BS EN 61882:2016

BSI Standards Publication

Hazard and operability studies (HAZOP studies) — Application guide

bsi.

National foreword

This British Standard is the UK implementation of EN 61882:2016. It is identical to IEC 61882:2016. It supersedes BS IEC 61882:2001 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2016

ISBN 978 0 580 87354 6
ICS 03.100.50; 03.120.01; 13.020.30

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2016.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 61882

June 2016

ICS 03.100.50; 03.120.01; 13.020.30

English Version

Hazard and operability studies (HAZOP studies) - Application guide (IEC 61882:2016)

Études de danger et d'exploitabilité (études HAZOP) - Guide d'application (IEC 61882:2016)

HAZOP-Verfahren (HAZOP-Studien) - Anwendungsleitfaden (IEC 61882:2016)

This European Standard was approved by CENELEC on 2016-04-14. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

European foreword

The text of document 56/1653/FDIS, future edition 2 of IEC 61882, prepared by IEC/TC 56 "Dependability" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 61882:2016.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2017-01-14
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2019-04-14

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 61882:2016 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60812:2006	NOTE	Harmonized as EN 60812:2006 (not modified).
IEC 61025:2006	NOTE	Harmonized as EN 61025:2007 (not modified).
IEC 61160:2005	NOTE	Harmonized as EN 61160:2005 (not modified).
IEC 61511-3:2003	NOTE	Harmonized as EN 61511-3:2004 (not modified).
IEC 62502:2010	NOTE	Harmonized as EN 62502:2010 (not modified).
IEC/ISO 31010:2009	NOTE	Harmonized as EN 31010:2010 (not modified).

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu

Publication	Year	Title	EN/HD	Year
IEC 60050-192	-	International electrotechnical vocabulary - Part 192: Dependability	-	-

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.

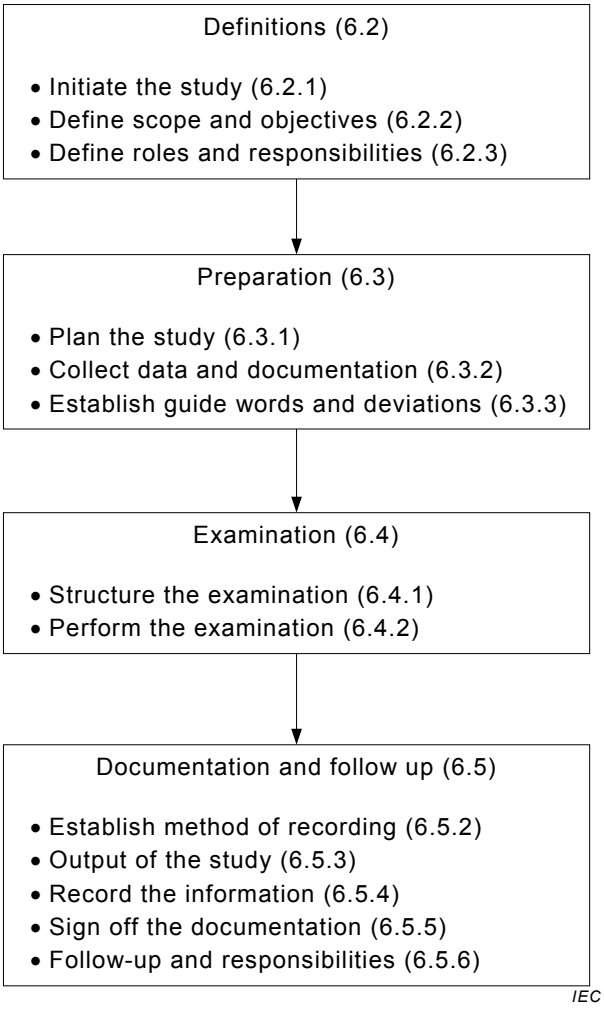

Figure 1 – The HAZOP study procedure

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).

