Contribution à l'analyse des risques : Proposition d'une méthode par scénarios et capitalisation de la connaissance

Laurent Froquet

INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE

N° attribué par la bibliothèque

T H E S E

pour obtenir le grade de

DOCTEUR DE L'INPG

Spécialité : Automatique-Productique

préparée au Laboratoire d'Automatique de Grenoble
dans le cadre de
l'Ecole Doctorale Electronique, Electrotechnique, Automatique, Télécommunications, Signal

présentée et soutenue publiquement

par

Laurent FROQUET

le 4 avril 2005

Contribution à l'analyse des risques : Proposition d'une méthode par scénarios et capitalisation de la connaissance

_____

***Directeur de thèse** : M. Jean-Marie FLAUS*

_____

JURY

Mme. Sylviane GENTIL,	Présidente
M. Jean-Louis ERMINE,	Rapporteur
M. André LAURENT,	Rapporteur
M. Jean-Marie FLAUS,	Directeur de thèse
M. Eric NIEL,	Co Encadrant
M. Jean-Baptiste LEGER,	Examinateur

A mes parents
A mon frère

Remerciements

Les travaux de recherche présentés dans ce mémoire ont été développés au Laboratoire Automatique de Grenoble

Je tiens à remercier vivement tout ceux qui ont contribué à l'aboutissement de ce travail :

- Madame Sylviane Gentil qui m'a fait l'honneur d'accepter de présider le jury,
- Monsieur Eric Niel pour son soutien et ses conseils,
- Messieurs André Laurent et Jean-Louis Ermine, rapporteurs, qui ont accepté d'évaluer ce travail,
- Monsieur Jean-Baptiste Leger, de la société PREDICT, qui a accepté d'être examinateur de ce travail,
- Messieurs Luc Dugard et Alain Barraud qui m'ont accueilli au sein de leur laboratoire,
- La région Rhône-Alpes qui a financé ces travaux.

Je remercie aussi tout particulièrement Monsieur Jean-Marie Flaus par lequel j'ai eu le plaisir d'être encadré. Il m'a toujours fait confiance et soutenu tout au long de ces années.

J'adresse un grand merci à toutes les personnes qui m'ont soutenu et encouragé durant tout mon parcours.

Et j'ai également une pensée très forte pour mes parents et mon frère qui m'ont toujours soutenu et aidé au cours de ces années.

Table des matières

Remerciements.....5

Liste des figures.....11

Chapitre 1
L'analyse des risques.....19

1.1 Introduction.....19

1.2 Les notions de base.....20

1.2.1 Définitions.....21

1.2.2 La notion de criticité.....22

1.2.2.1 L'analyse qualitative.....22

1.2.2.2 L'évaluation quantitative.....23

1.2.3 Un outil d'analyse de propagation de fautes pour représenter les enchaînements d'événements.....23

1.2.4 Notion de modèle orienté dysfonctionnement.....24

1.3 Les modèles pour l'analyse de risques.....24

1.3.1 Introduction.....24

1.3.2 Modèle et système.....24

1.3.3 Notions de flux, modèle MADS.....25

1.3.4 Représentation des interactions.....26

1.3.5 Le modèle MoDyF.....27

1.3.6 Modélisation de la causalité.....28

1.3.7 La modélisation systémique de l'installation....28
1.4 Les méthodes d'analyse de risques....29
1.4.1 Démarche générale d'une analyse des risques....29
1.4.2 La méthode AMDEC....31
1.4.3 La méthode HAZOP....33
1.4.4 La méthode HACCP....34
1.4.5 Les autres méthodes....35
1.5 Limites des méthodes actuelles....36
1.5.1 AMDEC....36
1.5.1.1 Types de résultats....36
1.5.1.2 Limites....36
1.5.2 HAZOP....37
1.5.2.1 Types de résultats....37
1.5.2.2 Limites....37
1.5.3 HACCP....37
1.5.3.1 Type de résultats....37
1.5.3.2 Limites....38
1.6 Discussion....38
1.6.1 Cahier des charges....38
1.6.2 Exemple....38
1.6.2.1 Analyse de risque....39
1.6.2.2 Modélisation du système....40

Chapitre 2
La méthode ScénaRisK....45
2.1 Introduction....45
2.2 La genèse de ScénaRisK....47
2.2.1 Les prémisses de ScénaRisK....47
2.2.2 L'ébauche de ScénaRisK....48
2.2.3 La maturation de ScénaRisK....48
2.3 Eléments de scénarios génériques....48
2.3.1 Les structures de bases génériques....48
2.3.1.1 Les attributs qualitatifs descriptifs....48
2.3.1.2 Etat....49
2.3.1.3 Les événements....50

2.3.1.4 Les conditions.....*51*
2.3.2 Systèmes d'automates 51
2.4 Le modèle de danger.....53
2.4.1 Introduction.....53
2.4.2 Elément de scénario de danger 53
2.4.3 Elément de scénario d'accident.....55
2.4.4 Elément de scénario de post accident.....56
2.4.5 Scénario de danger élémentaire.....58
2.4.6 Les éléments de scénarios d'évolutions des attributs.....58
2.4.7 L'interface modèle de l'installation / modèle de danger.....59
2.4.7.1 La correspondance physique / danger.....*59*
2.4.7.2 La correspondance danger / physique.....*60*
2.5 Construction du modèle de danger à partir du modèle structurel et fonctionnel.....61
2.5.1 Introduction.....61
2.5.2 Description structurelle 61
2.5.3 Description fonctionnelle.....62
2.5.3.1 Les fonctions statiques.....*62*
2.5.3.2 Les fonctions dynamiques.....*63*
2.5.4 Synthèse de la méthode.....64
2.6 Les étapes d'utilisation de ScénaRisK.....65
2.6.1 Introduction.....65
2.6.2 Exemple 66
2.6.3 Etape 1. description structurelle de l'installation.....66
2.6.4 Etape 2. description fonctionnelle de l'installation.....67
2.6.4.1 Fonctions statiques.....*67*
2.6.4.2 Fonctions dynamiques.....*69*
2.6.5 Construction de la base de connaissances.....72
2.6.6 Etape 3. Les scénarios d'interfaces.....75
2.6.7 Etape 4. identification des états à risques.....77
2.6.8 étape 5. recherche des enchaînements de scénarios 78
2.7 Aide à l'utilisation de la méthode.....79
2.8 Lien avec différentes méthodes d'analyse de risque.....80
2.8.1 HAZOP.....80
2.8.2 AMDEC.....80
2.8.3 MOSAR.....81

Chapitre 3
Exemple d'application.....83
3.1 Présentation et caractéristiques du procédé industriel.....84
3.1.1 Introduction.....84
3.1.2 La description des appareils.....84
3.1.3 Le mode opératoire.....86
3.1.4 Les actions de sécurité.....87
3.2 La démarche de ScénaRisK.....88
3.2.1 Etape 0 : construction de la bibliothèque.....88
3.2.2 Etape 1 : description structurelle de l'installation.....90
3.2.3 Etape 2 : description fonctionnelle de l'installation.....94
3.2.4 Étape 3 : description des éléments de scénarios d'interface.....95
3.2.5 Etape 4 : recherche des états de pré dangers (des scénarios).....97
3.2.6 Etape 5 : recherche des enchaînements de scénarios.....98

Conclusion et perspectives.....103

Glossaire.....105

Références Bibliographiques.....111

Annexes.....117

Liste des figures

figure 1.1 Exemple de grille probabilité gravité 22
figure 1.2 MADS 26
figure 1.3 Interaction de flux MADS 26
figure 1.4 Modèle dysfonctionnement d’une entité [Flaus 2003] 27
figure 1.5 Découpage systémique 28
figure 1.6 Démarche d'analyse des risques [PRIHSE 2002] 30
figure 1.7 Méthode de réalisation d'une AMDE [Villemeur 1988] 32
figure 1.8 Principe d'analyse de l'HAZOP 34
figure 1.9 Vue d'ensemble du robot 39
figure 1.10 Représentation du robot 40
figure 1.11 Représentation de l'interrupteur 40
figure 1.12 Représentation de la porte 41
figure 1.13 Représentation du contacteur de la porte 41
figure 1.14 Représentations de l'arrêt d'urgence et de la reprise 41
figure 1.15 Contacteur de la porte avec les états de défaillances 42
figure 1.16 Position de l'opérateur 42
figure 1.17 Etat dangereux de l'installation 43
figure 2.1 Objectif de ScénaRisK 45
figure 2.2 La méthode ScénaRisK 46
figure 2.3 Evénement 50

figure 2.4 Exemple 51
figure 2.5 ST étiqueté 52
figure 2.6 Etat de danger réversible 55
figure 2.7 Etat de danger non réversible 55
figure 2.8 Elément de scénario d'accident 56
figure 2.9 Element de scénario de post accident 57
figure 2.10 Scénario de danger élémentaire 58
figure 2.11 Elément de scénario d'évolution des attributs 59
figure 2.12 Les interfaces spécifiques génériques 59
figure 2.13 Correspondance physique / danger 60
figure 2.14 Correspondance danger / physique 60
figure 2.15 Description structurelle d'une entité 62
figure 2.16 Fonction statique 63
figure 2.17 Fonction dynamique 64
figure 2.18 Détail de la méthode ScénaRisK 65
figure 2.19 Exemple : agroalimentaire 66
figure 2.20 Exemple : le système de stockage 67
figure 2.21 Exemple : liste des fonctions statiques 68
figure 2.22 Exemple : évolution des valeurs des attributs 69
figure 2.23 Exemple : liste des fonctions dynamiques 70
figure 2.24 Exemple : détail de la phase de fonctionnement stockage 70
figure 2.25 Exemple : détail de la phase de fonctionnement nettoyage 71
figure 2.26 Exemple : détail de la phase de fonctionnement rinçage 71
figure 2.27 Exemple : élément de scénario de danger 74
figure 2.28 Exemple : élément de scénario d'accident 75
figure 2.29 Exemple : élément de scénario de post accident 75
figure 2.30 Exemple : correspondance physique / danger 76
figure 2.31 Exemple : correspondance danger / physique 76
figure 2.32 Exemple : scénario de danger 79
figure 3.1 Procédé industriel d’évaporation 85
figure 3.2 Recette de la partie évaporation 87
figure 3.3 Elements de scénarios génériques 88
figure 3.4 Scénarios d'évolution des attributs génériques 89
figure 3.5 Détail de l'entité capteur calculateur actionneur 91
figure 3.6 Détail de l'entité réacteur 92

figure 3.7 Détail de l'entité circuit de re circulation 93
figure 3.8 Détail de l'entité boucle eau froide 94
figure 3.9 Détail de la fonction statique étanche 94
figure 3.10 Détail des fonctions dynamiques 95
figure 3.11 Élément de scénarios d'interface 95
figure 3.12 Exemple graphique de ScénaRisK 99
figure 3.13 OU logique 99
figure 3.14 Scénario de danger 101

Introduction

Les industries actuelles doivent mettre en place des méthodes d'analyse des risques garantissant que leurs installations suivent les normes en vigueur. Un large choix de méthodes est à leur disposition. Mais, actuellement, très peu de méthodes permettent à partir d'une représentation de l'installation de réaliser une analyse des risques permettant la validation des barrières matérielles ou méthodologiques.

Les enquêtes qui se déclenchent après un accident et les explications qu'elles fournissent ne remettent presque jamais en cause la capacité des méthodes et des expertises qui ont été mises en oeuvre dans l'analyse et l'évaluation des risques. Nous évoquons la défaillance technique tout en étant prêt à accepter qu'elle soit inhérente à la technologie. Par contre, on retient souvent l'erreur humaine et on va rechercher la faute. Il est vrai que les enquêtes poussées montrent que les causes profondes se sont surtout révélées aux niveaux de l'organisation et du management, c'est-à-dire au niveau décisionnel. Cependant force est de constater que tout se passe comme si dans la recherche sur le processus de production de l'accident, on exclut une phase importante, celle justement de l'analyse et de l'évaluation des risques présente normalement à toutes les phases du système, depuis sa conception jusqu'à son démantèlement ou sa mise au rebut. Et pourtant ce sont les informations fournies par l'analyse et l'évaluation au travers de ces méthodes qui ont servi de base à la décision.

C'est justement l'absence d'évaluation des risques qui constitue souvent l'objet de la faute en question, pourraient rétorquer certains. Ce serait faire une trop grande confiance à l'opération d'analyse et d'évaluation des risques et surtout aux méthodes qu'elle met en oeuvre. Incontestablement, les concepteurs et ensuite les exploitants sont pour l'essentiel des ingénieurs.

Leurs compétences techniques et leurs méthodes rigoureuses souvent performantes partout ailleurs, ne tolèrent guère la critique. Au contraire, elles ont induit une culture excessive des certitudes dans les esprits.

La notion d'analyse et d'évaluation des risques est très ancienne ; elle est liée à l'existence du danger. Comparativement, les méthodes d'analyse et d'évaluation des risques sont beaucoup plus récentes. Les présentations de ces méthodes sont en nombre abondant dans les ouvrages de la sûreté de fonctionnement. Lorsque nous effectuons des analyses, c'est bien dans le but d'obtenir des résultats qui sont utiles pour une prise de décision. Les méthodes sont nées à partir des préoccupations autour de la fiabilité et de la disponibilité, c'est-à-dire la réussite de la mission des systèmes entièrement techniques. Plus tard, la sécurité fût intégrée aux deux premiers concepts "fiabilité et disponibilité" pour constituer la sûreté de fonctionnement. Cependant, elle a souvent été traitée plus ou moins en parallèle aux deux premiers concepts.

- On n'a considéré que la sécurité des personnes, des biens et de l'environnement comme le produit qui découle automatiquement et d'une façon complète de l'activité de sûreté de fonctionnement sous-estimant ainsi les compromis parfois importants qui ont lieu lorsque les deux objectifs (disponibilité, sécurité) s'affrontent c'est-à-dire dans le cas où les mesures de sécurité ne sont pas nécessaires à la réussite de la mission essentielle du système en question.
- On a qualifié d'objective voire de fiable toute évaluation des risques mettant en oeuvre des techniques mathématiques plus ou moins sophistiquées. Or, cette tendance excessive à vouloir chiffrer tout, exclut nécessairement des parties entières du champ d'analyse. On a parfois l'impression que c'est le problème qui est réduit à la taille de la capacité de l'outil. [Phoebus 2000]

L'objectif des travaux présentés dans ce mémoire est le développement d'une méthode d'analyse des risques pouvant être mise en oeuvre de façon informatique permettant la génération de scénarios danger de façon automatique. La première difficulté est de permettre une représentation des connaissances des experts dans différents domaines industriels. Pour cela, nous avons réalisé une base de connaissances référencées par des mots clefs spécifiques au domaine étudié. La deuxième difficulté a été de construire une méthode de description d'une installation, permettant la recherche des clefs pour l'utilisation de la base des connaissances. Cette méthode permet de réaliser une analyse des risques "de base", et cette modélisation est une aide pour la réalisation de méthodes d'analyses de risques les plus utilisées dans l'industrie.

Ce mémoire présente la description de la méthode que nous avons appelée ScénaRisK composée d'une base des connaissances et d'une représentation de l'installation spécifique permettant la réalisation d'une analyse des risques.

Nous avons donc choisi de présenter dans le premier chapitre l'état de l'art de l'analyse des risques, dans ce but nous présenterons les outils minimum ainsi qu'une description des principales méthodes, et une synthèse comprenant les avantages et les inconvénients de chacune de ces méthodes.

Une synthèse critique des différentes méthodes nous permet de décrire les points importants, que doit posséder notre base de connaissances, ainsi que les modifications à apporter pour la réalisation d'une analyse des risques automatisée.

Dans le deuxième chapitre, nous présenterons la structure de la base de connaissances, qui permet de représenter tous les accidents imaginables. Cette structure permet ensuite d'envisager la réalisation d'une méthode d'analyse des risques à partir d'une représentation de l'installation physique basée sur des attributs caractéristiques décrits dans la base de connaissances. Ensuite, nous décrirons la base de connaissances, et la description de l'installation spécifique à partir d'un exemple académique issu du domaine agro-alimentaire.

A partir de la description du chapitre précédent, nous décrirons dans le troisième chapitre un exemple industriel, issu d'une installation chimique réelle.

En conclusion, nous donnerons les avantages et les inconvénients d'une méthode basée sur une liste d'attributs, et nous détaillerons les perspectives possibles d'une base de connaissances, dans le domaine de la qualité ou de la traçabilité.

Chapitre 1

L'analyse des risques

1.1 Introduction

Tant qu'une société ne satisfait pas les besoins matériels de ses membres (occident il y a un siècle, les pays en voie de développement aujourd'hui), il y a globalement une foi dans le "progrès" et la technique. Les accidents sont perçus comme découlant de l'erreur humaine individuelle. Aujourd'hui en occident, les accidents sont perçus comme résultant d'un système. C'est l'entreprise, la branche industrielle (la chimie, l'agroalimantaire), voire l'industrie dans son ensemble qui est perçue comme responsable [Codegepra 2003].

La société réclame, face aux nouvelles technologies, plus de transparence et d'information. La démarche d'identification, d'analyse et de maîtrise des risques initiée dans le nucléaire et l'aéronautique s'étend aux autres domaines. Pour permettre l'utilisation de ces méthodes, il faut avoir à tout moment les composants et l'historique, ceci peut être regroupé sous le nom de traçabilité concernant le produit, que ce soit pour un produit agroalimentaire, par la liste des composants (cas actuellement de l'ajout de l'utilisation des Organismes Génétiquements Modifiés), de leurs origines (produits issus de l'agriculture biologique), et de leur provenance, regroupés sous le nom de traçabilité.

La prise en compte du risque dans les entreprises doit s'adapter à cette évolution. Elle embrasse un champ de plus en plus large. Partant de préoccupations techniques, elle s'est ouverte à l'erreur humaine, aux problèmes d'organisation. Aujourd'hui, il est question d'analyse systémique, de responsabilité collective et d'approche sociétale. Cette approche doit s'appliquer dès la conception du procédé, et être poursuivie tout au long de son cycle de vie, en particulier à travers le « système de management de la sécurité » jusqu'au démantèlement.

Le but des industries du début du siècle étant essentiellement de produire des biens, les accidents étaient inévitables, pour que le progrès avance, et que la qualité de vie des personnes évolue. Les révolutions industrielles ont apporté un changement dans la façon de travailler et dans l'organisation, pour toujours plus de rendement au détriment des personnes qui y travaillent. Les personnels travaillaient alors dans des conditions difficiles ou les accidents avec amputations et décès étaient fréquents, que ce soit dans l'entreprise elle même ou sur les populations vivant autour du site (fumée toxique, explosion ...).

L'explosion d'un entrepôt d'engrais en 1921 usine de BASF à Oppau (Allemagne), explosion de 5400 tonnes de nitrate d'ammonium (600 morts) n'a pas donné lieu à une loi réglementant tous les dépôts, car la société avait besoin de ces industries pour continuer son évolution. L'accident AZF de Toulouse en 2001, lui, n'a pas eu le même impact, d'une part, grâce aux médias et d'autre part, car la société recherche maintenant la production de tous les produits sous un facteur sécurité et l'utopie du risque zéro. L'évolution de la société, par le législateur (B.I.T. Bureau International du Travail) a donc fait évoluer les industries pour les obliger dans quel domaine que ce soit à respecter les règles de sécurité et à produire des documents prouvant qu'elles respectent les normes en vigueur.

La recherche a longtemps porté essentiellement sur des préoccupations techniques : modéliser physiquement l'accident (de l’échelle macroscopique à l’échelle microscopique) pour en connaître les mécanismes (et ainsi les prévenir) et prévoir des distances de sécurité. Elle s’est ensuite déplacée vers les méthodes d'analyse des risques. Dans ce chapitre, nous allons dans un premier temps détailler les outils qui sont utilisés dans le domaine de l'analyse, ensuite, nous allons décrire les différentes méthodes d'analyse des risques, en donnant leurs objectifs, et leurs domaines d'application.

1.2 Les notions de base

Dans ce paragraphe, nous allons présenter les notions indispensables pour la réalisation d'une analyse des risques. Nous allons développer la notion de danger, de risque, de criticité et de probabilité ainsi que la notion de source de danger, de même nous présenterons un outil d'analyse: l'arbre de défaillances.

1.2.1 Définitions

Nous allons débuter par quelques définitions [Flaus 2002-2] utiles pour la suite des explications .

Définition

***Danger** : qui menace la sûreté [Petit Robert 2000]. Le danger est un concept qualitatif et descriptif. On effectue l'inventaire des événements non souhaités et leurs conséquences. On dimensionne, on ne quantifie pas.*

*Le **risque** est un concept quantitatif à deux dimensions*
1. Probabilité d'occurrence (à priori) ou fréquence (à postériori) de l'événement non souhaité.
2. La gravité de cet événement non souhaité.

*Une s**ource de danger** est un élément ou système pouvant générer un événement non souhaité sur un système cible.*

*Un **scénario de danger** est la représentation des enchaînements conduisant à un accident sous une forme structurée et réutilisable.*

*La **prévention** est la diminution de l'occurrence (ou de la fréquence) d'un Evénement Non Souhaité (ENS). En d'autres termes l'action de prévention consiste à tout faire pour que l'événement ne se produise pas. On agit sur un élément constitutif de l'ENS. La prévention est aussi appelée sécurité primaire par certaines Techniques du Danger telles que la Sécurité des installations et la Sûreté de fonctionnement.*

*La **protection** intervient si à la suite d'un échec toujours possible de la prévention, l'Evénement Non Souhaité a eu lieu, on peut alors minimiser sa gravité. La protection est aussi appelée sécurité secondaire par certaines Techniques du Danger telles que la Sécurité des installations et la Sûreté de fonctionnement.*

1.2.2 La notion de criticité

Une fois les scénarios de danger déterminés, il faut être capable de les classer, pour déterminer les scénarios les plus probables et les plus dangereux. Cette classification sous forme de grille permet aussi de vérifier les différentes barrières de protection prévention introduites à la fin de la présentation de la méthode proposée. Ces grilles, permettant de donner une criticité se retrouvent dans plusieurs méthodes d'analyse des risques. La figure 1.1 présente une grille de probabilités (P1, P2, P3, P4) gravités (G1, G2, G3, G4) à 4 niveaux. Il est recommandé d'utiliser des grilles comportant des niveaux pairs, pour ne pas avoir un niveau indécis. Sur cette grille nous avons tracé une limitation en acceptabilité, donnant les scénarios acceptables, et les scénarios inacceptables sur lesquels, nous devons ajouter des préventions, et des protections pour faire évoluer le système et permettre que les scénarios inacceptables deviennent acceptables. La construction des grilles de probabilité gravité sont réalisées à partir d'un retour d'expérience et de différents abaques dont disposent les experts de chaque domaine concerné.

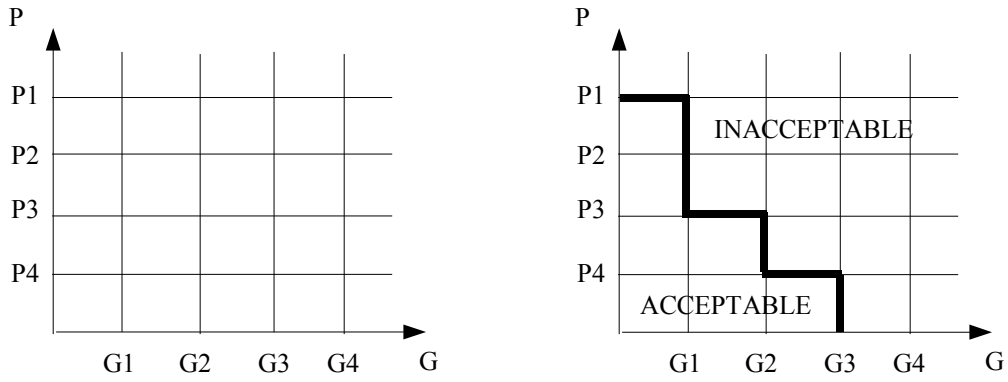


figure 1.1 Exemple de grille probabilité gravité

1.2.2.1 L'analyse qualitative

Une modélisation de l'installation que ce soit sous la forme d'un modèle systémique ou une analyse fonctionnelle, constitue un préalable à toutes les analyses. En effet, elle permet la structuration de la compréhension du système et de ses sous-systèmes et éléments.

Toutes les méthodes ont une capacité d'analyse qualitative importante. Mais cela restera conditionné par la connaissance que l'on a des composants du système. Pour des composants ou une banque de données existe, la recherche de ces modes peut être relativement exhaustive. Le risque est alors de ne considérer que les systèmes sur lesquels nous avons de l'information.

L'analyse des défaillances permet de déterminer des scénarios critiques. Nous pouvons en extraire une liste des scénarios ou combinaisons d'événements de base dont la conjonction des occurrences conduit inévitablement à l'événement non souhaité. La notion de scénario est surtout

dans la prévision. Le retour d'expérience fournit certes, une bonne partie de l'information mais pas toutes les informations.

1.2.2.2 L'évaluation quantitative

La mesure du risque est ramenée généralement à la considération de deux paramètres (gravité et probabilité d'occurrence). Certaines méthodes intègrent, chacune selon le processus de son déroulement, les deux paramètres. L'aspect purement quantitatif ne concerne que les probabilités.

Au départ, le chiffrage élémentaire du risque a été effectué selon un produit de ces deux quantités. Plus tard, les experts de la sécurité de fonctionnement réaliseront que l'association de la probabilité et de la gravité dans la forme d'un produit réduit l'information sur les risques et donc réduit les possibilités d'action et de gestion.

Une approche plus réaliste a conduit à placer les paramètres dans un plan défini par deux axes orthogonaux représentant la gravité et la probabilité. Ces axes sont dotés d'une échelle. Le risque lié à un événement est alors représenté par son image ponctuelle sur ce repère. Il faut alors se demander comment sont graduées les échelles. C'est là encore où la notion de négociation et de compromis prend place.

L'échelle de gravité est liée à l'importance des conséquences que peut avoir l'événement sur tout ou partie du système y compris, bien sûr, sa composante humaine et son environnement. Cette échelle est définie au cas par cas selon la nature du système et les activités concernées. Elle est souvent influencée par l'obligation réglementaire à satisfaire à la législation du travail ou celle de l'environnement.

1.2.3 Un outil d'analyse de propagation de fautes pour représenter les enchaînements d'événements

Un arbre des défaillances permet d'obtenir après la réalisation d'une ou plusieurs analyses de risques les enchaînements logiques conduisant à un événement sommet.

Définition

> *Un arbre des défaillances (ou arbre des causes) est un modèle graphique qui permet de mettre en évidence les combinaisons de défaillances qui peuvent causer l'évenement principal auquel l'étude s'intéresse, appelé évenement sommet. Ces évenements sommets sont des évenements qui peuvent avoir été identifiés par une autre méthode d'analyse des risques.*

1.2.4 Notion de modèle orienté dysfonctionnement

Définition

Le modèle d'un système physique est une description plus ou moins détaillée de sa structure physique avec en plus les modèles (comportementaux ou fonctionnels) de chacun de ses constituants [De Kleer et al, 1987].

Un modèle est une description mentale (intériorisée) ou figurée (diagrammes, formules mathématiques, ...) qui, pour un champ de questions, est pris comme représentation abstraite d'une classe de phénomènes, plus ou moins habilement dégagés de leur contexte par un observateur pour servir de support à l'investigation et/ou la communication [AFCET, 1988].

La qualité d'un modèle réside moins dans son aptitude à décrire des phénomènes que dans sa conformité avec les objectifs pour lesquels il a été conçu [Penalva, 1990].

Un modèle pour réaliser une analyse des risques doit être orienté dysfonctionnement, ces aspects étant difficiles à décrire de façon mathématique. L'utilisation dans les méthodes sont des modèles qualitatifs, ou des relations de causalité. De plus, s'il faut identifier les dysfonctionnements, il est utile de connaître les fonctions des différents systèmes. Sachant que la description organique (structurelle) d'un système ne permet pas forcément d'en déduire ses fonctions.

1.3 Les modèles pour l'analyse de risques

1.3.1 Introduction

Dans ce paragraphe, nous allons décrire les différents outils qui servent pour réaliser une analyse des risques. Pour cela, nous allons d'abord introduire la notion de modèle, puis le lien entre les modèles et les systèmes, ensuite nous décrirons les flux, et les interactions.

1.3.2 Modèle et système

Pour analyser un système réel il faut toujours réaliser une analyse à l'intérieur d'une problématique. Un système ne doit pas être considéré comme rencontré, mais il doit être construit, pour cela, nous devons réaliser une modélisation.

Définition

Un système est une totalité organisée d'éléments solidaires ne pouvant être définis que les uns par rapport aux autres, ensemble d'éléments en inter connecté et en interaction. Le tout est supérieur à la somme des parties.

L'approche systémique, est une approche basée sur un découpage en systèmes, suivant le système, le découpage systémique peut être complexe, nous n'utiliserons alors pas une modélisation mathématique et donc quantitative, mais une approche qualitative.

La complexité [Le Moigne, 1990] se dit de l'ensemble d'un tout dont les éléments sont combinés d'une façon qui n'est pas immédiatement claire à l'analyse. Il existe deux types de complexité :

- phénomènes mal connus entre plusieurs sous-systèmes (par exemple la science du vivant),
- phénomènes simples, mais en très grands nombres.

