted route for transport of MTI	a	Working discipline	Route not established properly			To be investigated
1.5.7	C	Close supervision of all movements of MTI is required	a	Supervision and support	Not performed properly			To be investigated
1.5.8	C	Radiotelephone must be available during the MTI transport	a	Supervision and support	Not performed properly			To be investigated
1.5.9	C	Absorbing material, slaked lime and extinguisher available at central storage	a	Availability	Not available	Escalation of consequences in case of an accident		Check routine inspection of accident protective measures
1.5-.10	C	Fire alarm and gas alarm system at local storage (PMP control system)	a	Test and maintenance	Malfunction of alarm systems	Undetected fire or release		Check maintenance procedures
1.6.0	**I**	**Provide Isophoron**						
1.6.1	M	Transport by lorry to local storage	a	Flammable	Leakage → release → ignition	Fire, domino effects		Fire hazard moderate
1.6.2	M	Unload isophoron container	a					

FUNCTION			HAZARDOUS PROCESS CHARACTERISTICS - PMP PLANT					
REF	T	DESCRIPTION	k	KEYWORD	MAIN VARIANCE	CONSEQUENCES	MITIGATION	NOTES
1.6.3	C	Spill basin	a	Flammable	Ignition	Fire, domino effects		
			b	Capacity				OK
1.6.4	C	Operation manual	a	Working practice	Procedures not followed			
1.8.0	I	Provide xylene						
1.8.1	M	Warehouse operations	a	Flammables	Release during storage	Fire, domino effects	Regular inspection of storage Fire alarm (see 1.8.6)	
1.8.2	M	Load xylene drum onto truck	a		Release during handling		Handling procedures	
1.8.3	M	Transport by truck to local storage	a		Release during transport		Transportation procedures	
1.8.4	M	Unload from truck into local storage	a		Release during handling		Handling procedures	Xylene ignition source
1.8.5	C	Operation manual	a	Working practice	Procedures not followed			
1.8.6	C	Fire alarm in central storage	a	Test and maintenance	Malfunction of alarm system	Undetected fire or release		Check maintenance procedures
1.8.7	C	Xylene gas detector in local storage	a		Malfunction of gas detector			
2.0	I	Pre-treatment						
2.1	M	Add water to batch reactor	a	Pipeline, below, drum	Leakage, spill	Release of toxic chemicals	Swamp installed	
2.2	M	Add MAP	a	Reaction	Wrong addition	Useless product	Sequence control	
2.3	M	Conditioning of pH	a	Reaction	Wrong pH	Useless product	Sequence control	
2.4	M	Conditioning of temperature	a	Reaction				No hazards
3.0	I	Reacting						
3.1	M	Add MCF via feedsystem	a	Pipeline, feedsystem	Leakage, spill	Release of toxic chemicals	Swamp installed	

FUNCTION			HAZARDOUS PROCESS CHARACTERISTICS - PMP PLANT					
REF	T	DESCRIPTION	k	KEYWORD	MAIN VARIANCE	CONSEQUENCES	MITIGATION	NOTES
3.2	M	Reacting MAP and MCF to MHPC	a	Reaction: mildly exothermic	Failure of temperature control and omission of addition of ice	Temperature can reach boiling point	Temperature alarm at 30°C installed	
			b	Chemicals: MHPC				MHPC not hazardous
3.3	M	Conditioning of pH	a	Reaction	See 2.3			
3.4	M	Conditioning of temperature	a	Reaction	See 3.2a			
3.5	M	Add MTI via feedsystem	a	Pipeline, feedsystem	Leakage, spill	Release of toxic chemicals	Swamp installed	
3.6	M	Reacting MHPC and MTI to PMP	a	Reaction: Mildly exothermic	See 3.2a			
			b	Chemicals: PMP				No hazards PMP is not classified
3.7	C	Sequence control (PMP control system)	a	Reaction	Wrong sequence	Useless product		
3.8	C	Process condition control (PMP control system)	a	Reaction	Wrong process conditions	Useless product		
3.9	C	Process unit control (PMP control system)	a	Equipment	Failure in process units or components	Leaks, spills, stop of process	Alarm system installed	
3.10	C	Operation manual	a	Working practice	Procedures not followed			
4.0	I	Post-treatment						
4.1	M	Decrease pH	a	Separation	Wrong pH	Bad separation		
4.2	M	Add isophoron via isophoron subsystem and NaCl to the reactor	a	Pipeline, isophoron subsystem	Leakage Bad connection from subsystem to reactor	Release containing water, isophoron and chemicals	Swamp installed	
4.3	M	Separation of water and isophoron phases	a	Pipeline	Leakage	Release containing water, isophoron and chemicals	Swamp installed	
4.4	M	Pump isophoron phase from reactor	a	Pump				

