Apport de la modélisation et de la simulation à l'analyse des risques et la prévention des accidents d'un site de stockage de GPL

Dahlia Oueidat

THÈSE DE DOCTORAT

de l'Université de Recherche Paris Sciences et Lettres
PSL Research University

Préparée à MINES ParisTech

Apport de la modélisation et de la simulation à l'analyse des risques et la prévention des accidents d'un site de stockage de GPL

Ecole doctorale n°432

SCIENCES ET METIERS DE L'INGENIEUR

Spécialité: SCIENCES ET GENIE DES ACTIVITES A RISQUE

COMPOSITION DU JURY :

M. Gilles Dusserre
Mines d'Alès, Rapporteur

M. Tullio Joseph Tanzi
Institut Mines-Telecom - Telecom ParisTech, Président

M. Emmanuel Garbolino
MINES ParisTech / Psl Research University, Examinateur

M. Franck Guarnieri
MINES ParisTech / Psl Research, Examinateur

M. Karim Hardy
Embry-Riddle Aeronautical University, Examinateur

M. Ali Jaber,
Université du Liban, Examinateur

Soutenue par Dahlia **OUEIDAT**
Le 13 décembre 2016

Dirigée par **Emmanuel Garbolino**
et Franck Guarnieri

REMERCIEMENTS

Tout d’abord, j'adresse toute ma gratitude et reconnaissance à mon directeur de thèse Monsieur Franck Guarnieri. Je le remercie de m'avoir permis d’intégrer son équipe au sein du Centre de Recherche sur les Risques et les Crises (CRC) de MINES ParisTech / PSL Rersearch University. Monsieur, merci pour votre dévouement et votre soutien sans faille tout au long de cette thèse.

Mes remerciements vont également à mon codirecteur de thèse, Monsieur Emmanuel Garbolino pour m’avoir conseillé et orienté dans la conduite de mes travaux. Je le remercie en particulier pour sa disponibilité durant la période cruciale et délicate de rédaction du manuscrit.

Je remercie très respectueusement Messieurs Tullio Tanzi, Professeur à Télécom ParisTech, et Gilles Dusserre, Directeur de Recherche à MINES d’Alès, qui ont accepté d’être les rapporteurs de ce travail. C’est un grand honneur qu’ils me font.

Mes plus sincères remerciements, à Monsieur Ali Jaber, Maître de Conférence à l’Université Libanaise ; il a accepté d’être examinateur de mon travail, il a été mon professeur en Master, il est enfin à l’origine de mon recrutement au sein du CRC.

Je tiens à remercier Karim Hardy, Maître de conférences à Embry-Riddle Aeronautical University, pour son expérience mise généreusement à ma disposition.

Je remercie vivement l’équipe de chercheurs du Centre de recherche sur les Risques et les Crises.

Merci aux enseignants chercheurs et chercheurs associés (Jean-Luc Wybo, Christophe Martin, Aldo Napoli, Éric Rigaud, Valérie Godfrin, Aurélien Portelli, Wim van Wassenhove, Sébastien Travadel) ainsi qu’aux doctorants que j’ai côtoyés. Une pensée particulière pour Constance, Florie, Hortense, Amal, Sophie, Thomas, Justin, Raphael, Thibaut, Martin, Clément, Cécile, Aissame, Stéphanie, Amaury et Diana. Je tiens aussi à remercier Samuel, Sandrine, Myriam, Brigitte et Sylvie.

Je remercie aussi les stagiaires, Théo Agostino qui m’a aidé dans le travail de simulation avec Anylogic et Guillaume Poirrier sur l’application de STAMP dans le domaine du pétrole.

Toute ma reconnaissance aux responsables du groupe Total, Bertrand Lejay et André Marblé qui ont accompagné financièrement et intellectuellement ce travail.

Je remercie également mes parents, Ghassan et Lina. Je vous adore. Merci pour votre soutien et votre confiance qui m'ont permis de suivre cette formation dans les meilleures conditions.

Merci à mon frère Mounif pour son encouragement et ses déplacements pour me tenir compagnie. Courage dans ta carrière d'ingénieur civil, d'ingénieur exploration production pétrole/gaz, de magistrat et voire même de chercheur. Les opportunités ne manquent pas, et je sais que tout est facile pour toi.

À mon frère Ibrahim, merci pour ta tendre affection. Je te souhaite un avenir brillant dans toutes les universités prestigieuses du monde qui font balancer ton cœur.

À Carla, Ahmad et tata Aimée, merci pour votre présence à mes côtés. Carloutta, trois ans plus tard, Franck attend toujours la fiche de lecture de son livre sur l'épuisement professionnel…

Je remercie Monsieur Gebran Boutros, qui m'a permis de bénéficier de sa rigueur intellectuelle et de son efficacité certaine tout au long de mes années d'étude. Je vous exprime mon attachement et ma profonde gratitude.

Je tiens à remercier ma très chère amie Sara El Dana. Finalement avec de la persévérance, le bavardage en classe, les mauvaises notes, les mises à la porte…, n'empêchent pas de mener une carrière dans la recherche. Merci pour ta présence dans toutes les étapes de ma vie depuis le lycée.

Enfin mes remerciements vont à mes cousins et mes amis pour leur présence divertissante à mes côtés.

De l'idée à la thèse

Les modèles d'analyse des risques et de prévention des accidents industriels recouvrent des méthodes et des démarches qui visent à traiter la sécurité des systèmes industriels. Cependant, ces modèles restent limités face à la complexité des systèmes sociotechniques à haut risque, caractérisée par des relations de dépendance entre un grand nombre de composants et l'incertitude liée à l'évolution de leur état et de leur comportement dans le temps et l'espace. La présence, indispensable, d'hommes et de femmes (par plusieurs dizaines, centaines, voire milliers d'opérateurs selon les sites) dans les composants du système et l'implication de phénomènes aléatoires ou chaotiques rendent non-déterministe le comportement de tels systèmes. Une autre caractéristique importante de ces systèmes est que, lorsque l'on intègre un nouveau composant, on se retrouve souvent face à des propriétés émergentes non prévues initialement. Un tel système est donc bien plus que le simple regroupement de ses composants et de ses processus associés. Au sein de ces systèmes à haut risque, même la sécurité devient une propriété émergente. Elle doit donc être traitée par des modèles qui s'appuient sur une approche globale et systémique.

L'objectif de cette thèse est donc de proposer une démarche systémique d'analyse des risques d'un système industriel complexe. La démarche consiste à utiliser les techniques de modélisation et de simulation d'un système, pour comprendre le principe de son fonctionnement en mode normal et en mode dégradé. Selon cette démarche, il ne s'agit pas de procéder à une analyse détaillée des moyens de prévention et de protection d'un système donné, mais plutôt de présenter une méthode de raisonnement en matière de sécurité industrielle qui s'appuie sur un exemple concret. La méthode de modélisation retenue dans ces travaux s'appuie sur les concepts du modèle d'accident systémique appelé STAMP (*System-Theoretic Accident Modeling and Processes*) énoncés par Nancy Leveson, Professeure au MIT (États-Unis) en 2004.

Dans cette démarche, le travail de simulation représente un outil supplémentaire de vérification de la pertinence des moyens de prévention et de gestion des risques du site industriel. Elle peut ainsi être appliquée en phase de conception ou d'exploitation d'une unité industrielle à risques (Garbolino, Chery, et Guarnieri 2016). Elle représente également un élément de description et de compréhension de l'installation pour le

personnel de l'entreprise et les services de l'État en charge de l'inspection. Elle concerne enfin la formation des ingénieurs car elle favorise par la modélisation et la simulation, une meilleure connaissance des dimensions tant techniques, humaines qu'organisationnelles du système industriel considéré.

Plus globalement, l'ambition de la thèse est de contribuer à une série d'expérimentations conduites au sein du CRC depuis 2007, en partenariat étroit avec l'équipe de Nancy Leveson, et ce à la suite des thèses de Karim Hardy, sur la mise en œuvre de STAMP dans le domaine du traitement des déchets (soutenue en 2010), de Jaleh Samadi, sur les risques du stockage et du captage du CO2 (soutenue en 2012) et de Stéphanie Alvarez, sur les risques liés aux véhicules autonomes (thèse en cours, soutenance prévu en juin 2017). Il s'agit d'évaluer les applications possibles de STAMP à des domaines industriels non encore traités par les collègues du MIT ou d'autres membres de réseau international STAMP, ici les risques liés à l'exploitation du GPL.[1]

L'originalité de cette thèse réside aussi dans l'intégration des résultats de la mise en œuvre de STAMP au sein d'une plateforme logicielle de simulation : Anylogic. Cette plateforme permet de mettre en œuvre des modèles de simulation selon trois approches (évènements discrets – dynamique des systèmes - multi-agents). Il s'agit là d'un apport très important à l'analyse des risques car le recours à la simulation permet de prendre en compte le rapport au temps.

Le manuscrit de cette thèse est organisé en cinq chapitres. Un bref aperçu de chacun est donné ci-après.

Le premier chapitre présente le concept d'accident et la contribution des modèles d'accident à la maîtrise des activités industrielles à haut risque.

Le deuxième chapitre détaille le modèle STAMP, développé au sein du MIT, modèle pour lequel la sécurité est formulée comme un problème de contrôle plutôt que simplement comme un problème de fiabilité (ou de disponibilité). La défaillance de composants (et le manque de fiabilité des composants du système) est toujours envisagée, mais plus généralement, les accidents surviennent lorsque les pannes de

[1] Une expérimentation a aussi été conduite par la mise en œuvre de STAMP et de son module d'analyse d'accident CAST sur le retour d'expérience d'un accident dans le secteur du pétrole en mer. L'analyse est présentée en annexe de cette thèse.

composants, les perturbations extérieures, ou que les interactions indésirables et dangereuses entre les composants du système ne sont pas adéquatement traitées, c'est-à-dire contrôlées, conduisant de fait à un comportement dangereux.

Le troisième chapitre présente le système industriel retenu dans le cadre de la thèse. Il s'agit d'un site de stockage/distribution de GPL. Ce site est une installation classée pour la protection de l'environnement soumis à autorisation avec servitude d'utilité publique pour fonctionner. Dans ce chapitre, l'ensemble des moyens de prévention et de protection sont décrits selon une vue pédagogique afin de présenter la démarche d'analyse des risques d'un système industriel selon le modèle STAMP.

Le chapitre 4 détaille la problématique industrielle et la contribution de STAMP dans l'approche d'analyse des risques inhérents à l'activité. L'application de STAMP met en exergue les notions de contrainte, de structure hiérarchique et de modèles de processus (boucles de contrôle). L'objectif de cette application est d'établir une stratégie globale d'évaluation de la sécurité et la formulation des recommandations pour réduire les vulnérabilités.

Le chapitre 5 décrit le « couplage » entre STAMP et une plateforme logicielle de simulation : Anylogic. Les données préalablement acquises et modélisées sont reprises afin de conduire une série de simulations en considérant le fonctionnement du site en mode normal puis en mode dégradé. Le couplage des résultats de l'analyse des risques avec la plateforme de simulation permet ensuite d'évaluer les dangers et de proposer des pistes concrètes pour la prévention.

TABLE DES MATIERES

CHAPITRE 1: Le concept de l'accident 13
1. Définition générale du concept d'accident 14
1.1 Classification des causes de l'accident 16
1.1.1 Approche linéaire d'analyse des causes de l'accident 17
1.1.2 Approche multifactorielle d'analyse des causes de l'accident 17
1.1.3 Approche systémique de l'analyse des causes de l'accident 18
2. Bref retour historique 19
2.1.1 L'ère des facteurs techniques 20
2.1.2 L'ère du facteur humain 21
2.1.3 L'ère du facteur organisationnel 22
2.1.4 L'ère des facteurs inter-organisationnels 24
3. Les modèles conceptuels de l'accident 25
3.1 Le modèle conceptuel du Domino 25
3.1.1 Les modèles conceptuels construits sur les base du modèle Domino 26
3.1.2 Chaîne d'événements multilinéaires 28
3.2 Les modèles conceptuels sociotechniques 29
3.2.1 Le modèle conceptuel de Reason 30
3.2.2 Intégration d'une chaîne évènementielle dans le modèle de Reason 31
4. Les limites des modèles conceptuels de l'accident 32
4.1 Limite des modèles traditionnels 34
4.1.1 Subjectivité dans la sélection des évènements 35
4.1.2 Subjectivité dans la sélection des conditions 36
4.1.3 Recherche des facteurs de cause de l'accident 37
4.2 Les répercussions des limites des modèles conceptuels traditionnels dans les systèmes industriels complexes 38
4.2.1 Des composants fiables mais des interactions entre composants sont dangereuses 39
4.2.2 Dangereux mais fiables 40
4.3 Les limites des greffes des facteurs systémiques sur les modèles conceptuels 41
5. Synthèse du chapitre 45
CHAPITRE 2: Presentation de STAMP 47
1. Petite histoire de la systémique 48
2. La démarche induite de la systémique pour l'analyse de l'accident 52
2.1.1 L'émergence de la structure hiérarchique 54
2.1.2 Principe de rétroaction 56
3. Le modèle STAMP 58
3.1 Les hypothèses de base du modèle STAMP 59
3.1.1 Le manque de contrôle provoque l'accident 60
3.1.2 Les modèles conceptuels traditionnels d'analyse des accident représentent des limites 60

3.1.3 L'approche probabiliste d'analyse des risques et de prévention des accidents représente des limites 61
3.1.4 L'environnement de travail influence le comportement de l'opérateur 61
3.1.5 La présence des systèmes automatisés fiables de contrôle du processus n'est pas suffisant pour maîtriser la sécurité 62
3.1.6 La migration du système vers un état accidentel peut être anticipée par un travail de conception approprié au système 62
4. Le concept STAMP 64
4.1 Conception des lois de contrôle (contraintes de sécurité) 64
4.2 Modélisation de la structure hiérarchique 65
4.3 Les modèles de contrôle des processus 66
5. Classification factorielle des accidents selon STAMP 69
5.1 Le fonctionnement du système de contrôle 70
5.1.1 Des données d'entrées dangereuses 71
5.1.2 Algorithme de contrôle non fiable 71
5.1.3 Les actionneurs et les processus contrôlés 71
5.1.4 Coordination et communication entre contrôleurs et décideurs 72
5.1.5 Contexte et environnement 72
6. Les outils de STAMP 72
6.1 STPA 72
6.1.1 Phase Statique 74
6.1.2 Phase dynamique 74
6.1.3 Finalité de STPA : 74
6.2 Le modèle CAST (Causal Analysis Based on System Theory) 75
6.3 Le logiciel XSTAMPP 77
6.4 STPA tools 77
6.5 SafetyHAT 78
6.6 ASTPA 79
7. Conclusion 80
CHAPITRE 3: Presentation du systeme d'etude 81
1. Situation règlementaire 82
1.1 Organisation en matière de prévention des risques majeurs 85
1.1.1 Politique de prévention des accidents majeurs 85
1.1.2 Système de gestion de la sécurité (SGS) 85
1.1.3 Plan d'opération interne 86
1.1.4 Plan Particulier d'Intervention (PPI) 86
2. Présentation de l'installation technique 87
2.1 Réservoir sous-talus de propane 89
2.1.1 Dimension 89
2.1.2 Pressions 90
2.1.3 Equipements d'exploitation et de sécurité 90
2.2 Pomperie 91
2.3 Canalisation 92
2.4 Postes de transfert 93
2.4.1 Le poste chargement / déchargement 93
2.4.2 Les deux postes de chargement 94
2.4.3 Les équipements de transfert 94
3. Description des opérations de transfert 95

3.1 Procédure de transfert du site 96
3.2 Identification et déroulement de l'activité de transfert 97
3.2.1 Cas opération de chargement 97
3.2.2 Cas opération de déchargement 98
3.3 Méthode de calcul du poids à charger 99
4. Les dispositifs de sécurité 99
4.1 Arrêts d'urgence (Boutons poussoirs) 101
4.2 Les Détecteurs gaz 102
4.2.1 Principe de contrôle du système de détection de gaz 102
4.2.2 Traitement du signal 103
4.2.3 Les électrovannes 103
4.2.4 Les actionneurs 103
4.2.5 Les vannes 103
4.2.6 Les caplets internes 103
4.3 Les détecteurs de flammes 107
4.3.1 Principe de contrôle du système de détection de flamme 107
4.3.2 Traitement du signal 107
4.3.3 Arrosage 108
4.3.4 Les conséquences suite à la détection de flamme 108
4.4 Alarmes techniques du réservoir sous-talus 109
5. Conclusion 111
CHAPITRE 4: Demarche de modelisation STPA 113
1. Explication brève de la démarche STPA 113
1.1 Identification des accidents 113
1.1.1 Délimitation du cadre du système d'étude 114
1.2 Identification des dangers 116
1.3 La structure de contrôle organisationnel (hiérarchique) 116
1.4 Identification des dangers sur les instructions contrôles-commandes du système (étape 1) 119
1.4.1 La méthode simplifiée 119
1.4.2 Méthode dite systématique 120
1.5 Énoncer les exigences et les contraintes de sécurité 122
1.5.1 L'action commandée fournie par le contrôleur ou le système de contrôle est dangereuse 124
1.5.2 L'action commandée fournie est appropriée et requise, cependant elle n'est pas appliquée ou exécutée correctement 124
1.6 Développer des recommandations à partir des causes identifiées 124
1.7 Evaluer les composants de la structure hiérarchique 125
2. L'étude de cas 125
2.1.1 Le phénomène UVCE 129
2.1.2 Le phénomène BLEVE 130
2.2 Les accidents considérés dans cette étude de cas 131
2.3 Les dangers du système d'étude 131
2.4 La structure organisationnelle de contrôle de la sécurité 132
2.4.1 Structure générale de contrôle de la sécurité de l'installation 133
2.4.2 Exemple de la structure de contrôle de la sécurité de l'installation technique 134
2.5 Les variables du processus contrôlé 135

2.5.1 Associer une action commandée à chaque variable 137
2.6 Les actions dangereuses déclenchées par commande (étape 1) 138
2.6.1 Cas où l'action commandée est générée par le système de contrôle 139
2.6.2 Cas où le système ne génère pas la fermeture de la vanne (par commande) 143
2.7 Assigner les contraintes de sécurité aux actions dangereuses avec STPA 144
2.8 Etude des causes des actions dangereuses (étape 2) 145
2.8.1 Analyse des causes de l'AD (Action Dangereuse) 146
2.8.2 Les causes relatives aux actions déclenchées (par commande) et non exécutées 147
3. Conclusion et discussions des résultats 148
CHAPITRE 5: Modele de simulation 151
1.1 Étapes de modélisation et de simulation 151
1.1.1 La formulation du problème 153
1.1.2 Objectifs et organisation 153
1.1.3 Modélisation 154
1.1.4 Exécution de la simulation 154
2. L'outil de modélisation et de simulation AnyLogic 155
2.1 L'approche par la dynamique des systèmes 155
2.2 L'approche par les systèmes multi-agents 156
2.3 L'approche par événement discret 158
2.3.1 Initialisation de la réplique 159
2.3.2 Gestion des entités 159
2.3.3 Gestion des évènements 160
2.3.4 Les files d'attente 160
3. Modélisation multi-paradigmes de la sécurité d'un site industriel 161
3.1 Agent Chauffeur 162
3.2 Agent « GrosPorteurs » 166
3.3 La classe Main 167
3.3.1 Les objets utilisés pour la modélisation en système à événement discret SED dans l'interface main 169
3.3.2 Alertes sur les réservoirs 175
3.3.3 Les différents modes de contrôle des opérations 177
3.4 L'agent Pompiste 179
3.4.1 Les composants de l'actionchart 182
3.5 Poste de déchargement 182
3.5.1 Procédure de transfert 184
3.5.2 Compilation du modèle au poste de déchargement 190
4. Conclusion du chapitre 192
Conclusions et perspectives 195
Annexe 199
Références 211

LISTE DES FIGURES

Figure 1-1 Évolution de la pensée dans l'approche de l'analyse des risques et prévention des accidents (Groeneweg, 2002) 20
Figure 1-2 L'accident un événement dans une chaîne séquentiel ordonnée 26
Figure 1-3 Modèle conceptuel évènementiel, séquentiel et conditionnel (Qureshi, 2007) 29
Figure 1-4 Intégration d'une chaîne séquentielle dans le modèle conceptuel de Reason (Qureshi, 2007) 32
Figure 1-5 Types de facteurs systémiques (Leveson, 2011) 43
Figure 1-6 : Cadre de Rasmussen (Hardy, 2011a; Leveson, 2011) 44
Figure 2-1 Degré de complexité (Leveson, 2011) 53
Figure 2-2 Structure hiérarchique (Hardy, 2010; Leveson, 2011) 66
Figure 2-3 Boucle de contrôle 68
Figure 2-4 Classification des causes de l'accident selon STAMP 69
Figure 2-5 Les causes des problèmes de manque de contrôle 70
Figure 2-6 Interface du logiciel STPA tool 78
Figure 2-7 Interface principale du logiciel SafetyHAT 79
Figure 2-8 Interface du logiciel XSTAMPP pour une étude STPA 80
Figure 3-1 Installations et servitudes techniques 88
Figure 3-2 Réservoir sous talus de propane 89
Figure 3-3 Compresseur ballon 91
Figure 3-4 les pompes 92
Figure 3-5 Présentation des deux phases de déchargement des camions gros Porteurs 96
Figure 3-6 La chaîne de détection de gaz 104
Figure 3-7 Implantation détecteurs 105
Figure 3-8 La chaîne de détection de flamme 109
Figure 4-1 Conditions et évènements 116
Figure 4-2 Structure de contrôle du processus d'exploitation et d'opération 117
Figure 4-3 Boucle de contrôle de la sécurité 118
Figure 4-4 Composition d'une action dangereuse 120
Figure 4-5 Classification des fateurs de causalité contribuants aux dangers 123
Figure 4-6 Diagramme PID 126
Figure 4-7 Grille MMR 127
Figure 4-8 Les causes d'un UVCE 130
Figure 4-9 Structure administrative et organisationnelle 133
Figure 4-10 Structure administrative locale chargée de la sécurité de l'installation 134
Figure 4-11 Exemple de la structure de contrôle de la sécurité au niveau du système d'exploitation 135
Figure 4-12 Classification des variables d'un système 137
Figure 5-1 Les étapes de la démarche (Cantot, 2006) 153
Figure 5-2 Les agent du projet de simulation 161
Figure 5-3 Interface agent chauffeur 162
Figure 5-4 Simulation de la formation d'une population de chauffeurs camion gros porteur 166
Figure 5-5 Interface agent « GrosPorteurs» 166
Figure 5-6 Image du site introduite dans la classe main 168

Figure 5-7 Partie SED du Main distinguant les différentes branches possibles selon le niveau de formation du chauffeur du camion gros porteur 170
Figure 5-8 Conséquence du déclenchement de l'alerte niveau bas sur le système d'événements discrets. 173
Figure 5-9 Evénements pouvant se déclencher lorsque le niveau du réservoir varie ... 176
Figure 5-10 Alerte de niveau bas sur le réservoir. 176
Figure 5-11 Réservoir et différents événements liés. 177
Figure 5-12 Panneau de contrôle : mode dégradé 177
Figure 5-13 Perte de contrôle manque de ressource pompiste 178
Figure 5-14 Conséquence du manque de ressource pompiste. 178
Figure 5-15 Perte de contrôle : manque de temps entrainant une volonté d'accélérer.. 178
Figure 5-16 Perte de contrôle : cascade de manque de temps, compétence, et ressource. 179
Figure 5-17 Interface de l'agent pompiste 180
Figure 5-18 Propriété de la ressource "Pompiste" et des unités de ressources "pompistes" 181
Figure 5-19 Actionchart de la fonction d'identification des chauffeurs par le pompiste 182
Figure 5-20 Camion gros porteur arrêté pour identification 183
Figure 5-21 Résultat de l'identification (premier cas) 183
Figure 5-22 Résultat de l'identification (second cas) 184
Figure 5-23 Résultat de l'identification (troisième cas) 184
Figure 5-24 Résultat de l'identification (quatrième cas) 186
Figure 5-25 Diagramme états-transitions procédural du poste de déchargement 188
Figure 5-26 Diagramme stock-flux du poste de chargement 188
Figure 5-27 Diagramme états-transitions opérationnel du poste de chargement 189
Figure 5-28 Début de déchargement. Vue en système d'événements discrets. 190
Figure 5-29 Phase 1 : début de déchargement. Etapes oubliées ou mal réalisées. 191
Figure 5-30 Phase 2 : Fin de déchargement. Vue en dynamiques de système. 191
Figure 5-31 Propriété de l'événement « StopperChargement » déclenché par condition (le petit porteur est rempli quand il atteint 3% du volume du réservoir. 192

LISTE DES TABLES

Table 2-1: Les hypothèses 63
Table 3-1: Arrêtés préfectoraux de l'établissement étudié 83
Table 3-2: AS : Autorisation avec servitudes A : Autorisation D : Déclaration 83
Table 3-3:Canalisation 92
Table 3-4: Les dispositions matérielles 96
Table 3-5: Cause et conséquence du déclenchement des alarmes de détection fuite de gaz 106
Table 3-6: Cause et conséquence du déclenchement des alarmes de niveau RST 110
Table 4-1: Les actions de contrôle dangereuses 119
Table 4-2: Tableau de contextes concernant une action de type fournie par le système de contrôle 121
Table 4-3: Tableau de contextes l'inaction du système automatisé 122
Table 4-4: Les accidents d'ordre général à prévenir dans ce système 131
Table 4-5: Les dangers d'ordre général à prévenir dans ce système 132
Table 4-6: Les dangers liés à la commande de fermeture des vannes d'emplissage 139
Table 4-7: Table de contexte cas ou le système initie la commande de Fermeture des vannes 141
Table 4-8: Table de contexte cas ou le système n'enclenche pas commande de Fermeture des vannes 144
Table 4-9: Les actions dangereuses et les contraintes de sécurité correspondantes 145
Table 5-1: Les éléments du modèle 163
Table 5-2: Les éléments du modèle SED dans la classe main 171
Table 5-3: Explication des objets du diagramme SED 174
Table 5-4: Orientation de l'objet (SelectOutput5) 175
Table 5-5: modélisation des étapes du processus de déchargement 187

CHAPITRE 1: LE CONCEPT DE L'ACCIDENT

Un concept est la « représentation mentale d'un objet » (Centre National de Ressources Textuelles et Lexicales). Il regroupe l'ensemble des prédicats relatifs à la perception d'un sujet donné. Le concept d'accident englobe les différentes théories construites par l'esprit humain et scientifique pour appréhender un objet ou un phénomène. On peut ainsi appréhender la notion d'accident en suivant la loi des trois états de la connaissance énoncée par Auguste Comte (Garbolino et al., 2010).

Dans sa tentative de trouver des réponses à la complexité, l'esprit humain passe par trois états (l'état théologique, l'état métaphysique et l'état scientifique) pour appréhender des phénomènes comme celui qui nous concerne ici : l'accident.

L'état théologique correspond à l'approche qui s'attache à déterminer les causes de l'accident. On attribue alors l'intention des objets (fétichisme), l'existence de forces surnaturelles ou d'un dieu responsable à la survenue de ce phénomène. L'état métaphysique se situe dans la suite de l'évolution des connaissances humaines. Les agents surnaturels sont alors remplacés par des forces abstraites : on parle de la « Nature » chez Spinoza, du « Dieu géomètre » chez Descartes, de la « Matière » chez Diderot, de la « Raison » au siècle des Lumières. Enfin l'état scientifique repose sur le recours aux faits, à l'expérimentation, à l'épreuve de la réalité, la recherche par l'usage unique du raisonnement et de l'observation les lois effectives pour expliquer les phénomènes et notamment l'accident. La base de la pensée scientifique s'appuie donc sur la raison, la mesure et l'analyse. Elle se fixe comme règle la décomposition des éléments emboîtés en éléments plus simples afin de rechercher la cause d'un événement.

La démarche de construction de la société industrielle ainsi que la démarche d'évolution des découvertes scientifiques et technologiques des siècles derniers se sont appuyées sur une méthode de pensée analytique et cartésienne. Cependant, les scientifiques confrontés progressivement à la complexité et à la globalité ont ressenti le besoin d'adopter de nouvelles méthodes, voire de trouver un nouveau paradigme, d'où

la nécessité d'adopter les aspects de la systémique dans la tentative d'approche de la vérité des accidents technologiques.

L'approche systémique de l'accident permet de saisir les principes, les modèles et les lois nécessaires à la compréhension des relations et des interdépendances entre les composants (techniques, humaines et organisationnels) d'un système complexe (Hardy, 2010). Au départ, dans la démarche d'approche de la vérité de l'accident, les facteurs systémiques sont ajoutés aux causes linéaires de l'accident. Cet aspect de la systémique ne semble pas se différencier de l'approche analytique. C'est à travers la dynamique des systèmes et la modélisation des phénomènes complexes que la pensée scientifique tente actuellement de se démarquer en mettant l'accent sur l'intelligibilité du comportement du système en prenant en compte le temps pour appréhender l'accident.

Dans ce chapitre, il s'agira de décrire l'évolution des différentes perceptions de l'accident. Tout d'abord, nous évoquerons les définitions de l'accident (section 1). Nous décrirons ensuite le développement du courant de la pensée scientifique du concept d'accident qui accompagne les modes de gestion de la sécurité (section 2). Nous exposerons aussi les différents modèles conceptuels proposés par la communauté scientifique pour expliquer les causes d'un accident (section 3). Enfin, nous expliquerons d'une façon concise les limites de ces modèles (section 4).

1. Définition générale du concept d'accident

Le mot « accident » vient du latin « accidens » et signifie la circonstance d'une cause, d'un sinistre, d'un événement imprévu ou d'un malheur. Il provient aussi du verbe latin « accidere » qui veut dire « survenir ». La survenue d'un accident est donc souvent impromptue, imprévue et soudaine, accompagnée irrémédiablement de dégâts corporels et matériels. Les dégâts peuvent être plus ou moins importants, à caractère temporaire ou permanent.

C'est donc une rupture fortuite, sans motif apparent qui affecte une personne ou un groupe de personnes, en interrompant le déroulement normal, probable et attendu des choses. Les termes décrivent une situation qui découle d'un flux de danger, et qui peut

être décrite comme désastreuse, catastrophique, troublante, calamiteuse, tragique, urgente ou de crise. Flou et imprécision, aléa et instabilité, ambiguïté, incertitude et imprévisibilité constituent une combinaison inhérente de la complexité qui entoure le terme d'accident. Ces caractères complexes de l'accident résident donc dans la multiplicité des composants, dans la diversité de leurs interrelations ainsi que dans l'imprévisibilité potentielle des comportements, suscitant des phénomènes d'émergence intelligibles, mais non toujours prévisibles.

Au-delà des événements d'échec, la définition plus large de l'accident dans un contexte complexe comprend les mécanismes systémiques aléatoires, directs et indirects, qui ont induit l'accident. L'approche de la vérité de l'accident exige la connaissance exhaustive et la compréhension de la structure et des lois de fonctionnement des processus complexes. La temporalité ainsi que la sensibilité de ces processus présentent un rôle fondamental dans la compréhension de ce phénomène.

C'est ainsi que les processus sont appréhendés dans une logique d'évolution dynamique d'ordre et de désordre qui rend bien souvent imprévisibles, en tout cas incertain, les modifications des contraintes qui entrainent l'accident dans un système complexe. L'accident majeur ou l'accident technologique lié à l'activité industrielle de l'homme entraine souvent des dégâts humains, matériels, et environnementaux. Leveson, (2011) définit l'accident qui survient dans un système industriel complexe ainsi :

Un accident est une perte indésirable dû à un imprévu, à un évènement non souhaité. Cette perte peut entraîner mort d'homme et un préjudice, mais il peut également impliquer d'autres pertes majeures, notamment de mission, matérielles, financières et perte d'informations. Les pertes résultent des défaillances de composants, de troubles à l'extérieur du système, des interactions entre composants du système, et les comportements individuels des composants du système qui conduisent à des états dangereux du système. Des exemples de dangers incluent le rejet de produits chimiques toxiques d'une raffinerie de pétrole, un patient recevant une dose médicamenteuse

mortelle, deux aéronefs violant l'espace minimum de séparation requise, et de trains de banlieue dont les portes s'ouvrent de manière inattendue entre deux gares.[2]».

Les accidents sont donc des processus complexes impliquant l'ensemble sociotechnique du système.

1.1 Classification des causes de l'accident

Dans un contexte technologique, la manière de percevoir un accident a évolué. On distingue d'abord une pensée linéaire dans les modèles conceptuels de l'accident. Venus de la sécurité industrielle, ils reflètent les facteurs inhérents à la protection des installations de production mais aussi des travailleurs contre les blessures ou la maladie. Plus tard, ces mêmes modèles furent appliqués à l'ingénierie et à l'exploitation des systèmes techniques et sociaux complexes.

Au début, l'accent en matière de prévention des accidents du travail était porté sur les conditions dangereuses. Bien que l'effort mobilisé autour de la prévention des conditions dangereuses s'est avéré très efficace et a permis de réduire les accidents du travail, l'émergence de flux de danger de nature nouvelle a conduit à ralentir le progrès dans la diminution des facteurs à risques. Cela a donc nécessité l'emploi de nouvelles méthodes pour maîtriser l'impact de ce flux de danger. L'accent est alors mis sur les actes dangereux : les accidents ont commencé à être considérés comme étant la faute d'un individu, plutôt que d'un événement qui aurait pu être évité par un changement adéquat.

Cette démarche de pensée qualifiée de traditionnelle, évènementielle, séquentielle, directe et linéaire présente des limites. Pour pallier alors aux inconvénients de la pensée linéaire, d'autres aspects de causalité se sont développés. Dans cette section, nous allons aborder brièvement ces aspects de causalité puisqu'ils constituent

[2] An accident is an unplanned and undesired loss event. That loss may involve human death and injury, but it may also involve other major losses, including mission, equipment, financial, and information losses. Losses result from component failures, disturbances external to the system, interactions among system components, and behavior of individual system components that lead to hazardous system states. Examples of hazards include the release of toxic chemicals from an oil refinery, a patient receiving a lethal dose of medicine, two aircraft violating minimum separation requirements, and commuter train doors opening between stations.
.

les fondements de base des modèles conceptuels des accidents étudiés dans les chapitres suivants.

1.1.1 Approche linéaire d'analyse des causes de l'accident

Quand on parle de la pensée linéaire (Morin, 2015), chaque phénomène se voit ainsi relié à une cause. Un évènement est donc représenté comme une relation simple de cause à effet. Se déroule alors une chaîne d'évènements liés par une relation de cause à effet. C'est ainsi que l'on peut interpréter l'accident comme un phénomène qui réside dans une chaîne d'évènements défaillants liés par une simple relation de cause à effet (Heinrich, 1941).

Depuis René Descartes (Laporte, 1988), mais déjà depuis Aristote (Rodrigo, 2011), la recherche scientifique est fondée sur le postulat de la causalité : les phénomènes du monde peuvent être expliqués par un enchaînement de causalités. Si un phénomène apparaît comme trop complexe, il suffit de le décomposer en plusieurs enchaînements de causalités pour l'analyser. Cette démarche est dite analytique.

Avec la théorie systémique (Durand, 1979), la démarche est totalement différente. La systémique est une méthode scientifique permettant d'aborder des sujets complexes qui apparaîssaient réfractaires à l'approche parcellaire des sciences exactes issues du cartésianisme.

1.1.2 Approche multifactorielle d'analyse des causes de l'accident

La causalité multifactorielle (Peretti-Watel, 2004) juxtapose un grand nombre de facteurs contributifs, chaque facteur serait dû alors à un ensemble de causes contributives. Des modèles conceptuels sont issus de cet aspect de causalité multifactorielle à des fins de gestion de la sécurité industrielle ou pour des fins de représentation d'une séquence accidentelle. Néanmoins, l'aspect de causalité multifactorielle se heurte à des limites. L'augmentation exponentielle du nombre des facteurs ainsi que le suivi temporel des causes contributives à considérer rendent la séquence difficile pour comprendre un phénomène (Revet, 2009).

Pour saisir la réalité, il faut par exemple par cette approche se perdre dans le désert et dénombrer chaque grain de sable. Les moyens requis pour agir augmentent de façon exponentielle. L'acquisition d'une vision d'ensemble devient de plus en plus difficile, ce qui constitue, en soi, un nouveau facteur de difficulté. C'est ainsi que l'on passe de l'étude d'un ensemble à l'étude d'un système. La causalité revêt alors un nouvel aspect qualifié de systémique.

1.1.3 Approche systémique de l'analyse des causes de l'accident

L'approche systémique permet de montrer que la multitude des facteurs sont en réalité reliés les uns aux autres (Perrin et al., 2012). Il ne s'agit jamais de variables purement indépendantes. Chacun contribue peut-être à l'effet final, mais influence aussi d'autres facteurs au sein de chaînes causales : le facteur A influence le facteur B, qui lui-même a une influence sur le facteur C, etc.

La mise en évidence de ces chaînes d'influence simplifie les raisonnements. La causalité systémique n'est pas « linéaire » mais « circulaire ». La causalité s'organise dans des chaînes plus ou moins longues qui forment une boucle sur elles-mêmes. La causalité systémique intègre l'histoire, mais elle peut être parfois considérée comme un processus sans mémoire. La causalité systémique offre un schéma explicatif qui illustre comment se manifeste un phénomène (Bouloiz et al., 2013). Elle indique des tendances et des conséquences possibles.

La causalité systémique met en évidence des pistes inédites. De nombreuses pistes d'action ont trait aux relations entre les facteurs, aux phénomènes de couplage (ou de découplage), etc. Ces pistes d'action sont généralement ignorées lorsqu'on se concentre sur les seuls facteurs. La causalité systémique montre aussi l'importance du temps (Hardy, 2010). Pour agir avec justesse, il faut savoir intégrer ce paramètre : comme s'ajuster aux temps de réaction spontanés des processus ou exploiter le temps comme un allié plutôt que de l'avoir comme un ennemi.

2. Bref retour historique

Cambon (2007) montre comment l'appréhension de la vérité de l'accident s'est faite par étapes (Figure 1-1). La manière d'appréhender cette question se centra d'abord sur les composants techniques du système jusqu'aux années 50-60, puis sur le facteur humain, jusqu'au milieu des années 80, pour enfin s'attarder sur les aspects organisationnels voire inter-organisationnels. Les modèles conceptuels d'accident, engendrés par les perspectives de retour d'expérience, sont principalement à l'origine de cette évolution (Cambon et al., 2006).

En vue de protéger les vulnérabilités, les autorités publiques imposent la mise en application de réformes règlementaires. Au cours des années 1970-1980, les industriels ont dû se conformer aux prescriptions, normes et exigences des autorités. La croissance rapide du développement technologique rend cependant impossible la gestion de la multitude des facteurs à risque uniquement par le recourt au prescrit (la loi, la règle).

Dans certains pays, l'autorégulation par l'industriel se tourne vers les organisations normatives. La législation internationale et notamment européenne appelée directive Seveso est imposée à l'ensemble des pays de l'Union européenne ; les législations et réglementations nationales sont pour la plupart conformes aux directives internationales et européennes. En France, on retrouve l'autorité de régulation des installations classées pour l'environnement. Bien que plus ancienne que la directive européenne de Seveso, elle est cependant conforme à cette dernière. Les mesures préventives réglementaires relèvent de trois aspects :

- La prévention des risques professionnels, les risques industriels étant essentiellement de même nature que les risques industriels majeurs ;
- Les mesures supplémentaires spécifiques aux accidents majeurs et susceptibles de réduire l'importance des dégâts causés tant au niveau des victimes humaines que de l'environnement (pollution et constructions) ;
- Les mesures relatives à l'organisation des secours et des interventions post-accident.

Les mesures réglementaires appliquées aux entreprises où existent des risques majeurs font l'objet de contrôles et d'autorisations périodiques par les services préfectoraux (installations classées, DRIRE devenues les DREAL). En fonction de leur nature, les mesures de prévention, qu'elles soient réglementaires ou non, relèvent de deux types :

- les mesures techniques correspondant à la mise en place de moyens matériels liés aux processus opératoires : équipements de sécurité et de contrôle, interdiction ou restriction dans l'emploi de certains produits très dangereux, processus opératoires sécurisés, etc. ; - les mesures à caractère organisationnel et administratif, par exemple la classification des installations classées, le plan particulier d'intervention (PPI) ou le plan de prévention des risques technologiques (PPRT).

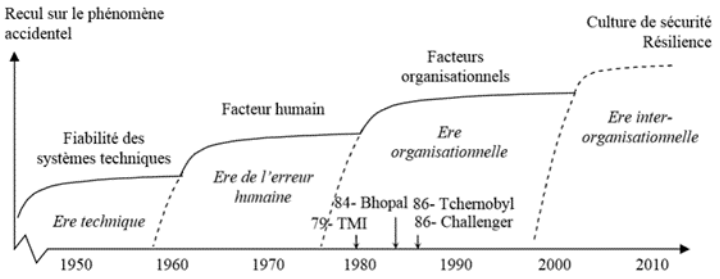


Figure 1-1 Évolution de la pensée dans l'approche de l'analyse des risques et prévention des accidents (Groeneweg, 2002)

2.1.1 L'ère des facteurs techniques

Dans les années 30 (Guarnieri et al., 2008), on fournissait une interprétation empirique de l'accident tout en envisageant la fiabilité et la sécurité technique appelées aussi sûreté de fonctionnement. Après la Seconde Guerre mondiale, la fiabilité des éléments techniques commence à être valorisée à travers un mode de gestion de la sécurité proactive. En effet, le principe de concevoir des équipements fiables est recherché, plutôt que d'attendre les défaillances et ensuite les réparer. C'est dans les années 50 et 60 que les premières méthodes de sûreté de fonctionnement (AMDEC, APR, analyse quantitative des risques, etc.) apparaissent, notamment dans le domaine de l'aéronautique, du nucléaire et de l'électronique et contribuent à accroître la fiabilité

des systèmes (Fadier, et al., 1990; Villemeur et al., 1988). Au cours de cette première « ère », l'accident est ainsi vu comme un problème technique. Le management de la sécurité repose donc sur l'amélioration de la fiabilité des systèmes techniques. Bien que l'hypothèse d'équivalence entre la sécurité et la fiabilité ait accompagné toutes les perspectives historiques de l'accident sans pour autant démontrer sa consistance, les premières études scientifiques montrent cependant qu'à partir des années 60, en plus des défaillances techniques, les interprétations des accidents doivent s'expliquer aussi à travers des erreurs commises par l'homme.

2.1.2 L'ère du facteur humain

A travers une pensée linéaire transposée de l'ère technique et pour interpréter l'accident comme la conséquence d'une erreur humaine, on attribue des causes équivalentes comme l'écart par rapport à une procédure, à une norme, ou à un cadre prescrit de référence. L'accident a lieu dès lors que la procédure prescrite n'est pas strictement respectée par les opérateurs, assimilés à des « composants humains » (Abramovici et al., 1990). On responsabilise les opérateurs tout en ignorant qu'ils ne détiennent pas des moyens, des compétences et de l'autorité. Les psychologues quant à eux définissent le concept d'erreur humaine comme une déviation par rapport à l'intention de l'individu. Elle résulte selon eux des défaillances dans les processus mentaux intrinsèques de l'individu. Ces défaillances cognitives peuvent être accentuées par certains facteurs de contexte qui influencent son état interne (stress, fatigue, température, pression temporelle).

Les approches fiabilistes et psychologiques de l'erreur humaine considèrent dès lors le facteur humain comme une source de défaillance susceptible de mener à l'accident. Cependant force est de constater, malgré l'occurrence répétée de ces erreurs, que les accidents demeurent rares et que l'acteur, capable d'erreur humaine, est aussi capable de les récupérer et de rattraper celles du système. Ces modèles simples et séduisants, transposant les aspects techniques aux aspects humains, se révèlent finalement trop simplistes (Bieder, 2006). De nouvelles hypothèses seront introduites par les ergonomes : l'accident ne s'explique pas par la seule occurrence d'une erreur humaine ni celle d'une seule panne technique, mais d'un mauvais couplage entre

l'opérateur et son environnement direct de travail (poste de travail, pupitre de commande, etc.). Les ergonomes reconnaissent la robustesse des systèmes sociotechniques et la variabilité de la performance humaine qu'ils considèrent comme inévitables mais aussi essentiels pour le système (Fadier et Mazeau, 1996).

On s'intéresse dès lors à l'amélioration du couplage de l'opérateur et de son environnement direct de travail. Cette approche se traduit sur le terrain par diverses pratiques comme par exemple le développement d'une meilleure visibilité du risque (affichage, signalétiques, etc.), d'une meilleure perception et appréhension du risque par l'opérateur (formation), la mise en place de protection collective et individuelle, la préconception ergonomique des postes de travail, la révision des procédures. Le milieu des années 80 et les catastrophes industrielles emblématiques qui les marquent (Three Miles Island, Bhopal, Tchernobyl, Challenger) laissent perplexes les spécialistes du facteur humain (Guarnieri et al., 2008). Les analyses à posteriori de ces accidents parviennent toutes à la conclusion selon laquelle leur apparition reste inexplicable sur la seule base des erreurs humaines individuelles déconnectées du contexte organisationnel dans lequel elles se sont produites (Cullen, 1993; Llory, 1996; Perrow, 1984; Reason, 1990, 2013; Vaughn, 1996). Un changement de paradigme se produit progressivement : celui du passage de l'erreur humaine aux facteurs organisationnels.

2.1.3 L'ère du facteur organisationnel

Sans qu'elle ne soit complètement mise à l'écart, la notion d'erreur humaine se comprend à partir des années 80-90 comme la résultante de causes organisationnelles en amont, c'est-à-dire comme la conséquence d'un environnement organisationnel de travail contraignant l'individu à l'erreur. Les erreurs de l'opérateur sont toujours sources de risque mais c'est l'organisation qui est considérée ici comme l'élément fondamental de sa performance. Le contexte organisationnel, mis en avant par les approches ergonomiques, devient désormais une donnée d'entrée pour comprendre la performance humaine. L'heure est alors à l'identification des facteurs organisationnels de risque favorisant l'erreur de l'opérateur (Desmorat et al., 2013).

L'objectif de la démarche réside dans l'étude de l'organisation dans laquelle évolue l'opérateur et dans l'identification des facteurs organisationnels qui influencent ses actes. Comme le précisent (Bird and Loftus, 1976), le terme d'« *Error Forcing Context* », utilisé aux États-Unis, traduit particulièrement bien cette idée selon laquelle l'opérateur est contraint à l'erreur par les forces et les contraintes exercées sur lui par le contexte organisationnel de travail. L'opérateur peut être comparé à une marionnette dont les mouvements sont influencés par l'organisation qui en actionnerait les fils.

Il convient désormais d'étudier sous cette perspective en amont les caractéristiques organisationnelles qui vont influencer, sur le terrain, la performance de l'opérateur, comme par exemple le rythme de travail, la formation, la communication, etc. Cette évolution dans la manière d'appréhender l'erreur humaine marque au final une double évolution par rapport aux approches prudentes du facteur humain. C'est tout d'abord une évolution dans le temps puisque ce sont les décisions qui ont été prises en amont, dans le passé, qui sont désormais analysées. C'est aussi une évolution géographique puisque, seules les erreurs commises par les opérateurs de première ligne étaient précédemment pointées du doigt. Ce sont désormais les mauvaises décisions d'autres acteurs (managers, supérieurs et ingénieurs) en matière de gestion, conception, maintenance, formation, etc. qui sont sous le feu des projecteurs.

Reason est l'auteur qui a largement inspiré cette perspective et qui a contribué à son développement. Il introduit, avec son célèbre *modèle gruyère*, les notions d'erreurs actives qui ne peuvent se comprendre qu'en référence aux conditions latentes qui demeurent cachées dans le système (Reason, 2016; Reason, 1995). L'approche de management de la sécurité proposée par cette perspective repose sur l'identification des conditions latentes de défaillances cachées dans le système, sur l'élimination ou la diminution de leur influence, sur la fiabilisation des processus organisationnels, l'analyse de la qualité de la gestion de la sécurité et la mise en place de systèmes de management de la sécurité.

2.1.4 L'ère des facteurs inter-organisationnels

De nouveaux fondements scientifiques, actuellement en cours de développement et de formalisation, viennent depuis peu compléter cette approche organisationnelle de la sécurité, qualifiée par certains de linéaire (Bieder, 2006) ou encore d'épidémiologique (Hollnagel, 2004). Ils partent des principes proposés par les perspectives précédentes mais reconnaissent en outre le fait que l'organisation puisse récupérer ses propres erreurs tout comme le fait qu'elle évolue dans un environnement complexe évoluant sans cesse. Ainsi des approches systémiques ou inter-organisationnelle (Fahlbruch and Wilpert, 2001; Hollnagel, 2006; Wilpert and Fahlbruch, 1998), proposent de nouvelles façons d'appréhender la sécurité. Ces approches tentent de dépasser les frontières structurelles de l'organisation en la modélisant sous la forme d'un système complexe ouvert, imbriqué dans un environnement en constante évolution qui exerce des contraintes sur elle : contraintes politiques, économiques, sociales, concurrence, pression de l'autorité de tutelle, etc.

Ces contraintes peuvent être prévues, lentes, durables mais peuvent également constituer un choc soudain ou une agression surprise pour l'organisation sans que celle-ci n'ait vraiment les moyens de les contrôler ou de les contourner. Les agressions que l'organisation subit peuvent également provenir de son propre environnement interne : pression des salariés, mouvements de grève, jeux stratégiques des acteurs, etc.
Alors que dans la perspective organisationnelle précédente, l'accent était mis sur la maîtrise de l'environnement organisationnel de travail de l'opérateur, l'enjeu est davantage ici celui de construire, entretenir, maintenir la capacité de l'organisation à faire face ou à anticiper toutes les évolutions et agressions potentielles de son environnement (interne et externe) afin qu'elle soit capable de continuer à fonctionner. L'approche se focalise ainsi sur les conditions de dégradation de la sécurité de l'organisation et sur les mécanismes d'adaptation, de résilience de l'organisation face aux chocs provenant de son environnement.

Ces approches restent cependant très exploratoires. Leur instrumentalisation, ainsi que les techniques de management auxquelles elles renvoient, nécessitent d'être développées (Bieder, 2006; Groeneweg, et al., 2007).

3. Les modèles conceptuels de l'accident

Au cours de la partie précédente, nous avons abordé les différents courants interdisciplinaires qui ont accompagné l'évolution historique de la perspective d'approche de l'accident. L'historique de la conception et du développement des modèles d'accidents ainsi que les diverses démarches d'approches de la vérité de l'accident ont été discutés par de très nombreux chercheurs du champ des « Safety Sciences ». De nombreux chercheurs se sont en effet emparés de la question comme les sciences de l'ingénieur, l'ergonomie, la psychologie, la sociologie, l'informatique… (Ferry, 1988; Hollnagel and Woods, 2005; Leveson and Dulac, 2005; Perrow, 1984; Reason, 1995; Skelt, 2002). Ils ont fourni une vue d'ensemble des principaux modèles d'accidents depuis les années 1950 qui reflète clairement l'évolution des différentes compréhensions de la nature de l'accident.

Dans cette partie, nous allons tout d'abord recenser les représentations recueillies dans la revue de littérature pour ensuite évoquer les limites de ces prototypes à travers les démarches d'approche de la vérité inatteignable de l'accident. Une démarche triviale pour tenter d'approcher cette vérité de l'accident débute par le fait d'accorder un intérêt particulier aux causes qui ont contribué à l'avènement de ce phénomène. Nous présentons dans cette section un état de l'art des modèles conceptuels de l'accident.

3.1 Le modèle conceptuel du Domino

Le *modèle Domino* de Heinrich, publié en 1931 (Heinrich, 1941), est aussi connu sous le nom de *modèle d'évènement séquentiel*. Ce modèle suppose que la cause de l'accident résulte de l'occurrence d'évènements discrets dans une série ordonnée. Selon Heinrich, cinq facteurs entrent en jeu dans la séquence d'accident. Il compare donc la séquence générale à cinq dominos debout : 1) l'environnement social (les situations qui se présentent pour une personne et qui la conduit par suite à prendre ou à accepter des risques); 2) la faute de la personne; 3) les actes ou les conditions dangereuses (mauvaise planification, équipement dangereux, environnement dangereux); 4) l'accident; 5) les pertes, dégâts et blessures.

Lorsque le premier domino tombe, il frappe automatiquement l'évènement directement connexe et ainsi de suite jusqu'à ce que le préjudice se produise.

En cas d'accident, cette séquence générale explique que l'environnement social déclenche l'effet domino qui influence directement le comportement d'une personne. Le comportement maladroit d'une personne provoque directement des conditions dangereuses qui sous l'effet de certaines conditions entrainent un accident et des pertes. (Figure 1-2). Ces modèles ont très fortement mis l'accent sur la fiabilité humaine et plus particulièrement sur l'erreur humaine (Leveson, 2011). En effet, les accidents ont commencé à être considérés comme étant la faute d'un individu, plutôt que d'un événement qui aurait pu être évité par une modification de l'usine, du procédé ou du produit final.

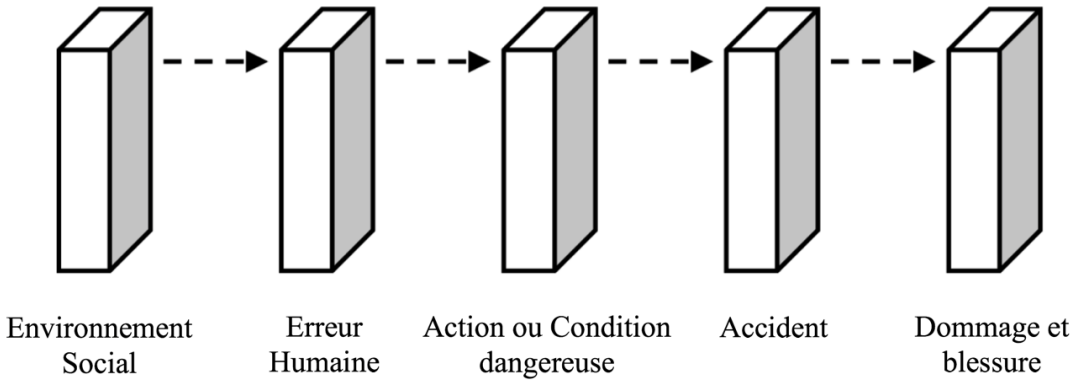


Figure 1-2 L'accident un événement dans une chaîne séquentiel ordonnée

3.1.1 Les modèles conceptuels construits sur les base du modèle Domino

La théorie du Domino appartient à la classe des modèles d'accident orienté « événement ». Ces modèles sous-tendent la plupart des modèles qui traitent les causes fondamentales, causes immédiates, causes latentes et systémiques de Reason, ainsi que les outils d'analyse des risques (Larouzée et Guarnieri, 2014).

En 1976, (Bird and Loftus, 1976) étendent la base du modèle Domino pour y inclure la prise de décision du gestionnaire comme facteur influant dans la chaîne des

évènements de défaillance. Le manque de contrôle est considéré comme initiateur des causes principales de la dégradation des facteurs gestionnaires et du comportement des employés). Cela crée un environnement propice de non-respect des pratiques/règles/conditions, et de la négligence des erreurs et des défaillances, ce qui provoque des causes immédiates qui entrainent de fait un accident ou un incident.

La même année, Adams cité par Leveson (2011) propose un autre modèle qui inclut :

- Une structure de gestion comprenant les objectifs, l'organisation, et les opérations, qui peuvent engendrer des erreurs opérationnelles généralement liées au comportement du contrôleur ou à des erreurs tactiques provoquées par un employé insatisfait par les conditions de travail. Ces erreurs provoquent l'accident ou l'incident et entrainent des dommages aux biens et aux personnes.
- L'occurrence de l'accident est détectée dans une chaîne où les événements défaillants sont directement liés les uns aux autres. Ainsi, afin d'expliquer l'accident, il suffit d'évaluer les risques en regardant la chaîne des événements défaillants qui ont conduit à la perte. Les événements les plus courants considérés dans ces modèles sont les pannes de composants qui sont utilisés pour assurer la sûreté de fonctionnement.

L'emploi des techniques d'analyse pour prédire et réduire les risques et empêcher l'occurrence d'un accident permet d'identifier les séquences d'événements qui peuvent entraîner des risques ou des accidents. La probabilité d'une séquence d'évènements défaillants est estimée, les mesures de prévention sont axées sur l'intégrité, sur l'introduction des composants redondants afin d'anticiper les événements d'échec et afin de réduire la probabilité de survenue de l'accident (ATEA, 1998; Leveson, 1986). Cette approche de l'accident est adaptée à l'étude des pertes causées par des défaillances de composants physiques ou par les erreurs humaines pour des systèmes relativement simples. Les modèles d'analyse et de prévention des risques qui sous-tendent le modèle Domino et visent à proposer les démarches de prévention d'un accident, d'un incident, d'une défaillance ou d'une panne sont les suivants : Failure

Mode and Effect Analysis (FMEA), Fault Tree Analysis (FTA), analyse Cause-Conséquence (Courtois et Leveson, 1996).

3.1.2 Chaîne d'événements multilinéaires

Afin de dépasser la principale limite du modèle Domino qui ne considérait qu'une seule chaîne d'événements, un modèle dit « séquentiel » a été élaboré afin de représenter, par plusieurs séquences d'événements et sous la forme de hiérarchies (des arborescences d'événements et des réseaux), une situation accidentelle. Une description détaillée de ces modèles a été entreprise par Bird and Loftus (1976) (Courtois et Leveson, 1996).

Les événements considérés dans ce type de modèles correspondent généralement et classiquement à la défaillance d'un composant ou d'une erreur humaine. Une chronologie est incluse afin d'illustrer l'enchaînement de distribution des événements et des conditions de l'accident (Figure1-3). Plusieurs chaînes d'événements, correspondant à différents acteurs, sont synchronisées à l'aide d'un scénario.

L'accident débute lorsqu'une situation stable est perturbée. Si l'acteur impliqué dans la séquence s'adapte à la perturbation, l'accident est évité. Les contre-mesures peuvent être formulées par l'examen de chaque événement pour identifier les modifications qui peuvent être introduites au processus. Les événements ont une relation linéaire.

Ces modèles décrivent donc une causalité linéaire, et il est dès lors difficile d'incorporer des relations non linéaires. Le premier événement de la chaîne est souvent considéré comme l'événement déclenchant, sa sélection reste arbitraire. De plus, des événements précédents et des conditions peuvent toujours être ajoutés (Leveson, 2001). Enfin, le dernier évènement, avant l'accident, peut être considéré comme étant la cause sans que cela ne soit réellement le cas.

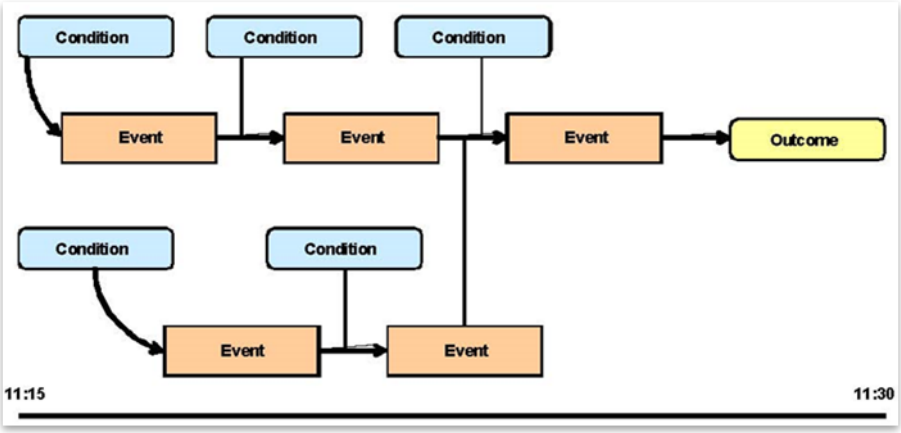


Figure 1-3 Modèle conceptuel évènementiel, séquentiel et conditionnel (Qureshi, 2007)

3.2 Les modèles conceptuels sociotechniques

Dans les systèmes complexes modernes, l'homme se trouve dans un environnement où il va manipuler des machines et des technologies compliquées. Les résultats de ces interactions homme/machine ne peuvent pas être appréhendés d'une façon analytique. En effet, on ne peut pas comprendre le résultat de ces interactions si l'homme ou la technologie sont étudiés chacun isolément de leur contexte. Les systèmes composés d'agents humains et d'artefacts techniques sont souvent ancrés dans des structures sociales complexes telles que les objectifs de l'organisation, ses stratégies, la culture d'entreprise, sa situation économique, juridique, politique et environnementale.