1.3.3 Notions de flux, modèle MADS

Le modèle MADS [Godard 1994] est une première approche pour modéliser la notion de danger. Ce modèle a été conçu dans le contexte du *paradigme systémique*.

Pour décrire un processus, on est amené à décrire :

- d'une part la dualité des objets processés (subissant le changement)/ objets processeurs (produisant le changement)
- et d'autre part, la liste des changements que subissent les objets processés.

Les relations des objets entre eux dans le cadre d'un processus, que ces objets soient acteurs ou sujets, et les relations avec l'environnement sont représentées :

- d'une part par des transactions sous forme de *Matière*, *Energie* ou d'*Information*, qui sont appelées *Flux*.
- et d'autre part par une capacité d'influence de l'environnement sur le système, appelée C*hamp*.

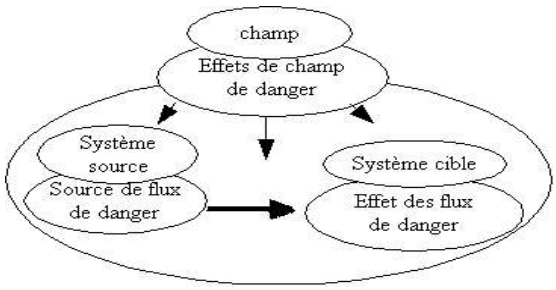


figure 1.2 MADS

Dans ce contexte, le modèle MADS permettant de conceptualiser la notion de danger est exprimé sous la forme d'un *processus de danger* générique (figure 1.2).

Le flux de danger décrit les transactions non désirées entre le système et son environnement. Le système à l'origine du flux de danger est appelé système source de danger tandis que la partie du système subissant les effets du flux de danger sera appelée système cible. Le champ de danger est l'environnement actif susceptible d'influer les systèmes sources et cibles du flux de danger.

Ce modèle conceptuel permet de formaliser une étude de danger et d'effectuer celle-ci à partir de l'inventaire des différents processus de danger existants pour le système considéré dans son environnement.

1.3.4 Représentation des interactions

La figure 1.3 est une représentation des entrées, et des sorties sous forme de flux du modèle MADS. Ces interactions permettent la propagation des différents flux de dysfonctionnements, ou de dangers, dans la modélisation d'un système. Chaque flux d'entrée peut être soit de l'énergie, de la matière ou de l'information. Les flux de sortie générés par le système vont se retrouver dans les flux d'entrée des autres systèmes (système générateur). Les flux permettant la propagation des danger sont appelés des flux de danger. Nous retrouvons alors des flux de danger typés énergie, matière et information.

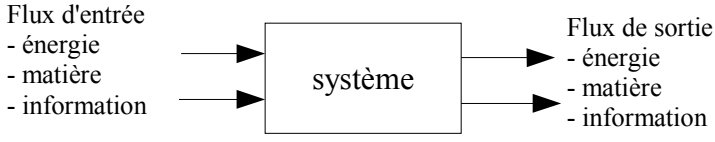


figure 1.3 Interaction de flux MADS

1.3.5 Le modèle MoDyF

Le modèle MoDyF (Modèle de Dysfonctionnement Formel) [Flaus 2003] permet de décrire un réseau d'entités en relation de dysfonctionnement :

L'état physique de chaque entité est représenté par un ensemble de variables caractérisant, à un instant donné, dans quelle situation se trouve l'entité. A chaque ensemble de valeurs de l'état physique, on associe un état dit de fonctionnement. Celui ci peut prendre trois valeurs correspondant aux états normaux, anormaux non dangereux et anormaux dangereux. On peut donc représenter l'évolution des états de fonctionnement par un automate à états finis.

Les dysfonctionnements sont propagés par des relations causales entre les entités. MoDyf s'appuie sur une représentation discrète, c'est à dire que seules les relations de dysfonctionnements de type événementiel sont considérées.

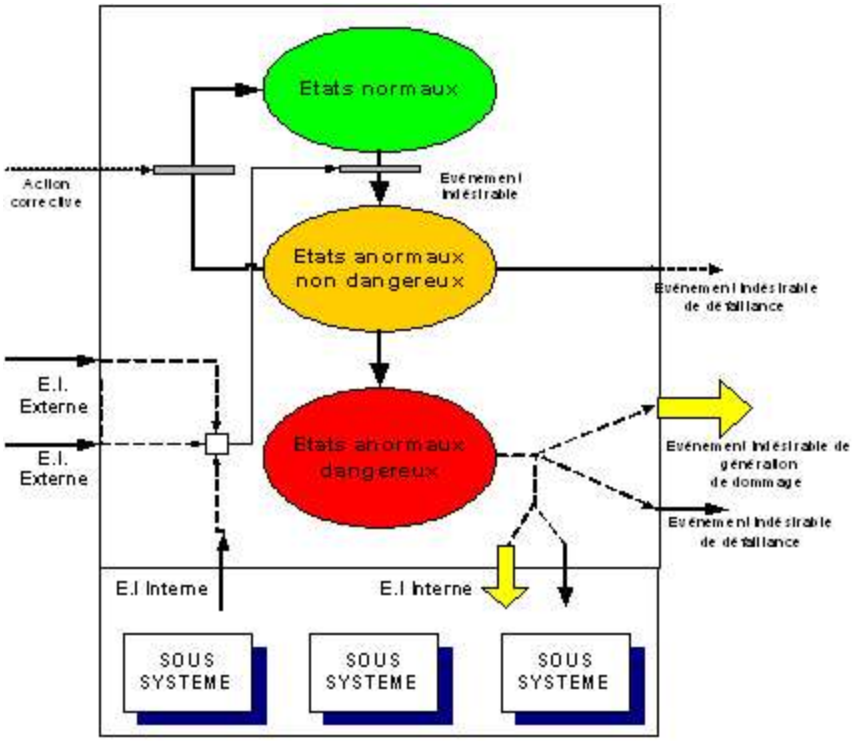


figure 1.4 Modèle dysfonctionnement d'une entité [Flaus 2003]

Ce modèle complète MADS en faisant apparaître l'état interne de chaque entité, qui peut être normal ou non, et permet donc la représentation d'une propagation séquentielle des dysfonctionnements d'entité en entité et de faire intervenir des combinaisons logiques d'événements indésirables.

L'ensemble des entités/relations forme un graphe appelé *graphe causal de dysfonctionnement*. L'objectif de l'analyse des risques est de construire ce graphe causal de dysfonctionnement.

1.3.6 Modélisation de la causalité

Dans un contexte général, la causalité représente la relation entre les causes premières d'une dégradation et la dégradation, elle même. La causalité peut être assimilée à une chaîne causale ayant pour origine une cause première et aboutissant à la dégradation finale par propagation de dégradations. Ces causes peuvent être liées à la conception, la fabrication ou l'exploitation du système. Dans le cadre de l'analyse des risques, la représentation de la causalité a donc pour objectif d'identifier l'ensemble des causes afin de les faire évoluer, il s'agit alors d'un scénario.

1.3.7 La modélisation systémique de l'installation

Devant la complexité de l'analyse des risques il est nécessaire de décomposer l'installation en systèmes et sous-systèmes [Le Moigne 1990]. Il faut faire appel ici à une décomposition à différents niveaux suivant l'importance de l'installation. Dans le cas d'un système complexe, par exemple dans une installation industrielle (figure 1.5) comportant plusieurs ateliers de productions il sera nécessaire de décomposer en suivant les différents ateliers. Il faut ensuite décomposer chaque atelier qui devient à son tour le système à décomposer. Pour réaliser une analyse des risques il faut connaître à quel moment, nous devons arrêter la description systémique.

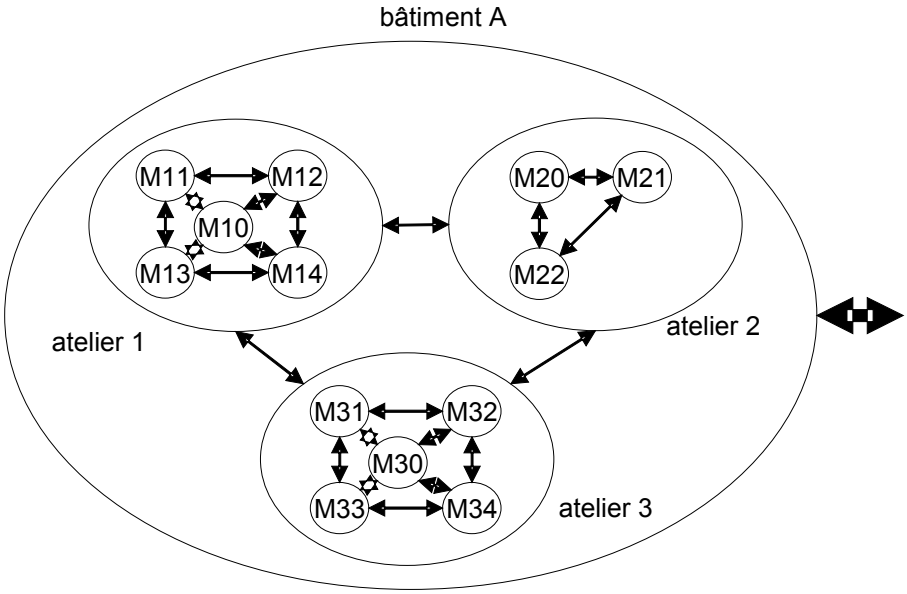


figure 1.5 Découpage systémique

1.4 Les méthodes d'analyse de risques

Dans ce paragraphe, nous allons décrire les principales méthodes d'analyse des risques s'appuyant sur les modèles que nous avons décrits précédemment (d'autres méthodes sont décrites à l'annexe A). Dans un premier temps, nous allons décrire la démarche générale d'une analyse des risques, puis nous décrirons pour chacune des méthodes, les objectifs, le domaine d'application et les contraintes de sa mise en place.

1.4.1 Démarche générale d'une analyse des risques

La démarche de maîtrise des risques suit quatre grandes étapes :

- *Première étape* : caractériser ce que l'on fait ou ce que l'on veut faire, et comment on va le faire, avec quels moyens et à quels niveaux de performance; identifier notre périmètre de décision, c'est-à-dire la frontière en deçà de laquelle nous avons les moyens d'agir car la décision nous appartient et au-delà de laquelle nous devons subir car la décision ne nous appartient plus. Autrement dit, il s'agit de définir le système sur lequel vont porter nos choix de décisions, ses limites, son environnement, ses milieux extérieurs et ses interfaces.

Pour aider à atteindre cette première étape ont été développées des méthodes dites d'analyse fonctionnelle avec différentes variantes de mises en oeuvre mais qui ont toutes le même objectif : associer fonctions et performances requises à solutions et caractéristiques utilisables

- *Deuxième étape* : identifier de la façon la plus exhaustive possible, et sans a priori les installations dont l'entreprise ou l'organisation a la responsabilité, ou, même plus généralement, pour lesquels la responsabilité de l'entreprise ou de l'organisation pourrait être recherchée. Parallèlement, se fixer ses critères, ses limites d'acceptabilité. Là encore des méthodes ont été développées pour supporter et aider la démarche : telle que Méthode Organisée et Systématique d'Analyse des Risques MOSAR ou l'Analyse Préliminaire des risques (APR).

- *Troisième étape* : décider des événements redoutés dont le risque, comparé aux critères d'acceptabilité, sera acceptable : c'est-à-dire ni trop faible, et peut être trop coûteux en précautions, ni trop important, et nécessitant des dispositions pour le réduire. Dans le cas contraire, la démarche, et les méthodes qui la sous tendent, permettront de suggérer des améliorations, d'en évaluer l'efficacité et d'apporter la justification du bien fondé des dispositions techniques et /ou organisationnelles retenues. C'est en particulier à ce niveau de la démarche que l'on pourra faire appel à des méthodes de la Sûreté de Fonctionnement.

- *Quatrième étape* : tracer l'ensemble de la démarche, justifiant ainsi les hypothèses, les raisonnements, les conclusions tirées et les décisions prises, puis mettre en place les conditions

de la mise en oeuvre de ces conclusions et décisions, ainsi que du bien fondé des hypothèses faites et des raisonnements menés. Et le cas échéant, face au constat du non respect d'une hypothèse, d'une erreur de raisonnement, ou plus couramment de l'occurrence de nouvelles conditions remettant en cause certaines hypothèses, vérifier le bien fondé du maintien des conclusions et les décisions correspondantes ; faisant ainsi de l'analyse de risques un véritable outil de pilotage, de direction en temps réel de l'entreprise.

L'ensemble des méthodes d'analyses des risques que l'on retrouve dans la littérature est basé sur la méthode d'analyse générale des risques de la figure 1.6.

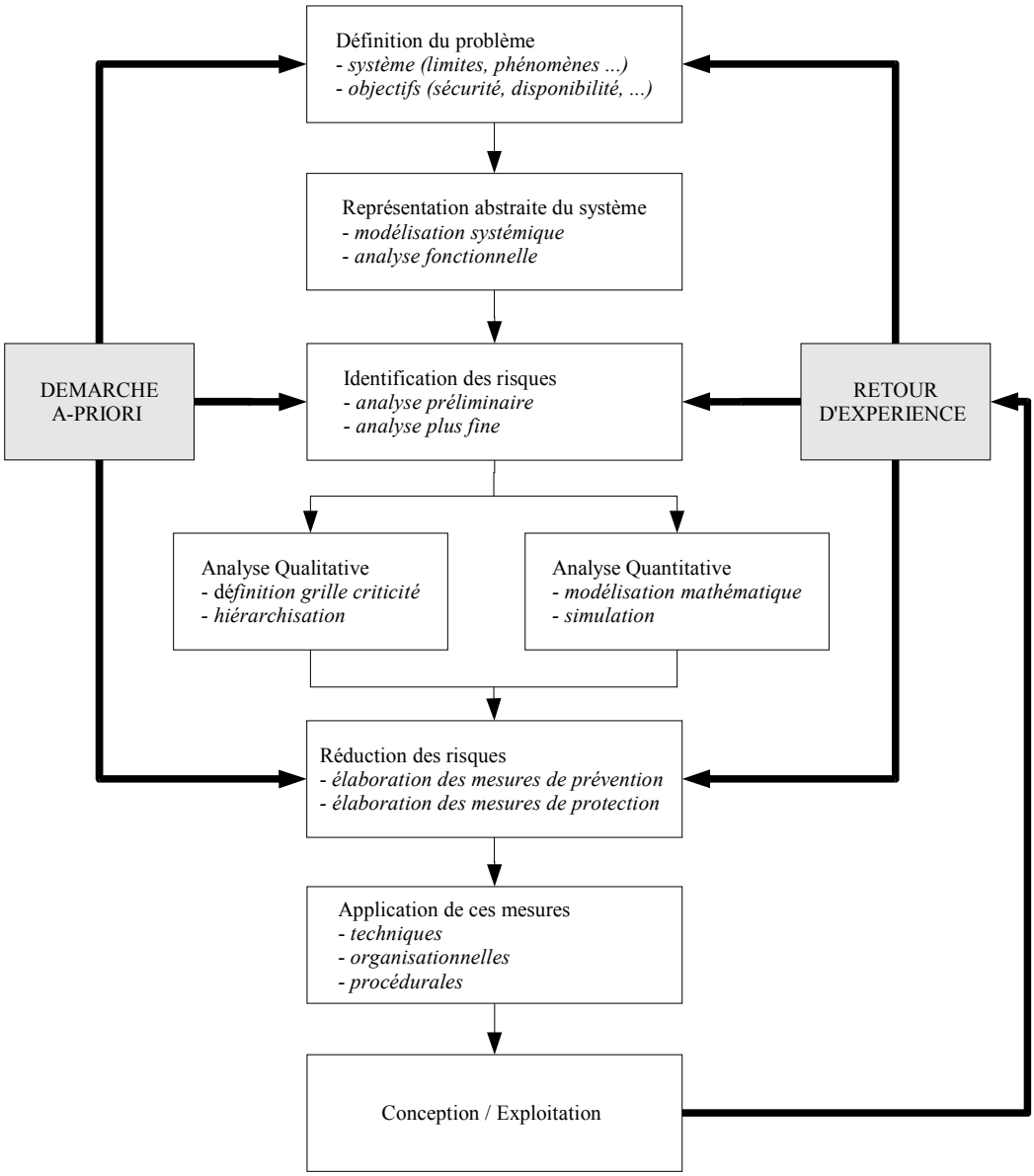


figure 1.6 Démarche d'analyse des risques [PRIHSE 2002]

Les travaux que nous développons dans ce mémoire concernent la représentation abstraite du système, l'identification des risques, et une analyse qualitative, ou si possible, une analyse quantitative.

Les méthodes ont toutes le même but : apporter au décideur les éléments lui permettant de prendre une bonne décision sinon la meilleure à partir de l'ensemble des résultats de l'analyse. La richesse et la fiabilité de ces résultats dépendent en grande partie de la capacité de la méthode. La capacité de la méthode est aujourd'hui envisagée sous deux aspects, l'analyse qualitative et, lorsque cela est possible, une analyse et une évaluation quantitative.

1.4.2 La méthode AMDEC

L'identification de l'ensemble des relations entre les causes, les dégradations et les effets, de nombreuses méthodes synthétisées en [Lievens 1976] [Villemeur 1988] [Limnios 1991] [Zwingelstein 1995] est basée sur les connaissances expertes. Nous retiendrons essentiellement l'Analyse des Modes de Défaillances et de leurs Criticités (AMDEC) et l'HAZard and OPerability study (HAZOP) qui constituent réellement des méthodes synthétiques accompagnées de règles d'analyse se basant sur une description du système

L'Analyse des Modes de Défaillances et de leurs Effets et Criticités (AMDEC) [IEC 1985] est une méthode d'analyse inductive et qualitative étudiant les défaillances d'un système en s'aidant d'une liste quasi-exhaustive de modes de défaillances génériques. Pour permettre une meilleure identification de modes de défaillances, la méthode AMDEC est précédée d'une analyse structurelle ou fonctionnelle du système [Mohafid 1994]. A chaque composant, sous système et système, l'analyste associe des modes de défaillances considérés vraisemblables et poursuit l'analyse par l'identification des causes et des conséquences de ce mode de défaillance sur le fonctionnement à ce niveau de décomposition et sur les niveaux supérieurs du système (figure 1.7). Lorsque les modes de défaillance ne sont pas connus a priori, ils peuvent être issus de la liste des modes génériques en recherchant les spécificités de l'équipement (moteur, circuit électrique, vérin, pompe, ...) et en raisonnant par analogie. Dans le même objectif l'identification des modes de défaillances est exhaustive.

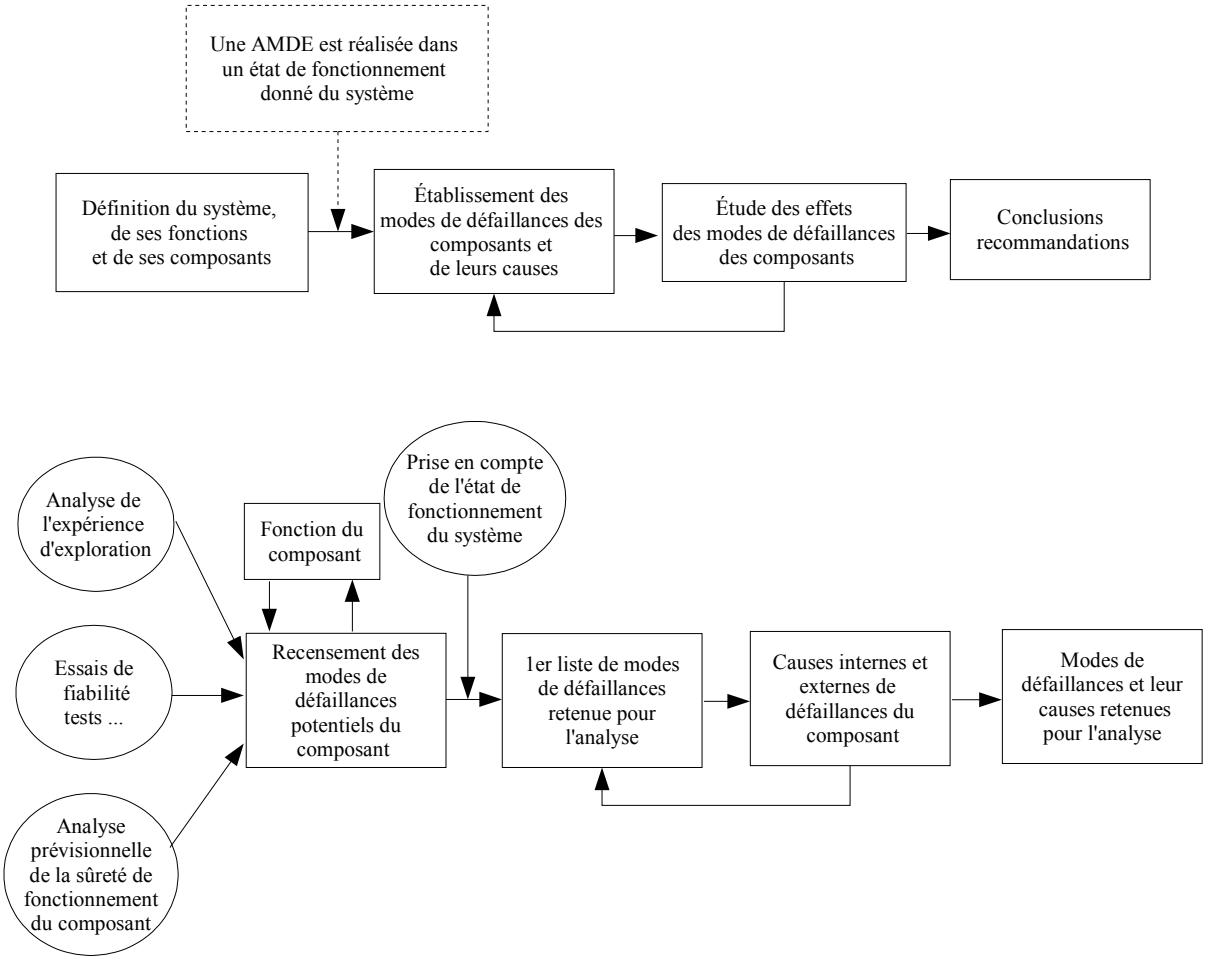


figure 1.7 Méthode de réalisation d'une AMDE [Villemeur 1988]

L'AMDEC a pour objectif d'examiner comment chaque entité d'une installation peut tomber en panne (ou être utilisée de façon incorrecte). On définit les notions de modes de défaillances, de causes de défaillances et d'effets d'une défaillance.

Le mode de défaillances

C'est l'effet par lequel une défaillance est observée (norme CEI)

- en d'autres termes :

- le mode est la façon, la manière par laquelle la défaillance d'une entité se manifeste de façon physique (concrète) à l'utilisateur

- alors que la défaillance est la cessation de l'aptitude d'une entité à assurer une fonction requise.

La cause d'une défaillance

C'est la circonstance liée à la conception, la fabrication ou l'emploi et qui a entraîné une défaillance (norme CEI)

Effet d'une défaillance

- C'est l'ensemble des manifestations de toutes natures qui se produisent après l'apparition

d'un mode de défaillances

- Ces manifestations peuvent être :

- sur la disponibilité du moyen de production
- sur la qualité du produit fabriqué
- sur les coûts de maintenance [AFNOR 1994]
- sur la sécurité, l'hygiène, l'environnement

L'objectif de la méthode est d'identifier tous les composants et leurs modes de défaillances pouvant conduire à un problème.

1.4.3 La méthode HAZOP

L'HAZOP est fondamentalement différente de l'AMDEC puisqu'elle se focalise non pas sur les composants mais sur les flux échangés entre les composants. En effet, la méthode (figure 1.8) étudie l'ensemble des déviations d'un flux en se basant sur des déviations types et analyse les causes et les effets de ces déviations sur le système [Lawley 1974]. Comme l'AMDEC, cette méthode est accompagnée d'une analyse structurelle pour recenser l'ensemble des flux du système.

L'analyse HAZOP se fait en s'intéressant à ce que l'on appelle points d'étude, et qui sont de deux types :

- les éléments ou sections du procédé
- les étapes du mode opératoire

Ces points d'étude sont analysés un par un. On détermine l'ensemble des variables qui caractérisent ce point. Puis est appliquée à chaque variable une liste de mots clefs pour construire toutes les déviations possibles et examiner celles entraînant des risques.

Remarque : l'AMDEC permet une représentation sous une forme fonctionnelle, alors que l'HAZOP est une approche basée sur la déviation des variables et la propagation des flux.

L'analyse HAZOP (Hazard and Operability study) a pour objectif l'identification des risques et l'étude de leur prévention / protection en s'appuyant sur le principe qu'un groupe d'experts peut interagir d'une façon créative et systématique et identifier plus de problèmes en travaillant ensemble qu'en travaillant chacun de son côté. Une revue HAZOP permet d'analyser en détail et de façon systématique une installation, un mode opératoire ou des procédures.

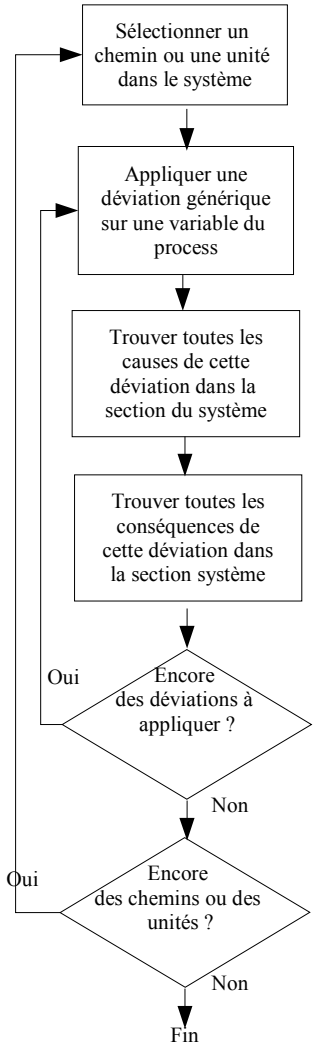


figure 1.8 Principe d'analyse de l'HAZOP

1.4.4 La méthode HACCP

La méthode HACCP (Hazard Analysis Critical Control Point) ou analyse des risques maîtrise des points critiques utilisés dans le secteur agroalimentaire.

Pendant l'identification, l'évaluation des dangers et les opérations ultérieures pour la conception et la mise en œuvre du système HACCP, il y a lieu de prendre en compte l'impact d'éléments tels que matières premières, ingrédients, Bonnes Pratiques de Fabrication ainsi que le rôle joué par des procédés de fabrication dans la maîtrise des dangers, la destination finale vraisemblable du produit, les populations de consommateurs à risques et les preuves épidémiologiques relatives à la salubrité des aliments. L'objectif du système HACCP est de mettre l'accent sur les actions de maîtrise à exercer au niveau des CCP (Critical Control Point). La conception de l'opération doit être envisagée lorsqu'un danger est identifié et qu'aucun CCP n'a été établi.

L'application du système HACCP doit se faire sur chaque procédé pris séparément. Les CCP

identifiés pour tout exemple donné dans tout code d'usages en matière d'hygiène du Codex peuvent ne pas être les seuls CCP identifiés pour une application spécifique ou peuvent être de nature différente.

L'application du système HACCP doit être révisée et les changements nécessaires effectués lors de toute modification apportée au produit, au procédé ou à toute étape de la production. Lors de l'application du système HACCP, il importe de faire preuve de souplesse en fonction du contexte particulier de l'application.

Cette méthode est basée sur la réalisation de sept principes:

- Principe 1 : lister les dangers éventuels associés à chacune des étapes, effectuer une analyse des risques et lister toutes les mesures destinées à maîtriser les dangers identifiés.
- Principe 2 : déterminer les points critiques pour la maîtrise des dangers.
- Principe 3 : établir les limites extrêmes pour chaque point critique.
- Principe 4 : établir un système de surveillance pour chaque point critique.
- Principe 5 : établir les actions correctives
- Principe 6 : établir des procédures de vérification
- Principe 7 : établir un système d'enregistrement et de documentation.

Définition

Un point critique (CCP) étant défini comme tout point, lieu, personnel, opération ou protocole pour lequel la perte de la maîtrise peut entraîner un risque inacceptable pour la qualité du produit. Il s'agit de tout produit, étape ou opération pour laquelle la maîtrise doit être assurée et tout danger peut être éliminé, prévenu ou réduit à un niveau acceptable.

Dans une étude HACCP, il faut suivre le flux de matière à l'intérieur de l'installation. La recherche des points critiques est difficile quand le système est fortement automatisé. En effet, le déroulement de la recette est automatique, et le nettoyage en place (NEP) est un système complet ayant sa propre recette.

1.4.5 Les autres méthodes

Dans la littérature, il existe de nombreuses méthodes permettant de réaliser une modélisation du système à partir d'une méthode exhaustive. Nous allons décrire dans ce paragraphe deux de ces méthodes : les graphes de Markov et les réseaux de Petri (RdP) stochastiques.

Les graphes de Markov sont couramment utilisés pour l'évaluation de la disponibilité et de la fiabilité des systèmes. Ils peuvent aussi, sous réserve de certaines modifications être utilisés pour

l'évaluation de la sécurité [Niel 1992]. Les graphes de Markov s'appliquent en principe aux systèmes markoviens pour lesquels le taux de défaillances et de réparation des composants sont constants. Dans ce cas, l'approche consiste à déterminer les états possibles du système et les probabilités de transition associées. Généralement, les états pris en compte sont les suivants : état normal, état de fonctionnement dégradé, état de panne, état critique,... Par convention, la transition d'état peut s'effectuer par l'occurrence d'un taux de défaillances ou dans le cas contraire par un taux de réparation.