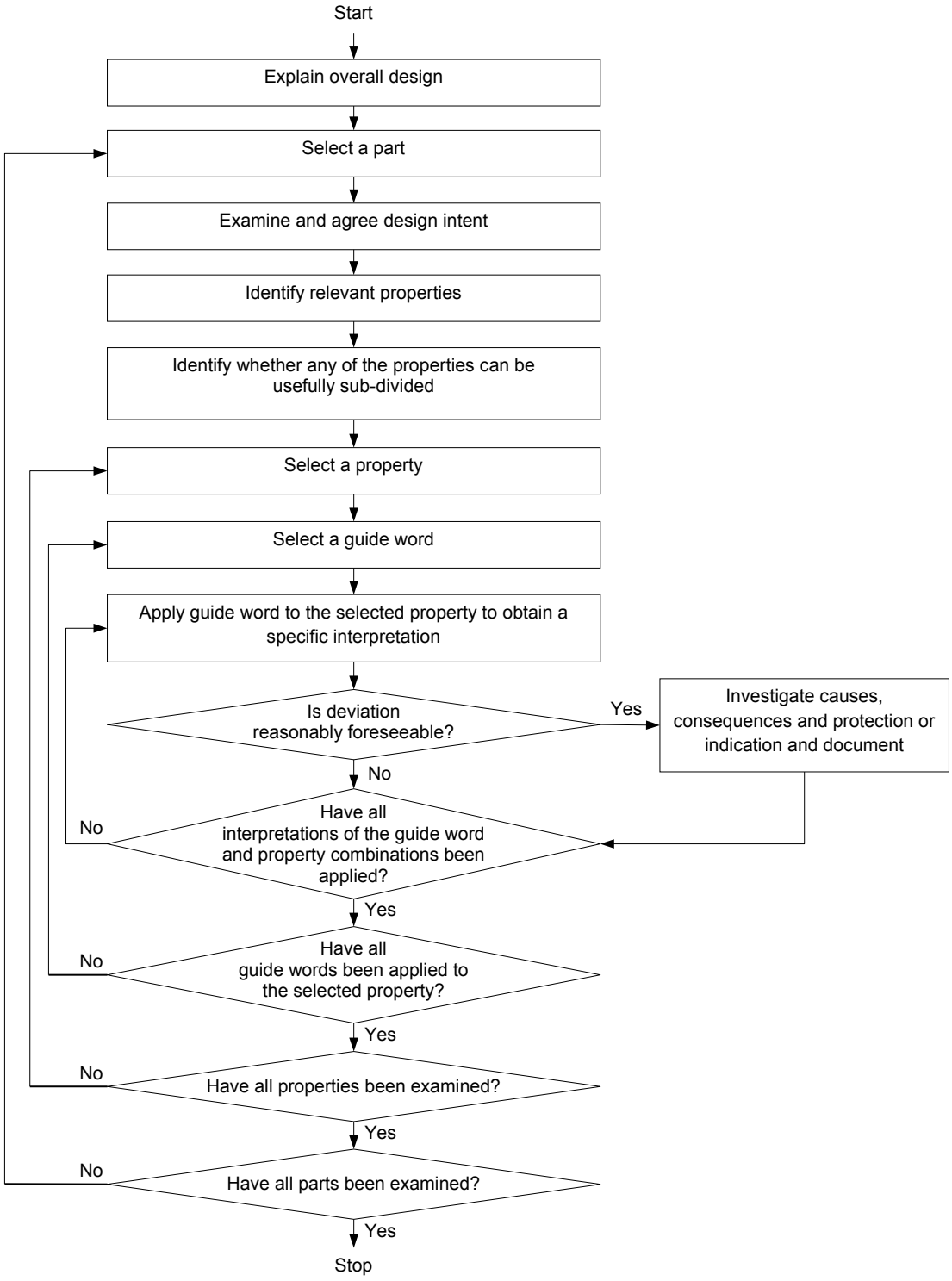

Figure 2 – Flow chart of the HAZOP examination procedure – Property first sequence