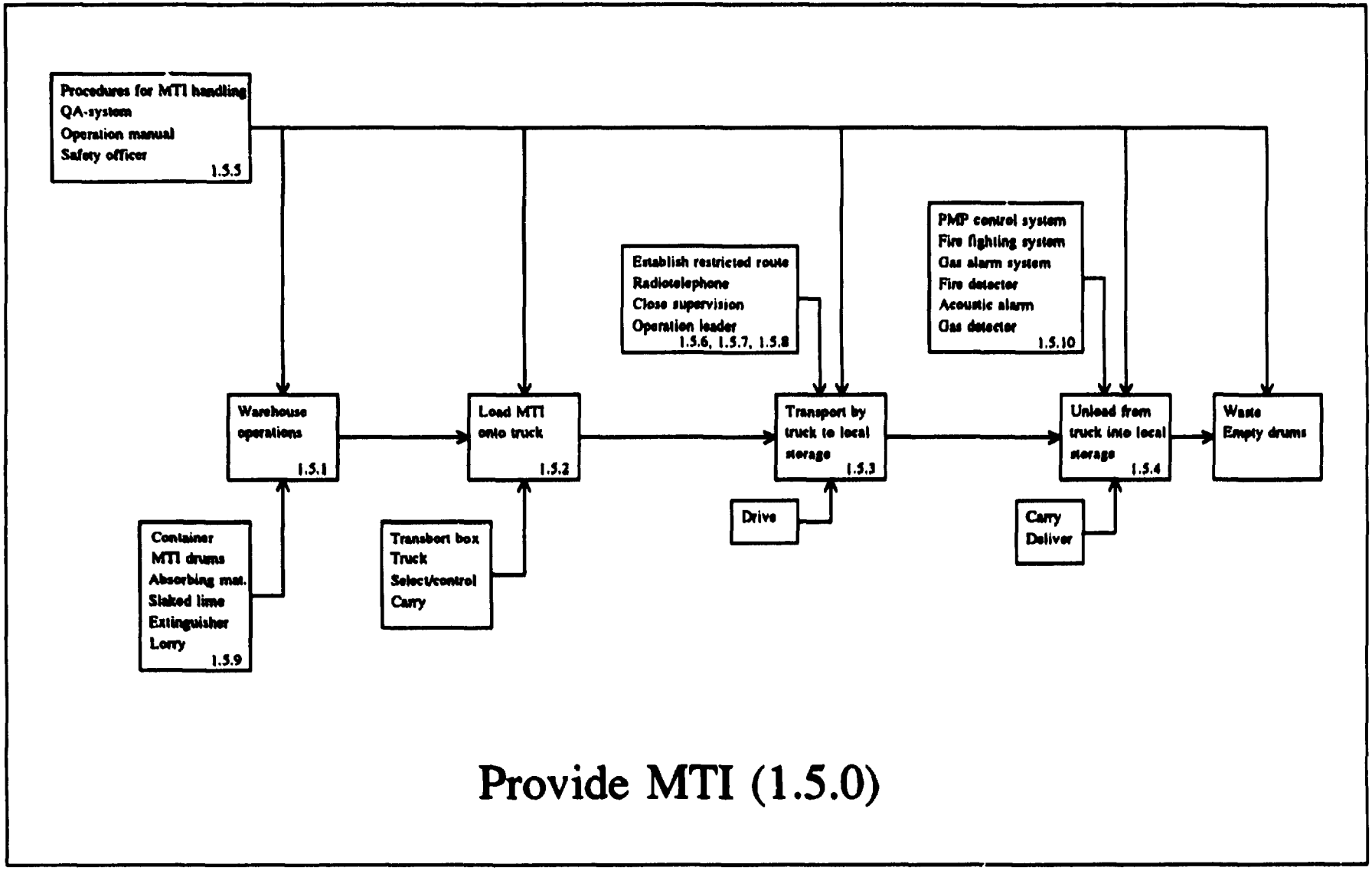
FUNCTION			HAZARDOUS PROCESS CHARACTERISTICS - PMP PLANT					
REF	T	DESCRIPTION	k	KEYWORD	MAIN VARIANCE	CONSEQUENCES	MITIGATION	NOTES
4.5	M	Dry the isophoron phase in thin layer evaporator	a	Evaporator: hot air	Leakage → ignition	Fire	Fire fighting system installed	
4.6	M	Pump isophoron phase to the formulation tank.	a	Pump				
4.7	M	Add auxiliary substances, xylene (product Herbaphene)	a	Formulation	Wrong addition	Useless product	Sequence control	
			b	Flammables	Release during addition	Fire, domino effect		Xylene ignition source
4.8	C	Sequence control (PMP control system)	a	See 3.7				
4.9	C	Process condition control (PMP control system)	a	See 3.8				
4.10	C	Process unit control (PMP control system)	a	See 3.9				
4.11	C	Operation manual	a	Working practice	Procedures not followed			
5.0	**I**	**Store final product**						
5.1	M	Warehouse operations	a	Chemicals: PMP				No hazards PMP not classified
5.2	C	Operation manual	a	Working practice				No hazards
6.0	**I**	**Manage the operation**						
6.1	M	Climate and cultures	a	Public relations	Discussions with local society			From time to time discussions with local politicians and organisations about hazardous activities at the plant
			b	Corporate culture	Lack of shared values			
6.2	M	Organisation structure	a	Decision-making hierarchy	Informal decision structure			Discuss if structure is too complex

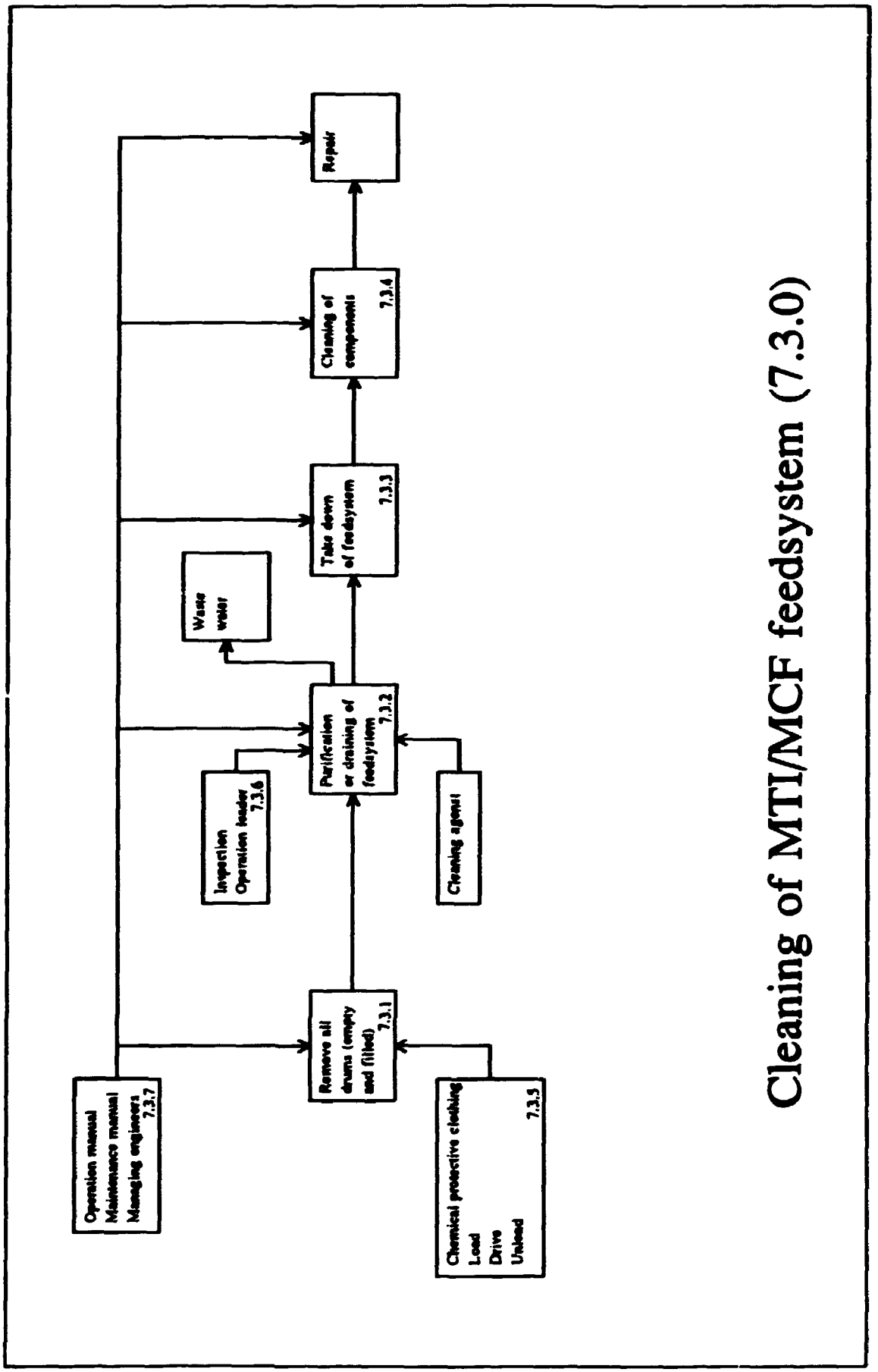
FUNCTION			HAZARDOUS PROCESS CHARACTERISTICS - PMP PLANT					
REF	T	DESCRIPTION	k	KEYWORD	MAIN VARIANCE	CONSEQUENCES	MITIGATION	NOTES
6.3	M	Management structure	a	Safety responsibilities	Some areas not specified			OK
			b	Handling emergencies	Deficiencies in emergency plan			OK
6.4	M	Information	a	Information quality	Lack of information			
6.5	M	Communications	a	Incident reporting and investigations	Some relevant events not included			No incidents reported
6.6	C	Quality assurance system		See 6.6.0				
6.6.0	I	Quality assurance system						
6.6.1	M	Operation manual	a	Working practice	Manuals not followed and updated			Essential with respect to handling of MCF and MTI
6.6.2	M	Construction manual	a	Working practice	Manuals not followed and updated			
6.6.3	M	Repair and maintenance manual	a	Working practice	Manuals not followed and updated			
6.6.4	M	Emergency plan	a	Emergency exercises and training	Personnel not capable in case of an emergency			
7.0	I	Support the operation						
7.1	M	PMP control system		See 7.1.0				
7.2	M	Clean plant area	a	Orderly, tidy	Disorder			
7.3	M	Clean process equipment		See 7.3.0				
7.4	M	Emergency system		See 7.4.0				
7.5	M	Waste disposal		See 7.5.0				
7.6	M	Training of personnel		Qualifications and education	Personnel not qualified			
7.7	C	Quality assurance system		See 6.6.0				
7.1.0	I	PMP control system						
7.1.1	M	Sequence control	a	Reaction	Wrong sequence	Useless product		

