IEC 61882

Edition 2.0 2016-03

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

## Hazard and operability studies (HAZOP studies) – Application guide

## Études de danger et d'exploitabilité (études HAZOP) – Guide d'application

IEC 61882:2016-03(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch


**About the IEC**
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

**About IEC publications**
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

**IEC Catalogue - webstore.iec.ch/catalogue**
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

**IEC publications search - www.iec.ch/searchpub**
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

**IEC Just Published - webstore.iec.ch/justpublished**
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

**Electropedia - www.electropedia.org**
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

**IEC Glossary - std.iec.ch/glossary**
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

**IEC Customer Service Centre - webstore.iec.ch/csc**
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

---

**A propos de l'IEC**
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

**A propos des publications IEC**
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

**Catalogue IEC - webstore.iec.ch/catalogue**
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

**Recherche de publications IEC - www.iec.ch/searchpub**
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

**IEC Just Published - webstore.iec.ch/justpublished**
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

**Electropedia - www.electropedia.org**
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

**Glossaire IEC - std.iec.ch/glossary**
65 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

**Service Clients - webstore.iec.ch/csc**
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 61882

Edition 2.0 2016-03

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

## Hazard and operability studies (HAZOP studies) – Application guide

## Études de danger et d'exploitabilité (études HAZOP) – Guide d'application

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 03.100.50; 03.120.01; 13.020.30

ISBN 978-2-8322-3208-8

# CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

# HAZARD AND OPERABILITY STUDIES (HAZOP STUDIES) – APPLICATION GUIDE

## FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61882 has been prepared by IEC technical committee 56: Dependability.

This second edition cancels and replaces the first edition published in 2001. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) clarification of terminology as well as alignment with terms and definitions within ISO 31000:2009 and ISO Guide 73:2009;
b) addition of an improved case study of a procedural HAZOP.

The text of this standard is based on the following documents:

| FDIS | Report on voting |
|---|---|
| 56/1653/FDIS | 56/1666/RVD |

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

# INTRODUCTION

This standard describes the principles for and approach to guide word-driven risk identification. Historically this approach to risk identification has been called a hazard and operability study or HAZOP study for short. This is a structured and systematic technique for examining a defined system, with the objectives of:

- identifying risks associated with the operation and maintenance of the system. The hazards or other risk sources involved can include both those essentially relevant only to the immediate area of the system and those with a much wider sphere of influence, for example some environmental hazards;
- identifying potential operability problems with the system and in particular identifying causes of operational disturbances and production deviations likely to lead to non-conforming products.

An important benefit of HAZOP studies is that the resulting knowledge, obtained by identifying risks and operability problems in a structured and systematic manner, is of great assistance in determining appropriate remedial measures.

A characteristic feature of a HAZOP study is the examination session during which a multi-disciplinary team under the guidance of a study leader systematically examines all relevant parts of a design or system. It identifies deviations from the system design intent utilizing a set of guide words. The technique aims to stimulate the imagination of participants in a systematic way to identify risks and operability problems. A HAZOP study should be seen as an enhancement to sound design using experience-based approaches such as codes of practice rather than a substitute for such approaches.

Historically, HAZOP and similar studies were described as hazard identification as their primary purpose is to test in a systematic way whether hazards are present and, if so, understand both how they could result in adverse consequences and how such consequences could be avoided through process redesign. ISO 31000:2009 defines risk as the effect of uncertainty on objectives, with a note that an effect is a deviation from the expected. Therefore HAZOP studies, which consider deviations from the expected, their causes and their effect on objectives in the context of process design, are now correctly characterized as powerful risk identification tools.

There are many different tools and techniques available for the identification of risks, ranging from checklists, failure modes and effects analysis (FMEA) to HAZOP. Some techniques, such as checklists and what-if/analysis, can be used early in the system life cycle when little information is available, or in later phases if a less detailed analysis is needed. HAZOP studies require more detail regarding the systems under consideration, but produce more comprehensive information on risks and weaknesses in the system design.

The term HAZOP is sometimes associated, in a generic sense, with some other hazard identification techniques (e.g. checklist HAZOP, HAZOP 1 or 2, knowledge-based HAZOP). The use of the term with such techniques is considered to be inappropriate and is specifically excluded from this document.

Before commencing a HAZOP study, it should be confirmed that it is the most appropriate technique (either individually or in combination with other techniques) for the task in hand. In making this judgment, consideration should be given to the purpose of the study, the possible severity of any consequences, the appropriate level of detail, the availability of relevant data and resources and the needs of decision-makers.

This standard has been developed to provide guidance across many industries and types of system. There are more specific standards and guides within some industries, notably the process industries where the technique originated, which establish preferred methods of application for these industries. For details see the bibliography at the end of this standard.

# HAZARD AND OPERABILITY STUDIES (HAZOP STUDIES) – APPLICATION GUIDE

## 1 Scope

This International Standard provides a guide for HAZOP studies of systems using guide words. It gives guidance on application of the technique and on the HAZOP study procedure, including definition, preparation, examination sessions and resulting documentation and follow-up.

Documentation examples, as well as a broad set of examples encompassing various applications, illustrating HAZOP studies are also provided.

## 2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050-192, *International electrotechnical vocabulary – Part 192: Dependability* (available at http://www.electropedia.org)

## 3 Terms, definitions and abbreviations

### 3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050-192 and the following apply.

NOTE Within this clause, the terms defined are in *italic* type.

**3.1.1**
**characteristic**
qualitative or quantitative property

EXAMPLE Pressure, temperature, voltage.

**3.1.2**
**consequence**
outcome of an event affecting objectives

Note 1 to entry: An event can lead to a range of consequences.

Note 2 to entry: A consequence can be certain or uncertain and can have positive or negative effects on objectives.

Note 3 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 4 to entry: Initial consequences can escalate through knock-on effects.

[SOURCE: ISO Guide 73:2009, 3.6.1.3]

**3.1.3**
**control**
measure that is modifying *risk* (3.1.12)

Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

[SOURCE: ISO Guide 73:2009, 3.8.1.1]

**3.1.4**
**design intent**
designer's desired, or specified range of behaviour for properties which ensure that the item fulfills its requirements

**3.1.5**
**property**
constituent of a part which serves to identify the part's essential features

Note 1 to entry: The choice of properties can depend upon the particular application, but properties can include features such as the material involved, the activity being carried out, the equipment employed, etc. Material should be considered in a general sense and includes data, software, etc.

**3.1.6**
**guide word**
word or phrase which expresses and defines a specific type of deviation from a property's design intent

**3.1.7**
**harm**
physical injury or damage to the health of people or damage to assets or the environment

**3.1.8**
**hazard**
source of potential *harm* (3.1.7)

Note 1 to entry: Hazard can be a *risk source* (3.1.14).

[SOURCE: ISO Guide 73:2009, 3.5.1.4]

**3.1.9**
**level of risk**
magnitude of a *risk* (3.1.12) or combination of risks, expressed in terms of the combination of *consequences* (3.1.2) and their likelihood

[SOURCE: ISO Guide 73:2009, 3.6.1.8]

**3.1.10**
**manager**
person with responsibility for a project, activity or organization.

**3.1.11**
**part**
section of the system which is the subject of immediate study

Note 1 to entry: A part can be physical (e.g. hardware) or logical (e.g. step in an operational sequence).

**3.1.12**
**risk**
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected – positive and/or negative.

Note 2 to entry: Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

Note 3 to entry: Risk is often characterized by reference to potential events and *consequences* (3.1.2) or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

Note 5 to entry: Uncertainty is the state, even partial, or deficiency of information related to, understanding or knowledge of an event, its *consequence*, or likelihood.

[SOURCE: ISO Guide 73:2009, 1.1]

**3.1.13**
**risk identification**
process of finding, recognizing and describing *risks* (3.1.12)

Note 1 to entry: Risk identification involves the identification of *risk sources* (3.1.14), events, their causes and their potential *consequences* (3.1.2).

Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs.

[SOURCE: ISO Guide 73:2009, 3.5.1]

**3.1.14**
**risk source**
element which alone or in combination has the intrinsic potential to give rise to *risk* (3.1.12)

Note 1 to entry: A risk source can be tangible or intangible.

[SOURCE: ISO Guide 73:2009, 3.5.1.2]

**3.1.15**
**risk treatment**
process to modify *risk* (3.1.12)

Note 1 to entry: Risk treatment can involve:

– avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
– taking or increasing risk in order to pursue an opportunity;
– removing the *risk source* (3.1.14);
– changing the likelihood;
– changing the *consequences* (3.1.2);
– sharing the risk with another party or parties (including contracts and risk financing); and
– retaining the risk by informed decision.

Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

Note 3 to entry: Clarification of risk treatment and risk *control* (3.1.3) – a risk control is already in place whereas a risk treatment is an activity to improve risk controls. Hence, an implemented treatment becomes a control.

[SOURCE: ISO Guide 73:2009, 3.8.1, modified — Note 3 to entry replaces the existing note 3]

## 3.2 Abbreviations

ATP automatic train protection
EER escape, evacuation and rescue
ETA event tree analysis

| | |
|---|---|
| FMEA | failure mode and effects analysis |
| FTA | fault tree analysis |
| GPA | general purpose alarm |
| HAZOP | hazard and operability |
| LH | left hand |
| LOPA | layer of protection analysis |
| OIM | offshore installation manager |
| P&IDs | process and instrumentation diagrams |
| PAPA | prepare to abandon platform alarm |
| PA | public address |
| PES | programmable electronic system |
| PPE | personal protective equipment |
| QP | qualified person |
| RH | right hand |

# 4 Key features of HAZOP

## 4.1 General

A HAZOP study is a detailed process carried out by a dedicated team to identify risks and operability problems. HAZOP studies deal with the identification of potential deviations from the design intent, examination of their possible causes and assessment of their consequences.

Key features of a HAZOP study include the following.

- The study is a creative process that proceeds by systematically using a series of guide words to identify potential deviations from the design intent and employing these to stimulate team members to envisage how the deviation might occur and what might be the consequences.
- The study is carried out under the guidance of a trained and experienced study leader, who has to ensure comprehensive coverage of the system under study, using logical, analytical thinking. The study leader is preferably assisted by a recorder who records pertinent data associated with identified risks and/or operational disturbances for risk analysis, evaluation and treatment.
- The study relies on specialists from various disciplines with appropriate skills and experience who display intuition and good judgement.
- The study should be carried out in an atmosphere of critical thinking in a frank and open atmosphere.
- A HAZOP study produces minutes or software to record the deviations, their causes, consequences and recommended actions together with marked up drawings, documents or other representations of the system that indicate the associated minute number and where possible the recommended action.
- The development of risk treatment actions for identified risks or operability problems is not a primary objective of the HAZOP examination, but recommendations should be made where appropriate and recorded for consideration by those responsible for the design of the system.
- The initial HAZOP study might be done in a progressive fashion so that design changes can be incorporated but the completed HAZOP study has to correlate to the final design intent.

- Existing HAZOP studies should be reviewed at regular intervals to evaluate whether there have been any changes to the design intent or hazards and also during other stages in the life cycle such as the enhancement stage.

### 4.2 Principles of examination

The basis of a HAZOP study is a “guide word examination” which is a deliberate search for deviations from the design intent. To facilitate the examination, a system is divided into parts in such a way that the design intent or function for each part can be adequately defined. The size of the part chosen is likely to depend on the complexity of the system and the potential magnitude and significance of the consequence. In complex systems or those where the level of risk might be expected to be high, the parts are likely to be small in comparison to the system. In simple systems or those where the level of risk might be expected to be low, the use of larger parts will expedite the study.

The design intent for a given part of a system is expressed in terms of properties, which convey the essential characteristics of the part and which represent natural divisions of the part. The selection of properties to be examined is to some extent a subjective decision in that there might be several combinations which will achieve the required purpose and the choice can also depend upon the particular application. Parts can be discrete steps or stages in a procedure, clauses in a contract, individual signals and equipment items in a control system, equipment or components in a process or electronic system, etc.

In some cases it might be helpful to express the function of a part in terms of:

– the input material taken from a source;

– an activity which is performed on that material;

– an output which is taken to a destination.

Thus the design intent will contain the following elements: inputs and outputs, functions, activities, sources and destinations, which can be viewed as properties of the part.

Properties can often be usefully defined further in terms of characteristics that can be either quantitative or qualitative. For example, in a chemical system, the inputs could be defined further in terms of characteristics such as temperature, pressure and composition. For a transport activity, characteristics such as the rate of movement, the load or the number of passengers might be relevant. For computer-based systems, communication, interfaces, and data processing are likely to be the characteristic of each part.

For each part in turn, the HAZOP study team examines each property for deviation from the design intent which can lead to undesirable (or desirable) consequences. The identification of deviations from the design intent is achieved by a questioning process using predetermined guide words. The role of the guide word is to stimulate imaginative thinking, to focus the study and elicit ideas and discussion, thereby maximizing the chances of study completeness. An example of basic guide words and their meanings is given in Table 1.

**Table 1 – Example of basic guide words and their generic meanings**

| Guide word | Meaning |
|---|---|
| NO OR NOT | Complete negation of the design intent |
| MORE | Quantitative increase |
| LESS | Quantitative decrease |
| AS WELL AS | Qualitative modification/increase |
| PART OF | Qualitative modification/decrease |
| REVERSE | Logical opposite of the design intent |
| OTHER THAN | Complete substitution |

A further example of additional guide words relating to clock time and order or sequence is given in Table 2.

**Table 2 – Example of guide words relating to clock time and order or sequence**

| Guide word | Meaning |
|---|---|
| EARLY | Relative to the clock time |
| LATE | Relative to the clock time |
| BEFORE | Relating to order or sequence |
| AFTER | Relating to order or sequence |

Additional guide words can be used to facilitate identification of deviation, provided they are identified before the examination commences.

Having selected a part for examination, the design intent of that part is specified in terms of discrete properties. Each relevant guide word is then applied to each property, thus a thorough search for deviations is carried out in a systematic manner. Having applied a guide word, possible causes and consequences of a given deviation are examined and mechanisms for control of the predicted consequences can also be investigated. The results of the examination are recorded in an agreed format (see 6.5.2).

Guide word/property associations can be regarded as a matrix. Within each cell of the matrix thus formed will be a specific guide word/property combination. To achieve a comprehensive risk identification, it is necessary that the properties cover all aspects of the design intent and guide words cover all possible deviations. Not all combinations will give credible deviations, so the matrix can have several empty spaces when all guide word/property combinations are considered.

In general the study leader will predefine the applicable guide word/property combinations to make the risk identification process more efficient and make best use of the participant expertise and time.

There are two possible sequences in which the cells of the matrix can be used for the examination of the chosen part: column by column (i.e. property first), or row by row (i.e. guide word first). The details of examination are outlined in 6.4 and both forms of examination are illustrated in Figures 2 and 3. In principle the results of the examination should be the same.

As well as applying guide words to defined properties of a part there can be other attributes such as access, isolation, control, and the work environment (noise, lighting, etc.) that are important to the desired operation of the system and to which a subset of the guide words can be applied.

### 4.3 Design representation

#### 4.3.1 General

An accurate and complete design representation of the system under study is a prerequisite to the examination task. A design representation is a descriptive model of the system adequately describing the system under study, its parts and identifying their properties. The representation could be of the physical design or of the logical design and it should be made clear what is represented.

The design representation should convey the system function of each part and element in a qualitative or quantitative manner. It should also describe the interactions of the system with other systems, with its operator/user and possibly with the environment. For example, P&IDs are likely to provide the level of detail required for the design representation. The

conformance of properties or characteristics to their design intent determines the correctness of operations and in some cases the safety of the system.

The representation of the system consists of two basic components:

– the system requirements; and
– a physical and/or logical description of the design.

The value of a HAZOP study depends on the completeness, adequacy and accuracy of the design representation including the design intent. Any modifications from the original design should be shown in the design representation. Before starting the examination, the team should review this information package, and if necessary have it revised so that it accurately represents the system.

### 4.3.2 Design requirements and design intent

The design requirements consist of qualitative and quantitative requirements that the system has to satisfy, and provide the basis for development of system design and design intent. All reasonably foreseen ways in which the system could be used or misused should be identified. Both the design requirements and resulting design intent have to meet customer requirements and those of any relevant legislation, norms or standards.

On the basis of system requirements, a designer develops the system design; for instance, a system configuration is arrived at, and specific functions are assigned to subsystems and components. Components are specified and selected. The designer should not only consider what the system should do, but also ensure that it will not fail under any foreseeable set of conditions, or that it will not fail or degrade during the specified lifetime. Undesirable behaviours or features should also be identified so they can be designed out, or their effects minimized by appropriate design or maintenance.

The design intent forms a baseline for the examination and should be accurate and correct, as far as possible. The verification of design intent (see IEC 61160) is outside of the scope of the HAZOP study, but the study leader should ascertain that it is accurate and correct to allow the study to proceed. In general most documented design intents are limited to basic system functions and parameters under normal operating conditions.

Reasonably foreseeable abnormal operating conditions and undesirable activities that might occur (e.g., severe vibrations, extreme weather events, abnormal stoppages or third party interventions) should be identified and considered during the examination. Also deterioration mechanisms such as decay, corrosion and non-compliance of procedures and other mechanisms which cause deterioration in system properties should be identified and considered in a study using appropriate guide words. If necessary, a more detailed study looking specifically at failure modes and effects may be required (see IEC 60812).

Expected life, reliability, maintainability and supportability should also be identified and considered together with risk sources which could be encountered during maintenance and logistic support activities, provided they are included in the scope of the HAZOP study.

## 5 Applications of HAZOP

### 5.1 General

Originally a HAZOP study was a technique developed for systems involving the treatment of a fluid medium or other material flow in the process industries where it is now a major element of process safety management. However its area of application has steadily widened in recent years and for example includes usage for:

– software applications including programmable electronic systems;

– systems involving the movement of people by transport modes such as road, rail, and air;
– examining different operating sequences and procedures;
– assessing administrative procedures in different industries;
– assessing specific systems, for example medical devices;
– software and code development;
– assessing proposed organizational change and defining the mechanisms to achieve those changes;
– testing and improving draft contracts and other legal documents;
– testing and improving documents including instructions and procedures for critical activities.

A HAZOP study is particularly useful for identifying weaknesses in systems (existing or proposed) involving the flow of materials, people or information, or a number of events or activities in a planned sequence or the procedures controlling such a sequence. HAZOP studies can also be used for non-operational conditions such as storage and transport. As well as being a valuable tool in the design and development of new systems, HAZOP can also be profitably employed to identify risks and potential problems associated with different operating states of a given system: for example, for start-up, standby, normal operation, normal shutdown, emergency shutdown states. It can also be employed for batch and unsteady-state processes and sequences as well as for continuous ones. HAZOP is an integral part of the overall design process and one of the methods that can be employed for risk identification as part of the risk management process (see ISO 31000).

### 5.2 Relation to other analysis tools

A HAZOP study can be used in conjunction with other risk identification and analysis methods (see IEC/ISO 31010) such as FMEA (see IEC 60812) and FTA (see IEC 61025) or LOPA (see IEC 61511-3:2003, Annex F). Such combinations might be utilized in situations when:

– the HAZOP study clearly indicates that the performance of a particular component of a system is critical and needs to be examined in greater depth; the HAZOP study can then be usefully complemented by an FMEA of that component;
– having examined single property deviations by a HAZOP study, it is decided to use FTA and ETA to analyse the effect of multiple deviations or to quantify the likelihood of the failure event and its consequences.

FMEA starts with a possible component/function failure and then proceeds to investigate the consequences of this failure on the system as a whole. Thus the investigation is unidirectional, from cause to consequence. A HAZOP study, on the other hand, is concerned with identifying possible deviations from the design intent and then proceeds to find the potential causes of the deviation and to predict its consequences.

FTA may be used after single property deviations have been identified by HAZOP, to analyse the effect of multiple deviations or to quantify the likelihood of the failure event and its consequences.

LOPA uses the data developed by HAZOP and documents the initiating cause and the protection layers that modify the risk. This can then be used to determine the amount of risk reduction achieved by existing controls and to ascertain whether further treatment is needed.

### 5.3 HAZOP study limitations

Whilst HAZOP studies have proved to be extremely useful in a variety of different industries, the technique has limitations that should be taken into account when considering a potential application. Some of the limitations are mentioned below.

- A HAZOP study is a risk identification technique which considers system parts individually and methodically examines the effects of deviations on each part. Sometimes a very high risk will involve the interaction between several of parts of the system. In these cases the risk should be analysed in more detail using techniques such as ETA (see IEC 62502) and FTA (see IEC 61025).
- As with any technique for the identification of risks or operability problems, there can be no guarantee that all will be identified in a HAZOP study. The study of a complex system should not, therefore, depend just upon a HAZOP study. The technique should be used in conjunction with other suitable approaches and other relevant studies should be coordinated within an effective, overall management system.
- Many systems are highly interlinked, and a deviation in one part can have causes and consequences in other parts of the system. To understand the risk and take appropriate risk treatment actions, the causes and consequences have to be followed across the system. However, where the system is highly interlinked there is a danger that the follow through is not comprehensive of every eventuality and a more rigorous event analysis might be required.
- The success of a HAZOP study depends greatly on the ability and experience of the study leader and the knowledge, experience and level of interaction between team members.
- A HAZOP study can only consider those parts that appear on the design representation. Activities and operations which do not appear on the representation might not always be considered. This can be partially overcome by applying a set of additional, non-specific guide words to a part that are not strictly properties, such as access and maintenance and also by adding to the process a step whereby, on completion, a final ‘common sense check’ is applied using a checklist.

### 5.4 Risk identification studies during different system life cycle stages

#### 5.4.1 Concept stage

In the concept phase of a system’s life cycle, the design concept and major system parts are decided but the detailed design and documentation required to conduct the HAZOP study do not exist. However, it is necessary to identify major risks at this time, to allow them to be considered in the design process and to facilitate future HAZOP studies. To carry out these studies, other basic methods should be used (for example descriptions of some of these methods see IEC/ISO 31010).

#### 5.4.2 Development stage

The most cost effective time to carry out a HAZOP study is when the detailed design is available and methods of operation have been decided upon. There can be several iterations as the design is being finalized. It is important to have a process that will assess the implications of any changes made after the study has been carried out. This process should be maintained throughout the life of the system.

#### 5.4.3 Realization stage

During the realization phase, it is advisable to carry out an additional study prior to commissioning, when initial operation or start-up of the system can lead to significant levels of risk and proper operating sequences and instructions are critical. The study should also be carried out or repeated when there has been a substantial change of design or intent at a later stage. Additional data such as commissioning and operating instructions should be available at this time. In addition, the study should also review all actions raised during earlier studies to ensure that these have been completed.

#### 5.4.4 Utilization stage

The application or update of a HAZOP study should be considered before implementing any changes that could affect the normal operation of a system, particularly if these changes

could lead to high levels of risk. Periodically, the system should also be studied to detect and understand the effects and implications of slowly acting changes. It is important that the design documentation and operating instructions used in such a study are up to date.

### 5.4.5 Enhancement stage

The enhancement stage is concerned with improving performance, making changes to respond to new operating conditions, extending operating life and addressing obsolescence. HAZOP studies can be used to understand the implications of any proposed changes to judge if they are acceptable and whether new controls or changes to existing controls are required. When conducting studies to identify risks associated with any proposed changes it is important to consider the implications and responses for the whole system and not just restrict the study to the part or property being changed.

### 5.4.6 Retirement stage

In the retirement stage, a study of activities related to decommissioning, cessation of use or disposal might be required if it leads to different risks from those in normal operations. Once the sequence of activities has been defined HAZOP studies can be applied to the sequence and procedures as well as any interim operating modes.

## 6 The HAZOP study procedure

### 6.1 General

HAZOP studies consist of four basic sequential steps, shown in Figure 1.

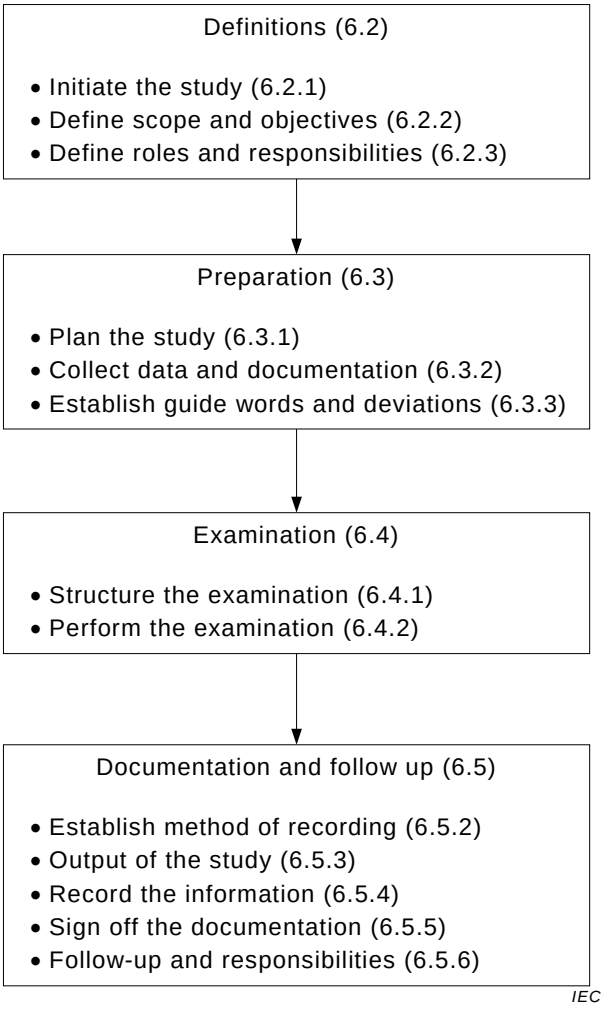


**Figure 1 – The HAZOP study procedure**

## 6.2 Definitions

### 6.2.1 Initiate the study

The study is generally initiated by a person with responsibility for a project, activity or organisation, who in this guide is called the manager. The manager should determine when a study is required, appoint a study leader and provide the necessary resources to carry it out.

The need for such a study will often have been identified during planning, due to legal requirements or because it is an organization's policy. With the assistance of the study leader, the manager should define the scope and objectives of the study and ensure that members appointed to the study team have the appropriate competencies to undertake the study.

The manager is ultimately accountable for ensuring that any actions that arise from the study are completed.

### 6.2.2 Define scope and objectives

The scope of a study should be clearly stated, to ensure that:

– the system boundaries, and its interfaces with other systems and the environment are clearly defined; and

– the study team is focused, and does not stray into aspects irrelevant to the objectives.

The scope will depend upon a number of factors, including:

– the boundaries and extent of the system;
– the number and level of detail of the design representations available;
– the scope of any previous studies carried out on the system; and
– any regulatory requirements, standards or norms which are applicable to the system.

The following factors should be considered when defining objectives of the study:

– the relevant objectives of the organization;
– the purpose for which the results of the study will be used and how it relates to the organization’s objectives;
– the phase of the life cycle at which the study is to be carried out (for details see 5.4);
– operability considerations, including effects on product quality;
– persons or property that may be at risk, for example staff, the general public, the environment, the system;
– the performance requirements of the system.

### 6.2.3 Define roles and responsibilities

The roles and responsibilities of a study team should be clearly defined by the manager and agreed with the study leader at the outset of the study. The study leader should review the design representation to determine what information is available and what skills are required from the study team members. A programme of activities should be developed, which reflects the timing of decision making, to enable any recommendations to be carried out in a timely fashion.

It is the study leader's responsibility to ensure that a suitable mechanism is in place to communicate the results of the study. It is the responsibility of the manager to ensure that the results of the study are followed up and decisions regarding necessary actions are properly documented.

The manager and the study leader should agree whether the study team activity is to be confined to identification of risks and problem areas (which are then referred back to the manager and any designers for resolution) or whether they are also to suggest possible risk treatments. In the latter case there also needs to be agreement as to the responsibility and mechanism for selecting preferred risk treatments and securing appropriate authorization for any actions that have to be taken.

A HAZOP study is a team effort, with each team member being chosen for a defined role. The team should be as small as possible and consistent with the relevant skills and experience available. The larger the team, the slower the process, however, all relevant areas of knowledge should be represented.

Where a system has been designed by a contractor, the study team should contain personnel from both the contractor and the client.

Recommended roles for team members are as follows:

– **Study leader**: not closely associated with the design team and the project. Trained and experienced in leading HAZOP studies. Responsible for communications between management and the study team. Plans the study. Agrees study team composition. Ensures the study team is supplied with a design representation package. Suggests guide words and guide word/property combinations to be used in the study. Facilitates the study. Ensures accurate recording of the results.

– **Recorder**: records proceedings of meetings. Documents the risks and problem areas identified, recommendations made and any proposed actions. Assists the study leader in planning and administrative duties. In some cases, the study leader can carry out this role. The recorder should have good technical knowledge of the subject being studied, linguistic skills and a good ability to listen and understand.
– **Designer(s)**: explains the design and its representation. Explains how a defined deviation can occur and the corresponding system or organizational response.
– **User(s)**: explains the operational context within which the system will operate, the operational consequences of a deviation and the extent to which deviations might lead to unacceptable consequences.
– **Specialists**: provide expertise relevant to the system, the study, the hazards and their consequences. They could be called upon for limited participation.
– **Maintainer**: someone who will maintain the system going forward.

Other people such as suppliers of major system items, manufacturer, and other stakeholders might also be needed.

The viewpoint of the designer and user are always required for the study. However, depending on the particular phase of the life cycle in which the study is carried out, the type of specialists most appropriate to the study might vary.

Either all team members should have sufficient knowledge of the HAZOP methodology to enable them to participate effectively in the study, or suitable training should be provided.

### 6.3 Preparation

#### 6.3.1 Plan the study

The study leader is responsible for the following preparatory work:

a) obtaining the information about the system;
b) converting the information into a suitable format;
c) planning the sequence of the study meetings or workshops; and
d) arranging the necessary meetings.

In addition, the study leader might arrange for a search to be made of databases, etc. to describe historical experience of the same or similar systems.

The study leader is responsible for ensuring that an adequate design representation is available. If the design representation is flawed or incomplete, it should be corrected before the study begins. In the planning stage of a study, the parts and properties should be identified and agreed with a person very familiar with the design.

The study leader is responsible for the preparation of a study plan that should contain the following:

- objectives and scope of the study;
- the study team;
- technical details:
  – a design representation divided into parts with defined design intent and for each part, a list of components, materials and activities and their properties;
  – a list of proposed guide words to be used, and their application to systems properties as outlined in 6.4.3;
- a list of appropriate reference, design criteria, standards or norms;

- administrative arrangements, schedule of meetings, including their dates and times and locations;
- form of recording required (see Annex A); and
- adequate room facilities and visual and recording aids should be provided to facilitate efficient conduct of the meetings.