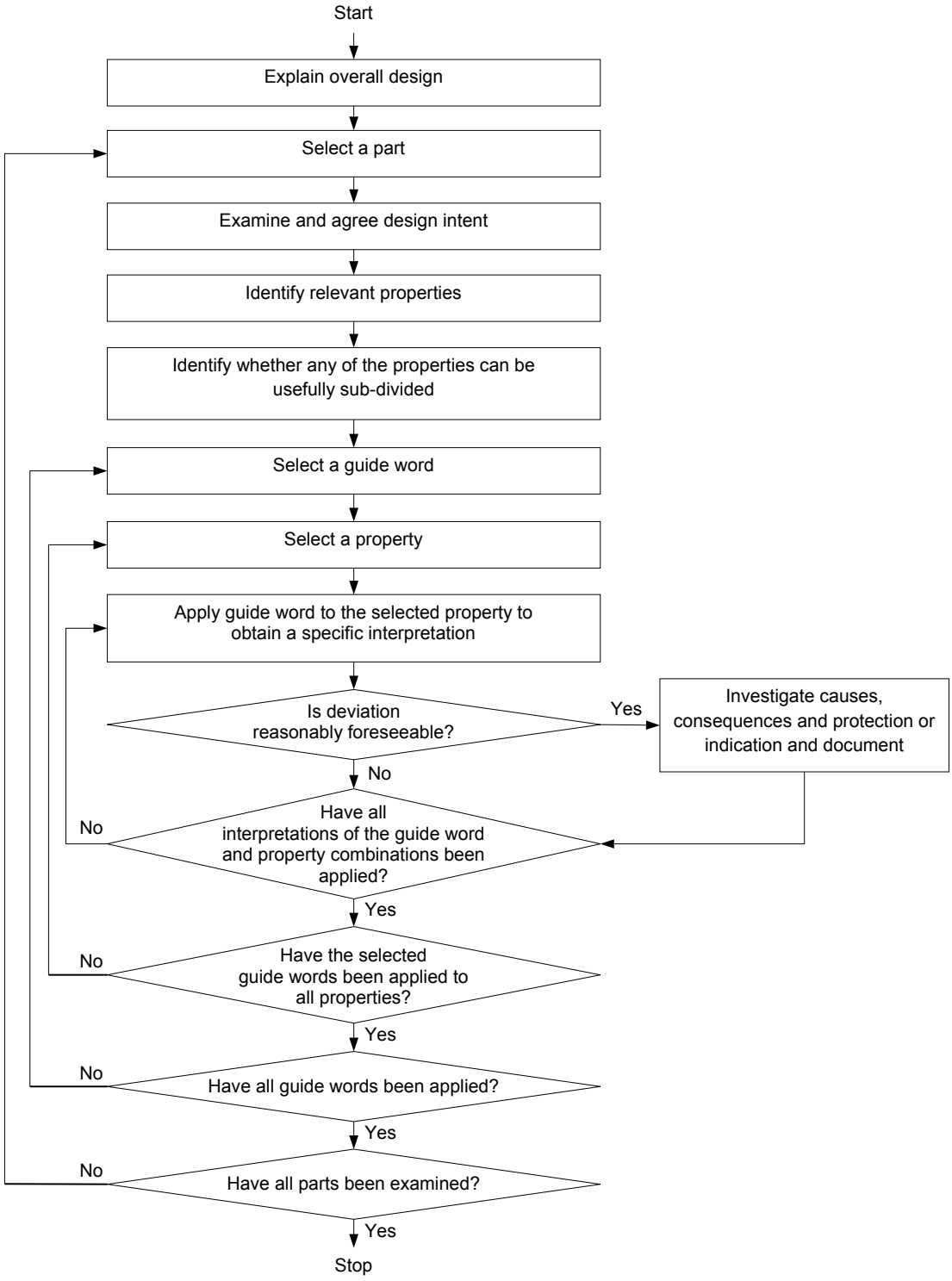

Figure 3 – Flow chart of the HAZOP examination procedure – Guide word first sequence

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.