FUNCTION			HAZARDOUS PROCESS CHARACTERISTICS - PMP PLANT					
REF	T	DESCRIPTION	k	KEYWORD	MAIN VARIANCE	CONSEQUENCES	MITIGATION	NOTES
7.1.2	M	Process condition control	a	Temperature	Wrong temperature	Temperature can reach boiling point	Temperature alarm at 30°C installed	
			b	pH	Wrong pH	Useless product		
7.1.3	M	Process unit control	a	Equipment	Failure in process units or components	Leaks, spills, stop of process	Alarm system installed	
7.1.4	M	Fire alarm system	a	Test and maintenance	Malfunction of fire alarm system	Undetected fire		Check maintenance procedures
7.1.5	M	Gas alarm system	a	Test and maintenance	Malfunction of gas alarm system	Undetected release of gas		Check maintenance procedures
7.1.6	C	QA-system		See 6.6.0				
7.1.7	C	Set-points, alarm levels, passwords etc.)	a	Equipment	Malfunction of alarms and controls	Critical conditions not detected		Check maintenance procedures
			b	Software	Software errors			To be investigated
7.3.0	**I**	**Clean process equipment (feed-system)**						
7.3.1	M	Remove all drums	a	Health hazard: Chemical contact	Chemical protective clothing in bad conditions or not used	Chemical exposure (small amounts released)		
7.3.2	M	Purification and drainage of feedsystem	a	Health hazard: Chemical contact	Cleaning operations not performed properly	Chemical exposure (small amounts released)		
			b	Supervision and support	Not performed properly			
7.3.3	M	Take down of feedsystem	a	Health hazard: Chemical contact				Low hazard, small amounts of chemicals
7.3.4	M	Cleaning of components	a	Health hazard: Chemical contact				Low hazard, small amounts of chemicals
7.3.5	C	Chemical protective clothing	a	Health hazard	Chemical protective clothing in bad conditions or not available	Chemical exposure (small amounts released)		

FUNCTION			HAZARDOUS PROCESS CHARACTERISTICS - PMP PLANT					
REF	T	DESCRIPTION	k	KEYWORD	MAIN VARIANCE	CONSEQUENCES	MITIGATION	NOTES
7.3.6	C	Inspection	a	Supervision and support	Not performed properly			
7.3.7	C	Operation and maintenance manuals	a	Working practice	Manuals not followed			
7.4.0	I	Emergency system						
7.4.1	M	PMP unit alarms	a	Test and maintenance	Malfunction of alarms	Release/fire not detected		Check test procedures
7.4.2	M	General emergency system at the enterprise (local, internal and external)	a	Test and maintenance	Malfunction of alarms			To be investigated
			b	Emergency communication				
7.4.3	C	Gas alarm system	a	Test and maintenance	Malfunction of gas alarms	Release of gas not detected		Check test procedures
7.4.4	C	Fire alarm system	a	Test and maintenance		Fire not detected		Check test procedures
7.4.5	C	Emergency plan		See 6.6.4				
7.5.0	I	Waste disposal						
7.5.1	M	Collect solid waste, empty drums (MAP, MCF, MTI, xylene etc.)	a	Health hazards	Drums not handled properly	Exposure		
7.5.2	M	Destruction of chemicals	a	Health hazards	Drums and destruction chemicals not handled properly	Exposure		
7.5.3	M	Collection of waste water (from separation, see 4.3)	a	Equipment	Leakage, spills	Release to sewer or swamp of water containing chemicals		To local waste water treatment plant, problem ?
7.5.4	M	Exhausted air from PMP production building	a	Equipment: pipeline	Leaks	Release of air containing small amounts of chemicals		
7.5.5	M	Ventilation system, combustion (power plant or smokestack)	a	Equipment	Flammable gases not detected	Explosion ?		To be investigated
7.5.6	C	QA-system		See 6.6.0				

FUNCTION			HAZARDOUS PROCESS CHARACTERISTICS - PMP PLANT					
REF	T	DESCRIPTION	k	KEYWORD	MAIN VARIANCE	CONSEQUENCES	MITIGATION	NOTES
7.5.7	C	Gas detector in ventilation system	a	Test and maintenance	Malfunction of gas detector	Explosion ?		To be investigated
7.5.8	C	Control and supervision	a	Communication	Boiler tender not contacted before start of production			
8.0	I	Protect the environment from the plant						
8.1	M	Contain process fluids	a	Equipment	Overfilling Pipe leakage	Release to drain/sewer		
						Release to sea		Very unlikely
8.2	M	Avoid accidental releases	a	Equipment	Malfunction of scrubber system	Toxic release (small amounts of chemicals)		
			b	Equipment	Malfunction of ventilation system	Toxic release (small amounts of chemicals)		
8.3	M	Control waste disposal		See 8.1 and 8.2				
9.0	I	Control the plant from the environment						
9.1	M	Protect against natural disasters	a	Earthquake				No hazards
			b	Flood				No hazards