A briefing package consisting of the study plan and necessary references should be sent to the study team members in advance of the first meeting to allow them to familiarize themselves with its content. A physical review of the system is desirable.

The success of the study strongly depends on the alertness and concentration of the team members and it is therefore important that the sessions are not too long and that there are appropriate intervals between sessions. How these requirements are achieved is ultimately the responsibility of the study leader.

### 6.3.2 Collect data and documentation

Typically this can consist of some of the following documentation that should be clearly and uniquely identified, approved and dated:

a) for all systems:
   – design intentions, requirements and descriptions;
b) for hardware systems:
   – flow sheets, functional block diagrams, control diagrams, interfaces, electrical circuit diagrams, engineering data sheets, arrangement drawings, 3D models (where available), utilities specifications, operating and maintenance requirements and instructions;
c) for process flow systems:
   – piping/process and instrumentation diagrams, material specifications and standards equipment, piping and system layout;
d) for programmable electronic systems:
   – data flow diagrams, object-oriented design diagrams, state transition diagrams, timing diagrams, logic diagrams;
e) for procedure or document related systems:
   – draft documents;
   – results of any task analyses or operational breakdown matrices.

In addition, the following information might also be provided:

– the extent and location of the boundaries of the system being studied and the interfaces at the borders;
– information about the external and internal environment in which the system will operate;
– operating and maintenance arrangements for the system;
– information about user interface design;
– historical experience with similar systems.

### 6.3.3 Establish guide words and deviations

In the planning stage of a HAZOP study, the study leader should propose an initial list of guide words to be used. The study leader should test the proposed guide words against the system and confirm their adequacy. The choice of guide words should be considered carefully, as a guide word which is too specific can limit ideas and discussion, and one which is too general might not focus the HAZOP study efficiently. Some examples of different types of deviation and their associated guide words are given in Table 3.

**Table 3 – Examples of deviations and their associated guide words**

| Deviation type | Guide word | Example interpretation for process industry | Example interpretation for a programmable electronic system, PES |
|---|---|---|---|
| Negative | NO | No part of the intention is achieved, e.g. no flow | No data or control signal passed |
| Quantitative modification | MORE | A quantitative increase, e.g. higher temperature | Data is passed at a higher rate than intended |
| | LESS | A quantitative decrease e.g. lower temperature | Data is passed at a lower rate than intended |
| Qualitative modification | AS WELL AS | Impurities present Simultaneous execution of another operation/step | Some additional or spurious signal is present |
| | PART OF | Only some of the intention is achieved, i.e. only part of an intended fluid transfer takes place | The data or control signals are incomplete |
| Substitution | REVERSE | Covers reverse flow in pipes and reverse chemical reactions | Normally not relevant |
| | OTHER THAN | A result other than the original intention is achieved, i.e. transfer of wrong material | The data or control signals are incorrect |
| Time | EARLY | Something happens early relative to clock time, e.g. cooling or filtration | The signals arrive too early with reference to clock time |
| | LATE | Something happens late relative to clock time, e.g. cooling or filtration | The signals arrive too late with reference to clock time |
| Order or sequence | BEFORE | Something happens too early in a sequence, e.g. mixing or heating | The signals arrive earlier than intended within a sequence |
| | AFTER | Something happens too late in a sequence, e.g. mixing or heating | The signals arrive later than intended within a sequence |

Guide word/property combinations can be interpreted differently in studies of different systems, at different phases of the system life cycle, and when applied to different design representations. Some of the combinations might not have meaningful interpretations for a given study and should be disregarded. Generally the study leader will predefine the appropriate guide word/property combinations for the study. The interpretation of all guide word/property combinations should be defined and documented. If a given combination has more than one sensible interpretation in the context of the design, all interpretations should be listed. On the other hand, it can also be found that the same interpretation is derived from different combinations. When this occurs, appropriate cross-references should be made.

## 6.4 Examination

### 6.4.1 Structure the examination

The examination sessions should be structured, with the study leader facilitating the discussion and following the study plan. At the start of a study meeting the study leader or a team member who is familiar with the process to be examined and its problems should:

- outline the study plan, to ensure that the team is familiar with the system and objectives and scope of the study;
- outline the design representation and explain the proposed guide words and properties to be used;
- review any previously identified risks and operational problems and potential areas of concern.

### 6.4.2 Perform the examination

The analysis should follow the flow or sequence related to the subject of the analysis, tracing inputs to outputs in a logical sequence. There are two possible sequences of examination: ‘property first’ and ‘guide word first’, as shown in Figures 2 and 3 respectively. The study leader and team should agree which sequence to use. The decision will be influenced by the detailed manner in which the HAZOP examination is conducted. Other factors involved in the decision include the nature of the technologies involved, the need for flexibility in the conduct of the examination and, to some extent, the training which the participants have received.

The ‘property first’ sequence is described below.

a) The study leader starts by selecting a part of the design representation as a starting point and marking it. The design intent of the part is then explained and the relevant properties identified.

b) The study leader chooses one of the properties and agrees with the team whether the guide word should be applied directly to the term itself or to the characteristics of that property. The study leader identifies which guide word is to be applied first.

c) The first applicable guide word interpretation is examined in the context of the property or characteristic being studied in order to see if there is a possible deviation from the design intent. If a possible deviation is identified, it is examined for possible causes and consequences.

d) The team should identify whether any control will be present that will detect and/or indicate a deviation or respond to it, which could be included within the selected part or other parts of the system. The presence of such controls should not stop the risk or operability problem being identified or for further risk treatment to be specified.

e) The team should specify the actions required to treat the risk if appropriate. Recommended change should be marked up on the representation and taken into account as the study proceeds. If necessary a completed part should be re-examined as a result of a change in another part.

f) The study leader should summarize the results as they are being recorded by the recorder. Where there is a need for additional follow-up work, the name of the person responsible for ensuring that the work is carried out should also be recorded. The progress of the study should also be recorded at the end of a study session.

g) The process is then repeated for any other interpretation for that guide word; then for another guide word; then for each property of the part under study. After a part has been fully examined, it should be marked as completed. The process is repeated until all parts have been studied.

At the completion of the study of each part of the system, the team is invited to consider any other attributes such as access, isolation, control, and the work environment (noise, lighting, etc.) that are important to the desired operation of the system. This could involve the consideration of the system as a whole as opposed to dealing with each part in isolation.

An alternative method of guide word application to that described above, is to apply the first guide word to each of the properties that apply to a part in turn. When this has been completed, the study proceeds with the next guide word which again is applied to all properties in turn. The process is repeated until all the guide words have been used for all the properties that apply to a particular part before moving on to another part (see Figure 3).

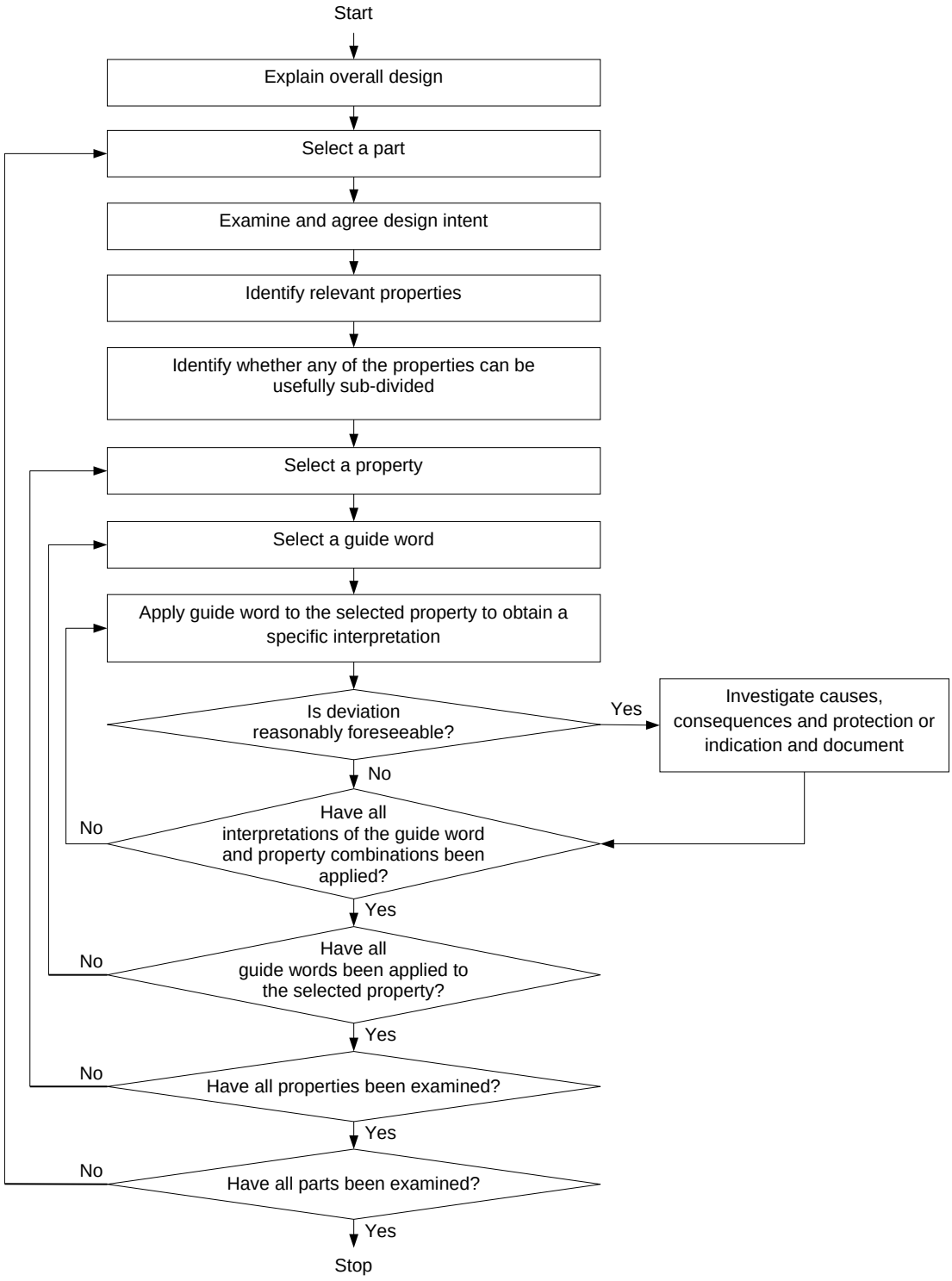


**Figure 2 – Flow chart of the HAZOP examination procedure – Property first sequence**

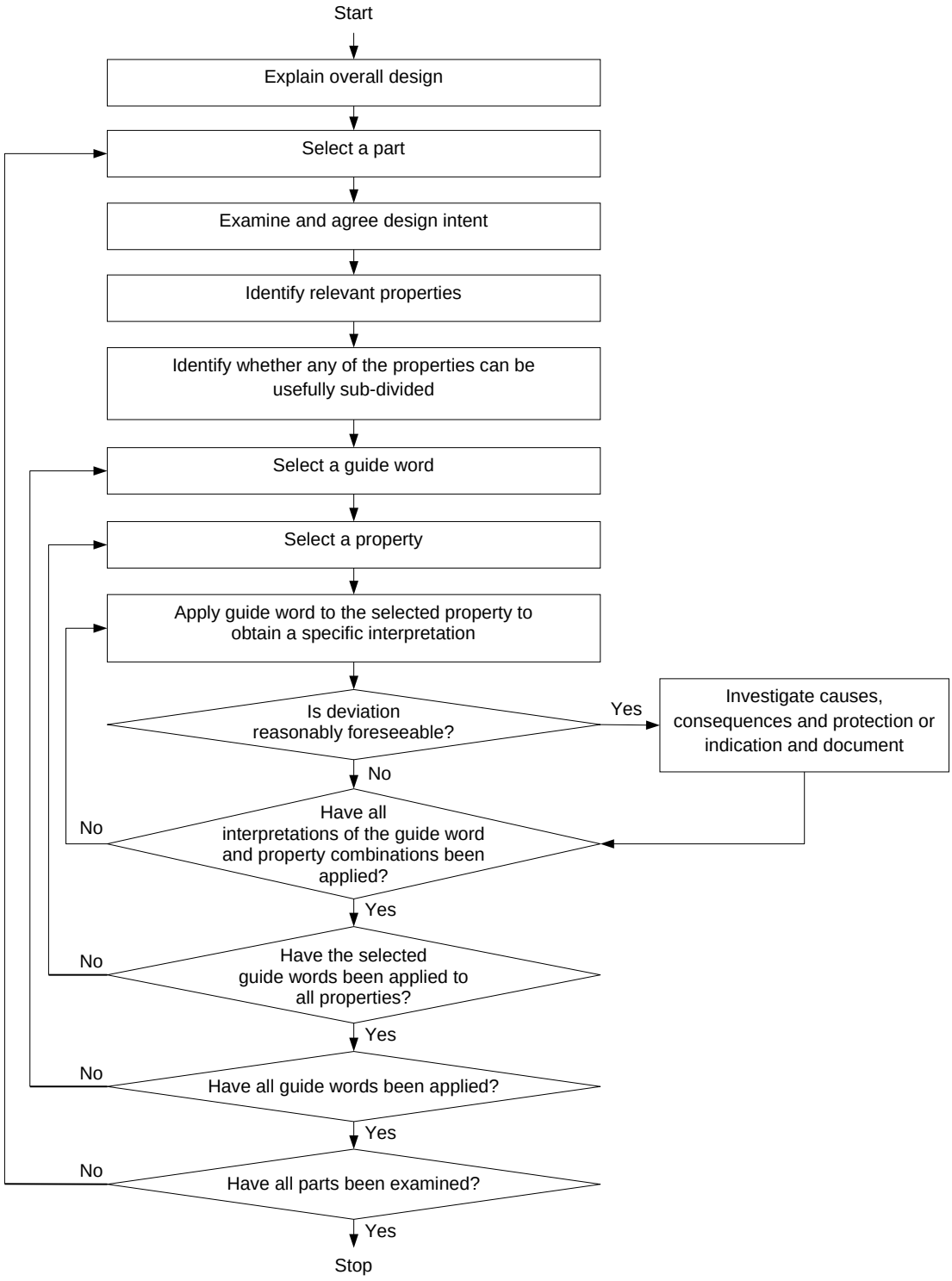


**Figure 3 – Flow chart of the HAZOP examination procedure – Guide word first sequence**

## 6.5 Documentation and follow up

### 6.5.1 General

A HAZOP study involves the systematic, disciplined and documented study of a system. To achieve full benefits from a study, it has to be properly documented and any suggested

actions completed. The study leader is responsible to ensure that suitable records are produced for each meeting. Various methods of reporting are discussed in Annex A.

### 6.5.2 Establish method of recording

There are two basic forms of recording: full, and by exception only. The method of recording should be decided before any sessions take place, and the recorder advised accordingly.

- Full recording involves documenting all results on applying each guide word/property combination to every part or element of the design representation. This method, though cumbersome, provides the evidence that the study has been thorough and should satisfy most regulatory or corporate requirements.
- By exception recording involves documenting only the identified risks and operability problems together with the follow-up actions. Property/guide word combinations where no risk or operability issue is identified are not included. Recording by exception results in more easily managed documentation. However, it does not document the thoroughness of the study and it could lead to an unnecessary, repeated study in the future.

In deciding the form of reporting to be employed, the following factors should be considered:

- regulatory requirements;
- contractual obligations;
- company policies;
- the need for traceability and auditability of the study;
- the importance of the system to the organization’s objectives;
- the time period and resources available.

### 6.5.3 Output of the study

The output from a HAZOP study should include the following:

- details of identified risks and operability problems together with details of any provisions for their treatment including the means by which they would be detected;
- the marked-up design representation used in the study (see Clause A.3);
- recommendations for any further studies of specific aspects of the design using different techniques, if necessary;
- recommendations of options for risk treatment based on the team’s knowledge of the system (if within the scope of the study);
- notes which draw attention to particular points which need to be addressed in the operations and maintenance;
- a list of team members for each session;
- a list of all the parts considered in the analysis together with the rationale where any have been excluded;
- a list of the guide words and properties used; and
- listing of all drawings, specifications, data sheets, reports, etc. used, quoting revision numbers.

With by exception recording, these outputs will normally be contained within the HAZOP worksheets. With full recording, the required outputs can be summarised from the study worksheets.

### 6.5.4 Record information

The recorded information should conform to the following:

- every risk and operating problem should be recorded as a separate item;
- all risks and operating problems together with their causes should be recorded regardless of any control already existing in the system;
- every question raised by the team for consideration after the meeting, should be recorded, together with the name of a person who might answer it;
- a numbering system should be adopted to ensure that every risk, operational problem, question, recommendation, etc. is uniquely identifiable;
- the study documentation should be archived for retrieval, as and when required, and referenced in the management system log for the system (if such exists).

Precisely who should receive a copy of the final report will be largely dictated by internal company policy or by regulatory requirements but should normally include the manager, the study leader and the people responsible for actions (see 6.2.3).

### 6.5.5 Sign off the documentation

At the end of the study, the report of the study should be produced and agreed upon by the team. There should be an official sign-off and approval of the final report by the team leader and management representative (preferably the manager that instigated the study). If agreement cannot be reached, the reasons for divergent views should be recorded.

### 6.5.6 Follow-up and responsibilities

The purpose of the HAZOP study is to review and not re-design a system. It is also not usual for the study leader to be accountable for the completion of the actions recommended by the team.

Before any significant changes resulting from the findings of the HAZOP study have been implemented, and once a revised design representation is available, the manager should consider reconvening the HAZOP study team to ensure that no new risks or operability or maintenance problems have been introduced.

In some cases, as indicated in 6.2.3, the manager can authorize the HAZOP study team to implement the recommendations and carry out design changes. In this case the HAZOP study team might be required to do the following additional work:

– agree on outstanding actions and revise the design or the operating and maintenance arrangements;
– verify the changes and communicate their completion to the manager and receive his or her approval;
– conduct further HAZOP studies of the revised system.

# Annex A
(informative)

# Methods of recording

## A.1 Recording options

Various recording options are available.

– Manual recording on prepared forms can be perfectly adequate, particularly for small studies, provided that the basic needs for legibility are met. Manuscript HAZOP study notes can be entered into software after the session, to produce a legible copy for issue.
– Word-processing or spread-sheet software can be used to produce the worksheets during the session.
– Specific HAZOP study recording software can be used.

If software is used, the study results can be projected as they are created. This ensures the team agrees with the record at the time.

## A.2 HAZOP worksheet

A worksheet should be used to record the results of examinations and follow-up. Regardless of the recording option chosen, the worksheet should contain the features given below. The layout of the worksheet will vary depending on whether it is created manually or as part of software.

The header should contain the following information: project, subject of the study, design intent, part of the system being examined, members of the team, drawing or document being examined, date, page number, etc.

The headings (titles) of the columns can be as follows:

a) for those completed during the examination:
   1) reference number;
   2) guide word;
   3) property;
   4) deviation/event;
   5) cause;
   6) consequences;
   7) existing controls;
   8) suggested actions.

Additional information such as comments can also be recorded.

b) for those completed during the follow-up:
   1) agreed action;
   2) responsibility for action;
   3) status of action.

NOTE The columns mentioned in b)1), b)2) and b)3) can also be completed at the meetings themselves.

Using a computer offers greater flexibility in layout, better presentation of information and ease of preparation of required reports such as:

– detailed worksheets;
– reports sorted by causes and/or consequences;
– follow-up reports with responsibilities and status.

Several software packages are available which aim to simplify the task of recording data and generating reports. Such packages are valuable in aiding the task of the recorder. However, some packages attempt to replace the study leader by generating a checklist of guide word/property pairs. Whilst these packages will identify some risks and produce a print-out which resembles the print-out from a HAZOP study, this will not have been produced from a rigorous and systematic study. The use of software to replace the study leader entirely is to be discouraged.

The random application of *ad hoc* checklists cannot be regarded as a HAZOP study as defined in this standard.

## A.3 Marked-up representation

The design representation can be marked-up to indicate the worksheet reference number for each part that has been studied and to show any changes to the design that the study team recommends.

This might limit misunderstandings that might arise from just a word description of the parts or recommended changes. It forms an important part of the report information. A photograph of the marked-up design representation is usually sufficient for the report with the originals kept by the manager until all actions have been completed.

## A.4 HAZOP study report

A final report of the HAZOP study should be prepared and contain the following:

– summary;
– conclusions;
– scope and objectives;
– output of the study itemized as given in 6.5.3;
– HAZOP study worksheets;
– the marked-up design representation;
– a list of the drawings and documentation referred to;
– any historical information that was used in the study.

# Annex B
(informative)

# Examples of HAZOP studies

## B.1 General

The purpose of the examples contained in Annex B is to illustrate how the principles of a HAZOP study, outlined in this standard (particularly in 4.2, 6.3 and 6.4) are applied to a range of applications encompassing various industries and activities. It should be noted however that the examples have been simplified significantly for illustrative purposes and do not purport in any way to reproduce all the detailed technical complexity of real case studies. It should also be noted that only sample outputs are provided.

## B.2 Introductory example

The purpose of this example is to introduce the reader to the basics of the HAZOP examination method. The example is adopted from one given in the original publication on HAZOP studies.

Consider a simple process plant, shown in Figure B.1. Materials A and B are continuously transferred by pumps from their respective supply tanks to combine and form a product C in the reactor. Suppose that A always has to be in excess of B in the reactor to avoid an explosion hazard. A full design representation would include many other details such as the effect of pressure, reaction and reactant temperature, agitation, reaction time, compatibility of pumps A and B, etc. but for the purposes of this simple illustrative example they will be ignored. The part of the plant being examined is shown in bold.

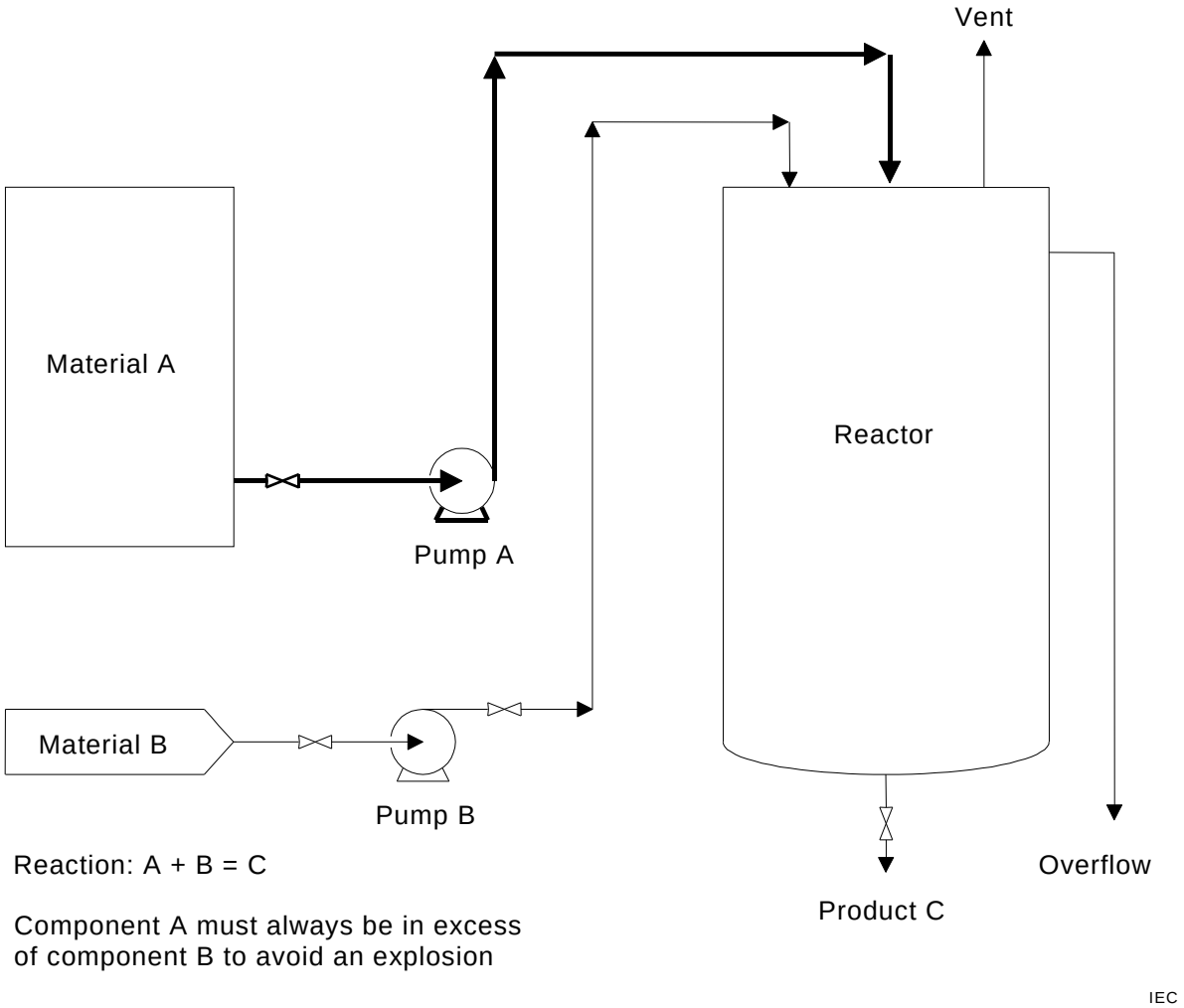


**Figure B.1 – Simple flow sheet**

The part of the system selected for examination is the line from the supply tank holding A to the reactor, including pump A (see Table B.1). The design intent for this part is to continuously transfer material A from the tank to the reactor at a rate greater than the transfer rate of material B . In terms of the properties suggested in 4.2, the design intent is given in the previous paragraph of Clause B.2.

**Table B.1 – Properties of the system under examination**

| Material | Activity | Source | Destination |
|---|---|---|---|
| A | Transfer (at a rate > B) | Tank for A | Reactor |

Each of the guide words indicated in Table 3 (plus any others agreed as appropriate during the preparatory work, (see 6.3.3)) is then applied to each of these properties in turn and the results recorded on HAZOP worksheets. Examples of possible HAZOP outputs are indicated in Table B.2, where the 'by exception' style of reporting is utilized and only meaningful deviations are recorded. Having examined each of the guide words for each of the properties relevant to this part of the system, another part (say the transfer line for material B) would be selected and the process repeated. Eventually all parts of the system would be examined in this manner and the results recorded.

## Table B.2 – Example HAZOP worksheet for introductory example

| | | |
|---|---|---|
| **STUDY TITLE:** PROCESS EXAMPLE | | **SHEET:** 1 of 4 |
| **Drawing No.:** | **REV. No.:** | **DATE:** December 17, 1998 |
| **TEAM COMPOSITION:** | LB, DH, EK, NE, MG, JK | **MEETING DATE:** December 15, 1998 |
| **PART CONSIDERED:** | **Transfer line from supply tank A to reactor** | |
| **DESIGN INTENT:** | **Material:** A **Activity:** Transfer continuously at a rate greater than B<br>**Source:** Tank for A **Destination:** Reactor | |

| No. | Guide word | Element | Deviation | Possible causes | Consequences | Existing controls | Comments | Actions required | Action allocated to |
|---|---|---|---|---|---|---|---|---|---|
| 1 | NO | Material A | No material A | Supply tank A is empty | No flow of A into reactor<br>Explosion | None shown | Situation not acceptable | Consider installation on tank A of a low-level alarm plus a low-level trip to stop pump B | MG |
| 2 | NO | Transfer A (at a rate > B) | No transfer of A takes place | Pump A stopped, line blocked | Explosion | None shown | Situation not acceptable | Measurement of flow rate for material A plus a low flow alarm and a low flow which trips pump B | JK |
| 3 | MORE | Material A | More material A: supply tank over full | Filling of tank from tanker when insufficient capacity exists | Tank will overflow into bounded area | None shown | Remark: This would have been identified during examination of the tank | Consider high-level alarm if not previously identified | EK |
| 4 | MORE | Transfer A | More transfer of A<br>Increased flow rate of A | Wrong size impeller<br>Wrong pump fitted | Possible reduction in yield<br>Product will contain large excess A | None | | Check pump flows and characteristics during commis-sioning<br>Revise the commissioning procedure | JK |

| No. | Guide word | Element | Deviation | Possible causes | Consequences | Existing controls | Comments | Actions required | Action allocated to |
|---|---|---|---|---|---|---|---|---|---|
| 5 | LESS | Material A | Less A | Low level in tank | Inadequate net positive suction head<br>Possible vortexing and leading to an explosion<br>Inadequate flow | None | Unacceptable<br>Same as 1 | Low-level alarm in tank<br>Same as 1 | MG |
| 6 | LESS | Transfer A (at rate > B) | Reduced flow rate of A | Line partially blocked, leakage, pump under-performing, etc. | Explosion | None shown | Not acceptable | Same as 2 | JK |
| 7 | AS WELL AS | Material A | As well as A there is other fluid material also present in the supply tank | Contaminated supply to tank | Not known | Contents of all tankers checked and analysed prior to discharge into tank | Considered acceptable | Check operating procedure | LB |
| 8 | AS WELL AS | Transfer A | As well as transferring A, something else happens such as corrosion, erosion, crystallization or decomposition | The potential for each would need to be considered in the light of more specific details | | | | | NE |
| 9 | AS WELL AS | Destination reactor | As well as to reactor<br>External leaks | Line, valve or gland leaks | Environmental contamination<br>Possible explosion | Use of accepted piping code/ standard | Qualified acceptance | Locate flow sensor for trip as close as possible to the reactor | DH |
| 10 | REVERSE | Transfer A | Reverse direction of flow<br>Material flows from reactor to supply tank | Pressure in reactor higher than pump discharge pressure | Back contamination of supply tank with reaction material | None shown | Position not satisfactory | Consider installing a non-return valve in the line | MG |

| No. | Guide word | Element | Deviation | Possible causes | Consequences | Existing controls | Comments | Actions required | Action allocated to |
|---|---|---|---|---|---|---|---|---|---|
| 11 | OTHER THAN | Material A | Other than A<br>Material other than A in supply tank | Wrong material in supply tank | Unknown<br>Would depend on material | Tanker contents identity checked and analysed prior to discharge | Position acceptable | | |
| 12 | OTHER THAN | Destination reactor | External leak<br>Nothing reaches reactor | Line fracture | Environmental contamination and possible explosion | Integrity of piping | Check piping design | Specify that proposed flow trip should have a sufficiently rapid response to prevent an explosion | MG |

## B.3 Procedures

Consider a small batch process for the manufacture of a safety critical plastic component. The component has to meet a tight specification in terms both of its material properties and its colour. The processing sequence is as follows:

a) take 12 kg of powder “A”;

b) place in blender;

c) take 3 kg of colourant powder “B”;

d) place in blender;

e) start blender;

f) mix for 15 min; stop blender;

g) remove blended mixture into 3 × 5 kg bags;

h) wash out blender;

i) add 50 l of resin to mixing vessel;

j) add 0,5 kg of hardener to mixing vessel;

k) add 5 kg of mixed powder (“A” and “B”);

l) stir for 1 min;

m) pour mixture into molds within 5 min.