La théorie sociotechnique implique donc que les agents humains et les institutions sociales fassent partie intégrante des systèmes techniques, et que la réalisation des objectifs de l'organisation ne soient pas atteints par le système d'optimisation de la technique, mais par l'articulation des aspects techniques et sociaux (Trist, 1951). Ainsi, l'étude des systèmes complexes modernes nécessite une compréhension des interactions et des interrelations entre les aspects techniques, humains, sociaux et organisationnels du système.

Charles Perrow (Perrow, 1984) à travers sa théorie de l'accident normal fournit une approche de l'accident dans les industries complexes (nucléaire, pétrochimie, aviation, navires, espace, armes nucléaires). Il analyse plusieurs problèmes d'accidents

impliquant des systèmes complexes comme l'accident nucléaire de Three Miles Island en 1979. Il considère que la complexité des interactions et le couplage fort de ces systèmes complexes font irrémédiablement migrer le système technique et les organisations vers l'accident.

Un système complexe est constitué de plusieurs composants en interaction. Ces interactions peuvent être linéaires ou compliquées. Les interactions non-linéaires correspondent aux séquences étranges, imprévues, inattendues, invisibles, incompréhensibles au départ. Selon Perrow (1984) deux ou plusieurs évènements discrets peuvent interagir sous cette forme difficile à prédire par les concepteurs et difficile à maitriser par les opérateurs.

3.2.1 Le modèle conceptuel de Reason

Les travaux consacrés à la gestion du risque ont montré que les accidents survenus dans les milieux industriels complexes (par exemple les catastrophes de Fukushima ou de Bhopal) ne résultent jamais des seules erreurs humaines mais de l'imbrication en chaîne de nombreuses causes ou des facteurs favorisants. Ces causes, appelées systémiques ou latentes, sont plus difficilement identifiables que les erreurs humaines qui apparaissent comme les causes évidentes, immédiates des accidents (Larouzée et Guarnieri, 2015).

Ces causes systémiques ne créent pas d'accidents à elles seules mais sont délétères et synergiques lorsque surviennent une ou des erreurs humaines. Elles sont par ailleurs la raison principale des défaillances futures. Ces causes ne se révèlent que lors des enquêtes approfondies dites systémiques qui mettent le plus souvent en évidence la mauvaise organisation ou coordination du système plutôt que le manque de compétence des professionnels. Ces enquêtes approfondies sont un objet essentiel de la démarche de gestion des risques.

On comprend ainsi que la mauvaise organisation du travail, l'ambition excessive du rendement, un personnel mal formé ou en nombre insuffisant, des coordinations mal pensées, une gouvernance locale instable et peu présente, sont la source principale des

catastrophes observées, bien avant les questions de manque de compétences techniques de chaque acteur impliqué.

Les travaux de Reason (2013) ont mis l'accent sur l'aspect multifactoriel et la nécessité de promouvoir une analyse non culpabilisante afin de pouvoir apprendre de ses erreurs pour améliorer la sécurité. Apprendre d'une erreur nécessite un diagnostic approfondi et approprié des causes.

3.2.2 Intégration d'une chaîne évènementielle dans le modèle de Reason

Les modèles conceptuels basés sur les chaînes d'évènements à l'origine sont utilisés pour décrire la propagation des défauts dans les systèmes techniques. Le modèle conceptuel du fromage suisse de Reason est destiné à décrire les facteurs organisationnels et les relations de causalité avant les erreurs de l'opérateur conduisant à un accident (Reason et Hollnagel, 2006).

Dans les systèmes sociotechniques, ordinateurs et artefacts techniques sont de plus en plus étroitement intégrés avec les activités humaines. Reason considère que les défaillances dans les systèmes sociotechniques sont le résultat des multiples facteurs engrenés dans une causalité complexe reparties sur le réseau hiérarchique des différents niveaux organisationnels.

Besnard et Baxter (2003) considèrent qu'il faut qu'il y ait simultanément des défaillances techniques et organisationnelles pour s'emparer du maillage de cette causalité conduisant à l'accident. Ils proposent d'intégrer alors les modèles conceptuels des chaînes d'évènements avec le modèle de Reason afin de trouver le maillage de causalité qui entraine l'accident et effectuent les approches suivantes pour soutenir leurs propositions.

Un système peut être représenté selon plusieurs niveaux. Chaque niveau contient un sous-système susceptible d'affecter le fonctionnement de l'ensemble général du système. Les défaillances sont influencées par les conditions instables qui sont généralement présentes sans avoir d'effet immédiat. Une défaillance de ce point de vue

est donc la confrontation d'une combinaison improbable d'un certain nombre de facteurs contributifs (erreurs latentes *conditions instables). Dans de tels systèmes, Besnard et Baxter (2003) considèrent que les événements se propagent. Les accidents ne sont donc pas causés par la survenue des circonstances défavorables soudaines. Ils sont générés par des défauts initiaux qui, sous certaines conditions, déclenchent un événement indésirable. L'effet d'escalade des évènements se manifeste à travers des défaillances latentes reparties sur le système complet.

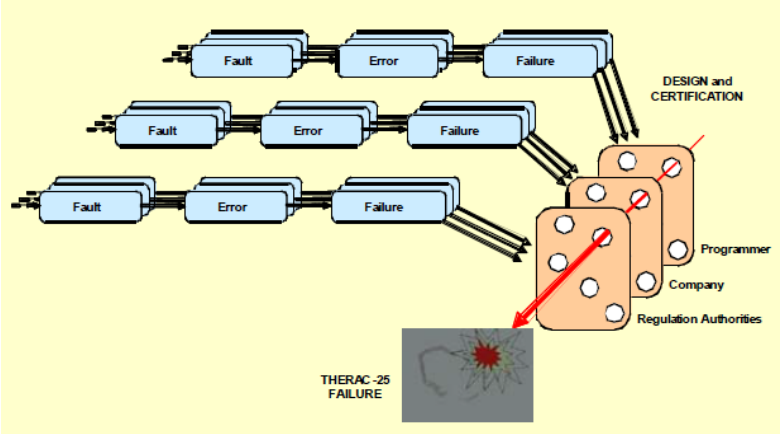


Figure 1-4 Intégration d'une chaîne séquentielle dans le modèle conceptuel de Reason (Qureshi, 2007)

Dans les années 1980, une nouvelle forme de modèles d'accident est apparue, qualifiée « d'épidémiologique ». Elle a pour ambition d'expliquer la cause des accidents au sein de systèmes dits « complexes ». Le modèle « épidémiologique » prend en compte les événements conduisant à des accidents analogues à la propagation d'une maladie, c'est-à-dire, comme le résultat d'une combinaison de facteurs, qui coexistent dans le temps et dans l'espace (Perneger, 2005). Le modèle de fromage suisse de Reason (2016, 1990) est la référence en la matière car il met en évidence les relations entre causes latentes et causes immédiates.

4. Les limites des modèles conceptuels de l'accident

Les modèles conceptuels d'accident peuvent être classés en trois catégories: (a) modèles séquentiels (ou des modèles traditionnelles linéaires simples), (b) les modèles

épidémiologiques (ou des modèles de systèmes linéaires complexes), et (c) des modèles systémiques (Hollnagel, 2004, 2006).

Les modèles séquentiels sont les plus simples, et sont souvent conformes à notre compréhension naturelle des accidents. Ces modèles mettent l'accent sur la prévention des accidents dans les systèmes relativement simples, par exemple, pour un opérateur travaillant avec une machine.

Les modèles épidémiologiques peuvent être considérés comme une réponse à la demande pour les modèles d'accidents plus puissants et plus complexes. Ils sont plus complets et mieux adaptés pour l'analyse de systèmes complexes. Une caractéristique importante des modèles épidémiologiques est la notion de conditions latentes, qui rappelle aux enquêteurs d'analyser plus en profondeur les facteurs organisationnels afin de prévenir de futurs accidents.

Les modèles systémiques décrivent la prestation caractéristique au niveau du système, plutôt qu'au niveau des mécanismes de cause à effet spécifiques ou des facteurs épidémiologiques mêmes. Une caractéristique notable des modèles systémiques est l'analyse de la portée des accidents aux organismes de réglementation et le niveau de gouvernement même de la morale et des normes sociales.

La plupart des modèles qui précèdent sont construits à partir d'un environnement de gestion réactive à la sécurité, donc à des fins de compréhension de la vérité derrière l'accident. Ils sont également utilisés dans des principes de gestion proactive et prédictive de la sécurité et donc à des fins de prévention et d'anticipation des accidents.

Selon les principes de gestion de la sécurité (réactive, proactive, prédictive), ces modèles sont transposés et utilisés dans toutes les époques respectives de la tendance d'explication des origines de défaillances derrière la vérité de l'accident : technique, humaine, organisationnelle et inter-organisationnelle (Hollnagel, 2014).

Les concepteurs des systèmes de sécurité et les investigateurs d'accidents sont induits en erreur à travers l'emploi de ces démarches. En effet, les notions formelles et informelles, pour représenter la chaîne des événements, ont des limitations importantes dont principalement la subjectivité dans le choix des événements à inclure dans l'identification de chaînage des conditions et dans l'exclusion des facteurs systémiques.

Ces démarches relèvent d'une analyse empirique, analytique et cartésienne pour approcher la vérité de l'accident ou pour l'anticiper. Elles, sont fondées sur des principes de linéarité et se résument à une simple relation de cause à effet. Pour éviter l'accident, ces modèles admettent qu'il suffit de briser le lien entre l'accident et l'évènement qui le précède directement dans la chaîne.

Cela suppose qu'une seule cause directe entraine l'accident, et si cette cause unique peut être identifiée et éliminée, l'accident ne sera pas répété. La réalité est que les accidents ont toujours plus d'un facteur intervenant. Les accidents sont des processus complexes impliquant l'ensemble du système sociotechnique. Les modèles ne peuvent pas décrire ce processus adéquatement puisqu'ils ne dévoilent pas la représentation de la complexité réelle et la confrontation des interactions qui peuvent entrainer l'accident. Nous allons résumer les limites de ces modèles évoqués.

4.1 Limite des modèles traditionnels

Les modèles qui représentent une chaîne d'évènements impliquent une relation de cause à effet entre deux évènements consécutifs dans la chaîne. Ces relations de liens sont donc considérées comme directes et linéaires. Un évènement a lieu si l'évènement direct qui le précède a eu lieu et si les conditions de liaison sont présentes pour le déclencher. Ainsi, les modèles de chaînes d'événement favorisent la causalité linéaire, et il leur est difficile, voire impossible d'incorporer des relations non linéaires. Les facteurs de causalités identifiés en utilisant le modèle de chaîne d'événements dépendent de la sélection des conditions qui font le lien entre les événements ; cependant, le choix des événements à inclure ainsi que les conditions restent subjectives (Leveson, 2011). Chacune de ces deux limites est considérée à son tour dans ce qui suit.

4.1.1 Subjectivité dans la sélection des évènements

La sélection des événements à inclure dans une chaîne dépend de la règle d'arrêt déterminée, de la séquence explicative ou du raisonnement d'interprétation de l'approche de la vérité de l'accident. Bien que le premier événement dans la chaîne soit souvent appelé la cause initiatrice d'événement, la sélection de cette dernière reste arbitraire. Parfois l'événement déclencheur est sélectionné car il représente un type d'événement qui est familier, acceptable comme motif ou parce qu'il s'avère représenter un écart par rapport à une norme. Dans d'autres cas, l'événement initiateur est choisi parce qu'il est le premier événement pour lequel on estime qu'une intervention pourrait empêcher l'accident. Le chaînage peut également s'arrêter parce que le chemin causal disparaît en raison du manque d'information.

Pour Rasmussen (1997) la difficulté principale réside dans la poursuite de la recherche inverse « à travers » un être humain, c'est-à-dire si la cause des évènements est étrange aux opérateurs ou s'ils ne sont pas impliqués directement. D'autres événements ou explications peuvent être exclus ou non examinés de manière approfondie, car ils soulèvent des questions qui sont embarrassantes pour l'organisation ou pour ses entrepreneurs ou qu'elles sont politiquement inacceptables. L'évènement qui précède directement l'accident est considéré généralement comme la cause primordiale. Toutefois, ce principe dans la sélection de l'évènement peut révéler une approche non fondée et induit souvent les enquêteurs des accidents en erreur.

A titre d'exemple, le cas du « Friendly fire » qui a abattu deux hélicoptères Black Hawk en Iraq (AAIB, 1994) : le tir de missiles par les pilotes du F-15 a été identifié comme la cause « primordiale », et par la suite les pilotes ont été considérés responsables de l'accident. Toutefois, le rapport d'accident a démontré qu'il y avait un grand nombre de facteurs et des événements qui ont contribué à l'accident.

L'une des raisons de cette tendance à rechercher une cause unique réside dans la volonté d'attribuer à l'accident un responsable physique humain et par la suite le blâmer, ceci souvent à des fins juridiques. Occasionnellement, un enquêteur d'accident

va s'arrêter à un événement particulier ou sur une condition qui lui est familière et certainement l'utiliser comme une explication acceptable de l'accident.

On remarque dans ces modèles des notations formelles et informelles pour la représentation de la chaîne d'événements. En effet, d'une part les chaînes peuvent contenir uniquement des événements et d'autre part, les chaînes peuvent contenir des conditions qui ont conduit aux événements. La différence entre les événements et les conditions réside dans le fait que les événements sont limités dans le temps, alors que les conditions persistent et changent quand un événement se produit. Généralement, dans ces modèles, il n'y a pas de critère objectif pour distinguer un facteur ou plusieurs facteurs des autres facteurs qui composent la cause de l'accident (Leveson, 2001).

4.1.2 Subjectivité dans la sélection des conditions

En plus de la subjectivité dans la sélection des événements, des événements initiateurs, des conditions ou des liens directs qui peuvent entrainer la succession des événements sont choisis de manière très subjective. Leveson (2011) fait remarquer que les liens sont justifiés par les connaissances ou les règles de différents types (physiques et organisationnelles).

Le même événement peut ainsi donner lieu à différents types de liens selon les représentations mentales que l'analyste a de la réalisation de cet événement. Lorsque plusieurs types de règles sont possibles, l'analyste appliquera celles qui lui semblent proches de son modèle mental au regard de la situation en jeu.

L'approche de la vérité de l'accident peut paraitre inatteignable du fait de la subjectivité de la sélection des événements, des conditions et des liens d'influence. On n'obtiendra pas toujours une vérité absolue mais par contre des vérités plausibles dont chacune pourra servir comme une explication de la séquence d'événements qui conduit à l'accident.

Ainsi, la compréhension de l'accident et l'apprentissage pour prévenir de nouveaux accidents exigent l'identification de tous ces facteurs pour expliquer l'entrée

incorrecte et les subjectivités qui induisent en erreur. Pour cela il convient d'adopter un modèle d'accident qui utilise et guide une analyse complète à plusieurs niveaux du système technique et social. Nous allons expliquer dans ce qui suit la démarche de cette approche.

4.1.3 Recherche des facteurs de cause de l'accident

Les limites des modèles de chaînes d'événements ne se résument pas simplement au niveau de la sélection des événements mais aussi dans l'étiquetage de certaines causes et conditions arbitraires et incomplètes considérées comme principales et nécessaires à inclure dans la chaîne. Les chaînes d'événements développées pour expliquer un accident se concentrent habituellement sur les événements précédant immédiatement la perte. Mais les facteurs accidentogènes sont souvent présents des années à l'avance (Leveson, 2011). Un événement déclenche simplement la perte, mais si cet événement n'est pas advenu, un autre événement lié indirectement peut conduire à une perte.

Bon nombre des facteurs de causalité systémiques ne sont qu'indirectement liés aux conditions précédant la perte et les événements. La catastrophe de Bhopal fournit un bon exemple. En général, les modèles basés sur des événements ne représentent pas les facteurs systémiques de l'accident comme : les déficiences structurelles de l'organisation, la gestion de la prise de décision et la faible culture de la sécurité de l'entreprise ou d'une industrie. Un modèle d'accident devrait encourager une vue d'ensemble des mécanismes de l'accident qui élargit l'enquête au-delà des événements immédiats : une focalisation sur des composants technologiques et des activités d'ingénierie pure ou une focalisation étroite similaire sur les erreurs d'opérateurs peut conduire à négliger certains facteurs plus importants en termes de prévention des accidents.

Le modèle de l'accident pour expliquer pourquoi l'accident s'est produit ne devrait pas seulement encourager l'inclusion de tous les facteurs de causalité, mais devrait également fournir des indications pour identifier ces facteurs.

4.2 Les répercussions des limites des modèles conceptuels traditionnels dans les systèmes industriels complexes

Les approches analytiques, que l'on retrouve dans les prototypes classiques de représentation d'un accident, sont fondées sur des principes de linéarité. Cet aspect de linéarité ne semble pas être approprié pour comprendre ou anticiper la nature imprévisible des interactions présentes au sein d'un environnement industriel, surtout en présence de la combinaison des facteurs techniques, humains, organisationnels et inter-organisationnels.

En effet, cette démarche se concentre plutôt sur la nature des interactions simples sans pour autant se soucier des conséquences des interactions complexes qui peuvent entrainer ou éviter un accident. Elle est considérée comme séquentielle et ne tient pas compte de la représentation de la complexité de la réalité ainsi que des interactions qui peuvent entrainer l'accident. Les modèles séquentiels peuvent induire en erreur du fait qu'ils reposent sur l'amélioration de la fiabilité pour rendre un système sûr et empêcher l'accident ou sur l'amélioration de la sûreté en rendant plus fiable les barrières qui provoquent l'évènement indésirable.

La confusion sur ce point est illustrée par l'accent mis sur les événements d'échec dans la plupart des accidents et l'analyse des incidents. Certains chercheurs qui s'intéressent aux approches organisationnelles de la sécurité, font également cette erreur en laissant entendre que les organisations de haute fiabilité (HRO) seront en sécurité (Roberts, 2009).

En effet, il faut bien intégrer l'idée que la fiabilité et la sûreté sont deux concepts différents, et par la suite on peut rencontrer des systèmes fiables mais pas sûrs et des systèmes sûrs mais dangereux ou non fiables. Puisque cette hypothèse sur l'équivalence entre la sécurité, la sûreté et la fiabilité est si largement répandue, la distinction entre ces deux propriétés doit être soigneusement considérée. Leveson (2011) considère qu'il existe des systèmes fiables mais dangereux et des systèmes dangereux mais fiables.

4.2.1 Des composants fiables mais des interactions entre composants sont dangereuses

Dans un système complexe, chaque composant d'un système considéré analytiquement peut fonctionner individuellement jusqu'à atteindre sa propre finalité. Néanmoins, les interactions entre les composants d'un système complexe peuvent provoquer un accident. En effet, la cause d'un tel accident réside dans les interactions dysfonctionnelles entre les composants fiables du système. Pour illustrer cela, Leveson prend l'exemple de l'accident de Mars Polar Land la navette spatiale de la Nasa lancée le 3 janvier 1999 pour l'étude de sol de Mars. La description de l'accident indique que la cause directe de l'accident remonte à la « présence des signaux parasites générés lors du déploiement des pieds de la sonde » (Knight, 2002).

Selon Leveson (2011), les défaillances des composants et les pannes sont généralement traités comme des phénomènes aléatoires. Il est donc impossible de prédire les éventuelles interactions entre les composants et de les anticiper. Cependant l'absence de défaillance des comportements dangereux ne peut constituer un événement aléatoire.

Dans les accidents liés à l'interaction des composants, il peut n'y avoir aucun échec et les erreurs de conception de système, donnant lieu à des comportements dangereux, ne sont pas des événements aléatoires. Ce bruit est normal et attendu et ne représente pas une défaillance dans le système de la sonde. Le logiciel embarqué a interprété ces signaux comme une indication que l'atterrissage avait eu lieu (les ingénieurs logiciels ont été informés de tels signaux) et a coupé les moteurs de descente prématurément, conduisant le vaisseau à s'écraser sur la surface de Mars. L'accident s'est donc produit parce que les concepteurs du système n'ont pas tenu compte de toutes les interactions possibles entre le déploiement de la jambe d'atterrissage et le logiciel de commande du moteur de descente.

Un échec de conception peut ainsi induire une déviance même lorsque les composants satisfont les exigences spécifiées (comme éteindre les moteurs de descente quand un signal est reçu), même si les exigences peuvent inclure un comportement qui

n'est pas souhaitable dans un contexte de système plus vaste, cette composante n'a pas manqué.

4.2.2 Dangereux mais fiables

La présence de composants fiables n'est pas nécessairement une condition suffisante pour procurer la sécurité d'un système. Même, si le système dans son ensemble de fonctionnement est fiable, on ne peut confirmer qu'il n'est pas dangereux.

Pour comprendre les caractéristiques de la fiabilité et de la sécurité, il faut faire une distinction entre les exigences et les contraintes. Les exigences sont dérivées de la représentation ou la raison d'existence même de l'organisation. La mission de l'usine chimique est de produire des produits chimiques. Les contraintes représentent les façons acceptables que le système ou l'organisation se donne pour atteindre les objectifs de la mission : ne pas exposer les passants à des polluants et ne pas polluer l'environnement sont des contraintes sur la façon dont la mission (production de substances chimiques) doit être conduite.

Alors que dans certains systèmes industriels, la sécurité fait partie de la mission ou de la raison d'être du système, comme le contrôle du trafic aérien ou les soins de santé, dans d'autres, la sécurité n'est pas la mission mais est au contraire une contrainte sur la mission elle-même. Non seulement les contraintes de sécurité entrent parfois en conflit avec les objectifs de la mission, mais les exigences de sécurité peuvent même entrer en conflit entre eux (Leveson, 2011). Une seule contrainte de sécurité sur un système de porte de train automatisé, par exemple, est que les portes ne peuvent s'ouvrir à moins que le train ne soit arrêté. Une autre contrainte de sécurité est que les portes doivent s'ouvrir n'importe où pour l'évacuation d'urgence des usagers.

La résolution de ces conflits est une des étapes importantes en sécurité et en ingénierie des systèmes. Il existe toujours plusieurs objectifs et contraintes pour n'importe quel système. Le défi consiste donc à identifier et analyser les conflits, à faire les compromis appropriés entre des exigences contradictoires et des contraintes puis de

trouver des moyens d'accroître la sécurité de l'installation sans compromettre la fiabilité du système.

4.3 Les limites des greffes des facteurs systémiques sur les modèles conceptuels

Les systèmes à grande échelle représentent une collection d'artefacts technologiques mais ils reflètent aussi le travail de conception d'ingénierie, la structure de gestion, les procédures et relèvent de la culture de l'organisation. Généralement, ils sont aussi le reflet de la société dans laquelle ils ont été créés. (Miles, 1973) en décrivant les concepts de base de la théorie des systèmes, note que : « La présence au moins d'une science fondamentale, sous-jacente à chaque technologie, même si cette dernière est souvent bien développée, avant que la science n'ait émergé. Le recouvrement de tous les systèmes techniques ou civils est un système social qui fournit l'objet, objectifs et critères de décision. Prévenir efficacement les accidents, dans les systèmes complexes, exige l'utilisation de modèles d'accident qui inclue ce système social ainsi que la technologie et la science sous-jacente. Sans comprendre le but, les objectifs et les critères de décision qui permettant de construire et d'exploiter des systèmes, il n'est pas possible de bien comprendre et de mieux prévenir les accidents » [3].

La prise de conscience de l'importance des aspects sociaux et organisationnels de la sécurité date des années 60. Lederer (1986) alors directeur de la NASA chargé du programme de sécurité aérienne pour le programme Apollo, a écrit : « la sécurité des systèmes couvre le spectre total de la gestion des risques. Il dépasse le matériel et les procédures connexes de l'ingénierie du système. Il s'agit des : attitudes et motivation des créateurs et producteurs, rapport employé/gestion, la relation des associations industrielles entre elles et avec le gouvernement, le facteur humain dans la supervision et le contrôle qualité, la documentation sur les interfaces de sécurité publique et industrielle avec le design et les opérations, l'intérêt et les attitudes des cadres supérieurs, les effets du système juridique sur les enquêtes d'accidents et les échanges d'informations, la certification des travailleurs critiques, des considérations politiques,

[3] Underlying every technology is at least one basic science, although the technology may be well developed long before the science emerges. Overlying every technical or civil system is a social system that provides purpose, goals, and decision criteria

ressources, sentiment public et beaucoup d'autres techniques qui représentent des influences vitales sur la réalisation d'un niveau acceptable de maîtrise des risques. Ces aspects non techniques de sécurité de l'installation ne peuvent pas être ignorés. [4]»

Trop souvent, cependant, ces aspects non-techniques sont ignorés. Au moins trois types de facteurs doivent être considérés dans la causalité de l'accident. Le premier est la chaîne d'événements immédiats, le second est le type des informations qui recouvre les conditions qui ont contribué à l'occurrence de la chaîne des événements. Et enfin, le troisième concerne l'ensemble des facteurs de causalité qui ne sont qu'indirectement liés aux événements et aux conditions. Ces facteurs indirects sont essentiels pour bien comprendre pourquoi l'accident s'est produit et donc comment faire pour prévenir la survenance de nouveaux accidents.

Plusieurs tentatives ont été faites pour greffer des facteurs systémiques sur les modèles d'événements, mais toutes ont des limitations importantes. L'approche la plus courante consiste à ajouter des niveaux hiérarchiques au-dessus de la chaîne d'événements. Dans les années soixante-dix, Johnson propose une approche et une méthode de séquençage qui décrit l'accident comme des chaînes d'événements directs. Les facteurs de causalité des évènements sont déterminés à partir des facteurs contributifs, qui découlent eux-mêmes de facteurs systémiques (Figure 1-5).

[4] System safety covers the total spectrum of risk management. It goes beyond the hardware and associated procedures of system safety engineering. It involves: attitudes and motivation of designers and production people, employee/management rapport, the relation of industrial associations among themselves and with government, human factors in supervision and quality control, documentation on the interfaces of industrial and public safety with design and operations, the interest and attitudes of top management, the effects of the legal system on accident investigations and exchange of information, the certification of critical workers, political considerations, resources, public sentiment and many other non-technical but vital influences on the attainment of an acceptable level of risk control. These non-technical aspects of system safety cannot be ignored.
.

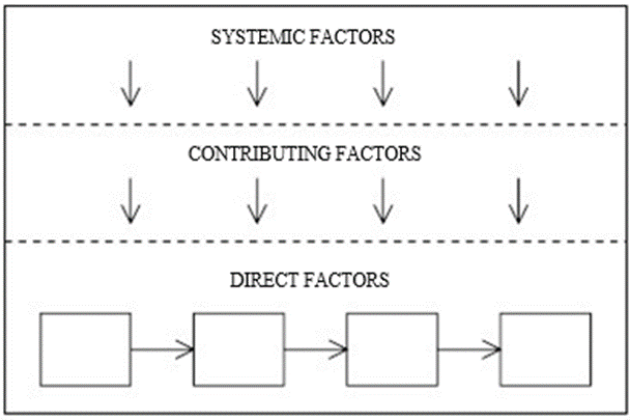


Figure 1-5 Types de facteurs systémiques (Leveson, 2011)

Johnson (1980) a également tenté de mettre les facteurs de gestion dans les arbres de défaillances (une technique appelée la MORT (Management Oversight and Risk Tree), ou arborescence de gestion et de contrôle du risque), mais a fini par simplement fournir une liste de vérifications générales pour l'audit des pratiques de gestion de la sécurité. Alors qu'une telle liste peut être très utile, elle suppose que toutes les erreurs peuvent être prédéfinies et être recensées dans un formulaire de liste de contrôles (check-list). La liste de contrôles est composée d'un ensemble de questions qui doivent être posées au cours d'une enquête sur les accidents.

La greffe systémique la plus sophistiquée aux chaînes d'événements est le modèle conçu par Rasmussen et Svedung (2000) et concerne la hiérarchie du système sociotechnique impliqué dans la gestion des risques. Ce système comprend une structure de contrôle hiérarchique, plusieurs niveaux concernant les législateurs, les niveaux d'organisation et les modes de fonctionnement des systèmes de gestion, les opérateurs du système. À tous les niveaux, des flux d'informations sont caractérisés. La Figure 1-6 montre un exemple représentatif, bien que l'organigramme d'une organisation puisse varier d'une industrie à l'autre.

Le niveau L1 décrit les activités du gouvernement, qui légifère en termes de sécurité. Le niveau L2 décrit les activités des autorités de réglementation, les associations professionnelles et les syndicats (mais aussi les services de médecine et de santé, les ingénieurs conseils…) qui sont en charge de l'application de la loi dans leurs secteurs respectifs. Le niveau L3 décrit les activités d'une entreprise en particulier, et

mobilise des connaissances sur l'économie, le comportement organisationnel, les modes de décision, la sociologie des acteurs. Le niveau L4 décrit les activités de la gestion d'une entreprise en particulier la stratégie politique déployée pour contrôler la sécurité des établissements industriels, de gérer et de contrôler le travail de leur personnel. La connaissance des théories de gestion industrielle et de psychologie organisationnelle est utilisée pour comprendre ce niveau. Le niveau L5 décrit les activités des acteurs qui à titre individuel interagissent directement avec la technologie ou le processus contrôlés. Ce niveau nécessite des connaissances dans des disciplines telles que la psychologie, les interactions homme-machine et les facteurs humains. Le niveau L6 décrit l'application des disciplines d'ingénierie impliquées dans la conception de matériels et procédés potentiellement dangereux et les procédures de fonctionnement, de contrôle de ces derniers. Comprendre ce niveau nécessite la connaissance de la science et des diverses disciplines des sciences de l'ingénieur.

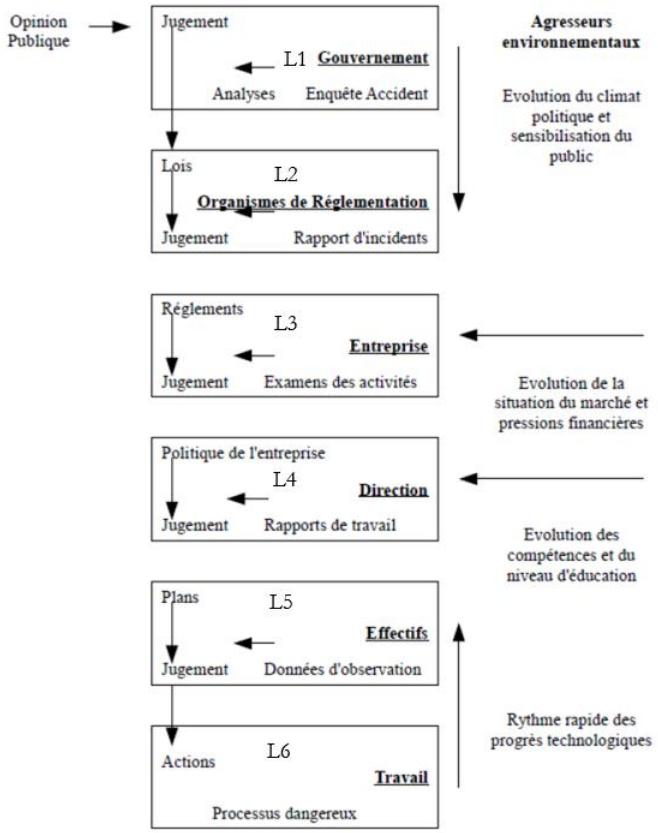


Figure 1-6 : Cadre de Rasmussen (Hardy, 2011a; Leveson, 2011)

5. Synthèse du chapitre

Dans ce chapitre, nous sommes brièvement revenus sur la notion d'accident et ce tour d'horizon historique nous a permis de dresser un état des modèles classiquement utilisés dans l'industrie pour caractériser la dangerosité d'un système sociotechnique. Ces modèles apportent de nombreux bénéfices mais présentent des limites intrinsèques à leurs propres fondements théoriques. Comme alternative, nous proposons d'étudier les apports d'un modèle systémique d'accidents appelé STAMP (System Theoretic Accident Model and Processes) (Leveson, 2011). Ce modèle est basé sur la théorie des systèmes et offre une vue plus exhaustive des causes des accidents et les interactions indirectes ou non-linéaires entre des événements. Selon STAMP, la sécurité est reformulée comme un problème de manque (ou d'absence) de contrôle d'un système plutôt que simplement un problème de fiabilité (ou de disponibilité). La défaillance de composants (et le manque de fiabilité des composants du système) sont toujours envisagés, mais plus généralement les accidents sont réputés survenir lorsque les pannes de composants, les perturbations extérieures, ou quand les interactions indésirables et dangereuses entre les composants du système ne sont pas adéquatement traitées, c'est-à-dire contrôlées, conduisant à un comportement du système non sécuritaire. Le comportement dangereux du système est défini en termes de comportement avec des contraintes de sécurité requises qui n'ont pas été respectées. Le chapitre 2 présente le modèle STAMP.

CHAPITRE 2: PRESENTATION DE STAMP

La sémantique qui accompagne les approches systémiques de l'analyse des systèmes, de la dynamique des systèmes, de la théorie des systèmes…, repose essentiellement sur la notion système. L'étude formelle des systèmes est apparue au XIXe siècle avec la naissance de l'industrie. En réponse aux limites et techniques classiques d'analyse face à des systèmes industriels de plus en plus complexes, le concept moderne de système a émergé dans la seconde moitié du XXe siècle en différents domaines scientifiques (Samadi, 2012a) . (Durand, 1979) nomme cinq pionniers célèbres :

- Ludwig von Bertanlanffy (1901-1972), le biologiste autrichien, avec le premier ouvrage sur la « Théorie générale des systèmes (Bertalanffy, 1969)»
- Norbert Wiener (1894-1964), mathématicien américain et professeur au MIT (Massachusetts Institute of Technology), qui a appliqué la théorie des systèmes au contrôle commande et aux communications (Leveson, 2011). Son célèbre livre sur la « Cybernétique », publié en 1948 (Wiener, 1961).
- Claude Elwood Shannon (1916-2001), mathématicien américain et ingénieur des télécommunications, qui a publié « Une théorie mathématique de communication » en 1948 (Shannon, 2001).
- Warren Sturgis McCulloch (1898-1969), neurophysiologiste américain, qui élargi ses recherches en mathématiques et en génie industriel.
- Jay Wright Forrester (1918-), ingénieur américain et professeur au MIT, qui développe l'application de la théorie des systèmes à la dynamique industrielle et créé la Dynamique des Systèmes.(Forrester, 1968).

Le développement moderne de la théorie des systèmes est introduit par deux publications : « Les limites à la croissance » (Meadows, 1972) et « Le macroscope », publié en France en 1975 (Rosnay, 1975, 2014).

1. Petite histoire de la systémique

Le point de départ se situe dans la série des dix séminaires organisés entre 1946 et 1953 à la Josiah Macy Foundation (Cambien, 2008). Sociologues, mathématiciens, biologistes ou encore anthropologues s'y côtoient, discutant cybernétique, complexité, système. Notons également que c'est au cours de cette seconde décennie que s'est développée la bionique et que le biologiste von Bertalanffy fonde la société pour l'étude des systèmes généraux (Society for General Systems Research.(ISSS.). Au milieu de ce bouillonnement d'idées se constituent les bases d'un langage commun qui deviendra celui de la systémique (Garbolino et al., 2010).

Les grands principes de la systémique se fondent sur des travaux interdisciplinaires. Le mathématicien Norbert Wiener, professeur au MIT, et le neurophysiologiste Arturo Rosenblueth, chercheur à la Harvard Medical School s'intéresse à l'étude des analogies pouvant exister entre le comportement des organismes vivants et celui des servomécanismes. Un servomécanisme est un engin dont la caractéristique fondamentale est l'existence en lui-même d'une rétroaction de l'information. On entend par rétroaction de l'information un processus en vertu duquel, lorsque l'on agit sur un système déterminé, on obtient en permanence de l'information sur les résultats des décisions prises (l'information rétroagit) (Arcil, 1998).

Cette expérience célèbre dans l'histoire de la systémique permet de mettre en évidence d'une part les phénomènes oscillatoires qui viennent perturber la stabilité d'un système donné. Et par analogie d'expliquer ces phénomènes par l'existence de boucles de rétroaction dans les systèmes physiologiques et techniques. C'est ainsi que les bases d'une nouvelle discipline, la cybernétique, sont posées. Les idées de Wiener et de Rosenblueth suscitent l'intérêt de chercheurs, surtout la recherche de similitudes entre disciplines et domaines aussi variées que l'économie, la sociologie, la psychiatrie ou encore l'anthropologie. Ce dialogue a lieu pour l'essentiel au sein du prestigieux Massachusetts Institute of Technology (MIT) à Boston. La circulation d'idées contribue au transfert de méthodes et de terminologies d'une discipline à l'autre. En trois bonds

d'environ dix ans chacun, les travaux réalisés au sein du MIT vont conduire du développement de la Cybernétique à celui de la dynamique des systèmes.

Dans les années 50, le perfectionnement des premiers ordinateurs va permettre d'aborder la complexité sous un angle neuf. L'un des plus rapides, le Whirlwind II fut construit au MIT en 1951 et utilise pour la première fois une mémoire magnétique ultra rapide à l'époque inventée par Jay Forrester (Forrester, 1995). À la tête du Lincoln laboratory, cet ingénieur est chargé par l'US Air force en 1952 de coordonner la mise au point d'un système d'alerte et de défense mettant en œuvre radars et ordinateurs dans le but de détecter et d'empêcher toute attaque ennemie sur le territoire américain. Cette expérience dans le domaine de la défense du territoire exacerbe la prise de conscience de Forrester concernant l'importance de l'approche systémique dans la compréhension et dans le contrôle d'organisations complexes faisant intervenir des hommes et des machines interconnectées en temps réel, c'est-à-dire capables de prendre des décisions vitales au fur et à mesure de l'arrivée des informations.

Cette connaissance acquise, Forrester va s'intéresser, au sein de la Sloan School of Management du MIT dans laquelle il enseigne à la fin des années 50, à l'organisation de l'entreprise conçue comme système complexe. En 1961, il crée la dynamique industrielle, discipline dont le but est de tenter de comprendre et de prévoir, par la simulation informatique, notamment, le comportement des entreprises appréhendées comme des systèmes cybernétiques. L'extension de ses travaux à l'objet ville puis au monde forme l'essentiel de ce qui fonde la dynamique des systèmes.

À partir des années 70, sont réunies un certain nombre de conditions culturelles, scientifiques et institutionnelles qui vont permettre, à partir des différentes approches développées au cours des trois décennies précédentes, de voir se constituer la science des systèmes ou pensée systémique.

Le passage de sciences développant des approches systémiques à la Systémique conçue comme épistémologie repose sur une « inter fécondation » des idées entre les différentes disciplines et sur le rôle déterminant d'un certain nombre de chercheurs

américains et français. Ces derniers sont en effet conscients de la nécessité d'une synthèse à un niveau théorique de l'ensemble des lois qui semblent fonder la science des systèmes. Parmi eux, H. Simon, H. von Foerster, J. Forrester, E. Morin, I. Prigogine, H. Atlan, J.L. Le Moigne.

Le premier à s'être attelé à cette tâche est le biologiste Ludwig Von Bertalanffy qui, en 1968, à New York, rassemble ses différents travaux dans un ouvrage de synthèse intitulé General System Theory (Bertalanffy, 1969), traduit en français sous le titre « La théorie générale des systèmes » (Chabrol, 1973). Dans cet ouvrage, qui fait la part belle aux systèmes biologiques, l'auteur définit un certain nombre de concepts tels que ceux de systèmes ouverts, d'homéostasie, d'équifinalité, etc. Von Bertalanffy prône une appréhension globale du système, insistant sur l'importance de la compréhension des relations entre les différents éléments, et non, comme préconisé par la pensée classique, une saisie analytique des éléments du système. Approximativement à la même époque, Herbert Simon (SIMON : 1974) et Kenneth Boulding (Boulding, 1956) contribuent eux aussi à théoriser les principes développés dans le cadre de leurs travaux.

La définition des concepts d'arborescence et de niveaux d'organisation constituent ainsi une première étape vers l'effort de construction d'une typologie des systèmes que Boulding (Boulding, 1956) propose selon huit niveaux. Du premier niveau correspondant aux objets statiques et simples de la physique et de la chimie jusqu'au dernier niveau de la socio-culture, le mouvement est celui d'une complexification croissante. La compréhension du système représenté par le huitième niveau suppose celle de tous les niveaux précédents. Dans les années 70, la tentative de généralisation de ses différents travaux par Jay Forrester, dont le rôle a été prépondérant, abouti à la constitution d'une nouvelle discipline, la dynamique des systèmes (Forrester, 1995).

Le caractère opérationnel de la dynamique des systèmes explique en grande partie le succès immédiat qu'elle connaît dans des domaines aussi variés que la biologie, l'environnement, la gestion, et l’industrie. Par la suite, la théorie du système général consiste désormais, après les travaux de Forrester, à aborder une problématique en la modélisant dans un environnement actif, et c’est ainsi que les chercheurs vont donner

une autre représentation des phénomènes, distingués en phénomènes décomposables, phénomènes quasi décomposables et phénomènes différenciables mais indécomposables sans mutilation (c.à.d. indissociables de leur environnement et irréductibles à un seul élément). Cette vision (Cambien, 2008) se démarque la théorie des systèmes par le fait de mettre clairement l'accent sur la place dynamique des acteurs dans le système et de considérer qu'il n'y a plus d'observateur extérieur, mais que l'observation est une action qui contribue à le modifier (modèles mentaux).

C'est ainsi que la dynamique des systèmes sous les travaux de modélisation de Jay Forrester, la différenciation de la systémique en deux courants est induite. D'un côté, la systémique de première génération, en filiation directe de la cybernétique, s'appuie sur des méthodes quantitatives et sur l'outil informatique pour, au-delà de la seule compréhension du système, tenter de prévoir son comportement. La systémique de seconde génération, appelée «System Thinking», s'inscrit dans une perspective un peu différente par rapport à la démarche prospectiviste de la systémique de première génération (Cambien, 2008).

L'approche « System Thinking» s'inscrit dans une perspective de conception, qui tend à mettre l'accent sur l'intelligibilité du comportement du système. Le but étant de concevoir des modèles qualitatifs, qui permettent d'entrer dans l'intelligence du phénomène et, éventuellement, d'en orienter l'action. La notion de rétroaction, découverte notamment au travers du croisement des travaux de Wiener et Rosenblueth (Rosenblueth et al., 1943) représente le mécanisme de base de la dynamique des systèmes de Jay Forrester. Les processus à l'origine de ce fonctionnement finalisé et adaptatif reposent sur l'articulation des boucles de rétroaction positives et des boucles de rétroaction négatives, sous la pression permanente de l'environnement extérieur. Tout système présente donc deux types fondamentaux d'existence et de fonctionnement, le maintien et le changement.

Dans le premier cas, ce sont les boucles négatives qui assurent la stabilité, alors que dans le second, c'est la domination des boucles positives qui entraînent le changement. La coexistence de ces deux dynamiques au sein de tout système permet au

système de sauvegarder sa survie. Au-delà de la finalité du simple maintien de l'équilibre initial, il existe donc au sein de tout système une finalité de la survie qui explique que, sous la pression de l'environnement, le système se modifie pour retrouver un équilibre. Dans un premier temps, les boucles positives prennent l'ascendant sur les boucles négatives pour déclencher et conduire une transformation du système, avant de laisser à nouveau les boucles négatives prendre le dessus et assurer le maintien d'un équilibre qui peut être tout à fait différent de la situation initiale.

Cette systémique de seconde génération a connu elle aussi un grand succès notamment au Mexique et, surtout, en France. Jean-Louis Le Moigne (Le Moigne, 1990), professeur à l'université d'Aix-Marseille a particulièrement contribué, par l'animation du groupe de modélisation de la complexité par exemple, au développement et aux applications de la pensée systémique. Il convient de citer, l'Association Française de Sciences des Systèmes Cybernétiques Cognitifs et Techniques[5], qui travaillent en groupes d'études pluridisciplinaires facilitant les échanges entre chercheurs et organisant tous les trois ans un congrès européen de systémique.

Pour atteindre les objectifs fixés, un nouveau fondement théorique est nécessaire pour la sécurité du système. La théorie des systèmes prévoit ce fondement. Ce qui vient d'être exposé présente les concepts de base en théorie des systèmes et la façon dont cette théorie est reflétée dans l'ingénierie des systèmes, et comment tout cela se rapporte à la sécurité du système.

2. La démarche induite de la systémique pour l'analyse de l'accident

Dans la méthode scientifique traditionnelle, les systèmes sont décomposés en parties distinctes afin que les parties puissent être examinées séparément : d'une part l'aspect technique des systèmes est décomposé en des composantes techniques distinctes, tandis que le fonctionnement est décomposé en événements discrets au fil du temps.

- Aspects technique → Séparer les composants techniques
- Fonctionnement→ Événements discrets au fil du temps

[5] : http://www.afscet.asso.fr/

Cette décomposition (officiellement appelée réduction analytique) sous-tend que chaque élément, composant ou sous-système, fonctionne de façon autonome et que les résultats d'analyse des composants considérés séparément ne sont pas déformés lorsque le composant est replacé dans son environnement. Cette hypothèse implique que les composants ou les événements ne sont pas soumis à des boucles de rétroaction et autres interactions non-linéaires et que le comportement des composants est le même quand examiné isolément comme quand ils jouent leur rôle dans l'ensemble. Une hypothèse fondamentale est que les principes relatifs à l'assemblage des composants dans l'ensemble (les interactions) sont simples.

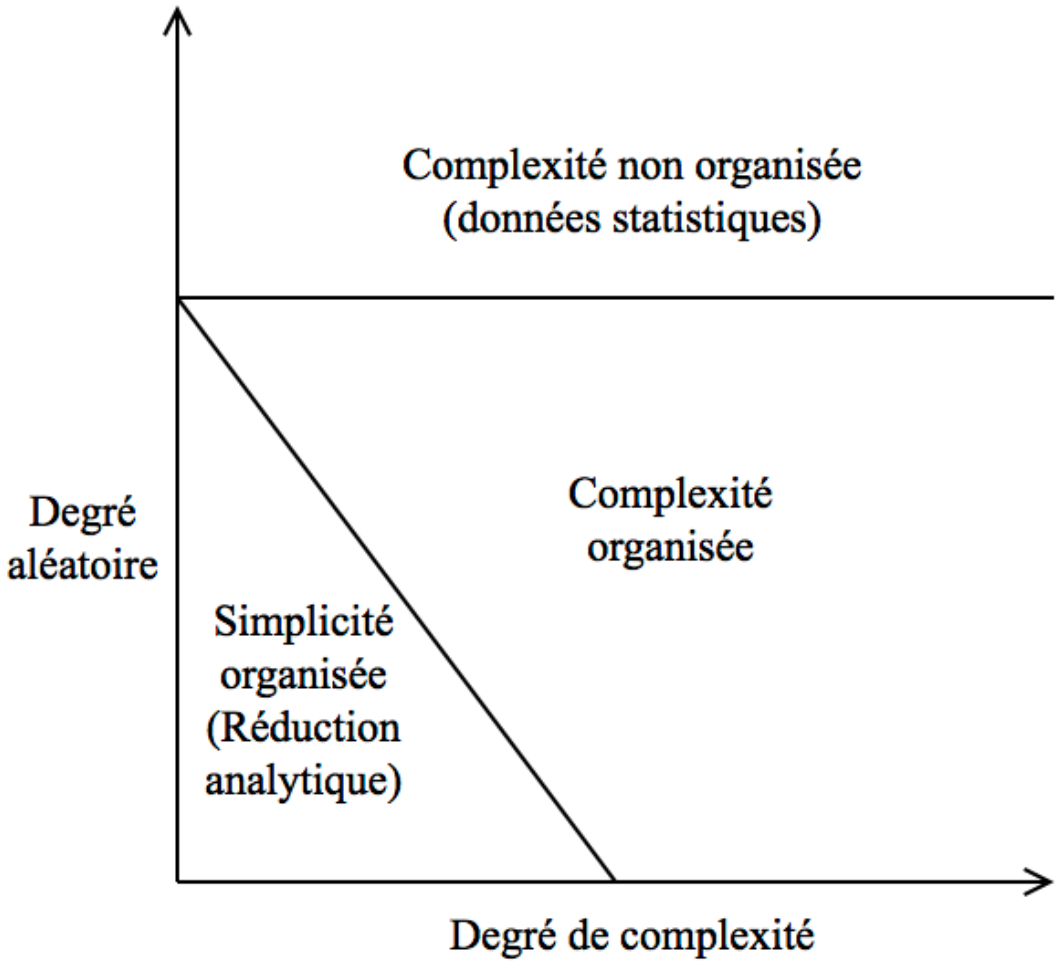


Figure 2-1 Degré de complexité (Leveson, 2011)

Il existe une hypothèse concernant les systèmes que les théoriciens appellent systèmes à complexité organisée. Ces systèmes sont trop complexes pour analyse complète et trop organisés pour les statistiques ; les moyennes sont dérangées par la structure sous-jacente]. De nombreux systèmes d'ingénierie complexes de l'après Seconde Guerre mondiale, ainsi que des systèmes biologiques et des systèmes sociaux, entrent dans cette catégorie.

La complexité organisée représente particulièrement bien les problèmes auxquels sont confrontés ceux qui tentent de construire le logiciel complexe, et il explique la difficulté que les informaticiens ont eue en essayant d'appliquer l'analyse et les statistiques sur les logiciels. La théorie des systèmes a été développée pour ce troisième type de système. L'approche des systèmes se concentre sur le système pris dans son ensemble, et non pas sur les pièces prises séparément. Il suppose que certaines propriétés des systèmes peuvent être traitées uniquement dans leur intégralité, en tenant compte de tous les aspects sociaux, techniques ou autres.

Ces propriétés du système découlent des rapports entre les parties du système : comment les pièces interagissent et s'ajustent. Se concentrer sur l'analyse et la conception d'un tout indépendamment des composants des composants ou pièces fournit représente un moyen d'étudier les systèmes présentant une complexité organisée. Les fondements de la théorie des systèmes reposent sur deux paires d'idées : (1) l'émergence de la structure hiérarchique et (2) rétroaction et le contrôle.

2.1.1 L'émergence de la structure hiérarchique

Un modèle général de systèmes complexes peut être exprimée en termes d'une hiérarchie de niveaux d'organisation, chacun plus complexe que celui du dessous, où un niveau se caractérise par la présence de propriétés émergentes. Les propriétés émergentes n'existent pas au niveau inférieur ; elles n'ont aucun sens dans la langue appropriée à ces niveaux. (Leveson, 2011) La forme d'une pomme, bien que finalement explicable en termes de cellules de pomme, n'a aucun sens à ce niveau inférieur de description. Le fonctionnement du processus aux niveaux inférieurs de la hiérarchie suite à un niveau de complexité supérieur - celui de la pomme entière elle-même - qui a

propriétés émergentes, l'une d'elles concerne la pomme elle-même. Le concept d'émergence est l'idée qu'à un certain niveau de complexité, certaines propriétés caractéristiques de ce niveau (émergeant à ce niveau) sont irréductibles.

Elle traite des différences fondamentales entre un niveau de complexité et un autre. Son objectif ultime est d'expliquer les relations entre les différents niveaux : ce qui génère des niveaux, ce qui les sépare, et quels sont les liens entre eux. Les propriétés émergentes associées à un ensemble de composants à un niveau dans la hiérarchie sont liées à des contraintes sur le degré de liberté de ces composants. Décrire les propriétés émergentes résultant de l'imposition de contraintes nécessite un langage à un niveau plus élevé (un méta niveau) différent de celui décrivant les éléments eux-mêmes. Ainsi, différents langages de description sont appropriés à différents niveaux.

La fiabilité est une propriété d'un composant. Les conclusions peuvent être obtenues sur la fiabilité d'une vanne en isolation, où la fiabilité est définie comme la probabilité avec laquelle le comportement de la vanne va être conforme aux spécifications dans le temps et dans des conditions données. La sécurité, d'autre part, est manifestement une propriété émergente des systèmes : La sécurité ne peut être déterminée que dans le contexte de l'ensemble.

Déterminer si une usine est suffisamment en sécurité n'est pas possible, par exemple, en examinant une seule vanne dans l'usine. En fait, les déclarations sur la " sécurité de la vanne " sans informations sur le contexte dans lequel cette vanne est utilisée sont dénuées de sens. La sécurité est déterminée par la relation entre le vanne et les autres composants de l'installation. Comme autre exemple, les procédures que le pilote exécute lors d'un atterrissage pourraient être sûres dans un avion ou dans un ensemble de circonstances mais dangereux dans un autre. Bien qu'elles soient souvent confondues en procédures, la fiabilité et la sécurité sont des propriétés différentes.

Les pilotes peuvent exécuter de manière fiable les procédures d'atterrissage d'un avion ou dans un aéroport dans lesquels ces procédures sont dangereuses (Leveson, 2011). Une arme à feu lorsqu'elle est déchargée sur un désert avec aucune présence

d’êtres vivants peut être à la fois sûre et fiable. Quand l’arme est déchargée dans un centre commercial bondé, dans ce cas la fiabilité n’est pas mise en question, mais la sécurité assurément. Parce que la sécurité est une propriété émergente, il n'est pas possible de prendre un seul composant du system, comme par exemple un composant technique ou une seule action humaine, en l’isolant de son environnement. Un composant qui est tout à fait en sécurité dans un système ou dans un environnement peut ne pas continuer à l’être dans un autre.

Le nouveau modèle d'accidents introduit et intègre la théorie de base des niveaux hiérarchiques systèmes, où les contraintes ou l'absence de contraintes à des niveaux plus élevés de contrôle ou permettent de perturber le comportement. La sécurité est traitée comme une propriété émergente à chacun de ces niveaux (Leveson, 2011). La sécurité dépend de l'application de contraintes sur le comportement des composants dans le système, notamment des contraintes sur leurs interactions potentielles.

2.1.2 Principe de rétroaction

La deuxième grande paire d'idées en théorie des systèmes est la communication et le contrôle (Leveson, 2011). Un exemple de réglementation ou de contrôle d’action est l'imposition de contraintes de façon pertinente à un niveau d'une hiérarchie, qui définissent les « lois de comportement » à ce niveau. Ces lois de comportement rendent l’activité significative à un niveau plus élevé. Les hiérarchies sont caractérisées par les processus de contrôle d'exploitation au niveau des interfaces entre les niveaux. Le lien entre mécanismes de contrôle étudiés dans les systèmes biologiques et ceux développés dans les systèmes automatisés a été expliqué par une partie de théorie des systèmes connus comme cybernétique.

Le contrôle est toujours associé à l'imposition de contraintes et pour tenir compte d'un processus de contrôle ceci requiert nécessairement la prise en compte au moins de deux niveaux hiérarchiques. À un niveau donné, il est souvent possible de décrire le niveau en écrivant les équations dynamiques, en partant de l'hypothèse qu'une particule est représentative de la collection et que les forces à d'autres niveaux n'interfèrent pas. Mais toute description d'un processus de contrôle implique un niveau

supérieur imposant des contraintes sur la partie inférieure. Le niveau supérieur est une source d'une description alternative (plus simple) du niveau inférieur en termes de fonctions spécifiques émergent à la suite de l'imposition de contraintes.

Imposer des contraintes de sécurité joue un rôle fondamental dans l'approche de sécurité présentées dans ce concept. La focalisation limite à se concentrer sur les moyens d'éviter les échecs, ce qui est commun dans le domaine de la maîtrise des risques aujourd'hui, est remplacée par la notion plus large d'imposer des contraintes sur le comportement du système pour éviter que les événements ou les conditions dangereuses, c'est-à-dire les risques, ne surviennent. Le contrôle dans les systèmes ouverts (ceux qui possèdent des entrées et sorties de leur environnement) implique un besoin accru pour préserver la sécurité du système.

Bertalanffy a distingué entre systèmes fermés, dans lesquels les composants immuables agissent dans un état d'équilibre et des systèmes ouverts, qui peuvent être éjectés en dehors de l'équilibre par des échanges avec leur environnement (Bertalanffy, 1969; Leveson, 2011). En théorie du contrôle, les systèmes ouverts sont considérés comme des éléments interdépendants qui sont maintenus dans un état d'équilibre dynamique par boucles de rétroaction de l'information et de contrôle. La performance globale de l'usine doit être contrôlée afin de produire le produit désiré tout en répondant à des objectifs de coûts, de sécurité, d'ordre général et des contraintes de qualité. Pour commander un processus, quatre conditions sont requises (Leveson, 2011) :

- Condition sur l'objectif : Le contrôleur doit avoir un objectif ou des objectifs (par exemple, maintenir le point de consigne).
- Condition d'action : Le contrôleur doit être en mesure d'affecter l'état du système. En ingénierie, les actions de contrôle sont mises en œuvre par les actionneurs.
- Condition sur le modèle : Le contrôleur doit être (ou contenir) le modèle du système
- Condition d'observabilité : Le contrôleur doit être en mesure de déterminer l'état du système. Dans le domaine de l'ingénierie la terminologie, l'observation de l'état du système est fournie par des capteurs.

3. Le modèle STAMP

Dans les systèmes complexes modernes, l'homme se trouve dans un environnement où il va manipuler des machines et des technologies compliquées. Les résultats de ces interactions homme/machine ne peuvent pas être appréhendés selon une approche cartésienne. En effet on ne peut pas comprendre le résultat de ces interactions si l'homme ou la technologie sont étudiés chacun de manière isolé de leur contexte. Les systèmes composés d'agents humains et d'artefacts techniques sont souvent ancrés dans des structures sociales complexes telles que les objectifs de l'organisation, ces stratégies, la culture d'entreprise, sa situation économique, juridique, politique et environnementale.

La théorie sociotechnique implique que les agents humains et les institutions sociales soient partie intégrante des systèmes techniques, et que la réalisation des objectifs de l'organisation ne soient pas atteints par le système d'optimisation de la technique, mais par l'articulation des aspects techniques et sociaux.

Ainsi, l'étude des systèmes complexes modernes nécessite une compréhension des interactions et des interrelations entre les aspects techniques, humains, sociaux et organisationnels du système. Ce chapitre présente un modèle d'analyse des risques et de prévention des accidents conçu par Nancy Leveson, professeur au MIT : STAMP (Systems-Theoretic Accident Model and Processes).

Ce modèle est largement utilisé dans le secteur industriel du pétrole et du gaz (Aas, 2010; AlKazimi, 2015; Altabbakh et al., 2014; Budde, 2012, 2012, Carlson, 2014, 2015; Dobi et al., 2013; Grantham, 2013; Hoel, 2012; John L Thorogood, 2015; Leveson, 2013a; Pasman, 2015; Pelegrín, 2012; Sagvolden, 2013; Samadi and Garbolino, 2011; Sefer et al., 2015; Syvertsen, 2012a; Thammongkol, 2014; Torgauten, 2013; Unnikrishnan et al., 2008; Yang and Haugen, 2014).