Procedures for MTI handling
QA-system
Operation manual
Safety officer
1.5.5
Establish restricted route
Radiotelephone
Close supervision
Operation leader
1.5.6, 1.5.7, 1.5.8
PMP control system
Fire fighting system
Gas alarm system
Fire detecter
Acoustic alarm
Gas detecter
1.5.10
Warehouse operations
1.5.1
Load MTI onto truck
1.5.2
Transport by truck to local storage
1.5.3
Unload from truck into local storage
1.5.4
Waste
Empty drums
Container
MTI drums
Absorbing mat.
Slaked lime
Extinguisher
Lorry
1.5.9
Transbort box
Truck
Select/control
Carry
Drive
Carry
Deliver
Provide MTI (1.5.0)


Cleaning of MTI/MCF feedsystem (7.3.0)
Operation manual
Maintenance manual
Managing engineer
7.3.7
Remove all drums (empty and filled)
7.3.1
Chemical protective clothing
Lead
Drive
Unload
7.3.5
Inspection
Operation leader
7.3.6
Purification or draining of feedsystem
7.3.2
Cleaning agent
Waste water
Take down of feedsystem
7.3.3
Cleaning of components
7.3.4
Repair

B Case study of a section of a continuous process plant

B.1 Introduction

The section of plant chosen for study is a methanator and compressor, shown in Figure B1. This example has been extensively studied and reported upon elsewhere (Anon. 1993, Wells et al. 1993) and only a brief description is given here, in B.2, below. The main conclusions and recommendations from this example are summarized i chapter 5 of the main report together with the corresponding results from the batch reactor example.

B.2 A brief plant section description

The plant section is shown in Figure B1. A mixture of hydrogen and methane gas, containing oxides of carbon as CO and CO_2, enters from the upstream absorber D-1004. The mixture passes through heat exchanger E-101, where it is heated before passing over a platinum catalyst in reactor R-101.

In R-101, oxides of carbon react with hydrogen and are converted to methane and water, liberating considerable heat; the reaction is unstable. The gas exits the reactor and is cooled in E-101 by exchanging heat with the incoming gas stream. Because the reaction is exothermic and unstable, a trip system is provided which, when triggered, bypasses the flow of gas around the reactor.

The gas is further cooled in heat exchanger E-102 and then passes to a knock-out pot, D-102, where entrained water is removed by gravity. Waste water from D-102, which contains dissolved hydrogen and methane and some dissolved salts from the upstream process, is released to the sewer drains by a level controller which maintains a water seal.

Downstream of D-102, some of the gas is bled off as fuel and a relief valve is provided to cope with overpressure conditions. The remaining gas is compressed in a reciprocating compressor and passes to the downstream process. The compressor is provided with its own trip system, which operates upon either low lubricating oil in the compressor or upon high water level in D-102. In the event of a compressor trip, the relief valve, RV1, is expected to lift.

It must be noted that the P&I diagram, while based upon a real plant, is intended to be a preliminary diagram, to be used as an undergraduate and post-graduate exercise in hazard identification. It is therefore acknowledged that Figure B1, as drawn, contains many omissions and is not intended to be representative of good practice.

B.3 Plant section functional model

The plant-section functional model was developed according to the methods described in the text, starting with the Intent of the *plant as: From a hydrogen & methane gas mixture with CO/CO_2 content of nominally 2% (max 10%) and at a pressure of 20bar, produce a gas mixture with CO/CO_2 content ≤ 10ppm and at a pressure of 40bar.*

The model was produced on the assumption that the plant-section was not yet fully designed and that less information was available than is actually given in the

P&I diagram of Figure B1. Since the section falls roughly into two stages: Methanation and Compression, these were chosen as the two initial Methods. Alternatively, three Methods could have been chosen: Methanation; Water removal; and Compression.

To these two Methods, two more standard Methods were added: *Support the operation* and *Manage the operation*, and two standard Constraints: *Protect the plant from the environment* and *Protect the environment from the plant.*

The model was then expanded, item by item, to a level that was felt to be reasonable for an early stage of plant design. Note that, though it appears as Method 4, *Manage the operation* has not been expanded; this decision was made for two reasons: Firstly, this is a section of a plant and no information is available as to the overall management structure. Certainly, one could have been created but it was felt that this would be a rather artificial exercise. Secondly, the example in Appendix A treats this aspect at some length and, since it was difficult to imagine that the management of a continuous plant would be radically different from one devoted to batch processes, an elaborate treatment of management would be repetitious.

It has already been remarked (paragraph 5.3, above) that substantial repetition of the same hazards occurs during this kind of analysis; it is interesting to note that there is evidence for this in the construction of the model, even before hazard identification has begun. For example, Method 3, *Support the operation*, includes the sub-Method 3.6, *Security*, as part of the suggested standard expansion; however, Constraint 6, *Protect plant from the environment*, contains the sub-Method 6.4, *Protect against unauthorised access to plant.* Clearly these requirements overlap and it is probable that other areas of overlap could be identified. While the natural tendency is to eliminate such duplication, it is felt that things should be left as they are for the moment until more experience has been gained. Clearly, however, the existence of such duplicates offers a useful cross-check against accidentally omitting a function. Note that in the subsequent analysis, the sub-Method 3.6, *Security*, has not been developed because the necessary information occurs lower down at sub-Method 6.4, *Protect against unauthorised access to plant*; this was done merely to save space.

B.4 Hazard analysis of the functional model

As recommended in the description of the method (paragraph 4, above) the CHA process of hazard identification was applied bottom-up; i.e. starting, literally, at Intent 12.0 on the analysis form. Keywords were taken from the list given in an earlier report [Anon., 1993], supplemented by the keywords NOT, for every stage of the model, and TOO MUCH, and TOO LITTLE where this was felt to be appropriate. The following discussion follows the bottom-up approach of the original analysis; only points of interest are elaborated in detail.

Functions 9.0, 10.0, 11.0, and 12.0: these have not been developed. The flowsheet does not have sufficient information to analyse these functions for hazards; consequently they have been left with the note: *Process engineering to advise.*

Function 8.0: has been given the keyword NOT. It is known that the purpose of this section of the plant is to remove the oxides of carbon which will cause problems for the downstream plant. The rest of the analysis follows from this premise.

Function 7.0: an increase in oxide level leads to an increase in the exothermic reaction in R-101; clearly such a condition is hazardous and should be alarmed and integrated with the existing methanator trip.

Function 6.4: This shows the utility of the keywords and of the proposed standard Methods. It is interesting to note that, as well as the obvious problems of

sabotage and theft, the method reveals the possibility of 'well-intentioned' intruders, such as the media and family members, gaining access to the site during emergencies and interfering with the activities of the emergency services.

Function 6.3: has four occurrences of the keyword EXTREME_WEATHER and required the analyst's imagination to apply this keyword in such a way as to obtain useful results; suggesting that this keyword would benefit from sub-categories.