L'avantage des graphes de Markov réside dans leur aptitude à tenir compte des dépendances entre composants et dans la possibilité d'obtenir différentes mesures à partir d'un même modèle (fiabilité, disponibilité, ...) Toutefois, dans le cas de systèmes complexes, l'utilisation des graphes de Markov peut mener à l'explosion rapide du nombre d'états. De plus, l'hypothèse du système markovien reste très restrictive [Zaytoon 1993].

Les réseaux de Petri stochastiques [Movaghar 84] traitent des phénomènes qui ne peuvent pas être correctement modélisés en utilisant des durées constantes. Un temps aléatoire est associé au franchissement d'une transition. Afin d'utiliser les RdP stochastiques pour la modélisation de la SDF, les jetons peuvent représenter des fautes ou des composants sains. Aux transitions sont associés des temps aléatoires exprimant le MTTF (temps moyen jusqu'à la défaillance) ou le MTTR (temps moyen jusqu'à la réparation). Ces temps sont en fonction des lois de probabilité de défaillances et de réparation. Il existe de nombreux outils de simulation, basés sur les RdP. Nous remarquons par la description de ces deux méthodes qu'il s'agit d'outils de représentation de l'installation dans le but de réaliser une analyse quantitative et non des méthodes d'analyse des risques.

1.5 Limites des méthodes actuelles

1.5.1 AMDEC

1.5.1.1 Types de résultats

Une analyse AMDEC génère une table qualitative et systématique des équipements, de leurs modes de défaillances et de leurs effets. Une estimation des conséquences dans le pire des cas est fournie ainsi que les recommandations pour éviter le problème.

1.5.1.2 Limites

Une analyse AMDEC n'est pas une analyse systémique, ceci pose un problème pour déterminer le niveau de détail à lequel l'analyse doit être réalisée, elle ne permet pas une représentation de la déviation des flux. Enfin, l'AMDEC par nature ne prend pas en compte la

simultanéïté des défaillances. L'AMDEC reste par nature l'une des rares méthodes en industrie mais dont la mise en oeuvre reste fastidieuse, de quelques mois à quelques années pour une étude complète.

1.5.2 HAZOP

1.5.2.1 Types de résultats

Les résultats obtenus par ce type de revue comprennent l'identification des risques et des problèmes d'exploitation ainsi que les recommandations pour améliorer la conception ou les procédures. Les causes, effets et mesures de prévention de chaque déviation analysée sont mises sous forme de table. L'HAZOP permet une représentation des modes dégradés.

1.5.2.2 Limites

La méthode HAZOP repose sur la déviation des variables, mais ne prend pas en compte les défaillances, ni les enchaînements que peuvent entraîner les déviations de ces variables. Enfin, cette méthode ne représente pas l'installation sous une forme structurée facilement informatisable.

1.5.3 HACCP

1.5.3.1 Type de résultats

Cette méthode est bien adaptée à la maîtrise de la sécurité et de la non qualité des procédés agroalimentaires tant qu'on considère des procédés simples opérés manuellement. Elle permet d'éliminer les sources de danger et de non-qualité élémentaire. Par contre, lorsqu'on étudie des systèmes complexes, on découvre qu’ils sont composés d'un certains nombres d'opérations en cascade, pour lesquelles les scénarios de dysfonctionnement sont complexes. Une exploitation systématique du retour d'expérience serait souhaitable pour gérer ces systèmes.

En effet, si l'automatisation des procédés a certes apporté un plus à la sécurité et à l'homogénéité des produits fournis aux clients, elle rend aussi les choses plus complexes et peut être moins robuste vis à vis des aléas. Par ailleurs, un des dangers de l'automatisation est qu'elle peut donner l'impression à l'utilisateur d'une limitation totale des risques, les automates et outils de régulation étant supposés sûrs. On peut à ce sujet remarquer que les pannes ou dysfonctionnements de l'outil automatique ne sont que très rarement pris en compte par HACCP, et que la mise en place, même d'un outil automatisé, peut dans certains cas être une préconisation HACCP.

1.5.3.2 Limites

La méthode HACCP ne repose pas sur une étude systémique, de plus sa mise en place n'est pas simple sur une installation fortement automatisée.

1.6 Discussion

1.6.1 Cahier des charges

Dans ce chapitre nous allons décrire le cahier des charges que nous devons respecter pour la construction d'une méthode d'analyse des risques "idéale".

- être générique et utilisable dans différents secteurs industriels (agro alimentaire, chimique, métallurgie),
- pouvoir choisir les cibles (celles-ci peuvent être un produit, une installation globale ou une partie d'un système) pour réaliser l'analyse,
- construire une capitalisation de la connaissance permettant une sauvegarde et une réutilisation des analyses déjà réalisées (les scénarios),
- être systémique pour permettre le choix de la finesse de la représentation de l'installation (exemple une analyse doit être possible soit au niveau d'un site industriel global, soit au niveau d'une chaîne de production, soit au niveau d'un poste de travail) pour éviter les oublis ou les erreurs,
- cette méthode doit pouvoir être réalisée de façon simple indépendamment de la complexité de l'installation,
- l'objectif final de la modélisation est d'obtenir les scénarios de dangers possibles sur une installation,
- cette méthode devra être programmable pour permettre la gestion et le stockage des informations.

Pour construire une méthode d'analyse des risques qui respecte ce cahier des charges, il faut construire les scénarios directement et les enregistrer dans une base de connaissances, pour qu'ils soient réutilisables. Nous avons dans un premier temps cherché à utiliser les méthodes existantes, en utilisant par exemple un automate à états.

1.6.2 Exemple

Nous allons présenter un exemple (voir figure 1.9) composé d'une robot industriel qui doit ranger des produits sur des palettes. Ce robot se situe dans une zone de sécurité constituée d'une grille entourant le robot et d'une porte permettant d'accéder à la zone du robot. Cette porte possède un capteur permettant de stopper le robot en cas d'ouverture (arrêt d'urgence). Nous

utiliserons les entités suivantes : le robot, le capteur qui détecte l'ouverture de la porte, le bouton de commande du robot, la porte, l'arrêt d'urgence et l'opérateur.

Pour chaque entité, nous décrivons les différents états possibles :

- état du robot (marche en mouvement, marche en attente, arrêt, arrêt d'urgence)
- état de la porte (ouverte, fermée)
- état du capteur de la porte (ouvert, fermé)
- état du bouton de commande du robot (marche, stop)
- état de l'opérateur (hors de la zone sécurisée ou dans la zone sécurisée)

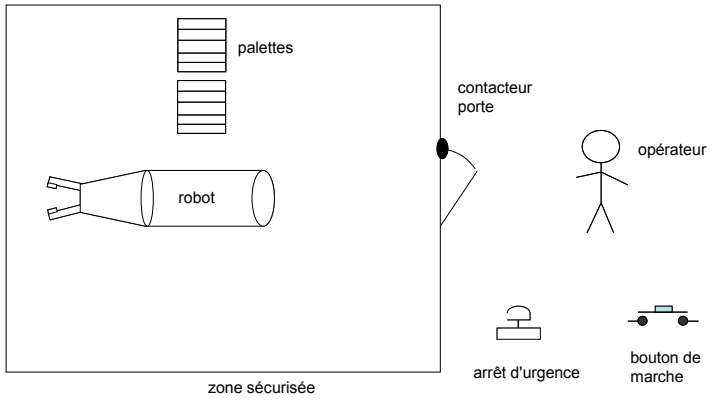


figure 1.9 Vue d'ensemble du robot

1.6.2.1 Analyse de risque

Avec ces quatre éléments de l'installation nous pouvons réaliser une analyse de risque et rechercher tous les scénarios qui peuvent être construits.

Dans un état normal, le robot est dans l'état de marche en attente, il y a ouverture de la porte, l'événement initiateur est un dysfonctionnement du capteur qui ne détecte pas l'ouverture de la porte. L'état de danger est un état ou le robot est en marche, en attente avec une personne dans la zone de sécurité. Dans un cycle normal, le robot passe dans un état de marche en mouvement. Il y a alors apparition d'un état d'accident ou le robot va percuter la personne dans la zone de sécurité. Enfin, il y a un état de fin d'accident quand un opérateur aura utilisé le système de sécurité pour sécuriser la zone du robot , l'état de fin d'accident va être défini par les dommages causés à la personne dans la zone du robot. Ce scénario représente un scénario de danger possible.

Nous allons maintenant chercher à retrouver cette description dans un modèle de dysfonctionnement complet de l'installation. Pour cela, nous utiliserons une modélisation sous la forme d'un automate à états.

1.6.2.2 Modélisation du système

Pour représenter le robot (figure 1.10) nous pouvons le faire sous la forme d'un système d'automate (voir 2.3.1.4 Système d'automate page 51) utilisant une synchronisation par message [Laroussinie 1999].

- l'état 1 représente l'arrêt normal,
- l'état 2 représente la marche en attente, le robot est dans sa position d'arrêt en attente d'une palette,
- l'état 3 représente la marche en mouvement, le robot est en mouvement,
- l'état 4 représente l'arrêt d'urgence qui se déclenche sous l'action d'un arrêt coup de poing ou par l'ouverture de la porte.

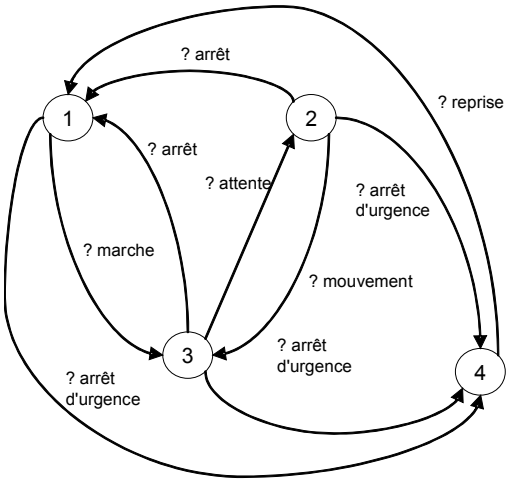


figure 1.10 Représentation du robot

Pour représenter l'interrupteur de commande, nous le réalisons avec un automate (voir figure 1.11)

- l'état 5 représente l'état d'arrêt du robot interrupteur ouvert,
- l'état 6 représente l'état de marche du robot interrupteur fermé.

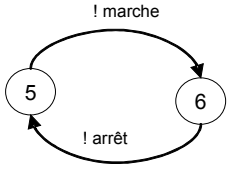


figure 1.11 Représentation de l'interrupteur

Pour représenter la porte, nous utilisons les automates présentés figure 1.12, le premier représente les états de la porte, le suivant représente l'état du capteur d'arrêt d'urgence de la porte.

- l'état 7 représente la porte ouverte,
- l'état 8 représente la porte fermée.

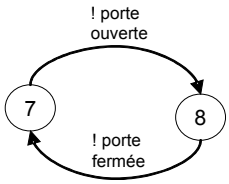


figure 1.12 Représentation de la porte

Les états du contacteur de la porte, enclenchant l'arrêt d'urgence sont représentés figure 1.13.

- l'état 9 représente le contacteur ouvert donc le système est dans un état d'arrêt d'urgence,
- l'état 10 représente le contacteur fermé donc le système en fonctionnement normal.

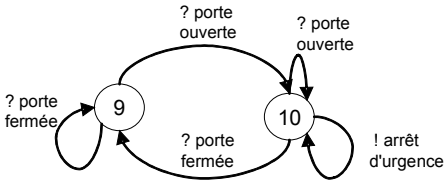


figure 1.13 Représentation du contacteur de la porte

Les états de l'arrêt d'urgence sont présentés figure 1.14.

- l'état 11 représente l'état de l'arrêt d'urgence non déclenché,
- l'état 12 représente le déclenchement de l'arrêt d'urgence.

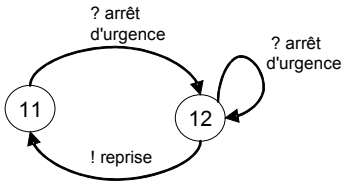


figure 1.14 Représentations de l'arrêt d'urgence et de la reprise

La figure 1.15 représente le contacteur de la porte avec un état de dysfonctionnement, le contacteur ne détectant pas l'ouverture de la porte.

- l'état 13 représente un état ou le contacteur est bloqué fermé, quand la porte est ouverte. Cet état est un état de danger, car il n'y a pas d'événement d'arrêt d'urgence généré par l'état 13.

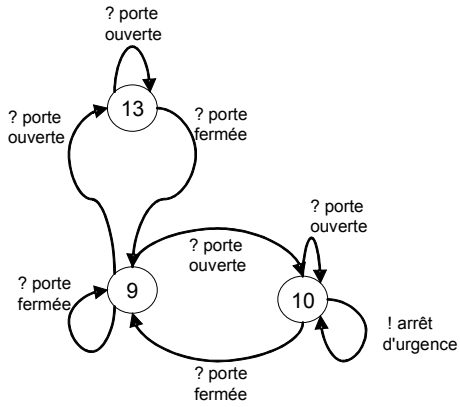


figure 1.15 Contacteur de la porte avec les états de défaillances

Les états représentant les emplacements de l'opérateur sont décrits dans la figure 1.16.

- l'état 14 représente l'opérateur hors de la zone sécurisée.
- l'état 15 représente l'opérateur dans la zone sécurisée.

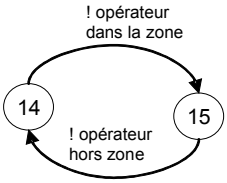


figure 1.16 Position de l'opérateur

A partir de la figure 1.15 si l'automate est dans l'état 13 alors le robot peut se trouver dans l'état 1, 2, ou 3, le robot est alors en fonctionnement et la porte est ouverte. Nous obtenons les deux premières évolutions d'un enchaînement de scénario de danger.

Cette représentation de l'installation permet de déterminer un état de danger de l'installation possible, à partir d'une défaillance. Ici, un état de danger (figure 1.17) est composé des états suivants : 2, 6, 8, 11, 13 et, 15. Cette méthode demande la construction d'un modèle par composant de l'installation ainsi que leurs synchronisations. Cette méthode devient alors pour une installation industrielle très difficile à réaliser, et demande de modéliser l'installation dans son ensemble, ainsi que la synchronisation de tous les automates.

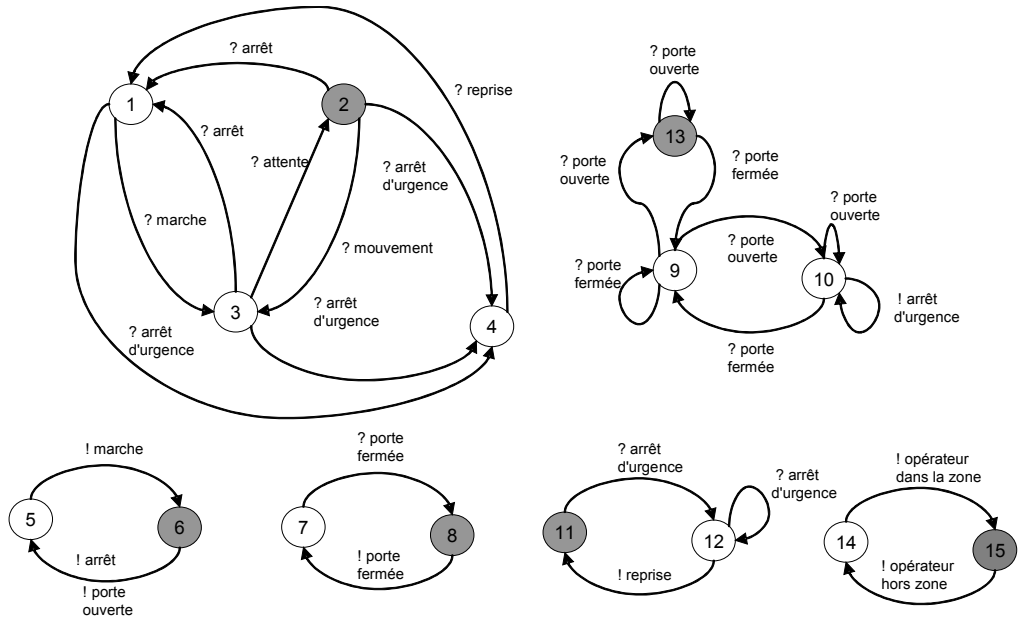


figure 1.17 Etat dangereux de l'installation

Pour la réalisation d'une analyse de risque, nous constatons que nous n'avons besoin que de certains de ces états. Nous remarquons que nous n'avons besoin que de certaines caractéristiques permettant de définir les états dangereux de chaque élément de l'installation (dans l'exemple de la figure 1.9, il s'agit du dysfonctionnement du contacteur, la modélisation du fonctionnement du robot n'apporte aucune information). Si nous pouvons déterminer les caractéristiques permettant de caractériser les états dangereux, nous remarquons qu'il n'est plus nécessaire de représenter le fonctionnement de l'installation dans son ensemble. Mais seulement les caractéristiques dangereuses et les enchaînements dangereux possibles que celles-ci peuvent entraîner. Nous n'avons alors pas besoin de réaliser une simulation de l'installation par l'utilisation d'un modèle quantitatif, mais d'une représentation des caractéristiques possiblement dangereuses de l'installation donc un modèle qualitatif. Cette représentation permet d'obtenir des scénarios effectifs, nous pouvons simuler le fonctionnement de l'installation, mais la représentation est longue à construire pour une installation de taille normale.

Dans la suite de ce chapitre, nous allons détailler certaines méthodes d'analyse de risques existantes, qui ont servi à l'élaboration de ScénaRisK.

La méthode MoDyf ne permet pas la réalisation d'une description car dans ce modèle il faut pour chaque entité construire l'ensemble des états normaux et anormaux, ce qui demande un découpage et une description de toutes les entités, ce modèle est difficile à construire car il faut représenter toutes les intéractions entre les entités. Les résultats de l'analyse dépendent de la

précision de la description.

Il faut représenter l'ensemble des états possibles normaux de l'installation, ce qui est possible, mais il faut aussi représenter les états anormaux, que ce soit des états anormaux dangereux ou non dangereux, ainsi que toutes les interactions possibles entre les entités. Grâce à cette modélisation nous obtenons une représentation des différents états possibles (normaux et anormaux) pour chaque entité et pour le système de commande. Pour que l'étude soit possible et permette de réaliser une analyse des risques pour obtenir l'ensemble des scénarios de danger, il faut pouvoir modéliser l'ensemble des bons fonctionnements de l'installation pour réaliser une simulation.

Les graphes de Markov et les réseaux de Petri stochastiques ont une approche des scénarios basée sur la description de tous les éléments physiques en vue de la réalisation d'une simulation. Nous désignons ces scénarios par le nom de scénarios effectifs. Les scénarios de la méthode MADS-MOSAR [Périlhon 1998] sont appelés scénarios possibles car ils font abstraction de la réalité en vue de la recherche des événements et des états dangereux [Flaus 2001]. Notre modélisation s'appuie sur des scénarios de type possible, en faisant abstraction de la réalité, notre but n'étant pas la réalisation d'une simulation de l'installation, mais la recherche des scénarios de dangers.

L'analyse des risques à partir des méthodes (AMDEC, HAZOP ...) repose sur les acteurs de la mise en oeuvre qui en sont les principaux atouts. Il n'y a pas de conservation des connaissances sous une forme exploitable par des personnes qui ne sont pas expertes dans le domaine concerné. Il n'y a aucun lien entre les méthodes d'analyse des risques et la construction d'un arbre des défaillances qui doit être réalisé à la main. Pour pouvoir construire un arbre de défaillances de façon automatisée, il faut être capable de représenter les enchaînements conduisant à un accident sous une forme structurée pour être exploitable. Ainsi que la réalisation d'une description de l'installation permettant l'utilisation de la représentation des scénarios de danger.

Pour la réalisation d'une méthode d'analyse des risques, il existe deux manières :

- un modèle complet de l'installation et de son fonctionnement, tel l'exemple du robot, qui n'est pas adapté à notre cas
- ou un modèle simplifié n'utilisant que les éléments comportant un risque, c'est cette solution que nous allons détailler dans la suite.

Dans le chapitre suivant, nous présenterons une modélisation de la base de connaissances pour une modélisation abstraite de l'installation, permettant la génération de scénarios de dangers.

Chapitre 2

La méthode ScénaRisK

2.1 Introduction

La méthode ScénaRisK (figure 2.1) a pour objectif de générer des scénarios de danger à partir d'une librairie d'éléments de scénarios existante et d'une représentation spécifique de l'installation. Pour atteindre cet objectif, nous devons être capable de représenter l'apparition d'un danger, d'un accident, et d'un post accident.

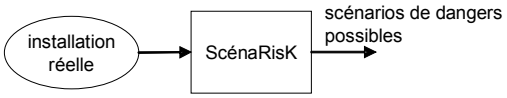


figure 2.1 Objectif de ScénaRisK

La figure 2.2 présente le déroulement de la méthode dans son ensemble. Pour cela, nous disposons d'une base de connaissances (1) construite à partir d'une liste d'attributs génériques (1.1) et d'un ensemble de scénarios de danger (1.2) caractérisé par les attributs. A partir de l'installation réelle (0), nous réalisons un découpage arbitraire de l'installation (3) sous la forme d'entités structurelles. Pour chacune des entités structurelles nous recherchons la liste des attributs caractéristiques (3.1) qui la compose à partir de la base de connaissances. D'autre part un modèle fonctionnel, où nous devons déterminer les fonctions (2) de l'installation. A partir de ces fonctions nous recherchons la liste des entités qui interviennent pour la réalisation de chacune des fonctions (2.1). Nous construisons aussi les correspondances physique / danger (3.2) et les correspondances danger / physique (3.3), qui représentent les scénarios spécifiques de

l'installation. Enfin à partir des éléments de scénarios de danger de la base de connaissances, des scénarios spécifiques et de la description fonctionnelle, nous générons les scénarios de dangers (2.2) possibles pour chaque fonction.

Définition

*Un **scénario de danger** est la représentation des enchaînements conduisant à un accident sous une forme structurée et réutilisable.*

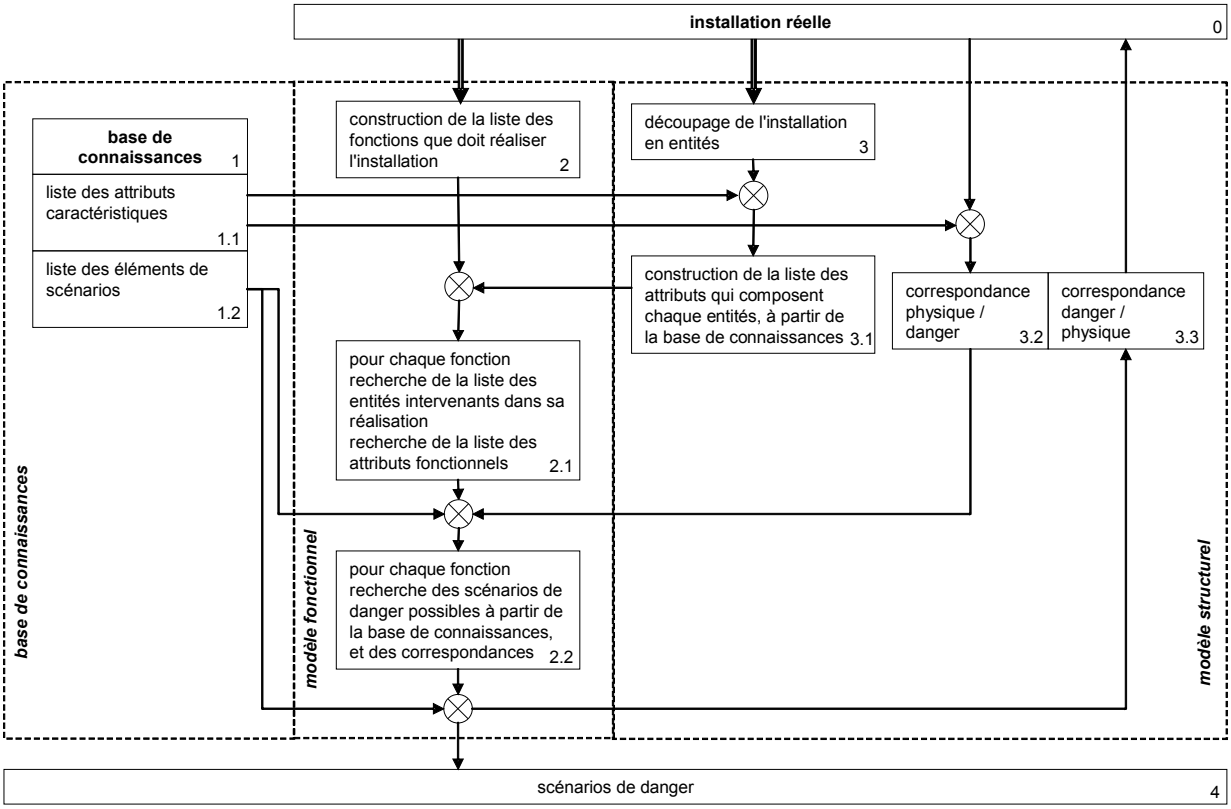


figure 2.2 La méthode ScénaRisK

Dans ce chapitre, nous allons dans un premier temps présenter la genèse de l'outil, les évolutions principales ayant permi d'aboutir à ScénaRisK, puis nous présenterons une modélisation possible des éléments de scénario de danger, d'accident, et de post accident sous la forme d'un automate à états. Ensuite, nous décrirons la modélisation spécifique de l'installation, nous permettant une utilisation simple et efficace du modèle générique de danger. Enfin, nous terminerons par l'utilisation possible de ces modèles génériques, ainsi que la description d'un exemple ayant permi de tester la méthode ScénaRisK.

2.2 La genèse de ScénaRisK

2.2.1 Les prémisses de ScénaRisK

Après avoir défini le cahier des charges, il est apparu que nous devions construire une méthode avec deux parties distinctes :

- une représentation des enchaînements conduisant à un accident, indépendant de l'installation réelle que nous appelons la base de connaissances (permettant une réutilisation de la base de connaissances quelque soit l'installation étudiée),
- et une description de l'installation réelle pour utiliser la base de connaissances, et permettre la génération de scénarios de dangers, cette description doit aussi être réutilisable en introduisant des éléments génériques.

La première approche, s'appuie sur la modélisation MoDyf, nous avons construit une représentation de tout ce que l'installation peut faire. Cette approche est basée sur un découpage en entités. Chaque entité est décrite sous la forme d'état normaux, anormaux non dangereux et anormaux dangereux. Dans la seconde partie il faut donner la liste de tous les flux entre les entités (flux d'informations, flux de matières) le but de cette démarche est de réaliser la simulation de l'installation afin de déterminer les scénarios de danger issus de la base de connaissances.

Pour la construction de la base de connaissances nous avons déterminé un scénario de danger minimum (état de pré danger, état de danger, état d'accident, état de post accident). Cette approche de la base de connaissances est théorique, car nous ne pouvons pas la rendre systématique et réutilisable à cause de la description de l'installation qui ne permet pas de déterminer facilement les éléments dangereux. Cette démarche a été abandonnée pour les raisons suivantes :

- la modélisation de l'installation sous forme d'entité et de flux est lourde à réaliser, donc la méthode n'est pas utilisable dans le domaine industriel.
- nous n'utilisons qu'une petite partie de la description de l'installation pour la recherche des scénarios de danger, une simplification est obligatoire.
- les liens entre la base de connaissances et la description de l'installation ne sont pas simples et nous obtenons une liste de scénarios unique pour chaque entité.
- la base de connaissances n'est ni structurée ni générique et, elle est donc difficile à construire.

2.2.2 L'ébauche de ScénaRisK

Dans l'approche que nous avons détaillée au paragraphe précédent, nous remarquons que la description de l'installation n'est pas adaptée à l'analyse des risques. En effet, quand nous décrivons une installation, nous n'avons besoin pour la réalisation de notre étude que de certaines caractéristiques permettant la description des entités. Ces caractéristiques sont appelées des attributs qualitatifs, et permettent de ne décrire que les éléments possibles dangereux dont nous avons besoin pour une analyse des risques. Grâce aux attributs, nous avons simplifié la description de l'installation tout en ne conservant que les éléments indispensables pour l'analyse.

En introduisant les attributs dans la base de connaissances, nous remarquons qu'ils permettent la description de tous les états de façon simple (un état est décrit par une liste d'attributs) et deviennent de ce fait les éléments de base permettant la structuration et la description de la base de connaissances.

2.2.3 La maturation de ScénaRisK

Après avoir décrit les avantages des attributs, nous avons réalisé une description plus poussée de l'installation sous la forme d'une description structurelle (en utilisant des entités génériques) et sous une forme fonctionnelle. La base de connaissances a évolué pour permettre la description de tous les accidents à partir de la liste des attributs caractéristiques. Les liens entre la base de connaissances étant maintenant réalisés par les attributs qualitatifs, il est simple d'extraire de la base de connaissances les scénarios qui peuvent être issus de la description de l'installation.

Enfin, un outil informatique a évolué en parallèle à la méthode nous permettant la validation de celle-ci.

