PLANOP

A method for performing loss of containment analyses

April 2005

Federal Public Service Employment, Labour and Social Dialogue
Industrial Safety Administration
Department for the Supervision of Chemical risks

This document and the associated software may be obtained from:

FPS Employment, Labour and Social Dialogue
Department for the Supervision of Chemical risks
Ernest Blerotstraat 1
1070 BRUSSELS
Tel: 02 233 45 12 - Fax: 02 233 45 69
e-mail: CRC@meta.fgov.be

This brochure is also available on the website:
www.meta.fgov.be (look for "Prevention of major accidents").

Cette brochure peut être également obtenue en français.
Deze brochure is ook verkrijgbaar in het Nederlands.

Introduction

PLANOP, which is an acronym of 'Progressive Loss of Containment Analysis – Optimizing Prevention', is a software-assisted method for performing 'loss of containment' analyses for process installations.

The objective of a loss of containment analysis is to identify the causes and consequences of an undesired release of substances or energy. However, PLANOP is not limited to simply performing loss of containment analyses. It also assists the user in specifying measures (hence 'Optimizing Prevention'), and it includes performing a 'hazard analysis', which means investigating which substances and reactions are present in the installation and their hazardous properties. Performing a hazard analysis is an essential prerequisite for performing a loss of containment analysis. Finally PLANOP also supports the risk evaluation of loss of containment scenarios by means of the LOPA-method (Layers of Protection Analysis).

A PLANOP analysis is performed using the PLANOP software, which can be obtained via (verkregen) the website www.PLANOP.be.

This manual describes the principles of the method and the features of the software. How to use the software is not described in detail in this manual, but can be found in the help-function of the software.

In addition to this manual, worked examples will be available on the PLANOP-website. It is recommended to explore the PLANOP-software using these examples while reading this manual.

Table of Contents

1

The benefits of PLANOP

This chapter gives an overview of the features of PLANOP, however without going into detail on how these are realised. This will be the subject of the next chapters.

PLANOP essentially has two main benefits. Firstly PLANOP offers a integral methodology for risk analysis, in the sense that PLANOP incorporates all the elements of a risk analysis and combines them into a coherent process.

A second important asset is that this methodology is implemented by means of a database application. Executing a PLANOP analysis is equivalent to storing safety-related information about the installation under consideration in a database. The result of a PLANOP analysis will be a structured overview of hazards, risks and measures. The use of a database not only permits to easily modify this information, but is also a powerful tool in managing and conserving the process safety knowledge available within the organisation.

1.1 A complete risk analysis methodology

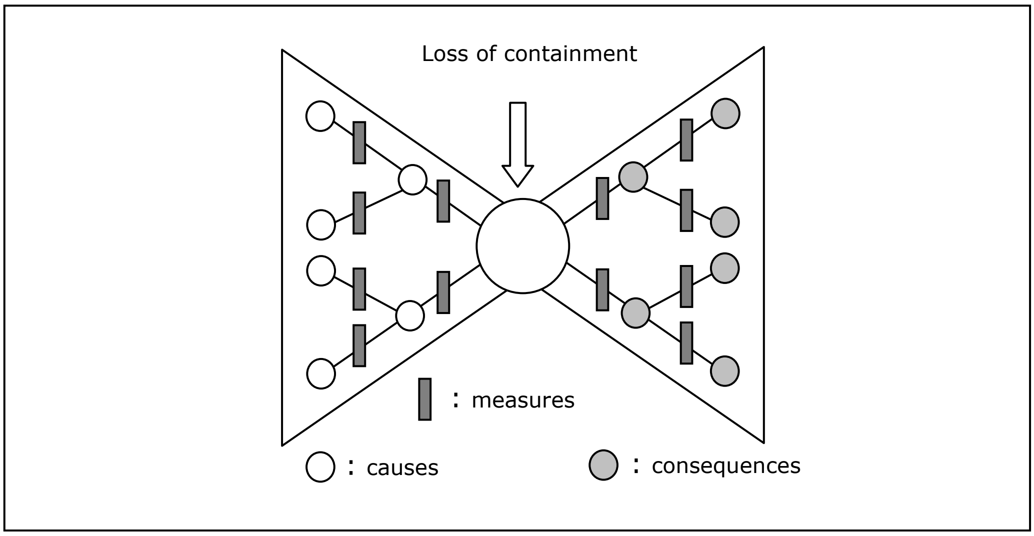
A risk analysis consists of the following elements:

- identifying hazards, this means identifying possible sources of damage
- identifying risks, this means identifying possible accident scenarios in which these hazards actually cause damage
- evaluating the risk, this means judging whether sufficient measures have been taken to prevent accidents and to limit possible damage.

1.1.1 Identifying risks of loss of containment

PLANOP was created specifically to investigate accident scenarios in which dangerous substances or dangerous amounts of energy are released from an installation that was intended to keep substances and energy contained. The analysis of these types of accident scenarios is called loss of containment analysis or bowtie analysis. The word “bowtie” refers to the shape in which these accident scenarios can be represented. This is illustrated in figure 1.1. The undesired release is the central node. The left half of the bowtie depicts the diversity of causes that can lead to the release. The right half represents the possible events resulting from the release. In this bowtie representation, measures can be seen as barriers or layers of protection that interrupt the chain of subsequent causes and consequences.

Figure 1.1: The release scenario in bowtie representation



A loss of containment analysis is not performed on a process installation as a whole but for individual parts of the installation. So before starting the actual analysis the installation needs to be divided into parts or, in PLANOP terminology, subsystems.

The PLANOP-software allows to define subsystems for each installation and to elaborate the release scenarios for each subsystem in a graphical manner, where the chain of causes and consequences – like in the bowtie concept – is represented graphically and measures can be placed directly between cause and consequence. For practical reasons, in PLANOP the bowtie is cut into smaller pieces and the elaboration of the tree structures of causes and consequences is done downwards instead of to the left or to the right. The graphics in PLANOP therefore don't actually look like a bowtie, but they contain the same type of information as a bow tie representation of a loss of containment scenario.

PLANOP not only allows elaborating release scenarios graphically, but also helps to identify the causes and consequences. PLANOP contains typical cause trees and typical consequence trees that can be used as a starting point to elaborate the trees for the subsystem to be analysed. These typical cause and consequence trees also contain typical measures. In that way the PLANOP user is also guided in choosing appropriate measures.

1.1.2 <u>Identifying the hazards of substances and reactions</u>

As explained, the second part of a risk analysis, the identification of accident scenarios, is in PLANOP restricted to the identification of a specific type of accident scenarios: loss of containment of substances or energy in a process installation. As a result, the hazard analysis in PLANOP will also have a specific meaning. The damage sources relevant for loss of containment scenarios are the dangerous substances and the chemical reactions that are present or could be present in the subsystems of the process installation. The properties of the substances and the conditions of pressure and temperature at their release determine the damage potential. A chemical reactions can produce large amounts of energy that could lead to substantial damage when the subsystem containing it fails.

Evidently substances and reactions not only determine the consequences of an undesired release, but will also be of importance in causing the release.

The hazard analysis supporting the loss of containment analysis therefore consists of the following:

- identifying all substances and reactions present or possibly present in the installation
- locating these substances and reactions in the installation: where can they be present in normal and abnormal conditions
- investigating the relevant properties of the substances and reactions.

PLANOP supports all these activities. Furthermore, PLANOP allows connecting the hazard analysis and the loss of containment analysis. Typical cause and consequence trees can be linked to substances and reactions. When these substances or reactions are present in a subsystem, these trees will be offered to the user as a starting point for the specific analysis of the subsystem.

1.1.3 Evaluating risks with LOPA

A third and final element of the risk analysis is the risk evaluation. In this stage of the analysis we judge whether sufficient measures were taken to prevent loss of containment. To this end PLANOP uses the LOPA-method. LOPA is an acronym for 'Layer of Protection Analysis' and is a simplified quantitative risk evaluation technique. For the application of this method the chain of events in the accident scenario and the measures interrupting this chain must be identified. Therefore LOPA is an obvious technique to be combined with a bowtie analysis. In itself LOPA has a number of important advantages.

A first advantage of LOPA is that due to the quantitative character of the method, the risk evaluation is performed following strict rules. As a consequence the risk evaluation becomes objective and transparent. LOPA also leads the user to critically analysing the quality of the proposed measures. Finally, LOPA allows determining directly the desired reliability of safety systems. The latter is an important part of the application of the international standards IEC 61508 and 61511 on functional safety. It is expected that these will become the international reference standards as to specifying, designing and maintaining instrumented safety systems.

1.2 Risk analysis using a database application

An essential characteristic of the PLANOP method is that performing a PLANOP analysis coincides with creating a structure of relevant safety information. The PLANOP method is therefore inseparably connected to the PLANOP software that allows creating and maintaining this data structure. Several important advantages are the result of this approach.

1.2.1 Creating and maintaining process safety documentation

A first benefit involves the use of the results of the PLANOP analysis.

The output of a PLANOP analysis is a structured overview of all the information that is relevant to the issue of loss of containment:

- the causes and consequences of losses of containment
- the preventative and mitigating measures, and
- the relevant data on substances and reactions.

This type of overview is an essential input to the safety management system, which is tasked with the maintenance, regular review (re-examination) and continuous improvement of these measures.

When changes are made to an installation, a structured overview of the causes and consequences of losses of containment forms a good starting point for investigating the impact of the changes on the question of loss of containment. After all, you cannot work efficiently if you have to repeat each risk analysis from the very beginning or if you do not have access to readable, structured results from previous risk analyses.

Furthermore, it is important for critical safety-related design choices (which are usually passive measures) to be well documented and well reasoned, in order to prevent them from being changed in new projects without due consideration.

PLANOP allows various types of measure lists to be generated. These lists can be used for a variety of purposes, such as:

- checking the completeness of inspection and maintenance programmes
- checking whether operational procedures and instructions properly describe the critical safety-related interventions that have been defined as measures and explain why these activities are critical for safety.

It is thus important for the information in the PLANOP files to be kept current and for this information to be updated when new risks are identified or new measures are specified.

1.2.2 Integrating risk analysis into the design process

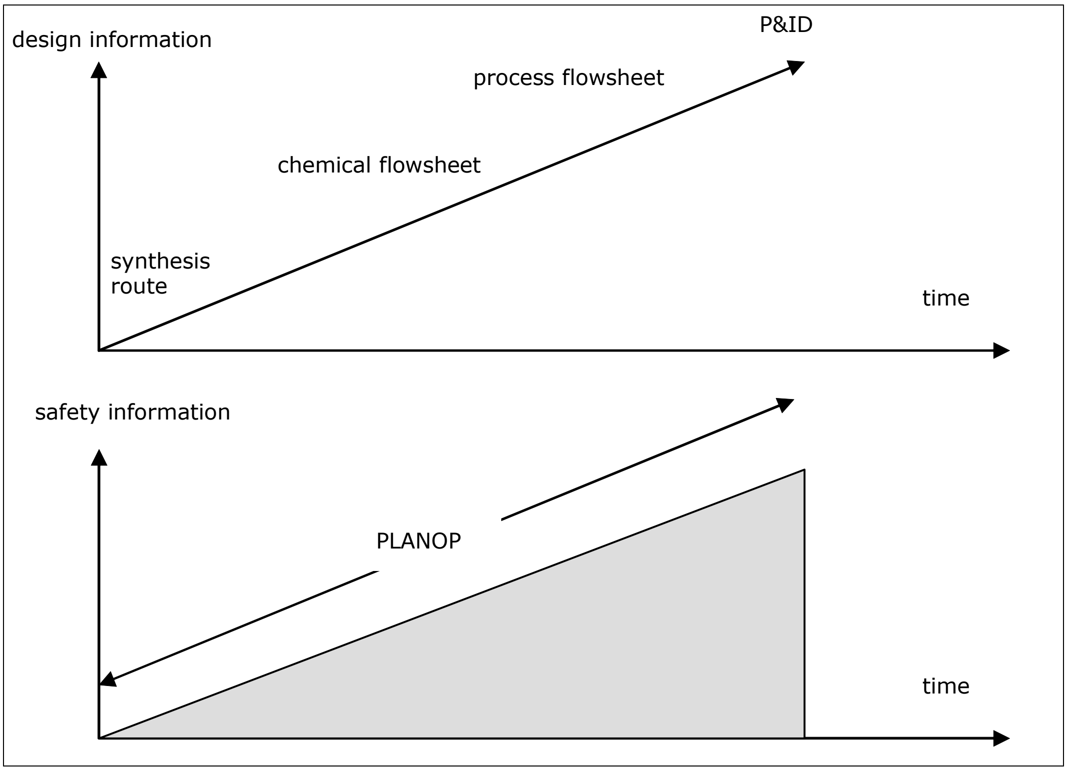
A second important benefit of the database approach is the possibility of integrating the PLANOP analysis in the design process of the installation.

The PLANOP data structure is constructed such that the level of detail of the data increases as the structure is further elaborated. The PLANOP data structure can thus be built up in parallel with the various stages of the design process, using the information about the installation being designed that becomes available at each stage. This is shown graphically in figure 1.2.

Figure 1.2 depicts the design process as a process in which the amount of information about the installation being designed (or modified) increases continuously as a function of time. This evolution is characterised by the generation of various documents and plans. The documents in figure 1.2 depicting the evolution of the design are purely illustrative. Naturally, they may vary from company to company. The conceptual design stage concludes with the generation of the piping and instrumentation diagrams, which, in a manner of speaking, form the synthesis of all previous design data. As more design data become available, the PLANOP data structure can be further expanded. Naturally, there will also be an input from the PLANOP analysis into the design (more specifically, this consists of the measures resulting from the PLANOP analysis).

This concept is what is expressed by the word 'progressive' in the PLANOP acronym. The intention of the PLANOP program is to make carrying out a risk analysis a forward-acting, dynamic procedure, so the installation will truly be designed on the basis of a risk analysis, with the risk analysis being more than just a deviation analysis of the final result of the design process.

Figure 1.2: Integrating PLANOP into the design process



2

An introduction to the PLANOP-software

The details on how to use the PLANOP software can be found in the help-function of the software and are therefore not described in this manual.

Nevertheless it is necessary to have a basic insight in the way the information is stored in the different PLANOP files.

Furthermore, this chapter describes a number of general functionalities of the software that are used in several parts of the program: copying of information and the use of the 'suggestion lists'.

2.1 The data files of PLANOP

PLANOP uses three kinds of data files:

- Analysis files contain information regarding the installations
- Substances files contain information regarding substances and reactions
- Expertise files contain the expert knowledge that supports the analysis.

2.1.1 Analysis files, Substance files and their connection

The Analysis files contain the following information:

- the structure of subsystems in which the installation is subdivided
- the substances and reactions present in these subsystems
- the causes and consequences of losses of containment
- the measures preventing releases and limiting the consequences.

Information about the properties of substances and reactions is not specific to a certain installation and is therefore stored in a separate file: the Substances file. Substances and reactions are defined and their properties documented in this Substances file.

An Analysis file is always linked to a Substances file. The substances and reactions that are linked to a subsystem are a selection of the items in this Substances file.