A HAZOP study is carried out to examine ways in which below-specification material might be produced. As a procedural sequence, the parts under examination during the HAZOP process are the relevant sequential instructions. Extracts from a HAZOP study of the sequence are given in Table B.3. A “by exception” reporting system has been employed.

**Table B.3 – Example HAZOP worksheet for procedures example**

| | | |
|---|---|---|
| **STUDY TITLE:** PROCEDURES | | **SHEET**: 1 of 3 |
| **PROCEDURE TITLE:** Small scale manufacture of component X | **REVISION No.**: | **DATE**: |
| **TEAM COMPOSITION:** BK, JS, LE, PA | | **MEETING DATE:** |
| **PART CONSIDERED:** | **INSTRUCTION 1:** Take 12 kg of powder 'A' | |

| No. | Property | Guide word | Deviation | Possible causes | Consequences | Existing controls | Comments | Actions required | Action allocated to |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Take powder A | NO | No 'A' taken | Operator error | Final material will not set | Operator should see mass in blender is much too small. Colour would also be far too bright. | Complete absence of material 'A' charge not considered credible | None | |
| 2 | Take powder A | AS WELL AS | Additional material is added with 'A' | Material 'A' is contaminated with impurities | Colour specification might not be met. Final mix might not set properly | Sample from all deliveries of 'A' are tested prior to use | | Check quality assurance procedures at manufacturers | BK |
| 3 | Take powder A | OTHER THAN | Material other than 'A' is taken | Operator uses a bag of wrong material | Mix cannot be used. Financial loss | Only bags of 'A', 'B' and blend to be kept in blender area | | Check house-keeping standards on a weekly basis. Consider having uniquely coloured bags for each raw material and blended product | BK |
| 4 | Take 12 kg | MORE | Too much 'A' taken | Faulty weighing/ Operator error | Colour specification will not be met | Check weighing carried out weekly.<br>Weighing machine serviced every 6 months | | JS to emphasize to operators the need for accurate weighing | JS |
| 5 | Take 12 kg | LESS | Too little 'A' taken | Faulty weighing/ Operator error | As above | As above | | As above | JS |
| 6 | Blender | OTHER THAN | Material 'A' is placed other than in the correct blender | Operator error | | There is currently only one blender | | Review the position if there are proposals to fit additional blenders | BK |

| No. | Property | Guide word | Deviation | Possible causes | Consequences | Existing controls | Comments | Actions required | Action allocated to |
|---|---|---|---|---|---|---|---|---|---|
| 7 | Add hardener | NO | No hardener is added | Operator error | Final mix will not set properly<br>Financial loss | Operator has to sign batch sheet confirming hardener has been added. Testing of strength of final item | | Review error rate to see if additional safeguards are required | BK |
| 8 | Add hardener | AS WELL AS | Additional material is added with hardener | Hardener is contaminated with impurities | Final mix might not be usable | Quality assurance guaranties from supplier<br>Sample testing on all deliveries | | None | |
| 9 | Add hardener | OTHER THAN | Material other than hardener is added | | Final mix will not be usable | Physical segregation of different hardeners Operator checks | If proposal to order pre-weighed bags of hardener is adopted, scope for mix-up is further reduced | Await outcome of hardener. Purchasing enquiry and review | JS |
| 10 | Add 0,5 kg | MORE | Too much hardener is added | Faulty weighing<br>Operator error | Component will be too brittle; could fail catastrophically | Weekly check weighing. Weighing machine serviced every 6 months | Safeguards not considered adequate | Investigate possibility of obtaining hardener in pre-weighed 0,5 kg bags. Sample checks on each delivery | JS |
| 11 | Add 0,5 kg | LESS | Too little hardener | As above | Final mix will not set properly<br>Financial loss | As above | As above | As above | JS |

## B.4 Automatic train protection system

### B.4.1 General

The purpose of Clause B.4 is to give a small example of a typical HAZOP study at the system block diagram level to illustrate some of the points in this standard. The example will be presented in two sections:

– a brief description of the system and a block diagram;
– sample HAZOP worksheets exploring some of the potential deviations, reported "by exception only" (see Table B.4).

It should be noted that the design used in this example is of a system at a limited level of detail. The design and the sample HAZOP study worksheets are illustrative only and are not taken from a real system. They are included to show the process and are not claimed to be complete.

### B.4.2 Application

#### B.4.2.1 System purpose

The application concerns train-carried equipment for automatic train protection (ATP). This is a function implemented on many metro trains and some mainline trains. ATP monitors the speed of the train, compares that speed with the planned safe speed of the train and automatically initiates emergency braking if an overspeed condition is recognized. On all ATP systems there is equipment on both the train and trackside whereby information is transferred from the track-side to the train. There are many different ATP systems in existence, all differing in the detail of how they fulfil the basic requirement.

#### B.4.2.2 System description

On board the train there are one or more antennae which receive signals from the trackside equipment giving information on safe speeds or stopping points. This information goes through some processing before being passed to a programmable electronic system (PES). The other major input to the PES is from tachometers or other means of measuring the actual speed of the train. The major output of the PES is a signal to safety relays such as the one controlling the emergency brake. Figure B.2 gives a simple block diagram of this process.

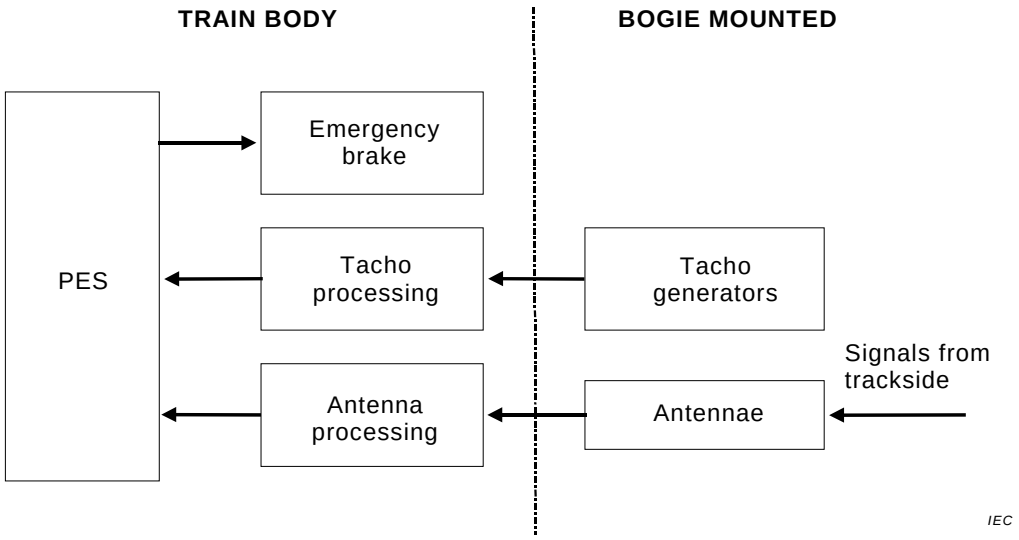


**Figure B.2 – Train-carried ATP equipment**

## Table B.4 – Example HAZOP worksheet for automatic train protection system

| | | |
|---|---|---|
| **STUDY TITLE:** AUTOMATIC TRAIN PROTECTION SYSTEM | | **SHEET:** 1 of 2 |
| **REFERENCE DRAWING No.:** ATP BLOCK DIAGRAM | **REVISION No.:** 1 | **DATE:** |
| **TEAM COMPOSITION:** DJ, JB, BA | | **MEETING DATE:** |
| **PART CONSIDERED:** | INPUT FROM TRACKSIDE EQUIPMENT | |
| **DESIGN INTENT:** | TO PROVIDE SIGNAL TO PES VIA ANTENNAE GIVING INFORMATION ON SAFE SPEEDS AND STOPPING POINTS | |

| No. | Part | Property | Guide word | Deviation | Possible causes | Consequences | Controls | Comments | Actions required | Action allocated to |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Input signal | Amplitude | NO | No signal detected | Transmitter failure | Considered in separate study of trackside equipment | | | Review output from trackside equipment study | DJ |
| 2 | Input signal | Amplitude | MORE | Greater than design amplitude | Transmitter mounted too close to rail | Could damage equipment | Checks to be carried out during installation | | Add check to installation procedure | DJ |
| 3 | Input signal | Amplitude | LESS | Smaller than design amplitude | Transmitter mounted too far from rail | Signal can be missed | As above | | Add check to installation procedure | DJ |
| 4 | Input signal | Frequency | OTHER THAN | Different frequency detected | Pick up of a signal from adjacent track | Incorrect value passed to processor | Currently none | | Check if action is needed to protect against this occurring | DJ |
| 5 | Antennae | Position | OTHER THAN | Antennae is in other than the correct location | Failure of mountings | Could hit track and be destroyed | Cable should provide secondary support | | Ensure that cable will keep antennae clear of track | JB |
| 6 | Antennae | Voltage | MORE | Greater voltage than expected | Antennae short to live rail | Antennae and other equipment become electrically live | | | Check if there is any protection against this occurring | DJ |
| 7 | Antennae | Output signal | OTHER THAN | A different signal is transmitted | Pick-up of stray signals from adjacent cabling | Incorrect signal might be acted upon | | | Ensure that there is adequate protection from cabling interference | JB |
| 8 | Tacho-meter | Speed | NO | No speed is measured | Sudden wheel lock | Might show zero speed | | | Check protection against this occurring | DJ |

| No. | Part | Property | Guide word | Deviation | Possible causes | Consequences | Controls | Comments | Actions required | Action allocated to |
|---|---|---|---|---|---|---|---|---|---|---|
| 9 | Tacho-meter | Speed | OTHER THAN | Other than correct speed is detected | Sudden release of locked wheels gives confusing signal | Could show wrong speed | | | Check protection against this occurring | BA |
| 10 | Tacho-meter | Speed | AS WELL AS | Many speeds indicated | Sudden changes in output caused by wheel spin | Could cause action based on wrong speed | | | Check if this is a problem in practice | BA |
| 11 | Tacho-meter | Output voltage | NO | No output | Axles locked | Might show zero speed | | | Check implications of this occurring | DJ |
| 12 | Tacho-meter | Output signal | AS WELL AS | Confused output signal | Other signals mixed in | Might indicate wrong speed | | | Investigate whether this is a credible failure | BA |

## B.5 Example involving emergency planning

Organizations make plans to deal with a variety of anticipated emergencies. These emergencies can vary from reaction to a bomb threat, the provision of emergency power supplies or the escape of personnel in the event of a fire. The validity and integrity of these plans can be tested in a variety of ways – typically by some form of rehearsal. Such rehearsals are valuable, but can be expensive and, by their very nature, disrupt normal working. Fortunately, real emergencies which test the system are rare and in any case, even rehearsals are unlikely to cover all possibilities.

HAZOP studies offer a relatively inexpensive way of identifying many of the deficiencies which can exist in an emergency plan, in order to supplement the experience obtained by the relatively infrequent rehearsal or the even rarer actual emergency itself (see Table B.5).

On an offshore oil and gas platform there needs to be in place effective arrangements for EER in the event of potentially life-threatening incidents. These arrangements would aim to ensure that personnel are quickly alerted to the existence of a dangerous situation, are able to make their way rapidly to a safe muster point, then evacuate the platform preferably in a controlled manner by helicopter or lifeboat and then be rescued and taken to a place of safety. Effective EER arrangements are an essential part of an overall offshore installation system. Within typical EER arrangements there are usually a number of different stages (elements) such as:

a) raising the GPA by automatic instruments or manually by any operator;

b) communicating the situation both to the local stand-by vessel and to onshore emergency services;

c) personnel making their way along designated access routes to the muster point;

d) mustering involving registration of personnel present;

e) donning of survival equipment, etc.;

f) await PAPA which has to be initiated by the OIM or his deputy;

g) egress in which personnel make their way from the muster point to the chosen method of evacuation;

h) evacuation normally by helicopter or by special forms of lifeboat;

i) escape directly into the sea if the preferred means of evacuation is not available;

j) rescue, where either personnel in a lifeboat or those who had escaped directly into the sea would be recovered and taken to a place of safety.

**Table B.5 – Example HAZOP worksheet for emergency planning**

| | |
|---|---|
| **PART CONSIDERED:** | ALARM SYSTEM |
| **DESIGN INTENT:** | TO SOUND A GPA |
| **PARTS:** | INITIATION SIGNAL |
| **INPUTS:** | ELECTRICAL ENERGY |
| **ACTIVITIES:** | TO EMIT AUDIBLE ALARM AND TRANSMIT THE SOUND TO PERSONNEL |
| **SOURCES:** | ALL ALARM GENERATORS |
| **DESTINATIONS:** | ALL PERSONNEL ON PLATFORM |

| No. | Property | Guide word | Deviation | Possible causes | Consequences | Existing controls | Comments | Actions required | Action by |
|---|---|---|---|---|---|---|---|---|---|
| 1 | GPA initiation signal and electrical energy | NO | No inputs | 1) Instruments or personnel do not initiate GPA | Failure to alert personnel | None | Unlikely but possible | None | |
| | | | | 2) Personnel try to initiate GPA, but signal fails to reach alarm | As above | Duplicated connections and fail safe logic, i.e. "Current to open, spring to close" | Unlikely | | |
| | | | | 3) No electrical energy | As above | Uninterruptible power supply | As above | | |
| 2 | | MORE | More inputs | 1) False alarm | Personnel stressed unnecessarily | None | Possible | Should initiation require two buttons? | |
| | | | | 2) Mischief alarm | As above | Discipline and code of practice | Unlikely | None | |
| 3 | Inputs | MORE | More inputs | More electrical energy | Damage to alarm system | Dedicated protected power supply | Unlikely | None | |
| 4 | | LESS | Less initiation | Initiation signal only reaches some alarms | Some personnel not alerted | Routine alarm checks | | None | |

| No. | Property | Guide word | Deviation | Possible causes | Consequences | Existing controls | Comments | Actions required | Action by |
|---|---|---|---|---|---|---|---|---|---|
| 5 | | | Less electrical energy | Some loss of power | Alarms might not sound | Dedicated power supply | Unlikely | None | |
| 6 | | AS WELL AS | As well as initiation | Initiation triggers other activities | | Not possible with dedicated hard-wired circuit | | None | |
| 7 | | | As well as electrical energy | Some energy in wrong form, e.g. spikes | Possible damage | Screened supply circuit | | None | |
| 8 | | PART OF | Part of inputs | Signal but no energy or energy but no signal | Personnel not alerted | | Already considered above | | |
| 9 | | REVERSE | Reverse inputs<br><br>Reverse electrical energy | Reverse of alarm initiation<br><br>No constructive meaning | | | System as described does not include the sounding of an "all clear" | Develop an "all clear" system | |
| 10 | Inputs | OTHER THAN | Other than inputs | Multiple | Depends on inputs | Unlikely with dedicated shielded circuits | Might need "battle proof" system | Consider Pyrotenax wiring | |
| 11 | Activities emit alarm and transmit to personnel | NO | No alarm sounded | Sound equipment failure<br><br>Cable damage | Personnel not alerted | Dual PA system<br><br>Dual cabling<br>Dual power supplies<br>Multiple speakers | Unlikely | None | |
| 12 | | MORE | More alarm | Sound equipment too powerful | Personnel suffer ear damage | Sound equipment rated to not exceed safe level | | None | |
| 13 | | LESS | Less alarm | Sound too weak | Some personnel not alerted | None | | Ensure system provides a minimal of 15 dB above background noise | |

| No. | Property | Guide word | Deviation | Possible causes | Consequences | Existing controls | Comments | Actions required | Action by |
|---|---|---|---|---|---|---|---|---|---|
| 14 | | AS WELL AS | As well as alarm and transmit | Distortion of alarm, overtones or echoes | Lack of clear signal to personnel | None | | Investigate need for acoustic engineering | |
| 15 | | PART OF | Part of alarm and transmit | Alarm but transmission inadequate | No signal to personnel | | As for less alarm above | | |
| 16 | | REVERSE | Reverse alarm and transmit | | | | See comments above reverse initiations and "all clear" | | |
| 17 | | OTHER THAN | Other than emit GPA alarm and transmit | System initiates PAPA by mistake | Confusion amongst personnel. Some could abandon platform by mistake | None | | Review signal logic so that PAPA can only be sounded after GPA | |
| 18 | | SOONER | Alarm and transmit sounded too soon | GPA initiated before situation requires this action | Unnecessary alarm and disruption of work | None | | Establish clear guidelines for platform personnel | |
| 19 | | LATER | Alarm and transmit sounded too late | GPA initiation after situation required this action | Some personnel could be trapped or forced to use alternative and less desirable route | None | | Clear guidelines as above | |

## B.6 Piezo valve control system

The piezo valve control system shows how a HAZOP study can be applied to a detailed electronic system (see simplified Figure B.3, Table B.6 and Table B.7).

A piezo valve is a valve driven by a piezo ceramic. The ceramic element is electrically driven and lengthens itself in the charged state. A charged piezo ceramic closes the valve. A discharged piezo ceramic opens the valve. If the piezo ceramic does not lose or gain charge, the state of the valve is kept.

The system sprays a flammable and explosive liquid into a reaction vessel (not shown). The overall system with reactor vessel, pipes, pumps, etc. is part of a separate HAZOP study. Here only the application of a HAZOP study to an electronic unit is shown.

The operation of the unit is a two-state process designed to close the valve on demand, “state 1”, and open it on demand, “state 2”.

An electrical charge from capacitor C1 is conducted via the transistor T1 to the coupling capacitor C2 and via the power wire to the piezo valve to close it. In this case transistor T2 and the protection transistor T3 are closed (high resistance).

Capacitor C2 is discharged by transistor T2 to open the valve. To prevent asymmetric charging of the piezo valve, for example by mechanical or thermal stress, transistor T4 connects the low side to ground.

An electrical shield around the twisted wires of the cable prevents electro-magnetic influences from affecting the valve.

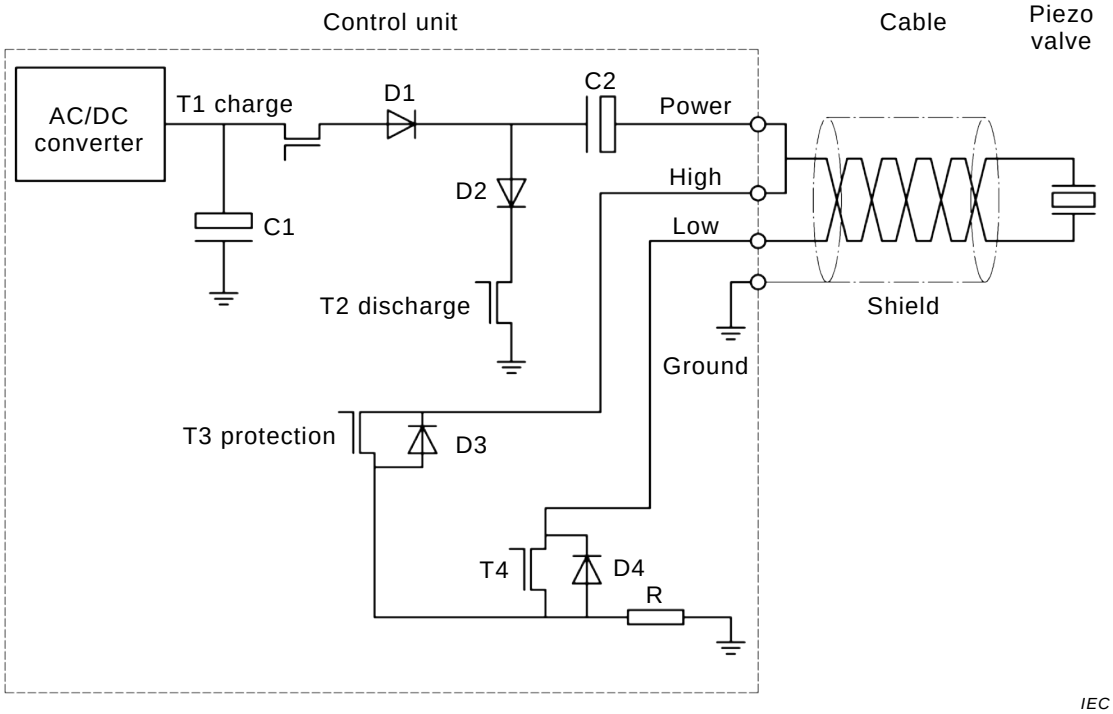


**Figure B.3 – Piezo valve control system**

**Description of state 1:** close valve.

**Part considered:** cable from AC/DC converter and from capacitor C1 via transistor T1, diode D1, capacitor C2 to the power side of the valve and from the ground side of the valve via transistor T4 and resistor R to ground.

**Description of state 2:** open valve.

**Part considered:** cable from power side of valve via transistor T3, diode D3 and resistor R to ground.

**Table B.6 – System design intent**

| Input | Activity | Source | Destination |
|---|---|---|---|
| State 1: Close valve<br>1. Charge in C1 | 1. Transfer charge via T1, D1 and C2 | C1 and converter | 1. Power to power side of valve |
| Characteristics:<br>Voltage<br>Capacity | 2. Transfer charge via T4 and R to ground | Low side of valve | 2. Low side charge to ground |
| 2. Control signals to T1, T3 and T4 | 3. Control opening via T1 and T4 from ground<br>4. Isolate via T2<br>5. Prevent overcharge via T3 | Signal from controller | T1, T3 and T4<br>Overcharge to ground |
| | 6. Prevent reverse flow of charge via D2 | Power side of valve | |
| State 2: Open valve<br>1. Discharge power side of valve<br>Characteristics:<br>Voltage<br>Capacity | 1. Isolate from C1 and converter via T1<br>2. Transfer power charge via D2 and T2<br>3. Transfer any charge of valve via D3, D4 and R | Power side of valve and C2 | Ground |
| 2. Control signals to T1, T2 and T4 | 4. Isolate low charge side of valve via T4 | Signals from controller | T1, T2 and T4 |

## Table B.7 – Example HAZOP worksheet for piezo valve control system

| | | | |
|---|---|---|---|
| **STUDY TITLE:** PIEZO VALVE CONTROL SYSTEM | | | **SHEET:** 1 of 3 |
| **Drawing No:** | | **REVISION No.:** | **DATE:** |
| **TEAM COMPOSITION:** Development engineer, System engineer, Quality manager | | | **MEETING DATE:** 04.11.97 |
| **Part considered:** | State 1: System closes valve | | |
| **Design intent:** | Transfer a defined quantity of electrical charge to the piezo actuator to close the valve at a defined time | | |

| Property | Guide word | Deviation | Possible causes | Consequences | Controls | Comments | Actions required | Action allocated to |
|---|---|---|---|---|---|---|---|---|
| Input:<br>Charge in C1 | NO | No charge; including don't transfer | Power outage<br>Failure of converter<br>Fault in C1<br>T1 is permanently closed<br>T2 is permanently open<br>T1 faulty<br>Diodes (D1, D3) failure:<br>– Diode D1 with open circuit; no current flows<br>– Diode D3 shortened; shortcut via D4 to low side of piezo valve or via R to ground<br>C2 faulty<br>Broken wires<br>T4 faulty<br>R faulty<br>T3 faulty | No flow via C2 into piezo valve<br>Valve does not close; permanently open<br>Reactive material running into the vessel | None | Situation not acceptable<br>Design change required | High-level alarm<br>Test routine | J. Smith |

| Property | Guide word | Deviation | Possible causes | Consequences | Controls | Comments | Actions required | Action allocated to |
|---|---|---|---|---|---|---|---|---|
| Input: Charge in C1 | MORE | More charge than defined | Charge in C2 too high<br>Faulty converter<br>Transistor T1 does not close in time<br>C2 faulty<br>AC/DC converter delivers too high voltage<br>Transistor T1 does not close in time<br>Faulty protection T3 | Piezo valve closes earlier than defined<br>Damaged piezo valve | Flow meter shows too high quantity; transistor T3 discharges piezo valve;<br>None shown | Situation not acceptable | Consider high level alarm | Peter Peterson |
| Charge in C1 | LESS | Less charge than specified | Insufficient capacity exists<br>Faulty insulation of cable; charge disappears<br>T1 closes too early<br>T2 is partly open | Insufficient charge in C2<br>Valve closes later than specified | None | Situation not acceptable | Alarm | J. Smith |
| Input: Charge in C1 | AS WELL AS | T1 as well as T2 is open | Less charge to C2<br>Valve does not close<br>Reactive material runs into the reaction vessel | Uncontrolled chemical reaction | None shown | Small differences could be acceptable | Alarm<br>Test routine<br>Reset<br>Define acceptable differences | J. Smith |

## B.7 HAZOP of a train stabling yard horn procedure

Trains in a stabling yard are required to sound the horn prior to any movement. The procedure was required to be changed due to planning restrictions concerning noise. The new procedure requires a suitably qualified person, in addition to the train guard, to check the area around the train prior to any movement to ensure it is safe to do so.

The procedure is as follows:

1. Start procedure
    - 1.1 Driver observes STOP indication from leading crew compartment.
    - 1.2 QP stands adjacent to the leading crew compartment.
    - 1.3 Driver to confirm to QP that driver preparation is complete or that driver has changed ends and to commence checking procedure.
    - 1.4 Driver advises guard (internal PA) to commence checking procedure.
2. QP checking procedure
    - 2.1 QP checks the first 4 cars on LH side of train.
        - 2.1.1 If not clear, remove/clear obstruction then check the first 4 cars on LH side again.
        - 2.1.2 If clear, QP gives one long, loud whistle blast to warn of train departing.
    - 2.2 QP checks the first 4 cars on RH side of train.
        - 2.2.1 If not clear, remove/clear obstruction then check the first 4 cars on RH side again.
        - 2.2.2 If clear, QP gives one long, loud whistle blast to warn of train departing.
    - 2.3 QP advises driver that both sides have been checked and all is clear
3. Guard checking procedure
    - 3.1 Guard opens doors on both sides of train.
    - 3.2 Make internal and external PA announcement on both sides of train, “Stand clear this train is about to depart the yard from No. x road”.
    - 3.3 Check the last 4 cars on the RH side of train.
        - 3.3.1 If not clear, remove/clear obstruction then check the last 4 cars on same side again.
        - 3.3.2 If clear, guard gives one long, loud whistle blast to warn of train departing.
    - 3.4 Check the last 4 cars on the LH side of train.
        - 3.4.1 If not clear, remove/clear obstruction then check the last 4 cars on same side again.
        - 3.4.2 If clear, guard gives one long, loud whistle blast to warn of train departing.
    - 3.5 Close doors on both sides and check by visual inspection and by checking that the Door Open indicator is extinguished.
    - 3.6 Give the ALL RIGHT bell signal to driver.
4. Complete departure procedure
    - 4.1 Driver advises QP that the guard has completed the departure process.
    - 4.2 QP contacts signal box to advise the signaller that the train is ready to depart.
        - 4.2.1 If the signal cannot be cleared within approximately 1 min then maintain signal at STOP and advise the QP of the approximate time to clear and

advise the QP prior to clearing so that QP and guard can restart checking procedure.

4.2.2 After receiving confirmation from QP that the train is ready to depart, clear the relevant signals.

4.3 Driver confirms PROCEED indication and performs modified inching movement.

5. Driver takes train to whistle sign and tests train horn.

An operational breakdown matrix is given in Table B.8 and an example of a HAZOP worksheet is given in Table B.9.