2.3 Eléments de scénarios génériques

Nous venons de présenter les étapes qui nous ont permis d'aboutir aux choix des attributs. Nous allons maintenant décrire plus en détail la structure de la base de connaissances ainsi que la méthode utilisant cette base de connaissances.

2.3.1 Les structures de bases génériques

2.3.1.1 Les attributs qualitatifs descriptifs

Les attributs qualitatifs sont très importants dans notre analyse, il s'agit de l'élément de base dans la construction de notre modèle. Un attribut qualitatif est, soit non déterminé donc aucune utilisation de sa valeur ne peut être faite, soit défini et alors, il doit être décrit par un ensemble de valeurs possibles, sachant qu'une valeur est prise à chaque instant par l'attribut. Pour permettre le

changement de ces valeurs, nous construisons les éléments de scénarios d'évolution des attributs.

Nous décrirons une entité à partir d'une liste d'attributs, par exemple une entité peut être décrite par sa taille et sa couleur

Pour la couleur, il peut exister un attribut couleur composé des valeurs suivantes :
couleur = {jaune, /jaune, ?}

- jaune, la couleur de l'entité est jaune
- /jaune, la couleur de l'entité n'est pas jaune
- ?, la couleur de l'entité n'est pas précisée

Un attribut qualitatif permet de décrire (par un ensemble de valeurs) une caractéristique d'un produit ou d'un matériel physique. Il s'agit alors d'un attribut caractéristique, ou attribut qualitatif.

Définition

***Attribut qualitatif** : Un attribut qualitatif représente une caractéristique applicable à un état. Les attributs peuvent être soit des caractéristiques physiques (toxique, combustible, agroalimentaire) soit des caractéristiques fonctionnelles (étanche, stérile).*

Un attribut qualitatif est défini par un n uplet donnant les différentes valeurs possibles.
Soit l'attribut

$$P^k = \{?, V^k_1, V^k_2, ..., V^k_n\}$$

Les V^k_n représentent les n différentes valeurs que peut prendre l'attribut P^k.

Un exemple applicatif concerne un fruit, des bananes qui sont décrites par deux attributs :

- L'attribut couleur est défini par l'ensemble couleur = {?, jaune, brun, noir}.
- L'attribut taille est défini par l'ensemble taille = {?, petit, moyen, grand}.

2.3.1.2 Etat

Un attribut qualitatif est une caractéristique applicable à un élément physique, un élément peut aussi avoir plusieurs attributs permettant de le définir. Nous allons alors introduire la notion d'état. Un état est alors défini par un ensemble d'attributs qualitatifs.

Définition

***Etat :** Un état est défini par la donnée d'un certain nombre d'attributs ou propriétés. Un état est dit à risques s'il contient un sous ensemble d'attributs*

inclus dans un état de pré-danger de scénario de danger. C'est un n uplet élément du produit cartésien des valeurs possibles des attributs.

Un état est défini par un ensemble d'attributs. Exemple l'état e permettant de définir les différents états d'une banane est le produit cartésien entre la couleur et la taille des bananes :

e = couleur x taille

e = { (?, ?), (?, petit), (?, moyen), (?, grand)
(jaune, ?), (jaune, petit), (jaune, moyen), (jaune, grand)
(brun, ?), (brun, petit), (brun, moyen), (brun, grand)
(noir, ?), (noir, petit), (noir, moyen), (noir, grand) }.

2.3.1.3 Les événements

Les événements permettent de décrire les changements d'état du système sous la forme de la propagation des dangers, des effets, des dommages et des accidents. Ils représentent un changement de valeur d'un attribut, d'une valeur de départ à une valeur finale.

Exemple : Présence toxique, présence agroalimentaire, présence choc.

Définition

L'occurrence d'événement, dans un système à événements discrets, permet un changement d'état du système, ceci correspond à la variation de la valeur d'un attribut.

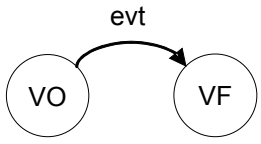


figure 2.3 Evénement

Un événement "evt" est donc défini comme un changement de valeur d'un attribut la figure 2.3 d'une valeur VO à une valeur VF.

Exemple : si l'état de la banane passe d'un état jaune à un état brun, il y eu réception d'un événement, le changement de couleur ou, VO est la couleur jaune et VF la couleur brune, evt étant le changement de couleur du fruit.

Les événements sont générés par les états, nous parlons alors d'événements dangereux, ou par les états d'accidents : les événements d'accidents. Dans notre modèle, les événements permettent l'enchaînement et la propagation des effets, et des dommages. Les événements permettent de

représenter la propagation des flux tels que décrits dans le modèle MADS.

2.3.1.4 Les conditions

Les conditions vont permettre l'ajout de conditions sur les transitions telle qu'une analyse par ajout des statistiques, pour rechercher les scénarios les plus probables ou les conditions possibles. Les conditions sont des expressions booléennes, si la condition est vraie alors la transition est franchissable. Les conditions sont souvent associées aux événements pour définir une transition nous parlons alors d'événements / conditions (E/C).

2.3.2 Systèmes d'automates

Pour réaliser une description de tous les enchaînements qui peuvent se produire, nous avons choisi de les représenter sous la forme d'un système à transitions (ST).

Définition

Un système à transitions *est défini par la donnée d'un quadruplet* (S, T, α, β)

S est un ensemble fini d'états

T est un ensemble de transitions

α *et* β *sont des applications de T vers S qui associent à chaque transition t élément de T les états* $\alpha(t)$ *et* $\beta(t)$ *respectivement source et cible de la transition.*

L'exemple de la figure 2.4 décrit un système à transitions composé de 3 états et 3 transitions.
((1,2,3),(a,b,c),(a,1)(b,2)(c,3),(a,2)(b,3)(c,1))

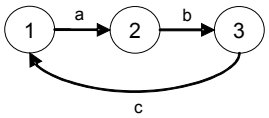


figure 2.4 Exemple

De façon à permettre la communication entre les différents éléments de notre modèle, nous ajoutons au modèle précédent une étiquette à chaque transition, qui peut correspondre à l'envoi d'un message m, noté !m ou à sa réception, notée ?m. [Laroussinie 1999]

Enfin, une transition sera validée par une condition, définie à partir de la valeur de variables de l'espace d'état S.

Définition

Un ST étiqueté *est défini par la donnée d'un ST noté STet et par trois applications l1, l2, l3, Prop, E.*

Prop est l'ensemble des propriétés logiques définies sur S

E est un ensemble d'étiquettes

l1 : $T \rightarrow Prop$ associe à chaque transition une proposition logique, appelée condition, et qui doit être vraie pour permettre son franchissement

l2 : $T \rightarrow E$ associe à chaque transition une étiquette qui est reçue pour permettre son franchissement

l3 : $T \rightarrow E$ associe à chaque état une étiquette qui est émise.

Un exemple de ST étiqueté est présenté figure 2.5, les événement émis sont représentés sous la forme d'action associée à un état.

ST = (S, T, α, β)

$S = \{ état\ 1,\ état\ 2 \}$;

$T = \{ t1 \}$;

$\alpha = t1 \rightarrow état\ 1$;

$\beta = t1 \rightarrow état\ 2$;

ST avec étiquettes

$l1 = \emptyset$

$l2 = t1 \rightarrow E / C$;

$l3 = evt$

$Prop = \{ \emptyset \}$

$E = \{ E / C \}$;

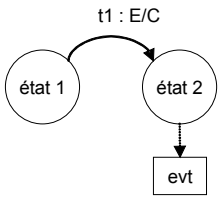


figure 2.5 ST étiqueté

2.4 Le modèle de danger

2.4.1 Introduction

Dans cette partie, nous allons répondre de façon systémique et systématique aux questions suivantes :

- Comment peut-on dans une installation aboutir à une situation dangereuse ?
- Comment peut-on et dans quelles conditions avoir une situation d'accident ?

Le modèle de danger permet de représenter sous la forme d'un système à événement discret asynchrone, le fonctionnement de l'apparition et l'évolution pouvant conduire à l'apparition d'un accident. Ces différentes étapes sont représentées sous la forme d'un automate à états. Pour cela, nous devons décrire un état de pré-danger ou si une transition constituée d'événements et ou de conditions est franchissable nous aboutissons dans un état de danger.

2.4.2 Elément de scénario de danger

Définition

***État de pré-danger** : Un état de pré-danger est un état permettant d'identifier les dangers. Cet état peut être décrit par la présence de caractéristiques (attributs) présents ou non présents sous forme d'un n uplet (ex chaud ou pas chaud, toxique ou pas toxique), exemple (agroalimentaire, étanche, stérile) où les noms représentent les attributs associés à l'état de pré-danger.*

Nous représentons un état de pré-danger par un ensemble d'attributs, il est alors possible si l'ensemble des attributs est présent dans cet état, d'évoluer vers un état de danger, si la transition qui suit est vraie.

Définition

***État de danger :** état décrivant un danger par un ensemble d'attributs, et des événements de danger générés*

***État de danger non réversible :** un état de danger où aucun retour n'est possible à l'état initial.*

***État de danger réversible** : un état de danger, où il est possible de revenir à l'état initial.*

Un changement d'état d'un état de pré danger à un état de danger peut générer des événements

de danger, qui vont permettre la propagation de ce danger, soit en agissant sur une transition d'un élément de scénario, soit en modifiant une condition. La transition est composée d'événements et de conditions. Il existe deux états de danger différents :

- Un état de danger réversible (figure 2.6) est un état à partir duquel, il est possible de revenir à l'état initial. Par exemple, pour un état initial composé d'un produit agroalimentaire, dont la température doit être comprise entre 2 et 4 °C, si la température n'est pas maintenue pendant un temps t inférieur au temps maximum, il est possible de revenir dans l'état de pré-danger.
- Un état non réversible (figure 2.7) est un état à partir duquel, il n'est pas possible de revenir à l'état de pré-danger. Par exemple, l'ajout de bactéries pathogènes dans un produit agroalimentaire va conduire vers un état de danger, dont le retour à l'état de pré-danger n'est pas possible.

Un état de pré-danger et un état de danger permettent de représenter un élément de scénario, appelé élément de scénario de danger.

ST = (S, T, α, β)

$S = \{agro\ alimentaire, denrée\ contaminée\};$

$T = \{t1, t2\};$

$\alpha = t1 \rightarrow agroalimentaire\ maintien\ en\ température, t2 \rightarrow denrée\ contaminée;$

$\beta = t1 \rightarrow denrée\ contaminée, t2 \rightarrow agroalimentaire\ maintien\ en\ température;$

ST avec étiquettes

$l1 = \emptyset$

$l2 = t1 \rightarrow présence\ de\ non\ maintien\ en\ température,$
$t2 \rightarrow présence\ de\ maintien\ en\ température;$

$l3 = développement\ de\ bactéries$

$Prop = \{\emptyset\}$

$E = \{présence\ de\ non\ maintien\ en\ température, présence\ de\ maintien\ en\ température\};$

figure 2.6 Etat de danger réversible

ST = (S, T, α, β)

$S = \{agro\ alimentaire, denrée\ contaminée\}$;

$T = \{t1\}$;

$\alpha = t1 \rightarrow agroalimentaire$;

$\beta = t1 \rightarrow denrée\ contaminée$;

ST avec étiquettes

$l1 = \emptyset$

$l2 = t1 \rightarrow ajout\ bactéries\ pathogènes$;

$l3 = evt\ dangereux$

$Prop = \{\emptyset\}$

$E = \{ajout\ bactéries\ pathogènes\}$;

figure 2.7 Etat de danger non réversible

2.4.3 Elément de scénario d'accident

Définition

État accident *: Etat décrivant un accident, par un ensemble d'attributs, et des événements d'accidents générés.*

Nous avons décrit précédemment un état où il est possible sous l'occurrence d'un événement ou d'une condition d'aboutir à un état de danger. De cet état, il est alors possible d'atteindre un état d'accident. Cet état d'accident est composé d'une liste d'attributs, et de la possibilité de génération d'événements d'accidents, qui vont propager ce danger, soit en agissant sur une transition d'un élément de scénario, soit en modifiant une condition.

Un état de danger, une transition composée d'E/C, et un état d'accident permettent de décrire un élément de scénario d'accident (figure 2.8).

ST = (S, T, α, β)

$S = \{agro\ alimentaire\ et\ bactéries\ pathogènes, intoxication\};$

$T = \{t1\};$

$\alpha = t1 \rightarrow agroalimentaire\ et\ bactéries\ pathogènes;$

$\beta = t1 \rightarrow intoxication;$

ST avec étiquettes

$l1 = \emptyset$

$l2 = t1 \rightarrow présence\ de\ consommation;$

$l3 = evt\ accidentel$

$Prop = \{\emptyset\}$

$E = \{présence\ de\ consommation\};$

figure 2.8 Elément de scénario d'accident

2.4.4 Elément de scénario de post accident

Définition

***État post accident** : Liste des attributs décrivant l'état après l'enchaînement du scénario de danger.*

Nous venons de décrire l'enchaînement permettant d'aboutir à un accident, il faut maintenant être capable de décrire l'état auquel il est possible d'aboutir après la fin de l'accident. Par exemple, après la consommation d'un produit agroalimentaire contaminé par des bactéries pathogènes, il est possible d'avoir plusieurs post accidents à l'état d'accident intoxication :

- soit les bactéries ne sont pas très toxiques alors, l'état de post accident de la personne est malade.
- Soit les bactéries seront très virulentes et alors la personne peut décéder.
- L'état de post accident peut aussi dépendre d'un autre paramètre tel que la faiblesse de la personne qui consomme l'aliment contaminé.

Les états de post accidents (figure 2.9) nous permettent de décrire l'ensemble de ce qui peut se passer après l'apparition d'un état d'accident (suivant les cibles considérées). Un état d'accident, une transition et un état de post accident représentent un élément de scénario de post accident.

ST = (S, T, α, β)

$S = \{intoxication, malade\};$

$T = \{t1\};$

$\alpha = t1 \rightarrow intoxication;$

$\beta = t1 \rightarrow malade;$

ST avec étiquettes

$l1 = \emptyset$

$l2 = t1 \rightarrow présence\ personne\ forte;$

$l3 = evt\ post\ accidentel$

$Prop = \{\emptyset\}$

$E = \{présence\ personne\ forte\};$

figure 2.9 Element de scénario de post accident

2.4.5 Scénario de danger élémentaire

Un scénario de danger (figure 2.10) peut être construit à partir des trois éléments de scénarios, l'occurrence de danger, l'occurrence d'accident et l'occurrence de post accident. Un scénario de danger est suffisant pour décrire un enchaînement simple conduisant à un accident, mais il n'est pas suffisant pour construire un enchaînement, ni pour faire le lien avec l'installation réelle, pour cela nous devons ajouter d'autres éléments de scénarios.

Cette forme de la représentation de l'apparition d'un danger et la propagation par un accident, peut être décrite dans une librairie de scénarios Cette libraire sera constituée de tous les éléments de scénarios de type occurrence de danger, accident, post accident. Elle va nous permettre de décrire les scénarios de danger.

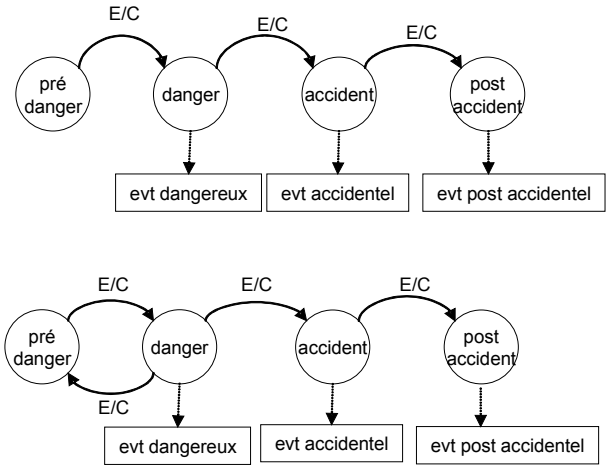


figure 2.10 Scénario de danger élémentaire

2.4.6 Les éléments de scénarios d'évolutions des attributs

Nous avons décrit les éléments de scénarios d'occurrence de danger, accident, de post accident, il existe d'autres éléments de scénarios nous permettant de construire un scénario de danger. Les éléments de scénarios d'évolution de l'attribut permettent de décrire le passage pour un attribut d'une de ces valeurs à une autre valeur (figure 2.11). Tous les attributs fonctionnels peuvent avoir une évolution il s'agit alors de la non réalisation d'une fonction, d'un dysfonctionnement ou d'une défaillance. Pour les attributs physiques, les scénarios d'évolution sont la modélisation d'une détérioration.

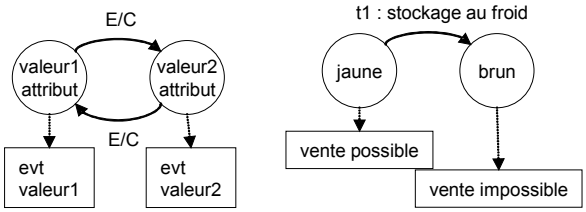


figure 2.11 Elément de scénario d'évolution des attributs

2.4.7 L'interface modèle de l'installation / modèle de danger

La correspondance modèle de l'installation réelle / modèle de danger représente l'interface entre l'installation physique réelle et le modèle de danger de l'installation, qui lui est générique. La figure 2.12 montre les correspondances physique / danger permettant de faire le lien entre le système physique et le modèle de danger de l'installation. Les correspondances danger / physique font le lien entre le modèle de l'installation et le système physique. L'installation est une représentation spécifique, alors que le modèle de danger est générique.

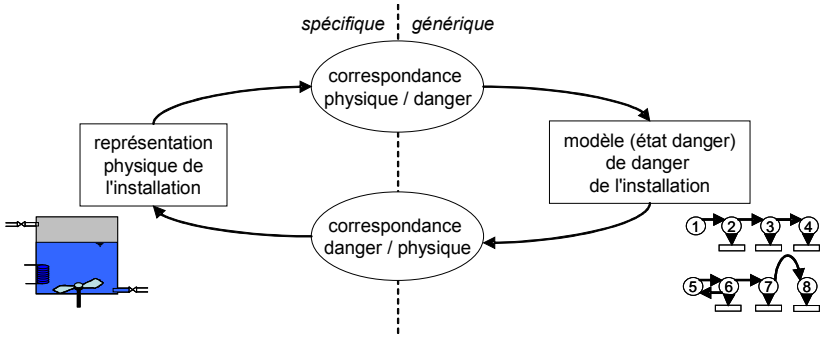


figure 2.12 Les interfaces spécifiques génériques

2.4.7.1 La correspondance physique / danger

Nous avons décrit dans le modèle de danger, une représentation des différents éléments de scénarios permettant de modéliser l'enchaînement conduisant à un accident. Cette modélisation est générique, et n'a aucun lien avec les composants du système réel. Les correspondances physique / danger (figure 2.13) décrivent quant à elles le lien entre un matériel et un attribut du modèle de danger. Il s'agit donc des interfaces d'entrées du modèle de danger. Les défauts ou défaillances matérielles sont spécifiques à l'installation étudiée alors que les attributs sont génériques et dépendent du modèle de danger. La recherche des correspondances physique / danger peut être réalisée à partir d'une analyse AMDEC.

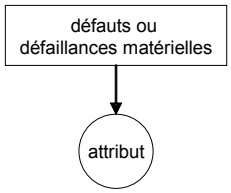


figure 2.13 Correspondance physique / danger

2.4.7.2 La correspondance danger / physique

Les correspondances danger / physique permettent d'apporter des informations sur les défaillances spécifiques qui peuvent être à l'origine d'un changement d'attribut. Inversement, il faut aussi savoir quels peuvent être les effets d'un accident sur le système réel. Ces effets possibles sont représentés sous la forme de correspondances danger / physique (voir figure 2.14). Ces éléments d'interfaces sont dépendants de l'installation étudiée, ils dépendent de la technologie utilisée, ainsi que de l'analyse réalisée. Les attributs sont génériques, alors que les effets et dommages sont spécifiques à l'installation que l'on étudie.

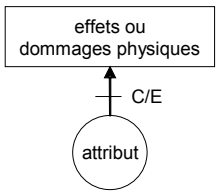


figure 2.14 Correspondance danger / physique

La figure 2.18 représente la méthode ScénaRisK dans son ensemble, l'état permettant l'utilisation de la base des connaissances à partir de la description de l'installation, sous la forme de liste d'attributs permettant la représentation d'états. Les correspondances physique / danger et danger / physique sont un concept important nous permettant d'utiliser des modèles génériques.

A ce stade de la description, nous pouvons rechercher les scénarios de danger décrits dans le modèle de danger qui peuvent s'appliquer à l'installation. L'analyse consiste à définir les liens entre le modèle de l'installation et les ensembles décrits dans le modèle de danger par un ensemble d'attributs.

Ceci n'étant valable que pour les états de pré dangers. Les états de danger peuvent ne pas être inclus dans l'ensemble de départ. Le lien est alors réalisé par les interfaces (correspondance physique / danger et correspondance danger / physique).

2.5 Construction du modèle de danger à partir du modèle structurel et fonctionnel

2.5.1 Introduction

Dans cette partie, nous allons présenter la construction d'une modélisation spécifique de l'installation, permettant l'utilisation de la base de connaissances. Nous avons construit les éléments de scénarios de danger à partir d'une représentation des attributs. Ces attributs permettent de décrire les états qui pour certains peuvent être des départs de pré-danger des scénarios de danger. Dans la suite, nous allons décrire dans un premier temps le découpage possible de l'installation, que nous appellerons description structurelle. Ensuite, nous décrirons la description fonctionnelle permettant la description des fonctions que doit réaliser l'installation.

L'ensemble des attributs pour le modèle de l'installation permet ensuite d'utiliser le modèle de danger.

2.5.2 Description structurelle

La description structurelle est une représentation spécifique de l'installation, pour cela, il faut procéder à un découpage de l'installation. Ce découpage est réalisé en entités et constituants, suivant les parties de l'installation que l'on souhaite analyser. Seulement deux niveaux ont été retenus pour retirer la complexité. Cette description, permettra de déterminer les attributs physiques de l'installation.

Une entité est un groupe de matériels physiques issu du découpage de l'installation. Il est possible de définir pour chaque entité une liste d'attributs globaux physiques. Cette liste d'attributs concerne toute l'entité. Par exemple, une entité décrivant un produit "lait" peut être caractérisée par l'attribut "agroalimentaire".

Définition

*Une **entité** (figure 2.15) permet la modélisation d'un ensemble d'éléments physiques, il est possible de découper une entité en constituants. Un constituant est caractérisé à partir d'une liste d'attributs physiques.*

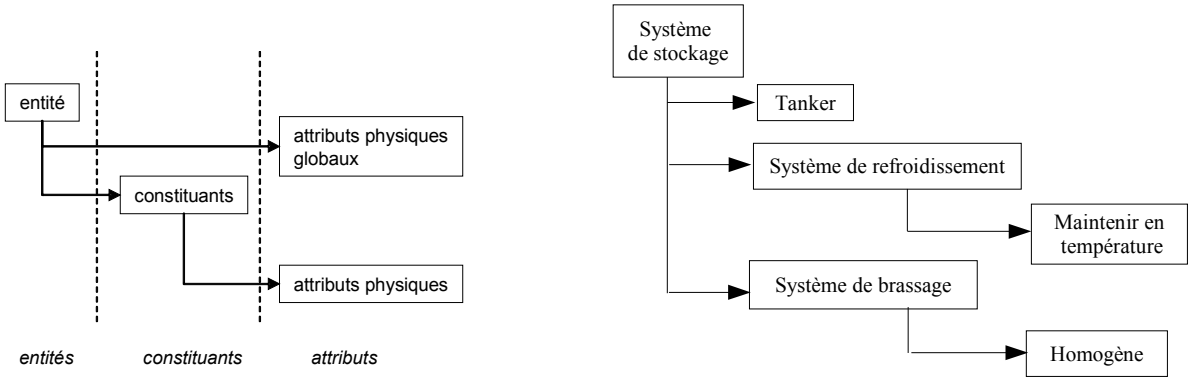


figure 2.15 Description structurelle d'une entité

Les entités sont décrites par un ensemble constitué d'attributs physiques globaux et d'attributs physiques issus des constituants qui la composent.

2.5.3 Description fonctionnelle

La description fonctionnelle permet de décrire l'ensemble des fonctions que doit réaliser l'installation. Pour cela, nous avons identifié deux types de fonctions :

- Les fonctions statiques,
- Les fonctions dynamiques.

2.5.3.1 Les fonctions statiques

Définition

*Une **fonction statique** représente une fonction valable pour une entité quel que soit l'état de l'entité, elle n'est pas décomposable en phases de fonctionnement. (exemple: étanche, résister à la pression)*

***Entité liée :** Une entité A est liée à une autre entité B pour une fonction statique donnée, quand les changements d'attributs d'une entité A liée à la fonction statique vont obligatoirement modifier l'attribut de l'entité B.*

Une fonction statique (figure 2.16) représente une fonction valable pour une entité quelque soit l'état de l'entité, elle n'est pas décomposable en phases de fonctionnement (ex: étanche, résister à la pression), elle représente une aide pour la recherche des attributs de l'installation. Pour chaque fonction statique, il faut répertorier la liste des entités, et des constituants qui interviennent dans la réalisation de cette fonction. Pour les entités, il faut aussi ajouter les entités liées.

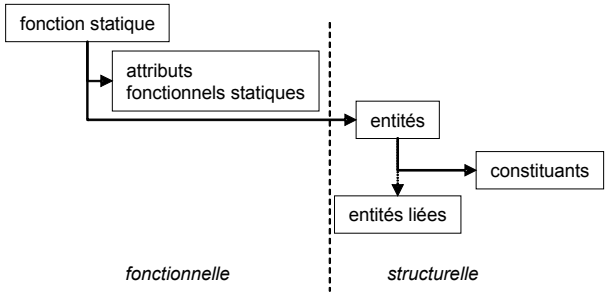


figure 2.16 Fonction statique

2.5.3.2 Les fonctions dynamiques

Définition

*Une **fonction dynamique** représente une réalisation décomposable en phases de fonctionnement, faisant intervenir des constituants de l'entité.*

Une fonction dynamique représente une réalisation décomposable en phases de fonctionnement (figure 2.17), faisant intervenir des constituants de l'entité. Une phase de fonctionnement décrit une étape permettant de réaliser une fonction. Une phase de fonctionnement est décrite par une liste d'entités, et par les constituants de l'entité intervenant dans la réalisation de la phase de fonctionnement.

Définition

*Une **entité de proximité** est une entité se trouvant dans le champ (proximité physique) d'une autre entité. Les événements générés par une entité de proximité vont être pris en compte dans la génération des scénarios comme faisant partie de la phase de fonctionnement considérée.*

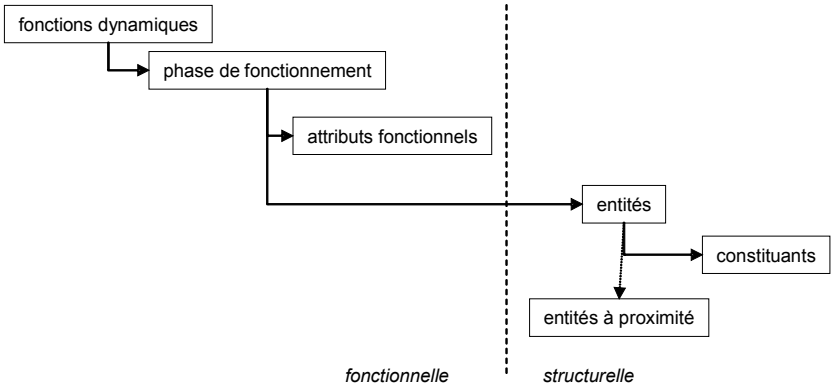


figure 2.17 Fonction dynamique

2.5.4 Synthèse de la méthode

La méthode ScénaRisK permet d'obtenir des scénarios de danger à partir de la description d'une installation physique et d'une base de connaissances. La figure 2.18 présente la méthode ScénaRisK. A partir d'une installation physique réelle, nous réalisons une description de l'installation. Cette description est décomposée en deux parties

- une description structurelle décrivant les éléments physiques qui composent l'installation. La description structurelle est composée d'une description structurelle générique.décrite dans la base de connaissances et d'une description structurelle spécifique, qui ne dépend que de l'installation et n'est pas décrite dans la base de connaissances.
- une description fonctionnelle décrit les différentes fonctions que doit réaliser l'installation.

A partir de cette description structurelle et fonctionnelle, nous pouvons en déduire les états potentiellement dangereux de l'installation. Grâce à ces différents états, et à la base de connaissances, nous pouvons alors déduire les scénarios de danger possibles de l'installation. La modélisation physique de l'installation représente l'installation sous forme de schéma d'ensemble ou chaque élément est représenté par un nom, il s'agit d'une modélisation fidèle de l'installation physique.

1. A partir de l'installation physique, nous construisons la description générique d'une base de connaissances générique utilisant des éléments génériques.

2. Le lien entre les éléments génériques et l'installation réelle physique est réalisé par une liste de correspondances avec la description spécifique.

3. Si des éléments de l'installation physique ne se trouvent pas dans la description générique, il faut alors réaliser une description structurelle spécifique.

4. Pour que la modélisation de l'installation soit complète il faut réaliser à partir de l'installation physique une description fonctionnelle générique.

5. A partir de la modélisation structurelle et fonctionnelle, nous pouvons générer l'état de

l'installation à un instant donné. De cet état et de la base de connaissances, nous pouvons en déduire la liste des événements et des propriétés qui seront utilisés.