The Substances file that accompanies the Analysis file can be altered at any time, which means that a different Substances file can be linked to the Analysis file. Obviously, it is necessary to be very careful about changing the link between a Substances file and an Analysis file. If the Analysis file contains references to specific substances and reactions (i.e., ones that are present in the installations being investigated) and a different Substances file is selected, the information in the Analysis file will naturally become meaningless. Consequently, the link between an Analysis file and a Substances file should not be changed except in one of the following situations:

- A new Analysis file has been created and an incorrect Substances file has been selected (for instance, an existing Substances file has been linked to the Analysis file but you would rather work with a new Substances file).
- A Substances file is temporarily being shared by two Analysis files, but you want to continue the analysis using two separate Substances files.
  In this case, you can make a copy of the current Substances file and continue working with the copy.

2.1.2 Spreading the installations over different Analysis files

A user can create different Analysis files and different Substances files and link a Substances file to an Analysis file. Multiple Analysis files can use the same Substances file.

An important choice the user has to make is: what installations shall I analyse in the same Analysis file and for what installations shall I use separate Analysis files?

If the installations contain entirely different substances and reactions, it can be appropriate to use separate Analysis files and to use a different Substances file for each Analysis file.

If more than one person will create and maintain the analyses of the installations, it can also be convenient to use separate files.

However, if an Analysis file contains several installations, the information can be copied from one installation to another, which can be convenient for installations that are alike.

2.1.3 Expertise files and suggestion lists

The third type of file is the Expertise file. This file contains the 'suggestion lists' that are provided in PLANOP to support the analysis.

Chapter 1 mentioned that PLANOP will support the user by offering typical cause and consequence trees. These typical trees have exactly the same form as the tree structures that are being created during the analysis. As such, this typical information can be copied to the Analysis file. The user will of course have to adjust this information from the suggestion list to the specific context of the subsystem under consideration. For example a typical cause tree is provided for a runaway reaction scenario. This tree can be copied to a reactor that is defined as a subsystem in the Analysis file. Subsequently the typical cause tree will have to be adapted to fit the reactor that is being analysed.

The typical cause trees are part of the 'Event Source Suggestion list' and the typical consequence trees of the 'Release Event Suggestion list'. The notions 'event source' and 'release event' will be explained in chapter 4.

Two other suggestion lists used in PLANOP are:

- the 'Suggestion list Items of consideration for Measures', that helps define factors contributing to the reliability and effectiveness of measures;
- the 'Suggestion list Items of consideration for Installations', to analyse general safety aspects on the installation level (e.g. selection of substances, plant location issues, etc.)

In order to prevent that information is copied and not adapted afterwards all information copied from a suggestion list will be marked with the text '[SL]'.

A final suggestion list is the 'Suggestion list Undesired Substances' that can help identifying substances that can be present in the subsystem in abnormal conditions.

The PLANOP-software is delivered with a 'default' Expertise file. Users can modify the suggestion lists according to their own insights. This way, the expertise on process safety in the organisation can be saved in a form that is practically usable. It is recommended that modifications to the suggestion lists would only be made by persons strongly acquainted to the PLANOP methodology.

It is possible to create a new empty Expertise file or to link an Analysis file to a different (existing) Expertise file. It is also possible to make a copy of an Expertise file and use this copy to make modifications (e.g. experiment with it) and keep the original one intact. However there is not much benefit in using several different Expertise files within an organisation. The most common situation is that all analysts are using the same Expertise file.

2.2 Copying information

The PLANOP-software allows opening several windows simultaneously. Information can be copied from one window to another window (containing information of the same nature) by using the 'drag and drop' technique (i.e. dragging the information to the new location).

Within one window information can also be moved using 'drag and drop'. If the 'CTRL-button' is pressed during the 'drag and drop', information will be copied instead of moved. Information that is copied will be marked with the extension '[copy]'. When dragging a measure within a cause tree, pressing the 'SHIFT-button' will result in inserting the same measure a second time (see chapter 4).

2.3 Saving information

PLANOP is a Microsoft Access application. Microsoft Access has the specific behaviour that information is saved whenever the relevant window is closed. Therefore, PLANOP has no 'Save' function.

The PLANOP-software allows the user to make backups of the Analysis and Substances files. Frequent use of this possibility is recommended. This allows the user to fall back on previous versions of these files if information would accidentally get changed or deleted.

During the working process, the data files can become very large. PLANOP offers the possibility to compact these files (reduce the size).

Use of special software such as WINZIP will furthermore reduce file size drastically.

2.4 Defining action points

When a risk analysis is being performed, it is commonly necessary to identify actions to be taken. The PLANOP program allows action items to be formulated at various points in the analysis by using the Action button.

The following information can be documented for an action point:

- a description (only the first line of this field will be shown in the Action Items Summary list)
- the name of the person responsible for carrying out the action
- a due date
- a completion date (i.e. the date the action was completed)
- a status (e.g. in progress, completed, no longer applicable, etc.).

The PLANOP-software will add to each action point in what part of the analysis the action point was defined, so the user doesn’t need to document this himself.

It is possible to view a list of all the action points in the Analysis file. The listed action items can be sorted by the responsible person, the due date or the completion date, by clicking on the appropriate button at the top of the list. It is also possible to add items to this list immediately.

2.5 Printing information

The printer button that can be found in several places in the software, allows to print the information of the active window.

Often it is possible to choose up to what detail the information should be printed. For example it is possible to print all the information in the Analysis file from the window with the installation overview.

Every printout has a header containing a logo and company name. It is possible to enter your own company logo and name in the PLANOP-software so they will be present on the printouts.

3

Subdividing the installation

The objective of a loss of containment analysis is to identify the causes and consequences of undesired releases. It is not practical to perform such an analysis on an installation as a whole. A thorough, systematic and readily understandable manner of working presupposes subdividing the installation into installation subsystems, with a separate loss of containment analysis being performed for each individual subsystem. As the subdivision of the installation into subsystems becomes finer, the analysis becomes more thorough and more detailed, but the scope of the analysis and the amount of time required increase accordingly.

If PLANOP is used in the development of a new installation, it will be necessary to make the subdivision of the installation increasingly finer and more specific, in a step-by-step manner, as the installation becomes better defined on the drawing board.

3.1 Choosing installations, sections and subsystems

PLANOP uses three types of objects for subdividing a process installation: 'installations', 'sections' and 'subsystems'.

Installations form the highest level of the subdivision. A logical choice for an installation would be a (more or less) autonomous production unit.

A section is a collection of subsystems of an installation. Subsystems are not defined directly as elements of an installation. In order to generate a structured overview of the subsystems, an intermediate level is formed using sections. Sections can form a hierarchical structure having any number of levels. One or more sections must always be defined under each installation. Additional sections and subsystems can be defined under each section.

The structure of installations, sections and subsystems can be compared to the file structure of a computer, with an installation corresponding to a disk, a section to a folder and a subsystem to a file. Any desired folder tree can be created, but the object types at the highest and lowest levels are always the same.

Installations, sections and subsystems are represented in a tree structure. Several operations are possible in order to modify the current structure, like:

- changing the order of installations, sections or subsystems;
- repositioning sections and subsystems.

Subsystems can also be copied, so the analysis of an existing subsystem can be conveniently used as a starting point for the analysis of a similar subsystem.

3.2 Information for installations, sections and subsystems

The information concerning installations, sections and subsystems can be divided into background information and information inherent (proper) to the actual to the PLANOP analysis.

3.2.1 Background information

PLANOP offers the possibility to enter the following background information concerning installations, sections or subsystems in the Analysis file:

- a description of each installation, section and subsystem
- an overview of the risk analyses previously performed on each installation
- an illustration of a subsystem
- an overview of the components of each subsystem
- an overview of the weak points and openings of each subsystem.

Entering this background information is as such not part of the PLANOP analysis. However, the presence of this information can be a more or less important support during the analysis. The user can judge for himself whether or not to use these documenting possibilities.

A Describing installations, sections and subsystems

The description can be entered in a text field and a hyperlink can be included to a file that describes the installation. A hyperlink is a reference to another file. The hyperlink specifies the name of this file and the location where it can be found.

PLANOP-analysts and third persons (within or outside the organisation) can certainly benefit from the presence of these descriptions of installations, sections and subsystems.

B The list of risk analyses for an installation

For each installation a list can be maintained of risk analyses performed in the past. For each analysis the following data fields are available: the time when performed, the technique used (e.g. PLANOP, HAZOP, FMEA, What If, etc.) and the occasion (e.g. a certain design stage, an incident, a modification, etc.) can be documented. In addition a hyperlink can be defined for each analysis, e.g. to the worksheets or the report of the analysis.

When maintaining a complete and up-to-date overview of risks and measures in PLANOP, it will be necessary to add new information resulting from other risk analyses to the PLANOP files. In that perspective it can be convenient to keep a list of all the analyses that have contributed to the PLANOP information.

C Illustration of the subsystem

It is possible to include an illustration to each subsystem description. The display quality of the illustration depends on the file type and the dimensions of the illustration.
It is not recommended to enter ‘piping and instrumentation diagrams’: these drawings contain to much detailed information and they are subject to frequent modifications. ‘Process flow diagrams’ showing the position of the subsystem in the section or the installation are better suited.

D Overview of the components of a subsystem

A component is an apparatus, device, pipe or other part of an installation that contains or can contain hazardous substances. As a rule (at least in good design documentation), each component is individually and unambiguously identified by a number or code (such as a tag code). When subdividing an installation, you can define subsystems to be the same as individual components or the same as groups of several components.

Regardless of which option you choose, it is very important to unambiguously define and demarcate each subsystem. PLANOP allows the components making up each subsystem to be listed.

It is also possible to display a summary of all components contained in the Analysis file. A summary of components can be used for a variety of purposes, such as:

- determining the subsystem to which a particular component belongs;
- determining whether a particular component is included in the PLANOP analysis;
- determining which components may be missing from the PLANOP analysis.

E The list of weak points and openings in a subsystem

Weak points are for instance:

- sight glasses
- level glasses
- joints
- small bore piping
- manometers in direct connection with the internals of the envelope
- expansion joints
- flexible connections.

Listing these weak points is useful because they need extra attention during the analysis of the causes of loss of containment.

3.2.2 Information inherent to the PLANOP analysis

The following information of installations and subsystems is part of the actual PLANOP analysis:

- items of consideration for installations
- substances (possibly) present in each subsystem
- (possible) chemical reactions possible in each subsystem
- the causes of losses of containment and the measures preventing releases them for each subsystem
- the consequences of losses of containment and the measures mitigating them for each subsystem.

Items of consideration for installations can be used to analyse and document safety issues that are relevant for the whole of the installation. This will be explained later in this chapter.

Making an inventory of substances and reactions in subsystems is part of the hazard analysis and will be explained in chapter 7.

Identifying causes and consequences and specifying appropriate measures is part of the loss of containment analysis described in chapter 4.

Take notice that no part of the PLANOP analysis is performed on the section level. The only function of sections is to divide the installation into a logical structure.

3.3 Items of consideration for installations

A PLANOP analysis focuses on loss of containment analyses for the subsystems of an installation. However, certain safety aspects cannot be treated at the level of the individual subsystems of an installation, but are addressed more appropriately at the level of the entire process installation. Some examples are:

- the choice of the production process
- the choice of the substances used
- the limitation of the quantities
- the supply of raw materials
- the possible impact of the (internal or external) surroundings on the installation
- the possible impact of the installation on its (internal or external) surroundings
- the effects of certain natural phenomena
- hazardous area classification
- etc.

In PLANOP, these more general safety aspects are treated systematically using ‘items of consideration for installations’. The information for such an item of consideration is limited to a name and a description. The name shortly indicates the problem, the description can be used to document specific aspects of the problem for the installation under consideration.

PLANOP has a suggestion list containing typical items of consideration for installations. These items can be copied to the Analysis file. The intention is that the user should answer the questions given in the description field or delete any questions that are not relevant.

4

The loss of containment analysis

A loss of containment analysis consists of identifying the causes and consequences of undesired releases of substances or energy. In PLANOP, the loss of containment analysis is performed individually for each subsystem.

In chapter 1 the 'bowtie' concept was mentioned. As there can be a wide range of causes and consequences of loss of containment from a subsystem, the bowtie in PLANOP is broken up in several elements.

In order to tackle the task of identifying causes and consequences in a structured manner, PLANOP uses two concepts that are fundamental to the method: 'event sources' and 'release events'.

The 'event source' concept makes it possible to systematically identify the *causes* of an undesired release, while the 'release event' concept does the same for the *consequences* of an undesired release.

Event sources are phenomena, conditions or properties of an installation that *could* lead to an accidental release of substances or energy. For every event source the underlying causes leading to the event source should be identified. These causes are structured in a tree structure together with the measures affecting the cause and preventing a release.

Release events are critical events that can happen after a loss of containment. They are the 'stages' in the course of an accident resulting from an undesired release. Release events are also represented in a tree structure together with the measures that mitigate the consequences of the release.

The loss of containment analysis in PLANOP consists of the following:

- identifying the event sources for each subsystem
- elaborating a cause tree for each event source
- elaborating a release event tree for each subsystem.

These steps doesn't need to be strictly performed in this order, but can run more or less parallel.

4.1 The 'event source' concept

Event sources are phenomena that *could* lead to an accidental release of substances or energy. The presence of event sources means that there is a possibility or chance that a loss of containment will occur. These phenomena are inherent to the process and challenge the installation that should keep these phenomena under control or prevent their occurrence.

4.1.1 Types and subtypes of event sources

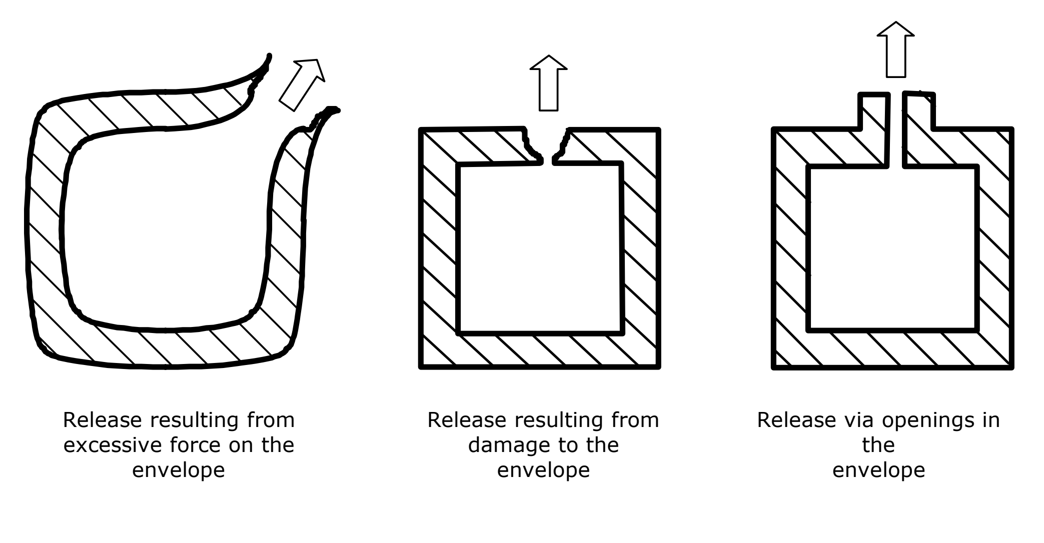
PLANOP defines three types of event sources:

1. phenomena producing forces on the envelope
2. phenomena threatening the construction materials of the envelope
3. phenomena leading to a release through an opening in the envelope.