**Table B.8 – Operational breakdown matrix for train stabling yard horn procedure**

| No. | Step | Conditions at start | Information needed | Communication who, why, when | Control points | Finish conditions |
|---|---|---|---|---|---|---|
| 1 | Start procedure<br>– Driver observes STOP indication from leading crew compartment<br>– Driver to confirm to QP that driver preparation is complete or that driver has changed ends and to commence checking procedure<br>– Driver advises guard (internal PA) to commence checking procedure | – Train standing in yard with signal at STOP<br>– QP standing adjacent to leading crew compartment<br>– Guard on train in guard's compartment | – Site induction and track safety awareness<br>– Training (driver, guard, signalling, QP)<br>– Train no. and road train is on | – Driver to QP verbally when driver preparation is complete or when driver has changed ends<br>– Driver to guard by internal PA when driver preparation is complete or when driver has changed ends | – Driver to have observed STOP indication | – Train standing in yard with signal at STOP<br>– QP standing adjacent to leading crew compartment<br>– Guard on train in guard's compartment |
| 2 | QP checking procedure<br>– QP checks the first 4 cars on LH side of train<br>– If not clear, remove/clear obstruction then check the first 4 cars on LH side again<br>– If clear, QP gives one long, loud whistle blast then checks the first 4 cars on RH side of train<br>– If not clear, remove/clear obstruction then check the first 4 cars on RH side again<br>– If clear, QP gives one long, loud whistle blast<br>– QP advises driver that both sides have been checked and all is clear | – Train standing in yard with signal at STOP<br>– QP standing adjacent to leading crew compartment<br>– Guard on train in guard's compartment | – Site induction and track safety awareness<br>– Training (driver, guard, signalling, QP) | – QP whistle on each side when all clear<br>– QP to driver verbally when finished checking (and clearing) both sides | – QP has to be able to see to the end of the first 4 cars on either side, which could mean walking some distance alongside the train.<br>– The road is clear if there is nothing to obstruct the train (on tracks or either side, in train envelope) | – Train standing in yard with signal at STOP<br>– QP standing adjacent to leading crew compartment<br>– Guard on train in guard's compartment<br>– All clear for first 4 cars |

| No. | Step | Conditions at start | Information needed | Communication who, why, when | Control points | Finish conditions |
|---|---|---|---|---|---|---|
| 3 | Guard checking procedure<br>– Guard opens doors on both sides of train<br>– Make internal and external PA announcement on both sides of train, “Stand clear this train is about to depart the yard from No. x road”.<br>– Check the last 4 cars on the RH side of train<br>– If not clear, remove/clear obstruction then check the last 4 cars on same side again<br>– If clear, guard gives one long, loud whistle blast<br>– Check the last 4 cars on the LH side of train<br>– If not clear, remove/clear obstruction then check the last 4 cars on same side again<br>– If clear, guard gives one long, loud whistle blast<br>– Close doors on both sides<br>– Give the ALL RIGHT bell signal to driver | – Train standing in yard with signal at STOP with doors open | – Site induction and track safety awareness<br>– Training (driver, guard, signalling, QP)<br>– Knowledge about the type of train being checked | – Guard internal and external PA after opening doors<br>– Guard whistle on each side when all clear<br>– Guard bell to driver when all clear for last 4 cars | – Initially all doors to open on both sides of train (check Door Open light and visual check)<br>– Guard has to be able to see to the end of the train on both sides.<br>– The road is clear if there is nothing to obstruct the train (on tracks or either side, in train envelope)<br>– When clear on each side, doors to close for that side (check Door Open light and visual check)<br>– Guard will not hear bell if it fails | – Train standing in yard with signal at STOP with doors closed |

| No. | Step | Conditions at start | Information needed | Communication who, why, when | Control points | Finish conditions |
|---|---|---|---|---|---|---|
| 4 | Complete departure procedure<br>– Driver advises QP that the guard has completed the departure process<br>– QP contacts signal box to advise the signaller that the train is ready to depart<br>– If the signal cannot be cleared within approximately 1 min then signaller to maintain signal at STOP and advise the QP of the approximate time to clear and advise the QP prior to clearing so that QP and guard can restart checking procedure.<br>– After receiving confirmation from QP that the train is ready to depart, clear the relevant signals.<br>– Driver confirms PROCEED indication and performs modified inching movement. | – Train standing in yard with signal at STOP with doors closed<br>– QP standing adjacent to leading crew compartment<br>– Guard on train in guard's compartment | – Site induction and track safety awareness<br>– Training (driver, guard, signalling, QP) | – Driver to QP verbally when guard's bell heard<br>– QP to signaller via radio (or mobile phone, or signal phone, as backups) when driver advises that departure process completed | – Signal must be giving a PROCEED indication<br>– Driver has to hear from both QP and guard that all is clear before departure process complete | – Train moving past PROCEED signal |
| 5 | Driver takes train to whistle sign and tests train horn. | – Train moving past PROCEED signal | – Site induction and track safety awareness<br>– Training (driver, guard, signalling, QP) | None | – Procedure is complete when horn blown successfully at whistle sign | – Train has left stabling yard |

**Table B.9 – Example HAZOP worksheet for train stabling yard horn procedure**

| | | | |
|---|---|---|---|
| **STUDY TITLE:** TRAIN STABLING YARD HORN PROCEDURE | | | **SHEET:** 1 of x |
| **Drawing No:** | | **REVISION No.:** | **DATE:** |
| **TEAM COMPOSITION:** Driver, Guard, Area Controller, Train Crewing Manager, Manager Network Control | | | **MEETING DATE:** |
| **Part considered:** | Step 1: Start procedure | | |
| **Design intent:** | Prepare train and personnel for checking procedure | | |

| Property | Guide word | Deviation | Possible causes | Consequences | Existing controls | Comments | Actions required | Action allocated to |
|---|---|---|---|---|---|---|---|---|
| Start Procedure | WRONG ACTION | | QP, driver, guard do not begin procedure | Operational delay – train does not move | Procedure will ensure train will not depart<br>Training<br>Employee vigilance | | None | |
| Start Procedure | EXTRA ACTION | | QP receives a mobile phone call | Operational delay – train does not move | Procedure will protect by not allowing train to depart<br>Training<br>Employee vigilance | | None | |
| Start Procedure | CLARITY | | Procedure refers to left and right side of train | Confusion as to which side of train is being referred to | | | To remove possibility of confusion, change the procedure to refer to driver's side and off side, rather than left and right | J. Suffield |
| Start Procedure | MORE TIME | | Operator takes more time than expected to complete an activity | Operational delay – train does not move | Procedure will protect by not allowing train to depart<br>Training<br>Employee vigilance | | Another separate procedure will be undertaken<br>Training<br>Employee vigilance | None |

| Property | Guide word | Deviation | Possible causes | Consequences | Existing controls | Comments | Actions required | Action allocated to |
|---|---|---|---|---|---|---|---|---|
| Start Procedure | ABNORMAL CONDITIONS | | Signal failure | This procedure will be stopped and another procedure will be used to address the signal failure | Another separate procedure will be undertaken<br>Training<br>Employee vigilance | | None | |
| QP checking procedure | NO ACTION | | QP does not begin checking both sides of the train | Operational delay – train does not move | Procedure will protect by not allowing train to depart<br>Training<br>Employee vigilance | | None | |
| QP checking procedure | NO ACTION | | QP begins checking the train but does not complete the task | No change to current consequence (same applies throughout entire network) | Procedure will protect by not allowing train to depart<br>Training<br>Employee vigilance | | None | |
| QP checking procedure | MORE ACTION | | QP performs additional activity that is not part of the procedure (attends to a distraction that prevents him from completing procedure) | Operational delay – train does not move | Procedure will protect by not allowing train to depart<br>Training<br>Employee vigilance | | None | |
| QP checking procedure | EXTRA ACTION | | QP receives a mobile phone call | Operational delay – train does not move | Procedure will protect by not allowing train to depart<br>Training<br>Employee vigilance | | None | |

| Property | Guide word | Deviation | Possible causes | Consequences | Existing controls | Comments | Actions required | Action allocated to |
|---|---|---|---|---|---|---|---|---|
| QP checking procedure | MORE TIME | | QP takes longer than expected to check train | Operational delay – train does not move | Procedure will protect by not allowing train to depart<br>Training<br>Employee vigilance | | None | |
| QP checking procedure | LESS TIME | | QP completes his procedure and talks to the signaller prior to receiving feedback from driver acknowledging that the guard has completed his procedure | Signaller clears the road and driver proceeds, or driver waits for the guard bell. No change to current consequence. | Inching movement<br>Horn for emergency<br>8 km/h speed limit<br>Training<br>Employee vigilance<br>Procedure | | None | |
| QP checking procedure | ABNORMAL CONDITIONS | | Signal failure | This procedure will be stopped and another procedure will be used to address the signal failure | Another separate procedure will be undertaken<br>Training<br>Employee vigilance | | None | |
| QP checking procedure | ABNORMAL CONDITIONS | | Severe weather, darkness, utility (lights) failure, QP slips over | QP slips, trips or falls<br>Procedure ensures that the train will not move and eventually someone would notice his absence<br>Operational delay | PPE<br>Torch<br>Training<br>Driver and signaller vigilance<br>Procedure<br>Training<br>Employee vigilance | | None | |

| Property | Guide word | Deviation | Possible causes | Consequences | Existing controls | Comments | Actions required | Action allocated to |
|---|---|---|---|---|---|---|---|---|
| Guard checking procedure | PURPOSE | | Unclear why this procedure is applied and why it is not conducted elsewhere, as it appears not to be associated with horn | Opening doors introduces risk of people jumping onto the train and getting caught in doors or knocked onto the ground<br>Opening doors introduces risk of over-carries gaining access to rail corridor | The guard and the QP are acting as look-outs to observe this behaviour<br>Training<br>Employee vigilance<br>Additional staff checking train prior to its arriving at stabling yard and managing people on train | | Consider changing procedure so that the doors remain closed. As having the doors opened was a recommendation from a previous risk assessment, check that this action does not adversely affect the risk level. | J. Suffield |
| Guard checking procedure | PURPOSE | | Because doors open on both sides and close simultaneously, guard could unknowingly allow someone to get on (or off) the train (on opposite side to where he is checking) | Person could get on and off the train, exposing themselves to danger (adjacent track infrastructure) | | | Consider changing the procedure so that doors only open one side at a time or, alternately, review the need to open doors. As having the doors opened was a recommendation from a previous risk assessment, check that this action does not adversely affect the risk level. | J. Suffield |
| Guard checking procedure | NO ACTION | | PA system fails to work | Procedure does not provide guidance to the guard as to what to do in this situation | Training<br>Employee vigilance | | Update the procedure to ensure that appropriate action is taken in the event of PA failure | J. Suffield |
| Guard checking procedure | NO ACTION | | Guard fails to check as per procedure | No difference to the rest of network except no horn warning. Potential fatality | Inching movement<br>Horn for emergency<br>8 km/h speed limit<br>Training<br>Employee vigilance<br>Procedure | | None | |

| Property | Guide word | Deviation | Possible causes | Consequences | Existing controls | Comments | Actions required | Action allocated to |
|---|---|---|---|---|---|---|---|---|
| Guard checking procedure | WRONG ACTION | | Guard uses bell as per procedure | Driver wrongly interprets guard's bell and proceeds against signal. Potentially fatal for QP. | Inching movement<br>Horn for emergency<br>8 km/h speed limit<br>Training<br>Employee vigilance<br>Procedure | Change the procedure to replace the guard's bell with an intercom communication | | J. Suffield |
| Guard checking procedure | MORE TIME | | Guard takes more time than expected to complete an activity | Operational delay – train does not move | Procedure will protect by not allowing train to depart<br>Training<br>Employee vigilance | | None | |
| Guard checking procedure | WRONG INFORMATION | | Guard and driver have been placed on wrong train | QP applies procedure to check wrong train<br>Operational delay Wrong train dispatched (big operational impact) | Signaller will tell QP that it is the wrong train | | None | |
| Guard checking procedure | ABNORMAL CONDITIONS | | Signal failure | This procedure will be stopped and another procedure will be used to address the signal failure | Another separate procedure will be undertaken<br>Training<br>Employee vigilance | | None | |

| Property | Guide word | Deviation | Possible causes | Consequences | Existing controls | Comments | Actions required | Action allocated to |
|---|---|---|---|---|---|---|---|---|
| Guard checking procedure | ABNORMAL CONDITIONS | | Guard unable to see last 4 cars and there is no requirement | Last 4 cars not checked, so no assurance that they are clear<br>Procedure is not explicit about what to do | Inching movement<br>Horn for emergency<br>8 kph speed limit<br>Training<br>Employee vigilance<br>Procedure | | Review procedure and advise an appropriate action (it is currently inconsistent with the QP role) | J. Suffield |

# Bibliography

IEC 60812:2006, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 61025:2006, *Fault tree analysis (FTA)*

IEC 61160:2005, *Design review*

IEC 61511-3:2003, *Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels*

IEC 62502:2010, *Analysis techniques for dependability – Event tree analysis (ETA)*

IEC/ISO 31010:2009, *Risk Management – Risk Assessment Techniques*

ISO 31000:2009, *Risk Management – Principles and guidelines*

ISO Guide 73:2009, *Risk Management – Vocabulary*

Defence Standard 00-58:2000, HAZOP Studies on Systems containing Programmable Electronics, Ministry of Defence, UK

*A Guide to Hazard and Operability Studies.* Chemical Industries Association, London, UK, 1992

*Das PAAG-Verfahren.* International Social Security Association, (ISSA), c/o BG RCI, Heidelberg, Germany, 2000, ISBN 92-843-7037-X (see also http://www.issa.int/ger/resurs/resources/das-paag-verfahren)

*Storingsanalyse Waarom? Wanneer? Hoe?* Directoraat-Generaal van de Arbeid 1982, ISBN 9053070427, 9789053070420 (body of text in Dutch, appendices in English)

Kletz, Trevor A. HAZOP and HAZAN – Identifying and Assessing Chemical Industry Hazards, (4th Edition), Taylor & Francis, 2006, ISBN 0852955065

Knowlton, Ellis. *An Introduction to Hazard and Operability Studies, the Guide Word Approach*, Chemetics International, Vancouver, Canada, 1992, ISBN 0-9684016-0-0 (also available in French, Spanish, Finnish, Arabic, Chinese, Hindi and Korean)

Knowlton, Ellis. *A manual of Hazard & Operability Studies, The creative identification of deviations and disturbances*. Chemetics International, Vancouver, Canada, 1992, ISBN 0-9684016-3-5

Redmill, Felix; Chudleigh, Morris and Catmur, James. *System Safety: HAZOP and Software HAZOP*. Wiley, 1999, ISBN 0-471-98280-6

Crawley, Frank; Preston, Malcolm and Tyler, Brian. *HAZOP: Guide to best practice. Guidelines to best practice for the process and chemical industries*. Ed 2 European Process Safety Centre, Chemical Industries Association & Institution of Chemical Engineers, Rugby, England, IChem, 2008, ISBN 978 0-85295-525 3

*Guidelines for Hazard Evaluation Procedures.* Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, USA, 1999, ISBN 0-8169-0491-X

_____

# SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

# ÉTUDES DE DANGER ET D'EXPLOITABILITÉ (ÉTUDES HAZOP) – GUIDE D'APPLICATION

## AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 61882 a été établie par le comité d'études 56 de l'IEC: Sûreté de fonctionnement.

Cette deuxième édition annule et remplace la première édition parue en 2001. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) terminologie clarifiée, et alignement sur les termes et définitions de l'ISO 31000:2009 et du Guide ISO 73:2009;
b) ajout d'une étude de cas améliorée d'un HAZOP de procédure.

Le texte de cette norme est issu des documents suivants:

| FDIS | Rapport de vote |
|---|---|
| 56/1653/FDIS | 56/1666/RVD |

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

# INTRODUCTION

La présente norme décrit les principes et l'approche relatifs à l'identification des risques à partir de mots-guides. Historiquement, cette approche de l'identification des risques a été appelée étude de danger et d'exploitabilité ou, par abréviation, étude HAZOP. Il s'agit d'une technique structurée et systématique appliquée à l'examen d'un système défini en vue:

- d'identifier les risques liés à l'exploitation et à la maintenance du système. Les phénomènes dangereux ou les autres sources de risque peuvent comprendre à la fois ceux qui se présentent seulement à proximité immédiate du système et ceux qui ont des effets plus étendus, par exemple certains phénomènes dangereux environnementaux;
- d'identifier les problèmes potentiels d'exploitabilité posés par le système et, en particulier, les causes des perturbations d'exploitation et des écarts dans la production susceptibles d'entraîner la fabrication de produits non conformes.

Un avantage important des études HAZOP est que la connaissance qu'elles apportent, en identifiant de manière structurée et systématique les risques et les problèmes d'exploitabilité, s'avère d'une grande utilité pour déterminer les mesures à prendre.

Une des caractéristiques d'une étude HAZOP est la session d'examen durant laquelle une équipe multidisciplinaire dirigée par un chef d'étude examine systématiquement toutes les parties d'une conception ou d'un système concernées par l'étude. Elle identifie les écarts par rapport à l'intention de conception du système, en utilisant un ensemble de mots-guides. La technique vise à stimuler de manière systématique l'imagination des participants pour les aider à identifier les risques et les problèmes d'exploitabilité. Il convient de considérer une étude HAZOP comme une amélioration d'une conception juste, utilisant des approches basées sur l'expérience, telles que les règles de bon usage, plutôt qu'un succédané de ces approches.

Historiquement, les études HAZOP et assimilées étaient présentées comme une identification des phénomènes dangereux dont l'objectif premier est de soumettre à l'essai de manière systématique la présence de phénomènes dangereux et, le cas échéant, de comprendre à la fois comment ils pourraient provoquer des conséquences négatives et comment une nouvelle conception du processus pourrait les éviter. L'ISO 31000:2009 définit le risque comme l'effet de l'incertitude concernant les objectifs, en notant que l'effet est un écart par rapport à ce qui est escompté. C'est pourquoi les études HAZOP, qui ont trait aux écarts par rapport à ce qui est escompté, ainsi qu'à leurs causes et à leurs effets sur les objectifs dans le cadre de la conception du processus, sont désormais correctement caractérisées comme de puissants outils d'identification des risques.

Il existe de nombreux outils et techniques destinés à identifier les risques, depuis les listes de contrôle jusqu'à HAZOP en passant par l'analyse des modes de défaillance et de leurs effets (AMDE). Certaines techniques, telles que les listes de contrôle et l'analyse par simulation, peuvent être utilisées dès le début du cycle de vie du système alors qu'il existe peu d'informations, ou lors d'une phase ultérieure si une analyse moins détaillée est nécessaire. Les études HAZOP exigent plus de détails sur les systèmes à l'étude, mais fournissent des informations plus complètes sur les risques et les faiblesses dans la conception du système.

Le terme HAZOP est parfois associé, dans un sens plus large, à d'autres techniques d'identification des phénomènes dangereux (par exemple HAZOP sur liste de contrôle, HAZOP 1 ou 2, HAZOP basé sur les connaissances, etc.). L'utilisation du terme HAZOP en relation avec ces techniques est considérée comme inappropriée et elle est volontairement exclue de ce document.

Avant de commencer une étude HAZOP, il convient de s'assurer qu'il s'agit de la technique la plus appropriée (autant individuellement qu'en combinaison avec d'autres techniques) pour la présente tâche. Il convient que cette appréciation prenne en compte l'objet de l'étude, la sévérité de toutes les conséquences possibles, le niveau approprié de détail, la disponibilité des données et des ressources pertinentes ainsi que les besoins des décisionnaires.

La présente norme a été mise au point pour donner les lignes directrices dans un grand nombre d'industries et types de systèmes. Dans certaines industries, notamment les industries de transformation où cette technique a vu le jour, il existe des normes et des guides plus spécifiques qui établissent des méthodes d'application préférentielles pour ces industries. Pour plus de détails, voir la bibliographie donnée en annexe de la présente norme.

# ÉTUDES DE DANGER ET D'EXPLOITABILITÉ (ÉTUDES HAZOP) – GUIDE D'APPLICATION

## 1 Domaine d'application

La présente Norme internationale constitue un guide pour les études HAZOP de systèmes qui utilisent des mots-guides. Elle donne des lignes directrices relatives à l'application de la technique et à la procédure de l'étude HAZOP, y compris la définition, la préparation, les sessions d'examen ainsi que les documents et le suivi qui en résultent.

Elle fournit également des exemples de documentation ainsi qu'un grand choix d'exemples concernant diverses applications qui présentent les études HAZOP.

## 2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60050-192, *Vocabulaire électrotechnique international – Partie 192: Sûreté de fonctionnement* (disponible à l'adresse http://www.electropedia.org)

## 3 Termes, définitions et abréviations

### 3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'IEC 60050-192 ainsi que les suivants s'appliquent.

NOTE Dans cet article, les termes définis sont en caractères *italiques*.

**3.1.1**
**caractéristique**
propriété qualitative ou quantitative

EXEMPLE Pression, température, tension.

**3.1.2**
**conséquence**
effet d'un événement affectant les objectifs

Note 1 à l'article: Un événement peut engendrer une série de conséquences.

Note 2 à l'article: Une conséquence peut être certaine ou incertaine, elle peut avoir des effets positifs ou négatifs sur l'atteinte des objectifs.

Note 3 à l'article: Les conséquences peuvent être exprimées de manière qualitative ou quantitative.

Note 4 à l'article: Des conséquences initiales peuvent déclencher des réactions en chaîne.

[SOURCE: ISO Guide 73:2009, 3.6.1.3]

**3.1.3**
**moyen de maîtrise**
mesure qui modifie un *risque* (3.1.12)

Note 1 à l'article: Un moyen de maîtrise du risque inclut n'importe quels processus, politique, dispositif, pratique ou autres actions qui modifient un risque.

Note 2 à l'article: Un moyen de maîtrise du risque n'aboutit pas toujours nécessairement à la modification voulue ou supposée.

[SOURCE: ISO Guide 73:2009, 3.8.1.1]

**3.1.4**
**intention de conception**
gamme de comportements que souhaite ou spécifie le concepteur pour les propriétés qui assurent que l'élément satisfasse à ses exigences

**3.1.5**
**propriété**
composant d'une partie servant à identifier les caractéristiques essentielles de la partie

Note 1 à l'article: Le choix des propriétés peut dépendre de l'application particulière, mais les propriétés peuvent inclure des caractéristiques telles que le matériel concerné, l'activité exécutée, l'équipement utilisé, etc. Il convient que le matériel soit considéré au sens large et comprenne les données, le logiciel, etc.

**3.1.6**
**mot-guide**
mot ou phrase qui exprime et définit un type particulier d'écart par rapport à l'intention de conception d'une propriété

**3.1.7**
**dommage**
blessure physique et/ou atteinte à la santé des personnes, aux biens ou à l'environnement

**3.1.8**
**phénomène dangereux**
source de *dommage* (3.1.7) potentiel

Note 1 à l'article: Un phénomène dangereux peut être une *source de risque* (3.1.14).

[SOURCE: ISO Guide 73:2009, 3.5.1.4]

**3.1.9**
**niveau de risque**
importance d'un *risque* (3.1.12) ou combinaison de risques, exprimée en termes de combinaison des *conséquences* (3.1.2) et de leur vraisemblance

[SOURCE: ISO Guide 73:2009, 3.6.1.8]

**3.1.10**
**directeur**
personne responsable d'un projet, d'une activité ou d'une organisation

**3.1.11**
**partie**
section du système faisant l'objet de l'étude actuelle

Note 1 à l'article: Une partie peut être physique (par exemple: matériel) ou logique (par exemple: étape d'une séquence de fonctionnement).

**3.1.12**
**risque**
effet de l'incertitude sur l’atteinte des objectifs

Note 1 à l'article: Un effet est un écart positif et/ou négatif, par rapport à une attente.

Note 2 à l'article: Les objectifs peuvent avoir différents aspects (par exemple buts financiers, de santé et de sécurité, ou environnementaux) et peuvent concerner différents niveaux (niveau stratégique, niveau d'un projet, d'un produit, d'un processus ou d'un organisme tout entier).).

Note 3 à l'article: Un risque est souvent caractérisé en référence à des événements et des *conséquences* (3.1.2) potentiels ou à une combinaison des deux.

Note 4 à l'article: Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa vraisemblance.

Note 5 à l'article: L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.

[SOURCE: ISO Guide 73:2009, 1.1]

**3.1.13**
**identification des risques**
processus de recherche, de reconnaissance et de description des *risques* (3.1.12)

Note 1 à l'article: L'identification des risques comprend l’identification des *sources de risque* (3.1.14), des événements, de leurs causes et de leurs *conséquences* (3.1.2) potentielles.

Note 2 à l'article: L'identification des risques peut faire appel à des données historiques, des analyses théoriques, des avis d'experts et autres personnes compétentes et tenir compte des besoins des parties prenantes.

[SOURCE: ISO Guide 73:2009, 3.5.1]

**3.1.14**
**source de risque**
tout élément qui, seul ou combiné à d'autres, présente un potentiel intrinsèque d'engendrer un *risque* (3.1.12)

Note 1 à l'article: Une source de risque peut être tangible ou intangible.

[SOURCE: ISO Guide 73:2009, 3.5.1.2]

**3.1.15**
**traitement du risque**
processus destiné à modifier un *risque* (3.1.12)

Note 1 à l'article: Le traitement du risque peut inclure:

– un refus du risque en décidant de ne pas démarrer ou poursuivre l'activité porteuse du risque;
– la prise ou l'augmentation d'un risque afin de saisir une opportunité;
– l'élimination de la *source de risqu*e (3.1.14);
– une modification de la *vraisemblance*;
– une modification des *conséquences* (3.1.2);
– un partage du risque avec une ou plusieurs autres parties [incluant des contrats et un **financement du risque et**
– un maintien du risque fondé sur une décision argumentée.

Note 2 à l'article: Les traitements du risque portant sur les conséquences négatives sont parfois appelés «atténuation du risque», «élimination du risque», «prévention du risque» et «réduction du risque»

Note 3 à l'article: Eclaircissement concernant le traitement du risque et le *moyen de maîtrise* (3.1.3) du risque – un moyen de maîtrise du risque est déjà en place, tandis qu'un traitement du risque est une activité destinée à améliorer les moyens de maîtrise du risque. Un traitement mis en œuvre devient donc un moyen de maîtrise.

[SOURCE: ISO Guide 73:2009, 3.8.1, modifié — la note 3 à l'article remplace la note 3 existante]

### 3.2 Abréviations

| | |
|---|---|
| ATP | automatic train protection (protection automatique des trains) |
| EER | escape, evacuation and rescue (évacuation et sauvetage) |
| AAE | analyse par arbre d'événement |
| AMDE | analyse des modes de défaillance et de leurs effets |
| AAP | analyse par arbre de panne |
| GPA | general purpose alarm (alarme générale) |
| HAZOP | hazard and operability (danger et exploitabilité) |
| G | gauche |
| LOPA | layer of protection analysis (analyse de la couche de protection) |
| OIM | offshore installation manager (directeur d'installation en mer) |
| P&IDs | process and instrumentation diagrams (schémas de processus et d'instrumentation) |
| PAPA | prepare to abandon platform alarm (alarme de préparatifs pour abandonner la plate-forme) |
| PA | public address (annonce du public) |
| PES | programmable electronic system (système électronique programmable) |
| EPI | équipement de protection individuelle |
| PQ | personne qualifiée |
| D | droite |

## 4 Principales caractéristiques de HAZOP

### 4.1 Généralités

Une étude HAZOP est un processus détaillé réalisé par une équipe spécialisée, destiné à identifier les risques et les problèmes d'exploitabilité. Les études HAZOP s'attachent à l'identification des écarts potentiels par rapport à l'intention de conception, à l'examen de leurs causes possibles et à l'évaluation de leurs conséquences.

Les principales caractéristiques d'une étude HAZOP sont, entre autres, celles indiquées ci-dessous.

- L'étude est un processus créatif qui consiste à utiliser systématiquement une série de mots-guides pour identifier des écarts potentiels par rapport à l'intention de conception et à les utiliser pour inciter les membres de l'équipe à trouver ce qui pourrait provoquer l'écart et quelles pourraient en être les conséquences.
- L'étude se déroule sous la direction d'un chef d'étude qualifié et expérimenté qui doit veiller à l'examen exhaustif du système à l'étude, s'appuyant sur une pensée logique et analytique. Le chef d'étude est assisté de préférence par un rapporteur qui consigne les données pertinentes associées aux risques et/ou aux perturbations d'exploitation identifiés pour arriver à une analyse, une évaluation et un traitement du risque.
- L'étude est confiée à des spécialistes de diverses disciplines qui ont les compétences et l'expérience appropriées et font preuve d'intuition et de perspicacité.
- Il convient que l'étude soit menée dans une atmosphère de réflexion critique, dans une atmosphère de franchise et d'ouverture.
- Une étude HAZOP fait l'objet de procès-verbaux ou produit des logiciels dans lesquels sont consignés les écarts, leurs causes, leurs conséquences et les mesures

recommandées, accompagnées de dessins annotés, de documents ou d'autres représentations du système comportant le numéro du rapport associé et si possible l'action recommandée.

- Le principal objectif de l'examen HAZOP n'est pas de développer des actions de traitement du risque pour les risques ou les problèmes d'exploitabilité identifiés. Il convient cependant de faire des recommandations, lorsqu'elles sont appropriées, et de les consigner pour être consultées par les responsables de la conception du système.
- L'étude HAZOP initiale pourrait être réalisée de manière progressive afin de pouvoir incorporer les modifications de conception, mais l'étude HAZOP achevée doit correspondre à l'intention finale de conception.
- Il convient de revoir régulièrement les études HAZOP existantes pour apprécier si l'intention de conception ou les phénomènes dangereux ont changé, mais aussi de les revoir à d'autres phases du cycle de vie, comme la phase d'amélioration.

### 4.2 Principes de l'examen

Le principe d'une étude HAZOP est l'"examen avec des mots-guides", qui est une recherche réfléchie des écarts par rapport à l'intention de conception. Pour faciliter l'examen, un système est divisé en plusieurs parties de telle sorte que l'intention de conception ou la fonction puisse être définie de manière adéquate pour chacune d'elles. La taille des parties choisie dépend généralement de la complexité du système et de l'importance et de la portée potentielle des conséquences. Dans des systèmes complexes ou dans ceux où le niveau de risque escompté pourrait être élevé, les parties peuvent être petites par rapport au système. Dans des systèmes simples ou dans ceux où le niveau de risque escompté pourrait être faible, des parties plus grandes seront utilisées pour mener l'étude.

L'intention de conception pour une partie donnée d'un système est formulée en termes de propriétés, qui indiquent les caractéristiques essentielles de la partie et en représentent les divisions naturelles. Le choix des propriétés à examiner est dans une certaine mesure une décision subjective, puisqu'il pourrait exister plusieurs combinaisons qui mèneront au but exigé, et que le choix peut également dépendre de l'application particulière. Les parties peuvent être des étapes ou des phases discrètes d'une procédure, des clauses d'un contrat, des signaux individuels et des pièces d'équipement d'un système de commande, un équipement ou des composants d'un processus ou d'un système électronique, etc.

Dans certains cas, il pourrait être utile d'exprimer la fonction d'une partie dans les termes suivants:

– matériau d'entrée provenant d'une certaine source;
– activité réalisée sur ce matériau;
– élément de sortie transporté vers une destination.

L'intention de conception comprendra donc les éléments suivants: entrées et sorties, fonctions, activités, sources et destinations, qui peuvent être considérés comme des propriétés de la partie.

La définition des propriétés peut souvent être utilement précisée en termes de caractéristiques, qui peuvent être soit quantitatives, soit qualitatives. Par exemple, dans un système chimique, les entrées pourraient être définies plus précisément en termes de caractéristiques telles que la température, la pression et la composition. Pour une activité de transport, des caractéristiques telles que la vitesse de déplacement, la charge ou le nombre de passagers pourraient être pertinentes. Pour des systèmes informatiques, les caractéristiques de chaque partie seront par exemple la communication, les interfaces et le traitement des données.

Pour chacune des parties, l'équipe de l'étude HAZOP vérifie si chaque propriété présente, par rapport à l'intention de conception, un écart qui peut avoir des conséquences non souhaitables (ou souhaitables). Pour identifier ces écarts par rapport à l'intention de

conception, elle emploie un système de questions dans lequel interviennent des mots-guides prédéfinis. Le rôle du mot-guide est de stimuler l'imagination, de focaliser l'étude et de soulever des idées et des discussions, de façon à optimiser les chances de réaliser une étude complète. Un exemple de mots-guides fondamentaux et de leurs significations est présenté dans le Tableau 1.