Il trouve son application notamment avec les travaux de (Hanan Altabbakh et al., 2014) où le modèle est employé pour effectuer une analyse d'accident sur une installation de traitement de pétrole brut. Le recours au modèle STAMP est aussi adopté

dans la thèse de (Rolf-Arne Haugen Syvertsen, 2012) pour analyser l'accident de la plateforme pétrolière Deepwater Horizon. Dans la thèse de (Silje Frost Budde, 2012) il permet de modéliser un blowout pendant un forage. Dans celle de (Samadi, 2012b) il permet d'effectuer une analyse de risque de captage et de stockage de CO_2. Dans (Pitiporn Thammongkol, 2014) il permet d'analyser l'accident de la raffinerie Richmond opérée par Chevron survenue en août 2012 en Californie San Francisco Bay. Dans ses travaux pour les industries pétrochimiques, Nancy Leveson (Leveson, 2013b) l'utilise pour concevoir des indicateurs globaux de gestion des risques.

Le cadre théorique STAMP présume que toutes les pratiques dangereuses sur le système sont le résultat des actions appliquées suivantes (Leveson, 2011) :

- L'opération de contrôle qui vise à préserver la sûreté de fonctionnement et la sécurité du système n'est pas déclenchée.
- L'opération de contrôle engagée expose le système à des difficultés qui compromettent à la sécurité.
- L'opération de contrôle pour assurer la sûreté de fonctionnement et la sécurité du système n'est pas communiquée à terme.
- L'exécution des commandes de contrôle est interrompue ou est poursuivie sur une longue période.

L'aspect de causalité de ce modèle suit des lois préconçues adaptées à la complexité des systèmes contemporains. Afin de mieux exploiter et de comprendre le modèle STAMP nous allons présenter les lois de base de la démarche d'approche de l'accident. Ces lois couvrent tous les éléments impliquant le contrôle de la sécurité des systèmes complexes.

3.1 Les hypothèses de base du modèle STAMP

Sept hypothèses de base sont considérées pour démontrer l'aspect innovant du modèle STAMP (Leveson, 2011). Dans ce modèle la survenance d'un accident est interprétée à travers un problème de manque de contrôle, c'est ainsi qu'une démarche qui vise à fonder la réflexion sur des hypothèses qui permettent de placer l'étude de

l’accident dans un cadre global qui tient compte des processus, structure et hiérarchie complexe.

3.1.1 Le manque de contrôle provoque l’accident

La Haute fiabilité n’est pas une condition nécessaire et suffisante pour garantir la sécurité d’un système. En effet, la construction d’un système plus sûr implique de se rendre au-delà de la mise au point habituelle sur la défaillance et la faillibilité d’un composant et de mettre l'accent sur les dangers du système, de les supprimer ou de réduire leur présence. Cette démarche présente des conséquences importantes sur les approches d'analyse de l’accident et les approches de conception des systèmes en sécurité. Les techniques d'ingénierie et d’analyse de la fiabilité, telles que l'analyse des modes et effets de défaillance (AMDEC), ne sont pas appropriées pour l'analyse de la sécurité dans une problématique de contrôle. Il en est de même pour les arbres de défaillance.

3.1.2 Les modèles conceptuels traditionnels d’analyse des accident représentent des limites

Les Accidents sont des processus complexes impliquant l’ensemble du système sociotechnique. Les modèles traditionnels de type « chaîne d'événements » ne peuvent décrire le processus d’accident rigoureusement. La plupart des modèles d’accidents qui sous-tendent l'ingénierie de la sécurité proviennent d’une époque (les années 1960) où les systèmes étaient beaucoup plus simples. Les nouvelles technologies et la prise en compte des facteurs humain et organisationnel (durant les années 1990) sont des changements fondamentaux dans l'étiologie des accidents, qui provoquent de fait une évolution dans les mécanismes explicatifs utilisés pour les comprendre et les techniques d'ingénierie appliquées afin d’en éviter la survenance.

Les modèles basés sur des événements sont limités dans leur capacité à représenter les accidents comme des processus complexes, en particulier en ce qui concerne les facteurs d'accident systémique en lien direct avec les déficiences structurelles de l'organisation, le manque de gestion et les failles dans la culture de la sécurité de l'entreprise ou d’une industrie (Pidgeon, 1991). Il est désormais admis qu’il faut comprendre comment l'ensemble du système, y compris les composantes

organisationnelles et sociales, fonctionnent ensemble, et comment il peut lui-même se conduire à sa perte. Les extensions de modèles de type « chaîne d'événements » proposées à ce jour, ne sont pas satisfaisantes (Woods et al., 2012). Un modèle d'accident devrait mettre en valeur une vue d'ensemble des mécanismes de l'accident qui élargit l'enquête au-delà des événements immédiats : une focalisation sur l'opérateur, les défaillances des composants physiques et de la technologie peut conduire à négliger certains des facteurs des plus importants en termes de prévention des accidents futurs (Leveson, 2004). La notion de « cause principale » doit donc être reconsidérée (Leveson, 2011).

3.1.3 L'approche probabiliste d'analyse des risques et de prévention des accidents représente des limites

Le Risque et la sécurité doivent être communiqués et expliqués à travers une approche différente de celle de l'analyse probabiliste des risques. Comprendre le risque est important dans le processus décisionnel. Les professionnels de la sécurité supposent que les informations sur les risques sont plus convenablement communiquées sous la forme d'une probabilité. Les opérateurs et exploitants peuvent pourtant rencontrer des difficultés dans l'interprétation des probabilités. Il peut s'avérer que ces valeurs soient correctement utilisées, cependant les outils de calcul des probabilités de défaillance, ont de sérieuses limites (Hollnagel et al., 2007). Un modèle d'accident qui ne repose pas uniquement sur les défaillances de composants, peut donc fournir une base entièrement nouvelle pour comprendre et évaluer la sécurité et, plus généralement, les risques.

3.1.4 L'environnement de travail influence le comportement de l'opérateur

Le comportement de l'opérateur est influencé par l'environnement dans lequel il opère et agit. Afin de réduire l'« erreur » de l'opérateur, il convient de maîtriser l'environnement dans lequel l'opérateur travaille. Modifier cet environnement sera beaucoup plus efficace pour éviter l'erreur de l'opérateur que l'approche béhavioriste (Guenebeaud, 2013) habituelle fondée sur la récompense et la punition. Sans changer l'environnement, l'erreur humaine ne peut être réduite pour longtemps. Comme l'a soutenu Rasmussen (Leveson, 2016), un modèle d'analyse des accidents efficace suppose l'explication des rôles et des responsabilités des opérateurs et superviseurs

humains. Dans ce contexte, en cas d'accident, l'étude de l'erreur humaine (écarts de procédures normatives) suppose de mettre l'accent sur les mécanismes et les facteurs qui influencent le comportement humain. Il est donc nécessaire de comprendre le contexte dans lequel les actions humaines ont lieu et les décisions sont prises. La modélisation de comportement en elle-même par la décomposition dans les décisions et les actions ou les événements, dans la plupart des modèles d'accidents actuels tous les font, et ils l'étudient comme un phénomène isolé du contexte dans lequel le comportement a lieu et ceci n'est pas un moyen efficace pour comprendre le comportement.

3.1.5 La présence des systèmes automatisés fiables de contrôle du processus n'est pas suffisant pour maîtriser la sécurité

Dans les industries, on retrouve de plus en plus des systèmes automatisés de contrôle des processus. Un système automatisé très fiable n'est pas nécessairement sans danger (Thomas et al., 2012). Augmenter la fiabilité de ces machines a peu d'impact sur la sécurité si elle est isolée du contexte global. Un système automatisé est intégré dans un environnement de travail et interagit avec une bonne partie des composants du système, et parfois avec des composants sensibles (les capteurs par exemples) d'où la notion d'impact modéré de sa fiabilité.

3.1.6 La migration du système vers un état accidentel peut être anticipée par un travail de conception approprié au système

Le travail de conception de la sécurité doit comprendre les démarches de prévention des risques qui permettent de traiter l'adaptation et les modes de changement d'un système au cours du temps. Pour cela, tout travail suppose l'étude de l'ensemble de processus impliqué dans la sécurité et non seulement les conditions et les évènements. Les procédures de contrôle doivent intégrer une étape de description du système et du comportement humain requis. Le travail de conception de la sécurité doit comprendre une approche pour expliquer les facteurs sociaux et organisationnels. Tout travail de conception de la sécurité doit être traité comme un problème complexe impliquant l'ensemble de la structure sociotechniques d'un système notamment les lois et les règlements, les organismes gouvernementaux les associations industrielles et les

compagnies d'assurance, la gestion de l'entreprise, opérateur technique et ingénieur, les opérations, et ainsi de suite.

Table 2-1: Les hypothèses

Les hypothèses fondamentales des modèles traditionnels	Les hypothèses fondamentales de STAMP
La sécurité évolue en développant la fiabilité des composants ou de l'ensemble du système.	La fiabilité n'est pas une condition nécessaire et suffisante pour la sécurité.
L'accident est provoqué selon une chaîne d'événement directement lié. Pour comprendre l'accident et évaluer les risques, il suffit d'examiner la chaîne d'événement qui a entrainé la perte.	Les accidents sont des processus complexes impliquant l'ensemble du système sociotechnique. Le modèle de chaîne d'événement ne représente pas le processus adéquatement.
L'approche probabilistique d'analyse des risques, fondée sur le modèle de chaîne d'événement, est supposée la plus rigoureuse dans la démarche d'évaluation et de communication des informations en lien avec les risques et la sécurité	L'approche d'analyse des risques et de maîtrise de la sécurité doit être traitée et communiquée autrement (non pas à travers une analyse de probabilité).
Le facteur humain représente la cause de la plupart des accidents. Récompenser les opérateurs pour leurs efforts à préserver la sécurité ou les responsabiliser de leurs erreurs permet ainsi d'empêcher et réduire significativement l'impact des accidents.	L'erreur de l'opérateur est induite par l'environnement dans lequel il opère. Pour réduire le nombre d'erreurs de l'opérateur il faut modifier et développer l'environnement de travail.
Les systèmes automatisés extrêmement fiables ne sont pas dangereux.	Les systèmes automatisés fiables ne sont pas nécessairement sans risques. Le développement de la faillibilité des logiciels représente un impact infime à la sécurité.
Les accidents résultent de l'occurrence d'événements aléatoires simultanés	Les risques ont tendances à se développer et à évoluer dans un système. La prévention de ces risques peut être assurée depuis la phase conception ou pendant la phase exploitation à travers les indicateurs de performance de sécurité.
Responsabiliser et sanctionner est une	Les sanctions et la mise en cause des personnes est

approche nécessaire pour l'apprentissage, le retour d'expérience et la prévention des accidents	l'ennemi de la sécurité. L'important est de comprendre comment le comportement de l'ensemble du système contribue à l'accident et non pas de trouver un coupable.

4. Le concept STAMP

Nancy Leveson, publie en 2002 (Leveson, 2002, 2004) un modèle d'accident STAMP (Leveson, 2012) basé sur la théorie des systèmes, considérée comme un moyen utile d'analyse des accidents. Cette théorie appréhende un système comme une structure hiérarchique dans laquelle chaque niveau impose des contraintes de sécurité sur l'activité du niveau inférieur. Les modèles d'accident fondés sur la théorie des systèmes considèrent que les accidents résultent des interactions incontrôlées entre les différents niveaux de la structure d'un système. Dans ce contexte, les accidents résultent alors d'un problème de contrôle au sein du système. Ce cadre permet alors d'évaluer les actions commandées par une structure de contrôle et d'identifier les mécanismes défaillants sur les modes d'imposition et d'application des contraintes de sécurité. Pour cela, dans cette partie, nous allons introduire les trois concepts de bases à l'origine de ce modèle : les contraintes de sécurité, la structure hiérarchique et les modèles de contrôle des processus.

4.1 Conception des lois de contrôle (contraintes de sécurité)

La notion de contrainte est au cœur du modèle STAMP (Hardy, 2011b). Dans ce contexte, les contraintes sont les conditions et les règles obligatoires à satisfaire afin de préserver la sécurité (tout au long de la durée de vie d'un système). Selon Leveson, il existe des contraintes passives et des contraintes actives. Les contraintes passives, dont la sécurité est maintenue par leur simple présence (ex : barrière physique : porter un casque de protection, dispositif de confinement…). Les contraintes actives (Underwood et Waterson, 2014) nécessitent une action commandée par un système de contrôle, pour générer la sécurité (ex : détecteurs, dispositifs d'arrêt d'urgence, réseau de lutte contre incendie).

4.2 Modélisation de la structure hiérarchique

Le système chargé d'imposer les contraintes de sécurité doit être modélisé sous forme d'une structure hiérarchique. La figure 2-2 montre un exemple de structure de contrôle (Hardy, 2011a, 2016, Hardy and Guarnieri, 2011a, 2011b, 2011c, 2013). Dans cet exemple, il existe deux structures de contrôle. La structure A, impose les contraintes de la phase développement et conception, la structure B impose les contraintes de la phase exploitation. Leveson (Leveson, 2016) souligne que les installations industrielles (Processus physique) contemporaines disposent des systèmes de contrôle automatiques ou semi-automatiques avec superviseur humain. Comme le montre le cadre F, l'opérateur peut avoir une action commandée directe sur le processus contrôlé (flèches pointillées) ou à travers une interface à distance. L'actionneur exécute les actions commandées par le système de contrôle. Leveson explique que les actionneurs peuvent être des opérateurs humains ou des machines. Les capteurs fournissent l'information sur l'état du processus contrôlé. Les automates et contrôleurs commandent le processus d'imposition des contraintes de sécurité sur les activités et opérations. Chaque composant de cette structure est chargé d'assumer ces responsabilités dans le processus de gestion de la sécurité. Cette structure peut encourir des modifications au fil du temps, cependant il faut veiller à ce que les contraintes de sécurité en place ne soient pas négativement affectées. Leveson confirme que les accidents surviennent souvent après un changement dans une structure de contrôle. Dans une entreprise, les systèmes de management de la sécurité fournissent les procédures liées à la gestion du changement. Ces procédures, souvent mal suivies et non strictement appliquées, traitent uniquement les changements planifiés et prévus. Les imprévus liés à l'environnement et au comportement humain doivent aussi être adressés dans ces procédures pour empêcher les accidents. STAMP fournit une démarche pour traiter cette problématique. (Leveson, 2011) considère aussi que la culture de sécurité est un aspect important qui doit être imposé au sein d'une structure comme partie intégrante de contrôle de la sécurité.

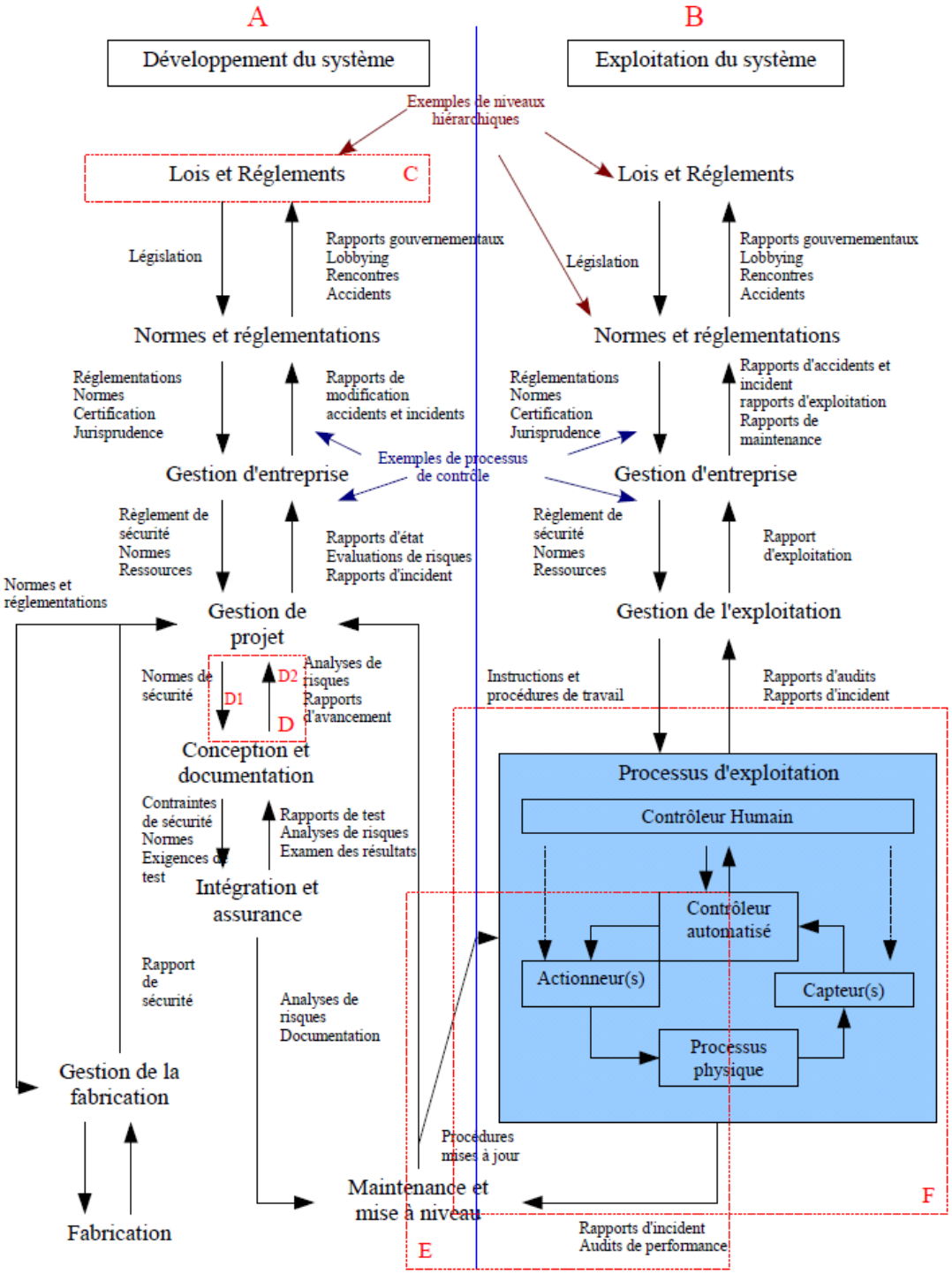


Figure 2-2 Structure hiérarchique (Hardy, 2010; Leveson, 2011)

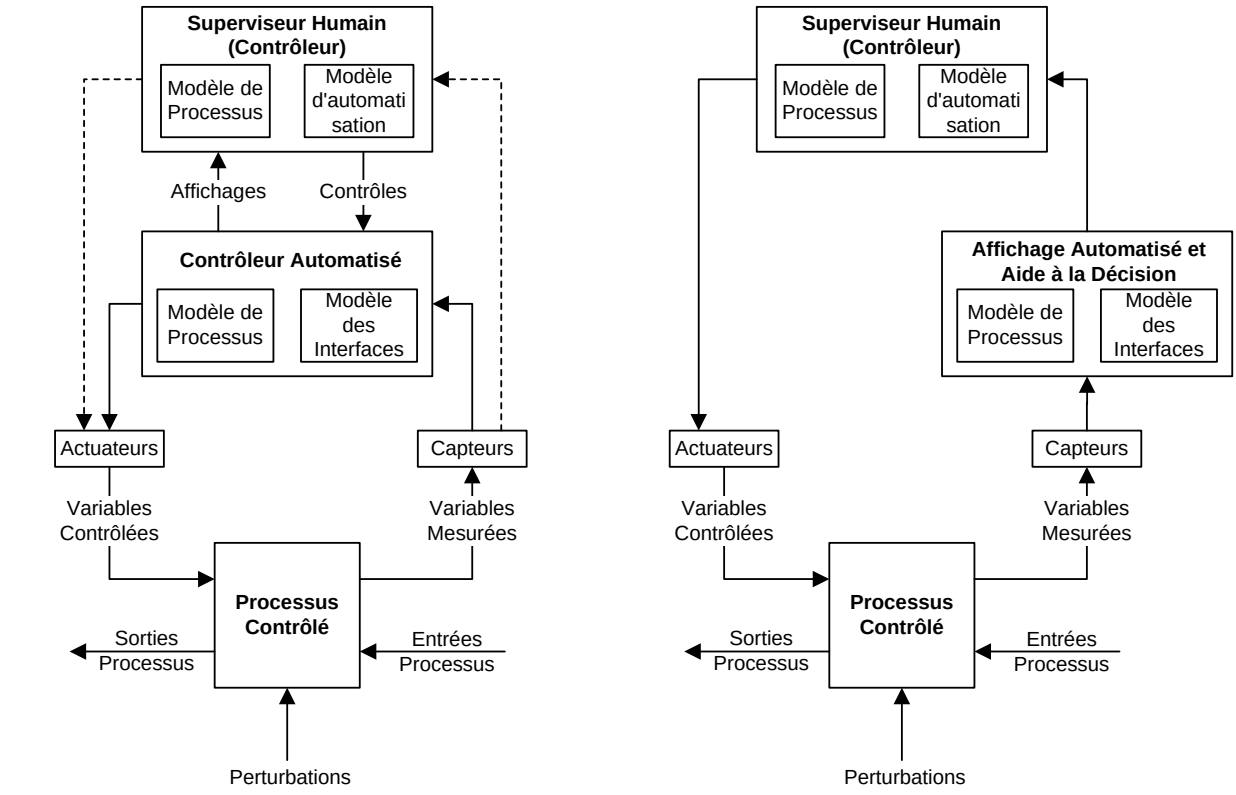
4.3 Les modèles de contrôle des processus

Les opérateurs humains et les systèmes de contrôle automatisés requièrent un modèle de processus. Les modèles de processus correspondent à l'algorithme

implémenté au sein d'un système de contrôle automatisé. Pour les opérateurs humains, c'est l'équivalent des procédures et du modèle mental. Ces modèles déterminent donc les étapes pour procéder au contrôle du système. En théorie du contrôle, les systèmes ouverts sont considérés comme éléments interdépendants qui sont maintenus dans un état d'équilibre dynamique par boucles de rétroaction et de contrôle. Quatre conditions sont requises pour le contrôle des processus industriels à travers l'imposition de contraintes de sécurité :

- Condition sur l'objectif : Le contrôleur doit avoir un objectif ou des objectifs (par exemple, imposer l'application des contraintes de sécurité dans le système).
- Condition d'action : Le contrôleur doit être en mesure d'affecter l'état du système. En ingénierie, les actions de contrôle sont mises en œuvre par les actionneurs.
- Condition sur le modèle : Le contrôleur doit être (ou contenir) le modèle du système
- Condition d'observabilité : Le contrôleur doit être en mesure de vérifier l'état du système. Dans le domaine de l'ingénierie les informations sur l'état du processus contrôlé sont fournies par des capteurs.

Le modèle de processus doit contenir les informations liées à l'imposition des contraintes, aux variables mesurées de l'état du système et les modes de changement d'état du processus contrôlé. Le modèle de processus est un moyen à disposition du système de contrôle pour générer les actions commandées. Le modèle de processus doit être implémenté dans tous les systèmes de contrôle qui composent la structure hiérarchique.



(a) Automatisation émettant directement des commandes sous la supervision d'un contrôleur humain

(b) contrôle humain avec l'assistance automatisée

Figure 2-3 Boucle de contrôle

La figure 2-3 schématise un archétype de boucle de contrôle modélisant un système de contrôle automatique supervisé par un opérateur humain. Les flèches en pointillées désignent le fait qu'un opérateur humain peut avoir une perception directe sur l'état du système (autre que celle transmise par les systèmes d'information). Il peut ainsi manipuler et commander l'état du processus contrôlé manuellement et pas uniquement à travers d'un système de contrôle commande. La deuxième figure montre une boucle de contrôle où l'opérateur humain gère le processus contrôlé en se basant sur un outil d'aide à la décision. Les outils d'aide à la décision doivent donc inclure un modèle de processus puisque ce sont des systèmes qui contrôlent indirectement le processus.

5. Classification factorielle des accidents selon STAMP

STAMP suppose que les infractions aux contraintes de sécurité provoquent les accidents au sein d'un système. Les infractions résultent des défaillances et des dérèglements techniques, des perturbations provoquées par l'environnement, ou des dysfonctionnements provoqués par l'interaction des composants du système. Sur l'ensemble de la structure hiérarchique, les comportements à risque résultent de l'absence de contraintes, ou des modes inappropriés d'imposition d'une contrainte conduisant ainsi à son infraction.

L'approche STAMP suppose que chaque composant de la boucle de contrôle est susceptible d'appliquer incorrectement les contraintes de sécurité. Il faut alors évaluer la contribution de chaque élément de la boucle de contrôle à la migration du système vers l'état accidentel. (Leveson, 2011) propose deux facteurs de classification des accidents (Figure2-4) : (1) l'action commandée par le système de contrôle est inappropriée, (2) l'action commandée est exécutée incorrectement par l'actionneur. Ces facteurs peuvent être transposés sur chaque niveau de la structure hiérarchique. En effet pour chaque niveau de la structure, il est nécessaire d'évaluer le contexte de prise de décision, les mécanismes qui influencent la mise en forme d'une action dangereuse.

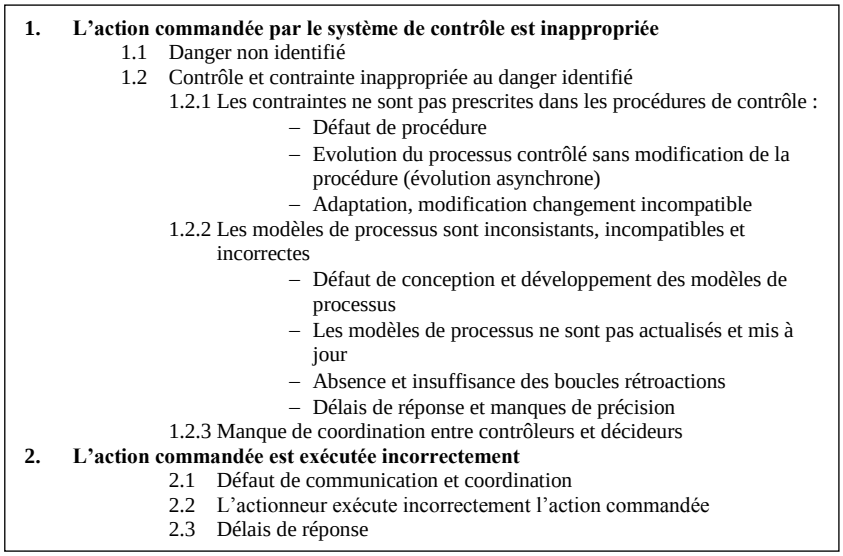


Figure 2-4 Classification des causes de l'accident selon STAMP

Les facteurs de causalité des accidents peuvent être divisés en trois catégories générales : (1) le fonctionnement du système de contrôle, (2) le comportement des actionneurs et des processus contrôlés, et (3) la communication et la coordination entre les contrôleurs et les décideurs. Lorsque les opérateurs humains sont impliqués dans la structure de contrôle, le contexte et les mécanismes qui influencent le comportement jouent un rôle important dans l'analyse des causes de l'accident. (Figure 2-5)

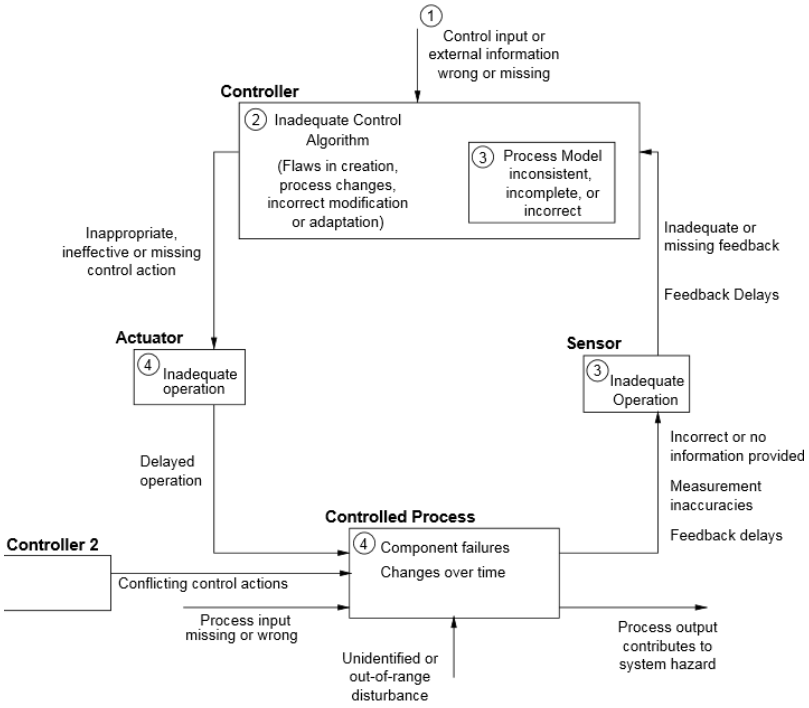


Figure 2-5 Les causes des problèmes de manque de contrôle

5.1 Le fonctionnement du système de contrôle

Le système de contrôle s'appuie sur trois éléments : les données d'entrées, l'algorithme ou les procédures de contrôle et les modèles de processus. Un défaut dans l'un de ces trois éléments (les données d'entrées, l'algorithme ou les procédures de contrôle et les modèles de processus) entraine un processus d'application inadéquat des contraintes de sécurité.

5.1.1 Des données d'entrées dangereuses

Chaque contrôleur de la structure de contrôle hiérarchique est contrôlé par les contrôleurs du niveau supérieur. Ces contrôleurs peuvent manquer d'information sur le processus à emprunter pour préserver la sécurité du système.

5.1.2 Algorithme de contrôle non fiable

Dans ce contexte, l'algorithme de contrôle désigne les procédures développées par les ingénieurs pour les systèmes de contrôle automatisés et les opérateurs humains. L'algorithme de contrôle risque de ne pas assurer sa fonction de contrôle qui est celle de l'imposition des contraintes de sécurité. Ceci est dû généralement à une mauvaise conception et développement de l'algorithme. Leveson (Leveson, 2001, 2011, 2013a, 2013b) précise que le processus contrôlé peut encourir un changement, par la suite l'algorithme peut devenir dangereux s'il n'est pas adapté au changement. Les procédures prescrites pour les opérateurs humains sont affectées si les formations à la sécurité ne sont pas actualisées, ou les modifications dans les procédures ne sont pas suivies. Les délais et les retardements doivent être pensés pendant la phase conception et développement des algorithmes de contrôle. Ces délais se manifestent dans les boucles de contrôle au niveau des fonctions de mesures et d'envoie des paramètres du processus contrôlé et dans l'imposition d'une action commandée. Ces délais peuvent ne pas être distinctement décelés. Lorsque les délais ne sont pas suffisamment pris en compte dans l'algorithme de contrôle, les accidents peuvent se produire.

5.1.3 Les actionneurs et les processus contrôlés

Le système de contrôle impose une contrainte de sécurité sur le comportement du processus contrôlé. La sécurité du processus contrôlé dépend des données d'entrée, du système de contrôle, des actionneurs et des flux de transferts des actions commandées. Le système de contrôle doit être en mesure de gérer les perturbations externes. Dans une structure de contrôle hiérarchique, les actionneurs et les processus contrôlés exécutent les actions commandées sur un processus de niveau inférieur. Dans ce cas, les défauts dans l'exécution de la commande sont les mêmes que celles décrites précédemment pour un contrôleur. Encore une fois, ces types de défauts ne s'appliquent

pas simplement au système technique mais aussi au niveau du système de conception et le développement.

5.1.4 Coordination et communication entre contrôleurs et décideurs

Lorsqu'il existe plusieurs contrôleurs (opérateur humain, système de contrôle automatisé ou semi-automatisé), les commandes délivrées par ces systèmes peuvent être insuffisamment coordonnées. Ces commandes peuvent être aussi contradictoires et en conflit. Pour cela, il faut aussi concevoir et définir les barrières dans les zones où peuvent se présenter des chevauchements.

5.1.5 Contexte et environnement

Le processus de prise de décision chez un opérateur humain se base sur des flux d'informations et sur le modèle de processus. Cependant le modèle de processus ainsi que le flux d'information peuvent être mal fondés et inexactes. Nancy Leveson explique que le contexte et l'environnement de travail influencent le comportement et la conduite d'un opérateur humain. Pour ces facteurs elle emploie le terme «behavior shaping mechanisms» (Leveson, 2011), ce sont les facteurs qui permettent de comprendre le comportement humain.

6. Les outils de STAMP

Afin de faciliter la mise en œuvre de STAMP, une série de dispositifs et d'outils logiciels ont été développés. Deux d'entre eux, STPA et CAST ont été mis en œuvre dans le cadre de cette thèse. L'ensemble des dispositifs et outils repérés à ce jour sont décrits ci-après.

6.1 STPA

L'analyse des dangers STPA (Hardy, 2010; Samadi, 2012b) est un processus itératif fondé sur le modèle d'accident STAMP permettant d'analyser les origines et les causes d'un accident. Dans STPA, le système est vu comme un ensemble de boucles de contrôle interagissant entre elles. L'accident se traduit par un contrôle inadéquat. L'objectif étant, dans une démarche d'enquête accident, de mettre en exergue les actions de contrôle constituant la cause d'une migration du système vers l'état accidentel.

Toute analyse d'accident STPA débute par une identification des dangers « système » afin de les traduire en contraintes de sécurité à un niveau stratégique. L'étape suivante définit la structure de contrôle de la sécurité en mettant en évidence les contrôles et rétroactions à l'œuvre au sein du système. Cette structure de contrôle de la sécurité est utilisée comme un « guide » pour effectuer l'enquête et chaque contrôle de la hiérarchie est évalué en matière d'incidence. Une identification des actions de contrôle inadéquates sert à préciser les contraintes de sécurité inadéquatement appliquées. Enfin, après avoir identifié les actions de contrôle dangereuses ayant pu mener à l'accident, des recommandations sont formulées.

Deux types de modèles, mobilisés lors de deux phases d'analyse, sont généralement nécessaires à l'étude d'un accident.

Le premier est un modèle statique de contrôle de la sécurité permettant de visualiser l'organisation du système accident ainsi que les interactions au sein de ce système :

- Les exigences et les contraintes de sécurité en place ;
- Les actions de contrôles défaillantes ;
- Le contexte (social, politique, économique, environnemental…) au moment de l'accident ;
- Les défauts dans les modèles cognitifs des acteurs du système ;
- Les défauts de coordination, de communication et d'interaction des acteurs du système.

Un second modèle, dynamique et portant sur le comportement, vise quant à lui à comprendre le comportement du système au moment de l'accident ainsi que sa migration d'un état « sûr » vers un état accidentel.

Ces modèles sont utilisés pour comprendre un accident et valider des amendements à apporter à la culture de sécurité d'un système sociotechnique mis à mal par l'accident. Ils peuvent être exploités pour évaluer et analyser les causes d'un

accident et détecter si le niveau de sécurité a atteint un niveau inacceptable menant irrémédiablement à l'accident. Enfin, ces modèles permettent d'évaluer les impacts potentiels des changements et des décisions ayant modifié la structure d'un système, le faisant migrer vers un état accidentel.

6.1.1 Phase Statique

La phase statique consiste à élaborer une description générale du système et les interactions qu'il engendre, elle comporte cinq étapes :

- Étape 1 : analyse préliminaire des risques système et identification des exigences et des contraintes système ;
- Étape 2 : Élaboration de la structure de contrôle de la sécurité qui consiste à définir les rôles et les responsabilités des éléments et les mécanismes de rétroaction ;
- Étape 3 : Intégration des exigences et de contraintes système au niveau des éléments ;
- Étape 4 : analyse de la structure de contrôle et des modèles de processus pour identifier les contrôles inadéquats ;
- Étape 5 : Catégorisation (immédiat long terme et standard) dans le temps et gestion des risques (boucles de contrôle) ;

6.1.2 Phase dynamique

Elle a pour objectif de chercher à comprendre le comportement du système au moment de l'accident et les raisons de son passage de l'état sûr vers un état accidentel. Les étapes de la phase dynamique ne sont pas dissociées de la phase statique et elles lui sont complémentaires par deux étapes supplémentaires :

- Étape 6 : Modélisation dynamique ;
- Étape 7 : Résultats et recommandations ;

6.1.3 Finalité de STPA :

Toutes ces étapes consistent à examiner les parties de la boucle de contrôle pour chaque contrôle d'action dangereuse, pour voir si on peut contrôler la conception et les mesures d'atténuation du risque, ou évaluer les mesures existantes si l'analyse est

effectuée sur une conception existante. Pour plusieurs contrôleurs du même composant ou contrainte de sécurité, cela permet d'identifier les conflits potentiels et les problèmes de coordination.

Examiner comment les contrôles en place pourraient se dégrader au fil du temps et de construire dans le domaine de la protection, y compris :

- Les procédures de gestion des changements pour s'assurer que les contraintes de sécurité sont appliquées dans les changements prévus ;
- Les audits de performance, les audits opérationnels et les hypothèses qui résultent d'une démarche d'analyse des risques permettent de déceler les causes à l'origine de la transgression des instructions de sécurité ;
- Analyse de l'incident pour retrouver la trace des anomalies sur les dangers existants à la conception du système.

6.2 Le modèle CAST (Causal Analysis Based on System Theory)

CAST (Dong, 2012; Kim et al., 2016; McCarthy, 2013; Spiegel et al., 2013; Syvertsen, 2012b; Thammongkol, 2014; Underwood, 2013; Yang and Tian, 2015) est un modèle d'analyse des causes de l'accident. Un accident est considéré comme le résultat d'un processus complexe. L'analyse des accidents selon STAMP suppose alors de comprendre la dynamique du processus qui a mené à la perte de contrôle. La démarche consiste à documenter les directives imposées par la structure de contrôle de sécurité sociotechnique pour le système concerné ainsi que les instructions de sécurité qui ont été violées à chaque niveau de cette structure de contrôle.

Ce modèle permet de faire apparaitre directement des recommandations et des directives de sécurité à imposer sur les opérations et exploitation du système industriel. La démarche peut servir aussi de guide aux enquêteurs dans la préparation des questions de l'enquête. Les étapes suivantes sont à suivre :

1. Identifier les systèmes et les dangers impliqués dans la perte de contrôle.
2. Identifier les directives de sécurité du système et les instructions à suivre selon les dangers identifiés.
3. Documenter la structure de contrôle de la sécurité en place. Les rôles et les responsabilités de chaque acteur du système dans la structure. La documentation

doit inclure les rôles et les responsabilités de chaque acteur du système, ainsi que les procédures fournies dans le but de contrôler la sécurité de l'installation.

4. Déterminer les événements conduisant à la perte de contrôle.
5. Analyser la perte au niveau du système de l'installation physique : il s'agit d'identifier la contribution à l'accident : des manques de contrôle physique et opérationnel, des pannes physiques, des interactions dysfonctionnelles, défauts de communication et de coordination, perturbations non gérées. Il faut aussi déterminer pourquoi les contrôles physiques en place étaient inefficaces pour prévenir le danger.
6. Après avoir dessiné la structure de contrôle hiérarchique de la sécurité de l'installation technique, la démarche consiste à parcourir chaque niveau de la structure échoue dans l'application de mesure de contrôle de la sécurité. Le modèle suppose pour chaque directive de sécurité, aucune instruction n'a été soumise soit les acteurs de la structure de contrôle n'applique pas les instructions recommandées. Le processus décisionnel et les commandes inadéquatement exécutées sont alors étudiés. Pour cela, il suffit d'enquêter les informations dont dispose le décideur ainsi que toute information qui n'était pas disponible, le contexte et les influences sur le processus décisionnel,
7. Évaluer la coordination et la communication entre les opérateurs au moment de l'accident.
8. Identifier les changements dans le système lié à l'affaiblissement de la structure de contrôle de la sécurité au cours du temps.
9. Proposer des recommandations.

En général, la description du rôle de chaque composant dans la structure de contrôle doit comporter ce qui suit :

- Les instructions et les directives de sécurité
  - Les boucles de contrôles
- ·Contexte :
  - Rôles et responsabilités
  - Facteurs environnementaux et behavior-shaping factors (facteurs déterminant les comportements)

- Interactions dysfonctionnelles, défaillances, et les processus décisionnels incorrects conduisant à une déviance dans l'exécution de la procédure
- Raisons pour les actions de contrôle défectueux et les interactions dysfonctionnelles
  - Défauts d'algorithme de contrôle
  - Modèles de processus ou interface incorrectes.
  - Mauvaise coordination ou communication entre plusieurs contrôleurs
  - Défauts de canal de référence
  - Défauts de rétroaction

  Voir l'annexe 1 pour un exemple d'application CAST à l'analyse de l'accident de la bouée de déchargement du FPSO DALIA

6.3 Le logiciel XSTAMPP

Le logiciel XSTAMPP a été développé par Asim Abdelkhaleq (Abdulkhaleq et al., 2015 ; Abdulkhaleq and Wagner, 2015a, 2015b, 2014a, 2014b; Kraus et al., 2015). Abdulkhaleq est un doctorant et assistant chercheur à la faculté de technologie de l'Université de Stuttgart. Ses travaux de thèse ont permis de concevoir un prototype de véhicule autonome dont l'étude des risques a été conduite à l'aide de STAMP. Il a développé une plateforme logicielle extensible pour fournir un support méthodologique à la mise en œuvre de STAMP (STPA et CAST) et afin d'encourager l'application de cette technique par les analystes de sécurité dans les différents domaines du secteur industriel. Trois autres outils de support à STPA ont été développés depuis et ont été présentés à la Troisième Conférence Internationale STAMP en 2014 au MIT. Ils sont brièvement décrits ci-après.

6.4 STPA tools

Suo et Thomas ont développé un outil appelé « STPA tools » pour généraliser la démarche de Thomas (Thomas, 2013) employée lors de l'étape 1 de STPA. Cette démarche consiste à identifier les actions de contrôle dangereuses en se basant sur les variables des modèles de processus. Le prototype permet aux utilisateurs de lister les dangers et de dessiner la structure de contrôle de la sécurité. Ce prototype compile les données et génère automatiquement la table qui détermine le contexte et les scénarios

d’une action dangereuse commandée par le système de contrôle (Suo and Thomas, 2014) .

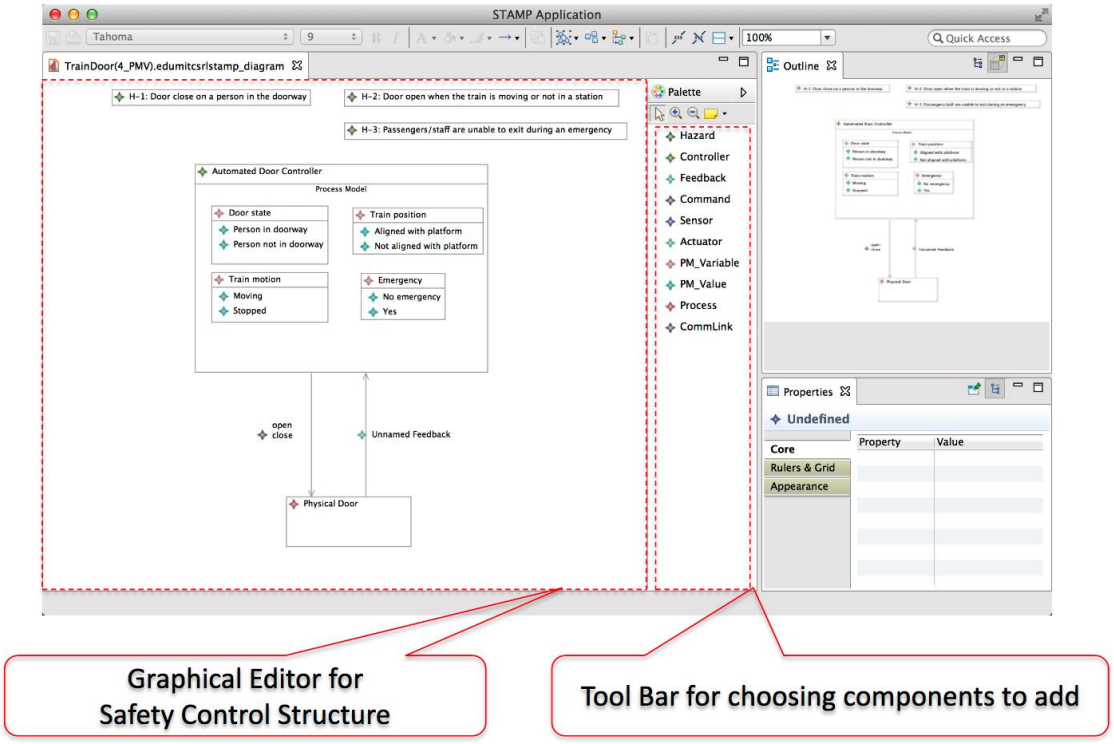


Figure 2-6 Interface du logiciel STPA tool

6.5 SafetyHAT

Volpe (2014)a développé SafetyHAT, pour faciliter l’usage de STPA. SafetyHAT est élaboré sur un cadre d’étude spécifique aux systèmes de transports. C’est un support qui guide dans l’élaboration de la démarche d’analyse des risques STPA.

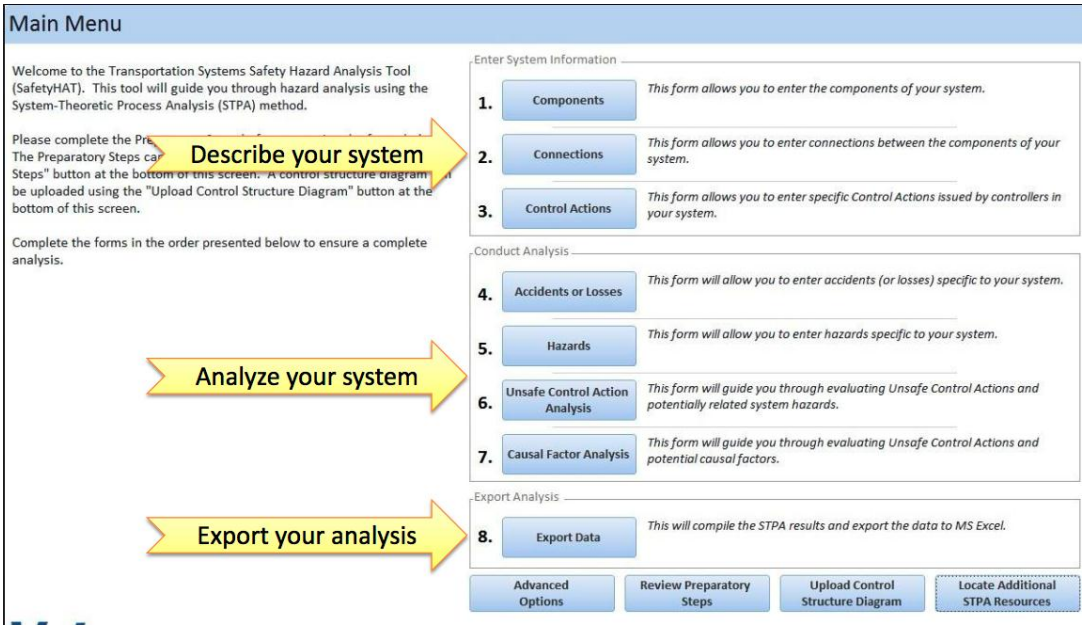


Figure 2-7 Interface principale du logiciel SafetyHAT

6.6 ASTPA

ASTPA est un module de XSTAMPP qui sert de support pour élaborer les étapes de STPA telles qu'elles sont proposées par Leveson (Leveson, 2011). L'interface permet de suivre l'intégralité des étapes et de documenter les principes fondamentaux de la démarche de l'analyse des risques. Ce logiciel permet aussi de concevoir le diagramme de la structure de contrôle, de documenter les actions dangereuses et les contraintes de sécurité. Il permet aussi d'intégrer les modèles de processus au sein des systèmes de pilotage et de contrôle.

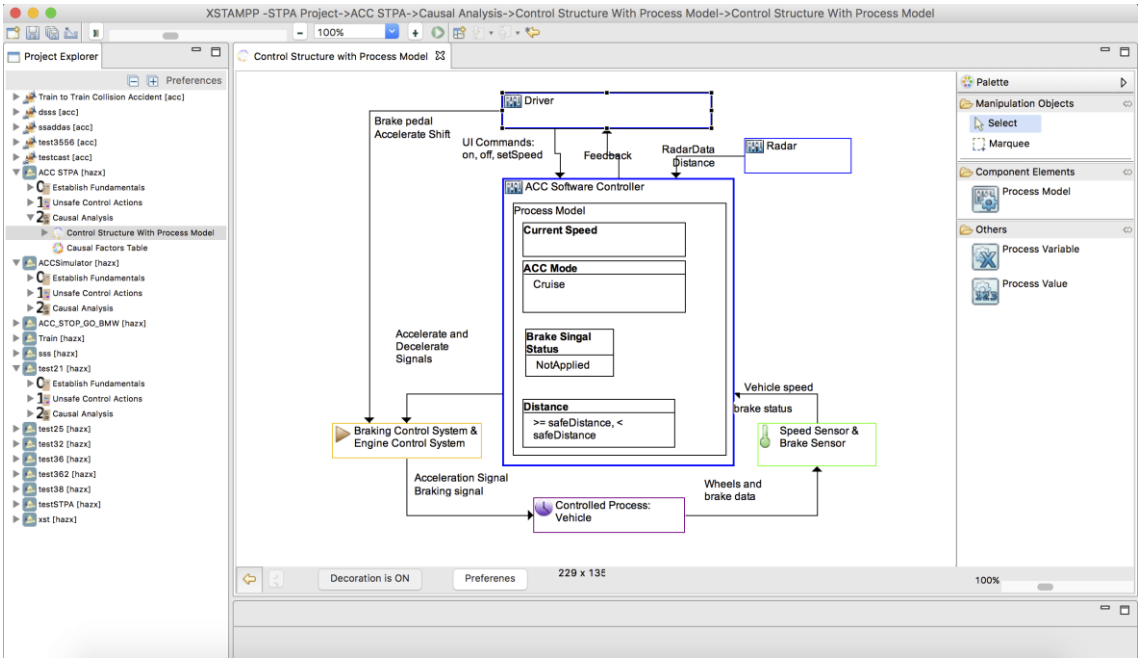


Figure 2-8 Interface du logiciel XSTAMPP pour une étude STPA

7. Conclusion

Ce chapitre présente la théorie des systèmes et le modèles d'analyse des risques et de prévention des accidents STAMP. Selon Leveson « l'hypothèse qui sous-tend le modèle STAMP consiste à considérer que la théorie du système est un moyen utile pour analyser les accidents ». L'approche de maîtrise de la sécurité, proposé par ce modèle, suppose de traiter les problèmes de manque de contrôle par le biais d'une structure hiérarchique. Ce chapitre expose les concepts de base de ce modèle à savoir (les contraintes de sécurité, la structure hiérarchique et le modèle de processus). Ce chapitre présente les démarches pour une analyse STAMP et les logiciels développés pour la compilation des données de l'analyse. Le chapitre 3 présente le système d'étude qui va faire l'objet d'une analyse STPA.

CHAPITRE 3: PRESENTATION DU SYSTEME D'ETUDE

La directive Seveso est un acte normatif pris par les institutions de l'Union Européenne. Cette directive impose aux Etats Membres de l'Union Européenne d'identifier les sites industriels et de prendre des mesures de prévention des risques d'accidents majeurs. En France, la directive Seveso a notamment été transposée par le biais du Code de l'Environnement et de l'arrêté du 10 mai 2000 relatif à la prévention des accidents majeurs dans les installations classées.

Le Code de l'Environnement regroupe des textes juridiques relatifs au droit de l'environnement. Le code comporte sept livres, divisés en titres, chapitres, sections, sous-sections et paragraphes. Le titre 1 du livre V intitulé *Prévention des pollutions, des risques et des nuisances,* comporte les dispositions législatives et règlementaires de l'application de la loi sur les installations classées pour la protection de l'environnement.

D'après l'article L. 511-1, les installations classées pour la protection de l'environnement soumises aux dispositions du titre 1, sont les usines, ateliers, dépôts, chantiers et, d'une manière générale, les installations exploitées ou détenues par toute personne physique ou morale, publique ou privée, qui peuvent présenter des dangers ou des inconvénients soit pour la commodité du voisinage, soit pour la santé, la sécurité, la salubrité publiques, soit pour l'agriculture, soit pour la protection de la nature, de l'environnement et des paysages, soit pour l'utilisation rationnelle de l'énergie, soit pour la conservation des sites et des monuments ainsi que des éléments du patrimoine archéologique.

Les installations visées par l'article L. 511-1 sont définies dans la nomenclature des installations classées établie par décret en Conseil d'État, pris sur le rapport du ministre de l'écologie, de l'environnement et du développement durable, après avis du Conseil Supérieur de la Prévention des Risques Technologiques (CSPRT). Ce décret soumet les installations à autorisation, à enregistrement ou à déclaration suivant la gravité des dangers ou des inconvénients que peut présenter leur exploitation. Les sites industriels à hauts risques sont soumis à une autorisation pour fonctionner. Cette autorisation est décrétée sous forme d'un arrêté préfectorale fixant les dispositions que

l'exploitant devra respecter pour assurer la protection des vulnérabilités et de l'environnement.

Ce chapitre présente un site industriel autorisé par arrêté préfectoral avec servitude (AS), depuis fin 1996, à exercer son commerce de stockage et de vente de GPL (Gaz de Propane liquéfié). Cet établissement est implémenté, en France, sur un terrain d'une superficie de 18 000 m^2. Cet établissement dispose d'un réservoir sous-talus de stockage de 400 m^3 de GPL, des installations de chargement, déchargement et 50 tonnes de bouteilles de butane et de propane. Le stockage de bouteilles ayant été arrêté, l'activité du site est aujourd'hui essentiellement consacrée au stockage et à la distribution du gaz de pétrole liquéfié. Cette logistique permet aux camions petits porteurs de charger le GPL destiné à la clientèle de proximité (les trois quarts de la clientèle sont des particuliers ou industriels).

1. Situation règlementaire

L'établissement est classé SEVESO seuil haut soumis au régime d'Autorisation avec Servitude d'utilité publique (AS) ; il s'agit d'une Installation Classée pour la Protection de l'Environnement. L'exploitant doit donc fournir une étude de danger, définir une politique de prévention des accidents majeurs ; de s'assurer du maintien du niveau de maîtrise des risques tout au long de la vie de l'installation et d'informer les exploitants d'installations classées voisines des risques d'accidents majeurs identifiés dans l'étude de dangers, dès lors que les conséquences de ces accidents majeurs sont susceptibles d'affecter lesdites installations. Le Préfet impose par arrêté aux établissements Seveso seuil haut la mise en place d'un système de gestion de la sécurité (SGS).

Concernant les servitudes, elles recouvrent en tant que besoin : la limitation ou l'interdiction du droit d'implanter des constructions ou des ouvrages et d'aménager des terrains autour de l'installation. Le périmètre de la zone concernée est soumis à une enquête publique et à l'avis des conseils municipaux des communes. Les établissements Seveso seuil haut font aussi l'objet d'un plan de prévention des risques technologiques (PPRT). La prescription du PPRT a pour objet de résoudre les situations difficiles en matière d'urbanisme héritées du passé et mieux encadrer l'urbanisation future.

Le code de l'environnement impose qu'un plan d'opération interne (POI) soit mis en place par l'exploitant, et l'article R741-18 du code de la sécurité intérieure impose qu'un plan particulier d'intervention (PPI) soit mis en place par le préfet. Les arrêtés préfectoraux qui autorisent l'exploitation du site sont présentés dans la Table 3-1.

Table 3-1: Arrêtés préfectoraux de l'établissement étudié

Date	**13 décembre 1996**	**24 janvier 2001**	**25 mai 2009**
Activité autorisée	Exploiter un dépôt de 400 m3 de GPL et 50 tonnes de bouteilles de propane et de butane	Aménagement d'une aire de stationnement camions petits porteurs sécurisée	Donne acte de l'étude de dangers de 2007 et prescrit des mesures complémentaires de réduction des risques

La nomenclature des installations classées permet de déterminer la situation règlementaire et le régime applicable (Table 3-2).

Table 3-2: AS : Autorisation avec servitudes A : Autorisation D : Déclaration

NC : Non Classé C : soumis au contrôle

N° Rubrique	**Désignation des activités**	**Capacité de l'installation**	A, D, AS	Rayon d'affichage
1412	Stockage en réservoirs manufacturés de gaz inflammables liquéfiés, à l'exception de ceux visés explicitement par d'autres rubriques de la nomenclature : Les gaz sont maintenus liquéfiés à une température telle que la pression absolue de vapeur correspondante n'excède pas 1,5 bar (stockage réfrigérés ou cryogéniques) ou sous pression quelle que soit la température. 1. La quantité totale susceptible d'être présente dans l'installation	– Réservoir sous talus de 400 m^3 (propane) soit : 0,9 x 0,515 x 400 = **185,4 t** – 2 citernes enterrées de propane de 1 000 kg et 1 750 kg = **2,7 t** – Stockage de bouteilles **30 t** (bouteilles pleines + 5% bouteilles vides) – 8 véhicules-vrac de 6 tonnes soit **48 t** – 4 véhicules UB de 5,5 t soit **22 t** **soit au total : 288,1 t**	**AS**	**4 km**

	étant supérieure ou égale à 200 t.			
1414	Installation de remplissage ou de distribution de gaz inflammables liquéfiés : 2. Installations de chargement ou déchargement desservant un dépôt de gaz inflammables soumis à autorisation	2 postes de chargement 1 poste de chargement/ déchargement camion	**A**	**1 km**
1432	Stockage en réservoirs manufacturés de liquides inflammables de la catégorie de référence : 2.b Représentant une capacité équivalente totale supérieure à 10 m^3 mais inférieure ou égale à 100 m^3	Réservoirs de gasoil, utilisé pour les chariots automoteurs : **500 l**	**DC**	
2920	Installation de compression fonctionnant à des pressions effectives supérieures à 105 Pa, et comprimant ou utilisant des fluides inflammables ou toxiques, la puissance absorbée étant supérieure à 10 MW	1 Compresseur propane de puissance totale **30 kW** 2 Compresseurs pour la fourniture d'air comprimé de puissance totale absorbée = 1,1 kW et 2,2 kW Soit **3,3 kW**	**NC**	

Dès 2008, les inspecteurs des installations classées ont analysé l'étude de dangers du site et des mesures de maîtrise des risques (réduction à la source) ont été actées dans un arrêté préfectoral du 22/05/2009.Après prise en compte de la démarche de maîtrise des risques à la source, le Préfet a demandé l'élaboration d'un PPRT par l'arrêté préfectoral du 16/10/2009 par lequel il a fixé le périmètre d'étude du PPRT. Le périmètre d'étude ou périmètre d'exposition aux risques est symbolisé par un cercle rouge de rayon 260 M au Nord et 250 M au Sud. Le site étant classé sous le régime (AS) la loi n° 2003-699 du 30 juillet 2003 relative à la prévention des risques technologiques et naturels et à la réparation des dommages rend obligatoire la réalisation d'un Plan de Prévention des Risques Technologiques (PPRT) pour les installations Seveso seuil haut afin de :

- Limiter l'urbanisation future autour du site ;
- Renforcer la protection offerte par le bâti existant ;
- Diminuer la population exposée lorsque cela est nécessaire.

1.1 Organisation en matière de prévention des risques majeurs

La réglementation associée aux établissements Seveso, et plus particulièrement aux établissements Seveso seuil haut, impose la mise en place d'une organisation spécifique à la prévention des risques majeurs, intégrant aussi les aspects intervention en cas d'incident (Sanseverino-Godfrin, 2010). Ainsi, les exploitants des établissements Seveso doivent mettre en place une politique spécifique à la prévention des accidents majeurs et, en ce qui concerne les établissements seuil haut, un système de gestion de la sécurité et un plan d'opération interne. Les préfets doivent, quant à eux, mettre en place un plan particulier d'intervention tandis que l'inspection des installations classées doit réaliser des visites périodiques de contrôle de ces établissements.