The envelope is the physical barrier that 'contains' the substances and energy.

Each type of event source corresponds to one of the three ways in which substances or energy can be released from an envelope. These three mechanisms are illustrated in Figure 4.1.

Figure 4.1: The three mechanisms for the undesired release of substances or energy



Release resulting from excessive force on the envelope

Release resulting from damage to the envelope

Release via openings in the envelope

For each type of event source, two or more subtypes are defined. A summary of the types of event sources and their associated subtypes is given in Table 4.1

Table 4.1: Types and subtypes for event sources

Event source types	Event source subtypes
1. Phenomena leading to forces on the envelope	1.1 Phenomena leading to high pressure 1.2 Phenomena leading to low pressure 1.3 Phenomena leading to forces other than pressure
2. Phenomena threatening the construction materials of the envelope	2.1 Phenomena leading to corrosion or chemical attack 2.2 Phenomena leading to high temperatures (threatening the envelope) 2.3 Phenomena leading to erosion and wear 2.4 Phenomena leading to low temperatures 2.5 Phenomena leading to cyclic stresses (fatigue risks)
3. Openings in the envelope	3.1 Manual operations opening the installation 3.2 Process upsets leading to a release through an opening

An extensive suggestion list of ‘typical’ event sources is one of the central resources of the PLANOP method. This suggestion list can be consulted for examples of event sources.

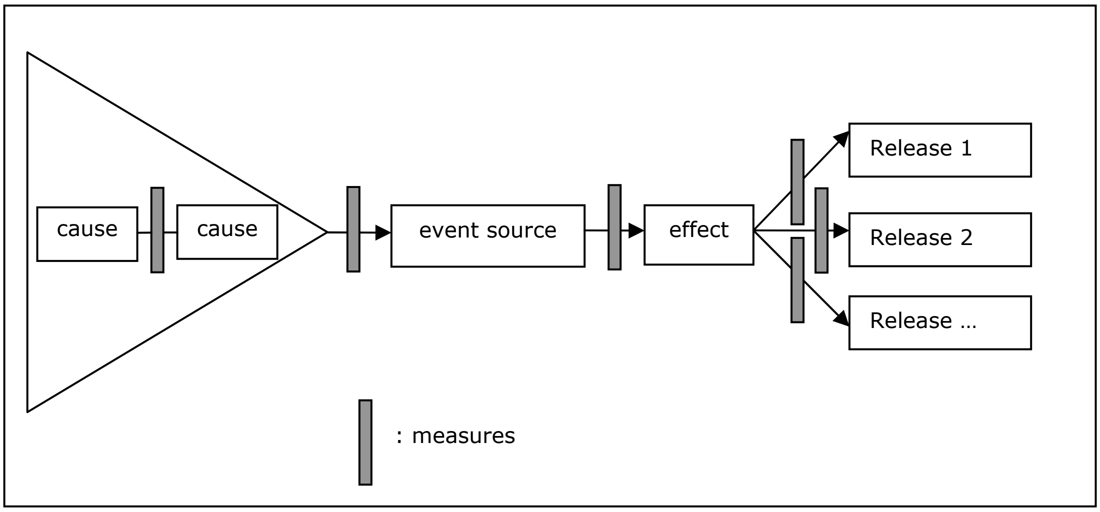
4.1.2 <u>Cause trees for event sources</u>

Event sources are the starting point of the search for causes of loss of containment. Event sources are for PLANOP what deviations of process parameters are for HAZOP and failure modes for FMEA.

Identifying the event sources is only the first step in identifying the causes for loss of containment. The next step is creating cause trees for these event sources.

Figure 4.2 shows the place of event sources in the cause trees.

Figure 4.2: The cause tree in PLANOP



The triangle to the left of the event source represents the tree structure of causes that can lead to the event source.

The event source itself can lead to a so-called 'effect'. For each event source there can be only one effect. This can be for instance: high pressure, low pressure, corrosion, etc.

An effect can lead to one or more releases. Consider for instance a vessel that can be pressurized due to the heat input of a heat exchanger. 'Heat input of heat exchanger' would be the event source, 'high pressure' the effect. This high pressure can lead to a rupture of the vessel (first possible release). If a safety valve is present, the event source could also lead to a release through the safety valve (second possible release).

This example illustrates that is possible to link more than one release to an event source. It is also possible (and probable) that several event sources lead to the same release. Usually more than one phenomenon can for example lead to a rupture of a vessel.

The grey blocks in figure 4.2 represent measures. As shown in the figure, measures can be placed in between two consecutive elements of the cause tree. Measures can be considered as barriers that prevent or cut the chain of events described by the elements of the cause tree.

The cause tree elaborated for each event source can be considered as a part of the left side of the bowtie representing all causes of loss of containment. In PLANOP however, the cause tree is elaborated not to left (as in the bowtie representation) but downwards giving each additional level in the tree structure an indent to the right. To clearly show which causes are on the same level, they are connected with vertical dotted lines. Every cause tree starts with the effect and the event source. Figure 4.3 illustrates this principle.

Figure 4.3: Left to right representation of the cause tree

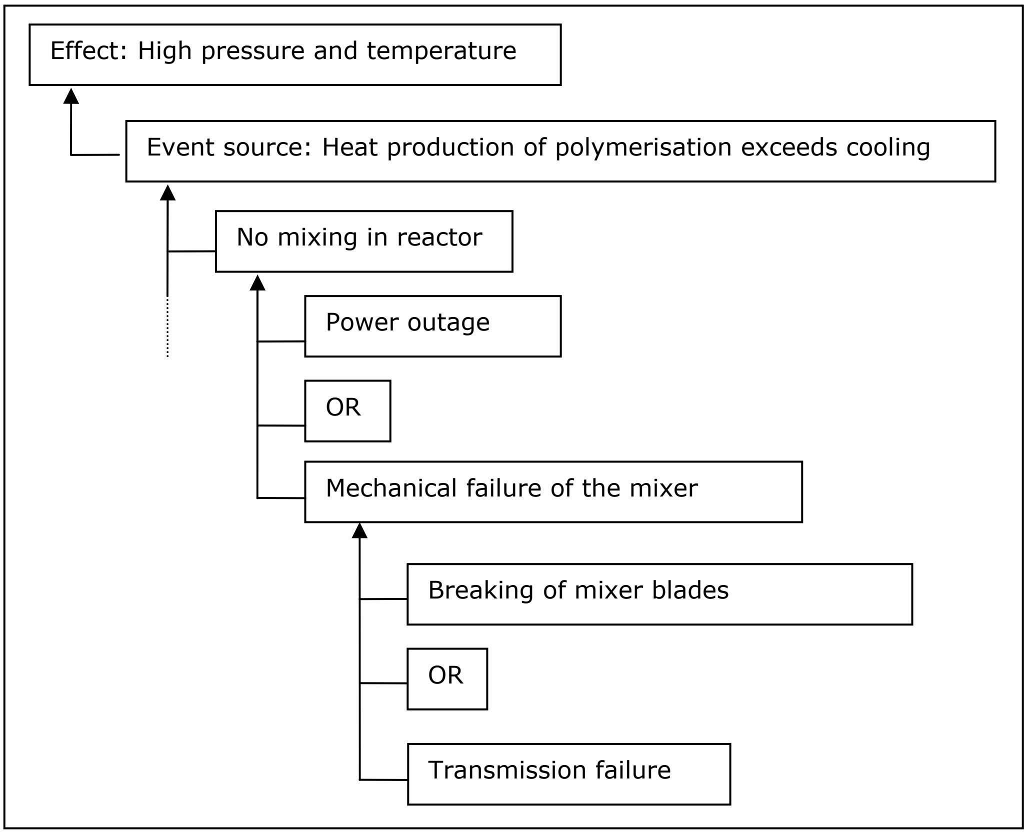
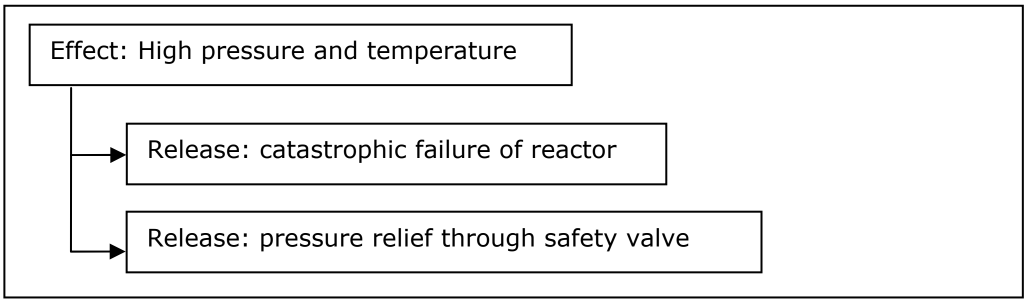

Effect: High pressure and temperature
Event source: Heat production of polymerisation exceeds cooling
No mixing in reactor
Power outage
OR
Mechanical failure of the mixer
Breaking of mixer blades
OR
Transmission failure

Figure 4.2 also shows the links from the effect to the different possible releases. These links are represented in PLANOP separately (on a different screen), again starting from the effect. This is illustrated in figure 4.4.

Figure 4.4: Representation of the links from the effect to the releases

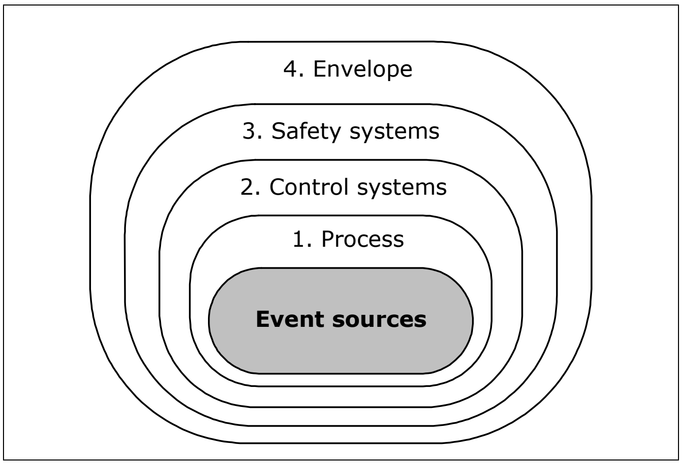

Effect: High pressure and temperature
Release: catastrophic failure of reactor
Release: pressure relief through safety valve

4.1.3 The concept ‘measure’ in PLANOP

PLANOP aims for a very broad interpretation of the concept ‘measure’. Every aspect of the installation or its operation that contributes to the prevention of a release, is to be considered a measure. This broad interpretation of the concept ‘measure’ is important as it comes to risk management. Measures need to be maintained and protected against uncontrolled modification. What is not regarded as a measure, will likely escape the management procedures that are in place with regards to measures.

This interpretation of the concept ‘measure’ can be illustrated using the protection layer model, as shown in figure 4.5.

Figure 4.5: The protection layers surrounding the event sources



In the core we find the event sources; these are hazardous phenomena that result from design choices: substances, chosen reaction routes, process stages, etc.

A first protection layer represents those design choices that are important to the prevention or suppression of event sources. If, for instance, the quantity of a reactant in batch reactor can be limited by feeding it using a vessel whose volume is limited to a safe value, than this vessel (having a 'safe' volume) is a measure to prevent an overproduction of heat.

A next protection layer is provided by the control systems that are active during normal operation of the process.

A third protection layer is formed by the safety systems. Usually these are instrumented systems or pressure relief devices. Normally these measures are only active when the control systems fail.

The ultimate protection layer before release is the envelope of the subsystem. If this envelope can withstand the phenomena that are attacking it, the substances and energy will remain contained. A vessel that can withstand the maximum pressure caused by an event source, is considered in PLANOP as a measure located between the effect (high pressure) and the release (e.g. fracture or rupture).

The broad interpretation of the concept 'measure' also affects the way cause trees are constructed. By considering control systems as measures, the failure of these control systems is not to be considered an initial cause. The initial cause will be the process condition that is being controlled by this control system. This can be illustrated with an example.

Figure 4.6 shows a 'classic' representation of a fault tree. The initial event is the failure of the control system.
Figure 4.7 shows the PLANOP-approach in which the control system is defined as a measure and the initial cause is formulated as the process operation itself.

Figure 4.6: 'Traditional' representation: failure of the control system is the initial event

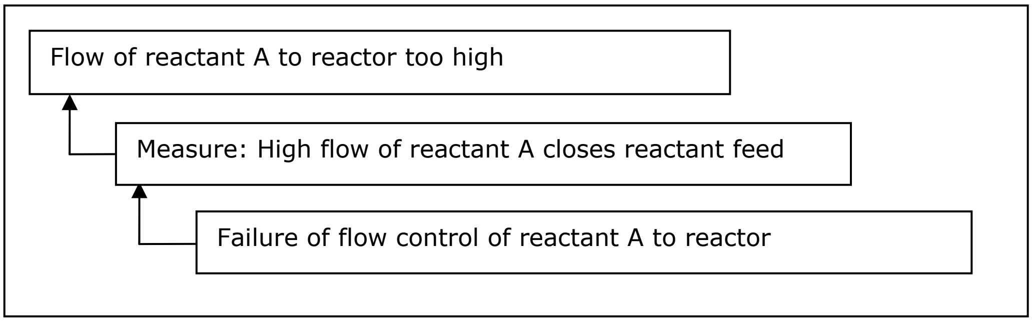
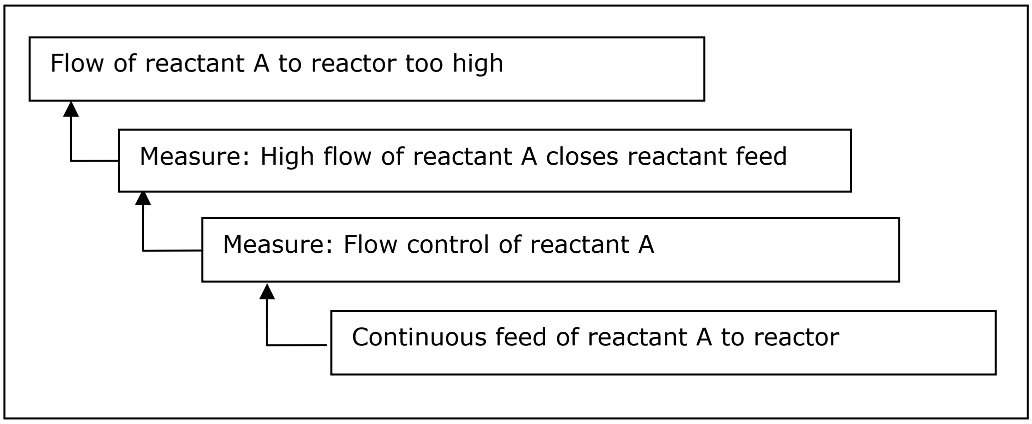

Flow of reactant A to reactor too high
Measure: High flow of reactant A closes reactant feed
Failure of flow control of reactant A to reactor

Figure 4.7: Representation in PLANOP: control system is measure


Flow of reactant A to reactor too high
Measure: High flow of reactant A closes reactant feed
Measure: Flow control of reactant A
Continuous feed of reactant A to reactor

It is important to recognise that with the 'event source' concept, PLANOP takes a completely different approach to the concepts of 'risk' and 'measure' than the approach characteristically taken by traditional risk analysis techniques (such as HAZOP, FMEA, What If and fault tree analysis). In these methods, you search for deviations (from process parameters, for example, in HAZOP) or errors (such as an ineffective measurement in the case of FMEA, or the failure of a process component in the case of a fault tree analysis). In other words, the starting point in these methods is an existing, finalised design, and this final design is screened for design errors.