**Tableau 1 – Exemple de mots-guides fondamentaux et de leurs significations génériques**

| Mot-guide | Signification |
|---|---|
| NE PAS FAIRE | Négation totale de l'intention de conception |
| PLUS | Augmentation quantitative |
| MOINS | Diminution quantitative |
| EN PLUS DE | Modification/augmentation qualitative |
| PARTIE DE | Modification/diminution qualitative |
| INVERSE | Contraire logique de l'intention de conception |
| AUTRE QUE | Remplacement total |

Le Tableau 2 donne un autre exemple de mots-guides relatifs à l'heure, à un ordre ou une séquence.

**Tableau 2 – Exemple de mots-guides relatifs à l'heure et à un ordre ou une séquence**

| Mot-guide | Signification |
|---|---|
| PLUS TOT | Relatif à l'heure |
| PLUS TARD | Relatif à l'heure |
| AVANT | Relatif à un ordre ou une séquence |
| APRES | Relatif à un ordre ou une séquence |

Des mots-guides supplémentaires peuvent servir à faciliter l'identification des écarts, à condition d'avoir été définis avant le début de l'examen.

Une fois que la partie à soumettre à l'examen a été choisie, l'intention de conception de cette partie est spécifiée sous forme de propriétés discrètes. Chacun des mots-guides pertinents est alors appliqué à chaque propriété pour procéder à une recherche systématique des écarts. Après l'application d'un mot-guide, les causes et les conséquences possibles d'un écart donné sont examinées. Les mécanismes destinés à contrôler les conséquences prévues peuvent aussi faire l'objet d'une enquête. Les résultats de l'examen sont enregistrés sous un format convenu (voir 6.5.2).

Les associations mot-guide/propriété peuvent être assimilées à une matrice. Chaque case de la matrice ainsi formée contiendra une combinaison mot-guide/propriété particulière. Pour parvenir à une identification complète du risque, les propriétés doivent recouvrir tous les aspects de l'intention de conception et les mots-guides doivent recouvrir tous les écarts possibles. Toutes les combinaisons ne donneront pas des écarts crédibles, de sorte que la matrice peut présenter plusieurs cases vides quand toutes les combinaisons mot-guide/propriété sont prises en compte.

Le chef d'étude prédéfinira en général la combinaison mot-guide/propriété applicable pour que le processus d'identification des risques soit plus efficace et pour exploiter au mieux les compétences et le temps des participants.

Les cellules de la matrice peuvent être utilisées suivant deux séquences pour examiner la partie choisie: colonne par colonne (c'est-à-dire la propriété d'abord) ou ligne par ligne (c'est-

à-dire le mot-guide d'abord). Les détails de l'examen sont présentés en 6.4 et les Figures 2 et 3 présentent les deux formes d'examen. En principe, il convient que les résultats de l'examen soient identiques.

En plus d'appliquer des mots-guides à des propriétés définies d'une partie, il peut également exister d'autres attributs, comme l'accès, l'isolation, le contrôle et l'environnement de travail (bruit, éclairage, etc.), qui sont importants pour l'exploitation souhaitée du système et auxquels un sous-ensemble de mots-guides peut être appliqué.

### 4.3 Plan de conception

#### 4.3.1 Généralités

Une des conditions préalables à la réalisation de l'examen est de disposer d'une représentation précise et complète de la conception du système à l'étude. Le plan de conception est un modèle descriptif du système qui décrit de manière appropriée le système à l'étude et ses parties, et qui identifie leurs propriétés. Le plan pourrait représenter la conception physique ou la conception logique: il convient d'indiquer clairement ce qu'il représente.

En règle générale, il convient que le plan de conception indique la fonction de chaque partie et élément du système, de façon qualitative ou quantitative. Il convient qu'il décrive également les interactions du système avec d'autres systèmes, avec son opérateur/utilisateur et, éventuellement, avec l'environnement. Par exemple, les P&ID sont susceptibles de fournir le niveau de détail exigé par le plan de conception. La conformité des propriétés ou caractéristiques à l’intention de conception détermine le bon fonctionnement et, dans certains cas, la sécurité du système.

La représentation du système se décompose en deux composants essentiels:

– les exigences du système; et
– une description physique et/ou logique de la conception.

La valeur d'une étude HAZOP dépend de l'étendue, de l'exactitude et de la précision du plan de conception, y compris l'intention de conception. Il convient que toute modification apportée à la conception d'origine soit représentée dans le plan de conception. Avant de commencer l'examen, il convient que l'équipe revoie l'ensemble des informations et qu'elle le corrige le cas échéant pour qu'il représente le système de manière appropriée.

#### 4.3.2 Exigences de conception et intention de conception

Les exigences de conception comprennent des exigences qualitatives et quantitatives auxquelles le système doit satisfaire et constituent la base du développement de la conception du système et de l'intention de conception. Il convient d'identifier toutes les manières d'utiliser le système de manière correcte ou incorrecte qui pourraient raisonnablement être prévues. Les exigences de conception ainsi que l'intention de conception qui en résulte doivent satisfaire aux exigences du client et à celles de la législation, des normes et des règles en vigueur.

Sur la base des exigences du système, le concepteur développe la conception du système; cela aboutit à une configuration du système où des fonctions spécifiques sont affectées aux sous-systèmes et aux composants. Les composants sont spécifiés et choisis. Il convient que le concepteur ne considère pas seulement ce que le système est censé faire, mais qu'il s'assure aussi que le système ne tombera pas en panne dans des conditions prévisibles ou qu'il ne présentera pas de défaillance ou de dégradation durant la durée de vie spécifiée. Il convient également qu'il identifie les comportements ou caractéristiques indésirables de manière à pouvoir les éliminer dès la conception ou à réduire le plus possible leurs effets par une conception ou une maintenance appropriée.

L'intention de conception forme la base de l'examen. Il convient qu'elle soit appropriée et correcte dans la mesure du possible. Bien que la vérification de l'intention de conception (voir l'IEC 61160) n'entre pas dans le domaine d'application de l'étude HAZOP, il convient que le chef d'étude s'assure que l'intention de conception est appropriée et correcte avant de permettre la poursuite de l'étude. En général, la plupart des intentions de conception documentées se limitent aux fonctions et paramètres fondamentaux du système dans les conditions normales d'exploitation.

Il convient d'identifier et de prendre en compte lors de l'examen les conditions d'exploitation anormales raisonnablement prévisibles et les activités non souhaitables qui pourraient se produire (par exemple vibrations importantes, conditions météorologiques extrêmes, arrêts anormaux ou intervention de tiers). Il convient d'identifier également les mécanismes de détérioration comme l'affaiblissement, la corrosion, le non-respect des procédures et d'autres mécanismes qui détériorent les propriétés du système et de les prendre en compte dans une étude qui utilise des mots-guides appropriés. Une étude plus détaillée concernant en particulier les modes de défaillance et leurs effets peut être exigée le cas échéant (voir l'IEC 60812).

Il convient également d'identifier et de prendre en compte la durée de vie prévue, la fiabilité, la maintenabilité et la supportabilité, ainsi que les sources de risque qui pourraient survenir au cours des activités de maintenance et de soutien logistique, dans la mesure où ces dernières font partie du domaine d'application de l'étude HAZOP.

## 5 Applications de HAZOP

### 5.1 Généralités

A l'origine, l'étude HAZOP était une technique développée pour les systèmes impliquant le traitement d'un fluide ou autre flux de matière dans les industries de transformation. De nos jours, il s'agit d'un élément clé pour la gestion de la sécurité des processus. Cependant, son domaine d'application n'a cessé de s'étendre au cours des dernières années, et la technique HAZOP s'applique aujourd'hui, par exemple:

– aux applications logicielles, y compris les systèmes électroniques programmables;
– aux systèmes assurant le déplacement des personnes par différents modes, tels que le transport routier, ferroviaire et aérien;
– à l'examen de différentes séquences et procédures d'exploitation;
– à l'évaluation des procédures administratives dans différentes industries;
– à l'évaluation de systèmes spécifiques, par exemple les dispositifs médicaux;
– au développement de logiciels et de codes;
– à l'évaluation des modifications organisationnelles proposées et à la définition des mécanismes permettant de les réaliser;
– à l'essai et à l'amélioration des projets de contrats et d'autres documents juridiques;
– à l'essai et à l'amélioration des documents, notamment des instructions et procédures pour les activités critiques.

Une étude HAZOP est particulièrement utile dans l'identification des faiblesses des systèmes (existants ou proposés) impliquant la circulation de matériels, de personnes ou d'informations, ou un certain nombre d'événements ou d'activités d'une séquence planifiée, ou les procédures contrôlant cette séquence. Les études HAZOP peuvent aussi être utilisées dans un domaine autre que l'exploitation, par exemple le stockage et le transport. HAZOP n'est pas seulement un outil précieux pour la conception et le développement de nouveaux systèmes, mais peut aussi être utilisé avec profit pour identifier les risques et les problèmes potentiels liés à différents états d'exploitation d'un système donné, par exemple les états de démarrage, d'attente, de fonctionnement normal, d'arrêt normal, d'arrêt d'urgence. Il peut également être employé dans les processus et les séquences de fabrication par lot et en régime instable,

ainsi que dans les processus et séquences continus. HAZOP fait partie intégrante du processus de conception. C'est une des méthodes qui peuvent être utilisées pour l'identification des risques dans le cadre du processus de gestion des risques (voir l'ISO 31000).

### 5.2 Relation avec d'autres outils d'analyse

L'étude HAZOP peut être utilisée en association avec d'autres méthodes d'identification et d'analyse du risque (voir l'IEC/ISO 31010) comme l'AMDE (voir l'IEC 60812) et l'AAP (voir l'IEC 61025) ou la LOPA (voir l'IEC 61511-3: 2003, Annexe F). De telles combinaisons pourraient être utilisées dans les situations exposées ci-dessous:

– l'étude HAZOP indique clairement que les performances d'un composant particulier d'un système sont critiques et doivent être examinées de façon plus approfondie: l'étude HAZOP peut alors être utilement complétée par une AMDE de ce composant;

– une fois que les écarts par rapport à une propriété donnée ont été examinés par une étude HAZOP, il est décidé d'appliquer l'AAP et l'AAE pour analyser l'effet de plusieurs déviations ou pour quantifier la vraisemblance d'une défaillance et ses conséquences.

L'AMDE part d'une défaillance possible d'un composant/d'une fonction, pour étudier ensuite les conséquences de cette défaillance sur l'ensemble du système. L'étude est donc unidirectionnelle dans le sens cause à effet. D'autre part, une étude HAZOP a pour but d'identifier les écarts possibles par rapport à une intention de conception puis de trouver les causes potentielles de l'écart et d'en prévoir les conséquences.

L'AAP peut être appliqué une fois que les écarts par rapport à une propriété donnée ont été identifiés par une étude HAZOP afin d'analyser l'effet de plusieurs déviations ou de quantifier la vraisemblance d'une défaillance et ses conséquences.

L'analyse LOPA utilise les données mises au point par l'étude HAZOP et indique la cause de déclenchement ainsi que les couches de protection qui modifient le risque. Elle peut ainsi être appliquée pour quantifier la réduction du risque obtenue par les moyens de maîtrise existants et pour vérifier si un traitement supplémentaire est nécessaire ou non.

### 5.3 Limites de l'étude HAZOP

Bien que les études HAZOP aient fait preuve d'une extrême utilité dans différentes industries, la technique a des limites dont il convient de tenir compte dans le choix d'une application. Un certain nombre de limites sont indiquées ci-après.

- Une étude HAZOP est une technique d'identification des risques qui étudie individuellement les parties d'un système et examine méthodiquement les effets des écarts sur chaque partie. Parfois, un risque très élevé impliquera une interaction entre un certain nombre de parties du système. Dans ces cas, il convient d'analyser le risque plus en détail à l'aide de techniques comme l'AAE (voir l'IEC 62502) et l'AAP (voir l'IEC 61025).
- Comme pour toute technique d'identification des risques ou des problèmes d'exploitabilité, il ne peut être garanti que l'étude HAZOP les identifiera tous. Par conséquent, il convient que l'étude d'un système complexe ne repose pas uniquement sur une étude HAZOP. Il convient d'utiliser la technique conjointement avec d'autres approches pertinentes et de la coordonner à d'autres études appropriées dans un système global efficace de gestion.
- La plupart des systèmes sont fortement interconnectés. Un écart dans une partie peut donc avoir des causes et des conséquences dans d'autres parties du système. Les causes et les conséquences doivent être suivies dans tout le système pour comprendre le risque et lui appliquer le traitement approprié. Cependant, quand le système est fortement lié, il existe un danger que le suivi de toutes les éventualités ne soit pas complet. Une analyse plus rigoureuse des événements pourrait alors être exigée.
- Le succès d'une étude HAZOP dépend en grande partie de la capacité et de l'expérience du chef d'étude, et de la connaissance, de l'expérience et du niveau d'interaction des membres de l'équipe.

- Une étude HAZOP peut uniquement prendre en compte les parties qui apparaissent sur le plan de conception. Les activités et les opérations qui n'y apparaissent pas pourraient ne pas toujours être prises en compte. Ce problème peut être en partie résolu en appliquant à une partie une série de mots-guides supplémentaires non spécifiques qui ne sont pas à proprement parler des propriétés, comme l'accès et la maintenance, et aussi en ajoutant au processus une étape à la fin de laquelle un "contrôle de bon sens" est réalisé en utilisant une liste de contrôle.

## 5.4 Etudes d'identification des risques durant les différentes phases du cycle de vie du système

### 5.4.1 Phase de conception

Dans la phase de conception du cycle de vie d'un système, le concept et les principales parties du système sont décidés, mais la conception et la documentation détaillées exigées pour l'exécution de l'étude HAZOP n'existent pas. Cependant, les principaux risques doivent être identifiés au cours de cette phase, afin de pouvoir les prendre en considération dans la conception et de faciliter les études HAZOP ultérieures. Pour réaliser ces études, il convient d'utiliser d'autres méthodes fondamentales (certaines de ces méthodes sont décrites à titre d'exemple dans l'IEC/ISO 31010).

### 5.4.2 Phase de développement

D'un point de vue économique, le meilleur moment pour réaliser une étude HAZOP est celui où la conception détaillée est disponible et les méthodes d'exploitation ont été arrêtées. Il peut y avoir plusieurs itérations jusqu'à ce que la conception soit finalisée. Il importe de disposer d'un processus qui évaluera les implications de toute modification effectuée après l'exécution de l'étude HAZOP. Il convient que ce processus soit conservé pendant toute la durée de vie du système.

### 5.4.3 Phase de réalisation

Pendant la phase de réalisation, il est recommandé de réaliser une étude supplémentaire avant la mise en service, quand l'exploitation ou le démarrage initial du système peuvent mener à des niveaux significatifs de risque et que des séquences et des instructions de fonctionnement correctes sont critiques. Il convient aussi de réaliser ou de répéter l'étude quand un changement important a eu lieu dans la conception ou dans l'intention à une phase ultérieure. Il convient à ce stade que des données supplémentaires, telles que les instructions de mise en service et d'exploitation, soient disponibles. De plus, il convient que l'étude examine toutes les questions soulevées durant les études antérieures pour s'assurer qu'elles ont été traitées.

### 5.4.4 Phase d'utilisation

Il convient d'envisager d'appliquer ou de mettre à jour l'étude HAZOP avant la mise en œuvre d'une modification qui pourrait avoir des effets sur l'exploitation normale d'un système, en particulier si ces modifications pourraient amener des niveaux élevés de risque. Il convient d'envisager d'appliquer l'étude HAZOP avant la mise en œuvre d'une modification qui pourrait avoir des effets sur le fonctionnement normal d'un système, en particulier si ces modifications peuvent amener des niveaux élevés de risque. Il importe que la documentation de conception et les instructions d'exploitation utilisées dans une telle étude soient à jour.

### 5.4.5 Phase d'amélioration

La phase d'amélioration a pour but d'améliorer les performances, d'apporter des modifications qui répondent aux nouvelles conditions d'exploitation, de prolonger la durée d'exploitation et de remédier à l'obsolescence. Les études HAZOP peuvent être utilisées pour comprendre les implications de toute modification proposée, pour décider si elles sont acceptables et si de nouveaux moyens de maîtrise ou des modifications de moyens de maîtrise existants sont exigés. En menant des études destinées à identifier les risques associés à toute modification

proposée, il est important de prendre en compte les implications et les réponses pour le système global sans limiter l'étude à la partie ou à la propriété en cours de modification.

### 5.4.6 Phase de mise hors service

Lors de la phase de mise hors service, il pourrait être exigé de réaliser une étude relative aux activités de mise hors service, à l'arrêt de l'utilisation ou à l'élimination, si celle-ci révèle des risques différents de ceux de l'exploitation normale. Dès que la séquence des activités a été définie, des études HAZOP peuvent être appliquées à la séquence et aux procédures ainsi qu'aux modes d'exploitation provisoires.

## 6 Procédure de l'étude HAZOP

### 6.1 Généralités

Les études HAZOP comprennent essentiellement quatre étapes exécutées dans l'ordre de la Figure 1.

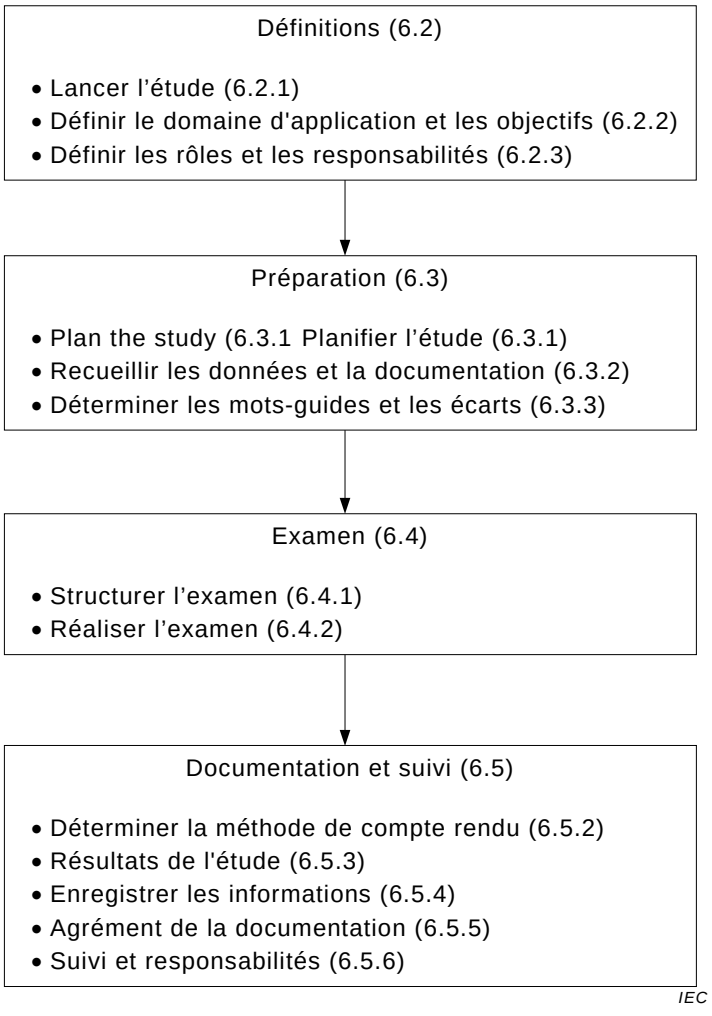


**Figure 1 – Déroulement d'une étude HAZOP**

## 6.2 Définitions

### 6.2.1 Lancer l'étude

En règle générale, l'étude est lancée par une personne responsable d'un projet, d'une activité ou d'une organisation, appelée "directeur" dans le présent guide. Il convient que le directeur décide du moment où il doit mener une étude, nomme un chef d'étude et lui fournisse les moyens nécessaires pour la réaliser.

La nécessité d'une telle étude aura souvent été ressentie durant la planification du fait d'exigences légales ou de la politique de l'organisation. Avec l'assistance du chef d'étude, il convient que le directeur définisse le domaine d'application et les objectifs de l'étude, mais également qu'il s'assure que les membres composant l'équipe de l'étude font preuve des compétences nécessaires pour la réalisation de cette étude.

Le directeur porte la responsabilité finale de s'assurer que toutes les actions liées à l'étude sont réalisées.

### 6.2.2 Définir le domaine d'application et les objectifs

Il convient d'établir clairement le domaine d'application d'une étude afin que:

– les frontières du système, ainsi que ses interfaces avec d'autres systèmes et l'environnement soient clairement définies;
– l'équipe d'étude se concentre sur certains aspects et ne se disperse pas dans d'autres aspects étrangers aux objectifs.

Le domaine d'application dépendra d'un certain nombre de facteurs comprenant:

– les frontières et l'étendue du système;
– le nombre et le niveau de détails du plan de conception disponible;
– le domaine d'application d'études antérieures dont le système a fait l'objet; et
– toute exigence réglementaire, toute règle ou norme applicable au système.

Pour définir les objectifs de l'étude, il convient de tenir compte des facteurs suivants:

– les objectifs pertinents de l'organisation;
– le but dans lequel les résultats de l'étude seront utilisés et ses relations avec les objectifs de l'organisation;
– la phase du cycle de vie du système au cours de laquelle l'étude doit être réalisée (pour les détails, voir 5.4);
– les questions d'exploitabilité, y compris les effets sur la qualité du produit;
– les personnes ou la propriété qui peuvent être exposées à un risque, par exemple le personnel, le public, l'environnement, le système;
– les exigences du système quant aux performances.

### 6.2.3 Définir les rôles et les responsabilités

Il convient que les rôles et les responsabilités de l'équipe d'étude soient clairement définis par le directeur, en accord avec le chef d'étude, dès le début de l'étude. En règle générale, il convient que le chef d'étude examine le plan de conception pour déterminer quelles sont les informations disponibles et quelles sont les qualifications exigées des membres de l'équipe. Il convient de mettre au point un programme d'activités qui indique le moment où sont prises les décisions, afin que toutes les recommandations puissent être appliquées en temps voulu.

Le chef d'étude est chargé d'assurer qu'il existe un mécanisme adapté pour communiquer les résultats de l'étude. Le directeur est chargé d'assurer le suivi des résultats de l'étude et de documenter de manière appropriée les décisions concernant les actions nécessaires.

Il convient que le directeur et le chef d'étude décident ensemble si l'équipe d'étude doit limiter son activité à identifier les risques et les problèmes (qui sont ensuite rapportés au directeur et aux concepteurs en vue de leur résolution) ou si elle suggère aussi les traitements possibles du risque. Dans le dernier cas, il est également nécessaire d'établir un accord concernant la responsabilité et le mécanisme destiné à choisir les traitements préférentiels du risque et à obtenir les autorisations appropriées pour toutes les mesures qui doivent être prises.

Une étude HAZOP est un effort d'équipe, chaque membre de l'équipe étant choisi pour remplir un rôle défini. Il convient que l'équipe soit aussi petite et homogène que possible et qu'elle dispose des compétences et de l'expérience nécessaires. Plus l'équipe est grande, plus le processus est lent. Il convient cependant que tous les domaines de connaissance soient représentés.

Lorsqu'un système a été conçu par un sous-traitant, il convient que l'équipe d'étude comprenne du personnel provenant à la fois du sous-traitant et du client.

Les rôles recommandés pour les membres de l'équipe sont les suivants:

– **Chef d'étude**: il n'est pas étroitement associé à l'équipe de conception et au projet. Il a été formé et a l'expérience de la direction d'études HAZOP. Responsable des communications entre la direction et l'équipe d'étude. Il planifie l'étude. Il donne son accord sur la composition de l'équipe d'étude. Il s'assure que l'équipe d'étude dispose des données représentatives de la conception. Il suggère des mots-guides et des combinaisons mot-guide/propriété à utiliser dans l'étude. Il facilite l'étude. Il assure que les résultats sont correctement consignés.
– **Rapporteur**: il rapporte les questions abordées lors des réunions. Il documente les risques et les problèmes identifiés, les recommandations faites et les mesures proposées. Il assiste le chef d'étude dans la planification et les tâches administratives. Dans certains cas, le chef d'étude peut tenir ce rôle. Il convient que le rapporteur ait des connaissances techniques d'un bon niveau en ce qui concerne le sujet à l'étude, des aptitudes linguistiques, et une bonne capacité d'écoute et de compréhension.
– **Concepteur (un ou plusieurs)**: il explique la conception et sa représentation. Il explique comment un écart défini peut se produire et la réponse correspondante du système ou de l'organisation.
– **Utilisateur (un ou plusieurs)**: il explique le contexte d'exploitation dans lequel le système fonctionnera, les conséquences d'un écart sur le fonctionnement et la mesure dans laquelle les écarts pourraient provoquer des conséquences inacceptables.
– **Spécialistes**: ils apportent une compétence concernant le système, l'étude, les phénomènes dangereux et leurs conséquences. Il pourrait être fait appel à eux pour une participation limitée.
– **Agent de maintenance**: personne qui maintiendra le système en état de fonctionnement.

Il pourrait également être nécessaire de faire appel à d'autres personnes comme les fournisseurs d'éléments importants du système, le fabricant et d'autres intervenants.

Les points de vue du concepteur et de l'utilisateur sont toujours exigés pour l'étude. Cependant, selon la phase du cycle de vie au cours de laquelle se déroule l'étude, le type de spécialiste le plus apte à participer pourrait varier.

Il convient que tous les membres de l'équipe aient une connaissance suffisante de la méthodologie HAZOP pour participer de façon efficace à l'étude; dans le cas contraire, il convient de leur fournir une formation appropriée.

### 6.3 Préparation

#### 6.3.1 Planifier l'étude

Le chef d'étude est responsable des travaux préparatoires suivants:

a) obtenir les informations sur le système;

b) convertir des informations dans un format approprié;

c) planifier la succession des réunions d'étude ou des ateliers; et

d) organiser les réunions nécessaires.

Par ailleurs, le chef d'étude pourrait réaliser une recherche dans des bases de données, etc., pour faire un historique des expériences liées aux mêmes systèmes ou à des systèmes similaires.

Le chef d'étude doit s'assurer qu'un plan de conception adéquat est disponible. Si le plan de conception est imparfait ou incomplet, il convient de le corriger avant le début de l'étude. Lors de la phase de planification d'une étude, il convient que les parties et les propriétés soient identifiées et fassent l'objet d'un accord avec une personne qui connaît très bien la conception.

Le chef d'étude est responsable de la préparation d'un plan d'étude; il convient que ce plan d'étude contienne les éléments suivants:

- les objectifs et le domaine d'application de l'étude;
- l'équipe d'étude;
- les détails techniques:
  - un plan de conception divisé en plusieurs parties avec la définition de l'intention de conception et, pour chaque partie, une liste des composants, du matériel et des activités ainsi que leurs propriétés;
  - une liste de mots-guides proposés et leur application aux propriétés du système décrit en 6.4.3;
- une liste de référence, de critères de conception, de règles ou de normes appropriés;
- les dispositions administratives, le programme des réunions, y compris les dates, heures et lieux;
- le formulaire de compte rendu exigé (voir l'Annexe A); et
- il convient de prévoir des locaux adaptés et des moyens audiovisuels pour permettre un déroulement efficace des réunions.

Il convient qu'une documentation de base, comprenant le plan de l'étude et les références nécessaires, soit envoyée aux membres de l'équipe d'étude avant la première réunion pour leur permettre de se familiariser avec son contenu. Un examen physique du système est souhaitable.

Le succès de l'étude dépend en grande partie de la vivacité et de la concentration des membres de l'équipe. Il est donc important que les séances ne soient pas trop longues et de les organiser à des intervalles appropriés. Il appartient finalement au chef d'étude de faire en sorte que ces exigences soient remplies.

#### 6.3.2 Recueillir les données et la documentation

Elle peut typiquement comprendre une partie de la documentation suivante qu'il convient d'identifier de façon claire et unique, d'approuver et de dater:

a) pour tous les systèmes:

- intentions de conception, exigences et descriptions;

b) pour les systèmes matériels:
   - schémas de circulation, schémas de blocs fonctionnels, schémas de contrôle, interfaces, schémas des circuits électriques, fiches techniques, dessins de montage, modèles en 3D (s'ils sont disponibles), spécifications des installations, exigences et instructions d'exploitation et de maintenance;

c) pour les systèmes d'écoulement:
   - schémas de tuyauterie/processus et d'instrumentation, spécifications du matériel et des équipements normalisés, disposition des canalisations et du système;

d) pour les systèmes électroniques programmables:
   - organigrammes des données, schémas de conception orientés objet, diagrammes de transition, chronogrammes, schémas logiques;

e) pour les systèmes liés à une procédure ou à un document:
   - projet de documents;
   - résultats des analyses de tâches ou matrices de décomposition fonctionnelle.

Les informations suivantes pourraient également être fournies:

- étendue et localisation des frontières du système à l'étude et des interfaces;
- informations concernant l'environnement externe et l'environnement interne dans lesquels fonctionnera le système;
- dispositions d'exploitation et de maintenance concernant le système;
- informations concernant la conception de l'interface utilisateur;
- historique de l'expérience issue de systèmes similaires.

### 6.3.3 Déterminer les mots-guides et les écarts

Dans la phase de planification d'une étude HAZOP, il convient que le chef d'étude propose une liste initiale de mots-guides à utiliser. Il convient qu'il soumette à l'essai les mots-guides proposés sur le système et confirme leur justesse. Il convient de choisir soigneusement les mots-guides. En effet, un mot-guide trop spécifique peut limiter les idées et la discussion, et un mot-guide trop général pourrait ne pas cerner correctement l'objet de l'étude HAZOP. Le Tableau 3 donne des exemples de différents types d'écarts avec les mots-guides associés.