1.1.1 Politique de prévention des accidents majeurs

Il s'agit plus précisément, pour l'exploitant, de mettre en place une politique en vue de prévenir les accidents majeurs identifiés dans l'étude de dangers et de limiter leurs conséquences sur l'homme et sur l'environnement. L'exploitant doit définir les objectifs, les orientations et les moyens pour l'application de cette politique et s'engager à améliorer en permanence la maîtrise des dangers liés aux accidents majeurs. Les moyens doivent être proportionnés aux risques d'accidents majeurs identifiés. L'exploitant doit également informer le personnel de l'établissement sur la politique de prévention des accidents majeurs. De plus, il doit, tout du long de la vie de l'installation, veiller à l'application de la politique de prévention des accidents majeurs et assurer le maintien du niveau de maîtrise du risque au sein de son établissement. La politique de prévention des accidents majeurs doit être réexaminée au moins tous les cinq ans et mise à jour si nécessaire. Elle doit par ailleurs être réexaminée en cas de mise en service d'une nouvelle installation, de changement notable ou à la suite d'un accident majeur.

À noter que le document qui définit la politique de prévention des accidents majeurs ainsi que les réexamens périodiques dont il fait l'objet sont soumis à l'avis du comité d'hygiène, de sécurité et des conditions de travail (CHSCT) de l'établissement.

1.1.2 Système de gestion de la sécurité (SGS)

Les exploitants des établissements Seveso seuil haut ont l'obligation de mettre en place un système de gestion de la sécurité (SGS). L'ensemble de la structure organisationnelle, les responsabilités, les pratiques, les procédures, les procédés et les

ressources sont définis pour mettre en œuvre la politique de prévention des accidents majeurs.

1.1.3 Plan d'opération interne

Le code de l'environnement précise qu'un plan d'opération interne (POI) doit être élaboré en vue de contenir et maîtriser les incidents de façon à en minimiser les effets et à limiter les dommages causés à la santé publique, à l'environnement et au bien. Il doit définir les mesures d'organisation, les méthodes d'intervention et les moyens nécessaires que l'exploitant doit mettre en œuvre pour protéger la santé publique, les biens et l'environnement contre les effets des accidents majeurs. Le POI doit, de plus, être mis à jour et testé à minima tous les trois ans. Le projet de POI est soumis à la consultation du personnel travaillant dans l'établissement au sens du code du travail, y compris le personnel sous-traitant, dans le cadre du comité d'hygiène, de sécurité et des conditions de travail.

1.1.4 Plan Particulier d'Intervention (PPI)

Le code de la sécurité intérieure indique que les plans particuliers d'intervention sont établis, en vue de la protection des populations, des biens et de l'environnement, pour faire face aux risques particuliers liés à l'existence ou au fonctionnement d'ouvrages ou d'installations dont l'emprise est localisée et fixe. Ils mettent en œuvre les orientations de la politique de sécurité civile en matière de mobilisation de moyens, d'information et d'alerte, d'exercice et d'entraînement. Le plan particulier d'intervention s'appuie sur les dispositions générales du plan ORSEC (Organisation de la Réponse de Sécurité Civile) départemental. Le PPI doit décrire les dispositions particulières, les mesures à prendre et les moyens de secours pour faire face aux risques particuliers considérés. Il doit comprendre notamment :

- La description générale des installations pour lesquelles il est établi, et la description des scénarios d'accident et des effets pris en compte par le plan ;
- Les mesures d'information et de protection prévues au profit des populations et, le cas échéant, les schémas d'évacuation éventuelle de celles-ci, y compris l'indication de lieux d'hébergement ;
- Les mesures incombant à l'exploitant pour la diffusion immédiate de l'alerte auprès des autorités compétentes et l'information de celles-ci sur la situation et

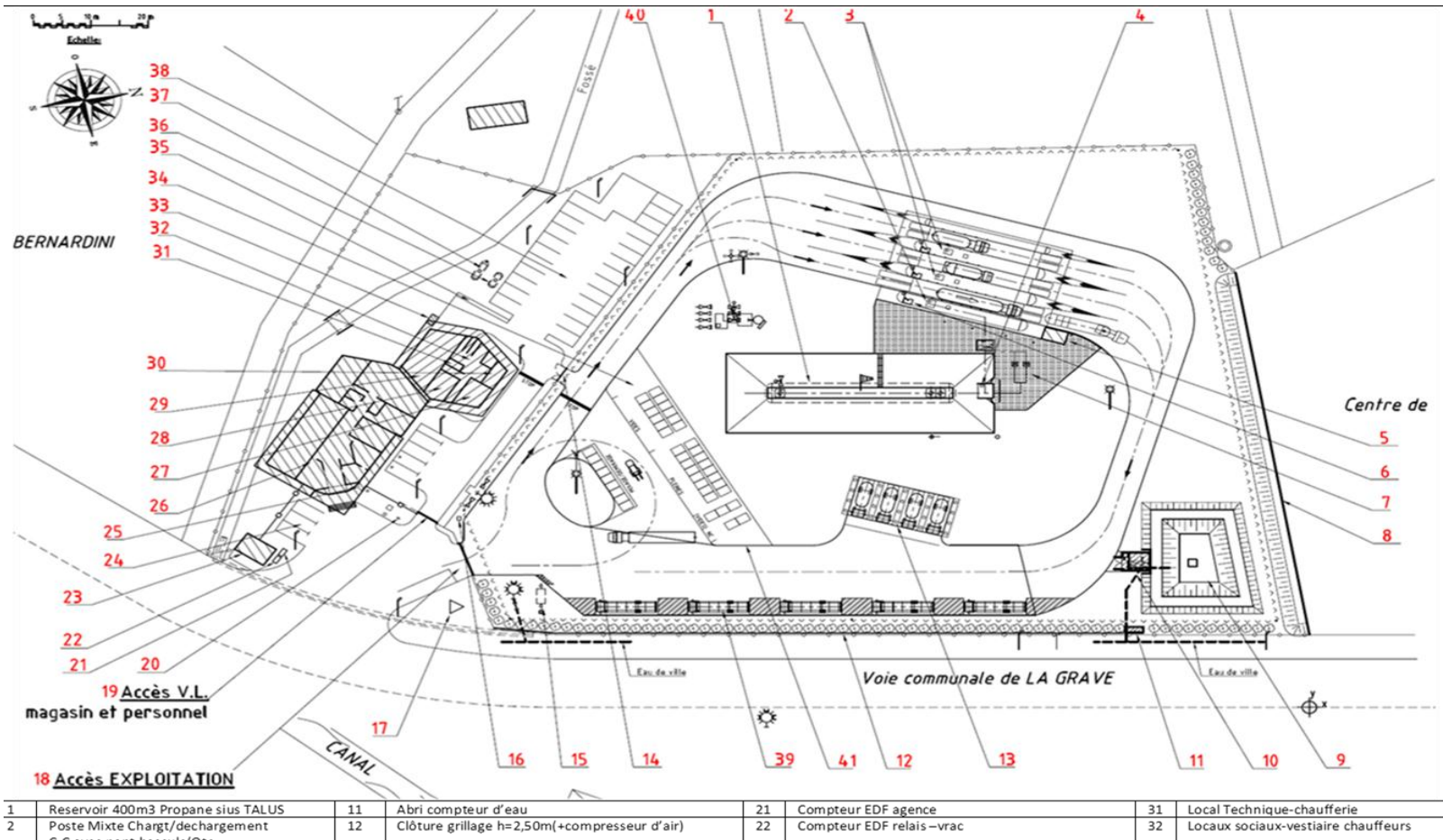
son évolution, ainsi que, le cas échéant, la mise à la disposition de l'État d'un poste de commandement aménagé sur le site ou au voisinage de celui-ci;

- Les mesures incombant à l'exploitant à l'égard des populations voisines et notamment, en cas de danger immédiat, les mesures d'urgence qu'il est appelé à prendre avant l'intervention de l'autorité de police (diffusion de l'alerte, interruption de la circulation et éloignement des personnes au voisinage du site);
- Les modalités d'alerte et d'information des autorités d'un État voisin s'il est concerné ;
- Les dispositions générales relatives à la remise en état et au nettoyage de l'environnement à long terme après un accident l'ayant gravement endommagé.

2. Présentation de l'installation technique

La description des installations du site s'articule autour des points suivants :

- Un réservoir sous talus de propane de capacité 400 m^3,
- Les équipements de transfert situés en zone pomperie (pompes/ compresseur / tuyauterie),
- Un poste de chargement / déchargement des camions citernes gros porteurs et deux postes de chargement des camions citernes petits porteurs,
- Une zone de stockage de bouteilles (vides et pleines),
- Une zone de stationnement camions citernes et bouteilles,
- Des bâtiments d'exploitation,
- Une zone parkings.



1	Reservoir 400m3 Propane sius TALUS	11	Abri compteur d'eau	21	Compteur EDF agence	31	Local Technique-chaufferie
2	Poste Mixte Chargt/dechargement C.C.avec pont bascule(Qte:	12	Clôture grillage h=2,50m(+compresseur d'air)	22	Compteur EDF relais –vrac	32	Locaux sociaux-vestiaire chauffeurs
3	Poste de chargement C.C.avec pont bascule(Qte=2)	13	Parking P.L(4 PP vrac)	23	Local Transformateur E.D.F.(250 KVA pour PRIMAGAZ)	33	Abri cuve G0(500 l) + huiles en bidon (100l)
4	Boitier protection cathodique	14	Portail (ouvrant =3m) avec portillon piéton intégré	24	Parking V.I.visiteurs-3 places	34	Stockage bouteilles pleines ou vides< 50t
5	Local pesage	15	Séparateur d'Hydrocarbures	25	Portillon piéton(Vantail larg.1m, Haut.2m	35	Comptoir bouteilles pleines
6	Abri personnel (Qte=3)	16	Borne de mise à la terre	26	Agence	36	Citerne enterrée Eternella 1000Kg (Bât. Exploitation)
7	Pomperie GPL: 2 pompes 50m3/h+1 compresseur 110 m3/h	17	Mat logo PRIMAGAZ	27	Salle de contrôle	37	Citerne enterrée Eternella 1750Kg (Bât. Exploitation)
8	Merlon de protection (h=3,50m)	18	Accès P.J. (Portail coulissant automatique larg.7m)	28	Bureau de passage	38	Parking V.I.- 21 places
9	Reserve "eau incendie" V=300 m3	19	Accès V.I. (Portail coulissant automatique larg.4m)	29	Atelier- magasin (compresseur d'air 2,2Kw)	39	Fosse vannes d'arrosage asservies
10	Pomperie Incendie: 1GMP 150m3/h (+compresseur d'air)	20	Compteur EAU agence et relais –vrac	30	Local T.G.B.T	40	Local Technique-chaufferie

Figure 3-1 Installations et servitudes techniques

2.1 Réservoir sous-talus de propane

Le propane est stocké à température ambiante sous pression de vapeur saturante dans un réservoir sous talus à axe horizontal de capacité nominale de 400 m3 (Figure 3-2). Le réservoir repose sur un lit de sable. L'épaisseur du talus de terre est d'un mètre minimum ; cette épaisseur est contrôlée annuellement. Le réservoir est protégé contre la corrosion externe par un revêtement en bitume et fil de verre de 6 mm d'épaisseur, ainsi que par une protection cathodique par électrodes sacrificielles.

Figure 3-2 Réservoir sous talus de propane

2.1.1 Dimension

Le RST est constitué par une virole cylindrique terminée à chaque extrémité par une demi-sphère avec un soutirage équipé d'une double enveloppe.

Ses dimensions sont :

- Longueur totale : 33,12 m
- Diamètre externe : 4 m,

Épaisseur du réservoir : 16,4 mm minimum + surépaisseur de 1 mm (protection anticorrosion). Il est notamment équipé de :

- Un tunnel béton de protection des lignes de soutirage,
- Un escalier d'accès au réservoir,
- Un poste de contrôle de protection cathodique du réservoir,
- Une manche à air.

2.1.2 Pressions

Les conditions de dimensionnement retenu sont les suivantes :

- Pression maximale de service : 12 bars relatifs,
- Pression d'épreuve : 18 bars relatifs
- Pression d'utilisation : -0,5 bar à 10 bars relatifs.

2.1.3 Equipements d'exploitation et de sécurité

Les équipements d'exploitation et de sécurité du réservoir sont les suivants :

- Une ligne d'emplissage en pluie en phase liquide de diamètre 4 pouces, équipée de deux vannes motorisées à sécurité positive et à sécurité feu dont l'une est implantée à l'intérieur du réservoir et d'un clapet anti-retour interne,
- Une ligne de soutirage composée de deux canalisations de diamètre 4 pouces (en phase liquide) équipée de 3 vannes motorisées à sécurité positive et à sécurité feu en série. La partie de la canalisation de soutirage comprise entre les parois du réservoir et la première vanne automatique est à double enveloppe.
- Une ligne de retour liquide des pompes de diamètre 2 pouces équipée d'une vanne motorisée
- Externe à sécurité positive et à sécurité feu et d'un clapet anti-retour, en partie haute,
- Une ligne de purge d'un diamètre ¾ pouce en partie basse équipée d'une vanne motorisée à sécurité positive et à sécurité feu, le tronçon situé entre le réservoir sous talus et cette première vanne est protégée par une double enveloppe,
- Une ligne de liaison avec l'aspiration des compresseurs d'un diamètre 3 pouces, équipée d'une vanne
- Motorisée à sécurité positive et à sécurité feu, en partie haute,
- Des piquages avec vannes manuelles, consignées fermées, utilisées lors des opérations de dégazage et de remplissage en eau, pour essai ou intervention, en partie haute,
- Une sonde de pression, en partie haute,
- Une sonde de température, en partie haute,
- Une jauge de niveau en continu avec cadran de lecture locale et avec une transmission associée à 5 seuils d'alarme calés à 7,5% (niveau très bas), 10%

(niveau bas), 84,5% (niveau d'exploitation), 89% (niveau haut), 94% (niveau très haut), en partie haute,

- Une jauge de niveau indépendante avec deux seuils d'alarme, niveau haut à 89% et très haut à 94%,

2.2 Pomperie

Le site dispose des équipements de transfert situés en zone de pomperie :

- Un compresseur dédié au poste de déchargement des camions gros porteurs. Son débit est de 110 m^3/h. Le compresseur dispose d'un piège à liquide (ballon) à son aspiration et d'un pressostat à son refoulement qui déclenche l'arrêt du compresseur à un seuil de 12 bars. Un petit compresseur a été ajouté sur la ligne de chargement des camions afin de récupérer les purges des bras en fin du chargement (Figure 3-3).

Figure 3-3 Compresseur ballon

- Deux pompes d'expédition associées au stockage pour l'alimentation des postes de chargement Ces 2 pompes sont des pompes verticales « à barrel », leur débit unitaire est de 50 m3/h. Chacune des pompes est munie de clapet anti-retour constitué d'une soupape et d'un système de recirculation. Ce dispositif protège les pompes contre les surpressions et leur assure un débit minimum lorsque les clapets sont ouverts. La ligne de recirculation est reliée à la partie supérieure du réservoir. Les pompes sont munies de pressostats dont la fonction est d'assurer

leur protection contre les risques de cavitation en cas de baisse de la pression d'aspiration. Les pompes et le compresseur sont isolables du réseau de canalisation par des vannes manuelles. Ils s'arrêtent sur perte d'énergie électrique.

Figure 3-4 les pompes

2.3 Canalisation

Les canalisations sont aériennes. Leur diamètre est indiqué dans la table ci-dessous :

Table 3-3:Canalisation

Canalisation	État (L : Liquide, G : gazeux)	Diamètre (en pouce)	Longueur (m)
Ligne depuis le réservoir vers les pompes	L	4	20
Ligne depuis les pompes vers les postes de chargement	L	4	35
Ligne de puis le réservoir vers le compresseur	G	3	30
Ligne depuis le compresseur vers le poste de chargement	G	3	27

Les canalisations sont en acier norme NFA 49211 nuance TUE 250 B. Les canalisations phase liquide sont pourvues de soupapes de sécurité montées sur les lignes d'expansion thermiques avec clapet de décharge (retour sur ligne gazeuse). A leurs extrémités, elles sont munies de vannes automatiques à sécurité positive et à sécurité feu au niveau du réservoir, des postes de chargement et de déchargement.
Elles sont toutes reliées à la terre. Les canalisations sont aériennes. Le site est constitué de manière à ce que les canalisations soient protégées de tout risque de collision avec les camions en mouvement sur le site (rack, trottoir). Les canalisations aériennes présentent effectivement des avantages en termes de maintenance et d'inspection et permettent de limiter les risques de corrosion. De plus, l'arrêté ministériel du 2 février 1998 relatif aux prélèvements et à la consommation d'eau ainsi qu'aux émissions de toute nature des installations classées pour la protection de l'environnement soumises à autorisation précise que : « Les canalisations de transport de fluides dangereux ou insalubres et de collecte d'effluents pollués ou susceptibles de l'être sont étanches et résistent à l'action physique et chimique des produits qu'elles sont susceptibles de contenir. Elles sont convenablement entretenues et font l'objet d'examens périodiques appropriés permettant de s'assurer de leur bon état. Sauf exception motivée par des raisons de sécurité ou d'hygiène, les canalisations de transport de fluides dangereux à l'intérieur de l'établissement sont aériennes ».

2.4 Postes de transfert

Les trois postes de transfert sont situés côte à côte, dans une zone spécialement aménagée, desservie par une voie de circulation permettant un accès aux postes en marche avant. Les postes ne sont pas couverts. Un poste de chargement/déchargement et deux postes de chargement sont présents sur cette zone.

2.4.1 Le poste chargement / déchargement

Les camions déchargés sur le site sont des camions gros porteurs d'une capacité de 20 tonnes ; 554 transferts de camions gros porteurs ont été réalisés en 2011. Cette action conduit à l'emplissage du réservoir de stockage sous talus. Le poste alimente le réservoir sous talus via une canalisation aérienne de 100 mm de diamètre. Le

déchargement camions s'effectue par l'intermédiaire d'un bras liquide (2 pouces et d'un bras gazeux (2 pouces).

2.4.2 Les deux postes de chargement

Les camions chargés sont des camions petits porteurs d'une capacité 3,5 tonnes, 6 tonnes ou 9 tonnes. 3319 transferts de camions petits porteurs ont été effectués en 2011. Le remplissage de camions petits porteurs aux postes de chargement s'effectue à partir du réservoir de stockage (sous talus). Ce sont ces camions qui livreront en propane la clientèle de la région. Le chargement des camions s'effectue par l'intermédiaire d'un bras liquide (2 pouces). Les postes sont alimentés par une canalisation aérienne de diamètre 100 mm réduit à 80 mm provenant de la pomperie. Le passage des tuyauteries s'effectue en rack au-dessus du sol afin de réduire les risques liés à la corrosion et aux chocs.

2.4.3 Les équipements de transfert

Le branchement sur les citernes routières est réalisé à l'aide de raccords de type « Rego » ou « Weco ». Un dispositif de purge permet d'évacuer le produit contenu entre la vanne bout de bras et la vanne de la citerne avant chaque débranchement. Chaque bras est équipé :

- D'une vanne manuelle à boisseau sphérique en bout de bras,
- D'un boîtier de rupture (système FLIP-FLAP), qui se rompt instantanément en cas
- D'arrachement du bras, avec fermeture mécanique à chaque extrémité.
- D'une vanne de pied bras à sécurité positive asservie à la détection gaz, feu, aux boîtiers d'alarme, à la mise à la terre du véhicule et à la mise en sécurité du site.
- Les postes de transfert sont également équipés des dispositifs de sécurité suivants :
- Un dispositif d'indentification du chauffeur et du camion-citerne permettant de vérifier si ceux-ci sont autorisés pour le transfert prévu,
- Un bouton d'arrêt d'urgence permettant la mise en sécurité du site,
- L'ouverture du bras est asservie à la détection d'une mise à la terre effective,

- Un système de mise à la terre (DCMT) est implanté sur chaque poste.
- La fermeture des clapets de fond des camions est déclenchée par la fonte d'un fusible thermique, par action sur le frein à main parking du camion, par l'action sur le bouton d'arrêt d'urgence ou par la mise en sécurité du site,
- Un dispositif de collecte des purges des bras au-dessus des soupapes,
- Un dispositif homme-mort (une pression du bouton par le chauffeur est nécessaire toutes les 30 secondes pour poursuivre le transfert).

En outre les camions sont dotés du dispositif CISC « Coupleur Intelligent Sécurité Camion » permettant de coupler la fermeture du clapet de fond des camions à la mise en sécurité du site.

3. Description des opérations de transfert

Le déchargement des camions gros porteurs se fait à l'aide des compresseurs et selon deux phases :

- 1ère phase : la phase gaz du stockage fixe est aspirée, comprimée et injectée dans la phase gaz de la citerne à vidanger. La pression dans la citerne augmente alors et le liquide est chassé vers le stockage ;
- 2ème phase : lorsque toute la phase liquide a été transférée, la vanne liquide est fermée, le sens du transfert du compresseur est inversé au moyen d'une vanne 4 voies. Cette phase permet de dépressuriser la citerne en aspirant une partie de la phase gazeuse vers le stockage. A l'aspiration de chaque compresseur, se trouve un réservoir de condensation destiné à piéger le liquide éventuellement présent dans les lignes. La pression au refoulement des compresseurs est limitée par un pressostat, asservi au compresseur et à une soupape.

Le chargement des camions se fait par le ciel gazeux des citernes (chargement en pluie) à l'aide d'un bras liquide 2 pouces et via une pompe située sur l'aire de pompage. Le déroulement des opérations de chargement et déchargement est détaillé plus précisément au paragraphe suivant.

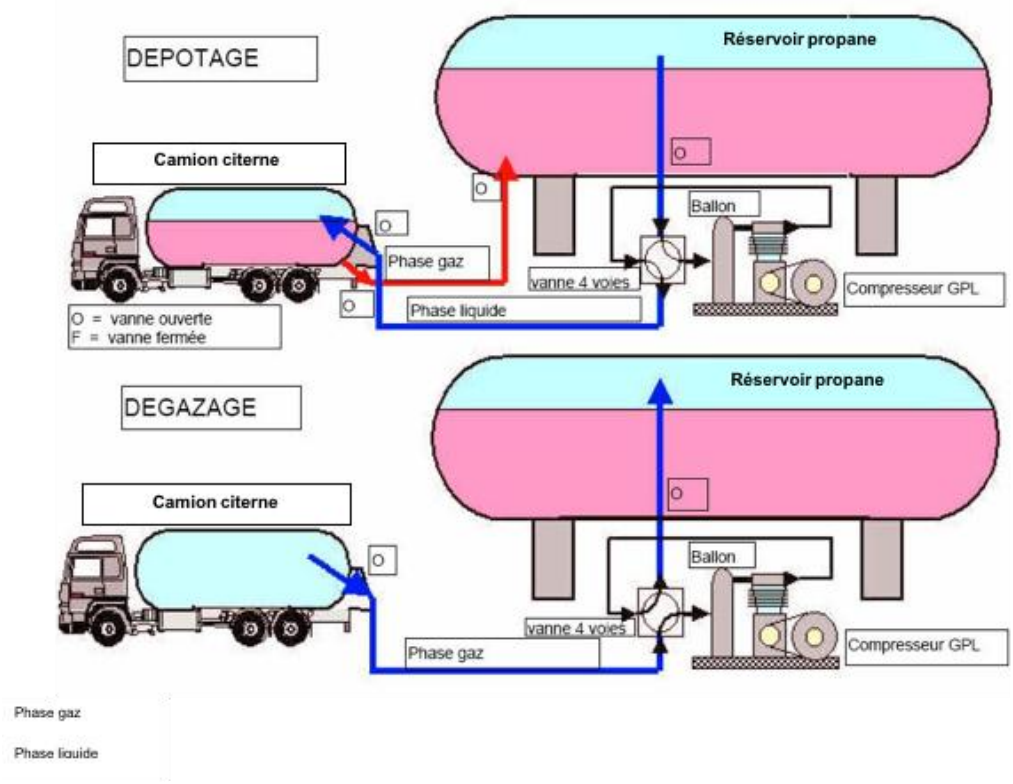


Figure 3-5 Présentation des deux phases de déchargement des camions gros Porteurs

3.1 Procédure de transfert du site

Les dispositions matérielles de fonctionnement en self-service sont assurées par le matériel suivant :

Table 3-4: Les dispositions matérielles

À l'entrée	– Système de télécommande, – Système de mise à la terre et de pare-flamme sur le pot d'échappement (pour les camions non équipés de pot catalytique ou de pare-étincelle intégré)
Sur chaque Poste	– Pont bascule, – Une pince DCMT (Dispositif de Contrôle de Mise à la Terre), – Un CISC (Coupleur Intelligent de Sécurité pour Camion GPL), – Une borne de reconnaissance par badge de type PRECIA, – Un calculateur de type RUBIS S, – Un dispositif « homme mort » (Protection Travailleur Isolé).

Le détail des opérations effectuées est décrit dans les étapes suivantes :

3.2 Identification et déroulement de l'activité de transfert

Le système vérifie :

- Si le chauffeur est autorisé à charger (formation CFBP, …),
- Si la citerne est autorisée et conforme (immatriculation),
- Si le tracteur est autorisé et conforme (immatriculation),
- Si l'opération est autorisée et que les quotas sont respectés (code opération),
- Si le code est reconnu valide, alors le processus d'identification du transfert est terminé.

Un bulletin de chargement est ensuite émis. Le chauffeur se dirige ensuite vers le poste de transfert, conformément au plan de circulation.

3.2.1 Cas opération de chargement

Les opérations de chargement sont effectuées en libre-service chauffeur sous la surveillance du pompiste :

a. Début de chargement
   - Calage du véhicule
   - Branchement de la pince du DCMT sur la citerne (attendre que le voyant blanc s'allume),
   - Branchement du CISC
   - Branchement du bras liquide à l'orifice de remplissage,
   - Ouverture du clapet de fond et la vanne d'emplissage de la citerne,
   - Vérification de l'étanchéité des raccords,
   - Ouverture de la vanne d'extrémité du bras liquide de chargement,
   - Mises-en route de la pompe,
   - Enclenchement du bouton poussoir "Chargement",
   - Le poids chargé s'affiche au poste via une indication fournie par le pont bascule.

b. Fin de chargement

   Lorsque le poids escompté est atteint :

   - Enclenchement du bouton "Arrêt", ou arrêt automatique (par détection que la charge utile est atteinte),

- Les vannes se ferment et les pompes s’arrêtent

c. Débranchement
   - Fermeture de la vanne et du clapet interne du camion,
   - Fermeture de la vanne d'extrémité de bras liquide,
   - Purge de l'extrémité du bras liquide,
   - Débranchement du bras et du CISC puis du DCMT (rangement sur leur support),
   - Émission du bulletin vrac si le chargement est correct.

3.2.2 Cas opération de déchargement

Les opérations de déchargement sont effectuées en libre-service sous surveillance du pompiste :

a. Début de déchargement
   - Calage du véhicule
   - Vérification du bon positionnement de la vanne 4 voies sur la position "déchargement",
   - De l'absence de liquide dans le ballon anti-envahissement,
   - Branchement de la pince du DCMT sur la prise de la citerne (attendre que le voyant blanc s'allume),
   - Branchement du CISC,
   - Branchement des bras liquide et gazeux aux orifices de remplissage (vérification que les deux bras sont bien sortis),
   - Ouverture du clapet de fond et les vannes de la citerne,
   - Vérification de l'étanchéité des raccords,
   - Ouverture de la vanne d'extrémité des bras liquide et gazeux afin d'équilibrer la pression entre le camion et le réservoir,
   - Enclenchement du bouton "Marche" de la télécommande à cordon,
   - Mises-en route du compresseur.

b. Fin de déchargement
   - Enclenchement du bouton "Arrêt",
   - Les vannes de pied de bras se ferment,
   - Arrêt du compresseur,
   - Fermeture de la vanne de la canalisation liquide de la citerne et du bras liquide,

- Passage de la vanne 4 voies du compresseur sur la position "Aspiration",
- Aspiration de la citerne jusqu'à une pression de 2 bar,
- Les vannes de pied de bras se ferment automatiquement,
- Arrêt du compresseur.

c. Débranchement

- Fermeture de la vanne d'extrémité du bras gazeux,
- Fermeture de la vanne de la canalisation gazeuse et les clapets internes du camion-citerne,
- Purge de l'extrémité des bras liquide et gazeux,
- Débranchement des bras (rangement sur leur support),
- Remise des bouchons sur les orifices de la citerne,
- Retour de la vanne 4 voies du compresseur sur la position "Déchargement",
- Débranchement du CISC,
- Débranchement le câble de mise à la terre et l'accrocher sur son support,
- Enlèvement et rangement des cales.

3.3 Méthode de calcul du poids à charger

Il existe plusieurs règles de calcul permettant de déterminer la quantité maximale de GPL à charger. Ces règles sont :

- Le volume de la citerne,
- Le poids à vide de la citerne,
- Le PTCA (Poids Total en Charge Autorisé) du véhicule,
- Le PTR (Poids Total Remorquable) du tracteur,
- Le poids présent sur le pont.

Le volume de la citerne permet, à l'aide d'un coefficient multiplicateur qui dépend du produit chargé, de calculer le poids de la charge maximale de la citerne (respect du ciel gazeux). A cette charge, il faut ôter la différence entre le poids d'entrée et le poids à vide (produit restant dans la citerne).
Le poids de cette charge maximale + le poids à l'entrée du véhicule doit être inférieur au PTCA et au PTR, le poids pris en compte étant le plus bas.

4. Les dispositifs de sécurité

Le site est équipé :

- D’un réseau de détection gaz comprenant 16 détecteurs repartis sur le site, dont les informations sont traitées par une ou des centrales gaz. Ce réseau a été modifié au deuxième semestre 2013 pour inclure 10 nouveaux détecteurs gaz soit un total de 26 détecteurs,
- D’un réseau de détection incendie comprenant 5 détecteurs flamme repartis sur le site, dont les informations sont traitées par une ou des centrales flammes,

- D’alarmes :
  - Protection du travailleur isolé (PTI),
  - Anomalie centrales détection incendie, gaz,
  - Anti-intrusion,
  - Démarrage GMPI.

- D’un réseau d’arrêt d’urgence manuel

- D’instruments de mesure :
  - La mesure de pression du réservoir (pression haute),
  - La mesure de température du réservoir (température haute),
  - La mesure de niveau dans le réservoir (niveau très bas, bas, d’exploitation, haut, très haut),
  - La mesure de niveau indépendante (niveau haut et très haut).
- De vannes automatiques munies de fusibles thermiques, fondant en cas de source de chaleur à proximité et entraînant la fermeture des vannes.

Tous ces dispositifs déclenchent une alarme et certains entraînent la mise en sécurité du site. La mise en sécurité du site correspond à la coupure de l'ensemble des installations électriques non nécessaires à la sécurité, à l'arrêt de tous les transferts et à la fermeture instantanée de toutes les vannes asservies aux dispositifs de sécurités automatiques.

Lors de la coupure électrique, le circuit d’air comprimé est rapidement purgé, il commande alors des électrovannes, fermées en fonctionnement normal de l’installation entraînant :

- L’arrêt des pompes et des compresseurs,
- La fermeture des vannes d’emplissage et de soutirage de la sphère,
- La fermeture des vannes de pieds de bras des postes camions,
- La fermeture des clapets de fond des camions,
- Le démarrage automatique des pompes incendie,
- La mise en pression du réseau incendie,
- Le déclenchement de l’arrosage.

4.1 Arrêts d’urgence (Boutons poussoirs)

L’action manuelle d’un opérateur sur un bouton poussoir déclenche les sécurités suivantes :

- Mises-en purge rapide du circuit d’air comprimé qui commande des électrovannes asservies (normalement fermées) d’où :
- Arrêt des pompes et des compresseurs,
- Fermeture vannes automatiques remplissage et soutirage du réservoir,
- Fermeture vannes automatiques chargement et déchargement camion-citerne,
- Fermeture du clapet de fond des camions,
- Démarrage automatique des pompes incendie,
- Mise en pression du réseau incendie,
- Arrosage des postes de transfert et zone de stationnement des véhicules,
- Intervention de l’exploitant pendant les heures ouvrées, ou envoi d’une alarme vers la société de télésurveillance et intervention de l’astreinte PZF en dehors des heures ouvrées.

Les boutons d’alarme, au nombre de 6 répartis sur l’ensemble du site, sont gérés et les informations centralisées au local T.G.B.T. Le système est à sécurité positive (mise en sécurité du site en cas de défaut).

Les arrêts d’urgence agissent sur la coupure électrique de distribution à l’exclusion de l’éclairage, de l’alimentation du local incendie, des chaînes de détection gaz et flamme, des arrêts d’urgence et du bâtiment administratif.

4.2 Les Détecteurs gaz

La détection de gaz est gérée par centrale d'alarme placée dans la salle de contrôle de l'installation. Le câblage est à sécurité positive (mise en sécurité du site en cas de défaut).

Le site comprend actuellement 16 détecteurs de gaz répartis sur l'ensemble du site (Figure 3-7) ,10 nouveaux détecteurs de gaz ont été installés durant le 2e semestre 2013. 26 détecteurs de gaz seront donc présents sur le site à la fin 2013.

Deux niveaux de déclenchement des détecteurs gaz existent sur le site.

. La chaîne de détection gaz (Figure 3-6) est composée :

- Les détecteurs gaz
- L'unité de traitement des signaux transmis par les détecteurs
- Les actionneurs et les éléments terminaux : les électrovannes, les vannes et les clapets internes des réservoirs

4.2.1 Principe de contrôle du système de détection de gaz

Le contrôle semestriel se fait sur site par le constructeur et concerne les installations complètes de détection gaz (centrales + détecteurs).

Le contrôle consiste en trois étapes :

- Examen des documents d'exploitation,
- Inspection visuelle de l'installation,
- Contrôles techniques et opérations de maintenance : l'étalonnage des détecteurs est effectué à l'aide d'une bouteille de gaz.

Lors de ces contrôles, chaque détecteur est testé par le constructeur. L'essai consiste à vérifier les seuils de déclenchement préalarme/alarme. Une bouteille test contenant un gaz titré composé de butane, d'oxygène et d'azote est ouverte à proximité du détecteur. Il faut alors vérifier que la valeur maximale correspond au pourcentage LIE du mélange contenu dans la bouteille test. Dans le cas contraire, un réglage de gain doit être effectué. Lors des phases de test, tous les détecteurs sont testés par l'activation du capteur jusqu'à la télésurveillance sans mise en sécurité du site. Un capteur privilégié (différent à chaque test) est testé jusqu'à l'automate et le déclenchement des asservissements. Étant donné le câblage de la centrale de détection gaz, le test de

l’ensemble des détecteurs et la mise en sécurité à partir d’un détecteur est satisfaisant pour s’assurer du fonctionnement de la chaîne de détection gaz à partir de n’importe quel détecteur.

4.2.2 Traitement du signal

Le contrôle de la centrale a lieu tous les 6 mois en même temps que celui des détecteurs. Toute la chaîne de mise en sécurité est testée tous les 6 mois.

4.2.3 Les électrovannes

Les électrovannes sont utilisées tous les jours. Ces équipements sont donc régulièrement testés.

4.2.4 Les actionneurs

Les actionneurs sont utilisés tous les jours. Ces équipements sont donc régulièrement testés.

4.2.5 Les vannes

La maintenance et la remise à neuf des vannes automatiques de stockage (IPS) a lieu tous les dix ans. Les vannes sont utilisées tous les jours. Ces équipements sont donc régulièrement testés.

4.2.6 Les caplets internes

La maintenance et la remise à neuf des clapets internes a lieu tous les dix ans.
Tous les 15 jours, la centrale hydraulique est contrôlée visuellement :

- Etanchéité
- Vérification que les niveaux de pression hydraulique sont corrects (entre 34 et 38 bars)
- Resserrage des raccords si besoin

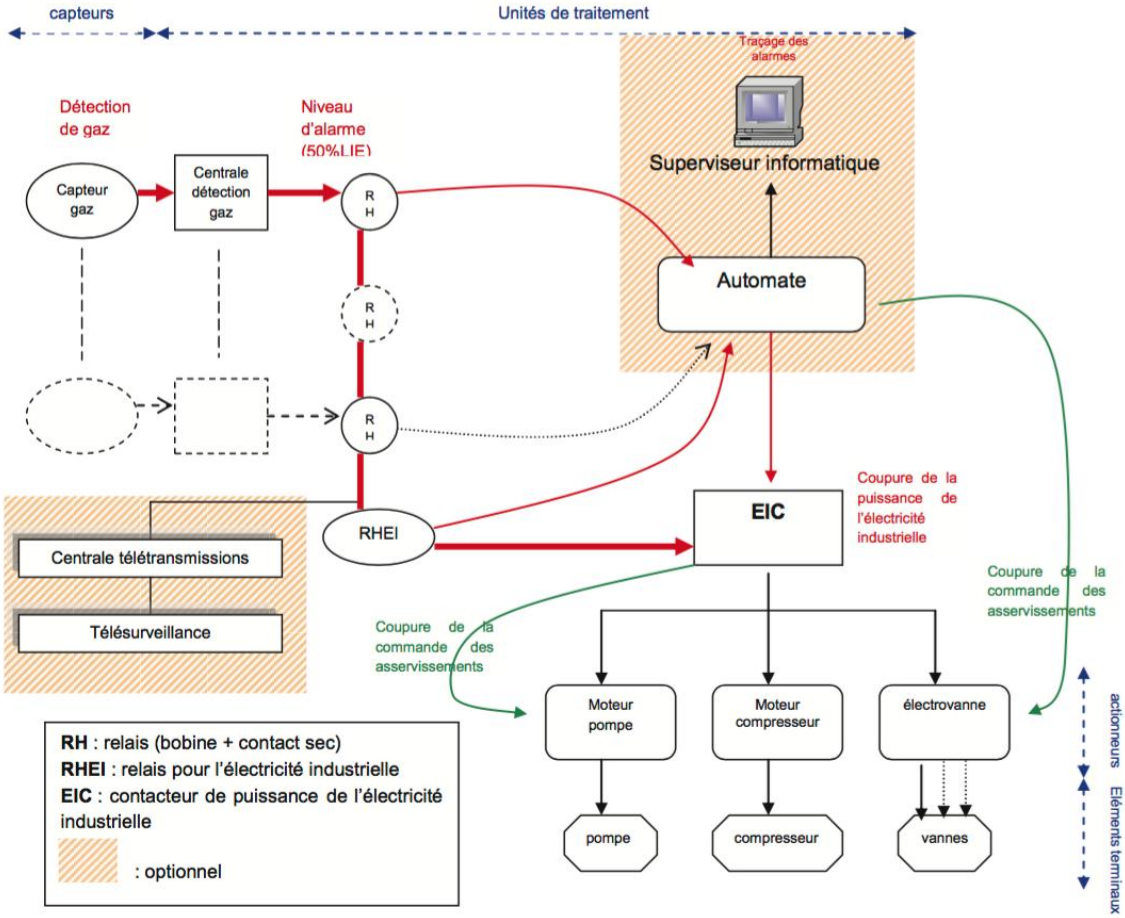


Figure 3-6 La chaîne de détection de gaz

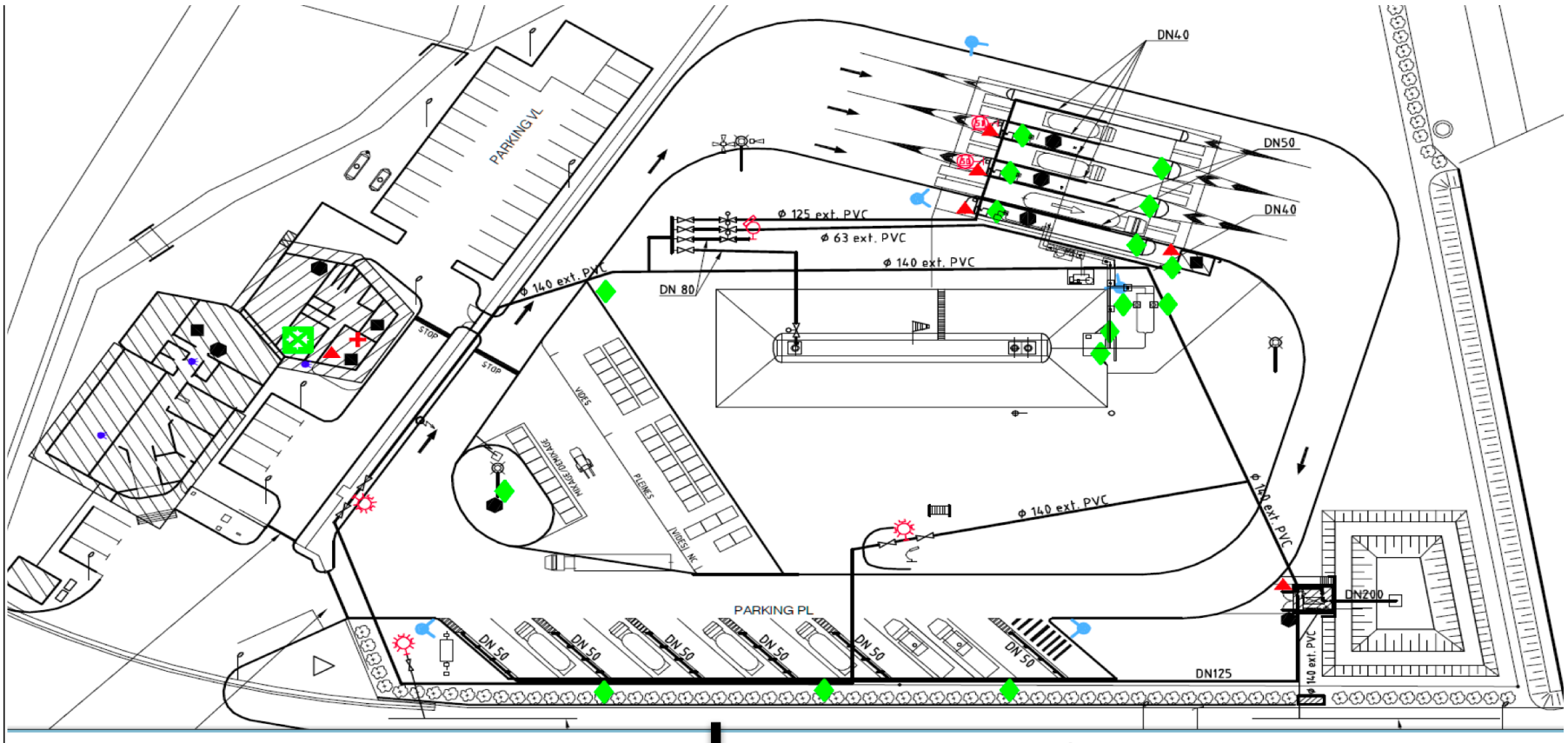


Figure 3-7 Implantation détecteurs

Table 3-5: Cause et conséquence du déclenchement des alarmes de détection fuite de gaz

Alarme	Cause	Conséquence
Préalarme gaz à 20% de la LIE, qui se déclenche suite à une fuite de gaz dont la concentration atteint 20% de la LIE	– Fuite d'un organe de transfert, – Purge en exploitation – Soupape de sécurité en échappement – Joint défectueux	– Arrêt des pompes et des compresseurs gaz, – Fermeture des vannes à sécurité positive, – Fermeture du clapet de fond des camions, – Signal sonore ou visuel, – Consignation sur le superviseur, – Intervention de l'exploitant pendant les heures ouvrées, ou envoi d'une alarme vers la société de télésurveillance et intervention de l'astreinte PZF en dehors des heures ouvrées.
– Alarme gaz à 40% de la LIE qui se déclenche suite à fuite de gaz dont la concentration atteint 40% de la LIE	– Fuite d'un organe de transfert, – Purge en exploitation – Soupape de sécurité en échappement	– Mise en sécurité de l'installation (coupure de l'électricité, fermeture vannes, arrêt des pompes et des compresseurs), – Fermeture du clapet de fond des camions, – Mise sous pression du réseau incendie et déclenchement arrosage, – Sirène d'alarme continue, – Consignation sur le superviseur, – Intervention de l'exploitant pendant les heures ouvrées, ou envoi d'une alarme vers la société de télésurveillance et intervention de l'astreinte PZF en dehors des heures ouvrées.

4.3 Les détecteurs de flammes

La chaîne de détection flamme (Figure 3-8) est composée des éléments suivants :

- Le capteur optique détecte la présence de flammes par variation des fréquences d'oscillation dans la pièce
- L'unité de traitement des signaux
- Les actionneurs et les éléments terminaux : les électrovannes, les vannes, les clapets internes des réservoirs.
- L'arrosage (GMPI, réseau d'eau, réserve incendie)

4.3.1 Principe de contrôle du système de détection de flamme

En interne, les détecteurs sont régulièrement contrôlés visuellement (nettoyage écran capteur …).

Le contrôle semestriel se fait sur site par le constructeur et concerne les installations complètes de détection incendie (centrales + détecteurs). Le contrôle consiste en trois étapes :

- Examen des documents d'exploitation,
- Inspection visuelle de l'installation,
- Contrôles techniques et opérations de maintenance : l'étalonnage des détecteurs est effectué.

Lors des contrôles semestriels, le fournisseur réalise un test de fonctionnement des détecteurs et de toute la chaîne de détection flamme.

Lors des phases de test, chaque détecteur est testé par l'activation du capteur jusqu'à la télésurveillance sans mise en sécurité du site. Un capteur privilégié (différent à chaque test) est testé jusqu'à l'automate et le déclenchement des asservissements.

Étant donné le câblage de la centrale, le test de l'ensemble des détecteurs et la mise en sécurité à partir d'un détecteur est satisfaisant pour s'assurer du fonctionnement de la chaîne de détection flamme à partir de n'importe quel détecteur.

4.3.2 Traitement du signal

Le contrôle de la centrale a lieu tous les 6 mois en même temps que celui des détecteurs. Toute la chaîne de mise en sécurité est testée tous les 6 mois.

4.3.3 Arrosage

Un organisme extérieur réalise une maintenance semestrielle. Une liste des vérifications réalisées (à l'arrêt et en cours d'essai) est remise à l'exploitant.

En interne, le démarrage des GMPI est testé tous les 15 jours, en mode automatique, afin de valider le démarrage du groupe motopompe ainsi que la mise en pression du réseau incendie sur un déclenchement d'alarme. Un contrôle des bassins est réalisé tous les trois ans : nettoyage et curage du bassin état de la bâche.

4.3.4 Les conséquences suite à la détection de flamme

L'alarme incendie est gérée par une centrale. Le site comprend 5 détecteurs de flamme répartis sur l'ensemble du site. L'implantation des détecteurs flamme est présentée en (Figure 3-7). Sur détection d'une flamme, les sécurités suivantes se déclenchent :

- Mise en sécurité de l'installation (coupure de l'électricité, fermeture vannes, arrêt des pompes et des compresseurs),
- Fermeture du clapet de fond des camions,
- Mise sous pression du réseau incendie et déclenchement arrosage,
- Sirène d'alarme continue,
- Consignation sur le superviseur,
- Intervention de l'exploitant pendant les heures ouvrées, ou envoi d'une alarme vers la société de télésurveillance et intervention de l'astreinte PZF en dehors des heures ouvrées.

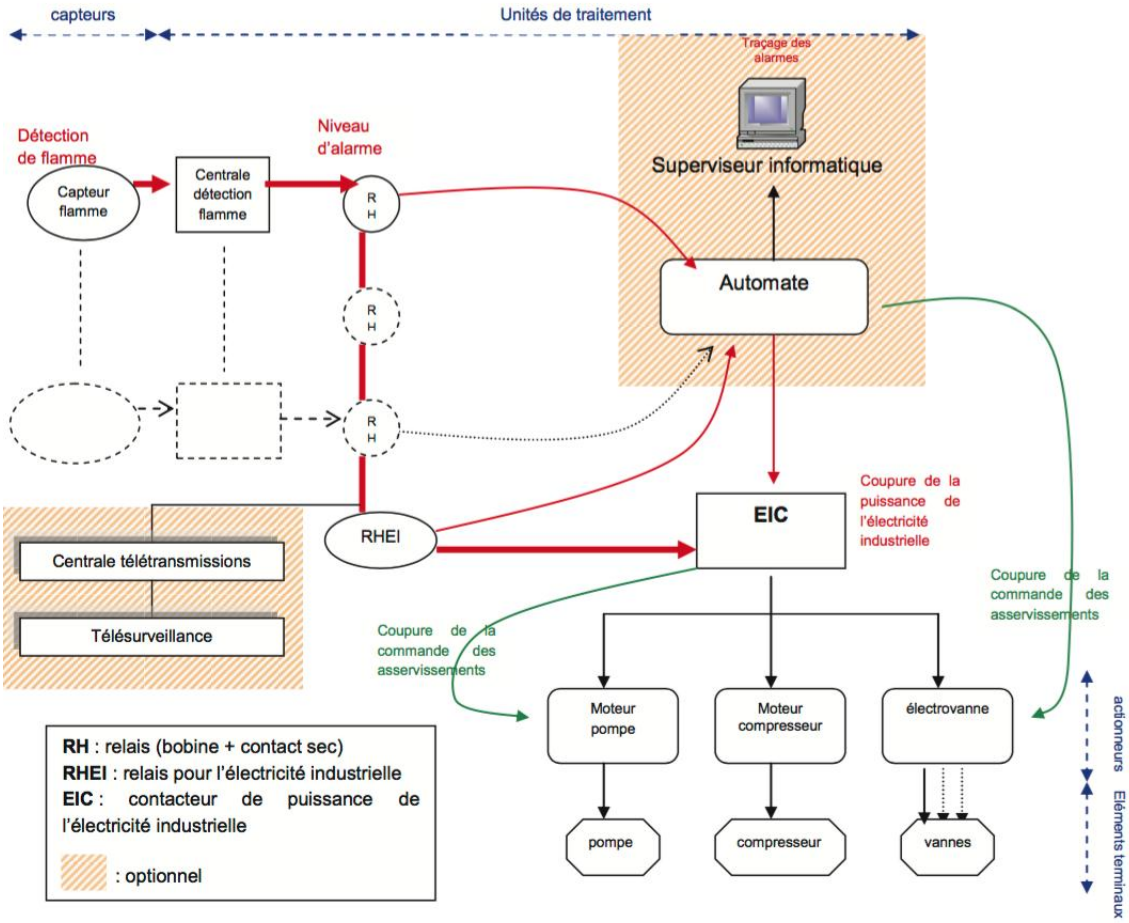


Figure 3-8 La chaîne de détection de flamme

4.4 Alarmes techniques du réservoir sous-talus

La quantité de matière dangereuse présente sur site ne doit pas dépasser les 200 tonnes. Des détecteurs de niveau sont implémentés au niveau du réservoir. Une mesure de niveau est effectuée pour détecter la présence de liquide en un point donné. Lorsqu'il est atteint, un signal est envoyé à un système de commande qui permet la mise en sécurité du site (cas d'un niveau haut 89% ou très haut 94%). La chaîne de niveau est composée des éléments suivants :

- Mesure du niveau
- L'unité de traitement des signaux
- Les actionneurs et les éléments terminaux : arrêt du compresseur et fermeture des vannes d'emplissage (électrovanne et actionneur de vanne)

Table 3-6: Cause et conséquence du déclenchement des alarmes de niveau RST

Alarme	Déclenchement	Les sécurités associées
Alarme « Niveau Haut »	L'alarme de niveau haut se déclenche en cas de remplissage à 89 % du réservoir.	– Arrêt de l'opération de déchargement camions (arrêt compresseur et fermeture des vannes automatiques de la ligne d'emplissage du RST), – Fermeture du clapet de fond des camions, – Signal sonore, – Consignation sur le superviseur, – Intervention de l'exploitant pendant les heures ouvrées, ou envoi d'une alarme vers la société de télésurveillance et intervention de l'astreinte PZF en dehors des heures ouvrées.
Alarme « Niveau Très Haut »	L'alarme de niveau très haut se déclenche en cas de remplissage à 94 % du réservoir et de dysfonctionnement du niveau haut.	– Mise en sécurité de l'installation (coupure de l'électricité, fermeture de toutes les vannes automatiques, arrêt des pompes et des compresseurs), – Fermeture du clapet de fond des camions, – Mise en pression du réseau incendie, – Sirène d'alarme continue, – Consignation sur le superviseur, – Intervention de l'exploitant pendant les heures ouvrées, ou envoi d'une alarme vers la – Société de télésurveillance et intervention de l'astreinte PZF en dehors des heures ouvrées.
Alarme « Niveau Exploitation »	L'alarme de niveau d'exploitation se déclenche en cas de remplissage à 84,5 % du réservoir.	– Mise en sécurité de l'installation (fermeture des vannes à sécurité positive, arrêt du compresseur), – Sirène d'alarme continue, – Consignation sur le superviseur, – Intervention de l'exploitant pendant les heures ouvrées, ou envoi d'une alarme vers la société de télésurveillance et intervention de l'astreinte PZF en dehors des heures ouvrées.
Alarme « Niveau Bas »	L'alarme de niveau bas se déclenche en cas de remplissage à 10 % du réservoir	– Sirène d'alarme continue, – Consignation sur le superviseur, – Intervention de l'exploitant pendant les heures ouvrées, ou envoi d'une alarme vers la société de télésurveillance et intervention de l'astreinte PZF en dehors des heures ouvrées.
Alarme « Niveau Très Bas »	L'alarme de niveau très bas se déclenche en cas de remplissage à 7,5 % du réservoir.	– Sirène d'alarme continue, – Consignation sur le superviseur, – Intervention de l'exploitant pendant les heures ouvrées, ou envoi d'une alarme vers la société de télésurveillance et intervention de l'astreinte PZF en dehors des heures ouvrées.
Alarme « Pression Haute »	L'alarme de pression haute se déclenche lorsque la pression est égale à 10,8	– Sirène d'alarme continue, – Consignation sur le superviseur, – Intervention de l'exploitant pendant les heures ouvrées, ou envoi

	bar.	d'une alarme vers la société de télésurveillance et intervention de l'astreinte PZF en dehors des heures ouvrées.
Alarme "Température haute"	L'alarme de température haute se déclenche lorsque la température dans le réservoir est égale à 35°C.	– Alarme sonore, – Consignation sur le superviseur, – Intervention de l'exploitant pendant les heures ouvrées ou/et intervention de l'astreinte PZF en dehors des heures ouvrées.

5. Conclusion

Ce chapitre décrit le système d'étude qui va faire l'objet d'une analyse STPA dans le chapitre suivant. Nous avons présenté la réglementation européenne relative aux établissements industriels les plus dangereux (dits « Seveso ») qui impose aux États membres de prendre des mesures pour que la sécurité de leurs établissements. Nous avons décrit le site industriel en présentant sommairement des différents composants techniques

CHAPITRE 4: DEMARCHE DE MODELISATION STPA

Ce chapitre présente l'analyse des risques sur un site de stockage/distribution de Gaz Propane Liquide (GPL). Le système de contrôle de sécurité de l'installation est automatisé, les opérateurs peuvent intervenir pour l'arrêt d'urgence de l'installation (boutons poussoirs). On se contente dans ce chapitre de présenter la démarche STPA (Systems-Theoretic Process Analysis) pour modéliser les systèmes de contrôle/commande qui permettent l'arrêt de fonctionnement de l'installation en cas d'urgence. Pour cela, nous allons exposer la démarche adoptée et expliquer son déploiement pour le site de stockage de GPL.

1. Explication brève de la démarche STPA

STPA dispose d'un ensemble de procédures bien déterminées pour extraire les informations relatives à un système, et établir l'analyse qui sert à identifier les actions à risques générées par les systèmes de contrôle (automatisées, ou semi automatisées en présence de superviseurs humains) des installations. La démarche STPA débute d'abord par l'identification des accidents et des dangers en lien avec les accidents. Il s'agit ensuite de construire une structure de contrôle hiérarchique qui tient compte des contraintes de sécurité. Ainsi les résultats d'une analyse STPA peuvent servir à évaluer la sécurité d'un système déjà existant, ou à émettre des exigences de sécurité d'un système en phase de conception.

1.1 Identification des accidents

Comme nous l'avons vu, l'approche scientifique et d'ingénierie de la sécurité des systèmes repose sur l'identification des accidents et des pertes à éviter. En général, l'inventaire des accidents est établi par l'exploitant, des focus groupes, des compagnies d'assurance, des sociétés professionnelles, des organisations normatives, et l'Etat pour les installations réglementées par les organismes gouvernementaux. L'accident est défini comme un événement non planifié et indésirable conduisant à des blessures, des pertes de vies humaines, des dégâts matériels, des pertes d'exploitation, de la pollution de l'environnement et l'échec de la mission relative à la gestion de sécurité.

Les accidents sont décrits en fonction d'une situation ultime à éviter et non sous forme d'évènements intermédiaires. Par exemple, la fuite sur une bride[6] (une des composantes du système GPL) ne représente pas un accident au niveau de l'intégralité du système technique, cependant cela reste bien une cause d'accident au niveau d'un composant du système.

Dans un site de stockage distribution de GPL, les accidents généralement considérés concernent la perte de confinement, l'exposition des opérateurs ou de la population à l'extérieur du site à des fuites nocives, la perte de l'activité de stockage et de distribution, la perte des installations et servitudes techniques, etc.

1.1.1 Délimitation du cadre du système d'étude

En se basant sur ce qui précède, il est important de délimiter les frontières du système d'étude dans la démarche d'identification des risques et des dangers du système. L'exploitant peut ainsi identifier les conditions dangereuses du système ou les conditions dangereuses faisant partie de l'environnement du système. Afin de faciliter la délimitation du système, l'exploitant peut recourir à cette posture qui est celle d'étudier les conditions qui peuvent être maîtrisées et contrôlées sur le plan de l'ingénierie des systèmes. La conception des systèmes de sécurité suppose d'éliminer ou de contrôler les dangers et d'éviter ainsi les accidents. La démarche de maîtrise et de contrôle des dangers doit alors être une partie intégrante de la conception du système. Cette exigence de contrôle est la raison qui mène à distinguer entre les dangers et les accidents : les accidents impliquent certains aspects de l'environnement sur lequel le concepteur du système ou l'exploitant n'a aucun contrôle.

Une fois les frontières du système délimitées, les concepteurs de systèmes ont la mission d'implémenter les exigences de sécurité, d'assurer la maîtrise des dangers et le contrôle du système. Concernant l'établissement de stockage/distribution de GPL étudié, un exemple d'évènement indésirable serait la mort ou les blessures des opérateurs du site et des habitants autour de l'installation (évènement de perte de vie

[6] Une bride est un organe mécanique de blocage utilisé en tuyauterie ou en plomberie pour assembler des organes hydrauliques tels que des tubes, des vannes, des clapets, des robinets et des instruments de mesure.

humaine). Il existe plusieurs facteurs impliqués dans de telles pertes qui sont indépendants de la volonté des concepteurs de l'installation et de l'exploitant, comme par exemple les conditions atmosphériques telles que la vitesse ou la direction du vent au moment de la libération de matière dangereuse. D'autres facteurs sont impliqués lors d'un accident, par exemple les facteurs liés à l'urbanisation et le nombre de populations exposées installées autour de l'installation. En France, pour les ICPE (Installations Classées Pour l'Environnement) ces facteurs peuvent être sous le contrôle de l'autorité locale ou de l'État. Les concepteurs des ICPE ont la responsabilité de fournir les informations nécessaires pour la conception et le fonctionnement des équipements, d'établir des plans et des procédures appropriées aux situations d'urgence. Sa responsabilité première est de concevoir et d'implémenter des dispositifs qui empêchent toutes pertes de confinement.