6. L'état permet de déduire les scénarios de dangers à partir de la base de connaissances.

7. L'état de l'installation permet de déterminer la liste des scénarios d'évolution des attributs.

8. Pour déterminer les scénarios de dangers nous avons besoin de la liste des événements et de l'état de l'installation.

9. Les scénarios de danger déterminés influencent la liste des événements et des attributs.

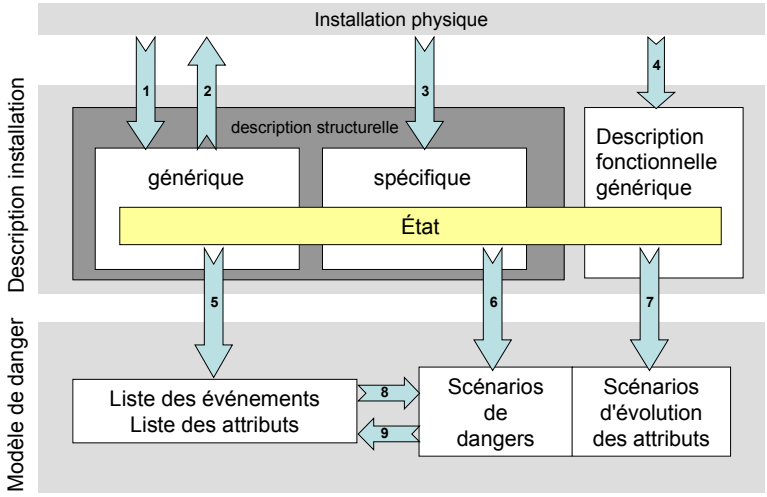


figure 2.18 Détail de la méthode ScénaRisK

2.6 Les étapes d'utilisation de ScénaRisK

2.6.1 Introduction

La création du modèle de danger a été motivée par une simplification de représentation classique sous la forme d'états normaux, anormaux. Cette représentation ne permet pas de construire un modèle utilisable dans l'industrie, et possède beaucoup d'informations dont nous n'avons aucune utilité pour notre étude. Nous avons dû, de ce fait, la simplifier en utilisant les attributs qualitatifs. Le modèle de l'installation est une représentation de l'installation sous une forme structurelle et fonctionnelle, utilisable pour déterminer la liste des attributs physiques ou de dysfonctionnement. Nous allons maintenant décrire les différentes étapes pour réaliser une analyse des risques basée sur la méthode ScénaRisK. La mise en oeuvre de la méthode est décomposée en 5 étapes principales :

- étape 1. description structurelle de l'installation
- étape 2. description fonctionnelle de l'installation
- étape 3. construction des scénarios d'interfaces

- étape 4. recherche des états de pré-dangers
- étape 5. recherche des enchaînements de scénarios

Dans cette partie, nous allons décrire chacune des différentes étapes, illustrées par un exemple simple, constituées d'un conteneur de produit agroalimentaire, dans notre cas du lait et nous allons réaliser l'analyse en fonction des risques suivants : le risque électrique et le risque bactériologique.

2.6.2 Exemple

L'exemple de la figure 2.19 que nous utilisons pour décrire les différentes étapes de la méthode est composé :

- d'un conteneur conçu pour conserver des produits alimentaires
- d'un système de remplissage avec vannes et tuyaux
- d'un système de vidange avec vannes et tuyaux
- d'un camion prévu pour le transport du produit
- un produit agroalimentaire : du lait

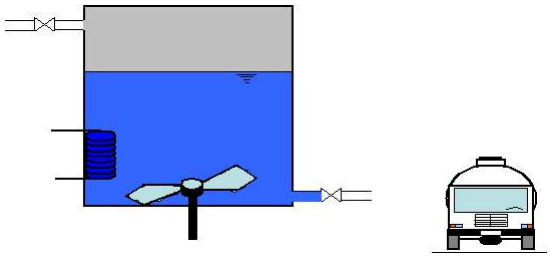


figure 2.19 Exemple : agroalimentaire

2.6.3 Etape 1. description structurelle de l'installation

Dans cette première étape, nous devons procéder à un découpage arbitraire de l'installation en entités et constituants. Pour chaque entité il faut donner la liste des attributs physiques globaux, et pour chaque constituant, il faut rechercher la liste des attributs physiques.

Liste des entités issues du découpage arbitraire de l'installation.

1. Système de stockage
2. Produit (lait)
3. Produit nettoyage
4. Eau de rinçage

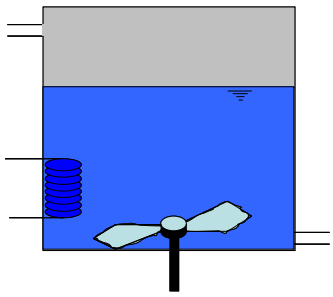
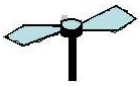
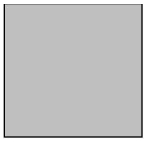


figure 2.20 Exemple : le système de stockage

Nous nous intéresserons dans notre exemple principalement au système de stockage. Le système de stockage est composé des constituants suivants : système de refroidissement, système de brassage, tanker. Le symbole A est utilisé pour repérer un attribut.

système de stockage	
	système de refroidissement A maintient en température A électrique
	système de brassage A homogène A électrique
	tanker A étanche

Les différents systèmes et sous systèmes sont décrits en fonction des attributs qui le composent. Il nous faut maintenant construire la liste des fonctions ainsi que la liste des entités et des constituants intervenant dans chacune de ces fonctions.

2.6.4 Etape 2. description fonctionnelle de l'installation

Dans un premier temps, nous allons rechercher les fonctions statiques, puis les fonctions dynamiques de l'installation.

2.6.4.1 Fonctions statiques

Dans notre exemple, nous allons fournir la liste des fonctions statiques figure 2.21 et la liste

des entités, permettant d'assurer la fonction. Si tous les constituants d'une entité possèdent un attribut statique alors, il ne faut indiquer que le nom de l'entité. Sinon, si un seul constituant ne possède pas l'attribut statique, l'entité ne possède pas l'attribut statique. Dans ce cas, seulement un ou plusieurs constituants de l'entité possède l'attribut statique.

fonctions statiques	attributs (valeur)	entités	constituants
étanche	est étanche	système de stockage système de brassage système de refroidissement	tanker
stérile	est stérile	système de stockage système de brassage système de refroidissement	
température constante	maintien en température	système de stockage	système de refroidissement
mélange homogène	homogène	système de stockage	système de brassage

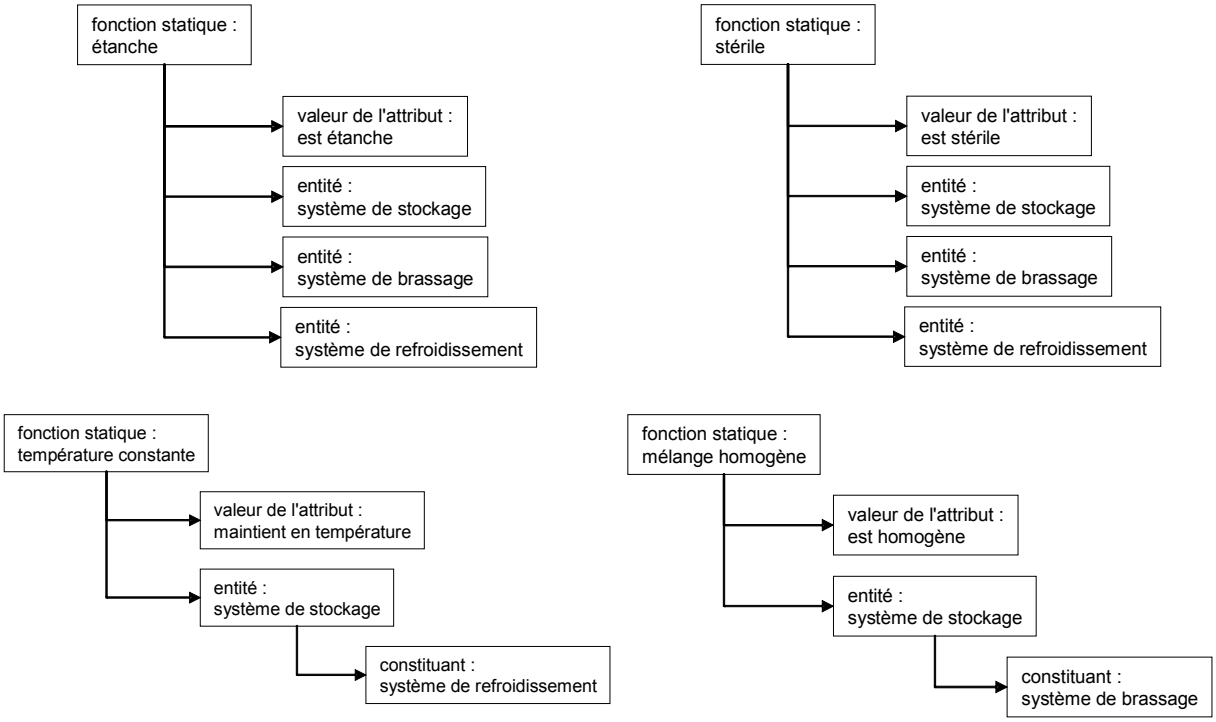


figure 2.21 Exemple : liste des fonctions statiques

Pour chacun des attributs, nous devons décrire les éléments de scénarios d'évolution des attributs, ceci correspond à la modélisation du comportement de l'installation. Pour les attributs fonctionnels, les éléments de scénarios d'évolution des attributs sont les suivants :

attribut (valeurs)	événements ou conditions	attribut(valeurs)
stérile	Présence de bactéries pathogènes	non stérile
maintient en température	Présence défauts système de refroidissement	non maintient en température
homogène	Présence défauts système de brassage	non homogène
étanche	Présence de choc	fuite présente

Cette représentation graphique correspond à la figure 2.11 et permet une évolution de la valeur des attributs.

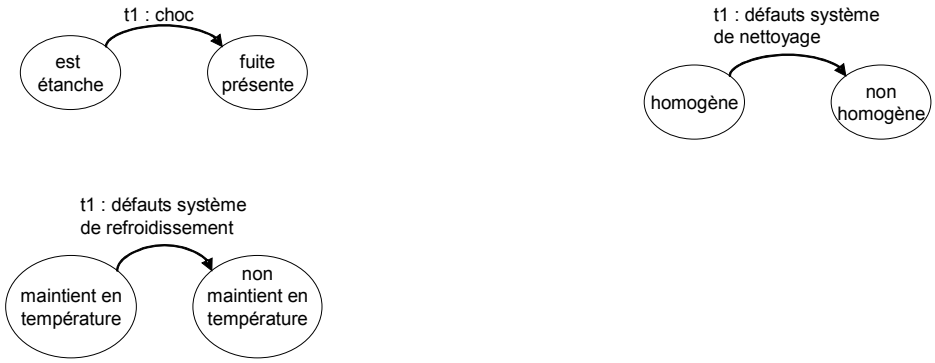


figure 2.22 Exemple : évolution des valeurs des attributs

2.6.4.2 Fonctions dynamiques

Les fonctions dynamiques décrivent ce que doit faire l'installation, sous la forme de phases de fonctionnement, chaque phase peut être réalisée de façon séquentielle, ou en parallèle, ceci est déterminé par les phases de fonctionnement. Non donnons ici la liste des fonctions, la liste des phases de fonctionnement (figure 2.23) qui permettent la réalisation de la fonction, ainsi que les étapes dans lesquelles peuvent être réalisées les différentes phases.

fonction dynamique	phases de fonctionnement	attributs fonctionnels	numéro étape	entités	constituants
cycle d'utilisation	stockage	non vide	1	système de stockage produit agroalimentaire	tanker
	nettoyage	non vide	2	système de stockage produit nettoyage	tanker système de brassage
	rinçage	Non vide	3	système de stockage eau	tanker système de brassage

Pour chaque fonction dynamique, nous recherchons la liste des phases de fonctionnement (figure 2.23) nécessaire pour réaliser la fonction, ici pour le cycle d'utilisation, nous décrivons trois phases de fonctionnement : une phase de stockage, une phase de nettoyage, et une phase de

rinçage. Pour chacune de ces phases, nous donnons le rang de la phase pour une utilisation séquentielle. Les phases ayant le même numéro sont des phases en parallèle. Enfin, nous décrivons les entités et les constituants qui permettent la réalisation de la phase de fonctionnement (figure 2.24, figure 2.25, figure 2.26).

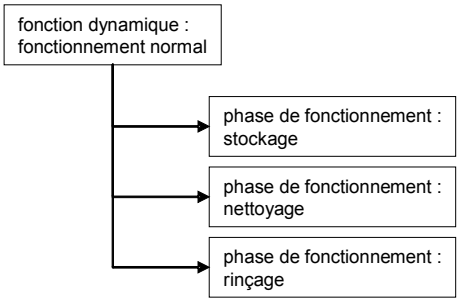


figure 2.23 Exemple : liste des fonctions dynamiques

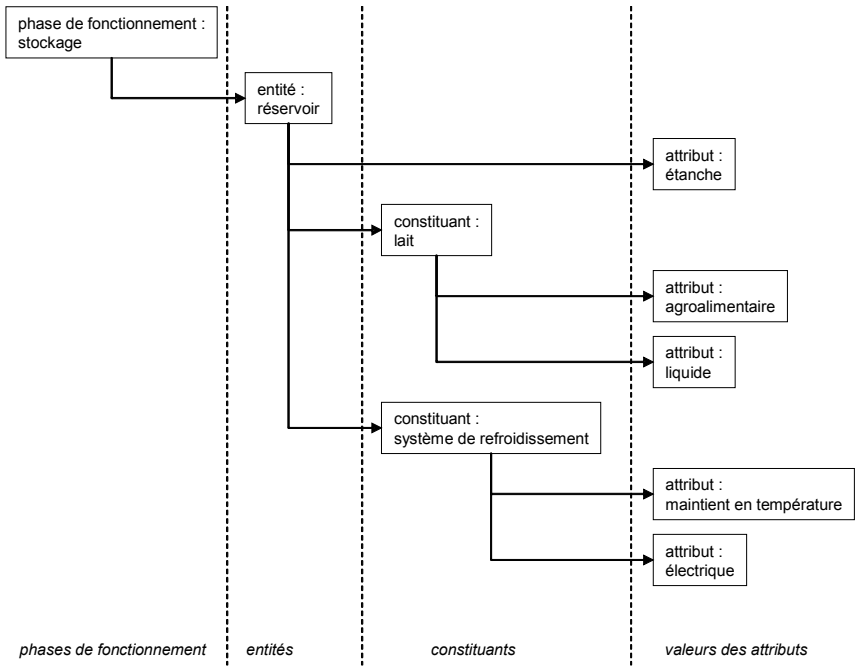


figure 2.24 Exemple : détail de la phase de fonctionnement stockage

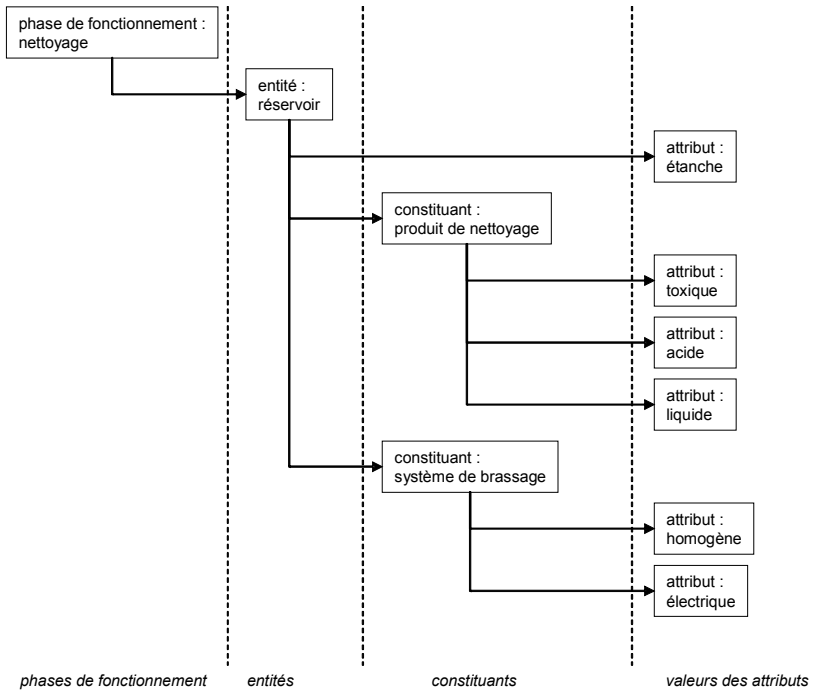


figure 2.25 Exemple : détail de la phase de fonctionnement nettoyage

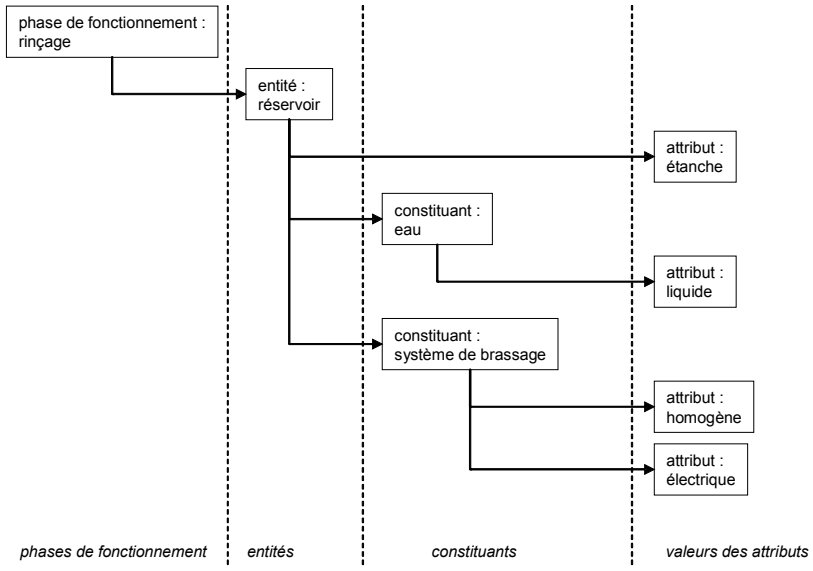


figure 2.26 Exemple : détail de la phase de fonctionnement rinçage

Dans cet exemple, nous voyons que pour chacune des phases, nous allons pouvoir en déduire l'état, qui est constitué de l'ensemble des attributs physiques et fonctionnels. Nous remarquons que sur la forme graphique, la liste des attributs qui interviennent pour chacune des phases de fonctionnement est simple à déterminer, il s'agit de la "feuille" des branches de l'arbre. Nous allons maintenant détailler la liste des attributs qualitatifs par phase de fonctionnement.

Pour la phase de stockage	Pour la phase de nettoyage	Pour la phase de rinçage
A étanche	A étanche	A étanche
A agroalimentaire	A acide	A liquide
A électricité	A toxique	A homogène
A liquide	A liquide	
A homogène	A homogène	
A maintien en température		

Nous avons déduit pour chacune des phases précédentes la liste des attributs définissant l'état de l'installation dans une phase de fonctionnement donnée. Par la suite, nous allons rechercher tous les départs de scénarios possibles à partir de ces différentes phases, la liste des attributs constitue les clefs permettant de déterminer les départs de scénarios.

2.6.5 Construction de la base de connaissances

Pour réaliser une analyse de risques à partir de la méthode ScénaRisK, il faut au préalable avoir construit une librairie de scénarios à partir d'une liste d'attributs pré-définie. C'est sur cette liste d'attributs que va s'appuyer la recherche des états de pré-dangers. L'ensemble des éléments de ce paragraphe est pré défini et constitue notre base des connaissances.

A partir d'une description de l'installation, des schémas fonctionnels, structurels, et des différents plans existants ou disponibles, il faut rechercher les attributs qualitatifs (liste non exhaustive) fonctionnels et physiques, qui sont présents dans le fonctionnement de l'installation. Cette recherche se fait à partir de la liste des attributs qualitatifs existants, mais si un attribut n'existe pas dans la base des connaissances, il faut l'ajouter et en donner une description.

Pour chaque nouvel attribut, et pour les combinaisons d'attributs existants, il faut rechercher l'ensemble des scénarios possibles. Si un ou plusieurs scénarios ne sont pas dans la librairie des scénarios existants, on les ajoute. Cette approche permet une capitalisation de la connaissance. Les attributs représentent les clefs qui vont permettre de faire le lien entre la base des connaissances et la description spécifique de l'installation.

Dans cette base de connaissances, nous retrouvons l'ensemble des éléments de scénarios de dangers, d'accidents et de post accidents, qui vont nous permettre de construire les scénarios de danger.

Pour l'exemple de la figure 2.19, la liste des attributs que nous pouvons déterminer par une première approche de l'exemple peut être la suivante.

Les attributs sont représentés par le nom de l'attribut puis une liste de valeurs si celles-ci sont présentes. Par exemple l'attribut électricité peut avoir deux valeurs utilisation d'électricité et non utilisation d'électricité. Un état possédant l'attribut électricité est décrit par une des valeur de l'attribut électricité.

La liste des attributs physiques :

- électricité : contient les valeurs {utilisation électricité, non utilisation électricité, ?}
- alimentaire : contient les valeurs {agroalimentaire, non agroalimentaire, ?}

La liste des attributs fonctionnels :

- étanche contient les valeurs {est étanche, fuite présente, ?}
- hygiène contient les valeurs {stérile, non stérile, ?}
- homogène contient les valeurs{homogène, non homogène, ?}
- température constante contient les valeurs {maintient température, non maintient en température, ?}

Pour chacun des attributs de la liste précédente, nous devons rechercher toutes les combinaisons des attributs possibles, et vérifier si ces combinaisons sont des états de pré-dangers possibles.

Pour construire les éléments de scénarios nous partons de la liste des états composés à la liste de tous les états possibles. A partir de la liste des valeurs des attributs, nous ne conservons que les états potentiellement à risque.

- agroalimentaire
- agroalimentaire et non stérile
- agroalimentaire et non homogène
- agroalimentaire et non maintien en température
- utilisation électricité et fuite.

Pour permettre la construction de scénarios de dangers, il faut ajouter des attributs qualitatifs génériques dépendant du secteur étudié (répartie en collection), dans notre exemple il faut ajouter la contamination du produit liée au secteur agroalimentaire, les court-circuits liés à l'électricité et le facteur humain.

La collection générique alimentaire utilise les attributs suivants :

- contamination contient les valeurs {bactéries pathogènes, pas de bactéries pathogènes,?}.

La collection générique électrique possède les attributs de dangers génériques suivants :

- court circuit contient les valeurs {court circuit, ?}.

La collection générique humain possède des attributs de dangers génériques suivants :

- contact contient les valeurs {en contact, ?}
- consommation contient les valeurs {en consommation, ?}
- forme physique contient les valeurs {faiblesse, forte, ?}

Le tableau suivant représente un exemple de la liste des éléments de scénarios de danger existants pour la figure 2.19 ainsi que la liste des événements de dangers générés sous la forme de la figure 2.27.

Remarque : la forme "=1" des tableaux représente un événement toujours vrai.

Liste des valeurs des attributs de l'état de pré-danger	Liste des événements et des conditions de la transition	Liste des valeurs des attributs de l'état de danger	Liste des événements générés par l'état de danger
Agroalimentaire	Présence bactéries pathogènes	Agroalimentaire et bactéries pathogènes	Présence contamination
Agroalimentaire	Présence contact / contamination	Agroalimentaire et non stérile	Présence bactéries pathogènes
Agroalimentaire	Présence non maintient en température	Dégradation produit	Présence bactéries pathogènes
Agroalimentaire	Présence non homogène	Dégradation produit	Présence bactéries pathogènes
Utilisation électricité et fuite	Présence dégradation conducteur	Court circuit	Présence de court circuit

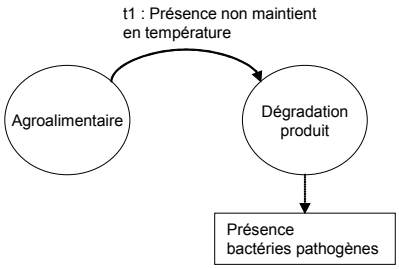


figure 2.27 Exemple : élément de scénario de danger

Le tableau suivant représente un exemple de la liste des éléments de scénarios d'accident existants pour la figure 2.19 ainsi que la liste des événements d'accidents générés (figure 2.28).

Liste des valeurs d'attributs de l'état de danger	Liste des événements et des conditions de la transition	Liste des valeurs des attributs de l'état d'accident	Liste des événements générés par l'état d'accident
Agroalimentaire et bactéries pathogènes	Présence consommation	Intoxication	Présence d'intoxication
Dégradation produit	Présence consommation	Intoxication	Présence intoxication
Court circuit	Présence contact	Électrisation	Présence électrisation

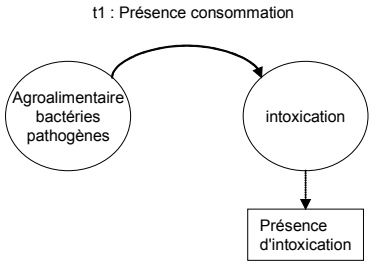


figure 2.28 Exemple : élément de scénario d'accident

Le tableau suivant représente un exemple de la liste des éléments de scénarios de post accident (figure 2.29) existants pour la figure 2.19.

Liste des valeurs des attributs de l'état d'accident	Liste des événements et des conditions de la transition	Liste des valeurs des attributs de l'état de post accident
Agroalimentaire et bactéries pathogènes	Personne faible	décès
Agroalimentaire et bactéries pathogènes	Personne forte	malade

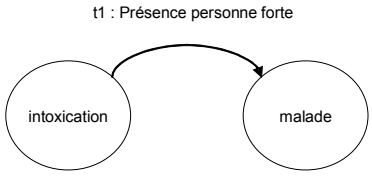


figure 2.29 Exemple : élément de scénario de post accident

Cette étude permet de déterminer les attributs, et de construire les éléments de scénarios qui vont nous permettre de réaliser une analyse des risques de l'installation. Il faut considérer que la librairie est déjà constituée de nombreux éléments de scénarios, chacun de ces éléments de scénario étant référencé par un ou plusieurs attributs. Nous remarquons que la liste des attributs qualitatifs possède beaucoup d'attributs qualitatifs de dangers génériques que nous retrouverons dans de nombreuses analyses. Il n'est donc pas nécessaire pour chaque analyse de détailler tous les attributs génériques ayant un rapport avec l'opérateur ou un domaine déjà étudié, ceci permet une réutilisation des connaissances de la base des connaissances.

2.6.6 Etape 3. Les scénarios d'interfaces

Dans ce paragraphe, nous allons construire les scénarios spécifiques pour l'exemple de la figure 2.17. Comme nous l'avons décrit précédemment, nous allons construire les interfaces,

nous permettant de déterminer les effets et les dommages probables à partir de l'évolution d'un scénario de danger. Ces éléments scénarios dépendent des choix techniques utilisés pour concevoir l'installation, ainsi que de l'utilisation qui en est faite.

Pour notre exemple, nous proposons les éléments de scénarios spécifiques suivants :

La correspondance physique / danger

Représentation du système réel			Représentation du système générique
Système réel	Événements ou conditions	Attributs	Événements générés
Système de brassage	Présence de rupture mécanique	Défauts système de brassage	Présence défauts du système de brassage
Système de refroidissement	Présence de rupture mécanique	Défauts système de refroidissement	Présence défauts du système de refroidissement

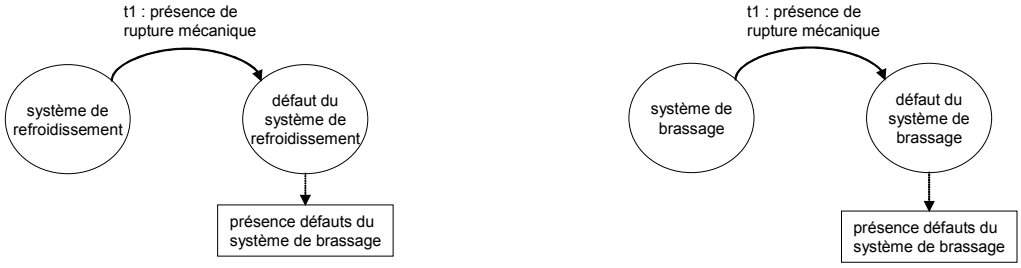


figure 2.30 Exemple : correspondance physique / danger

La correspondance danger / physique

Représentation du système générique		Représentation du système réel	
Attributs	Événements ou conditions	Système réel	Événements générés
Bactéries pathogènes	=1	Contamination du système de production	Arrêt de la production, blocage de la production

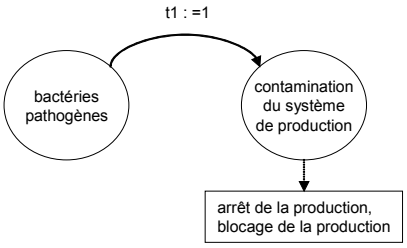


figure 2.31 Exemple : correspondance danger / physique

2.6.7 Etape 4. identification des états à risques

Le but de cette étape est de déterminer les états de pré-dangers possibles qui sont les états de départs possibles des scénarios de danger. Pour qu'un état soit un état de pré-danger, il faut pour chaque phase que ce soit :

- un état de pré-danger des scénarios de danger,
- un état d'un scénario d'évolution des attributs, car tous les changements de valeurs des attributs peuvent être un départ de scénario.
- un état d'une interface d'entrée ou de sortie, le départ de scénario est lié à une modification du système réel.

