

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

AVANT-PROPOS

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

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

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

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

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

Le texte de cette norme est issu des documents suivants:

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

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

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

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

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

INTRODUCTION

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

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

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

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

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

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

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

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

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

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

1 Domaine d'application

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

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

2 Références normatives

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

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

3 Termes, définitions et abréviations

3.1 Termes et définitions

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

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

3.1.1

caractéristique

propriété qualitative ou quantitative

EXEMPLE Pression, température, tension.

3.1.2

conséquence

effet d'un événement affectant les objectifs

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

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

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

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

[SOURCE: ISO Guide 73:2009, 3.6.1.3]

3.1.3**moyen de maîtrise**

mesure qui modifie un *risque* (3.1.12)

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

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

[SOURCE: ISO Guide 73:2009, 3.8.1.1]

3.1.4**intention de conception**

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

3.1.5**propriété**

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

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

3.1.6**mot-guide**

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

3.1.7**dommage**

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

3.1.8**phénomène dangereux**

source de *dommage* (3.1.7) potentiel

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

[SOURCE: ISO Guide 73:2009, 3.5.1.4]

3.1.9**niveau de risque**

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

[SOURCE: ISO Guide 73:2009, 3.6.1.8]

3.1.10**directeur**

personne responsable d'un projet, d'une activité ou d'une organisation

3.1.11**partie**

section du système faisant l'objet de l'étude actuelle

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

3.1.12

risque

effet de l'incertitude sur l'atteinte des objectifs

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

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

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

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

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

[SOURCE: ISO Guide 73:2009, 1.1]

3.1.13

identification des risques

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

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

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

[SOURCE: ISO Guide 73:2009, 3.5.1]

3.1.14

source de risque

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

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

[SOURCE: ISO Guide 73:2009, 3.5.1.2]

3.1.15

traitement du risque

processus destiné à modifier un *risque* (3.1.12)

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

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

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

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

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

3.2 Abréviations

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

4 Principales caractéristiques de HAZOP

4.1 Généralités

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

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

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

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

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

4.2 Principes de l'examen

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.3 Plan de conception

4.3.1 Généralités

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

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

La représentation du système se décompose en deux composants essentiels:

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

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

4.3.2 Exigences de conception et intention de conception

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

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