Les conditions environnementales qui contribuent à l'accident peuvent changer au fil du temps. L'établissement potentiellement dangereux peut être initialement situé loin d'une concentration de population, mais au cours d'un certain temps, les populations ont tendance à s'installer autour de l'installation afin de vivre à proximité de leur emploi par exemple ou parce que les prix des terrains peuvent être moins élevés dans les régions éloignées ou à proximité des usines. Le concepteur de l'installation n'a généralement aucun contrôle sur ce phénomène de déplacement des populations ainsi, on peut considérer le système délimité par l'établissement de stockage et qualifier de risque tout rejet non contrôlé de GPL de l'installation. Si la conception d'un système de contrôle de la sécurité est envisagée pour l'ensemble du système sociotechnique, le concepteur doit évaluer qu'il y a un nombre plus important de risques et de dangers potentiels et qu'il y a une augmentation des mesures de prévention. Par exemple le concepteur peut demander par le biais de la réglementation liée au zonage du territoire de limiter les bâtis autour du site ou de prévoir des plans d'évacuation d'urgence et de prise en charge médical suite à un accident. L'objet de cette discussion est d'expliquer en quoi la définition des dangers associés à un système est une mesure arbitraire mais importante permettant de garantir la sécurité du système et en quoi un effort d'ingénierie est nécessaire pour étudier l'ensemble du système sociotechnique. Une des premières étapes de conception d'un système, après la définition d'un accident ou de la perte et la délimitation des frontières des sous-systèmes, est d'identifier les risques et les

dangers qui doivent être éliminés ou contrôlés par les concepteurs de ce système ou sous-système.

1.2 Identification des dangers

La théorie des systèmes et les *Safety Science*s, définissent un danger comme la situation d'un système où un ensemble de conditions environnementales défavorables menant à l'accident : Danger + conditions environnementales ⇒ Accident (Perte).

D'après cette définition un danger peut donc être expliqué sous la forme de conditions et d'évènements. La figure 4-1, explique que la différence entre les événements et les conditions résident dans le fait que les événements sont limités dans le temps, alors que les conditions persistent et changent quand un événement se produit.

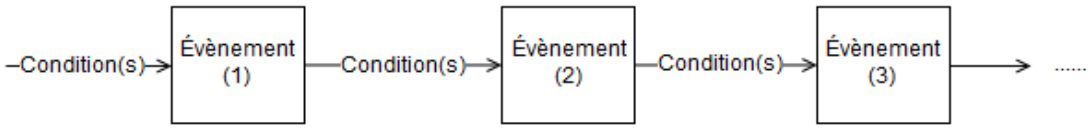


Figure 4-1 Conditions et évènements

Par exemple sur un site de stockage de GPL, le danger serait la fuite de matière dangereuse confinée (évènement) ou la présence d'une source d'ignition dans l'environnement (condition).

1.3 La structure de contrôle organisationnel (hiérarchique)

La structure de contrôle organisationnel est un modèle hiérarchique qui détaille les fonctionnalités de contrôle et les modes d'application des contraintes de sécurité d'un système. Dans le cas où le système est encore en phase de conception, selon STAMP, on peut envisager un premier modèle de structure hiérarchique de contrôle d'ordre général ou dit de haut niveau (*high level*). Il faut ensuite l'affiner au fur et à mesure que les décisions concernant la conception de la sécurité du système sont mieux définies, en se basant sur les résultats de l'analyse des risques STPA qui détaille les fonctionnalités de contrôle et les modes d'application des contraintes de sécurité d'un système.

Selon STAMP la structure de contrôle de la sécurité doit être hiérarchique, de sorte que pour un niveau élevé donné, le contrôleur doit assurer ses responsabilités en déclenchant les actions commandées de contrôle du processus ou du contrôleur du niveau hiérarchique inférieur. Le feedback est communiqué par les composants de niveau inférieur aux contrôleurs de niveau supérieur pour décider du type d'action commandée à fournir (Figure 4-2).

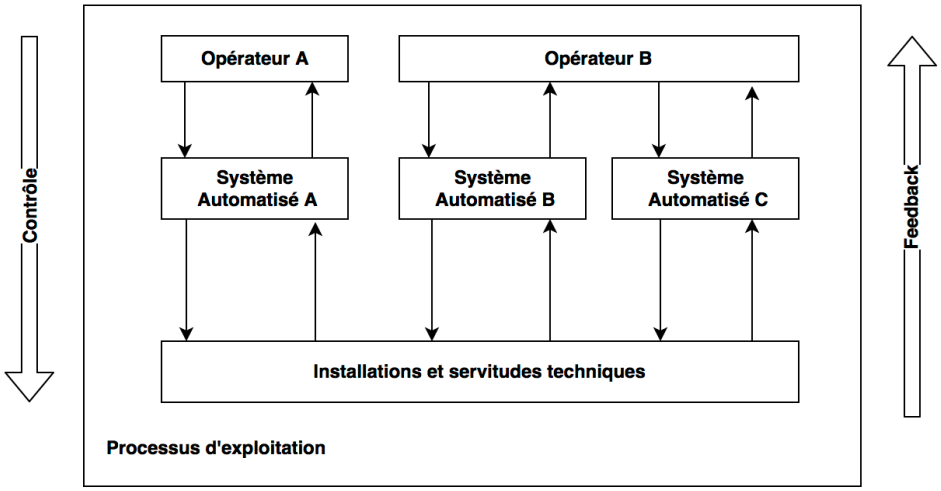


Figure 4-2 Structure de contrôle du processus d'exploitation et d'opération

Le processus physique de l'installation est considéré comme étant le niveau hiérarchique de base de la structure. Pour un système bien déterminé, la modélisation structure de contrôle de sécurité consiste à identifier les systèmes de contrôle / opérateurs de contrôle et leurs responsabilités en matière de sécurité. Les flèches (vers le bas) représentent les actions de contrôle, les flèches (vers le haut) les rétroactions, d'autres voies de communication de la structure sont nécessaires pour assumer les responsabilités liées à la sécurité.

Les modèles de processus doivent également être définis. Comme indiqué précédemment, chaque système de contrôle contient un modèle guide pour le contrôle du processus appelé « modèle de processus ». Le modèle de processus est utilisé par les contrôleurs pour déterminer les mesures de contrôle nécessaires. Par conséquent, le modèle de processus doit contenir les informations qui permettent au contrôleur de prendre les décisions qui préservent la sécurité du système.

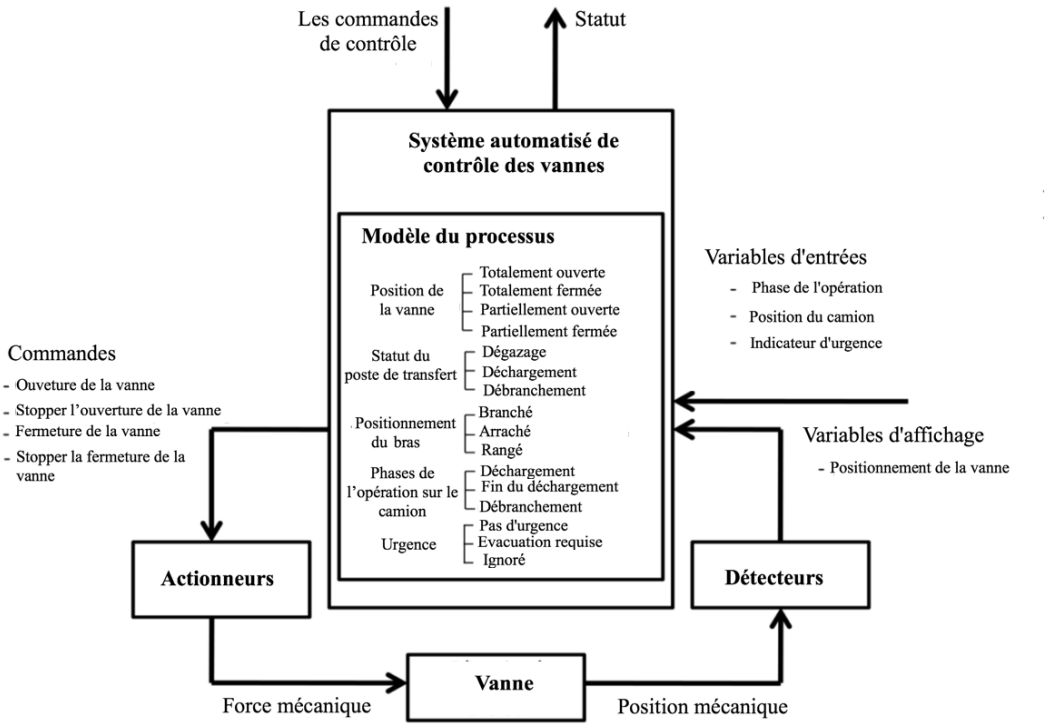


Figure 4-3 Boucle de contrôle de la sécurité

La figure 4-3 montre les modèles des processus requis pour commander le fonctionnement des vannes. Sur les bases du modèle des processus, le système de contrôle lance une action commandée.

En fonction des valeurs des variables du modèle de processus, on peut évaluer si les commandes émises par le système de contrôle sont potentiellement dangereuses. Par exemple, l'instruction « ouverture de la vanne » peut être dangereuse dans un contexte où les valeurs des variables du modèle des processus sont : « le camion est stoppé, pas d'urgence, le bras de transfert est arraché ».

Dans ce contexte, l'ouverture de la vanne est une mesure dangereuse. Cette structure nous permet par la suite d'identifier les dangers générés par une action commandée par le système automatisé et les dangers dans le cas de l'inaction du système automatisé.

1.4 Identification des dangers sur les instructions contrôles-commandes du système (étape 1)

Chaque système peut générer une commande et contrôler le comportement du processus. Dans le diagramme de la structure de contrôle, les flèches vers le bas désignent les actions de contrôle exercées par le système, les flèches vers le haut représentent le transfert d'information Nécessaire pour contrôler le comportement du processus.

.

1.4.1 La méthode simplifiée

STAMP classifie le danger des instructions contrôles/commandes selon les critères suivants :

1) Une action commandée requise n'est pas déclenchée par le système de contrôle

2) Une action commandée déclenchée génère un danger

3) Une action commandée requise pour la sécurité est déclenchée hors séquence, trop tôt ou trop tard

4) Une action commandée requise pour la sécurité est longuement déployée ou interrompue prématurément

Table 4-1: Les actions de contrôle dangereuses

Action de contrôle	**1) N'est pas initiée**	**2) Est initiée**	**3) Est initiée hors séquence, trop tôt ou trop tard**	**4) Longuement déployée ou interrompue prématurément**
Ouverture des vannes d'extrémité des bras liquide et gazeux	Les vannes d'extrémité des bras liquides et gazeux ne sont pas commandées ouvertes afin d'équilibrer la pression entre le camion et le réservoir,	Sont commandées ouvertes pendant l'arrachement du bras	Sont commandées ouvertes trop tard après la mise à la terre (L'ouverture des vannes du bras est asservie à la détection d'une mise à la terre effective,)	N/A

Pour évaluer les actions commandées par les systèmes de contrôle, il faut éviter de supposer que les barrières de sécurité implémentées au sein du système sont fiables et appropriées. L'analyse STPA tend à divulguer les comportements qui peuvent générer un danger dans un contexte défavorable. Les conditions défavorables sont les cas où les barrières de sécurité implémentées au sein du site ne fonctionnement pas correctement.

1.4.2 Méthode dite systématique

Selon cette méthode, l'approche adoptée pour évaluer les actions commandées par les systèmes de contrôle, suppose, par hypothèse, que chaque action de contrôle n'est pas dangereuse par nature. Par exemple, l'instruction ouverture de la vanne d'extrémité du bras de chargement, est une commande sans danger cependant elle peut s'avérer dangereuse dans un contexte bien déterminé. L'ouverture de la vanne d'extrémité du bras de chargement suite à un arrachement de bras est une action dangereuse. Il est nécessaire que le contrôleur soit guidé par un modèle de processus pour initier toute action commandée.

Le modèle de processus regroupe les informations sur lesquelles doit se baser le contrôleur pour prendre les décisions nécessaires à la sécurité du système.

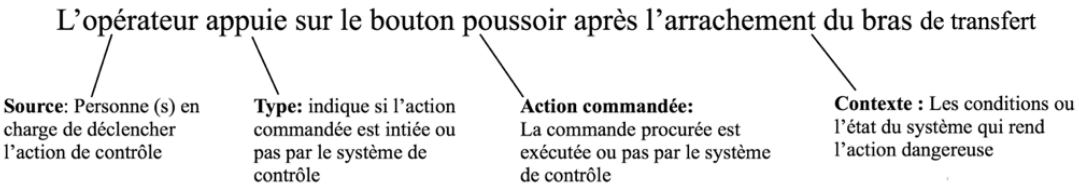


Figure 4-4 Composition d'une action dangereuse

La première étape de la méthode dite systématique consiste pour une action de contrôle donnée de construire un tableau de contextes.

Table 4-2: Tableau de contextes concernant une action de type fournie par le système de contrôle

Action de Contrôle (AC)	Mouvement du camion	Urgence	Positionnement du bras	Dangers ?		
				AC fournie à tout moment dans ce contexte	AC fournie trop tôt dans ce contexte	AC fourni trop tard dans ce contexte
Ouverture de la vanne	Camion en mouvement	Pas d'urgence	Rangé	Oui	Oui	Oui
	Camion en mouvement	Urgence	Rangé	Oui	Oui	Oui
	Camion est stoppé	Urgence	Rangé	Oui	Oui	Oui
	Camion est stoppé	Pas d'urgence	Arraché	Oui	Oui	Oui
	Camion est stoppé	Pas d'urgence	Branché	Non	Non	Non

Chaque ligne du tableau 4-2 permet d'évaluer et de déterminer si l'action de contrôle est dangereuse dans un contexte donné. Les résultats de l'évaluation sont indiqués par un « oui » ou un « non ». Il est possible de faire un tableau pour montrer les dangers dans le cas où cette même action de contrôle n'est pas fournie par le système de contrôle.

Chaque colonne du tableau précise le contexte dans lequel la commande « ouverture de la vanne » peut être lancée par le système automatisé. Le contexte est déterminé à partir des valeurs du modèle des processus. Selon le contexte, on peut ensuite déterminer si l'action de contrôle est dangereuse ou sans danger. Les trois colonnes de droite du tableau contiennent les résultats de l'évaluation. Le tableau montre que la commande « ouverture de la vanne » dans un contexte de situation d'urgence et un camion sur poste est dangereuse.

Il est également nécessaire de déterminer les contextes dans lesquels l'inaction du système automatisé peut s'avérer dangereux. La même démarche de base est adoptée : identifier les variables, du modèle des processus, correspondantes, et les valeurs potentielles, puis déterminer si l'inaction peut s'avérer dangereuse dans un contexte donné.

Table 4-3: Tableau de contextes l'inaction du système automatisé

Action de Contrôle (AC)	Mouvement du camion	Urgence	Positionnement du bras	Statut du transfert	Danger si elle n'est pas fournie
Ouverture de la vanne n'est pas initiée	Camion stoppé	Pas d'urgence	Branché	Déchargement	Non
Ouverture de la vanne n'est pas initiée	Camion stoppé	Pas d'urgence	Arraché	Déchargement	Non
Ouverture de la vanne n'est pas initiée	Camion stoppé	Pas d'urgence	Branché	Dégazage	Oui
Ouverture de la vanne n'est pas initiée	Camion stoppé	Pas d'urgence	Arraché	Dégazage	Non
Ouverture de la vanne n'est pas initiée	Camion stoppé	Urgence	Rangé	Débranchement	Non
Ouverture de la vanne n'est pas initiée	Camion stoppé	(Peu importe)	Rangé	Débranchement	Non

La prochaine étape consiste à énoncer les contraintes de sécurité à partir des résultats obtenus concernant les dangers au niveau des actions commandées par le système.

1.5 Énoncer les exigences et les contraintes de sécurité

A la suite de l'étape précédente il est possible de fixer les contraintes (exigences et mesures) de sécurité qui doivent être appliquées pour empêcher les accidents. Par exemple pour une Commande Dangereuse (CD) donnée, on définit une Contrainte de Sécurité (CS) :

- **CD 1 :** Les vannes sont commandées ouvertes pendant l'arrachement du bras de transfert
- **CS1 :** Les vannes ne doivent pas être en position ouverte suite à l'arrachement du bras de transfert

La suite de la démarche STPA consiste à évaluer la structure de contrôle de la sécurité pour comprendre comment sont initiées les actions dangereuses et pourquoi les

actions requises pour préserver la sécurité du système ne sont pas mises en œuvre (étape 2).

Une fois que les contraintes de sécurité sont définies, il faut identifier les facteurs qui peuvent contribuer à la violation des contraintes de sécurité. La figure 4-5 montre la boucle de contrôle où sont indiqués en général les types de facteur de causalité d'un éventuel accident. Dans la figure, la ligne diagonale en bleu sépare deux façons qui se complètent pour comprendre les facteurs de causalité liées à la violation d'une contrainte de sécurité :

– L'action commandée fournie par le contrôleur est dangereuse (partie supérieure de la ligne diagonale bleue)

– L'action commandée (sans danger) fournie par le contrôleur n'est pas exécutée (partie inférieure de la ligne diagonale bleue)

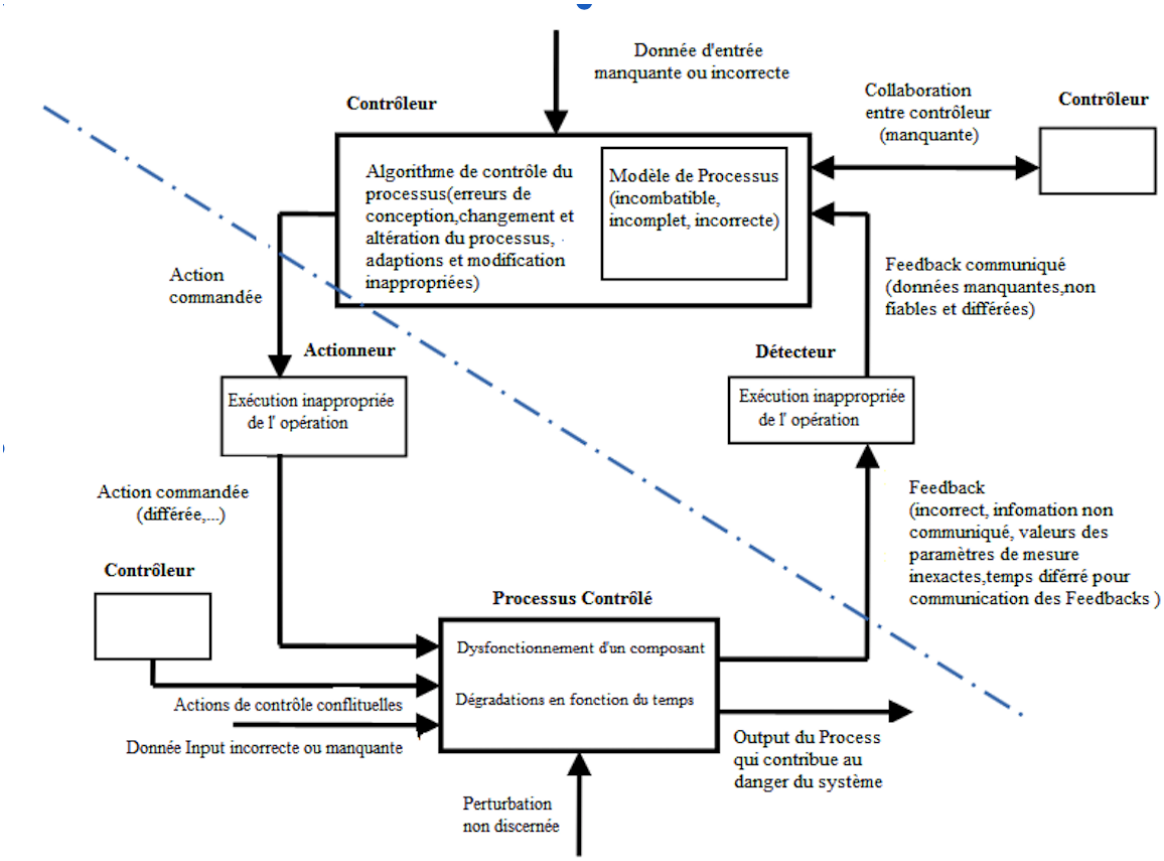


Figure 4-5 Classification des fateurs de causalité contribuants aux dangers

Selon la démarche STPA, il faut étudier chacun des cas et identifier tous les facteurs qui contribuent à la violation des contraintes de sécurité.

1.5.1 L'action commandée fournie par le contrôleur ou le système de contrôle est dangereuse

Tous les facteurs qui peuvent déclencher une action à risque doivent être identifiés. Par exemple pour l'action commandée suivante :

- **CD 1 :** Les vannes sont commandées ouvertes pendant l'arrachement du bras de transfert.

Le système de contrôle ou le contrôleur se base sur le modèle de processus pour émettre les actions commandées. Un modèle de processus incomplet et incohérent peut générer des commandes dangereuses issues du système de contrôle. Concernant l'exemple discuté dans cette partie, le contrôleur peut avoir une information sur la position ouverte d'une vanne contraire à la réalité au niveau technique de l'installation (vanne fermée). La raison des failles dans un modèle de processus est irrémédiablement liée au feedback incorrect, la défaillance des détecteurs, données communiquées en temps différé. Différents scénarios peuvent être développés pour essayer de comprendre les causes d'un accident en étudiant l'interaction entre les différents composants du système.

1.5.2 L'action commandée fournie est appropriée et requise, cependant elle n'est pas appliquée ou exécutée correctement

Il faut identifier les facteurs qui contribuent à la violation des contraintes de sécurité lorsqu'une action commandée appropriée est fournie par le système de contrôle.

1.6 Développer des recommandations à partir des causes identifiées

Pour un système en phase de conception, l'étude des facteurs de causalité peut servir pour élaborer les exigences de sécurité. L'étude d'un système en phase de développement et opération, suppose de vérifier si les facteurs de causalité présentés dans le paragraphe 1.6 ont é traités dans la phase conception. On peut alors vérifier si le travail de conception des barrières de sécurité empêche les accidents dans le système.

1.7 Evaluer les composants de la structure hiérarchique

Au départ, l'approche STPA suppose la modélisation de la structure de contrôle de la sécurité du système d'un point de vue macroscopique. Les actions de contrôle et les feedbacks sont représentés à un niveau d'ordre général. Chaque étape de la démarche STPA peut être appliquée par une approche itérative en mode top-down pour intégrer des contraintes de sécurité selon les besoins.

2. L'étude de cas

L'étude de cas pour les travaux de recherche concerne l'application de la démarche STPA sur un site de stockage de GPL. Le contrôle de la sécurité dans ce site de stockage est automatisé et nécessite dans certains cas l'intervention d'un opérateur.

Dans cette section, la démarche porte uniquement sur les opérations de déchargement des gros porteurs effectuées au sein du site. Cette même démarche peut être transposée sur l'ensemble du système (management, maintenance, conception et développement) ainsi que le chargement des petits porteurs. Le diagramme générique de l'installation technique est représenté dans la figure 4-6. Hors opération de transfert, l'activité du site se limite aux opérations de stockage de GPL et aux opérations de maintenance de l'installation. Le GPL est maintenu liquéfié à température ambiante sous pression de vapeur saturante dans un réservoir sous talus à axe horizontal de capacité nominale de 400 m^3. Les valeurs de la pression d'utilisation sont définies sur un intervalle compris entre [0,5 ; 10] bars, ces valeurs correspondent à la pression de service. La pression maximale de service est relativement de 12 bars, cette pression correspond à la pression dynamique la plus élevée en régime permanent sur le réseau (hors coup de bélier). C'est la pression que l'installation ne doit pas dépasser pendant son utilisation nominale. La valeur de la pression d'épreuve est approximativement de 18 bars. Elle correspond à la pression appliquée à l'installation pendant les opérations de maintenance dans le but de vérifier l'intégrité physique de l'installation. Sur le réseau d'emplissage, il existe deux vannes auxquelles l'exploitant a attribué le même nom (vanne d'emplissage, vanne automatique, vanne automatique de remplissage, vanne motorisée à sécurité positive, vannes motorisées à sécurité positive et à sécurité feu,

vanne à sécurité positive). L'une de ces vannes est implémentée à l'intérieur du réservoir suivi d'un caplet anti-retour interne. Ces vannes automatiques sont munies de fusibles thermiques fondant en cas de source de chaleur à proximité entrainant la fermeture de ces vannes. En cas de coupure d'électricité suite à la mise en sécurité du site, le circuit d'air comprimé est rapidement purgé, il commande alors les électrovannes[7] qui provoquent la fermeture de ces vannes, du compresseur et de la pompe. La ligne de liaison du réservoir avec le compresseur[8] 110m3/h d est équipée de ce même type de vanne (Figure 4-6).

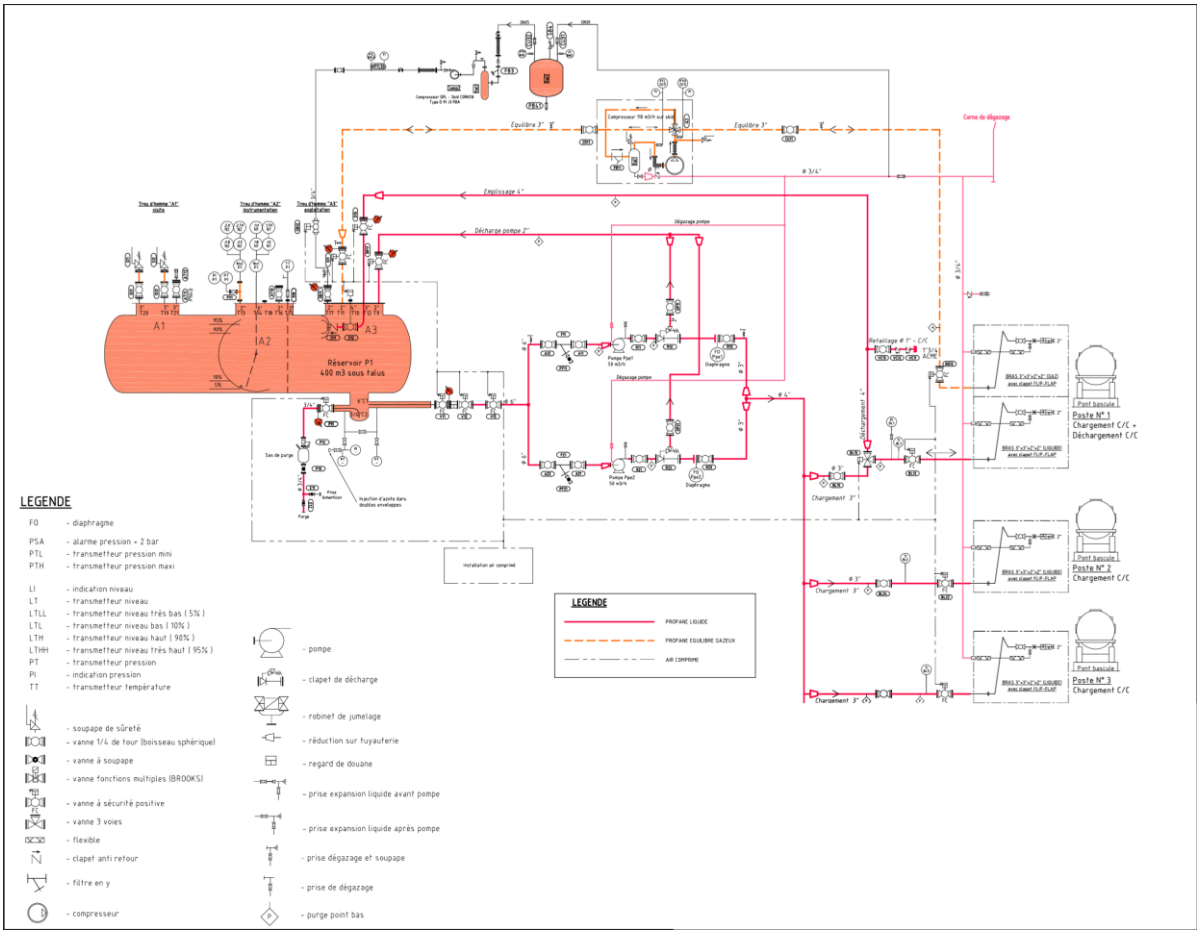


Figure 4-6 Diagramme PID

Dans le cadre des ICPE, l'étude des dangers désigne l'identification des évènements indésirables conduisant à des pertes. Elle permet d'indiquer pour chaque

[7] Les électrovannes sont fermées en fonctionnement normal

[8] Ce compresseur sert à équilibrer la pression entre le camion gros porteur et le réservoir

accident les composants concernés (réservoir de stockage, pompes). Dans l'étude de danger menée par l'exploitant du site, une grille MMR (figure 4-7) est utilisée comme modèle pour positionner chacun des accidents potentiels.

Gravité		Probabilité E	D	C	B	A
	Désastreux	**MMR rang 2** BLEVE camion à poste BLEVE camion en stationnement VCE suite à arrachement bras camion à poste Jet enflammé suite à arrachement bras de camion à poste* VCE suite à rupture canalisation DN > 25 mm Jet enflammé suite à rupture canalisation DN > 25 mm	**NON rang 1**	**NON rang 2**	**NON rang 3**	**NON rang 4**
	Catastrophique	**MMR rang 1** VCE suite à rupture d'un piquage ou d'une canalisation DN ≤ 25 mm Jet enflammé suite à rupture d'un piquage ou d'une canalisation DN ≤ 25 mm Jet enflammé suite à ouverture soupape de réservoir Jet enflammé suite à ruine du compresseur	**MMR rang 2**	**NON rang 1**	**NON rang 2**	**NON rang 3**
	Important	**MMR rang 1**	**MMR rang 1**	**MMR rang 2**	**NON rang 1**	**NON rang 2**
	Sérieux			**MMR rang 1**	**MMR rang 2**	**NON rang 1**
	Modéré					**MMR rang 1**

Figure 4-7 Grille MMR

D'après cette grille, les accidents identifiés correspondent à une case « MMR » et aucun accident n'est situé dans une case « NON ». Le nombre total d'accidents situés dans des cases « MMR rang 2 » est supérieur à 5 (6 scénarios), le risque global est équivalent à un accident situé dans une case « NON rang 1 ».

Le risque global du site peut être jugé comme acceptable dans le cas où :

– Le nombre de phénomènes dangereux peut être ramené à 5 par la mise en place de nouvelles mesures de maîtrise du risque,

– Le niveau de probabilité des phénomènes dangereux situés en « MMR Rang 2 » en cas de défaillance de l'une des mesures de maîtrise du risque est conservé.

Or pour le scénario menant au phénomène suivant situé en « MMR 2 », « jet enflammé suite à l'arrachement du bras de camion à poste », il s'avère que sa classe de probabilité (E) est maintenue si l'on considère la défaillance de la barrière avec le niveau de confiance le plus important. Ainsi, le risque global des accidents du site peut être jugé comme acceptable.

Les accidents considérés dans la suite de l'étude de danger et susceptibles d'engendrer ces phénomènes dangereux sont :

– BLEVE d'un camion petit porteur en stationnement (propane).
– BLEVE d'un camion gros porteur à poste (propane).
– UVCE ou jet enflammé suite à la rupture guillotine de la canalisation de soutirage 4 pouces du réservoir de 400 m^3.
– UVCE ou Jet enflammé suite à l'arrachement bras de chargement camion petit porteur.
– UVCE ou Jet enflammé suite à l'arrachement bras de déchargement camion gros porteur.
– UVCE ou jet enflammé suite à la rupture d'une canalisation 1 pouce.
– UVCE ou jet enflammé suite à une fuite de brides sur canalisations de 2, 3 ou 4 pouces.
– UVCE ou jet enflammé suite à une fuite sur les garnitures de pompes.
– UVCE ou jet enflammé suite à la ruine du compresseur.
– UVCE ou jet enflammé suite à l'ouverture de soupape sur le réservoir sous talus.
– UVCE ou jet enflammé suite à l'ouverture de soupape de ligne.

2.1.1 Le phénomène UVCE

Un UVCE (*Unconfined Vapor Cloud Explosion*) est une explosion de gaz à l'air libre. Dans le cas d'un gaz inflammable, tel que les GPL, cette explosion produit :

- Des effets thermiques,
- Des effets de pression.

Un UVCE comprend les étapes suivantes :

- Rejet dans l'atmosphère d'un GPL, le produit étant en phase gaz ou en phase liquide,
- Mélange avec l'oxygène de l'air pour former un volume inflammable,
- De manière concomitante, dilution et transport du nuage de gaz dont une partie du volume reste inflammable,
- Inflammation de ce nuage
- Propagation d'un front de flamme des parties inflammables du nuage ; ce front de flamme, associé à l'expansion des gaz brûlés, agit à la manière d'un piston sur les gaz frais environnants et peut être à l'origine de la formation d'une onde de pression aérienne, appelée déflagration, si sa vitesse de propagation est suffisante,
- Enfin, le cas échéant, mélange avec l'air et combustion des parties du nuage qui étaient initialement trop riches en combustible pour être inflammables

Le vocabulaire distingue, selon les effets produits, l'UVCE du *Flash fire*, ou *Feu de nuage*. De manière générale, le terme UVCE s'applique lorsque des effets de pression sont observés, alors que le terme Flash fire est réservé aux situations où la combustion du nuage ne produit pas d'effets de pression. Cependant il s'agit dans les deux cas du même phénomène physique, à savoir la combustion d'un mélange gazeux inflammable.

Pour obtenir un UVCE, il faut que deux conditions se réalisent simultanément :

- Un nuage de gaz inflammable (dont la concentration en combustible se situe entre la LII (Limite Inférieur d'Inflammabilité) et la LSI (Limite Supérieur d'Inflammabilité),
- Une source d'inflammation.

Tous les phénomènes de rupture de canalisation ou de fuite d'un GPL peuvent engendrer un UVCE. La fuite peut être liquide ou gazeuse, mais à condition de fuites équivalentes (pression, température, section de fuite). Une fuite en phase liquide produit des nuages inflammables toujours beaucoup plus grands qu'une fuite en phase gazeuse, car le débit rejeté est beaucoup plus élevé (pour les GPL dans des conditions ambiantes, 1 litre de phase liquide engendre de l'ordre de 250 litres de phase gazeuse).

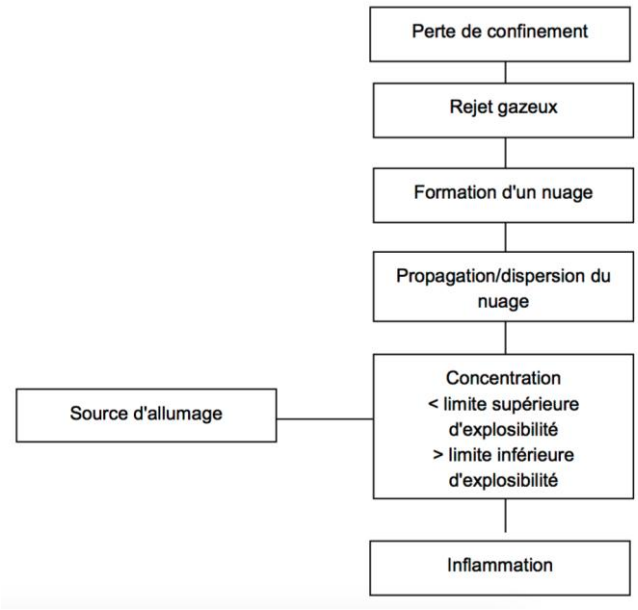


Figure 4-8 Les causes d'un UVCE

2.1.2 Le phénomène BLEVE

Un BLEVE (*Boiling Liquid Expanding Vapor Explosion*) peut être défini comme la vaporisation violente à caractère explosif consécutive à la rupture d'un réservoir contenant un liquide à une température significativement supérieure à sa température d'ébullition dans la pression atmosphérique. Tous les stockages de gaz liquéfiés sous pression sont susceptibles d'être le siège d'un BLEVE. En effet, le BLEVE est associé avant tout à un changement d'état à caractère explosif, et non à une réaction de combustion. Aussi, il n'est pas nécessaire que le produit concerné soit inflammable pour parler de BLEVE. Toutefois, il n'est question dans cette fiche que des gaz inflammables liquéfiés. Les effets d'un BLEVE sur l'environnement se manifestent généralement de trois manières :

– Effet de pression : propagation d'une onde de surpression,

– Effet missiles : projection de fragments à des distances parfois très importantes,

– Effet thermique : dans le cas d'un BLEVE de gaz liquéfié inflammable, rayonnement de la boule de feu,

2.2 Les accidents considérés dans cette étude de cas

Conformément à l'approche STAMP, il faut identifier les accidents au niveau du système global. Le tableau 4-3 résume les accidents cadrés par cette étude :

– Les blessures et pertes de vie humaine (A-1) : les opérateurs ainsi que la population sont exposés aux dangers de l'activité du site.

– Les pertes liées à l'environnement industriel (A-2) : elles concernent toute fuite incontrôlée de propane provoquant des explosions, des incendies et la pollution grave de l'environnement.

– Les dégâts matériels (A-3) : il s'agit de toute perte liée à un dommage matériel, ou une défaillance, détérioration due à la fatigue et à la corrosion des équipements de l'installation technique.

– Arrêt de l'activité du site de relais vrac (A-4) : il s'agit de tout évènement non planifié qui entraine l'arrêt des opérations au sein de l'établissement.

Table 4-4: Les accidents d'ordre général à prévenir dans ce système

A-1 : Blessures et pertes des vies humaines
A-2 : Pertes liées à l'environnement industriel
A-3 : Dégâts matériels
A-4 : Arrêt de l'activité du site de relais vrac

2.3 Les dangers du système d'étude

Cette étape consiste à identifier les dangers correspondants à chaque accident l'étape précédente tableau 4-4. La fuite de produit liquéfié ou non (H-1) se réfère à toute fuite incontrôlée au niveau des composants techniques du système. Toute perte de confinement doit être contrôlée pour empêcher les accidents (A-1 et A-2) dû à l'exposition de la population et de l'environnement et au danger de fuite de matière

dangereuse. L'augmentation de la température en présence de chaleur (H-2) est une condition dangereuse qui peut provoquer chacun des accidents cités dans la partie précédente (par exemple : la présence de chaleur un pic de pression dans l'installation incendie et explosion). La détérioration, fatigue et corrosion du matériel (H-3) concerne le dépassement des limites de sécurité dans l'exploitation des équipements et de l'installation.

Table 4-5: Les dangers d'ordre général à prévenir dans ce système

Danger	**Accident**
H-1 : Fuite de produit liquéfié ou non (gaz)	A-1, A-2
H-2 : Augmentation de la température en présence de chaleur	A-1, A-2, A-3, A-
H-3 : Détérioration, fatigue et corrosion du matériel	A-3, A-4
H-4 : Panne et arrêt intempestive de l'installation	A-4

2.4 La structure organisationnelle de contrôle de la sécurité

Cette étape permet d'obtenir une vision globale du système étudié, mais aussi de mettre en évidence l'ensemble des interactions entre les niveaux hiérarchiques du système. Par cette structure de contrôle, les rôles et les responsabilités sont intégrés et il est ainsi plus aisé de déterminer les influences entre éléments. Cette structure décrit l'ensemble du système d'un point de vue statique en montrant les rôles et les responsabilités de chaque niveau hiérarchique. Ces rôles et responsabilités servent de support à la définition et à l'intégration des contraintes au niveau de chaque acteur de la structure s'effectuant au cours de la méthodologie STPA. La structure ainsi définie a pour objectif de représenter les interactions entre les différents niveaux hiérarchiques, permettant de caractériser les contrôles entre éléments. Ce travail de modélisation pose les limites de l'analyse afin de déterminer par la suite les contrôles potentiellement inadéquats entre niveaux.

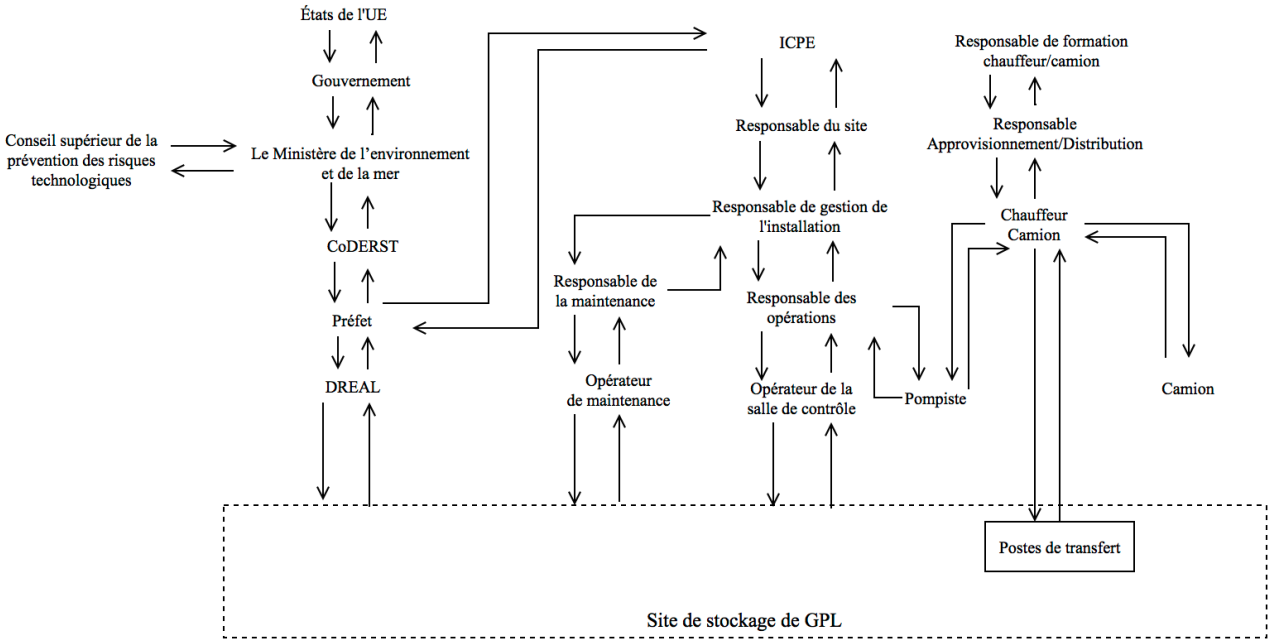


Figure 4-9 Structure administrative et organisationnelle

2.4.1 Structure générale de contrôle de la sécurité de l'installation

Les institutions européennes ont mis en place des mesures obligatoires en vue d'éviter ou de diminuer l'importance des dégâts causés par les accidents industriels majeurs.

En France, la maîtrise des risques et des accidents industriels majeurs est confiée au ministère de l'Environnement de l'Écologie et de la Mer. Le Conseil Départemental de l'Environnement et des Risques Sanitaires et Technologiques (CoDERST).

Le préfet du département est le représentant de l'Etat qui a l'autorité administrative sur le service d'inspection. Il est lui-même placé sous l'autorité du ministre chargé des installations classées (le ministre de l'environnement, de l'énergie et de la mer[9]). Le service d'inspection, sous l'autorité du préfet pour la majorité des établissements industriels l'inspection, est assurée principalement par les Directions Régionales de l'Environnement, de l'Aménagement et du Logement (DREAL) ou par la Direction Régionale et Interdépartementale de l'Environnement et de l'Energie (DRIEE) en Île de France. Les inspecteurs, ingénieurs, techniciens, sont les agents assermentés de l'Etat. Ex-Conseil Départemental d'Hygiène (CDH) ou des Carrières, le Conseil Départemental de l'Environnement et des Risques Sanitaires et Technologiques (CoDERST) réunit sous la présidence du préfet des administrations et des personnes extérieures (conseillers généraux, maires, représentants du monde professionnel, etc.).

[9] Le Ministère de l'écologie, du développement durable et de l'énergie

Ce conseil concourt à l'élaboration, à la mise en œuvre et au suivi des politiques publiques dans les domaines de la protection de l'environnement, de la gestion durable des ressources naturelles et de la prévention des risques technologiques. Pour les installations classées, le CoDERST est chargé d'émettre un avis par exemple sur l'application du PPRT. Il permet de recueillir des avis extérieurs à l'administration et d'engager un dialogue sur le dossier considéré.

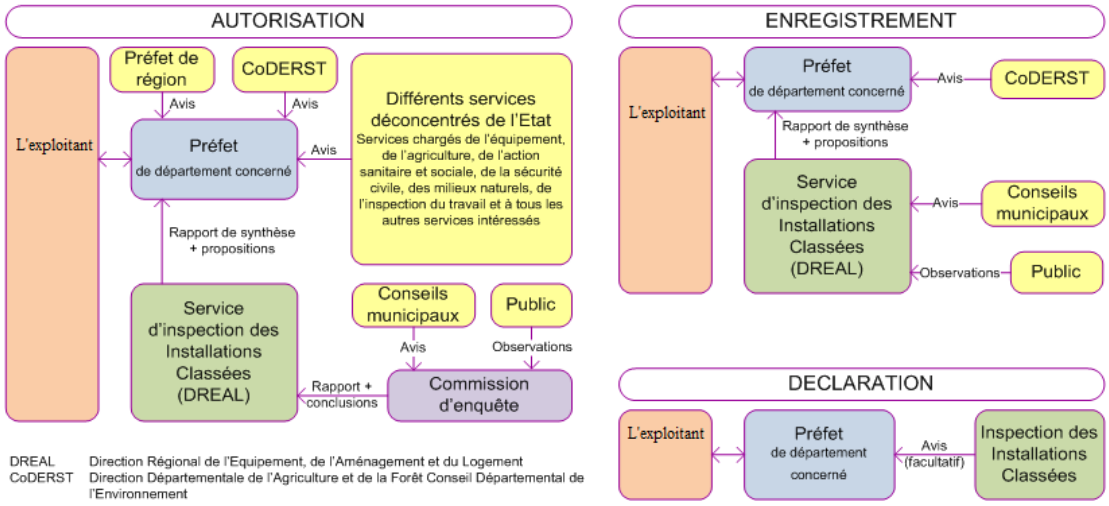


Figure 4-10 Structure administrative locale chargée de la sécurité de l'installation

Le site de stockage alimente tous les besoins en GPL (particuliers, professionnels, stations...) des départements. Sous le contrôle et la supervision du pompiste, une flotte de poids lourds petits porteurs, appartenant aux sociétés viennent y charger à chaque fois entre 3,5 à 9 tonnes de GPL., destiné à environ 2000 clients. Un plan de maintenance permettant d'assurer une exploitation sécurisée permanente. Les opérations de maintenance, ainsi que leurs périodicités, sont détaillées selon les équipements.

2.4.2 Exemple de la structure de contrôle de la sécurité de l'installation technique

La figure 4-11 montre une partie générale de la structure de contrôle de la sécurité. Les détecteurs gaz détectent toutes fuites ou formation de mélange d'air avec des gaz combustibles tels que le propane et le butane (ainsi que le gaz naturel, le méthane, l'hydrogène ou des vapeurs de dissolvants à pression élevée). En cas de détection, l'automate assure la coupure des asservissements les électrovannes s'ouvres et actionnent la fermeture des vannes automatiques à sécurité positive permettant ainsi

d'isoler une fuite de gaz non enflammée. Le même principe pour la détection d'une présence de flamme, la chaîne de sécurité permet de couper l'électricité industrielle (alimentation des commandes des électrovannes, des pompes et des compresseurs), ce qui entraîne la mise en sécurité du site. Elle entraîne également le démarrage des moyens d'arrosage.

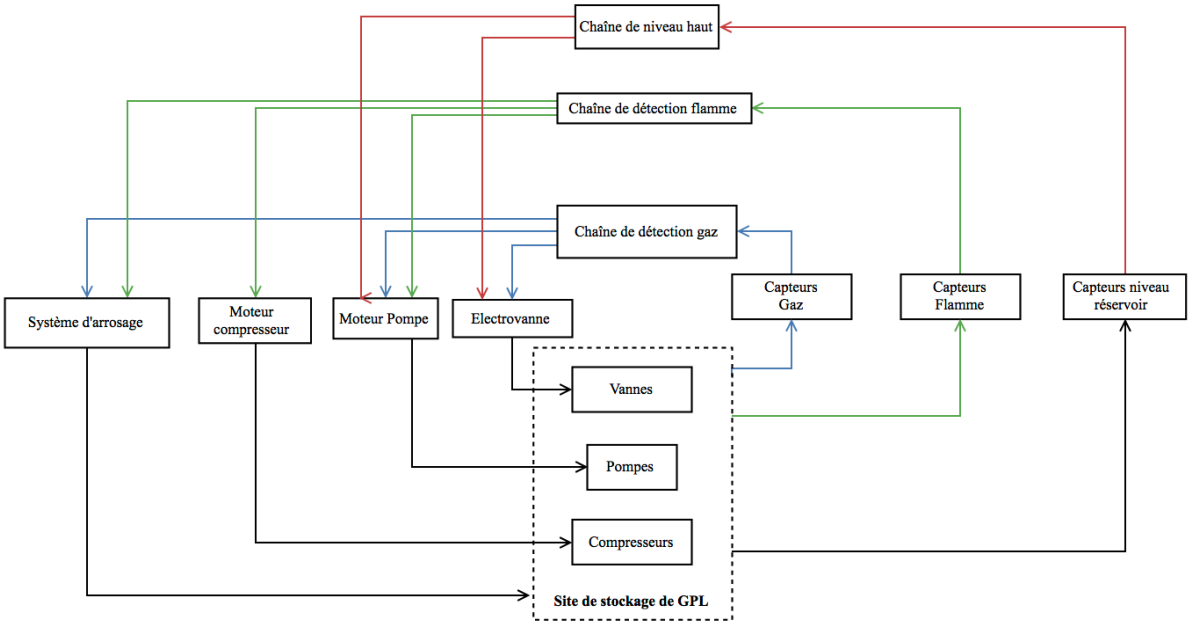


Figure 4-11 Exemple de la structure de contrôle de la sécurité au niveau du système d'exploitation

2.5 Les variables du processus contrôlé

Les variables du processus procurent au contrôleur les informations nécessaires pour décider des commandes de contrôle à engager.

Le modèle STAMP nous permet d'abord de suggérer une première distinction qui concerne l'origine des variables (figure 4-12) :

– Variable exogène : extérieure au système. Par exemple, la température de l'air (Le système considéré est le réservoir).

– Variable endogène : interne au système. Par exemple, la pression du gaz dans le réservoir.

Le temps est un cas particulier sur lequel nous reviendrons. Il peut être exogène (cas d'un simulateur temps réel lié à une horloge), ou endogène (si c'est le modèle qui en commande l'avance, ce qui est typiquement le cas d'une simulation à événements discrets).

Nous pouvons affiner l'analyse d'une variable exogène en analysant son influence sur le système :

- Variable de décision : permet à l'opérateur d'influer sur l'évolution du système (ex. : les étapes à suivre, si elles sont imposées dynamiquement par l'opérateur, par exemple à l'aide d'un système semi-automatique).
- Variables non contrôlées : il s'agit de variables qui sont déterminées par un modèle externe au système. Elles peuvent être déterministes (ex. : température de l'air, si elle est calculée à partir des conditions météo) ou aléatoires (ex. : le nombre de camions en attente dans un site de stockage /distribution, qui est généralement un phénomène stochastique).

De la même façon, nous distinguerons dans les variables endogènes les variables « indispensables » de celles qui n'ont qu'un but utilitaire :

- Variables d'état : comme nous l'avons déjà vu, elles décrivent l'état du système (ex. : pression, niveau, température...).
- Variables statistiques ou variables informatives : elles ne sont pas indispensables pour caractériser l'état du système, mais peuvent s'avérer utiles pour le fonctionnement du modèle, l'information de l'opérateur ou le dépouillement ultérieur des résultats de la simulation (ex. : la distance parcourue).

Enfin, une caractérisation pourra être faite suivant la durée de vie des variables :

– Variables persistantes ou permanentes : elles existent et ont une valeur significative pendant toute la durée d'une exécution de la simulation.

– Variables temporaires : elles n'existent ou n'ont de signification que pendant certains intervalles de temps.

– Variables transitoires : elles apparaissent que durant un instant déterminé (ou

un pas de temps pour une simulation à temps discret).

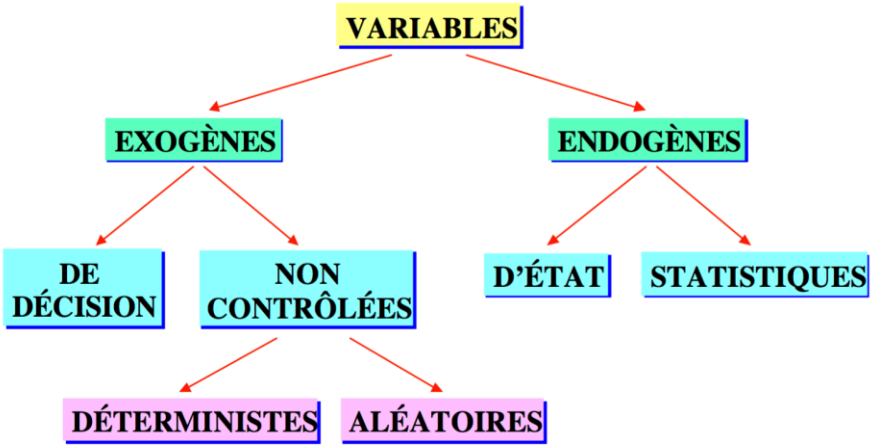


Figure 4-12 Classification des variables d'un système

2.5.1 Associer une action commandée à chaque variable

A chaque variable, on peut associer une action commandée. Par exemple, les variables associées aux actions commandées à la fermeture des vannes doivent être identifiées en analysant les fonctionnalités des vannes automatiques. En fonctionnement normal, les vannes s'ouvrent automatiquement durant une opération de transfert. La fermeture de ces vannes est nécessaire dans des conditions particulières suivantes :

- Cas de détection de fuite de gaz ;
- Cas de détection d'une flamme ;
- Le niveau du réservoir est haut (89% de sa capacité de stockage) ;
- Le niveau du réservoir est très haut (94% de sa capacité de stockage) ;
- Cas de des dégâts du matériel.

Ces conditions dangereuses sont liées à une perte de confinement, sur les installations fixes, réservoir sous-talus, d'un camion à poste ou en zone de stationnement. Ces conditions dangereuses résultent des pannes et défaillances matérielles, par exemple une perte de confinement sur l'installation fixe (fuite sur pompe, ruine du compresseur…). Ces conditions dangereuses peuvent être aussi causées par les principales soupapes de sûreté qui sont ouvertes par inadvertance ou au mauvais moment. Ces conditions nécessitent la fermeture des vannes pour contrôler la

situation et empêcher toute perte. En cas de présence de flamme, la chaîne de détection de flamme doit être engagée pour la fermeture des vannes, le déclenchement de l'arrosage... Pour cela, les informations sur les variables mesurées peuvent être aussi transmises par le biais des capteurs de l'ensemble des chaînes de détection. Ces informations sont nécessaires pour le processus décisionnel du contrôleur ou du système pour déclencher la fermeture de la vanne.

Les variables mesurées concernant la fermeture des vannes peuvent être identifiées et déterminées comme suit :

- Rupture de canalisation qui provoque une fuite incontrôlée de GPL
- Une fuite sur la ligne d'emplissage du réservoir qui peut provoquer un mélange gazeux proche des limites d'explosivité ;
- Une fuite au niveau du compresseur qui ruine l'ensemble de l'installation.

2.6 Les actions dangereuses déclenchées par commande (étape 1)

La démarche d'analyse des dangers se décompose en deux étapes. La première étape suppose l'identification des commandes dangereuses : il est donc nécessaire de choisir un système de contrôle et un processus contrôlé. Les vannes d'emplissage du réservoir s'ouvrent automatiquement pendant l'opération de déchargement et se ferment automatiquement en fin d'opération. Ces vannes sont munies de fusibles thermiques, fondant en cas de source de chaleur à proximité et entraînant la fermeture des vannes. Les électrovannes sont les actionneurs de la fermeture de ses vannes sous commande des composants des chaînes de détection (gaz, niveau, flamme).

Table 4-6: Les dangers liés à la commande de fermeture des vannes d'emplissage

Commande	Dangers			
	Cause un danger si elle n'est pas déclenchée	**Cause un danger si elle est déclenchée**	**Cause un danger si elle est déclenchée hors séquence**	**Cause un danger si elle est durablement appliquée ou stoppée prématurément**
Fermeture des vannes d'emplissage	La fermeture de la vanne n'est pas déclenchée suite à une fuite sur pipe [H-2, H-1, H-3]	La fermeture de la vanne est déclenchée sans qu'il n'y ait de fuite [H-4] La fermeture de vanne est déclenchée grâce aux fusibles et non pas aux électrovannes (en panne) [H-2, H-1, H-3]	La fermeture de la vanne est déclenchée très tôt au moment où la pression dans l'installation est importante [H-2, H-3] La fermeture de la vanne est déclenchée très tard après la fuite [H-1, H-2, H-3, H-4]	N/A

Le tableau de contexte est ensuite construit en se référant aux variables mesurées contrôlées définies précédemment (section 2.5).

2.6.1 Cas où l'action commandée est générée par le système de contrôle

La 1ère colonne du tableau 4-7 désigne les actions commandées soumises à l'analyse. Dans le tableau, la 2ème jusqu'à la 5ème colonne, désignent les variables de contrôle du processus. La 6ème colonne précise dans quel contexte la fermeture des vannes peut s'avérer dangereuse. Par exemple la première ligne décrit une situation pendant une opération de transfert où il est dangereux de déclencher la fermeture de la vanne dans le cas où il n'a pas de rupture ou de fuite. Concernant cette ligne, la fermeture de cette vanne entraîne l'arrêt intempestif de l'opération de transfert H-4. Le système de support de sécurité, en cas de fermeture intempestive des vannes lors de l'opération de transfert, serait la fermeture de la vanne du bras de déchargement. Si le système de support n'est pas opérationnel pour ce cas (vanne du bras de chargement ouverte), cela va augmenter le débit dans la ligne d'emplissage ce qui peut entraîner le danger (H-2 ligne 9 colonne 6). Si la mise en sécurité du site est conduite, la fermeture intempestive de la vanne pendant l'opération de transfert n'est pas une action

dangereuse (lignes 2-8, colonne 6). Si pour des raisons données, les barrières de sécurité ne fonctionnent pas, le système peut encourir les dangers (lignes 10-16, colonne 6). Ce tableau est employé pour traiter les comportements dangereux. Par exemple, la ligne 1 colonne 6 de la table 8 l'action de fermeture de la vanne pendant une opération de transfert est considérée dangereuse même si le contexte n'est pas dangereux (pas de rupture, pas de fuite, le système de support opérationnel). A l'inverse le contexte décrit à ligne 2, en cas de rupture de canalisation la colonne 6 n'est pas marquée comme dangereuse puisque la fermeture de la vanne dans ce contexte est nécessaire pour éviter l'accident.

Table 4-7: Table de contexte cas ou le système initie la commande de Fermeture des vannes

	1	2	3	4	5	6	7	8
	Action De contrôle	**Canalisation Et tuyauterie**	**Condition de ligne d'emplissage**	**Condition du compresseur**	**Statu des systèmes de support de sécurité**	**Action de contrôle Dangereuse?**	**Action de contrôle si trop tard?**	**Action de contrôle dangereuse si trop tôt?**
1	***Fermeture des vannes***	Pas de rupture	Pas de fuite	Pas de fuite	Opérationnel	H-4	H-4	H-4
2		Rupture	Pas de fuite	Pas de fuite	Opérationnel	No	H-1, H-2, H-3, H-4	H-3, H-4
3		Pas de rupture	Fuite	Pas de fuite	Opérationnel	No	H-2, H-3, H-4	No
4		Pas de rupture	Pas de fuite	Fuite	Opérationnel	No	H-2, H-3, H-4	No
5		Rupture	Fuite	Pas de fuite	Opérationnel	No	H-1, H-2, H-3, H-4	H-3, H-4
6		Pas de rupture	Fuite	Fuite	Opérationnel	No	H-2, H-3, H-4	No
7		Rupture	Pas de fuite	Fuite	Opérationnel	No	H-1, H-2, H-3, H-4	H-3, H-4
8		Rupture	Fuite	Fuite	Opérationnel	No	H-1, H-2, H-3, H-4	H-3, H-4
9		Pas de rupture	Pas de fuite	Pas de fuite	Non Opérationnel	H-2, H-4	H-2, H-4	H-2, H-4
10		Rupture	Pas de fuite	Pas de fuite	Non Opérationnel	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
11		Pas de rupture	Fuite	Pas de fuite	Non Opérationnel	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
12		Pas de rupture	Pas de fuite	Fuite	Non Opérationnel	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4

13		Rupture	Fuite	Pas de fuite	Non Opérationnel	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
14		Pas de rupture	Fuite	Fuite	Non Opérationnel	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
15		Rupture	Pas de fuite	Fuite	Non Opérationnel	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4
16		Rupture	Fuite	Fuite	Non Opérationnel	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4	H-1, H-2, H-3, H-4

2.6.2 Cas où le système ne génère pas la fermeture de la vanne (par commande)

Bien que le déclenchement d'une action par commande puisse être dangereux, ne pas imposer l'application des contraintes de sécurité peut aussi s'avérer dangereux. Le tableau 4-8 montre les dangers dans le cas où le système ne déclenche pas, par commande, la fermeture de la vanne. Dans le cas d'absence de rupture ou de fuite, le maintien de l'ouverture de la vanne n'est pas dangereux (ligne 1 et 9). Cependant en cas de fuite ou de rupture, différents dangers peuvent être expérimentés en fonction de la partie du système affecté. Si un composant de la canalisation et tuyauterie est cassé et les vannes automatiques ne sont pas fermées, on peut témoigner alors des fuites dans les différentes parties du système (H-1) et en cas d'opération de transfert, le volume déverser peut devenir incontrôlable. Si dans la zone du compresseur, il existe une fuite et la commande pour la fermeture des vannes automatiques n'est pas déclenchée, la fuite peut alors causer un mélange gazeux proche des limites d'explosivité (H-2).

Table 4-8: Table de contexte cas ou le système n'enclenche pas commande de Fermeture des vannes

	1	2	3	4	5	6
	Action de contrôle	**Canalisation Et**	**Condition de ligne emplissage**	**Condition zone compresseur**	**Statu des systèmes de support de**	**Commande non fourni provoque un danger?**
1		Pas de rupture	Pas de fuite	Pas de fuite	Opérationnel	No
2		Rupture	Pas de fuite	Pas de fuite	Opérationnel	H-1, H-2, H-3, H- 4
3		Pas de rupture	Fuite	Pas de fuite	Opérationnel	H-2, H-3
4		Pas de rupture	Pas de fuite	Fuite	Opérationnel	H-2, H-3
5		Rupture	Fuite	Pas de fuite	Opérationnel	H-1, H-2, H-3, H- 4
6		Pas de rupture	Fuite	Fuite	Opérationnel	H-2, H-3
7		Rupture	Pas de fuite	Fuite	Opérationnel	H-1, H-2, H-3, H- 4
8		Rupture	Fuite	Fuite	Opérationnel	H-1, H-2, H-3, H- 4
9		Pas de rupture	Pas de fuite	Pas de fuite	Opérationnel	No
10	***Fermeture De la vanne***	Rupture	Pas de fuite	Pas de fuite	Non Opérationnel	H-1, H-2, H-3, H- 4
11		Pas de rupture	Fuite	Pas de fuite	Non Opérationnel	H-2, H-3
12		Pas de rupture	Pas de fuite	Fuite	Non Opérationnel	H-2, H-3
13		Rupture	Fuite	Pas de fuite	Non Opérationnel	H-1, H-2, H-3, H- 4
14		Pas de rupture	Fuite	Fuite	Non Opérationnel	H-2, H-3
15		Rupture	Pas de fuite	Fuite	Non Opérationnel	H-1, H-2, H-3, H- 4
16		Rupture	Fuite	Fuite	Non Opérationnel	H-1, H-2, H-3, H- 4

2.7 Assigner les contraintes de sécurité aux actions dangereuses avec STPA

Pour chaque action dangereuse du tableau 4-8, on associe une contrainte ou mesure de sécurité.

Table 4-9: Les actions dangereuses et les contraintes de sécurité correspondantes

Action Dangereuse (AD)	**Contrainte de sécurité (CS)**
AD 1 : Cas où le système de support est opérationnel mais la fermeture de la vanne n'est pas déclenchée par commande suite (rupture sur canalisation, fuite sur la ligne d'emplissage, ou fuite sur la zone du compresseur...)	**CS 1** : Les vannes doivent être commandées « fermer[10] » en cas de fuite (rupture sur canalisation, fuite sur la ligne d'emplissage, ou fuite sur la zone du compresseur...) même si le système de support est opérationnel
AD 2 : Cas où le système de support n'est opérationnel et la fermeture de la vanne n'est pas déclenchée par commande suite à des fuites	**CS 2** : Les vannes doivent être commandées « fermer » en cas de fuite même si le système de support n'est pas opérationnel
AD 3 : Cas où la vanne est commandée « fermer » suite à une rupture de canalisation mais le système de support n'est pas opérationnel	**CS 3** : Les vannes doivent être commandées « fermer » suite à une rupture de canalisation même si le système de support n'est pas opérationnel
AD 5 : Cas où la vanne est commandée fermer trop tard suite à une rupture ou une fuite	**CS 5** : la vanne ne doit pas être commandée fermer trop tard suite à une rupture ou une fuite
AD 6 : Cas où la vanne est commandée « fermer » sans qu'il n'y est une rupture ou une fuite	**CS 6** : la vanne ne doit pas être commandée « fermer » pendant un transfert sans qu'il n'y est une rupture ou une fuite

2.8 Etude des causes des actions dangereuses (étape 2)

L'identification des actions dangereuses est une étape importante de l'analyse STPA. Cette deuxième étape concerne l'identification des facteurs qui engendrent des commandes dangereuses dans le système. Cette étape permet aussi d'identifier les actions commandées par le système de contrôle nécessaire pour la sécurité et non exécutées correctement par les composants de la structure de contrôle.

[10] Par arrêt d'urgence de l'installation

Comme nous l'avons précisé dans la section (1.6) deux éléments peuvent contribuer à transgresser les contraintes de sécurité :

(1) Le système déclenche (par commande) une action dangereuse.

(2) Le système déclenche une action (par commande) mais elle n'est pas exécutée ou mise en œuvre.

Les causes présentées dans la figure 4-5 sont utilisées pour effectuer cette analyse.

2.8.1 Analyse des causes de l'AD (Action Dangereuse)

Dans cette section, les causes des actions dangereuses identifiées dans le tableau 4-9 sont analysées. On se contente dans la partie qui suit de présenter les causes de AD1.

AD 1 : Cas où le système de support est opérationnel mais la fermeture de la vanne n'est pas déclenchée par commande suite (rupture sur canalisation, fuite sur la ligne d'emplissage, ou fuite sur la zone du compresseur…).

(1) Systèmes de barrières de sécurité

a. Présence de deux situations concomitantes qui induisent l'opérateur en erreur. Par exemple, un problème dans l'opération de transfert peut survenir simultanément avec une rupture de canalisation.

b. Les conditions qui nécessitent la fermeture de la vanne ne sont pas évidentes

c. La progression de l'événement indésirable est trop lente et non décelée

(2) Affichage émanant du processus contrôlé (feedback)

d. Pas de réplication d'information de l'état de la canalisation en salle de contrôle ou au niveau de poste de transfert

e. La pression au niveau des canalisations est incorrecte ou communiquée en temps différé

f. La mesure des niveaux est incorrecte

g. Des données conflictuelles dérivants une fausse situation

h. Panne dans le système de détection

i. La fuite n'est pas reportée

(3) Opérateur

- L’opérateur pense qu’il n’y a pas de rupture au niveau de la canalisation
- L’opérateur pense qu’il n’y a pas de fuite au niveau de la ligne d’emplissage
- L’opérateur pense qu’il n’y a pas de fuite au niveau de la zone du compresseur
- L’opérateur est confus au sujet de la procédure à suivre
- L’opérateur est confus en raison d’affichage conflictuel des indicateurs
- L’opérateur est réticent au déclenchement de l’arrêt d’urgence de l’installation.
- L’opérateur attend que les barrières de sécurité gèrent la situation
- L’opérateur est en manque d’information sur la situation à cause des affichages erronés
- L’opérateur déclenche la fermeture d’une vanne différente.

2.8.2 Les causes relatives aux actions déclenchées (par commande) et non exécutées

Dans cette partie, nous allons analyser les actions déclenchées (par commande) et non exécutées par l’actionneur. Pour cela, nous allons évaluer les causes liées à l’application inappropriée des contraintes de sécurité. On se contente d’effectuer l’analyse pour les contraintes de sécurité suivantes :

- **CS 1 :** Les vannes doivent être commandées « fermer » en cas de fuite (rupture sur canalisation, fuite sur la ligne d’emplissage, ou fuite sur la zone du compresseur…) même si le système de support (fusible thermique) est opérationnel.
- **CS 2 :** Les vannes doivent être commandées « fermer » en cas de fuite même si le système de support n’est pas opérationnel.

Scénario de base : L’opérateur déclenche (par commande) la fermeture de la vanne mais la vanne ne se ferme pas.

(1) Systèmes de barrières de sécurité :

a. Panne technique ou défaillance du matériel
b. La commande de l’opérateur n’est pas reçue
c. Défauts de fabrication

d. La suite d'instruction (algorithme de contrôle) n'est pas adaptée au problème

e. Panne ou coupure électrique

(2) Les détecteurs

a. Les détecteurs ne transmettent pas un signal à la centrale de traitement

b. Panne technique ou défaillance des détecteurs

c. Défauts de fabrication

d. Panne ou coupure électrique

(3) Les électrovannes (actionneurs pour vannes)

a. L'alimentation en air n'est pas coupée[11]

b. Défauts de fabrication

c. Pas de coupure électrique

(4) La vanne

a. La pression de l'air est très faible et empêche le piston de tourner

b. Les débris à l'intérieur empêchent sa fermeture complète ou partielle

c. Défauts de fabrication

d. Panne ou défaillance technique

3. Conclusion et discussions des résultats

Dans ce chapitre, nous avons présenté une partie de la démarche de modélisation STAMP/STPA. Cette analyse nous a permis d'identifier des dangers autres que ceux mentionnés dans l'étude de danger de l'exploitant.

L'étude de danger basée sur STAMP procure une analyse approfondie qui comprend la description des modes de contrôle. Bien que cette étude ne couvre qu'une

[11] Les actionneurs pour vannes déclenchent par rappel du ressort, la rotation d'un robinet, dirigeant un boisseau se trouvant dans la vanne. Suivant la position de ce boisseau, la vanne est ouverte ou fermée. Les actionneurs pneumatiques sont de type simple effet. Leur position de repos correspond à la fermeture de la vanne. L'ouverture de la vanne s'effectue avec apport d'air moteur. Cette configuration est maintenue jusqu'à ce que l'alimentation en air soit coupée. La pression en air n'étant alors plus suffisante pour comprimer les pistons, ceux-ci se détendent entraînant la rotation de l'axe et la fermeture de la vanne.

partie limitée du système, certaines des informations importantes peuvent être déduites en examinant les causes des actions de contrôle dangereuses pour les scénarios étudiés. Un exemple de cette analyse est la difficulté de détecter une rupture sur la canalisation à partir des indicateurs. Le système automatisé et l'opérateur sont susceptibles de déclencher une action commandée en temps différé. Dans ce cas, la sécurité de l'installation dépend des capacités de détection et d'intervention de l'opérateur. L'opérateur peut ne pas paraître fiable car d'autres facteurs peuvent influencer le processus de prise de décision de l'opérateur. Les causes concernant le comportement de l'opérateur sont identifiées dans (l'étape 2) de l'analyse STPA. Les facteurs identifiés peuvent être utilisés pour améliorer la conception de l'interface homme/machine.

L'étude ne comporte pas une analyse des risques approfondies pour chaque composant du système pris individuellement. Les problèmes liés aux manques de contrôle révélés par cette analyse représentent un point de départ pour une analyse détaillée qui peut faire appel à des outils de simulation. Cette étude montre qu'une configuration incorrecte de l'ordonnancement des tâches prioritaires (des systèmes de contrôle des opérations et de la sécurité) peut causer un danger par exemple si la fermeture de la vanne est ignorée. L'exploitant doit s'assurer que les actions nécessaires pour assurer la sécurité de l'installation doivent être prioritaire au sein de chaque système de contrôle. Pour cela, plusieurs options peuvent se présenter dans l'imposition des contraintes de sécurité pour que la commande de fermeture de la vanne ne soit pas ignorée dans un contexte donné.

Le chapitre suivant présente le travail de recours à la simulation pour évaluer le comportement du système à un niveau hiérarchique inférieur qui concerne l'opération de transfert effectué au sein du site en mode normal et dégradé. Du modèle a la simulation

La modélisation (d'un système complexe) consiste à représenter les composants d'un système et leurs interactions. La simulation est l'implémentation dynamique du modèle (du travail de modélisation). Dans ce chapitre, on présente avec le logiciel Anylogic le travail de modélisation et de simulation du comportement et les évolutions dans le temps au niveau des composants du système d'étude. Pour cela, nous allons d'abord présenter la démarche adoptée. Nous détaillerons ensuite le logiciel AnyLogic

pour enfin exposer le travail de simulation et discuter des résultats.

CHAPITRE 5: MODELE DE SIMULATION

Ce chapitre a pour objectif de présenter un cadre d'application de la modélisation dynamique des systèmes au sein d'un site industriel en tant que support à la démarche d'évaluation des risques. La mise en œuvre de cette démarche, appuyée par l'utilisation d'un logiciel, donne au décideur les moyens pour modéliser le système et de simuler le comportement au cours du temps. Il s'agit donc d'une démarche d'analyse dynamique des risques industriels qui repose sur des phases complémentaires permettant une réflexion et une amélioration continue de la gestion des risques.

La phase de conception du modèle dynamique et de simulation du comportement du système repose principalement sur le choix des variables qui décrivent l'état des éléments du système en interaction à chaque instant et la définition des hypothèses qui établissent les interactions en vue de la formalisation du système envisagé.

L'analyse des dangers fondée sur une méthode bien déterminée, telle que la méthode STAMP, permet d'identifier tous les problèmes de perte de contrôle possibles et aussi, grâce au modèle dynamique, d'étudier les éventuelles variations du comportement du système au cours du temps.

La simulation des conséquences des problèmes de contrôle est conduite à l'aide du logiciel de simulation Anylogic pour mesurer l'efficacité des moyens de prévention, de protection mis en œuvre. Elle permet ainsi de définir de nouveaux moyens si cela s'avère nécessaire.

1.1 Étapes de modélisation et de simulation

L'approche par simulation peut être déployée pour développer la sécurité d'un système. L'utilisation de la simulation à des fins d'ingénierie de la sécurité du système suppose la réalisation d'un prototype virtuel, modèle numérique du système complet, pour étudier, tester, les solutions possibles, avant qu'un prototype réel, souvent coûteux, ne soit mis en œuvre. Les approches méthodologiques possibles de la modélisation et de la simulation d'un système respectent généralement le schéma proposé dans la figure 5-

1 (Cantot, 2006) :

- Formuler le problème ;
- Préciser les objectifs et organiser le projet ;
- Effectuer la modélisation et collecter les données ;
- Rédiger le code qui permet de compiler le modèle dans un logiciel de simulation;
- Vérifier le code et les données ;
- Valider le modèle et les données ;
- Exécuter la simulation ;
- Analyser (avec un regard critique) les résultats ;
- Rédiger le rapport final ;
- Mettre en service l'application et/ou capitaliser le modèle :

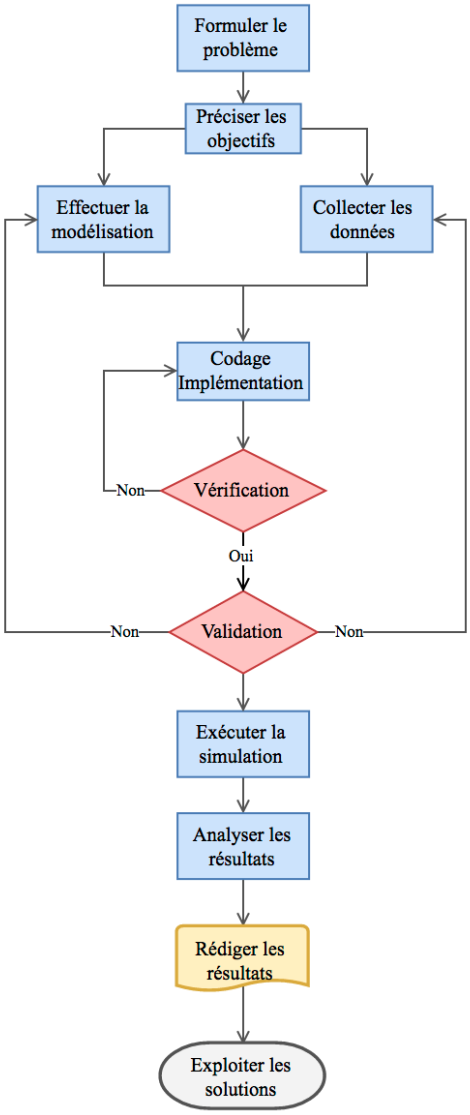


Figure 5-1 Les étapes de la démarche (Cantot, 2006)

1.1.1 La formulation du problème

Comme dans tout travail de modélisation et de simulation, on commence par énoncer les besoins, en l'occurrence les problèmes que nous souhaitons résoudre par le biais de la simulation. Dans la continuité du travail présenté dans le chapitre 4, on souhaite évaluer par le biais de la simulation les problèmes liés aux procédures de déroulement des opérations au sein du site de stockage de GPL. Dans cette étape, la démarche consiste d'abord à s'assurer auprès du partenaire industriel de la bonne vision du problème posé (identification et délimitation du système étudié...).

1.1.2 Objectifs et organisation

Dans cette étape, il est important de préciser les spécifications de la simulation :

les objectifs à atteindre (i.e. questions à résoudre ou fonctionnalités attendues), scénarii, précision du modèle, critères de validation, exigence de qualité (réutilisabilité, évolutivité...), contraintes particulières (utilisation de certains outils logiciels comme Anylogic). Les objectifs servent à évaluer le résultat. Il est important de définir les modules assez tôt, pour déterminer les conditions dans lesquelles le système simulé va évoluer.

L'exploitant s'est plus particulièrement intéressé, pour le travail de modélisation et de simulation, à faire apparaître les modules suivants :

- Module qui génère l'arrivée des camions ;
- Module pour contrôler la demande d'entrée à l'intérieur du site ;
- Module de vérification des compétences du chauffeur ;
- Module qui détaille le déroulement du processus d'identification ;
- Module qui décrit les processus de chargement et de déchargement au cours du temps ;
- Module qui représente le flux d'échange de GPL entre le camion et le RST ;
- Module qui enclenche les alertes sur le site ;
- Module qui représente le déroulement des opérations en mode (normal, dégradé et fortement dégradé) ;

1.1.3 Modélisation

Le travail de modélisation effectué avec STAMP, nous a permis d'analyser le système en particulier en ce qui concerne ses constituants et leurs caractéristiques. L'essentiel de la modélisation avec le logiciel Anylogic consiste à déterminer les variables d'état et les lois d'évolution. Cela suppose en particulier de prendre en compte les aspects statiques, dynamiques (lois d'évolution...), temporels et aléatoires des caractéristiques de la simulation.

1.1.4 Exécution de la simulation

On appelle « run » ou « réplique » l'exécution d'une simulation selon un scénario donné. Dans le cas des modèles stochastiques, le résultat de plusieurs exécutions successives d'un modèle avec les mêmes données d'entrée peut produire des résultats différents. Aussi, il est impossible de conclure à l'issue d'une seule réplique. Par conséquent, on exécutera un grand nombre de fois la simulation en sauvegardant à

chaque fois dans un fichier de sortie
(« journal ») les valeurs des variables (d'état ou statistiques) que l'on souhaite étudier. Par la suite, on effectuera des calculs statistiques sur ces variables pour en déduire les tendances générales : c'est l'opération d'exploitation des résultats de la simulation.

Ces exécutions multiples sont très lourdes en mode interactif (avec l'utilisateur dans la boucle). C'est pourquoi de nombreuses simulations destinées à des analyses de Monte Carlo sont conçues pour pouvoir fonctionner dans un mode fermé, sans utilisateur dans la boucle, appelé « batch ». Toutes les données d'entrée doivent être déterminées dès le départ, de sorte que plusieurs dizaines de répliques puissent être effectuées à la chaîne (ou en parallèle) sur un calculateur sans intervention de l'utilisateur.

2. L'outil de modélisation et de simulation AnyLogic

AnyLogic est un outil de simulation dynamique développé entièrement en Java, fournissant un environnement de programmation graphique. Il permet de concevoir des modélisations et des simulations à partir de trois types d'approches : la dynamique des systèmes (haut niveau d'abstraction), les systèmes multi-agents (niveau médian), et les systèmes d'événements discrets (bas niveau) en ajoutant aussi la combinaison de ces trois modèles. En outre, différents types de simulation peuvent être effectués : optimisation, variation de paramètres, comparaison de trajectoires, Monte-Carlo, etc. Enfin, le logiciel donne la possibilité de produire des animations représentées en 2D et même en 3D. L'environnement de programmation orienté-objet d'AnyLogic permet la construction modulaire et incrémentale de grands modèles.

2.1 L'approche par la dynamique des systèmes

Au milieu des années 50, Jay Forrester, Professeur au MIT, pose les principes et le langage de modélisation de la dynamique des systèmes qui se définit comme un « *mode d'étude du comportement des systèmes industriels permettant de montrer comment des politiques, des décisions, des structures et des délais sont en interrelation pour influencer la croissance et la stabilité* » (Forrester, 1961 *in* Garbolino et al., 2010). Les notions d'état du système, de boucles de rétroaction, de non-linéarité, de délai et

d'évolution structurelle caractérisent l'analyse de causalité produisant un modèle qualitatif, exprimé sous la forme d'un graphe sagittal, puis formalisé quantitativement en modèle de simulation. La dynamique des systèmes est une méthode d'étude qui suggère que l'on devrait :

- Prendre un point de vue endogène, c'est-à-dire modéliser le système comme une structure causalement close qui définit elle-même son comportement.
- Mettre en évidence les boucles de rétroaction (causalité circulaire) dans le système qui constituent le cœur de la dynamique des systèmes.
- Identifier les stocks (accumulations) et les flux qui les affectent. Les stocks sont la mémoire du système et des sources de déséquilibre.
- Prendre une vue continue où les événements et les décisions sont flous.

La modélisation en dynamique des systèmes se fait par étapes :

- Choisir les variables décrivant l'état des éléments en interaction à tout moment ;
- Définir les hypothèses établissant les interactions qui permettent de distinguer le système de son environnement ;
- Elaborer un modèle de relations causales entre les variables par les connaissances et hypothèses tout en distinguant les boucles à rétroaction ;
- Désagréger, par une démarche descendante, les phénomènes de causalité afin d'appréhender la complexité au bon niveau pour en attendre de possibles conséquences sur l'évolution dynamique ;
- Ecrire les relations établies sous la forme d'équations différentielles dans un cadre informatique qui permette les simulations ;

Cette approche permet ainsi de :

- Mettre en évidence les éventuels comportements périodiques
- Montrer le comportement à long terme
- Visualiser les conséquences d'un changement structurel
- Faire apparaître les conséquences des décisions stratégiques

2.2 L'approche par les systèmes multi-agents

Les Systèmes Multi-Agents sont un des axes de recherche de l'Intelligence

Artificielle Distribuée qui a pour objectif l'étude de la résolution de problèmes par une communauté d'agents autonomes (Ferber, 1999). Il s'agit de faire coopérer un ensemble d'agents dotés d'un comportement intelligent et de coordonner leurs buts et leurs plans d'action pour la résolution d'un problème.

On peut ne pas savoir comment le système se comporte entièrement et quelles en sont les variables clés et les dépendances entre chacune d'elles. Plus simplement, il est difficile d'en saisir le processus. Néanmoins, on peut avoir des aperçus de la manière dont les objets se comportent individuellement dans le système. Par conséquent, on peut commencer à construire un modèle à partir du bas et monter en identifiant ces objets (les agents) et en définissant leurs comportements.

La communication est également une notion importante. La transmission de l'information peut se faire entre deux agents, ou entre un agent et un acteur humain. Pour cela, les modes de communication reposent sur l'envoi de messages, ou le partage d'informations. Il peut y avoir plusieurs langages de communication reposant sur la théorie des actes de langages. La plupart des modèles multi-agents travaillent en temps discret. Les interactions, les prises de décision et les états changent instantanément. Le mécanisme de simulation n'est pas très différent de celui utilisé pour la modélisation à événements discrets. L'approche par multi-agent permet de traiter

- Un grand nombre d'activités concurrentes, il est possible de créer et de détruire une activité ;
- L'approche permet de traiter de multiples événements instantanés, par le biais d'une réplique déterministe ou aléatoire.
- L'approche permet de créer un réseau qui assure l'interopérabilité entre les agents ;
- L'outil Anylogic permet de représenter en 2D, 3D ou sur une carte géographique, les fonctionnalités des agents

Si les dynamiques internes des agents ou les dynamiques des environnements relèvent d'éléments en temps continu, comme des équations différentielles, le mécanisme de simulation doit inclure des méthodes numériques et supporter l'hybride

temps discret/continue.

Il n'existe pas d'architecture standard pour la réalisation d'agents logiciels intelligents (Jaber et al., 2001). Toutefois, l'architecture d'agent est donc toujours composée de modules. Par exemple, une architecture simple composée de cinq modules : savoir-faire, croyances, contrôle, expertise, et communication. Un autre exemple d'architecture, plus détaillée, se décompose des modules allant de la perception jusqu'à l'apprentissage, en passant par l'interprétation, le raisonnement et la prise de décision, le tout guidé par des bases de connaissances à la fois sur les objectifs propres de l'agent, mais aussi des autres agents.

Les agents interagissent entre eux pour remplir leurs objectifs, soit de manière indépendante, en coopération (mise en commun des ressources et compétences), ou bien de façon antagoniste (situation de compétitions ou de conflits). Les agents logiciels intelligents peuvent être structurés de deux manières au sein d'un SMA : structure horizontale (les agents sont au même niveau) et structure verticale (les agents sont à plusieurs niveaux, et on peut retrouver une structure horizontale à un même niveau).

La communication est également une notion importante. La transmission de l'information peut se faire entre deux agents, ou entre un agent et un acteur humain. Pour cela, les modes de communication reposent sur l'envoi de messages ou le partage d'informations. Il peut y avoir plusieurs langages de communication reposant sur la théorie des actes de langages.

2.3 L'approche par événement discret

Un système à événements discrets est un système dont l'état change de façon discontinue en un certain nombre d'instants pouvant être ou apparaître aléatoires. La simulation par événements discrets (Discreet Event Simulation, habituellement abrégée DES) traite de la modélisation de tels systèmes. L'exemple typique est celui des camions arrivant au poste de transfert de GPL : le poste est un système à événements discrets. L'entrée d'un objet camion constitue un événement qui va modifier l'état du système.

Dans une simulation à événements discrets, on rencontre habituellement les éléments suivants :

- Entités : les objets, les composants par lesquels le système est défini ;
- Ressources : éléments du système fournissant un service ;
- Éléments de contrôles : permettent de modifier la réponse du système à un événement, par l'intermédiaire de switches, compteurs, règles logiques ou arithmétiques... Par exemple, une contrainte horaire (fermeture du site pendant la pause de midi) ;
- Opérations : ce sont les manipulations effectuées par ou sur les entités évoluant au sein du système ;

Les principes de base des SED reposent sur l'initialisation d'une réplique, la gestion des entités, la gestion des évènements, et la création des files d'attente.

2.3.1 Initialisation de la réplique

Une réplique (*replication* ou *run* en anglais) est une exécution d'une simulation. Typiquement, on effectue des séries de répliques pour des simulations comprenant des modèles stochastiques. Ces répliques vont produire des résultats qui seront analysés ensuite hors exécution (*batch* ou *off-line*) par des techniques statistiques telles que Monte-Carlo.

La phase d'initialisation peut parfois nécessiter une part importante du code de la simulation :

- La lecture des paramètres de la simulation et du scénario ;
- L'initialisation des variables (compteur de temps, les variables statistiques...) ;
- La création des entités de la simulation ;
- La détermination des événements peut être prédéterminée (par exemple les événements fixes prévus par le scénario ou les événements aléatoires indépendants). Par exemple, il est possible de déterminer à l'avance, par des tirages aléatoires, la date d'arrivée des camions d'un guichet, sachant que l'écart de temps séparant deux arrivées suit une loi exponentielle. On postera à l'avance tous ces événements dans la file d'événements ;

2.3.2 Gestion des entités

On fait évoluer les entités en fonction de leur modèle comportemental, du

scénario, de leur environnement, des événements qui surviennent, etc. Chacune des entités est une instance d'un ensemble de variables (variables d'état, variables statistiques...), généralement regroupées au sein d'une structure dont l'implémentation typique est une instance de classe. Le moteur de simulation maintien une liste des entités et de leur état. Cette liste peut être implémentée sous diverses formes (listes chaînées, tableaux, arbres...). Chaque entité suit un cycle de vie (création, attente, activité, destruction...), dont la forme est fonction du moteur de simulation utilisé.

2.3.3 Gestion des évènements

Dans une simulation à événements discrets, l'avance du temps est généralement conditionnée par les événements qui se produisent. Il est donc nécessaire, pour que le moteur de simulation puisse calculer le nouveau temps, que soit connue la date du prochain événement (qui, à un instant T donné, se trouve dans le futur à T +DT). Ceci est possible en simulation à événements discrets par la connaissance préalable de l'enchaînement des événements futurs. En effet, comme on l'a vu précédemment à propos de la phase d'initialisation, la date des événements futurs, même aléatoires, peut souvent être prédéterminée soit lors de l'initialisation, soit à une date antérieure à l'événement. C'est pourquoi la simulation n'a pas besoin d'évoluer suivant un temps continu ou un pas de temps régulier : elle peut se contenter de sauter d'un événement à l'autre, à condition toutefois de traiter chaque événement dans l'ordre chronologique (problème de la causalité).

Afin de pouvoir à tout moment déterminer la date et la nature du prochain événement, le moteur de simulation maintient une liste ordonnée chronologiquement de tous les événements générés au cours de la simulation qui n'ont pas encore été traités. Ces événements peuvent être prédéterminés lors de l'initialisation. Néanmoins, d'autres événements peuvent être produits en cours d'exécution. Il faut donc pouvoir stocker tous ces événements dans une structure de données ordonnée et dynamique (création/insertion et destruction fréquentes d'éléments), dont le premier élément (le prochain événement) doit pouvoir être aisément accessible et dans laquelle les opérations d'insertion doivent être simples. La structure de donnée classiquement utilisée en simulation pour cela est la file d'attente ou FIFO (First In, First Out).

2.3.4 Les files d'attente

Les files d'attente (queues) sont des structures de données informatiques de type liste, dans lesquelles l'ajout d'une donnée se fait à une extrémité de la liste, et la lecture à partir de l'autre extrémité. Ainsi, le premier élément stocké dans la file d'attente est le premier lu d'où l'appellation de FIFO.

3. Modélisation multi-paradigmes de la sécurité d'un site industriel

L'approche de simulation à l'aide du logiciel Anylogic suppose que chaque objet du projet soit considéré comme un agent (excepté l'objet Simulation). Chaque agent est un objet d'une classe. Dans le logiciel se trouve une interface New Agent avec assistance permettant de créer les agents : cette interface apparaît lorsque l'on glisse sur le diagramme un élément agent de la palette.

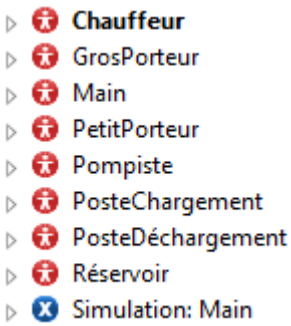


Figure 5-2 Les agent du projet de simulation

La figure 5-2 montre les agents crées dans ce projet. Il s'agit des acteurs du système, par exemple le « Chauffeur », les agents « GrosPorteur », « PetitPorteur ». Les agents « PosteChargement » et « PosteDéchargement » sont des interfaces secondaires qui permettent de suivre le déroulement dynamique par le biais de la simulation les procédures de transfert de GPL.

En termes de modélisation par SED nous avons aussi défini les postes de transfert dans le modèle comme des ressources.

L'agent « Réservoir », quant à lui, est caractérisé par son paramètre « niveau ». De plus, il contient les fonctions permettant le déclenchement des alertes de niveau, ainsi que les fonctions de réinitialisation des événements. Enfin, une couche supplémentaire a été ajoutée permettant de faire fonctionner le modèle à travers différents modes de contrôle, afin de mettre en évidence différentes pertes de contrôle possibles du système.

3.1 Agent Chauffeur

Une population de 400 chauffeurs a été recréée. Chaque chauffeur est un agent décrit par son diagramme état-transitions.

Le but de cet agent est de modéliser les compétences des chauffeurs qui sont formés aux risques que représentent les Gaz de Pétrole Liquéfiés (GPL), au chargement en libre-service sous surveillance d'un pompiste, à l'exploitation pomperie et à la formation Astreinte. Les chauffeurs reçoivent, lors de leur stage de formation et de recyclage (tous les 3 à 5 ans), une formation de base à la lutte contre l'incendie tel que le maniement des extincteurs ou l'extinction de feux réels.

Le diagramme états-transitions est ce qui caractérise les systèmes multi-agents dans AnyLogic. Chaque agent possède son propre diagramme, et il peut passer par n'importe quel état. Il ne peut être que dans un seul état à la fois par diagramme (il pourrait y avoir plusieurs diagrammes états-transitions pour un type d'agent) (figure 5-3).

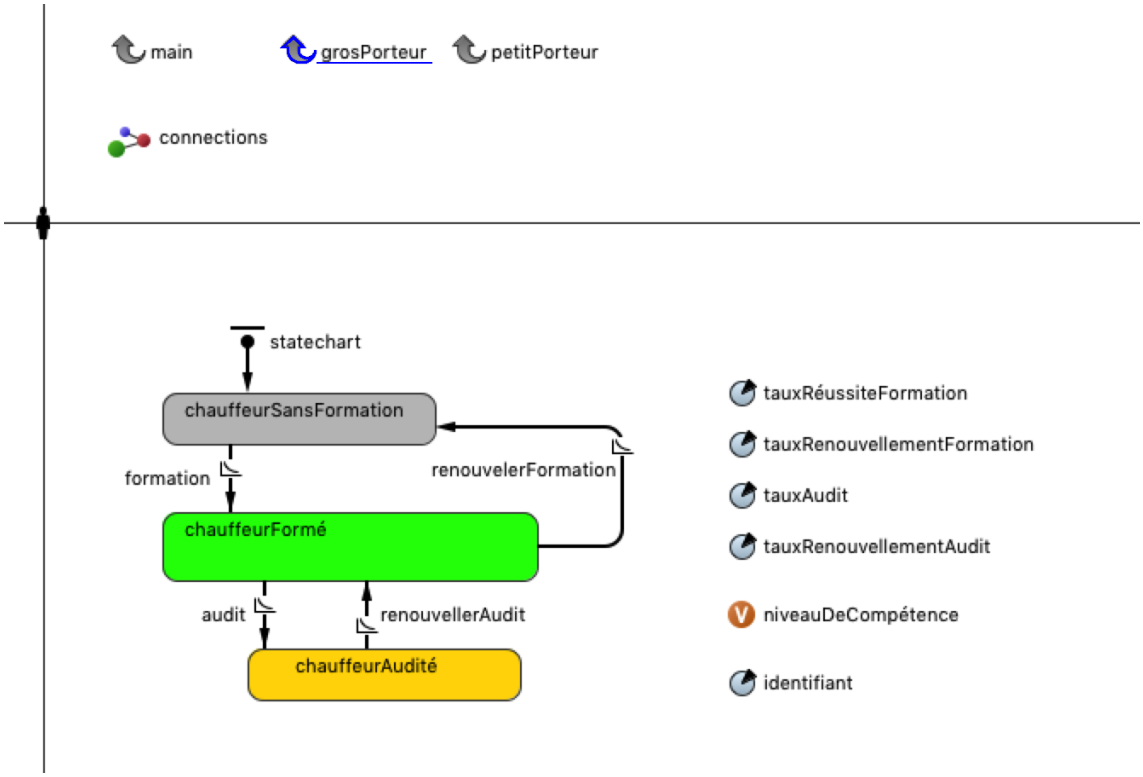
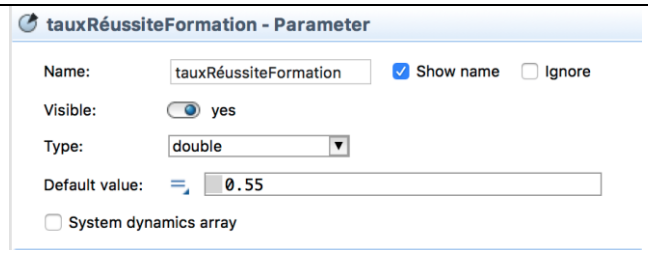
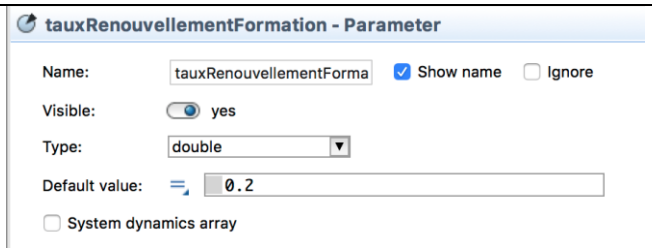
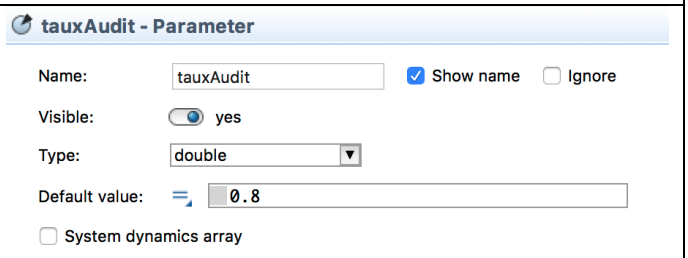
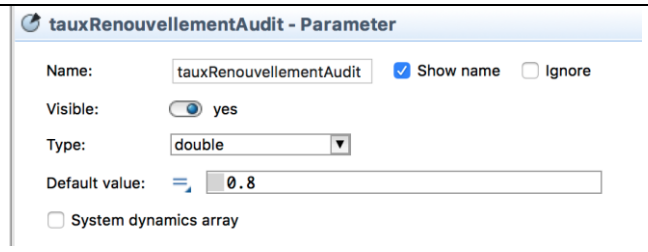
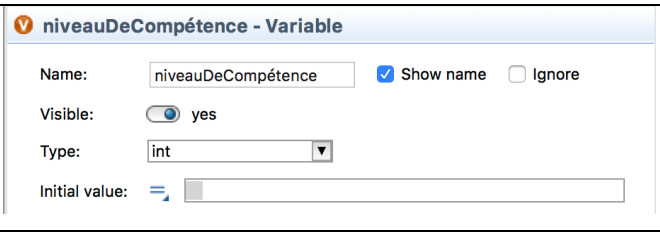
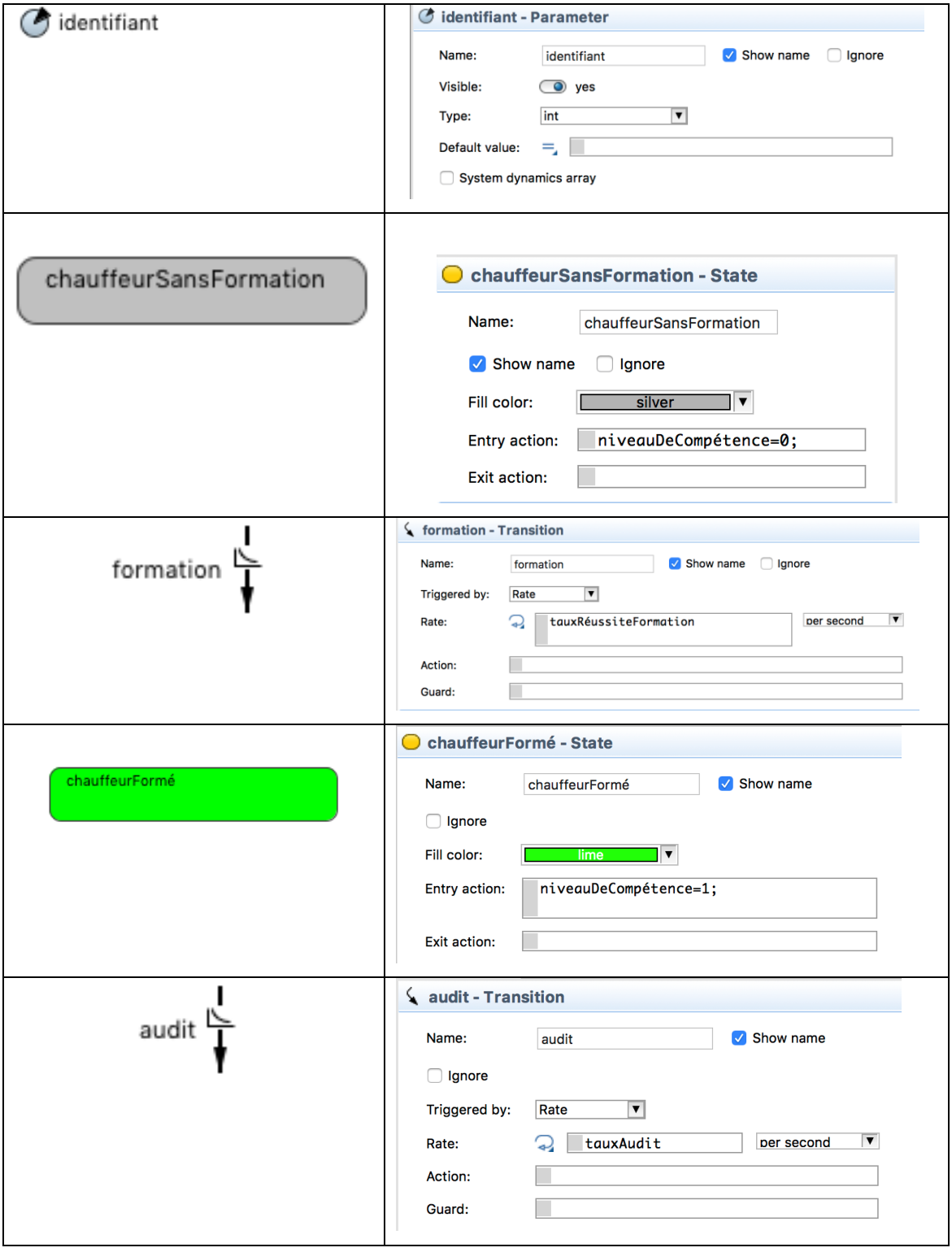


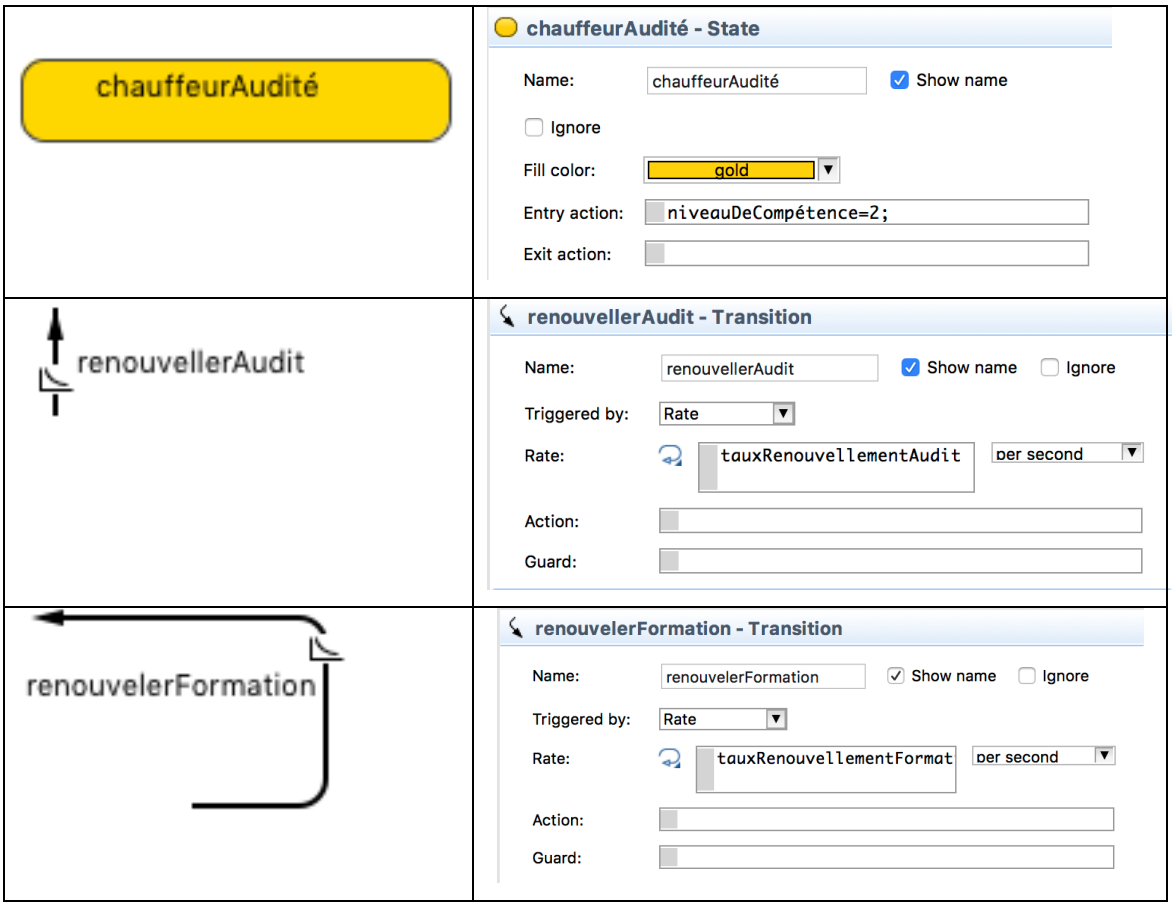
Figure 5-3 Interface agent chauffeur

Le tableau 5-1 explique les éléments présents dans l'interface agent « Chauffeur » et les instructions de code qui régissent le modèle.

Table 5-1: Les éléments du modèle

Eléments	Interface de codage
tauxRéussiteFormation	
tauxRenouvellementFormation	
tauxAudit	
tauxRenouvellementAudit	
niveauDeCompétence	


identifiant
identifiant - Parameter
Name: identifiant
Show name
Ignore
Visible: yes
Type: int
Default value:
System dynamics array
chauffeurSansFormation
chauffeurSansFormation - State
Name: chauffeurSansFormation
Show name
Ignore
Fill color: silver
Entry action: niveauDeCompétence=0;
Exit action:
formation
formation - Transition
Name: formation
Show name
Ignore
Triggered by: Rate
Rate: tauxRéussiteFormation
per second
Action:
Guard:
chauffeurFormé
chauffeurFormé - State
Name: chauffeurFormé
Show name
Ignore
Fill color: lime
Entry action: niveauDeCompétence=1;
Exit action:
audit
audit - Transition
Name: audit
Show name
Ignore
Triggered by: Rate
Rate: tauxAudit
per second
Action:
Guard:



Les chauffeurs, au nombre de 400, changent donc d'état au cours du temps. À un moment donné, chaque chauffeur est passé par chaque état. La formation des opérateurs suit une loi exponentielle de paramètre les taux de transition. La transition se fait entre les états "chauffeurSansFormation", "chauffeurAudité" et "chauffeurFormé" . Ainsi, au cours du temps, on peut avoir une idée des proportions des chauffeurs sans formation, formés ou audités. La figure 5-4 montre un exemple de scénario où moins de 20% des chauffeurs sont sans formation, environ 40% de chauffeurs sont audités et plus de 40% de chauffeurs sont formés.

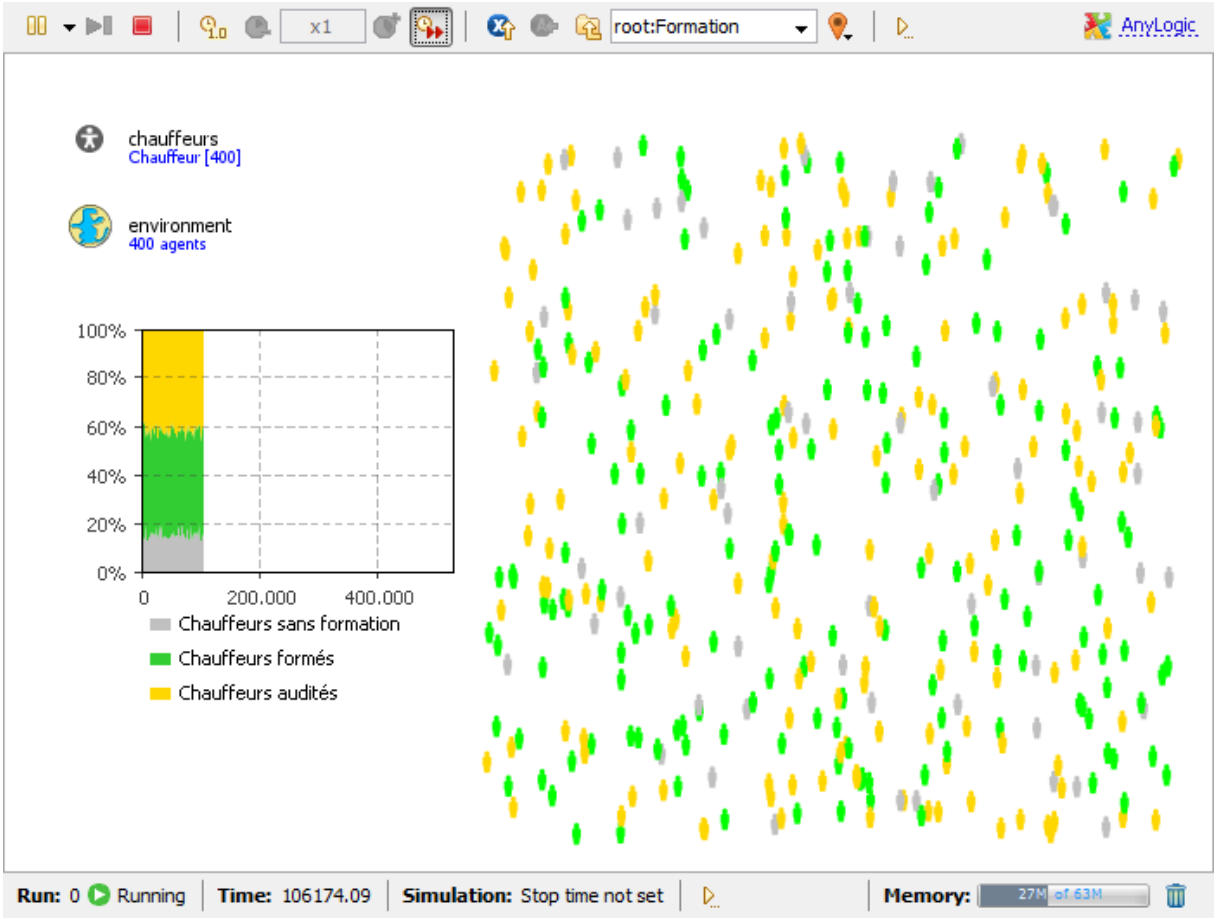


Figure 5-4 Simulation de la formation d'une population de chauffeurs camion gros porteur

3.2 Agent « GrosPorteurs »

Dans cette interface, on crée la population des camions gros porteurs. La figure 5-5 montre objet chauffeur crée pour lier un objet de l'agent « Chauffeur » à un gros porteur.

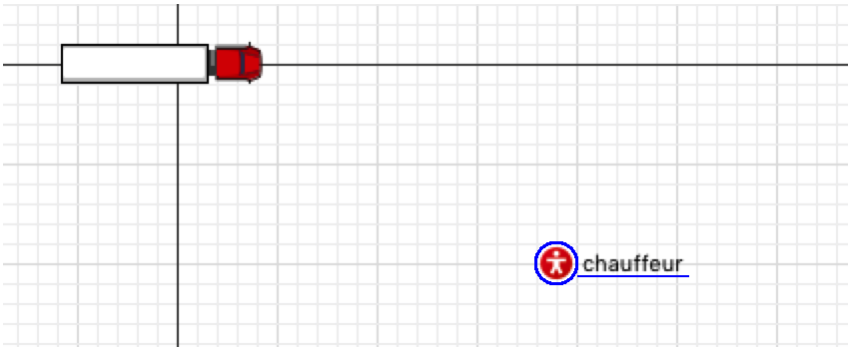


Figure 5-5 Interface agent « GrosPorteurs»

3.3 La classe Main

La classe « Main » est considérée comme l'interface principale du modèle de simulation.

Il s'agit de la photographie (figure 5-6) du site, sur lequel est tracé le réseau nœuds-lignes. Il contient notamment la modélisation SED permettant l'animation 2D. La classe

« Main » comprend aussi un module d'affichage des informations concernant le niveau du réservoir, les résultats du processus d'identification des chauffeurs, le nombre d'erreur de manipulation...

Dans cette partie, nous allons aborder les différents éléments que nous avons placés dans l'interface principale.

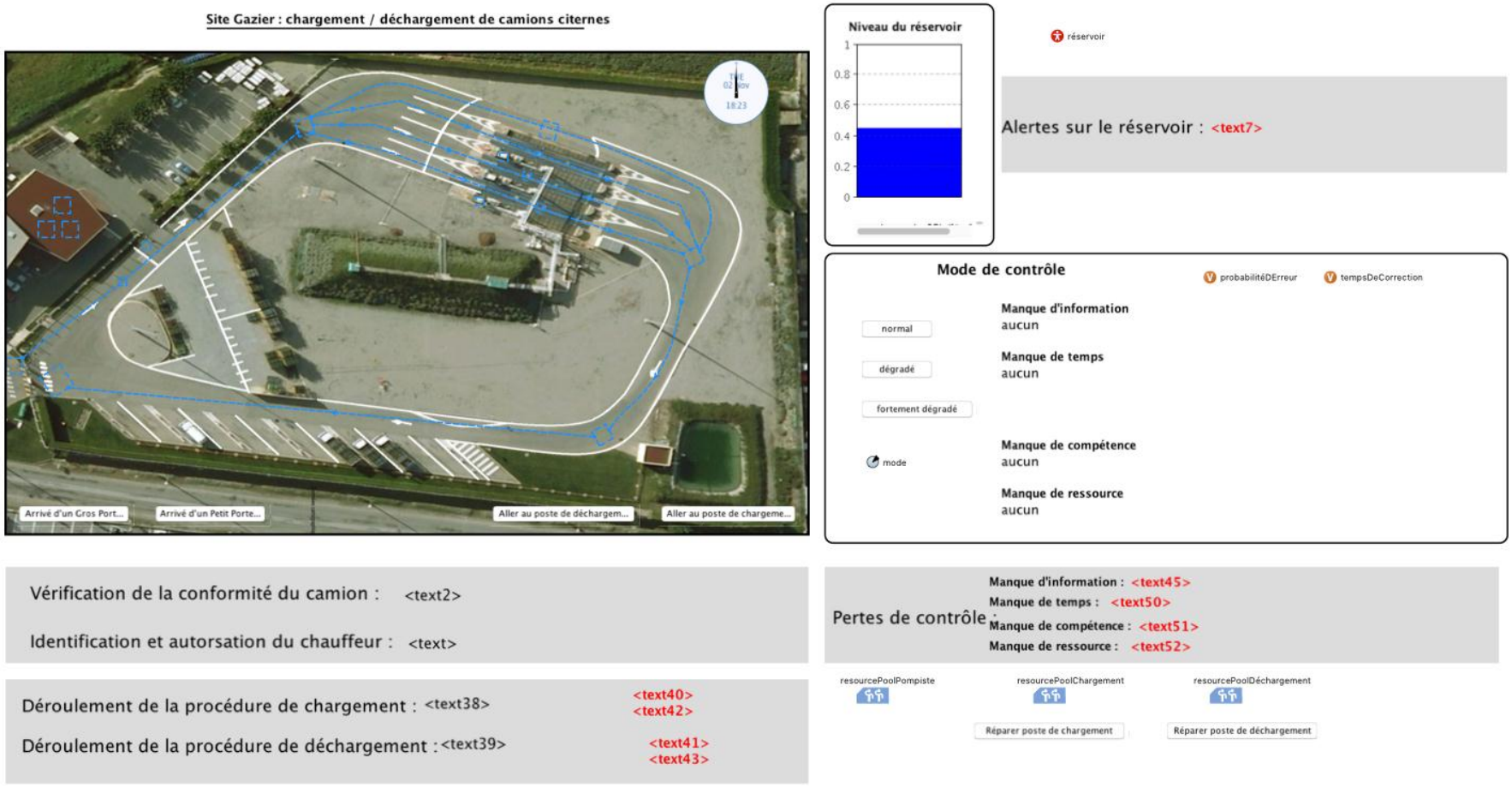


Figure 5-6 Image du site introduite dans la classe main

3.3.1 Les objets utilisés pour la modélisation en système à événement discret SED dans l'interface main

Le premier élément de la figure 5-7 est un objet « source ». Cet élément génère l'arrivée des camions au site de stockage de GPL (figure 5-6). Le deuxième objet permet de modéliser et de simuler une file d'attente. Une file d'attente est créée lorsque :

- Un GrosPorteur est déjà dans le site ;
- Le réservoir est au-delà de 84,5% ;

Un GrosPorteur peut sortir de cet objet de deux manières :

- Soit par la sortie normale, si le temps d'attente est plus inférieur à une heure ;
- Soit par la sortie "T", si le temps d'attente dépasse une heure ;

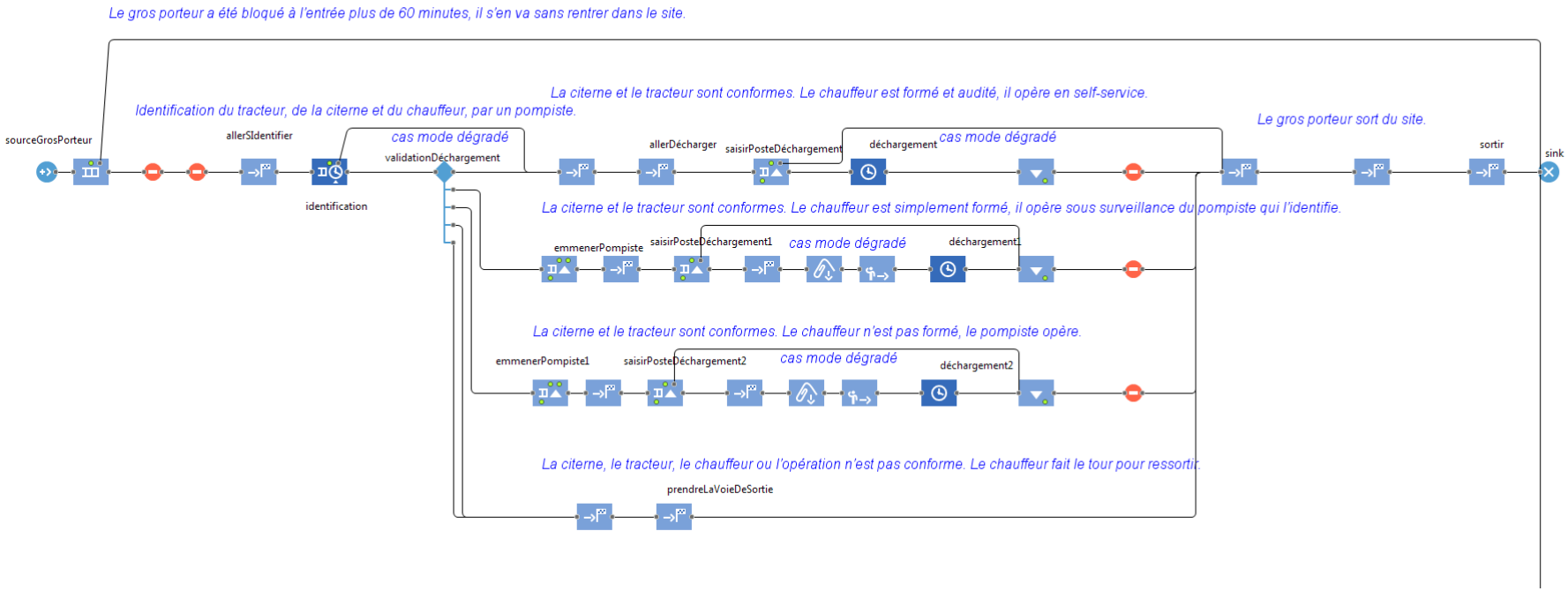
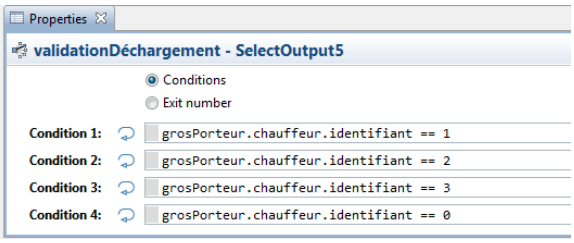


Figure 5-7 Partie SED du Main distinguant les différentes branches possibles selon le niveau de formation du chauffeur du camion gros porteur

Table 5-2: Les éléments du modèle SED dans la classe main

sourceGrosPorteur 	Cet objet génère l'arrivée des camions
queue 	Cet objet dans Anylogic permet la création d'une file d'attente et permet deux possibilités de cheminer un agent : – Chemin de la procédure : C'est le chemin que le GP emploie quand il a fini de faire la queue – Chemin alternatif : C'est le chemin que le GP emploie si il est toujours dans la queue au bout du Timeout : hour()
hold2 	Bloque les gros porteurs lorsque le réservoir atteint un trop haut niveau de GPL. Ce hold initialement ne bloque pas le GP que lorsqu'une alerte de niveau haut est déclenchée. Cet objet débloque le GP lorsque le réservoir revient à son niveau normal
hold5 	Bloque les gros porteurs lorsqu'un gros porteur est déjà dans le site. Un seul gros porteur peut entrer dans le site. (Le prochain GP qui arrive au site tant que le premier n'est pas sorti
allerSIdentifier 	Déplace le GP porteur au nœud « node 1 » qui correspond au point d'identification.
identification 	Cet objet est un service il permet d'assurer le processus d'identification et de vérification
validationDéchargement 	Cette entité permet de continuer l'animation selon les différentes conditions de l'identification 
moveTo 	Dépendamment des cas, elle permet d'animer le déplacement des camions
allerDécharger 	Cette entité déplace l'objet au poste de déchargement donc au nœud « node5 »

saisirPosteDéchargement 	Cet objet « saisirPosteDéchargement » s'assure de la disponibilité de la ressource qui est dans ce cas une ressource « ressourcePoolDéchargement » « static » (PosteDéchargement) Le statut du poste déchargement. De base la capacité du poste est 1. Lorsque le poste est : – Utilisé : Le poste ne peut pas servir un autre camion et une file d'attente est créée – Usé – En Réparation – Endommagé
déchargement 	Cet objet décrit le temps de chaque étape de déchargement selon le mode :
release5 	Cet objet permet de libérer la (les) unité(s) de ressource(s) saisie(s).
hold6 	Cet objet permet de bloquer le gros porteur dans le cas où le temps disponible est écoulé, alors que le temps nécessaire n'est pas fini

moveTo1 	Ce code est exécuté lors de l'arrivée du camion au nœud « node6 »
	//Réinitialise le texte "Identification et autorisation du chauffeur"
	text.setText ("");
	//Réinitialise le texte "Vérification de la conformité du camion"
	text2.setText ("");
	//Réinitialise le texte "Etapes de déchargement" du posteDéchargement
	posteDéchargement.text1.setText ("");
	//Réinitialise le texte "Erreurs / oublis corrigé(e)(s)" du posteDéchargement
	posteDéchargement.text4.setText ("");

moveTo2 	Cet objet permet de déplacer le gros porteur du nœud d'intersection « node6 » au nœud « node10 »

sortir 	Lorsque le camion sort définitivement du site, ce code est exécuté ;
	//Débloquer l'entrée d'un gros porteur dans le site.
	hold5.unblock ();
	//Réinitialise le texte "Déroulement de la procédure de déchargement" et réinitialise sa couleur à noir.
	text39.setText(""); text39.setColor(black);
	//Réinitialise le paramètre "tempsPasséDéchargement" du posteDéchargement à 0.
	posteDéchargement.tempsPasséDéchargement=0;
	//Réinitialise le paramètre "tempsDisponibleDéchargement" du posteDéchargement à 20 minutes (/bug/je ne sais plus si c'est utile/debug/).
	posteDéchargement. tempsDisponibleDéchargement=20*minute ();
	//Réinitialise le texte affichant le nombre d'erreurs/oublis durant la procédure de déchargement.
	text41.setText ("");
	//Reinitialise le texte affichant le comportement du chauffeur face à un retard.
	text43.setText ("");
	//Réinitialise le texte "Manque d'information"

	text45.setText (""); //Réinitialise le texte "Manque de temps" text50.setText (""); //Réinitialise le texte "Manque de compétence" text51.setText (""); //Réinitialise le texte "Manque de ressource" text52.setText ("");
sink	Fin de l'animation pour une source donnée

Les objets « hold » permettent de bloquer les entités. C'est pourquoi ils sont souvent précédés d'un objet « queue », modélisant une file d'attente. D'ailleurs, si l'attente dépasse un certain temps, l'entité peut être redirigée dans une autre branche du SED. Dans la figure 5-8 le 3ième et le 4ième objet qui représentent un « hold » :

- Bloque les gros porteurs lorsque le réservoir atteint un trop haut niveau de GPL.
- Bloque les gros porteurs lorsqu'un gros porteur est déjà dans le site. Un seul gros porteur peut entrer au site.

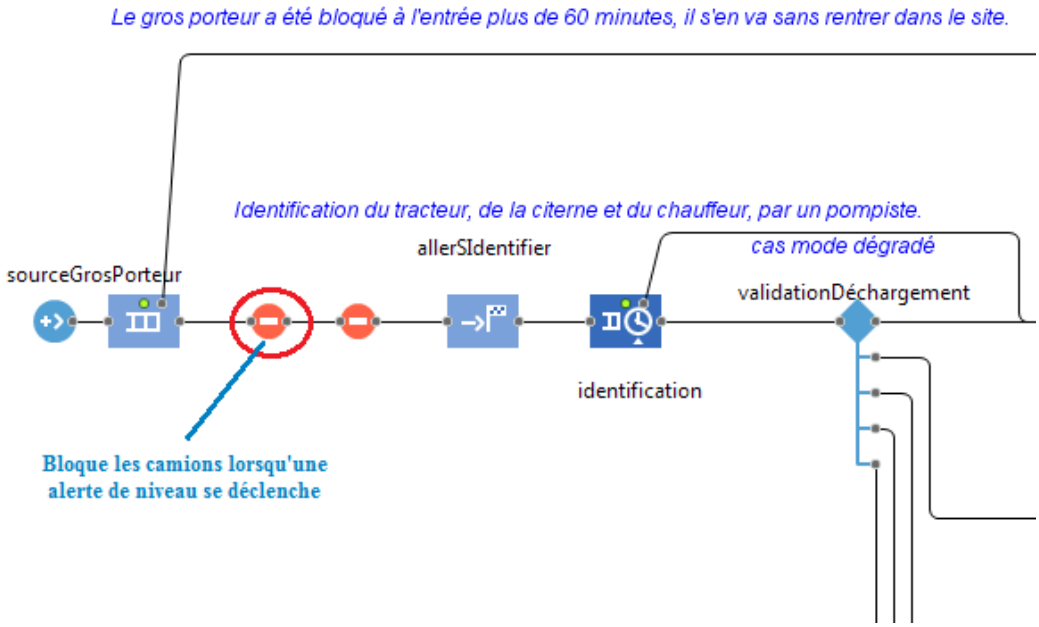


Figure 5-8 Conséquence du déclenchement de l'alerte niveau bas sur le système d'événements discrets.

L’objet « allerSIdentifier » permet le déplacement du GP de l'entrée du site nœud <node> vers le nœud destiné à l'identification <node1>.

L’objet (Service) « identification » (figure 5-7,5-8), permet d’orienter l’agent vers l’une des 2 bornes de sortie de cet objet en fonction des instructions du code informatique, la sortie par l’une des deux bornes peut alors assurer selon des conditions, aléatoirement ou en indiquant par instruction de ligne de code le numéro de la borne de sortie.

Pour assurer la fonction d’identification, cet objet « Service » nécessite la sollicitation d’une entité nommée dans la librairie du logiciel « Ressource Pool ».

Table 5-3: Explication des objets du diagramme SED

Objets		
Service 	Ressource Pool 	Ressource Pool 
Deux objets assurent l’identification : – Service : Un service est constitué de trois sous objets encapsulés (Seize + Delay + Release) • Seize : cet objet sollicite une unité de ressource de la RessourcePool (RessourcePoolPompiste) • Delay : cet objet retarde le camion pendent un certain temps (2*minutes) • Release : cet objet relâche l’unité sollicitée – RessourcePool : cet objet possède plusieurs unités. Elles peuvent être de 3 types (Moving, Static, Portable) : • Moving : ce type permet aux unités de se déplacer • Static : ce type ne permet pas aux unités de se déplacer • Portable : ce type permet aux unités d’être portées par des agents (ne se déplace qu’avec un agent)		

Trois pompistes sont présents dans la salle de contrôle : à l'arrivée d'un camion, l'un se déplace selon la disponibilité définie dans l'objet « ressourcePoolPompiste ».

Avant la sortie de cet objet (On at exit), la fonction « Identification » de l'interface agent « Pompiste » est sollicité (figure12). Le résultat de cette fonction est enregistré dans le paramètre « identifiant » dans l'interface agent « Chauffeur ».

Le contrôle s'effectue dans l'interface Agent Pompiste par sollicitation de la fonction <Identification> voir (section 3.2).

L'hypothèse de départ est qu'un camion-citerne (petit porteur ou gros porteur) est entré dans le site et s'est arrêté au stop. En termes de simulation, cela signifie qu'une des deux sources a généré un agent (petit ou gros porteur), et que cet agent a atteint l'objet Service, appelé « identification ». Ainsi, le pompiste est appelé (une unité de ressource « pompiste » est saisie), l'identification prend quelques minutes, puis, à la sortie de l'objet service, la fonction « Identification » du pompiste est appelée (prenant le chauffeur en argument) et renvoie un chiffre (1, 2, 3 ou 0) (Figure 5-7, 5-8). L'objet (SelectOutput5) nommé « validationDéchargement » oriente l'agent vers une des bornes de sorties dépendamment du paramètre identifiant.

Table 5-4: Orientation de l'objet (SelectOutput5)

identifiant= 0	identifiant= 1	identifiant= 2	identifiant= 3
La citerne, le tracteur, le chauffeur ou l'opération n'est pas conforme. Le chauffeur fait le tour pour ressortir.	La citerne et le tracteur sont conformes. Le chauffeur est formé et audité, il opère en self-service.	La citerne et le tracteur sont conformes. Le chauffeur est simplement formé, il opère sous surveillance du pompiste qui l'identifie.	La citerne et le tracteur sont conformes. Le chauffeur n'est pas formé, le pompiste opère.
Sorties 4 et 5	Sortie 1	Sortie 2	Sortie 3

3.3.2 Alertes sur les réservoirs

A chaque fois que le réservoir est sollicité (lors des opérations de transfert), son niveau augmente ou diminue.

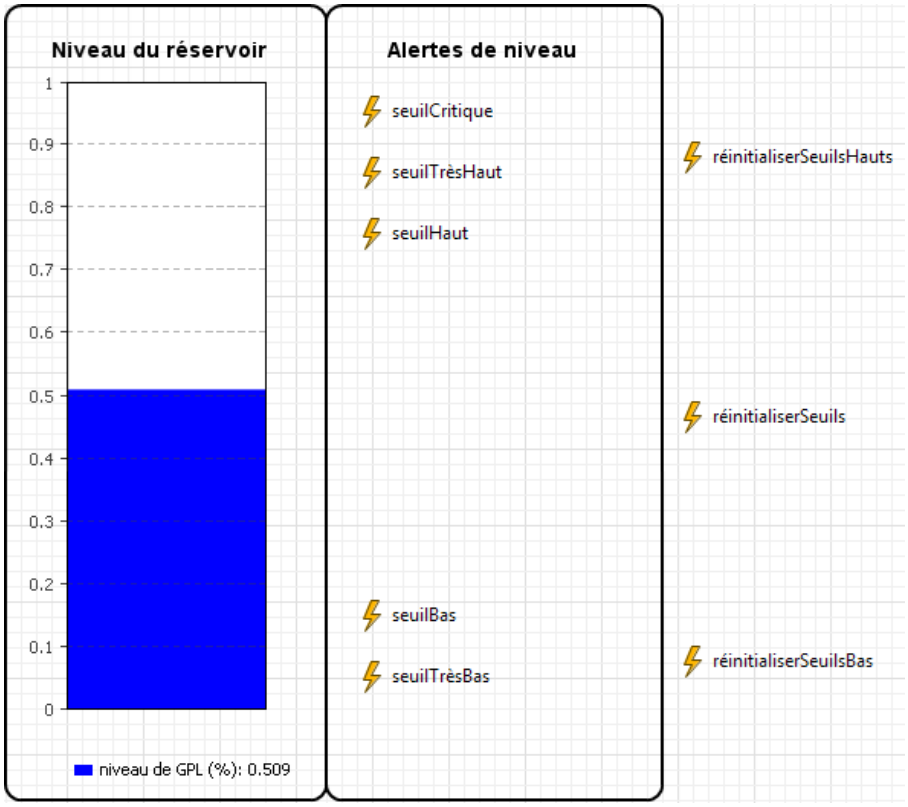


Figure 5-9 Evénements pouvant se déclencher lorsque le niveau du réservoir varie

Cette alerte est le résultat du déclenchement d'un objet « event » conditionnel, la condition étant que le niveau du réservoir est inférieur à 10%.

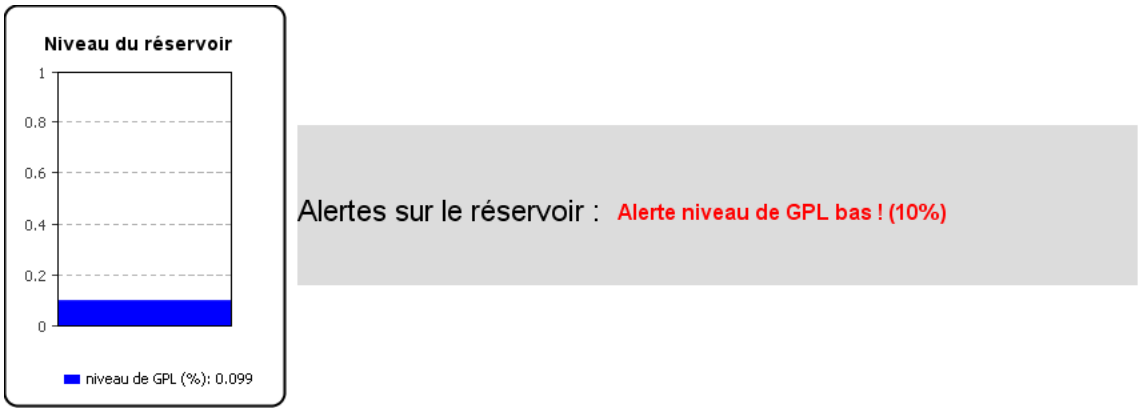


Figure 5-10 Alerte de niveau bas sur le réservoir.

Le déclenchement de l'événement « seuilBas » exécute une fonction qui, d'une part, bloque les camions correspondant à l'entrée du site, et d'autre part réinitialise les autres événements conditionnels. Les autres alertes fonctionnent d'une manière similaire.

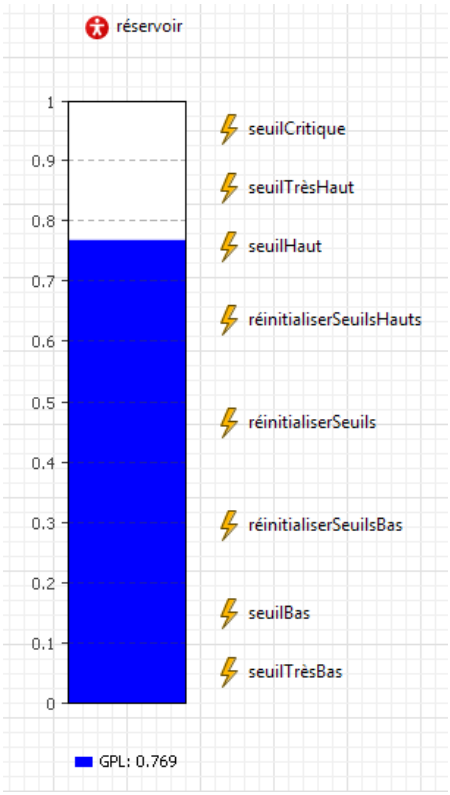


Figure 5-11 Réservoir et différents événements liés.

3.3.3 Les différents modes de contrôle des opérations

Cette interface (figure 5-12) permet d'afficher les actions dangereuses exercées par les agents et qui peuvent conduire à des incidents et des accidents.

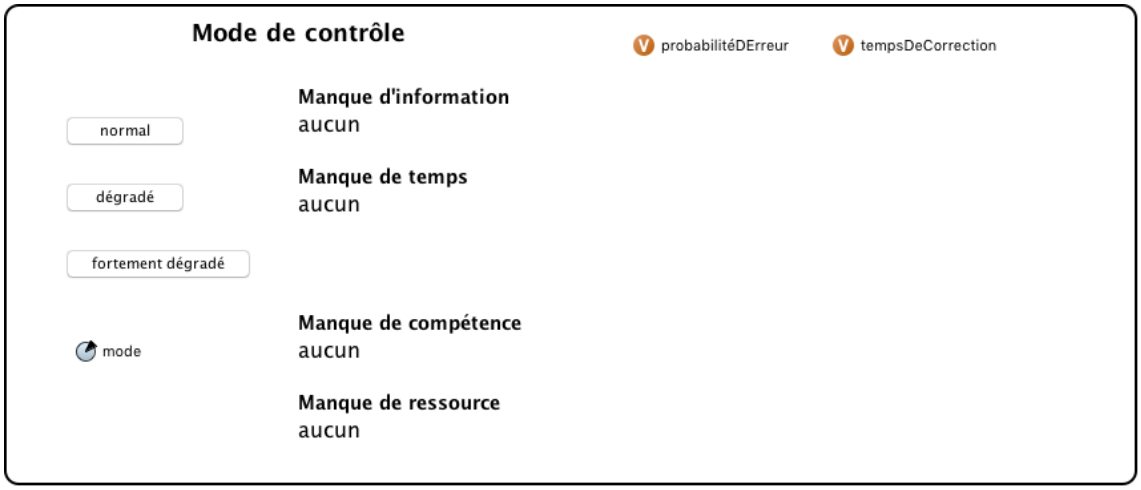


Figure 5-12 Panneau de contrôle : mode dégradé

Vérification de la conformité du camion : Tracteur et citerne conforme.

Identification et autorsation du chauffeur : Le chauffeur est simplement formé. Le pompiste est déjà occupé.

Figure 5-13 Perte de contrôle manque de ressource pompiste

Pertes de contrôle :
Manque d'information : Un chauffeur non-audité opère sans être identifié.
Manque de temps :
Manque de compétence :
Manque de ressource :

Figure 5-14 Conséquence du manque de ressource pompiste.

Déroulement de la procédure de déchargement : Temps disponible : 1530.0 secondes Nombre d'erreurs : 3
Temps nécessaire : 1471.25 secondes Le chauffeur accélère

Pertes de contrôle :
Manque d'information :
Manque de temps : Le chauffeur est en retard
Manque de compétence :
Manque de ressource :

Figure 5-15 Perte de contrôle : manque de temps entrainant une volonté d'accélérer.

Déroulement de la procédure de déchargement : Temps disponible : 1380.0 secondes Nombre d'erreurs : 5
Le chauffeur accélère

Pertes de contrôle :
Manque d'information :
Manque de temps : Le chauffeur est en retard
Manque de compétence : Une succession d'erreurs a usé le poste de déchargment.
Manque de ressource : Un poste de déchargement est usé.

Figure 5-16 Perte de contrôle : cascade de manque de temps, compétence, et ressource.

3.4 L'agent Pompiste

L'agent « Pompiste » est une ressource saisie par les « petitPorteur » et « gros-porteur » lors de leur entrée dans le site. C'est lui qui exécute le processus d'identification, redirigeant les chauffeurs sans formation, formés et audités dans des branches différentes du SED. La classe
« Pompiste » est considérée comme une sous-classe de la classe « Agent ». Un diagramme états-transitions peut naturellement être utilisé pour savoir ce que fait et ce que peut faire cet agent (figure 5-17).

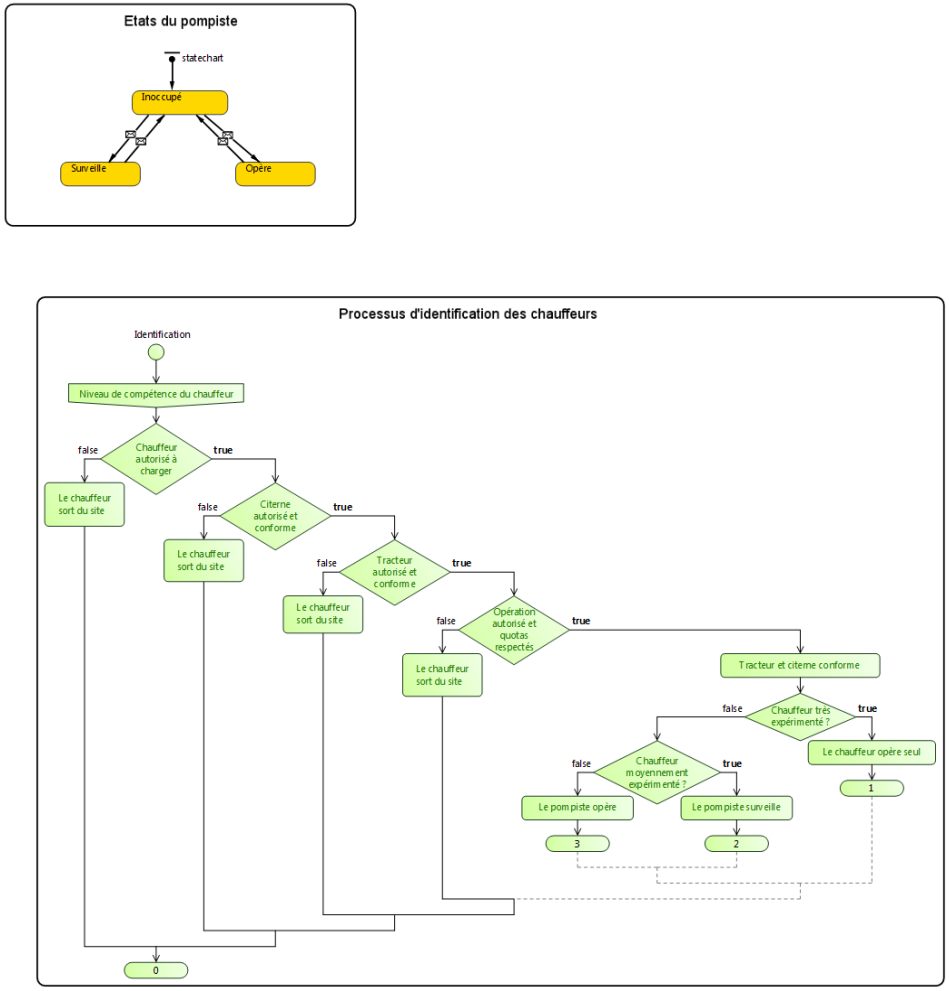


Figure 5-17 Interface de l'agent pompiste

Les objets « pompiste » issus de la classe « Pompiste » sont considérés comme des unités de ressources mobiles (ils peuvent se déplacer au travers du réseau lignes-nœuds). Ils sont au nombre de trois en mode normal (ils sont deux en mode dégradé et il n'y en a qu'un en mode fortement dégradé). Leur vitesse de déplacement a été calculée en pixels/heure grâce à une règle de trois (600 pixels correspondent à 112,5 m sur la photographie, et un homme est supposé marcher à 5 kilomètre/heure). Lorsque les pompistes sont inoccupés, ils occupent les nœuds 9, 12 et 14 dans le réseau.

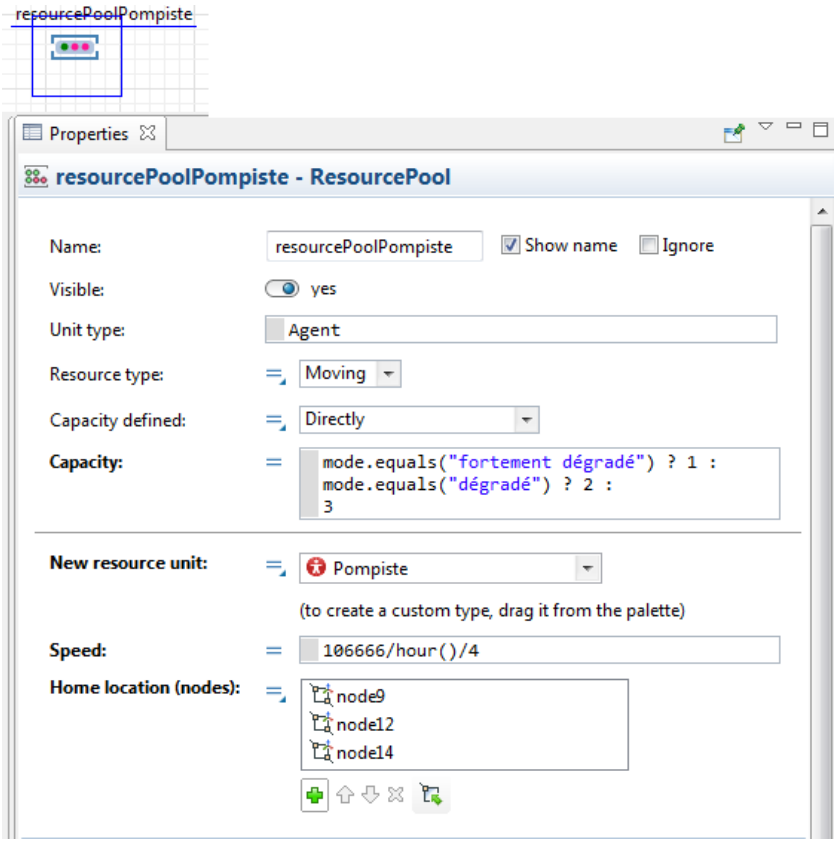


Figure 5-18 Propriété de la ressource "Pompiste" et des unités de ressources "pompistes"

Cette fonction est exécutée lorsque le pompiste identifie le chauffeur et son camion-citerne dans l'objet « identification » du SED figure 5-7.

Elle renvoie un code chiffré selon le niveau de compétence du chauffeur figure 5-3, ce qui le redirige dans une des quatre branches.

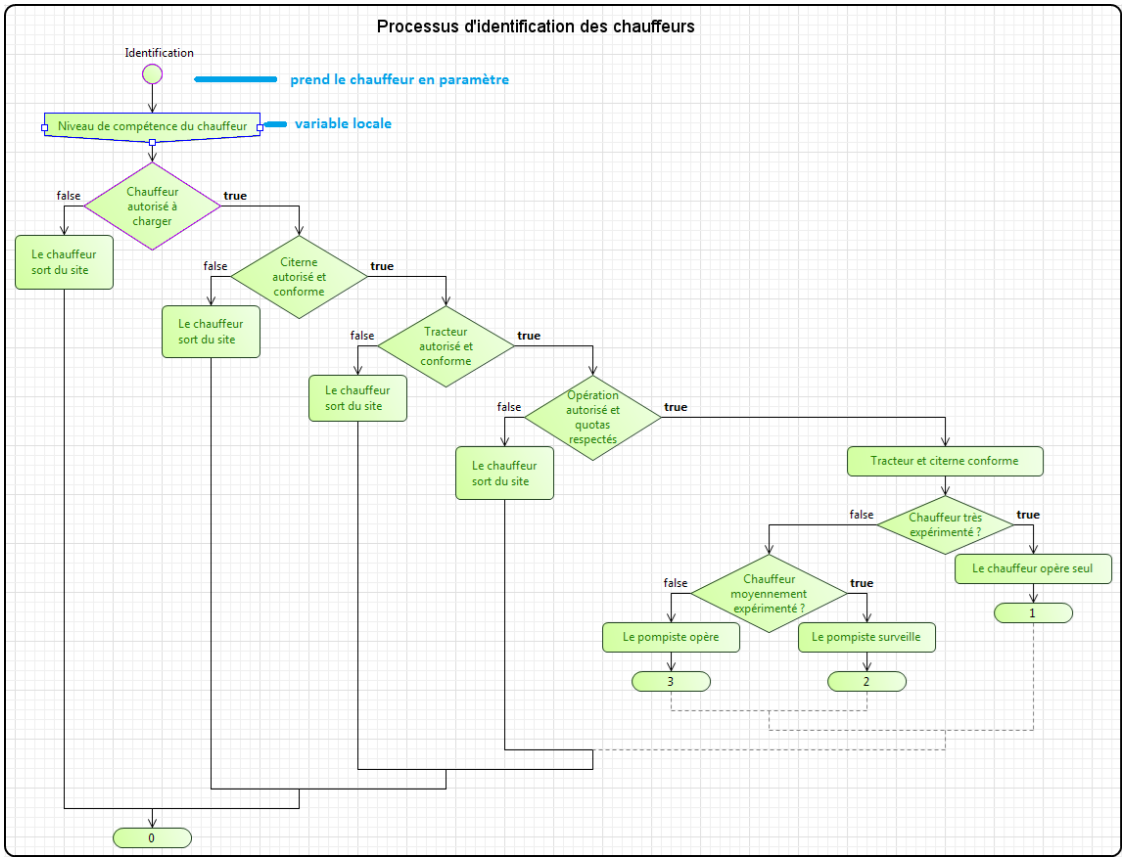


Figure 5-19 Actionchart de la fonction d'identification des chauffeurs par le pompiste

3.4.1 Les composants de l'actionchart

L'approche consiste à s'assurer, à travers le travail des pompistes, que toute personne se présentant sur le site détient les compétences pour effectuer les opérations de transfert. Pour cela, nous avons construit à l'aide de la palette « actionchart » du logiciel Anylogic la fonction

« Identification », qui, en soit, est un emboitement de « if, else », Elle est écrite sous forme de diagramme graphique ce qui permet d'avoir une meilleure représentation et moins de problèmes liés au fait de savoir dans quelle partie du « if » ou du « else » se trouve telle ou telle autre instruction.

3.5 Poste de déchargement

L'hypothèse de départ est qu'un camion-citerne (petit porteur ou gros porteur) est entré dans le site et s'est arrêté au stop. En termes de simulation, cela signifie qu'une

des deux sources a généré un agent (petit ou gros porteur), et que cet agent a atteint l'objet service, appelé « identification ». Ainsi, le pompiste est appelé (une unité de ressource « pompiste » est saisie), l'identification prend quelques minutes, puis, à la sortie de l'objet service, la fonction « Identification » du pompiste est appelée (prenant le chauffeur en argument) et renvoie un chiffre (1, 2, 3 ou 0).

Figure 5-20 Camion gros porteur arrêté pour identification

Dans le cas où la fonction renvoie le chiffre « 1 », alors le chauffeur peut opérer en en self-service.

Vérification de la conformité du camion : Tracteur et citerne conforme.

Identification et autorsation du chauffeur : Le chauffeur est formé et audité. Il opère seul.

Figure 5-21 Résultat de l'identification (premier cas)

Si l'identification renvoie le chiffre « 2 », alors le chauffeur peut opérer sous surveillance du pompiste.

Vérification de la conformité du camion : Tracteur et citerne conforme.

Identification et autorsation du chauffeur : Le chauffeur est simplement formé. Le pompiste surveille.

Figure 5-22 Résultat de l'identification (second cas)

Si la fonction d'identification renvoie le chiffre "3", alors le pompiste opère et le chauffeur regarde.

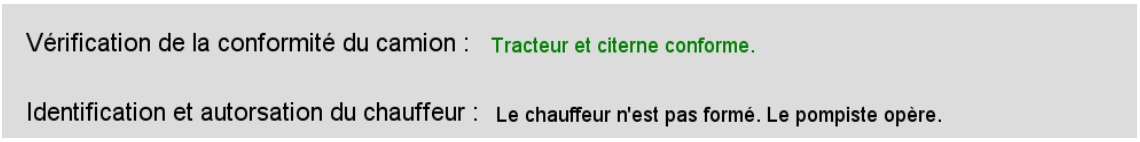
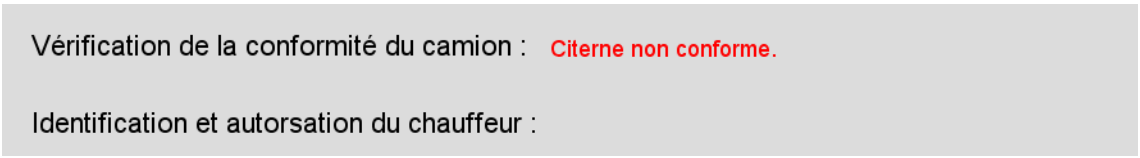


Figure 5-23 Résultat de l'identification (troisième cas)

Finalement, si la fonction renvoie le chiffre « 0 », le chauffeur doit faire le tour et ressortir du site. Il y a quatre cas où la fonction renvoie « 0 » : le chauffeur n'a pas l'autorisation, le tracteur n'est pas conforme, la citerne n'est pas conforme ou les quotas ne sont pas respectés.



3.5.1 Procédure de transfert

Chacun des éléments du système d'événements discrets est un « delay ». Chaque délai représente le temps moyen écoulé pour réaliser une étape de la procédure de transfert. Par exemple, la procédure de déchargement se décompose en trois phases de plusieurs étapes :

- Début du déchargement
- Fin du déchargement
- Débranchement

La modélisation de ce processus revient à modéliser uniquement le temps de chacune de ces étapes. Ces étapes sont modélisées de la sorte dans le logiciel de simulation. On définit d'abord les variables et les paramètres suivants.

probabilitéDErreur	Probabilité d'erreur	Cette variable définit la probabilité qu'un opérateur fasse une erreur lors d'une opération de chargement ou de déchargement.
tempsDisponibleDéchargement	Temps Disponible de déchargement	Ce paramètre représente le temps disponible pour effectuer le transfert. Il correspond au temps du délai (déchargement/déchargement1/déchargement2) dans l'interface principale. Il est utilisé ici pour déclencher les événements "manqueDeTempsDéchargement" et "retardDéchargement".
tempsNécessaire	Temps nécessaire	Ce paramètre permet de compter le temps nécessaire de toute la procédure. A chaque fois qu'une étape est résolue, on ajoute à ce paramètre le temps qu'elle a pris.
tempsPasséDéchargement	Temps passé au déchargement	Ce paramètre compte le temps déjà passé dans la procédure de déchargement. Il est utilisé ici pour déclencher les événements "manqueDeTempsDéchargement" et "retardDéchargement".
tempsMoyenDUneOpération	Temps moyen d'une opération	Ce paramètre représente le temps moyen d'une étape dans la procédure. Souvent ce temps est multiplié par 2 ou 3 selon la complexité de l'opération.
NombreDErreurs	Nombre d'erreur	Ce paramètre permet de compte le nombre d'erreurs lors de la procédure. Il est utilisé, dans le statechart1, pour transité de l'état "Opérationnel" à "Usé" et de "Usé" à "Endommagé".
NombreDUtilisations	Nombre d'utilisation	Ce paramètre permet de compter le nombre de fois que le poste a été utilisé. Il est utilisé, dans le statechart1, pour transité de l'état "Opérationnel" à "Usé" et de "Usé" à "Endommagé".
manqueDeTempsDéchargement	Manque de temps de Déchargement	Signal à l'opérateur qu'il ne lui reste qu'une minute et demie pour finir la procédure
CorrectionDeLErreurDéchargement	Correction de l'erreur de déchargement	L'opérateur a fini de corriger l'erreur
retardDéchargement	Retard dans le déchargement	Signal à l'opérateur qu'il est officiellement en retard.
opérationDéchargementCourante	Opération de déchargement courante	Cette variable permet d'enregistrer l'opération courante. Elle est utilisée dans l'événement "CorrectionDeLErreurDéchargement" pour pouvoir faire repartir la procédure.

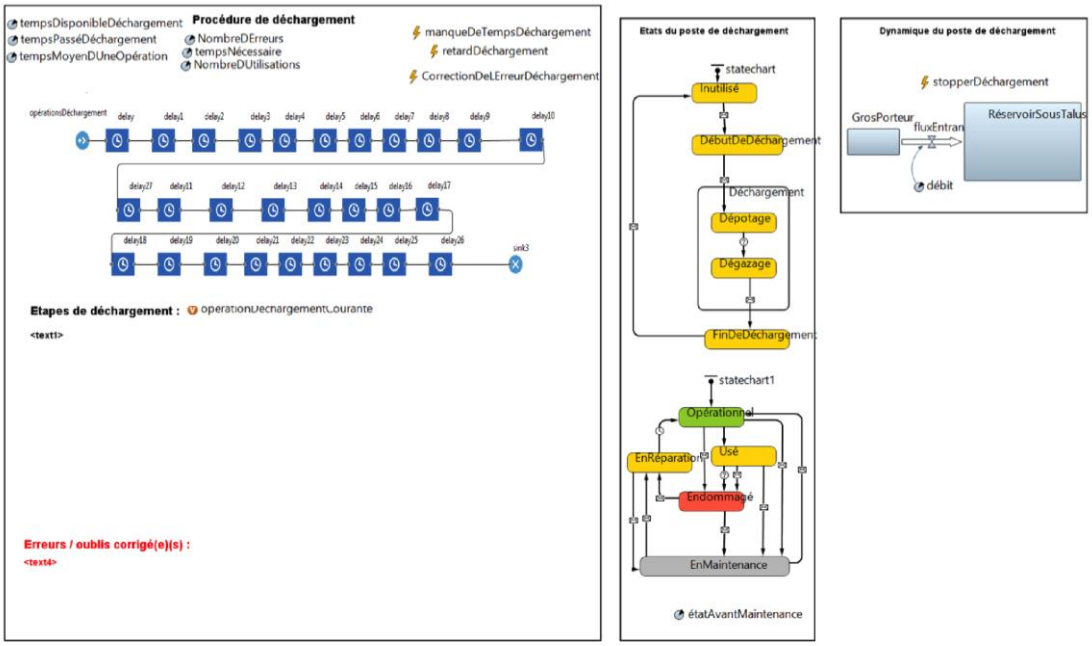


Figure 5-24 Résultat de l'identification (quatrième cas)

Delay	**Etape**
« delay »	Calage du véhicule
« delay 1 »	Vérification du bon positionnement de la vanne 4 voies sur la position déchargement
« delay 2 »	Vérification de l'absence de liquide dans le ballon anti-envahissement
« delay 3 »	Branchement de la pince du DCMT sur la prise de la citerne (attendre que le voyant blanc s'allume)
« delay 4 »	Branchement du CISC
« delay 5 »	Branchement des bras liquide et gazeux aux orifices de remplissage (vérification que les deux bras sont bien sortis
« delay 6 »	Ouverture du clapet de fond et les vannes de la citerne
« delay 7 »	Vérification de l'étanchéité des raccords
« delay 8 »	Ouverture de la vanne d'extrémité des bras liquide et gazeux afin d'équilibrer la pression entre le camion et le réservoir
« delay 9 »	Enclenchement du bouton Marche de la télécommande à cordon
« delay 10 »	Mise en route du compresseur
« delay 27 »	Déchargement

« delay 11 »	Enclenchement du bouton Arrêt
« delay 12 »	Les vannes de pied de bras se ferment
« delay 13 »	Fermeture de la vanne de la canalisation liquide de la citerne et du bras liquide
« delay 14 »	Passage de la vanne 4 voies du compresseur sur la position Aspiration
« delay 15 »	Aspiration de la citerne jusqu'à une pression de 2 bars
« delay 16 »	Les vannes de pied de bras se ferment automatiquement
« delay 17 »	Arrêt du compresseur
« delay 18 »	Fermeture de la vanne d'extrémité du bras gazeux
« delay 19 »	Fermeture de la vanne de la canalisation gazeuse et les clapets internes du camion-citerne
« delay 20 »	Purge de l'extrémité des bras liquide et gazeux
« delay 21 »	Débranchement des bras (rangement sur leur support)
« delay 22 »	Remise des bouchons sur les orifices de la citerne
« delay 23 »	Retour de la vanne 4 voies du compresseur sur la position Déchargement
« delay 24 »	Débranchement du CISC
« delay 25 »	Débranchement le câble de mise à la terre et l'accrocher sur son support
« delay 26 »	Enlèvement et rangement des cales

Table 5-5: modélisation des étapes du processus de déchargement

La modélisation de ce processus revient à modéliser uniquement le temps de chacune de ces étapes. Ce temps aléatoire suit une loi de Bernoulli. Il vaut zéro avec la probabilité « probabilitéDErreur » et vaut son temps moyen avec la probabilité complémentaire.

A chaque fois qu'une phase commence, un message est envoyé au diagramme « statechart » pour effectuer la transition vers le nouvel état.

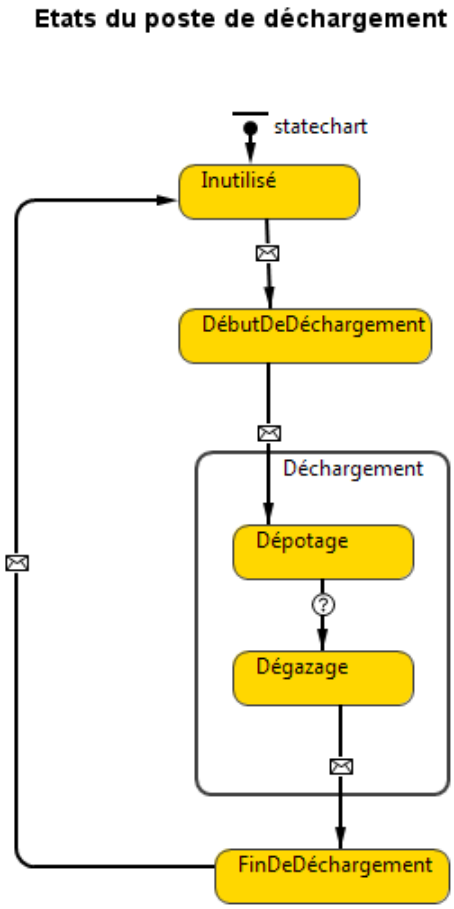


Figure 5-25 Diagramme états-transitions procédural du poste de déchargement

Les transferts entre les camions citernes et le réservoir sont modélisés par des diagrammes en DS.

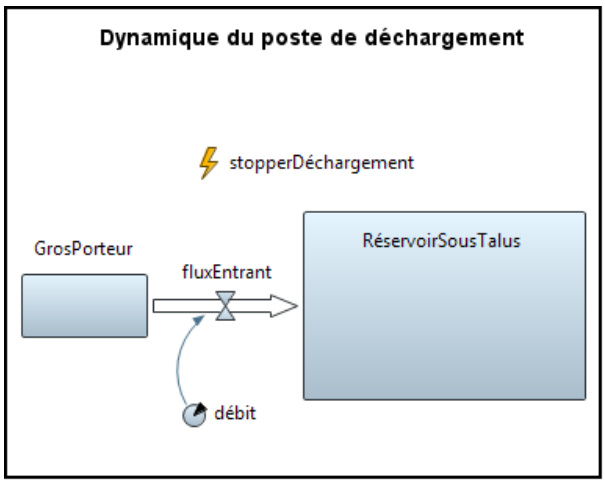


Figure 5-26 Diagramme stock-flux du poste de chargement

Le lien entre le SED modélisant les étapes et la DS modélisant le transfert est réalisé grâce à un diagramme états-transitions représentant les grandes phases du processus. L'état
« inutilisé » transite vers « débutDeDéchargement » lorsque la première étape débute puis le passage de « débutDeDéchargement » à « Déchargement | Dépotage » fait varier le paramètre
« débit » créant la dynamique du système. De la même manière, l'événement
« stopperDéchargement » se déclenche lorsque le camion est vide, ce qui fait transiter l'état
« Dépotage » à « Dégazage ». Finalement, lorsque le délai représentant le déchargement se termine, un message est envoyé au « statechart » passant à l'état « FinDeDéchargement » jusqu'à ce que toutes les étapes soient terminées.

Un second diagramme d'états-transitions permet de modéliser les états opérationnels du poste.

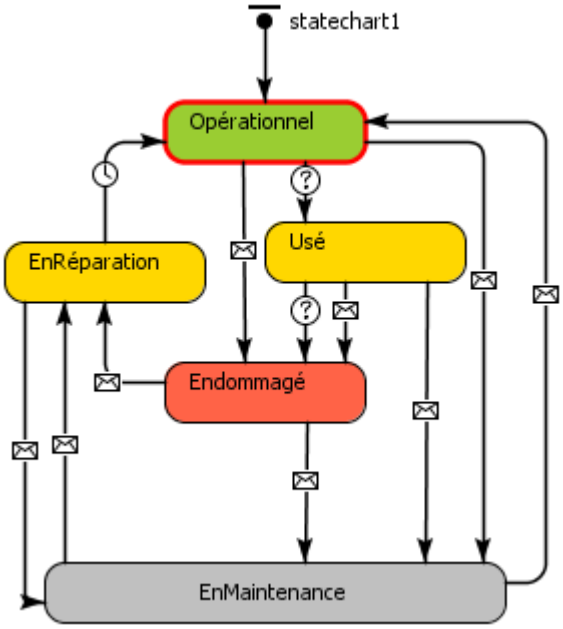


Figure 5-27 Diagramme états-transitions opérationnel du poste de chargement

Le poste de transfert peut passer de l'état « Opérationnel » à « Usé » lorsqu'un chauffeur a réalisé un grand nombre d'erreurs lors de la procédure (j'ai supposé qu'à

force de faire des erreurs, l'une d'entre-elles avaient des chances d'user le matériel), ou bien lorsque le poste de transfert a été utilisé un grand nombre de fois.

Les états « Endommagé » et « EnMaintenance » peuvent s'activer avec les nouvelles propriétés « Failure » et « Maintenance » de l'objet « RessourcePool ». Enfin, l'état « EnRéparation » est activé par l'utilisateur grâce à un bouton présent dans le « Main » côté interface. La transition d'« EnRéparation » à « Opérationnel » prend quatre heures.

3.5.2 Compilation du modèle au poste de déchargement

L'hypothèse de cette démonstration suppose que l'identification a renvoyé les chiffres « 1 », « 2 » ou « 3 ».

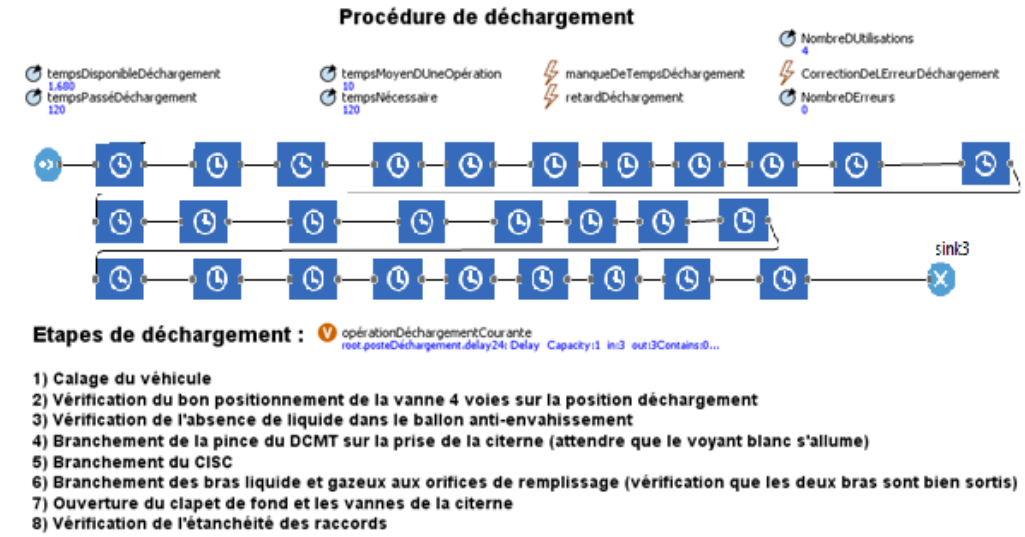


Figure 5-28 Début de déchargement. Vue en système d'événements discrets.

Une unité de ressource poste de chargement ou poste de déchargement est saisie et l'opération prend plusieurs dizaines de minutes. En effet, à l'entrée de l'objet délai « déchargement », une entité est injectée dans la source « opérationsDéchargement » du SED du poste de déchargement. Cette entité représente l'avancement de l'opérateur dans la procédure de déchargement.

Erreurs / oublis corrigé(e)(s) :

2) Vérification du bon positionnement de la vanne 4 voies sur la position déchargement
3) Vérification de l'absence de liquide dans le ballon anti-envahissement
9) Ouverture de la vanne d'extrémité des bras liquide et gazeux afin d'équilibrer la pression entre le camion et le réservoir

Figure 5-29 Phase 1 : début de déchargement. Etapes oubliées ou mal réalisées.

Lorsqu'une erreur ou un oubli se produit, l'événement « CorrectionDeLErreurDéchargement » de type « temps d'arrêt » se déclenche. Au bout du temps « tempsDeCorrection », l'étape est résolue et la procédure se poursuit.

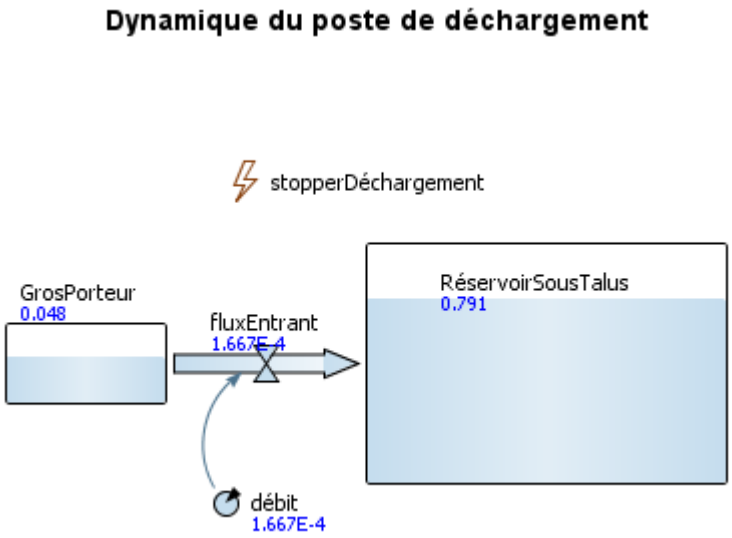


Figure 5-30 Phase 2 : Fin de déchargement. Vue en dynamiques de système.

Le transfert est modélisé avec un modèle DS simple, le camion et le réservoir sont reliés par un flux dont la valeur passe de zéro à une valeur positive.
Lorsque le diagramme « statechart » transite d'un état vers un autre, cela peut influencer la modélisation dynamique du poste de transfert. En pratique, lorsque le chargement débute, le stock « RéservoirSousTalus » est actualisé à sa nouvelle valeur et le stock « PetitPorteur » est initialisé à la valeur zéro. Puis, lorsque le poste de chargement transite vers l'état « FinDeChargement | Dépotage », le paramètre « débit » prend sa valeur positive et le GPL s'écoule du réservoir vers le camion.

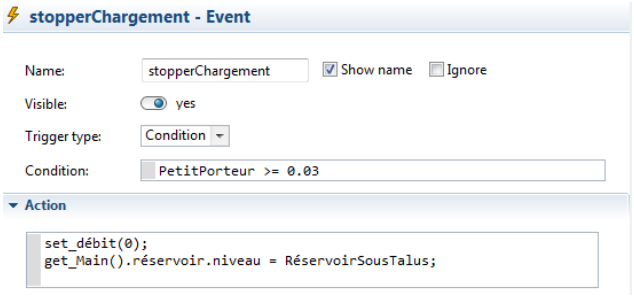


Figure 5-31 Propriété de l'événement « StopperChargement » déclenché par condition (le petit porteur est rempli quand il atteint 3% du volume du réservoir.

L'arrêt se fait grâce aux objets « stopperChargement » et « stopperDéchargement ». Ces objets sont des événements. Ils se déclenchent quand la condition est satisfaite (PetitPorteur >= 0.03 ce qui correspond à 3% du volume du réservoir sous talus et GrosPorteur < 0). Dans ce cas, le code contenu dans la case « Action » est exécuté, c'est-à-dire le paramètre « débit » passe à zéro et le niveau du réservoir est mis à jour.

4. Conclusion du chapitre

En utilisant les trois paradigmes de modélisation-simulation, nous avons pu construire un modèle pour le management de la sécurité d'un système. L'outil AnyLogic nous a permis d'évaluer les procédures de sécurité mises en place sur le site industriel gazier. L'objectif a été d'abord d'évaluer la procédure d'identification mise en place et qui sert à empêcher l'entrée de personnes non fichées sur site. L'approche consiste à modéliser le comportement du camion-citerne, le chauffeur et le pompiste. Un objet du paradigme fonctionnel, la fonction « identification », relie les déplacements à l'intérieur du site en fonction de la formation des chauffeurs. Ensuite pour les opérations de transferts, les risques majorants de ce site de relai-vrac de gaz propane liquide (GPL), ont été modélisés. Les trois approches de modélisation coopèrent pour rendre compte à la fois des étapes de la procédure, et aussi de la possibilité d'oubli, voire d'erreur, d'une ou plusieurs étapes. De plus, le niveau du réservoir sous talus, contenant le GPL, a été relié à des alertes. Celles-ci se déclenchent lorsque le réservoir atteint un niveau inquiétant (soit trop haut, soit trop bas). Grâce aux objets événements, de type conditionnel, le système d'événements discrets bloque les camions susceptibles d'augmenter ce risque. Enfin, une couche supplémentaire couvre les trois points précédents, illustrant le fonctionnement du système au travers de trois modes. Le mode normal peut être dégradé deux fois, entrainant des pertes de contrôle du système, ou illustrant le maintien du contrôle dans un

environnement dégradé. Les pertes de contrôle sont expliquées au travers de quatre facteurs : l'information, le temps, la compétence, et la ressource.

CONCLUSIONS ET PERSPECTIVES

Cette thèse a consisté à concevoir et mettre en œuvre une démarche méthodologique qui a permis, pas à pas, de coupler le modèle d'accident STAMP à une plateforme logicielle de simulation, Anylogic. Un cas d'application a été choisi : un site de stockage/distribution de Gaz Propane Liquide (GPL). Le cas a fait l'objet d'une importante collecte de données et d'une modélisation fine.

L'effort de modélisation du système a permis de se représenter le système industriel, et donc de se l'approprier, en insistant sur ses propriétés mises en évidence au cours de la simulation de son comportement. L'utilisation d'un environnement de modélisation (STAMP) et d'un outil de simulation (Anylogic) ont été particulièrement utile pour comprendre la complexité du système en considérant tout à la fois les dimensions techniques, humaine et organisationnelle. Cela s'est révélé aussi comme un possible support de communication, et de formation, des opérateurs, des responsables du site et des services de l'Etat. A ce stade, les travaux de thèse ont permis très concrètement :

- D'évaluer les propriétés critiques intrinsèques du contrôle de la sécurité du système industriel.
- De proposer une architecture de contrôle de sa sécurité.
- De développer un cahier des charges des recommandations issues de l'analyse des risques.
- De documenter la logique de conception.
- De soumettre les résultats de l'analyse, par le recours aux résultats de STAMP et aux différentes simulations, aux experts et ingénieurs de la sécurité du système industriel.

Trois perspectives se dessinent à court, moyen et long terme et selon des directions tout à la fois académique et résolument opérationnelle.

A court terme, il conviendrait de rédiger un guide méthodologique à visée pédagogique afin d'expliciter les étapes de la mise en œuvre de STAMP et STPA sur un cas donné. Ce guide pourrait servir de base à une offre de formation pour les industriels

en se fondant sur une approche comparée entre les outils traditionnels de l'analyse des risques, pour la plupart issus de la sureté de fonctionnement, et STAMP.

A moyen terme, il serait particulièrement intéressant d'approfondir le travail initié sur les Systèmes Multi-Agents à l'aide d'Anylogic afin de mieux caractériser les dimensions humaines et organisationnelles. Puisqu'un système multi-agents (SMA) est un système composé d'un ensemble d'agents, situés dans un certain environnement et interagissant selon certaines relations, cela nous apparait une voie particulièrement adaptée. Objet de longue date de recherches en intelligence artificielle distribuée, les systèmes multi-agents forment en effet un type intéressant de modélisation de « sociétés », et ont, à ce titre, des champs d'application larges allant jusqu'aux sciences humaines. De fait, il nous parait particulièrement opportun de les convoquer pour participer à la modélisation et à la simulation des situations à risque.

A long terme, à la suite d'une revue de littérature bien plus étoffée que celle réalisée dans le cadre de cette thèse et sur une période longue, il serait pertinent de réfléchir à la création d'une ontologie sur les modèles d'accidents. Les ontologies peuvent être divisées en trois catégories en fonction du niveau de représentation :

- Ontologies de haut niveau (utilisées pour la conceptualisation de concepts généraux tels que l'évènement)
- Ontologies de domaine (en rapport avec un domaine particulier comme la médecine, la gestion de crise ou dans un secteur industriel donné (pétrole, nucléaire…)
- Ontologies d'application (liées à un thème particulier au sein d'un domaine de connaissances spécifique ; par exemple, les équipes d'urgentistes d'un hôpital ou la description d'une pollution par hydrocarbures…)

Un premier état de l'art a été conduit. Quelques auteurs ont produit des ontologies dans le champ des « catastrophes, accidents, urgences »:(Babitski et al. 2009; Delir Haghighi et al. 2013; Batres et al. 2014). Ces ontologies sont des ontologies d'applications et sont clairement axées sur la partie opérationnelle de la gestion d'accidents et d'urgences ; dans un but d'améliorer l'efficacité des services d'urgences notamment. Signalons aussi les travaux de (Provitolo, Dubos-Paillard, et Müller 2009) qui présentent une ontologie de domaine des risques et catastrophes. Dans le secteur

industriel, il existe une ontologie de domaine « Intégration de données de cycle de vie pour les industries de "process", y compris les usines de production de pétrole et de gaz». Cette ontologie est devenue la norme IS015926. Cette ontologie semble plus être une ontologie descriptive et il y a débat sur sa structure (Leal 2005). Enfin, il existe des ontologies de haut niveau sur les évènements, notamment les travaux de (Gangemi et al. 2002; Kaneiwa, Iwazume, et Fukuda 2007; Scherp et al. 2009). Ces ontologies pourraient être un support pour nous aider à concevoir une ontologie de haut niveau mais il est plus probable que notre ontologie sera une ontologie de domaine ou d'application principalement fondé sur le retour d'expérience de grands accidents.