The 'event source' concept allows PLANOP does not use the installation as a starting point, but the process itself. The process is the challenge and in PLANOP this challenge is described by the event sources. The installation is the 'solution' to the problem and this solution is described by measures in PLANOP. These measures can relate to every aspect of the process installation: the strength of the subsystems (design pressures), the choice of materials, the control system, pressure relief, instrumented safety loops and the entire range of mitigating measures.

4.2 Identifying event sources

A list of relevant event sources must be created for every subsystem. In this list the event sources are classified according to the three event source types and their subtypes.

4.2.1 Copying event sources from the Event Source Suggestion List

It is strongly recommended, certainly for inexperienced analysts, to use the Event Source Suggestion List, since a correct application of PLANOP requires a correct interpretation of the ‘event source’ concept.

Furthermore the Event Source Suggestion List will help elaborating the cause trees. A ‘correct’ cause tree is important for evaluating the risks with LOPA.

The information in the Event Source Suggestion List can be copied to the subsystem where the suggestion list was opened. One or more event sources can be selected in the list and subsequently ‘transferred’ to the subsystem.

In transferring one or more event sources to a subsystem, the software will ask what information should be copied:

- name, description and effect
- name, description, effect and causes
- name, description, effect, causes and measures.

The minimum that is transferred is thus the name of the event source and the effect (the exact interpretation of ‘effect’ will be explained later). It is optional to transfer the typical cause tree and the typical measures.

In choosing between these three options, one can consider the following. The more information is transferred, the more the analyst is ‘supported’. On the other hand all the information must be adapted to fit the specifics of the subsystem under consideration. Some users will consider it more practical starting with an ‘empty sheet’ rather than modifying existing information.

4.2.2 Defining new event sources

The Event Source Suggestion List that is by default in the PLANOP package, contains a large number of event sources, but can obviously not be considered complete (this would be a dangerous assumption).
It is therefore important that, after considering the list of typical event sources, for each event source subtype the question is raised whether any other phenomena can be imagined. These extra event sources can be entered into the subsystem directly as new event sources.

4.2.3 Copying event sources between subsystems

Event sources can also be copied between subsystems: they can be dragged from one subsystem to another (using drag and drop). Obviously the copied information has to be adapted and made specific for the target subsystem.

4.2.4 Event sources linked to substances and reactions

Apart from transferring event sources from the suggestion list, creating new event sources and copying event sources between subsystems, there is a fourth way to add event sources to a subsystem. This fourth way is transferring event sources that were linked to substances or reactions that are added to a subsystem. This will be explained in chapter 7 'The hazard analysis'.

4.2.5 Naming event sources

Regardless of the identification route of the event source, it is essential to formulate the name of the event source as specific as possible. A loss of containment analysis is performed on a specific subsystem and consequently one should name the risks and measures for every subsystem as specific as possible for the given situation. For instance, if you transfer the typical event source 'Generation of heat or gas by a desired reaction' from the suggestion list, one should modify this name to also state the specific reaction that occurs in the subsystem.

4.3 Elaborating the cause tree

As mentioned before, the elements that constitute the cause tree are:

- causes leading to the manifestation of the event source
- the (name of the) event source
- the effect resulting from the event source
- one or more releases
- measures.

Examples of cause trees can be found in the Event Source Suggestion List. Some cause trees are very complex, others can be relatively simple.

4.3.1 The 2 parts of the cause tree

For practical reasons, the cause tree are represented in the PLANOP-software in two separate parts:

- the part 'causes – event source – effect'
- the part 'effect – releases'.

The event source and its effect are the central elements of the cause tree and the starting point for the further elaboration. This elaboration is done in two directions:

- elaborating causes that can lead to the event source
- linking one or more releases to the effect.

Cause trees can be shown on screen with or without the measures. When studying, modifying or creating cause trees, it can be convenient not to show the measures to keep a better overview.

4.3.2 2 types of causes: conditions and events

Two kinds of causes are distinguished: conditions and events. The difference is mainly important during the risk evaluation.

A condition is a certain situation that can exist for a period of time. A duration can be appointed to this condition, that is, the fraction of time that the condition will (can) be present. This is a value without a dimension. In the cause tree a condition will be represented with a little flag symbol.

An event occurs on a specific moment in time. The probability that the event occurs is expressed as ‘number of times per year’. An event is represented in the cause tree as a little bomb with a burning fuse.

Causes are combined using ‘AND-gates’ and ‘OR-gates’.

4.3.3 Measures in cause trees

The cause tree also contains measures. Measures for event sources have a preventative effect: they help preventing a loss of containment. In the cause tree they are represented with a pair of scissors.

The location of the measure indicates how the measure will intervene in the chain of events and conditions making up the cause tree. A measure can be put between:

- two causes (events or conditions)
- a cause and the event source
- the event source and the effect
- the effect and a release.

When placed between two elements of the cause tree, the effect of the measure is as follows: the measure reacts in response to the “deeper lying” element of the cause tree and it makes the higher element less likely (or less intense).

Also notice that the bottom level of a cause tree can not be a measure.

During the risk evaluation a probability will be calculated for each path that can be created from an initial cause to a release. For this calculation to have a meaningful result, the cause tree has to comply with certain rules. This will be explained in chapter 6.

4.3.4 Editing cause trees

Several operations are possible on cause trees:

- delete and create new causes
- move causes (including underlying causes and measures)
- copy causes (including underlying causes and measures) from one event source to another
- change the order and hierarchy of causes (i.e. move causes to a higher or lower level in the tree structure).

The following information is documented for a cause in the cause tree:

- a name
- a description
- data regarding its probability.

The probability data will be explained in chapter 6.

The information that is documented for measures will be discussed in chapter 5.

4.4 The ‘release event’ concept

Release events have the same significance for the consequences of loss of containment events as event sources have for their causes. Release events are critical events that can result from a loss of containment. They are the ‘stages’ in the course of an accident resulting from an undesired release.

Release events are represented in a tree structure that illustrates the relation and order of these events.

PLANOP distinguishes five types of release events:

1. Release
2. Dispersion
3. Impact
4. Damage
5. Victims.

To support the elaboration of a tree structure containing the release events, the PLANOP software includes a suggestion list with typical release event trees.

As mentioned earlier, release events of the type ‘release’ have a specific significance. They are the connection between the cause tree and the release event tree. Furthermore they are important to the risk evaluation process. Target frequencies (i.e. acceptable probabilities) will be attributed to the releases and compared to calculated probabilities. This will be explained in chapter 6.

The information documented for a release event is limited to its name and description. Only for events of the type ‘release’ an extra field is available for the target frequency.

The release event tree can also include measures. These can be placed in between each couple of consecutive release events.

4.5 Elaborating the release event tree

The release event tree always starts with an event of the first type: a release. Defining these releases will primarily be the result of the elaboration of the cause trees, since the release is also their final point.

The nature of the release (quantity or energy released) will depend on the event source. Some event sources can lead to explosive failure, some to a rupture, continuous leak, a BLEVE, etc. Distinguishing different releases will also allow using different target frequencies.

With these releases as a starting point, the release event tree(s) can be elaborated.

As for event sources there are also four ways to add release events to a subsystem.

4.5.1 Adding release events to the tree structure

The first way to add release events to the tree is to use the Release Events Suggestion List. Using the suggestion list, you can select typical release events that you consider to be relevant for the subsystem and then ‘transfer’ them to the tree structure of release events for the subsystem.

When you transfer a release event from the Release Events Suggestion List to the subsystem, you will be asked which of the following information is to be copied over:

- the release event and all linked release events;
- the release event, all linked release events and typical measures.

A second way to add a release event to a subsystem is to create a new empty release event.

Release events can also be copied from one subsystem to another.

There is also a fourth way to add release events to a subsystem, which is by transferring release events that are linked to substances and reactions that are added to the subsystem. This is further described in chapter 7 ‘The hazard analysis’.

As for event sources, release events have to be named specifically for the subsystem under consideration.

4.5.2 <u>Measures in release event trees</u>

Mitigating measures can be placed in the release event tree. As in the cause tree, the location in the release event tree represents when the measure will intervene in the sequence of events.

Placing a measure in between two release events means that the measure will become active when the previous release event (‘higher’ in the tree structure) occurs and will render the next release event (deeper in the tree structure) less likely or less intense. Therefore a measure can never be the first or last level in the release event tree.

For a release event of the first type ‘release’, measures to limit the release of substances should be specified. This includes measures such as confinement systems, ‘excess flow’ valves, check valves, detection systems, devices and procedures to reduce the pressure and content of leaking vessels, and so on.

For a ‘dispersion’ type of release event, measures to counter the dispersion of the released substances or energy should be specified. This includes measures such as a building in which the subsystem can be placed, containment dikes, water seals in sewage lines, water curtains and so on. For an ‘impact’ type of release event, measures related to the impact of specific phenomena should be specified, for instance fire-fighting resources in the case of the release event ‘fire’.

For a release event of the type ‘victims’, measures are to be specified to limit the number of victims or to the extent of their injuries. Some examples of such measures are procedures to reduce the presence of people in the hazard zone, procedures for evacuation, personal protection equipment, emergency showers, etc.

Note that some measures can have both preventative and damage-limiting functions. In other words, they can be specified for both event sources and release events. For instance, a sprinkler installation can address the event source ‘external fire’ (which can lead to high pressure), thus making it a preventative measure for limiting the pressure increase in a subsystem. Naturally, the same sprinkler installation can also act to extinguish an external fire if the source of the fire is located within the effective area of the sprinkler installation. In the latter case, the sprinkler installation can be considered to be a damage-limiting measure for the release event ‘fire’.

5

Specifying and analysing measures

In the previous chapter we explained the function of the measures in the cause and release event trees.

In this chapter the process of specifying measures will be treated in more detail. We will see that in this respect, it is important maintain a one-to-one relation between the measure as an ‘object’ in the database and the measure as a physical ‘reality’.

Furthermore we will discuss the analysis of these measures. By elaborating event sources into cause trees and constructing the release event trees the need to specify measures will be revealed. To achieve the desired risk reduction, these measures need to be sufficiently effective and reliable. The analysis of measures is concerned with the factors that are significant with regard to their effectiveness and reliability.

5.1 Specifying measures

Measures are the ‘output’ of a risk analysis. In PLANOP these measures are stored in a database. In order to use this information in the best manner, it is important to maintain an unambiguous relation between the measure as an ‘object’ in the database and the measure as a physical reality in the actual process installation.

Adding measures can be done by positioning the cursor on the appropriate position in the cause tree or release event tree and clicking the measure button. The user will be offered three options:
- ‘New measure’;
- ‘Existing measure’, a list of previously defined measures to choose from is presented;
- ‘Copy an existing measure’, a list of previously defined measures to choose from is presented.

5.1.1 Creating new measures in the analysis file

The option ‘new measure’ will create a new object in the database. The user should make sure that for each measure in the installation exactly one measure is created in the analysis file.

To this end in the first place measures should be named unambiguously. It is for instance not good practice to name a measure ‘safety valve’. To get a one-to-one relationship with the real installation the valve should be identified unequivocally, for instance by using a number: ‘safety valve SV301/A’.

5.1.2 Inserting previously defined measures

Secondly one should avoid creating multiple objects in the database for the same measure. No ‘duplicates’ should exist in the database. Of course it will be possible that a measure is to be specified on several occasions in the loss of containment analysis. For instance the safety valve SV301/A on vessel 301 may function as a measure for multiple event sources all leading to high pressure in the same vessel 301. In that case, it will be necessary to include this safety valve in several cause trees. One should not create in PLANOP on each occasion a new measure with the same name ‘safety valve SV301/A’. On the contrary, one should use the existing measure ‘safety valve SV301/A’ a second time. For that purpose the user can select the second option that will allow selecting an existing measure from a list of measures. Take notice that PLANOP offers a search function: typing part of the measure name will restrict the available options.

For each measure a list can be consulted indicating for what event sources or release events this measure was already specified.

5.1.3 Copying measures

The third option in the option menu allows to create a copy of an existing measure. With this option, a new measure will be created, being a duplicate of the existing measure. Of course this duplicate should be altered so it becomes unique in itself. This option can be used to define a new measure that is very much alike a measure already in the database.

When transferring event sources or release events from the suggestion lists, one can also choose to copy the typical measures that were already defined for the typical cause or release event trees concerned. Naturally, you will have to delete, expand or modify these typical measures to suit the subsystem for which the event source or release event is defined.

Measures transferred from the suggestion lists are always individual objects. Some of these transferred measures may be in fact referring to the same physical measure. For instance for each event source leading to high pressure a ‘safety valve’ will be defined as a typical measure. If several event sources with this measure ‘safety valve’ are transferred from the suggestion list to the analysis file, it will be necessary to rename one of these ‘safety valve’s more specifically and replace all the other ones with this one. In the overview listing all the measures this can be done in a simple and fast manner by selecting a duplicate in the list and replacing all references to this measure with a reference to the ‘original’ measure. Thereafter, the duplicate will be removed automatically.

5.1.4 Information stored for a measure

In addition to the name of the measure, that should be as specific as possible, the following information can be saved for each measure:

- a description
- the measure type
- information concerning the effectiveness, the independence and the reliability
- items of consideration for measures.

By using the measure type, the measure can be classified in several groups. As a consequence, lists can be generated of certain types of measures. For instance if a list of all safety valves is desired, a measure type ‘safety valves’ can be defined, and all the safety valves should be classified as such.

PLANOP has a number of default measure types. The user can however define new types or modify existing types using the maintenance mode. When doing so, the user should always bear in mind the question: of which measure types do we want to create lists?

Effectiveness, independence and reliability are three important criteria to which a measure should comply in order to be taken into consideration during the risk evaluation using LOPA. For each of these criteria a text field is available to the user to document the necessary considerations.
For reliability, a quantitative value can also be attributed to allow the LOPA risk evaluation.

When taking a measure into account in the LOPA analysis, it is necessary that this measure is independent from other causes and measures. Therefore it is possible to indicate for each measure in the "independence" tab sheet, what causes or other measures the measure under consideration is dependent (i.e. not independent) of.

Chapter 6 explains the reliability and independence of measures in more detail.

A systematic qualitative analysis of the factors contributing to the effectiveness and reliability of measures can be done using the items of consideration for measures. This will be explained in the next section.

5.2 Analysing measures

The identification and elaboration of event sources and the redaction of the release event tree(s) will show where a need to specify measures exists. To achieve the desired risk reduction, these measures need to be sufficiently effective and reliable.