Pour chaque phase de fonctionnement (décrit à l'étape 2) nous devons rechercher la liste des attributs (état de la phase de fonctionnement) permettant de la définir.

Pour définir cet état, il faut faire le produit cartésien des attributs :

- statiques des entités et des constituants
- physiques des constituants
- physiques globales des entités
- fonctionnelles.

A partir de cet état, issu d'une description spécifique de l'installation, nous pouvons réaliser une analyse de risques et rechercher les scénarios de dangers possibles.

Pour la phase de fonctionnement stockage faisant intervenir l'entité unité de stockage la liste des attribut est l'union :

- des attributs issus de l'entité unité de stockage : {agroalimentaire, stérile},
- des attributs issus du constituant tanker {étanche},
- des attributs issus du système de refroidissement {électricité, maintient en température},
- des attributs issus du système de brassage {électricité, homogène}.

L'état décrivant la phase de fonctionnement stockage est constitué de la liste des attributs suivants : {agroalimentaire, stérile, électricité, maintient en température, homogène, étanche}.

A partir de la liste des attributs de la phase de fonctionnement stockage, il faut rechercher les états de pré-danger possibles issus de la base de connaissances. Pour qu'un état de pré-danger de la base soit un état de pré-danger de la phase de fonctionnement stockage, il faut que l'état de pré-danger soit inclus dans l'état définissant la phase de fonctionnement. Nous obtenons alors la liste des états de pré-danger suivant :

- système de brassage,
- système de refroidissement,
- agroalimentaire

La liste des états de pré-danger permet de déterminer la liste des départs de scénarios de danger possibles. La dernière étape de la méthode est la recherche des enchaînements de scénarios.

2.6.8 étape 5. recherche des enchaînements de scénarios

Dans les étapes précédentes, nous avons construit un modèle structurel et fonctionnel de l'installation, nous sommes capables de retrouver la liste des états de pré-danger possibles. La dernière étape consiste à rechercher l'ensemble des scénarios possibles pour chaque état de pré-danger, et à construire les interactions entre les différents éléments de scénarios (propagation des flux). Il faut pour cela réaliser une recherche de scénarios pour chacune des phases de fonctionnement. Pour les phases qui peuvent se produire en parallèle, il faut réaliser la propagation des flux, en fait, nous propageons la modélisation des flux ici les événements.

A partir de la librairie que nous avons détaillée dans l'étude préliminaire, nous pouvons obtenir les scénarios suivants pour notre exemple de la figure 2.11; il existe d'autres scénarios pour cet exemple, nous ne donnons ici qu'un seul enchaînement possible, avec notre librairie et la liste des attributs suivants {étanche, stérile, non vide, utilisation électricité, homogène, maintien en température, agroalimentaire}.

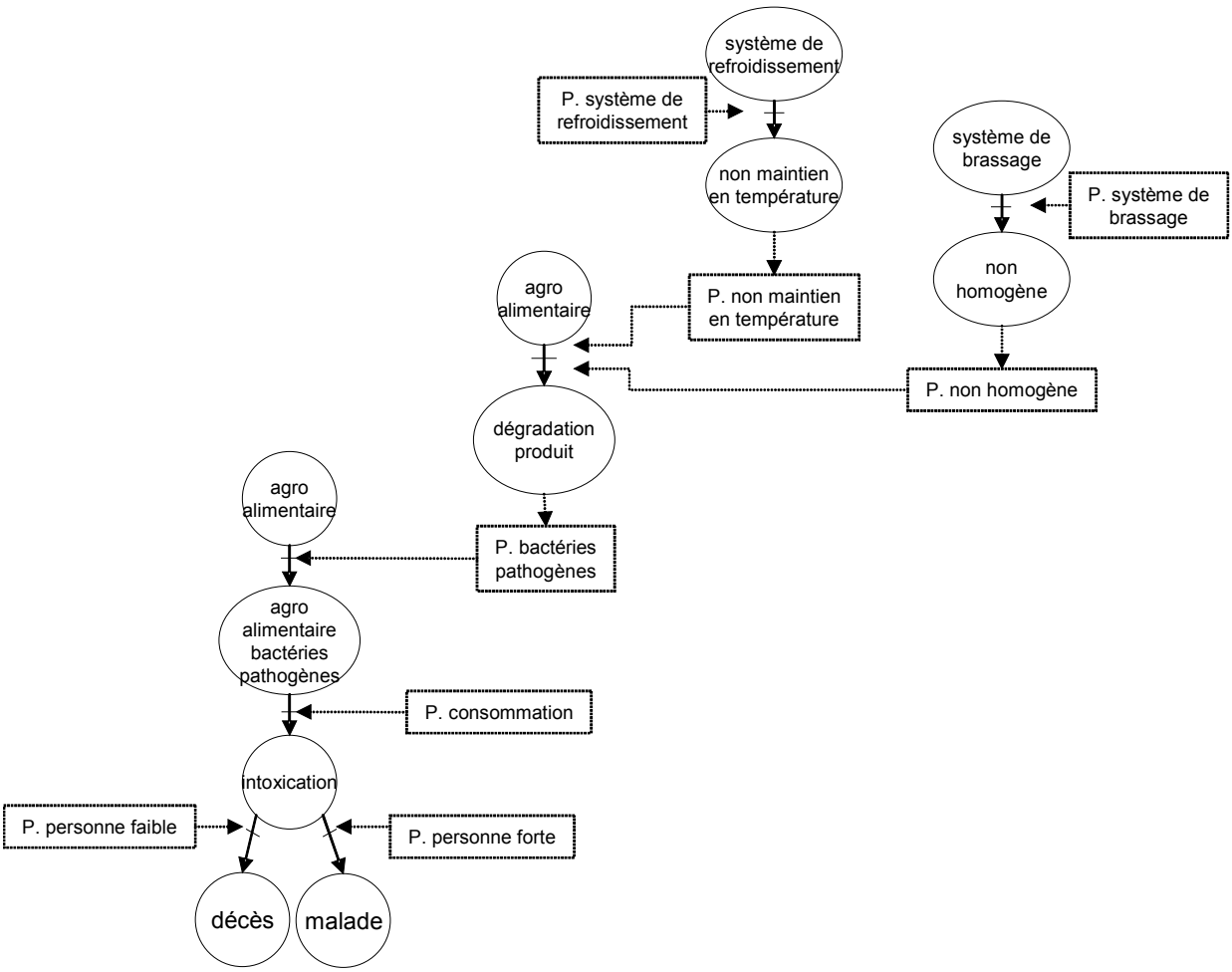


figure 2.32 Exemple : scénario de danger

La figure 2.32 donne un exemple de scénario de danger sous la forme d'un automate utilisant seulement les éléments que nous avons décrits dans la base de connaissances.

2.7 Aide à l'utilisation de la méthode

La méthode que nous venons de décrire s'appuie sur une base de connaissances. La première étape consiste à réaliser une base pour le domaine concerné, cette base doit être le plus générique possible en vue d'une réutilisation dans d'autres domaines que le domaine de départ.

Pour permettre une utilisation rapide de cette méthode, nous avons développé des outils informatiques. Le premier est une interface graphique permettant la saisie d'une base des connaissances à partir d'une interface graphique écrite en Java Server Pages (JSP). Cet outil permet d'obtenir la liste de tous les scénarios possibles contenus dans la base de connaissances. Cet outil n'a pu évoluer en même temps que la méthode car son architecture est trop rigide. Pour

cette raison, nous avons développé un deuxième outil moins ergonomique (sans interface graphique et en ligne de commande) mais plus évolutif.

Le deuxième outil n'utilise pas d'interface mais permet la description de l'installation et de la base de connaissances pour la recherche de scénarios pour chaque phase de fonctionnement de l'installation. Sa structure est basée sur des fichiers texte de type XML ce qui lui a permis d'évoluer rapidement en fonction des évolutions de la méthode. C'est sur ce dernier outil que les algorithmes de recherche de scénarios ont été testés.

2.8 Lien avec différentes méthodes d'analyse de risque

Dans ce paragraphe, nous allons décrire le lien entre les méthodes HAZOP, AMDEC, et MOSAR, et ce que peut leur apporter la méthode ScénaRisK.

2.8.1 HAZOP

La méthode HAZOP consiste à définir un certain nombre de points d'étude sur le système, à caractériser ces points par des variables d'état comme la pression ou la température, puis à appliquer des mots clefs prédéfinis pour obtenir la liste des déviations possibles pour ce point d'étude. On étudie ensuite les éventuels effets de cette déviation sur le fonctionnement et la sécurité et on recherche les causes.

La méthode HAZOP dans le cadre du modèle ScénaRisK correspond à l'analyse des variations des variables. En effet si une variable comporte un risque possible pour l'installation, elle va être décrite sous la forme d'un attribut. Les valeurs de l'attribut vont correspondre aux variations des mots clefs de la méthode HAZOP. Si la méthode ScénaRisK détermine des scénarios de danger avec comme états de pré-danger une variation d'une variable définissant l'installation, nous obtenons alors une partie des résultats que nous obtenons avec HAZOP. ScénaRisK apporte en plus les scénarios de danger possibles à partir de la variation de la variable.

2.8.2 AMDEC

La méthode AMDEC s'appuie sur une analyse des dysfonctionnements élément par élément. On commence d'abord par déterminer la liste des fonctions de l'entité considérée, puis on en déduit les dysfonctionnements possibles et les modes de défaillances associés. Ensuite, pour chaque cas, les effets sont évalués. S'ils présentent une certaine gravité, alors on analyse les causes possibles du dysfonctionnement. Les résultats sont regroupés dans un tableau. Il est alors possible de construire les scénarios de dangers.

Une des difficultés de l'analyse AMDEC est de savoir quelles causes retenir parmi la chaîne de causalité. La même question se pose pour les effets.

Le formalisme ScénaRisk permet de construire la liste des défaillances et dysfonctionnements à l'origine des départs de scénarios, grâce aux interfaces, correspondance physique / danger et danger / physique, nous pouvons lister les modes de défaillances pouvant conduire à un scénario de danger mais la liste n'est pas exhaustive. Il est alors possible de générer de façon automatisée les scénarios de danger liés aux défaillances de l'installation.

2.8.3 MOSAR

La méthode MOSAR s'appuie sur une modélisation MADS pour construire une liste des sources de danger et un graphe représentant les scénarios. Chaque entité est analysée par rapport à une grille de sources de danger générique et on construit un modèle boîte noire comportant en entrée les événements indésirables pouvant déclencher l'accident lié au risque analysé et en sortie les événements générés par cet accident. MOSAR est donc facile à interpréter dans le cadre du formalisme ScénaRisK, car nous obtenons une liste de scénarios de danger qui peuvent ensuite être étudiés suivant la phase A de MOSAR; pour la phase B l'utilisation de l'AMDEC peut être exprimée avec le formalisme ScénaRisK. La méthode ScénaRisK est un complément à la méthode MADS/MOSAR, permettant la structuration des scénarios qui peuvent ensuite être analysés.

Chapitre 3

Exemple d'application

Un grand nombre de procédés industriels a pour objectif de transformer de la matière. C'est le cas en chimie, pharmacie, agroalimentaire, etc. Cette transformation peut être réalisée de façon continue ou discontinue. Dans le premier cas, un flux constant de différentes matières entre dans le procédé et est transformé. Dans le deuxième cas, on parle de procédés batch ou par lots, car la matière est traitée par lots en suivant une recette, à la manière d'une recette de cuisine. Les procédés batch sont de plus en plus présents dans ce type d'industrie de par leur très grande flexibilité qui permet de produire plusieurs types de produits en petites quantités avec le même équipement. Nous verrons que ce mode de production est de nature hybride car la matière subit une série d'opérations de transformation continue (mélange, chauffage, réaction chimique, etc.) et chemine par lots de quantité finie dans le système de production en suivant de façon séquentielle une recette. Cette classe de systèmes que l'on appelle systèmes dynamiques hybrides sera étudiée plus en détail au paragraphe suivant.

La description complète des différents aspects des procédés de transformation nécessite différents types d'informations. Dans ce travail, nous avons attaché un soin particulier à l'identification de ces différents aspects, car ils représentent les éléments de base d'un modèle de type déclaratif du procédé.

Cet inventaire est illustré sur un procédé industriel de polycondensation [Thevenon 2001] [Flaus 2000] et qui nous sert de cas d'étude. C'est un atelier de production discontinu de polyamide 66, composé de 3 lignes de fabrication correspondants à différentes qualités de polyamide. Chaque ligne comprend un évaporateur, 2 autoclaves, une plate-forme de granulation et une trémie mélangeuse. Nous nous intéressons ici à la partie évaporation de ce procédé. En effet, cette partie est suffisamment complexe (en terme de nombres d'unités et de diversités des

phénomènes) pour illustrer les principaux aspects d’un procédé batch, et montrer l’intérêt de notre approche.

3.1 Présentation et caractéristiques du procédé industriel

3.1.1 Introduction

Dans ce paragraphe, nous allons présenter l'exemple qui va nous servir pour décrire la méthode développée pour les procédés agro alimentaire et qui peut aussi être appliquée aux systèmes chimiques. Nous allons d'abord présenter le procédé, puis nous suivrons les cinq étapes de la méthode permettant d'obtenir les scénarios de dangers possibles.

3.1.2 La description des appareils

La topologie du procédé est décrite par un schéma TI (Tuyauterie-Instrumentation). Outre l’interconnexion des équipements composant le procédé, ce schéma définit également les actionneurs et les instruments qui agissent sur le procédé. On distingue deux types d’instruments, les organes de mesure (capteurs, alarmes et sécurités, analyseurs) et les organes commandés (vannes, moteurs) qui sont représentés par un cercle relié à un trait et à la tuyauterie ou à l'appareil. Afin de faciliter la réutilisation et la lecture de ces schémas, un système de symbolisation graphique des instruments a été créé. Nous ne décrirons ici que les principes de bases et les principaux éléments graphiques utilisés par la suite. Pour de plus amples détails, on pourra se reporter au standard [ANSI/ISA-5.1, 1992] [ANSI/ISA-88.01, 1995].

Tous ces éléments représentent les conteneurs de l'installation. Lorsqu'on écrit le modèle d'un procédé, il apparaît rarement explicitement et indépendamment. En général, toute cette information est cachée dans la partie du modèle qui décrit la transformation de la matière. Cependant, si on cherche à modéliser un atelier batch ou flexible, souvent rencontré en agroalimentaire, et dans lequel un même appareil peut être utilisé pour plusieurs transformations, on gagnera en généralité en faisant apparaître le modèle des équipements. Celui-ci peut même être requis lorsqu'on s'intéresse à des aspects comme la traçabilité ou l'analyse de sécurité de l'installation.

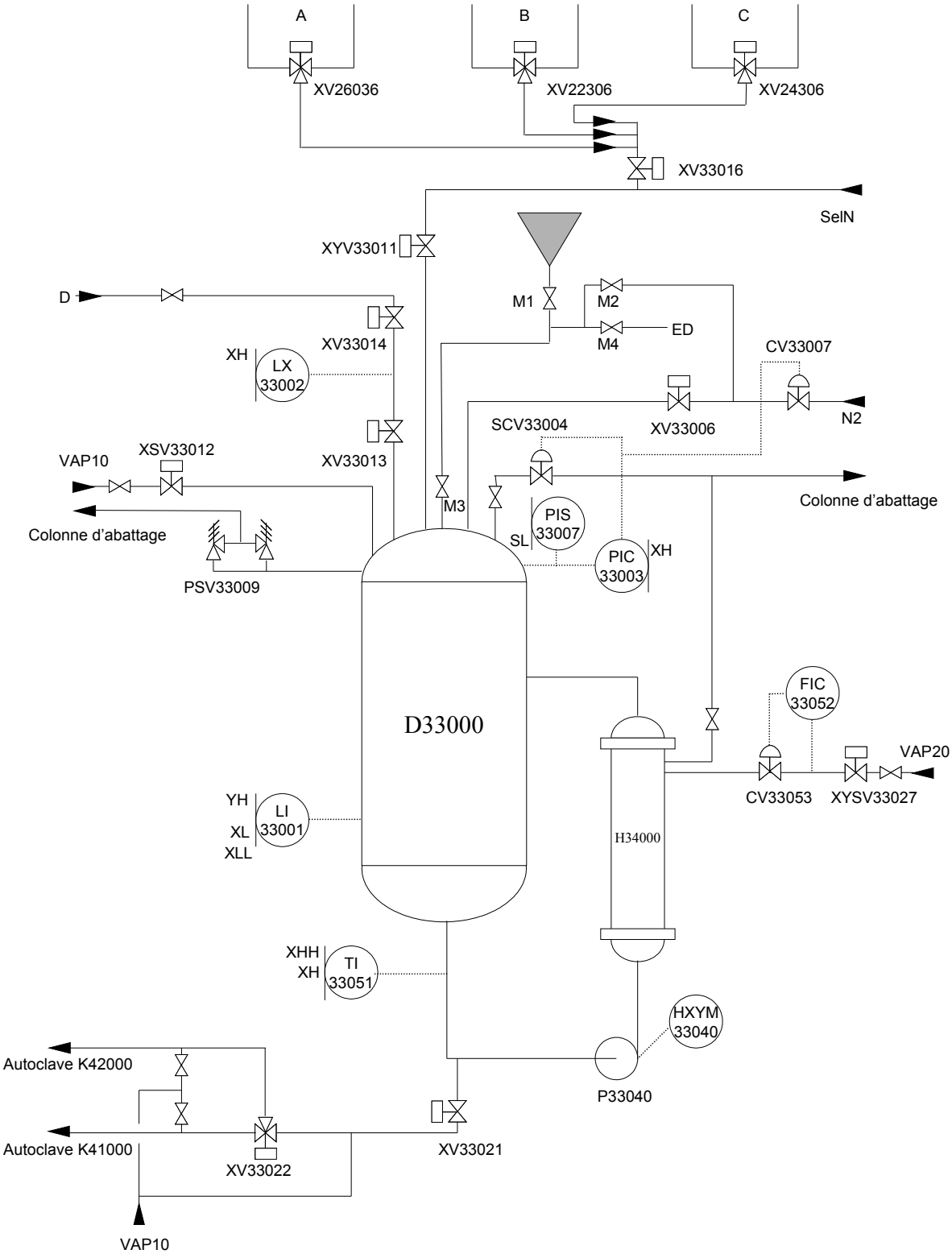


figure 3.1 Procédé industriel d'évaporation

Le schéma TI du procédé d'évaporation est représenté Figure 2.2.1. Il est composé de:

- l'évaporateur (D33000),
- un échangeur de chaleur (H34000),
- une ligne d'alimentation en sel N,
- quatre lignes d'alimentation pour les adjuvants (A, B, C et D),
- une pompe de re-circulation (P33040),
- quatre vannes 3-voies (XV26036, XV22306, XV24306, XV33022),
- trois vannes de régulation (CV33053, SCV33004, CV33007),
- huit vannes on/off,
- six capteurs principaux,
- plusieurs mécanismes de sécurité (un dans le système de sécurité, et un pour l'alimentation manuelle),
- un grand nombre de tuyaux et de systèmes de nettoyage.

Le but du procédé d'évaporation est de concentrer le sel N ainsi qu'un certain nombre d'adjuvants de 52 à 80% par évaporation d'eau. L'évaporateur fonctionne en régulation de pression, grâce aux vannes proportionnelles CV33007 et SCV33004. La température masse est la principale indication de l'état d'évolution du produit et déclenche les changements de phase. La chauffe du produit est assurée par l'échangeur de chaleur qui est muni d'une régulation du débit vapeur (vanne proportionnelle CV33053).

3.1.3 Le mode opératoire

Le mode opératoire du procédé décrit le mode de fabrication d'un produit. On peut distinguer d'une part la recette de fabrication, et d'autre part les procédures opérateur regroupant les actions manuelles requises pour la conduite ou en cas de fonctionnement anormal.

La façon de décrire une recette dans le cas d'un procédé batch a été normalisée. Elle représente le mode de marche normale automatique. Une recette fournit un moyen de décrire les produits et comment ces produits sont fabriqués. Elle ne contient pas de contrôle direct des équipements, mais des ordres orientés procédé. Une recette peut être interrompue par le déclenchement d'une sécurité, ou une commande manuelle provenant de l'opérateur. Elle est décrite par un formalisme séquentiel comme le GRAFCET.

La recette de fabrication du procédé d'évaporation est composée de six phases principales consécutives (figure 3.2).

PHASE 0 : ATTENTE				*Durée* **15 mn**
	T (°C)	P (bars)		Lorsque l'ensemble de la masse réactionnelle a été transférée dans l'autoclave, et après fermeture de la vanne de transfert, l'évaporateur est décomprimé au travers de la colonne d'abattage,
start	205	10		
end	205	1		
PHASE 1 : CHARGEMENT				*Durée* **8 mn**
	T (°C)	P (bars)		Chargement du sel N et de l'ensemble des adjuvants, La pompe de recirculation est redémarrée lorsqu'un seuil a été atteint dans le chargement du sel
start	205	1		
end	50	1		
PHASE 2 : PRECHAUFFAGE				*Durée* **16 mn**
	T (°C)	P (bars)		La masse réactionnee est chauffée par l'echangeur extérieur jusqu'à ce que la pression dans l'autoclave atteigne 2 bars, ce qui correspond à une température de 154°
start	50	1		
end	154	2		
PHASE 3 : EVAPORATION				*Durée* **53 mn**
	T (°C)	P (bars)		Dans cette phase, la concentration en eau dans la masse réactionnelle passe de 45 à 20%, La pression est régulée à 2 bars
start	154	2		
end	200	2		
PHASE 4 : SURCHAUFFAGE				*Durée* **4 mn**
	T (°C)	P (bars)		La vanne de régulation de pression est fermée, la chauffe se poursuit jusqu'à 205°C qui correspond à une pression à l'équilibre de 2,2 bars,
start	200	2		
end	205	2,2		
PHASE 5 : TRANSFERT				*Durée* **15 mn**
	T (°C)	P (bars)		La vanne de transfert vers l'autoclave est ouverte et l'évaporateur est gonflé sous 10 bars de vapeur
start	205	3		
end	205	10		

figure 3.2 Recette de la partie évaporation

3.1.4 Les actions de sécurité

Les procédures de sécurité sont composées de défauts (conditions d'activation), d'actions à effectuer en cas de défaut, et des principes de désactivation de ces actions. Un défaut de sécurité est un événement détectant une déviation anormale ou dangereuse du procédé (changement d'état ou dépassement de seuils) nécessitant une ou plusieurs actions afin de limiter ou d'annuler les conséquences de la déviation. Un défaut de sécurité doit être acquitté par l'opérateur afin de disparaître. De plus, il peut être condamné par l'opérateur, c'est-à-dire qu'il ne déclenche plus la ou les actions de sécurité associées, et seule la détection subsiste. Une action de sécurité est le positionnement automatique d'un actionneur sur détection d'un défaut. Elle est prioritaire sur toute commande de l'actionneur (recette ou commande manuelle). Plusieurs types d'actions existent :

- **action de sécurité normale (N)** : à l'apparition d'un défaut concernant cette action, celle-ci est activée. A la disparition de ce défaut, l'action n'est plus maintenue.
- **action de sécurité à réarmement (R)** : elle subsiste après la disparition du ou des défauts l'ayant déclenchée. Ce n'est qu'ensuite que l'opérateur peut la supprimer.
- **action de sécurité verrouillable (V)** : elle peut être supprimée temporairement par l'opérateur tant qu'un défaut déclenchant cette action subsiste. A la disparition du ou des

défauts concernés, le verrou disparaîtra automatiquement pour que l'action s'effectue de nouveau dès la réapparition d'un des défauts. Elle est surtout utilisée lors des démarrages pour les actions de sécurité qui du fait de leur activation, maintiennent le défaut de sécurité l'ayant déclenchée.

Les procédures de sécurité sont souvent représentées par une matrice appelée matrice de sécurité. Elles peuvent être modélisées par un ensemble d'équations logiques de type conditions et éventuellement d'automates à états finis. Les actions de sécurité sont en général implantées en utilisant une technologie plus fiable que les systèmes de conduites classiques et toujours de façon indépendante.

3.2 La démarche de ScénaRisK

Dans ce paragraphe, nous allons réaliser les cinq étapes de la méthode ScénaRisK sur un procédé chimique d'évaporation. Les différentes étapes sont les suivantes :

- étape 0. construction de la bibliothèque
- étape 1. description structurelle de l'installation
- étape 2. description fonctionnelle de l'installation
- étape 3. description des éléments de scénarios d'interface
- étape 4. recherche des états de pré-danger
- étape 5. recherche des enchaînements de scénarios

3.2.1 Etape 0 : construction de la bibliothèque

Ici, nous allons partir du principe qu'il s'agit de la première analyse dans le domaine chimique, il n'existe donc aucun élément de scénarios dans notre librairie. La première étape consiste donc à rechercher tous les attributs qualitatifs qui permettent de définir le procédé chimique décrit au paragraphe précédent. D'après la description du procédé, nous pouvons en extraire les attributs qualitatifs suivants :

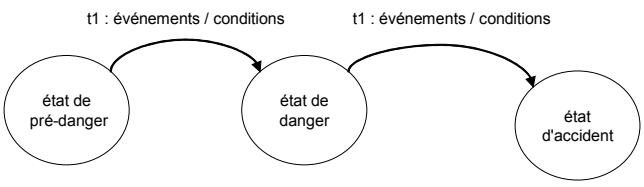


figure 3.3 Elements de scénarios génériques

Liste des éléments de scénarios de danger génériques (figure 3.3)

Etat de pré-danger (attributs)	Transitions événements / conditions	Etat de danger (attributs)	Transitions événements / conditions	Etat d'accident (attributs)
- conteneur - pression utile - hermétique	Présence pression danger	- conteneur - pression danger - hermétique	Présence pression de rupture	Eclatement
Comburant	Présence de combustible	- comburant - combustible	Présence énergie d'activation	Incendie
Combustible	Présence de comburant	- comburant - combustible	Présence énergie d'activation	Incendie
- Véhicule en mouvement - solide en mouvement	Présence de perte de contrôle véhicule -> Présence arrêt du véhicule <-	Perte de contrôle du véhicule	Présence de contact	Accident voiture

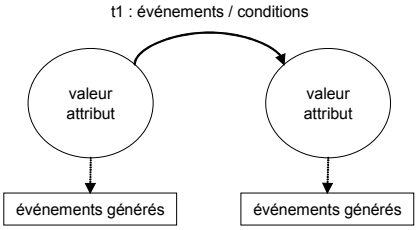


figure 3.4 Scénarios d'évolution des attributs génériques

Liste des scénarios d'évolution des attributs génériques prédéfinis (figure 3.4)

Attribut		Transitions événements / conditions	Attributs	
Valeur attribut	Événements générés		Valeur attribut	Événements générés
Pression utile	Présence pression utile	Présence pas de régulation de pression	Pression danger	Présence pression danger
Pression danger	Présence pression danger	Présence défaut organe sécurité	Pression rupture	Explosion
Régulation pression	Présence régulation pression	Présence défaut capteur de pression OU Présence défaut calculateur pression OU Présence défaut actionneur pression OU Présence défaut mécanique	Pas régulation pression	Présence pas régulation pression

Attribut		Transitions événements / conditions	Attributs	
Valeur attribut	Événements générés		Valeur attribut	Événements générés
Régulation température	Présence régulation température	Présence défaut capteur de température OU Présence défaut calculateur température OU Présence défaut actionneur température OU Présence défaut mécanique	Pas de régulation température	Présence pas régulation température

La liste des attributs contenus de notre base de connaissances est la suivante :

- conteneur
- pression {pression utile, pression de danger, pression de rupture}
- hermétique {hermétique, non hermétique}
- combustible
- comburant
- régulation pression {régulation pression, pas régulation pression}
- régulation température {régulation température, pas régulation température}
- défaut organe de sécurité
- défaut capteur de pression
- défaut capteur de température
- défaut calculateur
- défaut actionneur

.
.

3.2.2 Etape 1 : description structurelle de l'installation

La recherche des états de pré-danger que nous désirons étudier, nous permet de choisir les entités et la granularité de notre découpage arbitraire. Le découpage que nous avons choisi est le suivant.

Analyse systémique, découpage de l'installation :

- réacteur (R 33030)
- circuit d'eau froide tuyaux eau et échangeur eau froide (E 33040)
- circuit de re circulation produit tuyau, pompe (P33040) et échangeur produit (E33040)
- régulation de la pression réacteur capteur (PIS 33007), calculateur (PIC 33003), actionneur (SCV33004)
- régulation débit d'eau, froide capteur (PIS 33007), calculateur (PIC 33003), actionneur (SCV33004)

- circuit sécurité débit d'eau trop faible capteur (FI 33053), actionneur (XV33041)

Détail pour chaque groupe capteur, calculateur et, actionneur

attributs statiques :

- étanche //signifie que l'entité doit être étanche
- mesurer //décrit que cette entité fournit une mesure
- actionner //cette entité est un actionneur physique

L'entité suivante est composée de trois constituants : un capteur, un calculateur et un actionneur, nous décrivons cette entité pour l'étude qui nous intéresse comme composée d'un attribut mesurer et d'un attribut actionner.