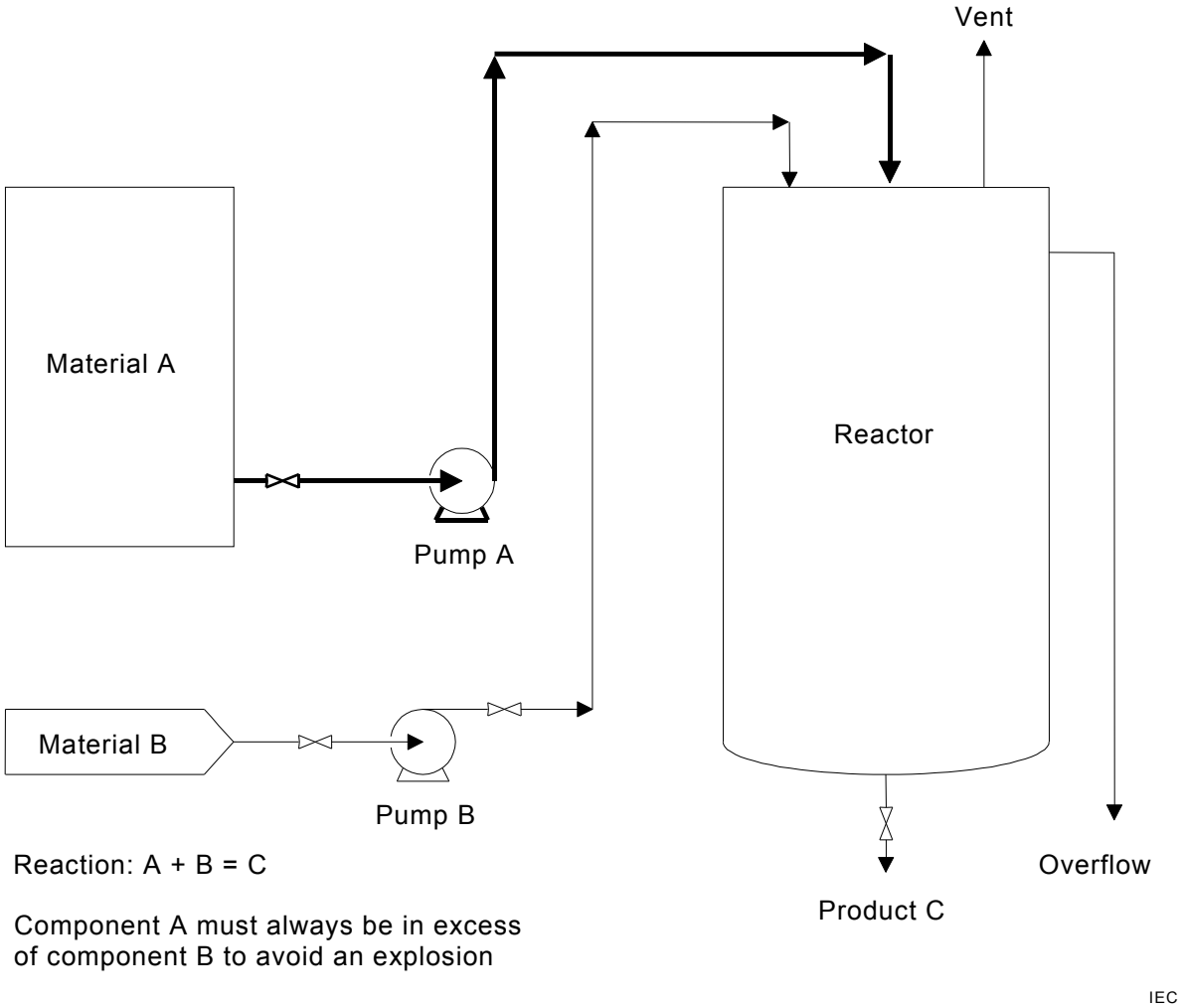

Figure B.1 – Simple flow sheet

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 **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 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 Increased flow rate of A	Wrong size impeller Wrong pump fitted	Possible reduction in yield Product will contain large excess A	None		Check pump flows and characteristics during commis-sioning 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 Possible vortexing and leading to an explosion Inadequate flow	None	Unacceptable Same as 1	Low-level alarm in tank 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 External leaks	Line, valve or gland leaks	Environmental contamination 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 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 Material other than A in supply tank	Wrong material in supply tank	Unknown Would depend on material	Tanker contents identity checked and analysed prior to discharge	Position acceptable		
12	OTHER THAN	Destination reactor	External leak 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. 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 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 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 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 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.