**Tableau 3 – Exemples d'écarts et mots-guides associés**

| Type d'écart | Mot-guide | Exemple d'interprétation pour l'industrie de transformation | Exemple d'interprétation pour un système électronique programmable, PES |
|---|---|---|---|
| Négatif | NE PAS FAIRE | Aucune partie de l'intention n'est remplie, par exemple pas d'écoulement | Pas de données ou de signal de commande |
| Modification quantitative | PLUS | Augmentation quantitative, par exemple température plus élevée | Débit de données plus élevé que prévu |
| | MOINS | Diminution quantitative, par exemple température inférieure | Débit de données plus faible que prévu |
| Modification qualitative | EN PLUS DE | Présence d'impuretés<br>Exécution simultanée d'une autre opération/étape | Présence de signaux supplémentaires ou erronés |
| | PARTIE DE | Une partie seulement de l'intention est réalisée, c'est-à-dire que seulement une partie du transfert de fluide prévu a lieu | Les données ou les signaux de commande sont incomplets |
| Substitution | INVERSE | S'applique à l'inversion de l'écoulement dans les canalisations et à l'inversion des réactions chimiques | En principe non pertinent |
| | AUTRE QUE | Un résultat différent de l'intention originale est obtenu, c'est-à-dire transfert du mauvais matériau | Les données ou les signaux de commande sont incorrects |
| Temps | PLUS TOT | Un événement se produit avant l'heure prévue, par exemple refroidissement ou filtrage | Les signaux arrivent en avance par rapport à l'horloge |
| | PLUS TARD | Un événement se produit après l'heure prévue, par exemple refroidissement ou filtrage | Les signaux arrivent en retard par rapport à l'horloge |
| Ordre ou séquence | AVANT | Un événement se produit trop tôt dans une séquence, par exemple mélange ou chauffage | Les signaux arrivent plus tôt que prévu dans une séquence |
| | APRES | Un événement se produit trop tard dans une séquence, par exemple mélange ou chauffage | Les signaux arrivent plus tard que prévu dans une séquence |

Les combinaisons mot-guide/propriété peuvent être interprétées différemment dans les études de différents systèmes, à différentes phases du cycle de vie du système, et si elles sont appliquées à différents plans de conception. Certaines combinaisons pourraient ne pas avoir d'interprétations significatives pour une étude donnée et il convient de les ignorer. Le chef d'étude prédéfinira en général les combinaisons mot-guide/propriété qui sont appropriées pour le système. Il convient de définir et de documenter l'interprétation de toutes les combinaisons mot-guide/propriété. Si une combinaison donnée a plus d'une interprétation cohérente dans le contexte de la conception, il convient d'énumérer toutes les interprétations. D'autre part, il peut aussi arriver que la même interprétation vaille pour des combinaisons différentes. Dans ce cas, il convient de faire des renvois.

### 6.4 Examen

#### 6.4.1 Structurer l'examen

Il convient d'organiser les sessions d'examen de sorte que le chef d'étude facilite la discussion et suive le plan d'étude. Au début de la réunion d'étude, il convient que le chef d'étude ou un membre de l'équipe familiarisé avec le processus à étudier et ses problèmes:

- présente les grandes lignes du plan d'étude pour informer l'équipe de la nature du système ainsi que des objectifs et du domaine d'application de l'étude;
- présente de façon générale le plan de conception et explique les mots-guides ainsi que les propriétés proposées;

- passe en revue les risques et les problèmes d'exploitation identifiés ainsi que les secteurs critiques potentiels.

### 6.4.2 Réaliser l'examen

Il convient que l'analyse suive le déroulement ou la séquence relatifs au sujet de l'analyse, en procédant des entrées aux sorties dans une séquence logique. Il existe deux séquences d'examen possible: "propriété d'abord" et "mot-guide d'abord", comme le montrent respectivement les Figures 2 et 3. Il convient que le chef d'étude et l'équipe décident de la séquence à utiliser. La décision dépendra du détail d'exécution de l'examen HAZOP. D'autres facteurs de décision sont par exemple la nature des technologies concernées, le besoin de souplesse dans la conduite de l'examen et, dans une certaine mesure, la formation qu'ont reçue les participants.

La séquence "propriété d'abord" est décrite ci-après.

a) Le chef d'étude commence par choisir une partie du plan de conception comme point de départ et par la marquer. L'intention de conception de la partie est ensuite expliquée et les propriétés pertinentes sont identifiées.

b) Le chef d'étude choisit une des propriétés et consulte l'équipe pour savoir s'il convient d'appliquer le mot-guide directement au terme lui-même ou aux caractéristiques de cette propriété. Le chef d'étude détermine le mot-guide qui doit être appliqué en premier.

c) La première interprétation applicable au mot-guide est examinée dans le contexte de la propriété ou de la caractéristique à l'étude pour voir s'il existe un écart possible par rapport à l'intention de conception. Si un écart possible est identifié, ses causes et ses conséquences possibles sont recherchées.

d) Il convient que l'équipe décide s'il y aura un contrôle qui détectera et/ou indiquera un écart ou qui y répondra et qui pourrait être compris dans la partie choisie ou d'autres parties du système. Il convient que la présence de tels contrôles n'empêche pas d'identifier le risque ou le problème d'exploitabilité ni de spécifier le traitement ultérieur du risque.

e) Il convient que l'équipe spécifie les actions exigées pour traiter le risque le cas échéant. Il convient que la modification recommandée soit notée sur le plan et prise en compte dans la suite de l'étude. Il convient de réexaminer une partie, le cas échéant, à la suite d'une modification apportée à une autre partie.

f) Il convient que le chef d'étude résume les résultats lorsqu'ils sont enregistrés par le rapporteur. Si des travaux supplémentaires de suivi s'avèrent nécessaires, il convient que le nom du responsable de l'exécution de ces travaux soit également mentionné dans le compte rendu. Il convient de consigner l'avancement de l'étude à la fin de chaque séance.

g) Le processus est ensuite répété pour toute autre interprétation d'un mot-guide; puis pour un autre mot-guide; ensuite pour chaque propriété d'une partie à l'étude. Après l'examen complet d'une partie, il convient que le chef d'étude marque cette partie comme ayant été examinée. Le processus est répété jusqu'à ce que toutes les parties aient été étudiées.

Une fois que l'étude de chaque partie du système est terminée, l'équipe est invitée à examiner d'autres attributs comme l'accès, l'isolation, le contrôle et l'environnement de travail (bruit, éclairage, etc.), qui sont importants pour l'exploitation souhaitée du système. Cela pourrait impliquer d'examiner le système comme un tout au lieu de voir chaque partie isolément.

Une autre méthode d'application du mot-guide consiste à appliquer tour à tour le premier mot-guide à chacune des propriétés qui s'appliquent à une partie. Une fois cette opération terminée, l'étude passe au mot-guide suivant, qui est à nouveau appliqué tour à tour à chaque propriété. Le processus est répété jusqu'à l'utilisation de tous les mots-guides pour toutes les propriétés qui s'appliquent à la partie examinée, avant de passer à une autre partie (voir la Figure 3).

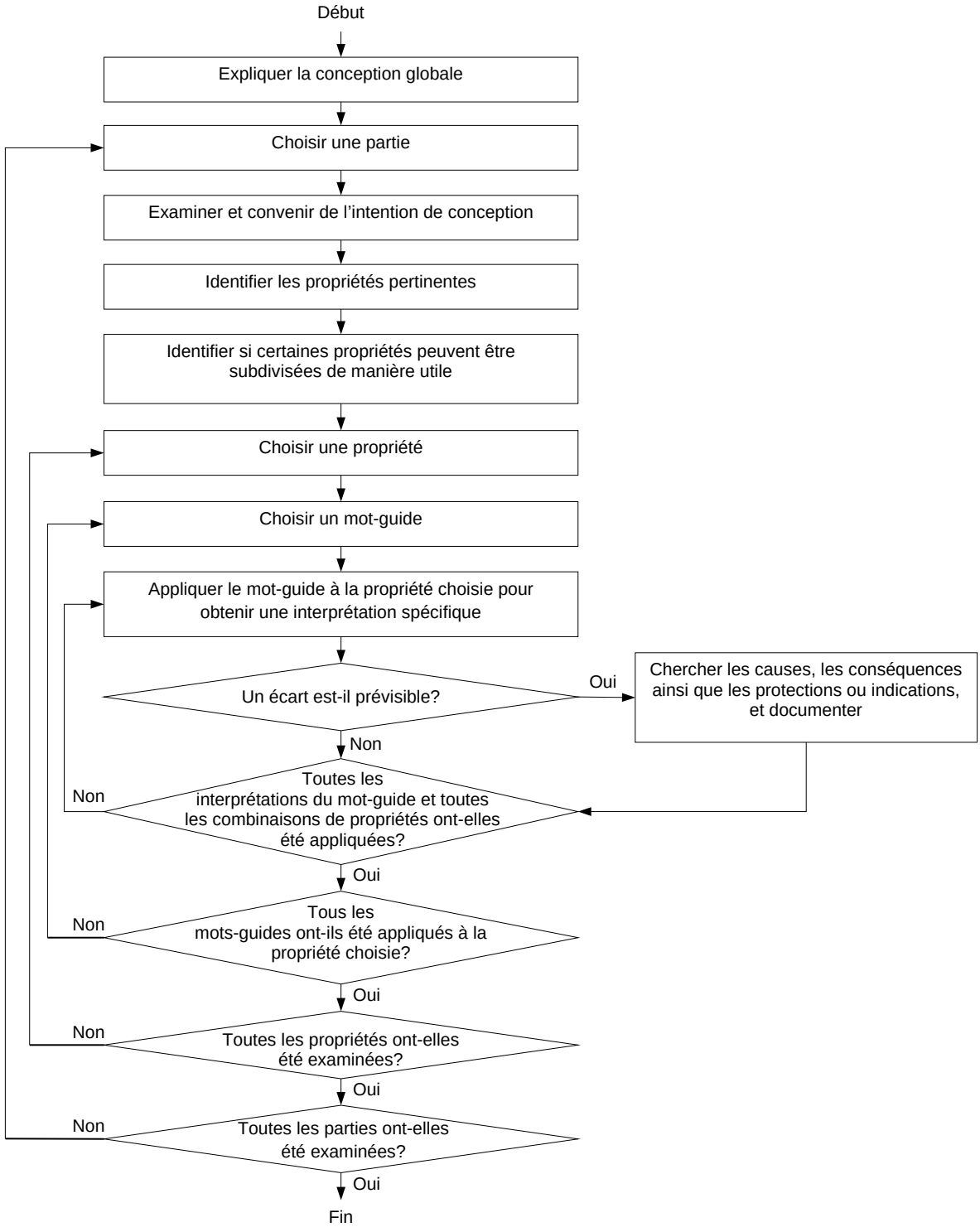


**Figure 2 – Organigramme de la procédure de l'examen HAZOP – Séquence propriété d'abord**

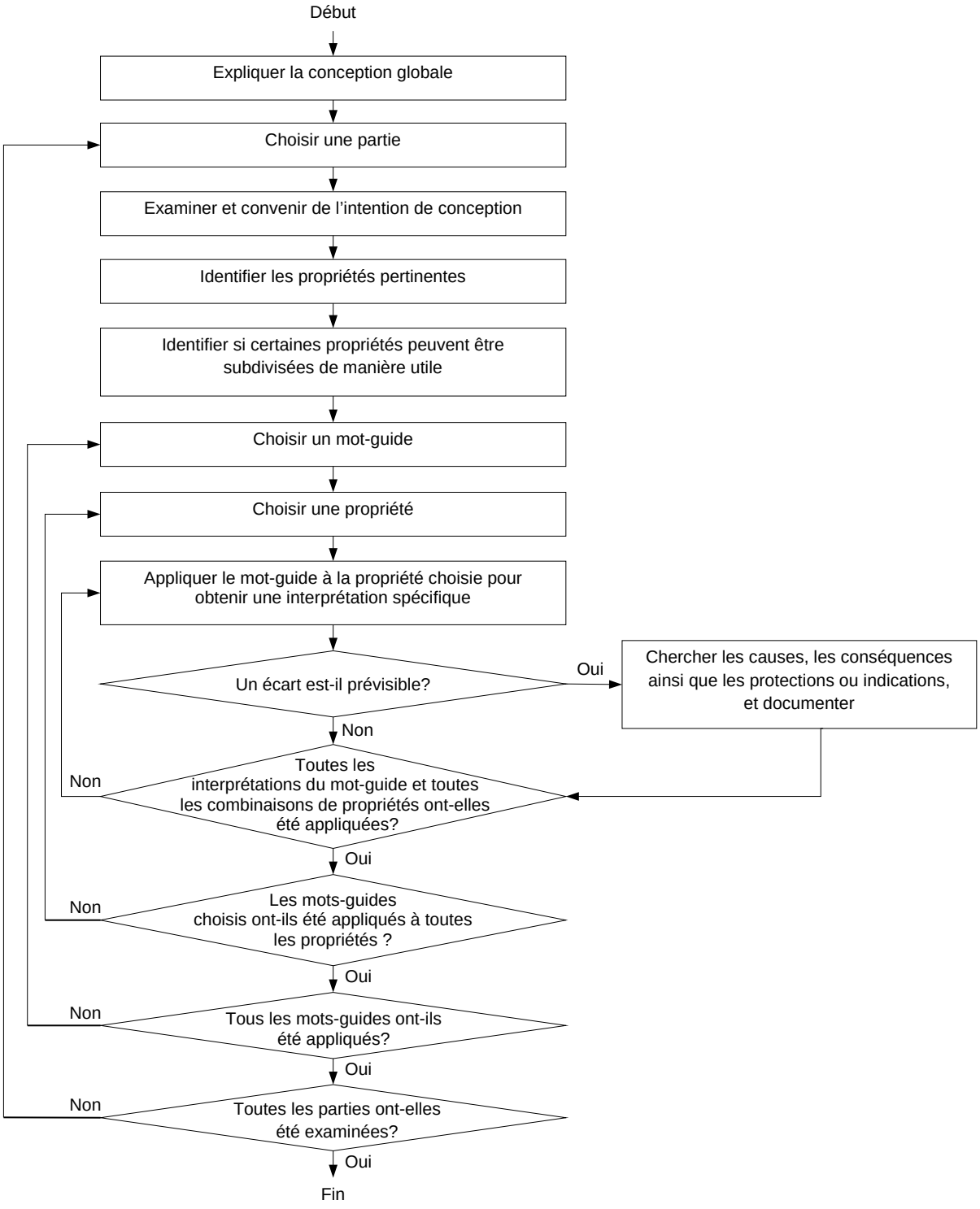


**Figure 3 – Organigramme de la procédure d'examen HAZOP – Séquence mot-guide d'abord**

### 6.5 Documentation et suivi

#### 6.5.1 Généralités

Une étude HAZOP implique que l'étude d'un système soit systématique, raisonnée et documentée. Pour tirer tout le profit possible d'une étude, elle doit être correctement documentée et les actions suggérées doivent être réalisées. Le chef d'étude est chargé de s'assurer de l'établissement de comptes rendus appropriés après chaque réunion. Les diverses méthodes de compte rendu sont présentées à l'Annexe A.

#### 6.5.2 Déterminer la méthode de compte rendu

Il existe deux formes fondamentales de compte rendu: intégral et par exception. Il convient de choisir la méthode de compte rendu avant chaque session et d'en aviser le rapporteur.

- Le compte rendu intégral consiste à documenter tous les résultats lors de l'application de chacune des combinaisons mot-guide/propriété à chaque partie ou élément du plan de conception. Bien qu'elle soit lourde, cette méthode fournit les preuves que l'étude a été effectuée de manière approfondie. Il convient qu'elle satisfasse aux exigences les plus sévères de la législation ou de l'entreprise.
- Le compte rendu par exception consiste à ne documenter que les risques et les problèmes d'exploitabilité identifiés, ainsi que les mesures de suivi. Les combinaisons propriété/mot-guide pour lesquelles aucun risque ou aucun problème d'exploitabilité n'a été identifié ne sont pas prises en compte. Cette méthode de compte rendu permet une gestion plus facile de la documentation. Cependant, elle ne rend pas compte de la précision de l'étude. Par la suite, une étude sur le même sujet pourrait alors être menée et serait par conséquent inutile.

Il convient que la décision relative à la forme de compte rendu à adopter repose sur les facteurs suivants:

- exigences réglementaires;
- obligations contractuelles;
- politiques d'entreprise;
- nécessité que l'étude soit traçable et puisse faire l'objet d'un audit;
- importance du système dans les objectifs de l'organisation;
- période de temps et moyens disponibles.

#### 6.5.3 Résultats de l'étude

Il convient qu'une étude HAZOP aboutisse au moins aux résultats suivants:

- présentation détaillée des risques et des problèmes d'exploitabilité identifiés, ainsi que des dispositions prises pour y remédier, y compris les moyens qui serviraient à les détecter;
- plan de conception annoté utilisé pour l'étude (voir l'Article A.3);
- recommandations d'études plus poussées sur des aspects particuliers de la conception utilisant différentes techniques, si nécessaire;
- recommandations pour des solutions de traitement du risque basées sur la connaissance que l'équipe a du système (si cela relève du domaine d'application de l'étude);
- notes attirant l'attention sur des points particuliers qui doivent être résolus lors de l'exploitation et de la maintenance;
- liste des membres de l'équipe pour chaque session;
- liste de toutes les parties examinées dans l'analyse, avec la justification de leur exclusion pour celles qui ont été exclues;

- liste des mots-guides et des propriétés utilisés; et
- liste de tous les dessins, spécifications, fiches techniques, comptes rendus, etc., qui ont été utilisés, avec leurs numéros de révision.

Pour les comptes rendus par exception, ces résultats tiendront normalement dans les tableaux HAZOP. Pour les comptes rendus intégraux, les résultats exigés peuvent être résumés à partir des tableaux de l'étude.

### 6.5.4 Enregistrer les informations

Il convient que les informations enregistrées soient conformes aux règles suivantes:

- il convient que chaque risque et chaque problème d'exploitation soient enregistrés séparément;
- il convient que tous les risques et problèmes d'exploitation, ainsi que leurs causes, soient enregistrés quel que soit le moyen de maîtrise qui existe dans le système;
- il convient que toute question que l'équipe désire soumettre après la réunion soit enregistrée, ainsi que le nom de la personne qui pourrait y répondre;
- il convient d'adopter un système de numérotation de manière à identifier de façon unique chaque risque, problème d'exploitation, question, recommandation, etc.;
- il convient d'archiver la documentation de l'étude en vue de recherches ultérieures, lorsque cela est exigé, et d'y faire référence dans le journal du système de gestion (s'il en existe un).

La désignation des destinataires du rapport final sera en grande partie dictée par la stratégie interne de l'entreprise ou par des exigences réglementaires mais il convient normalement qu'elle comprenne le directeur, le chef d'étude et les responsables des actions (voir 6.2.3).

### 6.5.5 Agrément de la documentation

A la fin de l'étude, il convient que le rapport de l'étude soit rédigé et approuvé par l'équipe. Il convient que le chef d'équipe et le représentant de la direction (de préférence le directeur de l'étude) établissent un agrément et une approbation officiels du rapport final. Si aucun accord ne peut être trouvé, il convient de consigner les raisons de la divergence de point de vue.

### 6.5.6 Suivi et responsabilités

L'étude HAZOP a pour but de passer en revue le système, non pas de le reconcevoir. Il n'est pas habituel que le chef d'étude soit responsable de réaliser les actions que recommande l'équipe.

Avant de mettre en œuvre toute modification significative adoptée à la suite des résultats de l'étude HAZOP, et dès qu'un plan révisé de conception est disponible, il convient que le directeur envisage de réunir à nouveau l'équipe d'étude HAZOP pour s'assurer qu'aucun nouveau risque ni problème d'exploitabilité ou de maintenance n'a été introduit.

Dans certains cas, comme indiqué en 6.2.3, le directeur peut autoriser l'équipe d'étude HAZOP à mettre en œuvre les recommandations et à effectuer des modifications de conception. Il pourrait alors être exigé de l'équipe d'étude HAZOP qu'elle effectue les travaux supplémentaires suivants:

– déterminer l'ensemble des actions en suspens et réviser la conception ou les dispositions d'exploitation et de maintenance;
– vérifier les modifications, informer le directeur qu'elles ont été réalisées et recevoir son approbation;
– mener d'autres études HAZOP sur le système révisé.

# Annexe A
(informative)

# Méthodes de compte rendu

## A.1 Options de compte rendu

Il existe différentes options de compte rendu:

– L'enregistrement manuel sur des formulaires préétablis peut convenir parfaitement, en particulier pour les petites études, sous réserve que les conditions essentielles de lisibilité soient satisfaites. Les notes manuscrites de l'étude HAZOP peuvent être saisies sur un logiciel après la session pour créer un exemplaire lisible pour l'édition.
– Un logiciel de traitement de texte ou un tableur peuvent être utilisés pour produire les tableaux pendant la session.
– Un logiciel spécifique de compte rendu d'étude HAZOP peut être utilisé.

Si un logiciel est utilisé, les résultats de l'étude peuvent être projetés dès leur création. Cela permet à l'équipe d'approuver le compte rendu au même moment.

## A.2 Tableau HAZOP

Il convient d'utiliser un tableau pour consigner les résultats de l'examen et le suivi. Quelle que soit l'option de compte rendu retenue, il convient que le tableau comprenne les caractéristiques ci-dessous. La disposition du tableau variera selon qu'il est créé à la main ou par logiciel.

Il convient que l'en-tête comprenne les informations suivantes: projet, sujet de l'étude, intention de conception, partie du système soumise à l'examen, membres de l'équipe, plan ou document examiné, date, nombre de pages, etc.

Les en-têtes (titres) des colonnes peuvent avoir comme libellé:

a) Pour les colonnes remplies au cours de l'examen:
   1) numéro de référence;
   2) mot-guide;
   3) propriété;
   4) écart/événement;
   5) cause;
   6) conséquences;
   7) moyens de maîtrise existants;
   8) actions suggérées.

D'autres informations, comme des commentaires, peuvent également être consignées.

b) Pour les colonnes remplies au cours du suivi:
   1) action convenue;
   2) responsabilité des mesures à prendre;
   3) statut de l'action.

NOTE Les colonnes mentionnées en b)1, b)2) et b)3) peuvent également être remplies lors des réunions elles-mêmes.

L'utilisation d'un ordinateur permet une plus grande souplesse dans la disposition, une meilleure présentation des informations et une plus grande facilité de préparation des comptes rendus exigés, notamment pour les documents suivants:

– tableaux détaillés;
– comptes rendus triés par causes et/ou conséquences;
– rapports de suivi avec responsabilités et états.

Il existe plusieurs suites logicielles dont le but est de simplifier la tâche d'enregistrement des données et la production des comptes rendus. Ces logiciels sont très utiles et facilitent le travail du rapporteur. Cependant, certaines suites tentent de remplacer le chef d'étude en produisant une liste de contrôle des paires mot-guide/propriété. Même si ces suites identifieront certains risques et produiront un imprimé qui ressemble à l'imprimé issu d'une étude HAZOP, celui-ci n'aura pas été produit par une étude rigoureuse et systématique. L'utilisation d'un logiciel pour remplacer totalement le chef d'étude doit être déconseillée.

L'application aléatoire de listes de contrôle *ad hoc* ne peut pas être considérée comme une étude HAZOP définie dans la présente norme.

## A.3 Plan annoté

Le plan de conception peut être annoté afin d'indiquer le numéro de référence du tableau pour chaque partie étudiée et de présenter les modifications que l'équipe d'étude recommande d'apporter à la conception.

Ceci pourrait limiter les méprises qui pourraient résulter d'une simple description textuelle des parties ou des modifications recommandées. Il constitue une part importante des informations du compte rendu. Une photographie du plan de conception annoté suffit en général pour le compte rendu, les originaux étant conservés par le directeur jusqu'à ce que toutes les actions aient été réalisées.

## A.4 Rapport d'étude HAZOP

Il convient d'établir un rapport final de l'étude HAZOP contenant les chapitres suivants:

– sommaire;
– conclusions;
– domaine d'application et objectifs;
– résultats de l'étude par éléments, comme indiqué en 6.5.3;
– tableaux de l'étude HAZOP;
– plan de conception annoté;
– liste des dessins et de la documentation de référence;
– informations d'historique qui ont servi à l'étude.

# Annexe B
(informative)

# Exemples d'études HAZOP

## B.1 Généralités

Les exemples contenus dans l'Annexe B ont pour but de montrer comment les principes d'une étude HAZOP, présentés dans la présente norme (en particulier en 4.2, 6.3 et 6.4), sont appliqués à une large plage d'applications dans diverses industries et activités. Il convient cependant de noter que les exemples donnés ont été simplifiés de manière significative dans un but explicatif et n'ont pas pour but de reproduire en détail la complexité technique d'études de cas réels. Il convient également de noter que seule une partie des résultats est donnée.

## B.2 Exemple introductif

Cet exemple simplifié a pour but d'initier le lecteur aux fondements de la méthode d'examen HAZOP. L'exemple est repris de la publication originale sur les études HAZOP.

Une unité de transformation simple représentée à la Figure B.1 est examinée. Les matériaux A et B sont transférés par des pompes en continu de leurs réservoirs respectifs d'approvisionnement pour se combiner et former un produit C dans le réacteur. Il est pris pour hypothèse que la quantité de A doit toujours être supérieure à la quantité de B dans le réacteur pour éviter un risque d'explosion. Un plan de conception complet comprendrait beaucoup d'autres détails, tels que l'effet de la pression, la température de la réaction et du réactant, l'agitation, le temps de réaction, la compatibilité des pompes A et B, etc., mais pour les besoins de cet exemple simple, utilisé à titre d'explication, ils seront ignorés. La partie de l'usine examinée est représentée en gras.

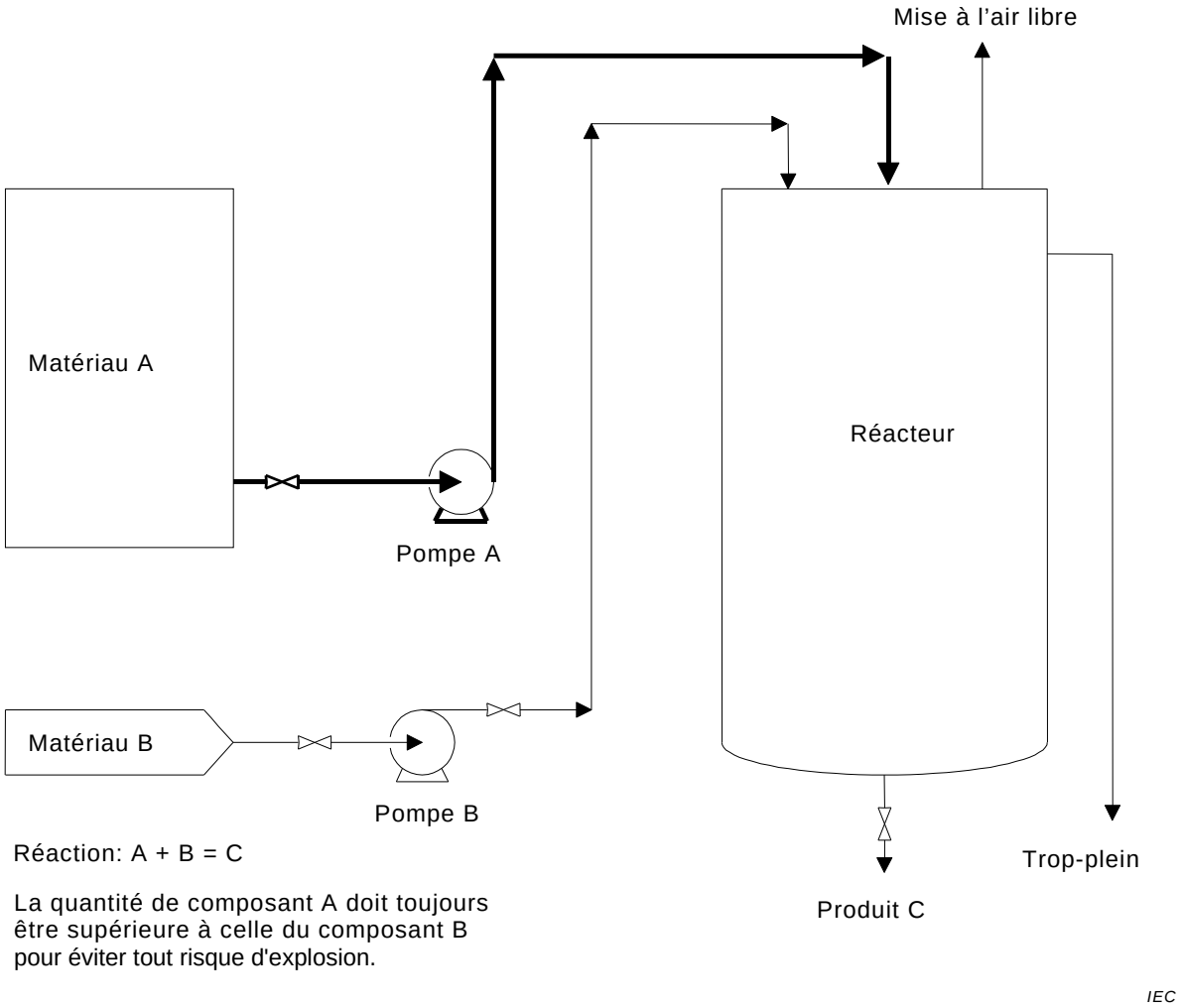


**Figure B.1 – Schéma de circulation simple**

La partie du système retenue pour l'examen est le conduit allant du réservoir d'approvisionnement qui contient A au réacteur, y compris la pompe A (voir le Tableau B.1). L'intention de conception pour cette partie est de transférer en continu le matériau A du réservoir vers le réacteur à un débit supérieur à celui du matériau B. Concernant les propriétés suggérées en 4.2, l'intention de conception est donnée à l'alinéa précédent de l'Article B.2.

**Tableau B.1 – Propriétés du système soumis à l'examen**

| Matériau | Activité | Source | Destination |
|---|---|---|---|
| A | Transfert (à un débit > B) | Réservoir pour A | Réacteur |

Chacun des mots-guides indiqués dans le Tableau 3 (ainsi que ceux qui ont été convenus au cours des travaux préparatoires, voir 6.3.3) est alors appliqué tour à tour à chacune de ces propriétés, et les résultats sont consignés sur des tableaux HAZOP. Le Tableau B.2 donne des exemples de résultats HAZOP possibles, la méthode de compte rendu "par exception" étant utilisée et seuls les écarts significatifs étant consignés. Après l'examen de chacun des mots-guides pour chacune des propriétés concernées dans cette partie du système, une autre partie (par exemple le conduit de transfert du matériau B) serait choisie et le processus répété. Finalement, toutes les parties du système seraient examinées de la même manière et les résultats consignés.