5.2.1 Items of consideration for measures

In PLANOP, measures are analysed using 'items of consideration'. These items allow to document different factors that influence the effective and reliable functioning of the measures.

These factors relate to items such as:

- correct dimensioning or design of the measures (e.g., the relief capacity of a safety valve)
- influences exercised on the measures by the process (e.g., deposits on a measuring instrument or damage to a measuring instrument)
- maintenance and inspection of physical measures
- training and supervision for procedural measures.

The result of the analysis of a measure can be:

- additional specifications related to the detailed design of the measure (e.g. the location of a measurement element)
- organisational measures related to maintaining or enforcing the measure (e.g. including the measure in a regular maintenance or inspection plan)
- additional measures (e.g. a rupture disc to prevent a safety valve from being affected by the process).

5.2.2 The Suggestion List Items of Consideration for Measures

To assist in the analysis of measures, the Suggestion List Items of Considerations for Measures can be opened. You can select a single item or several items in this suggestion list and transfer them to the analysis file.

In this suggestion list typical items of consideration are listed for different categories of measures, such as pressure relief, safety instrumented systems, procedural measures, etc. In the maintenance mode, these categories can be modified by the user. Also note that the categories of the measures in the suggestion list don't need to be the same as the measure types used to classify measures for the purpose of listing.

5.2.3 Information stored for an item of consideration

The information documented for an item of consideration is the following: a name, a type and a description.

The name usually refers to the problem under consideration, for instance 'pressure drop' (a possible item for pressure relief systems). The description of the item should contain the solution to the problem. For 'pressure drop' this could be a calculation showing that this pressure drop was accounted for in the design. The type refers to the nature of the solution, in this case it would be 'design specification'.

Each item of consideration in the analysis can be attributed a so called 'type', for example: 'inspection', 'instruction', 'design specification', etc. This permits to easily find the relevant items of consideration for measures on the printouts.

5.2.4 Organising the analysis of measures

Each measure is to be analysed separately. This analysis can be organised in various manners.

The first option is to analyse measures when they are specified. In this case, the analysis of the measures can be performed (for example)

- immediately after each measure is specified;
- after all the measures for a specific event source or release event have been specified, or
- after all the measures for a particular subsystem have been specified.

Alternatively, analysing the measures can be regarded as a separate part of the PLANOP analysis that is independent of specifying the measures, with the analysis being performed at a different time than during the identification of the measures.

6

Risk evaluation using LOPA

Risk evaluation is judging whether the risk is sufficiently controlled, whether the measures taken are sufficient.

To this end PLANOP incorporates the LOPA-technique. LOPA is an acronym for 'Layer of Protection Analysis'. LOPA is not a single well defined technique, several variants are possible. Evidently this manual will only describe the PLANOP-variant. For more background information on LOPA you can read the book 'Layer of Protection Analysis, Simplified Process Risk Assessment', which is a publication by the Centre for Chemical Process Safety.

6.1 LOPA, a simplified quantitative technique

LOPA is a simplified quantitative technique for evaluating risks.

6.1.1 Quantification of probabilities

As in other quantitative risk evaluation techniques, in LOPA the probability of a certain event (the so called final event) is calculated and compared with a previously chosen acceptable probability, the so called target frequency. If the calculated probability is higher than the target frequency, additional measures need to be taken or the reliability of the current measures needs to be improved so that the new calculated probability is equal or smaller than the target frequency.

6.1.2 Evaluating single cause scenario's

Classic quantitative risk evaluation techniques calculate cumulated probabilities. For a certain final event a fault tree is constructed identifying all possible causes leading to the top event. Next the frequencies of all these causes are combined in order to calculate the frequency of the top event.

LOPA, however, only calculates scenarios with a single initial cause. The probability is calculated that the final event will occur as a result of one single cause, the so called initial event. Such a single cause scenario is equal to one 'path' that can be identified in a fault tree starting from an initial cause at the bottom of the tree structure all the way up to the top event. The probabilities of the different scenarios (or paths) that lead to the same top event are not cumulated in LOPA.

By using single cause scenarios, LOPA avoids some disadvantages of quantitative fault tree analysis. The elaboration of a complete and correct fault tree (suitable for the purpose of doing calculations) is very difficult and time consuming. Such fault trees also tend to become very large and unclear. The calculation of the top event probability is a hard mathematical exercise, especially when several causes and measures in the tree are identical or not independent.

6.1.3 The meaning of calculated probabilities

The probabilities that are calculated for single cause scenarios in LOPA evidently have no 'absolute' value. For example, when applying LOPA one doesn't calculate the probability of the explosion of vessel X, but one calculates the probability of an explosion of vessel X due to one specific cause. However, by following a number of strict rules, the resulting probability does have a sound relative value, that can be compared to other values resulting from the application of the same rules. The frequency of the single cause scenario is a relative quantitative measurement of the quality of risk control in this scenario.

The question can be raised what real value can be attributed to the cumulated probabilities that result from fault tree analysis. These probabilities have a large margin of error, especially considering the inaccuracy of the figures used. Moreover, this margin of error will be enlarged if the fault tree is incomplete in any way.

6.1.4 The benefits of LOPA

The advantage of quantitative techniques is the obligation to unambiguously identify the risk and the measures and to assess them by attributing numerical values. Furthermore the independence, the reliability and the effectiveness of the measures must be evaluated. Due to its quantitative character, LOPA offers clarity and transparency, qualities that risk assessments using techniques as the risk graph or the risk matrix are often lacking. These techniques allow classifying the risk in a category without explicitly identifying or documenting all the elements contributing to this classification.

Since LOPA is a simplified technique, it can easily be applied to a large number of scenarios. LOPA will especially be appropriate to evaluate risks that are controlled with so called active measures, since the reliability of these measures depends to a large degree on their design and maintenance. Active measures in the process industry are typically:

- mechanical safety systems, such as safety valves or bursting disks
- instrumented safety systems
- measures requiring a human intervention.

Since using LOPA implies attributing reliabilities to measures, a SIL-classification can directly be determined in conformity with the standards IEC61508 and IEC61511 on functional safety.

6.2 Selection of the final event

6.2.1 Evaluating the release

During the risk evaluation, the severity and probability of the ultimate damage (to people, to the environment or economic damage) is often assessed. LOPA also allows choosing the ultimate damage as the final event.

In PLANOP however, the final event for the purpose of risk evaluation is chosen much earlier in the chain of events, that is, at the undesired loss of containment of substances or energy. This means that PLANOP will attribute target frequencies to these releases. There are several good reasons to choose a release as the final event rather than the ultimate damage.

6.2.2 Avoiding the complexity of post-release events

To make calculations on a single cause scenario, all the events linking the initial event to the final event must be identified. It is clear that the chain of events from initial event to release will be much shorter than the chain leading from initial event all the way up to the ultimate damage. A number of intermediate events occurring between the release and the ultimate damage can be identified. For instance, for a release of a flammable substance to lead to casualties, first an explosive atmosphere must be formed, this explosive mixture must find a source of ignition, and people must be present and sufficiently exposed to the flames or the pressure wave resulting from the explosion. Therefore to calculate the probability of the final event 'fatality', the probabilities of al these intermediate events need to be determined. This will render the evaluation much more difficult. Not only do we have to identify all intermediate event, we also have to attribute probabilities to these events. Furthermore, phenomena that occur after the release are by definition less controlled and more random than phenomena that occur inside the installation (before the loss of containment). As a consequence it is much harder attributing meaningful probabilities to events occurring after the release than to events occurring before the release.

Besides the probability of the events, one also has to take into account the reliability of the measures that will act on these events, for instance the use of explosion proof equipment, fire fighting systems, evacuation possibilities, etc. The reliability and effectiveness of these mitigating measures are much more difficult to assess than of measures preventing a release. Furthermore, every mitigating measure may cause the event tree to split up. Both the successful functioning and the failure of these measures have to be taken into account since both cases may lead to damage.

Every loss of containment can lead to large number of possible damage cases, depending on the occurrence of certain phenomena and on the functioning of the mitigating measures. The final damage can also be differentiated according to the nature of the receptor (people, environment, business). Instead of evaluating all these cases separately, one can choose to evaluate only the loss of containment. When fixing the target frequency for the release, one can account for all the potential consequences to man, environment or business.

6.2.3 Avoiding a trade-off between prevention and mitigation

Not only practical difficulties arise when evaluating final damage cases. There is also a problem in using these results.

Taking mitigating measures into account may lead to some odd conclusions. Imagine that it would be possible to sufficiently reduce the frequency of the final event for all initial causes only by means of preventative measures. In that case the calculated probability of the release will already be smaller than the target frequency of the ultimate damage. One might draw the conclusion that in this case mitigating measures are unnecessary. In practice however, mitigating measures (such as dikes, fire fighting systems, evacuation routes, first aid provisions, etc) are taken regardless of the probability of the loss of containment, in compliance with codes of good practice or regulations.

The inverse argumentation could also be made. By taking extra mitigating measures one can obtain the same probability for the final event with less preventative measures. One could draw the conclusion that a more frequent occurrence of a loss of containment is acceptable if more mitigating measures are in place. This conclusion however is not supported by industry practice. Usually organisations that put a lot of effort in mitigation will also be trendsetters in prevention.

In practice LOPA is used to determine the desired reliability of preventative safety systems (e.g. SIL classification of instrumented safety systems as defined in the standard IEC61508). To achieve this goal it is sufficient to determine the probability of the loss of containment.

6.2.4 Avoiding acceptable frequencies for loss of human life

A final argument against using damage as a final event in LOPA concerns the attribution of target frequencies. It is not easy, neither from a scientific nor from a social point of view, to attribute an acceptable frequency to the loss of human life. Add to this that the calculated frequencies of fatality hardly have an absolute value because of the large margins of error on the numerical data (especially for events and measures after the loss of containment) and the principle of single cause scenarios. As mentioned before, the calculated frequencies in LOPA need to be considered as relative indications of the quality of the measures preventing the final event. It is however difficult to attribute a relative and not an absolute significance to the tolerable frequency for loss of life.

6.3 Choosing the target frequency for the final event

The use of the loss of containment as the final event in LOPA is a fixed element in PLANOP. The PLANOP user is to attribute target frequencies to the releases. In order to do this in a consistent manner, criteria need to be used. The responsibility for determining the form and content of these criteria lies within the company operating the installation that is analysed. These criteria should indicate which parameters are used to characterise the loss of containment and what target frequencies will be attributed according to these parameters.

6.3.1 A matrix with target frequencies

The nature and quantity of the substances that can be released are obvious parameters to characterise the loss of containment. PLANOP offers a matrix with target frequencies for combinations of these two parameters. The matrix can be consulted when target frequencies are to be assigned to releases. This matrix however needs to be calibrated using the maintenance mode. The hazard categories, quantities and target frequencies that are in the matrix by default have no purpose but to provide a starting point. Of course it is not obligatory to use this matrix in PLANOP.

6.3.2 Calibrating the risk evaluation criteria

A possible approach to calibrate this matrix or other rules to determine the target frequencies, is to elaborate a number of scenarios for installations that are considered to be protected with the “best available technology”. This judgement may be based on compliance with a standard industry practice for that kind of installation (e.g. an LPG storage tank) or it can be based on the results of risk evaluation using different methods (like QRA). The calculated frequencies for the scenarios of this ‘reference installation’ can be considered valid target frequencies. As such, these target frequencies are not an indication of tolerable damage, but an indication of the quality of preventative measures required for these scenarios. In this way, the target frequencies are calibrated according to the best available practices.

Based on previous experience with LOPA, it should technically and economically be possible to reduce the probability for undesired loss of containment for a single cause release scenario to the order of 10^{-4} or 10^{-5} per year.

6.4 Identifying and calculating single cause scenarios

In PLANOP single cause scenarios will be calculated for each event source. The software will identify all paths starting with an initial cause in the cause tree and leading to a release. If the cause tree has five initial causes and two releases, than ten single cause scenarios will be identified.

An initial cause is a cause

- without underlying causes or
- with underlying causes and with a 'manually' attributed frequency.

Every initial cause should have a frequency or no calculation can be performed. It is however possible to attribute a frequency to a cause and elaborating this cause in underlying causes without attributing frequencies to these underlying causes. After all it is sometimes desirable to analyse a cause for qualitative reasons (to improve insight in the occurrence of this cause and to define appropriate measures), without using these underlying causes for calculation purposes.

If the user indicates that he wants to use LOPA for an event source, all the single cause scenarios will automatically be deferred from the cause tree and calculated using the probabilities attributed to the causes and the reliabilities attributed to the measures.

This calculation will only be possible if the cause tree complies with certain rules and if all necessary values were attributed to causes and measures.

6.5 Numerical values for causes and measures

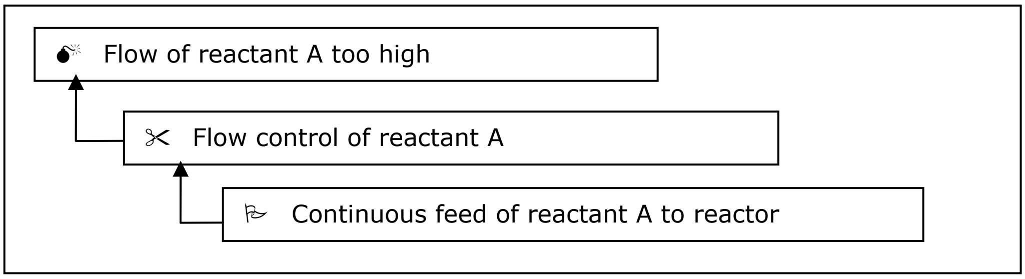
6.5.1 Causes

Causes can be events or conditions. The user has to make the appropriate choice.

Events are characterised by an average frequency of occurrence, which is a value expressed as 'number of times per year'. For instance a pump trip is an event whose frequency could be: once a year.

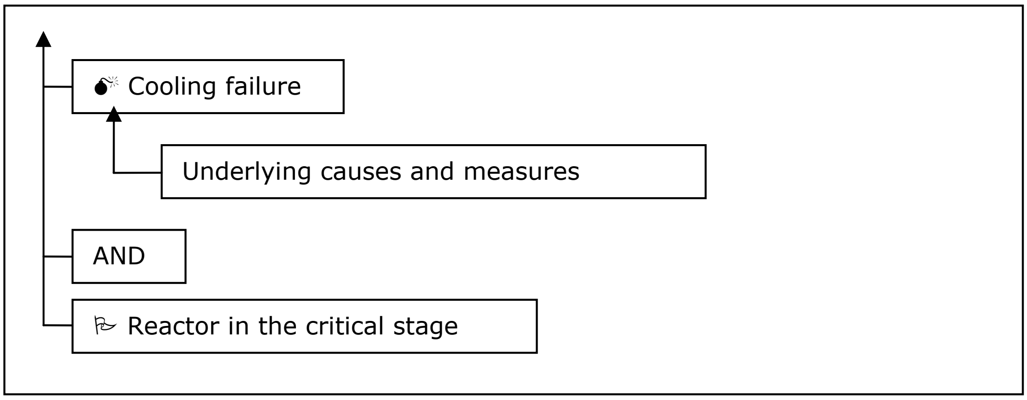
Conditions are characterised by the fraction of the time they exist, which is a value without a dimension. Conditions are usually found in the bottom of the cause trees as an initial cause. They are often the underlying causes for control systems. In chapter 4 was explained that in order to consider these control systems as measures, an underlying 'cause' needs to be defined. This underlying cause is the condition that needs controlling. For instance the 'continuous feed of reactant A' to a reactor is a cause of the type 'condition' for which a measure can be defined: 'flow control of reactant A' (see figure 6.1).