Functions 6.2 and 6.1: these two standard Methods appear to be complementary; it may be necessary to revise them or make a very precise distinction between a 'man-made disaster' and an 'incident in adjacent plant'. At present, the only difference seems to be one of scale.

Function 6.0: as an Intent, anything recorded here would merely repeat the results of the lower-level expansions and so it has been left blank.

Function 5.3: it is evident that the keyword TOXICITY ought to be applied to the disposal of effluent; however, the P&I diagram has no information on the toxicity or otherwise of spent platinum catalyst. In practice, this would have been resolved in the Substances List, before the analysis was begun but constraints of time and space have precluded this. However, it does underline the necessity for a complete substance list to be prepared before the analysis is undertaken and raises the question of the scope of such a list: some substances may need to be listed in 'before and after' states.

Functions 3.1.7 and 3.1.8: each of these functions refers to maintenance of a trip system, which, since it operates on demand, must be tested at frequent intervals. At this level of decomposition, none of the existing keywords would lead to a consideration of such test problems. However, further decomposition would (should) introduce trip system testing as a sub-Method; in which case, keywords such as NOT and TOO MUCH would reveal the potential problem.

Again, some modification to the keyword list seems to be indicated. In the example, the keyword TEST was used, though this may not be generally applicable and may be too specific to these circumstances. The question to be resolved is, bearing in mind that TOMHID is a high-level analysis method: do we expect the keyword list to lead to problems at this level of detail or not?

Function 3.1.5 and 3.1.4: again, a new keyword has been introduced.

Functions 3.1.3, -.2, -.1, and -.0: here, by way of illustration, the opposite procedure has been adopted to that used in Function 6.0. Because analysis suggests that, at this level of detail, Functions 3.1.1, 3.1.2, and 3.1.3 all share common hazards, which they also share with 3.1.4 through 3.1.8, it makes sense to consolidate these hazards into a single set of statements under the Intent, Function 3.1.0.

This highlights one aspect of a problem already identified in previous analyses: the repetitive nature of many of the hazards found by this method. In this case, the hazards are not repetitive across different functions (E.g. as between Functions 3.6 and 6.4) but within a Function. One way to resolve this aspect of the problem (already proposed in WP4, software specification) is by the use of a hazard library which, by stating hazards in a standard form would allow duplicates to be readily identified by the software. That done, the user can take appropriate action: where duplicates occur within a function, they can be collected and moved up to the function's Intent; where duplicates occur across functions, they can be tied to the most appropriate place and then cross-referenced at the other places where they occur.

This leads naturally to the concept of a Specific Hazard Dictionary, a data-base which, analogously to a data dictionary in software engineering, would list the identified hazards against where they occur in the analysis.

Function 3.7: while it is known that start-up, and the presence of process lines which are used only for that purpose, constitute a source of hazards for this sys-

tem it was felt that the P&I diagram, as at present given, offers no information to allow this aspect of operation to be analysed. Consequently, it has been left unresolved.

Function 3.6: as already noted, this duplicates Function 6.4 and requires no further analysis.

Function 3.4: has not been developed because no information yet exists as to an emergency plan for the plant.

Function 3.3: has not been developed because the system is not under centralised control and the trip systems themselves are treated throughout the analysis.

Function 1.2.0 and its expansions: these clearly form a duplicate of the analysis under Constraint 2.2 and so have been referenced to it, illustrating the scheme proposed above.

Functions 6 and 5: here, the hazards identified by the sub-functions have been collected and listed under each parent functions 'Consequences'. Certainly, doing so offers a person reading the analysis the opportunity to view the hazards without having to read further and as such this approach may be advantageous. However, to do so in every case would clearly result in an enormous amount of duplicated information. It seems possible that the Specific Hazard Dictionary, proposed above under Functions 3.1.5 and 3.1.4, might be a better solution to the problem.