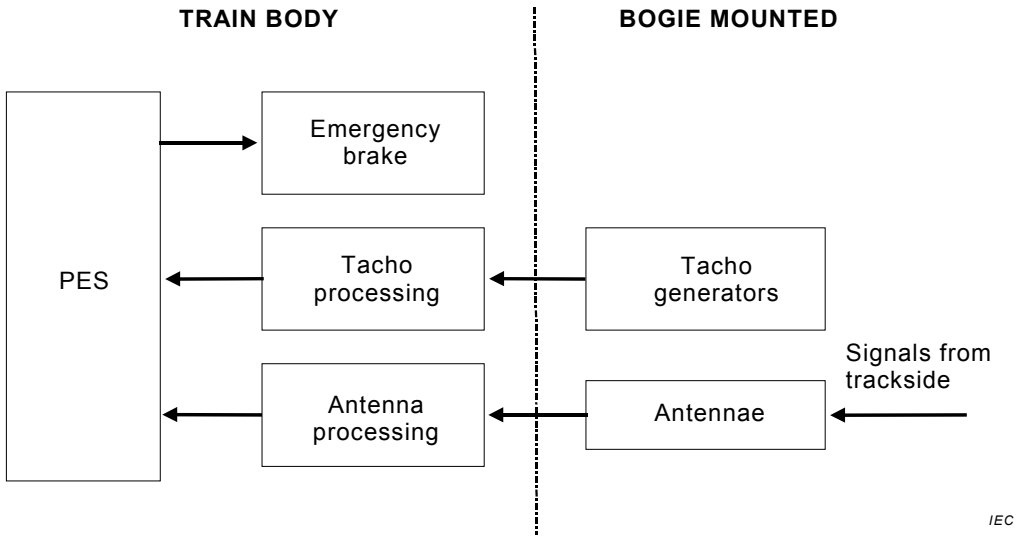

Figure B.2 – Train-carried ATP equipment

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 Reverse electrical energy	Reverse of alarm initiation 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 Cable damage	Personnel not alerted	Dual PA system Dual cabling Dual power supplies 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.