Figure 6.1: A condition as an initial cause


Flow of reactant A too high
Flow control of reactant A
Continuous feed of reactant A to reactor

Conditions can also be used to express 'enabling conditions'. These are conditions that need to be fulfilled so that the scenario may occur. Loss of cooling on a reactor for instance may lead to a large heat production and high pressure. Suppose this can only happen in a certain stage of the reaction cycle and the reactor is only in this stage for 10% of the time. An 'enabling condition' for this scenario would be that the reactor is in this specific reaction stage. If the cooling fails once every ten years and the reactor is only 10% of the time in this critical stage, the probability of a large heat production would be once every hundred years (see figure 6.2).

Figure 6.2: 'Enabling condition': Reactor in the critical stage

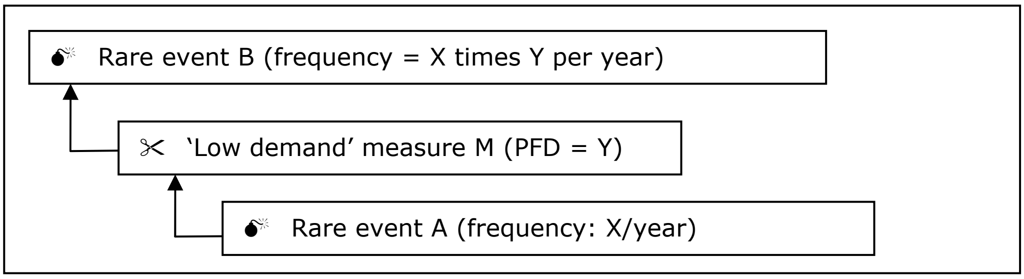


6.5.2 <u>Measures</u>

As it is the case for causes, measures can also be characterised by different 'types' of reliabilities.

The reliability of measures that have to function only every once in a while, is expressed with a PFD value. PFD is an acronym for 'probability of failure on demand' which is a value without dimension. A PFD of 10^{-2} means that if the measure is demanded a 100 times, it can be expected that on average it will fail once, or in other words, the probability of failure when the measure needs to function is 0,01. Safety systems are typical measures that are only called upon rarely (at least this should be the goal). This type of measures is called 'low demand' measures. As illustrated in figure 6.3 the frequency of the first event and the PFD of the measure will determine the frequency of the second event.

Figure 6.3: 'Low demand' measure


Rare event B (frequency = X times Y per year)
'Low demand' measure M (PFD = Y)
Rare event A (frequency: X/year)

Other measures function continuously or are very often in demand. They are called 'continuous demand' and 'high demand' measures. Control loops are typical 'high' or 'continuous demand' measures. The reliability of these measures is usually expressed as a failure frequency. A failure frequency is the number of times that the measure is expected to fail per time unit (usually a year).

'Continuous demand' measures act on conditions, 'high demand' measures react to frequent events. It is important to know that in the scenario calculations, the probability of the condition or the event that precedes the 'high' or 'continuous demand' measure will NOT be taken into account. This is illustrated in figures 6.4 and 6.5.

Figure 6.4: 'Continuous demand' measure

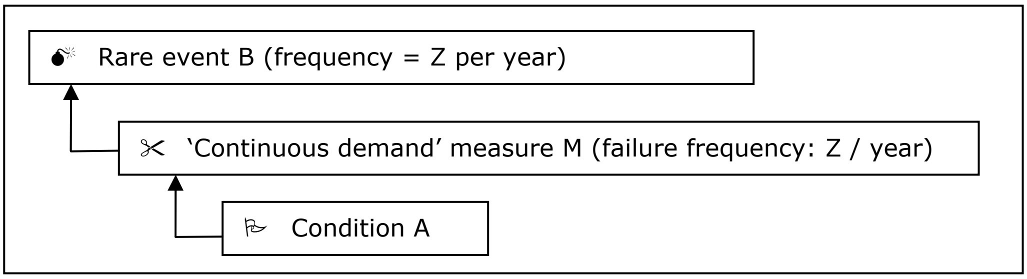
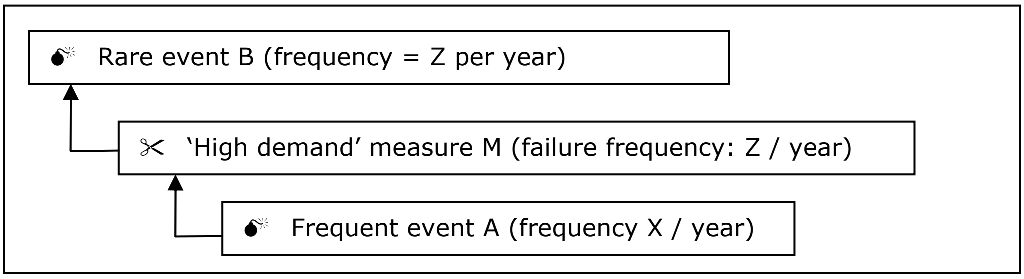

Rare event B (frequency = Z per year)
'Continuous demand' measure M (failure frequency: Z / year)
Condition A

Figure 6.5: 'High demand' measure


Rare event B (frequency = Z per year)
'High demand' measure M (failure frequency: Z / year)
Frequent event A (frequency X / year)

Reconsider the example concerning the flow control on the feed of reactant A. The probability of the event 'feed flow of reactant A too high' is equal to the failure frequency of the measure 'flow control of reactant A'. The probability of the condition 'continuous feed of reactant A to the reactor' is not taken into account.

For 'high demand' measures that imply a human intervention, the reliability can also be characterised by a PFD. For instance consider an operator who needs to perform a certain manipulation. The reliability of this operator can be expressed in two ways. Either the reliability is expressed as the number of times per year he is expected to make an error, or the reliability is expressed as the number of errors per number of manipulations. The figures 6.6 and 6.7 illustrate these possibilities.

Figure 6.6: The reliability of an operator expressed as a PFD

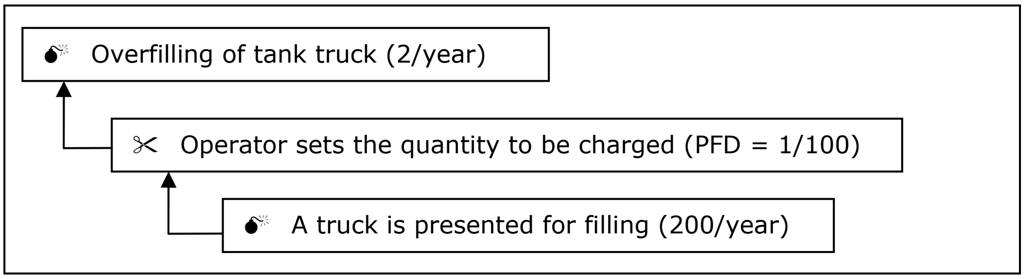
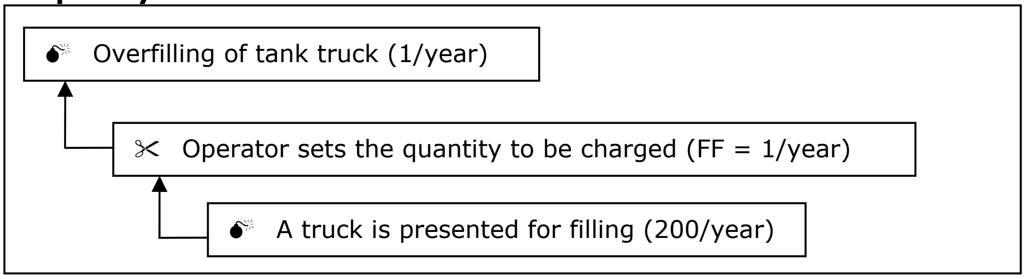
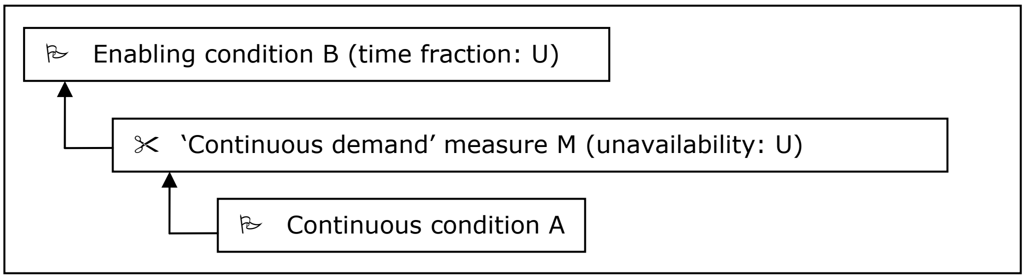

Overfilling of tank truck (2/year)
Operator sets the quantity to be charged (PFD = 1/100)
A truck is presented for filling (200/year)

Figure 6.7: The reliability of an operator expressed as a failure frequency


Overfilling of tank truck (1/year)
Operator sets the quantity to be charged (FF = 1/year)
A truck is presented for filling (200/year)

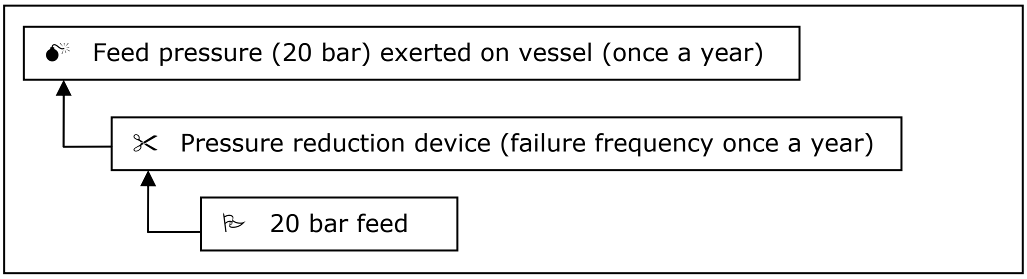
Besides a failure frequency or a PFD a third possible value may characterise the reliability of a measure: unavailability. The unavailability is the part of the time the measure is not functioning. The unavailability is the product of the failure frequency and the time that is needed to detect the failure and repair the measure. The unavailability is used if the result of the failure of the measure has to be a condition and not an event (see figure 6.8).

Figure 6.8: 'Continuous demand' measure with an unavailability


Enabling condition B (time fraction: U)
'Continuous demand' measure M (unavailability: U)
Continuous condition A

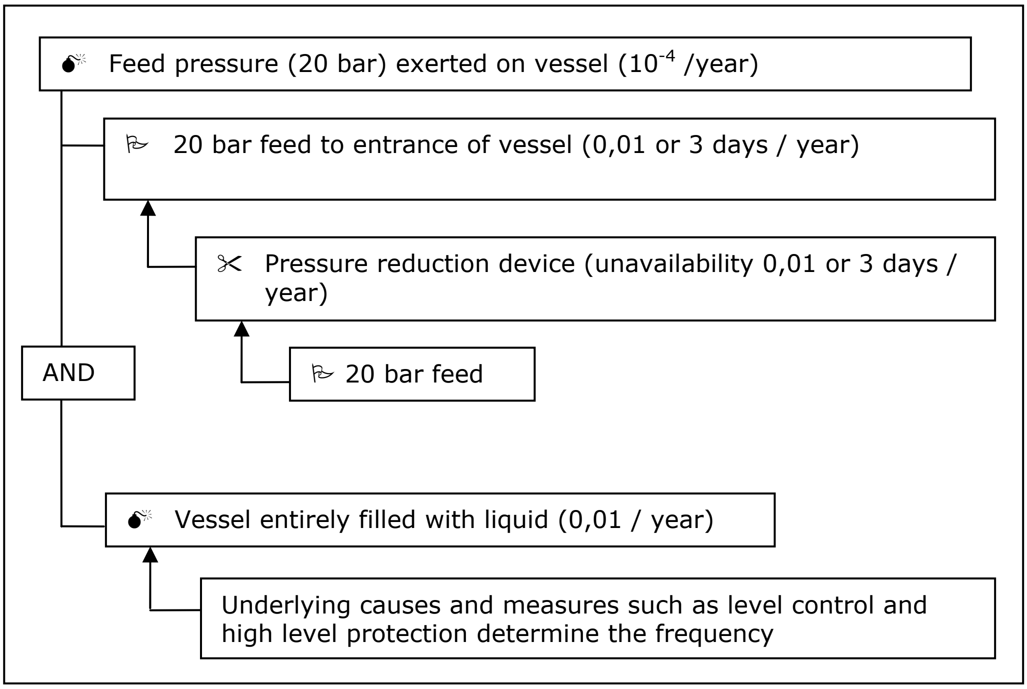
An example can illustrate this. Consider a vessel that is fed by a high pressure gas stream. Before entering the vessel, the pressure of feed flow is reduced by means of a pressure reducer. When this pressure reducer fails, the vessel will immediately receive the maximum feed pressure. This is an event (not a condition). Figure 6.9 represents the combination of measures and causes for this example. In this case the failure frequency of the pressure reduction device is used.

Figure 6.9: Measure with failure frequency leads to an event


Feed pressure (20 bar) exerted on vessel (once a year)
Pressure reduction device (failure frequency once a year)
20 bar feed

In case of a liquid feed however, the vessel needs to fill up entirely before the maximum feed pressure of 20 bar is exerted on the vessel. If the pressure reduction device fails, this will lead to the condition '20 bar feed to entrance of vessel' (that is, after the pressure reduction device). This condition needs to be in an 'AND' combination with the event 'Vessel entirely filled with liquid' for the event 'Feed pressure (20 bar) exerted on vessel' to occur. In this case unavailability will have to be used for the pressure reduction device in order to have a condition as a result (see figure 6.10).

Figure 6.10: A measure with unavailability results in a condition


Feed pressure (20 bar) exerted on vessel (10^{-4} /year)
20 bar feed to entrance of vessel (0,01 or 3 days / year)
Pressure reduction device (unavailability 0,01 or 3 days / year)
AND
20 bar feed
Vessel entirely filled with liquid (0,01 / year)
Underlying causes and measures such as level control and high level protection determine the frequency

6.6 Rules for creating a cause tree

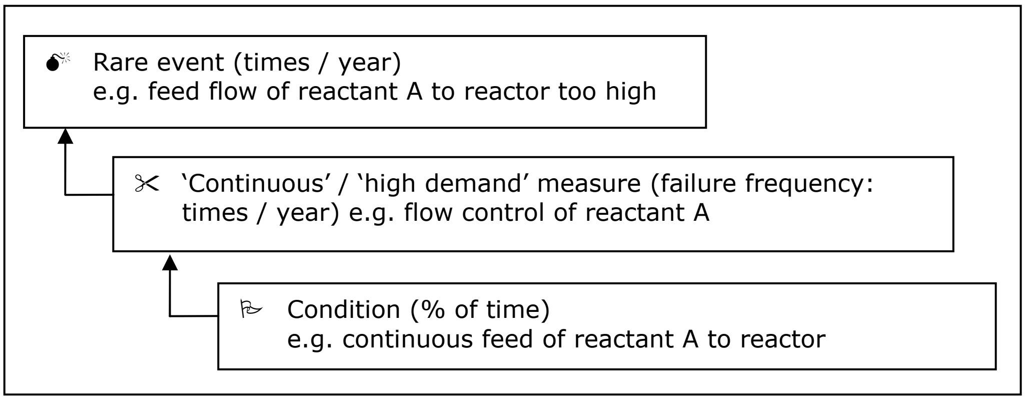
The PLANOP software will detect and report errors in the cause tree. Nevertheless it is important that the user understands the rules that need to be applied to create a cause tree that is 'mathematically' correct.