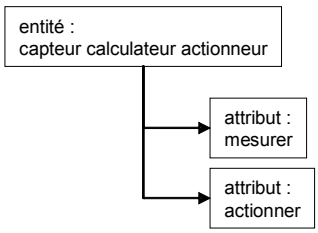


figure 3.5 Détail de l'entité capteur calculateur actionneur

réacteur R33030

Le réacteur est le conteneur où doit se produire la réaction, il doit donc avoir les caractéristiques d' un conteneur étanche et résistant à la pression.

attributs physiques :

- conteneur //décrit un attribut pouvant contenir un autre attribut

attributs statiques :

- étanche //signifie que l'entité doit être étanche
- pressurisé // signifie que l'entité résiste à la pression (à la pression utile)

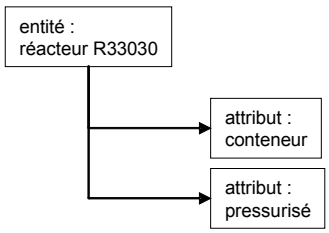


figure 3.6 Détail de l'entité réacteur

Circuit de re-circulation

Le circuit de re-circulation permet le maintient du réactif à une température donnée en créant une circulation de réactif. Pour cela, il est constitué de tuyau d'une pompe et de l'échangeur partie chaude. L'ensemble de ce circuit doit être un conteneur étanche et résistant à la pression.

tuyaux

attributs physiques :

- conteneur

attributs statiques :

- étanche

pompe

attributs physiques :

- conteneur

attributs statiques :

- étanche

échangeur (partie chaude)

attributs physiques

- conteneur

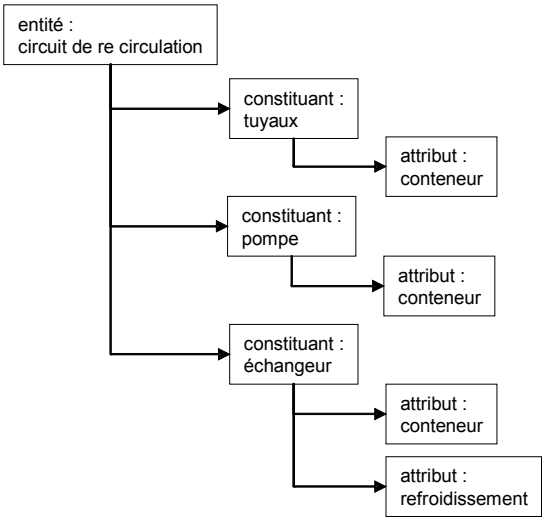


figure 3.7 Détail de l'entité circuit de re circulation

Boucle d'eau froide

La boucle d'eau froide permet de refroidir le mélange par l'intermédiaire de l'échangeur. La boucle d'eau froide est un conteneur étanche.

tuyaux

attributs physiques :

- conteneur

attributs statiques :

- étanche

échangeur

attributs physiques

- conteneur
- chaleur {réchauffement}

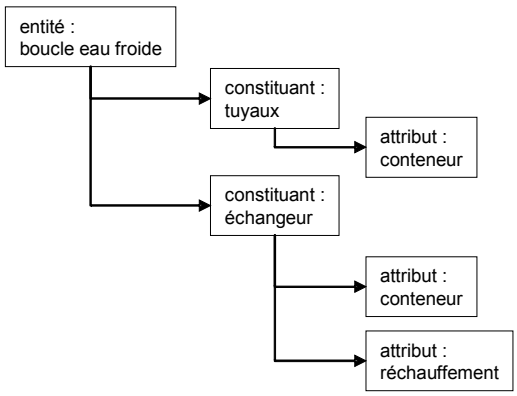


figure 3.8 Détail de l'entité boucle eau froide

3.2.3 Etape 2 : description fonctionnelle de l'installation

Dans cette étape, nous allons décrire les fonctions statiques (figure 3.9) de l'installation. Nous avons identifié la fonction statique étanche.

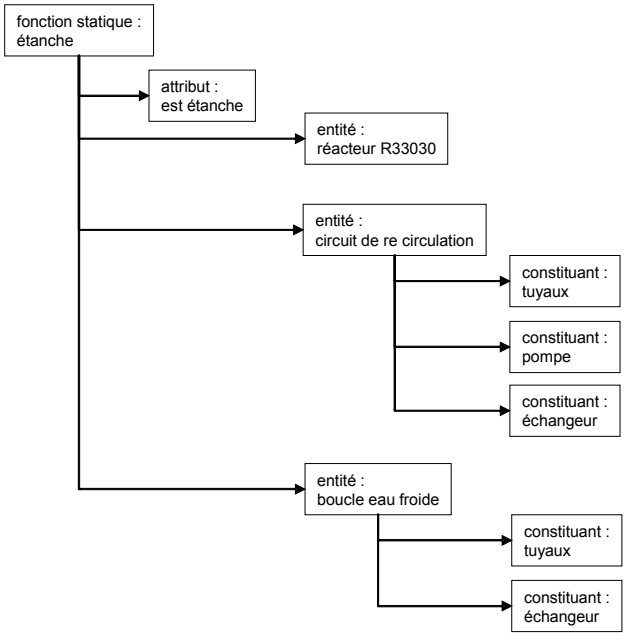


figure 3.9 Détail de la fonction statique étanche

Liste des différentes fonctions et phases de fonctionnement que doit réaliser l'installation, déterminée à partir du cahier des charges, il existe six phases de fonctionnement principales dans la fonction normale. Les phases de fonctionnement préchauffage et évaporation peuvent être réalisées en parallèle, cette possibilité se retrouvera dans l'étape 5 lors de la génération des scénarios danger.

Le détail des différentes phases de fonctionnement est défini à la figure 3.10, ainsi que le

matériel physique permettant la réalisation de ces différentes phases.

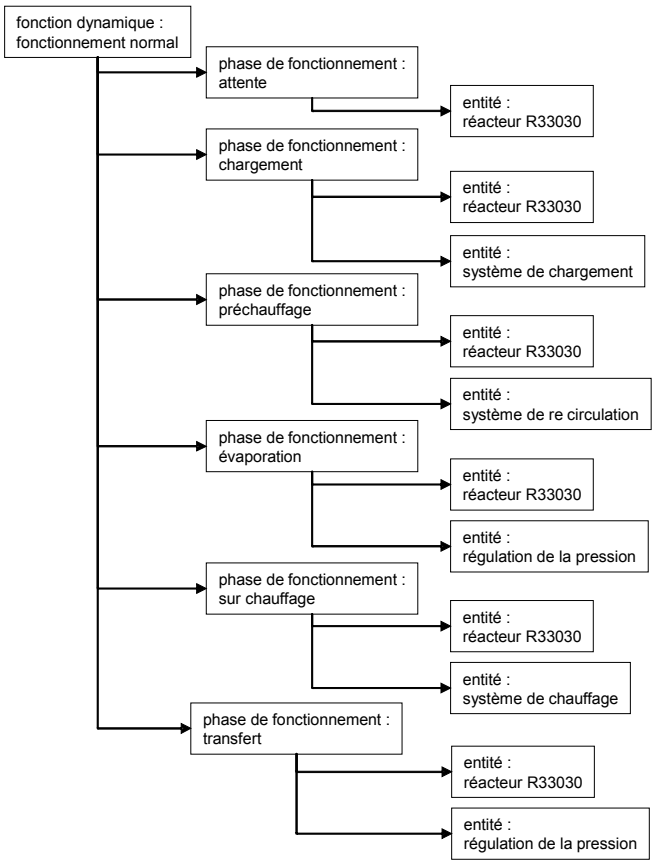


figure 3.10 Détail des fonctions dynamiques

3.2.4 Étape 3 : description des éléments de scénarios d'interface

Liste des scénarios d'interface de l'installation générique, qui permettent la modélisation des défaillances de l'installation (figure 3.11).

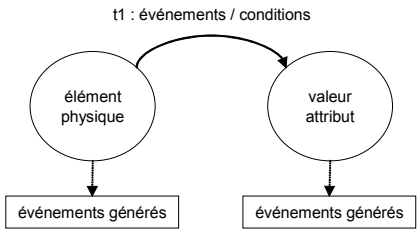


figure 3.11 Élément de scénarios d'interface

Installation réelle		Générique	Modèle de danger générique	
		Transitions événements / conditions		
Élément réel physique	Événements générés		Valeur attribut	Événements générés
Soupape de sécurité conteneur PSV33009		Présence choc OU Présence grippage OU Présence usure	Défaut de la soupape de sécurité	Présence défaut organe sécurité
Échangeur chaleur E33040		Présence bouchon OU Présence fuite	Pas de refroidissement	Présence pas de régulation température
Capteur température TI 33051		Présence pas alimentation OU Présence défaillance mécanique	Plus de mesure de température température fausse	Présence défaut capteur de température
Calculateur FIC 33052		Présence non alimentation		Présence défaut calculateur température
Actionneur vanne CX33053		Présence fuite OU Présence bouchon OU Présence pas alimentation		Présence défaut actionneur température
Capteur pression PIS 33007		Présence pas alimentation OU Présence défaillance mécanique		Présence défaut capteur de pression
Calculateur PIC 33003		Présence non alimentation		Présence défaut calculateur pression
Actionneur vanne SCV33004		Présence fuite OU Présence bouchon OU Présence pas alimentation		Présence défaut actionneur pression
Réacteur R33030		Présence choc OU Présence température élevée		Présence défaut conteneur
Capteur débit d'eau FI 33053		Présence pas alimentation OU Présence défaillance mécanique		Présence défaut capteur débit eau
Actionneur sécurité XV33041		Présence fuite OU Présence bouchon OU Présence pas alimentation		Présence défaut actionneur sécurité

		Transitions événements / conditions		
Élément réel physique	Événements générés		Valeur attribut	Événements générés
Pompe P33040		Présence défaillance mécanique OU Présence choc OU Présence pas alimentation	Plus de boucle de re-circulation	Présence défaut régulation température

3.2.5 Etape 4 : recherche des états de pré dangers (des scénarios)

Pour chacune des phases de fonctionnement, nous recherchons la liste des entités présente dans chacune des phases de fonctionnement (étape 2). Puis à partir de cette liste nous en déduisons la liste des attributs qui composent chaque phase de fonctionnement.

- attente
  - conteneur
  - hermétique
  - pression
- chargement
  - conteneur
- préchauffage
  - conteneur
  - régulation de la température
  - régulation de la pression
- évaporation
  - conteneur
  - régulation de la pression
  - régulation de la température
- transfert
  - conteneur

A partir de la liste des attributs pour chacune des phases de fonctionnement, et de la base de connaissances que nous avons construite (étape 0) nous pouvons en déduire la liste des états de pré-danger. Pour les phases de fonctionnement attente, chargement et transfert, nous n'avons pas identifié d'état de pré-danger correspondant à notre base de connaissances.

Préchauffage

- régulation de la température
- régulation de la pression

- pompe P33040
- capteur de pression PIS33007
- capteur débit d'eau FI33053
- calculateur PIC 33003
- soupape de sécurité PSV 33009
- actionneur vanne SCV 33004

Evaporation

- régulation de la température
- régulation de la pression
- pompe P33040
- capteur de pression PIS33007
- capteur débit d'eau FI33053
- calculateur PIC 33003
- soupape de sécurité PSV 33009
- actionneur vanne SCV 33004

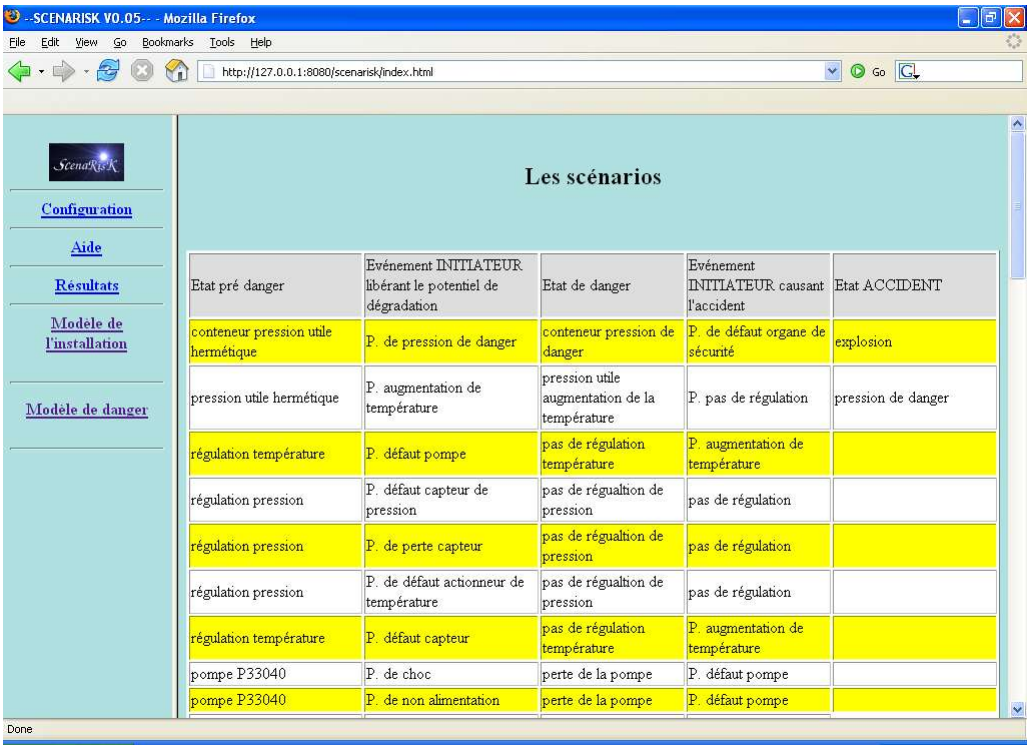
Sur chauffage

- régulation de la température
- régulation de la pression
- pompe P33040
- capteur de pression PIS33007
- capteur débit d'eau FI33053
- calculateur PIC 33003
- soupape de sécurité PSV 33009
- actionneur vanne SCV 33004

3.2.6 Etape 5 : recherche des enchaînements de scénarios

Les phases de fonctionnement qui nous permettent de générer des scénarios de danger en fonction de la bibliothèque sont les phases de préchauffage, évaporation, et surchauffage. Pour ces trois phases les scénarios de danger sont décrits figure 3.14. Pour construire cet enchaînement de scénarios nous recherchons tous les scénarios que nous pouvons construire à partir de la base de connaissances dont nous disposons. Grâce à cette recherche, nous obtenons une liste de tous les scénarios possibles. La figure 3.12 présente une interface graphique de ScénaRisk permettant

le calcul de tous les scénarios possibles pour l'exemple du réacteur.



Etat pré danger	Evénement INITIATEUR libérant le potentiel de dégradation	Etat de danger	Evénement INITIATEUR causant l'accident	Etat ACCIDENT
conteneur pression utile hermétique	P. de pression de danger	conteneur pression de danger	P. de défaut organe de sécurité	explosion
pression utile hermétique	P. augmentation de température	pression utile augmentation de la température	P. pas de régulation	pression de danger
régulation température	P. défaut pompe	pas de régulation température	P. augmentation de température	
régulation pression	P. défaut capteur de pression	pas de régualtion de pression	pas de régulation	
régulation pression	P. de perte capteur	pas de régualtion de pression	pas de régulation	
régulation pression	P. de défaut actionneur de température	pas de régualtion de pression	pas de régulation	
régulation température	P. défaut capteur	pas de régulation température	P. augmentation de température	
pompe P33040	P. de choc	perte de la pompe	P. défaut pompe	
pompe P33040	P. de non alimentation	perte de la pompe	P. défaut pompe	

figure 3.12 Exemple graphique de ScénaRisK

L'exemple de scénario de danger est construit à partir de la liste des éléments de scénarios précédents. Par convention la figure 3.13 représente un OU logique, il s'agit donc pour que la transition soit franchie soit que l'événement 1 OU l'événement 2 existe.

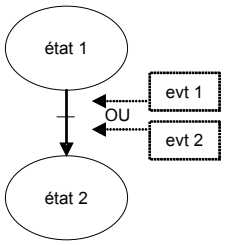


figure 3.13 OU logique

La liste de scénarios que nous obtenons en figure 3.14 tient compte d'une base de connaissances d'une taille très modeste. Sur une installation réelle comportant un nombre important d'entités, la liste des enchaînements de scénarios par phase de fonctionnement risque d'être très importante, il faut alors construire un système de classement de ces scénarios. La recherche des scénarios de danger les plus probables peut être réalisée à partir de différentes

méthodes :

- soit par recherche de tous les scénarios permettant d'aboutir à un état indésirable,
- soit par un système de classement des événements suivant les effets qu'ils peuvent générer.

Pour cette dernière partie il existe de nombreux outils permettant de réaliser une recherche de parcours de graphe, nous ne les détaillerons pas dans ce document. Le but étant de parvenir à la génération des scénarios de danger.

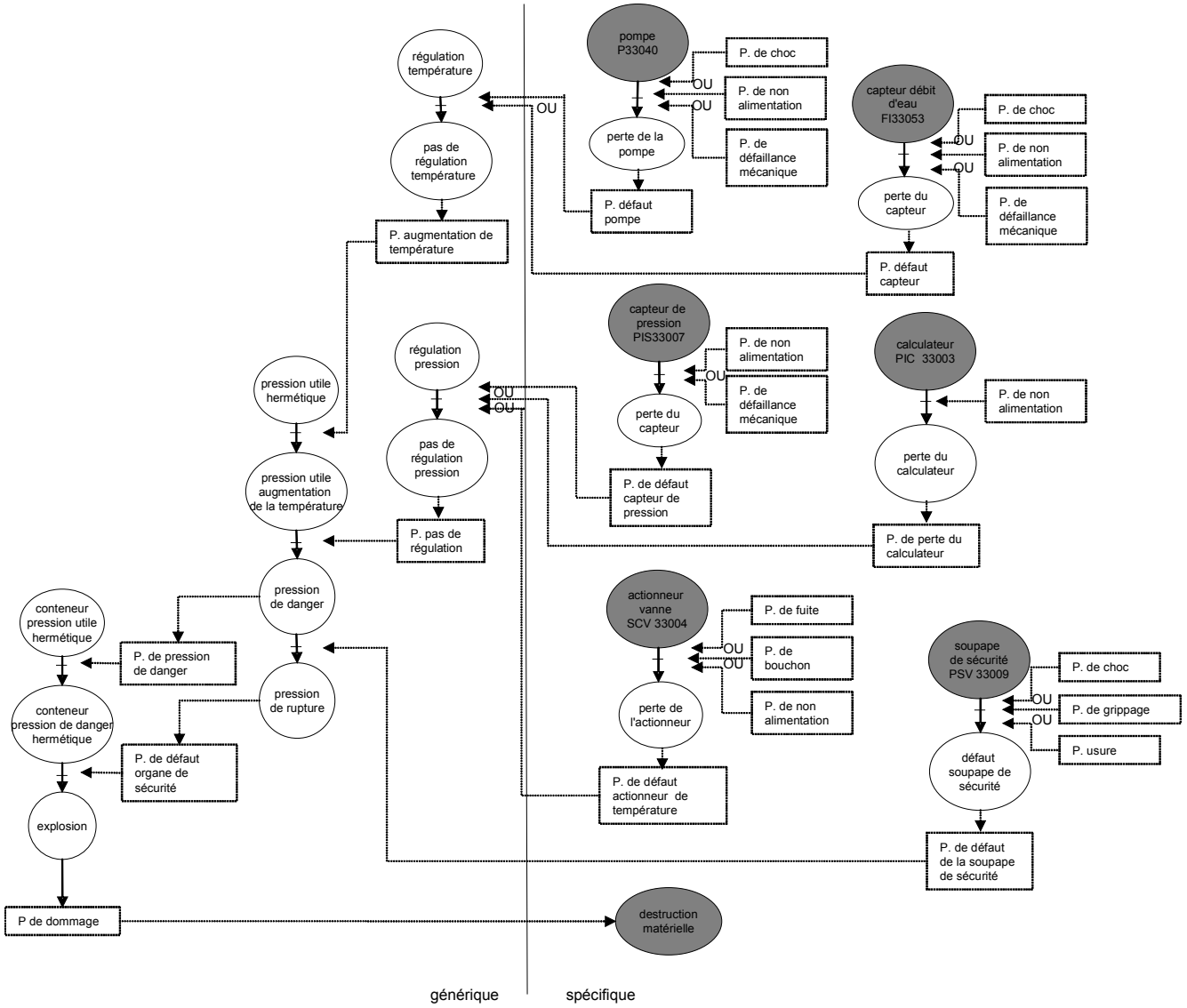


figure 3.14 Scénario de danger

Conclusion et perspectives

Dans ce mémoire, nous avons proposé une méthode d'analyse de risque par scénarios permettant de capitaliser la connaissance de l'analyste. L'approche repose sur la description des scénarios de danger sous une forme structurée et réutilisable, basée sur les attributs qualitatifs. Ce concept central de scénarios a été formalisé à partir du concept de scénarios génériques décomposés en trois parties :

- Les éléments de scénarios de danger réversibles et non réversibles représentant l'apparition d'un état dangereux
- Les éléments de scénarios d'accident représentant l'apparition d'un accident
- Les éléments de scénarios de post accident représentant la fin de l'accident.

Les scénarios de danger peuvent être sauvegardés dans une base de connaissances en vue de leurs réutilisations.

La modélisation de la base de connaissances nous a permis de développer une méthode d'analyse de risques automatisable basée sur une description structurelle et fonctionnelle, générique de l'installation. Les interfaces spécifiques / génériques permettent de représenter les départs de scénarios de danger dû à une défaillance, et les interfaces génériques / spécifiques permettent de relier l'aspect générique de l'analyse à l'aspect spécifique du système étudié.

Nous avons développé une maquette nous permettant à partir d'une interface graphique de réaliser la saisie de la base de connaissances, de la description fonctionnelle et structurelle de l'installation pour valider l'approche. Cet outil permet aussi la génération de tous les états de pré-

danger pour chacune des phases de fonctionnement, ainsi que la génération d'une partie des scénarios de danger. Pour rendre la maquette exploitable, il faut rechercher une méthode de génération de scénarios de danger plus évoluée, permettant un classement suivant plusieurs paramètres des scénarios générés et non pas une simple génération de tous les scénarios possibles pour une phase de fonctionnement donnée.

En utilisant la méthode de la base de connaissances et des attributs pour permettre une recherche des informations, il est possible en construisant des scénarios de qualité pour un produit ou une installation, de déterminer les causes possibles entraînant une perte de qualité et de ce fait une non commercialisation du produit. Les scénarios de qualité peuvent compléter les scénarios de danger dans de nombreux domaines tel que l'agroalimentaire.

Enfin, cette méthode peut avoir une vocation pédagogique, en permettant aux étudiants de se sensibiliser à l'analyse des risques par la construction d'une base de connaissances et la génération des scénarios de danger (à partir d'un outil informatique) après avoir réalisé une analyse de risques par des méthodes classiques (AMDEC, HAZOP, …).

Glossaire

Analyse de risques	Analyse des risques potentiels intrinsèques à une installation, et recherche des enchaînements pouvant y conduire.
Attribut qualitatif	Un attribut représente une caractéristique applicable à un état. Les attributs peuvent être soit des caractéristiques physiques (toxique, combustible, agroalimentaire) soit des caractéristiques fonctionnelles. Un attribut peut être défini ou non défini, il prend ses valeurs dans un ensemble.
Attribut qualitatif fonctionnel	Représente les attributs qui ont un rapport avec la fonction à réaliser. (étanche, stérile, ...)
Attribut qualitatif physique global	Un attribut qui s'applique à une entité, et donc à tous ses constituants. (L'entité lait contient un attribut physique global : "agroalimentaire")
Attribut qualitatif physique	Un attribut qui s'applique à un seul constituant.
Attribut statique	Un attribut statique décrit une caractéristique d'une fonction statique.
Automates	Ce que nous désignons par le terme d'automate emprunte des caractéristiques issues aussi bien de la notion d'automate fini en théorie des langages, que des notions de structure de Kripke ou de système de transitions dans d'autres domaines [Laroussinie 1999].
Champ de danger	C'est l'environnement actif susceptible d'influer les systèmes source et cible ainsi que le flux de danger. Il sera de nature physique, psychologique.

Danger	Danger : qui menace la sûreté [Petit Robert]. Le danger est un concept qualitatif et descriptif. On effectue l'inventaire des événements non souhaités et leurs conséquences. On dimensionne, on ne quantifie pas
Description structurelle	Description permettant une représentation de l'aspect matériel du système réel sous la forme d'entités et de constituants.
Dysfonctionnement	Altération ou non remplissement d'une fonction.
Entité	Groupe de matériels physiques issu d'un découpage arbitraire de l'installation. Représenté par une liste de constituants et par une liste d'attributs.
Entité de proximité	Une entité de proximité est une entité se trouvant dans le champ (proximité physique) d'une autre entité. Les événements générés par une entité de proximité vont être pris en compte dans la génération des scénarios comme faisant partie de la phase de fonctionnement considérée.
Entité liée	Une entité est liée à une autre entité pour une fonction statique donnée, quand les changements d'attribut d'une entité liée à la fonction statique vont obligatoirement modifier l'attribut de l'entité.
État	Un état est défini par la donnée d'un certain nombre d'attributs ou de propriétés. Un état est dit à risque s'il contient un sous ensemble d'attributs inclus dans un état initial de scénario de danger avec les mêmes valeurs.
État d'accident	Etat décrivant un accident, par un ensemble d'attributs, et d'événements d'accidents générés. (modification des attributs, génération d'événement)
État de danger	Etat décrivant un danger par un ensemble d'attributs, et des événements de danger générés.
État de danger non réversible	Un état de danger ou aucun retour n'est possible à l'état initial.
État de danger réversible	Un état de danger, où il est possible de revenir à l'état initial.

État initial ou de pré-danger Un état pré-danger est un état permettant d'identifier les dangers. Cet état peut être décrit par la présence de caractéristiques (attributs) présents ou non présents sous forme d'un n uplet (ex chaud ou pas chaud, toxique ou pas toxique), exemple (agroalimentaire, étanche, stérile) où les noms représentent les attributs associés à l'état de pré-danger.

État post accident Liste des attributs décrivant l'état après l'enchaînement du scénario de danger. (l'état de post accident décrit l'état après le déroulement du scénario de danger).

Événement Les événements représentent les changements d'état du système sous la forme de la propagation des dangers, des effets, des dommages et des accidents. Ils représentent un changement de valeur d'un attribut, d'une valeur de départ à une valeur finale.

Flux de danger Événement non souhaité généré par une source de danger, pouvant agir sur un système cible.

Fonction dynamique Une fonction dynamique représente une réalisation décomposable en phases de fonctionnement, faisant intervenir des constituants de l'entité.

Fonction statique Une fonction statique représente une fonction valable pour une entité quelque soit l'état de l'entité n'est pas décomposable en phases de fonctionnement. (exemple: étanche, résister à la pression)

Fonctions Capacité d'un système à réaliser un objectif
Librairie éléments de scénarios génériques

Méthode Programme réglant d'avance une suite d'opérations à accomplir et signalant certains événements à éviter, en vue d'atteindre un résultat déterminé.

Méthodologie Réflexion qui a pour objet d'examiner la nature, la valeur et le choix des matériaux avec lesquels nous pouvons construire notre connaissance en vue de déterminer à quels usages ils sont propres ou impropres.

Modèle

Le modèle d'un système physique est une description (schématique) de sa structure physique avec en plus les modèles (comportementaux ou fonctionnels) de chacun de ses constituants [De Kleer et al, 1987].
Schéma, c'est-à-dire description mentale (intériorisée) ou figurée (diagrammes, formules mathématiques, ...) qui, pour un champ de questions, est pris comme représentation abstraite d'une classe de phénomènes, plus ou moins habilement dégagés de leur contexte par un observateur pour servir de support à l'investigation et/ou la communication [AFCET, 1988]. La qualité d'un modèle réside moins dans son aptitude à décrire des phénomènes que dans sa conformité avec les objectifs pour lesquels il a été conçu [Penalva, 1990].

Occurrence danger

Un élément de scénario constitué d'un état de danger, d'un événement et d'un état d'accident.

Occurrence post accident

Un élément de scénario constitué d'un état d'accident, d'un événement et d'un état de post-accident.

Phase de fonctionnement

Une phase de fonctionnement décrit une étape permettant de réaliser une fonction. Une phase de fonctionnement est décrite par une liste d'entités, et par les constituants de l'entité intervenant dans la réalisation de la phase de fonctionnement.

Problématique

Ensemble des problèmes que pose un domaine particulier de la connaissance.

Prévention

Diminution de l'occurrence (ou de la fréquence) d'un Evénement Non Souhaité. En d'autres termes l'action de prévention consiste à tout faire pour que l'événement ne se produise pas. On agit sur un élément constitutif de l'ENS. La prévention est aussi appelée sécurité primaire par certaines Techniques du Danger telles que la Sécurité des installations et la Sûreté de fonctionnement.

Protection

A la suite d'un échec toujours possible de la prévention, l'Evénement Non Souhaité a eu lieu, on peut alors minimiser sa gravité. La protection est aussi appelée sécurité secondaire par certaines Techniques du Danger telles que la Sécurité des installations et la Sûreté de fonctionnement.

Risque

Le risque est un concept quantitatif à deux dimensions
1. Probabilité d'occurrence (à priori) ou fréquence (à postériori) de l'événement non souhaité.
2. La gravité de cet événement non souhaité.

Scénario d'interface Un scénario d'interface est un scénario permettant de faire le lien entre le modèle de danger générique de l'installation et l'installation physique.

Scénario de danger Un scénario de danger est la représentation des enchaînements conduisant à un accident sous une forme structurée et réutilisable.

Source de danger Un élément ou système pouvant générer un événement non souhaité sur un système cible.

Système Un système est une totalité organisée d'éléments solidaires ne pouvant être définis que les uns par rapport aux autres. Le tout est supérieur à la somme des parties.

Système à événement discret (SED) Système à espaces d’états discrets dont les transitions entre états sont associées à l’occurrence d’événements discrets asynchrones.

Références bibliographiques

[AFCET 1988] AFCET, 1988, Modèle et maîtrise des systèmes, Congrès AFCET.

[AFNOR 1994] AFNOR Norme expérimentale X60-010. Maintenance – Concepts et définitions des activités de maintenance. AFNOR, premier tirage, Paris 1994.

[Alonso 199] C. Alonso, et J. Gavalda, A method to determine environmental risk in chemical process industries. In Preceeding from ninth international symposium loss prevention and safety promotion in the process Industries (pp. 1219-1227).

[ANSI/ISA-5.1, 1992] American National Standards Institute / International Society of America - 5.1, *Instrumentation Symbols and identification*, 1992.

[ANSI/ISA-88.01, 1995] American National Standards Institute / Instrument Society of America - 88.01, *Batch Control Part 1: Models and Terminology*, 1995.

[Aupied 1994] J. Aupied Retour d'expérience appliqué à la sûreté de fonctionnement des matériels en exploitation. Collection de la Direction des études et Recherches d'Electricité de France. Edition Eyrolles, Paris ISSN 0399-4198, 1994.

[Bergsten 2001] H. Bergsten, Java Server Pages, Edition O'Reilly, 2001

[Bernardinello 1992] L. Bernardinello, F. De Cindio, A survey of Basic Net Models and Modular Net Classes, LNCS vol. 609, Springer Verlag, 1992

[Catino 1995] C.A. Catino, L.H. Ungar, Model based approach to automated hazard identification of chemical plants. AIChE J,41:97.

[Codegepra 2003] Compte rendu de la table ronde sécurité colloque codegepra 2003 Grenoble

[Delvosalle 1998] C. Delvosalle, C. Fievez, F. Benjelloun, Development of a methodology for identification of potential domino effects in Seveso industries. In Proceeding from ninth international symposium loss prevention ans safety promotion in the process industries (pp. 1252-1261).

[Dolladille 1999] O. Dolladille, Proposition d'une méthode d'analyse d'effet domino. Préventique-sécurité, 44, 62-70.

[Dubuisson 1990] B. Dubuisson Diagnostic et reconnaissance des formes, Hermès collection diagnostic et maintenance, Paris, ISBN 2-86601-240-2, 1990.

[Ermine 2000] J.-L. Ermine, Les systèmes de connaissances, Hermès, Paris, 1996 (deuxième édition 2000).

[Eckel 1998] B. Eckel, Thinking in Java, Prentice-All, 1998

[Flaus 1994] J. M. Flaus, La régulation industrielle, Edition Hermès, 1994.

[Flaus 2001] J.M. FLAUS, Une Formalisation explicite de l'état et des flux dans la méthode MOSAR, Congrès Français de Génie des Procédés, Nancy, 17-19 oct 2001

[Flaus 2002] J.M. FLAUS, O. GRANDAMAS, Towards a formalisation of MADS, system failure analysis model, µ13 / ESREL 2002, 19-22 avril , Lyon, 2002

[Flaus 2002-2] J.-M. Flaus, Support de cours PRISHE 2002 sécurité générale.

[Flaus 2003] J.-M. Flaus Un modèle de danger unifié pour l'analyse systémique des risques, SFGP Saint Nazaire 2003

[Froquet 2003] L. Froquet, J.-M. Flaus, Structural modelisation of automatic food processing for hazard studies, CESA Lille 2003

[Froquet 2003-2] L. Froquet, J.-M. Flaus, Analyse de risques pour procédés agroalimentaires automatisés, SFGP Saint-Nazaire septembre 2003.

[Gadd 1998] S. A. Gadd, D.G. Leeming T.N.K. Riley, Transport Riskat : The HSE quantified risk assessment tool for toxic and flammable dangerous goods transport by road and rail in Gread Britain. In Proceeding from ninith International symposium loss prevention and safety promotion in the process industries (pp 308-317).

[Gallardo 2003] D. Gallardo, E. Burnett, R. McGovern, Eclipse in Action: A Guide for Java Developers, ISBN 1930110960, 2003.

[Godard 1994] R. GODARD, MADS appliquée à MOSAR, Support de formation, CEA/INSTN, 1994.

[Ham 1998] K.J.M. Ham, H.J.C.M van Kessel, T. Wiersma, Experiences with a safety report according to seveso II: A pilot project in the Netherlands.In Proceeding from ninith International symposium loss prevention and safety promotion in the process industries (pp. 1326-1340).

[Hamscher, Console et de Kleer 1992] W. Hamscher, L. Console et de J. De Kleer Model-Based Diagnosic, Morgan Kaufman, ISBN 1-55860-249-6, 1992.

[Harel 1987] D. Harel, Statecharts : a visual formalism for complex systems, *Science*

[Heino 1995] P. Heino, E. Kotikunnas, W.F. Shei, C.C. Shao, C.H. Chen, Computer-aided HAZOP with knoledge-based identification of hazardous event chains, Loss Prevention and Safety Promotion in the Process Industries , Volume 1 (ed by J.J. Mewis, H. J. Pasman and E.E. De Rademaeker (Elsevier), 645-656).

[Henley 1992] E.J. Enley and H. Kumamoto, Probabilistic Risk Assement, Reliability Engineering, Design and Analysis (Prentice-Hall, Englewood Cliffs, NJ).

[Hopcroft et Ullman, 1979] J.E. Hopcrofot and J.D. Ullman, *Introduction to Automata theory, Languages and Computation*, Addison-Wesley, 1979.

[IEC 1985] IEC Norme Internationale 812-1985. Techniques d'analyse de la fiabilité des systèmes – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE). Reproduit dans la norme X 60-510, UTE, premier tirage, Paris, 1986

[Jäger 1998] P. Jäger, K. Kühnreich, Approach to a systematic determination ansd evaluation of risk potential. In Proceeding from ninith International symposiumloss prevention and safety promotion in the process industries (pp. 393-403).

[Jefferson 1995] M. Jefferson, J.T. Illidge, Activities and time usage in hazard and operability studies. Research Event 95 (IChemE, Rugby).

[Jezler 1998] W. Jezler, Earthquake safety of structures and installations in chemical industry in the context of risk analysis. In Proceeding from ninith International symposiumloss prevention and safety promotion in the process industries (pp. 414-421).

[Kao 1998] C.S. Kao, Y.S. Duh, Chemical runaway reaction hazard index and risk assessment. In Proceeding from ninith International symposiumloss prevention and safety promotion in the process industries (pp. 965-975)

[Kennedy 1998] R. Kennedy, B. Kirwan, Development of a hazard ans operability-based method for identifying safety management vulnerabilities in high risk systems. Safety Sciences, 30, 249-274.

[Khan 1998] F.I. Khan, S.A. Abbasi, Techniques and methodologies for risk analysis in chemical process industries. Journal of loss Prevention in the Process Industries, 11, 261-277.

[Korjusiommi 1998] E. Korjusiommi, R.Salo, R. Taylor, Hazard analysis for batch processes and for special operations. In Proceeding from ninith International symposiumloss prevention and safety promotion in the process industries (pp 422-431)

[Knab 2000] F.Knab, F.Lepoivre, F.Rivard, C.Sannier, J.Bernadac, XML et JAVA, Eyrolles, Paris, ISBN 2-212-09148-6 , 2000.

[Knowlton 1992] R.E. Knowlton A Manual of Hazard and Operability Studies (Chemetics Int Ltd, Vancouver, BC).

[Laroussinie 1999] F. Laroussinie, M. Bidoit, B. Bérard, A. Petit, Vérification de logiciels, Techniques et outils du model-checking, Vuibert, ISBN : 2-7117-8646-3

[Lawley 1974] H.G. Lawley, Operability Studies and Hazard Analysis. *Chemical Engeneering Progress* 70:105-116.

[Lees 1996] F.P. Less, Loss prevention in the process industries : hazards identification, assessment and control, Butterworth and Heinemann, Oxford, 2ème edition.

[Leger 1998] J.- B. Léger Contribution Méthodologique à la maintenance Prévisionnelle des Systèmes de Production. Actes de la journée du Groupement de Recherche pour la Productique, Groupe de travail S.P.S.F. Systèmes de Production Sûrs de Fonctionnement, Nancy 1998.

[Leger 1999] J.- M. Leger Contribution Méthodologique à la Maintenace Prévisionnelle des Systèmes Industriels de Production : Proposition d'un Cadre Formel de Modélisation. Thèse de Doctorat, Université Henri Poincaré, Nancy 23 avril 1999

[Le Moigne 1977] J.-L. Le Moigne La théorie du système général – théorie de la modélisation, Ed Presse Universitaire de France.

[Le Moigne 1990] J.-L. Le Moigne La modélisation des systèmes complexes, Afcet Systèmes, Dunod, ISBN 2-04-019704-4,1990.

[Leroy 1992] A. Leroy, J.-P. Signoret Que sais-je ?, Le risque technologique, Presses Universitaires de France, ASIN 2130447589.

[Lievens 1976] C. Lievens Sécurité des Systèmes. Cépaduès, collection Ecole Nationale Supérieure de l'Aéronautique et de l'Espace SUP'AERO, Toulouse, ISBN 2-85428-009-1, 1976.

[Limnios 1991] N. Limnios Arbres de défaillance. Hermès, Traité des nouvelles Technologies, Série Diagnostic et Maintenance, Paris ISBN 2-86601-299-2, 1991.

[McCoy 1999] S. A. McCoy et al., Hazid a computer aid for hazard identification, parts 1 to 5, Trans IchemE, part B, 1999, V77, 317-327 ; 1999, V77, 328-334 ; 1999, V77, 335-353 ; 2000, V78, 91-119 and 2000, V78, 120-142.

[Mohafid 1994] A. Mohafid Contribution de l'analyse fonctionnelle à la spécification et à la gestion prévisionnelle des dysfonctionnements. Thèse de Doctorat de l'Université d'Angers, Novembre 1994.

[Movaghar 84] A. Movaghar and J.F. Meyer Performability modeling with stochastic activity networks.IEEE symposium of the real-tile systems, New York, 1984.

[Niel 1989] E. Niel, J.-P. Simon La sécurité des installations robotisées. Editions Hermès, Collection Technologie de pointe, n°20, mars 1989.

[Niel 1992] E. Niel, et A. Jutard Contribution à la formation de la Sécurité Opérationnelle. Revue d'Automatique et de Production Appliquées, 1992.

[Niel 1994] E. Niel, De la sécurité opérationnelle des systèmes de production. Habilitation à diriger les recherches. INSA de Lyon, 1994.

[Niel 1998] E. Niel, Sécurité opérationnelle des systèmes de production, Technique de l'ingénieur, Mesures et Contrôle R7640 1998

[Oien 1998] K. Oien, S. Sklet, L. Nielsen, Development of risk level indicator for petroleum platform. In Proceeding from ninith International symposiumloss prevention and safety promotion in the process industries (pp 382-393)

[Penalva, 1990] J.-M. Pénalva, La représentation par les systèmes en situation complexe. Thèse de Doctorat, Université d'Orsay, 9 décembre 1997.

[Périlhon 1998] P. Périlhon, du risque à l'analyse des risques : Développement d'une méthode MOSAR, méthode organisée et systémique d'analyse des risques, document de travail 1998.

[Périlhon 2000] P.Périlhon, Eléments méthodiques d'analyse des risques, Phoebus, 12 (2000), p. 31 à 49.

[Pétin 1995] J.-F. Pétin Contribution méthodologique à l'Actionnement et à la Mesure Intelligents : application au projet ESPRIT III – PRIAM n°6188. Thèse de doctorat. Université Henri Poincaré Nancy, 1995.

[Petit Robert 2000] Le petit Robert, de la langue française, édition 2000.

[Phoebus 2000] Pheobus, La revue de la sûreté de fonctionnement. L'analyse des risques n°12 1er trimestre 2000

[Preston 1995] M.L. Preston, STOPHAZ support tools for process hazard and operability studies, 8th Int Symp on Loss Prevention and Safety Promotion in the Process Industries, vol 2, 655.

[Price 1991] C. Price, J. Hunt, Automating FMEA through multiple models, Br Comput Soc ESG conf.

[Puertas 1998] I. Puertas, J.C. Sanz, C. Vaquero, M. Marono, R. Sola, Procedure for the review of quantitave risk assessment of the process industries. In Proceeding from ninith International symposiumloss prevention and safety promotion in the process industries (pp 283-288).

[Rasmussen 1997] B. Rasmussen, C. Whetton, Hazard identification on plant functional modeling. Reliability Engineering and System Safety, 55, 77-84.

[Rogers 2000] R. L. Rogers, The RASE Project risk assement of unit operations and equipement. (pp 1-50).

[Rose 1991] P. Rose, M.A. Kramer, Quantitative analysis of causal feedback, AAAI-91.

[Sanders 1995] J.W. Sanders Process safety artificial intelligence system, 8th Int Symp on Loss Prevention ans Safety Promotion in the Process Industries, vol 1, 656.

[Sankey 1998] P.D. Sankey, An insurer's involvement in the risk reduction process. In Proceeding from ninith International symposiumloss prevention and safety promotion in the process industries (pp 441-450).

[Senni 1997] S. Senni, L. Colombo, M.L. Preston, STOPHAZ : a safety support tools for operatbility and hazard studies, ESREL (European Safety and Reliability) conf. Lisbon.

[Shimada 1995] Y. Shimada, Z.X. Yang, J.W. Song, K. Suzuki, H. Sayama, Computer-aided operability study for batch plant, 8th Int Symp on Loss Prevention and Safety Promotion in the Process Industries, vol 2, 587.

[Thevenon 2001] L. Thevenon Représentation des Systèmes Hybrides Complexes par Flux de Données : Développement d'un Outil de Modélisation et de Simulation des Procédés Batch. Thèse de Doctorat, INP Grenoble 16 octobre 2000

[Tiemessen 1998] G. Tiemessen, J.P. van Zweeden, Risk assessment of the transport of hazardous materials. In Proceeding from ninith International symposiumloss prevention and safety promotion in the process industries (pp 299-307).

[Toola 1992] A. Toola, Plant level safety analysis. Journal of loss Prevention in the Process industries 5 (2), 119-124.

[Tixier 2002] J. Tixier, G. Dusserre, O. Salvi, D. Gaston, Review of 62 risk analysis methodologies of industrial plants, J. Loss Prev. Process Industries, 2002, 15(4), 291-303.

[Vaidhyanathan 1995] R. Vaidhyanathan, V. Venkatasubramanian, Digraph-based models for automated HAZOP analysis, Relab Eng System Safety, 50:33.

[Van Schrick 1997] D. Van Schrick Technical fault and Qualuty Management – Terminology of Functions, Purposes and Means. Intelligent Manufacturing Systems, Ed. : Jongwon Kim, Elsevier Science, Oxford, ISBN 0-08-043025-2, 1997.

[Villemeur 1987] Sûreté de fonctionnement des systèmes industriels, Dunod, 1987

[Villemeur 1988] A. Villemeur Sûreté de fonctionnement des systèmes industriels- Fiabilité – Facteurs humains – Informatisation. Eyrolles, collection de la Direction des Etudes de Recherches et d'Electricité de France, Paris, ISSN 039964198, 1988.

[Wells 1993] G. Wells, M. Wardman, C. Whetton, Preliminary Safety analysis, J Loss Prev Process Ind, 6:47.

[Yang 1998] S. Yang, P.W.H. Chung, Hazard analysis and support tool for computer controlled processes. Journal of Loss Prevention in the Process Industries, 11, 333-345.

[Zaytoon 1993] J. Zaytoon Extension de l'Analyse Fonctionnelle à l'étude de la Sécurité Opérationnelle des Systèmes Automatisées de Production. Thèse de Doctorat, Institut National des Sciences Appliquées de Lyon, 1993.

[Zwingelstein 1995] G. Zwingelstein, Diagnostic des défaillances – théorie et pratique pour les systèmes industriels, Hermès, Traité des Nouvelles Technologie, série Diagnostic et Maintenance, Paris, ISBN 2-86601-463-4, 1995.

Annexe A

1. La méthode d'Analyse Préliminaire des Risques (APR)

Description

L'analyse préliminaire de sécurité a été élaborée par l'armée américaine dans les années 1960. Depuis elle a été utilisée par un certain nombres d'industries, notamment l'aéronautique, la chimie et le nucléaire. Le terme préliminaire signifie qu'elle est effectuée dans une phase préliminaire de développement du procédé, dans le cas ou celui ci existe, c'est une première étape pour dégrossir le problème d'analyse des risques. Cette méthode s'intéresse de façon générale aux risques des principaux produits et des grandes parties de l'installation. Elle est utilisée au début du développement et sert d'étape préliminaire à d'autres méthodes applicables lorsque les détails sont disponibles. Elle permet d'étudier les aspects suivants :

- produits initiaux, intermédiaires et finaux et leur interaction
- équipement de l'installation
- site
- mode d'exploitation
- interface entres les différentes parties du système

Objectif

L'objectif est d'évaluer les risques très tôt dans le cycle de développement de l'installation et permet d'effectuer une revue de la conception avant de passer à l'étude de détail. Le but est d'identifier de la façon la plus complète possible les risques potentiels que comporte l'installation, et d'évaluer leur gravité. Parallèlement, on y apporte des éléments de réponse.

Type de résultat

Les résultats de cette analyse sont de mettre en évidence des risques potentiels à criticité importante (on élimine les risques non réalistes) pour lesquels on peut apporter de premiers éléments de réponses ou qui nécessitent une étude plus détaillée pour évaluer leur criticité. Une APR fournit une description qualitative des principaux risques de l'installation.

Limites

La méthode préliminaire d'analyse des risques, permet donc une première analyse de l'installation, elle ne détaille pas les dysfonctionnements, les défaillances, les dommages, et l'évolution de l'installation.

2. La combinaison What-if / Checklist

Description

La méthode What-if qui peut être traduite par : "Que se passe-t-il si" c'est une approche basée brainstorming dans laquelle des personnes expérimentées qui sont familières avec le type de procédé étudié posent des questions et soulèvent des problèmes possibles à propos d'événements non désirés. Cette approche n'est pas aussi structurée que des méthodes telles que l'HAZOP ou l'AMDEC et repose en grande partie sur la pertinence du groupe de travail et en particulier de son animateur. Cette méthode est largement utilisée dans l'industrie, elle est simple à mettre en oeuvre, et elle permet d'apporter un éclairage neuf grâce à la présence de personnes d'expériences et d'horizons divers, dont certaines ne sont pas impliquées dans le projet ou la fabrication étudiée. Cette méthode permet des échanges fructueux grâce au rassemblement de personnes de sites différents mais rencontrant les mêmes types de problèmes. Enfin, le travail en groupe stimule la réflexion et l'association d'idées

Ce type d'approche combine le côté systématique d'une revue de type checklist avec le côté plus créatif de l'approche What-If. C'est souvent sous cette forme que les deux approches sont employées.

Objectif

L'objectif d'une revue What-if/Checklist est d'identifier les risques, de considérer les types généraux d'accidents qui peuvent arriver sur un procédé ou une activité, d'évaluer de façon qualitative les effets de ceux-ci et de déterminer si les mesures de prévention ou de protection sont adéquates.

Types de résultats

Une équipe utilisant une approche de type WhatIf/Checklist génère une liste des situations d'accidents potentiels, de leurs effets, des moyens et des mesures de prévention et de protection. Elle peut aussi générer une table des situations à risques avec leurs conséquences, les mesures de prévention et des suggestions pour la réduction des risques.

Limites

La méthode What-If est une étude de ce qui peut se produire à partir d'une liste de questions existante, elle ne donne ni les scénarios ni les enchaînements possibles, cette méthode dépend des intervenants qui réalisent l'analyse, la prise en compte des défaillances et des

dysfonctionnements n'est pas une chose simple. L'avantage est qu'il existe une base constituée d'une liste de questions génériques, qui peuvent être adaptées pour chaque installation. Cette méthode est non systématique, et les réponses aux questions peuvent ne pas être apportées sur le champ.

3. L'arbre des conséquences

Description

Un arbre des conséquences permet de représenter de façon graphique tous les résultats d'un événement initiateur. Pour chaque nouvel événement, on considère la réaction du système de sûretés et les modes de défaillances successifs de l'installation.

Cette approche est bien adaptée pour les systèmes complexes qui ont plusieurs niveaux de système de sécurité.

objectif

L'objectif est d'identifier les divers accidents qui peuvent se produire dans les systèmes complexes. Après avoir déterminé toutes les séquences liées à un problème individuel, les combinaisons sont étudiées avec un arbre des conséquences.

Types de résultats

Le résultat de ce type d'analyse consiste en un ensemble d'arbres d'événements qui permettent ou non de valider le système de sécurité.

Limites

L'arbre des conséquences ne peut pas être généré de façon automatique à partir du modèle de l'installation. Une analyse préalable est alors nécessaire, soit une analyse AMDEC ou HAZOP.

5. La méthode MADS-MOSAR

Description

La méthode MOSAR est une méthode organisée et systématique d'analyse des risques. Elle consiste à décomposer le système en sous système par une modélisation systémique.

Chaque sous système est analysé indépendamment, à l'aide d'une grille, comme récepteur d'événements non souhaités et comme générateur de tels événements. Cette étape conduit à la génération de scénarios de danger.

Dans une seconde phase, les événements initiateurs de la première phase sont analysés avec une méthode de type HAZOP ou AMDEC, ou de type analyse d'activité. On peut alors construire les arbres de défaillances pour chaque risque et les quantifier.

Objectif

L'objectif de cette méthode est de réaliser une analyse des risques (principale ou détaillée) et

de proposer des mesures de prévention et / ou de protection . Elle vise à être la plus exhaustive possible.

Type de résultats

Cette méthode peut être mise en oeuvre à différents niveaux. Pour une analyse se limitant à la première phase, on obtient une analyse préliminaire des risques. En allant plus loin, on obtient une analyse détaillée des risques. Elle permet la génération de scénarios de danger, et la génération des arbres des causes.

Limites

Cette méthode d'analyse est très lourde à mettre en place, elle ne permet pas d'obtenir des éléments réutilisables, elle repose pour beaucoup sur la personne chargée de réaliser l'analyse.

6. L'arbre des causes

Description

Cette approche part d'un accident particulier ou d'une défaillance du système principal et fournit une méthode pour rechercher les causes de cet événement. L'arbre des causes est un modèle graphique (arbre avec des blocs de conjonctions et de disjonctions) qui permet de représenter les différentes combinaisons de modes de défaillances de l'équipement et d'erreurs humaines à l'origine de la défaillance globale.

L'arbre des causes permet de mettre en évidence les combinaisons de défaillances qui peuvent causer l'événement principal auquel on s'intéresse, appelé événement sommet. Ces événements sommet sont des événements qui peuvent avoir été identifiés par une autre méthode d'analyse des risques (What-If, Hazop par exemple).

Qu'ils soient d'un type ou de l'autre, une hypothèse de base est que les différents éléments de l'installation sont, soit dans un état de dysfonctionnement, soit dans un état de fonctionnement correct.

Les défauts et les défaillances sont classés en trois catégories :

- défauts et défaillances primaires

  Ce sont les dysfonctionnements qui ont lieu lorsque l'entité fonctionne dans les conditions prévues
- défauts et défaillances secondaires

  Ce sont les dysfonctionnements qui ont lieu lorsque l'entité ne fonctionne pas dans les conditions prévues
- défauts et défaillances de commande

  Ce sont les dysfonctionnements qui sont dus aux informations apportées à l'entité et non à cause d'un problème interne de celle-ci.

Objectif

L'intérêt de cette méthode est de permettre d'identifier les combinaisons de défaillances à la base du problème et de permettre de prendre des mesures préventives pour réduire l'occurrence de celle-ci.

Types de résultats

Les résultats de ce type d'analyse sont représentés par un arbre logique qui décrit les enchaînements des combinaisons des différents modes de défaillances. Un grand nombre d'arbres peut être construit pour un procédé un peu complexe, puisqu'on en obtient un pour chaque accident (ou événement terminal) sélectionné.

Limites

L'arbre des causes ne peut pas être générer de façon automatique à partir du modèle de l'installation. Une analyse préalable est alors nécessaire, soit une analyse AMDEC ou HAZOP.

Annexe B

Les actionneurs

On distingue différents types d'actionneurs, dont les plus courants sont décrits dans le tableau suivant

Libellé	Symbole	Exemple
Fonctionnement progressif		
Fonctionnement par tout ou rien pneumatique ou hydraulique		
Fonctionnement progressif ou tout ou rien par moteur électrique		
Fonctionnement à ressort (soupape de sécurité)		

figure A1 actionneur

Les organes de mesure

La représentation graphique d'un organe de mesure est donnée figure A1

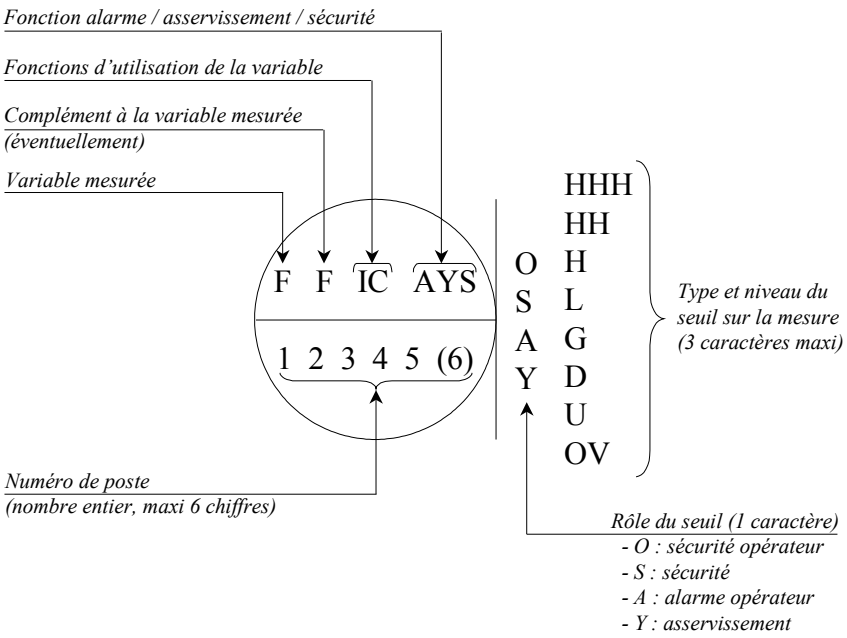


figure A2 Organe de mesure

Sur le schéma de la figure A1, on trouve six organes de mesure. Par exemple, l'organe PIC 33003 a la signification suivante :

- P: la variable mesurée est la pression.
- IC: les fonctions d'utilisation sont l'indication (I) et la régulation (C) de la pression.
- XH (à l'extérieur du cercle): seuil impliquant une action automatique (X) dans le cas d'un niveau haut (H) pour la pression.

Les organes commandés

La représentation graphique d'un organe de mesure est donnée . Elle est similaire à celle des organes de mesure, mais la nomenclature des lettres de codification est différente. La caractéristique d'un organe commandé est que la dernière lettre de son repère alphabétique est M, V ou Z.

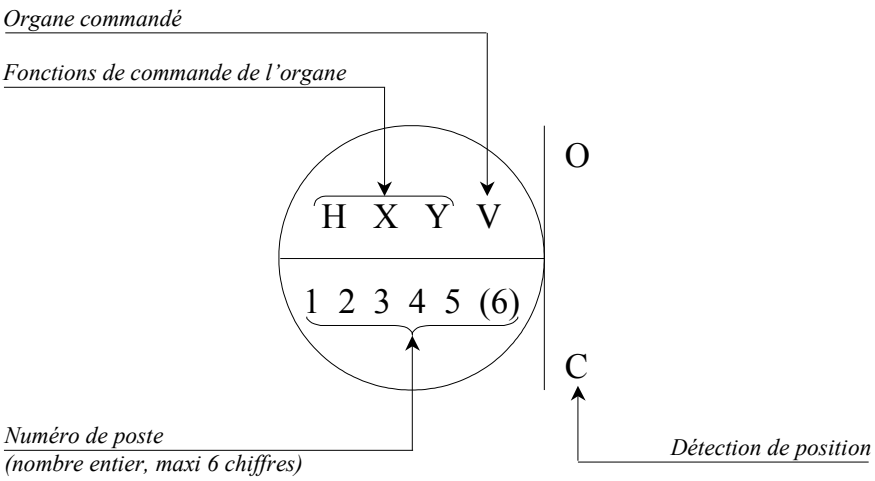


figure A3Organe commandé

Sur le schéma de la figure A3 on trouve un organe commandé. L'organe HXYM33040 associé à la pompe P33040, a la signification suivante :

HXY: les fonctions de l'organe sont la commande manuelle (H), l'automatisme (X) et l'asservissement (Y) de la pompe.

M: l'actionneur de la pompe est un moteur.