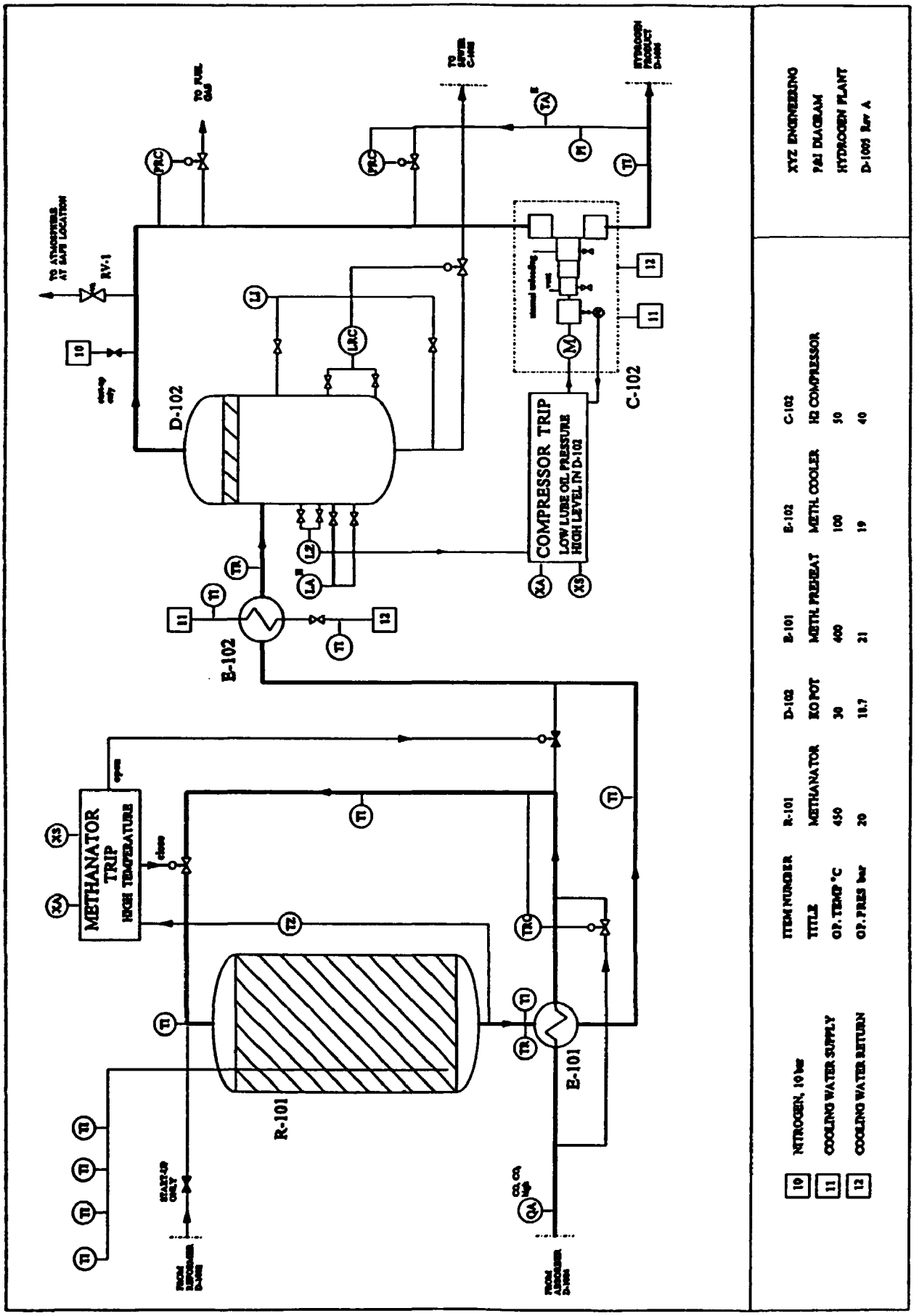


Figure B1. Example of a simplified P & I diagram - methanator and compressor

FUNCTION			HAZARD IDENTIFICATION					
Ref	**T**	**Description**	**k**	**Keyword**	**Main variance**	**Consequences**	**Mitigation**	**Notes**
0	I	From a hydrogen & methane gas mixture with CO/CO_2 content of nominally 2% (max 10%) and at a pressure of 20bar, produce a gas mixture with CO/CO_2 content ≤ *10ppm and at a* pressure of 40bar.						
1	M	Remove CO/CO_2						
2	M	Compress gas to 40bar						
3	M	Support operation						
4	M	Manage the operation						
5	C	Protect environment from plant.		See 5.1-5.4	See 5.1-5.4	Possible fire and explosion through loss of containment. Excess flaring will cause unnecessary loss of energy, bright lights at night, etc. Risks in disposal of used catalyst. Risk of explosion from hydrogen and/or methane in the sewers. Noise, giving risk of disturbance to local population and long-term hearing damage to plant personnel.	See 5.1-5.4	See 5.1-5.4

FUNCTION			HAZARD IDENTIFICATION					
Ref	**T**	**Description**	**k**	**Keyword**	**Main variance**	**Consequences**	**Mitigation**	**Notes**
6	C	Protect plant from environment		See 6.1-6.4	See 6.1-6.4	Impact from vehicles, leading to a release of flammables. External threats from explosion, fire, toxic release, and contaminating material. Environmental threats from high winds, freezing of entrapped water, brittle fracture of metals, etc. Plant at risk from deliberate or accidental intruders. Catalyst is valuable and theft of catalyst is possible during (un)loading operations or when catalyst is stored at site which may encourage intruders.	See 6.1-6.4	See 6.1-6.4
7	C	Inlet CO/CO_2 content ≤ 10%						
8	C	Outlet CO/CO_2 content ≤ 10ppm						
9	C	Inlet pressure 20 bar						

FUNCTION			HAZARD IDENTIFICATION					
Ref	**T**	**Description**	**k**	**Keyword**	**Main variance**	**Consequences**	**Mitigation**	**Notes**
10	C	Outlet pressure 40 bar						
11	C	Inlet temperature tbd						
12	C	Outlet temperature tbd						
1.0	I	Remove CO/CO_2						
1.1	M	Conversion of CO/CO_2 to methane and water by catalytic reaction.		See 1.1.0	See 1.1.0	See 1.1.0	See 1.1.0	See 1.1.0
1.2	M	Remove liquid water (as entrained droplets)		See 1.2.0	See 1.2.0	See 1.2.0	See 1.2.0	See 1.2.0
1.1.0	I	Convert CO/CO_2 to methane and water by catalytic reaction						
1.1.1	M	Heat inlet stream by heat-exchanger E-101		See 1.1.3	See 1.1.3	See 1.1.3	See 1.1.3	See 1.1.3
1.1.2	M	React over catalyst in reactor R-101	a b	NOT TOO MUCH	No reaction. Runaway reaction.	See 8.0 See 1.1.4	See 8.0 See 1.1.4	See 8.0 See 1.1.4
1.1.3	M	Cool outlet stream by heat-exchanger E-101	a b	NOT NOT	Overheated gas, exit R-101 Under heated gas, inlet R-101	Extra duty required of E-102 and D-102. Reaction in R-101 may not take place or proceed to completion, leading to off-spec product to down-stream plant. See 8.0		Process engineering to advise.

FUNCTION			HAZARD IDENTIFICATION					
Ref	**T**	**Description**	**k**	**Keyword**	**Main variance**	**Consequences**	**Mitigation**	**Notes**
1.1.4	C	Prevent runaway of exothermic reaction in R-101	a	NOT	Runaway exothermic reaction in R-101.	Catastrophic failure of reactor vessel, leading to release of flammables and probable explosion.	Methanator trip system.	Evidence suggests that monitoring the reactor outlet temperature will not provide a rapid enough response for a trip, nor will it detect hot-spots in the catalyst beds. Suggest trip system is revised to measure individual bed temps.
1.2.0	I	Remove water						
1.2.1	M	Cool inlet stream by heat exchanger E-102	a	NOT	See 2.2.a	See 2.2.a	See 2.2.a	See 2.2.a
1.2.2	M	Separate water from gas by gravity in KO-pot D-102	a	NOT	See 2.2.a	See 2.2.a	See 2.2.a	See 2.2.a
1.2.3	M	Discharge water to sewer	a b	NOT TOO MUCH	See 2.2.a See 5.3.c	See 2.2.a See 5.3.c	See 2.2.a See 5.3.c	See 2.2.a See 5.3.c
1.2.4	C	Maintain water seal in D-102 to prevent gas entering sewer.	a	NOT	Loss of water seal.	See 5.3.c	See 5.3.c	See 5.3.c
2.0	I	Compress gas to 40bar						
2.1	M	Compress gas in a reciprocating com-pressor	a b	NOT TOO MUCH	Low pressure at exit. High pressure at exit.	 Possible damage to down-stream plant.	 Pressure relief valve fitted.	Process engineering to advise. Consider adding high-pressure to comp. trip.
2.2	C	Gas to be compressed must be dry	a	NOT	Wet gas enters compressor.	Severe damage to compressor, leading to possible release of flammables.		

FUNCTION			HAZARD IDENTIFICATION					
Ref	**T**	**Description**	**k**	**Keyword**	**Main variance**	**Consequences**	**Mitigation**	**Notes**
3.0	1	Support operation						
3.1	M	Maintain process equipment		See 3.1.0-3.1.8	See 3.1.0-3.1.8	See 3.1.0-3.1.8	See 3.1.0-3.1.8	See 3.1.0-3.1.8
3.2	M	Disposal of waste	a	NOT	Fail safely to dispose of waste gasses.	Possible fire or explosion.		
			b	NOT	Fail to safely dispose of effluent from D-102	Possible pollution and fire or explosion from dissolved gasses.		
			c	NOT	Fail safely to dispose of spent catalyst from R-101			Insufficient information available on catalyst and its characteristics.
			d	NOT	Fail safely to dispose of lubricating oil from compressor C-102.			
3.3	M	Control the process						
3.4	M	Manage emergencies						
3.5	M	Catalyst loading	a	TOXICITY	Catalyst may present a toxic hazard.	Possible harm to personnel.		
			b	CONTAMI-NATION	Contaminated catalyst may cause adverse or runaway reactions.			
			c	DROP	Catalyst loading may involve manipulating heavy loads at elevated sites and in difficult conditions.	Possible injury to personnel.		Need to review catalyst loading/unloading procedures.