**Tableau B.2 – Exemple de tableau HAZOP pour un exemple introductif**

| | | |
|---|---|---|
| **TITRE DE L'ETUDE:** EXEMPLE DE PROCEDE | | **FEUILLE:** 1 de 4 |
| **N° du dessin:** | **N° DE REVISION:** | **DATE:** jeudi 17 décembre 1998 |
| **COMPOSITION DE L'EQUIPE:** | LB, DH, EK, NE, MG, JK | **DATE DE LA REUNION:** mardi 15 décembre 1998 |
| **PARTIE CONSIDEREE:** | **Conduit de transfert du réservoir d'approvisionnement A au réacteur** | |
| **INTENTION DE CONCEPTION:** | **Matériau:** A **Activité:** Transférer en continu à un débit supérieur à B<br>**Source:** Réservoir pour A **Destination:** Réacteur | |

| N° | Mot-guide | Elément | Ecart | Causes possibles | Conséquences | Moyens de maîrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|---|
| 1 | NE PAS FAIRE | Matériau A | Absence du matériau A | Réservoir d'approvisionnement A vide | Pas d'écoulement de A dans le réacteur<br>Explosion | Aucun apparent | Situation inacceptable | Prévoir l'installation sur le réservoir A d'une alarme de niveau bas, ainsi que d'un déclencheur à seuil bas pour arrêter la pompe B | MG |
| 2 | NE PAS FAIRE | Transférer A (à un débit > B) | Aucun transfert de A n'a lieu | Pompe A arrêtée, conduit obstrué | Explosion | Aucun apparent | Situation inacceptable | Mesurage du débit du matériau A, ainsi qu'une alarme de niveau bas, et un déclenchement de la pompe B en cas d'écoulement faible | JK |

| N° | Mot-guide | Elément | Ecart | Causes possibles | Conséquences | Moyens de maîrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|---|
| 3 | PLUS | Matériau A | Davantage de matériau A: le réservoir d'approvisionnement déborde | Remplissage du réservoir à partir du camion-citerne alors que la capacité est insuffisante | Le réservoir dépassera la limite de remplissage | Aucun apparent | Remarque: Ceci aurait dû être identifié durant l'examen du réservoir | Prévoir une alarme de niveau haut si non identifié précédemment | EK |
| 4 | PLUS | Transférer A | Davantage de transfert<br><br>Augmentation du débit de A | Dimensionnement incorrect de la pompe<br><br>Installation d'une mauvaise pompe | Réduction possible du rendement<br><br>Le produit contiendra beaucoup trop de A | Néant | | Vérifier les débits et les caractéristiques de la pompe pendant la mise en service<br>Revoir la procédure de mise en service | JK |
| 5 | MOINS | Matériau A | Moins de matériau A | Niveau bas dans le réservoir | Tête d'aspiration positive nette inadéquate<br>Turbulences possibles et risque d'explosion<br>Flux inadéquat | Néant | Inacceptable<br>Idem 1 | Alarme niveau bas dans le réservoir<br>Idem 1 | MG |
| 6 | MOINS | Transférer A (à un débit > B) | Diminution du débit de A | Conduit partiellement obstrué, fuite, pompe non performante, etc. | Explosion | Aucun apparent | Inacceptable | Idem 2 | JK |
| 7 | EN PLUS DE | Matériau A | En plus de A, un autre fluide est également présent dans le réservoir d'approvisionnement | Approvisionnement du réservoir contaminé | Inconnues | Vérification et analyse du contenu de tous les camions-citernes avant déchargement dans le réservoir | Jugé acceptable | Vérifier la procédure d'exploitation | LB |

| N° | Mot-guide | Elément | Ecart | Causes possibles | Conséquences | Moyens de maîrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|---|
| 8 | EN PLUS DE | Transférer A | En plus du transfert de A, quelque chose se passe: corrosion, érosion, cristallisation ou décomposition | Le risque potentiel pour chacun des éléments doit être examiné à la lumière de détails plus spécifiques | | | | | NE |
| 9 | EN PLUS DE | Réacteur de destination | En plus de la destination du réacteur<br>Fuites externes | Fuites dans le conduit, la vanne ou la bague d'étanchéité | Contamination de l'environnement<br>Risque d'explosion | Utilisation d'un code ou d'une norme/ agréés pour les canalisations | Acceptation qualifiée | Positionner le détecteur d'écoulement pour le déclenchement aussi près que possible du réacteur | DH |
| 10 | INVERSE | Transférer A | Inversion de la direction de l'écoulement<br>Le matériel circule du réacteur vers le réservoir d'approvisionnement | Pression dans le réacteur supérieure à la pression d'évacuation de la pompe | Contamination du réservoir d'approvisionnement par reflux du matériau de réaction | Aucun apparent | Position insatisfaisante | Prévoir l'installation d'un clapet de retenue dans le conduit | MG |
| 11 | AUTRE QUE | Matériau A | Autre que A<br>Matériau autre que A dans le réservoir d'approvisionnement | Mauvais matériau dans le réservoir d'approvisionnement | Inconnu Dépendraient du matériau | Contrôle et analyse de la nature du contenu du camion-citerne avant déchargement | Position acceptable | | |
| 12 | AUTRE QUE | Réacteur de destination | Fuite externe<br>Rien n'arrive au réacteur | Rupture du conduit | Contamination de l'environnement et risque d'explosion | Intégrité des canalisations | Vérifier la conception des canalisations | Spécifier qu'il convient que le détecteur d'écoulement proposé soit suffisamment rapide au déclenchement pour éviter une explosion | MG |

## B.3 Procédures

Un petit processus de fabrication par lots est examiné pour la fabrication d'un composant en plastique critique pour la sécurité. Le composant doit satisfaire à des spécifications strictes tant du point de vue des propriétés du matériau que de sa couleur. La séquence de traitement est la suivante:

a) prendre 12 kg de poudre "A";

b) la placer dans le mélangeur;

c) prendre 3 kg de poudre colorante "B";

d) la placer dans le mélangeur;

e) mettre le mélangeur en route;

f) mélanger pendant 15 min et arrêter le mélangeur;

g) retirer le mélange du mélangeur et le placer dans 3 sacs de 5 kg;

h) rincer le mélangeur;

i) ajouter 50 l de résine au récipient mélangeur;

j) ajouter 0,5 kg de durcisseur au récipient mélangeur;

k) ajouter 5 kg de poudre mélangée ("A" et "B");

l) remuer pendant 1 min;

m) verser le mélange dans des moules dans les 5 min qui suivent.

Une étude HAZOP est effectuée pour examiner comment un matériau d'une qualité inférieure à celle spécifiée pourrait être produit. En tant que procédure séquentielle, les parties examinées pendant/durant le processus HAZOP sont les instructions séquentielles concernées/pertinentes. Des extraits d'une étude HAZOP de la séquence sont donnés dans le Tableau B.3. Le système de compte rendu "par exception" a été utilisé

**Tableau B.3 – Exemple de tableau HAZOP pour les procédures**

| | | |
|---|---|---|
| **TITRE DE L'ETUDE:** PROCEDURES | | **FEUILLE**: 1 de 3 |
| **TITRE DE LA PROCEDURE:** Fabrication à petite échelle du composant X | **N° de REVISION**: | **DATE**: |
| **COMPOSITION DE L'EQUIPE:** BK, JS, LE, PA | | **DATE DE LA REUNION:** |
| **PARTIE CONSIDEREE:** | **INSTRUCTION 1:** Prendre 12 kg de poudre "A" | |

| N° | Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Prendre poudre A | NE PAS FAIRE | Ne pas prendre "A" | Erreur de l'opérateur | Le matériau final ne prendra pas | Il convient que l'opérateur voie que la masse dans le mélangeur est beaucoup trop faible. La couleur serait aussi beaucoup trop vive. | L'absence complète de charge de matériau "A" n'est pas jugée crédible | Néant | |
| 2 | Prendre poudre A | EN PLUS DE | Un matériau supplémentaire est ajouté avec "A" | Le matériau "A" contient des impuretés | La spécification de couleur pourrait ne pas être remplie. Le mélange final pourrait ne pas prendre correctement | Les échantillons de toutes les livraisons de "A" sont soumis à l'essai avant utilisation | | Contrôler les procédures d'assurance qualité auprès des fabricants | BK |
| 3 | Prendre poudre A | AUTRE QUE | Prise d'un matériau autre que "A" | L'opérateur utilise un sac du mauvais matériau | Le mélange ne peut pas être utilisé. Perte financière | Seuls les sacs de "A", "B" et de mélange doivent être gardés à proximité du mélangeur | | Contrôler les normes de gestion interne chaque semaine. Envisager l'utilisation de sacs de couleur différente pour chaque matière première et mélange | BK |
| 4 | Prendre 12 kg | PLUS | Trop de "A" pris | Erreur de pesée/ Erreur de l'opérateur | La spécification de couleur ne sera pas remplie | Contrôle hebdomadaire de la méthode de pesée.<br>Entretien de la balance tous les 6 mois | | JS doit insister auprès des opérateurs sur la nécessité d'une pesée précise | JS |
| 5 | Prendre 12 kg | MOINS | Trop peu de "A" pris | Erreur de pesée/ Erreur de l'opérateur | Comme ci-dessus | Comme ci-dessus | | Comme ci-dessus | JS |

| N° | Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|---|
| 6 | Mélangeur | AUTRE QUE | Le matériau "A" n'est pas dans le bon mélangeur | Erreur de l'opérateur | | Il n'y a en général qu'un seul mélangeur | | Revoir la position s'il existe des propositions d'installation de mélangeurs supplémentaires | BK |
| 7 | Ajouter durcisseur | NE PAS FAIRE | Pas de durcisseur ajouté | Erreur de l'opérateur | Le mélange ne prendra pas correctement<br>Perte financière | L'opérateur doit signer la feuille du lot pour confirmer que le durcisseur a été ajouté. Essai de la résistance du produit final | | Revoir le taux d'erreur pour voir si des protections supplémentaires sont exigées | BK |
| 8 | Ajouter durcisseur | EN PLUS DE | Matériau supplémentaire ajouté avec le durcisseur | Durcisseur contaminé avec des impuretés | Le mélange pourrait ne pas être utilisable | Assurance qualité garantie par le fournisseur.<br>Essai d'échantillons de toutes les livraisons | | Néant | |
| 9 | Ajouter durcisseur | AUTRE QUE | Ajout d'un matériau autre que le durcisseur | | Le mélange ne sera pas utilisable | Séparation physique des différents durcisseurs. Contrôles de l'opérateur | Si la proposition de commander des sacs de durcisseur prépesés est retenue, les risques d'erreur de mélange sont encore réduits | Attendre la solution du problème du durcisseur. Effectuer une enquête et un contrôle des achats | JS |
| 10 | Ajouter 0,5 kg | PLUS | Trop de durcisseur est ajouté | Erreur de pesée<br>Erreur de l'opérateur | Le composant sera trop cassant; pourrait entraîner une défaillance catastrophique | Contrôler le pesage une fois par semaine. Entretenir la balance tous les 6 mois | Protections jugées inadéquates | S'informer sur la possibilité d'obtenir du durcisseur prépesé dans des sacs de 0,5 kg. Effectuer des contrôles d'échantillons sur chaque livraison | JS |
| 11 | Ajouter 0,5 kg | MOINS | Pas assez de durcisseur | Comme ci-dessus | Le mélange ne prendra pas correctement<br>Perte financière | Comme ci-dessus | Comme ci-dessus | Comme ci-dessus | JS |

## B.4 Système de protection automatique des trains

### B.4.1 Généralités

L'Article B.4 a pour but de donner un petit exemple d'une étude HAZOP typique au niveau du schéma fonctionnel du système pour présenter certains points de la présente norme. L'exemple se divisera en deux parties:

– une brève description du système et un schéma fonctionnel;
– un extrait de tableau HAZOP examinant une série d'écarts potentiels présentés dans un compte rendu "par exception" (voir Tableau B.4).

Il convient de noter que la conception du système utilisée dans cet exemple est celle d'un système peu détaillé. La conception et l'extrait des tableaux HAZOP ne sont que des présentations et ne proviennent pas d'un système réel. Ils n'ont d'autre but que de montrer le processus et ne prétendent pas être complets.

### B.4.2 Application

#### B.4.2.1 Objet du système

L'application porte sur un équipement à bord d'un train pour la protection automatique des trains (ATP). Cette fonction est mise en œuvre sur beaucoup de rames de métro et sur certains trains de grande ligne. L'ATP surveille la vitesse du train, la compare à la vitesse de sécurité planifiée et déclenche automatiquement un freinage d'urgence en cas de détection de vitesse excessive. Sur tous les systèmes ATP, un équipement est installé à la fois sur le train et sur la voie et les informations sont transférées depuis la voie vers le train. Il existe différents types de systèmes ATP; ils se distinguent par la manière dont ils remplissent les exigences de base.

#### B.4.2.2 Description du système

A bord du train se trouvent une ou plusieurs antennes qui reçoivent les signaux de la voie donnant des informations sur les vitesses de sécurité ou les arrêts. Ces informations sont traitées avant d'être transférées à un système électronique programmable (PES). Les autres entrées principales du PES sont délivrées par des tachymètres ou d'autres moyens permettant de mesurer la vitesse réelle du train. La principale sortie du PES est un signal qui est transmis à des relais de sécurité, par exemple le signal de commande du freinage d'urgence. La Figure B.2 donne un schéma fonctionnel simple de ce processus.

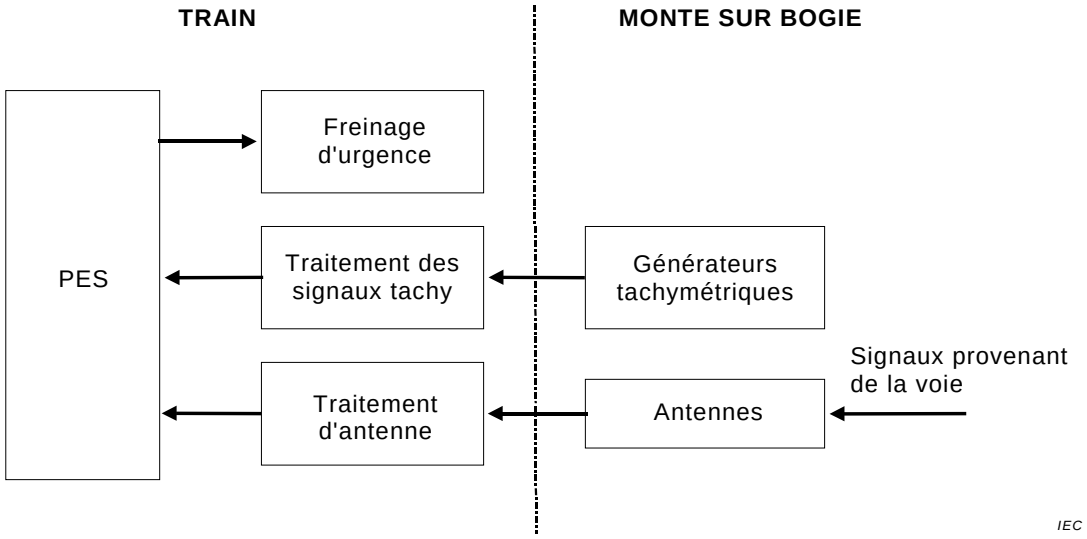


**Figure B.2 – Equipement ATP embarqué**

**Tableau B.4 – Exemple de tableau HAZOP pour un système de protection automatique des trains**

| | | |
|---|---|---|
| **TITRE DE L'ETUDE:** SYSTEME DE PROTECTION AUTOMATIQUE DES TRAINS | | **FEUILLE:** 1 sur 2 |
| **N° DU DESSIN DE REFERENCE:** SCHEMA FONCTIONNEL DE L'ATP | **N° DE REVISION:** 1 | **DATE:** |
| **COMPOSITION DE L'EQUIPE:** DJ, JB, BA | | **DATE DE LA REUNION:** |
| **PARTIE EXAMINEE:** | ENTREE DE L'EQUIPEMENT DE LA VOIE | |
| **INTENTION DE CONCEPTION:** | FOURNIR UN SIGNAL AU PES PAR LES ANTENNES POUR DONNER DES INFORMATIONS SUR LES VITESSES DE SECURITE ET LES ARRETS | |

| N° | Partie | Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise | Commen-taires | Actions exigées | Respon-sable actions |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Signal d'entrée | Amplitude | NE PAS FAIRE | Pas de signal détecté | Défaillance de l'émetteur | Examinés dans une étude séparée de l'équipement de la voie | | | Revoir les résultats de l'étude de l'équipement de la voie | DJ |
| 2 | Signal d'entrée | Amplitude | PLUS | Plus grand que l'amplitude de la conception | Emetteur monté trop près du rail | Pourrait endommager l'équipement | Contrôles à effectuer au cours de l'installation | | Ajouter le contrôle à la procédure d'installation | DJ |
| 3 | Signal d'entrée | Amplitude | MOINS | Plus petit que l'amplitude de la conception | Emetteur monté trop loin du rail | Le signal peut ne pas être détecté | Comme ci-dessus | | Ajouter le contrôle à la procédure d'installation | DJ |
| 4 | Signal d'entrée | Fréquence | AUTRE QUE | Autre fréquence détectée | Réception d'un signal de la voie adjacente | Une valeur erronée est transmise au processeur | Actuellement néant | | Vérifier si une mesure doit être prise pour la protection | DJ |
| 5 | Antennes | Position | AUTRE QUE | Antennes ailleurs qu'à l'emplacement correct | Défauts de montage | Pourrait heurter le rail et être détruite | Il convient que le câble fournisse un support secondaire | | S'assurer que le câble éloigne les antennes de la voie | JB |
| 6 | Antennes | Tension | PLUS | Tension plus élevée que prévu | Court-circuit entre l'antenne et le rail sous tension | Les antennes et autres équipements passent sous tension | | | Vérifier s'il y a une protection contre ce phénomène | DJ |

| N° | Partie | Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise | Commen-taires | Actions exigées | Respon-sable actions |
|---|---|---|---|---|---|---|---|---|---|---|
| 7 | Antennes | Signal de sortie | AUTRE QUE | Un autre signal est transmis | Réception de signaux parasites sur le câblage adjacent | Une action pourrait être menée sur le signal incorrect | | | S'assurer qu'il y a une protection adéquate contre les interférences du câble | JB |
| 8 | Tachy-mètre | Vitesse | NE PAS FAIRE | Pas de vitesse mesurée | Verrouillage soudain des roues | Pourrait indiquer une vitesse nulle | | | Vérifier s'il existe une protection contre ce phénomène | DJ |
| 9 | Tachy-mètre | Vitesse | AUTRE QUE | Vitesse autre que correcte détectée | Déblocage soudain des roues donnant un signal confus | Pourrait indiquer une vitesse incorrecte | | | Vérifier s'il existe une protection contre ce phénomène | BA |
| 10 | Tachy-mètre | Vitesse | EN PLUS DE | Un grand nombre de vitesses indiquées | Changements soudains dans la sortie causés par la rotation des roues | Pourrait provoquer une action basée sur une vitesse incorrecte | | | Vérifier s'il s'agit d'un problème dans la pratique | BA |
| 11 | Tachy-mètre | Tension de sortie | NE PAS FAIRE | Pas de sortie | Essieux bloqués | Pourrait indiquer une vitesse nulle | | | Vérifier les implications de ce problème | DJ |
| 12 | Tachy-mètre | Signal de sortie | EN PLUS DE | Signal de sortie confus | Autres signaux présents | Pourrait indiquer une vitesse incorrecte | | | Voir s'il s'agit d'une défaillance crédible | BA |

## B.5 Exemple avec planification en cas d'urgence

Les organisations font des plans pour traiter par anticipation différentes urgences. Ces urgences peuvent varier de la réaction à une alerte à la bombe à l'évacuation du personnel en cas d'incendie, en passant par l'alimentation en courant de secours. La validité et l'intégrité de ces plans peuvent être soumises à l'essai de différentes manières – le plus souvent, par une sorte de répétition générale. Ces répétitions générales sont très utiles, mais peuvent être coûteuses et, par leur nature même, perturbent le déroulement normal du travail. Heureusement, les urgences réelles qui éprouvent le système sont rares et de toute façon il est improbable que les répétitions générales couvrent toutes les éventualités.

Les études HAZOP offrent un moyen relativement économique d'identifier une grande partie des déficiences qui peuvent exister dans un plan d'urgence, et complètent l'expérience acquise lors des répétitions générales, relativement peu fréquentes, ou lorsque l'urgence elle-même, encore plus rare, apparaît (voir le Tableau B.5).

Sur une plate-forme pétrolière ou gazière en mer, un système efficace doit être mis en place pour l'évacuation et le sauvetage (EER) en cas d'incidents constituant une menace potentielle pour la vie des personnes. Ce système aurait pour objectif de prévenir rapidement le personnel de l'existence d'une situation dangereuse, de permettre au personnel de s'acheminer rapidement vers un point de rassemblement sûr, puis d'évacuer la plate-forme, de préférence sans panique, par hélicoptère ou canot de sauvetage, et d'être secouru et amené en lieu sûr. Un système EER efficace constitue un élément primordial du système global d'installation en mer. Un système EER typique comprend généralement un certain nombre d'étapes (éléments) différentes, par exemple:

a) déclenchement de l'alarme générale (GPA) par des instruments automatiques, ou manuellement par un opérateur;

b) communication de la situation à la fois à un vaisseau se tenant à proximité et aux services d'urgence à terre;

c) acheminement du personnel par des voies d'accès désignées vers le point de rassemblement;

d) rassemblement avec enregistrement du personnel présent;

e) distribution de matériel de survie, etc.;

f) attente du PAPA qui doit être déclenché par l'OIM ou son représentant;

g) sortie du personnel, qui s'achemine du point de rassemblement vers le moyen d'évacuation choisi;

h) évacuation, en général par hélicoptères ou par canots de sauvetage spécialement conçus;

i) fuite directe par la mer si les moyens d'évacuation préférentiels ne sont pas disponibles;

j) sauvetage du personnel évacué par canots ou des personnes qui se sont jetées à la mer, puis acheminement vers un lieu sûr

**Tableau B.5 – Exemple de tableau HAZOP pour une planification en cas d'urgence**

| | |
|---|---|
| **PARTIE CONSIDEREE:** | SYSTEME D'ALARME |
| **INTENTION DE CONCEPTION:** | FAIRE RETENTIR UN GPA |
| **PARTIES:** | SIGNAL DE DECLENCHEMENT |
| **ENTREES:** | ENERGIE ELECTRIQUE |
| **ACTIVITES:** | EMETTRE UNE ALARME AUDIBLE ET TRANSMETTRE LE SON AU PERSONNEL |
| **SOURCES:** | TOUS LES GENERATEURS D'ALARMES |
| **DESTINATIONS:** | ENSEMBLE DU PERSONNEL SUR LA PLATE-FORME |

| N° | Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Signal de déclenchement de l'alarme générale et énergie électrique | NE PAS FAIRE | Pas d'entrée | 1) Les instruments ou le personnel ne déclenchent pas l'alarme générale | Absence d'alerte du personnel | Néant | Improbable mais possible | Néant | |
| | | | | 2) Le personnel essaie de déclencher l'alarme générale, mais le signal n'atteint pas l'alarme | Comme ci-dessus | Duplication des connexions et logique de sécurité intrinsèque, c'est-à-dire "Courant pour ouvrir, ressort pour fermer" | Improbable | | |
| | | | | 3) Pas d'énergie électrique | Comme ci-dessus | Alimentation sans interruption | Comme ci-dessus | | |
| 2 | | PLUS | Plus d'entrées | 1) Fausse alarme | Personnel alerté inutilement | Néant | Possible | Convient-il que le déclenchement exige deux boutons? | |
| | | | | 2) Alarme déclenchée à tort | Comme ci-dessus | Discipline et règles de bon usage | Improbable | Néant | |

| N° | Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|---|
| 3 | Entrées | PLUS | Plus d'entrées | Davantage d'énergie électrique | Système d'alarme endommagé | Alimentation spécialisée protégée | Improbable | Néant | |
| 4 | | MOINS | Moins de déclen-chements | Le signal de déclenchement n'atteint que certaines alarmes | Une partie du personnel n'a pas été alerté | Contrôle périodique des alarmes | | Néant | |
| 5 | | | Moins d'énergie électrique | Perte de puissance électrique | Les alarmes pourraient ne pas retentir | Alimentation dédiée | Improbable | Néant | |
| 6 | | EN PLUS DE | En plus du déclen-chement | L'initiation déclenche d'autres actions | | Impossible dans un câblage dédié | | Néant | |
| 7 | | | En plus de l'énergie électrique | Energie présente sous une mauvaise forme, par exemple: parasites | Possibilité de dommages | Circuit d'alimentation protégé | | Néant | |
| 8 | | PARTIE DE | Partie des entrées | Signal mais pas d'énergie ou énergie mais pas de signal | Personnel non alerté | | Déjà examiné ci-dessus | | |
| 9 | | INVERSE | Entrées inversées<br><br>Energie électrique inversée | Inversion du déclenchement d'alarme<br><br>Pas de signification constructive | | | Le système décrit ne comprend pas l'émission d'une remise à zéro générale | Développer un système de remise à zéro générale | |
| 10 | Entrées | AUTRE QUE | Autre que les entrées | Multiple | Dépend des entrées | Improbable avec des circuits spécialisés protégés | Pourrait demander un système "battle proof" | Prévoir un câblage Pyrotenax | |

| N° | Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|---|
| 11 | Activités émission d'alarme et transmission au personnel | NE PAS FAIRE | Pas d'alarme | Défaillance de la sonorisation<br>Câble endommagé | Personnel non alerté | Système PA double<br>Câblage double<br>Alimentations doubles<br>Haut-parleurs multiples | Improbable | Néant | |
| 12 | | PLUS | Plus d'alarme | Sonorisation trop puissante | Problèmes auditifs parmi le personnel | La puissance de la sonorisation assignée ne doit pas dépasser le niveau de sécurité | | Néant | |
| 13 | | MOINS | Moins d'alarme | Son trop faible | Une partie du personnel n'a pas été alerté | Néant | | S'assurer que le système produit un minimum de 15 dB au-dessus du bruit de fond | |
| 14 | | EN PLUS DE | En plus de l'alarme et de la transmission | Distorsion de l'alarme, harmoniques ou échos | Le signal émis vers le personnel manque de clarté | Néant | | Examiner le besoin d'ingénierie acoustique | |
| 15 | | PARTIE DE | Seule une partie de l'alarme est transmise | Alarme mais transmission incorrecte | Pas de signal émis vers le personnel | | Comme pour moins d'alarme ci-dessus | | |
| 16 | | INVERSE | Alarme et transmission inversées | | | | Voir commentaires ci-dessus déclenchements inversés et remise à zéro générale | | |

| N° | Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|---|
| 17 | | AUTRE QUE | Autre qu'émission de l'alarme générale et transmission | Le système déclenche PAPA par erreur | Confusion parmi le personnel. Certains pourraient abandonner la plate-forme par erreur | Néant | | Revoir la logique de signalisation pour que PAPA ne puisse se déclencher qu'après l'alarme générale | |
| 18 | | PLUS TOT | Alarme et transmission prématurées | Alarme générale déclenchée avant que la situation l'exige | Alarme et interruption du travail inutiles | Néant | | Etablir des directives claires pour le personnel de la plate-forme | |
| 19 | | PLUS TARD | Alarme et transmission tardives | Alarme générale déclenchée après que la situation l'exige | Une partie du personnel pourrait être prise au piège ou obligée d'utiliser une autre issue de secours moins souhaitable | Néant | | Etablir des directives claires, comme ci-dessus | |

## B.6 Système de commande de vanne piézoélectrique

Le système de commande de vanne piézoélectrique montre comment une étude HAZOP peut être appliquée à un système électronique détaillé (voir la figure simplifiée B.3, le Tableau B.6 et le Tableau B.7).

Une vanne piézoélectrique est une vanne commandée par une céramique piézoélectrique. L'élément céramique est commandé électriquement et s'allonge lorsqu'il est chargé. Lorsqu'elle est chargée, la céramique piézoélectrique ferme la vanne. Lorsqu'elle est déchargée, elle ouvre la vanne. Si la céramique piézoélectrique ne perd pas ou ne gagne pas en charge, l'état de la vanne reste stable.

Le système pulvérise un liquide inflammable et explosif dans un caisson de réacteur (non représenté). L'ensemble du système, c'est-à-dire le caisson de réacteur, la tuyauterie, les pompes, etc., fait l'objet d'une étude HAZOP différente. Seule l'application d'une étude HAZOP à une unité électronique est décrite ci-dessous.

L'unité fonctionne suivant un processus à deux états conçu pour fermer la vanne à la demande, "état 1" et à l'ouvrir à la demande, "état 2".

La charge électrique du condensateur C1 est appliquée à travers le transistor T1 au condensateur de couplage C2 et par la ligne d'alimentation à la vanne piézoélectrique pour la fermer. Dans ce cas, le transistor T2 et le transistor de protection T3 sont fermés (résistance élevée).

Le condensateur C2 est déchargé par le transistor T2 pour ouvrir la vanne. Pour éviter un chargement asymétrique de la vanne piézoélectrique, par exemple sous l'effet d'une contrainte mécanique ou thermique, le transistor T4 relie le retour à la terre.

Un blindage électrique autour des fils torsadés du câble empêche les perturbations électromagnétiques d'affecter le fonctionnement de la vanne.

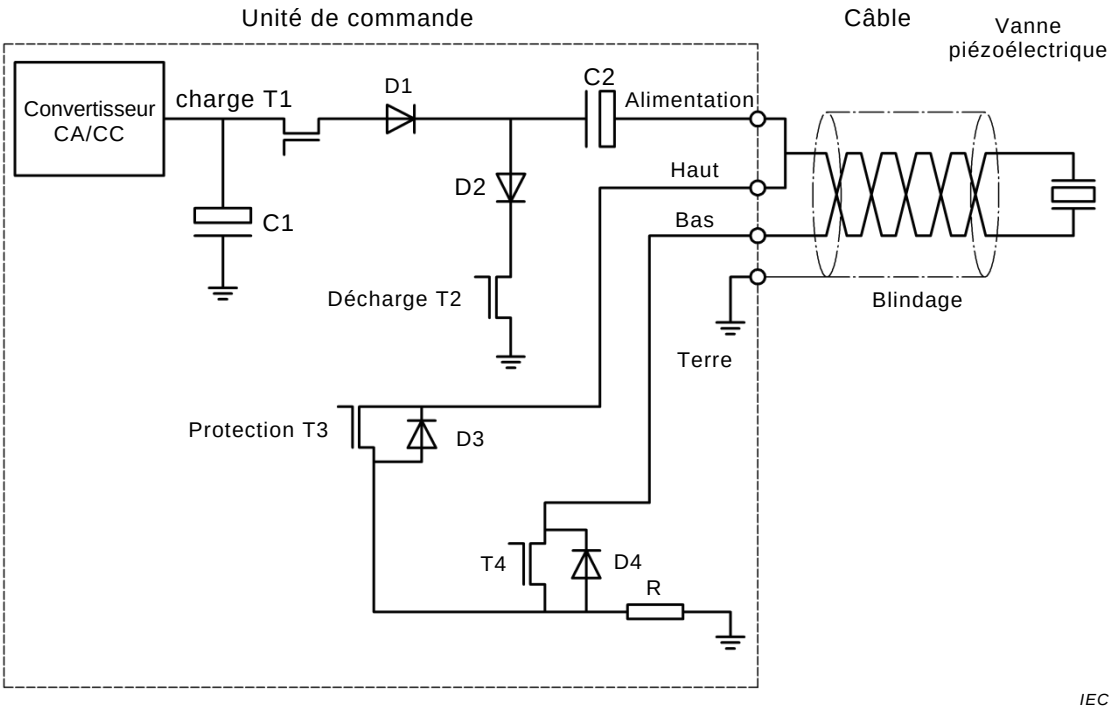


**Figure B.3 – Système de commande de vanne piézoélectrique**

**Description de l'état 1:** fermer la vanne.

**Partie examinée:** câblage du convertisseur en courant alternatif/continu et du condensateur C1 via le transistor T1, la diode D1, le condensateur C2 vers le côté alimentation de la vanne et du côté retour de la vanne à la terre via le transistor T4 et la résistance R.