The numerical values of the subsequent causes and measures in the chain of events leading from initial cause to final event (the release) are multiplied.

The final result of this calculation should always be expressed as 'times per year'. To ensure this, the following rules need to be fulfilled.

1. A condition (value: time fraction, no dimension) or a frequent event should always be followed by a 'continuous' or 'high demand' measure (value: failure frequency, times a year). The result is a rare event whose frequency is equal to the failure frequency of the 'continuous' or 'high demand' measure (see figure 6.11.

Figure 6.11: 'Continuous' or 'high demand' measure following a condition or frequent event

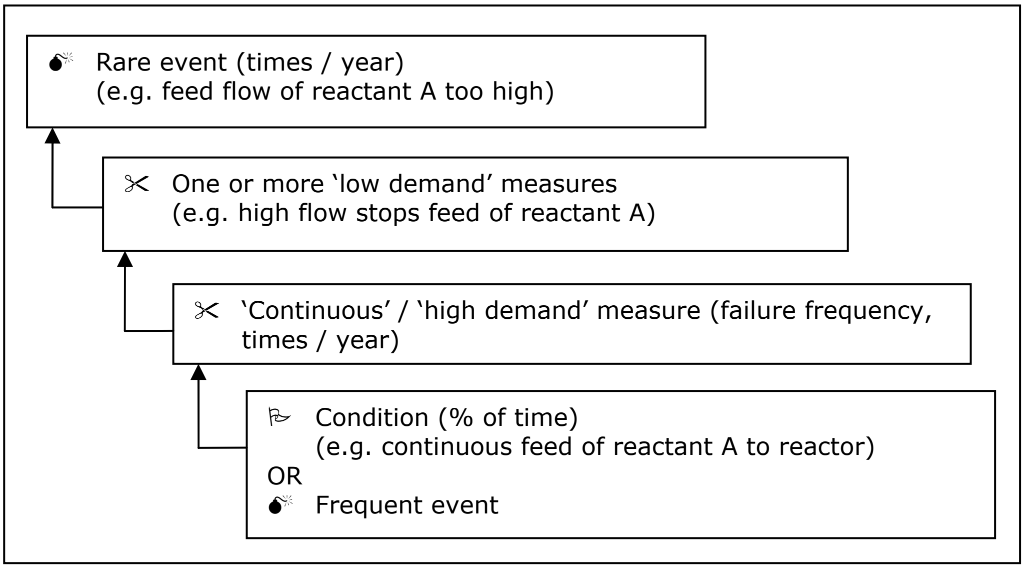

Rare event (times / year)
e.g. feed flow of reactant A to reactor too high
'Continuous' / 'high demand' measure (failure frequency: times / year) e.g. flow control of reactant A
Condition (% of time)
e.g. continuous feed of reactant A to reactor

2. A 'continuous' or 'high demand' measure followed by a 'continuous' or 'high demand' measure is pointless. This would mean that the first measure is of such poor quality that it fails so often that it would lead to a frequent event. The software nevertheless allows doing this. The user should be aware of the fact that in the calculation only the last 'high' or 'continuous demand' measure will be taken into account.

3. The combination of a condition or frequent event and a 'continuous' or 'high demand' measure may be followed by an unlimited number of 'low demand' measures. After all, the result of a condition and a 'continuous' or 'high demand' measure is a rare event (see figure 6.12).

4. An event can only be combined with a condition using an 'AND' gate. The result will be a new event. Two events can not be combined using an 'AND' gate. The probability of two independent events occurring at the exact same time is negligibly small.

Figure 6.12: 'Low demand' measures after a 'continuous' or 'high demand' measure


💣 Rare event (times / year)
(e.g. feed flow of reactant A too high)
✂ One or more 'low demand' measures
(e.g. high flow stops feed of reactant A)
✂ 'Continuous' / 'high demand' measure (failure frequency, times / year)
⚐ Condition (% of time)
(e.g. continuous feed of reactant A to reactor)
OR
💣 Frequent event

5. Events can be combined using 'OR' gates. The combination of an event and a 'high' or 'continuous demand' measure is also possible, since these measures result in an event (which does not need not be explicitly identified and given a name in the tree structure). The combination of events or the combination of an event and a 'high' or 'continuous demand' measure using an 'OR' gate always results in an event. An event can only be combined using an 'OR' gate with an event or with a 'high' or 'continuous demand' measure. It can not be combined using an 'OR' gate with a condition.

6. The combination of conditions either using an 'AND' gate or using an 'OR' gate will result in a condition. The combination of a condition with an 'unavailability' measure is possible and will result in a condition.

6.7 Dependencies

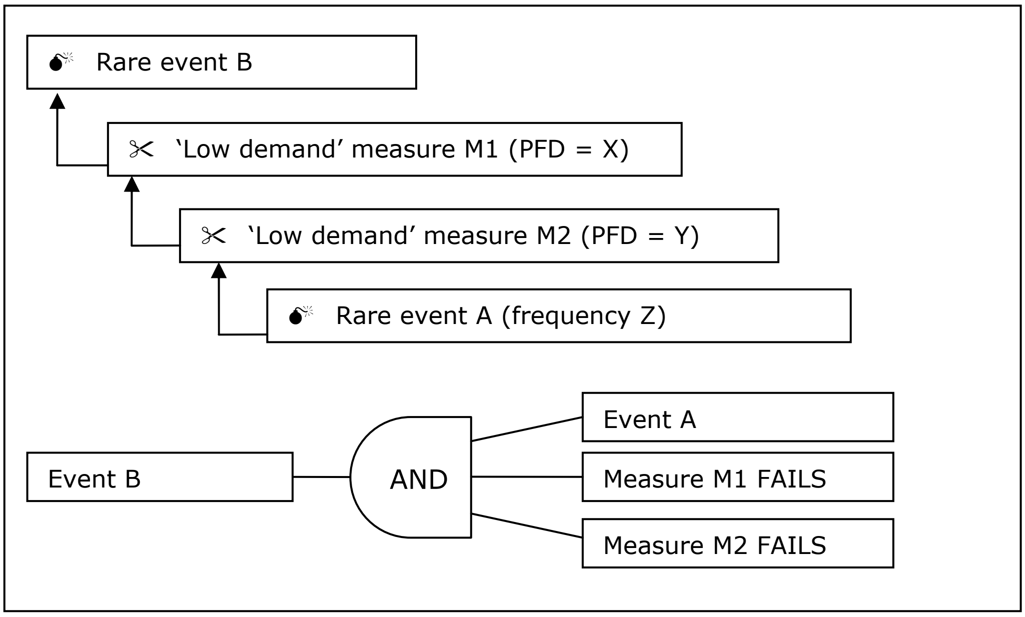
When calculating a single cause scenario, only causes and measures may be taken into account that are mutually independent.

6.7.1 Dependencies and their effect in LOPA

Measures are considered mutually dependent if a common error that can disable both measures at the same time is conceivable. If two measures have a physical component in common, they can not be considered independent for the application of LOPA.

A different representation of the events will clarify this. The chain of events in figure 6.13 can also be represented using a classic logical diagram containing an 'AND' gate. The event B will only occur if event A occurs, measure M1 fails AND measure M2 fails.

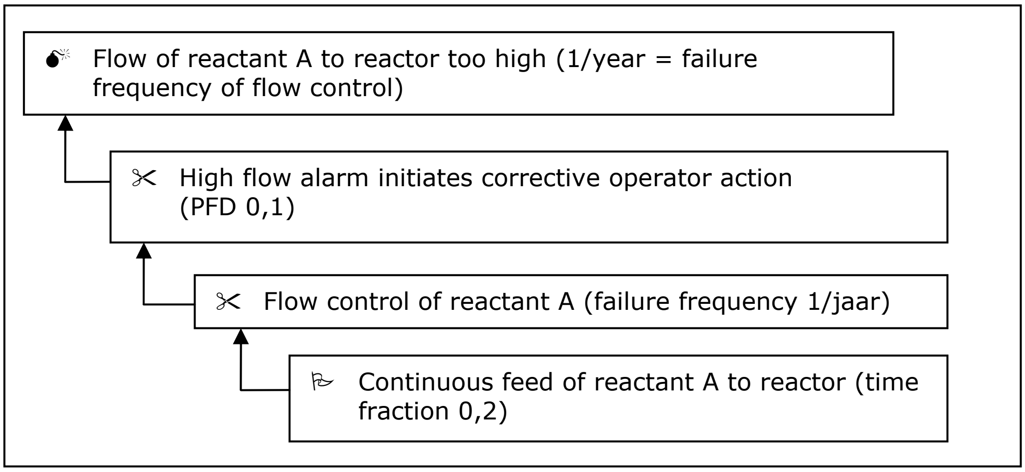
Figure 6.13: Logical diagram for measures


Rare event B
'Low demand' measure M1 (PFD = X)
'Low demand' measure M2 (PFD = Y)
Rare event A (frequency Z)
Event B
AND
Event A
Measure M1 FAILS
Measure M2 FAILS

The frequency of event B can be determined by multiplication of the probabilities (X * Y * Z), but only if they are independent of each other. If, for instance, M1 and M2 are not independent of each other (a common error can occur), than the probability of them both failing is not X*Y, but higher (i.e. more likely). This probability will certainly be smaller than X or Y, so the lowest of these two values can be used in a conservative manner. This means the probability of the event B will be equal to X*Z (or Y*Z if this is lower). This is exactly what the PLANOP-software does: if there is a dependency, the least reliable of the two measures will be discarded in the calculations.

Suppose that in the next example the high flow alarm is generated by the same control system that is also regulating the flow of reactant A. Consequently the measures 'High flow alarm initiates corrective operator action' and 'Flow control of reactant A' are not independent. A failure frequency can be attributed to the flow control and a PFD to the high flow alarm, but these values may not be multiplied to determine the probability of the event 'Flow of reactant A to reactor too high' (see figure 6.14).

Figure 6.14: Dependent measures do not all count in LOPA


Flow of reactant A to reactor too high (1/year = failure frequency of flow control)
High flow alarm initiates corrective operator action (PFD 0,1)
Flow control of reactant A (failure frequency 1/jaar)
Continuous feed of reactant A to reactor (time fraction 0,2)

Measures can also be dependent of causes. Consider a reactor equipped with a system for injecting a 'killing agent' that will stop the reaction if the pressure becomes too high. Suppose this measure is only effective if the reactor is sufficiently stirred, that is if the mixer is working. However, failure of the mixer may in itself be a cause for the runaway of the reaction due to accumulation of the reactants or reduced cooling. The emergency system of the reactor will be activated by the pressure rise following the mixer failure, but it will not lead to the desired effect. Therefore the measure should not be taken into account for the scenario 'failure of reactor due to mixer failure'.

6.7.2 Dealing with dependencies in PLANOP

It should not be the intent to leave one of the dependent measures out of the cause tree (in this case the high flow alarm). After all, it was the intention to identify and document as many measures as possible. Even though control and alarm are not mutually independent and they can not both be taken into account for LOPA, the alarm still has its value and it is important that this measure be well implemented and maintained (using instructions, training, inspections, etc.). Both measures need to be specified, but their mutual dependence is to be documented in PLANOP. This can be done quite simply: for each measure an overview can be opened of all the cause trees in which the measure is used. In this overview all other elements (causes or measure) the measure is not independent of can be selected. The PLANOP software will take this information into account for the calculations.

6.8 Determining reliabilities and frequencies

In the bottom level of the cause tree usually the initial conditions are found describing how the process is operated. The fractional duration of these conditions can be determined based on the knowledge and experience of the process (e.g. how often a device is in service). Usually these initial conditions are followed by 'continuous demand' measures which means that the fractional duration is in fact of no importance for the calculation, since the calculation will use the failure frequency of the measure. On the other hand, if conditions are used as 'enabling conditions', the fractional duration will be important.

Events can also describe the process characteristics, for instance the number of times a certain manipulation is performed. Again this frequency will be the result of these process characteristics. If this event is followed by a 'high demand' measure which has a failure frequency, then the frequency of the initial event will not be important in the calculations. The frequency will however count if the event is followed by a PFD measure (see figure 6.3).

Some initial events will be failures of certain systems, for instance pump failures, power outages, the fracture of a mixer, etc. For these 'elementary' failures appropriate values can be found in literature or own experience may be used.

'High' and 'continuous demand' measures are usually control systems or human interventions. Values for these can also be found in literature.

'Low demand' measures are usually either mechanical systems (pressure relief) or instrumented systems.

Values for mechanical systems can be found in literature. In case of safety valves distinction can be made between 'clean' and 'polluting' or corrosive conditions. The reliability of safety valves is influenced but little by their design, though redundancy evidently will increase the reliability of pressure relief. Parallel safety valves however may show common errors, for instance a common connection to the vessel or exposure to the same process conditions. The reliability of safety valves is highly influenced by the inspection frequency. The testing of a safety valve is an opportunity to test the opening pressure of the valve. By collecting this data a representative idea of the reliability can be obtained.

The reliability values of initial conditions, initial events and 'high' and 'continuous demand' measures can often not be calculated. Estimates have to be used. The accuracy of these estimates however is not extremely important as long as the same values are used consistently and the same set of values is taken into account when determining the rules used to set the (tolerable) target frequencies. As mentioned in the section on target frequencies, the calculated frequencies can be considered as a relative quantitative measure for the quality of the prevention. Some examples of PFD values are represented in table 6.1.

Table 6.1: Examples of PFD values in literature

Measure	PFD	Typical value
Open pressure relief	10^{-2} to 10^{-3}	10^{-2}
Flame arrestors / detonation arrestors	10^{-1} to 10^{-3}	10^{-2}
Pressure relief safety valve	10^{-1} to 10^{-5}	10^{-2}
Rupture disc	10^{-1} to 10^{-5}	10^{-2}
Control system	10^{-1} to 10^{-2}	10^{-1}
Instrumented safety loop SIL 1	10^{-1} to 10^{-2}	10^{-1}
Instrumented safety loop SIL 2	10^{-2} to 10^{-3}	10^{-2}
Instrumented safety loop SIL 3	10^{-3} to 10^{-4}	10^{-3}
Human intervention 10 min. time	1 to 10^{-1}	10^{-1}
Human intervention 40 min. time	10^{-1} to 10^{-2}	10^{-1}

The reliability of instrumented safety loops is determined by the architecture of the loop, the components used and the test frequency. Determining the reliability of instrumented systems is a specialised matter that goes beyond the scope of PLANOP. LOPA and PLANOP are used to determine the desired reliability of safety systems, not the actual reliability. Of course the desired and actual reliability should match. In case of new installations, sufficient information can usually be obtained from suppliers in order to calculate this for new loops. Determining the actual reliability of existing systems is much harder.