FUNCTION			HAZARD IDENTIFICATION					
Ref	**T**	**Description**	**k**	**Keyword**	**Main variance**	**Consequences**	**Mitigation**	**Notes**
3.6	M	Security						
3.7	M	Start-up the system safely.						
3.1.0	I	Maintain process equipment	a	FLAMMABLES	Release of flammables during maintenance.	Fire, explosion.		See also 3.5, catalyst loading.
			b	TEMPERATURE	*Personnel fail to observe* procedures for working on high temp. equipment.	*Burns to personnel.*		
			c	PRESSURE	Personnel fail to observe procedures for working on high press. equipment.	Kinetic injuries to personnel.		
3.1.1	M	Maintain R-101		See 3.1.0				
3.1.2	M	Maintain heat exchanger E-101		See 3.1.0				
3.1.3	M	Maintain heat exchanger E-102		See 3.1.0				
3.1.4	M	Maintain KO-pot D-102	a	See 3.1.0				
			b	PROCEDURE	Failure to observe procedures leads to loss of water seal in D-102.	Release of flammables, fire, explosion.		
			c	PROCEDURE	Failure to observe procedure leads to water carry-over from D-102.	Damage to downstream compressor.		

FUNCTION			HAZARD IDENTIFICATION					
Ref	k	Description	k	Keyword	Main variance	Consequences	Mitigation	Notes
3.1.5	M	Maintain compressor C-102	a b	See 3.1.0 PROCEDURES	Failure to observe procedures.	Damage to compressor; poss. damage to or loss of feed to downstream plant. Possible injury to personnel from rotating equipment, high voltages, etc.		
3.1.6	M	Maintain instrumentation and control systems.	a	NOT	Failure to maintain.	Loss of control leading to release of flammables or off-spec product.		
3.1.7	M	Maintain methanator trip system	a b c	NOT TEST TEST	Failure to maintain methanator trip system Fail to test trip system at prescribed intervals. Test trip system more often than prescribed.	Premature failure of trip system, with either spurious shutdown or loss of protection. Possibility of dormant failures. Increased exposure to real trip during test.		
3.1.8	M	Maintain compressor trip system	a b c	NOT TEST TEST	Failure to maintain compressor trip system Fail to test trip system at prescribed intervals. Test trip system more often than prescribed.	Premature failure of trip system, with either spurious shutdown or loss of protection. Possibility of dormant failures. Increased exposure to real trip during test.	None.	

FUNCTION			HAZARD IDENTIFICATION					
Ref	**T**	**Description**	**k**	**Keyword**	**Main variance**	**Consequences**	**Mitigation**	**Notes**
5.0	I	Protect environment from plant.						
5.1	M	Contain process fluids	a	NOT	Flammable gas released to atmosphere.	Possible fire and explosion.	Maintain standards of construction by regular inspections and preventive maintenance. Consider gas detectors and water sprays at critical locations.	
5.2	M	Avoid release of process materials.	a	NOT	Release flammable materials to flare, where they are burned.	Unnecessary loss of energy, bright lights at night, etc.	Consider use of off-spec gas as fuel.	
5.3	M	Ensure safe effluent disposal	a	NOT	Fail to ensure safe disposal of effluent which may be toxic or flammable.			
			b	TOXICITY				Need to determine whether spent catalyst or materials carried forward from upstream plant are toxic.
			c	FLAMMABLES	Fail to ensure safe disposal of liquid draining from D-102 which will contain dissolved hydrogen and methane.	Hydrogen and/or methane will be liberated in the sewers, where it may be transported considerable distances before reaching a source of ignition.	Install gas detectors and forced ventilation system with safe disposal of liberated gasses.	Consider a second vessel at near atmospheric pressure, where gasses may be safely liberated and disposed of before effluent is transferred to the sewer.

FUNCTION			HAZARD IDENTIFICATION					
Ref	T	Description	k	Keyword	Main variance	Consequences	Mitigation	Notes
5.4	M	Avoid acoustic emissions.	a	NOT	High noise levels generated by compressors and flares.	Disturbance to local population, leading to adverse publicity and general hostility to plant operations. Possible long-term hearing damage to plant personnel.	Personnel are provided with protective devices.	Need to examine actual noise levels or expected levels from prior experience.
6.0	I	Protect plant from environment						
6.1	M	Protect against incidents in adjacent plant.	a	See 6.2.b,c,d	See 6.2.b,c,d	See 6.2.b,c,d	See 6.2.b,c,d	See 6.2.b,c,d

FUNCTION			HAZARD IDENTIFICATION					
Ref	**T**	**Description**	**k**	**Keyword**	**Main variance**	**Consequences**	**Mitigation**	**Notes**
6.2	M	Protect against man-made disasters.	a	ACCIDENTAL IMPACT.	Vehicle impact with plant.	Vehicles moving within the plant boundary may impact with equipment, leading to a release of flammables.	Plant is separated from roadways by barriers. Vehicle movement within plant are subject to strict controls.	
						Vehicles outside the plant, ditto.		Need to examine railway lines and flight paths.
			b	EXTERNAL ENERGETIC EVENT	Energetic event in adjacent plant.	Explosion could cause blast and missile dunage, leading to release of flammables.	Plant is physically separated from nearest likely source of explosion.	
						Fire could cause weakening of structures, etc. leading to release of flammables.	Plant is separated from nearest fire source.	Verify fire-fighting procedures & equipment.
			c	EXTERNAL TOXIC EVENT	Toxic release from adjacent plant.	Toxic material from adjacent plant could kill or injure out-door workers and control-room personnel.	Control room is pressurised and fitted with toxic gas alarms.	Need to examine alarm procedures at source of toxic material and procedures for protecting outdoor workers.
			d	EXTERNAL CONTAMI-NATION	Release of contaminating material from adjacent plant.	Contaminating material could enter process and cause dangerous reactions or off-spec product.	It is considered unlikely that contamination could enter the system via the flare-stacks or via the sewers. It is possible to load contaminated catalyst and operating procedures in this area must be investigated.	