**Description de l'état 2:** ouvrir la vanne.

**Partie examinée:** câblage du côté alimentation de la vanne à la terre, via le transistor T3, la diode D3 et la résistance R.

**Tableau B.6 – Intention de conception du système**

| Entrée | Activité | Source | Destination |
|---|---|---|---|
| Etat 1: Fermer la vanne<br>1. Charger C1 | 1. Transférer la charge par T1, D1 et C2 | C1 et convertisseur | 1. Alimentation vers côté alimentation de la vanne |
| Caractéristiques:<br>Tension<br>Capacité | 2. Transférer la charge par T4 et R vers la terre | Côté retour de la vanne | 2. Retour de la charge à la terre |
| 2. Signaux de commande vers T1, T3 et T4 | 3. Commander l'ouverture par T1 et T4 depuis la terre<br>4. Isoler par T2<br>5. Empêcher la surcharge par T3 | Signal venant de la commande | T1, T3 et T4<br>Surcharge vers la terre |
| | 6. Empêcher l'inversion de l'écoulement de la charge par D2 | Côté alimentation de la vanne | |
| Etat 2: Ouvrir la vanne<br>1. Décharger côté alimentation de la vanne<br>Caractéristiques:<br>Tension<br>Capacité | 1. Isoler de C1 et du convertisseur par T1<br>2. Transférer la charge par D2 et T2<br>3. Transférer toute charge de la vanne par D3, D4 et R | Côté alimentation de la vanne et C2 | Terre |
| 2. Signaux de commande vers T1, T2 et T4 | 4. Isoler le côté faiblement chargé de la vanne par T4 | Signaux venant de la commande | T1, T2 et T4 |

**Tableau B.7 – Exemple de tableau HAZOP pour un système de commande de vanne piézoélectrique**

| | | | |
|---|---|---|---|
| **TITRE DE L'ETUDE:** SYSTEME DE COMMANDE DE VANNE PIEZOELECTRIQUE | | | **FEUILLE:** 1 de 3 |
| **N° du dessin:** | | **N° de REVISION:** | **DATE:** |
| **COMPOSITION DE L'EQUIPE:** Ingénieur développement, Ingénieur système, Directeur qualité | | | **DATE DE LA REUNION:** 04.11.97 |
| **Partie examinée:** | Etat 1: Le système ferme la vanne | | |
| **Intention de conception:** | Transférer une quantité définie de charge électrique au dispositif de commande piézoélectrique pour fermer la vanne à un instant donné | | |

| Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise | Commen-taires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|
| Entrée: Charger C1 | NE PAS FAIRE | Ne pas charger; y compris ne pas transférer | Panne de courant<br>Défaillance du convertisseur<br>Panne en C1<br>T1 est fermé en permanence<br>T2 est ouvert en permanence<br>T1 défectueux<br>Défaillance des diodes (D1, D3):<br>– Diode D1 en circuit ouvert, absence de courant<br>– Diode D3 en court-circuit, court-circuit via D4 vers le retour bas de la vanne piézoélectrique ou par R à la terre<br>C2 défectueux<br>Rupture des fils<br>T4 défectueux<br>R défectueux<br>T3 défectueux | Pas de flux par C2 vers la vanne piézoélectrique<br>La vanne ne se ferme pas; elle est ouverte en permanence<br>Afflux de réactif dans le caisson | Néant | Situation inacceptable<br>Changement de conception exigé | Alarme de niveau haut<br>Essai individuel de série | J. Smith |

| Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise | Commen-taires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|
| Entrée: Charger C1 | PLUS | Plus de charge que défini | Charge en C2 trop élevée<br>Convertisseur défectueux<br>Le transistor T1 ne se ferme pas en temps voulu<br>C2 défectueux<br>Le convertisseur en courant alternatif/continu fournit une tension trop élevée<br>Le transistor T1 ne se ferme pas en temps voulu<br>Protection T3 défectueuse | La vanne piézoélectrique se ferme plus tôt que prévu<br>Vanne piézoélectrique endommagée | Le débitmètre indique une quantité trop importante; le transistor T3 décharge la vanne piézoélectrique;<br>Aucune apparente | Situation inacceptable | Prévoir une alarme de niveau élevé | Peter Peterson |
| Charger C1 | MOINS | Moins de charge que spécifié | Capacité insuffisante<br>Isolation de câble défectueuse; la charge disparaît<br>T1 se ferme trop tôt<br>T2 est partiellement ouvert | Charge insuffisante en C2<br>La vanne se ferme plus tard que prévu | Néant | Situation inacceptable | Alarme | J. Smith |
| Entrée: Charger C1 | EN PLUS DE | T1 est ouvert en plus de T2 | Moins de charge appliquée à C2<br>La vanne ne se ferme pas<br>Afflux de réactif dans le caisson de réaction | Réaction chimique non contrôlée | Aucune apparente | De légères différences pourraient être acceptables | Alarme<br>Essai individuel de série<br>Remise à zéro<br>Définir des différences acceptables | J. Smith |

## B.7 HAZOP pour une procédure d'avertisseur sonore dans une aire de stationnement de trains

Les trains qui sont dans une aire de stationnement doivent faire retentir un avertisseur avant de se déplacer. Un changement de procédure a été exigé en raison des restrictions liées au bruit prévues. La nouvelle procédure exige, outre le chef de train, une personne suffisamment qualifiée (PQ) pour vérifier la zone autour du train avant tout déplacement afin de s'assurer qu'il peut être fait en toute sécurité.

La procédure est la suivante:

1. Procédure initiale
    - 1.1 Le conducteur observe l'indication STOP depuis la cabine de pilotage.
    - 1.2 La PQ se trouve à proximité de la cabine de pilotage.
    - 1.3 Le conducteur confirme à la PQ qu'il est prêt ou qu'il a modifié les extrémités, et commence la procédure de vérification.
    - 1.4 Le conducteur demande au chef de train (PA interne) de commencer la procédure de vérification.
2. Procédure de vérification de la PQ
    - 2.1 La PQ vérifie les 4 premières voitures du côté gauche du train.
        - 2.1.1 Si la voie n'est pas libre, supprimer/retirer l'obstacle puis recommencer à vérifier les 4 premières voitures du côté gauche du train.
        - 2.1.2 Si la voie est libre, la PQ donne un coup de sifflet durable et sonore pour signaler que le train part.
    - 2.2 La PQ vérifie les 4 premières voitures du côté droit du train.
        - 2.2.1 Si la voie n'est pas libre, supprimer/retirer l'obstacle puis recommencer à vérifier les 4 premières voitures du côté droit du train.
        - 2.2.2 Si la voie est libre, la PQ donne un coup de sifflet durable et sonore pour signaler que le train part.
    - 2.3 La PQ avertit le conducteur que les deux côtés du train ont été vérifiés et que la voie est entièrement libre.
3. Procédure de vérification du chef de train
    - 3.1 Le chef de train ouvre les portes de chaque côté du train.
    - 3.2 Faire une annonce PA interne et externe de chaque côté du train "Attention, ce train est sur le point de quitter l'aire de stationnement de la voie n° x".
    - 3.3 Vérifier les 4 dernières voitures du côté droit du train.
        - 3.3.1 Si la voie n'est pas libre, supprimer/retirer l'obstacle puis recommencer à vérifier les 4 dernières voitures du même côté du train.
        - 3.3.2 Si la voie est libre, le chef de train donne un coup de sifflet durable et sonore pour signaler que le train part.
    - 3.4 Vérifier les 4 dernières voitures du côté gauche du train.
        - 3.4.1 Si la voie n'est pas libre, supprimer/retirer l'obstacle puis recommencer à vérifier les 4 dernières voitures du même côté du train.
        - 3.4.2 Si la voie est libre, le chef de train donne un coup de sifflet durable et sonore pour signaler que le train part.
    - 3.5 Fermer les portes de chaque côté et vérifier par inspection visuelle et par vérification que le voyant Porte Ouverte est éteint.

3.6 Faire retentir la cloche TOUT EST EN ORDRE à l'intention du conducteur.

4. Terminer la procédure de départ

4.1 Le conducteur avertit la PQ que le chef de train a terminé le processus de départ.

4.2 La PQ prend contact avec le poste d'aiguillage pour avertir l'aiguilleur que le train est prêt à partir.

4.2.1 Si le signal ne peut pas être changé en "libre" dans un délai d'environ 1 min, maintenir le signal sur STOP, puis avertir la PQ du délai approximatif de changement et avertir la PQ avant le changement pour que la PQ et le chef de train puissent recommencer la procédure de vérification.

4.2.2 Après avoir reçu confirmation de la part de la PQ que le train est prêt à partir, changer les signaux concernés.

4.3 Le conducteur confirme l'indication VOIE LIBRE et réalise le mouvement progressif modifié.

5. Le conducteur fait faire au train le signal par sifflet et essaie l'avertisseur sonore du train.

Le Tableau B.8 est une matrice de la décomposition fonctionnelle et le Tableau B.9 un exemple de tableau HAZOP.

**Tableau B.8 – Matrice de décomposition fonctionnelle pour une procédure d'avertisseur sonore dans une aire de stationnement de trains**

| N° | Etape | Conditions initiales | Informations nécessaires | Communication, qui, pourquoi, quand | Points de contrôle | Conditions finales |
|---|---|---|---|---|---|---|
| 1 | Procédure initiale<br>– Le conducteur observe l'indication STOP depuis la cabine de pilotage<br>– Le conducteur confirme à la PQ qu'il est prêt ou qu'il a modifié les extrémités, et commence la procédure de vérification<br>– Le conducteur demande au chef de train (PA interne) de commencer la procédure de vérification | – Le train se trouve dans l'aire de stationnement, le signal indiquant STOP<br>– La PQ se trouve à proximité de la cabine de pilotage<br>– Le chef de train se trouve dans le compartiment du chef de train | – Introduction sur le site et sensibilisation à la sécurité des voies<br>– Formation (conducteur, chef de train, aiguilleurs, PQ)<br>– N° de train et voie du train affichés | – Le conducteur indique verbalement à la PQ qu'il est prêt ou qu'il a modifié les extrémités<br>– Conducteur à chef de train par le PA interne quand il est prêt ou quand il a modifié les extrémités | – Le conducteur a observé l'indication STOP | – Le train se trouve dans l'aire de stationnement, le signal indiquant STOP<br>– La PQ se trouve à proximité de la cabine de pilotage<br>– Le chef de train se trouve dans le compartiment du chef de train |
| 2 | Procédure de vérification de la PQ<br>– La PQ vérifie les 4 premières voitures du côté gauche du train<br>– Si la voie n'est pas libre, supprimer/retirer l'obstacle puis recommencer à vérifier les 4 premières voitures du côté gauche du train<br>– Si la voie est libre, la PQ donne un coup de sifflet durable et sonore puis vérifie les 4 premières voitures du côté droit du train<br>– Si la voie n'est pas libre, supprimer/retirer l'obstacle puis recommencer à vérifier les 4 premières voitures du côté droit du train<br>– Si la voie est libre, la PQ donne un coup de sifflet durable et sonore<br>– La PQ avertit le conducteur que les deux côtés du train ont été vérifiés et que la voie est entièrement libre | – Le train se trouve dans l'aire de stationnement, le signal indiquant STOP<br>– La PQ se trouve à proximité de la cabine de pilotage<br>– Le chef de train se trouve dans le compartiment du chef de train | – Introduction sur le site et sensibilisation à la sécurité des voies<br>– Formation (conducteur, chef de train, aiguilleurs, PQ) | – La PQ siffle de chaque côté quand la voie est entièrement libre<br>– La PQ indique verbalement au conducteur qu'elle a terminé la vérification (et supprimé les obstacles) des deux côtés | – La PQ doit pouvoir voir l'extrémité des 4 premières voitures de chaque côté, ce qui pourrait impliquer de marcher sur une certaine distance le long du train<br>– La voie est libre si rien ne gêne le train (sur les voies ou de chaque côté, dans l'espace autour du train) | – Le train se trouve dans l'aire de stationnement, le signal indiquant STOP<br>– La PQ se trouve à proximité de la cabine de pilotage<br>– Le chef de train se trouve dans le compartiment du chef de train<br>– Voie entièrement libre pour les 4 premières voitures |

| N° | Etape | Conditions initiales | Informations nécessaires | Communication, qui, pourquoi, quand | Points de contrôle | Conditions finales |
|---|---|---|---|---|---|---|
| 3 | Procédure de vérification du chef de train<br>– Le chef de train ouvre les portes de chaque côté du train<br>– Faire une PA interne et externe de chaque côté du train "Attention, ce train est sur le point de quitter l'aire de stationnement de la voie n° x".<br>– Vérifier les 4 dernières voitures du côté droit du train<br>– Si la voie n'est pas libre, supprimer/retirer l'obstacle puis recommencer à vérifier les 4 dernières voitures du même côté du train<br>– Si la voie est libre, le chef de train donne un coup de sifflet durable et sonore<br>– Vérifier les 4 dernières voitures du côté gauche du train<br>– Si la voie n'est pas libre, supprimer/retirer l'obstacle puis recommencer à vérifier les 4 dernières voitures du même côté du train<br>– Si la voie est libre, le chef de train donne un coup de sifflet durable et sonore<br>– Fermer les portes de chaque côté<br>– Faire retentir la cloche TOUT EST EN ORDRE à l'intention du conducteur | – Le train se trouve dans l'aire de stationnement, le signal indiquant STOP et les portes étant ouvertes | – Introduction sur le site et sensibilisation à la sécurité des voies<br>– Formation (conducteur, chef de train, aiguilleurs, PQ)<br>– Connaissance du type de train en vérification | – PA interne et externe du chef de train après l'ouverture des portes<br>– Sifflet du chef de train de chaque côté quand la voie est entièrement libre<br>– Le chef de train sonne la cloche pour prévenir le conducteur que la voie est entièrement libre pour les 4 dernières voitures | – Commencer par ouvrir toutes les portes de chaque côté du train (vérifier le voyant Porte Ouverte et vérification visuelle)<br>– Le chef de train doit pouvoir voir l'extrémité du train des deux côtés<br>– La voie est libre si rien ne gêne le train (sur les voies ou de chaque côté, dans l'espace autour du train)<br>– Quand la voie est libre de chaque côté, fermer les portes du côté en question (vérifier le voyant Porte Ouverte et vérification visuelle)<br>– Le chef de train n'entendra pas de cloche en cas de défaillance | – Le train se trouve dans l'aire de stationnement, le signal indiquant STOP et les portes étant fermées |

| N° | Etape | Conditions initiales | Informations nécessaires | Communication, qui, pourquoi, quand | Points de contrôle | Conditions finales |
|---|---|---|---|---|---|---|
| 4 | Terminer la procédure de départ<br>– Le conducteur avertit la PQ que le chef de train a terminé le processus de départ<br>– La PQ prend contact avec le poste d'aiguillage pour avertir l'aiguilleur que le train est prêt à partir<br>– Si le signal ne peut pas être changé en "libre" dans un délai d'environ 1 min, l'aiguilleur maintient le signal sur STOP, puis avertit la PQ du délai approximatif de changement et avertit la PQ avant le changement pour que la PQ et le chef de train puissent recommencer la procédure de vérification<br>– Après avoir reçu confirmation de la part de la PQ que le train est prêt à partir, changer les signaux concernés<br>– Le conducteur confirme l'indication VOIE LIBRE et réalise le mouvement progressif modifié | – Le train se trouve dans l'aire de stationnement, le signal indiquant STOP et les portes étant fermées<br>– La PQ se trouve à proximité de la cabine de pilotage<br>– Le chef de train se trouve dans le compartiment du chef de train | – Introduction sur le site et sensibilisation à la sécurité des voies<br>– Formation (conducteur, chef de train, aiguilleurs, PQ) | – Le conducteur indique verbalement au PQ qu'il a entendu la cloche du chef de train<br>– La PQ à l'aiguilleur par radio (ou téléphone mobile ou téléphone de signal, comme moyens de remplacement) quand le conducteur signale que le processus de départ est terminé | – Le signal doit porter l'indication VOIE LIBRE<br>– Le conducteur doit recevoir confirmation que la voie est entièrement libre à la fois de la PQ et du chef de train avant de terminer le processus de départ | – Le train franchit le signal VOIE LIBRE |
| 5 | Le conducteur fait faire au train le signal par sifflet et essaie l'avertisseur sonore du train | – Le train franchit le signal VOIE LIBRE | – Introduction sur le site et sensibilisation à la sécurité des voies<br>– Formation (conducteur, chef de train, aiguilleurs, PQ) | Néant | – La procédure est terminée quand l'avertisseur sonore a retenti avec succès au signal par sifflet | – Le train a quitté l'aire de stationnement |

**Tableau B.9 – Exemple de tableau HAZOP pour une procédure d'avertisseur sonore dans une aire de stationnement de trains**

| | | |
|---|---|---|
| **TITRE DE L'ETUDE:** PROCEDURE D'AVERTISSEUR SONORE DANS UNE AIRE DE STATIONNEMENT DE TRAINS | | **FEUILLE:** 1 sur x |
| **N° du dessin:** | **N° de REVISION:** | **DATE:** |
| **COMPOSITION DE L'EQUIPE:** Conducteur, Chef de train, Contrôleur de zone, Directeur d'équipe de train, Directeur contrôle de réseau | | **DATE DE LA REUNION:** |
| **Partie examinée:** | Etape 1: Procédure initiale | |
| **Intention de conception:** | Préparer le train et le personnel à la procédure de vérification | |

| Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|
| Procédure initiale | MAUVAISE ACTION | | La PQ, le conducteur, le chef de train ne commencent pas la procédure | Retard opérationnel – le train ne se déplace pas | La procédure garantira que le train ne démarrera pas<br>Formation<br>Vigilance des employés | | Néant | |
| Procédure initiale | ACTION SUPPLE-MENTAIRE | | La PQ reçoit un appel sur son téléphone portable | Retard opérationnel – le train ne se déplace pas | La procédure assurera la protection en ne permettant pas au train de démarrer<br>Formation<br>Vigilance des employés | | Néant | |
| Procédure initiale | CLARTE | | La procédure se réfère au côté gauche et au côté droit du train | Confusion sur le côté du train auquel il est fait référence | | | Pour supprimer l'éventualité d'une confusion, modifier la procédure en se référant au côté conducteur et au côté extérieur plutôt qu'au côté gauche et au côté droit. | J. Suffield |

| Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|
| Procédure initiale | PLUS DE TEMPS | | L'opérateur met plus de temps que prévu pour réaliser une activité | Retard opérationnel – le train ne se déplace pas | La procédure assurera la protection en ne permettant pas au train de démarrer<br>Formation<br>Vigilance des employés | | Une autre procédure distincte sera réalisée<br>Formation<br>Vigilance des employés | Néant |
| Procédure initiale | CONDITIONS ANORMALES | | Défaillance de signal | Cette procédure sera interrompue et remplacée par une autre pour faire face à la défaillance du signal | Une autre procédure distincte sera réalisée<br>Formation<br>Vigilance des employés | | Néant | |
| Procédure de vérification de la PQ | AUCUNE ACTION | | La PQ ne commence pas à vérifier les deux côtés du train | Retard opérationnel – le train ne se déplace pas | La procédure assurera la protection en ne permettant pas au train de démarrer<br>Formation<br>Vigilance des employés | | Néant | |
| Procédure de vérification de la PQ | AUCUNE ACTION | | La PQ commence à vérifier le train mais ne termine pas sa tâche | Les conséquences courantes ne sont pas affectées (il en va de même pour le réseau dans sa totalité) | La procédure assurera la protection en ne permettant pas au train de démarrer<br>Formation<br>Vigilance des employés | | Néant | |

| Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|
| Procédure de vérification de la PQ | DAVANTAGE D'ACTION | | La PQ réalise une activité supplémentaire qui ne fait pas partie de la procédure (une distraction l'empêche de terminer la procédure) | Retard opérationnel – le train ne se déplace pas | La procédure assurera la protection en ne permettant pas au train de démarrer<br>Formation<br>Vigilance des employés | | Néant | |
| Procédure de vérification de la PQ | ACTION SUPPLE-MENTAIRE | | La PQ reçoit un appel sur son téléphone portable | Retard opérationnel – le train ne se déplace pas | La procédure assurera la protection en ne permettant pas au train de démarrer<br>Formation<br>Vigilance des employés | | Néant | |
| Procédure de vérification de la PQ | PLUS DE TEMPS | | La PQ met plus de temps que prévu à vérifier le train | Retard opérationnel – le train ne se déplace pas | La procédure assurera la protection en ne permettant pas au train de démarrer<br>Formation<br>Vigilance des employés | | Néant | |
| Procédure de vérification de la PQ | MOINS DE TEMPS | | La PQ termine sa procédure et parle à l'aiguilleur avant de recevoir du conducteur une réponse qui confirme que le chef de train a terminé sa procédure | L'aiguilleur libère la voie et le conducteur agit, ou le conducteur attend la cloche du chef de train. Pas de changement à la conséquence courante. | Mouvement progressif<br>Avertisseur d'urgence<br>Vitesse limitée à 8 km/h<br>Formation<br>Vigilance des employés<br>Procédure | | Néant | |

| Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|
| Procédure de vérification de la PQ | CONDITIONS ANORMALES | | Défaillance de signal | Cette procédure sera interrompue et remplacée par une autre pour faire face à la défaillance du signal | Une autre procédure distincte sera réalisée<br>Formation<br>Vigilance des employés | | Néant | |
| Procédure de vérification de la PQ | CONDITIONS ANORMALES | | Mauvais temps, obscurité, défaillance de la régie d'électricité (éclairage), la PQ fait une chute | La PQ dérape, trébuche ou tombe<br>La procédure garantit que le train ne se déplacera pas, et quelqu'un finirait par remarquer son absence<br>Retard opérationnel | EPI<br>Lampe torche<br>Formation<br>Vigilance du conducteur et de l'aiguilleur<br>Procédure<br>Formation<br>Vigilance des employés | | Néant | |
| Procédure de vérification du chef de train | MISSION | | Mauvaise compréhension de la raison pour laquelle la procédure est appliquée et n'est pas réalisée ailleurs, dans la mesure où elle ne semble pas être associée à l'avertisseur | L'ouverture des portes crée un risque qu'une personne saute dans le train et soit prise dans les portes ou tombe sur le sol<br>L'ouverture des portes crée un risque que des passagers ayant manqué leur arrêt puissent accéder au couloir ferroviaire | Le chef de train et la PQ assurent un rôle de surveillance à l'égard de ce comportement<br>Formation<br>Vigilance des employés<br>D'autres employés vérifient le train avant qu'il ne parvienne à l'aire de stationnement et s'occupent des passagers du train | | Envisager de modifier la procédure pour que les portes restent fermées. Comme les portes sont ouvertes à la suite d'une recommandation issue d'une précédente évaluation des risques, vérifier que cette action n'a pas d'effet négatif sur le niveau de risque | J. Suffield |

| Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|
| Procédure de vérification du chef de train | MISSION | | Comme les portes s'ouvrent de chaque côté et se ferment simultanément, le chef de train pourrait par inadvertance permettre à quelqu'un de monter (ou de descendre) du train (du côté opposé à celui qu'il est en train de vérifier) | Une personne pourrait monter ou descendre du train et s'exposer à un danger (proximité de l'infrastructure des voies) | | | Envisager de modifier la procédure pour que les portes s'ouvrent d'un seul côté à la fois, ou évaluer le besoin d'ouvrir les portes. Comme les portes sont ouvertes à la suite d'une recommandation issue d'une précédente évaluation des risques, vérifier que cette action n'a pas d'effet négatif sur le niveau de risque | J. Suffield |
| Procédure de vérification du chef de train | AUCUNE ACTION | | Le système PA ne fonctionne pas | La procédure ne fournit aucune ligne directrice sur ce que doit faire le chef de train dans cette situation | Formation<br>Vigilance des employés | | Mettre à jour la procédure pour s'assurer que les mesures appropriées sont prises en cas de défaillance de PA | J. Suffield |
| Procédure de vérification du chef de train | AUCUNE ACTION | | Le chef de train ne fait pas la vérification selon la procédure | Pas de différence pour le reste du réseau, sauf qu'aucun avertisseur ne retentit. Possibilité d'accident mortel | Mouvement progressif<br>Avertisseur d'urgence<br>Vitesse limitée à 8 km/h<br>Formation<br>Vigilance des employés<br>Procédure | | Néant | |

| Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|
| Procédure de vérification du chef de train | MAUVAISE ACTION | | Le chef de train utilise la cloche selon la procédure | Le conducteur interprète mal la cloche du chef de train et agit contrairement au signal. Possibilité d'accident mortel pour la PQ. | Mouvement progressif<br>Avertisseur d'urgence<br>Vitesse limitée à 8 km/h<br>Formation<br>Vigilance des employés<br>Procédure | Modifier la procédure afin de remplacer la cloche du chef de train par une communication par interphone | | J. Suffield |
| Procédure de vérification du chef de train | PLUS DE TEMPS | | Le chef de train met plus de temps que prévu pour réaliser une activité | Retard opérationnel – le train ne se déplace pas | La procédure assurera la protection en ne permettant pas au train de démarrer<br>Formation<br>Vigilance des employés | | Néant | |
| Procédure de vérification du chef de train | MAUVAISE INFOR-MATION | | Le chef de train et le conducteur ne se trouvent pas sur le bon train | La PQ applique la procédure et vérifie un mauvais train<br>Retard opérationnel. L'autorisation de départ est donnée à un mauvais train (conséquences opérationnelles importantes) | L'aiguilleur signalera à la PQ qu'il ne s'agit pas du bon train | | Néant | |
| Procédure de vérification du chef de train | CONDITIONS ANORMALES | | Défaillance de signal | Cette procédure sera interrompue et remplacée par une autre pour faire face à la défaillance du signal | Une autre procédure distincte sera réalisée<br>Formation<br>Vigilance des employés | | Néant | |

| Propriété | Mot-guide | Ecart | Causes possibles | Conséquences | Moyens de maîtrise existants | Commentaires | Actions exigées | Responsable actions |
|---|---|---|---|---|---|---|---|---|
| Procédure de vérification du chef de train | CONDITIONS ANORMALES | | Le chef de train ne peut pas voir les 4 dernières voitures et il n'y a aucune exigence | Les 4 dernières voitures ne sont pas vérifiées, il n'est donc pas certain que la voie est libre pour elles<br>La procédure n'indique pas explicitement que faire | Mouvement progressif<br>Avertisseur d'urgence<br>Vitesse limitée à 8 km/h<br>Formation<br>Vigilance des employés<br>Procédure | | Revoir la procédure et proposer une mesure appropriée (elle ne correspond pas actuellement au rôle de la PQ) | J. Suffield |

# Bibliographie

IEC 60812:2006, *Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*

IEC 61025:2006, *Analyse par arbre de panne (AAP)*

IEC 61160:2005, *Revue de conception*

IEC 61511-3:2003, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 3: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité*

IEC 62502:2010, *Techniques d'analyse de la sûreté de fonctionnement – Analyse par arbre d'événement (AAE)*

IEC/ISO 31010:2009, *Gestion des risques – Techniques d'évaluation des risques*

ISO 31000:2009, *Management du risque – Principes et lignes directrices*

ISO Guide 73:2009, *Management du risque – Vocabulaire*

Defence Standard 00-58:2000, *HAZOP Studies on Systems containing Programmable Electronics*, Ministry of Defence, UK (disponible en anglais seulement)

*A Guide to Hazard and Operability Studies.* Chemical Industries Association, London, UK 1992 (disponible en anglais seulement)

*Das PAAG-Verfahren.* International Social Security Association (ISSA), c/o BG RCI, Heidelberg, Germany, 2000, ISBN 92-843-7037-X (voir aussi http://www.issa.int/ger/resurs/resources/das-paag-verfahren)

*Storingsanalyse Waarom? Wanneer? Hoe?* Directoraat-Generaal van de Arbeid 1982, ISBN 9053070427, 9789053070420 (corps du texte en hollandais, annexes en anglais)

Kletz, Trevor A. HAZOP and HAZAN – *Identifying and Assessing Chemical Industry Hazards* (4th Edition), Taylor & Francis, 2006, ISBN 0852955065 (disponible en anglais seulement)

Knowlton, Ellis. *Une introduction aux études sur les risques et l'exploitabilité: une approche qui utilise des mots-guides*. Chemetics International, Vancouver, Canada, 1992, ISBN 0-9684016-0-0 (disponible aussi en anglais, en espagnol, en finnois, en arabe, en chinois, en hindi et en coréen)

Knowlton, Ellis. *A manual of Hazard & Operability Studies, The creative identification of deviations and disturbances*. Chemetics International, Vancouver, Canada, 1992, ISBN 0-9684016-3-5 (disponible en anglais seulement)

Redmill, Felix; Chudleigh, Morris and Catmur, James. *System Safety: HAZOP and Software HAZOP*. Wiley, 1999, ISBN 0-471-98280-6 (disponible en anglais seulement)

Crawley, Frank; Preston, Malcolm and Tyler, Brian, *HAZOP: Guide to best practice. Guidelines to best practice for the process and chemical industries*. Ed 2 European Process Safety Centre, Chemical Industries Association & Institution of Chemical Engineers. Rugby, England, IChem, 2008, ISBN 978 0-85295-525 3 (disponible en anglais seulement)

*Guidelines for Hazard Evaluation Procedures.* Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, USA, 1999, ISBN 0-8169-0491-X (disponible en anglais seulement)

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel:  + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch