INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI®

Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

UNIVERSITÉ DE SHERBROOKE
Faculté des sciences appliquées
Département de génie mécanique

DÉVELOPPEMENT D'UNE MÉTHODOLOGIE DE CONCEPTION PERMETTANT L'INTÉGRATION SÉCURITAIRE DES AUTOMATES PROGRAMMABLES INDUSTRIELS (API) ET DES SYSTÈMES DE CONTRÔLE DISTRIBUÉS (SCD) AUX SYSTÈMES DE PRODUCTION AUTOMATISÉS DESTINÉS À L'INDUSTRIE QUÉBÉCOISE DES PÂTES ET PAPIERS

Mémoire de maîtrise ès sciences appliquées
Spécialité : génie mécanique

Patrik DOUCET

Sherbrooke (Québec), CANADA

Janvier 1998

Résumé

L'intégration des nouvelles technologies d'automatisation, particulièrement les automates programmables industriels (API) et les systèmes de contrôle distribués (SCD, a induit de nouveaux problèmes de sécurité dans l'industrie des pâtes et papier (P&P) du Québec. Dans le but d'augmenter la sécurité de l'opération et de l'entretien des équipements de cette industrie, une vaste étude a été lancée par l'Institut de recherche en santé et sécurité du travail du Québec (IRSST). Ce mémoire s'inscrit dans cette étude. Il présente une méthodologie pour la conception sécuritaire de systèmes de production automatisée.

Trois principaux objectifs y sont poursuivis. Le premier vise à définir une façon systématique d'intégrer les besoins fonctionnels liés à l'équipement. Le second vise à incorporer la gestion du risque à cette méthodologie. Ainsi, des méthodes pour l'analyse fonctionnelle et pour l'analyse du risque ont été systématiquement intégrées à la méthodologie développée. Finalement, le troisième et dernier objectif vise à s'assurer que cette méthodologie tienne compte des multiples contraintes auxquelles sont soumis les ingénieurs concepteurs de l'industrie québécoise des P&P.

RÉSUMÉ

L'automatisation de la production a permis aux diverses entreprises manufacturières non seulement d'augmenter leur compétitivité, mais aussi d'améliorer les conditions de travail de leurs employés. Cependant, l'automatisation de la production n'est pas le remède miracle pour contrer les accidents de travail : bien que les employés soient désormais davantage éloignés des machines, ils sont toujours présents dans son environnement. Par ailleurs, les techniques d'automatisation ont évolué au cours des dernières décennies. Ainsi, l'intégration des technologies programmables, comme les automates programmables industriels (API) et les systèmes de contrôle distribués (SCD), a induit de nouveaux problèmes de sécurité dans les industries. D'ailleurs, plusieurs accidents, directement liés à ces technologies, sont survenus. Ainsi, à la demande des industries québécoises des pâtes et papiers, l'Institut de recherche en santé et sécurité du travail du Québec (IRSST) a lancé un projet de recherche dont l'objectif est de rendre plus sécuritaires l'opération et l'entretien des équipements dotés d'API et de SCD, et ce en intervenant lors de leur conception. Ce projet de maîtrise s'inscrit dans la recherche qu'a lancée l'IRSST.

Par ailleurs, quelques méthodologies de conception, issues de centres de recherche, d'industries et de projets de normes permettant d'intégrer les aspects de santé et sécurité du travail lors de la conception existent. Cependant, toutes les méthodologies répertoriées sont souvent complexes à mettre en oeuvre, nécessitent beaucoup de connaissances et peuvent s'avérer très longues à appliquer. Par conséquent, elles ne cadrent pas dans la grande majorité des cas avec les pratiques de conception habituellement rencontrées dans l'industrie québécoise des pâtes et papiers.

Cette recherche a permis de mettre au point une méthodologie pour la conception sécuritaire et spécialement adaptée aux pratiques actuelles des concepteurs de systèmes de production automatisés (SPA) qui sont dotés de technologies programmables et destinés à l'industrie québécoise des pâtes et papiers. Elle permet de mieux prendre en compte les besoins fonctionnels liés à l'opération et à l'entretien des SPA de même que les aspects de santé et sécurité du travail grâce à l'intégration de méthodes d'analyse du risque.

AVIS

Dans le cadre de cette maîtrise, plusieurs activités ont été réalisées dans le but de mieux connaître les activités de conception de l'industrie québécoise des pâtes et papiers (P&P). Ainsi, dans le but de mieux comprendre comment la conception est effectuée dans cette industrie, le candidat à participé aux activités suivantes :

- visites de sept usines situées un peu partout au Québec ;
- observation et animation de deux groupes de discussion ;
- rencontre et discussion avec deux ingénieurs de firmes de consultants.

Au cours de ces activités, plusieurs personnes ayant des formations et des fonctions différentes au sein de leur entreprise ont été rencontrées, soit environ :

- 25 ingénieurs (en mécanique ou en électricité/instrumentation) ;
- 10 cadres supérieurs ;
- 10 superviseurs ou contremaîtres ;
- 20 opérateurs ou personnes assignées à l'entretien ;
- 15 personnes oeuvrant pour la santé et sécurité du travail.

Grâce à ces entrevues, plusieurs informations importantes et nécessaires à l'atteinte des objectifs de cette maîtrise ont été obtenues. Cependant, étant donné le caractère hautement confidentiel de ces informations, leurs sources ne peuvent pas être divulguées ; plusieurs constats ont donc été établis, mais aucune référence n'est donnée pour les appuyer. Ainsi, pour éviter toute confusion, toutes les informations issues de ces activités sont présentées uniquement dans les sections se rapportant spécifiquement à *l'industrie des P&P du Québec*.

REMERCIEMENTS

Mes plus sincères remerciements et ma plus vive reconnaissance vont aux personnes et aux organismes suivants pour leur soutien et leur collaboration tout au long de la recherche et de la préparation de ce mémoire :

François Charron, mon directeur de recherche, pour l'appui et la patience dont il a fait preuve à mon égard ainsi que pour les nombreuses connaissances qu'il m'a transmises ou qu'il m'a permis d'acquérir.

René Benoît, Réal Bourbonnière, Cécile Collinge, Caroline Monette et Joseph-Jean Paques, de l'*Institut de recherche en santé et sécurité du travail* du Québec, Gilles Bouchard, de *Sandwell* et Mark Mileshik, de *Cowan SNC-Lavallin*, qui m'ont permis de vivre des expériences enrichissantes au cours des diverses activités prévues dans le cadre de cette maîtrise.

Denis Proulx, directeur du département de génie mécanique, de même que François Gauthier, Éric Lemay, Anick Murray et René St-Amant, pour leur collaboration, leur appui et leur encouragement tout au long de ce périple.

Ludovic, mon fils, de même que ma famille et mes très proches amis et amies, qui ont tous su comprendre mes absences, m'encourager, me supporter dans ma démarche et m'endurer lorsque la fatigue et le manque de sommeil affectaient mon caractère!

L'*Institut de recherche en santé et sécurité du travail* du Québec, pour son soutien financier indispensable à cette recherche.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LEXIQUE

Actionneur

Mécanisme qui transforme un signal en un mouvement correspondant [CEI/IEC 351, 1994].

Analyse du risque

Utilisation des informations disponibles pour identifier les événements dangereux et estimer le risque [ISO/CEI 51, 1997].

Automate programmable industriel (API)

Composant électronique à base de microprocesseur(s) qui comporte une mémoire programmable par un utilisateur non informaticien à l'aide d'un langage adapté. Un automate programmable a pour fonction de commander, mesurer et contrôler, au moyen des modules d'entrées et de sorties, différentes sortes de machines ou de processus en environnement industriel [EDWARDS, R. et coll., 1992].

L'API est principalement utilisé pour exécuter les fonctions logiques séquentielles, mais il peut aussi traiter les fonctions analogiques.

Appréciation du risque

Processus d'analyse et d'évaluation du risque [ISO/CEI 51, 1997].

Automatique

S'applique à un processus ou à un dispositif qui, dans des conditions données, fonctionne sans l'intervention humaine [CEI/IEC 351, 1994].

Automatiser

Mettre en oeuvre les moyens permettant la réalisation de fonctions automatiques dans un système [CEI/IEC 351, 1994].

Auto-surveillance

Fonction de sécurité indirecte qui déclenche une action de sécurité si l'aptitude d'un composant ou d'un constituant à assurer sa fonction diminue, ou si les conditions de fonctionnement sont modifiées de telle façon qu'il en résulte un risque [EN 292-1, 1991].

Il y a deux catégories d'auto-surveillance [EN 292-1, 1991] :

- auto-surveillance *continue*, par laquelle une mesure de sécurité est immédiatement déclenchée lorsque se produit une défaillance ;
- auto-surveillance *discontinue*, par laquelle une mesure de sécurité est déclenchée à l'occasion du cycle de fonctionnement de la machine qui suit immédiatement une défaillance.

Bloc fonctionnel

Système ou élément comportant une ou plusieurs variables d'entrée et une ou plusieurs variables de sortie, symbolisé principalement par un rectangle dans lequel la relation fonctionnelle entre les variables d'entrée et de sortie est donnée [CEI/IEC 351, 1994].

Cahier des charges

Le cahier des charges est un document régissant les rapports entre le fournisseur, concepteur d'un matériel commandé, et son client, l'utilisateur futur de ce matériel. On y retrouve l'ensemble des attentes que le client a par rapport au matériel à concevoir [BLANCHARD, M., 1979].

Cahier des charges fonctionnels (CdCF)

Document par lequel le demandeur exprime son besoin (ou celui qu'il est chargé de traduire) en terme de fonctions de service et de contrainte. Pour chacune d'elles sont définies des critères d'appréciation accompagnés d'une échelle permettant de situer leur niveau (de nature quantitative) et chaque niveau est assorti d'une flexibilité [LEMAY, É., 1995].

Capteur

Dispositif sensible à un phénomène physique et qui donne un signal représentant la valeur de ce phénomène [CEI/IEC 351, 1994].

Commande

Action délibérée sur ou dans un système, en vue d'atteindre des objectifs définis. Le terme *régulation* est parfois utilisé [CEI/IEC 351, 1994].

Compteur

Circuit séquentiel où un nombre est mémorisé et auquel est ajouté un nombre entier constant dépendant d'une variable de commutation à l'entrée du compteur [CEI/IEC 351, 1994].

Consignation

Procédure composée de l'ensemble des quatre actions suivantes [prEN 1037, 1994] :

- séparation de la machine (ou de parties définies de la machine) de toute source d'énergie ;
- condamnation (ou autre forme d'immobilisation) de tous les appareils de séparation ;
- dissipation ou rétention de toute énergie accumulée susceptible d'être à l'origine d'un phénomène dangereux ;
- vérification, par un mode opératoire sûr, que les actions mentionnées ci-dessus ont produit les effets désirés.

Danger

État ou situation dans lequel un dommage (une blessure, un effet néfaste pour la santé) est raisonnablement prévisible [CAN/CSA Z432-94, 1994]. Dans le langage courant, le mot «danger» est souvent remplacé par le mot «risque» [GAUTHIER, F., 1997].

Défaillance

Une défaillance se définit comme la non-réussite d'un équipement à accomplir sa tâche conséquemment à un bris interne de celui-ci [MERLAUD, C. et coll. 1992]. Une défaillance est un événement, par opposition au défaut qui est un état [prEN 954-1, 1996].

Défaut

État d'une entité inapte à accomplir une fonction requise, excluant l'inaptitude due à la maintenance préventive ou à d'autres actions programmées ou due à un manque de moyens extérieurs. Un défaut est souvent la conséquence d'une défaillance de l'entité elle-même, mais peut exister sans défaillance préalable [prEN 954-1, 1996].

Défaut aléatoire

Défaut dont la cause n'est pas reproductible et son apparition imprévisible [DIN 0019251, 1992].

Défaut externe

Défaut survenant par suite d'influence extérieure telle que la température, les perturbations électromagnétiques, l'humidité, les chocs, etc. [DIN 0019251, 1992].

Défaut interne

Défaut se produisant sans influence extérieure, par suite de défaillances de certains composants par exemple [DIN 0019251, 1992].

Défaut systématique

Défaut dont la cause peut être systématiquement identifiée et reproduite (cause déterministe) [DIN 0019251, 1992].

Diagramme fonctionnel (pour système de commande)

Outil graphique de description et de représentation symbolique des systèmes de commande séquentielle [CEI/IEC 351, 1994].

Disponibilité

La disponibilité est la période durant laquelle le systèmes automatisé est en état de marche et est disponible pour produire [MERLAUD, C. et coll., 1992].

Dispositif de protection

Dispositif (autre qu'un protecteur) qui élimine ou réduit le risque, seul ou associé à un protecteur [EN 292-1, 1991].

Dispositif de verrouillage associé à un protecteur

Dispositif de protection associé à un protecteur et qui, lorsqu'on déplace ce protecteur, agit de sorte que [INRS, 1983a] :

- la mise en marche de la machine soit impossible tant que le protecteur est ouvert ;
- l'ouverture du protecteur pendant la marche de la machine provoque un ordre d'arrêt, la fermeture du protecteur autorisant la mise en marche, mais ne la provoque pas.

Dispositif d'interverrouillage associé à un protecteur

Dispositif de protection associé à un protecteur et conçu de manière que [INRS, 1983a] :

- la mise en marche de la machine soit impossible tant que le protecteur est ouvert ;
- l'ouverture du protecteur soit impossible tant que la machine (la partie dangereuse de la machine) est en mouvement.

Dommage

Blessure physique ou atteinte à la santé affectant des personnes soit directement, soit indirectement comme conséquence à un dégât causé aux biens ou à l'environnement [ISO/CEI 51, 1997].

Effecteur

Organe, dans une machine, chargé d'effectuer les opérations nécessaires à la fabrication d'un produit.

Éprouvé

Un élément est considéré comme éprouvé s'il a fonctionné sans modification essentielle un nombre de fois suffisant, pendant une période suffisante et dans des applications différentes sans que l'on ait constaté aucun défaut, ou seulement des défauts acceptables [DIN 0019251, 1992].

Évaluation du risque

Processus dans lequel des jugements sont portés quant à l'acceptabilité du risque, sur la base de l'analyse du risque et compte tenu des facteurs tels que les aspects sociaux, économiques et environnementaux [ISO/CEI 51, 1997].

Événement dangereux

Situation dangereuse qui conduit à un dommage [ISO/CEI 51, 1997].

Erreur

Une erreur est une anomalie de conception ou une déviation d'un état prévu ou attendu [LEVESON, N.G., 1995].

Faute

Une faute est le manquement d'un équipement de fonctionner tel que prévu en raison de défaillances intrinsèques ou de fautes d'équipements situés en aval ou en amont du système. Une faute est donc une défaillance ou l'effet d'une défaillance [MERLAUD, C. et coll. 1992].

Fiabilité (d'une machine)

Aptitude d'une machine, ou de composants, ou d'équipements, à accomplir sans défaillance une fonction requise, dans des conditions données et pendant un laps de temps donné [EN 292-1, 1991].

Fonction analogique

Fonction logique provenant d'un signal continu permettant de transmettre des valeurs variables dans le temps, telles que le courant électrique, la température, la pression, etc.

Fonction chien de garde

Il s'agit d'un dispositif servant à s'assurer que l'automate procède à son balayage dans un laps de temps acceptable [FISHER, T.G. 1990].

Fonction dangereuse d'une machine

Toute fonction d'une machine qui engendre un phénomène dangereux lorsque la machine fonctionne [EN 292-1, 1991].

Fonction de sécurité (des systèmes de commande)

Fonction initiée par un signal d'entrée et traitée par les sorties du système de commande relatives à la sécurité et qui conduisent la machine (en tant que système) à atteindre un état sûr [prEN 954-1, 1996].

Par exemple, en activant la commande d'arrêt d'urgence d'un équipement, le signal d'entrée est traité par la logique (câblée ou programmée) et le signal de sortie correspondant ordonnera la mise à l'arrêt (ou tout autre état plus sécuritaire) de l'équipement en question.

Fonction de sécurité directe

Ce sont les fonctions d'une machine dont le dysfonctionnement augmenterait immédiatement le risque de lésion ou d'atteinte à la santé [EN 292-1, 1991].

Elles sont classées en deux catégories : celles destinées à assurer spécifiquement la sécurité et celles conditionnant la sécurité [KNEPPERT, M. 1995] [EN 292-1, 1991].

Fonction de sécurité indirectes

Ce sont des fonctions dont la défaillance n'engendre pas immédiatement un phénomène dangereux, mais abaisse cependant le niveau de sécurité [KNEPPERT, M. 1995] [EN 292-1, 1991].

Fonction séquentielle

Fonction logique ayant une séquence prévue et ne pouvant prendre que des valeurs prédéterminées (*0 Volt* ou *5 Volts*, *Marche* ou *Arrêt*, etc.). Ce type de fonctions logiques est généralement géré par des automates programmables industriels.

Fonctionnement manuel

Mode de fonctionnement dans lequel toutes les fonctions du système de commande sont remplies par un opérateur humain [CEI/IEC 351, 1994].

Fonctionnement automatique

Mode de fonctionnement dans lequel toutes les fonctions du système de commande de processus sont remplies sans intervention d'un opérateur humain [CEI/IEC 351, 1994].

Fonctionnement semi-automatique

Mode de fonctionnement dans lequel une partie seulement des fonctions du système de commande de processus est remplie sans intervention d'un opérateur humain [CEI/IEC 351, 1994].

Graphe d'état

Représentation symbolique des états consécutifs d'un circuit séquentiel où les états individuels sont représentés par des cercles et les fonctions de transition par des lignes [CEI/IEC 351, 1994]. Par exemple, le GRAFCET est un graphe d'état.

Information pour l'utilisation

L'ensemble des mesures de sécurité qui consistent en des messages tels que des textes, des mots, des signes, des signaux, des symboles ou des diagrammes, utilisés séparément ou associés entre eux pour transmettre des informations à l'utilisateur professionnel et/ou non professionnel [EN 292-1, 1991].

Inhibition

Interruption automatique et temporaire de fonction(s) de sécurité par des parties du système de commande relatives à la sécurité [EN 954-1, 1996].

Intellectualiser

Revêtir d'un caractère intellectuel ; transformer par l'action de l'intelligence [Dictionnaires Le ROBERT, 1993]. Ce mot est associé au concept d'*intelligence artificielle* dans ce mémoire.

Intelligence artificielle (en commande automatique)

Aptitude d'un dispositif ou d'un système à accomplir des fonctions normalement associées à l'intelligence humaine comme le raisonnement, l'apprentissage et l'auto-perfectionnement [CEI/IEC 351, 1994].

Interface

Frontière commune entre deux entités fonctionnelles, définie par des caractéristiques fonctionnelles, des caractéristiques de signal, ou d'autres caractéristiques appropriées [CEI/IEC 351, 1994].

Interverrouillage

Action d'interrelier des dispositifs de verrouillage, à les rendre dépendants entre eux [INRS, 1983a].

Ladder

Langage de programmation très répandu pour les API. C'est de sa structure, en forme d'échelle (*ladder*), qu'a été emprunté son nom [COX, R.A., 1995].

Logiciel

Le logiciel est l'ensemble des programmes, procédés, règles et éventuellement de la documentation relatifs au fonctionnement d'un ensemble de traitement de l'information [JAULENT, P., 1992].

Logique (ou système logique)

Partie d'un système qui traite les fonctions logiques [ET, OU, SI, etc.] mais ne les exécute pas [CEI/IEC 1508-4, 1995].

Logique câblée

Type de logique où les opérateurs logiques matériels sont souvent réunis par des conducteurs électriques. Elle peut être de type électronique, électromécanique, pneumatique, hydraulique, etc. [DEI-SVALDI, D. et coll., 1996].

Il existe aussi des logiques câblées dont les fonctions sont entièrement assurées par des sources d'énergie autres que l'électricité, comme l'énergie pneumatique ou hydraulique.

Logique programmée

Type de logique où les opérateurs et les liaisons entre ceux-ci sont déterminés par un logiciel [DEI-SVALDI, D. et coll., 1996].

Machine

Ensemble de pièces ou d'organes liés entre eux, dont au moins un est mobile et, le cas échéant, d'actionneurs, de circuits de commande et de puissance, etc., réunis de façon solidaire en vue d'une application définie, notamment pour la transformation, pour le traitement, le déplacement ou le conditionnement d'un matériau.

Est également considéré comme *machine* un ensemble de machines qui, afin de concourir à un même résultat, sont disposées et commandées de manière à être solidaires dans leur fonctionnement [EN 292-1, 1991]. Dans ce cas, il est également question de *système de production* [BOUTEILLE, B. et coll., 1996]

Maintenabilité (d'une machine)

Aptitude d'une machine à être maintenue dans un état lui permettant d'accomplir sa fonction dans les conditions normales d'utilisation, ou à être remise dans un tel état, les actions nécessaires (maintenance) étant accomplies suivant des procédures et avec des moyens prescrits [EN 292-1, 1991].

Mauvais usage raisonnablement prévisible

Utilisation délibérée ou non d'un produit d'une façon anormale ou pour une tâche qui n'est pas la sienne [MUSTER, D., 1985].

Utilisation d'un produit, d'un procédé ou d'un service dans des conditions ou à des fins non prévues par le fournisseur, mais qui peut être induite par le comportement humain habituel en conjonction avec la conception du produit, du procédé ou du service, ou comme résultat de ce comportement [ISO/CEI 51, 1997].

Il convient de prendre particulièrement en compte les comportements suivants lors de l'identification des risques de mauvais usages [GAUTHIER, F., 1997] :

- le comportement anormal résultant d'une négligence ordinaire, sans toutefois être volontairement dans le but de faire un mauvais usage ;
- le comportement de certaines personnes, telles que les enfants ou les personnes handicapées [EN 292-1, 1991] ;
- le comportement réflexe d'une personne en cas de dysfonctionnement, d'incident, de défaillance, etc. ;
- le comportement résultant de l'application de la *loi du moindre effort*.

Mesure de prévention

Application de différentes méthodes de réduction du risque en vue d'obtenir au moins le risque tolérable (les mesures de prévention comprennent la sécurité intrinsèque, les protecteurs, les équipements de protection individuelle, l'information pour l'installation et l'utilisation, et la formation) [ISO/CEI 51, 1997].

Mise en marche

Passage du repos au mouvement d'une machine ou de l'un de ses éléments [prEN 1037, 1994].

Mise en marche imprévue (intempestive)

Toute mise en marche qui, à cause de sa nature imprévue, engendre un risque (de dommage) pour les personnes [EN 292-1, 1991].

Modèle

Un modèle est une représentation d'un système qui vise à en faciliter la compréhension, en mettant en évidence certains aspects ou certaines parties et en ignorant les autres [PLANCHE, R., 1988].

Opérateur

Personne chargée du fonctionnement de l'équipement [CAN/CSA Z432-94, 1994].

Opération booléenne

Fonction de commutation pour des variables de commutation binaires, basée sur des opérations algébriques booléennes [CEI/IEC 351, 1994]. Essentiellement, les opérations booléennes sont ET, OU et NON [LACHIVER, G., 1995].

Phénomène dangereux

Une source potentielle de dommage [ISO/CEI 51, 1997]. Le terme phénomène dangereux est généralement qualifié par son origine ou la nature du dommage causé. En français, le terme risque est très souvent employé au lieu de phénomène dangereux (par exemple, risque de choc électrique, risque d'écrasement, risque de coupure, risque toxique, risque d'incendie, risque de noyade, etc.) [ISO/CEI 51, 1997] [EN 292-1, 1991].

Prévention intrinsèque

L'ensemble des mesures de sécurité qui consistent à [EN 292-1, 1991] :

- éviter ou réduire autant de phénomène dangereux que possible en choisissant convenablement certains facteurs de la conception de la machine ;
- limiter l'exposition des personnes aux phénomène dangereux inévitables ou qui ne peuvent être suffisamment réduits.

Procédé

Principe d'élaboration d'un produit préalablement défini. Il est par essence immatériel [BIERCE, B. et coll. 1994].

Processeur

Dans un ordinateur, organe [micro-électronique] destiné à interpréter et exécuter les instructions [Dictionnaires Le Robert, 1993].

Processus

Ensemble d'opérations conjuguées par lesquelles de la matière, de l'énergie ou des informations sont transformées, transportées ou stockées [CEI/IEC 351, 1994].

Suite ordonnée d'opérations conduisant à un résultat [BIERCE, B. et coll. 1994].

Produit

Selon l'*Association française pour l'analyse de la valeur* [1989], le produit est ce qui est fourni à un utilisateur pour répondre à son besoin.

Programme (informatique)

Le programme assure le déroulement automatique de la fonction pour laquelle le système est prévu sans aucune intervention de la part de l'homme. Il est introduit par la programmation, ou encore par une disquette programmée. [AISS 1989]

Protecteur

Élément de machine utilisé spécifiquement pour réaliser une protection par obstacle (porte, barrière, écran, etc.) [INRS, 1983a]

Protecteur fixe

Protecteur immobilisé soit de manière permanente (soudé, etc.), soit au moyen d'assemblage (vis, etc.) rendant sa dépose impossible sans outils. [INRS, 1983a]

Protecteur mobile

Protecteur lié mécaniquement au bâti d'une machine ou à un élément fixe voisin, généralement par une articulation ou un guidage rectiligne et qu'il est impossible d'ouvrir sans faire usage d'aucun outil. [INRS, 1983a]

Protecteur réglable

Protecteur fixe ou mobile qui est réglable dans son ensemble ou qui comporte des parties réglables. Le réglage demeure fixe pendant une opération particulière [EN 292-1, 1991].

Protection

L'ensemble des mesures de sécurité qui consistent en l'emploi de moyens techniques spécifiques, appelés protecteurs et dispositifs de protection, afin de protéger les personnes contre les phénomènes dangereux que l'application des techniques de prévention intrinsèque ne permet raisonnablement ni d'éviter ni de limiter suffisamment [EN 292-1, 1991].

Redondance

Existence, dans une entité, de plus d'un moyen pour exécuter une fonction spécifiée [CEI/IEC 351, 1994].

Revue de conception

De manière générale, une revue de conception consiste en l'étude d'une conception, menée de façon complète et systématique à l'aide de documents, en vue d'évaluer sa capacité à satisfaire aux exigences du client, d'identifier les problèmes et, s'il y a lieu, de proposer le développement de solutions [BURGESS, J.A., 1984] [ISO 8402, 1994]

Risque

Une combinaison de la probabilité d'occurrence d'un dommage et de la gravité de ce dernier [ISO/CEI 51, 1997]. Le risque est une mesure d'un phénomène dangereux [MERLAUD, C. et coll., 1992].

Risque résiduel

Risque restant après que toutes les mesures de préventions aient été prises [ISO/CEI 51, 1997].

Risque tolérable

Risque accepté dans un certain contexte et fondé sur les valeurs actuelles de la société [ISO/CEI 51, 1997].

Robot industriel

Manipulateur multifonctionnel reprogrammable servant à déplacer du matériel, des parties de matériel, des outils ou des dispositifs spécialisés par le biais de mouvements programmés [CAN/CSA Z434 94, 1994].

Schéma fonctionnel

Représentation symbolique des actions dans un système par des blocs fonctionnels reliés par des lignes d'action [CEI/IEC 351, 1994].

Sécurité (d'une machine)

Aptitude d'une machine à accomplir sa fonction, à être transportée, installée, mise au point, entretenue, démontée et mise au rebut dans les conditions d'utilisation normales spécifiées dans la notice d'instructions et, dans certains cas, en deçà de la limite de temps fixée dans la notice d'instructions sans causer de lésions ou d'atteinte à la santé [EN 292-1, 1991].

Sécurité des systèmes de commande

Aptitude des parties relatives à la sécurité d'un système de commande à exécuter leur(s) fonction(s) de sécurité pendant un temps donné [prEN 954-1, 1996].

Sécurité positive

Situation théorique qui serait réalisée si une fonction de sécurité restait assurée en cas de défaillance du système d'alimentation en énergie ou de tout composant contribuant à la réalisation de cette situation [EN 292-1, 1991].

Signal

Grandeur physique dont un ou plusieurs paramètres sont porteurs d'informations concernant une ou plusieurs variables que le signal représente [CEI/IEC 351, 1994].

Situation dangereuse

Toute situation dans laquelle une personne est exposée à un ou plusieurs phénomènes dangereux [ISO/CEI 51, 1997] [EN 292-1, 1991].

Sûreté (de fonctionnement)

La sûreté de fonctionnement englobe à la fois la sécurité, la fiabilité et la disponibilité de la machine [MERLAUD, C. et coll. 1992].

La sûreté de fonctionnement englobe aussi parfois la maintenabilité et certains aspects de la qualité [ROUCHOUSE, G., 1992].

Sûreté intrinsèque

La sûreté intrinsèque est atteinte lorsque le niveau de sécurité d'un équipement est tel que le risque qu'un dommage survienne est négligeable.

Système

Un système est un ensemble de composants fonctionnant ensemble pour atteindre un certain nombre d'objectifs communs [PLANCHE, R., 1988].

Système commandé

Système sur lequel une commande est exercée [CEI/IEC 351, 1994].

Système d'arrêt d'urgence

Système ayant pour unique fonction d'arrêter de façon sécuritaire tout procédé dès qu'une faute suffisante est détectée.

Système de commande

Système constitué par un système commandé (réglé) et par son équipement de commande (de régulation), avec les transducteurs qui lui sont associés. Le terme *équipement de commande* est également parfois employé [CEI/IEC 351, 1994].

Système de contrôle distribué (SCD, de l'anglais *Distributed Control System, DCS*)

Composant électronique à base de microprocesseurs qui comporte une mémoire pouvant être programmée par un informaticien (ou d'autres personnes ayant de bonnes connaissances de l'informatique) à l'aide d'un langage adapté. Le SCD a pour fonction de commander, mesurer et contrôler, au moyen de modules d'entrées et de sorties, différentes sortes de machine ou de processus en environnement industriel [EDWARDS, R. et coll., 1992]

Le SCD traite généralement les fonctions analogiques, mais il peut aussi traiter les fonctions séquentielles.

Un terme français plus reconnu existe. Il s'agit d'un *système d'ordinateurs répartis* (SOR) [BOUCHARD, G., 1997]. Cependant, étant donné qu'il n'est que très peu répandu, le terme SCD, traduit de l'anglais, sera employé dans ce mémoire

Système de production

Un système de production est un processus permettant d'apporter une valeur ajoutée : partant de matière première, il élabore des produits de valeur supérieure (produits intermédiaires, produits finis, etc.) [BOUTEILLE, D. et coll., 1996].

Système d'information

Un système d'information est un système qui a pour objectifs de rassembler, de traiter, de manipuler et de fournir les informations nécessaires à certaines activités [PLANCHE, R., 1988].

Transmetteur

Les transmetteurs, dans un système de production automatisé, permettent de transmettre au système de commande les diverses informations provenant des capteurs.

Utilisation attendue

L'utilisation d'un produit, procédé ou service conformément aux spécifications, instructions et informations données par le fournisseur [ISO/CEI 51, 1997] [EN 292-1, 1991].

Verrouillage

Dispositif mécanique, électrique ou autre destiné à empêcher le fonctionnement d'une machine dans certaines conditions. [INRS, 1983a]

Zone dangereuse

Toute zone à l'intérieur et/ou autour d'une machine dans laquelle une personne exposée est soumise à un risque vis-à-vis de sa santé ou de sa sécurité [EN 292-1, 1991].

1. INTRODUCTION

L'introduction des technologies programmables comme les automates programmables industriels (API) et les systèmes de contrôle distribués (SCD) dans l'industrie québécoise des pâtes et papiers (P&P) a permis à ce secteur industriel d'accroître sa compétitivité et d'améliorer plusieurs conditions de travail. Néanmoins, l'introduction de ces nouvelles technologies a amené également de nouveaux problèmes de sécurité, soit des accidents directement liés à ces technologies [PAQUES, J.-J., 1991].

À la demande des papetières du Québec, l'*Institut de recherche en santé et sécurité du travail* du Québec (IRSST) a mis sur pied un vaste projet de recherche dont l'objectif ultime est de rendre plus sécuritaires l'opération et l'entretien des systèmes de production automatisés (SPA) dotés d'API et/ou de SCD. La stratégie envisagée pour atteindre cet objectif est de faire en sorte que les concepteurs de l'industrie québécoise des P&P développent les compétences nécessaires pour intégrer les aspects de sécurité aux SPA, et ce, dès leur conception. L'objet de ce projet de maîtrise consiste donc à développer une méthodologie de conception sécuritaire et adaptée aux pratiques des concepteurs de cette industrie.

Or, selon une étude menée par l'IRSST, *«[...] une cause commune d'accidents est la mauvaise adaptation aux besoins et à un usage sécuritaire des outils, des machines et des procédés industriels»* [BÉLANGER, R. et coll., 1991]. Ainsi, une méthodologie de conception devrait permettre aux concepteurs de mieux tenir compte des besoins liés à l'opération et à l'entretien des SPA qu'ils conçoivent. Pour y parvenir, plusieurs techniques existent, comme l'analyse fonctionnelle et son cahier des charges, le GRAFCET (*graphe de commande-étape-transition*), le GEMMA (*guide d'étude des modes de marche et d'arrêt*), etc. Il serait donc intéressant de voir, parmi les outils d'aide à l'analyse des besoins fonctionnels, lesquels pourraient être intégrés à la méthodologie de conception de même que la manière qu'ils pourraient l'être.

D'autre part, l'utilisation de méthodes d'analyse du risque constitue un moyen très efficace permettant d'identifier divers phénomènes dangereux pour ensuite trouver des solutions en vue de les maîtriser. Cependant, la plupart de ces méthodes ont été développées par des spécialistes en

sécurité issus des domaines de l'industrie chimique et nucléaire ; elles ne s'adaptent donc pas toujours très bien au travail des concepteurs dans le domaine des P&P [GAUTHIER, F., 1994]. Néanmoins, l'intégration de quelques méthodes d'analyse du risque aux activités de conception pourrait être une avenue intéressante.

Aussi, il existe plusieurs principes techniques permettant d'éviter que certains problèmes de sécurité ne surviennent. Par exemple, les programmes d'API peuvent être protégés en utilisant certains types de mémoire, la fiabilité des systèmes de commande peut être accrue grâce à des techniques de redondance, etc. Il pourrait alors être intéressant d'envisager l'intégration systématisée de quelques uns de ces principes à la méthodologie de conception.

Par ailleurs, pour que cette méthodologie soit réellement exploitée par les concepteurs de l'industrie québécoise des P&P, il est essentiel qu'elle tienne compte de leurs pratiques actuelles de même que des contraintes auxquelles ils sont soumis. Ainsi, suite à une série d'activités réalisées (visites d'usines, groupes de discussion, etc.), des informations provenant du milieu des papetières québécoises ont été obtenues. La prise en compte de ces dernières facilitera l'intégration de la méthodologie dans le secteur des papetières.

Le présent mémoire est subdivisé en quatre chapitres. Le chapitre 2 passe tout d'abord en revue l'état des connaissances sur les sujets d'intérêt dans le cadre de la recherche. La problématique découlant de l'état des connaissances est par la suite exposée au chapitre 3. Le chapitre 4 détaille l'objectif principal ainsi que les objectifs intermédiaires associés à la recherche. Puis, le chapitre 5 est consacré à la présentation de la méthodologie développée et des résultats obtenus. Finalement, la conclusion suivie des annexes et des appendices complètent ce mémoire.

En dernier lieu, il importe de souligner l'importance pour le lecteur de se référer constamment au lexique établi dans les pages préliminaires du présent document, car le vocabulaire utilisé dans ce mémoire, notamment en matière de sécurité, est très précis et diffère considérablement de celui utilisé au quotidien.

2. ÉTAT DES CONNAISSANCES

Ce chapitre permettra au lecteur de se familiariser avec l'ensemble des connaissances répertoriées pour ce mémoire. Le lecteur y trouvera des informations concernant l'automatisation de la production, les problèmes qu'elle a apportés au point de vue de la santé et de la sécurité du travail (SST) et les divers travaux effectués pour contrer cette problématique. En plus des informations recueillies dans diverses littératures, les textes normatifs viendront, lorsqu'applicables, enrichir l'état des connaissances. Également, lorsque disponibles, des informations relevant spécifiquement de l'industrie des pâtes et papiers (P&P) du Québec seront introduites.

L'état des connaissances est divisée en deux principales sections. La première sert à effectuer une mise en contexte et à mettre en relief divers problèmes liés à l'automatisation des systèmes de production. La seconde dresse un aperçu des diverses approches et méthodes favorisant la conception de système de production automatisé (SPA) sécuritaire.

2.1 Mise en contexte et problématique

Cette section permet dans un premier temps de situer le lecteur dans le contexte de cette recherche. En premier lieu, le concept d'automatisation de la production est introduit : son évolution, ses objectifs, ses contraintes et sa représentation sont détaillés. Par la suite, la partie commande des SPA est définie, puis sa composition et ses applications courantes sont établies. Finalement, des problèmes spécifiques à la SST reliés à l'automatisation de la production sont mis en relief.

2.1.1 Automatisation de la production

D'une façon tout à fait générale, *«l'automatisation consiste à remplacer l'homme par une machine pour l'exécution d'une tâche»* [CHALVET, J. 1966]. D'autre part, la production est l'ensemble des étapes permettant de partir de la matière première (comme le bois) pour en venir à un produit final (comme le papier ou les meubles) [BOUTEILLE, D. et coll., 1996]. L'automatisation de la production consiste donc, de façon tout à fait générale, à implanter des

de remplacer l'humain dans certaines tâches implicites à la fabrication des divers biens et services nécessaires à sa survie ou à son bien-être.

Cette section offre d'abord une brève revue de l'évolution des outils de production. Par la suite, la structure générale d'un système de production automatisé ainsi que les constituants sont présentés.

2.1.1.1 Évolution de la production

Globalement, on peut ramener toute production à la combinaison de trois éléments fondamentaux, soit *l'énergie*, la *commande* et le *contrôle*. Dans le présent contexte ces trois éléments sont définis comme suit [BOURBONNIÈRE, R. et coll., 1997] :

- l'*énergie* correspond à la *«propriété d'un système physique capable de produire du travail»* (énergie électrique, énergie pneumatique, etc.) [Dictionnaires Le ROBERT, 1993] ;
- la *commande* englobe les ordres, les choix ou les actions qui vont entraîner la libération des énergies nécessaires à la transformation du produit ;
- le *contrôle* est constitué des actions prises pour s'assurer que les objectifs de travail seront remplis dans les meilleures conditions possibles (contrôle de la qualité par exemple).

À l'aide de ces trois concepts, l'évolution des outils de production peut être présentée en quatre phases distinctes : ils ont tout d'abord été manuels, puis mécanisés, puis automatisés pour finalement être intellectualisés[1] [BOURBONNIÈRE, R. et coll. 1997] [GOSH, K. et coll., 1989]. La figure qui suit fait la synthèse des quatre phases d'évolution de la production en faisant ressortir l'apport respectif de l'homme (H) et de la machine (M) en fonction de l'énergie, de la commande et du contrôle. Ces quatre phases d'évolution sont par la suite présentées une à une.

[1] Le mot *intellectualiser* réfère à la notion d'*intelligence artificielle*, concept encore expérimental.

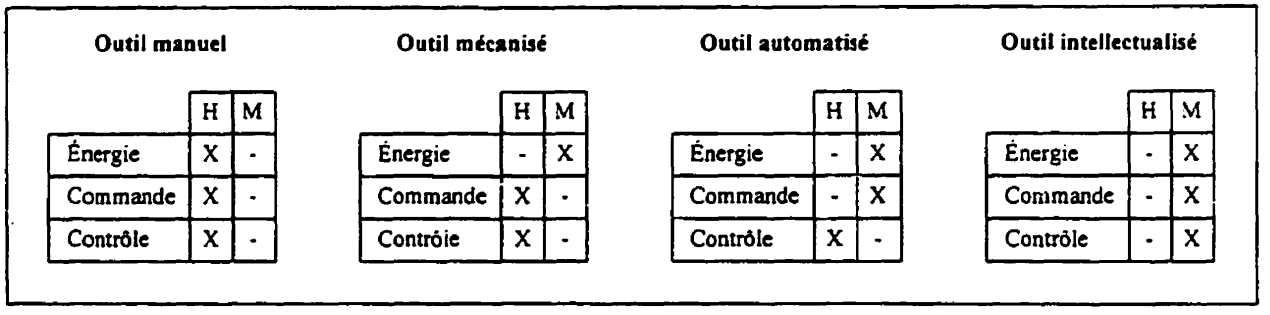

Figure 2.1 Les quatre phases de l'évolution de la production

La première phase correspond à *l'outil manuel* où l'énergie, la commande et le contrôle dépendent de l'homme. Par exemple, les outils de chasse que l'homme a conçu dans sa préhistoire sont probablement ses premiers outils manuels. Cependant, les besoins de l'homme sont grands : il doit se vêtir, se loger et se nourrir. Pour s'aider dans sa quête, il conçoit des outils de plus en plus élaborés, mais il commence à s'apercevoir qu'une aide extérieure pourrait lui être bénéfique [CHALVET, J., 1966].

Avec la domestication des animaux (2 000 ans av. J.C.), il accède à la phase de *mécanisation* où il commence à utiliser des formes d'énergie autres que sa force physique. Au fil des ans, ces dernières deviennent de plus en plus élaborées et variées : la force hydraulique (300 av. J.C.), le vent (718) puis la découverte énergétique qui a provoqué un grand virage technologique, la machine à vapeur de Watt (1775) sont des exemples d'énergies auxquelles l'homme a recours. Parallèlement à ces découvertes, l'élaboration de systèmes mécaniques se raffinait. Les grands maîtres, comme Léonard de Vinci, Salomon De Caus, Denis Papin et Vaucanson, pour n'en nommer que quelques uns, ont permis d'allier les découvertes énergétiques aux systèmes de production [CHALVET, J., 1966]. La mécanisation des outils de production allait dorénavant permettre d'accroître la production des biens et services dont l'homme a besoin.

Cependant, avec la révolution industrielle, le nombre de systèmes de production mécanisés augmente considérablement. Au fil des années, la compétition entre les divers fabricants oblige à produire plus rapidement, à moindre coût et avec une meilleure qualité. Les systèmes de production mécanisés ne suffisaient plus à la tâche : il fallait trouver de nouvelles façons de produire.

En remplaçant la commande humaine des systèmes de production par des technologies plus précises et plus rapides, la compétitivité des industries pouvait être accrue. La phase *d'automatisation* était maintenant entamée. Les premiers automatismes comportaient divers systèmes mécaniques assurant l'autonomie des fonctions, tels que les ressorts ou les cartes perforées. Avec l'apparition des relais électromécaniques en 1940, une nouvelle génération d'automatisation des systèmes de production naissait [ROUCHOUSE, G., 1992]. La commande du système était maintenant assurée par une disposition judicieuse de bobines et de contacts électriques qui activaient ou désactivaient, au moment prévu, les divers constituants de l'outil de production : cette technologie s'appelle la *logique câblée*. C'est avec l'arrivée des premiers ordinateurs que l'automatisation de la production a subi un nouveau virage. Plutôt que d'assurer la logique du système par une combinaison de composants électriques et électromécaniques (bobines, minuteries, relais, etc.), elle relevait maintenant d'un logiciel ; la logique programmée était née. L'arrivée de l'électronique programmable dans les commandes de mécanismes, aux alentours de 1965, a ainsi permis une percée de l'automatisation dans tous les secteurs industriels [BOUTEILLE, D. et coll., 1996].

Finalement, la phase *d'intellectualisation* est celle où, en plus de l'énergie et de la commande, le contrôle de l'outil de production ne dépend plus de l'action humaine ; il est alors souvent question d'intelligence artificielle. Ce type de système de production est relativement nouveau et n'est que très peu répandu dans l'industrie, pour ne pas dire inexistant.

2.1.1.2 Évolution de la production du papier

Que ce soit lors de la mise en forme du papyrus par les Égyptiens ou des fibres provenant de divers végétaux, la production du papier a tout d'abord été manuelle. De l'opération du défibrage au séchage en passant par la formation de la feuille et son pressage, toutes les étapes étaient manuelles. Au Québec, la première fabrique de papier a été installée à Saint-André-d'Argenteuil en 1803 [CHARLAND, J.-P., 1990]. Le papier y était fait de façon manuelle. La figure qui suit illustre la mise en forme manuelle d'une feuille de papier.

Figure 2.2 Fabrication manuelle du papier [DAWSON, S., 1994]

Cependant, comme l'illustre cette figure, la fabrication manuelle du papier est fastidieuse et longue. De plus, avec la mise en place des imprimeries, les besoins en papier augmentaient sans cesse ; la mécanisation des étapes s'imposait. La figure qui suit illustre un exemple de système de production mécanisé remplaçant la fabrication manuelle du papier : le simple fait d'ajouter une énergie externe pour entraîner l'engrenage principal (une roue à eau par exemple) permettait la fabrication d'une feuille de papier en continu.

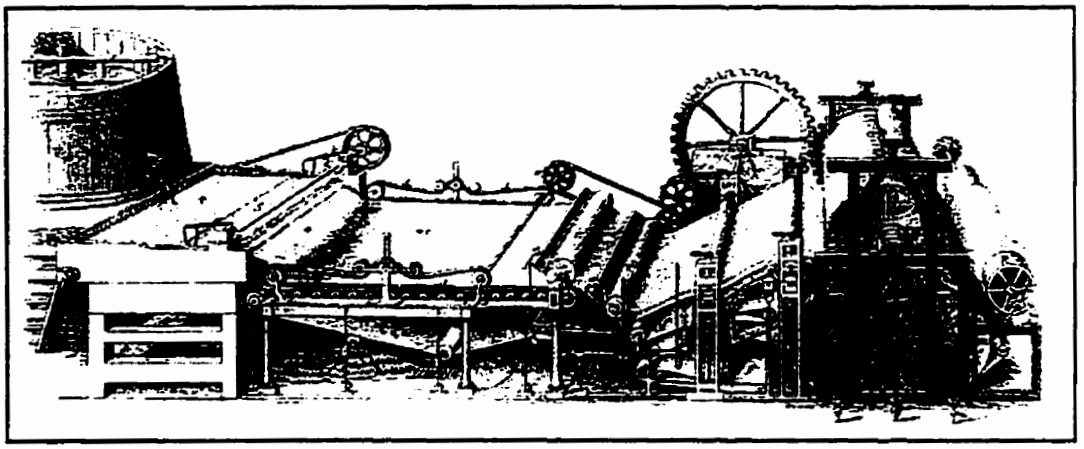

Figure 2.3 Machine à papier mécanisée (19^{e} siècle) [DAWSON, S., 1994]

En 1837, à Portneuf, la première machine à papier mécanisée a été installée au Québec. Cette machine pouvait produire une feuille de papier continue d'une largeur approximative de 1 mètre

(36 pouces) à une vitesse de production d'environ 7 km/h (30 pieds par minute) [CHARLAND, J.-P., 1990]. Malgré ce grand avancement technique, la demande dépassait toujours largement la capacité de production des outils mécanisés.

L'automatisation des outils de production allait enfin permettre à l'industrie québécoise des pâtes et papiers (P&P) de répondre à la demande. Comme dans tous les secteurs industriels, l'industrie des P&P accroît à un rythme exponentiel leur niveau d'automatisation. Utilisant d'abord la technologie de logique câblée, les besoins d'automatisation des machines étaient tels que la technologie de l'informatique a tôt fait son entrée dans le monde des P&P. Ainsi, en 1961, la papetière située à Lewiston (Idaho, États-Unis) était la première au monde à utiliser les services d'un ordinateur. Au Québec, c'est en 1963 que la *Canadian International Paper* faisait entrer cette technologie [CHARLAND, J.-P., 1990]. Aujourd'hui, le niveau d'automatisation des papetières permet la production de feuille ayant parfois une largeur de près de 10 mètres. Aussi, les vitesse moyennes de production sont d'environ 100 km/h, alors que les records oscillent autour de 160 km/h. La figure qui suit illustre une machine à papier qu'il est possible de rencontrer aujourd'hui dans n'importe quelle papetière québécoise.

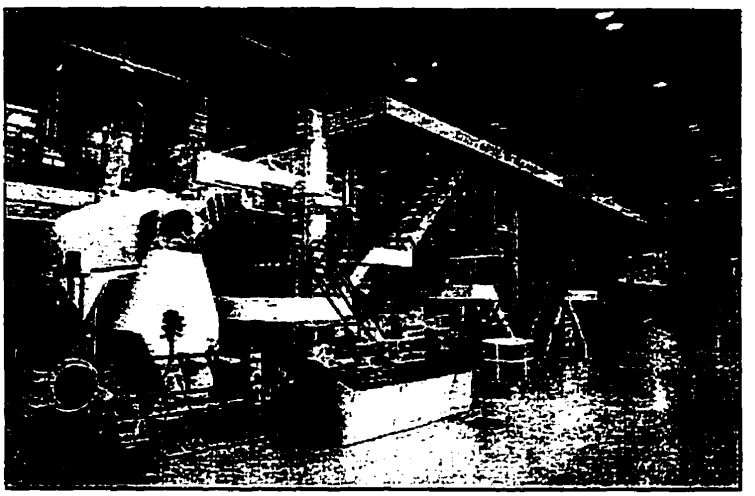

Figure 2.4 Machine à papier automatisée d'aujourd'hui [Helsinki University, 1997]

Comme la phase d'intellectualisation de la production n'est pas encore implantée dans l'industrie papetière du Québec et qu'en fait, la phase d'automatisation, très fortement entamée dans cette

industrie, pose encore aujourd'hui plusieurs difficultés, notamment en ce qui a trait à son niveau de sécurité, il sera dorénavant question de concept se rattachant à l'*automatisation*.

2.1.1.3 Objectifs et contraintes de l'automatisation

Les technologies d'automatisation se sont raffinées au fil des ans et aujourd'hui, le principal défi vise à augmenter la sûreté de fonctionnement des outils de production, c'est-à-dire de faire en sorte que ces derniers soient plus sécuritaires, plus faciles à entretenir et plus fiables de manière à ce qu'ils offrent plus de temps où ils sont disponibles pour produire[2]. Ces derniers doivent être plus performants, présenter moins de défaillances et, en cas de fautes, être réparés plus rapidement. Cette augmentation de la sûreté de fonctionnement a pour essentiel but l'atteinte des objectifs de l'automatisation, à savoir [BOUTEILLE, D. et coll., 1996] :

- diminuer les coûts de production ;
- augmenter la vitesse de production ;
- augmenter la qualité des produits ;
- améliorer les conditions de travail ;
- réaliser des opérations presque impossibles à réaliser autrement.

Aujourd'hui, la sûreté de fonctionnement de l'outil de production, notamment sa disponibilité, est d'une importance cruciale. Par exemple, pour une panne durant une heure chez le fabricant *Peugeot*, la compagnie est privée de la vente de 100 voitures, ce qui représente une perte de 4 millions de francs [ROUCHOUSE, G., 1992].

Cependant, en plus de l'augmentation de la disponibilité des outils de production, l'accroissement du niveau de sécurité est également très important. Dans son article, R.C. Waterbury [1991] énonce trois motifs valables justifiant l'implantation de SPA aussi sécuritaires que possible :

- sauvegarder des vies humaines, tant à l'intérieur qu'à l'extérieur de l'entreprise ;
- éviter des catastrophes environnementales ;
- protéger les investissements de l'entreprise.

---

[2] La sûreté de fonctionnement englobe donc à la fois la sécurité, la fiabilité, la maintenabilité et la disponibilité d'un équipement [MERLAUD, C., et coll., 1992] [ROUCHOUSE, G., 1992].

En revanche, il semble exister un conflit entre la sécurité et la disponibilité. En effet, pour accroître le niveau de sécurité d'un SPA, les pratiques couramment rencontrées en industrie visent très souvent à installer divers dispositifs de protection [GAUTHIER, F., 1997]. Il s'agit d'une pratique curatrice et qui résulte parfois en des solutions mal adaptées à l'usage et à l'entretien sécuritaire des SPA. Ainsi, il arrive à l'occasion que la conséquence directe de ces solutions est de diminuer la disponibilité de l'outil de production [ROUCHOUSE, G., 1992]. Par exemple, l'obligation pour un opérateur d'abaisser un garde protecteur pour se protéger d'une zone dangereuse à chaque fois qu'il veut qu'un équipement produise puis de devoir le relever dès que la pièce est prête fait en sorte que la disponibilité de l'équipement est considérablement diminuée, et ce pour des raisons de sécurité. Il apparaît donc que les objectifs de sécurité peuvent parfois être conflictuels avec les objectifs de productivité, d'où l'importance de s'assurer que les solutions retenues pour la sécurité entraveront le moins possible la productivité de l'équipement. D'ailleurs, plusieurs ouvrages abondent dans ce sens, dont la norme européenne EN 292 [1991].

2.1.1.4 Structure d'un système de production automatisé (SPA)

Avant d'introduire le concept de SPA, il convient de définir la machine automatisée. Cette dernière comporte essentiellement deux parties : une partie opérative (PO) et une partie commande (PC). La PO est celle qui agit sur la matière première (bois) pour effectuer sa transformation en vue d'obtenir un produit (papier) ; elle est donc principalement mécanique. Quant à elle, la PC est celle qui commande toutes les fonctions nécessaires à la réalisation adéquate des opérations effectuées par la PO ; c'est elle qui garantie l'automatisation des opérations. La figure suivante représente la structure élémentaire d'une machine automatisée.

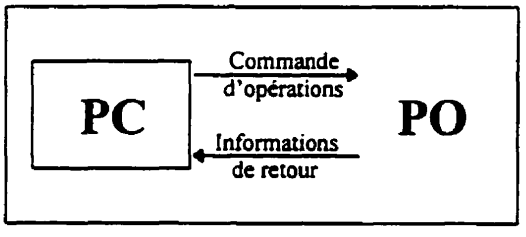

Figure 2.5 Structure élémentaire d'une machine automatisée

Un peu comme le cerveau humain, la partie commande reçoit toutes sortes d'informations, les traite puis retourne les réponses adéquates. La partie opérative peut, de la même manière, être associée au reste du corps : elle capte des informations, les transmet à la partie commande et exécute les ordres envoyés en retour. Par analogie, au même titre que l'humain possède à la fois un cerveau et un corps, les PC et PO sont parties intégrantes de la machine automatisée.

Bien qu'il n'existe aucune définition reconnue, un SPA peut être défini selon sa composition. Ainsi, un SPA est généralement composé d'au moins deux machines automatisées qui peuvent être agencées de plusieurs façons. Le premier type d'agencement est celui où toutes les machines sont autonomes et indépendantes. Il s'agit de la plus simple structure d'un SPA. Cependant, cette façon de procéder offre très peu de flexibilité pour l'ensemble du système. Pour accroître cette flexibilité et la coordination entre les machines, plusieurs façons de faire ont été élaborées. La figure 2.6 (page suivante) illustre l'évolution des structures du système de production automatisé, partant des machines autonomes pour terminer avec un système automatisé flexible, indépendant et coordonné.

Selon cette figure, la dernière structure présentée est la plus élaborée actuellement. La gestion et la coordination de l'ensemble des opérations du système sont assurées par un dispositif de supervision agissant sur et entre chacune des parties commandes des machines. Cet agencement offre une très grande flexibilité au système de production. Par exemple, si la machine 2 venait qu'à tomber en panne, alors la PC2 en aviserait la console de supervision ainsi que la PC1 et la PC3. L'opérateur étant maintenant conscient de l'état du SPA, il peut prendre la meilleure décision : continuer la production des machines 1 et 3 en reportant les activités de la machine 2 à plus tard, interrompre la production, etc.

Machines autonomes
Chaque machine réalise une étape dans l'élaboration du produit. Cette façon de faire est très peu flexible et nécessite de la manutention.

Machines associées en ligne
La structure du système est la même, à l'exception que le produit n'est pas manutentionné entre les postes. Si une machine fait défaut, le SPA entier est alors paralysé.

Cellule de production à commande centralisée
Cette façon de faire a permis d'accroître la coordination entre les machines mais a compliqué les interventions locales de réglage, etc.

Cellule à commande décentralisée et coordonnée
La décentralisation s'est donc imposée, mais on y a ajouté la coordination entre les machines.

Cellule flexible à commande répartie et hiérarchisée
Les machines peuvent traiter ou non les produits présentés (flexibilité) et des liaisons iso-niveau complètent le dialogue avec l'automatisme, assurant ainsi une meilleure coordination.

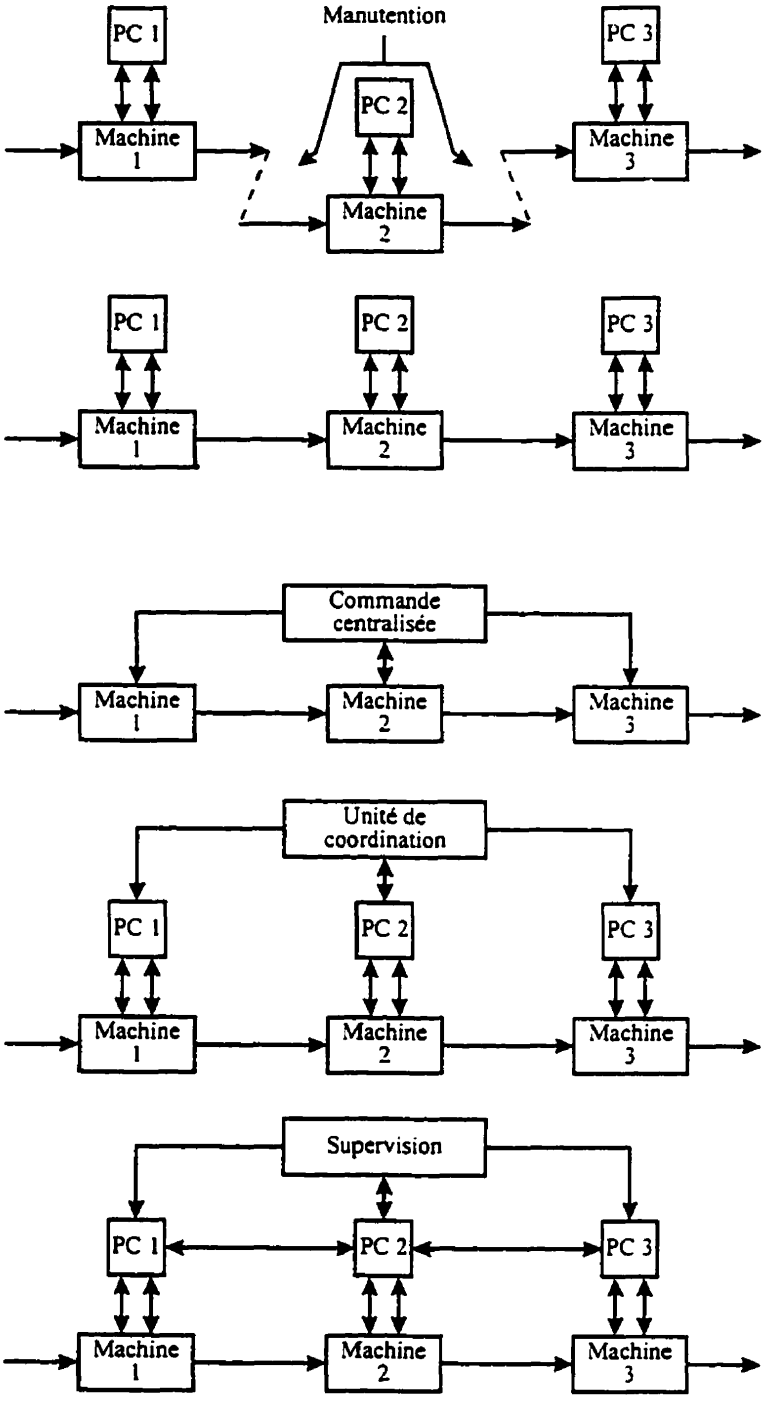

Figure 2.6 Évolution de la structure des SPA [BOUTEILLE, D. et coll., 1996]

2.1.2 Partie commande des SPA

Cette section donne en premier lieu un bref aperçu de ce qu'est la logique câblée puis définit les différents systèmes électroniques programmables (SÉP, de l'anglais *Programmable Electronic Systems, PES*) existant ainsi que leurs applications industrielles respectives. Comme deux de ces systèmes sont fréquemment utilisés en automatisation, soit les automates programmables industriels (API, de l'anglais *Programmable Logic Controllers, PLC*) et les systèmes de contrôle distribués (SCD, ou en anglais DCS, *Distributed Control Systems*), ils sont d'avantage explicités. Finalement, des applications typiques de ces deux technologies, notamment dans l'industrie québécoise des pâtes et papiers (P&P), sont présentées. Mais tout d'abord, la définition générale d'une partie commande doit être faite.

2.1.2.1 Définition de la partie commande

D'une manière tout à fait générale, la partie commande peut être représentée à l'aide de ces quatre parties principales :

- le bloc d'alimentation en énergie (fournit l'énergie requise à l'exécution des fonctions commandées) ;
- les modules d'entrées (convertissent ou transmettent les informations reçues à l'entrée en provenance de divers dispositifs, tels que les boutons poussoirs, les détecteurs de position, etc.) ;
- l'unité centrale de traitement ou UCT (traite toutes les entrées en vue d'activer les sorties prévues en respectant une logique préétablie) ;
- les modules de sorties (convertissent ou transmettent les signaux de commande provenant de l'UCT pour activer divers dispositifs, tels que les valves motorisées, les moteurs d'entraînement, etc.).

La figure 2.7 schématise la structure générale d'une partie commande.

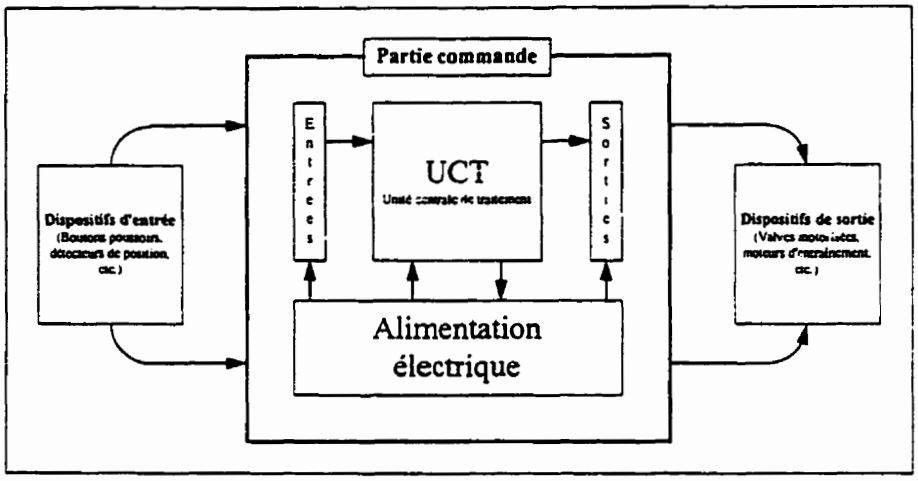

Figure 2.7 Structure générale d'une partie commande

Pour exécuter les fonctions de sortie qui correspondent aux signaux d'entrée reçus, la PC doit traiter adéquatement ces informations en respectant la logique prévue. Aujourd'hui, deux principaux types de logiques sont encore utilisées en automatisation industrielle : la logique câblée et la logique programmée qui sont présentées dans le paragraphe suivant.

2.1.2.2 Logique câblée et logique programmée

La logique câblée a fait son apparition dans les SPA dans les années 1940. Pour exécuter les fonctions logiques de la partie commande, une disposition judicieuse de divers composants électriques, électroniques et électromécaniques (comme les sectionneurs, les disjoncteurs, les relais, les contacteurs magnétiques, les résistances, etc.) doit être accomplie. Par exemple, un opérateur pourrait commander la mise en marche d'un moteur en appuyant sur un bouton poussoir comme le schématise la figure qui suit.

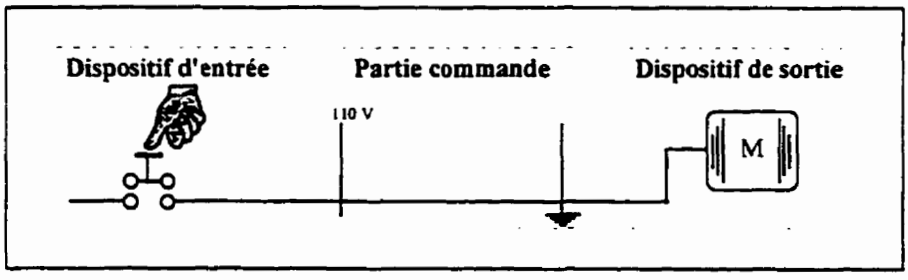

Figure 2.8 Mise en marche d'un moteur avec câblage direct

Dans ce cas-ci, la PC se limite à un simple fil électrique. Cependant, dès que l'opérateur relâchera le bouton poussoir, le contact s'ouvrira et le moteur s'arrêtera. Pour remédier à ce problème, l'installation d'un relais électromagnétique (R), qui agira comme électroaimant et maintiendra un contact fermé tant qu'il sera alimenté en courant électrique, permettra à l'opérateur de relâcher le bouton et au moteur de continuer son opération. La PC prend alors l'allure suivante.

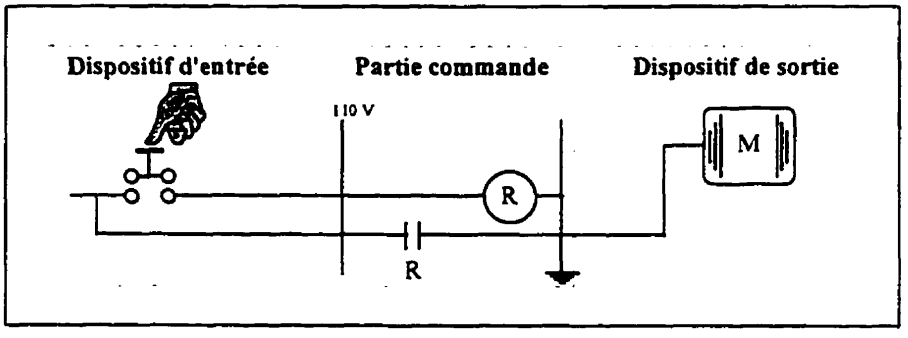

Figure 2.9 Mise en marche d'un moteur avec contact maintenu

Certes, il s'agit d'un exemple très simple ayant pour unique but de permettre au lecteur de comprendre le fonctionnement élémentaire de cette technologie. Il est bien évident que des fonctions logiques extrêmement complexes peuvent être réalisées avec la logique câblée ; tout est fonction de l'expertise de l'automaticien! Cependant, plus les fonctions deviennent complexes, plus le nombre de composants électriques, électroniques et électromécaniques ainsi que la quantité de câble les reliant sont élevés. Ainsi, avec la complexité croissante des SPA, les coûts nécessaires à la mise en place d'une logique câblée ainsi que les risques d'erreur dans le câblage ont considérablement été accrus [WILDI, T., 1991]. Une technologie plus flexible, permettant plus facilement les modifications aux machines et ayant une meilleure adaptabilité aux contraintes de production s'imposait. C'est principalement ce que permet la logique programmée.

La structure de la partie commande pour une machine utilisant la logique programmée est essentiellement la même, à l'exception qu'au lieu d'utiliser des composants électriques, électromécaniques ou électroniques pour exécuter les fonctions logiques, ces dernières sont effectuées par un système électronique programmable.

2.1.2.3 Définition des systèmes électroniques programmables (SÉP)

Une équipe de chercheurs oeuvrant pour l'INRS, l'*Institut national de recherche et de sécurité* (France), donne une définition plutôt générale d'un système électronique programmable [EDWARDS, R. et coll., 1992] :

> *«Appellation des systèmes électroniques basés sur un processeur et capables d'effectuer des calculs au sens large. Les composants en sont : les entrées ; la mémoire ; le (les) processeur (s) ; les sorties ; le logiciel.»*

Cette définition donne une description très large d'un SÉP. Elle permet donc d'englober les technologies suivantes [anonyme, 1992] [BOUTEILLE, D. et coll., 1996] :

- cartes électroniques standards ou spécifiques ;
- micro- et mini- ordinateurs.
- automates programmables industriels (API) ;
- systèmes de commandes distribuées (SCD) ;

En ce qui concerne les cartes électroniques (standards ou spécifiques), leur emploi est très limité en automatisation de production étant donné qu'elles doivent être fabriquées en grande série pour être rentabilisées. Elles sont plus fréquemment utilisées en automatisme grand public (parcomètres électroniques, guichets bancaires automatisés, etc.) [BOUTEILLE, D. et coll., 1996]. Il existe tout de même quelques applications industrielles, comme les machines de fabrication de cigarettes où les temps de réponse requis sont très critiques [BOURBONNIÈRE, R. et coll., 1997]. Quant à eux, les micro- et les mini- ordinateurs sont employés dans des domaines variant de l'utilisation personnelle à la recherche scientifique en passant par le contrôle des procédés à risques élevés, comme la pétrochimie, l'industrie nucléaire, etc. Ils sont également grandement utilisés en automatisation de production pour la gestion des processus, l'assistance à la sécurité globale des opérations, etc. Finalement, les API et les SCD sont les types d'électroniques programmables les plus utilisés en automatisation de production [BOUTEILLE, D. et coll., 1996]. Ces deux technologies sont au coeur de la présente recherche.

2.1.2.4 Automate programmable industriel (API)

L'inventeur des API est l'Américain Richard E. Morley qui a mis au point son premier prototype en 1969. Très vite, son invention s'est répandue si bien qu'en 1995, il existait plus de 50 fabricants d'API à travers le monde [COX, R.A., 1995] [WILDI, T., 1991]. Une définition couramment admise d'un API est celle que la *National Electrical Manufacturing Company* (NEMA, États-Unis) donne [COX, R.A., 1995] :

> *«A programmable controller is a digital electronic apparatus with a programmable memory for storing instruction to implement specific functions, such as logic, sequencing, timing, counting and arithmetic to control machines and process.»*

Une autre définition, francophone cette fois, est donnée par l'INRS [EDWARDS, R. et coll., 1992] :

> *«Composant électronique à base de microprocesseur(s) qui comporte une mémoire programmable par un utilisateur non informaticien à l'aide d'un langage adapté. [...] Un automate programmable a pour fonction de commander, mesurer et contrôler, au moyen des modules d'entrées et de sorties, différentes sortes de machines ou de processus en environnement industriel.»*

Selon cette définition, à la structure générale d'une PC présentée à la figure 2.7 s'ajoute un nouveau composant qui tient compte du caractère programmable de l'API, soit la *mémoire*. Ainsi, la composition de base d'un API est illustrée à la figure suivante.

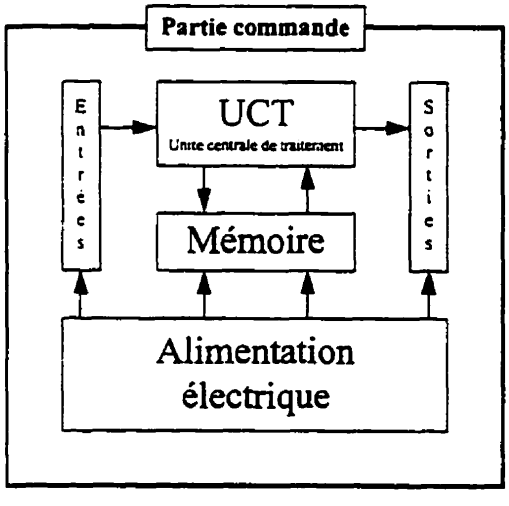

Figure 2.10 Architecture élémentaire d'un API

Cette figure met en évidence les constituants de base d'un API. Ainsi, l'UCT est un sous-ensemble qui gère le fonctionnement interne des différents autres sous-ensembles. Comme mentionné auparavant, l'UCT en technologie programmée n'est pas constitué de composants électriques ou électromécaniques ; il est composé de composants électroniques nommés microprocesseurs. Quant à elle, la mémoire permet l'enregistrement, la conservation et la restitution de l'ensemble des données relatives à la production ou au fonctionnement du système. Elle contient également deux types de programmes : le programme moniteur fourni par le constructeur qui régit le fonctionnement de base de l'API et qui y est inscrit de façon permanente (mémoire ROM, *Read Only Memory*) et le programme pilote qui contient toutes les instructions relatives au processus, au procédé ou au fonctionnement du système (il est chargé en mémoire vive, RAM, *Random Access Memory*). Ce dernier programme peut donc être modifié à volonté. Il existe aussi d'autres types de mémoires, tel que EPROM (*Erasable Programmable Read Only Memory*), UVPROM (*Ultra-Violet Programmable Read Only Memory*) etc., possédant toutes leurs avantages et leurs inconvénients ; le concepteur doit donc choisir celle qui convient le mieux à son application [COX, R.A., 1995]. Les modules d'entrées et de sorties (modules E/S) permettent de transformer, d'une part, les informations captées par les dispositifs d'entrées en signaux électriques compatibles avec la technologie de l'automate et, d'autre part, les informations émises en une forme compatible avec la technologie des dispositifs de sorties. Finalement, la carte d'alimentation électrique fournit l'énergie nécessaire aux différentes parties de l'automate [COX, R.A., 1995]. Elle doit être minutieusement conçue, car elle est en interaction directe avec les éléments perturbants de l'environnement (parasites, surtension, rayonnement électromagnétique, etc.) [DEI-SVALDI, D. et coll., 1984].

Il a été vu précédemment (section 2.1.1.4) qu'une machine automatisée se divise en deux parties : la partie opérative et la partie commande. L'automate programmable agit donc comme le cerveau de l'automatisme, il compose la PC. La figure suivante schématise la structure générale d'une machine automatisée ayant un API comme partie commande. Elle met en évidence l'interaction existant entre la partie commande, la partie opérative et le monde extérieur.

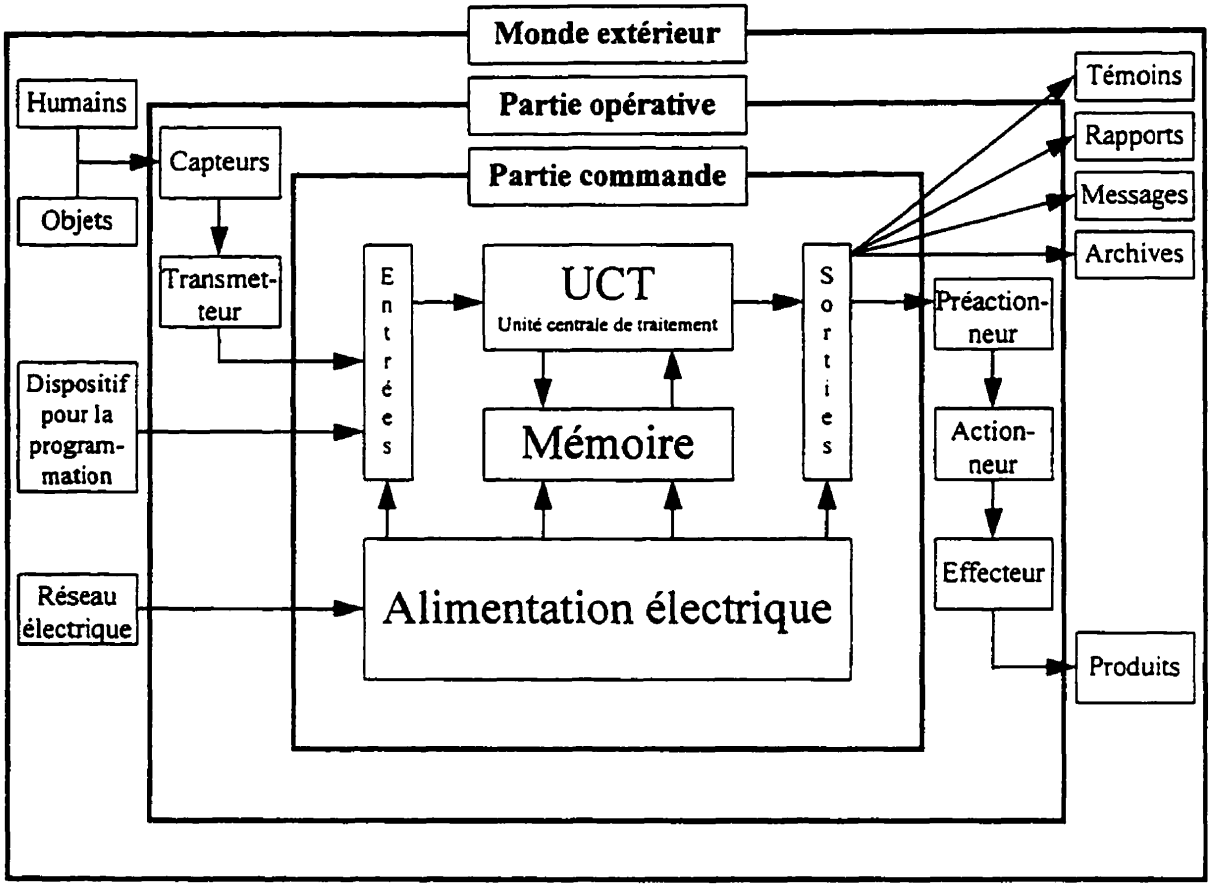

Figure 2.11 L'API aux commandes d'une machine automatisée

Le fonctionnement d'un automatisme utilisant un API peut être décrit à l'aide des trois étapes de balayage[3] qu'effectue l'UCT [COX, R.A., 1995] :

- l'inspection des états des entrées ;
- la confrontation logique des états des entrées au programme ;
- la mise à jour des instructions de sorties.

Ces étapes de balayage sont représentées dans la figure qui suit puis expliquées plus en détail par la suite.

[3] Contrairement à la logique câblée qui exécute ces fonctions de façon séquentielle (instruction par instruction), l'API procède plutôt à un balayage (*scan*) de son programme.

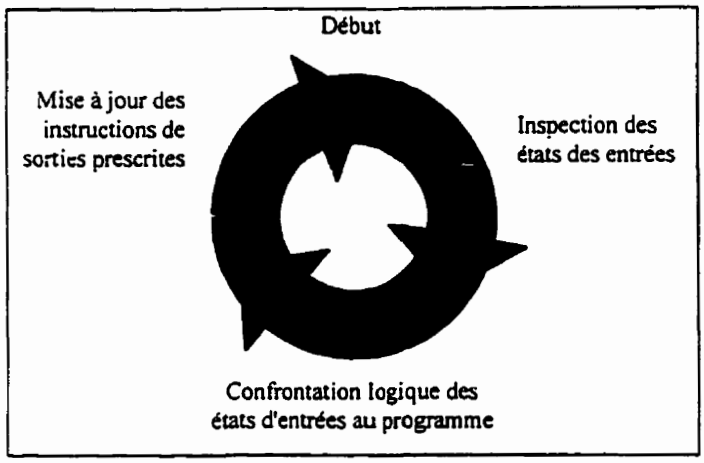

Figure 2.12 Étapes de balayage d'un API [COX, R.A., 1995]

Dès que l'API est mis en énergie, l'UCT effectue un test interne via son programme moniteur afin de s'assurer que son ensemble soit en bon état de marche. Une fois cette vérification terminée, il débute ses cycles de balayages.

Lors de la première étape, l'UCT inspecte les états des diverses entrées. Les renseignements obtenus sont automatiquement placés en mémoire. Dans sa seconde étape de balayage, les états d'entrées placés en mémoire sont confrontés au programme pilote placé aussi en mémoire. Le processeur effectue alors toutes les opérations logiques nécessaires pour traduire ces données en instructions de sortie qui seront aussi placées en mémoire. Finalement, la mise à jour des instructions de sorties est effectuée, ce qui a pour effet d'activer les modules de sorties qui activeront à leur tour les divers dispositifs de sorties.

Par exemple, l'opérateur pourrait appuyer sur le bouton de mise en marche d'un moteur. Cette action envoie un petit signal électrique que le module d'entrée reçoit et place à un endroit prédéterminé dans la mémoire de l'API. L'UCT, en effectuant son balayage, prendra connaissance du code placé en mémoire, confrontera ce dernier avec son programme et inscrira un nouveau code dans un autre endroit de la mémoire. Ce code sera transmis au module de sortie qui enverra le signal nécessaire à la mise en marche du moteur.

Tout au long de ce processus (qui en fait n'a pris que quelques centièmes de seconde), plusieurs informations sont transmises au module d'entrées de l'API via les dispositifs d'entrée. L'UCT,

effectuant ses balayages de façon cyclique, prendra connaissance de ces nouvelles données et continuera ce même cycle. Il est intéressant de noter que l'UCT peut faire jusqu'à quelques centaines de balayages par seconde [COX, R.A., 1995].

2.1.2.5 Système de contrôle distribué (SCD)

C'est au début des années 1970 que sont apparus les premiers SCD [CHATTAWAY, A.T., 1991]. Aujourd'hui, ils représentent encore le premier choix pour la gestion des opérations d'un système de production automatisé [BADER, F.P., 1995]. Tout comme les API, les SCD sont constitués d'un module d'entrées, d'un UCT, d'une mémoire, d'un module de sorties et d'un système d'alimentation électrique. Ils ont cependant généralement une bien plus grande capacité : plus d'entrées et de sorties ; processeur plus rapide et plus puissant ; plus grand nombre d'informations pouvant être mémorisées ; etc. La majorité des SCD permettent [GRENIER, D. 1994] :

- de mesurer et communiquer plusieurs informations relatives à la production ;
- de contrôler la production via une console d'opérateur ;
- de faciliter les interventions de maintenance et la planification de la production ;
- d'accroître la sûreté des installations grâce à des architectures redondantes.

Un exemple d'architecture d'un SCD est présenté à la figure suivante.

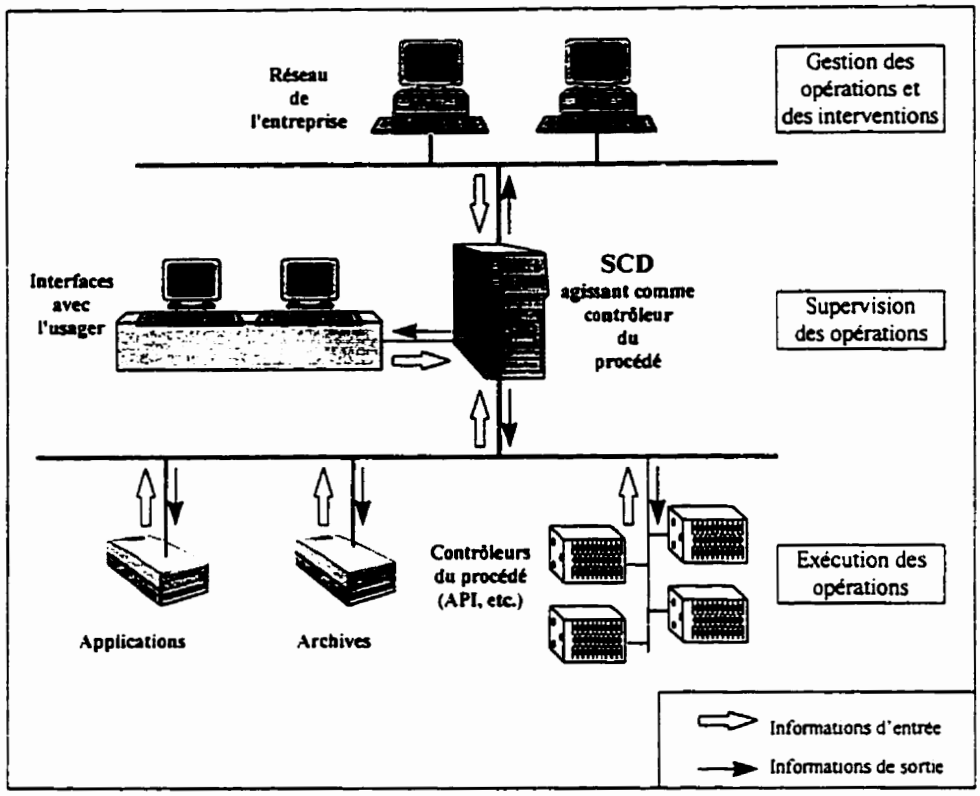

Figure 2.13 Exemple d'architecture d'un SCD [TAYLOR, M.A., 1994]

Cette figure fait ressortir trois principaux niveaux. Le premier est celui de la gestion des opérations (horaire de production, paramètres de production, etc.) et des interventions (planification, mise à l'arrêt) qui peuvent être effectuées par le biais de terminaux. Le second niveau est celui de la supervision des opérations où, à l'aide de moniteur ou d'autres moyens, le personnel peut veiller au bon déroulement des opérations et commander des fonctions liées au processus. Finalement, le dernier niveau est celui de l'exécution des opérations. Des systèmes électroniques programmables (souvent des API) commandent les opérations et transmettent toutes les informations soit au contrôleur du procédé ou encore à l'archive ou à d'autres applications.

Outre le coût et le niveau de difficulté de programmation plus élevés du SCD, la principale différence entre ces deux technologies (API et SCD) réside en la possibilité d'exécuter aisément ou non des fonctions analogiques. En effet, l'API peut difficilement traiter ce type de fonctions ; il est généralement limité à l'exécution des fonctions séquentielles. Par contre, le SCD peut aussi

bien traiter les fonctions analogiques que séquentielles. Cependant, étant donné son coût nettement plus élevé, le concepteur a tout avantage à confier les fonctions séquentielles à l'API et à réserver les entrées et les sorties du SCD pour les fonctions analogiques. La figure qui suit schématise une architecture souvent rencontrée en entreprise.

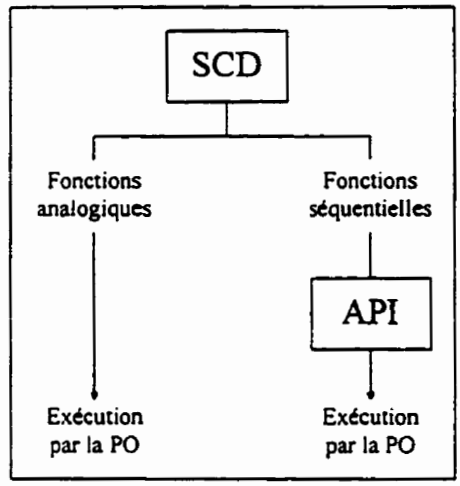

Figure 2.14 Gestion des fonctions séquentielles et analogiques par le SCD

Ainsi, selon cette structure, le SCD gère l'ensemble des opérations. Par contre, s'il doit exécuter des fonctions séquentielles, il les transmet alors à l'API. Ainsi, le SCD est davantage disponible pour l'exécution des fonctions analogiques, ce qui est économiquement avantageux.

2.1.2.6 Applications courantes des API et des SCD

L'application des systèmes électroniques programmables (particulièrement les API) la plus simple et la plus courante en automatisation est le remplacement de la logique câblée par cette technologie plus flexible. Ainsi, tous les composants électriques, électroniques et électromécaniques constituant la partie commande sont éliminés et remplacés par un microprocesseur et une unité de mémoire. Les opérations logiques qu'effectuaient les relais électromécaniques, les contacteurs magnétiques, les minuteries, etc. sont désormais assurées par le logiciel dont la principale caractéristique est son immatérialité. Les avantages d'une telle transformation sont une diminution du coût et du temps d'entretien ainsi qu'une plus grande facilité à modifier les divers paramètres de production accroissant ainsi la flexibilité du SPA.

Une autre application des SÉP est la gestion et la supervision des procédés. Ce sont généralement les SCD qui sont utilisés, mais l'utilisation des API est tout de même chose courante : *«Programmable systems in the form of programmable logic controllers (PLCs) [...] have become widely accepted for process control. Their high reliability, ease of programming and low cost have seen use [...] expanding.»* [McARTHUR, N., 1992].

Finalement, une application réservée presque exclusivement à l'industrie à haut risque (industries pétrochimique, nucléaire, etc.) pour des raisons économiques est le système d'arrêt d'urgence automatique : si l'humain, l'environnement ou l'équipement devient en danger, un système d'arrêt d'urgence fait le suivi d'un procédé et le guide vers un arrêt entièrement sécuritaire [HALANG, W.A. et coll., 1993][4]. Face à la complexité et la gravité des conséquences d'un accident dans ces domaines, il devenait dangereux de confier les prises de décision rapide seulement qu'aux opérateurs : *«Studies have shown that when faced with life-threatening, situations that required action within 60 seconds, people make incorrect decisions 99.9% of the time.»* [GRUHN, P., 1995]. Grâce à l'implantation des technologies programmables pour les systèmes d'arrêt d'urgence, l'opérateur n'a qu'à suivre l'évolution de la situation. R.C. Waterbury [1991] présente dans son article une grille permettant de comparer les divers types de technologies programmables utilisées pour les systèmes d'arrêt d'urgence en fonction de critères tels que leur coût, leur fiabilité et leur durée de vie.

2.1.2.7 Application des SÉP dans l'industrie québécoise des pâtes et papiers (P&P)

L'intégration des technologies programmables dans les industries des P&P québécoises a débuté, comme mentionné précédemment, en 1963. Elle ne cesse de progresser depuis ce jour. Ainsi, toutes les usines visitées dans le cadre de la recherche possédaient des SÉP servant à gérer la production du papier[5]. Le nombre d'API variait alors entre 40 et 150 tandis que chaque usine possédait entre 2 et 6 SCD. Aussi, il a pu être constaté que les marques d'API ou de SCD varient

[4] Il est souvent dit qu'un système d'arrêt d'urgence coûte cher. Une façon purement économique que T.G. Fisher utilise pour analyser ce point de vue est de considérer qu'un accident nécessitant un arrêt de travail peut coûter en moyenne 18 650 dollars américains et que pour une industrie employant 1 000 travailleurs, 9 d'entre eux se feront blesser. Pour amortir ces coûts, considérant une marge de profit de 3.7%, un total de 4.5 millions de dollars en vente sont nécessaires. Donc, même en excluant l'aspect éthique et moral qu'engendrent les accidents de travail, il s'agit d'une technologie rentable à court terme! [FISHER, T.G., 1990]

[5] Les SÉP rencontrés étaient principalement des API et des SCD, il n'y avait que très peu de robots industriels.

énormément, tant entre les usines qu'entre les départements d'une même usine. Cette particularité pose un certain problème quant à l'entretien, l'opération et la modification des SÉP utilisés. Cependant, la tendance actuelle vise justement à contrer cette difficulté en uniformisant, au sein d'une même entreprise, les marques des SÉP installés.

Il ressort donc que le niveau d'automatisation des industries de P&P québécoises est élevé, mais tout de même variable d'une usine à l'autre. Par exemple, certaines usines assurent encore le contrôle de certains procédés par des logiques pneumatiques. Par contre, d'autres assurent l'ensemble des opérations du processus de fabrication du papier tout entier ; de la réception des billes de bois au chargement du produit fini en passant par l'emballage personnalisé, les SÉP assurent toutes les opérations[6]! Par exemple, un SCD peut contrôler le procédé entier d'une machine à papier : il informe les opérateurs de l'état du procédé ; il gère le débit d'arrivée de la pâte ; il coordonne les vitesses des rouleaux d'entraînement via les API ; il contrôle l'épaisseur du papier et commande les ajustements nécessaires ; etc. Pour effectuer les modifications sur le procédé, le SCD peut faire appel aux API. Ce sont ces derniers qui effectuent généralement les séquences nécessaires aux réajustement de la vitesse des rouleaux par exemple. Pour schématiser cet exemple, la figure qui suit représente la structure informatique d'une papetière québécoise actuellement en opération. Cette structure permet à l'entreprise de recevoir des commandes d'un peu partout au monde, de les inscrire à l'horaire de production, de contrôler leur production, de spécifier le format et l'emballage souhaité par le client, d'entreposer le produit fini jusqu'à la date prévue de livraison et alors de l'orienter vers le bon quai de chargement.

[6] L'appendice I présente le schéma global de la technologie papetière où le processus entier de la fabrication du papier est présenté [AIFQ, 1997]

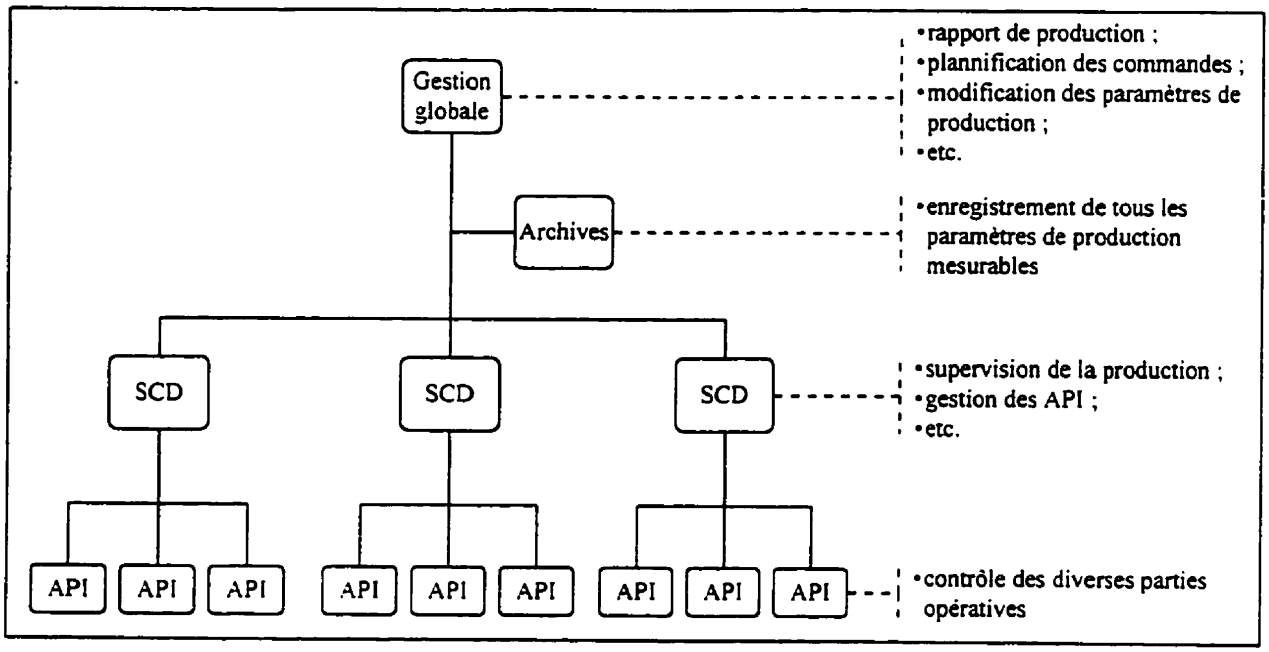

Figure 2.15 Structure informatique d'une papetière du Québec

2.1.3 Impacts sur la santé et sécurité du travail (SST) de l'automatisation avec les SÉP

La sensibilisation à la santé et à la sécurité du travail (SST) ne date pas d'hier. Face au nombre croissant d'accidents impliquant des machines industrielles, certains organismes ont tôt commencé à formaliser des solutions pratiques permettant de diminuer les risques d'accidents. Ainsi, la Grande-Bretagne a légiféré dès 1844 et les États-Unis ont suivi en 1877 [ROBERTS, V.L., 1984]. Depuis ce temps, de considérables efforts ont été déployés pour légiférer ce domaine et sensibiliser les gens concernés de près ou de loin par la SST, comme en témoigne l'abondante quantité d'articles, d'ouvrages et de normes.

2.1.3.1 Automatisation et accidents

L'automatisation n'est pas le remède miracle pour contrer les accidents de travail : «*Cette technique conduit donc à éloigner l'homme des machines [...]. Toutefois, l'homme n'est pas systématiquement évincé de son environnement.*» [EDWARDS, R. et coll., 1992]. Une note documentaire publiée par l'INRS en vient à la même conclusion : l'idée que l'automatisation supprimerait tout risque d'accident, en mettant l'humain hors de portée, est rejetée. Toutefois, elle ajoute que l'attitude de toujours blâmer les automatismes, en les nommant *robots tueurs*, est également rejetée [DEI-SVALDI, D. et coll., 1989]. Aussi, à côté du mythe du robot *voleur de job* ou de la machine *automatique qui marche toute seule*, on rencontre souvent une confiance quasi infinie dans la machine automatisée, ce qui a pour effet d'amoindrir la perception des dangers [BOURBONNIÈRE, R. et coll., 1997]. Conséquemment, l'automatisation des SPA est elle aussi responsable d'un bon nombre d'accidents.

Bien que peu nombreuses, quelques études portant sur des accidents impliquant des systèmes de production automatisés ont été menées notamment en Suède, au Japon, en Angleterre, en Allemagne [EDWARDS, R. et coll., 1992], en France [DEI-SVALDI, D. et coll., 1989] et plus récemment aux États-Unis [BACKSTRÖM, T. et coll., 1995] [JÄRVINEN, J. et coll., 1995]. Considérant que les données concernant principalement les parcs ou cellules robotisés ne sont pas d'intérêt pour ce mémoire, seuls les résultats des quatre dernières études, soit celles d'Angleterre, d'Allemagne, de France et des États-Unis, seront présentées.

L'étude conduite en Grande-Bretagne par le *Health and Safety Executive* (HSE) portait sur 284 accidents survenus entre le 1er avril 1987 et le 31 mars 1991. Cette étude générale, concernant l'automatisation, comprenait des machines et systèmes à commande numérique, des cellules robotisées et des véhicules guidés automatiquement. Les faits saillants qui en ressortent sont les suivants [EDWARDS, R. et coll., 1992] :

- 28% des accidents sont graves ;
- 78% des accidents affligent les opérateurs et 13% le personnel de maintenance ;
- 92% des accidents surviennent lors d'une intervention mineure ou majeure sur l'équipement automatisé (61% et 31% respectivement) ;
- 49% des accidents surviennent alors que la machine est en mode automatique ;
- pour 80% des cas, les systèmes de protection se sont avérés inefficaces, et de ceci, les mauvaises spécifications de sécurité en sont responsables pour une proportion de 65% ;
- dans 50% des cas, les facteurs humains sont significatifs.

Une autre étude, relatée par un institut de Stuttgart (Allemagne), tire des conclusions pour le moins surprenantes. Elle met en évidence le nombre d'accidents survenus par rapport au nombre d'heures travaillées, et ce pour quatre catégories de travailleurs. Le tableau qui suit présente les résultats.

TABLEAU 2.1 RATIO DU NOMBRE D'ACCIDENTS PAR RAPPORT AU NOMBRE D'HEURES TRAVAILLÉES

Groupe de travailleurs	Fréquence relative F des accidents (%)	Temps relatif T de travail (%)	Ratio F/T
Programmeurs et régleurs	57	5	1140
Équipe de nettoyage	26	5	520
Équipe de réparation	4	5	80
Équipe d'opération	13	85	15

Il ressort que ce ne sont pas les opérateurs chargés de faire fonctionner la machine qui sont les plus exposés aux phénomènes dangereux, mais surtout le personnel chargé de programmer, ajuster, nettoyer et réparer la machine [EDWARDS, R. et coll., 1992].

L'étude menée par l'INRS en collaboration avec les services de préventions des *Caisses régionales d'assurance maladie* (CRAM, France) portait sur un total de 54 accidents sur des sites automatisés français dans la période de 1983 à 1988. Les faits saillants ressortant de cette étude établissent que les accidents qui surviennent [DEI-SVALDI, D. et coll., 1989] :

- mettent en cause des systèmes partiellement ou complètement automatisés ;
- sont généralement très graves (72% des accidents nécessitent l'hospitalisation dont 33% se soldent par un décès) ;
- se produisent principalement à l'occasion d'une intervention succédant à un incident de fabrication (54%) ;
- se produisent principalement en mode de marche automatique (72%) ;
- concernent les opérateurs (46%) et le personnel de maintenance (46%) ;
- avaient dans 45% des cas des dispositifs de protection non appropriés alors que dans 31% des cas ces derniers étaient tout simplement inexistants.

Finalement, l'étude menée récemment aux États-Unis par J. Järvinen et W. Karwowski [1995] portait sur 103 accidents rapportés par diverses entreprises américaines. De ceux-ci, 63% étaient associés à des équipements fréquemment rencontrés dans l'industrie des P&P québécoise (convoyeur, équipement de manutention, etc.). Les points qui ressortent de l'étude sont les suivants :

- 67% des accidents affligent les opérateurs et 20% le personnel de maintenance ;
- 48% des accidents se produisent lors de diverses interventions non prévues (dépannage, réparation d'urgence, etc.) ;
- 55% des accidents surviennent alors que l'équipement est en mode automatique ;
- 57% des mouvements des parties opératives ayant causé les blessures étaient programmés alors que 24% étaient de nature intempestive ;
- 6% des victimes sont décédées alors que 37% ont dû prendre 3 jours ou plus de repos ;
- 74% des dispositifs de protection étaient inadéquats.

Le même article présente également les résultats d'une autre étude similaire conduite par T. Backström et M. Döös [1995]. Ces derniers résultats sont présentés directement dans le tableau synthèse où ils sont comparées aux résultats des études menées par l'équipe de D. Dei-Svaldi [1989], de l'équipe de R. Edwards [1992] et de l'équipe de J. Järvinen [1995].

TABLEAU 2.2 COMPARAISONS DES DIVERSES ÉTUDES D'ACCIDENTS[7]

	R. Edwards et coll. (1992)	**D. Dei-Svaldi** et coll. (1989)	**T. Backström** et coll. (1995)	**J. Järvinen** et coll. (1995)
Blessures sévères[8] et décès	28%	72%	43%	43%
Opérateurs blessés	78%	46%	64%	67%
Personnels de maintenance blessés	13%	46%	10%	20%
Mode d'opération automatique	49%	72%	-	55%
Intervention suite à un problème	92%	54%	60%	48%
Dispositif de protection inadéquat	80%	76%	-	74%

Cependant, une mise en garde est émise quant à la comparaison des résultats de ces études étant donné que plusieurs paramètres varient. Par exemple, la proportion d'accidents dus à des robots est indéterminée, les accidents survenus en France ne sont rapportés que lorsqu'ils sont passablement graves, etc. [EDWARDS, R. et coll., 1992]. Néanmoins, il est possible de tirer les conclusions générales suivantes :

- les accidents qui surviennent sur les sites automatisés sont souvent graves ;
- les opérateurs sont généralement les plus souvent victimes d'accidents, suivi d'assez près par le personnel d'entretien ;
- les accidents surviennent très souvent en mode de marche automatique pendant ou suite à des interventions (dépannages, réglages, maintenance, etc.) ;
- les dispositifs de protection, lorsqu'existant, sont souvent inefficaces et ce principalement en raison d'une conception déficiente ;
- les facteurs humains sont souvent significatifs.

Ainsi, bien que plusieurs gains résultent de l'automatisation (meilleures conditions de travail, etc.), il n'en demeure pas moins que de nouveaux phénomènes dangereux ont été introduits en même temps que ces nouvelles technologies et qu'il faut prendre des mesures particulières pour éviter les incidents pouvant en résulter [PAQUES, J.-J., 1991]. Le défi du concepteur aujourd'hui

[7] Ce tableau est fortement inspiré de celui proposé par R. Bourbonnière et J.-J. Paques [1997].

[8] Les blessures sévères comprennent les amputations, les fractures et les blessures irréversibles aux yeux.

se résume donc à concevoir des automatismes offrant plus de souplesse, mais également un plus haut niveau de sécurité [ADEPA, s.d.].

D'un autre point de vue, il ne faut pas oublier que les solutions techniques sont nécessaires mais non suffisantes pour diminuer le nombre d'accidents fâcheux. En effet, bien que la sécurité soit un critère important aux yeux des gens, elle est tout de même parfois reléguée au second plan pour favoriser la productivité, comme en témoigne les conclusions d'une enquête menée auprès de 800 employés : *«As expected, safety received the first priority vote by a narrow margin. However, production was considered more important overall.»* [BECKMAN, L.V., 1993].

Ainsi, en plus de persister dans la sensibilisation à l'aspect SST, des programmes de formation doivent être mis en place pour toutes les personnes appelées à interagir avec les SPA. À cet effet, l'*Association internationale de sécurité sociale* (AISS) fait ressortir la nécessité de la mise en place d'une telle formation [AISS, 1989] :

> *«L'évolution constante de ces nouvelles techniques et leur utilisation de plus en plus importante dans les entreprises modifient et diversifient les tâches de l'homme qui deviennent également plus complexes. L'automatisation de plus en plus poussée des tâches de production entraîne un glissement progressif des activités humaines liées directement à la production vers des activités de préparation, de réglage et de maintenance, ces dernières étant elles-mêmes de plus en plus assistées par des moyens informatiques. [...]* ***Il convient donc d'attacher la plus grande importance à la formation des hommes chargés de faire «vivre» ces systèmes.***
>
> *La sécurité des hommes, malgré les dispositions techniques prises à la conception, dépend pour une bonne part de cette formation. En effet, il est de plus en plus difficile pour l'homme, notamment lors de dysfonctionnements, de connaître avec suffisamment de précision la réaction d'un système à telle ou telle sollicitation.»*

2.1.3.2 Craintes face à l'application des SÉP aux fonctions de sécurité des SPA

L'automatisation des machines et des systèmes de production soulève donc actuellement un vif débat du point de vue SST ; l'automatisation est-elle la pire ou la meilleure des choses?[9] Certains jugent que *«parce qu'elle éloigne les travailleurs des zones dangereuses, elle va résoudre tous les*

[9] L'aspect éthique, moral et social que peut soulever cette brûlante question n'est pas traité dans ce mémoire. Seul l'aspect technique, et plus particulièrement l'aspect sécuritaire y est traité.

problèmes de sécurité au travail.» Par contre, tel que vu précédemment et souligné par J.-J. Paques [1991], *«on a pu observer des incidents et des pannes directement associés à ces nouvelles technologies [...]»*. Le débat s'articule donc principalement autour du rôle restreint que peuvent accomplir les SÉP (en particulier les API) du point de vue de la sécurité, comme en témoigne une quantité phénoménale d'articles. La grande majorité des auteurs s'entendent pour dire qu'on ne peut laisser l'API seul maître des fonctions de sécurité. Par contre, d'autres soutiennent que la fiabilité des API n'est plus à prouver. Ainsi, un dilemme s'établit, comme en témoigne ces deux assertions parfaitement antagonistes : *«Les API n'ont jamais été aussi sûrs.»* ; *«Pour traiter les sécurités, il est pour le moins dangereux de faire uniquement confiance au seul automate.»* [EDWARDS, R. et coll., 1992]. Un article publié par l'INRS accorde également le crédit de fiabilité aux API mais considère *«[...] que la caractérisation de la sécurité ne peut être uniquement déterminée par la seule notion de fiabilité»* [DEI-SVALDI, D., et coll. 1984]. Trois raisons principales quant aux réserves qu'ont les concepteurs envers les fonctions de sécurité traitées par les SÉP (en particulier les API) sont ici énoncées [CLAUZADE, B. et coll., 1984] [PAQUES, J.J., 1991] :

1. les modes de défaillance de l'automate programmable ne sont pas bien connus et son comportement sur défaut interne est imprévisible ;
2. l'environnement dans lequel opère l'automate est très agressif, ce qui peut engendrer des défaillances ;
3. la facilité de modification des programmes qui permet à presque n'importe qui d'apporter des correctifs (pas nécessairement sécuritaires) au processus ou au procédé.

Maintenant, chacune de ces assertions sont traitées dans les sections qui suivent.

2.1.3.3 Première crainte : modes de défaillance aléatoires

Contrairement à la logique câblée où les fautes, les erreurs et les modes de défaillances sont bien déterminés et que les façons de les contrer sont connues, la logique programmée pose certains problèmes de comportement [DEI-SVALDI, D. et coll., 1984] [DEI-SVALDI, D. et coll., 1989] [prEN 954-1, 1996] [ROUCHOUSE, G., 1992]. Il est en effet très difficile de prédire comment un SÉP fera défaut et qu'elle en sera alors les conséquences [PAQUES, J.-J., 1991] Les technologies programmables ont évolué si vite que l'on a pas eu le temps d'acquérir la

connaissance et l'expérience nécessaires à leur maîtrise, alors que les systèmes plus classiques bénéficient d'un savoir accumulé pendant de nombreuses années [ANDERSON, O. et coll., 1987]. Étant donné ce caractère particulier des SÉP et leur grande utilisation, de multiples recherches ont été entreprises pour tenter d'établir clairement leurs modes de défaillance en vue de les prévenir. Une de celles-ci concernait le fonctionnement d'un SPA commandé par des automates programmables industriels. Il ressort, tel que l'illustre la figure 2.16, que seulement 5% des défaillances du système relèvent de défauts internes et donc attribuables à l'automate programmable. De ces 5%, seulement 10% des défauts concernent les fonctions centrales de l'API, le 90% restant se rapportent aux modules E/S qui relèvent de la logique câblée et de composants électroniques simples. C'est donc dire que 5 défauts sur 1000 sont attribuables à l'UCT, à la mémoire, à l'alimentation ou au bus de communication [DEI-SVALDI, D. et coll., 1984].

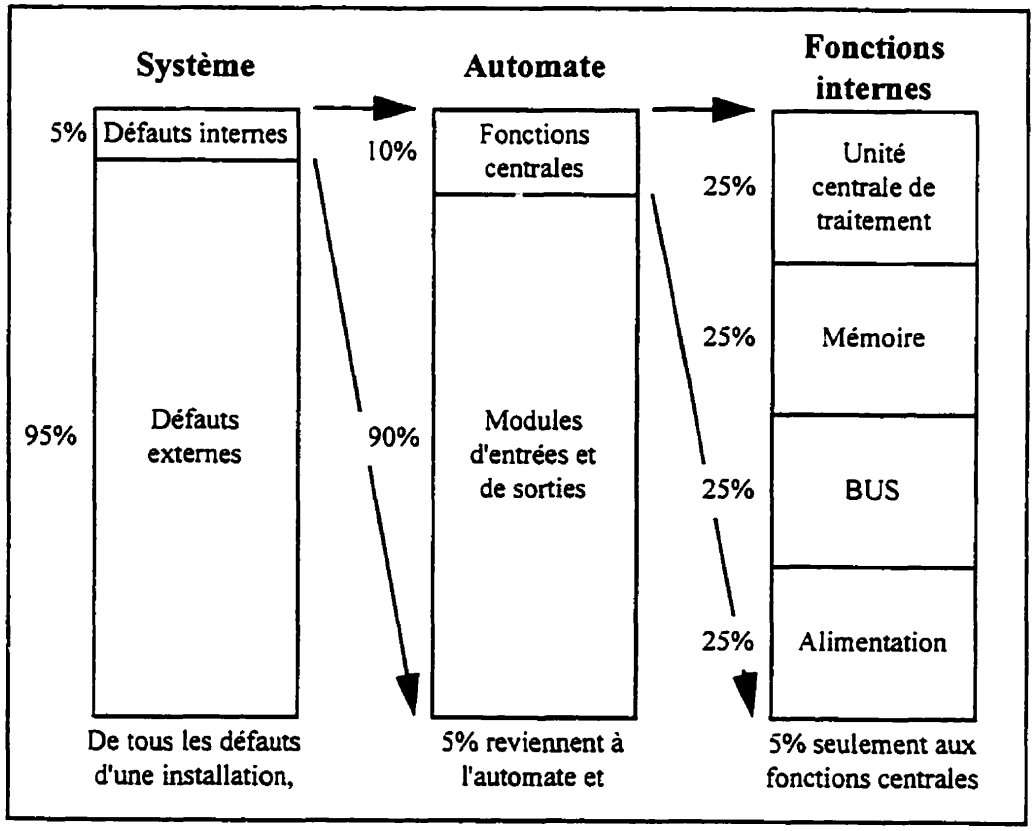

Figure 2.16 La part de responsabilité de l'automate lors des défaillances

Malgré ces excellents résultats, ce type de défaillance relève d'erreurs catalectiques, c'est-à-dire soudaines (donc non prévisibles) et irréversibles. C'est principalement pour cette raison qu'il est difficile de faire confiance uniquement à l'automate programmable pour assurer les fonctions de sécurité directes [ROUCHOUSE, G., 1992]. D'autres études confirment que les éléments les plus susceptibles de faire défaut sont souvent ceux utilisés comme interfaces (modules E/S, lien de communication, etc.) [PAQUES, J.-J., 1991]. Par exemple, une étude conclue que les trois principales causes d'arrêts des SPA sont, dans l'ordre : les défaillances des composants (modules d'entrées ou de sorties, etc.) ; les défaillances du logiciel ; les défaillances dues à des erreurs de la part des opérateurs [BATTLE, R.E. et coll. 1991].

Il semble donc que les défauts des machines automatisées soient généralement attribuables à des fautes externes à la PC, à des défaillances occasionnelles des modules d'entrée et de sortie, à des défaillances rares des fonctions centrales du contrôleur ou de la mémoire et finalement à des défaillances du logiciel. Les défaillances se produisent donc principalement sur le matériel du système de production et sur son logiciel d'exploitation.

Dans le cas des défaillances du matériel (dispositifs E/S, UCT, mémoire, modules E/S, etc.), elles peuvent résulter ou bien d'une dégradation, ou bien d'une erreur de conception ou de fabrication [KOCH, S. et coll., 1994]. Les défaillances matérielles des dispositifs E/S sont généralement faciles à contrer [LEVESON, N., 1995] [ROUCHOUSE, G., 1992]. Par contre, les défaillances matérielles impliquant les autres composants du SÉP (UCT et mémoire) sont souvent complètement imprévisibles et ont des actions ou des conséquences irréversibles.

Pour ce qui est des défaillances attribuables au logiciel, elles sont généralement le résultat d'erreur de programmation. En effet, presque 66% de ces dernières défaillances relèvent de mauvaises spécifications lors de la conception du logiciel, ce qui peut être attribué à l'absence d'une méthodologie systématique permettant de s'assurer qu'elles sont complètes et bien interprétées [ROUCHOUSE, G. 1992]. Cependant, il semble que ce type de défaillance soit injustement tenus responsables de plusieurs défaillances du système : *«It should be noted that all software failures are systematic but not all systematic failures are in software»* [CATMUR, J.R. et coll., 1992]. Par ailleurs, compte tenu du caractère informatique associé à l'identification des

défaillances du logiciel et à l'élaboration d'une méthodologie de développement d'un logiciel sécuritaire qui dépasse largement le cadre de cette recherche, les défaillances dues au logiciel ne seront plus discutées dans ce mémoire.

2.1.3.4 Deuxième crainte : perturbations externes

Les perturbations externes pouvant affecter les SÉP sont quant à elles plus nombreuses que pour les technologies non électroniques : il peut s'agir de perturbations physiques (chocs, etc.), chimiques (acide, gaz, etc.), électriques (surtension, fluctuation, etc.), électromagnétiques (champs magnétiques, etc.) ou environnementales (humidité, chaleur, etc.) [BOUTEILLE, D. et coll., 1996]. Bien que l'API soit spécialement conçu de façon à résister aux agressions habituellement rencontrées dans le milieu industriel [BOURBONNIÈRE, R. et coll., 1997], celles-ci peuvent tout de même perturber le comportement de l'API : altération des mémoires ; variation des valeurs de sortie, des temporisations et des compteurs de programme ; perte des communications ; etc. [DEI-SVALDI, D. et coll., 1984]. Si de telles perturbations affectent l'API, ce dernier peut ordonner des commandes non appropriées, comme des mises en marche intempestives de divers organes, des remises à zéro soudaines du programme ou encore des sauts d'étapes, des refus de lecture de certaines allocations de mémoire, etc. En somme, le comportement de l'API est généralement imprévisible en présence de telles perturbations.

2.1.3.5 Troisième crainte : modification du programme

La définition d'un API donnée précédemment met en évidence une des belles qualités de cette technologie : le niveau de compétence en informatique exigé pour la programmation est très faible en comparaison des autres technologies (cartes électroniques, micro- ou mini- ordinateurs et même les SCD). Cette force se veut aussi une faiblesse, car il n'est pas garanti que la personne qui modifie le programme connaît nécessairement bien le processus ou le procédé ou encore que les modifications apportées au programme seront mises à jour dans la documentation du SPA. Aussi, l'absence de procédure formelle de programmation et de modification de programmes est problématique. Il existe cependant des moyens de protection simples qui permettent de limiter

l'accès aux programmes et ainsi éviter ce type d'erreurs. Ils sont présentés à la section 2.2.5.1 de ce mémoire.

2.1.3.6 Solution actuellement acceptée

Les trois craintes face à l'application des SÉP dans les SPA précédemment dénoncées semblent donc, pour l'instant, porter effectivement atteinte à leur réputation À cet effet, l'organisme américain des *Industrial Risk Insurers* continue à faire pression sur les fabricants de SÉP (particulièrement les API) pour qu'une entente quant aux standards de sécurité et de fiabilité soit prise et qu'un laboratoire reconnu de validation soit instauré [WILSON, D.K., 1988].

En attendant une éventuelle amélioration des SÉP, la recommandation générale qui rallie la plupart des communautés à l'heure actuelle est d'assurer les principales fonctions de sécurité dans un premier temps par la logique câblée et, au besoin, par la logique programmée. Par exemple, l'*Institut de recherche en santé et sécurité du travail* du Québec (IRSST) recommande que les fonctions de sécurité directe (arrêt d'urgence, etc.) soient directement branchées (donc en logique câblée) sur le relais de sécurité principal [PAQUES, J.-J., 1991]. D'autres organismes ou auteurs préconisant cette pratique peuvent également être cités en exemple :

> *«[...] l'INRS déconseille de faire confiance à une logique de type programmée pour assurer les fonctions de sécurité directe. A fortiori celles-ci ne doivent en aucun cas être traitée par le seul automate programmable. Bien que l'apparition d'une nouvelle génération d'automates programmables dits à sécurité renforcée relance le débat, l'INRS maintient sa positon étant donné qu'aucune étude engagée sur ces dispositifs n'a encore offert de conclusions importantes.»* [KNEPPERT, M., 1995][10] ;
>
> *«Les fonctions de sécurité directe doivent être assurées par des circuits traités en sécurité positive insensibles à l'environnement et le plus près possible des actionneurs.»* [AISS, 1988a].

Un schéma très simple illustrant cette recommandation générale est ici présenté.

---

[10] Un séminaire tenu par l'INRS en juin 1997 présentait justement les résultats d'une telle étude [INRS, 1997]. Il en ressortait que, sous certaines conditions (certification des SÉP selon les projets de norme EN 954 [1996] et CEI/IEC 1508 [1995], reprogrammation impossible sans autorisation, etc.) les SÉP **pourraient** assurer les fonctions de sécurité directes et indirectes. Cependant, l'étude n'étant pas encore complétée, l'INRS maintient toujours ses recommandations émises en 1984.

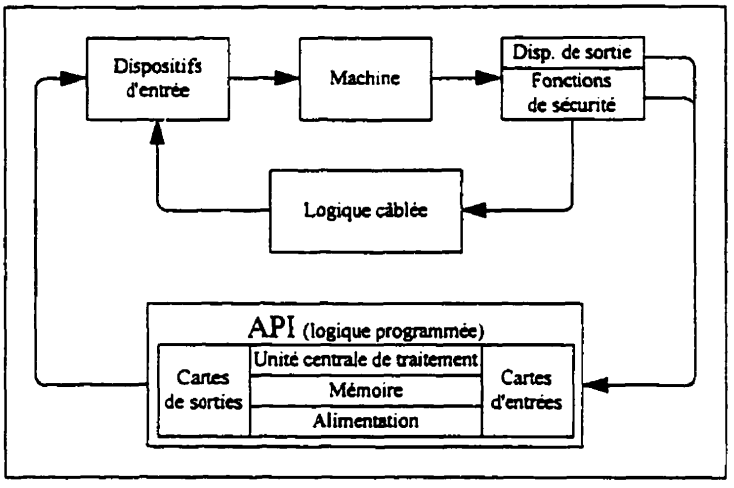

Figure 2.17 Double fonctions de sécurité [DEI-SVALDI, D. et coll., 1984]

De ce schéma, il ressort que l'API reçoit en entrée toutes les informations provenant des divers dispositifs de sorties. Ces informations concernent généralement les fonctions d'opération, mais peuvent aussi être des fonctions de sécurité. Cependant, les fonctions de sécurité les plus importantes, dont les arrêts d'urgence, devraient toujours être assurées dans un premier temps par une logique câblée. Cette façon de faire garantit, jusqu'à un certain point, un haut niveau de sécurité à un coût très abordable [MERLAUD, C. et coll., 1992].

2.1.3.7 Exemple de câblage sécuritaire d'un SPA

Dans le but de montrer un exemple concret de la recommandation schématisée à la figure 2.17, un schéma a été produit dans le cadre du projet de recherche de l'IRSST. La figure 2.18 (page suivante) présente ce dernier [MONETTE, C., 1997]. Ce schéma met en évidence trois façons de commander un arrêt du SPA : par le panneau de commande, par un arrêt d'urgence ou par une station de commande locale. Il est important de constater que l'arrêt d'urgence de même que les commandes transmises par la station de commande locale sont directement câblées à la source de puissance électrique. Ainsi, peu importe les dysfonctionnements dont pourraient être victimes l'API et/ou le SCD, il subsistera toujours ces deux moyens pour arrêter le SPA ; le principe de doubler certaines fonctions de sécurité commandées par l'API et/ou le SCD par une logique câblée est donc respecté. Par ailleurs, la figure montre également deux moyens pour consigner l'équipement. Le premier consiste à cadenasser le sectionneur principal situé dans le centre de

commande des moteurs (CCM). Cependant, pour couper l'alimentation électrique en ouvrant le disjoncteur principal, l'opérateur ou le personnel d'entretien doit nécessairement faire appel aux services d'un électricien, ce qui peut allonger la procédure de consignation dans certaines circonstances (électricien non disponible, etc.). Pour remédier à ce problème un autre moyen a été développé : il consiste à cadenasser un sectionneur local, placé à proximité de l'équipement. L'objectif principal de ce dernier dispositif est donc de permettre à un opérateur non électricien de consigner un équipement pour effectuer en toute sécurité une intervention. Bien que cette solution permette d'accélérer la procédure de consignation, il s'agit néanmoins d'une pratique encore controversée, notamment en raison du risque d'explosion électrique qui pourrait résulter d'une mauvaise utilisation des sectionneurs locaux, lors d'une remise sous tension trop brutale.

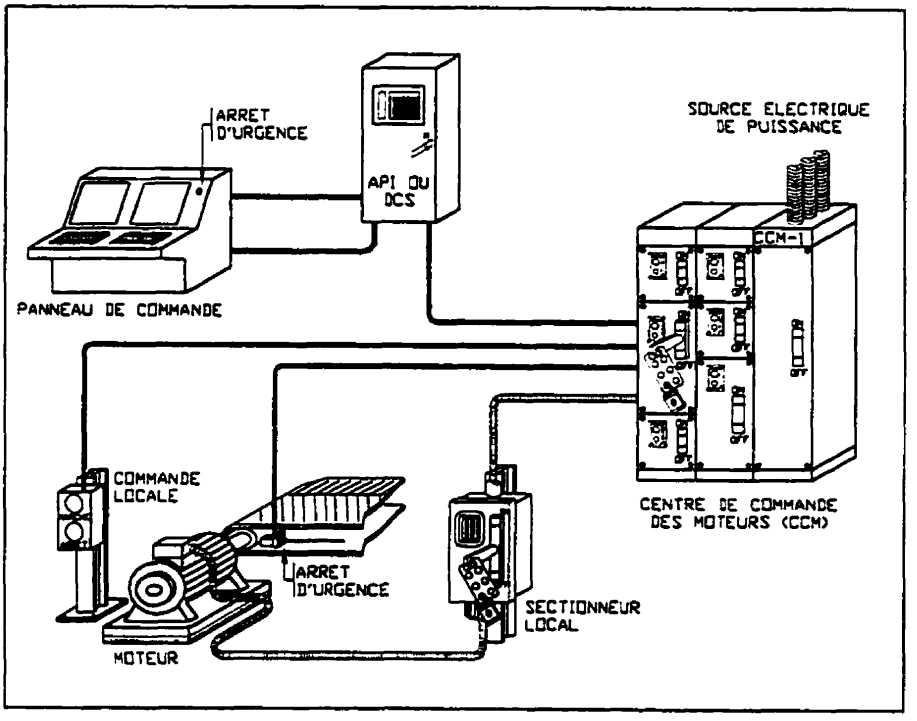

Figure 2.18 Circuits électriques de commande et de puissance [MONETTE, C., 1997]

2.1.3.8 Revues des normes de SST applicables aux SPA

Cette section a pour objectif de présenter brièvement les normes consultées dans le cadre de la présente recherche et qui peuvent avoir un apport pertinent. Certaines d'entre elles seront davantage explicitées dans des sections ultérieures.

Au Québec, la réglementation principale en vigueur est le *Règlement sur les établissements industriels et commerciaux* [Gouvernement du Québec, 1997]. Cette réglementation ne donne que des indications très générales et ne spécifie aucune mesure quant à la sécurité des SPA composés de technologies programmables. Les autres normes ou règlements québécois ne donnent pratiquement pas de détail supplémentaire sur les mesures spécifiques de protection à prendre envers les machines industrielles dangereuses [BOURBONNIÈRE, R. et coll., 1997].

Au niveau canadien, certaines normes spécifiques couvrent quelques aspects fonctionnels des machines dangereuses mais de façon peu détaillée. Par exemple, deux normes semblent se rattacher spécifiquement aux parties commandes des machines automatisées. Il s'agit de la norme sur la couleur des voyants lumineux et des boutons poussoirs [CAN/CSA Z431-M89, 1989] dont l'objectif est évident et de la norme sur les fonctions de sécurité utilisant les technologies électroniques [CAN/CSA C22.2, 1986] dont la portée est limitée [BOURBONNIÈRE, R. et coll., 1997]. Deux autres normes, plus récentes, traitent plus en détail des dispositifs de protection des machines dangereuses et de l'aspect sécuritaire des cellules et parcs robotisés. Ainsi, la norme CAN/CSA Z432-94 [1994] traite de la protection des personnes contre les risques que peut généralement présenter une machine. Des mesures concernant la conception, le choix des dispositifs de sécurité et des protecteurs ainsi que les généralités concernant l'ergonomie et l'identification des parties dangereuses sont présentées. Aussi, la norme CAN/CSA Z434-94 [1994] s'adresse spécifiquement aux diverses étapes du cycle de vie d'un robot ou d'une installation robotisée, qui sont, comme établi précédemment, des notions non couvertes dans ce mémoire. Enfin, une autre norme, d'une portée plus générale, dresse les grandes lignes concernant la gestion du risque [CAN/CSA Q634-91, 1991].

Au niveau international, les pays européens, à la faveur des efforts très importants de normalisation qui ont été engagés depuis plusieurs années, offrent une panoplie de normes touchant de multiples aspects de la SST et des SPA. Ces normes sont classées en 3 catégories, A, B et C [KNEPPERT, M. et coll., 1993].

Ainsi, il y a d'abord les normes de type A qui représentent des concepts de base, des principes de conception applicables à toutes les machines. La norme de référence sur les principes généraux

de conception en matières de sécurité des machines [EN 292, parties 1 et 2, 1991] offre plusieurs définitions et notions élémentaires de sécurité des machines associées aux risques et à leur analyse. Un autre ouvrage de référence est le projet de norme EN 1050 [1996] prescrivant les principes à respecter pour la gestion du risque. Aussi, un projet de norme actuellement en cours et rédigé par le *Comité électrotechnique international* (CEI) vise, un peu comme la norme EN 292, la gestion de la sécurité dans son sens le plus large [CEI/IEC 300, parties 1 à 3, 1995].

Quant à elles, les normes de type B traitent d'aspects particuliers liés à la sécurité, comme le niveau de bruit admissible, les distances homme-machine à respecter, les dispositifs de verrouillage et d'interverrouillage, etc. Du point de vue de la sécurité des systèmes de commande, deux projets de normes sont en cours [prEN 954, parties 1 et 2, 1996] [CEI/IEC 1508, parties 1 à 7, 1995], dont le dernier traite précisément des systèmes à base de technologies programmables. Également, un projet de norme traitant exclusivement des automates programmables et de leurs périphériques (outils de programmation et de déverminage, équipement de simulation, etc.) est actuellement en cours [CEI/IEC 1131, parties 1 à 5, 1993]. D'autre part, des normes concernant les arrêts d'urgence [prEN 418, 1990] [ISO/CEI 13850, 1995], les mises en marche intempestives [prEN 1037, 1994] et les dispositifs de verrouillages [prEN 1088, 1995] revêtent un caractère intéressant pour cette recherche.

Finalement, les normes de la catégorie C s'adressent à différents groupes ou types de machines bien spécifiques, comme les presses à métal, les machines dédies aux scieries, etc. Étant donné que ces normes sont très spécifiques et ne permettent pas de s'adapter facilement à l'évolution des technologies, elles ne seront pas exploitées dans la présente recherche.

Aussi, divers guides complémentaires ont été rédigés en vue de compléter et d'éclaircir certains aspects liés aux normes. Par exemple, le guide ISO/CEI 51 [1997] offre des principes directeurs pour inclure les aspects liés à la sécurité (tel que les définitions de termes, etc.) aux autres normes déjà existantes. Un autre guide présente uniquement les définitions de termes liés à la sécurité et ce pour de multiples applications et technologies [CEI/IEC 351, 1994]. Enfin, un guide a été rédigé en vue de permettre aux concepteurs de SPA désireux d'utiliser les normes existantes pour divers aspects (ergonomie, vibration, système de commande, etc.) dans le but de voir un peu plus

clair dans la panoplie de normes existantes [ISO/TC 199, 1996]. Il facilite grandement l'identification et la mise en application de ces diverses normes.

2.1.3.9 Les SÉP et la SST dans l'industrie québécoise des P&P

Tout au long des visites industrielles réalisées, quelques quatre mille (4000) rapports d'accidents survenus au cours des deux dernières années ont été recueillis [COLLINGE, C., 1998]. Cependant, ces accidents n'ont pas encore été analysés et ne sont très probablement pas tous liés à l'utilisation des SÉP pour l'automatisation des systèmes de production. Néanmoins, au cours des visites, il a tout de même été possible de constater que l'aspect de la santé et sécurité du travail est bien implantée dans l'industrie québécoise des P&P. Beaucoup de sensibilisation a été faite au cours des dernières années et les résultats sont visibles.

Par ailleurs, tous les employés ont été conscientisés des dangers qui sont associés à l'implantation des technologies programmables dans leur milieu de travail. Néanmoins, des pratiques plus ou moins sécuritaires ont pu être observées. À titre d'exemple, dans quelques usines, certains opérateurs utilisent les arrêts d'urgence, et même dans certains cas des arrêts commandés par le SCD pour effectuer des interventions de courte durée, comme débloquer un convoyeur de copeaux. Pourtant, toutes les usines visitées avaient des procédures strictes et très claires : avant d'effectuer une intervention sur un équipement, il faut consigner ce dernier, peu importe la durée de l'intervention. De plus, l'ensemble du personnel, y compris les opérateurs, savent très bien qu'un arrêt commandé par un SCD (ou un API) n'est pas fiable et que les arrêts d'urgence servent à arrêter l'équipement pour de véritables urgences. Néanmoins, des dérogations à ces règles de l'art ont tout de même pu être observées. Lorsque la discussion avec les opérateurs en question est poussée un peu plus loin, un problème est alors mis à jour : la procédure de consignation et les dispositifs de consignation ne facilitent pas toujours leur tâche. Comme ce problème est souvent dénoncé par les opérateurs, plusieurs solutions sont mises à l'essai : installation de sectionneurs locaux pour permettre à un opérateur non électricien de consigner un équipement (voir figure 2.18) ; installation de boutons d'arrêt pouvant être cadenassés ; etc.

Par contre, un point très marquant qui est ressorti surtout lors des deux groupes de discussion est l'importance qu'accordent tous les employés rencontrés à la consignation des équipements, et ce peu importe leur formation et leur fonction. Il semble en effet que cette procédure constitue leur passeport pour la sécurité. Or, comme il en sera question à la section 2.2.1.1, les *procédures* n'offrent pas toujours un bon niveau de sécurité, car ce dernier est fortement lié à la volonté et à la capacité de la personne concernée à respecter la procédure établie. La consignation des équipements est très importante, mais il y a aussi d'autres moyens pour assurer la sécurité des personnes!

Du point de vue technique, l'état de l'art en matière d'automatisation avec les SÉP semble être assez bien respecté. Les fonctions de sécurité directes sont généralement assurées par une logique câblée, comme recommandé par plusieurs auteurs et documents normatifs. Néanmoins, quelques lacunes ont pu être observées par rapport à l'utilisation de dispositifs de protection. Par exemple, il est très fréquent de retrouver des dispositifs de commande destinés à la surveillance de la production qui sont associés à des fonctions de sécurité. Or, bien qu'économiquement plus abordables, ces dispositifs ne doivent pas être utilisés pour garantir les fonctions de sécurité, car ils n'ont pas été conçus à cet effet. Leur mauvaise utilisation pourrait résulter en des accidents. Un autre exemple digne de mention est l'installation d'un câble d'acier relié à un dispositif d'arrêt d'urgence tout le long d'un convoyeur[11]. Malheureusement, le câble était si peu tendu qu'il fallait le tirer sur plus de dix mètres avant de mettre à l'arrêt l'équipement. Il semble donc que les concepteurs manquent de formation pour choisir et installer convenablement les dispositifs de protection qui sont offerts sur le marché.

Par ailleurs, un autre point important à considérer et pouvant être le siège d'éventuels accidents est la facilité de modification des programmes. Dans les usines visitées, aucun programme d'API n'était réellement protégé de telle sorte que les électriciens, les électrotechniciens et les ingénieurs pouvaient les modifier. Il a même été relaté un cas de sabotage via un API lors de négociations pour une convention collective! Sur les sept usines visitées, une seule fait exception

[11] Cette façon de faire, très courante et tout à fait correcte, a pour but de permettre l'interruption instantanée à partir de n'importe où le long de cet équipement (certains ont 100 mètres de longueur).

à la règle alors qu'il n'y avait que l'ingénieur en électricité/instrumentation qui pouvait modifier les programmes des API et des SCD. Par contre, les électriciens pouvaient *forcer* certaines fonctions du programme lorsque cet ingénieur n'était pas présent (la nuit ou les journées de congé par exemple). Cependant, lorsqu'une telle manoeuvre était effectuée, un mémo devait être rédigé et transmis à l'ingénieur. Aussi, l'usine prévoyait faire l'acquisition d'un logiciel pouvant détecter toutes modifications apportées aux programmes et ainsi permettre à l'ingénieur de suivre l'évolution des programmes. Cet exemple est le seul moyen efficace répertorié au cours des diverses activités réalisées avec les représentants de l'industrie des P&P du Québec.

Finalement, outre la facilité de modification des programmes, l'absence de procédures standardisées de programmation dans la plupart des usines visitées fait en sorte que les structures des programmes diffèrent énormément, parfois même au sein de la même usine. Ce problème a également été dénoncé lors d'un groupe de discussion.

2.2 Revue des approches, méthodes et outils de conception de SPA sécuritaires

La section précédente a fait ressortir que des problèmes de sécurité face à l'application des technologies programmables dans les automatismes industriels existaient. En fait, *«on a pu observer des incidents et des pannes directement associés à ces nouvelles technologies utilisées de façon non appropriée»* [PAQUES, J.-J., 1991].

Or, la *Loi sur la santé et la sécurité du travail* du Québec *«a pour objet l'élimination à la source même des dangers pour la santé, la sécurité et l'intégrité physique des travailleurs»* [Gouvernement du Québec, 1997]. D'autres documents de référence importants dont la norme canadienne sur la sécurité des machines industrielles [CAN/CSA Z-432, 1994] et la norme européenne sur les principes de base de la sécurité des machines [EN 292-1, 1991] abondent dans ce sens. Ainsi, par une conception appropriée, il faut tenter d'éliminer ces dangers potentiels.

Cette section a pour objectif de présenter les diverses stratégies mises en oeuvre pour parvenir à concevoir des SPA aussi sécuritaires que possible. Avant d'en entreprendre la lecture, le candidat tient à préciser que le vocabulaire introduit dans ces sections est très pointu. Il vous est donc conseillé de relire les définitions présentées dans le lexique en cas de doute sur l'interprétation des termes.

Dans un premier temps, la stratégie globale pour la maîtrise du risque est établie. Cette dernière permettra au lecteur de s'imprégner de la philosophie générale à observer dans tous les projets de conception où des dangers sont présents. Par la suite, en vue d'appliquer la stratégie globale pour la maîtrise du risque, les méthodes d'analyse du risque sont introduites et des modèles pour la gestion du risque sont présentés. Puis, divers outils permettant de mieux identifier, définir et structurer les besoins des utilisateurs des SPA sont exposés. Ensuite, quelques principes techniques permettant d'augmenter le niveau de sécurité des SPA utilisant des technologies programmables sont établis. Finalement, des démarches complètes de conception intégrant un ou plusieurs des éléments annoncés ci-dessus sont présentées. Ces dernières constituent le coeur de cette recherche.

2.2.1 Stratégie globale pour la maîtrise du risque

Cette section a pour but de permettre au lecteur de se familiariser avec le concept de la maîtrise des phénomènes dangereux. Dans un premier temps, le principe fondamental à mettre en oeuvre pour l'élaboration des solutions sécuritaires est présenté. Par la suite, un modèle théorique schématisant les liens causaux pouvant conduire à un accident est établi. Finalement, la présentation de la stratégie pour la maîtrise des phénomènes dangereux conclue cette section.

2.2.1.1 Échelle de priorité des solutions pour la maîtrise du risque

Un principe fondamental devant toujours être considéré est l'échelle de priorité des solutions pour la maîtrise du risque. L'échelle de priorité se compose de quatre niveaux que le concepteur doit parcourir dans l'ordre, à savoir [GALLAGHER, V.A., 1991][EN 292-1, 1992] :

1. éliminer le phénomène dangereux à la source ou en diminuer le risque ;
2. prévoir des protections contre les phénomènes dangereux qui n'ont pas pu être éliminés ou leur risques suffisamment diminués ;
3. informer les utilisateurs contre les risques résiduels ;
4. prendre toutes les dispositions supplémentaires nécessaires.

Le premier niveau, le plus souhaitable, est celui qui implique que c'est par sa conception même que le phénomène dangereux est éliminé ou son risque réduit. C'est précisément ce niveau que la littérature favorise. Cependant, c'est le second niveau qui est le plus fréquemment appliqué par les concepteurs d'aujourd'hui. Il s'agit d'une approche qui revêt souvent un caractère curateur et qui n'élimine pas toujours les phénomènes dangereux mais qui en minimise l'impact [GAUTHIER, F., 1997]. Le troisième niveau, celui des informations et des mises en garde, est souvent nécessaire pour prescrire les procédures et les modes opératoires prévus pour maîtriser les phénomènes dangereux, indiquer si une formation spéciale est requise et s'il faut prévoir un équipement de protection supplémentaire [EN 292-1, 1992]. Le quatrième niveau, comprenant entre autres les équipements de protection individuels et les procédures de travail (procédure de consignation, etc.), ne doit être utilisé qu'en dernier recours. En fait, le concepteur prudent n'utilise jamais ce niveau comme substitut à une mauvaise conception [GALLAGHER, V.A., 1991].

2.2.1.2 Modèle théorique de causalité des accidents

Il a été établi que l'application des technologies programmables dans les SPA a causé des accidents, que ce soit dans les phases nécessitant une présence humaine (réglage, surveillance, maintenance) ou pendant son fonctionnement normal [DEI-SVALDI, D et coll., 1984].

En vue de comprendre comment ces accidents se produisent, plusieurs modèles décrivant les liens de causalité menant à leur origine existent [LEVESON, N.G., 1995]. Ces modèles sont nécessaires pour identifier toutes les causes des dommages (ou des atteintes à la santé) dans le but d'élaborer une stratégie d'intervention sur ces causes afin de maîtriser les risques de dommage [REUNANEN, M., 1993]. Ils permettent également d'apprécier les multiples liens de causalité qui caractérise généralement les problèmes de sécurité [STOOP, J.A., 1990]. La figure qui suit représente un modèle simple illustrant les liens de causalité menant à un dommage potentiel. Cette dernière est inspirée du modèle proposé par F. Gauthier [1997] ; son contenu a simplement été mis à jour.

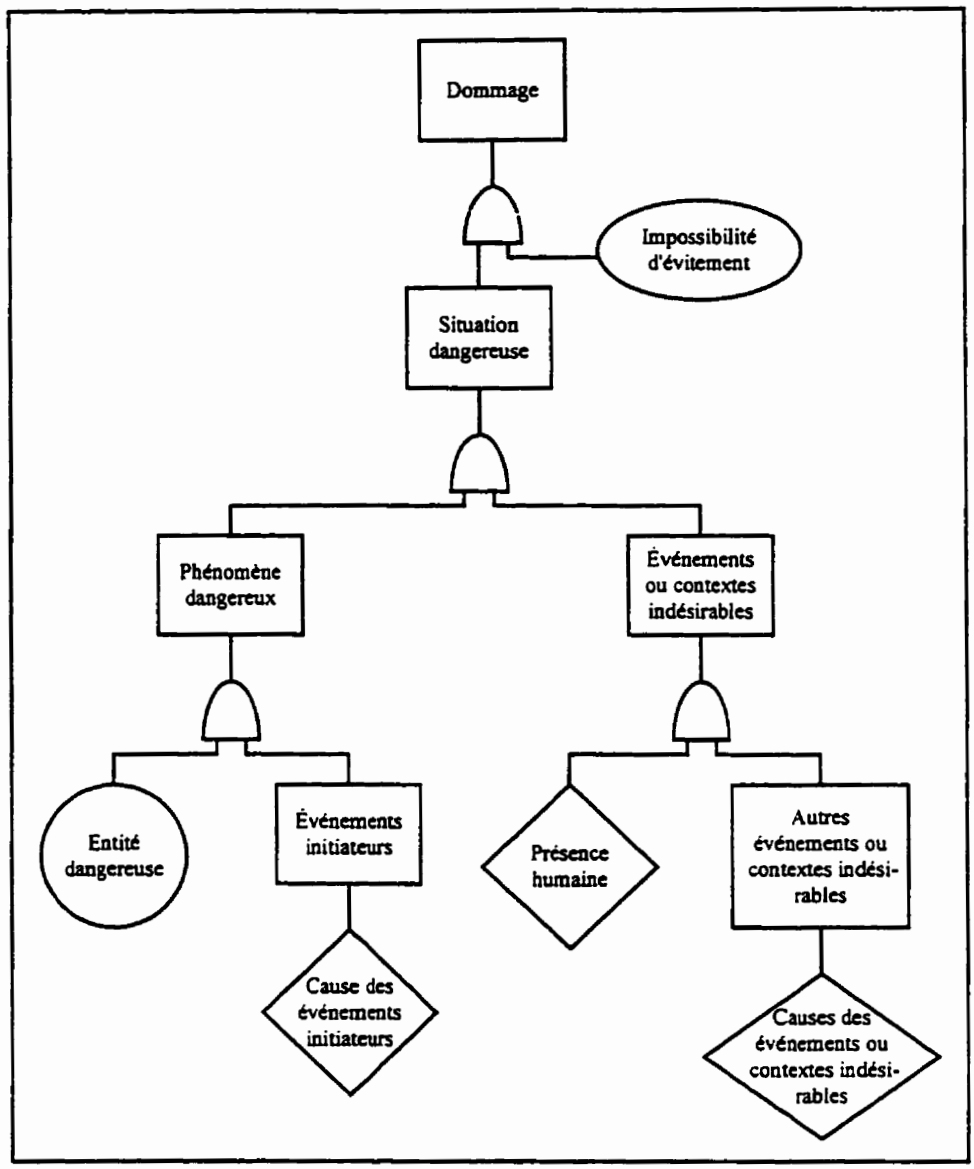

Figure 2.19 Modèle théorique simple de causalité des accidents

Les paragraphes qui suivent définissent chacune des étapes pouvant mener à un phénomène dangereux en vue de permettre au lecteur de mieux comprendre les événements et contextes qui en sont responsables. Pour en faciliter la compréhension, un exemple fictif est ici décortiqué en vue de mettre en relief les séquences et les événements qui ont conduit à l'accident décrit.

> *Alors qu'il procédait au nettoyage d'un défibreur, un mécanicien a subi des blessures sérieuses à un bras lorsque le moteur du défibreur s'est soudainement mis en marche. Après enquête, l'ordre d'arrêt du moteur (que l'API maintenait) a été interrompu en raison d'une interférence électrique dont la cause n'a pas encore été découverte.*

L'API a alors ordonné la mise en marche du moteur. Comme le mécanicien n'avait pas respecté les procédures de consignation, le moteur s'est mis en marche.

Les ***entités dangereuses*** sont des éléments d'un système ou d'une fonction auxquels sont associés des dangers intrinsèques [MERLAUD, C. et coll., 1992]. Les vis sans fin pour l'entraînement des copeaux, les conduites de vapeur d'eau sous pression et les bobines de papier enroulé sont des exemples d'entités dangereuses qu'il est possible de retrouver dans les papetières. Dans certains cas, le système entier est lui-même une entité dangereuse. Par exemple, la sécherie de la machine à papier est une entité dangereuse en raison de la chaleur qu'il y fait ou encore de la quantité imposante de rouleaux sécheurs en rotation qui s'y trouve. Dans l'exemple présenté, ce sont les couteaux du défibreur qui sont des entités dangereuses.

L'***événement initiateur*** est la condition qui fait en sorte que l'entité dangereuse devient effectivement un danger pour les personnes [GAUTHIER, F., 1997]. Dans l'exemple présenté, l'interférence électrique dont a été victime l'API est un événement initiateur.

Le ***phénomène dangereux*** est le résultat de l'association de l'entité dangereuse et de l'événement initiateur [ISO/CEI 51, 1997] [PAQUES, J.-J., 1997]. Toujours dans le même exemple, l'interférence électrique ordonnant l'activation intempestive des couteaux du défibreur est un phénomène dangereux.

L'***événement ou le contexte indésirable*** est la condition ultime pour que le phénomène dangereux dégénère en une situation dangereuse. L'activation intempestive des couteaux du défibreur était un phénomène dangereux qui pouvait provoquer ou non une situation dangereuse. La présence du mécanicien d'entretien au mauvais moment, au mauvais endroit et dans un contexte indésirable (non respect de la procédure de consignation) font que le phénomène dangereux a évolué vers une situation dangereuse ; l'intervention du mécanicien d'entretien sur l'équipement électrique non consigné est donc l'événement ou le contexte indésirable.

La ***situation dangereuse*** décrite par l'exposition des bras du mécanicien aux couteaux du défibreur activés intempestivement est la dernière condition avant qu'un dommage ne soit causé. S'il s'avère impossible d'éviter la situation dangereuse, un dommage en résultera. Dans

l'exemple présenté, le mécanicien n'a pas pu éviter cette situation dangereuse et a donc subi un dommage, soit de sérieuses blessures à un bras.

La figure qui suit montre les liens entre les divers éléments qui ont conduit au dommage et le tableau 2.3 (page suivante) résume son contenu et fait un lien entre cet exemple et le modèle théorique présenté à la figure 2.19.

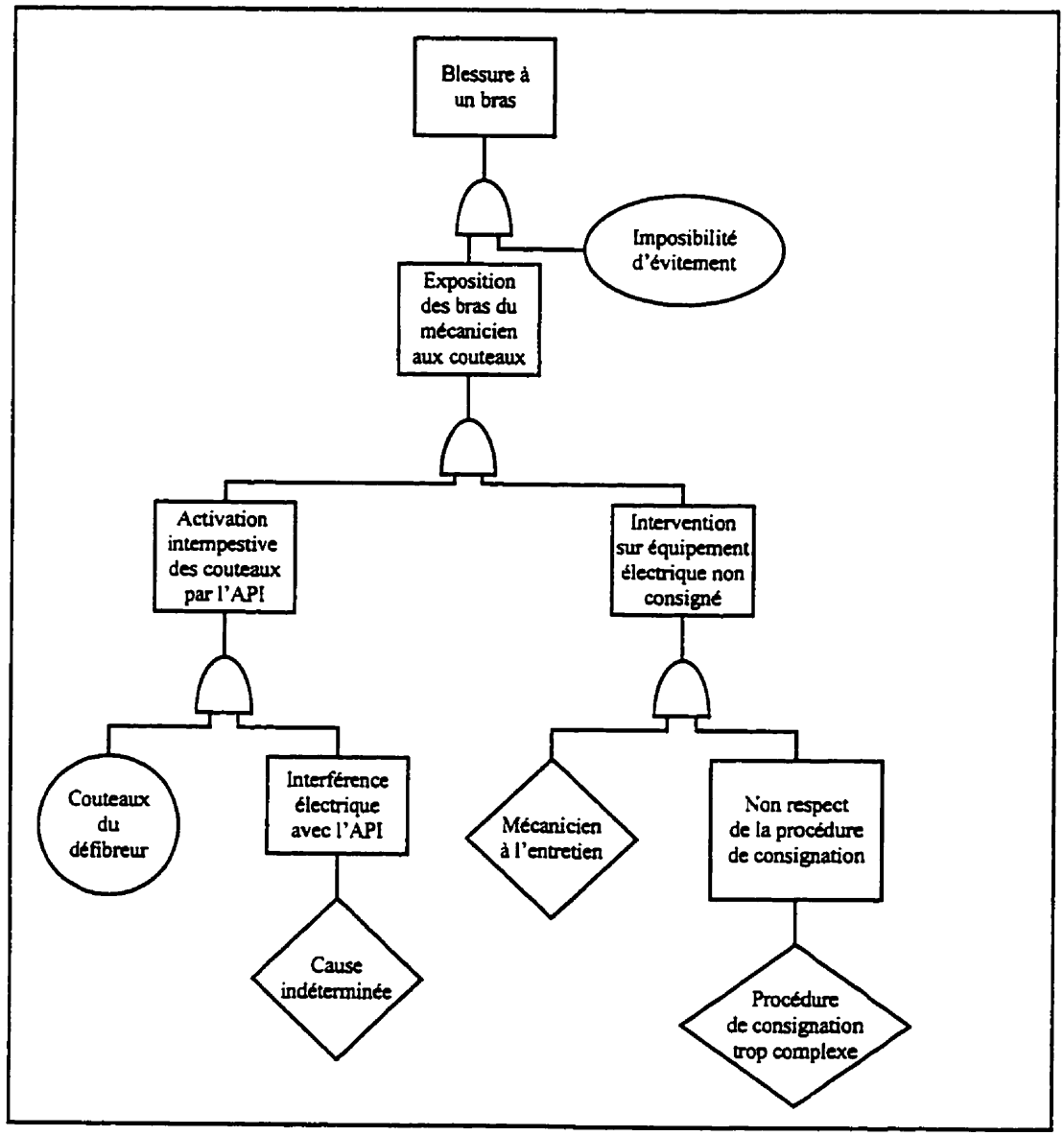

Figure 2.20 Exemple d'application du modèle théorique de causalité des accidents

TABLEAU 2.3 IDENTIFICATION DES COMPOSANTS DU SCÉNARIO D'ACCIDENT

Dommage	→	Blessure à un bras
Phénomène dangereux	→	Activation intempestive des couteaux
Entité dangereuse	→	Couteaux du défibreur
Événement initiateur	→	Interférence électrique avec l'API
Cause de l'événement initiateur	→	Indéterminée
Événements ou contextes indésirables	→	Intervention sur équipement électrique non consigné
Présence humaine	→	Mécanicien à l'entretien
Autres événements ou contextes indésirables	→	Non respect de la procédure de consignation
Cause de ces événements ou contextes indésirables	→	Procédure trop complexe pour la durée de l'intervention

2.2.1.3 Modèle théorique pour la maîtrise du risque

Selon le principe de l'échelle de priorité des solutions pour la maîtrise du risque établi précédemment, le premier niveau stipule qu'il faut tenter dans un premier temps d'éliminer le phénomène dangereux à la source ou d'en réduire son risque ; il s'agit donc d'obtenir une prévention intrinsèque. En appliquant ce principe au modèle théorique de causalité des accidents (figure 2.19), il ressort que pour atteindre cet objectif, il faut parvenir à réaliser l'une ou l'autre des actions suivantes ou encore une combinaison d'entre elles :

- supprimer l'entité dangereuse ou réduire la gravité qui lui est associée ;
- supprimer l'événement initiateur (et/ou ses causes) ou encore réduire sa probabilité d'occurrence ;
- supprimer la présence humaine ou à tout le moins réduire la fréquence de la présence humaine ;
- supprimer l'événement ou les contextes indésirables (et/ou leurs causes) ou encore réduire leur probabilité d'occurrence.

S'il s'avère impossible d'obtenir une prévention intrinsèque, il faut, comme l'indique le second niveau, protéger l'utilisateur contre les phénomènes dangereux en déployant des dispositifs de protection adéquats. Pour ce faire, il est possible dans un premier temps d'agir sur la conjonction entre *l'entité dangereuse* et *l'événement initiateur*. Dans ce cas, il faut rendre l'entité dangereuse insensible à l'événement initiateur par des principes techniques (tolérance aux fautes, etc.) qui seront présentés ultérieurement. Aussi, la détection de cette conjonction et la prescription de

moyens pour éviter que le phénomène dangereux se produise peuvent être de bonnes solutions. Dans un second temps, s'il est impossible d'intervenir au moment de la conjonction entre *l'entité dangereuse* et *l'événement initiateur*, il faut alors agir au niveau du phénomène dangereux lui-même en prescrivant un comportement du système tel que le phénomène dangereux sera éliminé dès qu'il se manifeste ou encore en installant des dispositifs de protection (garde protecteurs, etc.) qui réduiront son risque.

Puis, selon le troisième niveau, lorsqu'aucune parade n'est possible contre le phénomène dangereux, il faut informer l'utilisateur de ses risques résiduels. Il est alors possible de faire en sorte que l'utilisateur soit insensible au phénomène dangereux ou qu'il sache comment maîtriser ses risques, ou encore de rendre la situation dangereuse évitable ou de former l'utilisateur à détecter et à éviter cette dernière.

Enfin, le quatrième et dernier niveau, le moins préférable, peut se résumer à prévoir des moyens permettant de réagir au cas ou un dommage résulterait de la situation dangereuse (premiers soins, évacuation, etc.). La figure suivante intègre le principe de l'échelle de priorité des solutions pour la maîtrise du risque au modèle théorique de causalité des accidents présenté à la figure 2.19.

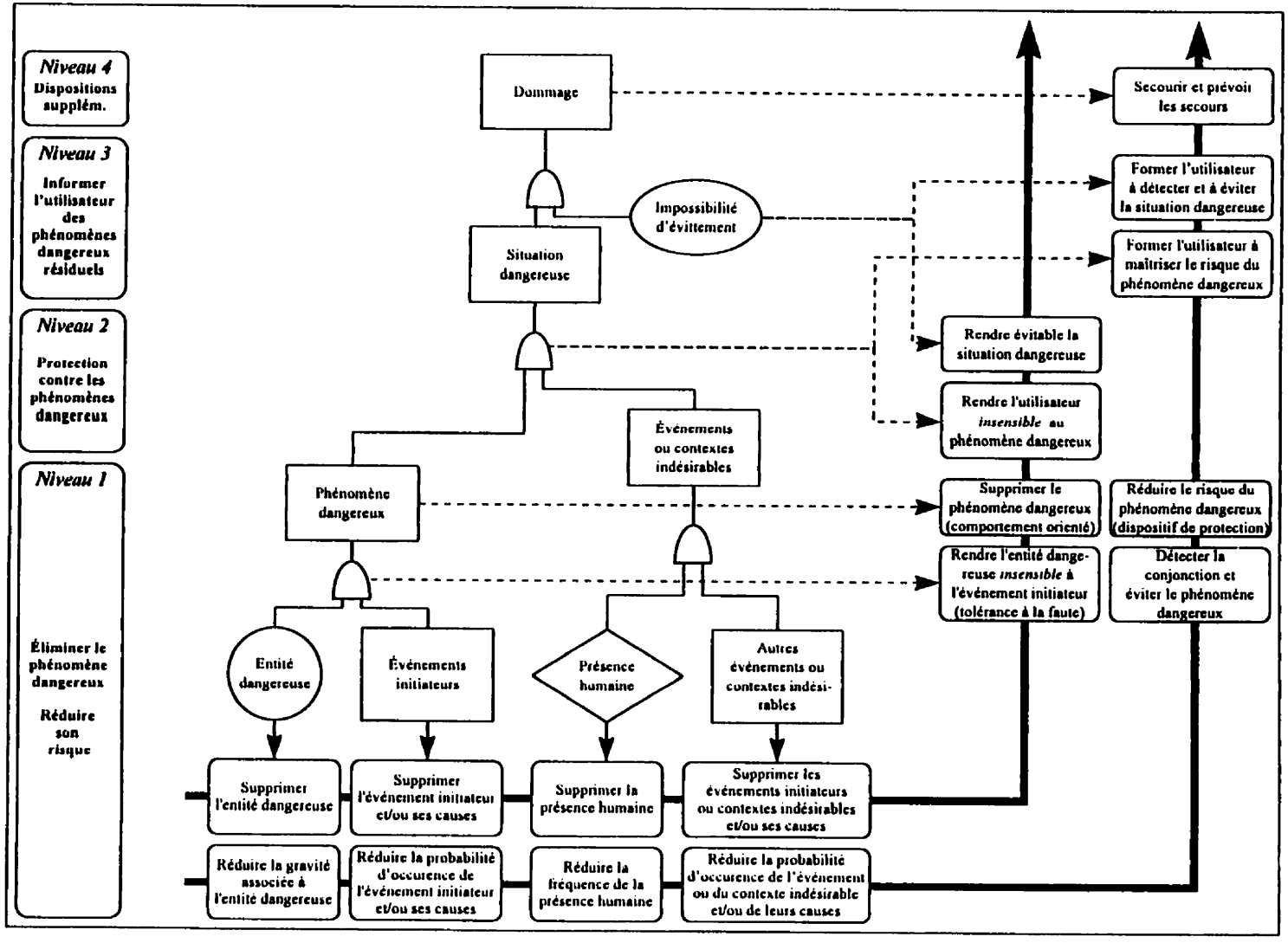

Figure 2.21 Modèle théorique pour la maîtrise du risque

2.2.2 Introduction aux méthodes d'analyse du risque

Comme établi en introduction à cette section, la mise en pratique de la stratégie pour la maîtrise des phénomènes dangereux débute par l'analyse de leur risque. Les paragraphes qui suivent traitent des méthodes d'analyse du risque.

2.2.2.1 Généralités

Il existe plusieurs méthodes dites *d'analyse du risque*. Ces méthodes ont été développées au fur et à mesure des besoins, le plus souvent par des spécialistes en fiabilité et en sécurité dans les domaines de l'industrie chimique, de l'aviation, de la défense et du nucléaire, et sont généralement assez bien décrites dans la littérature [REUNANEN, M., 1993]. Par exemple, un manuel (*System Safety Analysis Handbook*) de la *System Safety Society* présente brièvement 90 méthodes d'analyse du risque [STEPHANS, R.A. et coll., 1993]. De ces méthodes, certaines ont une application spécifique aux systèmes de production automatisés. De plus, quelques méthodes plus spécifiques aux applications informatiques s'ajoutent à cette liste [BARBET, J.F., 1991] [CEI/IEC 1508-7, 1995] [LEVESON, N.G., 1995] [ROUCHOUSE, G., 1991]. L'ensemble des méthodes répertoriées sont présentées à l'appendice 2.

Il convient également de préciser que plusieurs de ces méthodes ne sont en réalité que des dérivées de d'autres méthodes et qui ont été ajustées pour satisfaire un contexte particulier. Par exemple, la méthode *Damage Mode and Effect Analysis* est la version militaire de la méthode plus générale *Failure Mode and Effect Analysis*. Ceci laisse voir qu'il pourrait donc être possible d'adapter des méthodes existantes à différents contextes selon des besoins spécifiques [STEPHANS, R.A. et coll., 1993]. C'est la cas par exemple de la méthode HAZOP (*Hazard and Operability Analysis*) généralement utilisée pour l'analyse de la sécurité des procédés et qui a été adaptée à l'analyse des technologies programmables [CATMUR, J.R. et coll., 1992].

Dans un autre ordre d'idée, toutes les méthodes d'analyse du risque ne sont pas universellement applicables dans toutes les situations de conception ; certaines méthodes ont été conçues pour des domaines bien spécifiques. C'est le cas notamment de la méthode *Cryogenic System Safety Analysis* qui n'a d'application concrète que dans le domaine de la cryogénie [STEPHANS, R.A.,

1993]. Aussi, certaines sont davantage efficaces pour des analyses techniques alors que d'autres s'adressent à l'analyse des phénomènes dangereux associés aux facteurs humain [SUOKAS, J. et coll., 1988]. De plus, les méthodes offrent différents niveaux de détail dans l'analyse du risque. Par exemple, l'analyse énergétique est effectuée au niveau global tandis que les arbres de fautes permettent de modéliser des systèmes entiers à un niveau de détail très fin [STEPHANS, R.A., 1993]. Par ailleurs, comme il l'a été mentionné précédemment, bon nombre de ces méthodes ont été développées par des spécialistes en sécurité et en fiabilité provenant des industries chimiques et nucléaires. Ainsi, leurs procédures sont souvent conçues pour l'analyse de systèmes comportant des risques élevés [MASSÉ, S. et coll., 1994] [STOOP, J.A., 1993]. Conséquemment, elles ne sont pas nécessairement bien adaptées à l'analyse des phénomènes dangereux inhérents à la conception des SPA. Finalement, des études récentes ont démontré que plusieurs ingénieurs concepteurs de tous les domaines (et spécialement les ingénieurs en mécanique) ne connaissent pas ou n'utilisent pas les méthodes existantes pour l'analyse du risque [MAIN, B.W. et coll., 1992]. Il sera donc important d'établir des critères de sélection tenant compte de ces aspects en vue de proposer celles qui sont les plus pertinentes et susceptibles d'être appliquées lors de la conception de systèmes de production automatisés destinés à l'industrie québécoise des P&P. Les travaux de F. Gauthier du *Groupe de recherche en ingénierie simultanée* (GRIS) de l'Université de Sherbrooke pourraient alors être utilisés.

2.2.2.2 Classification des méthodes d'analyse du risque

Dans sa thèse, F. Gauthier [1997] a établi trois principaux critères pour classifier les méthodes d'analyse du risque :

a) selon leur nature ;
b) selon leurs objectifs ;
c) selon les facteurs de risque identifiés.

a) Classification des méthodes d'analyse du risque selon leur nature

Dans un premier temps, les méthodes d'analyse du risque peuvent être de deux natures : originale ou globale. Une méthode est dite originale lorsqu'elle propose une démarche spécifique pour faire l'analyse du risque à l'aide d'une méthodologie généralement bien définie. Quant à elles,

les méthodes globales proposent généralement un contexte particulier pour l'application d'une ou plusieurs méthodes originales. Elles ne spécifient pas comment faire l'analyse ou quelles méthodes originales utiliser ; elles indiquent plutôt à quel moment et dans quelles circonstances effectuer cette analyse [STEPHANS, R.A. et coll., 1983]. Une première classification des méthodes peut donc être faite selon ces deux critères ; c'est ce qu'illustre la figure suivante.

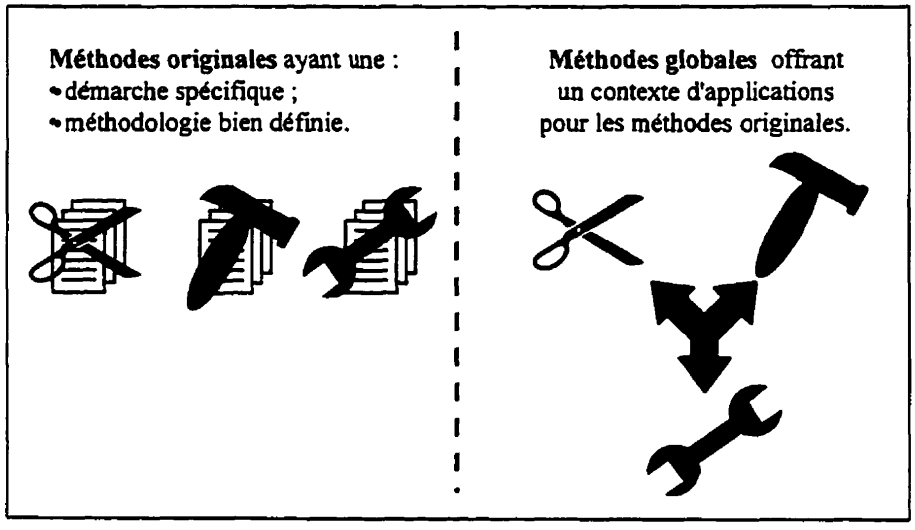

Figure 2.22 Méthodes originales et méthodes globales d'analyse des risques

b) Classification des méthodes d'analyse du risque selon leurs objectifs

Le second critère de classification tient compte cette fois des objectifs principaux que la méthode d'analyse du risque poursuit, soit [GAUTHIER, F., 1997] :

1. l'identification des phénomènes dangereux et de leurs causes ;
2. l'estimation du risque associé aux phénomènes dangereux.

Les méthodes d'identification des phénomènes dangereux et de leur causes ont essentiellement pour objectif de répertorier tous les phénomènes dangereux qui pourraient être présents dans l'environnement du SPA. Trois modes d'analyses sont distinguées dans ce cas : les analyses déductives, les analyses inductives et les analyses informatives [RAAFAT, H.M.N., 1979].

L'analyse inductive (des causes vers l'effet) débute par la définition des possibilités de faute pouvant survenir lors de l'utilisation d'un système de production automatisé pour en venir à prédire leurs conséquences probables, c'est-à-dire les phénomènes dangereux pouvant être

engendrés. À l'inverse, l'analyse déductive (de l'effet vers les causes) consiste à identifier les phénomènes dangereux qui peuvent survenir pour identifier par la suite toutes les causes qui pourraient en être responsables. La figure qui suit schématise la démarche de ces deux types d'identification des phénomènes dangereux et de leurs causes.

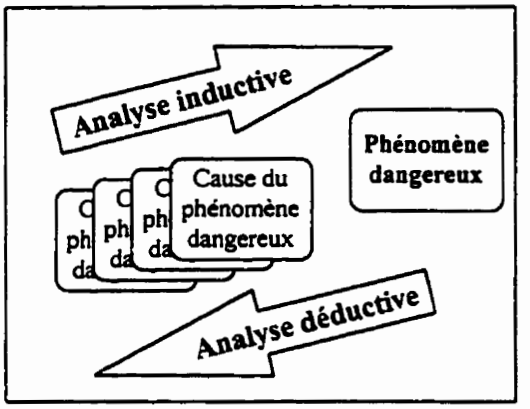

Figure 2.23 Analyse déductive et analyse inductive [GAUTHIER, F., 1997]

Finalement, l'analyse informative, qui est ni déductive, ni inductive, a pour objectif de recueillir des informations concernant les phénomènes dangereux et leurs causes et peut être utilisée en conjonction avec n'importe quelle autre méthode d'analyse [GAUTHIER, F., 1997].

Par ailleurs, l'identification des phénomènes dangereux et de leurs causes peut également suivre un mode rétrospectif ou prospectif. Dans le premier cas, l'historique du système automatisé à concevoir est étudié pour identifier les risques inhérents à son utilisation. Cet historique peut provenir de rapports d'accidents impliquants des systèmes semblables, de l'expérience des utilisateurs, etc. Quant à elle, les analyses prospectives cherchent à prédire quels pourraient être éventuellement les phénomènes dangereux engendrés par un système de production automatisé en conception [STOOP, J.A., 1990]. L'expérience et l'intuition des concepteurs sont les plus grandes sources d'informations disponibles lors de l'utilisation des méthodes prospectives.

En résumé, les méthodes d'identification des phénomènes dangereux et de leurs causes peuvent être regroupées sous quatre catégories, soit les méthodes permettant les analyses rétrospectives

déductives, prospectives déductives, prospectives inductives et informatives [GAUTHIER, F., 1997]. C'est ce que schématise la figure qui suit.

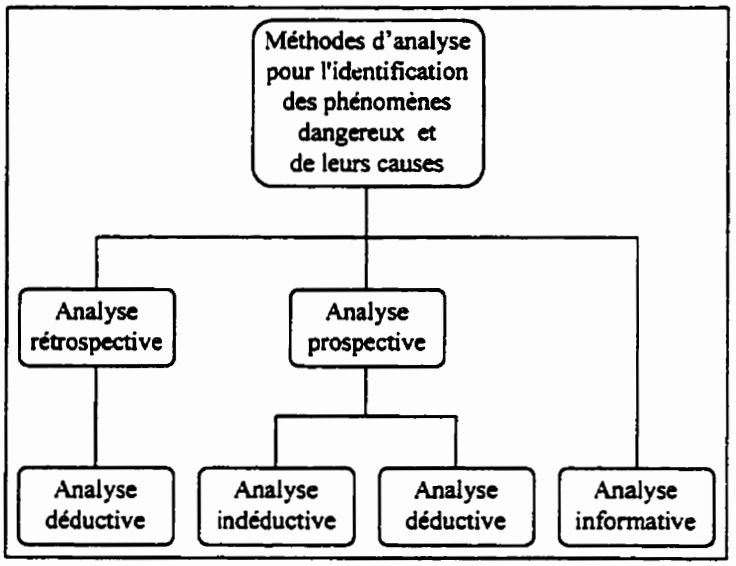

Figure 2.24 Méthodes d'identification des phénomènes dangereux et de leurs causes

D'autre part, le second objectif de certaines méthodes d'analyse du risque concerne l'estimation du risque. Ces dernières permettent aux concepteurs de mesurer le risque associé à un phénomène dangereux en évaluant principalement sa probabilité d'occurrence et la gravité des dommages possibles. Une façon simple de représenter le risque est de le projeter sur un plan probabilité-gravité, comme celui de la figure suivante [MERLAUD, C. et coll., 1992].

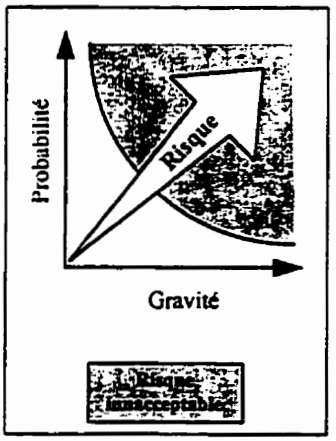

Figure 2.25 Représentation graphique du risque

La composante *gravité* permet d'évaluer les dommages que pourrait induire le phénomène dangereux analysé. Par exemple, il peut être question d'une gravité mineure, majeure, critique ou catastrophique [MERLAUD, C. et coll., 1992]. Cette classification possède généralement un caractère particulièrement subjectif, comme en témoigne d'ailleurs les termes donnés en exemple.

La composante *probabilité* exprime quant à elle la fréquence d'occurrence, observée ou estimée, d'une situation dangereuse [MERLAUD, C. et coll., 1992]. Cette composante du risque peut être évaluée quantitativement lorsque les données techniques (la fiabilité des composants par exemple) ou des statistiques d'accidents sont disponibles [GAUTHIER, F., 1997]. Par exemple, dans son livre *Sûreté des automatismes*, G. Rouchouse [1992] cite 9 banques de données de fiabilité de composants utilisés dans les systèmes de production automatisés. Le plus souvent cependant, cette évaluation est qualitative, basée sur le jugement d'experts, sur l'expérience des concepteurs et sur les données historiques disponibles [EN 292-1, 1992] [prEN 1050, 1996].

L'estimation du risque associé à un phénomène dangereux peut donc se faire de deux façons : par une analyse quantitative ou par une analyse qualitative. C'est ce qu'illustre la figure qui suit.

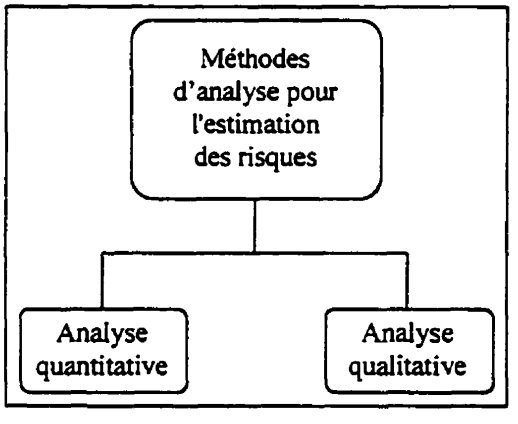

Figure 2.26 Méthodes d'estimation du risque

Les méthodes quantitatives d'estimation du risque font généralement appel à des notions de fiabilité qui peuvent devenir rapidement complexes [MERLAUD, C. et coll., 1992]. Les méthodes à caractère qualitatif sont donc souvent préférées étant donné leur facilité de mise en oeuvre. Parmi celles-ci, les grilles d'estimation du risque sont intéressantes. Le projet de norme EN 1050 [1996] en propose une relativement simple à compléter. Aux composantes probabilité

et gravité déjà présentées s'en ajoutent deux autres : la fréquence d'exposition au phénomène dangereux et la possibilité d'éviter ce dernier. La figure qui suit reproduit cette grille d'estimation du risque.

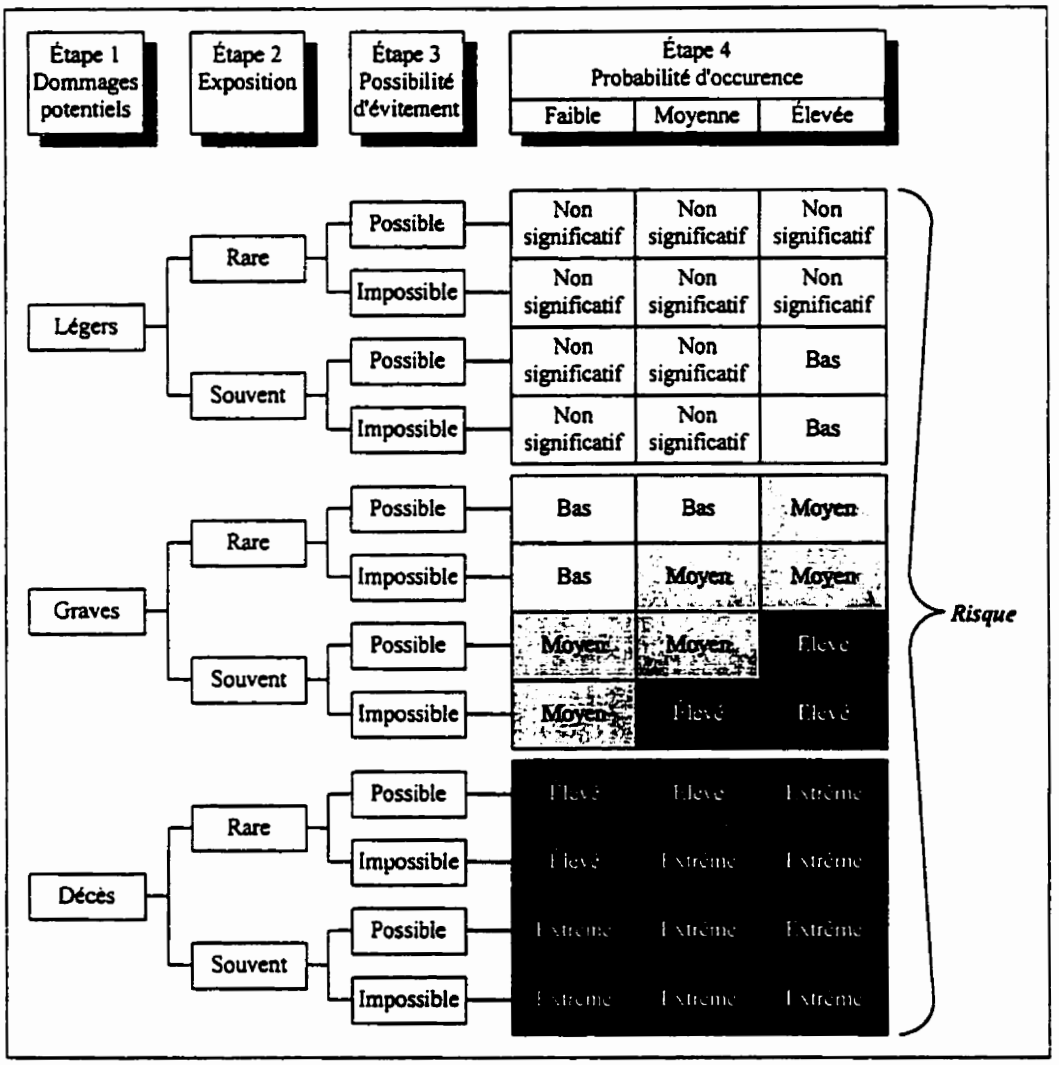

Figure 2.27 Grille d'estimation qualitative du risque [prEN 1050, 1996]

c) Classification des méthodes d'analyse du risque selon les facteurs de risque identifiés

Finalement, le dernier critère de classification prend en considération que les phénomènes dangereux généralement observés dans l'environnement immédiat d'un SPA peuvent provenir de différents facteurs de risque. Ainsi, il pourra être question de méthodes d'analyse considérant des facteurs de risque [SUOKAS, J. et coll., 1988] :

- humain (erreur humaine, mauvais usage, etc.) ;
- technique (défaillance d'un SÉP, bris d'un dispositif de verrouillage, etc.) ;
- organisationnel (procédure de consignation désuète, mauvaise communication, etc.) ;
- externe (phénomène naturel, incendie, etc.).

En résumé, cette section a permis d'établir que les méthodes d'analyse du risque peuvent être classifiés selon trois critères, soit :

- leur nature (globale ou originale) ;
- les objectifs qu'elles poursuivent, à savoir l'identification de phénomènes dangereux ainsi que leurs causes (selon un mode rétrospectif ou prospectif suivant une approche informative, déductive ou inductive) et l'estimation (quantitative ou qualitative) des risques associés aux phénomènes dangereux ;
- les types de facteurs de risque considérés (humain, technique, organisationnel et externe).

La figure qui suit présente donc la synthèse des classifications possibles des différentes méthodes d'analyse du risque.

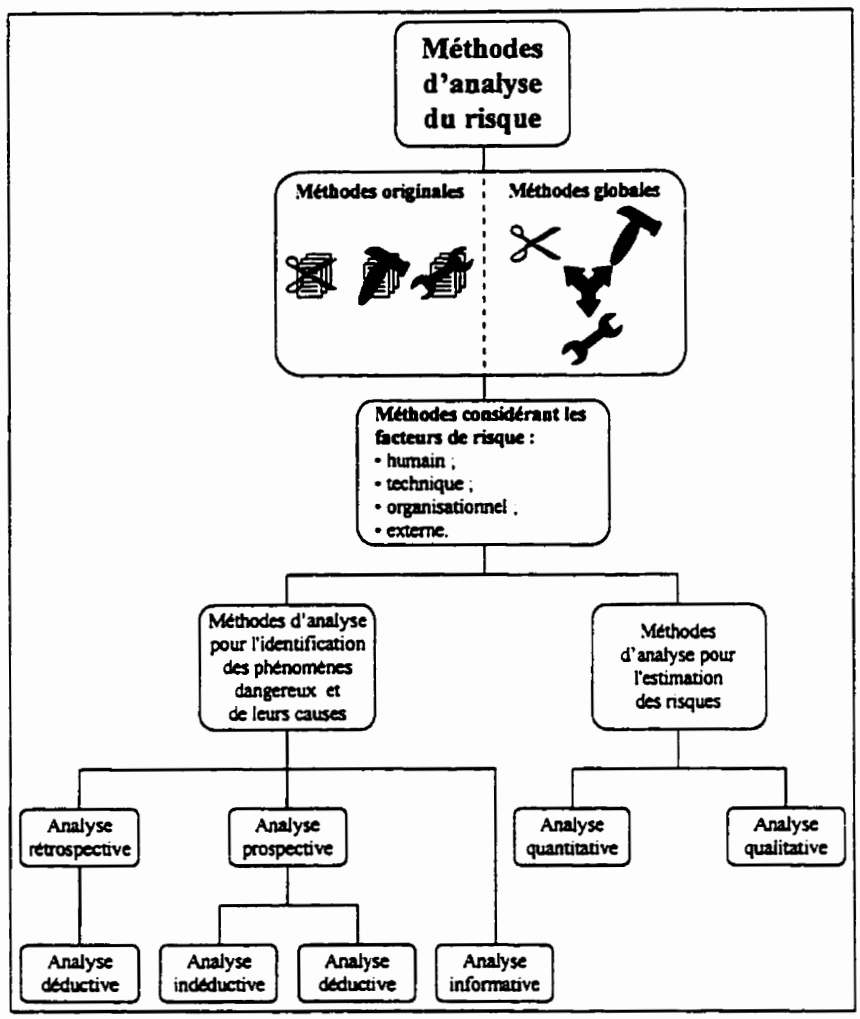

Figure 2.28 Synthèse des classifications possibles des méthodes d'analyse du risque

2.2.2.3 Méthodes d'analyse du risque utilisées pour la conception des SPA

Comme établi précédemment, plusieurs méthodes d'analyse du risque existent et plusieurs sont énumérées à l'appendice 2. Cependant, pour que les concepteurs puissent intégrer ces méthodes d'analyse du risque à leurs activités de conception, ces dernières doivent être limitées en nombre. En effet, *«une surcharge au niveau du nombre potentiel de méthodes à utiliser a toutes les chances de faire en sorte que l'approche paraisse trop complexe aux yeux des concepteurs»* [GAUTHIER, F., 1997]. Ce dernier auteur présente dans sa thèse quelques critères généraux permettant de restreindre le nombre de méthodes d'analyse du risque. Ainsi, pour qu'elle soit

considérée lors de la conception d'outils, de machine ou de procédés industriels commun, la méthode :

- doit être indépendante, c'est-à-dire qu'elle ne nécessite pas l'application d'une autre méthode pour obtenir les résultats ;
- ne doit pas être une combinaison d'un certain nombre de méthodes ;
- doit être raisonnablement facile à appliquer et utile pour la conception d'outils, de machines ou de procédés industriels communs ;
- doit être suffisamment documentée et cette documentation doit être raisonnablement accessible pour les concepteurs ;
- doit être assez connue et répandue dans l'industrie.

Grâce à ces critères, F. Gauthier [1997] a pu identifier 14 méthodes qu'il a intégré à sa démarche parmi les 91 qu'il avait répertoriées[12].

Par ailleurs, dans son ouvrage, G. Rouchouse [1992] mentionne que les méthodes les plus fréquemment rencontrées en conception d'automatismes sont :

- *Failure Mode and Effect Analysis* ;
- *Hazard and Operability Analysis* ;
- *Fault Tree Analysis* ;
- les graphes de Markov.

Ces mêmes méthodes sont mentionnées dans un grand nombre d'ouvrages consultés dans le cadre de cette recherche [CAN/CSA Q634-91, 1991] [CEI/IEC 1508, 1995] [prEN 954-1, 1996] [prEN 1050, 1996].

Ces informations seront donc très utiles lorsque viendra le temps d'identifier quelles méthodes, parmi celles présentées à l'appendice 2, seront retenues pour l'élaboration de la solution.

[12] Ces 14 méthodes sont davantage détaillées à l'appendice 3.

2.2.2.4 Revue des normes concernant les méthodes d'analyse du risque

Parmi toutes les normes consultées et présentées à la section 2.1.3.8, aucune n'exige clairement l'utilisation d'une méthode particulière d'analyse du risque. Par contre, quelques ouvrages importants prescrivent une étape d'analyse du risque [CAN/CSA Q634-91, 1991] [CEI/IEC 1508, 1995] [prEN 1050, 1996].

Ainsi, la norme canadienne Q 634-91 [1991] indique que des méthodes formelles d'identification des phénomènes dangereux doivent être appliquées et offre en exemple quelques méthodes, dont le *Failure Mode and Effect Analysis* (FMEA), le *Hazard and Operability Analysis* (HAZOP) et les arbres de faute (*Fault Tree Analysis, FTA*). En ce qui a trait à l'estimation du risque, il est indiqué qu'elle doit être faite pour tous les phénomènes dangereux identifiés. Cette dernière tient compte de la probabilité d'occurrence du phénomène dangereux ainsi que de la gravité de ses dommages potentiels et, tout comme pour le projet de norme EN 1050 [1996], est représentée dans une grille.

Par ailleurs, la norme française de référence EN 292 [1991] n'offre aucune prescription quant aux méthodes d'analyse du risque. Seule une liste de contrôle indique diverses sources de phénomènes dangereux qu'il faut considérer lors de la conception d'un équipement[13]. C'est le projet de norme EN 1050 [1996] qui traite de l'analyse du risque pour la normalisation européenne. Cette dernière stipule que *«tous les dangers, les situations dangereuses et les phénomènes dangereux doivent, conformément à la norme EN 292, être identifiés»*. Pour ce faire, encore là, aucune méthode n'est recommandée mais quelques unes (au nombre de 7) sont présentées à titre d'exemple. Aussi, un peu plus loin dans le texte normatif, il est écrit qu'après l'identification des phénomènes dangereux, l'estimation de leur risque doit être faite. La grille d'estimation du risque proposée par cette norme est celle qui a été présentée à la figure 2.27.

Par ailleurs, le projet de norme EN 954 [1996] propose une autre grille d'estimation des risques associés aux phénomènes dangereux comme l'indique la figure suivante.

---

[13] Le tableau 2.5 présente cette liste de contrôle un peu plus loin dans ce mémoire (page 100).

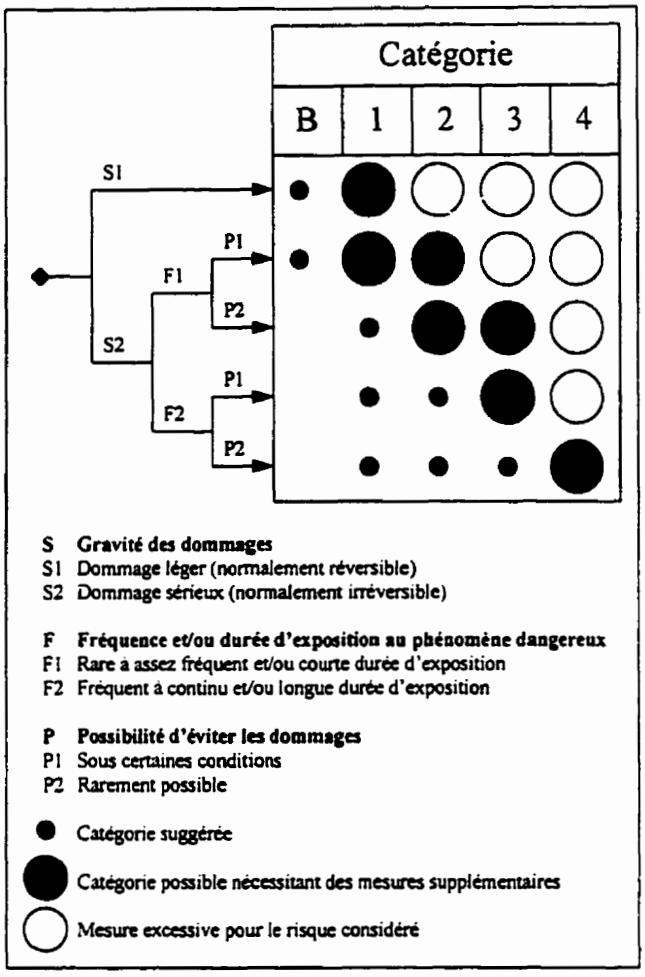

Figure 2.29 Estimation du risque par catégorie [prEN 954-1, 1996]

Ainsi, en se basant sur des critères très simples et non ambigus, l'estimation du risque mène à la sélection d'une catégorie (B, 1, 2, 3 et 4). Un aspect intéressant lié à ce concept est la prescription très claire de spécifications liées à la sécurité pour chacune de ces 5 catégories. Ainsi, en estimant le risque associé à un phénomène dangereux, la norme propose au concepteur des dispositions reliées à la sécurité qui sont adaptées au niveau de risque estimé et propose même des moyens techniques pour les mettre en oeuvre. Il s'agit là d'un concept très intéressant.

Finalement, le projet de norme IEC/CEI 1508 [1995] prescrit également une analyse du risque tout en indiquant que cette dernière peut se réaliser au moyen de diverses techniques. Quelques indications visant à orienter le choix parmi ces techniques sont présentées aux concepteurs, mais aucune classification ou recommandation n'est faite. À cet effet, la partie 7 de ce projet de norme

présente une imposante quantité de techniques d'analyse du risque dont plusieurs se rapportent spécifiquement au logiciel. La norme prescrit également une estimation du risque. Tout comme le projet de norme EN 954 divisait en catégorie le risque, des niveaux de sécurité (*Safety Integrity Level*) sont identifiés en fonction du risque estimé et des prescriptions très claires sont également émises, à l'exception que ces dernières concernent particulièrement les SÉP. Il va donc sans dire qu'il s'agit là d'un aspect intéressant pour la présente recherche.

2.2.2.5 Méthodes d'analyse du risque utilisées dans l'industrie québécoise des P&P

Lors des activités effectuées dans le cadre de cette recherche, il a pu être constaté qu'il n'y a pratiquement aucune méthode d'analyse du risque qui soit appliquée. En fait, parmi toutes les méthodes présentées à l'appendice 2, trois seulement ont été mentionnées. La première est le *Hazard and Operability Analysis* (HAZOP) dont le nom est souvent connu du milieu mais rarement appliquée. Les principales justifications invoquées sont le manque de disponibilité des ressources (humaines et financières) et le manque de temps lors de la réalisation d'un projet. D'ailleurs, un ingénieur qui a suivi une formation sur cette méthode avouait *«qu'il est impensable d'appliquer une telle méthode dans l'industrie papetière car il y a trop de choses urgentes à régler»*. Lors d'un groupe de discussion, une seconde méthode (*What If Analysis*) a été mentionnée par un ingénieur. Il semblerait qu'elle soit réellement mise en pratique dans leur entreprise. Finalement, quelques usines utilisent des listes de contrôle (*Check List*) pour certains points de sécurité. Cependant, il s'agit souvent de points relevant de la sécurité des bâtiments industriels (sortie d'urgence, douche pour les yeux, etc.). Aussi, elles sont généralement utilisées beaucoup trop tard : l'équipement est alors souvent fabriqué et sur le point d'entrer en opération.

Par ailleurs, aucune procédure systématique de revue de sécurité n'a été recueillie. Souvent, juste avant la fabrication des équipements, une approbation de plans est effectuée. Dans ce cas, la quantité de modifications associées à des problèmes de sécurité est négligeable. Ce n'est généralement qu'après l'installation des équipements et souvent même en cours de production que les problèmes de sécurité sont mis à jour. Par contre, lors d'une entrevue au cours d'une visite, le responsable de la SST de cette usine a indiqué qu'il intervient très tôt dans le processus de conception (lors de l'élaboration des dessins) en vue d'identifier des situations qui pourraient

s'avérer dangereuses. Cette nouvelle pratique est le résultat d'une intervention qu'il a effectué au cours d'un projet et grâce à laquelle plusieurs dizaines de milliers de dollars ont été économisés. Il s'agit là d'un cas très intéressant étant donné qu'une simple réunion informelle d'à peine trente minutes a permis d'identifier des problèmes de sécurité pour lesquels les correctifs n'ont engendrés presque aucun coût supplémentaire. Cet exemple donne un aperçu de ce que pourraient être les retombées de rencontres plus formelles où des méthodes d'analyse du risque seraient systématiquement utilisées.

2.2.3 Gestion du risque

La gestion du risque est la combinaison de deux importantes activités dans l'étude de la sécurité, soit l'appréciation du risque et la réduction du risque. La figure qui suit présente un processus de gestion du risque en accord avec les définitions et les principes issus de la norme EN 292 [1991] et du projet de norme EN 1050 [1996].

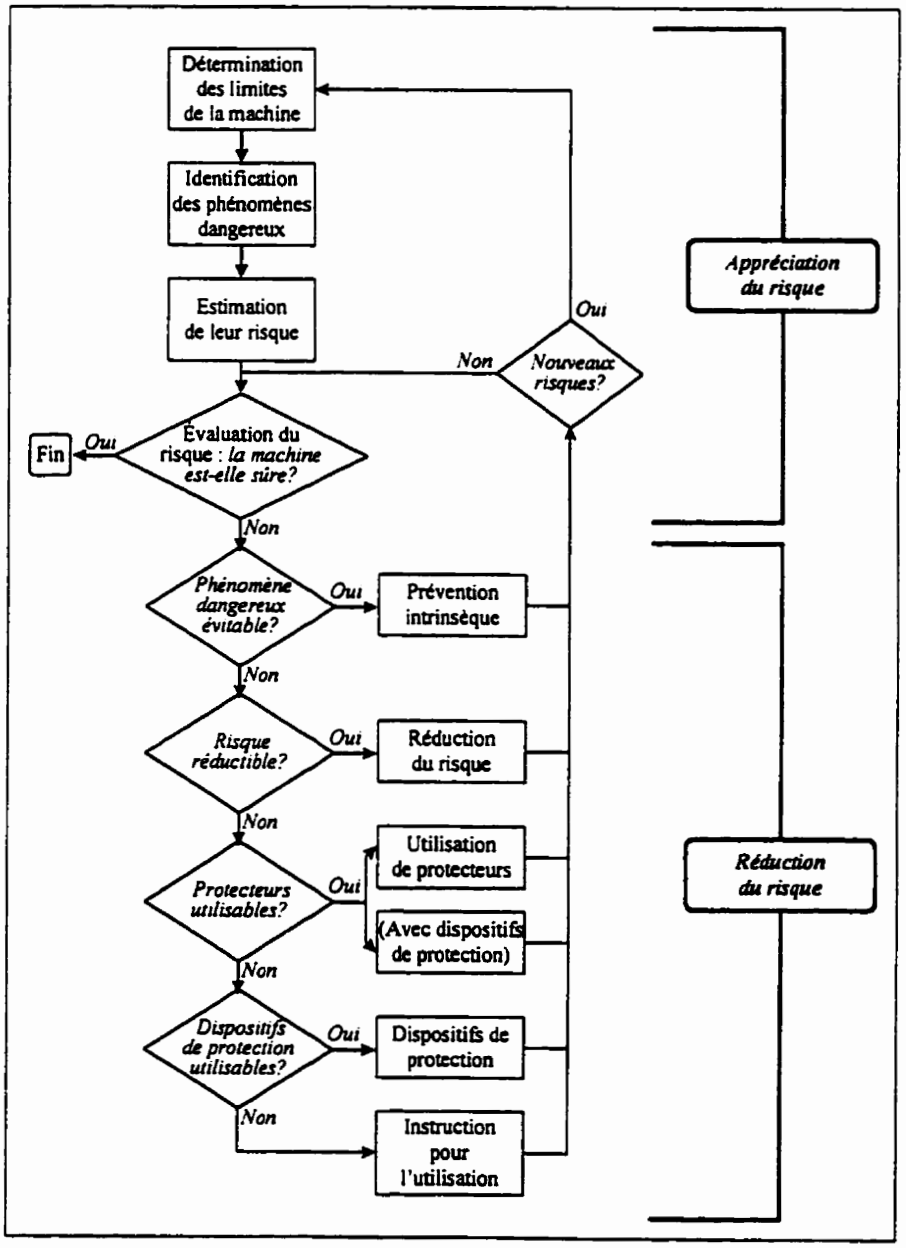

Figure 2.30 Gestion du risque [BOURBONNIÈRE, R. et coll., 1997]

Comme l'indique la figure 2.30, la première activité de la gestion du risque est l'appréciation du risque qui, à son tour, combine l'analyse du risque (identification des phénomènes dangereux et estimation de leur risque) de même que l'évaluation du risque. Ce dernier concept est un *«processus dans lequel des jugements sont portés quant à l'acceptabilité du risque, sur la base de l'analyse du risque et compte tenu des facteurs tels que les aspects sociaux économiques et environnementaux»* [ISO/CEI 51, 1997]. Cette activité d'évaluation du risque revêt donc un caractère très subjectif étant donné que la notion d'acceptabilité d'un phénomène dangereux diffère considérablement en fonction de plusieurs paramètres, tels que le niveau de scolarisation de l'individu, le niveau hiérarchique occupé au sein de l'entreprise, etc. [DIONNE-PROULX, J., 1992]. L'évaluation du risque permettra donc au concepteur de décider si la machine est sécuritaire ou non. Dans la négative, il devra alors procéder à la seconde activité de la gestion du risque, c'est-à-dire trouver les moyens techniques d'effectuer la réduction du risque. Le principe de l'échelle de priorité des solutions pour la maîtrise du risque présenté à la section 2.2.1.1 correspond essentiellement à cette activité. Un élément intéressant qui ressort de la figure 2.30 est qu'une fois que les moyens permettant de réduire le risque ont été identifiés, le concepteur doit vérifier si de nouveaux risques ont été induits par ces solutions. Si c'est effectivement le cas, il doit alors reprendre le processus d'appréciation du risque ; si non, il doit simplement évaluer si les solutions trouvées rendent effectivement la machine sécuritaire. Dans la négative, il doit alors trouver une nouvelle solution. La gestion du risque permet donc de faire un lien concret entre l'appréciation du risque, qui vise surtout une analyse et une évaluation théorique du risque, et la réduction du risque, qui permet de trouver des solutions concrètes aux problèmes de sécurité répertoriés.

Pour mieux guider le concepteur dans ce processus, diverses techniques de gestion du risque ont été créées. Par exemple, l'INRS a intégré quelques recommandations proposées par la norme EN 292 [1991] dans un schéma permettant aux ingénieurs d'optimiser leur conception en tenant compte des phénomènes dangereux présents, comme le schématise la figure qui suit [BIERCE, B. et coll., 1994].

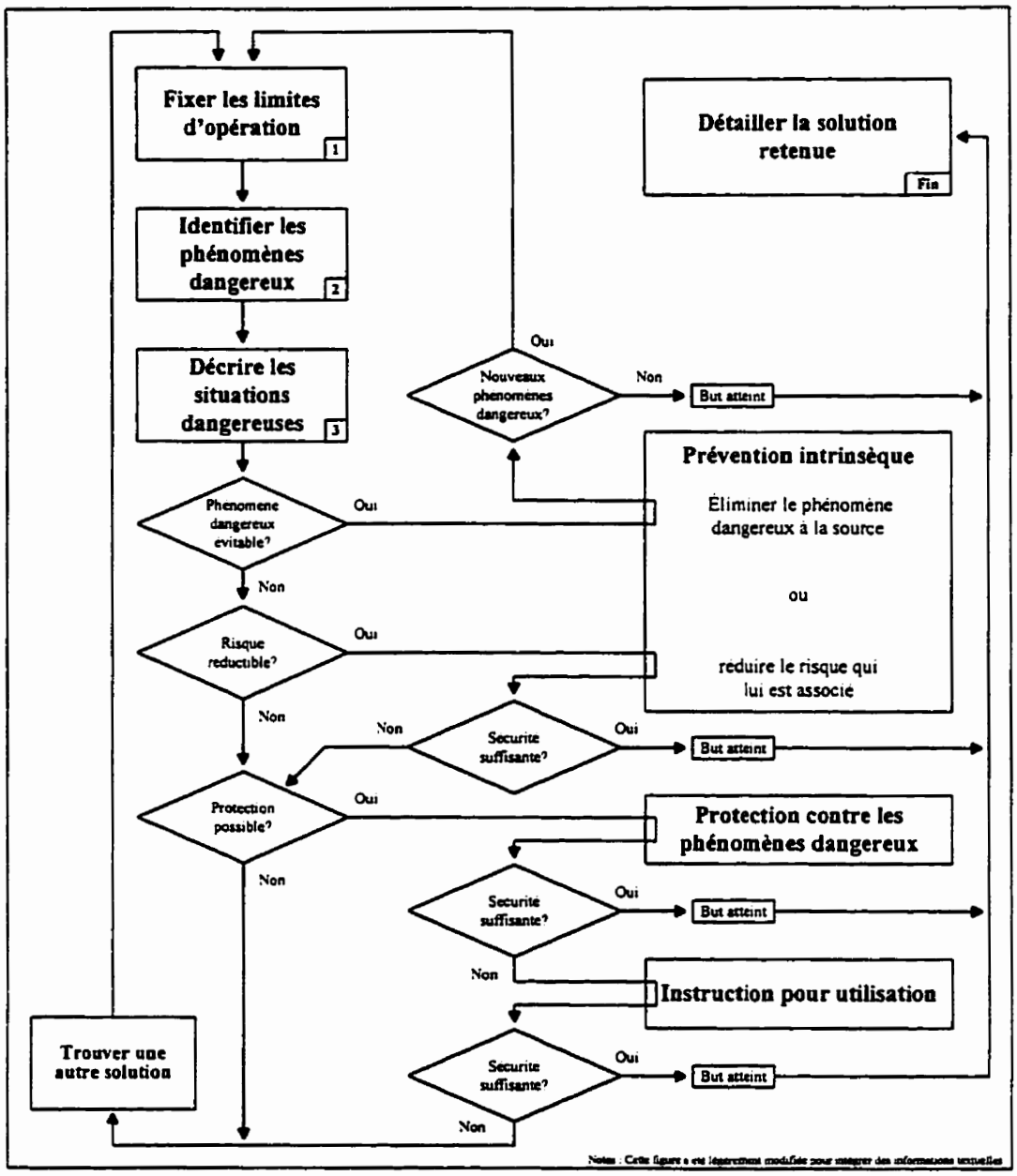

Figure 2.31 Appréciation du risque proposée par l'INRS

Dans le même ordre d'idée, la société Apave-Télémécanique a développé un outil équivalent [MERLAUD, C. et coll., 1992]. Cependant, ces deux outils ont quelques faiblesses, particulièrement au niveau de l'estimation et de l'évaluation des risques associés aux phénomènes dangereux identifiés qui y sont toutes les deux inexistantes.

Par ailleurs, F. Gauthier [1997] propose dans sa thèse une technique de gestion du risque issue notamment d'une abondante revue littéraire [BIERCE, B. et coll., 1994] [CAN/CSA Z432-94, 1994] [EN 292-1, 1991] [HARMS-RINGDHAL, L., 1987] [MERLAUD, C. et coll., 1992] [prEN 1050, 1996]. La figure qui suit est fortement inspirée de celle qu'il a proposée. Seul le vocabulaire a été légèrement modifié pour tenir compte des définitions présentées dans le lexique.

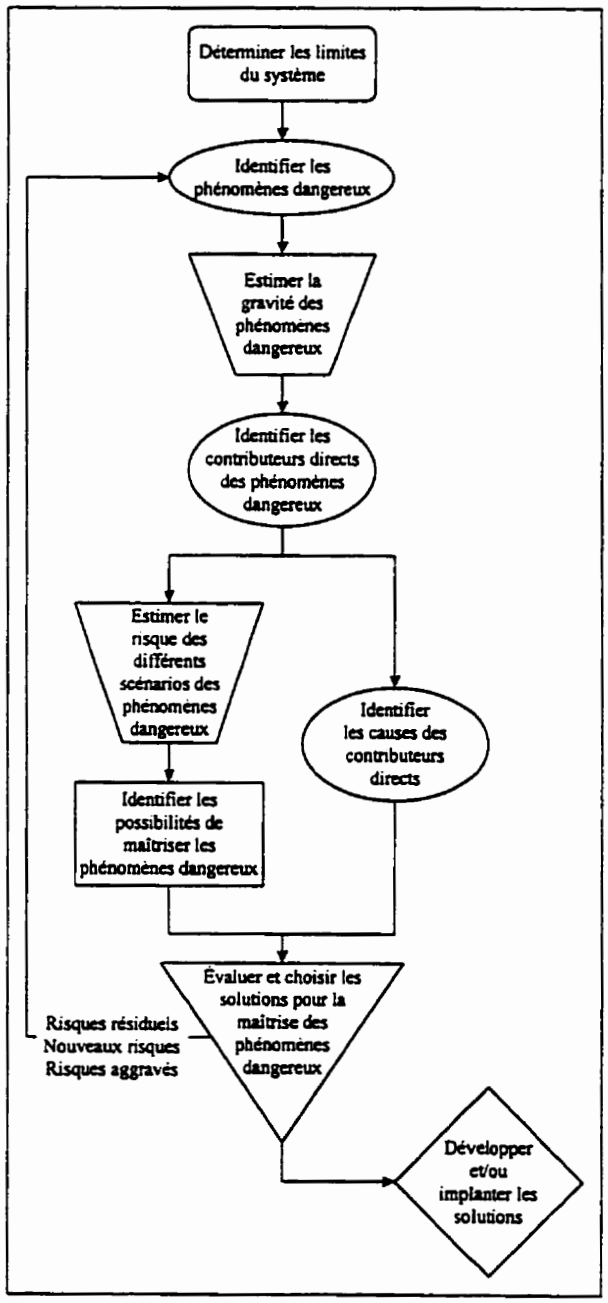

Figure 2.32 Gestion du risque inspirée par les travaux de F. Gauthier [1997]

Cette technique de gestion du risque est très simple à mettre en oeuvre et est complète puisqu'elle rencontre toutes les étapes permettant d'effectuer une appréciation du risque (identification des phénomènes dangereux, estimation et évaluation de leur risque) puis de trouver des solutions pour la réduction du risque. Les paragraphes qui suivent résument sa mise en oeuvre.

2.2.3.1 Déterminer les limites du système

Cette première étape consiste à déterminer les limites du système pour l'appréciation du risque. Ces limites concernent [GAUTHIER, F., 1997] :

- les différentes phases du cycle de vie du système ;
- les modes d'utilisation (incluant les mauvais usages) ;
- les personnes qui seront en contact avec le système ;
- les limites physiques du système ;
- les limites temporelles (durée de vie du système et de ses composants) ;
- les expositions prévisibles des personnes autres que les utilisateurs prévus.

Il s'agit là d'une étape essentielle permettant de mieux orienter les études subséquentes.

2.2.3.2 Identifier les phénomènes dangereux

Il s'agit à cette étape de répertorier le plus grand nombre possible de phénomènes dangereux. Une fois que les limites du système ont été clairement établies, l'identification des phénomènes dangereux peut être réalisée en utilisant diverses informations disponibles (données historiques, dessins de conception, etc.) ou les méthodes d'identification des phénomènes dangereux introduites à la section 2.2.2.

2.2.3.3 Estimer la gravité des conséquences des phénomènes dangereux identifiés

La sécurité absolue n'est pas un état pleinement accessible. En effet, il n'est pas techniquement et économiquement possible pour un fabricant de concevoir un système parfaitement sécuritaire [EN 292-1, 1991]. Le concepteur doit plutôt se fixer comme objectif d'atteindre le plus haut niveau de sécurité tout en tenant compte de l'état de la technique et des contraintes imposées, ces contraintes incluant également les limitations budgétaires et temporelles [MERLAUD, C. et coll.,

1992]. L'estimation des risques, tel qu'établi précédemment, permet au concepteur de définir le niveau d'importance de tous les phénomènes dangereux pouvant impliquer l'utilisation du SPA de façon à identifier ceux qui doivent être maîtrisés en premier.

Cette étape a pour but d'effectuer un premier tri parmi tous les phénomènes dangereux identifiés à l'étape précédente en évaluant la composante *gravité* associée à l'estimation des risques. Ainsi, le concepteur pourra donner une priorité absolue aux phénomènes dangereux dont les conséquences sont les plus graves (blessures irréversibles, morts, etc.). Par la suite, l'ingénieur pourra optimiser sa conception en s'attaquant aux phénomènes dangereux dont la gravité qui leur est associée est moindre, pour tenir compte des contraintes émises plus haut dans ce paragraphe.

Cette étape donne un avantage certain à la technique de gestion du risque proposée par F. Gauthier [1997] étant donné que très tôt dans le processus les efforts de conception sont canalisés vers l'élaboration des solutions permettant de maîtriser les risques les plus graves.

2.2.3.4 Identifier les contributeurs directs des phénomènes dangereux identifiés

Une fois que les phénomènes dangereux sont identifiés, les membres de l'équipe de conception doivent s'efforcer d'envisager toutes les situations qui pourraient induire les dommages redoutés [EN 292-1, 1991]. Les analyses rétrospectives et prospectives déductives sont suggérées pour cette étape [GAUTHIER, F., 1997]

2.2.3.5 Estimer le risque des différents scénarios des phénomènes dangereux identifiés

L'étape précédente a permis d'identifier plusieurs scénarios conduisant aux phénomènes dangereux identifiés et pouvant induire des dommages. Cependant, ces scénarios ne sont pas tous également probables. Certains peuvent même être invraisemblables. Toujours dans le souci de respecter les contraintes de temps et d'argent, il devient alors intéressant de terminer l'estimation du risque déjà entreprise à l'étape 3 (*estimer la gravité des conséquences des phénomènes dangereux identifiés*) en vue de poursuivre l'étude uniquement pour les scénarios les plus probables. L'utilisation des méthodes d'estimation du risque présentée à la section 2.2.2, telle que la grille proposée par le projet de norme EN 1050 [1996], est alors toute indiquée.

2.2.3.6 Identifier les causes des contributeurs directs

Comme le principe de l'échelle de priorité le stipule, il faut tenter d'éliminer à leur source les phénomènes dangereux identifiés. Cette étape a pour but d'identifier les causes originelles de chacun des contributeurs aux phénomènes dangereux identifiés en vue de les éliminer à la source. Encore une fois, les méthodes d'analyse rétrospective et prospective déductive sont recommandées [GAUTHIER, F., 1997]. Cependant, il arrive dans certains cas que l'identification des causes des contributeurs directs est essentielle pour estimer correctement les risques qui leur sont associés. C'est pour cette raison que cette étape peut se réaliser parallèlement à l'étape précédente.

2.2.3.7 Identifier les possibilités de maîtriser les phénomènes dangereux identifiés

Cette étape consiste à élaborer des solutions permettant de maîtriser les phénomènes dangereux identifiés. L'élaboration des solutions doit respecter le principe de l'échelle de priorité. Certaines approches, telle que celle proposée par l'INRS (figure 2.31), peuvent s'avérer utiles pour s'assurer du respect de ce principe fondamental.

Comme le but de cette étape est l'obtention des meilleures solutions possibles, les techniques d'aide à la créativité, comme le *brainstorming* et ses variantes, les matrices d'émergence et de convergence de Pugh, etc., sont recommandées pour aider l'ingénieur dans cette tâche [COUGER, J.D., 1995] [DOUCET, P., 1997] [LEMAY, É., 1995] [PROULX, D., 1995].

2.2.3.8 Évaluer et choisir les solutions pour la maîtrise des phénomènes dangereux

Cette dernière étape de l'appréciation du risque permet de choisir les solutions optimales pour la maîtrise des phénomènes dangereux. Ce choix doit tenir compte de plusieurs critères comme [GAUTHIER, F., 1997] :

- l'efficacité des solutions à maîtriser les phénomènes dangereux ;
- la fiabilité des solutions ;
- les nouveaux phénomènes dangereux engendrés par les solution retenues ;
- les autres phénomènes dangereux dont le risque est accru par les nouvelles solutions ;

- l'aptitude des solutions à ne pas entraver la fonctionnalité du système[14] ;
- leur coût ;
- l'influence des solutions sur le coût d'utilisation du système.

Suite à cette étape, les solutions développées sont implantées si le concepteur juge qu'elles éliminent convenablement ou réduisent suffisamment les risques associés aux phénomènes dangereux. Dans le cas contraire, les solutions développées ne sont pas implantées et sont soumises à une nouvelle analyse, comme l'indique la figure 2.32.

En conclusion, la méthode de gestion du risque proposée par F. Gauthier [1997] offre l'avantage très intéressant d'identifier, très tôt dans le processus, les phénomènes dangereux les plus graves. Ceci permet donc au concepteur d'accorder une priorité absolue au traitement de ces phénomènes dangereux et ainsi d'orienter ses efforts de conception vers les éléments les plus importants du point de vue SST. Par la suite, le concepteur consacrera ses énergies à gérer les autres phénomènes dangereux.

Finalement, le schéma proposé par l'INRS (figure 2.31) offre une représentation très claire des diverses étapes à suivre en vue de rechercher les solutions les plus sécuritaires. Le caractère simple et systématique de cette représentation est donc très intéressant.

---

[14] Comme fréquemment mentionné dans la littérature, toutes solutions de sécurité pouvant entraver significativement la fonctionnalité d'un équipement, et donc sa productivité, sont à proscrire étant donné qu'un jour ou l'autre, ces solutions pourraient être mises hors d'usage [EN 292-1, 1991] [MERLAUD, C. et coll., 1992] [ROUCHOUSE, G., 1991]. Certes, bien que l'objectif soit de maximiser la productivité, il peut arriver dans certains cas que les solutions permettant de réduire les risque entravent partiellement la productivité de l'équipement.

2.2.4 Méthodes d'élaboration et d'analyse des besoins pour la conception des SPA

L'élaboration et l'analyse des besoins permettent au concepteur de définir clairement les besoins et les contraintes par rapport au SPA à concevoir. Or, selon une étude récente menée à l'IRSST, *«[...] une cause commune d'accidents est la mauvaise adaptation aux besoins et à un usage sécuritaire des outils, des machines et des procédés industriels»* [BÉLANGER, R. et coll., 1991]. L'expression claire et nette de l'ensemble des besoins relatifs à un système de production automatisé est donc essentielle à la rencontre des objectifs de sécurité. Pour s'aider dans sa tâche, le concepteur peut faire appel à divers outils, comme l'analyse fonctionnelle, la méthode SADT, etc. Quelques outils (les plus connus) sont présentés dans cette section.

2.2.4.1 Expression des besoins et cycle de vie du SPA

Un des points clés de la réussite et du bon devenir du SPA à concevoir est l'expression et la caractérisation des objectifs et des contraintes de production qui lui sont liés. Une façon de procéder qui permet de garantir, jusqu'à un certain point, que la totalité de ces objectifs et contraintes ont été recensés consiste à les établir en étudiant chacune des étapes du cycle de vie du système [BIERCE, B. et coll., 1994] [CEI/IEC 1508-1, 1995] [MERLAUD, C. et coll., 1992] [prEN 292-1, 1991]. La figure qui suit schématise cette façon d'établir les besoins.

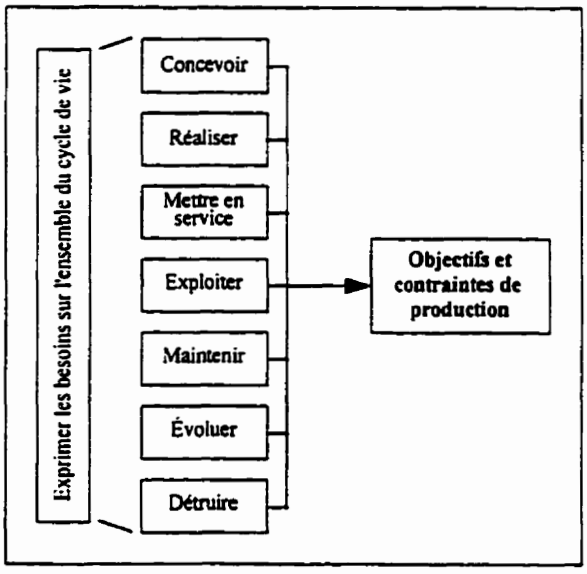

Figure 2.33 Expression des besoins sur l'ensemble du cycle de vie du SPA

Aussi, l'expression des besoins est d'autant plus complète que le nombre de personnes (et leur diversité disciplinaire) formant l'équipe de conception est élevé [BIERCE, B. et coll., 1994]. Les besoins ne devraient donc pas se limiter à ceux exprimés par les concepteurs, mais des spécialistes en SST, des opérateurs, des personnes de l'entretien, des programmeurs et des électrotechniciens devraient également exprimer leurs besoins. À ce propos, J.F. Barbet [1991] dit *«qu'on n'insistera jamais assez sur l'expérience des hommes de terrain»* pour établir et analyser les besoins liés à un SPA.

2.2.4.2 Analyse fonctionnelle et cahier des charges fonctionnel (CdCF)

L'analyse fonctionnelle est une méthode systématique d'expression des besoins qu'un produit, un système ou un processus doivent rencontrer, en termes d'usages et non de moyens, pour satisfaire un utilisateur [VALOREX, 1993]. Elle permet de faire abstraction des moyens techniques et technologiques pour bien cerner les véritables besoins de l'utilisateur. Pour y parvenir, le produit est *dématérialisé* en transposant les besoins exprimés sous forme de *fonctions*[15] [LEMAY, É., 1995].

L'analyse fonctionnelle permet essentiellement d'identifier systématiquement l'ensemble des fonctions à réaliser, d'établir un lien logique entre elles en les ordonnant et de les caractériser, c'est-à-dire de préciser de quelle manière ces fonctions devront être remplies. Par la suite, la rédaction d'un cahier des charges fonctionnel permet de circonscrire toutes ces informations dans un document de travail qui permettra notamment au concepteur de diriger la conception.

L'analyse fonctionnelle et la rédaction de son cahier des charges ne sont pas de nouveaux outils d'analyse du besoin ; déjà fortement implantée en Europe, elle est reconnue comme étant un atout considérable lors de la conception [BARBET, J.F., 1991] :

> *«Cette phase d'analyse fonctionnelle est capitale, car très efficace pour préciser les besoins à satisfaire aux différents niveaux de détail. Elle constitue le seul moyen*

[15] Par définition, les *fonctions* sont les actions d'un produit, ou de l'un de ses constituants, exprimées en termes de finalité en faisant abstraction de toute référence à des solutions [Association française pour l'analyse de la valeur, 1989].

pour fournir la preuve que les solutions retenues et les différentes précautions prises satisferont les besoins.»

L'application de l'analyse fonctionnelle pour l'identification systématique des besoins pourraient donc s'avérer un outil d'intérêt pour la présente recherche.

2.2.4.3 Graphe de commande-étape-transition (GRAFCET)

Créé en Europe en 1977, le GRAFCET a connu un immense succès depuis son arrivée dans les industries. Il s'agit d'une représentation graphique très rigoureuse du schéma logique de la PC permettant de déterminer et hiérarchiser les actions que doit transmettre la PC à la PO en vue d'accomplir les fonctions du système [BLANCHARD, M., 1979].

Comme son nom l'indique (graphe de commande-étape-transition), le GRAFCET est un graphe sur lequel les fonctions de commande sont représentées par des *étapes* et des *transitions*. Dans ce contexte, une étape correspond à *«une situation dans laquelle le comportement d'un système ou d'une partie du système par rapport à ses entrées et ses sorties est invariant»* ; les étapes sont inscrites dans un encadré. De même, une transition indique *«la possibilité d'évoluer d'une étape vers une autre»* ; elle est représentée par un trait horizontal [BLANCHARD, M., 1979].

Partant de l'expression des besoins du système, les diverses étapes et les transitions qui leurs sont associées sont mises en relief puis représentées graphiquement. Par exemple, la mise en marche d'un moteur via un interrupteur pourrait être représentée comme l'indique la figure suivante.

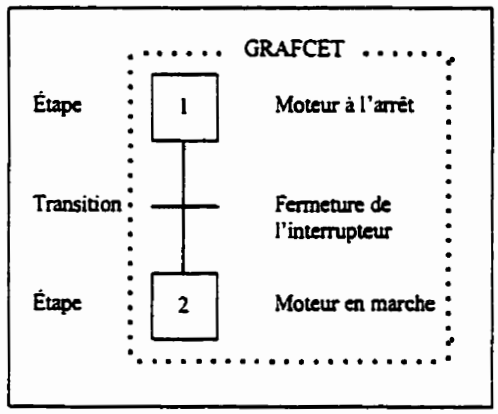

Figure 2.34 Exemple du GRAFCET pour la mise en marche d'un moteur

Cette façon de faire, très systématique, permet de s'assurer jusqu'à un certain point que l'ensemble des fonctions assurant le bon fonctionnement des commandes du SPA ont été recensées. Il existe d'ailleurs plusieurs logiciels simulant le fonctionnement du système tel que prescrit par le GRAFCET [BARBET, J.F., 1991]. Ainsi, si des fonctions ont été oubliées, la simulation pourrait les mettre en évidence. Aussi, des logiciels permettant de transposer directement le GRAFCET en langage d'API (*ladder*) existent.

Cependant, bien que cet outil soit rigoureux et très répandu à travers le monde, il a tout de même des limites. Par exemple, le GRAFCET s'applique principalement pour les procédés séquentiels. Par ailleurs, il permet une expression précise de certaines fonctions du SPA. Seul, il ne permet pas cependant l'approche systématique et globale nécessaire à une excellente conception ; il pourrait donc servir d'outil complémentaire (à l'analyse fonctionnelle par exemple) ou encore d'autres outils pourraient le compléter, comme le GEMMA présenté ci-après [ADEPA, s.d.] [CLOUTIER, G. et coll., 1988].

2.2.4.4 Guide d'étude des modes de marches et d'arrêts (GEMMA)

Tel que vu à la section 2.1.3.1, bien que la majorité des accidents surviennent en mode de marche automatique, il n'en demeure pas moins qu'un bon nombre surviennent tout de même alors que le SPA fonctionne en d'autres modes de fonctionnement [DEI-SVALDI, D. et coll., 1989] [EDWARDS, R. et coll., 1992]. Dans un autre ordre d'idée, il semble exister une confusion quant à la définition des divers modes de fonctionnement possibles : *«dans le domaine des modes de marche et d'arrêt, le vocabulaire pratiqué est imprécis et parfois même contradictoire : il conduit à des incompréhensions graves»* [ADEPA, s.d.]. Conséquemment, les spécifications fonctionnelles relatives aux divers modes de marche et d'arrêt peuvent être défaillantes ou incomplètes.

À cet effet, l'*Agence nationale pour le développement de la production automatisée* (ADEPA, France) a créé un *Guide d'étude des modes de marche et d'arrêt* (GEMMA) [ADEPA, s.d.]. Le GEMMA facilite l'analyse des besoins fonctionnels liés aux différents modes de marche et d'arrêt du SPA, ce qui permet de mieux compléter le cahier des charges. Aussi, il aide à la

conduite, à la maintenance et à l'évolution de la machine. Il définit un vocabulaire précis de tous les termes se rapportant aux modes de marche et d'arrêt. Ces modes sont classés en trois grandes familles :

- la famille F (fonctionnement) qui correspond aux procédures à appliquer pour tous les types de marches de la machine ;
- la famille A (arrêt) qui correspond à tous les types d'arrêts possibles ;
- la famille D (défaillance) qui englobe toutes les procédures en mode de défaillance.

Chacune de ces familles est à son tour divisée d'une manière telle que tous les états de marche et d'arrêt possibles soient clairement définis. Ainsi, un total de 16 modes de marche et d'arrêt sont définis et représentés dans un guide graphique simple à utiliser. L'appendice 4 présente la définition de ces 16 modes de marche et d'arrêt de même que leur représentation graphique.

L'utilisation du GEMMA est simple et très systématisée. Par exemple, pour élaborer le système de commande d'un SPA, le concepteur doit démarrer son raisonnement en supposant que l'équipement est à l'arrêt dans son état initial (case A1 du GEMMA). Si une procédure précise doit être suivie pour mettre en marche l'équipement, il doit alors se rendre à la case F2 (*marche de préparation*). Par contre, avant de s'y rendre, il devra déterminer quelle commande permettra au système de débuter sa procédure de démarrage, pour ensuite décrire cette dernière. Lorsque le concepteur a déterminé toutes ces fonctions et qu'il a déterminé de quelle manière le SPA détectera que la marche préparatoire est terminée, le GEMMA indique que la production normale (F1) peut débuter. Toujours en se référant au guide graphique, le concepteur doit parcourir les différents *chemins* prévus pour atteindre les divers états souhaités (*arrêt d'urgence*, *diagnostic des défaillances*, etc.) de même que les fonctions lui permettant d'y accéder et d'en sortir. Cette façon de faire, très systématique, permet de déterminer toutes les fonctions de commande nécessaires au bon fonctionnement du SPA.

Une fois le GEMMA complété, toutes les spécifications fonctionnelles recueillies en relation avec les divers modes de marche et d'arrêt pourraient alimenter le CdCF et/ou le GRAFCET. Sa rigueur, sa facilité de mise en oeuvre et son approche systématique font du GEMMA un outil complémentaire au GRAFCET de plus en plus employé dans le domaine de l'automatisation [ADEPA, s.d.].

2.2.4.5 Méthodes de modélisation d'un système d'information (SI)

L'ensemble des opérations que doivent assurer la plupart des SCD constitue un ensemble d'informations devant être gérées, traitées et manipulées de façon à ce que le SCD fournisse les commandes nécessaires à l'opération adéquate du SPA. Le SCD possède donc un *système d'information (SI)* [PLANCHE, R., 1988]. Toutes ces informations deviennent en fait des spécifications fonctionnelles qui doivent être éventuellement intégrées à l'analyse fonctionnelle et à son CdCF.

Or, le niveau de complexité du SI peut très rapidement devenir élevé à un tel point que des outils spécifiques doivent être mis en place en vue de faciliter la modélisation du SI. Pour ce faire, plusieurs méthodes existent, comme *les réseaux de Petri* [JAULENT, P., 1992], la *méthode Merise* [CHARTIER-KASTLER, C., 1991] [DIVINÉ, M., 1992] [GABAY, J., 1991] [GABAY, J., 1992] [JAULENT, P., 1992], la *méthode SA_RT* [HATLEY, D.J. et coll., 1990] [JAULENT, P., 1992], les *approches objet* [CASTELLANI, X., 1992] [JAULENT, P. et coll., 1993], la *méthode SADT* [JAULENT, P., 1992] [LEPLAT, J. et coll., 1990] [MARCA, D.A. et coll., 1988] [PLANCHE, R., 1988], etc.

Cependant, il est très important de comprendre que les systèmes d'information revêtent principalement un caractère logiciel. Aussi, tel que précisé auparavant, de la PC, seul le domaine du matériel est traité dans ce mémoire ; le domaine du logiciel étant beaucoup trop vaste et complexe pour être intégré dans cette recherche. De plus, tel qu'il le sera établi plus loin, ces outils de modélisation ne sont pas vraiment applicables pour la conception des SPA destinés à l'industrie québécoise des P&P.

Néanmoins, une de ces méthodes est également utilisée pour l'identification et la représentation de toutes les fonctions du système et de leurs supports : il s'agit de la méthode SADT [LEPLAT, J. et coll., 1990]. Cette méthode a été mise au point par l'américain Douglass T. Ross en 1973. Elle permet, dès les premières phases de conception, de mieux identifier les besoins fonctionnels à rencontrer, et ce au niveau de détail souhaité [MARCA, D.A. et coll., 1988]. Elle offre aussi une structuration des fonctions très intéressante. Cette représentation permet d'avoir une vue globale des fonctions du SPA à différents niveaux de détail (d'une vue globale à une vue

détaillée). Cette méthode pourrait donc aider à la structuration de l'analyse fonctionnelle [BARBET, J.F., 1991].

2.2.4.6 Étude de cas d'application de méthodes de spécification fonctionnelle des besoins

Précédemment, quelques méthodes d'analyse des besoins fonctionnels ont été introduites, dont l'analyse fonctionnelle et son CdCF, le GRAFCET, le GEMMA et les méthodes de modélisation des systèmes d'information, comme SADT. Or, le *Laboratoire universitaire de recherche en production automatisée* (LURPA) situé à Cachan (France) présente la synthèse de trois études de cas portant sur la conception d'automatismes industriels intégrant notamment ces méthodes d'analyse des besoins fonctionnels. Un des buts poursuivis par le LURPA était justement de vérifier l'utilisation possible de ces dernières dans des contextes pratiques, non théoriques. Ainsi la première étude a fait ressortir que la majorité des techniques ne sont pas concurrentes, mais plutôt complémentaires. Il est proposé par exemple de démarrer la conception par une modélisation globale, notamment à l'aide de SADT, pour ensuite procéder à un raffinement des fonctions, par exemple par le biais du GRAFCET et du GEMMA. Globalement, il est dit que [DENIS, B. et coll., 1995] :

- SADT est très efficace pour représenter des systèmes dont le niveau de complexité n'est pas très élevé ;
- le GEMMA est simple d'application et toujours intéressant à utiliser ;
- le GRAFCET, dont un grand avantage est qu'il est possible de l'informatiser pour l'analyser, demeure intéressant dans la mesure ou le système n'est pas trop complexe, sinon il devient difficile à lire.

2.2.4.7 Élaboration et analyse des besoins dans l'industrie québécoise des P&P

Lors de diverses visites effectuées dans des industries de P&P situées au Québec, il a été possible de constater que l'élaboration et l'analyse des besoins se fait de façon tout à fait informelle. L'application d'outils tels que l'analyse fonctionnelle ou la rédaction d'un CdCF ne semble jamais avoir été faite ; ils sont d'ailleurs généralement inconnus.

Une nouvelle tendance a cependant pu être observée dans plusieurs entreprises. Il s'agit de l'implication, lors de la définition des besoins, des diverses personnes appelées à intervenir

auprès du SPA au cours de son cycle de vie. Par exemple, les opérateurs, les électriciens, le personnel d'entretien et parfois les représentants SST émettent de plus en plus de besoins fonctionnels spécifiques. Ce nouveau phénomène est fort encourageant compte tenu du fait que les SPA conçus ou achetés sont mieux adaptés aux tâches de chacun. Cependant, il semble exister de sérieux problèmes de communication entre tous ces intervenants. Par exemple, les ingénieurs consultent rarement les opérateurs ; ils consultent plutôt leur superviseur. Ainsi, les besoins recueillis par les ingénieurs ont été inévitablement interprétés, ce qui est un facteur d'erreur. Deux raisons sont alors souvent invoquées. La première est rattachée aux contraintes de temps vécues lors d'un projet de conception. La seconde est rattachée à la taille de l'entreprise. Il est en effet plus difficile de consulter une centaine d'opérateurs qu'une dizaine. Il ressort donc qu'il existe des lacunes pour la consultation systématique des opérateurs et du personnel d'entretien. Par ailleurs, lorsque les ingénieurs consultent tout de même les opérateurs, cette consultation se résume souvent à l'approbation de plan. Or, rares sont les opérateurs qui savent lire des plans aussi complexes ; d'ailleurs, ils n'éprouvent généralement que peu d'intérêt à le faire. Ainsi, comme le soulignait un ingénieur lors d'un groupe de discussion, le désir d'améliorer la communication à tous les niveaux est là, mais la façon de s'y prendre leur est inconnue.

Outre les problèmes de communication nuisant à une bonne cueillette des besoins, les contraintes de productivité font en sorte que le temps pouvant être accordé par les concepteurs à cette étape est petit, si bien que l'analyse des besoins est très souvent incomplète : *«Il faut produire, on n'a pas le temps de s'attarder là-dessus, malgré que ce soit très important»*.

Finalement, pour ce qui est de l'analyse fonctionnelle, du CdCF, de SADT et du GEMMA, aucun concepteur rencontré au cours des visites n'avait entendu parler de ces outils. Seul le GRAFCET est un peu connu et les concepteurs, de même que les programmeurs, ont indiqué qu'il s'agissait d'un outil très intéressant mais peu pertinent dans le domaine des P&P compte tenu du caractère peu séquentiel des procédés utilisés pour la fabrication du papier.

2.2.5 Principes techniques de réduction des risques

Les principes techniques de réduction des risques sont en fait des solutions actuellement connues et appliquées qui permettent d'accroître le niveau de sécurité atteint par les SPA comportant des SÉP. Ces principes peuvent également être vus comme faisant partie des règles de l'art en matière de conception sécuritaire. Cependant, il est important que le lecteur réalise que ces principes techniques sont liées à la technologie et que cette dernière évolue à une vitesse considérable, surtout dans le domaine de l'électronique. Il ne serait donc guère pertinent de les présenter à un fin niveau de détail.

Le but premier de ces principes est d'abaisser le niveau de risque associé aux phénomènes dangereux (lorsque leur élimination à la source est impossible) en vue de le ramener à un niveau plus acceptable. La section 2.1.3.2 a fait ressortir diverses craintes qu'ont certains concepteurs face à l'application des technologies programmables pour les fonctions de sécurité commandées par le SPA : cette section présente donc des solutions permettant au concepteur de maîtriser les phénomènes dangereux qui justifient leurs craintes.

2.2.5.1 Réduction des phénomènes dangereux associés aux défauts internes

Comme la figure 2.16 l'illustre, les défauts internes ne représentent qu'environ 5% des défaillances d'un système automatisé. De ces quelques défaillances, 9 sur 10 sont attribuables aux modules E/S, l'autre dixième se répartissant de façon approximativement égale entre l'UCT, la carte de mémoire, le bus de communication et la carte d'alimentation [DEI-SVALDI, D. et coll., 1984].

Il semble donc que les modules d'entrées et de sorties subissent un bon nombre de défaillances. À cet effet, l'IRSST recommande l'utilisation d'un principe, appelé *chien de garde externe*, selon lequel une minuterie, extérieure à l'API, doit être remise à zéro après un laps de temps pouvant correspondre à 2 ou 3 balayages de programme, à défaut de quoi un contact s'ouvre et coupe l'énergie du système. Elle recommande également la surveillance des défauts des sorties. Dans ce cas, l'information des sorties est bouclée aux entrées de façon à les soumettre à un nouveau balayage [PAQUES, J.-J., 1991]. Dans son article, Hubby recommande l'utilisation d'un second

UCT destiné uniquement à la surveillance des entrées et des sorties, étant donné que la majorité des défaillances s'y produisent [HUBBY, R.N. et coll., 1991].

Pour ce qui est des principes permettant de réduire les défaillances de l'UCT, il en existe quelques-uns. Par exemple, une technique fréquemment appliquée est la fonction *chien de garde interne* (*Watch Dog*) où un dispositif servant à s'assurer que l'automate procède à son balayage dans un laps de temps acceptable est intégré [COX, R.A., 1995]. Certains constructeurs intègrent même systématiquement cette fonction à leurs API [HUBBY, R.N. et coll., 1991]. Cependant, en raison de diverses perturbations, la fonction chien de garde interne peut ne pas s'activer. En conséquence, il n'est pas recommandé de faire confiance uniquement à cette fonction pour assurer la sécurité de l'API. Elle devrait être doublée par d'autres techniques [DEI-SVALDI, D. et coll., 1984]. Un autre principe est celui du test du coprocesseur (*coprocessor test*) où un argument est envoyé à l'UCT et sa réponse est comparée à celle prévue et placée en mémoire. D'autres techniques s'apparentent à celle-ci. C'est le cas notamment de la division par zéro, du dépassement de registre (*overflow*), de la vérification de parité (*check parity*), du vérificateur de somme (*checksum*), etc. [FISHER, T.G., 1990] [HUBBY, R.N. et coll., 1991] [PAQUES, J.-J., 1991].

Pour contrer les défaillances de la carte de mémoire, les deux derniers principes (la vérification de parité et le vérificateur de somme) peuvent être appliqués. Un autre principe permettant de diminuer les risques de modifications indésirables du programme placé en mémoire est l'utilisation de mémoire permanente (PROM, EPROM, UVPROM, etc.) pour la programmation : *«The use of PROM or EPROM memory for program storage offers the only effective protection against unauthorized tampering.»* [FISHER, T.G., 1990].

Quant à elles, les défaillances du bus de communication sont le résultat de perturbations dues à l'environnement agressif d'utilisation des API. La prise en compte de ce fait lors de la conception du SPA est donc de mise. Néanmoins, il existe quelques méthodes permettant de vérifier l'efficacité des communications. Ces méthodes sont partiellement décrites dans l'article de l'équipe de R.N. Hubby [1991], mais leur description dépasse le cadre de cette recherche étant donné leur caractère informatique.

Finalement, les défaillances induites par la carte d'alimentation électrique peuvent être contrées par un principe d'alimentation électrique résistant aux pannes et aux fluctuations (connu en anglais sous l'appellation *uninterrutible power supply, UPS*). Son but est alors d'empêcher la mise hors énergie sporadique du SÉP afin que les données ainsi que le programme pilote (chargé en mémoire vive, RAM) ne se fassent pas interrompre.

2.2.5.2 Diminution des phénomènes dangereux associés aux défauts externes

Cette catégorie englobe tous les risques de défaillances associées aux composants extérieurs au SÉP, c'est-à-dire les divers capteurs, actionneurs, etc. La défaillance de ces composants, comme établi précédemment, représente de 90 à 95 % de l'ensemble des défaillances que peut avoir une machine automatisée [MERLAUD, C. et coll., 1992] [DEI-SVALDI, D. et coll., 1984]. L'utilisation d'un relais de sécurité pouvant couper l'énergie sur tous les éléments de sortie (pré-actionneurs, etc.) peut s'avérer une solution intéressante [PAQUES, J.-J., 1991]. Ces modes de défaillance sont bien connus et plusieurs solutions technologiques existent pour les contrer. Néanmoins, il arrive qu'il soit impossible ou trop coûteux d'élaborer les solutions permettant d'éliminer ces risques. Alors à défaut de parvenir à les éliminer, il faut se protéger contre ces risques potentiels.

C'est le rôle qu'accomplissent principalement les dispositifs de protection. Ces derniers ont pour principal objectif de protéger les utilisateurs de machines et installations contre les dangers qu'elles génèrent. Le dispositif doit permettre l'exécution aisée de toutes les fonctions en interaction avec l'humain [EN 292-1, 1991] ; il doit donc être bien conçu. Les protecteurs peuvent être fixes ou mobiles, matériels ou immatériels. Des mesures clairement définies quant à leur conception et leur installation sont disponibles dans la littérature [AISS, 1989] [BOURBONNIÈRE, R. et coll., 1997] [GILLOT, J., 1996] [INRS, 1989a].

Finalement, comme les opérations de réglage et de maintenance sont responsables d'une grande part des accidents, les procédures de consignation assurant que la mise en marche de l'automatisme ne peut se faire que par une action volontaire s'avèrent une bonne solution. Des techniques de mise en oeuvre d'une procédure de consignation et de déconsignation efficace sont

détaillées dans un article publié par l'*Association sectorielle paritaire pour la santé et sécurité du travail - Division construction* [ASP, 1991] ainsi que dans une brochure de l'INRS [1996].

2.2.5.3 Principe de panne ou comportement orienté

Le principe de base de la conception de système sûr est d'orienter son comportement en cas de défaillance [MERLAUD, C. et coll., 1992]. Ainsi, ce principe stipule que si le système automatisé, pour une raison quelconque, vient qu'à tomber en panne, son comportement sera prévisible, sécuritaire et n'introduira pas de nouveaux dangers pour l'utilisateur [McGILL, W.F. et coll., 1987]. À plus fortes raisons, les systèmes d'arrêt d'urgence doivent appliquer ce principe, étant donné que la fonction première d'un tel système est d'interrompre le procédé en le ramenant à un état sécuritaire [FISHER, T.G., 1990].

Ainsi, tout système de commande dit de sécurité devrait donc défaillir de façon sécuritaire : *«In short, a system is not safe unless it is fail safe.»* [WILSON, D.K., 1988].

2.2.5.4 Principe de tolérance aux fautes

Ce principe répond au besoin de prévoir des moyens de reprendre le contrôle d'un système après que celui-ci ait subi une entrée fautive ou un état de fonctionnement inhabituel sans devoir interrompre la production [KLETZ, T.A., 1991]. Le système doit avoir recours à la redondance définie, selon la norme CEI/IEC 351 [1994], comme étant *«l'existence, dans une entité, de plus d'un moyen pour exécuter une fonction requise»*. Ainsi, ce principe réside dans la multiplication de certains composants, fonctions, sous-systèmes, voire même du système entier dans le but d'assurer une mission donnée en présence de défaillances [MERLAUD, C. et coll., 1992].

Par ailleurs, l'IRSST recommande l'emploi de la redondance lorsque les conséquences économiques, environnementales ou humaines d'une défaillance le justifient [PAQUES, J.-J., 1991]. Les avantages à utiliser des systèmes tolérants aux fautes sont que [FISHER, T.G., 1990] :

- les opérations de production peuvent continuer même si un des équipements de contrôle est hors d'usage ;

- la défaillance d'un module n'affecte d'aucune façon les autres ;
- l'entretien et les réparations peuvent être effectuées sans pour autant interrompre le procédé ;
- chacun des systèmes peut servir à suivre le fonctionnement (et surtout les dysfonctionnement!) des autres systèmes ;
- un système indépendant peut également servir à suivre le fonctionnement des autres.

Par ailleurs, des nouveaux produits apparaissent actuellement sur le marché. Par exemple, un API possédant une architecture triredondante, tant au niveau matériel que logiciel, a relancé le débat en ce qui a trait à l'implication des technologies programmables pour les fonctions de sécurité [INRS, 1997]. Cet API a été conçu par trois constructeurs différents qui ont appliqués chacun leur technique et leur technologie. Les résultats sont très intéressants, si bien que l'Allemagne a autorisé la gestion des fonctions de sécurité par cet API. Ainsi, les SÉP évoluent sans cesse et de nouveaux produits, toujours plus performants, sont mis à la disposition du concepteur. Cependant, il est essentiel que l'ingénieur comprenne les enjeux qu'impliquent la conception d'un SPA du point de vue SST et qu'il réalise pleinement que la technologie la plus avancée ne palliera jamais une piètre conception.

2.2.5.5 Principes techniques de réduction des risques dans l'industrie québécoise des P&P

Lors des visites effectuées dans les papetières collaborant au projet de recherche, il a pu être observé que des principes de redondances étaient appliqués. La technique la plus souvent rencontrée était la *redondance matérielle sélective de type passif*, communément appelée *up-back-up* [BOURBONNIÈRE, R., 1997]. La figure qui suit présente cette architecture.

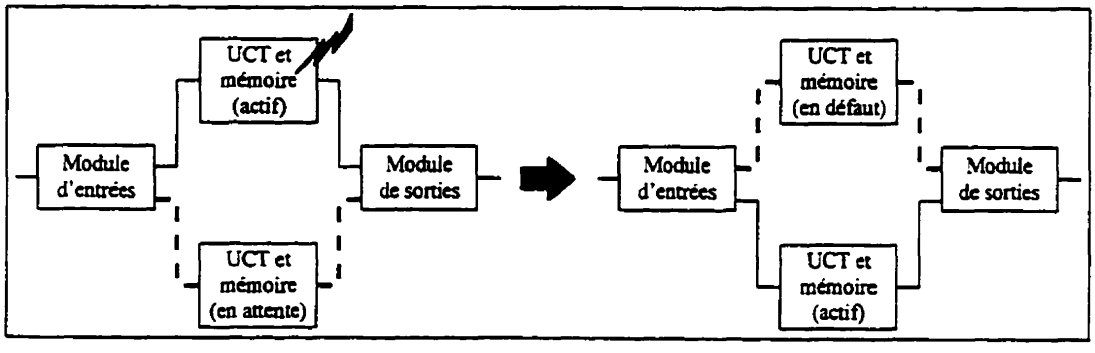

Figure 2.35 Redondance la plus commune dans l'industrie québécoise des P&P

Comme le schématise la figure 2.35, cette technique consiste à doubler l'UCT et la mémoire d'un équipement (SCD ou API) de telle sorte que si l'UCT actif détecte une faute provoquant une défaillance, le second UCT devient actif et assure la continuité des opérations[16]. Cette architecture ne permet pas cependant d'assurer la continuité des opérations si les modules E/S venaient à faire défaut ou si une erreur de programmation est commise étant donné que le même programme est chargé par l'API. Par ailleurs, un cas ou les fonctions logiques d'un SCD étaient triplées a également été recensé. Il s'agissait d'une application dont les risques étaient passablement élevés.

En ce qui concerne les principes permettant de diminuer les risques de mauvaises modifications du programme des SÉP, deux constats sont faits. Le premier concerne les SCD. Dans ce cas, l'utilisation de mots de passe permet l'accès au programme à différents personnels, le plus souvent des personnels cadres, et ce à différents niveaux de gestion du SCD. Cependant, aucune procédure formelle permettant de mettre à jour les programmes n'a été répertoriée ; le suivi des programmes est donc effectué par professionnalisme. Le second constat, plus grave, concerne les API. L'évolution constante des SPA (ajustement, modernisation, etc.) fait en sorte qu'il serait nuisible pour leur productivité d'empêcher l'accès au programmes des API par des techniques connues, comme l'utilisation des mémoires permanentes (EPROM, UVPROM, etc.). Le seul moyen de protection rencontré est la nécessité d'utiliser une clé (mécanique ou électronique) pour accéder au programme. Cependant, à l'exception du cas relaté à la section 2.1.3.9, le nombre d'intervenants y ayant accès est tel que cette sécurité n'a plus son sens ; d'ailleurs, plusieurs boîtiers d'API n'étaient pas verrouillés ou la clé se trouvait dans la serrure. Ainsi, n'importe qui ayant un minimum de connaissance des API peut modifier son programme. Tout comme c'est le cas pour les SCD, le suivi du programme est effectué par professionnalisme ; aucune procédure formelle n'est réellement appliquée.

[16] Ces défauts sont détectés par les techniques courantes, comme les fonctions internes *chien de garde*, *parity check*, *checksum*, etc.

2.2.6 Approches pour la conception de SPA sécuritaires

Il est reconnu depuis fort longtemps que le meilleur temps pour adapter la sécurité aux machines est lors de sa conception comme en témoigne cette citation tirée d'un éditorial datant de 1910 : *«We reiterate that the time to safeguard machinery is when it is on the drawing board ; and designers should awaken fully to a sense of their responsibility in this respect.»* [ROBERTS, V.L., 1984]. La philosophie est aujourd'hui encore la même : *«C'est dès la conception qu'il est nécessaire de prévoir les moyens nécessaires pour assurer la sécurité.»* [KNEPPERT, M., 1995]. Toutes les solutions de sécurité trouvées après conception, lorsqu'elles existent, sont souvent inefficaces, coûteuses et difficiles à mettre en oeuvre. De plus, le niveau de sécurité atteint n'est jamais aussi élevé qu'il aurait pu l'être en intégrant l'aspect SST dès la conception [IRSST, 1993]. Bien qu'il existe quelques approches ou méthodologies permettant d'intégrer l'aspect SST tôt dans le processus de conception d'une machine automatisée, il semble qu'elles soient ou bien mal connues ou bien inadéquates [GILLOT, J. 1994] :

> *«L'absence d'une démarche [de conception] suffisamment réfléchie fait que l'analyse des situations de travail prévisibles n'est qu'ébauchée. Cette analyse insuffisante conduit à élaborer des principes de prévention et des moyens de protection non adaptés à la réalité de l'exploitation projetée.»*

Quelques unes des méthodologies ou des principes de conception répertoriés dans le cadre de cette recherche sont présentés dans cette section.

2.2.6.1 Conscientisation faite par J.F. Barbet

Dans son article, J.F. Barbet ne propose pas une approche spécifique de conception ; il rappelle plutôt les étapes importantes que tout concepteur doit rencontrer. Cependant, la quasi totalité de son article traite de l'importance capitale qu'il faut accorder aux premières phases de conception, celles où la description fonctionnelle du système est effectuée. La démarche qu'il propose est résumée dans le tableau suivant [BARBET, J.F., 1991]. Il est important de noter que l'aspect séquentiel présenté dans le tableau ne reflète pas la démarche proposée ; cette dernière est en fait constituée d'une suite d'itérations.

TABLEAU 2.4 APPROCHE SUGGÉRÉE PAR J.F. BARBET [1991]

1- Étude préalable

1.1- Spécifications fonctionnelles préliminaires

Objectif : préciser les principales fonctions du système et leurs enchaînements.

Outils proposés et buts de leur application :

L'auteur recommande que l'analyse fonctionnelle soit utilisée dans le but d'identifier le plus grands nombre possible de besoins fonctionnels. Aussi, l'utilisation de certaines méthodes de modélisation des systèmes d'information, dont SADT, est recommandée en vue de mieux structurer l'ensemble des besoins fonctionnels. Finalement, une étude de fiabilité préliminaire, au niveau fonctionnel, est fortement recommandée dans le but d'établir, en plus des critères de performance, divers critères de fiabilité. Cependant, le candidat pense qu'une étude de fiabilité à ce stade-ci de la conception risquerait d'être difficile à mettre en oeuvre étant donné que le SPA est encore très peu élaboré.

1.2- Analyse de la mission

Objectif : préciser toutes les conditions dans lesquelles le système en conception sera utilisé.

Outils proposés et buts de leur application :

Bien que l'auteur ne recommande aucun outil spécifique, le candidat avance qu'il pourrait être intéressant d'intégrer le GEMMA étant donné que ce dernier permet justement de penser à tous les modes de marche et d'arrêt possibles (arrêt d'urgence, fonctionnement en mode dégradé, etc.).

1.3- Analyse préliminaire des risques

Objectif : préciser les événements redoutés susceptibles d'être générés par le système pour chaque phase du profil de la mission.

Outils proposés et buts de leur application :

L'auteur de l'article encourage les concepteurs à utiliser des listes de contrôle (*checklist*), car elles sont simple à mettre en oeuvre et efficaces. Par ailleurs, il insiste sur l'importance de mettre à profit *«l'expérience des hommes de terrain»*.

2- Spécifications du système

2.1- Spécifications fonctionnelles détaillées et allocations d'exigences

Objectif : Compléter la spécification fonctionnelle en respectant les exigences précisées par les besoins.

Outils proposés et buts de leur application :

Tant et aussi longtemps que le niveau de détail n'est pas tel que des méthodes spécifiques aux technologies envisagées soient nécessaires, l'auteur recommande l'utilisation d'outil classique, comme l'analyse fonctionnelle. Ainsi, la spécification fonctionnelle préliminaire pourra être complétée grâce à une analyse fonctionnelle plus approfondie.

2.2- Évaluation des spécifications fonctionnelles et analyse de faisabilité

Objectif : évaluer la faisabilité des spécifications fonctionnelles.

Outils proposés et buts de leur application :

Pour évaluer la faisabilité des spécifications fonctionnelles, plusieurs méthodes sont recommandées, dont l'AMDEC, les graphes d'état (GRAFCET, etc.). Aussi, pour les spécifications plus critiques, il est recommandé d'utiliser des techniques de simulation en vue de s'assurer de leur faisabilité.

TABLEAU 2.4 APPROCHE SUGGÉRÉE PAR J.F. BARBET (SUITE)

3- Spécifications du logiciel
Les activités de cette phase permettent d'obtenir les mêmes résultats que la phase précédente mais cette fois pour l'aspect logiciel du système. Comme mentionné auparavant, les méthodes de conception des logiciels ne font pas partie de ce mémoire et c'est pourquoi le candidat ne s'attardera pas sur les multiples outils et méthodes présentées dans l'article.
4- Conception et réalisation
Objectif : développer le système tant sur l'aspect matériel que logiciel en vue de le construire. *Outils proposés et buts de leur application :* Pour cette étape, l'auteur suggère d'utiliser des méthodes propres au matériel et au logiciel. Dans le cas du matériel, si une conception intrinsèquement sûre est retenue, l'utilisation d'outils d'aide à la conception, comme les revues de projet, les AMDEC, les simulations ou même l'expérimentation est conseillée. Si la conception résulte plutôt en une configuration tolérante aux fautes, les principes techniques de réduction des risques usuels sont recommandés. Les mêmes consignes s'appliquent dans la conception et la réalisation du logiciel.
5- Validation
Objectif : valider que le système développé répond à toutes les allocations d'exigences. *Outils proposés et buts de leur application :* En vue de s'assurer de la cohérence entre les précautions prises pour les logiciels et celles prises pour les configurations matérielles, et ce aux différents niveaux de détail et au niveau global, l'auteur recommande que des validations physiques, statistiques ou fonctionnelles, des simulations ou des essais réels soient effectués.

Cette approche donne les grandes lignes à suivre lors de la conception d'un SPA. Un avantage certain qui en ressort est l'intégration de plusieurs outils (AMDEC, liste de contrôle, analyse fonctionnelle, CdCF, GRAFCET, etc.) tout au long de l'évolution de la conception. D'autre part, l'auteur accorde une importance capitale à l'étape d'analyse des besoins, puisque l'adaptation du SPA aux besoins réels est à la base d'une bonne conception. À cet effet, il recommande fortement l'intégration de toutes les personnes en relation avec le SPA en vue de former une équipe pluridisciplinaire. Cependant, aux yeux du candidat, cette méthodologie n'est pas assez détaillée ni assez systématique pour s'assurer de l'intégration rigoureuse des outils mentionnés. En effet, ces derniers ne sont pas formellement intégrés à la méthodologie proposée ; ils sont plutôt suggérés, laissant ainsi plus de liberté aux concepteurs.

2.2.6.2 Approche proposée par Apave-Télémécanique

L'approche proposée dans le livre *La sûreté des machines et installations automatisées* [MERLAUD, C. et coll., 1992] est entièrement basée sur une nouvelle approche dite à *points de*

vue successifs. Cette dernière est le fruit de la combinaison de deux approches plus traditionnelles : l'approche *productique* et l'approche *cycle de vie*.

L'approche *productique* a pour principal objectif d'assurer la compétitivité du produit ainsi que la meilleure production possible : c'est la force majeure de cette approche. Une fois que les besoins reliés à ces deux dimensions sont clairement identifiés, le procédé et les moyens de fabrication sont établis. La seconde approche, basée sur le *cycle de vie* d'un produit quelconque, a l'avantage de tenir compte des besoins rattachés à la réalisation, à la mise en service, à l'exploitation, à la maintenance et parfois même à l'évolution et à la destruction éventuelle du produit.

Ainsi, la combinaison de ces deux approches (*productique* et *cycle de vie*) a permis de créer une nouvelle approche qui tient compte à la fois de la compétitivité du produit (et de sa production) et des besoins liés à certaines étapes de la vie du produit, dont la mise en service, l'exploitation et l'entretien. Il s'agit de l'approche par *points de vue successifs*. La figure qui suit résume ces quelques lignes.

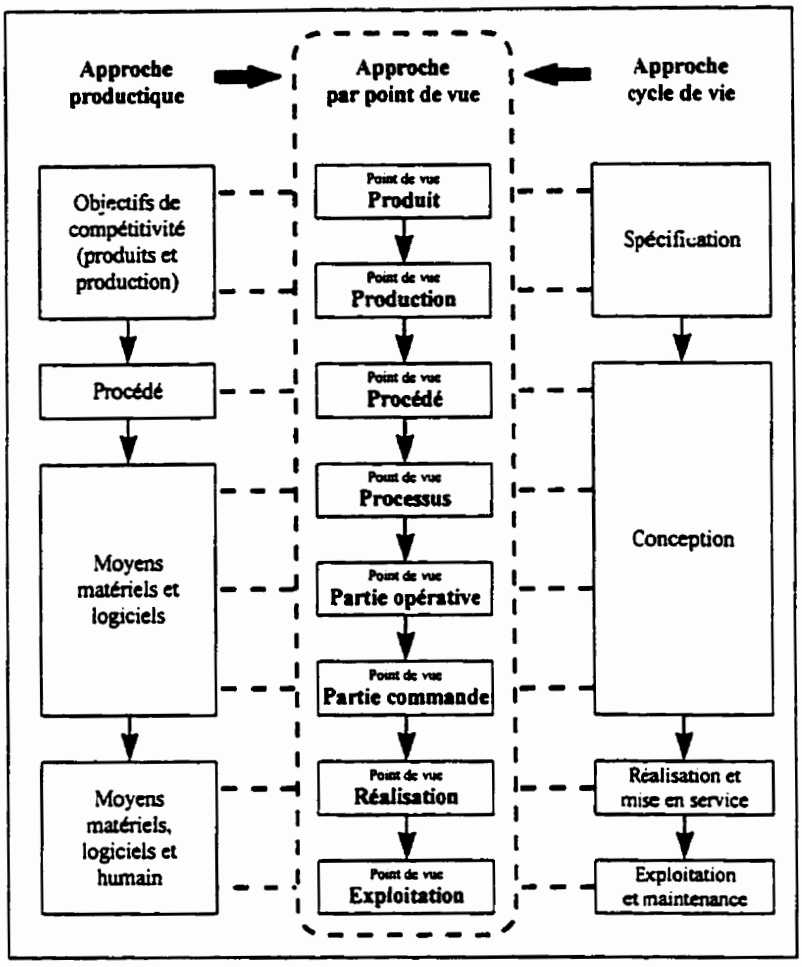

Figure 2.36 Approche par *points de vue successifs* et approches *productique* et *cycle de vie*

Par exemple, dans le cas où le SPA à concevoir serait une machine à papier, selon cette approche, au point de vue :

- *produit* pourrait être associé le type de papier à produire ;
- *production* pourrait être associée la quantité quotidienne de papier à fabriquer ;
- *procédé* pourraient être associées les étapes de fabrication du papier, comme son séchage ;
- *processus* pourrait être associés les moyens d'effectuer le séchage du papier, comme l'utilisation de rouleaux chauffés ;
- *partie opérative* pourrait être associée la façon d'entraîner les rouleaux sécheurs ;
- *partie commande* pourrait être associée la façon de régler la température des rouleaux ;
- *réalisation et mise en service* pourrait être associée la façon d'insérer les rouleaux de la machine lors de sa réalisation ;

- *exploitation et maintenance* pourraient être associés les moyens d'éviter d'entrer en contact avec les rouleaux et/ou la façon de les réparer ou de les remplacer.

Ainsi, en considérant successivement tous les points de vue, l'approche garantie en quelque sorte que tous les aspects en relation avec le SPA seront pris en compte.

La démarche proposée par l'Apave-Télémécanique débute en tout premier lieu par la recherche de tous les besoins associés à chacun des points de vue. Ces besoins sont par la suite soumis aux techniques d'analyse fonctionnelle pour être exprimés sous forme de fonctions et être finalement inclus dans le CdCF global. La figure qui suit illustre cette première étape.

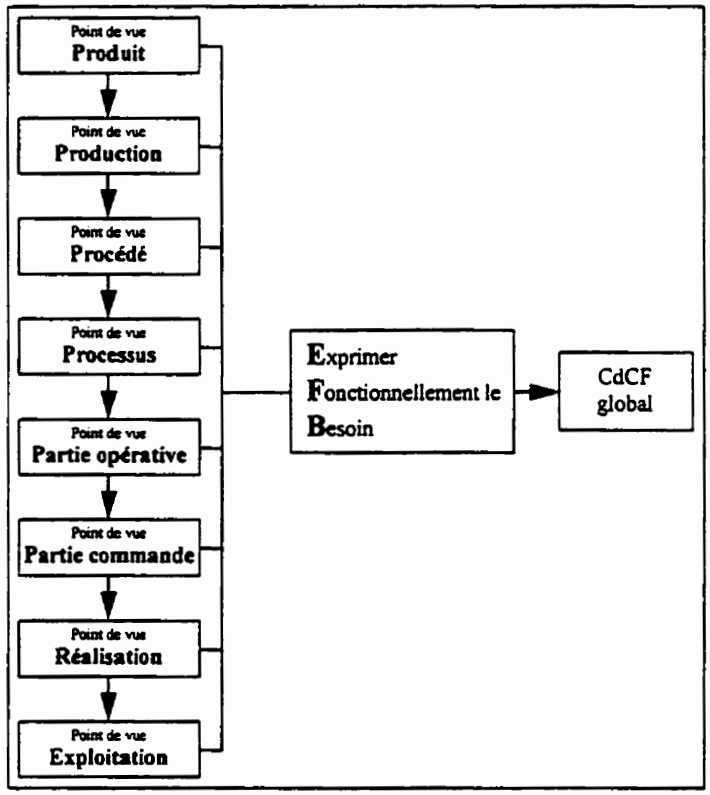

Figure 2.37 Expression fonctionnelle du besoin

Ce CdCF est préliminaire, car tout au long du processus, des contraintes seront identifiées ou mises en évidence, ce qui pourra créer de nouvelles fonctions. Une fois l'expression fonctionnelle des besoins terminée, la démarche propose de traiter chacune des fonctions, et ce pour chacun des points de vue, selon ces cinq phases :

1. caractériser le CdCF associé au point de vue en cours ;

2. faire l'analyse du risque pour chacune des fonctions identifiées et sélectionner celles pour lesquelles une étude de sécurité est nécessaire ;
3. rechercher des solutions satisfaisantes pour les phénomènes dangereux et les contraintes identifiés à chacune des fonctions ;
4. analyser les solutions proposées jusqu'à l'obtention d'une solution optimale pour chacune des fonctions ;
5. valider l'ensemble des solutions par une revue de projet du point de vue en cours.

Ces cinq phases sont schématisées dans la figure qui suit.

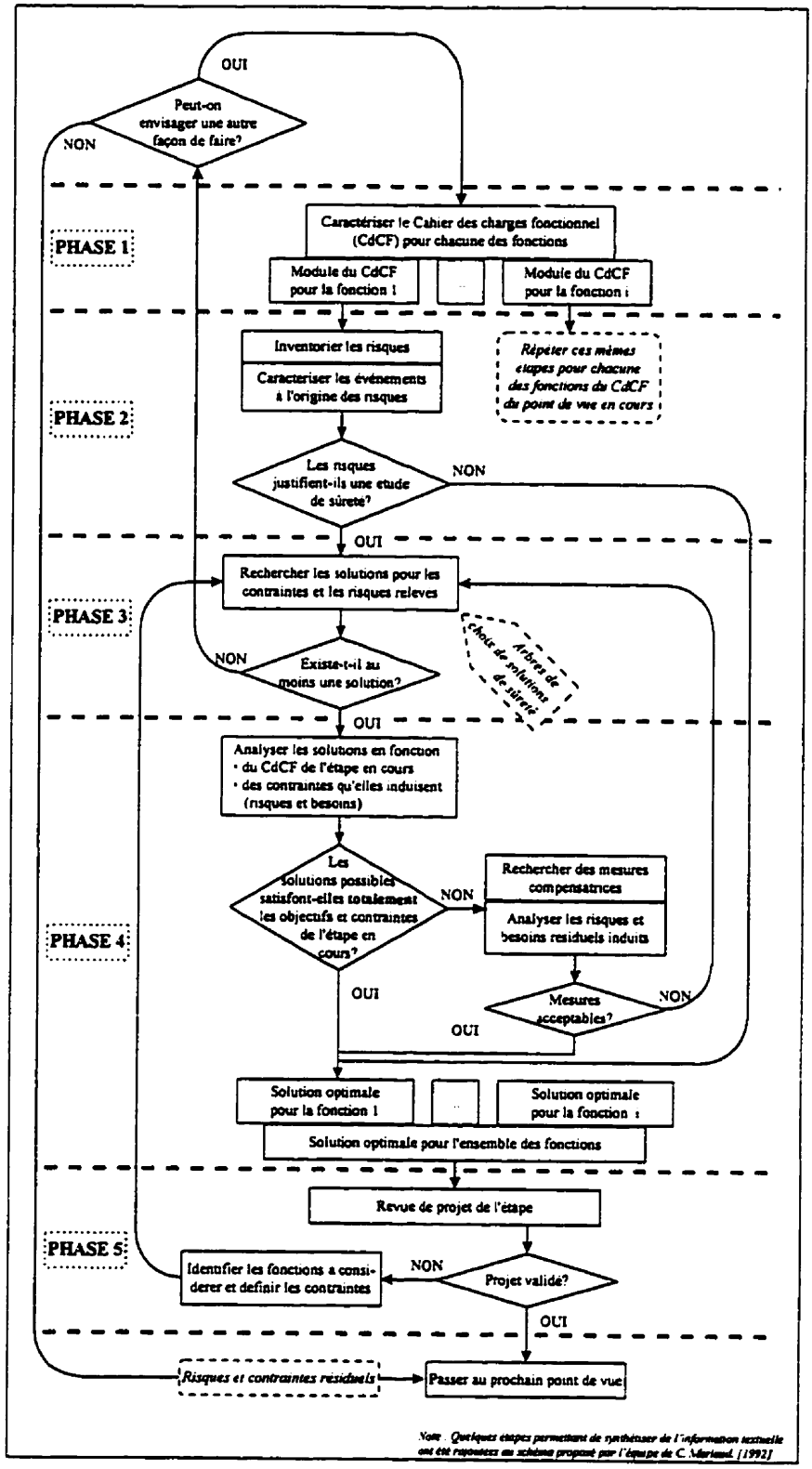

Figure 2.38 Schématisation des cinq phases de traitement des fonctions

La démarche globale consiste donc à appliquer ces cinq phases pour chacune des fonctions identifiées dans le CdCF global, et ce pour chacun des points de vue. Il est important de remarquer qu'à la phase 3, il est recommandé d'utiliser les *arbres de choix de solutions de sûreté*. Ces arbres permettent de choisir la solution la plus sûre et la plus économique en fonction du risque considéré.

Comme l'indique la figure 2.38, des risques et des contraintes résiduelles peuvent subsister suite au traitement des fonctions ; leur analyse est alors reportée au prochain point de vue pour permettre l'avancement du projet. Par exemple, pour la fabrication de la pâte Kraft, l'utilisation de produits chimiques dangereux, comme l'acide sulfurique, est nécessaire. Ainsi, l'analyse du point de vue *produit* permettra d'identifier les phénomènes dangereux qui peuvent résulter de l'utilisation d'un tel produit. Cependant, comme le procédé de fabrication de la pâte Kraft nécessite de tels produits, il n'est pas possible d'éliminer cette entité dangereuse. Par contre, grâce à l'approche proposée, l'analyse des phénomènes dangereux potentiels sera reportée au point de vue *production*, au point de vue *procédé* puis au point de vue *processus* où des solutions pourront alors être élaborées, comme prévoir l'étanchéité des réservoirs, la ventilation nécessaire, les mesures d'urgence en cas de difficultés hors de contrôle, etc. L'essentiel, et c'est ce que permet cette démarche, c'est que ces phénomènes dangereux soient traités, qu'ils ne soient pas oubliés en cours de route. La figure 2.39 (page suivante) représente la démarche globale proposée par Apave-Télémécanique.

Selon cette démarche, il est possible que des contraintes et des risques résiduels ne peuvent être éliminés ou ramenés à un niveau tolérable par ce processus. Ainsi, lors des activités d'exploitation et de maintenance (dernier point de vue), des protections supplémentaires et des consignes peuvent être nécessaires [MERLAUD, C. et coll., 1992].

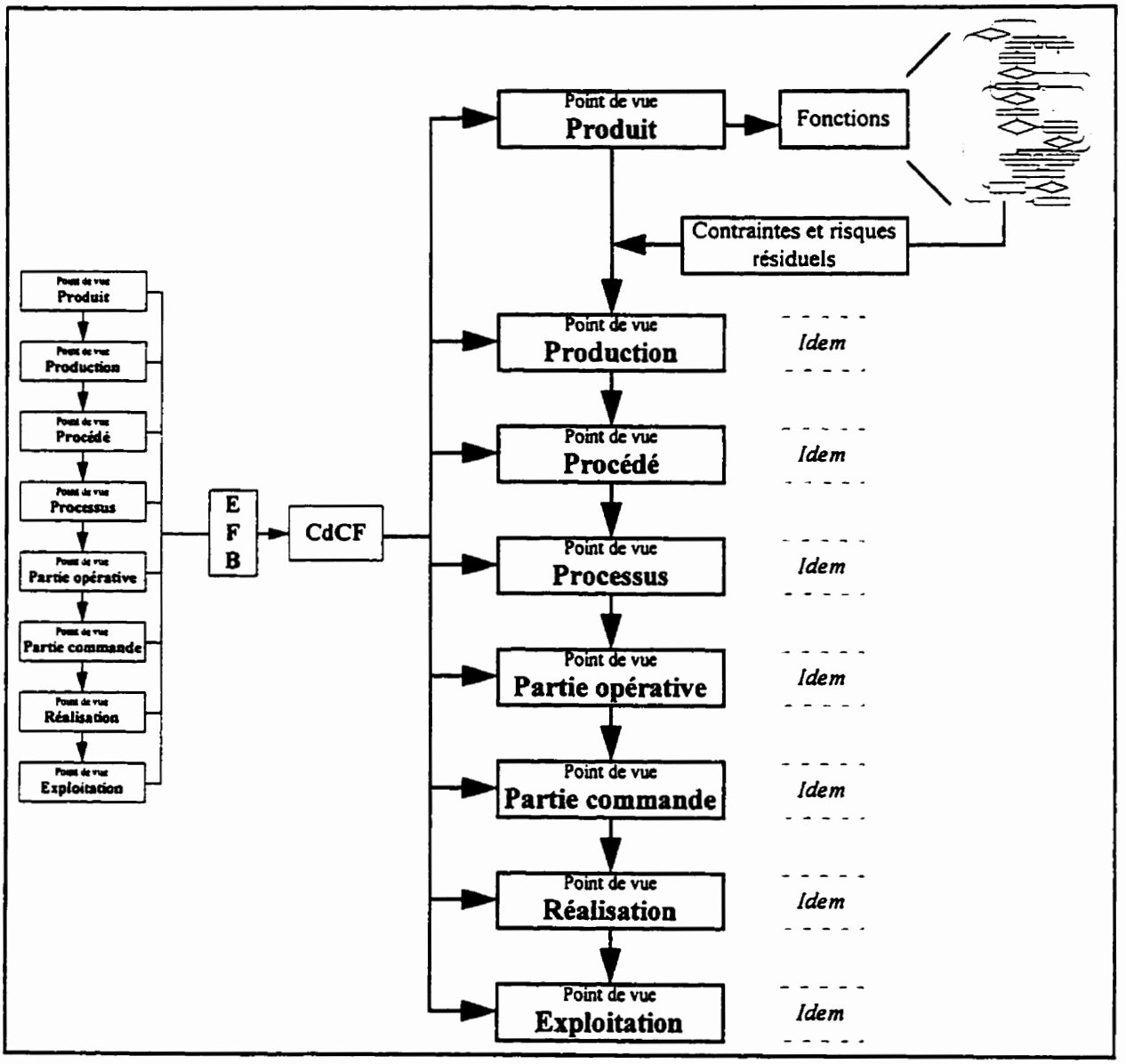

Figure 2.39 Démarche globale d'obtention d'un SPA sécuritaire

Aux premiers abords, l'application de cette méthodologie semble exiger une charge de travail monstrueuse. Néanmoins, l'approche par points de vue successifs semble offrir des avantages intéressants, dont celui de tenter d'éliminer certains phénomènes dangereux à la source la plus primaire, c'est-à-dire au point de vue du produit même. Un autre aspect intéressant est l'apparence très systématique des étapes à réaliser. En effet, un cheminement logique, précis et très détaillé est proposé aux concepteurs. Finalement, la réintégration systématique des risques résiduels à la démarche est un aspect très intéressant étant donné que le concepteur s'assure

jusqu'à un certain point que tous les risques associés aux phénomènes dangereux ont été appréciés. Le candidat avance donc que cette méthodologie, bien que beaucoup trop lourde pour être applicable dans l'industrie québécoise des P&P, comporte des éléments très intéressants qui pourraient être intégrés à la solution.

2.2.6.3 Approche proposée par l'Institut national de recherche et de sécurité (INRS)

Une méthodologie de conception élaborée à partir des concepts de sécurité émis dans la norme EN 292 [1991] est proposée par l'INRS. Tout comme la méthodologie précédente, elle propose une démarche basée sur l'identification et la maîtrise des risques par points de vue successifs (produit, production, processus, procédé, partie opérative, partie commande, réalisation/mise en service, exploitation/maintenance) [BIERCE, B. et coll., 1994]. Par contre, l'approche de l'INRS n'a pas, aux premiers abords, la lourdeur de réalisation de la méthode proposée par Apave-Télémécanique.

Aussi, tout comme dans le cas de la précédente approche, il faut dans un premier temps exprimer l'ensemble des besoins en se basant sur chacun des points de vue. Pour chacun de ces besoins, l'INRS propose de répertorier les phénomènes dangereux en s'inspirant d'une liste de contrôle (*checklist*) très générale représentée dans le tableau 2.5 (page suivante).

Conjointement à cette liste de contrôle, l'INRS encourage par ailleurs les concepteurs à utiliser les arbres de fautes (*Fault Tree Analysis, FTA*) en vue de s'assurer que toutes les causes possibles menant aux divers phénomènes dangereux analysés ont été recensées.

TABLEAU 2.5 LISTE DE CONTRÔLE POUR L'IDENTIFICATION DES PHÉNOMÈNES DANGEREUX

Phénomènes dangereux mécaniques : • risque d'écrasement ; • risque de cisaillement ; • risque de coupure ou de sectionnement ; • risque d'entraînement ou d'emprisonnement ; • risque de choc ; • risque de perforation ou de piqûre ; • risque d'abrasion ; • risque d'éjection de fluide sous pression ;
Phénomènes dangereux électriques pouvant causer des lésions ou la mort par choc électrique ou brûlure.
Phénomènes dangereux thermiques étant à l'origine de brûlures ou d'effets nocifs pour la santé ou fatal.
Phénomènes dangereux engendrés par le bruit.
Phénomènes dangereux engendrés par les vibrations.
Phénomènes dangereux engendrés par les rayonnements.
Phénomènes dangereux engendrés par les matériaux et des substances.
Phénomènes dangereux engendrés par le non-respect des principes ergonomiques.

Par la suite, chacun des phénomènes dangereux identifiés (ou leur cause) sont soumis au schéma de gestion du risque déjà présenté en section 2.2.3 (figure 2.31). Ainsi, pour chaque phénomène dangereux identifié et évalué, l'équipe de conception peut orienter sa conception en vue d'obtenir une solution qui respectera le principe de l'échelle de priorité. L'ensemble de la démarche est résumé dans la figure qui suit.

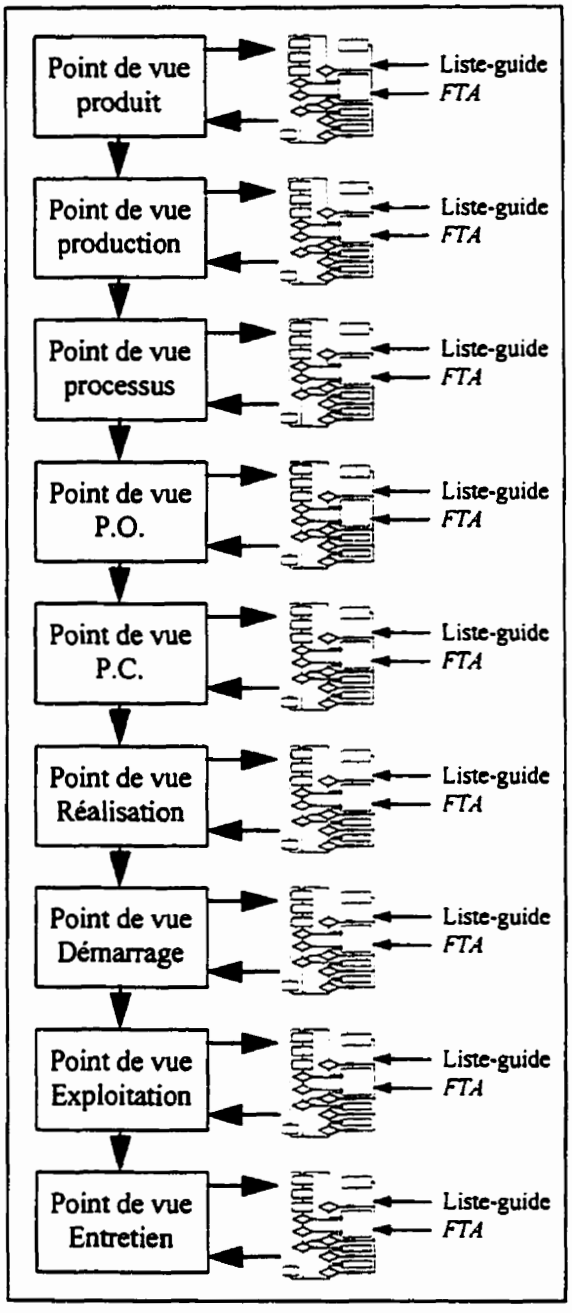

Figure 2.40 Approche proposée par l'INRS [BIERCE, B. et coll., 1994]

Cette approche s'apparente beaucoup à celle proposée par la société Apave-Télémécanique. La principale différence semble résider dans son apparence plus légère et plus facile à mettre en oeuvre. Les mêmes éléments intéressants en ressortent aussi, comme l'approche par point de vue et la réintégration systématique dans le processus de conception de tous les risques qui n'ont pu être éliminés ou suffisamment réduits.

2.2.6.4 Approche proposée par l'Industrial Technology institute (ITI)

Une approche proposée par l'*Industrial Technology Institute* (ITI), située à Ann Harbor dans l'état du Michigan, États-Unis, vise principalement à optimiser la conception d'un automatisme en vue de permettre aux employés d'effectuer leurs tâches respectives (installation, exploitation, mises au point, entretien, nettoyage, réparation et transport) dans des conditions aussi sécuritaires que possible [BUGAJSKI, P. et coll., 1991]. La méthodologie proposée, applicable pour la reconception ou la conception d'un SPA, est résumée à l'appendice 5.

L'approche proposée semble cependant concerner davantage l'optimisation des solutions pour la maîtrise des risques. Aussi, sa structure sous-entend que l'identification des phénomènes dangereux a déjà été effectuée avant d'appliquer cette méthodologie. Finalement, l'utilisation d'arbres de décision pour faciliter la mise en oeuvre de chacune des étapes donne un aspect de facilité de mise en oeuvre. Le candidat avance donc qu'il pourrait s'avérer intéressant de l'intégrer à une méthodologie plus complète, comme celles présentées jusqu'à maintenant.

2.2.6.5 Approche proposée par G. Rouchouse

La procédure présentée dans le livre *Sûreté des automatismes* est composée de quatre étapes principales [ROUCHOUSE, G., 1992] :

1. l'étude conceptuelle ;
2. l'analyse technique et fonctionnelle préliminaire ;
3. l'analyse qualitative ;
4. l'analyse quantitative.

Dans l'étude conceptuelle, les documents de base de l'analyse de sûreté sont élaborés. La première étape est l'étude du système où l'ensemble des besoins et des objectifs de production sont élaborés. Cette étape est accomplie en se fiant à l'expérience et aux savoir-faire des divers opérateurs et peut être complétée par une analyse fonctionnelle. Une fois l'ensemble des fonctions établies, les choix technologiques préliminaires des divers composants peuvent être faits. Finalement, l'élaboration et l'étude des schémas (électrique, mécanique et logiciel) viennent terminer cette étape. Dans la seconde étape, une analyse plus approfondie des résultats

précédents est effectuée. La conclusion de cette étape est donc la composition quasi finale du SPA. Dans la troisième étape, le système jusqu'à maintenant élaboré est qualifié en effectuant une analyse qualitative de sécurité. L'utilisation d'outils spécifiques, tel l'AMDE et les arbres de fautes, permet d'effectuer cette analyse. Une phase de validation vient compléter cette étape. Finalement, une dernière étape permet de quantifier le niveau de sécurité en effectuant des études de probabilités. Pour le lecteur désireux d'avoir un aperçu de cette méthodologie, elle est reproduite à l'appendice 6.

Cependant, malgré son aspect fortement systématisé, l'approche semble vide et non structurée aux yeux du candidat. Par exemple, les choix technologiques semblent être effectués bien avant que l'étude portant sur les besoins fonctionnels ne soient complètement terminée. Aussi, l'intégration des méthodes d'analyse du risque est tardive et très peu détaillée. De plus, la quantification globale du niveau de sécurité obtenu par des études de fiabilité semble revêtir une grande importance dans l'approche. Or, il est certes intéressant d'obtenir cette quantification, mais elle peut être extrêmement fastidieuse à évaluer et les informations qui en ressortent ne sont pas nécessairement pertinentes pour la conception de SPA destinés à l'industrie québécoise des P&P. Les énergies requises pour la mise en oeuvre d'une telle quantification pourraient être plus profitables dans l'analyse fonctionnelle des besoins ou pour la gestion du risque. Pour toutes ces raisons, l'approche proposée par G. Rouchouse [1992] ne sera pas considérée dans ce mémoire.

2.2.6.6 Approche proposée par F. Gauthier

Dans sa thèse de doctorat, F. Gauthier [1997] propose une approche méthodologique permettant l'intégration systématique de l'aspect SST dans le processus de conception d'outils, de machine ou de procédé industriels (OMP). L'approche proposée est basée sur trois hypothèses de départ. D'abord et tel que prescrit par plusieurs auteurs et organismes, pour être acceptée et utilisée par les concepteurs, toute approche d'intégration de la SST lors de la conception d'un OMP ne doit pas rallonger significativement le temps de développement de celui-ci. Ensuite, à la lumière des sources consultées par l'auteur, il semble justifier que c'est l'identification des phénomènes dangereux qui pose le plus grand défi pour les concepteurs et que cette activité est la clé de la majorité des problèmes SST dans les OMP. Enfin, il est largement reconnu que les moyens pris

pour assurer la sécurité ne doivent pas être élaborés sans égard aux besoins fonctionnels des utilisateurs, car toute solution imposée à ces derniers sans tenir compte des effets négatifs qu'elle peut avoir sur les autres aspects de la conception risque de ne pas être acceptée et, éventuellement, d'être retirée ou rendue inefficace par ceux-ci [EN 292-1, 1991].

Par ailleurs, dans la majorité des cas, la résolution des problèmes de sécurité (et particulièrement de SST) doit faire appel à plusieurs disciplines [STOOP, J.A., 1990]. De plus, ces problèmes donnent souvent lieu à des interrelations complexes, ce qui exige une étroite collaboration entre les experts de ces différentes disciplines [BRAUER, R.L., 1994] [CHARRON, F. et coll., 1995]. Il est donc de plus en plus reconnu que l'intégration de la sécurité dans le processus de conception doit se faire dans un contexte multidisciplinaire favorisant les échanges et les communications entre les intervenants [BRAUER, R.L., 1991] [RAHEJA, D.G., 1991]. Pour répondre à ce besoin multidisciplinaire marqué, l'approche proposée par F. Gauthier repose sur le processus de réalisation d'un produit issu de la philosophie de l'ingénierie simultanée[17].

Un des point clés de la méthodologie qu'il propose est l'application rigoureuse de sa démarche de gestion du risque présentée à la section 2.2.3. Un aspect très intéressant est que l'auteur propose des modes d'analyse du risque appropriés à chacune des étapes de la démarche, et ce en tenant compte de l'avancement de la conception de l'OMP. Ces modes d'analyse sont intégrées à la démarche de gestion du risque comme l'indique la figure suivante[18]. Cette figure est inspirée de celle proposée par F. Gauthier [1997] ; seul le vocabulaire a été adapté à celui utilisé dans ce mémoire.

---

[17] L'ingénierie simultanée est une approche systématique et multidisciplinaire qui vise à intégrer, de façon simultanée, les différentes phases de développement d'un produit et la gestion de son processus [PROULX, D., 1992]. Plusieurs ouvrages traitant de l'ingénierie simultanée et de son PRP ont été élaborés par les membres du GRIS de l'Université de Sherbrooke [CHARRON, F. et coll., 1996] [DOUCET, P., 1997] [GAUTHIER, F., 1993] [GAUTHIER, F., 1997] [LEMAY, É., 1995] [LEMAY, É. et coll., 1997] [MURRAY, A., 1996] [PROULX, D., 1992] [ST-AMANT, R., 1993].

[18] Ces 14 méthodes d'analyse du risque sont présentées plus en détail à l'appendice 3.

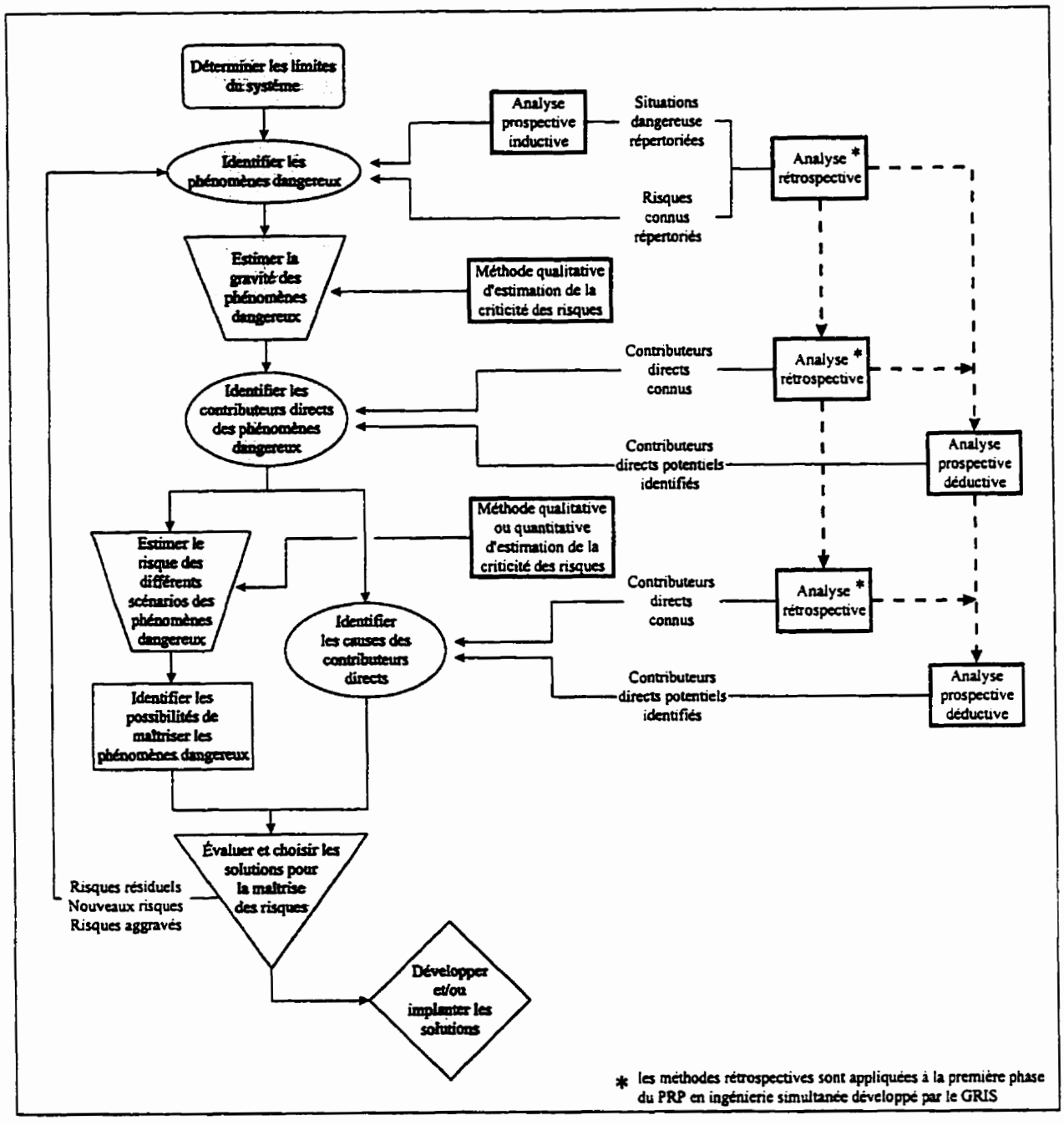

Figure 2.41 Intégration des méthodes d'analyse du risque à la gestion du risque.

Un autre point clé de la méthodologie proposée est l'établissement de flux d'information pouvant exister entre chacune des méthodes d'analyse du risque. Il s'agit là d'une très grande caractéristique étant donné que grâce à ces flux, le concepteur peut choisir parmi les méthodes d'analyse du risque sélectionnées celles qu'il préfère ou qu'il juge la mieux appropriée et celles

qui lui permettent d'amorcer ou d'approfondir l'analyse qu'il désire effectuer. Par exemple, l'application de la méthode *Task Analysis* peut servir à identifier dans un premier temps l'ensemble des situations de travail. Puis, l'application de la méthode *Critical Incident Technique* permettra d'identifier quelles sont, parmi les situations de travail identifiées, celles qui sont à risque.

Finalement, tel qu'établi précédemment, l'approche proposée s'intègre dans les diverses phases du PRP de l'ingénierie simultanée développé par le GRIS de l'Université de Sherbrooke. Aussi, l'analyse et la maîtrise des phénomènes dangereux doivent se faire à plusieurs niveaux de maturité de la conception : pré-étude, conception préliminaire, conception détaillée, etc.. Étant donné qu'à chacune des phases de conception la gestion du risque évolue, des phénomènes dangereux nouveaux, résiduels ou aggravés peuvent surgir. Ainsi, cinq applications (une par phase du PRP de l'ingénierie simultanée) de la démarche de gestion du risque sont prévues tout au long de l'avancement de la conception. La figure qui suit schématise l'idée générale de cette intégration.

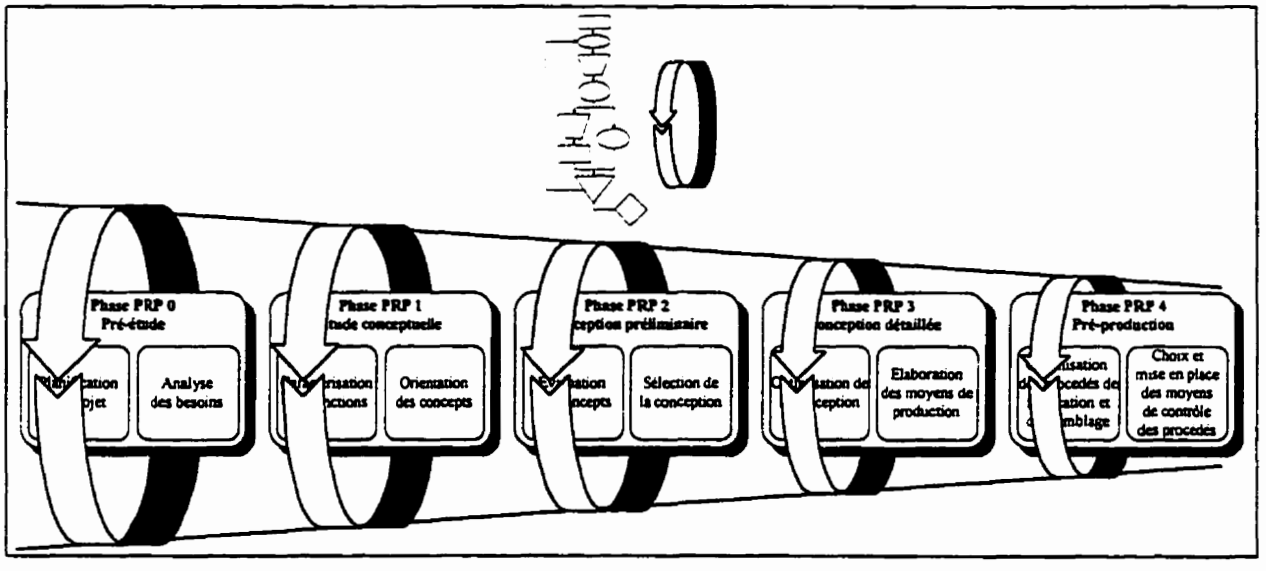

Figure 2.42 Intégration de l'appréciation du risque au PRP de l'ingénierie simultanée

La concrétisation de cette intégration repose sur trois principes de base. Le premier découle du fait que les activités d'appréciation du risque sont intégrées dans les autres activités de conception (élaboration des besoins, recherche des solutions, etc.). Le second est que dans chacune des

applications de la démarche, les activités d'analyse du risque peuvent être réalisées par l'utilisation d'une ou plusieurs des méthodes présentées précédemment. Enfin, la structure globale de l'approche repose sur le principe de mise à jour des activités pour la gestion du risque à chacune des phases du PRP. Ainsi, les activités normales de conception mettront en évidence quelques problèmes de sécurité et l'application de la démarche de gestion du risque à chacune des étapes du PRP donnera des informations, plus ou moins complètes selon la maturité du projet qui pourront ou bien être mises en oeuvre aussitôt, ou bien être reportées lors de l'analyse d'une phase ultérieure.

Par ailleurs, trois revues de sécurité permettant de faire le point à diverses étapes de la conception sont intégrées à la méthodologie. La figure qui suit indique à quel moment précis elles doivent être réalisées puis les objectifs de chacune d'elles sont établis par après.

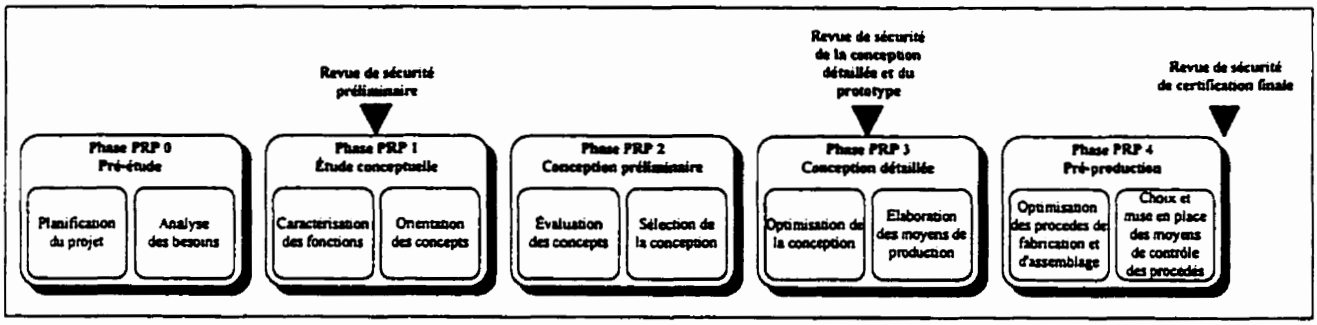

Figure 2.43 Revues de sécurité formelles dans le PRP de l'ingénierie simultanée

La *revue de sécurité préliminaire* vise à confirmer (et quelques fois à compléter) la liste des phénomènes dangereux répertoriés suite à l'analyse rétrospective réalisée en PRP 0 ainsi qu'à approuver les fonctions de sécurité et les caractéristiques de sécurité des fonctions[19] contenues dans le CdCF. Quant à elle, la *revue de sécurité de la conception détaillée et du prototype* vise à s'assurer de la conformité de l'OMP aux exigences de SST établies lors de la pré-étude. Si la conformité n'est pas intègre, les correctifs nécessaires devraient alors être apportés. Finalement, la *revue de sécurité de certification finale* a pour but de s'assurer que l'OMP conçu répond à

[19] Il ne faut pas confondre *fonction de sécurité* et *sécurité des fonctions*. Les *fonctions de sécurité* sont celles qui commandent au SPA d'atteindre un état sécuritaire prédéterminé. Dans le cas de la *sécurité des fonctions*, il est plutôt question des caractéristiques qui confine un aspect sécuritaire à une fonction donnée.

l'ensemble des exigences prévues par le client et par la loi ; il est donc assez sécuritaire pour être mis en service.

La démarche globale proposée par F. Gauthier est reproduite dans la figure qui suit.

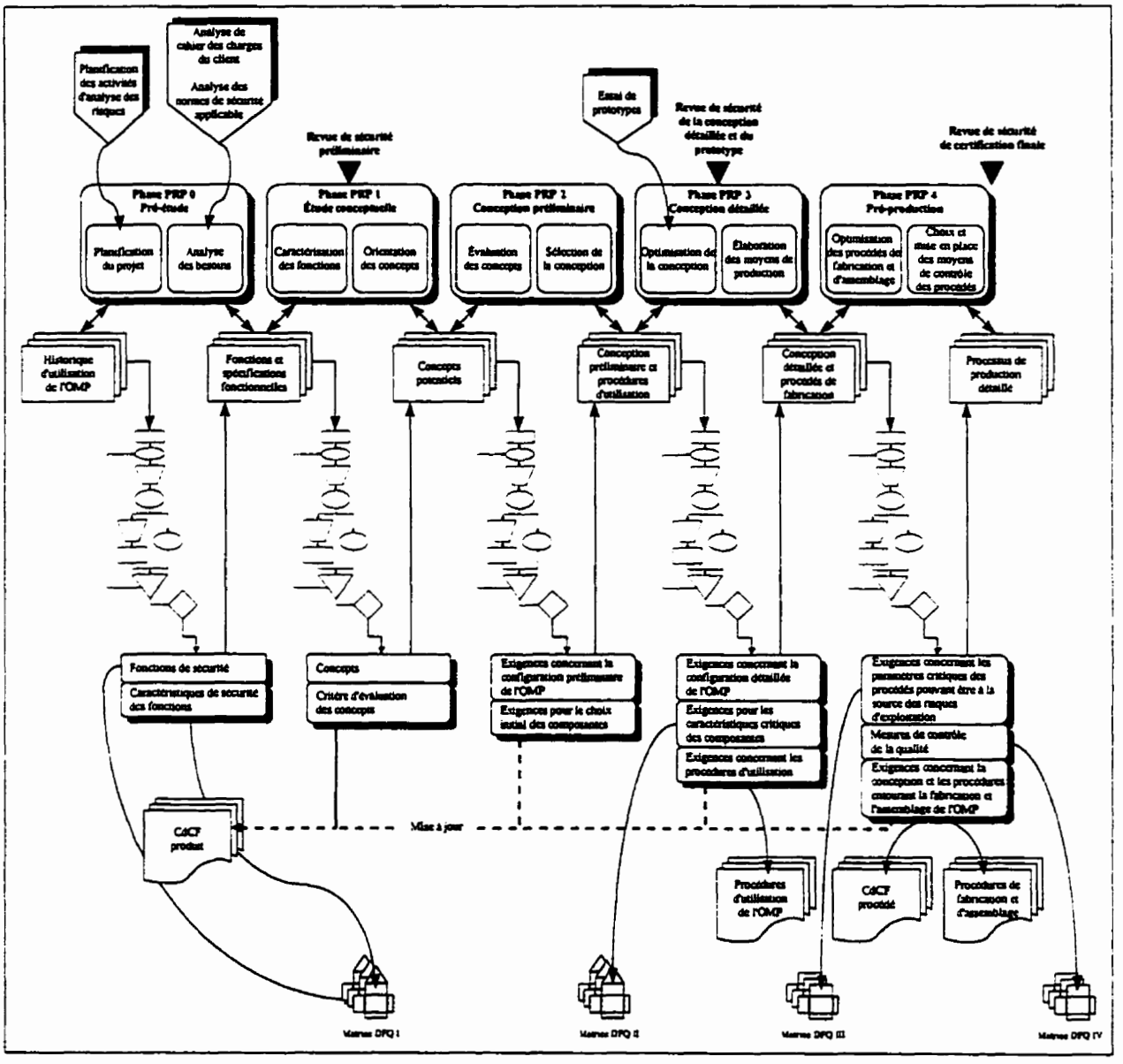

Figure 2.44 Méthodologie proposée par F. Gauthier [1997]

L'approche proposée par F. Gauthier est très intéressante pour quatre points de vue importants. Le premier est la classification tout à fait innovatrice des méthodes d'analyse du risque. Cette classification permet aux concepteurs de choisir la méthode appropriée en fonctions des divers

contextes : les méthodes permettant des analyses rétrospectives pour l'identification des phénomènes dangereux dans la première phase du PRP ; les méthodes permettant des analyses prospectives inductives pour l'identification des phénomènes dangereux et prospectives déductives pour l'identification de leurs causes ; les méthodes permettant l'estimation des risques associés aux phénomènes dangereux identifiés. Aussi, les méthodes ont été classifiées selon les types de facteurs de risque identifiés, ce qui permet aux concepteurs de choisir la ou les méthodes appropriées en fonction de leur contexte propre, basé sur la prépondérance des facteurs de risques techniques, humains, organisationnels ou externes. Aussi, à chacune des méthodes a été attribué un niveau de profondeur tenant compte de la difficulté d'application de la méthode en fonction des résultats obtenus. Finalement, les différentes interrelations possibles (flux d'information) permettent aux concepteurs d'utiliser conjointement les méthodes sélectionnées.

Le second point de vue à retenir est l'intégration des activités de gestion du risque à un processus de conception systématique et multidisciplinaire, celui de l'ingénierie simultanée. L'approche proposée permet d'effectuer les activités de gestion du risque simultanément avec les autres activités de conception d'un OMP. L'objet des analyses du risque et la nature des solutions pour la maîtrise des risques qui en découlent ont été adaptés aux contextes de chacune des phases du PRP.

Le troisième aspect à ne pas négliger est l'efficacité de l'approche. En effet, la démarche propose un cadre très systématique de façon à optimiser l'efficacité des activités visant à analyser et à maîtriser les phénomènes dangereux. Aussi, les solutions pour la maîtrise des phénomènes dangereux tiennent compte de l'aspect fonctionnel de l'OMP, comme le stipule la norme EN 292-1 [1991]. Finalement, elle permet de guider les concepteurs tout au long de la réalisation de l'OMP, de l'élaboration des besoins à l'élaboration des consignes de sécurité et des procédures d'installation, d'exploitation, d'entretien, etc. L'application de la démarche à une étude de cas fictive a d'ailleurs permis de vérifier l'efficacité de l'approche. Cependant, elle bénéficierait, au dire même de l'auteur, d'être validée par des applications concrètes en industrie.

Le quatrième élément marquant est la flexibilité de l'approche. Ainsi, cette dernière s'adapte au type et à la complexité du produit, au niveau d'innovation recherché, aux ressources et aux

expertises disponibles qui sont nécessaires à sa mise en oeuvre. La classification des méthodes d'analyse du risque ainsi que le nombre de ces dernières contribuent, au même titre que son adaptation au PRP de l'ingénierie simultanée, à la flexibilité de l'approche.

Cependant, un point très important mis en évidence par l'analyse de cette approche de conception et soulevé par l'auteur est qu'elle n'a pas été élaborée en tenant compte des OMP comportant des systèmes de commande constitués de SÉP. Néanmoins, l'approche pourrait très certainement être utilisée comme trame de fond à laquelle une approche d'intégration de l'aspect SST spécifiquement adaptée aux SÉP pourrait être greffée.

2.2.6.7 Revue des normes pour les approches de conception sécuritaire des SPA

Tel qu'établi précédemment, deux projets de norme propose des méthodologies spécialement développées pour la conception de SPA sécuritaires. La première approche présentée ici est celle proposée dans le projet de norme européen EN 954 [parties 1 et 2, 1996]. La seconde est celle qui est élaborée dans le projet de norme internationale CEI/IEC 1508 [parties 1 à 7, 1995].

a) Approche proposée dans le projet de norme EN 954 [parties 1 et 2, 1996]

Cette approche est composée de 5 étapes principales qui sont reproduites à la figure 2.45 (page suivante). La première étape se résume à effectuer l'appréciation du risque. Pour ce faire, il est recommandé de consulter les normes EN 292-1 [1991] et EN 1050 [1996]. Les sections 2.2.2 et 2.2.3 ont présenté respectivement les méthodes d'analyse du risque et les démarches de gestion du risque proposées par ces ouvrages normatifs. Cependant, l'estimation du risque, bien que pouvant être faite à l'aide de la grille proposée par le projet de norme EN 1050 [1996] (figure 2.27), devrait plutôt être faite à partir de celle proposée par le présent projet de norme (figure 2.29). Ainsi, les catégories à respecter en fonction des risques estimés seront identifiées. La seconde étape permet au concepteur de décider des mesures (redondance, autosurveillance, dispositifs de protection, etc.) qu'il pourrait envisager pour l'élimination des phénomènes dangereux ou la réduction de leur risque. Au niveau de la troisième étape, toutes les spécifications relatives aux fonctions de sécurité qui seront assurées par le système de commande doivent être établies en considérant les prescriptions des catégories identifiées précédemment.

Ces trois premières étapes sont donc essentiellement consacrées à la spécification des fonctions de sécurité qui devront être implantées dans le système de commande [CHARPENTIER, P. et coll., 1996].

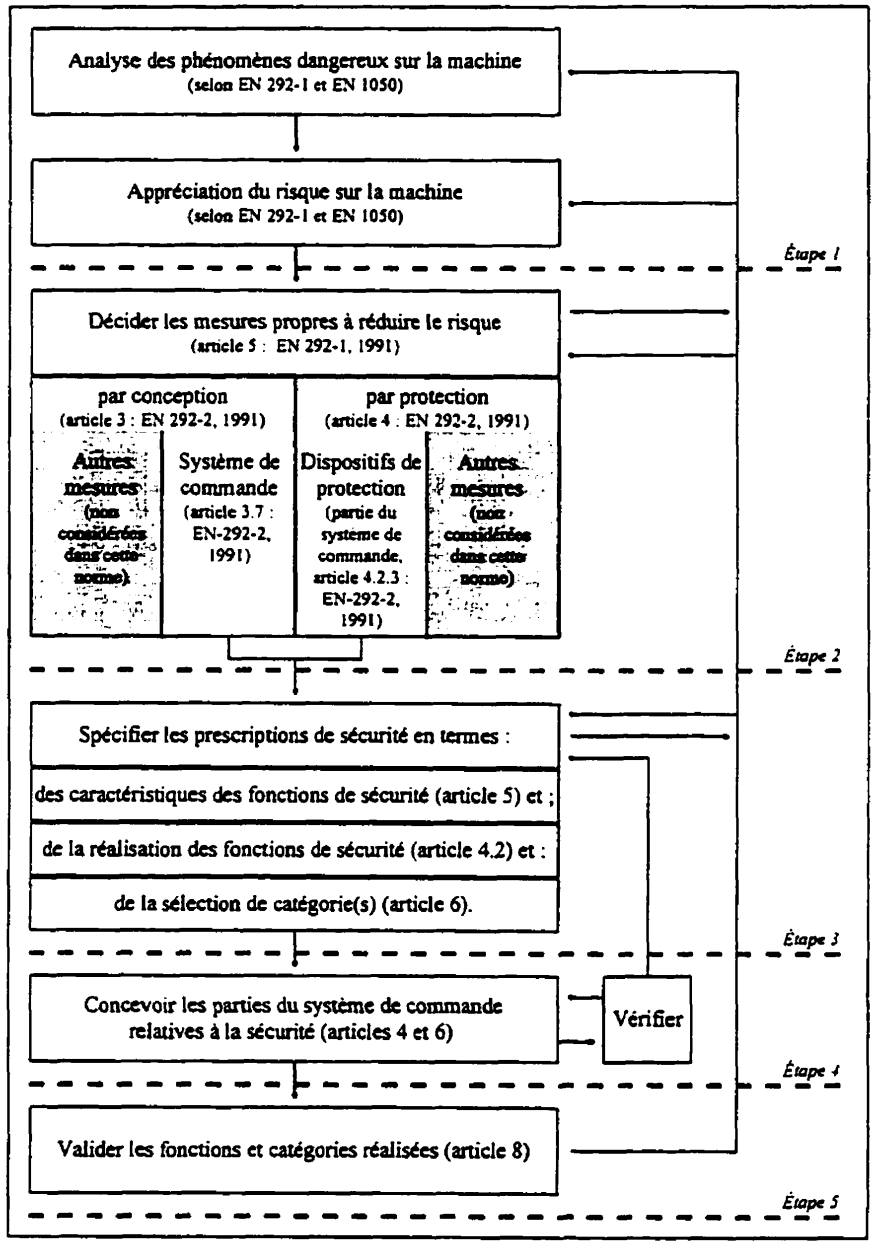

Figure 2.45 Approche de conception proposée par le projet de norme EN 954 [1996]

L'avant-dernière étape consiste à concevoir le système de commande tel que prescrit à l'étape 3 et à s'assurer que ce dernier respecte effectivement les exigences de conception établies par les

catégories retenues. Finalement, la cinquième et dernière étape consiste à valider les parties du système de commande relatives à la sécurité, donc à démontrer que ces parties respectent bien les exigences de la catégorie spécifiée. Cette validation peut être effectuée par analyse ou par simulation. Étant donné que le nombre de défauts possibles est très élevé et que la simulation de ces derniers n'est pas toujours faisables, cette étape est donc extrêmement complexe [CHARPENTIER, P. et coll., 1996]. Bien que la partie 2 du projet de norme propose une démarche de validation ainsi qu'une liste permettant d'identifier des défauts fréquemment rencontrés, cette étape demeure néanmoins toujours fastidieuse et complexe.

Par ailleurs, il pourrait être intéressant de retenir certains points de ce projet de norme. Par exemple, cette approche semble aux premiers abords assez simple et pas trop lourde à appliquer : les étapes sont peu nombreuses et leurs objectifs semblent réalisables. Aussi, le concept selon lequel l'estimation du risque mène à l'identification de catégories pour lesquelles des recommandations précises sont faites est également un aspect très intéressant. Finalement, très tôt dans le processus (à l'étape 2), le concepteur doit déterminer si les risques associés aux divers phénomènes dangereux seront réduits par une meilleure conception ou par une protection adéquate. Cette façon de faire, toute simple, incite donc le concepteur à considérer plus d'une solution pour la réduction du risque, ce qui est évidemment un point intéressant.

b) Approche proposée dans le projet de norme CEI/IEC 1508 [parties 1 à 7, 1995]

La seconde approche répertoriée dans la littérature normative est celle proposée par le projet de norme internationale CEI/IEC 1508 [parties 1 à 7, 1995]. Son principal objectif est d'accroître la sécurité des systèmes de commande en prévenant notamment leurs défaillances possibles [BRAZENDALE, J., 1995]. Les technologies des systèmes de commande visées par cette approche concernent particulièrement les technologies électriques, électroniques ou électroniques programmables (E/E/PES). Cependant, elle peut tout de même s'appliquer aux technologies plus traditionnelles (logique câblée, commandes pneumatique et hydraulique, etc.) [BELL, R. et coll., 1992] [BRAZENDALE, J., 1995] [CEI/IEC 1508-1, 1995]. Son approche est basée sur le *cycle de vie général de sûreté* d'un système de commande qui est reproduit à la figure 2.46.

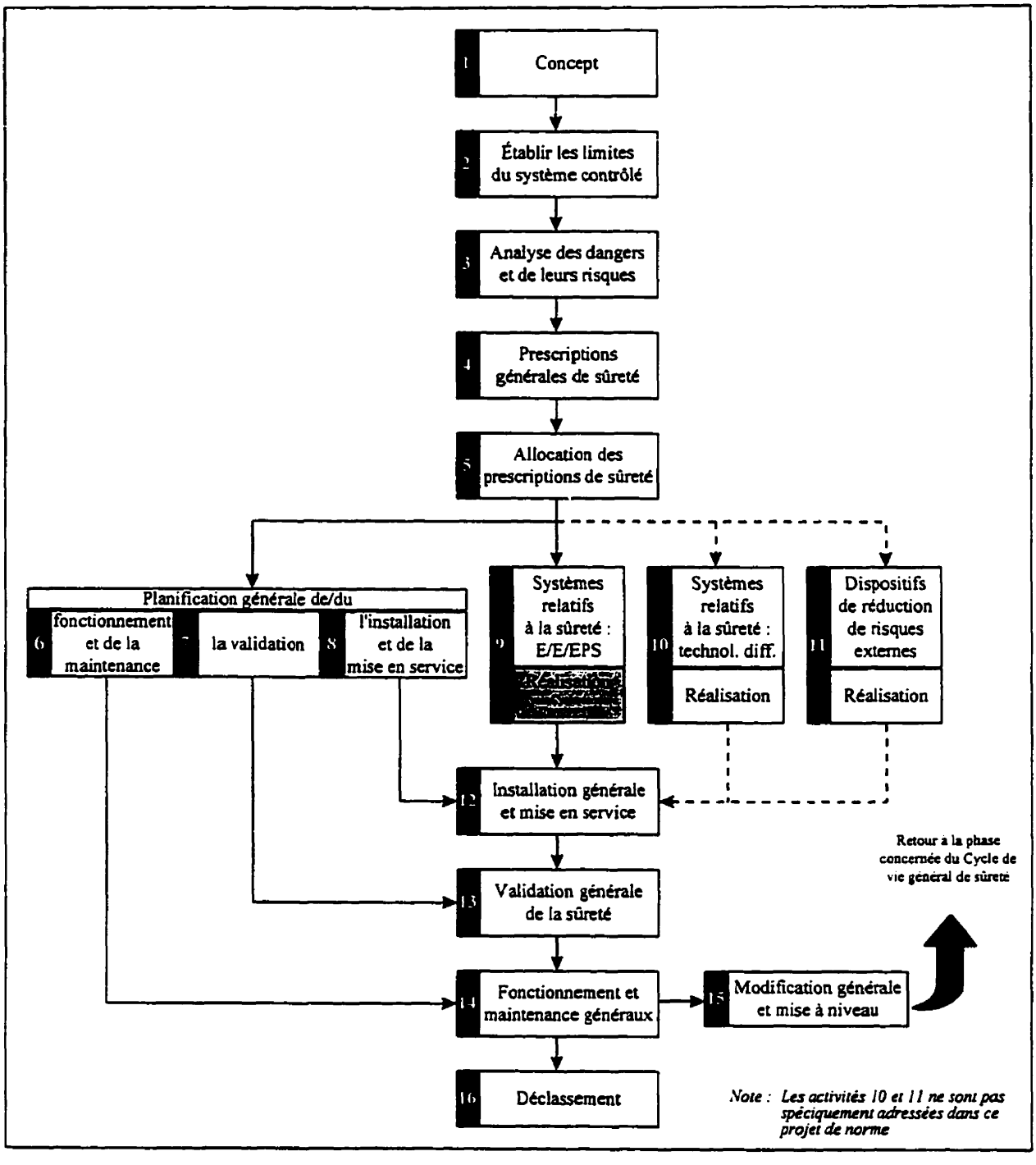

Figure 2.46 Cycle de vie générale de sûreté [CEI/IEC 1508-1, 1995]

Chacune des 16 étapes présentées dans cette figure a des données d'entrée, des objectifs clairement définis, des activités liées à la sécurité et des sorties précises (sous forme de livrables) ; d'ailleurs, ces dernières deviennent par la suite les données d'entrée de la phase

suivante et ainsi de suite. De plus, tout au long de ces activités doivent se dérouler en parallèle des activités de vérification et de validation. Par ailleurs, comme l'indique la figure 2.46, l'étape 3 est spécifiquement dédiée à l'analyse du risque. Cependant, dans le but de ne pas surcharger la figure, l'analyse du risque n'a été mentionnée qu'à cette étape, car toutes les étapes doivent comporter de ces analyses. En effet, à l'étape 3, la conception n'est pas suffisamment avancée pour que l'ensemble des phénomènes dangereux soient répertoriés ; des activités d'appréciation du risque doivent inévitablement se dérouler en parallèle.

Tout comme pour le projet de norme EN 954 [1996], ce projet de norme établit des prescriptions spécifiques en fonction de certains niveaux de sécurité (*Safety Integrity Level*). Ces derniers sont établis en fonction de le probabilité annuelle de défaillance qui demeure acceptable. Le tableau suivant présente ces niveaux de sécurité.

TABLEAU 2.6 NIVEAUX DE SÉCURITÉ ÉTABLIS [CEI/IEC 1508-1, 1995]

Niveau de sécurité	**Probabilité annuelle de défaillance**
1	$\geq 10^{-2}$ à $< 10^{-1}$
2	$\geq 10^{-3}$ à $< 10^{-2}$
3	$\geq 10^{-4}$ à $< 10^{-3}$
4	$\geq 10^{-5}$ à $< 10^{-4}$

Deux approches permettant d'obtenir ces niveaux de sécurité sont proposées. La première, celle qui est recommandée, est quantitative. Cependant et tel que mentionné précédemment, les approches quantitatives sont souvent très lourdes à appliquer et, compte tenu des contraintes connues dans les papetières québécoises, elles sont peu pertinentes dans le cadre de ce mémoire. Par contre, l'approche qualitative est assez simple et ressemble énormément à celle proposée par le projet de norme EN 954 [parties 1 et 2, 1996]. Elle est représentée dans la figure qui suit.

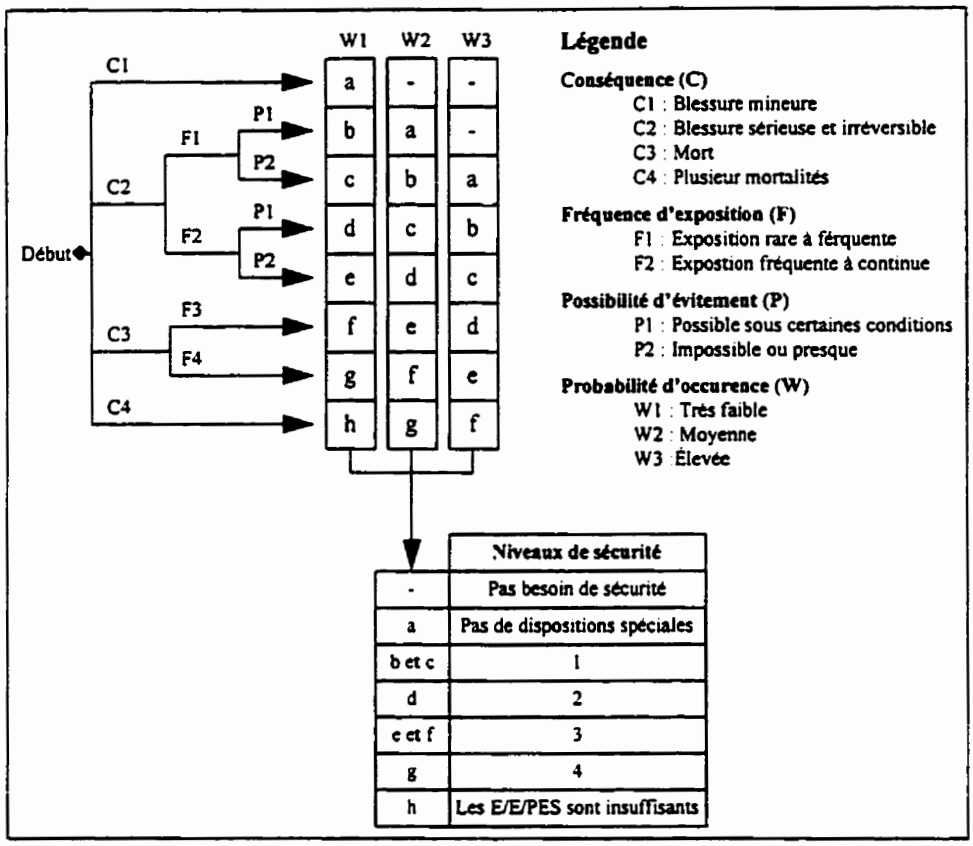

Figure 2.47 Attribution des niveaux de sécurité selon le risque estimé

Une fois les niveaux de sécurité obtenus, plusieurs recommandations, principes et moyens techniques sont suggérés pour permettre au concepteur d'obtenir le niveau de sécurité prescrit. Il est cependant intéressant de noter que ces derniers ne sont pas liés à la technologie, de telle sorte que l'évolution de cette dernière n'affecte pas ce projet de norme.

Bien que ce projet de norme soit exactement axé sur le sujet de recherche, à savoir l'intégration sécuritaire des technologies programmables aux SPA, il paraît être beaucoup trop lourd pour une application concrète dans l'industrie québécoise des P&P. Néanmoins, les recommandations, les principes et les moyens techniques proposés peuvent s'avérer très intéressant pour la solution à développer.

c) Comparaison sommaire de ces deux projets de norme

Ce qui différencie ces deux projets de norme n'est pas évident aux premiers abords. Dans les deux cas, une méthodologie de conception systématique et organisée est décrite, des activités

d'appréciation du risque sont prescrites (sans pour autant préciser, dans les deux cas, quelles méthodes d'analyse du risque devraient être utilisées), le concept de catégorie de risque selon lequel des recommandations claires sont faites en fonction des risques estimés est appliqué, etc. Ce sont donc des projets de norme qui présentent certaines similitudes. Malgré tout, deux importants aspects les différencient.

La première grande différence est que le projet de norme EN 954 repose sur une estimation qualitative des risques alors que le projet de norme CEI/IEC 1508 recommande très fortement un processus quantitatif [20]. Cette approche quantitative est d'ailleurs en grande partie à l'origine de la lourdeur de mise en oeuvre de ce projet de norme. Aussi, très peu de données statistiques concernant les taux de défaillance des SÉP (essentiel à la quantification) sont disponibles dans la littérature [ROUCHOUSE, G., 1992]. Ceci rend donc l'application de ce projet de norme encore plus ardue.

L'autre élément qui différencie considérablement ces deux projets de norme est leur domaine d'application. Bien que dans les deux cas l'objectif visé est la conception sécuritaire des systèmes de commande comprenant notamment des composants électriques, électroniques ou électroniques programmables, la profondeur de leur traitement diffère considérablement. Le projet de norme CEI/IEC 1508 est beaucoup plus exhaustif dans ce cas. D'ailleurs, presque le tiers de ses prescriptions sont spécifiquement consacrées aux SÉP, ce qui est loin d'être le cas pour le projet de norme EN 954.

Néanmoins, il est de l'avis du candidat que ces deux projets de normes ne sont pas applicables intégralement dans l'industrie papetières du Québec compte tenu des observations faites en usine et des informations issues des groupes de discussion. Seuls certains principes de conception pourraient être retenus, comme le concept de catégories de risque pour lesquelles des recommandations techniques sont faites.

---

[20] Bien qu'une estimation qualitative des risques soit présentée, le projet de norme CEI/IEC 1508 [1995] recommande néanmoins un processus quantitatif.

2.2.6.8 Conception des SPA dans l'industrie québécoise des P&P

Suite aux activités réalisées (visites d'usines, groupes de discussion, etc.), il ressort qu'il n'y a pratiquement aucune méthodologie de conception systématique et documentée utilisée dans l'industrie québécoise des P&P. Toutes les étapes de conception sont effectuées par expérience ; les informations pertinentes se trouvent donc dans la tête des concepteurs. Une seule usine sur les sept visitées fait exception à la règle. En effet, tous les concepteurs de cette usine suivaient une méthodologie standardisée pour concevoir ou modifier un équipement. De plus, très tôt dans le projet (bien avant l'approbation des fonds), une réunion d'information est prévue. À cette dernière, les consultants externes, les ingénieurs électriques, les ingénieurs responsables des systèmes de commande ainsi que l'ingénieur de projet sont présents et définissent ensemble le projet. Il s'agit là d'un exemple très intéressant montrant le désir de changer les choses dans les papetières québécoises.

Par ailleurs, la coopération entre les intervenants semble généralement déficiente. Les problèmes de communication établis précédemment en témoignent d'ailleurs. Par exemple, règle générale, ce sont des ingénieurs en mécanique qui composent le service d'ingénierie et qui gèrent les projets ; les autres départements interviennent habituellement comme service, mais souvent trop tard dans le processus de conception. Ils subissent alors beaucoup de pression. Une raison invoquée pour cette pratique est que la partie mécanique d'une machine revêt un caractère tangible, concret, alors que l'aspect électrique et automatique sont des concepts abstraits, non matériels et donc simples à réaliser et peu dispendieux. Évidemment, cette façon de faire engendre d'énormes erreurs d'appréciation. Par exemple, il arrive que la conception des systèmes de commande débute bien après la définition fonctionnelle et parfois même après la fabrication des principales machines, ce qui se traduit par d'interminables modifications de dernières minutes.

À la lumière des informations obtenues au cours de ces activités, deux constats généraux peuvent être établis. D'abord, il y a un évident manque de coopération entre tous les intervenants. Aussi, l'intégration des activités de conception est inexistante : elles se réalisent d'une manière très séquentielle et sont uniquement liées à l'expérience des concepteurs.

3. PROBLÉMATIQUE

L'opération et la maintenance des systèmes de production automatisés dotés de technologies programmables et destinés à l'industrie québécoise des pâtes et papiers posent des problèmes de sécurité. En effet, plusieurs accidents sont survenus sur ces équipements au cours des dernières années. Bien qu'une grande sensibilisation aux problèmes de SST ait été faite, les problèmes de sécurité n'ont qu'été partiellement réglés ; la conception même de ces systèmes ne tient pas suffisamment compte de la sécurité des activités d'opération et de maintenance.

3.1 Conception des SPA dans l'industrie québécoise des P&P

À la lumière des activités effectuées dans le cadre de cette recherche (visites industrielles, groupes de discussion, etc.), il ressort que la conception ou la modification des SPA réalisée dans l'industrie québécoise des P&P ne repose sur aucune approche de conception intégrant systématiquement toutes les activités de conception. Cette conception est plutôt basée sur l'expérience et le savoir faire de l'équipe de conception. Ainsi, lorsque des nouveaux ingénieurs sont engagés pour faire de la conception, le travail de ces derniers est très souvent dépendant de celui des concepteurs d'expérience, car leur savoir et leur savoir-faire ne sont pas documentés. D'ailleurs, si ces derniers venaient à quitter l'entreprise pour une quelconque raison, cette dernière perdrait toute leur expérience, car rien n'est documenté.

Par ailleurs, il ressort également que les personnes impliquées dans la conception ou la modification des SPA dans l'industrie québécoise des P&P sont généralement très limitées dans le temps pour réaliser leurs activités. Ces contraintes de temps lors de la conception aboutissent souvent à une conception non optimale et mal adaptée aux besoins réels des opérateurs et des personnes chargées de l'entretien du SPA. Ainsi, les personnes impliquées dans leur conception ou leur modification doivent par la suite consacrer du temps supplémentaire pour régler en catastrophe les problèmes identifiés, ce qui, plus tard, se transformera à nouveau en un manque de temps pour la conception ou la modification d'un autre SPA. Bref, les concepteurs dans l'industrie des P&P passent beaucoup de temps à *éteindre des feux* qu'ils ont eux même allumés.

3.2 Intégration de la SST dans la conception des SPA

Un principe reconnu est que l'intégration des aspects de SST à un système de production automatisé doit se faire aussi tôt que possible, c'est-à-dire lors de sa conception. Pour ce faire, quelques approches ont été répertoriées. Cependant, ces dernières ne sont pas applicables sous leur présente forme compte tenu des problèmes suivants :

- Premièrement, les contraintes de budget et surtout de temps sont très importantes dans l'industrie québécoise des P&P. Ce point a d'ailleurs déjà été abondamment discuté.

- Deuxièmement, aucune méthodologie de conception ou guide de conception n'est utilisé dans l'industrie québécoise des P&P. Ainsi, pour qu'une approche de conception permettant d'intégrer la sécurité puisse être implantée dans cette industrie, elle devra tenir compte du fait que les concepteurs qui l'utiliseront ne sont fort probablement pas familiers avec les approches et les outils de conception modernes qui ont été répertoriés dans la littérature. En fait, pour garantir jusqu'à un certain point que la solution développée sera effectivement utilisée, cette dernière ne devra pas trop chambarder leur pratique actuelle.

- Troisièmement, les approches de conception répertoriées recommandent des analyses du risque, mais elles ne précisent pas comment les mener. Une seule approche fait exception à la règle, celle développée par F. Gauthier [1997]. Néanmoins, les concepteurs de l'industrie québécoise des P&P ne sont pas du tout familiers avec ces méthodes d'analyse du risque. Il serait donc utopique d'espérer qu'ils réussissent à bien appliquer plusieurs de ces méthodes, du moins dans les premiers temps ; l'application adéquate de seulement quelques-unes d'entre elles serait donc déjà un grand pas pour eux.

3.3 Manque de coopération dans l'industrie québécoise des P&P

Comme établi dans l'état des connaissances, d'importants problèmes de communication ont pu être observés dans l'industrie québécoise des P&P, ce qui se traduit en bout de ligne en un manque de coopération à plusieurs niveaux. De ceci résultent plusieurs problèmes.

Le premier et le plus important est que, bien souvent, la conception du SPA ne repose sur aucune analyse des besoins fonctionnels. Le manque de consultation des opérateurs et du personnel de maintenance fait en sorte que l'élaboration des besoins fonctionnels n'est pas complète ou erronée. Certes, il arrive que les concepteurs descendent jusqu'au plancher opérationnel pour effectuer cette consultation ; cependant, cette dernière se résume souvent à l'approbation de plans. Or, les opérateurs et le personnel de maintenance n'ont généralement pas la formation et ne manifestent souvent que peu d'intérêt pour lire ces plans. Ce manque d'efficacité lors de l'élaboration des besoins fonctionnels résulte en une mauvaise adaptation du SPA aux besoins réels des utilisateurs, ce qui correspond à une situation reconnue comme étant le siège de problèmes de sécurité.

Un second problème identifié est le manque de retour d'informations suite aux diverses difficultés vécues. Par exemple, lorsque des modifications sont effectuées sur le SPA pour en accroître la fonctionnalité ou la sécurité, les concepteurs ne sont pas systématiquement mis au courant ; ces derniers risquent alors de répéter les mêmes erreurs dans leur futurs projets de conception ou de modification. Ce manque de retour d'informations est également présent entre les firmes de consultants externes et les entreprises qui font appel à leur services.

Finalement, un manque de coopération existe entre les divers spécialistes impliqués dans les projets de conception ou de modification d'un SPA. Par exemple, les ingénieurs mécaniques, qui gèrent souvent ces projets, ne prennent pas toujours en compte les demandes venant des ingénieurs électriques, des programmeurs, etc. Il en résulte souvent plusieurs réajustements de dernières minutes, un manque de vision globale du projet, des frustrations qui aggravent la communication entre ces spécialistes, etc. Les rôles de tous et chacun ne semblent donc pas être clairement définis et leur importance n'est souvent pas reconnue entre eux.

4. OBJECTIFS DES TRAVAUX DE RECHERCHE

Ce chapitre présente les divers objectifs poursuivis par ce projet de recherche. Dans un premier temps, l'objectif principal est formulé. Par la suite, les objectifs intermédiaires viennent préciser comment il sera possible d'atteindre cet objectif principal.

4.1 Objectif principal

Compte tenu de la problématique qui se dégage de l'état des connaissances, l'objectif principal de ce projet de recherche sera de **développer une approche de conception qui sera exploitable par les concepteurs de l'industrie québécoise des pâtes et papiers et qui leur permettra de rendre plus sécuritaires l'opération et la maintenance des systèmes de production automatisés dotés de technologies programmables.**

Pour que cet objectif soit atteint, plusieurs objectifs intermédiaires sont établis de telle sorte que l'ensemble des problèmes identifiés dans l'état des connaissances et rappelés au chapitre 3 puissent être résolus.

4.2 Objectifs intermédiaires

4.2.1 Adapter l'approche aux pratiques des concepteurs de l'industrie québécoise des P&P

Une des problématiques soulevées est que la conception dans cette industrie ne relève d'aucune méthodologie claire et documentée ; elle est plutôt basée sur l'expérience de tous et chacun. En fait, la plupart d'entre eux ne connaissent pratiquement aucune approche ou outil de conception moderne. Ainsi, pour que l'approche développée ait toutes les chances d'être réellement exploitée, elle devra être évolutive et par le fait même s'adapter à leur réalité. Par ailleurs, il est évident qu'un processus de conception établi et bien documenté, tel que celui de l'ingénierie simultanée, serait un atout considérable pour cette entreprise. Cependant, l'imposer dès le départ à ces concepteurs pourrait être en quelque sorte une garantie d'échec. Ainsi, **l'approche proposée devra, dans un premier temps, permettre aux concepteurs de l'industrie québécoise des P&P de l'assimiler d'une façon évolutive, quitte à ce qu'elle leur permette d'évoluer vers des pratiques de conception mieux définies et documentées lorsqu'ils en sentiront le besoin.**

4.2.2 Optimiser l'efficacité des activités de conception en terme de temps

Compte tenu des contraintes de temps auxquelles sont soumis les concepteurs de l'industrie québécoise des P&P, l'approche développée devra être efficace en terme de temps. Certes, les concepteurs pourraient être appelés à consacrer un peu plus de temps lors de la conception du SPA, mais compte tenu du fait que cette conception devrait être plus élaborée, le temps qu'ils investissent habituellement pour effectuer les modifications en cours de construction, d'installation et d'exploitation devrait être réduit. Ainsi, en bout de ligne, l'approche développée ne devrait pas allonger significativement le temps nécessaire à la réalisation de leur projet. En résumé, **l'approche développée devra optimiser l'efficacité des activités de conception en terme de temps** et faire en sorte que le temps total pour la réalisation d'un projet ne soit pas significativement allongé.

4.2.3 Intégrer les méthodes d'analyse du risque

L'intégration des méthodes d'analyse du risque aux activités de conception est à la base des principes de conception sécuritaire. L'approche développée devra donc suggérer l'application de méthodes d'analyse du risque spécifiques à chacune des étapes de conception. Par ailleurs, considérant la quantité de méthodes d'analyse du risque, une sélection parmi celle-ci devra être faite afin d'identifier les méthodes les plus susceptibles d'aider les concepteurs. Cependant, l'application de ces méthodes implique que les concepteurs de l'industrie québécoise des P&P doivent connaître et maîtriser ces dernières avant même de les utiliser dans leurs activités de conception. Ainsi, **étant donné que ces concepteurs ne connaissent pratiquement pas ces méthodes et considérant le temps qu'ils devront investir pour se familiariser avec elles, le nombre de ces dernières devra être peu élevé.** Par exemple, l'utilisation d'une liste de contrôle (*check list*) pourrait, surtout lors des premières applications de la méthode, s'avérer très intéressante.

4.2.4 Augmenter la coopération

Comme il est largement reconnu que la coopération entre tous les intervenants dans un projet de conception permet d'accroître la qualité de cette dernière, **l'approche développée devra favoriser cette coopération**, tout en tenant compte des problèmes de communication identifiés au chapitre 2.

4.2.5 Permettre aux concepteurs de tirer profits de leurs expériences

Finalement, le dernier objectif intermédiaire établi est de **faire en sorte que l'approche développée permette aux concepteurs des retours d'expérience**, c'est-à-dire des problèmes de conception vécus par eux, par leur collègue, voire même par les concepteurs des firmes externes ou des compagnies compétitrices.

5. SOLUTION PROPOSÉE

Ce chapitre présente l'ensemble des solutions proposées par le candidat en vue de répondre aux objectifs de la recherche. Aussi, pour l'élaboration des solutions, deux hypothèses ont dû être formulées et tous les résultats proposés reposent sur ces dernières. Ce chapitre présente dans un premier temps ces hypothèses. Ensuite, la structure globale de l'approche est exposée et comme elle réfère à trois guides de conception, chacun de ces derniers est présenté dans les trois dernières sections de ce chapitre.

5.1 Hypothèses de base

Règle générale, les principes techniques de réduction du risque (section 2.2.5) sont passablement bien connus des concepteurs de l'industrie québécoise des P&P, ou du moins, ces derniers peuvent assez facilement obtenir de l'information, voire même de la formation concernant ces principes techniques auprès de leurs fournisseurs. Cependant et compte tenu de la problématique qui se dégage de l'état des connaissances, l'intégration systématique des besoins fonctionnels de même que des activités pour la gestion du risque semblent poser un plus gros défi pour ces mêmes concepteurs. Ainsi, la première hypothèse formulée est qu'une approche principalement axée sur l'analyse des besoins fonctionnels et sur la gestion du risque devrait être très profitable pour les concepteurs de l'industrie québécoise des P&P. En effet, une approche permettant d'améliorer ces deux points de vue permettrait à ces concepteurs de développer des SPA mieux adaptés aux besoins des utilisateurs, ce qui contribue directement à rendre plus sécuritaire leur opération et leur entretien. L'approche développée sera donc entièrement consacrée à l'intégration des techniques pour l'analyse des besoins fonctionnels et pour la gestion du risque.

Par ailleurs et comme mentionné dans l'état des connaissances, aucune méthodologie de conception claire et documentée n'est appliquée dans l'industrie québécoise des P&P. Toutes les activités de conception sont basées sur l'expérience des concepteurs. Par contre, comme la plupart des usines réalisent sensiblement les mêmes étapes pour la conception d'un SPA, il est possible d'établir un processus de réalisation de projet (PRP) très général regroupant l'ensemble

de ces activités. La seconde hypothèse posée est donc que le PRP illustré à la figure 5.1 représente adéquatement les activités de conception qui ont pu être observées dans cette industrie.

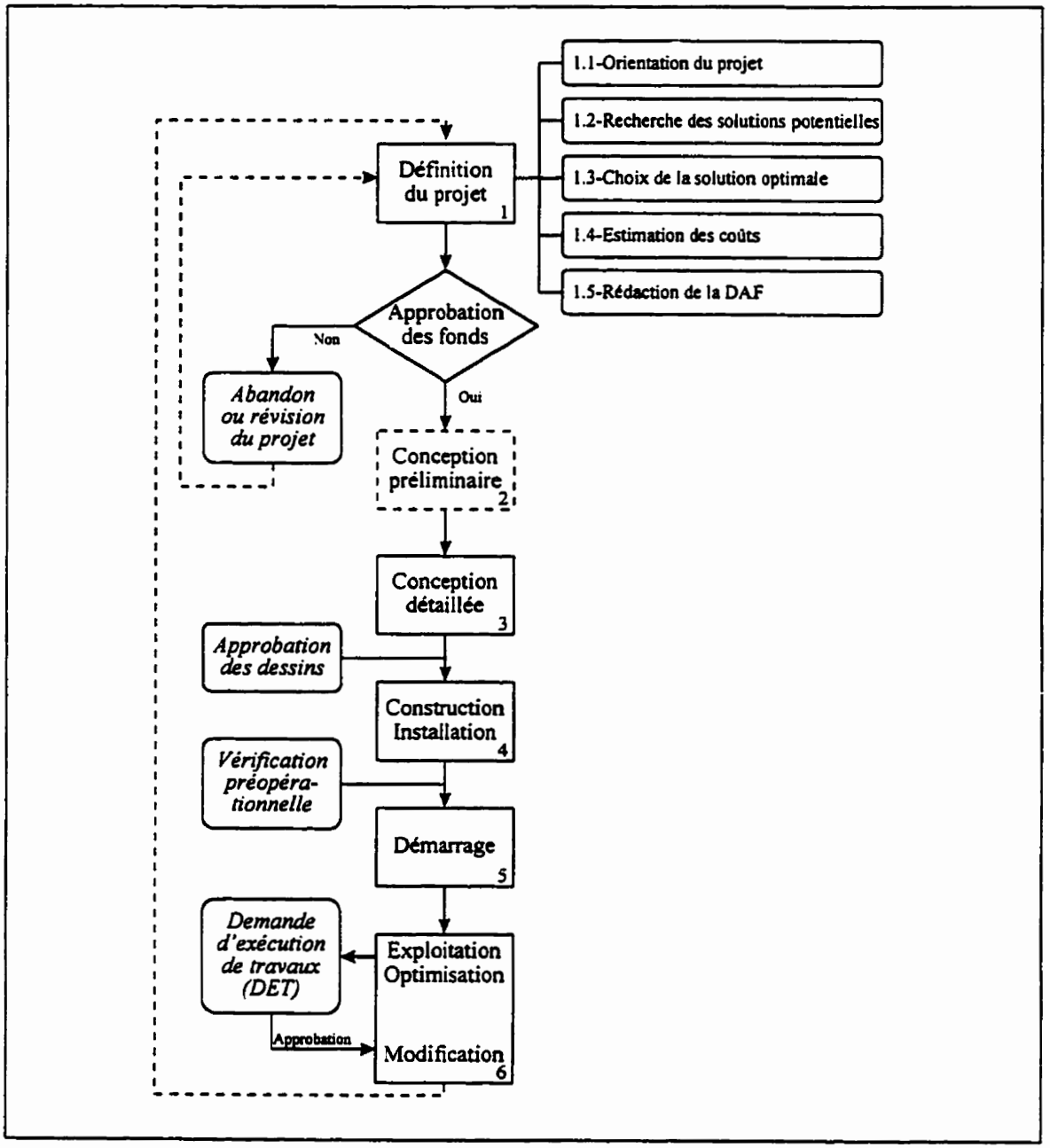

Figure 5.1 PRP représentant les activités de conception de l'industrie québécoise des P&P

5.1.1 Définition du projet

L'objectif principal de cette première étape est de préparer la demande d'approbation de fonds (DAF). Toutes les usines visitées doivent produire ce document (ou un document similaire), car c'est en se basant sur ce dernier que la direction décide d'accorder ou non les fonds nécessaires pour la réalisation du projet. L'étape de la définition du projet est typiquement composée de cinq activités qui sont présentées dans les sections qui suivent.

5.1.1.1 Orientation du projet

Lorsqu'une demande de projet est émise, soit par les superviseurs départementaux (opération, entretien, etc.) ou par l'ingénierie, cette dernière procède habituellement à une première analyse en vue de déterminer l'ampleur et la nature du projet. Suite à cette analyse, l'ingénierie est en mesure de décider de faire appel ou non à une firme de consultants externe et forme ensuite l'équipe de projet. Généralement, cette équipe est composée d'un ingénieur mécanique (souvent désigné comme chargé de projet) et des représentants des départements concernés par le projet (opération, entretien, instrumentation, électricité, etc.). Une fois l'équipe de projet formée, une analyse sommaire des besoins fonctionnels est faite. Il n'y a pas d'analyse du risque.

5.1.1.2 Recherche des solutions potentielles

Une fois les grandes orientations établies, l'équipe de projet recherche diverses solutions pouvant répondre aux besoins qui sont à l'origine de la demande. Pour les aider dans cette étape, il n'est pas rare que quelques individus effectuent des visites dans d'autres usines ou chez des fabricants d'équipements similaires à ce qu'ils recherchent. Quelques usines ont mentionné qu'elles font participer à l'occasion des opérateurs, des mécaniciens, des électriciens et même parfois des représentants de la SST à ces visites.

5.1.1.3 Choix de la solution optimale

Une fois que l'équipe de projet a pu se faire une idée des solutions possibles, elle prend une décision quant à la solution représentant le plus de potentiel. Cependant, cette décision repose

principalement sur le coût et sur la performance des solutions identifiées. Les besoins fonctionnels et le niveau de sécurité du SPA sont des aspects rarement pris en considération.

5.1.1.4 Estimation des coûts

À partir du moment où la solution est connue, l'estimation des coûts est effectuée. Bien qu'une consultation quasi systématique des diverses expertises (ingénierie mécanique, électrique, civile, etc.) est effectuée dans la plupart des usines, les informations recueillies permettent d'affirmer que ce n'est pas toujours le cas pour tous les projets.

5.1.1.5 Rédaction de la demande d'approbation de fonds (DAF)

Une fois que les coûts qu'engendrerait la réalisation du projet sont connus, la demande d'approbation de fonds (DAF) peut être rédigée. Il s'agit d'une étape critique dans tous les projets de conception de l'industrie québécoise des P&P, car c'est en se basant sur la DAF que la direction de l'usine décide si le projet sera réalisé ou non. Si la DAF est refusée, l'équipe de conception doit ou bien réviser son projet, ou bien tout simplement l'abandonner. De même, si la DAF est acceptée, le projet doit démarrer et l'équipe de conception a alors l'obligation de respecter son contenu, c'est-à-dire les budgets et les échéanciers qui ont été soumis à la direction. Il est donc essentiel que les étapes menant à la DAF soient réalisées avec la plus grande diligence possible, car tout le reste du projet de conception devra respecter son contenu.

Par contre, tant et aussi longtemps que les fonds ne sont pas octroyés par la direction, l'équipe n'a aucune garantie que leur projet sera réalisé ; elle n'a donc aucun intérêt à détailler davantage la définition du projet. Il en résulte que les besoins fonctionnels ne sont analysés que sommairement et que les aspects de SST ne sont que rarement considérés lors de la définition du projet. Une difficulté majeure est à ce moment-ci soulevée : après l'approbation des fonds, l'équipe de conception doit respecter les échéanciers et les budgets proposés dans la DAF. Ainsi, une fois que la DAF a été approuvée, il peut arriver au cours de la réalisation du projet que l'équipe de conception, même si elle découvre des problèmes évidents de sécurité, soit contrainte à appliquer les solutions préétablies, compte tenu des limitations de temps et d'argent auxquelles elle doit se soumettre. Certes, ces problèmes de sécurité seront corrigés ultérieurement. Par

exemple, une fois que l'installation du SPA est terminée, il sera possible de puiser dans les budgets de maintenance pour effectuer les modifications nécessaires. Néanmoins, cette procédure entraîne souvent des pertes de temps et d'argent pour l'entreprise.

Il serait donc avantageux pour tous que la DAF soit aussi complète que possible, tout en faisant en sorte que l'équipe de conception n'y consacre pas trop de temps étant donné que leurs efforts pour définir adéquatement le projet pourraient ne pas porter fruit si la direction n'octroie pas les fonds demandés.

5.1.2 Conception préliminaire

Selon la figure 5.1, la seconde étape à être parfois réalisée est la conception préliminaire. Lorsqu'elle est effectuée, c'est généralement très rapidement et par l'équipe de conception[21]. Au cours de cette étape, des versions préliminaires de certains documents majeurs sont ébauchées, comme les bilans de masse, les diagrammes de processus et d'instrumentation (P&ID, *process and instrumentation diagram*), etc. Généralement, les objectifs poursuivis sont alors de mieux connaître les étapes à réaliser, de mieux orienter la conception, de préciser l'échéancier, etc. L'analyse des besoins fonctionnels n'est généralement pas approfondie et aucune analyse du risque n'est effectuée.

5.1.3 Conception détaillée

Très souvent, immédiatement après l'approbation des fonds, l'équipe de conception entreprend la conception détaillée de la solution retenue lors de la définition du projet. C'est au cours de cette étape que le SPA entier sera pensé et élaboré. Habituellement, les documents en rapport avec le processus (comme les bilans de masse, les P&ID, etc.) sont finalisés à cette étape. Par la suite, l'aspect mécanique du projet est développé : dessins d'ensemble et de détail, choix des équipements principaux, etc. Parallèlement aux travaux des ingénieurs en mécanique, les activités d'ingénierie civile et électrique de même que celles reliées au tuyautage sont accomplies.

---

[21] Cette étape n'est pas réalisée par toutes les usines visitées. C'est d'ailleurs pour cette raison que son cadre sur la figure 5.1 est en tirets.

Finalement, une fois que tous les dessins mécaniques sont terminés, l'équipe de projet procède généralement à une étape de validation de leur conception. Cette dernière se résume habituellement à présenter les dessins d'ensemble aux opérateurs, au personnel de maintenance et parfois aux représentants de la SST dans le but que ces derniers apportent les correctifs nécessaires. Cependant, il arrive fréquemment que ces personnes ne sachent pas comment lire de tels dessins et, bien souvent, elles ne manifestent que peu d'intérêt pour ce type de participation au projet. Ainsi, bien qu'elles ne parviennent pas à identifier les problèmes, elles donnent leur accord à l'équipe de projet qui décide alors de procéder à la construction du SPA.

5.1.4 Construction et installation

C'est au cours de cette étape que le SPA prendra vie. Il sera construit tel que spécifié par l'équipe de projet. Dans la majorité des cas, la construction et l'installation des équipements s'effectuent par des entrepreneurs spécialisés, externes à l'entreprise. Aussi, c'est au cours de cette étape que la numérotation des équipements, la planification de l'entretien et l'élaboration des fiches pour la consignation des équipements débutent. Par ailleurs, c'est à ce moment-ci que les plus grandes considérations sont portées à la sécurité ; cependant, celles-ci se limitent souvent à l'application des consignes de sécurité pour les chantiers de construction.

Finalement, une fois que tous les équipements sont installés, une étape de vérification préopérationnelle est effectuée pour tous les projets. Pour la réaliser, l'équipe de conception (comprenant les consultants externes le cas échéant) aidée des opérateurs et du personnel d'entretien vérifie que tous les équipements mécaniques peuvent effectuer leur mouvement, que tous les raccords électriques sont adéquats et relient les bons équipements aux bons disjoncteurs, etc. C'est également à ce moment que tous les programmes (pour les API et/ou les SCD) sont vérifiés, souvent ligne par ligne, en vue de s'assurer que le SPA fonctionnera tel que prévu. D'autre part, comme c'est la dernière étape avant le démarrage et qu'il y a souvent des retards accumulés au cours des étapes antérieures, cette vérification s'effectue de manière très intense pour respecter les échéanciers. Ainsi, les personnes y oeuvrant travaillent sous pression et sont souvent très fatiguées en raison des nombreuses heures supplémentaires consacrées ; des erreurs et des oublis peuvent donc en résulter, ce qui pourrait engendrer des nouveaux phénomènes dangereux.

5.1.5 Démarrage

Lors de cette étape, tous les équipements sont mis en marche de manière progressive. Il est en effet très rare que le SPA tout entier soit mis en opération ; ce sont plutôt des parties du système formant un circuit qui sont mises en marche une à la suite de l'autre, ce qui permet à l'équipe de projet de mieux contrôler les opérations advenant le cas où une anomalie serait détectée.

Finalement, il est essentiel de rappeler que le démarrage d'un nouvel équipement est un événement générant beaucoup de stress à l'équipe de projet et que les membres de cette dernière travaillent encore sous pression alors qu'ils sont exténués. Comme mentionné par plusieurs personnes lors des entrevues en usine, *«il n'y a pas souvent d'accidents lors du démarrage, mais c'est uniquement une question de chance, parce qu'on est vraiment très fatigué»*.

5.1.6 Exploitation, optimisation et modification

Une fois que le SPA est entièrement opérationnel, son exploitation normale débute. Dans les premiers temps, plusieurs modifications et plusieurs ajustements sont nécessaires pour optimiser sa production. De plus, les problèmes identifiés lors de la construction, de l'installation ou du démarrage sont alors résolus. Aussi, maintenant que le SPA est en opération, il est souvent plus facile d'identifier les phénomènes dangereux présents (angle entrant sans protection, accès difficile pour l'ajustement ou l'entretien d'un équipement, bouton d'arrêt d'urgence manquant, etc.). Par ailleurs, peu importe l'ampleur des modifications devant être faites, il y a toujours une *demande d'exécution de travaux* (DET) qui est remplie pour décrire ce qui doit être fait, ce qu'il en coûtera, qui le fera et quand il faudra le faire. Cependant, lorsqu'il s'agit de modifications mineures (ajout d'un garde protecteur par exemple), il arrive souvent que l'ingénierie n'ait pas à intervenir : dans ces cas, les dessins ne sont pas modifiés et, bien souvent, elle n'est pas informée des modifications apportées. Finalement, lorsque les modifications devant être apportées sont majeures, une nouvelle demande de projet est parfois faite et toutes les étapes du PRP présentées sont alors réalisées à nouveau ; c'est ce qu'illustre la flèche de retour en tirets à la figure 5.1.

5.2 Structure globale de la solution proposée

La solution élaborée est un document de référence pour la conception basé sur le PRP typique décrit précédemment (figure 5.1). Ainsi, l'ensemble des activités de conception habituellement rencontrées dans les papetières du Québec sont intégrées systématiquement dans ce document. Aussi, de nouvelles activités ont été ajoutées pour tenir compte des objectifs de cette recherche. En accord avec la première hypothèse formulée, ces activités visent principalement l'analyse des besoins fonctionnels et la gestion du risque.

Pour simplifier l'intégration de ces dernières activités, trois guides de conception ont été développés, soit le *guide pour l'analyse des besoins fonctionnels*, le *guide pour la gestion du risque* et le *guide pour les revues de sécurité*. Ainsi, lorsque les activités de conception décrites dans le document de référence sont, par exemple, en relation avec la gestion du risque, une indication spéciale est donnée au concepteur pour qu'il se réfère au guide pour la gestion du risque. Il en est de même pour les autres guides. La figure 5.2 présente la structure de ce document de référence.

Par ailleurs, comme un des objectifs intermédiaires vise à faire en sorte que les concepteurs de l'industrie québécoise des P&P puissent assimiler progressivement l'approche, les guides de conception ont été développés en tenant compte de ce fait. Ainsi, chacun d'eux permet l'intégration des nouvelles activités de conception selon deux niveaux de difficulté de mise en oeuvre. Au premier niveau, l'utilisation d'outils et de principes simples est davantage suggérée. Par exemple, l'élaboration de listes de contrôle (*checklist*) pour la recherche des besoins fonctionnels et pour l'identification des phénomènes dangereux est recommandée. Pour ce qui est du second niveau, des outils beaucoup plus performants, mais tout de même plus difficiles à mettre en oeuvre, sont suggérés. Par exemple, l'analyse fonctionnelle est entre autres recommandée au second niveau du guide pour l'analyse des besoins fonctionnels.

Finalement, la structure de l'approche permet aux concepteurs d'améliorer continuellement leur pratique de conception en rendant possible l'intégration des retours d'expérience. Ainsi, la

structure des guides de conception est telle que ses utilisateurs peuvent ajouter ou enlever toute sorte d'informations pertinentes, selon les expériences vécues ou à vivre.

La figure suivante présente donc la structure générale du document de référence proposé pour la conception sécuritaire des SPA. Elle met aussi en relief les références aux trois guides de conception aux cours des diverses activités.

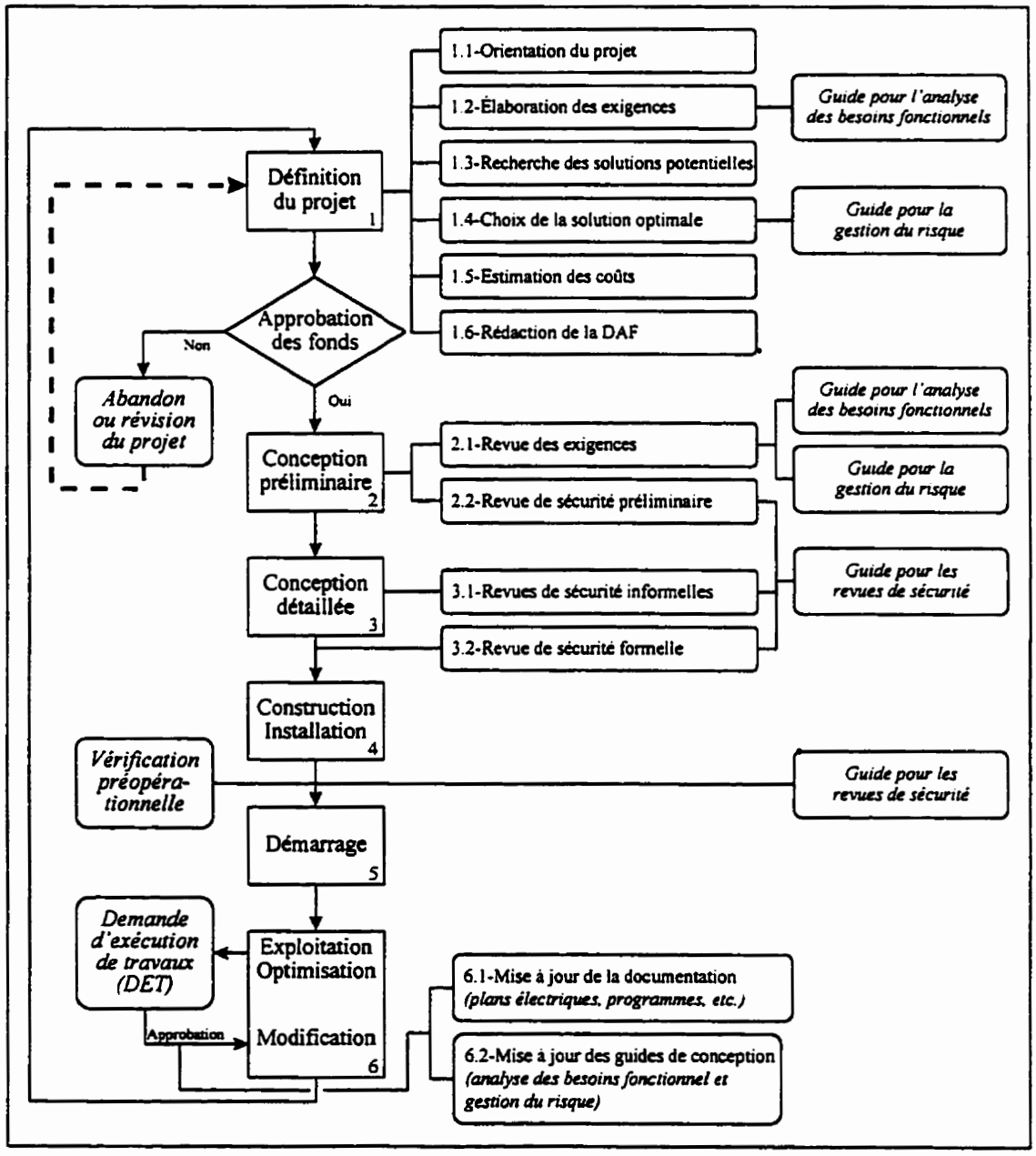

Figure 5.2 Structure générale du document de référence proposé

Les paragraphes qui suivent décrivent l'ensemble des activités de conception prévues dans le document de référence alors que les trois dernières sections de ce chapitre présentent les trois guide de conception développés.

5.2.1 Définition du projet

Pour la définition du projet, des activités spécifiques ou des recommandations en rapport avec l'organisation des activités de conception ont été apportées aux cinq activités présentées à la figure 5.1. De plus, une sixième activité a été ajoutée afin de prendre en compte les besoins fonctionnels liés à l'exploitation et à l'entretien du SPA : il s'agit de l'*élaboration des exigences*.

5.2.1.1 Orientation du projet

Une fois que les grandes orientations du projet ont été établies (généralement suite à une série de rencontres entre l'ingénierie et la direction), une étape importante de cette activité est la formation de l'équipe de projet qui, pour favoriser la coopération à tous les niveaux, devrait être multidisciplinaire. Ainsi, l'équipe devrait comprendre des opérateurs, des mécaniciens, des ingénieurs de système, des électriciens, etc. Aussi, des représentants de la SST devraient y être intégrés. Bref, au moins un représentant de toutes les disciplines pouvant être appelées à interagir de près ou de loin avec le SPA à concevoir, devraient faire partie de l'équipe de projet. Cependant, il est important de comprendre que cette équipe ne participera pas activement à toutes les activités de conception prévues. Elle participera plutôt à quelques unes et elle pourra offrir un support à l'ingénierie pour, notamment, les aspects de fonctionnalité et de SST. En fait, elle pourrait être vue comme une équipe consultative.

5.2.1.2 Élaboration des exigences

Comme établi dans l'état des connaissances, une cause commune d'accidents est la mauvaise adaptation des SPA aux besoins des personnes devant interagir de près ou de loin avec ces derniers. Pour remédier à cette situation, il est donc très important d'établir le plus tôt possible les principaux besoins fonctionnels de l'équipement à concevoir. Aussi, tel qu'indiqué sur la figure 5.2, il est prévu à ce moment-ci que les concepteurs utilisent le *guide pour l'analyse des*

besoins fonctionnels. Ce dernier est présenté à la section 5.3 de ce chapitre. Une fois que tous les principaux besoins fonctionnels rattachés au SPA à concevoir ont été identifiés, ces derniers doivent être inscrits sur la *liste des exigences*. Cette dernière deviendra au fur et à mesure de l'avancement du projet une référence pour toutes les spécifications de fonctionnalité et de sécurité, un peu comme un cahier des charges.

5.2.1.3 Recherche des solutions potentielles

Lors de cette étape, l'équipe de projet doit rechercher diverses solutions pouvant répondre aux objectifs du projet et aux besoins fonctionnels identifiés précédemment. Cette recherche peut se faire en consultant divers fournisseurs, en effectuant des visites dans d'autres usines (*benchmarking*), etc. Idéalement, l'équipe de projet devrait s'efforcer de trouver le plus grand nombre de solutions potentielles de manière à avoir l'embarras du choix lors de la sélection finale.

5.2.1.4 Choix de la solution optimale

Une fois que l'équipe de projet a identifié autant de solutions (ou de concepts) que possible, elle doit maintenant choisir parmi ces dernières celle qui semble être la meilleure. Le candidat recommande que cette sélection soit basée sur l'évaluation systématique de chacun des concepts par rapport à des critères bien établis. À ce sujet, plusieurs ouvrages traitant des techniques de convergence existent et devraient être consultés pour permettre à l'équipe de projet de faire une sélection plus éclairée [DOUCET, P., 1997] [LEMAY, É. et coll., 1997] [PROULX, D., 1995]. Par ailleurs et comme indiqué plus tôt, des considérations de performance et de coût motivent habituellement le choix de la solution optimale. Le candidat recommande que cette sélection repose en plus sur deux autres considérations : la satisfaction des principaux besoins fonctionnels et le niveau de sécurité offert par la solution.

Pour ce faire, il pourrait être intéressant dans un premier temps de donner une certaine hiérarchie aux besoins fonctionnels inscrits dans la liste des exigences de manière à ce que le choix de la solution repose sur les plus importants d'entre eux. Cette façon de procéder devrait faire en sorte que le concept choisi soit mieux adapté aux besoins réels d'exploitation et d'entretien du SPA, ce

qui devrait se traduire, selon l'équipe de R. Bélanger [1991], par une diminution du risque d'accidents.

Dans un second temps, l'équipe de projet devrait à ce moment-ci effectuer une première analyse du risque. Pour ce faire, les concepteurs doivent s'en remettre au guide pour la gestion du risque présenté à la section 5.4. Deux objectifs sont poursuivis par cette première analyse du risque. Le premier est de permettre à l'équipe de conception de s'assurer que la solution privilégiée est passablement sécuritaire. Le second est de faire en sorte que les coûts associés aux modifications nécessaires pour rendre le SPA sécuritaire seront pris en considération lors de l'estimation des coûts.

Finalement, il est fort probable que la solution privilégiée ne soit pas entièrement conforme aux besoins fonctionnels inscrits sur la liste des exigences et que son niveau de sécurité ne soit pas assez élevé. Toutes les modifications qui s'imposeront alors pour rendre la solution retenue sécuritaire et conforme aux besoins fonctionnels devront être ajoutées à la *liste des exigences*.

5.2.1.5 Estimation des coûts

L'unique but de cette étape est d'estimer, aussi précisément que possible, les coûts qu'engendrera le projet. Pour obtenir de bons résultats, il est alors essentiel de consulter les experts de chaque discipline : ingénieur civil, ingénieur électrique, ingénieur mécanique, fournisseurs, etc. Finalement, le candidat rappelle qu'un oubli lors de l'estimation des coûts pourrait contraindre l'équipe de projet à fonctionner avec un budget insuffisant.

5.2.1.6 Rédaction de la demande d'approbation de fonds (DAF)

L'étape finale de la *définition du projet* est la rédaction de la DAF. Ce document devrait contenir au minimum la définition du projet, la liste des exigences, la solution finale proposée et l'estimation de tous les coûts qu'engagerait la réalisation du projet.

Finalement, une fois que la DAF est rédigée, le candidat recommande que tous les membres de l'équipe de projet la signent comme quoi ils ont pris connaissance de son contenu.

5.2.2 Conception préliminaire

Comme mentionné plus tôt, cette étape n'est pas réalisée dans toutes les entreprises. Ainsi, très souvent, dès que les fonds sont octroyés, l'équipe de projet passe directement à la conception détaillée. Néanmoins, le candidat soutient qu'il est important de réaliser les deux activités présentées à la figure 5.2 de manière à ce que l'équipe de projet soit certaine que l'ensemble des exigences de fonctionnalité et de sécurité a été établi et que des solutions ont été élaborées pour rendre le concept retenu conforme à ces exigences.

5.2.2.1 Revue des exigences

Cette première activité devrait se dérouler immédiatement après l'approbation de la DAF et l'équipe de projet entière devrait y participer. L'objectif de cette activité est de s'assurer que toutes les exigences en rapport avec le SPA à concevoir (besoins fonctionnels, contraintes, solutions pour maîtriser les phénomènes dangereux, etc.) ont été identifiées et sont toujours pertinentes. Pour ce faire, le guide pour l'analyse des besoins fonctionnels et celui pour la gestion du risque doivent être utilisés. À la suite de cette revue, la liste des exigences devra être mise à jour, car elle deviendra un document de référence servant à diriger la conception, un peu comme un cahier des charges.

5.2.2.2 Revue de sécurité préliminaire

Cette seconde activité consiste à valider la solution retenue en s'assurant qu'elle réponde à toutes les exigences listées. Pour cette revue, plusieurs intervenants externes à l'équipe de projet (d'autres opérateurs, d'autres mécaniciens, etc.) pourraient participer. Le guide pour les revues de sécurité (section 5.5) doit alors être utilisé. Par ailleurs, plusieurs petites modifications pourraient résulter de cette activité (comme l'ajout de boutons d'arrêt d'urgence, l'ajout d'un panneau de commande, etc.). Ces modification devraient rendre le SPA conforme aux diverses exigences listées. Il va sans dire que ces modifications soient clairement documentées de manière à ce qu'elles soient considérées dans les étapes suivantes.

5.2.3 Conception détaillée

C'est au cours de cette étape que les solutions trouvées seront définies dans les moindres détails. Habituellement, les activités de cette étape relève principalement de l'ingénierie. Aussi, les principaux problèmes rencontrés lors de la réalisation de cette étape ne sont pas d'ordre technique : ce sont plutôt des problèmes de communication. Comme établi dans l'état des connaissances, pour valider leur conception, l'ingénierie présente souvent les plans à quelques intervenants, comme les opérateurs, le personnel d'entretien, etc. Cependant, ces derniers n'ont souvent pas l'habitude de lire des plans aussi complexes si bien qu'ils devraient investir beaucoup plus de temps et d'énergie pour bien les comprendre. Or, règle générale, ils n'ont souvent pas le temps pour le faire. Conséquemment, la validation de la conception détaillée faite par l'ingénierie sous forme d'approbation de dessin (voir figure 5.1) s'avère très souvent inefficace. Par contre, cette situation peut être corrigée en partie par les activités proposées dans les étapes précédentes. En effet, comme l'équipe de projet – formée entre autres d'opérateurs, du personnel d'entretien et de représentants de la SST – a suivi d'assez près l'élaboration des solutions préliminaires, elle connaît déjà très bien le projet lorsque la conception détaillée est effectuée. Ainsi, contrairement aux pratiques traditionnelles, l'équipe de projet pourra mieux valider les travaux effectués par l'ingénierie. Cependant, le candidat soutient qu'une seule validation faite à la toute fin de la conception détaillée n'est pas la situation idéale. En effet, si l'équipe de projet procédait à des consultations fréquentes tout au long de cette étape, elle pourrait mieux suivre l'évolution du projet et le nombre de modifications finales serait moins élevé étant donné que la conception serait régulièrement révisée et tenue à jour. Les deux activités suggérées dans la figure 5.2 permettent ce mode de validation et remplace l'*approbation des dessins* traditionnellement réalisée.

5.2.3.1 Revues de sécurité informelles

Les revues informelles sont caractérisées par une approche non structurée. Typiquement, ces revues ont lieu spontanément, autour de la table à dessin ou de l'écran avec un système de DAO (dessin assisté par ordinateur) où un ou plusieurs membres de l'équipe de projet (principalement des opérateurs et du personnel de maintenance) répondent aux questions du ou des concepteurs

dans le but de valider leur conception [MURRAY, A., 1996]. L'objectif de ces revues de sécurité informelles est donc de permettre à l'équipe de suivre l'évolution du SPA et d'offrir par ailleurs des informations supplémentaires à l'ingénierie leur permettant de mieux orienter leurs activités de conception. Pour les réaliser, les concepteurs doivent se référer au guide pour les revues de sécurité (section 5.5).

5.2.3.2 Revue de sécurité formelle

Une fois que la conception détaillée est terminée, une revue de sécurité formelle portant sur le SPA entier ou sur chacun de ses systèmes doit être menée. L'objectif premier de cette revue est de s'assurer que le SPA développé respecte l'ensemble des exigences établies. Cette revue de sécurité doit avoir lieu à une date prédéterminée et doit être conduite selon une approche structurée et systématique. Toute l'équipe de projet doit y assister. Aussi, il est recommandé que la revue soit présidée par une personne de l'ingénierie autre que le chargé de projet et qui n'est pas en lien d'autorité avec ce dernier [MURRAY, A., 1996]. Par ailleurs, une pratique assez courante pour ce type de revue de sécurité est l'utilisation d'une liste de contrôle – qui pourraient être la liste des exigences – pour faciliter la participation du comité de revue. Ainsi, tous les aspects importants de la conception seront couverts par cette démarche. Encore là, les concepteurs doivent se référer au guide pour les revues de sécurité pour réaliser cette étape. Finalement, lorsque les correctifs aux plans ont été apportés, la construction et l'installation des équipements peuvent être amorcées.

5.2.4 Construction et installation

Aucune activité supplémentaire à celles déjà pratiquées n'est proposée pour cette étape.

5.2.5 Démarrage

Comme l'indique la figure 5.1, lorsque l'installation du SPA est terminée, une vérification préopérationnelle est réalisée dans toutes les usines visitées. Cette vérification est habituellement menée de façon systématique et fait appel à des personnes de plusieurs disciplines. En plus de l'aspect technique qui est très étudié, quelques énergies sont également consacrées à l'aspect fonctionnel de même qu'à l'aspect sécuritaire. La difficulté majeure rencontrée au cours de cette

activité est très souvent un manque de temps découlant du non respect des échéanciers. À l'avis du candidat, bien qu'une meilleure planification des activités de conception pourrait aider l'équipe de projet à respecter l'échéancier, l'utilisation de listes de contrôle décrivant l'ensemble des points à valider lors de cette vérification préopérationnelle rendrait cette dernière plus systématique et probablement plus efficace[22]. Par ailleurs, le candidat recommande qu'une dernière revue de sécurité soit réalisée au cours de cette étape.

5.2.6 Exploitation, optimisation et modification

Lorsque des modifications doivent être apportées au SPA, il serait très intéressant que le même processus de réalisation de projet soit systématiquement emprunté, car ces modifications sont souvent effectuées à l'improviste ; leur conception étant mal pensée, les solutions qui en découlent sont souvent inefficaces. Cette procédure ferait donc en sorte que les modifications apportées soient mieux adaptées aux besoins des utilisateurs et du personnel d'entretien. La flèche de retour reliant les *modifications* à la *définition de projet* (en tirets sur la figure 5.1 et en ligne continue sur la figure 5.2) indique cette recommandation. Finalement, il est très important que, suite à l'approbation d'une DET, les modifications qui seront apportées au SPA soient documentées ; une activité (la *mise à jour de la documentation*) est donc prévue à cet effet[23]. Il est également prévu que le contenu de chacun des guides de conception soit mis à jour.

---

[22] Ces listes de contrôle pourraient par exemple comporter des points spécifiques à la programmation, à l'identification des équipements, au bon fonctionnement mécanique, etc. Pour ce qui est des aspects de fonctionnalité et de SST, la liste des exigences pourrait servir de liste de contrôle pour cette vérification préopérationnelle.

[23] Par documentation, le candidat fait référence aux plans mécaniques, aux schémas électriques, aux listings de programmes, etc.

5.3 Guide pour l'analyse des besoins fonctionnels

Comme l'indique la figure 5.2, les concepteurs doivent se référer au guide pour l'analyse des besoins fonctionnels lors de la définition du projet et lors de la conception préliminaire. L'objectif principal de ce guide de conception est de permettre à l'équipe de projet d'établir l'ensemble des besoins fonctionnels liés au SPA.

5.3.1 Utilisation du guide lors de la définition du projet

Lors de la définition du projet, il est prévu que les concepteurs utilisent ce guide pour l'*élaboration des exigences* (activité 1.2 de la figure 5.2). Au cours de cette étape, un document important doit être établi. Il s'agit de la *liste des exigences* dans laquelle l'ensemble des besoins fonctionnels liés à l'opération et à l'entretien du SPA sont entre autres transcrits. Cette liste, dont le concept est détaillé un peu plus loin, sera utilisée et complétée tout au long des autres activités de conception, un peu comme un cahier des charges.

5.3.1.1 Objectif

À ce stade-ci de la conception, l'objectif à atteindre est de mettre en relief les principaux besoins fonctionnels liés à l'opération et à l'entretien du SPA. Il est important de rappeler que tant et aussi longtemps que la DAF n'est pas approuvée par la direction, les efforts investis pour cette étape pourraient ne pas porter fruits ; l'équipe de projet ne devrait donc pas y consacrer trop de temps. Néanmoins, si l'élaboration des exigences n'est pas assez détaillée, la solution qui sera retenue pourrait être mal adaptée aux besoins des utilisateurs ; l'équipe de projet doit donc réaliser cette étape de manière consciencieuse sans toutefois faire un excès de zèle.

5.3.1.2 Mise en oeuvre

Comme annoncé précédemment, chacun des guides de conception suggèrent des solutions de deux niveaux de complexité de mise en oeuvre, le premier niveau étant le plus simple et le plus rapide à mettre en oeuvre alors que le second est plus complexe, mais également plus complet. Voici donc les solutions proposées pour ces deux niveaux de difficulté.

a) Niveau 1

Le premier niveau de la solution pour l'élaboration des exigences se résume au développement et à l'exploitation d'une liste de contrôle (*checklist*) dans laquelle figure une série de besoins fonctionnels typiquement spécifiés pour l'opération et l'entretien des SPA.

La toute première activité devant être réalisée, et ce, au cours d'un projet ou non, est le développement de la liste de contrôle générale pour l'identification des phénomènes dangereux. Pour ce faire, il est recommandé dans un premier temps que les concepteurs d'expérience fassent un premier jet des besoins pour l'opération et l'entretien des SPA typiquement exprimés dans la majorité des projets. Par la suite, ces concepteurs pourraient inviter des opérateurs d'expérience à valider les besoins déjà établis et à en ajouter des nouveaux pour ensuite répéter la même procédure avec des personnes affectées à l'entretien des SPA. Ainsi, grâce à ces efforts, une première version de la liste de contrôle sera établie. Par la suite, lorsque des projets seront mis en branle, les concepteurs pourront se baser sur cette version préliminaire pour identifier les besoins liés à l'opération et à l'entretien du SPA en cours de conception. Aussi, de nouveaux besoins spécifiques au projet en cours seront probablement mis en relief, surtout lors des premières applications de la méthode. Ces besoins devront être ajoutés à la liste de contrôle. Ainsi, au fil des années, cette liste de contrôle deviendra de plus en plus précise et complète.

Par ailleurs, l'exploitation de cette liste de contrôle est fort simple. Les concepteurs, assistés ou non des opérateurs et du personnel d'entretien, passent en revue chaque point de la liste de contrôle et identifient quels besoins devront être satisfait par le SPA à concevoir[24]. Tous ces besoins devront être par la suite transcrits sur la liste des exigences. Certes, cette liste des exigences pourrait en fait être la liste de contrôle, étant donné que son contenu et son format proviennent de cette dernière. Cependant, le candidat recommande que la liste des exigences constitue un document séparé, car son contenu est toujours spécifique à un projet donné.

[24] La présences de personnes chargées d'opérer ou d'entretenir le SPA n'est pas essentielle à ce stade-ci de la conception, mais tout de même recommandée par le candidat.

Par ailleurs, d'autres informations, issues notamment du guide pour la gestion du risque, seront ajoutées à la liste des exigences en cours de conception. À titre d'exemple, l'annexe A propose une structure générale de la liste de contrôle pour l'identification des besoins fonctionnels de même que celle de la liste des exigences.

b) Niveau 2

Pour le second niveau de la solution, le candidat recommande que le même concept de liste des exigences issues d'une liste de contrôle soit repris. Cependant, en vue de s'assurer que la liste de contrôle soit aussi complète que possible, l'intégration de quelques outils d'aide à l'analyse des besoins fonctionnels, comme ceux vus à la section 2.2.4, est recommandée.

Par contre, le candidat rappelle qu'à ce stade-ci de la conception, il n'est pas nécessaire d'obtenir un niveau de détail très fin de l'ensemble des besoins fonctionnels à combler. Ainsi, seule l'analyse fonctionnelle devrait être utilisée pour cette étape. Cependant, le candidat recommande que cette dernière s'effectue en suivant *l'approche par point de vue successif* présentée à la section 2.2.6, car elle permet d'adresser plusieurs aspects du SPA. Ainsi, pour chacun des points de vue, les concepteurs doivent s'efforcer de trouver toutes les fonctions liées à l'opération et à l'entretien du SPA. La figure suivante schématise cette recommandation.

Comme l'indique cette figure, toutes les fonctions identifiées lors de l'analyse fonctionnelle vont par la suite être transcrites dans la liste de contrôle générale. Certes, cette activité est beaucoup plus fastidieuse que celle proposée pour le premier niveau du présent guide. Néanmoins, elle offre des résultats beaucoup plus complets. Par ailleurs, il est de l'avis du candidat qu'il pourrait être inutile de la réaliser systématiquement à chaque nouveau projet. En effet, à chaque fois que l'analyse fonctionnelle sera réalisée, la liste de contrôle pour l'identification des besoins fonctionnels liés à l'opération et à l'entretien sera de plus en plus complète. Ainsi, il pourrait même s'avérer qu'au fil des années cette activité ne soit plus vraiment nécessaire ou, du moins, se réalisera beaucoup plus rapidement.

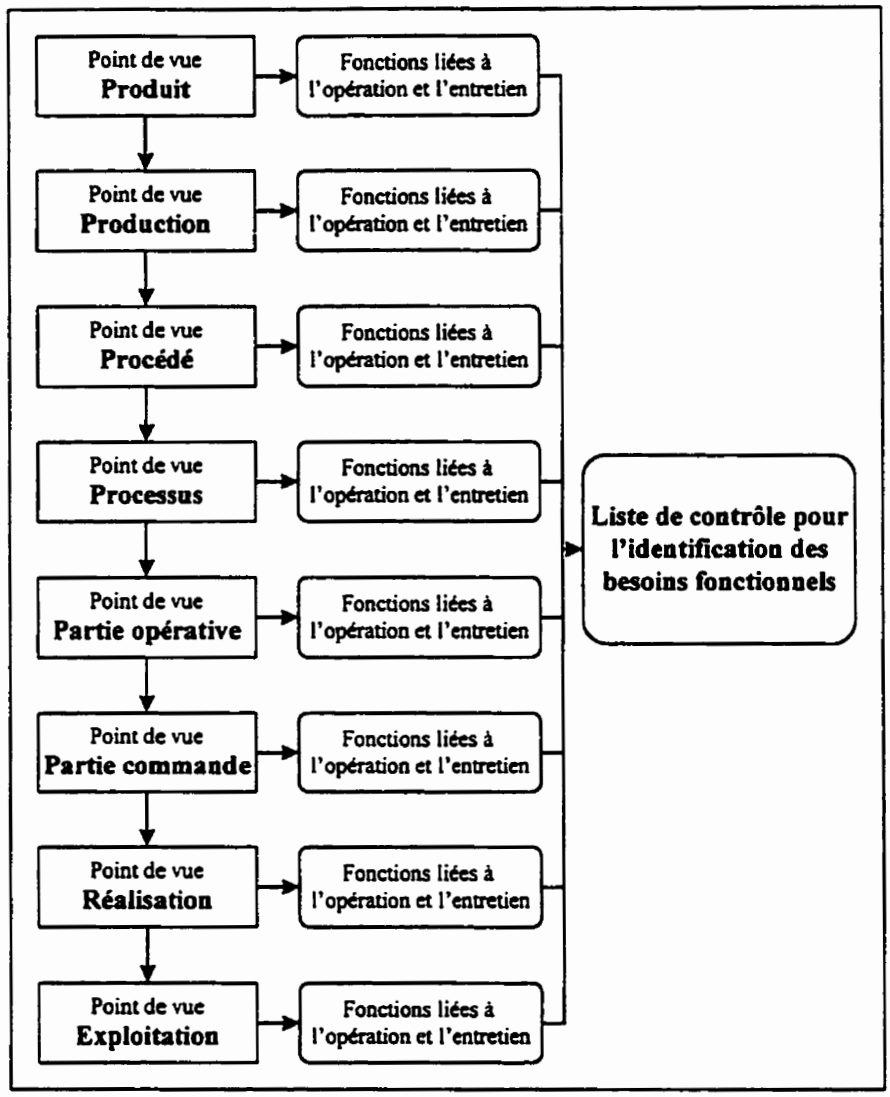

Figure 5.3 Élaboration des fonctions selon l'approche par point de vue successif

Finalement, le candidat avance que la rédaction d'un cahier des charges fonctionnel pourrait très bien remplacer l'élaboration de la liste des exigences. En effet, plutôt que d'utiliser la structure de cette dernière (annexe A), la structure du cahier des charges fonctionnel pourrait très bien être utilisée. Ainsi, plutôt que de traiter des exigences assorties de spécifications, les concepteurs traiteraient des fonctions caractérisées. Néanmoins, dans l'unique but de ne pas surcharger la présentation de la solution proposée, le concept de la liste d'exigences assorties de spécifications continuera à être exploité.

5.3.1.3 Intégration et exploitation des résultats

Une fois que la liste des exigences (version préliminaire) est établie, l'équipe de conception peut débuter la recherche des solutions potentielles. Par la suite, pour effectuer la sélection de la solution optimale, l'équipe de projet pourra se servir de la liste des exigences pour déterminer laquelle, parmi toutes les solutions identifiées, respecte le mieux l'ensemble des besoins fonctionnels listés.

Par ailleurs, avant qu'un concept particulier soit retenu par l'équipe de projet, il pourrait s'avérer difficile de spécifier certaines exigences. Par exemple, le nombre et l'emplacement des dispositifs d'arrêt d'urgence ne sont pas faciles à déterminer tant et aussi longtemps que le concept idéal n'était pas identifié. Une fois la sélection réalisée, l'équipe peut plus facilement terminer la spécification des exigences. Aussi, le candidat recommande que ces précisions soient apportées à ce moment-ci étant donné que certaines d'entre elles peuvent avoir une influence considérable sur l'estimation des coûts. De plus, il est de l'avis du candidat que la somme de travail nécessaire pour ainsi compléter la liste des exigences établies est passablement petite et que les efforts investis pour cette tâche seront très profitables pour le reste du projet, étant donné que l'équipe bénéficiera d'un budget plus réaliste et d'une définition de projet plus précise.

5.3.2 Utilisation du guide lors de la conception préliminaire

Lors de la conception préliminaire et comme indiqué à la figure 5.2, il est prévu que le guide pour l'analyse des besoins fonctionnels soit utilisé pour réaliser la revue des exigences (activité 2.1).

5.3.2.1 Objectif

L'objectif à atteindre pour cette étape est de s'assurer que toutes les exigences liées à l'opération et à l'entretien du SPA à concevoir sont bien inscrites dans la liste des exigences de même que leurs spécifications.

5.3.2.2 Mise en oeuvre

a) Niveau 1

Le lecteur se souviendra que les objectifs de la première version de la liste des exigences issue de la définition de projet étaient de mieux orienter la recherche de solutions potentielles et la sélection d'un concept à développer et de prévoir les coûts supplémentaires associés aux modifications devant être apportées pour que le concept retenu réponde aux principaux besoins fonctionnels ; la liste des exigences n'était donc pas nécessairement complète. Ainsi, avant d'entreprendre la revue des exigences, les concepteurs doivent dans un premier temps compléter cette liste. Une fois complétée, son contenu entier (exigences et spécifications) devra être révisé. Il est alors fortement recommandé que des opérateurs de même que quelques personnes de l'entretien participent activement à cette revue des exigences et mettent ainsi leur expérience à profit.

b) Niveau 2

Tout comme pour le premier niveau de la solution, la première activité devant être réalisée est de compléter la liste des exigences établies. Pour ce faire, une revue systématique de l'analyse fonctionnelle réalisée pour les différents points de vue est recommandée.

Par ailleurs, comme l'indiquaient le tableau 2.1, plusieurs accidents surviennent en mode de marche automatique pendant ou suite à des interventions imprévues. L'élaboration des divers

modes de marche et d'arrêt semble donc poser quelques difficultés aux concepteurs. Pour régler ce problème, le candidat recommande fortement que le GEMMA (voir appendice 4) soit utilisé lors de l'analyse fonctionnelle pour le point de vue *commande*. Sa simplicité de mise en oeuvre et la qualité des informations qu'il procure justifient cette recommandation. Ainsi, grâce à l'étude systématique des divers modes de marche et d'arrêt, le GEMMA permettra d'élaborer des fonctions spécialement adaptées aux besoins liés à l'opération et à l'entretien du SPA. D'autre part, l'utilisation du GRAFCET est également recommandée lorsque son application est possible (commandes séquentielles). Ainsi, des liens entre les diverses fonctions de commande établies pourront être mis en relief, ce qui pourrait d'ailleurs faire ressortir des lacunes indiquant que certaines fonctions de commande sont absentes. Le GRAFCET pourrait donc servir à valider et à compléter les fonctions de commande établies. Finalement, la représentation graphique de l'ensemble des fonctions de commande pour l'opération et l'entretien du SPA grâce à la méthode SADT peut s'avérer intéressante, dans la mesure où les concepteurs en ressentent la nécessité, car il est de l'avis du candidat qu'outre la qualité de sa représentation graphique, cette technique peut s'avérer coûteuse en terme de temps compte tenu du peu d'informations additionnelles qu'elle apporte par rapport à sa complexité de mise en oeuvre.

Ainsi, grâce à la revue de l'analyse fonctionnelle pour chaque point de vue et l'intégration du GEMMA et du GRAFCET, l'ensemble des exigences assorties de leurs spécifications compléteront la liste des exigences. Une fois complétée, la revue des exigences, où des opérateurs et des représentants de l'entretien doivent être présents, est réalisée.

5.3.2.3 Intégration et exploitation des résultats

Une fois que la revue des exigences a été réalisée, l'équipe de projet peut commencer à élaborer la solution retenue en vue de déterminer comment l'ensemble des exigences pourront être comblées par le futur SPA ; cependant, il n'est pas encore question de conception détaillée. Les concepteurs doivent plutôt consacrer leurs efforts pour mieux adapter la solution retenue aux diverses exigences établies.

5.4 Guide pour la gestion du risque

Comme l'indique la figure 5.2, les concepteurs doivent se référer au guide pour la gestion du risque lors de la définition du projet et lors de la conception préliminaire. L'objectif principal de ce guide de conception est de permettre à l'équipe de procéder à la gestion du risque, c'est-à-dire d'identifier les phénomènes dangereux, d'estimer et d'évaluer leur risque en vue d'élaborer les solutions qui permettront d'éliminer ou de réduire les risques inacceptables.

5.4.1 Utilisation du guide lors de la définition de projet

Il est prévu que ce guide soit utilisé au cours de la définition de projet lors de la sélection de la solution optimale (activité 1.4 de la figure 5.2). L'utilisation de ce guide de conception à cette étape du PRP poursuit essentiellement deux objectifs : l'élaboration de critères de sélection axés sur la sécurité et l'élaboration de solutions pour la réduction du risque pour optimiser l'estimation des coûts.

5.4.1.1 Premier objectif

Une fois que l'équipe de projet a répertorié une série de solutions potentielles, elle doit maintenant en sélectionner une qu'elle développera par la suite. Aussi, comme indiqué plus tôt, le candidat recommande que cette sélection repose entre autres sur des critères de sécurité. Le premier objectif de cette étape est donc de permettre à l'équipe de mieux orienter la sélection de la solution optimale en établissant des critères de sélection permettant de considérer la sécurité globale des solutions à évaluer.

5.4.1.2 Mise en oeuvre pour l'atteinte du premier objectif

Pour l'atteinte du premier objectif, l'approche proposée est la même pour le premier et le deuxième niveau de la solution. Ainsi, les concepteurs doivent, dans un premier temps, chercher à élaborer une seconde liste de contrôle, mais dont l'objet est maintenant l'identification des phénomènes dangereux typiquement présents dans les SPA. Pour ce faire, le candidat suggère que la liste de contrôle proposée par la norme européenne EN 292 [1991] (présentée dans le tableau 2.5) serve de point de départ. Ainsi, en combinant leurs expériences aux diverses

catégories de phénomènes dangereux proposées par la norme, les concepteurs, aidés ou non des opérateurs et du personnel d'entretien, pourront élaborer une première liste de contrôle pour l'identification des phénomènes dangereux. Par la suite, au fil des années, cette liste de contrôle pourra se compléter en mettant à profit les expériences acquises et vécues au cours de la réalisation future de divers projets ; la liste de contrôle pour l'identification des phénomènes dangereux est donc rétrospective et évolutive.

5.4.1.3 Intégration et exploitation des résultats pour le premier objectif

Grâce à la liste de contrôle pour l'identification des phénomènes dangereux, les concepteurs pourront établir quelques critères de sélection permettant de choisir parmi les solutions potentielles recensées celle qui offre le meilleur niveau global de sécurité. Ces critères de sélection devront être inscrits dans la liste des exigences déjà entamées (voir annexe A).

5.4.1.4 Second objectif

Quant à lui, le second objectif poursuivi ici vise à permettre à l'équipe de projet d'élaborer sommairement des solutions pour l'élimination ou la réduction des principaux risques en vue de prévoir les coûts associés aux modifications nécessaires pour rendre la solution retenue conforme aux exigences de sécurité établies.

5.4.1.5 Mise en oeuvre pour l'atteinte du second objectif

Étant donné qu'un concept a déjà été sélectionné, il est maintenant plus facile pour l'équipe de projet d'élaborer des solutions pouvant rendre sécuritaires l'opération et l'entretien du SPA. Aussi, pour permettre aux concepteurs de prévoir les coûts associés à ces solutions, deux niveaux de solution ont été élaborés.

a) Niveau 1

Lors de l'élaboration des critères de sélection, une première identification des phénomènes dangereux a été réalisée. Cependant, cette dernière était d'un ordre très général, car les phénomènes dangereux identifiés n'étaient pas spécifiques à un seul équipement. Maintenant

qu'un concept particulier doit être étudié, une seconde recherche des phénomènes dangereux doit être faite. Ainsi, pour ce premier niveau de la solution, le candidat recommande que l'utilisation de la liste de contrôle pour l'identification des phénomènes dangereux soit à nouveau utilisée.

Une fois que les phénomènes dangereux auront été identifiés, les concepteurs devront déterminer ceux pour lesquels une solution doit être élaborée[25]. Pour ce faire, le candidat recommande qu'un des principes suggérés par F. Gauthier [1997] selon lequel les concepteurs doivent concentrer dans un premier temps leurs efforts pour élaborer des solutions pour les phénomènes dangereux dont la **gravité** des dommages potentiels est élevée (c'est-à-dire pouvant engendrer des blessures irréversibles ou des décès) soit appliqué. Ainsi, uniquement pour les phénomènes dangereux graves, des solutions devront être élaborées sommairement en vue de réduire leur risque. Pour ce faire, le candidat recommande que les techniques de réduction du risque présentées dans l'état des connaissances soient suivies. En effet, il est de l'avis du candidat que la somme de travail nécessaire pour leur mise en oeuvre est petite et que les solutions élaborées en respectant ce principe seront plus efficaces pour l'intégration de la sécurité. La figure 5.4, présentée un peu plus loin dans ce mémoire (page 151), présente donc la gestion du risque recommandée lors de la définition de projet.

b) Niveau 2

Pour le second niveau de la solution, en plus de l'utilisation de la liste de contrôle générée précédemment pour l'identification des phénomènes dangereux, le candidat recommande que la méthode *What-if Analysis* soit utilisée, car, comme indiqué à l'appendice 3, cette méthode est facile à mettre en oeuvre et offre une grande polyvalence d'analyse puisqu'elle permet l'identification des quatre types de facteur de risque (humain, organisationnel, technique et externe). Ainsi, en peu de temps, les concepteurs, aidés des opérateurs et du personnel d'entretien, pourront identifier de nouveaux phénomènes dangereux liés au concept retenu.

---

[25] Le candidat tient à rappeler que, bien qu'une solution de réduction du risque devra être élaborée pour chaque phénomène dangereux dont le risque est inacceptable, l'objectif à ce stade-ci de la conception est simplement de prévoir le budget nécessaire pour rendre le futur SPA sécuritaire ; une étude exhaustive serait donc inutile, étant donné que l'équipe de projet n'a aucune garantie que les fonds seront octroyés par la direction.

Par ailleurs, les nouveaux phénomènes dangereux identifiés devront être retranscrits dans la liste de contrôle générale de manière à ce que, au fil des années, cette dernière évolue. Ainsi, elle devrait finir par être si complète que l'application de la méthode *What-if Analysis* sera inutile, ou du moins, elle sera appliquée plus rapidement. La figure 5.4 (page suivante) présente cette étape de mise à jour de la liste de contrôle.

Finalement, une fois que les phénomènes dangereux ont été identifiés, les concepteurs doivent élaborer sommairement les solutions pour l'élimination ou la réduction de leur risque. Pour ce faire, le candidat émet la même recommandation que celle émise pour le premier niveau, à savoir que l'estimation du risque doit se limiter à l'estimation de la gravité des dommages potentiels. La figure 5.4 présente donc la gestion du risque recommandée.

5.4.1.6 Intégration et exploitation des résultats pour le second objectif

Une fois que les solutions ont été sommairement élaborées en vue d'éliminer les phénomènes dangereux graves, ou du moins de diminuer la gravité de leurs dommages potentiels, les concepteurs doivent les transposer en exigences et en spécifications puis les transcrire dans la liste des exigences de manière à les considérer lors de l'estimation des coûts.

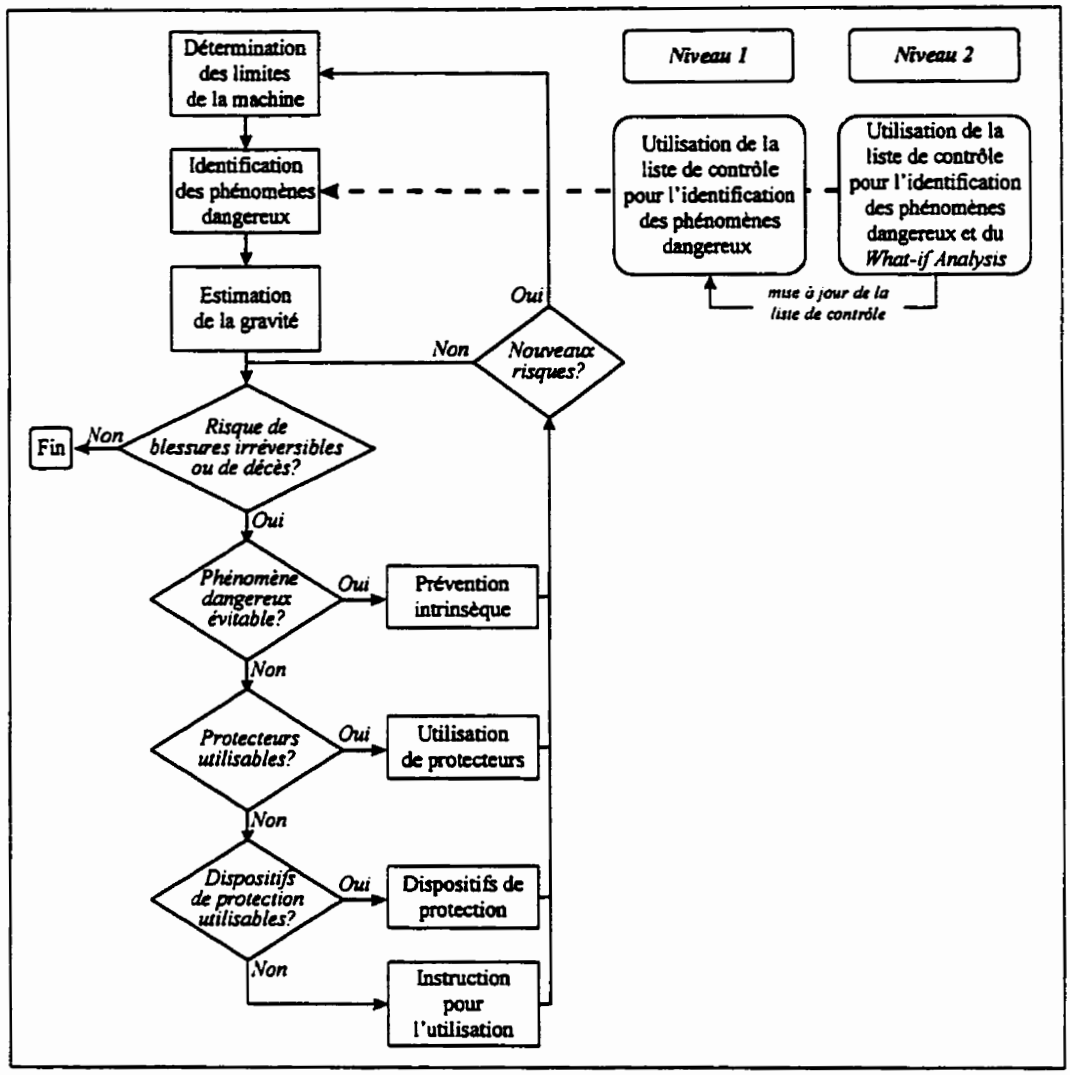

Figure 5.4 Gestion du risque recommandée lors de la définition de projet

5.4.2 Utilisation du guide lors de la conception préliminaire

Selon la figure 5.2, il est prévu que le guide pour la gestion du risque soit utilisé à nouveau lors de la conception préliminaire, pour la revue des exigences. Cependant, avant de procéder à cette activité, les concepteurs doivent dans un premier temps compléter cette liste.

5.4.2.1 Objectif

Le lecteur se souviendra que lors de la définition de projet, la gestion du risque n'était que sommaire, car elle n'avait pour buts que de permettre aux concepteurs de choisir le concept le plus sécuritaire et de prévoir les coûts pour régler les principaux problèmes de sécurité. L'objectif principal de cette seconde utilisation du guide est donc de compléter la liste des exigences pour pouvoir effectuer la revue des exigences.

5.4.2.2 Mise en oeuvre

Pour sa mise en oeuvre, deux niveaux de solution sont proposés.

a) Niveau 1

Lors de la définition de projet, les concepteurs, aidés des opérateurs et du personnel d'entretien, ont effectué une première identification des phénomènes dangereux. En vue de s'assurer que l'ensemble des phénomènes dangereux ont été identifiés, le candidat recommande qu'une seconde identification des phénomènes dangereux soit réalisée. Les concepteurs devraient alors se servir de la liste de contrôle.

Une fois que le SPA entier aura été étudié, tous les phénomènes dangereux identifiés doivent être soumis au processus d'estimation du risque. Le candidat recommande alors que l'estimation de leur risque s'effectue en utilisant la grille d'estimation qualitative proposée dans le projet de norme EN 1050 [1996] et présenté à la figure 2.27, page 59. Cette recommandation est basée sur le fait que cette grille est très simple d'utilisation, qu'elle couvre plusieurs dimensions du risque (probabilité, gravité, possibilité d'évitement et fréquence d'occurrence) et que les termes utilisés

sont sans ambiguïtés. Finalement, l'évaluation et la réduction du risque doivent se faire comme indiqué à la figure 5.5 (page 155).

b) Niveau 2

Au second niveau de la solution, l'identification des phénomènes dangereux devrait, à ce stade-ci de la conception, être plus élaborée. Comme établi dans l'état des connaissances, plusieurs méthodes d'analyse du risque existent et ont été étudiées dans le cadre de la thèse de F. Gauthier [1997]. Ainsi, en se basant sur des critères généraux, comme l'efficacité, la pertinence et la profondeur de la méthode, cet auteur a identifié quatorze méthodes d'analyse du risque pouvant être utilisées pour la conception d'outils, de machine et de procédés industriels communs[26] ; ces quatorze méthodes pourraient donc être utilisées pour la conception de SPA destinés à l'industrie québécoise des P&P. Néanmoins, le candidat propose de n'en retenir que quelques unes. Le tableau suivant présente donc les méthodes d'analyse du risque recommandées pour le second niveau de la solution.

TABLEAU 5.1 MÉTHODES D'ANALYSE DU RISQUE RECOMMANDÉES PAR LE CANDIDAT

Méthodes	***Motivation du choix***
Check List Analysis	Très simple d'utilisation, elle est d'ailleurs abondamment utilisée dans l'approche, sous l'appellation *listes de contrôle*.
Critical Incident Technique	Elle permet de mettre à profit très facilement les retours d'expérience en identifiant les phénomènes dangereux qui ont déjà conduit à un dommage ou à un *passé proche*. Aussi, elle permet l'identification des quatre facteurs de risque.
Fault Tree Analysis (FTA)	Elle permet aux concepteurs d'identifier la cause première de tous les phénomènes dangereux identifiés et facilite ainsi la prévention intrinsèque.
Hazard and Operability Analysis (HAZOP)	Cette méthode, mais particulièrement la version proposée par l'équipe de J.R. Catmur [1992] permettant l'analyse des SÉP, s'avère intéressante.
Safety Review	Les revues de sécurité sont déjà prévues dans l'approche (voir figure 5.2).
Task Analysis	Particulièrement intéressante pour l'identification des phénomènes dangereux spécifiquement liés à l'opération et à l'entretien du SPA, car les activités de travail de ces deux groupes de travailleurs pourront être analysées plus en détail.
What-if Analysis	Déjà recommandée, cette méthode est simple d'application et permet l'identification des quatre facteurs de risque.

[26] Le candidat rappelle que ces quatorze méthodes sont présentées à l'appendice 3.

Par ailleurs, le candidat rappelle que la liste de contrôle générale pour l'identification des phénomènes possède un caractère évolutif, c'est-à-dire qu'elle peut évoluer au fil des années. Ainsi, si ses utilisateurs prennent la peine de la maintenir à jour et d'y intégrer les nouveaux phénomènes dangereux identifiés notamment à l'aide des méthodes d'analyse du risque recommandées au tableau 5.1, cette liste de contrôle pourrait devenir suffisamment complète pour ne plus devoir appliquer ces méthodes, ou du moins leur application serait beaucoup plus simple et rapide.

Une fois l'identification des phénomènes dangereux terminée, les concepteurs doivent procéder à l'estimation de leur risque. Pour ce faire, le candidat recommande que les risques associés aux phénomènes dangereux qui sont en relation avec les commandes du SPA soient estimés selon la grille d'estimation du risque par catégorie proposée dans le projet de norme EN 954-1 [1996] (figure 2.29, page 64). Le principal avantage qui motive cette recommandation est que ce projet de norme propose des solutions techniques bien précises, éprouvées et reconnues comme étant efficaces pour la sécurité des fonctions de commande qui permettent de réduire le risque de ces phénomènes dangereux.

Par ailleurs, pour les phénomènes dangereux qui ne sont pas liés aux commandes du SPA, le même scénario proposé pour le premier niveau de la solution est conseillé. La figure 5.5 (page suivante) schématise ces recommandations.

5.4.2.3 Intégration et exploitation des résultats

Dans un premier temps, tous les nouveaux phénomènes dangereux identifiés doivent, comme spécifié à maintes reprises, être intégrés à liste de contrôle générale. Ensuite, grâce au processus de gestion du risque, plusieurs solutions potentielles ont été élaborées. Ces dernières, accompagnées des spécifications les décrivant, doivent alors être transcrites dans la liste des exigences. Une fois cette étape terminée, la liste des exigences devrait être complète. La revue des exigences peut alors être enfin effectuée, après quoi les concepteurs pourront compléter la conception préliminaire et entamer la conception détaillée.

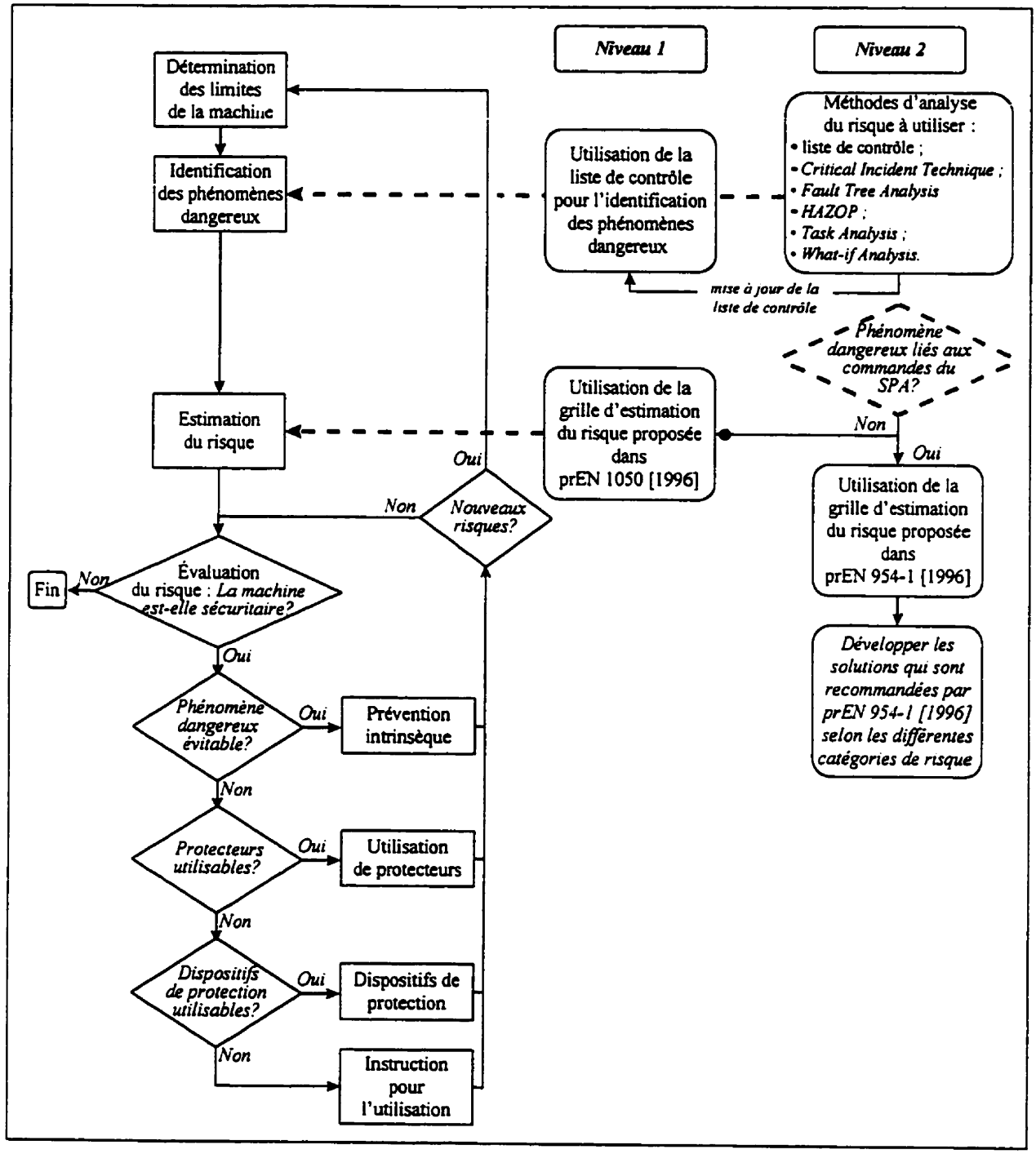

Figure 5.5 Gestion du risque recommandée lors de la conception préliminaire

5.5 Guide pour les revues de sécurité

5.5.1 Généralités

Les revues de sécurité consistent à rassembler les personnes ressources nécessaires pour effectuer des révisions régulières de la sécurité de la conception au fur et à mesure de son avancement [STEPHANS, R.A. et coll., 1993]. La conformité aux normes, l'analyse ergonomique, la hiérarchie des contrôles, la prédiction des mauvais usages et des erreurs d'opération, la formation des opérateurs, les mises en garde, etc. sont parmi les points examinés lors de ces revues [GAUTHIER, F., 1997]. Par ailleurs, il est recommandé que les revues de sécurité soient réalisées indépendamment de toutes autres activités de conception, afin d'assurer l'intégrité de l'objectif principal de cet exercice : la sécurité du SPA et des processus connexes [ASME, 1984]. Elles ne sont donc pas conduites dans le cadre des revues de conception traditionnelles. Chacune des revues nécessite plusieurs activités préparatoires qui doivent être effectuées avant la ou les rencontres. Les résultats des revues de sécurité dépendent donc fortement de la qualité du travail préparatoire, de l'expérience du président d'assemblée et de l'expertise des personnes formant l'équipe de revue.

5.5.2 Intégration des revues de sécurité au document de référence

Dans sa thèse de doctorat, F. Gauthier [1997] recommande trois revues de sécurité formelles, soit une lors de la conception préliminaire, une à la fin de la conception détaillée et une dernière suite à la préproduction. En se basant sur ces informations, le candidat recommande également que trois revues de sécurité soient menées. Ainsi, comme l'indique la figure 5.2, une première revue de sécurité est effectuée après la conception préliminaire, une autre après la conception détaillée et une dernière lors de la vérification préopérationnelle. Par ailleurs, il est de l'avis du candidat que plusieurs revues informelles menées au cours de la conception détaillée permettraient d'optimiser l'efficacité de l'approche en terme de temps de la conception détaillée. Étant donné que les membres de l'équipe de projet peuvent mieux suivre l'évolution de la conception, ils pourraient émettre leur avis au fur et à mesure que les solutions sont développées par les concepteurs. La réalisation des revues de sécurité informelles, bien que laissée à la discrétion des utilisateurs de ce guide, est recommandée par le candidat.

Les objectifs poursuivis par chacune des revues de sécurité conseillées sont maintenant présentés.

5.5.2.1 Objectif de la revue de sécurité formelle de la conception préliminaire

L'objectif poursuivi à ce stade-ci de la conception est de s'assurer que le concept qui a été sélectionné et dont la conception préliminaire est terminée rencontrera avec une très grande probabilité l'ensemble des exigences de sécurité spécifiées dans la liste des exigences. Après cette revue, les concepteurs détailleront alors les solutions trouvées.

5.5.2.2 Objectif des revues de sécurité informelle et formelle de la conception détaillée

Comme mentionné précédemment, le candidat recommande que des revues de sécurité informelles soient menées tout au long des activités de la conception détaillée dans le but de rendre plus efficace cette étape du projet. Ainsi, grâce à ces revues informelles, l'équipe de projet pourra suivre l'évolution du SPA et apporter simultanément leurs recommandations.

Par ailleurs, plusieurs revues de sécurité informelles peuvent être réalisées tout au long de la conception, mais il est aussi important qu'une revue de sécurité formelle soit menée [ISO 9001, 1994] [ISO 9004-1, 1994]. Ainsi, à la fin de la conception détaillée, une revue de sécurité formelle doit être menée dans le but de s'assurer que le SPA conçu répond aux exigences prescrites. Il est de l'avis du candidat que cette revue de sécurité formelle est d'une importance capitale étant donné qu'à la suite de cette dernière, le SPA sera construit et installé. Ainsi, toutes les erreurs de conception sécuritaire qui n'auront pas été identifiées feront l'objet de modifications du SPA en cours d'exploitation, ce qui engendrera des pertes de temps et d'argent pour l'entreprise.

5.5.2.3 Objectif de la revue de sécurité préopérationnelle

Au cours de la vérification préopérationnelle, l'équipe de projet toute entière doit qualifier le SPA installé en se basant entre autres sur l'ensemble des exigences établies. Bien que l'ensemble des spécifications de sécurité soient inclues dans la liste des exigences, le candidat recommande

qu'une dernière revue de sécurité formelle soit réalisée en vue de s'assurer que le SPA conçu, fabriqué et installé est conforme à toutes les exigences de sécurité prescrites.

5.5.2.4 Mise en oeuvre

Pour la mise en oeuvre des revues de sécurité, un seul niveau de solution est proposé. D'ailleurs, la mise en oeuvre des trois revues de sécurité formelles est la même. Pour le lecteur qui ne serait pas familier avec les revues de sécurité, l'appendice 7 présente sommairement la manière de les réaliser.

Par ailleurs, pour ce qui est de la réalisation des revues de sécurité informelles, ces dernières sont caractérisées par une approche non structurée. Typiquement, elles ont lieu spontanément, autour de la table à dessin ou de l'écran avec un système de DAO où un ou plusieurs membres de l'équipe de projet répondent aux questions du ou des concepteurs [MURRAY, A., 1996].

5.5.2.5 Intégration et exploitation des résultats

À chaque revue de sécurité, il est extrêmement important que les problèmes de conception sécuritaire identifiés soient clairement notés. Par la suite, les concepteurs doivent tout mettre en oeuvre pour élaborer des solutions y remédiant, car tous les phénomènes dangereux non maîtrisés devront l'être en cours d'exploitation.

CONCLUSION

Synthèse

Rappel des objectifs

L'objectif principal de cette recherche a été de développer une approche de conception qui sera exploitable par les concepteurs de l'industrie québécoise des pâtes et papiers et qui leur permettra de rendre plus sécuritaires l'opération et l'entretien des systèmes de production automatisés qui sont dotés de technologies programmables. Pour que cet objectif soit atteint, cinq objectifs intermédiaires ont été établis :

- adapter l'approche aux pratiques des concepteurs de l'industrie québécoise des P&P ;
- optimiser l'efficacité des activités de conception en terme de temps ;
- intégrer les méthodes d'analyse du risque ;
- augmenter la coopération ;
- permettre aux concepteurs de tirer profits de leurs expériences.

La solution développée devait donc tenir compte de ces cinq objectifs intermédiaires.

Adapter l'approche aux pratiques des concepteurs de l'industrie québécoise des P&P

Pour qu'elle ait toutes les chances d'être réellement exploitée, l'approche devait permettre aux concepteurs de SPA de l'industrie québécoise des P&P de l'assimiler d'une manière évolutive. Pour tenter d'atteindre cet objectif, un guide de référence a été développé en se basant sur les activités de conception habituellement rencontrées dans cette industrie, ces dernières étant regroupées dans un processus de réalisation de projet typique (PRP), et seulement quelques nouvelles activités de conception ont été ajoutées à ce PRP. Aussi, la mise en oeuvre des guides de conception référés par l'approche peut se réaliser selon deux niveaux de difficultés, le premier niveau n'intégrant que des outils simples et assez répandus.

le GEMMA, le GRAFCET et la méthode SADT) de même que pour la gestion du risque, comme l'utilisation de méthodes d'analyse du risque et des principes pour la réduction du risque.

Optimiser l'efficacité des activités de conception en terme de temps

Pour rencontrer cet objectif, la solution proposée mise sur trois points. Le premier est que l'élaboration plus approfondie de la conception préliminaire devrait permettre à l'équipe de projet, et particulièrement aux concepteurs, de se faire une idée plus précise du SPA à concevoir et des principales difficultés qui pourraient émerger dans les étapes subséquentes. Cette phase conceptuelle mieux élaborée devrait donc permettre d'importants gains de temps, ce qui est d'ailleurs un principe de plus en plus reconnu[27].

Le second point est que les trois revues de sécurité formelles effectuées au cours du PRP devraient permettre d'identifier et de régler les problèmes de sécurité qui auraient échappé aux concepteurs. Ainsi, comme les solutions auront été élaborées avant la mise en production du SPA, les pertes de production traditionnelles associées aux temps d'arrêts nécessaires pour effectuer ces modifications devraient être considérablement diminuées, sans compter le fait que l'opération et l'entretien du SPA seront plus sécuritaires. Ainsi, le temps supplémentaire investi pour identifier et corriger les problèmes de sécurité avant sa mise en marche devrait être largement récupéré en cours d'exploitation.

Finalement, le manque de documentation des activités de conception résulte parfois en des oublis et des dédoublement d'activités. La liste des exigences élaborées lors de la définition de projet et complétées lors de la conception préliminaire constitue un document unique dans lequel toutes les exigences à satisfaire sont inscrites. Ainsi, grâce au transfert du savoir et du savoir-faire des concepteurs vers l'organisation, ce document devrait permettre des gains de temps appréciables pour la conception du SPA.

---

[27] Une des forces de l'ingénierie simultanée est sa phase conceptuelle (pouvant correspondre entre autres ici à la conception préliminaire) qui est mieux élaborée. Grâce à elle, des réductions de temps de l'ordre de 25% ont été enregistrées dans des entreprises manufacturières du Québec [MARTEL, P., 1997]. D'autres études avancent même des gains de temps de l'ordre de 40% [BAKER, B. et coll., 1991].

Intégrer les méthodes d'analyse du risque

Comme établi dans la problématique, les concepteurs de l'industrie québécoise des P&P ne connaissent pratiquement pas les méthodes d'analyse du risque existantes. Aussi, dans le souci de respecter le premier et le second objectifs intermédiaires, l'intégration de seulement quelques méthodes d'analyse du risque a été faite pour la mise en oeuvre du guide pour la gestion du risque (au second niveau seulement). Ainsi, sept méthodes d'analyse du risque ont été jugées applicables et pertinentes pour la présente recherche. Parmi ces dernières, les listes de contrôle (*Check List Analysis*) ont été abondamment utilisées, notamment en raison de leur facilité de mise en oeuvre et de leur efficacité pour la mise à profit des retours d'expériences.

Augmenter la coopération

Dans l'état des connaissances, une difficulté majeure a été soulevée : un manque évident de communication, et donc de coopération, caractérise les pratiques de conception traditionnelles dans l'industrie québécoise des P&P. Ainsi, pour tenir compte de cette problématique, l'approche développée prévoit la formation d'une équipe de conception multidisciplinaire qui suivra et participera aux différentes activités de conception.

Permettre aux concepteurs de tirer profits de leurs expériences

Pour tenter de rencontrer cet objectif, l'approche a été développée de telle sorte que les expériences vécues puissent être intégrées aux deux listes de contrôle proposées (celle pour l'analyse des besoins fonctionnels et celle pour l'identification des phénomènes dangereux). Comme ces dernières sont évolutives, donc appelées à évoluer, les concepteurs pourront les mettre à jour en y ajoutant les diverses leçons qu'ils tireront de leurs futurs projets de conception.

Discussion et nouvelles perspectives de recherche

Dans l'introduction de ce mémoire, le candidat a identifié les principales difficultés à l'origine de ce projet de recherche. La première, très générale, est que l'opération et l'entretien des SPA dotés de technologies programmables et destinés à l'industrie québécoise des P&P ne sont pas sécuritaires. La principale raison alors invoquée est leur conception déficiente. Aussi, une difficulté pour l'analyse des besoins fonctionnels et pour l'identification et la résolution de problèmes de sécurité a été soulevée. Bien qu'ils bénéficient souvent d'une expérience incontestable en conception, leur manque de connaissances et surtout les contraintes de temps auxquels sont soumis les concepteurs de cette industrie peuvent expliquer en partie cette autre difficulté. Finalement, un problème important mis en relief dans l'état des connaissances est que l'ensemble des activités de conception reposent généralement sur le savoir et le savoir-faire des concepteurs : presque aucune procédure systématique et documentée existe dans cette industrie.

Le document de référence proposé auquel se greffent trois guides de conception a donc été développé spécifiquement dans le but de surmonter ces difficultés. Ainsi, grâce à ce dernier, l'ensemble des activités de conception réalisées dans l'industrie papetière a été systématisé. Cependant, sa validité repose essentiellement sur l'abondante revue littéraire effectuée et sur les informations tirées des diverses activités réalisées dans le milieu industriel des pâtes et papiers ; la validation de ce document de référence par une application réelle serait donc importante. Par contre, comme cette validation représente une somme de travail assez considérable, cette dernière pourrait être inscrite dans le cadre d'une autre recherche.

Aussi, la flexibilité de l'approche offerte par la mise en oeuvre des guides de conception selon deux niveaux de difficulté devrait permettre à ces concepteurs d'intégrer de manière évolutive cette nouvelle façon de concevoir les SPA.

Par ailleurs, comme une cause commune d'accidents est la mauvaise adaptation des SPA aux besoins réels des utilisateurs, le guide pour l'analyse des besoins fonctionnels devrait permettre de mieux prendre en considération les besoins exprimés par les personnes chargées d'opérer et d'entretenir les SPA. Par contre, il est important de noter que la qualité des résultats offerts par

ce guide de conception est intimement liée à l'efficacité des communications de même qu'au niveau de coopération entre ces deux groupes de personnes et l'ingénierie. Il pourrait donc être intéressant, au cours d'une recherche future, d'évaluer la possibilité d'intégrer un guide pour l'optimisation du travail en équipe qui rendrait plus efficaces les communications.

De plus, l'élaboration de listes de contrôle pour l'identification des besoins fonctionnels et pour l'identification des phénomènes dangereux est une idée intéressante qui permet de mettre à profit l'expérience de toute l'équipe de projet de même que les retours d'expérience. Ainsi, ces listes de contrôle pourraient évoluer au fil des années grâce aux diverses leçons tirées des projets réalisés, mais aussi grâce à l'utilisation d'outils plus systématiques pour l'analyse des besoins fonctionnels (comme l'analyse fonctionnelle et le GEMMA) et pour l'identification des phénomènes dangereux (comme les méthodes d'analyse du risque proposées). Il serait d'ailleurs intéressant d'étudier jusqu'à quel point ces listes de contrôle pourraient finir par être assez complètes pour devenir suffisantes pour l'analyse des besoins fonctionnels et l'identification des phénomènes dangereux. Par contre, une limitation à l'approche est ici soulevée : l'efficacité de ces liste de contrôle est directement liée à leur mise à jour par les concepteurs. Il pourrait donc être intéressant de vérifier comment cette mise à jour pourrait être rendue systématique.

D'autre part, bien que quelques recommandations techniques et technologiques aient été faites par le biais de l'intégration du projet de norme EN 954 [1996] au second niveau pour la mise en oeuvre du guide pour la gestion du risque, une avenue de recherche possible consisterait justement à élaborer des recommandations liées à la technologie des SÉP. Néanmoins, il est toujours de l'avis du candidat que les meilleures technologies ne pallieront jamais une piètre conception.

Finalement, le candidat tient à rappeler que le guide de référence pour la conception sécuritaire de SPA développé au cours de cette recherche relève d'un cadre principalement théorique et qu'il bénéficierait à être validé par une application concrète dans l'industrie papetière, ou dans un autre secteur industriel, ce qui constitue d'ailleurs une autre avenue de recherche intéressante.

Annexe A

Présentation du concept de la liste des exigences issues des listes de contrôles

Dans l'approche proposée, il est prévu que les concepteurs se réfèrent à différents guides de conception, dont ceux pour l'analyse des besoins fonctionnels et pour la gestion du risque. Aussi, pour simplifier la mise en oeuvre de ces derniers, le candidat propose que des listes de contrôle soient élaborées.

Ainsi, une première liste de contrôle pour l'analyse des besoins fonctionnels doit être créée. L'objectif alors poursuivi est de développer une liste de contrôle très générale, où plusieurs besoins fonctionnels typiquement précisés dans la majorité des projets de conception seront transcrits. Pour ce faire, il est recommandé que, dans un premier temps, l'expérience de plusieurs intervenants (ingénieurs, employés d'opération et d'entretien, représentants SST, etc.) soit mise à profit. De ceci devrait résulter une première ébauche de la liste de contrôle. Par la suite, cette dernière pourra être complétée, soit grâce à l'exploitation d'outils d'aide à l'analyse des besoins fonctionnels, comme le GRAFCET, le GEMMA, l'analyse fonctionnelle et son CdCF, etc., soit grâce aux retours d'expérience. Ainsi, au fil des années, la liste de contrôle pour l'analyse des besoins fonctionnels deviendra de plus en plus complète, à condition bien sûr que les concepteurs se donnent la peine de la mettre régulièrement à jour. À titre d'exemple, le tableau AA-1 propose un exemple de structure pour l'élaboration de cette liste de contrôle.

Dans le même ordre d'idée, ce principe est recommandé pour l'élaboration de la liste de contrôle pour l'identification des phénomènes dangereux devant être utilisée dans le guide pour la gestion du risque. Ainsi, en se basant sur la liste de contrôle proposée par la norme EN 292 [1991] (tableau 2.5) de même que sur l'expérience des mêmes intervenants, une première liste de phénomènes dangereux typiquement rencontrés sur les SPA de l'industrie papetière doit être créée. Cette dernière pourra par la suite évoluée grâce entre autres aux retours d'expérience, mais plus particulièrement grâce à l'application des méthodes d'analyse du risque recommandées au tableau 5.1. Le tableau AA-2 propose aussi un exemple de structure pour cette liste de contrôle.

TABLEAU AA-I EXEMPLE DE STRUCTURE POUR LA LISTE DE CONTRÔLE DES BESOINS FONCTIONNELS

Besoins liés à l'opération du SPA (les opérateurs doivent être consultés)		
Mise en marche	**Cochez**	**Commentaires :**
• station de commande locale		spécifiez nombre et endroit
• panneau de commande		
• etc.		
Opération normale	**Cochez**	**Commentaires :**
• dispositifs de surveillance des opérations		spécifiez type et endroit
• etc.		
Opération en mode dégradé	**Cochez**	**Commentaires :**
• dispositifs de détections d'anomalies de production		spécifiez type et endroit
• etc.		
Mise à l'arrêt	**Cochez**	**Commentaires :**
• station de commande locale		spécifiez nombre et endroit
• panneau de commande		
• boutons d'arrêt de sécurité		
• boutons d'arrêt d'urgence		spécifiez nombre et endroit
• dispositifs d'arrêt d'urgence		spécifiez type et endroit
• etc.		
Consignation des équipements	**Cochez**	**Commentaires :**
• consignation par des sectionneurs locaux		spécifiez nombre et endroit
• etc.		
Intervention mineure	**Cochez**	**Commentaires :**
• déblocage		élaborer procédure
• nettoyage de l'alimentation de la matière		élaborer procédure
• etc.		
Besoins liés à l'entretien du SPA (le personnel d'entretien mécanique, électrique, etc. doit être consulté)		
Consignation des équipements	**Cochez**	**Commentaires :**
• immobilisation des pièces mécaniques		spécifiez lesquelles
• purge des énergies (pneumatiques, hydraulique, etc.)		spécifiez lesquelles
• etc.		
Interventions mécaniques	**Cochez**	**Commentaires :**
• accès aux pièces mécaniques pour intervention		dimension min. pour accès
Interventions électriques et électroniques	**Cochez**	**Commentaires :**
• etc.		

TABLEAU AA-2 EXEMPLE DE STRUCTURE POUR LA LISTE DE CONTRÔLE DES PHÉNOMÈNES DANGEREUX

Phénomènes dangereux liés à l'entretien et à l'opération du SPA (l'opération et l'entretien doivent être consultés)			
Risque d'écrasement	**Cochez**	**Solution imaginée**	**Risque**
• accès à la zone tampon pour les bobines de papier			
• etc.			
Risque de cisaillement	**Cochez**	**Solution imaginée**	**Risque**
• accès à des pièces mécaniques en mouvement			
• etc.			
Risque de coupure ou de sectionnement	**Cochez**	**Solution imaginée**	**Risque**
• accès aux couteaux rotatifs de la bobineuse			
• etc.			
Risque d'entraînement ou d'emprisonnement	**Cochez**	**Solution imaginée**	**Risque**
• angle entrant non couvert			
• etc.			
etc.			

Finalement, lorsqu'une équipe sera formée pour réaliser un projet quelconque, elle pourra se baser sur ces deux listes de contrôle très générale pour identifier quels sont les besoins fonctionnels et les phénomènes dangereux qui sont spécifiques à leur projet et, enfin, établir la liste des *exigences* de ce projet[28]. La figure suivante schématise cette procédure.

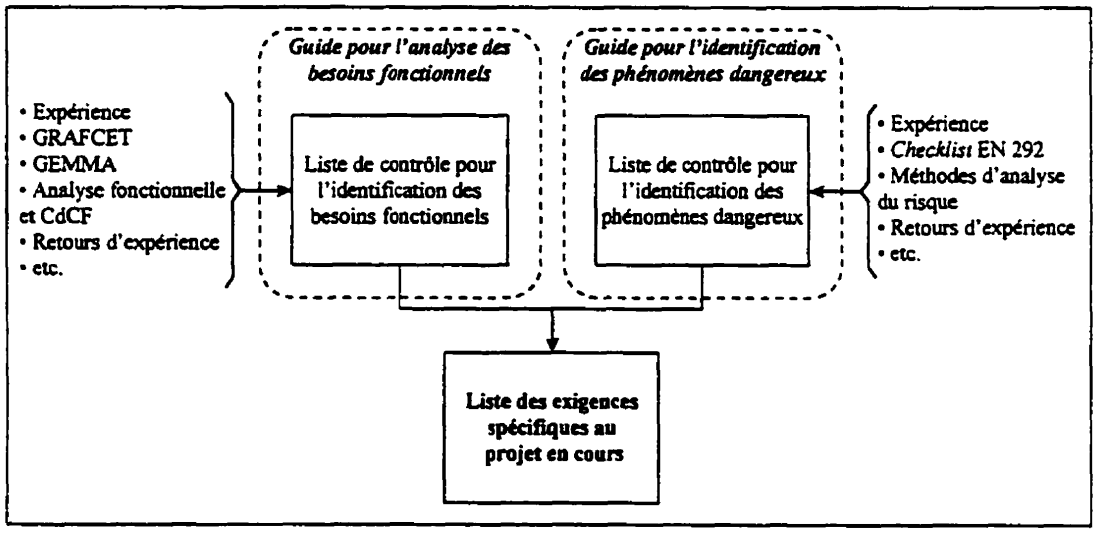

Figure AA-1 Formation de la liste des exigences

[28]Le candidat englobe les besoins de fonctionnalité et de sécurité dans le terme *exigence*.

Ainsi, grâce à ces listes de contrôle, l'équipe de conception pourra établir plus facilement les exigences de fonctionnalité et de sécurité spécifiques au projet en cours. Par la suite, en se basant sur ces dernières, l'équipe devra préparer la liste des exigences qui servira à diriger la quasi totalité des activités de conception, un peu comme un cahier des charges. Le tableau suivant propose une structure pour l'élaboration de la liste des exigences spécifiques à un projet donné.

TABLEAU AA-2 EXEMPLE DE STRUCTURE POUR LA LISTE DES EXIGENCES

Besoins liés à l'opération du SPA (les opérateurs doivent être consultés et doivent approuver ces besoins)		
Mise en marche	***Spécifications :***	
• station de commande locale	spécifiez nombre et endroit :	
• panneau de commande		
Opération normale		
• dispositif surveillance des opérations	spécifiez nombre et endroit :	
Mise à l'arrêt		
• station de commande locale	spécifiez nombre et endroit :	
• panneau de commande		
Mise à l'arrêt		
• station de commande locale	spécifiez nombre et endroit :	
• panneau de commande		
• boutons d'arrêts d'urgence	spécifiez nombre et endroit :	
• dispositifs d'arrêt d'urgence	spécifiez type et endroit :	
Intervention mineure		
• nettoyage de l'aliment. de la matière	élaborer procédure :	
Besoins liés à l'entretien du SPA (le personnel d'entretien doit être consulté et doit approuver ces besoins)		
Consignation des équipements	***Spécifications :***	
• immobilisation des pièces mécaniques	spécifiez nombre et endroit :	
• etc.		
Phénomènes dangereux liés à l'entretien et à l'opération du SPA (l'opération et l'entretien doivent être consultés)		
Risque d'écrasement	**Solution**	**Risque**
• angle entrant non couvert		
• accès à des pièces mécaniques en mouvement		
• etc.		

Annexe B

Liste des acronymes

ADEPA	Agence nationale pour le développement de la production automatisée
AdF	Arbre des fautes, de l'anglais *Fault Tree Analysis (FTA)*
AISS	Association internationale de sécurité sociale
AMDE (*FMEA*)	Analyse des modes de défaillances et de leurs effets, de l'anglais *Failure Modes and Effects Analysis* (*FMEA*)
AMDEC	Analyse des modes de défaillances, de leurs effets et de leur criticité, de l'anglais *Failure Modes, Effects and Criticality Analysis* (*FMECA*)
API	Automate programmable industriel
CCM	Centre de commande des moteurs
CdCF	Cahier des charges fonctionnel
CRAM	Caisse régionale d'assurance maladie
DAO	Dessin assisté par ordinateur
E/E/PES	Électrique/Électronique/Électronique programmable
EPROM	*Erasable Programmable Read Only Memory*
E/S	Entrées / Sorties (modules E/S, dispositifs E/S, etc.)
GEMMA	Guide d'étude des modes de marche et d'arrêt
GRAFCET	Graphe de commande-étape-transition
GRIS	Groupe de recherche en ingénierie simultanée
HAZOP	*HAZard OPerability Analysis*
HSE	*Health and Safety Executive*
INRS	Institut nationale de recherche et de sécurité
IRSST	Institut de recherche en santé et sécurité du travail du Québec
ITI	*Industrial Technology Institute*
LURPA	Laboratoire universitaire de recherche en production automatisée
OMP	Outil, machine, procédé
PC	Partie commande
P&P	Pâtes et papiers (industries des P&P)
SÉP	Système électronique programmable, de l'anglais *Programmable electronic systems (PES)*
PO	Partie opérative
PROM	*Programmable Read Only Memory*
PRP	Processus de réalisation d'un produit ou d'un procédé
RAM	*Random Access Memory*
ROM	*Read Only Memory*
SADT	*Structured Analysis and Design Technique*
SA_RT	*Structured Analysis in Real Time*
SCD	Système de contrôle distribué
SI	Système d'information
SOR	Système d'ordinateurs répartis
SPA	Système de production automatisé
SST	Santé et sécurité du travail
UCT	Unité centrale de traitement
UPS	*Uninterruptible Power Supply*
UVPROM	*Ultra Violet Programmable Read Only Memory*

Appendice 1

Schéma global de la technologie papetière
[AIFQ, 1997]

Appendice 2

Méthodes d'analyse du risque répertoriées dans le cadre
de la thèse de doctorat de F. Gauthier [1997]
(extrait de sa thèse)

Dénomination anglaise	Autres noms et variantes [STEPHANS, R.A., TALSO, W.W., 1993]	Dénomination française (reconnue)
Action Error Analysis		
Accident Analysis		
Barrier Analysis		
Bent Pin Analysis (BPA)		
Cable Failure Matrix (CFMA)		
Cause-Consequence Analysis		
Change Analysis		
Check List Analysis		Analyse par liste-guide
Chemical Process Quantitative Risk Analysis		
Common Cause Analysis	*Root Cause Analysis*	
Comparison-To-Criteria (CTC)	*Compliance Assessment*	
Confined Space Safety	*Enclosed Space Safety*	
Contingency Analysis		
Control Rating Code (CRC) Method		
Critical Incident Technique	*Reported Significant Observations; Unusual Operating reports*	
Criticality Analysis	*Criticality Assessment; Nuclear Criticality Analysis*	Analyse de la "criticité", Estimation du risque
Critical Path Analysis		
Cryogenic Systems Safety Analysis		
Damage Mode and Effects Analysis		
Digraph Utilization Within System Safety		
Double Failure Matrix		
Electromagnetic Compatibility Analysis and Testing		
Energy Analysis	*Flow Analysis*	Analyse énergétique
Energy Trace and Barrier Analysis		
Energy Trace Checklist	*Energetic Analysis*	
Environmental Risk Analysis	*Environmental Engineering Analysis*	
Event and Causal Factor		
Event Tree Analysis		Arbre des événements
External Events Analysis	*Natural Phenomena Hazards Mitigation*	
Facilities System Safety Analysis	*Process Safety Management Report*	
Fault Hazard Analysis		
Failure Modes And Effects Analysis (FMEA)	*Damage Mode and Effects Analysis; Software Failure Modes and Effects Analysis; Failure Modes, Effects, and Criticality Analysis (FMECA); Fault Hazard Analysis*	Analyse des modes de défaillance et de leurs effets (AMDE)
Failure Modes; Effects; and Criticality Analysis (FMECA)		Analyse des modes de défaillance, de leurs effets et de la "criticité" (AMDEC)
Fault Isolation Methodology	*Half-Step Search; Sequential Removal/Replacement; Mass replacement; Lambda Search; Point of Maximal Signal*	

Dénomination anglaise	Autres noms et variantes [STEPHANS, R.A., TALSO, W.W., 1993]	Dénomination française (reconnue)
	Concentration	
Fault Tree Analysis (FTA)		Arbre des fautes
Fire Hazards Analysis		
Flow Analysis		Analyse des flux
Hardware/Software Safety Analysis	*Preliminary Software Hazard Analysis; Follow-On Software Hazard Analysis*	
Hazard Totem Pole		
Hazard and Operability Study (HAZOP)		
Health Hazard Assessment (HHA)	*Process Hazard Analysis*	
Human Error Analysis		Analyse des erreurs humaines
Human Factors Analysis		Analyse du facteur humain; Analyse ergonomique
Human Reliability Analysis (HRA)		
Interface Analysis	*System Hazard Analysis*	
Job Safety Analysis	*Job Hazard Analysis*	
Laser Safety Analysis		
Management Oversight and Risk Tree (MORT)		
Materials Compatibility Analysis		
Maximum Credible Accident/ Worst Case	*Scenario Analysis*	
Modeling	*IDEF Modeling; Simulation; Simulation Modeling*	
Naked man		
Network Logic Analysis		
Nuclear Criticality Analysis	*Criticality Analysis; Criticality Assessment*	
Nuclear Safety Analysis	*Nuclear Safety Assessment; Safety Analysis Report*	
Nuclear Safety Cross-check Analysis		
Operating and Support Hazard Analysis	*Operating Hazards Analysis*	
Petri Net Analysis		
Preliminary Hazard Analysis (PHA)		Analyse préliminaire des dangers
Preliminary Hazard List	*Critical Hazards List; Hazards Tracking List*	
Probabilistic Risk Assessment (PRA)	*Quantitative Risk Analysis; Probabilistic Safety Analysis; Performance Assessment*	
Procedure Analysis	*Test Safety Analysis; Operation Safety Analysis; Maintenance Safety Analysis; Job Safety Analysis...*	
Process Hazard Analysis	*Process Hazard Evaluation*	
Production System Hazard Analysis		
Prototype Development	*Modeling; Simulation Modeling*	
Relative Ranking	*Dow and Mond Hazard Index*	
Repetitive Failure Analysis		
Root Cause Analysis		
Safety Review	*Safety Audit; Process Safety Review; Loss Prevention Review; Process Review*	Revue de sécurité

Dénomination anglaise	Autres noms et variantes [STEPHANS, R.A., TALSO, W.W., 1993]	Dénomination française (reconnue)
Scenario Analysis	*Brainstorming*	
Seismic Analysis		
Sequentially-Timed Events Plot (STEP)		
Single-Point Failure Analysis		
Sneak-Circuit Analysis	*Software Sneak Circuit Analysis (SSCA)*	
Software Failure Modes and Effects Analysis (SFMEA)	*Software fault Hazard Analysis; Software Hazardous Effects Analysis*	
Software Fault Tree Analysis	*Soft Tree Analysis*	
Software Hazard Analysis	*Software Safety Analysis*	
Software Sneak Circuit Analysis (SSCA)		
Statistical Process Control		
Structural Safety Analysis	*Structural Assessment*	
Subsystem Hazard Analysis	*Fault Hazards Analysis*	
System Hazard Analysis (SHA)		
Systemic Inspection		
Systematic Occupational Safety Analysis		
Task Analysis		Analyse de la tâche
Technique for Human Error Prediction (THERP)		
Test Safety Analysis (TSA)		
Time/Loss Analysis (TILA)		
Uncertainty Analysis		
Walk-Through Task Analysis		
What-If Analysis	*What If/Checklist Analysis*	
What If/Checklist Analysis		
Wind/Tornado Analysis		

Appendice 3

Description sommaire des quatorze méthodes d'analyse du risque retenues pour l'approche développée par F. Gauthier [1997] (extrait de sa thèse)

Action Error Analysis

Objectif de l'analyse: Identifier les risques résultant des déviations potentielles dans les actions humaines dans les contextes d'opération, de maintenance, de contrôle, de supervision, etc..

Objet de l'analyse: La description détaillée des diverses tâches (actions) effectuées par l'utilisateur, incluant les situations inhabituelles.

Description de la méthode: Cette méthode d'identification des risques débute par l'identification des possibilités de déviations dans les actions humaines. Pour ce faire, elle utilise une courte liste-guide définissant les différents types de déviations possibles:

- Action requise non accomplie ou partiellement accomplie;
- Action non requise accomplie;
- Action requise répétée;
- Action requise substituée par une autre;
- Action requise accomplie avec délai;
- Action requise accomplie hors séquence.

Les analystes procèdent donc systématiquement en appliquant la liste-guide à chacune des actions effectuées par le ou les utilisateurs. Lorsqu'une déviation possible (vraisemblable) est identifiée, l'analyse se poursuit dans un mode inductif pour l'identification des effets potentiels et des risques engendrés par cette déviation.

Limitations de la méthode: Les facteurs de risque techniques, organisationnels et externes ne sont généralement que très peu couverts par cette méthode. Elle permet d'identifier principalement les facteurs de risque humains. Toutefois, les causes de ces facteurs de risque, c'est-à-dire les causes des déviations dans les actions humaines (ou comment l'humain traite l'information), ne sont qu'exceptionnellement identifiées. De plus, la méthode ne permet pas d'identifier les risques engendrés par une combinaison de déviations dans les actions humaines.

Utilisation dans le PRP: La méthode peut être utilisée dans toutes les phases du PRP. Il est toutefois nécessaire que l'OMP soit suffisamment défini pour que les analystes soient en mesure d'établir la liste des diverses tâches (actions) effectuées par l'utilisateur. Son efficacité d'utilisation dans les premières phases du PRP peut donc être limitée.

Références: [WHALLEY, S.P., MAUND, J.K., 1986], [RYAN, J.P. 1986], [SUOKAS, J., 1988], [TOOLA, A., 1992], [REUNANEN, M., 1993a], [HARMS-RINGDAHL, L., 1993], [LEVESON, N.G., 1995], [AMERICAN INSTITUTE OF CHEMICAL ENGINEERS, 1992].

Check List Analysis

Objectif de l'analyse:	Faciliter l'identification de facteurs de risque en utilisant des listes préparées. Ces listes peuvent indiquer les bonnes pratiques à respecter, les situations à éviter, les types de déviations possibles, les éléments de la conception à considérer, etc..
Objets de l'analyse:	Cette méthode peut être utilisée pour faciliter l'identification de facteurs de risque dans plusieurs contextes: analyse de la structure fonctionnelle, analyse de la conception préliminaire ou détaillée, analyse de la tâche ou des procédures, etc..
Description de la méthode:	Les listes-guide sont depuis toujours utilisées en conception, que ce soit pour l'aspect SST, ou pour tout autre aspect du produit. Elles peuvent être applicables à une classe générale de problèmes ou à un problème spécifique à un produit particulier. Utilisée comme outil de conception, cette méthode peut être adaptée à l'identification des facteurs de risque présents dans une conception. L'application de cette méthode informative consiste à contrôler chacun des points de la liste sur le sujet analysé. Elle est généralement utilisée conjointement avec d'autres méthodes d'analyse des risques. Dans ce cas, la liste-guide utilisée correspond à l'optique particulière de la méthode utilisée conjointement.
Limitations de la méthode:	Le danger d'utilisation de cette méthode pour l'identification des risques est que les concepteurs ne s'en remettent uniquement à celle-ci pour assurer la sécurité de l'OMP. Par ailleurs, malgré une apparente simplicité, la préparation d'une bonne liste-guide requiert du temps, du sérieux et de l'expérience. L'efficacité de l'analyse dépend donc souvent de l'expertise de ceux qui ont préparé la liste. De plus, la majorité des listes-guide sont orientées vers l'identification de facteurs de risque techniques.
Utilisation dans le PRP:	Considérant que l'objet de l'analyse est aussi varié que les listes-guide elles-mêmes, cette méthode peut être utilisée dans toutes les phases du PRP.
Références:	[KOLB, J., ROSS, S.S., 1980], [ROBERTS, R.H., 1989], [STEPHANS, R.A., TALSO, W.W., 1993], [LEVESON, N.G., 1995] [AMERICAN INSTITUTE OF CHEMICAL ENGINEERS, 1992].

Critical Incident Technique

Objectif de l'analyse:	Répertorier les risques et les situations dangereuses vécus ou connus des personnes dans l'entourage de l'OMP.
Objet de l'analyse:	L'historique d'utilisation de l'OMP par le biais de l'expérience des utilisateurs et des informations écrites disponibles (rapports, littérature, banques de données, etc..).
Description de la méthode:	Cette méthode consiste d'une part à interroger (directement ou par questionnaire) les utilisateurs d'expérience de l'OMP à concevoir (ou d'un produit similaire), et, d'autre part, à analyser les informations écrites disponibles (rapports, littérature, banques de données, etc..) pour répertorier les risques et/ou les situations dangereuses vécus dans le passé. Moyennant une certaine préparation, cette méthode est simple, rapide et efficace. Les informations recueillies concernent les erreurs communes, les risques perçus, les incidents ("passer-proche" ou quasi-accidents) et leurs fréquences, ainsi les solutions apportées ou proposées pour éviter ces événements. Parfois, ces informations peuvent servir à estimer la "criticité" des risques identifiés.
Limitations de la méthode:	Cette méthode ne peut être appliquée qu'à un OMP qui dispose d'un historique d'opération suffisant. Elle est également limitée par l'étendue des informations concernant les situations dangereuses observées. Aussi, les utilisateurs de la méthode doivent prendre en considération la tendance naturelle des personnes à déformer les faits.
Utilisation dans le PRP:	La méthode étant une méthode rétrospective d'identification des risques et de leurs causes, elle doit normalement être utilisée dans la phase de pré-étude du PRP.
Références:	[STEPHANS, R.A., TALSO, W.W., 1993], [GALLAGHER, V.A., 1991], [KANIS, H., WEEGELS, M.F., 1990].

Criticality Analysis

Objectif de l'analyse:	Estimer la "criticité" des différents risques identifiés. La "criticité" aide les concepteurs à choisir les actions correctives nécessaires et leurs priorités et à établir clairement la frontière entre le risque acceptable et celui qui ne l'est pas.
Objet de l'analyse:	Une série de différents scénarios de risque. Un scénario de risque est la conjonction du risque et d'une de ses chaînes de causalité.
Description de la méthode:	Cette analyse consiste à estimer, à partir des meilleures informations disponibles, la "criticité" de différents scénarios de risque. La "criticité" est le résultat de la combinaison de l'estimation de la gravité des conséquences et de l'estimation de la probabilité d'occurrence des dommages. L'estimation peut être qualitative ou quantitative. Certaines normes identifient des lignes directrices pour la définition de la "criticité" d'un risque en fonction de sa probabilité d'occurrence et de la gravité des conséquences. Souvent, ces lignes directrices doivent être adaptées pour correspondre aux caractéristiques de chaque cas particulier. Il appartient également aux utilisateurs de ces normes de choisir les mesures de sécurité adéquates en fonction de leurs évaluations de la "criticité".
Limitations de la méthode:	Cette méthode démarre à partir des risques et de leurs causes identifiés par d'autres méthodes. De plus, l'estimation étant le plus souvent basée sur des informations qualitatives, les résultats de l'application de cette méthode doivent être pris comme des lignes directrices et non comme des absolus.
Utilisation dans le PRP:	Cette méthode est communément utilisée pour l'estimation de la "criticité" des risques dans toutes les phases du PRP.
Références:	[STEPHANS, R.A., TALSO, W.W., 1993], [NF X60-510], [MIL-STD-1629A], [prEN 1050, 1995].

Energy Analysis

Objectif de l'analyse:	Identifier les risques résultant de la présence ou de la libération de toutes les formes d'énergie présentes dans un OMP.
Objet de l'analyse:	La définition de l'OMP ou d'un de ses composants, incluant des informations sur les éléments (à un niveau fonctionnel, conceptuel ou tangible) qui contiennent, utilisent, ou transportent de l'énergie sous toutes ses formes. Des informations sur les risques occasionnés par certaines formes d'énergie peuvent également être nécessaires.
Description de la méthode:	Cette méthode se base sur l'hypothèse que si l'énergie contenue dans un système est connue et contrôlée, cette énergie ne pourra être une source de danger. Ainsi, l'analyste doit d'abord rechercher les différentes sources d'énergie présentes dans un OMP et les possibilités de libération de cette énergie. Puis, dans un mode d'analyse inductif, il doit identifier les risques associés à la présence ou à la libération de cette énergie. Cette méthode, quoique incomplète, présente tout de même l'avantage de montrer l'OMP sous un angle différent. La perception immatérielle de l'OMP qui s'offre au concepteur lui permet d'identifier des risques qui sont souvent bien cachés.
Limitations de la méthode:	La méthode est applicable à tous les OMP qui contiennent, utilisent, ou transportent de l'énergie sous toutes ses formes. L'identification des sources d'énergie et l'évaluation de l'efficacité des moyens mis en place pour les contenir ne posent généralement pas de problèmes. Toutefois, l'analyse peut devenir complexe si le système de contrôle de l'OMP joue un rôle important dans la maîtrise de l'énergie. Par ailleurs, la méthode ne permet d'identifier que dans une faible mesure les risques engendrés par une combinaison de différentes sources d'énergie.
Utilisation dans le PRP:	La littérature ne fait aucune allusion à des limitations en ce qui concerne l'application de cette méthode dans le PRP. Toutefois, il apparaît évident que l'efficacité de la méthode est à son meilleur lorsque la conception est juste assez définie pour permettre l'identification des principales formes d'énergie qui s'y trouvent, sans toutefois que le niveau de détail complique l'analyse. L'approche devrait donc être employée préférablement dans les phases conceptuelles du PRP, soit les phases PRP 1 et 2.
Références:	[STEPHANS, R.A., TALSO, W.W., 1993], [RAHEJA, D.G., 1991], [GALLAGHER, V.A., 1988], [HUNTER, T.A., 1992], [HARMS-RINGDAHL, L., 1987], [HARMS-RINGDAHL, L., 1993].

External Events Analysis

Objectif de l'analyse:	Identifier les risques pouvant être occasionnés par des événements extérieurs à l'OMP.
Objet de l'analyse:	La définition de l'OMP (conceptuel ou tangible) et de son environnement.
Description de la méthode:	La première étape de l'application de cette méthode consiste à identifier les événements qui peuvent se produire dans l'environnement de l'OMP (phénomènes naturels, incendie, défaillance d'un OMP connexe, sabotage, etc..). L'analyse de poursuit ensuite dans un mode inductif pour identifier les effets potentiels de ces événements sur l'OMP, et finalement les risques qu'ils peuvent engendrer. Les effets directs et indirects des événements externes doivent être considérés dans cette partie de l'analyse.
Limitations de la méthode:	La méthode ne permet d'identifier que les facteurs de risque externes et leurs conséquences. De plus, elle ne permet d'identifier que dans une faible mesure les risques engendrés par une combinaison d'événements externes.
Utilisation dans le PRP:	Théoriquement, cette méthode peut être utilisée dans toutes les phases du PRP. Toutefois, la littérature indique que son efficacité est à son meilleur lorsque la conception est bien définie. L'approche devrait donc être employée préférablement à partir de la phase PRP 2.
Référence:	[STEPHANS, R.A., TALSO, W.W., 1993].

Failure Modes And Effects Analysis (FMEA)

Objectif de l'analyse:	Identifier les risques résultant des défaillances potentielles des composantes de l'OMP.
Objet de l'analyse:	La définition de l'OMP et de ses éléments, incluant leurs divers modes de défaillances.
Description de la méthode:	L'analyse débute avec chacun des éléments du système, dont on étudie les possibilités de défaillances en fonction de tous les modes opérationnels. Elle se poursuit ensuite dans un mode inductif pour l'identification des effets potentiels de ces défaillances et des risques engendrés. Cette méthode est souvent utilisée conjointement avec la méthode *Criticality Analysis*, formant le *FMECA*.
Limitations de la méthode:	Le *FMEA* est une méthode de base, utilisée pour les analyses grossières, et doit être complétée par d'autres méthodes, notamment pour l'étude des défaillances multiples et des effets séquentiels. Cette méthode est néanmoins très exigeante en terme de temps et demande une certaine expérience pratique de la part de ses utilisateurs. Par conséquent, elle n'est que rarement utilisée sur des systèmes entiers, mais plutôt sur des sous-systèmes ou des composantes critiques. Par ailleurs, la méthode permet d'identifier presque exclusivement les facteurs de risque techniques reliés aux défaillances des composantes. Les facteurs de risque humains, organisationnels et externes ne sont pas couverts par cette méthode.
Utilisation dans le PRP:	La littérature précise généralement que cette méthode est à son meilleur dans la phase de conception détaillée de l'OMP (PRP 3). Toutefois, certains auteurs soutiennent qu'elle peut être tout aussi efficace lorsque appliquée à la structure fonctionnelle de l'OMP en phase PRP 1, moyennant une certaine adaptation de son approche en vue de l'analyse de fonctions au lieu de composantes.
Références:	[STEPHANS, R.A., TALSO, W.W., 1993], [KOLB, J. ROSS, S.S., 1980], [ROBERTS, N.H., et al., 1981], [TOOLA, A., 1992], [NF X60-510], [MIL-STD-1629A], [HALEBSKY, M., 1989], [AMERICAN INSTITUTE OF CHEMICAL ENGINEERS, 1992], [REUNANEN, M., 1993a], [HARMS-RINGDAHL, L., 1993], [LEVESON, N.G., 1995].

Fault Tree Analysis (FTA)

Objectifs de l'analyse:	Identifier les causes et développer les diverses chaînes de causalité d'un risque ou d'un facteur de risque (l'événement sommet). Dans certains cas, la méthode peut aussi servir à estimer quantitativement la probabilité d'occurrence de l'événement sommet.
Objet de l'analyse:	Un événement sommet quelconque, généralement un risque ou un facteur de risque de nature technique. Des facteurs de risque humains ou externes peuvent également faire l'objet de l'analyse.
Description de la méthode:	Cette méthode est une représentation graphique des multiples causes d'un événement. Elle permet de visualiser les relations entre les défaillances d'équipements, les erreurs humaines et les facteurs environnementaux qui peuvent conduire à des accidents. Les résultats qu'elle produit sont généralement qualitatifs, mais peuvent facilement être quantifiés si des données statistiques sont introduites dans le modèle. Dans la construction d'un arbre des fautes, on place l'effet indésirable que l'on souhaite étudier (l'événement sommet) en haut de l'arbre et on examine, dans un mode déductif, les événements (les fautes et les défaillances) qui peuvent l'engendrer. Les différentes relations entre les événements, fautes et défaillances sont exprimées par des symboles qui sont des opérateurs logiques d'algèbre booléenne. La méthode peut également être utilisée dans un mode rétrospectif pour la reconstitution détaillée d'événements passés.
Limitations de la méthode:	La construction de ces arbres peut être un exercice très coûteux en terme de temps, et doit être justifiée par l'importance de l'événement sommet choisi. Par conséquent, la méthode n'est généralement appliquée qu'à des risques ou des facteurs de risque très critiques.
Utilisation dans le PRP:	Compte tenu de la diversité des événements sommets qui peuvent être analysés, cette méthode peut être utilisée dans toutes les phases du PRP. Toutefois, lorsque l'analyse porte spécifiquement sur des aspects très techniques de fautes d'équipements (par exemple, la recherche des causes du démarrage intempestif d'un équipement automatisé), la méthode est plus efficace dans les phases PRP 3 et 4.
Références:	[STEPHANS, R.A., TALSO, W.W., 1993], [KAVIANIAN H.R., et al., 1990], [ROBERTS N.H., et al., 1981], [MARINISSEN A.H., et al., 1986], [TOOLA, A., 1992], [REUNANEN, M., 1993a], [HARMS-RINGDAHL, L., 1993], [LEVESON, N.G., 1995] [AMERICAN INSTITUTE OF CHEMICAL ENGINEERS, 1992].

Hazard and Operability Study (HAZOP)

Objectif de l'analyse: L'objectif poursuivi par l'utilisation de cette méthode est d'identifier les risques qui apparaissent lors d'une déviation des conditions normales de fonctionnement de l'OMP.

Objet de l'analyse: La définition de l'OMP ou d'un de ses composants (structure fonctionnelle et/ou dessins techniques, schémas de contrôle), ses conditions de fonctionnement, des informations sur les matériaux et produits transformés et, dans une certaine mesure, les procédures d'utilisation.

Description de la méthode: Cette méthode d'identification des risques débute par l'identification des possibilités de déviations dans le fonctionnement de l'OMP ou les actions humaines. Pour ce faire, elle utilise une série de mots clés définissant les différents types de déviations possibles:

- Pas, non, aucun;
- Plus;
- Moins;
- Aussi, pendant que;
- Partiellement;
- Inversé;
- Au lieu de.

La méthode favorise donc la recherche systématique et créative des déviations. Lorsqu'une déviation possible (vraisemblable) est identifiée, l'analyse se poursuit dans un mode inductif pour l'identification des effets potentiels et des risques engendrés par cette déviation. Finalement, la méthode se termine dans un mode déductif par l'identification sommaire des causes potentielles des déviations critiques identifiées.

Limitations de la méthode: Des études ont démontré que cette méthode était une des plus performantes en terme de la quantité de facteurs de risque identifiés. On note cependant certaines lacunes au niveau de l'identification des facteurs de risque externes et organisationnels. De plus, elle ne permet d'identifier que dans une faible mesure les risques engendrés par une combinaison de facteurs de risque.

Utilisation dans le PRP: La littérature ne fait aucune allusion à des limitations en ce qui concerne l'application de cette méthode dans le PRP. Toutefois, certains auteurs recommandent qu'elle soit appliquée tôt dans le PRP, de façon à ne pas limiter les possibilités de maîtriser les risques identifiés.

Références: [STEPHANS, R.A., TALSO, W.W., 1993], [TOOLA, A., 1992], [REUNANEN, M., 1993a], [HARMS-RINGDAHL, L., 1993], [LEVESON, N.G., 1995] [AMERICAN INSTITUTE OF CHEMICAL ENGINEERS, 1992].

Procedure Analysis

Objectif de l'analyse: Identifier les risques inhérents à la définition des procédures d'utilisation de l'OMP.

Objet de l'analyse: Les procédures d'utilisation écrites (préliminaires ou finales) de l'OMP, pour toutes les phases de son cycle de vie (essais, transport, installation, maintenance, opération, etc..).

Description de la méthode: Cette méthode consiste en une revue étape par étape des procédures d'utilisation de l'OMP afin d'identifier les risques auxquels peuvent être exposés les utilisateurs. Cette analyse inductive permet également d'identifier les effets potentiels du non-respect des procédures établies.

Limitations de la méthode: La méthode permet d'identifier prioritairement les facteurs de risques organisationnels tels que des défauts au niveau de:

- L'organisation du travail;
- Des communications;
- De la gestion de l'information;
- De la formation;
- De l'allocation des ressources;
- Etc..

Il n'est toutefois pas exclu que certains facteurs de risque humains soient identifiés par la méthode. Ainsi, dans certains cas les résultats obtenus peuvent recouper ceux obtenus par la méthode *Action Error Analysis*. Cette dernière est néanmoins plus détaillée et permet une identification plus complète des facteurs de risque humains.

Utilisation dans le PRP: Compte tenu des informations nécessaires à l'application de cette méthode (procédures d'utilisation écrites), celle-ci est difficilement applicable avant la phase PRP 3.

Références: [STEPHANS, R.A., TALSO, W.W., 1993], [LEVESON, N.G., 1995], [HAMMER, W., 1972].

Production System Hazard Analysis

Objectifs de l'analyse:	Rechercher les défauts et/ou les erreurs potentiels dans la fabrication de l'OMP qui pourraient être à la source de risque identifiés préalablement.
Objet de l'analyse:	Les procédures et procédés de fabrication et d'assemblage, les moyens de contrôle de la qualité, les procédures de tests, etc..
Description de la méthode:	Cette méthode prospective déductive démarre à partir de facteurs de risque techniques identifiés préalablement par d'autres méthodes. Pour ces facteurs de risque, l'analyste tente d'identifier leurs causes potentielles qui pourraient être introduites au moment de la fabrication de l'assemblage de l'OMP.
Limitations de la méthode:	En raison des analyses très pointues qu'elle propose, cette méthode ne peut servir à identifier les causes potentielles que d'un très petit nombre de facteurs de risque.
Utilisation dans le PRP:	Compte tenu des informations nécessaires à l'application de cette méthode (les procédures et procédés de fabrication et d'assemblage, les moyens de contrôle de la qualité, les procédures de tests, etc..), celle-ci ne peut être appliquée que durant les phases PRP 3 et 4, la dernière offrant généralement une efficacité maximale.
Références:	[STEPHANS, R.A., TALSO, W.W., 1993].

Safety Review

Objectifs de l'analyse:	Identifier les risques et leurs causes au fur et à mesure de l'avancement de la conception d'un OMP.
Objet de l'analyse:	La définition de l'OMP selon le niveau d'avancement de la conception ainsi que les résultats des analyses de risques réalisées au préalable.
Description de la méthode:	Cette méthode consiste à rassembler les personnes-ressources nécessaires pour effectuer des révisions régulières de la sécurité de la conception au fur et à mesure de son avancement. La conformité aux normes, l'analyse ergonomique, la hiérarchie des contrôles, la prédiction des mauvais usages et des erreurs d'opération, les risques résiduels, la formation des opérateurs, les mises en garde, etc.. sont parmi les points examinés lors de ces revues. Plus de détails concernant la planification et la réalisation des revues de sécurité formelles en conception sont présentés à l'appendice 5.
Limitations de la méthode:	Les revues de sécurité doivent être réalisées indépendamment de toute autre activité de conception afin d'assurer l'intégrité de l'objectif principal de cet exercice: la sécurité. De plus, chacune des étapes ou revues nécessite plusieurs activités préparatoires qui doivent être effectuées avant la ou les rencontres. Les résultats des revues de sécurité dépendent donc fortement de la qualité du travail préparatoire, de l'expérience du président d'assemblée et de l'expertise des personnes formant l'équipe de revue.
Utilisation dans le PRP:	On retrouve, règle générale, trois revues de sécurité formelles: la revue préliminaire (PRP 1), la revue de la conception détaillée et du prototype (PRP 3) et la revue de certification finale (PRP 4) (voir la section 6.3). En plus de ces revues formelles, plusieurs revues informelles peuvent être utilisées comme méthode d'analyse des risques (en mode inductif et déductif) dans le PRP.
Références:	[ASME, 1984], [FLORES, A., 1983], [KOLB, J., ROSS, S.S., 1980], [GALLAGHER, V.A., 1991], [STEPHANS, R.A., TALSO, W.W., 1993] [HUNTER, T.A., 1992], [AMERICAN INSTITUTE OF CHEMICAL ENGINEERS, 1992].

Task Analysis

Objectifs de l'analyse:	Identifier les risques et/ou les facteurs de risque inhérents à l'accomplissement d'une tâche quelconque pendant l'utilisation de l'OMP.
Objet de l'analyse:	La situation réelle de travail dans toutes les phases d'utilisation de l'OMP (essais, transport, installation, maintenance, opération, etc..).
Description de la méthode:	La méthode est basée sur l'observation de la situation réelle de travail pour y identifier les risques inhérents à la tâche ou les façons de faire pouvant constituer des facteurs de risque. L'analyse peut donc être réalisée à la fois dans un mode inductif et déductif. De plus, cette méthode peut être utilisée dans un mode rétrospectif pour l'identification et l'analyse de situations dangereuses vécues. Des entrevues avec les utilisateurs ainsi que des questionnaires peuvent également être utilisés pour réaliser ces analyses. Cette méthode est souvent utilisée conjointement avec d'autres méthodes de façon à accroître la compréhension de la situation de travail et ainsi favoriser l'identification des risques et de leurs causes.
Limitations de la méthode:	La méthode peut être difficile à appliquer à des situations de travail complexes ou nécessitant de multiples prises de décisions. Elle permet par ailleurs d'analyser en profondeur les risques identifiés sans pour autant que tous les risques présents soient répertoriés.
Utilisation dans le PRP:	La méthode peut être utilisée dans toutes les phases du PRP. Il est toutefois nécessaire qu'un OMP similaire à celui à concevoir soit déjà en utilisation. Elle ne peut donc pas être appliquée à des OMP complètement nouveaux.
Références:	[STEPHANS, R.A., TALSO, W.W., 1993], [LEVESON, N.G., 1995], [HAMMER, W., 1972], [HUNTER, T.A., 1992].

What-If Analysis

Objectif de l'analyse:	Identifier les risques potentiels découlant de facteurs de risque divers.
Objet de l'analyse:	Cette méthode peut être utilisée pour l'identification des risques dans plusieurs contextes: analyse de la structure fonctionnelle, analyse de la conception préliminaire ou détaillée, analyse de la tâche ou des procédures, etc..
Description de la méthode:	Cette méthode est la plus simple des méthodes d'analyse prospective inductive. Elle consiste à réaliser un *brainstorming* orienté pour la recherche des effets potentiels d'événements ou de situations définies. En posant la question "Qu'arrive-t-il si...?", les analystes envisagent les effets potentiels d'un événement ou d'une situation définie. Les facteurs de risque (les événements ou les situations définies) servant au démarrage de l'analyse peuvent être issus d'analyses précédentes ou être simplement identifiés dans le cadre du *brainstorming*. Idéalement, cette méthode est réalisée en groupes de 3 à 8 personnes.
Limitations de la méthode:	Cette méthode est simple et rapide, mais son optique est trop vague pour que tous les effets potentiels d'un événement ou d'une situation soient identifiés. Le niveau de profondeur de l'analyse est donc généralement faible.
Utilisation dans le PRP:	Cette méthode peut être utilisée pour des analyses prospectives inductives dans toutes les phases du PRP.
Références:	[STEPHANS, R.A., TALSO, W.W., 1993], [LEVESON, N.G., 1995], [AMERICAN INSTITUTE OF CHEMICAL ENGINEERS, 1992]

Les quatorze méthodes présentées dans le début de cet appendice ont également été classifiées par F. Gauthier [1997] selon les diverses catégories présentées dans l'état des connaissances à la section 2.2.2.2. Aussi, le degré de profondeur de l'analyse est donné pour chacune des quatorze méthodes présentées. Ainsi, une cote de 3 signifie que la méthode permet une très bonne profondeur d'analyse mais, en contrepartie, elle signifie que la méthode est souvent plus complexe à mettre en oeuvre.

TABLEAU A3-1 CLASSIFICATION DES QUATORZE MÉTHODES D'ANALYSE DU RISQUE [GAUTHIER, F., 1997]

Nom de la méthode	Estimation du risque	Identification des phénomènes dangereux et de leurs causes	Analyse informative	Analyse rétrospective (déductive)	Analyse prospective inductive	Analyse prospective déductive	Identification de facteurs de risque techniques	Identification de facteurs de risque humains	Identification de facteurs de risque organisationnels	Identification de facteurs de risque externes	Type ergonomique	Combinaison de facteurs de risque	Profondeur de l'analyse
Action Error Analysis		✓			✓			✓			✓		2
Check List Analysis		✓	✓				✓						1
Critical Incident Technique	✓	✓		✓			✓	✓	✓	✓			1
Criticality Analysis	✓												n/a
Energy Analysis		✓			✓		✓				✓		1
External Events Analysis		✓			✓					✓	✓		1
Failure Modes And Effects Analysis (FMEA)		✓			✓		✓						2
Fault Tree Analysis (FTA)	✓	✓		✓		✓	✓	✓		✓		✓	3
Hazard and Operability Study (HAZOP)		✓			✓	✓	✓	✓			✓		2
Procedure Analysis		✓			✓				✓		✓		1
Production System Hazard Analysis		✓				✓	✓	✓	✓				3
Safety Review		✓			✓	✓	✓	✓	✓	✓			1
Task Analysis		✓		✓	✓	✓	✓	✓	✓				3
What-If Analysis		✓			✓		✓	✓	✓	✓			1

Appendice 4

Le GEMMA : Guide d'étude des modes de marche et d'arrêt
[ADEPA, s.d.]

Le GEMMA, ou guide d'étude des modes de marche et arrêt, a été développé en vue de rendre systématique l'identification des divers modes opérationnels possibles pour un SPA. Le tableau suivant présente l'ensemble des définitions proposées pour établir un langage commun.

TABLEAU A4-1 ENSEMBLE DES ÉTATS DE MARCHE ET D'ARRÊT POSSIBLES SELON LE GEMMA

	Procédures de fonctionnement	
F1	*production normale*	Dans cet état, la machine produit normalement : c'est l'état pour lequel elle a été conçue.
F2	*marche de préparation*	Cet état est utilisé pour les machines nécessitant une préparation préalable à la production normale : préchauffage de l'outillage, remplissage de la machine, etc.
F3	*marche de clôture*	C'est l'état nécessaire pour certaines machines devant être vidées, nettoyées, etc. en fin de journée ou en fin de série.
F4	*marche de vérification dans le désordre*	Cet état permet de vérifier certaines fonctions ou certains mouvements sur la machine, sans respecter l'ordre du cycle.
F5	*marche de vérification dans l'ordre*	Dans cet état, le cycle de production peut être exploré au rythme voulu par la personne effectuant la vérification, la machine pouvant produire ou ne pas produire.
F6	*marche de test*	Les machines de contrôle, de mesure, de tri, etc. comportent des capteurs qui doivent être réglés ou étalonné périodiquement : la *marche de test* F6 permet ces opérations de réglage ou d'étalonnage.
	Procédures d'arrêt de la partie opérative	
A1	*arrêt dans l'état initial*	C'est l'état «repos» de la machine. Il correspond en général à la situation initiale du GRAFCET : c'est pourquoi, comme une étape initiale, il est entouré d'un double cadre.
A2	*arrêt demandé en fin de cycle*	Lorsque l'arrêt est demandé, la machine continue de produire jusqu'à la fin du cycle : c'est un état transitoire vers A3.
A3	*arrêt demandé dans état déterminé*	La machine continue de produire jusqu'à un arrêt en une position autre que la fin de cycle : c'est un état transitoire vers A4.
A4	*arrêt obtenu*	La machine est alors arrêtée en une autre position que la fin de cycle.
A5	*préparation pour remise en route après défaillance*	C'est dans cet état que l'on procède à toutes les opérations (dégagements, nettoyages, etc.) nécessaire à une remise en route après défaillance.
A6	*mise PO dans état initial*	La machine étant en A6, on remet manuellement ou automatiquement la partie opérative en position pour un redémarrage dans l'état initial.
A7	*mise PO dans état déterminé*	La machine étant en A7, on remet la PO en position pour un redémarrage dans une position autre que l'état initial.
	Procédures en défaillance	
D1	*arrêt d'urgence*	C'est l'état pris lors d'un arrêt d'urgence : on y prévoit non seulement les arrêts, mais aussi les cycles de dégagement, les procédures et précautions nécessaires pour éviter ou limiter les conséquences dues à la défaillance.
D2	*diagnostic et/ou traitement de défaillance*	C'est dans cet état que la machine peut être examinée après défaillance et qu'il peut être apporté un traitement permettant un redémarrage.
D3	*production tout de même*	Il est parfois nécessaire de continuer la production même après défaillance de la machine : on aura alors une «production dégradée» ou une «production forcée» ou une production aidée par des opérateurs non prévue en *production normale*.

Pour établir des liens entre tous ces modes de marche et d'arrêt, ces définitions ont été disposées sur un guide graphique standard reproduit à la figure A4-1 (page suivante).

La procédure à suivre est très simple : chacun des modes de marches et d'arrêts applicables à l'automatisme à concevoir sont identifiés, transposés sur le guide graphique et finalement reliés entre eux en indiquant quelles fonctions doivent être accomplies pour passer d'un état à l'autre. Ainsi, des spécifications fonctionnelles supplémentaires peuvent être obtenues, ce qui pourra compléter l'élaboration des besoins et des contraintes.

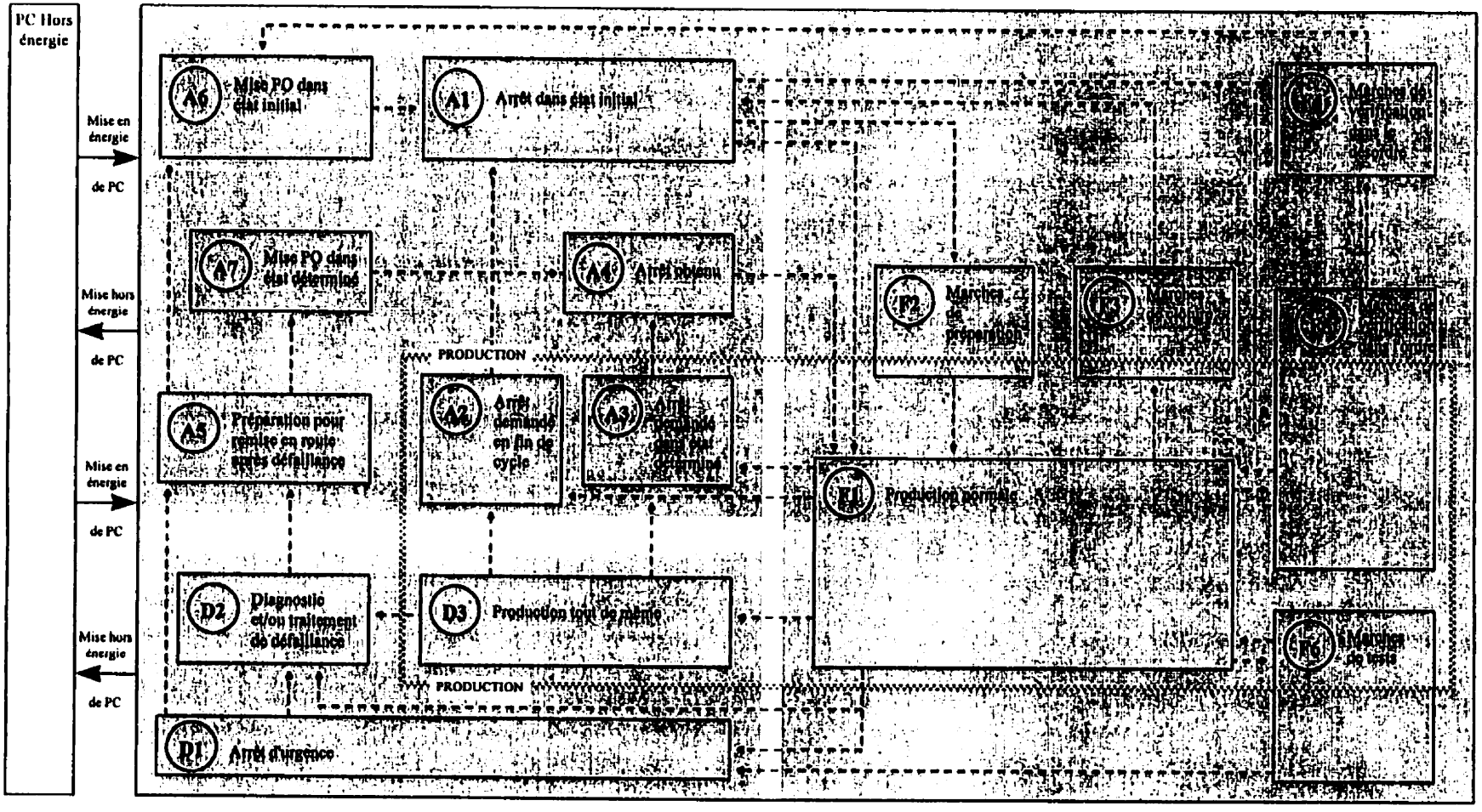

Figure A4-1 Représentation graphique des divers modes de marche et d'arrêt

Appendice 5

Approche proposée par l'*Industrial Technology Institute*
[BUGAJSKI, P. et coll., 1991]

L'approche proposée par l'*Industrial Technology Institute* (ITI) dont il a été question à la section 2.2.6.4 est résumée dans la figure qui suit. L'approche originale est davantage détaillée et est notamment présentée sous forme d'arbre de décisions. Cependant, pour éviter toute lourdeur, les informations pertinentes et importantes ont été regroupées dans cette figure.

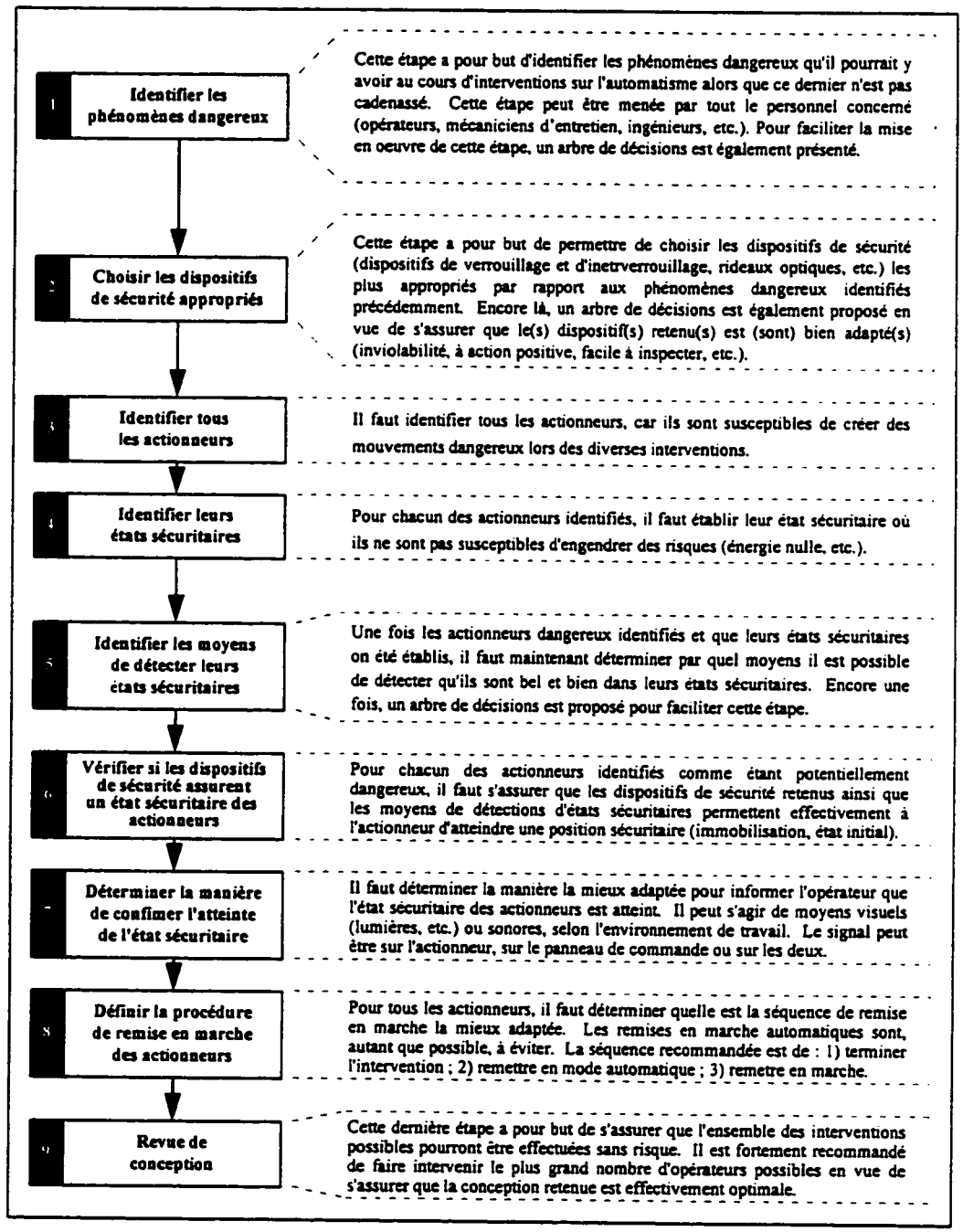

Figure A5-1 Approche proposée par l'ITI

Appendice 6

Approche proposée par G. Rouchouse [1992]

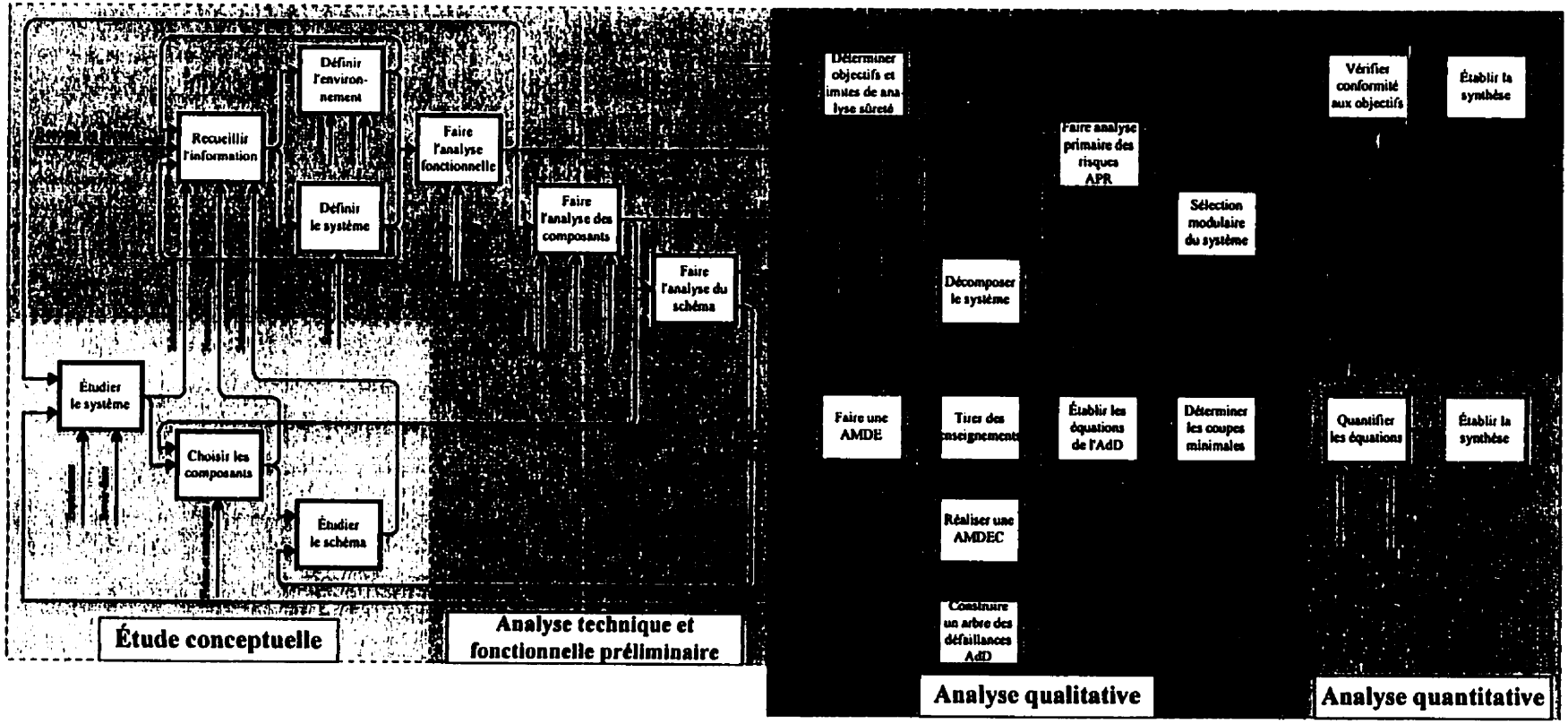

Figure A6-1 Approche proposée par G. Rouchouse [1992]

Appendice 7

Déroulement d'une revue de sécurité

La réalisation d'une revue de sécurité nécessite plusieurs activités préparatoires et la façon de la diriger, de même que la qualité de ces activités préparatoires, influencent donc l'efficacité de la revue de sécurité [GAUTHIER, F., 1997] [MURRAY, A., 1996]. Une revue de conception SST nécessite donc un ensemble d'actions spécifiques qui doivent être entreprises par les membres de l'équipe de conception. Voici quelques indications pouvant aider au succès d'une revue de sécurité[29].

Composition de l'équipe de revue

- L'équipe de revue est présidée par un responsable, typiquement un ingénieur senior, possédant tact et leadership de même qu'un solide bagage technique, des connaissances diversifiées (particulièrement sur les aspects de la SST) ainsi qu'une juste compréhension des exigences de la conception.
- L'équipe de revue comprend généralement le responsable du projet, les membres de l'équipe de conception et les spécialistes de l'entreprise qui, tout en possédant les connaissances et l'expérience nécessaires pour examiner la conception et en comprendre les implications, ne sont pas directement impliqués dans le développement du SPA de façon à pouvoir conserver leur objectivité. Au besoin, l'équipe de revue peut comprendre des personnes de l'extérieur de l'entreprise (consultants, experts, fournisseurs, etc..)
- Cinq (5) à dix (10) intervenants participent généralement à la revue. Il est toutefois possible, selon certains facteurs propres à l'organisation ou au SPA à concevoir, qu'un nombre supérieur de personnes assistent à la revue.
- Les intervenants doivent être suffisamment qualifiés pour être capables d'évaluer les divers aspects touchant la SST pour le SPA aussi bien que les autres aspects de la conception. Ils doivent également posséder de l'imagination combinée à un sens pratique et être aptes à fournir des critiques constructives et objectives, dénudées de préjugés.
- En situation contractuelle, un représentant du contractant doit être présent aux revues de sécurité.

---

[29] Cet appendice est basé sur l'appendice 10 du mémoire de A. Murray [1996] et sur l'appendice 5 de la thèse de F. Gauthier [1997].

Planification de la revue

- Le leadership en matière de planification des revues de sécurité revient habituellement à la fonction d'ingénierie, et plus spécifiquement, en règle générale, au responsable du projet. Celui-ci doit décider de la tenue de telles rencontres, fixer une date, en aviser l'organisation et nommer un président d'assemblée.
- Il doit au préalable définir l'optique de la ou des revues, en se basant sur les bonnes pratiques établies dans l'entreprise. En effet, pour un SPA complexe, il peut être choisi de mener plusieurs revues séparées, une pour chacun de ses principaux systèmes. Des équipes différentes peuvent alors être formées pour chacune de ces revues.
- Le président d'assemblée est en charge de l'élaboration de l'agenda de la rencontre ainsi que des divers détails concernant la logistique (locaux, matériel nécessaire, etc.).
- L'équipe de conception a pour responsabilité de rassembler toute l'information nécessaire à la revue (spécifications, dessins, *layouts*, exigences du client, résultats des analyses du risque, solutions proposées pour la maîtrise des phénomènes dangereux, estimation des coûts, résultats de tests, d'essais et d'analyses, calculs, etc.. en fonction du type de revue) ainsi que les informations décrivant l'état de la conception et l'approche de conception employée. Le dossier de sécurité de conception ainsi constitué est distribué, de pair avec l'agenda, aux intervenants qui participeront à la revue. L'information doit être envoyée suffisamment à l'avance afin de laisser le temps aux membres de l'équipe de revue de se familiariser avec la conception et de préparer leurs questions.

Déroulement de la revue

- La revue de sécurité se déroule habituellement en trois phases: l'introduction, la présentation des résultats et la clôture.
- La phase d'introduction débute normalement par une brève déclaration du président rappelant les objectifs de la rencontre et mettant l'accent sur l'importance d'une revue critique et objective. Le responsable de la conception expose ensuite les grandes lignes de la conception, c'est-à-dire les exigences importantes, les hypothèses clés, les principaux phénomènes dangereux identifiés, les problèmes encourus, etc. ainsi que l'approche employée.

- Au cours de la seconde phase, le concepteur expose méthodiquement chacun des aspects du SPA, en portant une attention particulière aux phénomènes dangereux identifiés, à leur risque et aux solutions envisagées. Tout au long de la présentation, les participants sont invités à intervenir et à poser des questions.
- Des listes de contrôle (*Checklist*) peuvent être utilisées pour favoriser une couverture complète des aspects de la SST du SPA.
- Le président d'assemblée clôture la revue en résumant les conclusions et les actions à prendre, et en s'assurant auprès des intervenants que tous les points d'intérêts ont été convenablement adressés et que la responsabilité des problèmes à résoudre a été assignée.
- Typiquement, la revue de sécurité devrait durer quelques heures, selon la complexité du SPA à réviser. Tel que mentionné précédemment, pour les OMP complexes il peut être choisi de mener plusieurs revues séparées, une pour chacun des principaux systèmes. Il existe cependant des cas exceptionnels pour lesquels la revue peut s'étendre sur plusieurs jours.
- Les problèmes soulevés au cours de la rencontre ainsi que les actions résultant de la revue doivent être notés par écrit sous forme d'un compte rendu de rencontre.

Suivi de la revue

- Suite à la revue, l'équipe de conception doit chercher à résoudre les problèmes soulevés lors de la rencontre et, si nécessaire, incorporer les solutions pour la maîtrise des risques à la conception.
- C'est au président d'assemblée que revient la responsabilité de s'assurer que chacun des problèmes soulevés a été résolu et que des actions correctives ont effectivement été déclenchées.
- Un rapport final exposant les problèmes soulevés au cours de la revue ainsi que l'investigation et la résolution de ces problèmes doit être rédigé. Ce rapport ainsi que le compte rendu de la rencontre doivent tous deux être approuvés et signés par le président d'assemblée, puis distribués à tous les membres de l'équipe de revue pour approbation. Ces deux documents constituent ensemble, conformément à la norme ISO 9001 [1994], le document d'enregistrement formel de la revue de sécurité.

Notes importantes

- Le but des revues n'est ni d'attaquer les concepteurs et de mettre en doute leurs compétences, ni de critiquer la fonction d'ingénierie de l'entreprise. Il s'agit plutôt d'étudier sous un angle critique la conception et d'émettre des suggestions constructives susceptibles d'aider les concepteurs dans leur démarche. Il est essentiel qu'une atmosphère d'objectivité et de professionnalisme soit maintenue tout au long de la rencontre.
- La revue du dossier de sécurité de conception par les participants, préalablement à la tenue de la rencontre, est une pratique fortement recommandée. Ainsi, davantage de temps pourra être consacré, au cours de la revue de sécurité, à la discussion plutôt qu'à l'explication des résultats de conception.
- Le suivi effectué suite aux revues de sécurité est essentiel et nécessaire. Il est primordial de voir à ce que tous les items identifiés comme étant problématiques soient résolus avant qu'ils ne deviennent des problèmes beaucoup plus critiques et coûteux.

BIBLIOGRAPHIE

ACHEMA (1994) *Machine pour l'industrie chimique*, ACHEMA 94 - Sécurité des machines, Frankfurt (Allemagne), 65 p.

ADEPA (s.d.) *GEMMA - Guide d'étude des modes de marche et d'arrêt*, Association pour le développement de la productique appliquée à l'industrie, Paris (France), 2e édition, 32 p.

AIFQ (1997) *L'industrie forestière du Québec : une expertise de calibre international*, Document préparé sur Internet (HTTP://WWW.AIFQ.QC.CA/FRANÇAIS/INDUSTRIE/FABRIQUE.HTML) par l'Association des industries forestières du Québec, 5 p.

AISS (1988a) *Guide pour la conception des systèmes industriels automatisés - 1re partie : descriptions des risques et des moyens de prévention*, Comité international «Protection-Machines» de l'Association internationale de sécurité sociale, Mannheim (Allemagne), 44 p.

AISS (1988b) *Règles pour la réalisation et l'équipement des commandes de sécurité dans les systèmes à fonctionnement automatique*, Comité international «Protection-Machines» de l'Association internationale de sécurité sociale, Mannheim (Allemagne), 15 p.

AISS (1989) *Guide pour la conception des systèmes industriels automatisés - 2e partie : Arrêt des installations, choix et caractéristiques des dispositifs de protection, information et formation*, Comité international «Protection-Machines» de l'Association internationale de sécurité sociale, Mannheim (Allemagne), 30 p.

AISS (1993) *Dispositifs de commande pour la sécurité des personnes travaillant à la machine*, Comité international «Protection-Machines» de l'Association internationale de sécurité sociale, Mannheim (Allemagne), 16 p.

ALLAIN, M. (1988) *L'aventure du papier*, Richmond Hill, Ontario (Canada), Nathan Communication, 32 p.

AMERICAN INSTITUTE OF CHEMICAL ENGINEERS (1992) *Guidelines for Hazard Evaluation Procedures*, New York (États-Unis), American Institute of Chemical Engineering, 140 p. + app.

ANDERSON, O., BELL, R., MEFFERT, K., VAUTRIN, J.-P. (1987) *Évaluation des systèmes électroniques programmables (PES) du point de vue de la sécurité en robotique*, INRS, Paris (France), Cahier de notes documentaires n° 127, p. 223-228.

ANDERSON, R., BLANK, V.L.G., LAFLAMME, L. (1997) *The Impact of Advances in Production Technology on Industrial Injuries : A Review of the Literature*, Safety Science, vol. 26, n° 3, p. 219-234.

ANDERSON, R., SIMMONS, J. (1991) *PLC/DCS Integration Techniques*, Proceedings of the Industrial Computing Conference, ISA, vol. 1, p. 125-130.

Anonyme (1992) *Safe Use of Programmable Controls, the Designer's Responsibility*, Gas Engineering and Management, vol. 32, p. 63-64.

ARKHIPOV, M.Y., MASLYUKOV, A.B., MEDVEDEV, I.V., RESHETNIKOV, V.V. (1989) *Principles for Constructing a Distributed Control System for Flexible Industrial Manufacture*, Soviet Journal of Computer and Systems Science, Moscou (Russie), vol. 27, n° 2, p. 9-12.

ARLAT, J., BLANQUART, J.-P., COSTES, A., CROUZET, Y., DESWARTE, Y., FABRE, J.-C., GUILLERMAIN, H., KAÂNICHE, M., KANOUN, K., LAPRIE, J.-C., MAZET,C., POWELL, D., RABÉJAC, C., THÉVENOD, P. (1995) *Guide de la sûreté de fonctionnement*, Toulouse (France), Cépaduès, 324 p.

ASME (1984) *An Instructional Aid for Occupational Safety and Health in Mechanical Engineering Design*, New York (États-Unis), ASME éd., 23 p.

ASP (1991) *Les grands dangers des chantiers industriels - Le cadenassage*, Association paritaire pour la santé et la sécurité du travail du secteur de la construction, Anjou (Canada), 21 p.

ASSOCIATION FRANÇAISE POUR L'ANALYSE DE LA VALEUR (1989) *Exprimer le besoin, Application de la démarche fonctionnelle*, Paris (France), AFNOR Gestion, 372 p.

AUMIAUX, M., RODDE G (1987) *Automatiser la production*, Paris (France), Masson, 228 p.

AUPIED, J. (1994) *Retour d'expérience appliqué à la sûreté de fonctionnement des matériels en exploitation*, Paris (France), Éditions Eyrolles, 380 p.

BACKSTRÖM, T., DÖÖS, M. (1995) *A Comparative Study of Occupational Accidents in Industries with Advanced Manufacturing Technology*, The International Journal of Human Factors in Manufacturing, vol. 5, n° 3, p. 267-282.

BADER, F.P. (1995) *Re-Engineering the DCS*, 1995 TAPPI/ISA PUPID Process Control, Electrical and Information Conference, p. 67-80.

BAERVELDT, A.-J. (s.d.) *A Safety System for Close Interaction Between Man and Robot*, s.l., p. 25-29

BAKER, B., CARTER, D.E. (1991) *Concurrent Engineering - The Product Development Environment for the 1990s*, Reading, Massachusetts (États-Unis), Addison-Wesley Publishing Company, 175 p.

BARBET, J.F. (1991) *Sûreté de fonctionnement des systèmes programmés - Harmonisation des méthodes*, Maintenance et Entreprise, n° 439, 5 p.

BATTLE, R.E., PAULA, H.M., ROBERTS, M.W. (1991) *Reliability Performance of Fault-Tolerant Digital Control Systems*, Plant/Operation Progress, vol. 10 n° 2, p. 115-128.

BECKMAN, L.V. (1993) *Selecting Redundant Microprocessor-Based Systems*, Hydrocarbon Processing, vol. 72, n° 2, p. 72, 74, 76.

BÉLANGER, R., BOURBONNIÈRE, R., MASSÉ, S., SIRARD, C. (1995) *Presse à embrayage à friction : détermination de l'emplacement des commandes bi-manuelles*, Guide technique R-100, Institut de recherche en santé et en sécurité du Québec, Montréal (Canada), 11 p.

BÉLANGER, R., BOURBONNIÈRE, R., MASSÉ, S., SIRARD, C. (1995) *Presse à embrayage à tour complet : détermination de l'emplacement des commandes bi-manuelles*, Guide technique R-101, Institut de recherche en santé et en sécurité du Québec, Montréal (Canada), 10 p.

BÉLANGER, R., CESTA, V., MASSÉ, S. (1991) *Sécurité en forêt, amélioration technique des machines de récolte forestière*, Institut de recherche en santé et en sécurité du Québec, Montréal (Canada), s.p.

BELL, R., REINERT, D. (1992) *Risk and System Integrity Concepts for Safety Related Control Systems*, Safety Science, vol. 15, n° 4-6, p. 283-308.

BIERCE, B., FONTENEAU, A., GAUBERT, P., GUYONVARCH, D., LACORE, J.-P., MERLAUD, C., STUDER, J. (1994) *Enseigner la prévention des risques professionnels : Concevoir une machine sûre*, INRS (France), ED 1520, 60 p.

BIXBY, K. (s.d.) *Robot risk assessment & hazard analysis : a systematic 21 step guide to performing a robot risk assessment*, Robotics Industries Association, 49 p.

BIXBY, K. (1996) *Robot Risk Assessment Workshop*, Novi, Michigan (États-Unis), Robotics Industries Association, 8th Annual National Robot Safety Conference, 61 p.

BLANCHARD, M. (1979) *Comprendre. maîtriser et appliquer le GRAFCET*, Toulouse (France), Cépaduès, 174 p.

BLOIS, J. (1991) *Level of Man Machine Interface (MMI) for Programmable Logic Controllers (PLC)*, Proceedings of the Industrial Computing Conference, ISA, vol. 1, p. 119-126.

BLOODGOOD, J.F. (1996) *Guidelines to the understanding and use of Safety of machinery standards*, ISO/TC 199 New work item proposal, 34 p.

BOIDIN, G., GIEZEK, F., GUYART, P., LEMAIRE, M., LUKOWSKI, D., MORET, J.-P., SCHAMPION, G., SEVIN, B., STUDER, J., TALASKA, D., VERBECQ, H. (1994) *Enseigner la prévention des risques professionnels : Maintenance et maîtrise du risque*, INRS (France), ED 1521, 82 p.

BOUCHARD, G. (1997), communication privée (24 septembre 1997).

BOUCHUT, Y., DUFOURT, D., JACOT, J.H., RUFFIER, J. (1980) *Automatisation : formes anciennes et formes nouvelles*, Centre AEH Institut des Études Économiques, Lyon (France), 178 p.

BOURBONNIÈRE, R., PAQUES, J.-J. (1997) *Formation sur les dispositifs de verrouillage et d'interverrouillage et autres systèmes de sécurité associés aux machines dangereuses*, Institut de recherche en santé et sécurité du travail, Montréal (Canada), 188 p.

BOURBONNIÈRE, R. (1997) communication privée (25 septembre 1997).

BOUTEILLE, D., BOUTEILLE, N., CHANTREUIL, S., COLLOT, R., FRACHET, J.-P., LeGRAS, H., MERLAUD, C., SELOSSE, J., SFAR, A (1996) *Les automatismes programmables*, Toulouse (France), 2e édition, Cépaduès, 286 p.

BRAUER, R.L. (1991) *Safety Engineers Have Obligation to Control Hazards Through Design*, Occupational Health and Safety, vol. 60, n° 6, p. 42-43.

BRAUER, R.L. (1994) *Safety and Health for Engineers*, New York (États-Unis), Van Nostrand Reinhold, 651 p.

BRAZENDALE, J. (1995) *IEC 1508 : Functional Safety, Safety Related Systems*, Proceedings of the 2nd IEEE International Software Engineering Standards Symposium, p. 8-17.

BUGAJSKI, P., DePIETRO, R., GILES, J., OSTROWIECKI, B., QUADIR, N. (1991) *Identifying and Controlling Hazards in Manufacturing Operations : A Systems Design Perspective*, Industrial Technology Institute, Ann Arbor, Michigan (États-Unis), 58 p.

BUKOWSKI, J.V., GLOBE, W.M. (1994) *Effects of Maintenance Policies on MTTF of Dangerous Failures in Programmable Electronics Controllers*, ISA Transactions, vol. 33, p. 185-193.

BUKOWSKI, J.V., GLOBE, W.M. (1995) *Using Markov Models for Safety Analysis of Programmable Electronic Systems*, ISA Transactions, vol. 34, n° 2, p. 193-198.

BURGESS, J.A. (1984) *Design Assurance for Engineers and Managers*, New York (États-Unis), Marcel Dekker inc., 303 p.

CAMPA, A., CHAPPERT, R., COJEAN, J. (1974) *L'automatique par les problèmes - Tome 1*, Paris (France), Éditions Foucher, 271 p.

CAN/CSA C22.2 No. 08-1986 (1986) *Safety Functions Incorporating Electronic Technology, Requirements for Safety of Electrical Products*, Etobicoke (Canada), Association canadienne de normalisation, s.p.

CAN/CSA Q634-91 (1991) *Risk Analysis Requirements and Guidelines*, Etobicoke (Canada), Association canadienne de normalisation, 42 p.

CAN/CSA Z142-M90 (1990) *Code for Punch Press and Break Press Operation : Health, Safety, and Guarding Requirements*, Etobicoke (Canada), Association canadienne de normalisation, 38 p.

CAN/CSA Z431-M89 (1989) *Couleur des voyants lumineux et des boutons poussoirs*, Etobicoke (Canada), Association canadienne de normalisation, 19 p.

CAN/CSA Z432-94 (1994) *Sécurité des machines - Santé et sécurité au travail*, Etobicoke (Canada), Association canadienne de normalisation, 63 p.

CAN/CSA Z434-94 (1994) *Industrial Robots and Robot Systems-General Safety Requirements*, Etobicoke (Canada), Association canadienne de normalisation, 27 p.

CASTELLANI, X. (1992) *MCO - Méthodologie générale d'analyse et de conception des systèmes objet*, Paris (France), Masson, 402 p.

CATMUR, J.R., CHUDLEIGH, M.F. (1992) *Safety Assessment of Computer Systems Using HAZOP and Audit Techniques*, Safety of Computer Control Systems 1992 (SAFECOMP'92) : IFAC Symposium, Zurich (Suisse), p. 285-292.

CEI/IEC 204-1 (1992) *Équipement électrique des machines industrielles - Partie 1*, Genève (Suisse), Commission électrotechnique internationale, norme CEI/IEC 204-1, s.p.

CEI/IEC 300–1 (1991) *Gestion de la sûreté de fonctionnement, Partie 1 : Gestion du programme de sûreté de fonctionnement*, Genève (Suisse), Commission électrotechnique internationale, norme CEI/IEC 300, s.p.

CEI/IEC 300-2 (1995) *Gestion de la sûreté de fonctionnement, Partie 2 : Éléments et tâches du programme de sûreté de fonctionnement*, Genève (Suisse), Commission électrotechnique internationale, norme CEI/IEC 300, 72 p.

CEI/IEC 300–3 (1995) *Gestion de la sûreté de fonctionnement, Partie 3 : Série de guides d'application* Genève (Suisse), Commission électrotechnique internationale, norme CEI/IEC 300, s.p.

CEI/IEC 351 (1994) *Mesure et commande dans les processus industriels*, Genève (Suisse), Commission électrotechnique internationale, norme CEI/IEC 351, 114 p.

CEI/IEC 1131-3 (1992) *Automates programmables - Langages de programmation*, Genève (Suisse), Commission électrotechnique internationale, projet de norme CEI/IEC 1131-3, 219 p.

CEI/IEC 1131-4 (1993) *Contrôleurs programmables - Directives pour l'utilisation*, Genève (Suisse), Commission électrotechnique internationale, projet de norme CEI/IEC 1131-4, 62 p.

CEI/IEC 1508-1 (1995) *Sûreté fonctionnelle : systèmes relatifs à la sûreté - Partie 1 : prescriptions générales*, Genève (Suisse), Commission électrotechnique internationale, projet de norme CEI/IEC 1508-1, 57 p.

CEI/IEC 1508-2 (1995) *Sûreté fonctionnelle : systèmes relatifs à la sûreté - Partie 2 : prescriptions concernant les systèmes électriques/électroniques/électroniques programmables*,

Genève (Suisse), Commission électrotechnique internationale, projet de norme CEI/IEC 1508-2, 59 p.

CEI/IEC 1508-3 (1995) *Sûreté fonctionnelle : systèmes relatifs à la sûreté - Partie 3 : prescriptions concernant les logiciels*, Genève (Suisse), Commission électrotechnique internationale, projet de norme CEI/IEC 1508-3, 52 p.

CEI/IEC 1508-4 (1995) *Sûreté fonctionnelle : systèmes relatifs à la sûreté - Partie 4 : définitions*, Genève (Suisse), Commission électrotechnique internationale, projet de norme CEI/IEC 1508-4, 19 p.

CEI/IEC 1508-5 (1995) *Sûreté fonctionnelle : systèmes relatifs à la sûreté - Partie 5 : lignes directrices pour la mise en oeuvre de la partie 1*, Genève (Suisse), Commission électrotechnique internationale, projet de norme CEI/IEC 1508-5, 42 p.

CEI/IEC 1508-6 (1995) *Sûreté fonctionnelle : systèmes relatifs à la sûreté - Partie 6 : lignes directrices pour la mise en oeuvre des parties 2 et 3*, Genève (Suisse), Commission électrotechnique internationale, projet de norme CEI/IEC 1508-6, 54 p.

CEI/IEC 1508-7 (1995) *Sûreté fonctionnelle : systèmes relatifs à la sûreté - Partie 7 : bibliographie des techniques*, Genève (Suisse), Commission électrotechnique internationale, projet de norme CEI/IEC 1508-7, 64 p.

CHALVET, J. (1966) *L'automatisation*, Paris (France), Armand Colin, 230 p.

CHARLAND, J.-P. (1990) *Les pâtes et papiers au Québec*, Québec (Canada), Bibliothèque nationale du Québec, 447 p.

CHARPENTIER, P., VAUTRIN, J.P., VIGNERON, C. (1996) *La sécurité en machinerie : Introduction au concept de catégorie*, INRS, Paris (France), Note documentaire n°163, p. 255-262.

CHARRON, F., GAUTHIER, F. (1995) *Design for Health and Safety : A Simultaneous Engineering Approach*, International Conference on Engineering Design, Prague (République Tchèque), 6 p.

CHARRON, F., PROULX, D. (1996) *GMC 156 - Méthodologie de conception*, Note de cours, Université de Sherbrooke, Sherbrooke (Canada), s.p.

CHARTIER-KASTLER, C. (1991) *Appliquer MERISE - Exercices et études de cas*, Paris (France), Eyrolles, 184 p.

CHATTAWAY, A.T. (1991) *Is there a Future for Distributed Control Systems?*, Proceedings of the Industrial Computing Conference, ISA, vol. 1, p. 527-532.

CICCOTELLI, J., MARSOT, J. (1995) *Contrôleurs de vitesse de rotation*, INRS, Nancy (France), note documentaire 2006-161-95, p. 497-508.

CLAUZADE, B., GÉRARDIN, J.-P., VAUTRIN, J.-P. (1984) *Systèmes électroniques analogiques et sécurité*, L'onde électrique, vol. 64, n° 1, p. 69-85.

CLOUTIER, G., PAQUES, J.-J. (1988) *GEMMA, the Complementary Toll of the GRAFCET*, Proceedings of the Fourth Annual Canadian Programmable Control & Automation Technology Conference & Exhibition, Toronto (Canada), 10 p.

COLLINGE, C. (1998) communication privée (23 avril 1998).

CONLEY, J.S., SIU, D.C. (1988) *Programmable Logic Device Testability. Will PLDs Make the Reliability Grade?*, Southcon/88 Conference Record, p. 148-153.

COUGER, J.D. (1995) *Creative Problem Solving and Opportunity Finding*, Boyd & Fraser Publishing Company, Danvers, Massachusetts (États-Unis), 468 p.

COX, R.A (1995) *Technician's Guide to Programmable Controllers*, 3e édition, New York (États-Unis), Delmar Publishers, 372 p.

CRAM (1991) *Dispositifs de verrouillage intrinsèquement sûrs pour protecteur fixe et protecteur mobile actionné occasionnellement*, Caisse régionale d'assurance maladie de Bourgogne Franche-Comté, Fiche 91-1, Dijon (France), 4 p.

CSST (1985) *Dispositifs de protectio ur les machines*, Commission de la santé et de la sécurité du travail, Bibliothèque nationale du Québec, Québec (Canada), 64 p.

DARVES-BORNOZ, M.(1990) *Conception des automatismes pneumatiques*, INRS, Nancy (France), Guide de conception, 36 p.

DAVID, R. (s.d.) *L'analyse du risque*, Caisse régionale d'assurance maladie de l'Île-de-France, Paris (France), 5 p.

DAVID, R., HUANG, J. (s.d.) *Fault Diagnosis of a Batch of Microprocessors*, (s.l.) p. 197-201.

DAWSON, S. (1994) *L'art et la manière de fabriquer son papier*, Éditions fleures, Paris (France), 142 p.

DEI-SVALDI, D., VAUTRIN, J.-P. (1984) *Les automates programmables : nouvelles technologies, nouveaux risques, principes de sécurité à appliquer*, INRS (France), Cahier de notes documentaires n° 117, p. 467-474.

DEI-SVALDI, D., VAUTRIN, J.-P. (1989) *Accident du travail sur sites automatisés*, INRS (France), Cahier de notes documentaires n° 136, p. 445-453.

DEI-SVALDI, D., VAUTRIN, J.-P. (1996) *Glossaire et définitions en sécurité*, Intervention au DESS, INRS, Nancy (France), 13 p.

DENIS, B., LESAGE, J.-J. (1995) *Un panorama de la recherche en conception de la conduite des systèmes de production*, Document préparé par le LURPA sur Internet (HTTP://WWW.LURPA.ENS-CACHAN.FR/CSAP/PUBLI/PUBU_95_2/MONTREAL_95_1.HTML).

DENIS, B., LESAGE, J.-J., PIETRAC, L., ROUSSEL, J.-M., TIMON, G. (1994) *Modèles de spécification fonctionnelle de la commande des systèmes de production : synthèse de trois études de cas*, Document préparé par le LURPA sur Internet (HTTP://WWW.LURPA.ENS-CACHAN.FR/CSAP/PUBLI/PUBU_94_4/PRIMECA94_1.HTML).

DICTIONNAIRES Le ROBERT (1993) *Le nouveau Petit Robert*, Montréal (Canada), DICOROBERT inc., 2491 p.

DIN 0019251 (1992) *Mesure et commande*, INRS (France), traduction n°545-94, 25 p.

DIONNE-PROULX, J. (1992) *La perception du danger : une approche nouvelle d'identification et d'intervention en SST*, Revue européenne de psychologie appliquée, (s.l.), vol. 42, n° 4, p. 297-304.

DIVINÉ, M. (1992) *Parlez-vous MERISE?*, Paris (France), Eyrolles, 4e édition, 240 p.

DOUCET, P. (1997) *GMC 126 - Introduction à l'ingénierie simultanée*, Note de cours, Université de Sherbrooke, Sherbrooke (Canada), 68 p.

EDWARDS, D.R (1989) *Safety in Computer Controlled Automated Manufacturing Systems : Some Basic Questions to Ask*, Health and Safety Executive, 8 p.

EDWARDS, R., NICOLAISEN, P., VAUTRIN, J.-P. (1992) *Robots et ensemble automatisés*, INRS (France), Cahier de notes documentaires n° 149, p. 455-478.

ELPHICK, J.R., PATTON, R.J., TYRELL, A.M. (1993) *Enhanced Distributed Recovery Blocks : A Unified Approach for the Design of Safety Critical Distributed Systems*, IEE Colloquium on Safety Critical Distributed Systems, Londres (Angleterre), 5 p.

EN 292-1 (1991) *Sécurité des machines - Principes fondamentaux, principes généraux de conception - Partie 1 : Terminologie de base, méthodologie*, Comité européen de normalisation, 23 p. + annexes.

EN 292-2 (1991) *Sécurité des machines - Principes fondamentaux, principes généraux de conception - Partie 2 : Principes techniques et spécifications*, Comité européen de normalisation, 30 p.

FANUC Robotics (s.d.) *Safety*, Fanuc Robotics Industries (États-Unis), 8 p.

FAUCONNET, M., LAMOUREUX, P., MOUGEOT, B., SCHUTZ, D. (1992) *Interrupteurs de position électromécaniques à clé*, INRS, Nancy (France), note documentaire 1902-149-92, p. 531-542.

FAUCONNET, M., MOUGEOT, B. (1989) *Blocs logiques pour commandes bi-manuelles*, INRS, Nancy (France), note documentaire 1718-134-89, p. 45-50.

FAVARO, M., MONTEAU, M. (1990a) *Bilan des méthodes d'analyse a priori des risques : 1. Des contrôles à l'ergonomie des systèmes*, INRS (France), Cahiers de notes documentaires, n° 138, p. 91-121.

FAVARO, M., MONTEAU, M. (1990b) *Bilan des méthodes d'analyse a priori des risques : 2. Principales méthodes de la sécurité des systèmes*, INRS (France), Cahiers de notes documentaires, n° 139, p. 363-389.

FISHER, T.G. (1987) *Designing Fail-Safe Alarm and Interlock Systems*, Proceeding of the Sixth Annual Control Engineering Conference, Rosemont, Illinois (États-Unis), p. 285-297.

FISHER, T.G. (1990) *Are Programmable Controllers Suitable for Emergency Shutdown Systems?*, ISA Transactions, vol. 29, n° 2, p. 1-11.

FLORES, A. (1983) *Safety Design: An Ethical Viewpoint*, Chemical Engineering Progress, vol. 79, n° 11, p. 11-14.

FORD, J.A. (1997) *Get a Lock on This*, Accident Prevention, p.24-25.

GABAY, J. (1991) *MERISE, étude de cas*, Paris (France), Masson, 210 p.

GABAY, J. (1992) *Apprendre et pratiquer MERISE*, Paris (France), 2e édition, Masson, 242 p.

GALL, H., RABE, G. (1995) *International and European Standardization of PLCs in Safety Critical Systems - Qualification, Type Testing, Certification and Licensing*, ISA transactions, vol. 34, n° 3, p. 273-281.

GALLAGHER, V.A. (1988) *Recognize Designs Defects and Reduce Workers Compensation Insurance*, vol. 33, n° 9, p. 22-25.

GALLAGHER, V.A. (1991) *Fall and Machine Hazards*, Professional Safety, vol. 36, n° 2, p. 22-26.

GASKILL, S.P. (1994) *Safety Issues in Modern Applications of Robots*, Computing and Control Division Colloquium on Safety and Reliability of Complex Robotics Systems, Bootle (Angleterre), p. 5/1-5/13.

GAUTHIER, F. (1993) *Intégration des coûts et des échéanciers à la méthodologie du déploiement de la fonction qualité*, Mémoire de maîtrise ès sciences appliquées, Université de Sherbrooke, Sherbrooke (Canada), 150 p.

GAUTHIER, F. (1994) *Projet de recherche sur l'intégration systématique de la santé et de la sécurité du travail lors de la conception d'outils, de machines ou de procédés*, Document de travail, Université de Sherbrooke, Sherbrooke (Canada), 72 p.

GAUTHIER, F. (1997) *Développement d'une approche méthodologique permettant l'intégration systématique des aspects de la santé et de la sécurité du travail dans le processus de conception d'outils, de machines et de procédés industriels*, Thèse de doctorat ès sciences appliquées, Université de Sherbrooke, Sherbrooke (Canada), 257 p.

GHOSH, A.K., JOHNSON, B.W., PROFETA, J.A. (1995) *System-Level Modeling in the ADEPT Environment of a Distributed Computer System for Real-Time Applications*, International Performance and Dependability Symposium, p. 194-203.

GHOSH, K., PAQUES, J.-J. (1989) *Automatisation et sécurité du travail : perspective pour le Québec*, Travail et santé, vol. 5, n° 2, p. 39-43.

GILLOT, J. (1994) *Intégration des résultats de la recherche en science du travail, ergonomie et sécurité dans la conception des machines et l'aménagement des postes de travail*, Caisse régionale d'assurance maladie, Paris (France), p. 168-172.

GILLOT, J. (1996) *Protecteurs et dispositifs de protection ; critères d'appréciation*, Caisse régionale d'assurance maladie de l'Île-de-France, Études techniques et assistance en prévention 95-695/JG-AFW. ? p.

GILMAN, J. (1993) *Honeywell Users Group Process Safety and Control System*, WIN/WIN'93 Honeywell Users Group, s.l., 31 p.

GOSH, A.K., JONHSON, B.W., PROFETA, J.A. (1996) *Safety Evaluation Using Behavioral Simulation Models*, Annual Reliability and Maintainability Symposium, p. 82-89.

GOUVERNEMENT DU QUÉBEC (1997) *Règlement sur les établissements industriels et commerciaux*, Loi gouvernementale, Québec (Canada), s.p.

GRENIER, D. (1994) *DCSs up Product Consistency, Quality, Output*, Chilton's Instrumentation and Control Systems, vol. 67, n° 9, p. 51-58.

GRUHN, P. (1991) *The Pros and Cons on Qualitative and Quantitative Analysis of Safety Systems*, Proceedings of the Industrial Computing Conference, ISA, vol. 1, p. 37-46.

GRUHN, P. (1995) *Independent Safety Systems*, Control & Instrumentation, vol. 27, n° 11, p. 37-38.

GRUHN, P. (1996) *ISA S84..."I Have to Do What"*, Intech, p. 42-44.

HALANG, W.A., JUNG, S.-K. (1994) *Programmable Logic Controller for Safety Critical Systems*, High Integrity Systems, vol. 1, n° 2, p. 179-193.

HALANG, W.A., SCHEEPSTRA, J. (1993) *PLC-Implementation of Emergency Shutdown Systems*, SAFECOMP'93, 12th International Conference on Computer Safety and Reliability, p. 53-62.

HALEBSKY, M. (1989) *System Safety Engineering as Applied to Ship Design*, Marine Technology, vol. 26, p. 245-251.

HAMMER, W. (1972) *Handbook of System and Product Safety*, Prentice-Hall Inc., Englewood Cliffs, New Jersey (États-Unis), s.p.

HARMS-RINGDAHL, L. (1986) *Experiences from Safety Analysis of Automatic Equipment*, Journal of Occupational Accidents, vol. 8, p. 139-148.

HARMS-RINGDAHL, L. (1987) *Safety Analysis in Design - Evaluation of a Case Study*, Accident Analysis and Prevention, vol. 32, p. 199-208.

HARMS-RINGDAHL, L. (1993) *Safety Analysis, Principles and Practice in Occupational Safety*, Elsevier Science Publishers Ltd., 280 p.

HATLEY, D.J., PIRBHAI, I.A. (1990) *Stratégies de spécification des systèmes temps réel (SA_RT)*, Paris (France), Masson, 346 p.

HELSINKI UNIVERSITY (1997) *Linkage Program*, Brochure émise par le Department of Forest Products Technology, Helsinki University of Technology, Espoo (Finlande), 6 p.

HILL, J.L. (1990) *PLC Meets Casting Machine's Special Safety Needs*, American Hydracast Inc., Chicago (États-Unis), vol. 63, n° 6, p. 91-92.

HONEYWELL (1996) *Honeywell Safety Management System*, The Journal of Industrial Automation and Control - Supplement, Bruxelles (Belgique) 35 p.

HSE (1989) *Computer Numerically Controlled Machining Centers, Lathes and Turning Machines*, Health and Safety Executive, Information Document HSE 228/3, 11 p.

HUBBY, R.N., TRIPP, R.P. (1991) *Implementation of a Fault Tolerant Distributed Control System*, ISA Transactions, vol. 30, n° 4, p. 33-43.

HUNTER, T.A. (1992) *Engineering Design for Safety*, McGraw-Hill Inc., 298 p.

INRS (1983a) *Guide pour la conception des dispositifs de verrouillage et d'interverrouillage associés à des protecteurs*, INRS (France), Cahier de notes documentaires, p. 365-379.

INRS (1983b) *Intégration de la sécurité dans la conception des systèmes de commande*, INRS (France), décret n° 80-543, 62 p.

INRS (1989a) *Interrupteurs de position à ouverture forcée et à commande mécanique positive utilisés pour la protection des personnes : choix et montage*, INRS, Nancy (France), Fiche pratique de sécurité ED 015, 4 p.

INRS (1989b) *ELISE : Logiciel de simulation et d'analyse de fonctionnement des circuits électriques de commande non programmable*, INRS (France).

INRS (1996) *Consignation et déconsignation*, INRS, Paris (France), ED 754, 23 p.

INRS (1997) *Résumé des interventions*, Séminaire d'information sur les automates programmables dédiés à la sécurité (APIdS), Vandoeuvre (France), 14 p.

IRSST (1993) Proposition d'un plan opérationnel 1992-1997 pour la recherche et le développement de la sécurité des outils, des machines et des procédés industriels, Institut de recherche en santé et sécurité du travail du Québec, Montréal (Canada), 14 p.

ISO 8402 (1994) *Management de la qualité et assurance de la qualité - Vocabulaire*, International Standard Organisation, Genève (Suisse), 39 p.

ISO 9001 (1994) *Systèmes qualité - Modèle pour l'assurance qualité en conception, développement, production, installation et prestations associées*, International Standard Organisation, 12 p.

ISO 9004-1 (1994) *Management de la qualité et éléments de système qualité - Partie 1 : Guide de gestion du programme de sûreté de fonctionnement*, International Standard Organisation, 12 p.

ISO/CEI 51 (1997) *Aspects liés à la sécurité - Principes directeurs pour les inclure dans les normes*, International Standard Organisation/Commission électrotechnique internationale, Genève (Suisse), 10 p.

ISO/CEI 13850 (1995) *Safety of Machinery-Emergency Stop-Principles for Design*, International Standard Organisation/Commission électrotechnique internationale, Genève (Suisse), 8 p.

ISO/TC 199 (1996) *Guideline to the Understanding and Use of Safety and Machinery Standards*, International Standard Organisation, 34 p.

JÄRVINEN, J., KARWOWSKI, W. (1995) *Analysis of Self-Reported Accidents Attributed to Advanced Manufacturing Technology*, The International Journal of Human Factors in Manufacturing, vol. 5, n° 3, p. 251-266.

JAULENT, P. (1992) *Génie logiciel : les méthodes*, Paris (France), 2e édition, Armand Colin, 295 p.

JAULENT, P., LARRIEUX, P. (1993) *La méthode objet - Une approche de l'ingénierie simultanée avec SYS_P_O*, Paris (France), Armand Colin Éditeur, 228 p.

KANIS, H., MARINISSEN, A.H. (1991) *Research in Industrial Design Engineering*, Designing for everyone: Proceedings of the 11th Congress of the International Ergonomics Association, Paris (France), Taylor and Francis, vol. 2, p. 1055-1057.

KANIS, H., WEEGELS, M.F. (1990) *Research into Accidents as a Design Tool*, Ergonomics, vol. 33, n° 4, p. 439-445.

KANNEGIETER, T. (1995) *Faultfinding Made Easy at Water Treatment Plant*, Process and Control Engineering (PACE), vol. 48, n°11, 2 p.

KARYDAS, D.M., PARASKEVAS, A.S. (1993) *Methodology to Evaluate the Reliability of a Safety System : Application to Electronic Programmable Controller*, Safety Engineering and Risk Analysis, ASME, p. 75-84.

KATO, E., SATO, Y. (s.d.) *On the Application of Safety Integrity Levels to Safety-Related Systems for Automobiles*, Japon, 6 p.

KAVIANIAN, H.R., WENTZ, C.A., PETERS, R.W., MARTINO, L.E. (1990) *Safety System Management for Design of Hazardous Processes*, Professional Safety, vol. 35, n° 3, p. 31-34.

KEMPS, K. (1992) *Shutdown Systems Using Fail Safe PLC's*, Safety and Reliability'92, p. 391-402.

KERN, A.G. (1990) *Batch Automation in a PLC : Software Design is the Key*, ISA Transactions, vol. 29, n° 2, p. 33-45.

KIM, K.H. (1988) *Designing Fault Tolerance Capabilities Into Real-Time Distributed Computer Systems*, Proceedings - Workshop on the Future Trends of Distributed Computing Systems in the 1990s, p. 318-328.

KIM, S., HAN, J.B. (1995) *PLC based DESFAS in nuclear power plants*, Proceedings of the 1995 International IEEE/IAS Conference on Industrial Automation and Control, Taipei (Taiwan), p. 686-692.

KLETZ, T.A. (1991) *Plant Design for Safety : A User-Friendly Approach*, Chemistry and Industry, n° 19, p. 725-726.

KNEPPERT, M. (1995) *Conception d'un automatisme*, INRS, Paris (France), ED 736, p. 309-315.

KNEPPERT, M., PAGLIÉRO, D., VAUTRIN, J.-P. (1993) *La sécurité en robotique*, Techniques de l'ingénieur, Mesures et contrôles, France, 14 p.

KNEPPERT, M., VAUTRIN, J.-P. (1984) *Tapis et planchers sensibles utilisés en protection industrielle*, INRS, Paris (France), note documentaire 1491-116-84, p. 333-346.

KOCH, S., RUETHER, J. (1994) *Common Mode Failure in Computer-Based Systems*, IEEE Control Systems Magazine, vol. 14, n° 2, p. 53-59.

KOLB, J., ROSS, S.S. (1980) *Product Safety and Liability: A Desk Reference*, McGraw-Hill, 688 p.

KOUMIS, L.S. (1990) *Reliability and Design Issues of Programmable Logic Devices in High Speed System Design*, WESCON/90 Conference Record, Los Angeles (États-Unis), p. 291-297.

KREUTKAMPF, F. (1994) *Configuration antirisque et sélection de commandes de machines - catégories de commandes d'après prEN 954, évaluation du risque, exemples de montages*, Colloque de l'IVSS, Francfort (Allemagne), 24 p.

LACHIVER, G. (1995) *GMC 450 - Cours de commande automatique*, Note de cours, Université de Sherbrooke, Sherbrooke (Canada), 197 p.

LAMOUREUX, P., OTTER, B. (1992) *Verrou électromagnétique avec contrôle intégré de position du pêne : choix et montage*, INRS, Paris (France), Fiche pratique de sécurité ED 039, 4 p.

LEMAY, É. (1995) *Intégration de l'analyse fonctionnelle à un processus de réalisation de produits selon l'approche de l'ingénierie simultanée*, Mémoire de maîtrise ès sciences appliquées, Université de Sherbrooke, Sherbrooke (Canada), 222 p.

LEMAY, É., ST-AMANT, R. (1997), *GMC 772 - Ingénierie simultanée*, Note de cours, Université de Sherbrooke, Sherbrooke (Canada), 68 p.

LEPLAT, J., De TERSSAC, G. et coll. (1990) *Les facteurs humains de la fiabilité dans les systèmes complexes*, Marseille (France), Éditions Ocatres, 383 p.

LEVESON, N.G. (1995) *Safeware*, Addison-Wesley Publishing Company, États-Unis, 680 p.

LEVINE, P.S. (1995) *The Programmable Logic Controllers : Adapting in an Environment of Change*, InTech, vol. 42, n° 3, p. 52-56.

MACK, D. (1993) *Industrial Programmable Controllers in Safety Applications*, IEE Colloquium on Safety Critical Distributed Systems, Londres (Angleterre), 5 p.

MAILLETTE, L. (1994) *Étude et développement systématique du contrôle de procédé pour l'encapsulation de microplaquettes*, Mémoire de maîtrise ès sciences appliquées, Université de Sherbrooke, Sherbrooke (Canada), 136 p.

MAIN, B.W., WARD, A.C. (1992) *What Do Design Engineers Really Know About Safety?*, Mechanical Engineering, vol. 114, n° 8, p. 44-51.

MANGOLD, V.L. (1996) *Response R15.06, Open action Items*, Robotics industries association, s.p.

MARCA, D.A., McGOWAN, C.L. (1988) *SADT - Structured Analysis and Design Technique*, McGraw Hill, États-Unis, 392 p.

MARGETTS, T. (1986) *PLCs for Alarm and Shutdown Systems*, Chemical Engineer, Londres (Angleterre), n° 427, p. 36-37.

MARSH, R.F. (1991) *Integration of DCS and Equipment Shutdown Systems*, Proceedings of the Industrial Computing Conference, ISA, vol. 1, p. 29-35.

MARSOT, J. (1996) *Détecteurs de position magnétiques à lames souples*, INRS, Nancy (France), note documentaire 2021-163-96, p. 185-196.

MARTEL, P. (1997), *L'ingénierie simultanée doit être préférée à l'ingénierie séquentielle*, Le Soleil, 30 octobre 1997.

MASSÉ, S., BÉLANGER, R., TELLIER, C. (1994) *La sécurité reliée aux machines*, Document de formation, Institut de recherche en santé et sécurité du travail du Québec, Montréal (Canada), s.p.

MASSEY, L.E. (1991) *The Development of Modular Batch Automation Techniques*, Proceedings of the Industrial Computing Conference, ISA, vol. 1, p. 27-33.

MAWKIN, S. (1991) *Developing DCS for Turnkey Projects*, Control & Instrumentation, vol. 23, n° 5, p. 69-71.

McARTHUR, N. (1992) *Taking PESs for Safety Serious*, Control & Instrumentation, vol. 24, n° 11, p. 45, 47, 48.

McGILL, W.F., SMITH, S.E., TWETE, C.A. (1987) *Safety: A System Approach*, Advances In Instrumentation, vol. 42, p. 123-131.

McKENNA, F. (1995) *Safety : Which Protection System Do I Select?*, Control & Instrumentation, vol. 27, n° 1, p. 34-35.

MERLAUD, C., MOREL, J.-P., SOURISSE, C. et coll. (1992) *La sûreté des machines et installations automatisées*, Paris (France), Sadave, 333 p.

MIL-STD-1629A (1980) *Military Standard : Procedures for Performing a Failure Mode, Effects and Criticality Analysis*, Washington (États-Unis), Department of Defense, 48 p.

MITCHELL, M.M., WILLIAMS, K. (1993) *Failure Experience of Programmable Logic Controllers Used in Emergency Shutdown Systems*, Reliability Engineering & System Safety, vol. 39, p. 329-331.

MONETTE, C. (1997) *Circuits électriques de commande et de puissance*, Document de travail, Institut de recherche en santé et sécurité du travail du Québec, Montréal (Canada).

MOON, I. (1994) *Modeling Programmable Logic Controllers for Logic Verification*, IEE Control Systems Magazine, vol. 14, p. 53-59.

MOREL, J.-P., POYARD, J.-L. (1987) *Les fonctions de sécurité dans la conception et la réalisation de l'automatisme des machines et appareils*, Revue technique de l'APAVE n° 237, Lyonnaise (France), p. 17-24.

MUSTER, D. (1985) *Harmonizing Safety and Design in Engineering Curricula*, Professional Safety, Vol. 30, n° 2, p. 35-40.

MURRAY, A. (1996) *Intégration des exigences en matière de système qualité à la démarche de l'ingénierie simultanée*, Mémoire de maîtrise ès sciences appliquées, Université de Sherbrooke, Sherbrooke (Canada), 335 p.

NF X 50.150 (1991) *Analyse de la valeur - Analyse fonctionnelle - vocabulaire*, Association française de normalisation, norme NF X 50.150, s.p.

NF X 50.151 (1984) *Guide pour l'élaboration d'un cahier des charges fonctionnelles*, Association française de normalisation, norme NF X 50.153, s.p.

NF X60-510 (1986) *Techniques d'analyse de la fiabilité des systèmes , Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*, Union technique de l'électricité, Paris (France), 22 p.

NICHOLS, A.K., RUTHERFORD, T. (1991) *Requirements, Specifications and Design Considerations for Implementation of a PLC-Based Burner Management System*, Conference Record of 1991 Annual Pulp and Paper Industry, p. 50-54.

NIEMANN, K.-H. (s.d.) *Reduction of Engineering Cost by Use of Modern Engineering Tools*, s.l., s.p.

PAQUES, J.-J. (1991) *Règles sommaires de sécurité pour l'utilisation des automates programmables industriels (API)*, Étude/Bilan de connaissances, Institut de recherche en santé et sécurité du travail du Québec, Montréal (Canada), 19 p.

PAQUES, J.-J. (1992) *Automatisation et sécurité : les interrupteurs de position, ces méconnus*, Conférence canadienne sur l'automatisation industrielle, Montréal (Canada), 4 p.

PAQUES, J.-J. (1997) Communication privée (11 décembre 1997).

PAULA, H.M. (1993) *Failure Rates for Programmable Logic Controllers*, Reliability Engineering & System Safety, vol. 39, p. 325-328.

PLANCHE, R. (1988) *Maîtriser la modélisation conceptuelle*, Paris (France), Masson, 256 p.

PREECE, C., WINGATE, G.A.S. (1991) *Analysis of Failure Data Collected from a TMR Microprocessor Controller*, Microprocessing and Microprogramming, vol. 32, n° 1-5, p. 861-868.

prEN 418 (1990) *Sécurité des machines - Équipement d'arrêt d'urgence - Aspects fonctionnels*, Comité européen de normalisation, 7 p.

prEN 954-1 (1996) *Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 1 : Principes généraux de conception*, Comité européen de normalisation, 44 p.

prEN 954-2 (1996) *Sécurité des machines - Parties des systèmes de commande relatives à la sécurité - Partie 2 : Validation*, Comité européen de normalisation, 44 p.

prEN 1037 (1994) *Sécurité des machines - Prévention de la mise en marche intempestive*, Comité européen de normalisation, 16 p.

prEN 1050 (1996) *Sécurité des machines - Principes pour l'appréciation du risque*, Comité européen de normalisation, 21 p.

prEN 1088 (1995) *Sécurité des machines - Dispositifs de verrouillage associés à des protecteurs - Principes de conception et de choix*, Comité européen de normalisation, 38 p.

PROULX, D. (1992) *GMC 901 - Projet de design 1, Méthodologie du design*, Note de cours, Université de Sherbrooke, Sherbrooke (Canada), 83 p.

PROULX, D. (1995) *AKI 700 - Créativité et innovation en ingénierie*, Note de cours, Université de Sherbrooke, Sherbrooke (Canada), s.p.

RAAFAT H.M.N. (1979) *Reliability in Design and Failure to Safety*, Engineering, p. 1425-1429.

RAHEJA, D.G. (1991) *Assurance Technologies, Principles and Practices*, New York (États-Unis), McGraw Hill, 342 p.

RAO, M., WANG, Q., ZHOU, J.(1995) *Intelligent Systems Approach to Conceptual Design*, International Journal of Intelligent Systems, vol. 10, n° 3, p. 529-293.

REUNANEN, M. (1993) *Systematic Safety Consideration in Product Design*, Thèse de doctorat, Université de Tampere (Finlande), 125 p.

ROBERTS, R.H. (1989) *Design Plants for Safety*, Hydrocarbon Processing, vol. 68, n° 9, p. 92-98.

ROBERTS, V.L. (1984) *Defensive Design*, Mechanical Engineering, vol. 106, n° 9, p. 88-93.

ROUCHOUSE, G. (1991) *Sûreté des automatismes*, Centre technique des industries mécaniques, Saint-Étienne (France), 139 p.

RUXTON, T., WANG, J. (1997) *A Review of Safety Analysis Method Applied to the Design Process*, Journal of Engineering Design, vol. 8, n° 2, p. 131-152.

RYAN, J.P. (1986) *Human Error and It's Consideration in Safe Product Design*, Professional Safety, vol. 31, n° 4, p. 20-24.

SANDWELL (1995) *Sandwell 95*, Vancouver (Canada), 60 p.

ST-AMANT, R. (1993) *Création d'un processus systématique de mise en oeuvre de plans d'expérience industrielle*, Mémoire de maîtrise ès sciences appliquées, Université de Sherbrooke, Sherbrooke (Canada), 194 p.

SIMMONS, J.M. (s.d.) *Safety Shutdown Systems*, p. 115-122.

SMITH, M.W. (1991) *PLC Emergency Shutdown Systems Used with a DCS in a Pilot Plant Environment*, Proceedings of the Industrial Computer Conference, vol. 1, p. 327-336.

STEPHANS, R.A., TALSO, W.W. 1993 *System Safety Analysis Handbook*, Albuquerque, New Mexico (États-Unis), System Safety Society, 491 p.

SUOKAS, J. (1988) *Evaluation of the Quality of Safety and Risk Analysis in the Chemical Industry*, Risk Analysis, vol. 8, n° 4, p. 581-591.

STERLE, L. (1991) *Applying PLCs in Safety Systems*, Control & Instrumentation, vol. 23, n° 1, p. 39-40.

STOOP, J.A. (1990) *Safety and the Design Process*, Thèse de doctorat, Université de Delft (Hollande), 125 p.

TAYLOR, M.A. (1994) *Performability Metrics for a Distributed Control System*, Proceedings of the Industrial Computing Conference, p. 385-392.

TÉLÉMÉCANIQUE (1989) *Les interrupteurs de sécurité XCK-J*, France, 11 p.

THOMAS, H.W. (1988) *A Quantitative Approach to the Use of Programmable Controllers in Safety Circuits*, American Institute of Chemical Engineers National Meeting, New York (États-Unis), 75B, 16 p.

THURSTON, C.W. (1994) *Programmable Electronic Systems Applied for Risk Control in Petrochemical Plants*, ISA Transactions, vol. 33, n° 1, p. 83-97.

TOOLA, A. (1992) *Safety Analysis in Conceptual Design of Process Control*, Thèse de doctorat, Technical Research Center of Finland (Finlande), VTT Publications 117, 100 p.

VALOREX (1993) *Programme de formation à l'analyse de la valeur*, Longueuil (Canada), Valorex inc., 93 p.

VILLEMEUR, A. (1988) *Sûreté de fonctionnement des systèmes industriels - Fiabilité, facteurs humains, informatisation*, Collection de la direction des études et recherches d'Électricité de France, Paris (France), Eyrolles, s.p.

WALCZAK, T.A. (1990) *Emergency PLC Controlled Shutdown*, Advances in Instrumentation Proceedings, vol. 45, partie 4, p. 1711-1725.

WARDEN, D.D., ZIMMER, D.R. (1991) *DCS, PLC Increase Safety of Chemical Storage Operation*, I&CS, vol. 64, n° 10, p. 47-50.

WATERBURY, R.C. (1991) *Fault-Tolerant/Fail-Safe Systems Are Fundamental*, INTECH, vol. 38, p. 35-37.

WHALLEY, S.P., MAUND, J.K. (1986) *Improving Human Reliability by Design*, Institution of Chemical Engineers Symposium Series, n° 97, p. 235-248.

WILDI, T. (1991), *Électrotechnique*, 2e édition, Presse de l'Université Laval, Ste-Foy (Canada), 908 p.

WILKINS, M.J. (1991) *The Design and Implementation of Modular Batch Automation Projects*, Proceedings of the Industrial Computing Conference, ISA, vol. 1, p. 69-73.

WILSON, D.K. (1988) *Failure Mode Management : A Loss Prevention Philosophy for Programmable Logic Controllers*, American Institute of Chemical Engineers National Meeting, New York (États-Unis), 75A, 14 p.