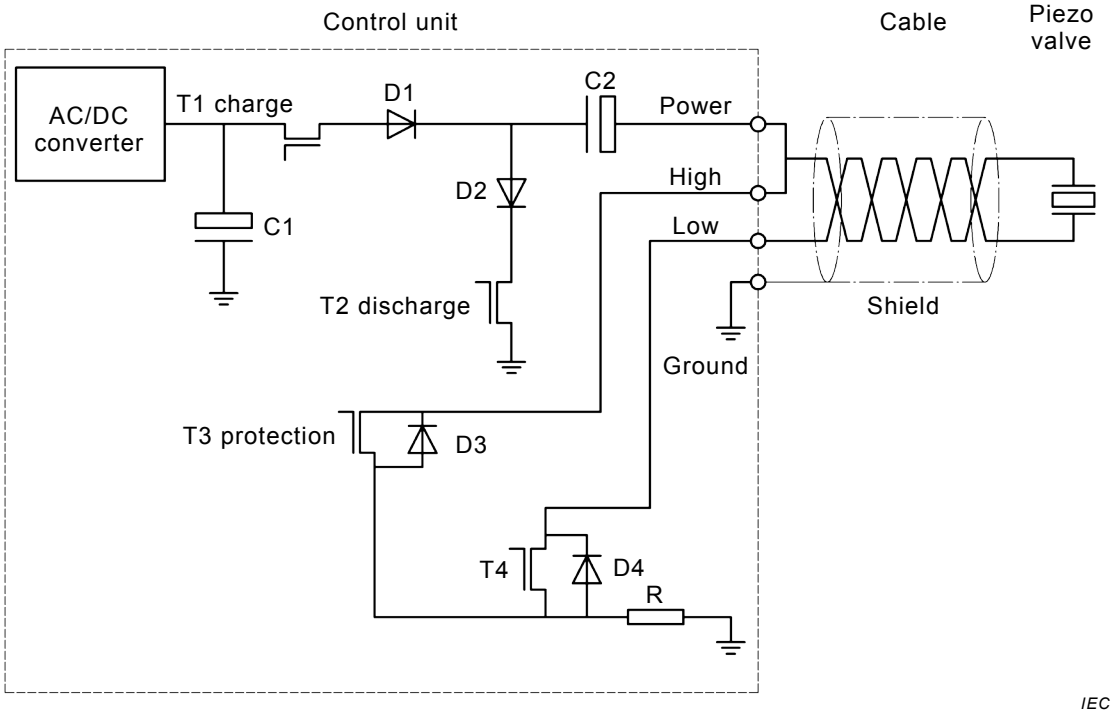

Figure B.3 – Piezo valve control system

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 1. Charge in C1	1. Transfer charge via T1, D1 and C2	C1 and converter	1. Power to power side of valve
Characteristics: Voltage 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 4. Isolate via T2 5. Prevent overcharge via T3	Signal from controller	T1, T3 and T4 Overcharge to ground
	6. Prevent reverse flow of charge via D2	Power side of valve	
State 2: Open valve 1. Discharge power side of valve Characteristics: Voltage Capacity	1. Isolate from C1 and converter via T1 2. Transfer power charge via D2 and T2 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: Charge in C1	NO	No charge; including don't transfer	Power outage Failure of converter Fault in C1 T1 is permanently closed T2 is permanently open T1 faulty Diodes (D1, D3) failure: – Diode D1 with open circuit; no current flows – Diode D3 shortened; shortcut via D4 to low side of piezo valve or via R to ground C2 faulty Broken wires T4 faulty R faulty T3 faulty	No flow via C2 into piezo valve Valve does not close; permanently open Reactive material running into the vessel	None	Situation not acceptable Design change required	High-level alarm 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 Faulty converter Transistor T1 does not close in time C2 faulty AC/DC converter delivers too high voltage Transistor T1 does not close in time Faulty protection T3	Piezo valve closes earlier than defined Damaged piezo valve	Flow meter shows too high quantity; transistor T3 discharges piezo valve; None shown	Situation not acceptable	Consider high level alarm	Peter Peterson
Charge in C1	LESS	Less charge than specified	Insufficient capacity exists Faulty insulation of cable; charge disappears T1 closes too early T2 is partly open	Insufficient charge in C2 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 Valve does not close Reactive material runs into the reaction vessel	Uncontrolled chemical reaction	None shown	Small differences could be acceptable	Alarm Test routine Reset 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 – Driver observes STOP indication from leading crew compartment – Driver to confirm to QP that driver preparation is complete or that driver has changed ends and to commence checking procedure – Driver advises guard (internal PA) to commence checking procedure	– Train standing in yard with signal at STOP – QP standing adjacent to leading crew compartment – Guard on train in guard's compartment	– Site induction and track safety awareness – Training (driver, guard, signalling, QP) – Train no. and road train is on	– Driver to QP verbally when driver preparation is complete or when driver has changed ends – 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 – QP standing adjacent to leading crew compartment – Guard on train in guard's compartment
2	QP checking procedure – QP checks the first 4 cars on LH side of train – If not clear, remove/clear obstruction then check the first 4 cars on LH side again – If clear, QP gives one long, loud whistle blast then checks the first 4 cars on RH side of train – If not clear, remove/clear obstruction then check the first 4 cars on RH side again – If clear, QP gives one long, loud whistle blast – QP advises driver that both sides have been checked and all is clear	– Train standing in yard with signal at STOP – QP standing adjacent to leading crew compartment – Guard on train in guard's compartment	– Site induction and track safety awareness – Training (driver, guard, signalling, QP)	– QP whistle on each side when all clear – 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. – 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 – QP standing adjacent to leading crew compartment – Guard on train in guard's compartment – 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 – Guard opens doors on both sides of train – 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”. – Check the last 4 cars on the RH side of train – If not clear, remove/clear obstruction then check the last 4 cars on same side again – If clear, guard gives one long, loud whistle blast – Check the last 4 cars on the LH side of train – If not clear, remove/clear obstruction then check the last 4 cars on same side again – If clear, guard gives one long, loud whistle blast – Close doors on both sides – 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 – Training (driver, guard, signalling, QP) – Knowledge about the type of train being checked	– Guard internal and external PA after opening doors – Guard whistle on each side when all clear – 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) – Guard has to be able to see to the end of the train on both sides. – The road is clear if there is nothing to obstruct the train (on tracks or either side, in train envelope) – When clear on each side, doors to close for that side (check Door Open light and visual check) – 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 – Driver advises QP that the guard has completed the departure process – QP contacts signal box to advise the signaller that the train is ready to depart – 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. – After receiving confirmation from QP that the train is ready to depart, clear the relevant signals. – Driver confirms PROCEED indication and performs modified inching movement.	– Train standing in yard with signal at STOP with doors closed – QP standing adjacent to leading crew compartment – Guard on train in guard's compartment	– Site induction and track safety awareness – Training (driver, guard, signalling, QP)	– Driver to QP verbally when guard's bell heard – 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 – 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 – 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 Training 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 Training 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 Training Employee vigilance		Another separate procedure will be undertaken Training 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 Training 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 Training 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 Training 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 Training 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 Training 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 Training 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 Horn for emergency 8 km/h speed limit Training Employee vigilance 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 Training Employee vigilance		None	
QP checking procedure	ABNORMAL CONDITIONS		Severe weather, darkness, utility (lights) failure, QP slips over	QP slips, trips or falls Procedure ensures that the train will not move and eventually someone would notice his absence Operational delay	PPE Torch Training Driver and signaller vigilance Procedure Training 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 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 Training Employee vigilance 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 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 Horn for emergency 8 km/h speed limit Training Employee vigilance 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 Horn for emergency 8 km/h speed limit Training Employee vigilance 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 Training Employee vigilance		None	
Guard checking procedure	WRONG INFORMATIO N		Guard and driver have been placed on wrong train	QP applies procedure to check wrong train 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 Training 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 Procedure is not explicit about what to do	Inching movement Horn for emergency 8 kph speed limit Training Employee vigilance 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

_____

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.