Previously we stated that the reliability of 'low demand' measures, both mechanical and instrumented, is strongly influenced by their inspection frequency. An important conclusion is that measures (instrumented or mechanical) that can not be inspected or tested (and that do not test themselves), can not be awarded a PFD value. Therefore it is essential that for each measure that is awarded a PFD, the inspection or test frequency is checked (and documented).

6.9 Overview of the risk evaluation in PLANOP

Let us recapitulate the different steps for performing the risk evaluation in PLANOP.

First a suitable cause tree should be elaborated for each event source, consisting of events, conditions and measures. As explained, during this process a number of rules must be followed.

The cause tree must be linked to one or more releases that were defined for the subsystem. For each release a target frequency is determined, that will be the criterion used to evaluate the identified paths.

For events or control measures (‘high demand’), failure frequencies are estimated. For other barriers (‘low demand’) a PFD value is determined. If ‘enabling conditions’ are used, a probability (‘fractional duration’) is to be attributed. Now the question has to be raised: are the measures in the cause tree independent from each other and independent from the causes? If not, these dependencies have to be documented.

Now the PLANOP software will do the rest: it will determine the initial events and the paths that lead to the release(s).
For every path a frequency is calculated by the PLANOP-software.
The objective is to specify sufficiently reliable measures so that the probability of every path (i.e. every single cause scenario) is equal or less than the target frequency of the release.

For each path PLANOP will show a data sheet indicating the elements of the path and the calculation. This data sheet will clearly show the influence of the individual measures and if necessary what can be done to achieve the target frequency.
Possibilities to improve the resulting frequency are for instance:

- adding extra measures
- increase the reliability of measures (e.g. the SIL classification of instrumented safety systems)
- make measures independent, for instance by implementing a control loop separately
- increasing the target frequency by adding mitigating measures that reduce the severity of the release.

7

The hazard analysis

It goes without saying that in a chemical process installation, the presence of substances and reactions has an important effect on the possible causes and consequences of losses of containment, or to use PLANOP terminology, on event sources and release events.

Consequently, it is not possible to perform a proper loss of containment analysis without also making a hazard analysis. In PLANOP, a hazard analysis consists of the following:

- for each subsystem, identifying the substances and reactions that are or can be present
- for each substance and reaction that is or can be present in the installation, investigating the properties of the substance or reaction that are relevant to the causes (event sources) and consequences (release events) of loss of containment.

PLANOP is intended to do more with the hazard analysis than simply compiling data that is only made available to risk analysts in a purely passive manner (even though this is a worthy objective in itself). With PLANOP, the intention is to allow data and knowledge about substances and reactions to be incorporated into the system in a manner such that this information is available in an active and semi-automatic manner when a loss of containment analysis is being performed.

The active link between the hazard analysis and the loss of containment analysis is implemented by allowing event sources and release events to be coupled to substances and reactions. Whenever you add substances or reactions to a subsystem, the PLANOP program will ask whether you want to copy the associated event sources and release events to the list of event sources and release events for this subsystem.

The hazard analysis has a preparatory and supportive function with respect to the loss of containment analysis. In practice, this part of the PLANOP analysis should therefore be performed before the loss of containment analysis whenever possible. It is only for purely didactic reasons that the hazard analysis is described after the loss of containment analysis in this manual.

7.1 Identifying substances and reactions

7.1.1 Substances present under normal and abnormal conditions

In order to take into account the influence of substances and reactions on undesired loss of containment, it will be necessary to generate for each subsystem an inventory as complete as possible of the substances and reactions that can be present under normal and abnormal conditions.

Generating a complete inventory of substances in a subsystem is not just a matter of identifying the substances that are present under normal conditions. Instead, it is primarily a matter of identifying the *undesired* substances that can be present in the subsystem under abnormal conditions. In PLANOP, identifying undesired substances is assisted by an Undesired Substances Suggestion List. This suggestion list can be modified by the user via the maintenance mode.

7.1.2 Commonly occurring substances

In order to simplify the process of identifying undesired substances, PLANOP uses the concept of 'commonly occurring substances'. Commonly occurring substances are substances that can be expected to be present in all or nearly all subsystems, such as water, air, lubricating oil, nitrogen and oxygen. Such substances thus do not have to be identified anew as undesired substances for each subsystem.

The list of commonly occurring substances can be modified by the user via the maintenance mode.

If any of these commonly occurring substances contributes to the risks, this will almost always be due to an undesired reaction between such a substance and other substances. In one way or another, the commonly occurring substances thus play a role in the identification of reactions in a subsystem. Exactly how such reactions are identified is explained further in this section.

7.1.3 Information on substances in subsystems

For each of the substances identified as possibly present the following information can be documented:

- substance name;
- aggregation state;
- quantity present under normal conditions;
- quantity present under abnormal conditions;
- a description field, where additional comments can be entered (such as the conditions under which the substance will be present in abnormal quantities).

The list of substances and reactions in a subsystem is information that is part of the Analysis file. The details of these substances and reactions (their properties) however are data stored in the Substances file. In chapter 2 the relation between the Substances file and the Analysis file was explained.
To add substances or reactions to a subsystem in the Analysis file (or in other words to add the substance or the reaction to the inventory of substances and reactions in the subsystem), a selection can be made out of the substances and reactions defined in the Substances file. Evidently it is also possible to define and add a 'new' substance or reaction to the subsystem. This substance or reaction will also be added to the list in the substances file.

It will therefore be easier to enter a list of substances and reactions in the Substances file first before starting the identification of the substances and reactions in each subsystem.

7.2 Identifying reactions

Similar to the list of substances, a list of reactions can be entered for each subsystem. Just as it is the case for substances, generating a complete inventory of reactions is primarily a matter of identifying *undesired* reactions in a subsystem.

PLANOP supports this part of the hazard analysis by allowing one or more reactions to be assigned to each combination of two substances. In practice, this is done using interaction matrices.

7.2.1 Types of interaction matrices in PLANOP

Interaction matrices are available on different levels in PLANOP:

- the interaction matrix on the level of the Substances file contains all substances of the Substances file (including the commonly occurring substances)
- the interaction matrix on the subsystem level contains all substances identified for that subsystem and also the commonly occurring substances
- the interaction matrix on the substance level is a one dimensional matrix that links the substance under consideration to all the substances of the Substances file (including the commonly occurring substances).

It is recommended to define as many reactions as possible in the interaction matrix of the Substances file. If afterwards substances are identified in a subsystem, these reactions will automatically appear in the interaction matrix for that subsystem.

7.2.2 The interaction matrix for a subsystem

For each subsystem, PLANOP provides a summary of all reactions that have been defined to occur between the various combinations of substances present in the subsystem and between the substances present in the subsystem and the commonly occurring substances. This list contains all the reactions of the interaction matrix for that subsystem. This list does not take the conditions in the subsystem into account. Some of the reactions in this list, even though they may be chemically possible, will only occur under conditions that never can be attained in the subsystem in question. It is thus up to the PLANOP user to select the reactions in this list that could possibly occur in the subsystem (those for which the conditions necessary for the reaction might possibly be attained). These are represented in bold text in the reaction inventory for the subsystem.

The interaction matrix on the subsystem level always includes the commonly occurring substances. Therefore it is not necessary to identify these substances for each subsystem over and over again. It was to this purpose that the concept ‘commonly occurring substances’ was created.

7.3 Investigating the properties of substances

Organisations usually have much information to their disposal regarding substances, for instance in the form of so called ‘material safety data sheets’.

However this information is not always complete or sufficient for the purpose of identifying process accidents. Most MSDS contain little or no information concerning the more ‘complex’ chemical properties of substances.

7.3.1 The list of hazards

To ensure that *all* properties relevant to the causes and consequences of loss of containment, are investigated, PLANOP uses a list of hazards.

The following hazards are defined by default:

- respiratory toxicity
- percutaneous toxicity
- fire and explosion
- decomposition
- polymerisation
- ecotoxicity.

This list can be modified by the user in the maintenance mode. The list of hazards is specific to the opened Substances file. Consequently, different Substances files can have different hazard lists.

The intention is that the applicable hazards are to be indicated for each substance. These hazards thus serve primarily as a checklist for the properties to be investigated.

For a particular substance, additional information for each hazard can be entered in a text field. It is up to the user to determine which information (quantitative or qualitative) is relevant in this regard. For each hazard, it is also possible to define a hyperlink to a document that provides additional clarification (a hazard sheet, an investigation report, a graphic, an article etc.). By generating hyperlinks to existing documents, the PLANOP databases can function as a sort of cataloguing system that allows you to quickly consult this information.

7.3.2 Other information on substances

Apart from these hazards, PLANOP has the possibility to document for each substance the following data:

- the CAS number
- the labelling
- R and S clauses
- an illustration (for example the structural formula of the substance).

For each substance, there is a field for entering any desired supplementary information about the substance. One can also define a hyperlink to an existing document containing more details about the substance (such as a Word document).

As mentioned before, for each substance a one dimensional interaction matrix can be opened This matrix allows defining the possible reactions of this substance with other substances in the Substances file or with commonly occurring substances.

Substance data sheets are not generated for commonly occurring substances. For such substances, it is only necessary to enter a substance name.

7.4 Investigating the properties of reactions

For reactions, there is no concept that is analogous to 'hazards' for substances.

For each reaction there is a text field. In addition an illustration (such as a reaction diagram or a chart showing the course of the reaction) can be entered for each reaction and a hyperlink can be defined to an existing document containing details about the reaction (such as a Word document).

7.5 Event sources and release events for substances and reactions

By allowing event sources and release events to be coupled to substances and reactions, an active link between the hazard analysis and the loss of containment analysis is implemented.

If you add an existing substance or reaction to a subsystem, PLANOP will show a summary of the event sources and release events linked to the substance. You can then select the event sources and release events you want to transfer to the subsystem.

7.5.1 Event sources linked to substances

The event sources that are linked to a substance are typically 'chemical' event sources of type 1 or type 2. Some examples are shown in Table 7.1.

Information about the conditions under which a substance can affect the envelope can be specified in the cause trees for the event sources in question. Some examples are also shown in Table 7.1. Suggestions for measures that can be taken in a subsystem in which these substances are present can also be added to these event sources. Naturally, it will be necessary to further elaborate the causes and measures when such event sources are added to a specific subsystem.

7.5.2 Event sources linked to reactions

It is clear that event sources can also be linked to reactions. For instance, an exothermic reaction can lead to an increase in pressure. Consequently, an exothermic reaction *X* could be linked to the event source 'release of heat by reaction *X*'. The causes can be used to elaborate the conditions under which the reaction will occur and/or under which the maximum amount of heat will be released. If this reaction is added to a subsystem, the event source 'release of heat by reaction *X*' can be incorporated into the subsystem (naturally, accompanied by the underlying information, such as causes and measures). As a result, you will already have a very good basis for further elaborating this event source (such as: how can the self-decomposition temperature be attained, how can rust particles or impurities be present, etc.).

Table 7.1: Examples of event sources for substances and their associated causes

Event sources	Causes
1. Phenomena leading to forces on the envelope	
1.1. Phenomena leading to high pressure	
• The decomposition of … (e.g. ethylene oxide)	The conditions under which the substance decomposes or polymerises, such as a certain minimum temperature, the catalytic effect of rust particles, etc.
• The polymerisation of … (e.g. acrylic acid)	
1.2. Phenomena leading to low pressure	
• The absorption of NH_3 in water	The presence or introduction of water in(to) the subsystem
2. Phenomena threatening the construction materials of the envelope	
2.1. Corrosive or chemically aggressive conditions	
• The corrosive effect of … (e.g. sulphuric acid)	The various concentrations for which the substance exhibits specific corrosive behaviour for specific materials
• The embrittling influence of hydrogen	
2.2. Erosive conditions	
• The erosive effect of … (e.g. chlorine)	The minimum velocity required to cause significant erosion

7.5.3 Release events linked to substances and reactions

Linking release events to substances also makes sense, given the fact that the properties of substances have an important influence on release and dispersion and determine the nature of the resulting loss or damage. For example, the release event 'intoxication resulting from contact with *X*' can be coupled to a substance *X* that is toxic on uptake through the skin. If the use of specific PPE is indicated in order to avoid such intoxication, this can be formulated as a measure for the release event. This way the information is semi-automatically made available to the loss of containment analysis.

Finally, it is also possible to couple release events to reactions.

In this way for each substance and reaction a list can be made of event sources and release events. One could say that every substance and reaction can be equipped with its own Event Source Suggestion List and Release Event Suggestion List.

8

The practical organisation of a PLANOP analysis

In this chapter some practical aspects of performing a PLANOP analysis will be discussed. Of course these are mere suggestions and the optimal organisation of PLANOP studies can differ from one company to another.

8.1 Organising a PLANOP session

It is essential for several experts from different disciplines to be involved in carrying out a risk analysis. Conducting risk analysis meetings with a multidisciplinary group of people is of fundamental importance for the quality of the risk analysis. Naturally, this also applies to PLANOP. Nevertheless, it is not necessary to do everything in a group environment, since the amount of time available for the activities of the group is usually scarce and valuable and must be employed in the best possible manner.

Consequently, certain parts of the PLANOP analysis should be performed by a single person or a limited number of persons, in preparation for the group sessions. These are the following parts:

- generating the PLANOP files
- inputting substances and reactions and filling in the Substance data sheets and Reaction data sheets
- defining the installations and subdividing the installations into sections and subsystems.

The following parts of the actual analysis can also be prepared in advance:

- identifying the substances and reactions in the subsystems (particularly substances that are normally present);
- identifying the event sources and release events;
- inputting measures (existing measures and suggestions for new measures).

This preparatory work is then to be evaluated and further elaborated in the team environment. This information can be presented directly from the PLANOP program using a data projector, or the necessary printed reports can be provided to the participants.

8.2 Integrating PLANOP into the design process

As explained in chapter 1, PLANOP is very well suited to be used during projects designing or modifying installations. The database structure of the information allows gradually increasing the level of detail.

In practice, PLANOP can be merged into the design process as follows. First, a person is appointed to act as the PLANOP coordinator. This person's role is to work out the PLANOP structure as much as possible, in accordance with the available data. At regular intervals (such as at the various stages defined in the design process), the design team is called together to evaluate and adapt this information. Naturally, different PLANOP coordinators can be employed in different project phases.

If the conceptual design is subjected to a verification technique, such as a HAZOP study, it is a good idea to add any additional risks and/or supplementary measures identified by such a study to the PLANOP data structure, in order to maintain a complete overview of the risks and measures. Naturally, this also applies to the results of any other type of analysis performed during the lifetime of the installation.

The editorial review of this document was concluded on April 29th 2005

Authors: ir. Koen Biermans and ir. Peter Vansina

Reference: CRC/IN/012-E
Version: 2.0

Distribution: Department of the Supervision of Chemical risks
Publisher: FPS Employment, Labour and Social Dialogue

Legal depot: D/2005/1205/25