FUNCTION			HAZARD IDENTIFICATION					
Ref	**T**	**Description**	**k**	**Keyword**	**Main variance**	**Consequences**	**Mitigation**	**Notes**
6.3	M	Protect against natural disasters.	a	EXTREME WEATHER	Lightning strikes to plant.	Could cause structural damage, leading to release and ignition of gas.		Extremes of solar radiation, flooding, or tidal waves are assumed unlikely because of the plant's location.
			b	EXTREME WEATHER	Wind damage.	High winds may cause collapse of especially tall structures.		
			c	EXTREME WEATHER	Extreme cold.	Freezing of entrapped water and other fluids, leading to fracture of pipes etc. on melting and subsequent release of flammables.		
			d	EXTREME WEATHER	Extreme cold.	Possible brittle fracture of metals, leading to release of flammables.		
			e	EARTHQUAKE	Structural damage.	Loss of plant integrity, leading to release of flammables.	Plant location makes seismic events extremely unlikely.	

FUNCTION			HAZARD IDENTIFICATION					
Ref	**T**	**Description**	**k**	**Keyword**	**Main variance**	**Consequences**	**Mitigation**	**Notes**
6.4	M	Protect against unauthorised access to plant.	a	NOT	Unauthorised persons gain access to plant.	Persons pose a risk to the plant through accidental or deliberate interference and are themselves at risk Well-intentioned intruders, eg press and families of staff, may interfere with emergency operations. Plant represents a dangerous reaction with a hazardous substance and sabotage would be simple and catastrophic. Catalyst is valuable but impossible to steal while operating! However, theft of catalyst is possible during (un)loading operations or when catalyst is stored at site.		
			b	EMERGENCY	as above			
			c	SABOTAGE	as above			
			d	THEFT	as above			
7.0	I	Inlet CO/CO_2 content $\leq 10\%$	a	NOT	CO/CO_2 content > 10%	Runaway reaction in R-101, leading to over-temperature, failure of R-101 and release of flammable gas.	CO/CO_2 content is monitored and alarmed by QA. R-101 is protected by a trip system.	Consider that QA should be integrated with the trip system.

FUNCTION			HAZARD IDENTIFICATION					
Ref	**T**	**Description**	**k**	**Keyword**	**Main variance**	**Consequences**	**Mitigation**	**Notes**
8.0	I	Outlet CO/CO_2 content ≤ 10ppm	a	NOT	CO/CO_2 content ≥10 ppm	Serious effects possible ito downstream process.	None.	Recommend trip system based on outlet conc. Which is worse: interrupt gas flow or supply off-spec gas? Process engineering to advise.
9.0	I	Inlet pressure 20 bar						Process engineering to advise.
10.0	I	Outlet pressure 40 bar						Process engineering to advise.
11.0	I	Inlet temperature tbd						Process engineering to advise.
12.0	I	Outlet temperature tbd						Process engineering to advise.

Bibliographic Data Sheet **Risø-R-712(EN)**

Title and author(s)

Hazard Identification Based on Plant Functional Modelling

Birgitte Rasmussen, Cris Whetton

ISBN	ISSN
87-550-1933-1	0106-2840

Dept. or group	Date
Systems Analysis Department	October 1993

Groups own reg. number(s)	Project/contract no.(s)
RAG-2714-00	STEP-CT90-0085

Pages	Tables	Illustrations	References
71	4	10	7

Abstract (Max. 2000 characters)

A major objective of the present work is to provide means for representing a process plant as a socio-technical system, so as to allow hazard identification at a high level. The method includes technical, human and organisational aspects and is intended to be used for plant level hazard identification so as to identify critical areas and the need for further analysis using existing methods. The first part of the method is the preparation of a plant functional model where a set of plant functions link together hardware, software, operations, work organisation and other safety related aspects of the plant. The basic principle of the functional modelling is that any aspect of the plant can be represented by an object (in the sense that this term is used in computer science) based upon an Intent (or goal); associated with each Intent are Methods, by which the Intent is realized, and Constraints, which limit the Intent. The Methods and Constraints can themselves be treated as objects and decomposed into lower-level Intents (hence the procedure is known as functional decomposition) so giving rise to a hierarchical, object-oriented structure. The plant level hazard identification is carried out on the plant functional model using the Concept Hazard Analysis method. In this, the users will be supported by checklists and keywords and the analysis is structured by pre-defined worksheets. The preparation of the plant functional model and the performance of the hazard identification can be carried out manually or with computer support.

Descriptors INIS/EDB
CHEMICAL PLANTS; FUNCTIONAL MODELS; HAZARDS; SAFETY ANALYSIS; SYSTEMS ANALYSIS

Available on request from Risø Library,Risø National Laboratory,(Risø Bibliotek,Forskningscenter Risø),
P.O. Box 49,
DK-4000 Roskilde, Denmark.
Telephone +45 46 77 46 77, ext. 4004/4005
Telex 43 116. Telefax +45 42 36 06 09.

RISØ

OBJECTIVE

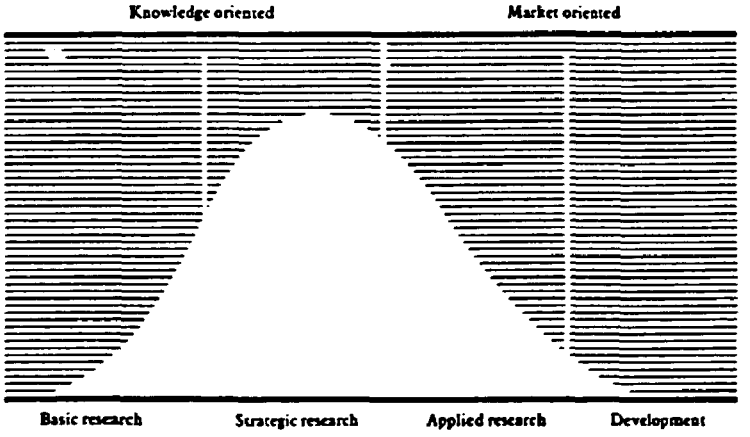
The objective of Risø National Laboratory is to further technological development in three main areas: energy, environment and materials.

USERS

Risø's scientific results are widely applied in industry, agriculture and public services. Risø contributes its share of new knowledge to the global research community.

RESEARCH PROFILE

Risø emphasises long-term and strategic research providing a solid scientific foundation for the technological development of society.



PRIORITY AREAS

- **Combustion and gasification**
- **Wind energy**
- **Energy materials**
- **Energy and environmental planning**
- **Assessment of environmental loads**
- **Reduction of environmental loads**
- **Safety and reliability of technical systems**
- **Nuclear safety**
- **Atomic structure and properties of materials**
- **Advanced materials and materials technologies**
- **Optics and fluid dynamics**

Risø-R-712(EN)
ISBN 87-550-1933-1
ISSN 0106-2840

Available on request from:
Risø Library
Risø National Laboratory
P.O. Box 49, DK-4000 Roskilde, Denmark
Phone +45 46 77 46 77, ext. 4004/4005
Telex 43116, Telefax 46 75 56 27