ANNEXE

Apport de la modélisation STAMP dans l'analyse des risques et la prévention des accidents : le cas des opérations d'enlèvement sur les FPSOs

Contribution of STAMP model in accident analysis; the case of offloading operations on FPSO

Dahlia Oueidat, Thibaut Eude

MINES ParisTech, PSL Research University, CRC - Centre de recherche sur les risques et les crises, CS 10207 rue Claude Daunesse 06904 Sophia Antipolis Cedex, France.

dahlia.oueidat@mines-paristech.fr

Résumé

STAMP est une nouvelle approche inventée par le MIT pour modéliser les accidents. Elle reprend les théories des systèmes et de la cybernétique développées au milieu, du XXe siècle. La démarche consiste à l'élaboration d'une analyse des risques sur les actions commandées par les systèmes de contrôle (automatisé, semi-automatisé avec superviseur humain),. Cette approche se démarque du paradigme utilisé dans les industries pétrolières et gazière puisqu'elle permet de parcourir l'ensemble de la structure sociotechnique d'un système pour comprendre l'accident. Ce modèle permet de mieux évaluer la contribution des facteurs technique, humain et organisationnel à l'accident. Dans ce papier le modèle STAMP est utilisé pour analyser l'accident survenu sur un FPSO du Golfe de guinée.

Summary

In order to understand an accident process in a highly technological system, it is necessary to take into consideration the complexity of the underlying feedback structure. In highly complex sociotechnical systems, such as those encountered in the petroleum industry, new types of safety issues and disastrous failure modes cannot be addressed within the traditional approach of accident analysis. Indeed, accident analysis cannot rely solely on the cause-effect approach, but must also take into account the safety control structure in addition to the process of enforcement of safety constraints in the system. It is therefore necessary to seek new approaches that reveal not only the control structure of the system (i.e. retroaction between system components over time), but also to understand the processes of regulation and safety that govern its behavior. Recent developments in systems theory and in particular the STAMP model, based on the control theory developed by the team led by Professor Nancy Leveson of MIT, allow to cover three basic concepts (safety constraints, hierarchical safety control structure and process models) when dealing with accident analysis. Collectively, these combined models help reveal the dynamic behavior that triggers the migration of the system in an accidental process. Indeed, by identifying the safety control structure and the safety constraints that were violated due to inadequate decisions and control actions, accidents can be understood more accurately. The aim of our research work is to provide a viable methodology based on system thinking and system theory approach for the analysis of accidents in the oil and gas industry. In this paper STAMP approach is applied to analyze an accident that occurred to an oil and gas marine installation.

Introduction

L'industrie pétrolière et gazière offshore utilise des systèmes FPSO (Floating Production Storage and Offloading) depuis les années 1970. Ces unités sont généralement déployées pour l'exploitation et la production dans les eaux profondes. Un système de production offshore est constitué d'une infrastructure de production construite sur le plancher océanique (Subsea Production System), d'un FPSO (Floating Production Storage and Offloading) une plateforme flottante de production et de stockage et d'une bouée de chargement vers un navire pétrolier. Cette bouée export (la transaction commerciale est accompagnée d'une transaction douanière puisque la cargaison quitte le pays producteur au moment de l'enlèvement), sur laquelle le navire enleveur (pétrolier) vient s'amarrer et se connecter pour y recevoir sa cargaison, est le maillon-clé de l'opération d'enlèvement. Ces installations assurent donc l'ensemble des processus de production du pétrole ; l'extraction, le traitement, le stockage dans les réservoirs du FPSO et finalement le chargement vers le tanker. Le système de stockage dans les réservoirs du FPSO est complexe en raison de la grande quantité de volume attribué et de la démarche à entreprendre pour garantir l'intégrité, la flottabilité et la stabilité de cette unité flottante. Les mouvements (chargement, déchargement, enlèvement, et transferts internes) doivent être effectués selon des critères bien définis ; autrement la coque pourrait être endommagée en raison des charges inégalement réparties. Les opérateurs à bord sont chargés de planifier les opérations et de s'assurer du bon déroulement des activités. Les travaux de recherche présentés dans ce papier, ont pour objet d'approfondir les axes de réflexion autour des modèles d'analyse des risques et de prévention des accidents. Plusieurs approches ont été explorées, la méthode STAMP (System Theoretic Accident Model and Processes) (N. Leveson 2011) a été retenue. L'approche consiste à formaliser les règles, directives et mesures de sécurité sur chaque système d'une structure hiérarchique d'organisation chargée du contrôle de la sûreté de fonctionnement et des opérations d'une installation industrielle donnée. Tout système sociotechnique étant régi par différents organismes et autorités de régulation, le système d'étude comprend plusieurs niveaux hiérarchiques permettant de contrôler les opérations industrielles de l'installation. Ces niveaux (technique, humain,

organisationnel, autorités réglementaires, organismes gouvernementaux) sont à considérer lors d'une analyse des risques. Cette approche permet ainsi de comprendre comment la structure chargée de contrôler la sécurité du système s'adapte pour maintenir les opérations et le fonctionnement conformément aux paramètres recommandés (Oueidat et al. 2015).

Objectifs de l'étude

Ce papier a pour but d'exposer les résultats obtenus dans l'étude de l'accident survenu sur un FPSO du golfe de Guinée en utilisant une approche systémique d'analyse accidentelle. La conséquence a été le déversement accidentel d'hydrocarbure en mer depuis une bouée d'enlèvement du FPSO, située à plusieurs dizaines de kilomètre au large des côtes. L'accident s'est produit durant une opération de transfert commercial, un enlèvement, de pétrole brut vers un pétrolier. L'objectif de l'étude est de proposer une démarche holistique et systémique permettant d'établir une structure dynamique et rétroactive de contrôle et de maîtrise de la sécurité des opérations de chargement et d'enlèvement d'un FPSO. Un rapport d'accident a été rédigé sur les bases d'un modèle conceptuel d'analyse d'accident traditionnel reposant sur le principe de causalité linéaire et évènementielle. Le déroulement des évènements est clairement décrit et un litige est remarqué dans le choix de la cause principale (évènement primaire déclencheur de l'accident).

Les données reportées dans ce rapport d'accident sont utilisées afin de démontrer, avec l'aide de STAMP, qu'il existe d'autres facteurs et causalité systémique impliqués dans le processus de l'accident. Le modèle d'accident CAST (Causal Analysis based on STAMP) offre un cadre permettant d'étudier l'ensemble du système sociotechnique. Le processus d'implémentation des mécanismes de contrôle de la sécurité depuis la phase de conception, à la phase de développement et des opérations est étudié . Un des objectifs du modèle CAST est de fournir à l'exploitant un retour d'expérience sur l'accident, ainsi qu'un moyen de réingénierie des mécanismes de contrôle du processus et de suivi du déroulement des opérations en sécurité.

Méthodologie de l'étude

La méthode STAMP privilégie la notion de « contrainte », plutôt que celle d'événement (Hardy et Guarnieri 2012). Les modèles traditionnels d'accident expliquent habituellement la cause des accidents selon une série d'événements, alors que l'approche STAMP considère l'accident comme le résultat d'un manque de contraintes (théorie du contrôle) imposées sur la conception du système et pendant le déploiement opérationnel. Ainsi, le processus qui provoque les accidents peut être compris comme des lacunes dans les boucles de contrôle entre les composants du système lors de la conception, du développement, de l'implémentation et des opérations d'exploitation. Ces failles peuvent être classées et utilisées pendant l'analyse de l'accident ou pendant l'activité de prévention des accidents pour aider à identifier tous les facteurs impliqués dans l'accident. Pour analyser l'accident sur le FPSO, on procède en analysant les instructions de sécurité qui ont été violées à chaque niveau de cette structure de contrôle.

Le modèle de causalité systémique CAST fondé sur STAMP (Leveson, 2012) est alors utilisé dans la démarche de l'analyse de l'accident. La démarche peut servir ainsi de guide aux enquêteurs dans la préparation des questions de l'enquête. Une analyse STAMP pour les rapports d'accident nécessite des informations cruciales pour bien comprendre les processus de perte de contrôle. Cette méthode est largement utilisée dans l'analyse des accidents industriels majeurs (Dong 2012; Kim, Salman, et Kjell 2016; McCarthy 2013; Spiegel et al. 2013; Q. Yang et Tian 2015; Underwood 2013a). Les principales étapes de l'analyse CAST sont au nombre de neuf :

Etapes	Description
	Identifier les systèmes et les dangers impliqués dans le processus de l'accident.
	Analyser les risques de chaque système, et identifier les directives de sécurité et les instructions imposées par le système de contrôle de la sécurité pour la prévention des accidents
	Documenter la structure de contrôle de la sécurité en place. Les rôles et les responsabilités de chaque acteur du système dans la structure. La documentation doit inclure les rôles et les responsabilités de chaque acteur du système, ainsi que les commandes fournies dans le but de contrôler la sécurité de l'installation.
	Déterminer les événements conduisant à la perte de contrôle du système.
	Analyser la perte au niveau du système de l'installation technique : il s'agit d'identifier la contribution à l'accident : des manques de contrôle physique et opérationnel, des pannes techniques, des interactions dysfonctionnelles, des défauts de communication et de coordination et des perturbations non gérées. Il faut aussi déterminer les raisons pour lesquelles les contrôles techniques en place étaient inefficaces pour prévenir le danger.

	Après avoir dessiné la structure de contrôle hiérarchique de la sécurité, la démarche consiste à parcourir chaque niveau de la structure et comprendre les failles dans les instructions et les modes d'exécution des directives de sécurité. Le modèle suppose que les directives de sécurité sont imposées selon une structure hiérarchique. Une instruction est donc émise par un composant d'un niveau hiérarchique supérieur et exécutée par un composant de niveau hiérarchique inferieur. Le modèle suppose que soit cette instruction n'ait jamais été assignée à l'un des composants de la structure, soit la hiérarchie n'a pas exercé un contrôle adéquat pour s'assurer que les instructions étaient exécutées conformément aux mesures de sécurité recommandées. Le processus décisionnel et les commandes inadéquatement exécutées sont alors étudiés. Pour cela, il convient de recueillir les informations dont dispose le décideur ainsi que toute information qui n'était pas disponible, le contexte et les influences sur le processus décisionnel.
	Évaluer la coordination et la communication entre les opérateurs au moment de l'accident.
	Identifier les changements dans le système lié à l'affaiblissement de la structure de contrôle de la sécurité au cours du temps
	Proposer des recommandations. En général, la description du rôle de chaque composant dans la structure de contrôle doit comporter ce qui suit : Les instructions et les directives de sécurité Les mécanismes et processus de contrôles Contexte Rôles et responsabilités. En général, la description du rôle de chaque composant dans la structure de contrôle doit comporter ce qui suit : Les instructions et les directives de sécurité Les mécanismes et processus de contrôles Contexte Rôles et responsabilités. Facteurs environnementaux et conditionnement opérant (les mécanismes de conditionnement du comportement, le contexte d'influence sur le processus de prise de décision). Interactions dysfonctionnelles, défaillances, et processus décisionnels incorrects conduisant à une déviance dans l'exécution de la procédure Raisons pour lesquelles les actions de contrôle étaient défectueuses et les interactions dysfonctionnelles Défauts d'algorithme de contrôle Modèles de processus ou interface incorrectes. Mauvaise coordination ou communication entre plusieurs contrôleurs Défauts de canal de référence Défauts de rétroaction

Les étapes sont décrites ci-après.

Etape 1 : Présentation du système analysé et des dangers du système

Le terrain d'observation et d'exploration de cette thèse est le système de transfert d'hydrocarbures entre le FPSO et les navires pétroliers. Ce système comprend deux lignes de transfert flexibles de diamètre 18,5'' pour le transfert de pétrole du FPSO vers la bouée d'enlèvement ancrée à 1942 mètres à l'Est du FPSO. La bouée permet le chargement de navires pétroliers de type VLCC (Very Large Crude Carrier), d'une capacité de 330 000 tonnes, approx. 2 millions de barils à un débit nominal de 40 000 barils par heure, l'opération d'enlèvement durant environ, 25 heures.

Le système de transfert FPSO/pétrolier comprend comme le montre la figure 1 les éléments suivants :

Le FPSO : est capable de traiter environ 250 000 barils par jour (environ 40 000 m3 / j), avec une capacité de stockage d'environ2 millions de barils de pétrole.

Le réseau d'enlèvement (chargement du pétrolier) : constitué des flexibles sous-marins vers la bouée, de la bouée et du flexible flottant de chargement vers le pétrolier : c'est la ligne ou circuit export.

La bouée d'enlèvement. Celle-ci possède une capacité, le Surge Tank, d'un volume de 100m3, calculé pour recevoir la quantité débitée pendant le temps de fermeture de la vanne SDV (Shut-Down Valve), vanne de garde (TOR) chargée d'isoler la ligne en cas de problème lors des opérations d'enlèvement.

Dans le cas où la pression monterait à 15 bars sur le réseau, un disque de rupture, organe de sécurité qui isole le Surge Tank du reste du réseau et possède une résistance mécanique définie, cède et le Surge Tank se remplit alors pour éviter une pollution accidentelle.

Le PLC, Process Logical Controller est un automate local installé sur la bouée, sa fonction est de fermer la vanne SDV. La fermeture de la SDV est activée dans les cas suivants : pression haute de 10 bars sur la ligne export, niveau haut dans le Surge Tank, témoin de rupture du disque enclenché. Le PLC fonctionne de façon autonome c'est-à-dire que les défauts locaux, notamment sur la bouée,) entrainent la fermeture de la vanne sans passer par le système de contrôle du FPSO.

La fibre optique. Elle transmet les informations relatives à la bouée au FPSO. Elle permet d'arrêter le chargement du pétrolier en cas de problème sur la bouée et d'opérer la vanne SDV depuis la salle de contrôle.

Le pétrolier enleveur : une fois amarré et connecté à la bouée, le pétrolier reçoit d'abord le fond des citernes (toutes celles sélectionnées pour l'enlèvement) du FPSO dans une seule des siennes ; c'est l'étape de « de-bottom-ing » qui sert en premier lieu à séparer, le cas échéant, l'eau issue notamment des puits de production et de la décantation de l'huile, mais aussi à vérifier la disposition du circuit et son étanchéité. Cette étape capitale est souvent faite à débit réduit. Puis le chargement du pétrolier suit son cours à débit nominal jusqu'à la livraison de la quantité demandée où le débit sera de nouveau réduit dans la dernière phase de chargement (complétion ou topping up) pour éviter tout débordement.

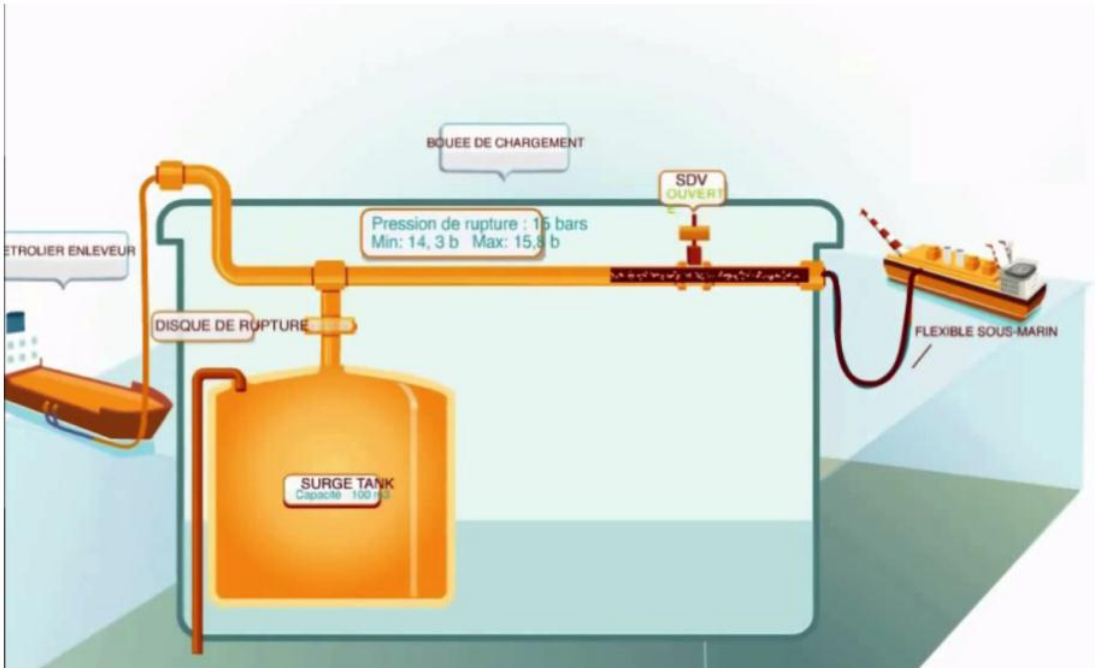


Figure 1 Système de transfert

Les phénomènes dangereux en lien avec cet accident sont la rupture de la connexion fibre optique entre la bouée d'enlèvement/FPSO (les données de la bouée ne sont plus transmises à la salle de contrôle). L'intervention pour l'installation d'un système de télétransmission radio provisoire reste infructueuse puisque la liaison radio n'assure pas aussi la transmission des données. Les intervenants effectuent une petite coupure électrique pour installer le système de télétransmission, cette coupure électrique provoque la fermeture de la SDV. La fermeture de la SDV n'est pas reportée et passe inaperçue car elle est hors scoop des intervenants télécom. Le jour de l'accident, lors de la préparation des circuits pour l'opération de chargement du pétrolier, l'opérateur aperçoit que la SDV est fermée, pour empêcher sa fermeture intempestive, elle est alors forcée ouverte. Cette manœuvre est dangereuse puisqu'elle inhibe les fonctions de contrôle de la sécurité du PLC et de l'opérateur de la salle de contrôle.

Etape 2 : Les contraintes de sécurité du système et les configurations requises

Pendant les opérations d'enlèvement, le pilote du pétrolier enleveur ou son assistant sont en communication radio continue avec le responsable des opérations du FPSO et le Loading Master du pétrolier. Les instructions échangées entre le FPSO et le navire pétrolier transitent via le pilote ou le Berthing Master. Tout changement dans la configuration de la vanne, sur le circuit de chargement du pétrolier, doit être notifié au pilote qui en informe le responsable des opérations du FPSO afin d'éviter tout risque de surpression dans les installations. Le Loading Master du pétrolier est chargé d'actionner les ouvertures ou les fermetures des vannes et de préserver la sécurité de la cargaison à bord du navire. L'arrêt d'urgence peut être déclenché en cas de problème au niveau de l'aussière d'amarrage, fuite incontrôlée d'hydrocarbures ou un accident majeur. Dans ce cas, le Loading Master du navire prévient le pilote avant la fermeture de la vanne au niveau du manifold. Le pilote à son tour informe le responsable des opérations sur le FPSO.

Les contraintes de sécurité (CS) imposées pendant les opérations de chargement sont :

L'opération de transfert d'hydrocarbure est continuellement sous contrôle positif

Des mesures doivent être préconisées pour protéger l'infrastructure et l'installation technique

Des mesures doivent être préconisées pour protéger l'environnement

Des mesures doivent être préconisées pour minimiser les pertes humaines et matérielles, si par inadvertance un incendie/explosion se produit.

Etape 3 : La structure hiérarchique de contrôle de la sécurité

La démarche d'analyse de l'accident selon CAST, suppose la modélisation de la structure de contrôle de la sécurité des opérations d'enlèvement. La figure 2 illustre la structure de contrôle chargée de garantir la sécurité par le biais d'imposition des contraintes de sécurité, depuis la phase de développement jusqu'à la phase d'opération et d'exploitation. Cette structure comprend les organisations internationales, les états, les organismes officiels de certification, les sociétés de classification promulguent les règlements et les exigences qui assurent la sécurité de l'industrie maritime dans son ensemble. L'exploitant s'engage dans sa responsabilité à assurer la sécurité des opérations et de l'environnement. Cette structure permet de visualiser les interactions entre les composants du système. La figure 2 illustre les actions commandées par un système de contrôle pour imposer l'application des contraintes de sécurité au niveau inférieur ainsi que les modes de vérification par retour d'information. Durant une enquête d'accident le modèle STAMP suppose l'évaluation la contribution de chaque élément de cette structure à la migration du système vers l'état accidentel. Les mécanismes de contrôle de la sécurité, représentés, doivent théoriquement assurer que les installations sont entièrement conformes aux exigences :

De l'Organisation Maritime Internationale (OMI), un organisme des Nations Unies en charge de l'administration de la mer et de la navigation maritime, qui édicte les conventions. A titre d'exemple, les conventions de première importance promulguées par l'OMI sont :

La convention internationale de 1974 pour la sauvegarde de la vie humaine en mer, telle que modifiée (SOLAS).

La convention internationale de 1973 pour la prévention de la pollution par les navires, telle que modifiée par les Protocoles de 1978 et de 1997 (MARPOL).

La convention internationale de 1978 sur les normes de formation des gens de mer, de délivrance des brevets et de veille, telle que modifiée, y compris les amendements de 1995 et les Amendements de Manille de 2010.

Des gouvernements, qui adoptent les règlements internationaux qui visent à assurer la sécurité maritime. Les organismes officiels de certification inspectent les installations et délivrent les certificats de conformité aux normes et aux réglementations internationales.

Concernant les FPSOs, une fois immobiles et reliés au fond, il n'est pas nécessaire qu'ils soient immatriculés auprès d'un Etat du pavillon et donc qu'ils soient en conformité avec la réglementation maritime internationale. Cependant, lors de leur voyage de transit vers leur lieu de production, les FPSOs sont généralement enregistrés comme des navires de commerce effectuant des voyages internationaux et, à ce titre, ils sont immatriculés auprès d'un Etat du pavillon. Une fois sur place et connecté au sol en permanence, les FPSOs peuvent garder leur pavillon de transit ou, si l'Etat côtier le

demande, se faire immatriculer auprès de l'Etat côtier. Dans les deux cas, les FPSOs sont soumis à la réglementation maritime internationale et aux exigences de l'Etat du pavillon (International Association of Oil and Gas Producers 2006).

Pour les navires pétroliers, l'armateur est responsable d'assurer la conformité à la réglementation maritime internationale comme requis par l'administration de l'Etat du pavillon.

Pour la conformité avec les exigences de l'Etat du pavillon, il est exigé la délivrance entre autres des éléments suivants :

Certificat de Management de la sécurité.

Certificat international de lutte contre la pollution d'hydrocarbure.

Certificat international de tonnage.

Certificat international des lignes de charge.

Certificats des formations des officiers et équipages.

Ces certificats sont émis par l'Etat du pavillon ou par les organismes officiels de certification au nom de l'Etat du pavillon. Les certificats suivants peuvent être aussi demandés à savoir :

Le certificat de classe (coque, machines, …).

Les certificats pour le levage d'équipement/de grues.

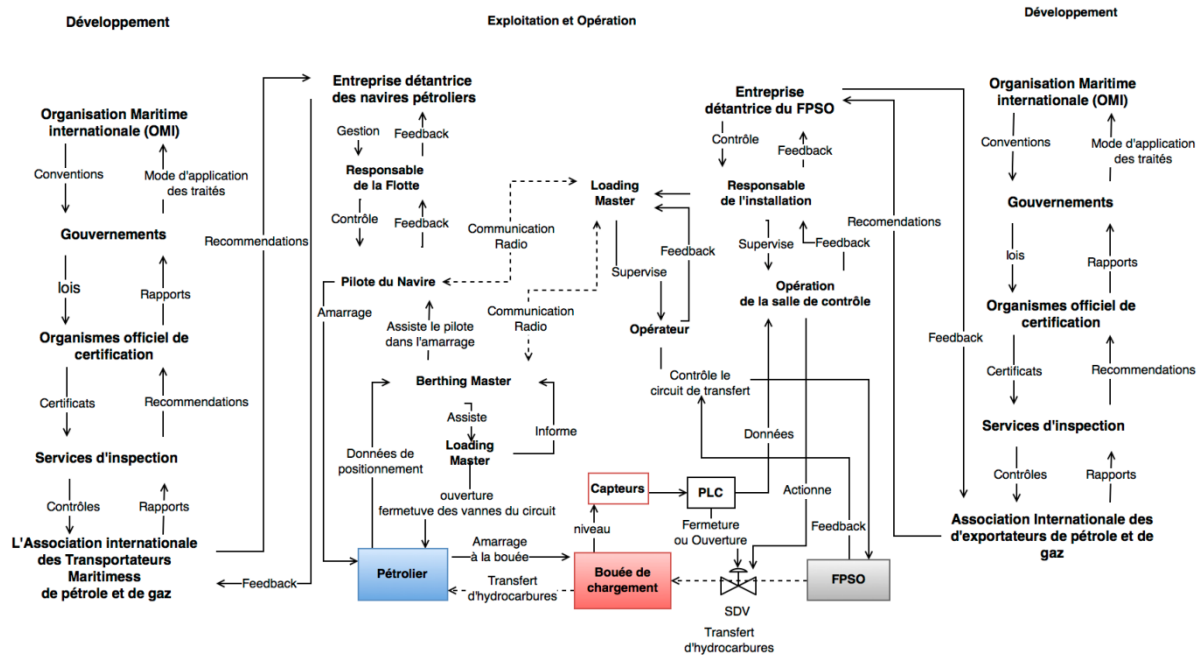


Figure 2 La structure de contrôle

Les actions commandées par les différents systèmes de contrôle servent à garantir la sécurité des opérations au niveau de l'installation technique. Plusieurs contrôleurs peuvent imposer les mêmes directives ou contraintes de sécurité.

Au niveau de l'installation technique représentée dans la figure 3, les processus contrôlés sont les citernes à cargaison (Cargo Tank) du FPSO, la vanne SDV et la bouée d'enlèvement. Le Loading Master est chargé de préparer la séquence d'enlèvement, l'opérateur utility (qui est l'interlocuteur du Loading Master depuis la salle de contrôle) est chargé d'exécuter le plan sous la supervision du Loading Master.

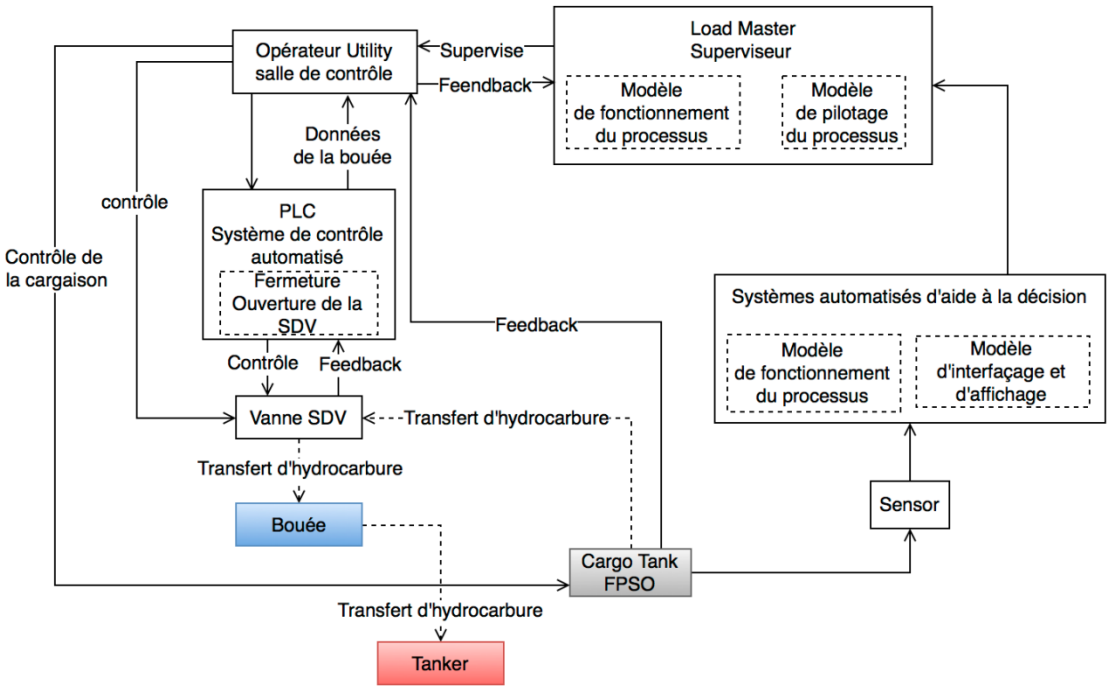


Figure 3 Modèle d'une structure de contrôle du processus de chargement d'un navire tanker

Etape 4 : Les faits de l'accident

L'accident tel qu'il est décrit dans le rapport d'enquête explique le déroulement des faits : un déversement important d'huile en mer s'est produit depuis la bouée de chargement d'un FPSO. L'ensemble du circuit de chargement entre le FPSO et le pétrolier enleveur est protégé de toute éventuelle surpression par le disque de rupture installé sur la bouée de chargement du tanker (figure 1). La pression de rupture étalonnée à 15 bars varie généralement entre un minimum de 14,3 bars et maximum de 15,8 bars. La séquence accidentelle a en fait commencé cinq mois avant. En effet, l'exploitant opère en mode dégradé car la liaison FPSO-bouée est tombée en panne en raison d'une (coupure de la fibre optique). Le jour de l'accident, le système de sécurité de la bouée fonctionne en mode local et, dans ce cas, la fonction automatique de la vanne d'arrêt de sécurité SDV est préservée. En revanche, les étapes d'arrêt de la séquence d'enlèvement sur le FPSO et la surveillance de la pression sur la bouée ne peuvent plus interagir. Ainsi, une pression haute sur la bouée provoque la fermeture de la vanne SDV, mais la séquence d'enlèvement ne s'arrête qu'avec une pression haute au refoulement des pompes (une fois la vanne SDV effectivement fermée).
La situation dégradée n'est identifiée que dix jours plus tard. Une intervention technique est effectuée, qui consiste à brancher un système de télétransmission provisoire sur la bouée. Une petite coupure électrique provoque la fermeture de la vanne SDV. Cette fermeture passe inaperçue tant pour l'intervenant que pour la salle de contrôle.
Quelques mois auparavant, alors qu'une opération d'enlèvement est planifiée, l'opérateur constate que le circuit et la vanne SDV sont fermés. Afin d'empêcher une fermeture intempestive de la vanne SDV, il est alors décidé de la forcer l'ouverture avec un signal de sortie automate spécifique, c.-à-d. de la maintenir physiquement en position ouverte. Une demande d'inhibition est lancée et accordée, mais la situation dégradée émise au départ n'est pas actualisée. Quinze jours plus tard, un nouvel essai de télétransmission entre la bouée et le FPSO est effectué : il se révèle infructueux car la communication est aléatoire et les données restent figées à l'écran. Le forçage de la vanne SDV en position ouverte est reconduit.
Le jour de l'accident, le chargement d'un pétrolier enleveur démarre en fin d'après-midi. Dans la soirée, un pic de pression atteint au moins 14,7 bars au refoulement des pompes sur le FPSO (cette pression est probablement liée à une manœuvre de vannes sur le pétrolier enleveur qui se trouve en fin de chargement). Suite à cette montée de pression, le disque de rupture cède, le « Surge Tank » (le réservoir de très petite capacité de réception de l'huile contenue dans la ligne export en cas de rupture du dit disque,) situé sur la bouée se remplit et déborde. Le PLC, Process Logical Controller, automate de contrôle de la vanne, dont l'action a été inhibée ne peut pas agir sur la vanne SDV. Peu après sur le pétrolier enleveur, la baisse de débit de réception est identifiée et l'anomalie est signalée et consignée. Malheureusement elle n'est pas prise en compte et elle n'est pas transmise au FPSO. Un quart d'heure environ après la rupture du disque, la baisse du débit de chargement alerte le Loading Master du pétrolier enleveur qui signale et consigne l'anomalie. Mais il n'alerte pas le Loading Master du FPSO (le Loading Master est la personne en charge de la préparation, du suivi des opérations d'enlèvement et qui protège les intérêts du client en cas de litiges sur la qualité/quantité du chargement ; il y a également un Loading Master côté FPSO qui assure les mêmes fonctions). Dans la salle de contrôle du FPSO on ne remarque rien : les données transmises depuis la bouée sont figées, en revanche les enregistrements des paramètres de transfert sur le FPSO montrent en premier la baisse du débit demandé conformément au programme de fin de chargement du tanker, ensuite le pic de pression et enfin le débit qui revient à sa valeur initiale et la pression qui s'établit à une valeur inférieure. Mais ces signaux ne sont pas identifiés et l'évènement passe inaperçu. Finalement, au cours de la nuit, une odeur d'hydrocarbures alerte un marin de l'équipage du pétrolier, le pompage est alors arrêté. Une quantité de pétrole brut a été déversée à la mer, à plus de 80 km de la côte. Une cellule de crise est activée, et les opérations de dépollution sont entreprises. Elles se termineront près de 3 semaines plus tard.

Etape 5 : Analyse des défaillances de l'installation technique

Pour analyser les causes de l'accident, la démarche consiste à procéder par une collecte de données pour identifier les risques inhérents à la perte de contrôle. Pour cela, les dysfonctionnements techniques qui ont provoqués l'accident sont analysés. Il est important d'identifier la contribution des mécanismes de contrôle suivant au processus de l'accident à savoir : contrôle de l'installation technique, déroulement des opérations pannes physique, dysfonctionnement, communication et les failles dans les troubles non traités (unhandled disturbances). Il est aussi primordial de documenter et d'expliquer pourquoi ces mécanismes de contrôle sont inappropriés et inhérents à la perte. Cette approche permet ainsi de mettre en place un plan de prévention des risques

Contrôle et Feedback inappropriés pour pallier au problème de la rupture de la fibre optique

Les causes de la rupture de la fibre optique ne sont pas analysées dans le rapport d'enquête. Il est important d'étudier ce phénomène pour empêcher des incidents similaires. Une entreprise externe intervient pour brancher un système de télétransmission radio provisoire (3 semaines après la rupture de la fibre optique) pour permettre le transfert des données de la bouée vers la salle de contrôle. Cette intervention ne fixe pas le problème, la transmission des données n'est pas rétablie. Dix jours plus tard, une deuxième intervention est reconduite par cette entreprise qui ne parvient aussi pas à résoudre le problème de télécommunication.

Contrôle et Feedback inappropriés à l'ouverture forcée de la SDV

Lors d'une visite de la bouée en préparation d'enlèvement, la vanne SDV est trouvée en position fermée, une analyse informelle de la situation mène à la décision de forcer en position ouverte la vanne de crainte d'une fermeture intempestive pendant les enlèvements susceptibles d'entraîner des coups de bélier dans le circuit. Cette intervention provoque l'inhibition de la commande (d'ouverture, fermeture) de l'automate de sécurité local PLC et des signaux qui alimentent le PLC (niveau Surge Tank, pression Surge Tank, état du disque de rupture). Les actions commandées depuis la salle de contrôle pour l'ouverture ou la fermeture de la SDV sont aussi inhibées.

Contrôle et feedback inappropriés suite à l'éclatement du disque de rupture

La rupture du disque d'éclatement en fonction a provoqué le remplissage et le débordement par un tube trop-plein du "Surge Tank" de la bouée. Aucune alerte n'est parvenue à la Salle de Contrôle du FPSO, et aucun automatisme n'a

fermé la vanne d'isolement de la bouée (SDV) ou les vannes de sécurité du circuit d'expédition du FPSO. L'expédition et la fuite ont été arrêtées à 21h54 sur demande du pilote à bord du pétrolier, après qu'un membre de l'équipage ait constaté une forte odeur de brut laissant suspecter une pollution.

Etape 6 : Analyse des composants de la structure hiérarchique

Après l'analyse et l'identification des éléments de perte de contrôle sur l'installation physique, l'étape suivante consiste à examiner successivement les niveaux hiérarchiques supérieurs. Cette étape consiste à comprendre les mécanismes qui conduisent à la perte de contrôle de l'installation physique. Il faut identifier pour chaque composant de la structure hiérarchique, les conduites qui favorisent la propagation d'un contrôle inadéquat. Pour chaque consigne de sécurité du système soit que son application n'ait pas été assignée a une composante du système de sécurité ou bien qu'elle n'ait pas été correctement exécutée ou bien que le niveau de la structure de contrôle n'a pas vérifiée que les consignes de sécurité ont été convenablement appliquée au niveau qui lui est inferieur dans la structure. A cet effet toute décision ou faille dans les actions commandées doivent être bien acquises en information disponibles pour les décideurs ainsi que toute information requise qui ne l'a pas été, la modélisation du comportement du mécanisme (le contexte et les influence sur le processus de décision) les structures à la base de ces décisions et pourquoi ces failles ont eu lieu.

Selon CAST, l'approche d'analyse de l'accident est bottom-up, le comportement des opérateurs de première ligne est d'abord étudié. Il faut remonter ensuite dans la structure de contrôle pour représenter la contribution comme suit (Figure 4) de chaque composant de la migration du système vers l'état accidentel. Dans ce qui suit, on se contente de présenter l'analyse effectuée sur l'opérateur de la salle de contrôle et l'opérateur de première ligne.

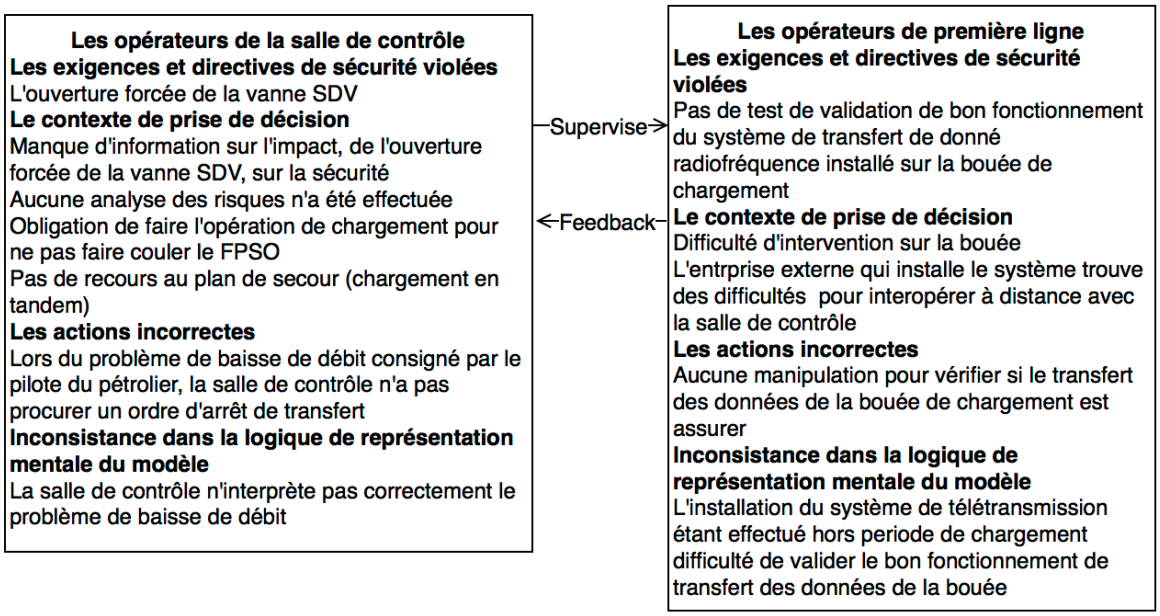


Figure 4 Analyse du comportement de l'opérateur

Etape 7 : Evaluation des aspects de coordination, de communication et de contrôle des composants de la structure hiérarchique

L'analyse élaborée dans l'étape précédente consiste à évaluer séparément chaque composant de la structure de contrôle. Dans cette étape, l'aspect de coordination et de communication entre les composants de la structure hiérarchique est analysé. L'approche permet d'identifier les conflits potentiels et les problèmes de coordination, et d'examiner comment les mécanismes de contrôle du processus, établis en phase de conception et de développement, se dégradent au fil du temps en phase de fonctionnement et opérationnelle. L'analyse montre de nombreux défauts de coordination et de communication.

Aspects de coordination et de communication inappropriées faille dans la gestion hiérarchique de la maintenance
L'intervention pour brancher le système de télétransmission provisoire montre un manque de contrôle et de coordination entre les différents corps de métier. Les tests de vérification des transmissions ne sont pas élaborer correctement. La coupure électrique pour effectuer le branchement, provoque la fermeture de la SDV, la fermeture de la SDV n'est pas reportée et passe inaperçue car elle est hors scope des intervenants télécom.

Aspects de coordination et de communication non appropriées
Le changement dans la configuration de la vanne sur le circuit de chargement du navire amène deux hypothèses liées à l'accident :

L'opérateur du navire ne semble pas notifier au responsable des opérations du FPSO la configuration de la vanne de circuit du chargement du navire en fin d'opération. Les enregistrements montrent un pic de pression de 14,7 bars sur les pompes export du FPSO. Cette défaillance de contrôle peut être interprétée par le manque de coordination dans les interventions aux différents niveaux de la structure (fermeture des vannes chez le pétrolier enleveur conformément à la fin de la procédure de chargement, manque d'échange et de transmission des paramètres de contrôles).

L'opérateur du navire informe le responsable des opérations du FPSO de la configuration de la vanne, sur le circuit de chargement, mais l'opérateur de la salle de contrôle du FPSO ne déclenche pas l'arrêt de transfert lorsqu'un pic de pression de 14,7 bars est mesuré sur les pompes export du FPSO

Aspects de coordination et de communication non appropriées pendant l'enlèvement

L'opération d'enlèvement étant effectuée en mode dégradé, la structure chargée de contrôler de la sécurité du système doit faire preuve de vigilance. Le *Loading Master* du pétrolier enleveur déclare l'anomalie de perte de débit, cependant cette alerte n'est est pas prise en considération par l'équipe du FPSO, qui ne déclenche pas l'arrêt de transfert..

Etape 8 : Modélisation de l'accident à l'aide de la dynamique du système

Chaque composant de la structure de contrôle est responsable du maintien de la sécurité au sein du système. Les moyens de communication et les aspects de coordination jouent un rôle important dans l'application des contraintes de sécurité commandées par les systèmes de contrôle. Cette étape permet de comprendre comment le contexte de prise de décision affecte les fonctions de contrôle de la sécurité au fil du temps. La figure 5 montre le modèle simplifié de l'accident où l'intégrité de l'installation technique n'est pas convenablement gérée. La rupture de la fibre optique ainsi que les défaillances du système de télétransmission conduisent à un délai dans l'arrêt des installations en cas d'urgence.

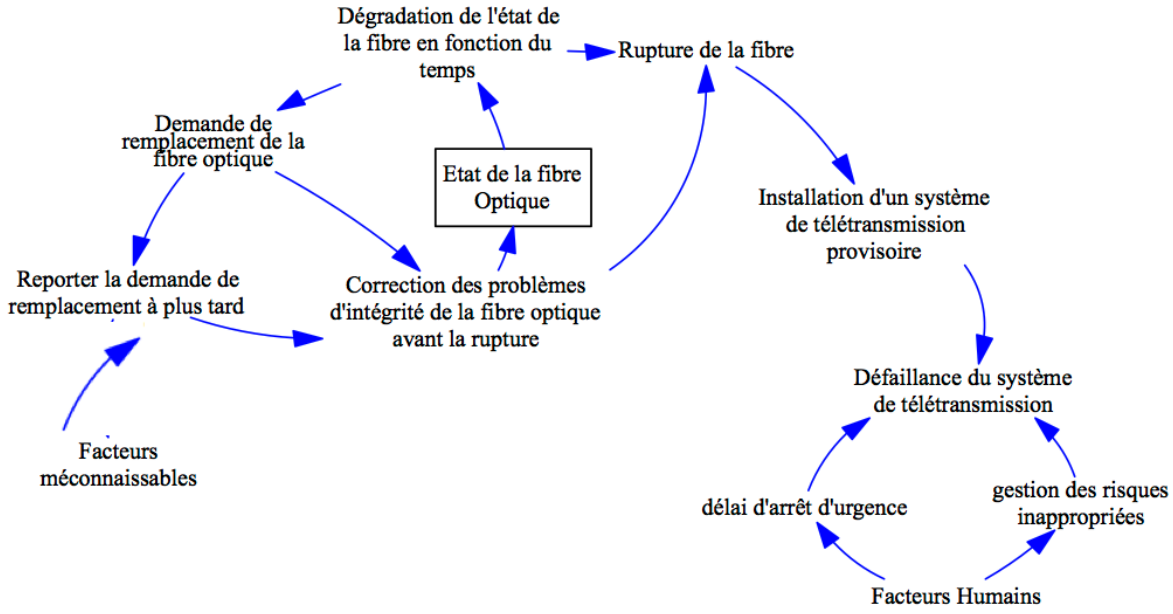


Figure 5 modèles simplifiés de l'accident

Etape 9 : Axes de progrès

Selon CAST l'objectif de l'analyse d'un accident ne doit pas être l'accusation ou la plainte contre le plus faible de la hiérarchie de contrôle, mais il s'agit d'en retirer un apprentissage pour les opérations de changement et la réingénierie du processus de sécurité. Une analyse complète selon CAST permet de faire apparaitre un ensemble de recommandations. Pour l'accident du FPSO, elles sont classées selon 4 catégories :

Infrastructure de l'installation technique

- La SDV doit être remise sous contrôle local du PLC de la bouée. Les opérateurs doivent superviser le déroulement des opérations, et les paramètres d'enlèvement, afin de pouvoir détecter au plus tôt les indicateurs de perte de contrôle.
- L'exploitant doit renforcer le système de contrôle des vannes ;
- Ajouter des alertes en dehors du système informatique ;

- Renforcer la perception physique directe des opérateurs (les opérateurs du FPSO n'étaient conscients de rien, car la perception des paramètres de contrôle ne vient que des données du PLC et avec la rupture de communication, le système de contrôle était en défaut.) ;
- Prévoir un Back up fiable pour la partie communication (pour éviter un fonctionnement en état dégradé sans contrôle).

Gestion de l'entreprise

Dans le cas du FPSO, il y a la compagnie pétrolière et la compagnie maritime. Chacune doit veiller de son coté à ce que leurs infrastructures respectives (FPSO et pétrolier enleveur) soit conformes aux règlements, normes et standards en vigueur dans leurs activités. Et lors de l'opération d'enlèvement, à l'interface entre les deux acteurs, il convient d'éviter la rupture du processus de contrôle de sécurité (par exemple, coordination en temps réel entre les opérateurs du FPSO et l'équipage du pétrolier, contrôle de la boucle automate du PLC ou autre).

Pour cela, il est nécessaire d'établir une stratégie de sécurité au sein de l'entreprise qui définit clairement :

- Les rôles, les autorités et les responsabilités correspondantes des différents acteurs de la structure de sécurité ;
- Les critères d'évaluation à adopter pour la décision, le design, et la mise en place du contrôle de la sécurité ;
- Exiger l'application systématique des contraintes de sécurité.
- L'organisation en charge du processus de contrôle de la sécurité doit assurer :
- La mise en application de la stratégie ;
- De Prévenir la direction des décisions relatives à la sécurité ;
- La réalisation des analyses de risque et des audits convenablement documentés ;
- La définition des contraintes de sécurités selon les activités et leur évolution ;
- La définition d'un standard pour les enquêtes d'accidents qui soit exhaustif ;
- L'établissement d'un Système d'Information propre au processus du contrôle de la sécurité ;
- L'établissement d'une structure de coordination et de rétroaction de l'information entre les différents acteurs.

Gestion et exploitation de l'installation

Il convient d'établir une stratégie de sécurité propre à l'infrastructure (*Physical Plant*) en plus de celle de l'entreprise :

- Pour conduire des analyses de risques ;
- Faire des enquêtes sur les raison et les conditions des incidents ;
- Établir des indicateurs de risque ;
- Collecter systématiquement des données ;
- Valider la formation des intervenants conformément aux stratégies adoptées.
- Les critères d'évaluation à adopter pour la décision, le design, et la mise en place du contrôle de la sécurité visent à :
- Exiger l'application systématique des contraintes de sécurité ;
- Renforcer la communication et la transparence ;
- Faire une validation des mesures de sécurité par le responsable de l'infrastructure ;
- Sécuriser la communication entre les différentes composantes de l'infrastructure.

En effet, dans notre cas, le démarrage de l'enlèvement a été effectué en mode dégradé (pas de vérification du branchement de la liaison radio, aucune réaction aux données figées, absence de communication entre les opérateurs du pétrolier enleveurs et le FPSO, etc.

Gouvernement et environnement

Il s'agit de ne pas isoler le système de son environnement social ni de négliger les engagements vis-à-vis des gouvernements et des lois qui régissent le contrôle de sécurité de l'activité.

CONCLUSION

Dans cet article, l'analyse de l'accident en utilisant CAST consiste en une description des actions de contrôle inadéquates commandées par chacune des composantes de la structure de contrôle de la sécurité. En se basant sur STAMP, les actions inappropriées sont analysées selon les facteurs accidentogènes (par exemple, des modèles

cognitifs défaillants, le manque de coordination entre les contrôleurs, des algorithmes de contrôle inadéquats ou la mauvaise exécution d'une action commandée par un composant de la structure, ou des feedbacks manquants, etc.). Cette démarche permet à partir du modèle d'analyse de comportement de l'opérateur (Figure 5) de comprendre le processus de prise de décision qui mène à l'accident. Une analyse approfondie CAST a cependant des limites dans le sens où :1) elle nécessite de nombreuses données associées à l'ensemble du système qui peuvent difficilement être pleinement obtenues à partir des ressources disponibles ; 2) l'exploitant peut rencontrer des difficultés dans l'application des recommandations qui résultent de l'analyse, en temps opportun. Concernant le cas de cette étude, il reste sûrement encore des questions non résolues, bien que cet article propose de nouvelles idées qui ouvrent des pistes pour une meilleure compréhension des accidents industriels en mer.

RÉFÉRENCES

Aas, A.L., 2010. Industrial Application of Human Factors Safety Standards. Nor. Univ. Sci. Technol. NTNU Nor. Dr. Philos. 17.

Abdulkhaleq, A., Wagner, S., 2015a. XSTAMPP: an eXtensible STAMP platform as tool support for safety engineering.

Abdulkhaleq, A., Wagner, S., 2015b. Integrated Safety Analysis Using Systems-Theoretic Process Analysis and Software Model Checking, in: Koornneef, F., Gulijk, C. van (Eds.), Computer Safety, Reliability, and Security, Lecture Notes in Computer Science. Springer International Publishing, pp. 121–134. doi:10.1007/978-3-319-24255-2_10

Abdulkhaleq, A., Wagner, S., 2014a. A software safety verification method based on system-theoretic process analysis, in: Computer Safety, Reliability, and Security. Springer, pp. 401–412.

Abdulkhaleq, A., Wagner, S., 2014b. Open Tool Support for System-Theoretic Process Analysis.

Abdulkhaleq, A., Wagner, S., Leveson, N., 2015. A Comprehensive Safety Engineering Approach for Software-Intensive Systems Based on STPA. Procedia Eng. 128, 2–11. doi:10.1016/j.proeng.2015.11.498

Abramovici, M., Breuer, M.A., Friedman, A.D., 1990. Digital systems testing and testable design, New York: Computer science press. ed.

AlKazimi, M.A., 2015. Investigating new accident causation, risk assessment, and mitigation strategy selection tools in the petroleum industry.

Altabbakh, H., AlKazimi, M.A., Murray, S., Grantham, K., 2014. STAMP – Holistic system safety approach or just another risk model? J. Loss Prev. Process Ind. 32, 109–119. doi:10.1016/j.jlp.2014.07.010

ATEA, 1998. The Procurement of Computer-Based Safety-Critical Systems .

Bertalanffy, L. von, 1969. General System Theory, New York: George Brazille. ed.

Besnard, D. et, Baxter, G., 2003. Human compensations for undependable systems.

Bieder, C., 2006. Les facteurs humains dans la gestion des risques: évolution de la pensée et des outils, Lavoisier. ed.

Bird, F.., Loftus, R.G., 1976. Loss control management. Inst. Press.

Boulding, K.E., 1956. General Systems Theory—The Skeleton of Science. Manag. Sci. 2, 197–208. doi:10.1287/mnsc.2.3.197

Bouloiz, H., Garbolino, E., Tkiouat, M., Guarnieri, F., 2013. A system dynamics model for behavioral analysis of safety conditions in a chemical storage unit. Saf. Sci. 58, 32–40. doi:10.1016/j.ssci.2013.02.013

Budde, S.F., 2012. Modeling Blowouts During Drilling Using STAMP and STPA. 101.

Cambien, A., 2008. Une introduction à l'approche systémique: appréhender la complexité.

Cambon, J., 2007. Vers une nouvelle méthodologie de mesure de la performance des systèmes de management de la santé-sécurité au travail - document. Ecole Nationale Supérieure des Mines de Paris.

Cambon, J., Guarnieri, F., Groeneweg, J., 2006. Towards a new tool for measuring Safety Management Systems performance." Learning from Diversity: Model-Based Evaluation of Opportunities for Process (Re)-Design and Increasing Company Resilience. Presses des MINES.

Carlson, S.J., 2015. NURail Project ID: NURail2012-MIT-R03 Transportation of Energy-Related Material.
Carlson, S.J., 2014. Understanding government and railroad strategy for crude oil transportation in North America (Thesis). Massachusetts Institute of Technology.
Centre National de Ressources Textuelles et Lexicales, concept. CONCEPT : Définition de CONCEPT [WWW Document]. URL http://www.cnrtl.fr/definition/concept (accessed 9.1.16).
Chabrol, J.B.T. et L. von B., 1973. Théorie générale des systèmes., Dunod. ed.
Courtois, P.-J., Leveson, N., 1996. Safeware: System Safety and Computers.
Cullen, L.W.D., 1993. The Public Inquiry into the Piper Alpha Disaster. Drill. Contract. U. S. 49:4.
Desmorat, G., Guarnieri, F., Besnard, D., Desideri, P., Loth, F., 2013. Pouring CREAM into natural gas: The introduction of Common Performance Conditions into the safety management of gas networks. Saf. Sci. 54, 1–7. doi:10.1016/j.ssci.2012.10.008
Dobi, S., Gleirscher, M., Spichkova, M., Struss, P., 2013. Model-based Hazard and Impact Analysis. Tech. Report, TU Munich, Comp. Sci. Dept.
Dong, A., 2012. Application of CAST and STPA to railroad safety in China. Massachusetts Institute of Technology.
Durand, D., 1979. La systémique, Presses universitaires de France. ed.
Fadier, E., Leplat, J., Terssac, G. de, 1990. Fiabilité humaine: méthodes d'analyse et domaines d'application.
Fadier, E., Mazeau, M., 1996. L'activité humaine de maintenance dans les systèmes automatisés : problématique générale. J. Eur. Systèmes Autom. 30, 1467–1486.
Fahlbruch, B., Wilpert, B., 2001. La notion de sécurité systèmique: un nouveau domaine de recherché pour la psychologie industrielle, L'Harmattan, Collection Risques Collectifs et Situations de Crise. ed.
Ferry, T.S., 1988. Modern Accident Investigation and Analysis. John Wiley & Sons.
Forrester, J., 1995. The beginning of system dynamics. McKinsey Q. 4–17.
Forrester, J.W., 1968. Industrial Dynamics—After the First Decade. Manag. Sci. 14, 398–415. doi:10.1287/mnsc.14.7.398
Garbolino, E., Chery, J.P., Guarnieri, F., 2010. Modélisation dynamique des systèmes industriels à risques, Lavoisier. ed, Technique & Documentation SRD - Sciences du risque et du danger : Série Notes de synthèse et de recherche, Franck GUARNIERI.
Grantham, K., 2013. HANAN MOHAMMAD ALTABBAKH. Missouri University of Science and Technology.
Groeneweg, J., 2002. Controlling the controllable: preventing business upsets. Presented at the Global Safety Group.
Groeneweg, J., Van Schaardenburgh-Verhoeve, K.N.R., Corver, S., Lancioni, G.E., Knudson, T., Braster, J.F.A., 2007. Accident investigation beyond the boundaries of organizational control. Presented at the Proceedings of Esrel 2007 Conference.
Guarnieri, F., Cambon, J., Boissieres, I., 2008. De l'erreur humaine à la défaillance organisationnelle : essai de mise en perspective historique. REE Rev. Lélectricité Lélectronique.
Guenebeaud, F., 2013. Les représentations sociales des risques majeurs au sein de la communauté éducative du second degré.
Hanan Altabbakh, Mohammad A.Alkazimi, Susan Murray, Katie Grantham, 2014. STAMP - Holistic system safety approach or just another risk model?

Hardy, K., 2016. Decisions Management during Wildland Fires: Accidents Viewed as a Spatiotemporal Inadequacy. Am. Sci. Res. J. Eng. Technol. Sci. ASRJETS 23, 63–77.
Hardy, K., 2011a. Contribution à l'étude d'un modèle d'accident systémique, le cas du modèle STAMP : application et pistes d'amélioration - document.
Hardy, K., 2011b. Contribution à l'étude d'un modèle d'accideny systémique, le cas du modèle STAMP:application et pistes d'amélioration. MINES ParisTech, Centre de Recherche sur les Risques et les Crises.
Hardy, K., 2010. Contribution à l'étude d'un modèle d'accident systémique, le cas du modèle STAMP : application et pistes d'amélioration. École Nationale Supérieure des Mines de Paris.
Hardy, K., Guarnieri, F., 2013. Hazard Mitigation through a Systemic Model of Accident to a Socio-Technical System: A Case Study. J. Energy Power Eng. 7, 775.
Hardy, K., Guarnieri, F., 2011a. Modelling and hazard analysis for contaminated sediments using stamp model, in: 14th International Conference on Process Integration, Modelling and Optimisation for Energy, Saving and Pollution Reduction. pp. 737–742.
Hardy, K., Guarnieri, F., 2011b. Using a Systemic Model of Accident for Improving Innovative Technologies: Application and Limitations of the STAMP model to a Process for Treatment of Contaminated Substances, in: The 15th World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI 2011.
Hardy, K., Guarnieri, F., 2011c. Analyzing Contaminated Sediments through a Systemic Model of Accident, in: 41st ESReDA Seminar - Advances in Reliability-Based Maintenance Policies. La Rochelle, France.
Heinrich, H.W., 1941. Industrial Accident Prevention. A Scientific Approach, McGraw-Hill Book Company Inc, New York. ed.
Hoel, F., 2012. Modeling Process Leaks Offshore Using STAMP and STPA.
Hollnagel, E., 2014. Safety-I and safety–II: the past and future of safety management. Ashgate Publishing, Ltd.
Hollnagel, E., 2006. Safety Management: from protection to resilience. UIC Saf. Platf. Paris 20-21.
Hollnagel, E., 2004. Barriers and accident prevention. Ashgate.
Hollnagel, E., Woods, D.D., 2005. Joint Cognitive Systems: Foundations of Cognitive Systems Engineering. CRC Press.
Hollnagel, E., Woods, D.D., Leveson, N., 2007. Resilience Engineering: Concepts and Precepts. Ashgate Publishing, Ltd.
ISSS, n.d. International Society for the Systems Sciences. Wikipedia Free Encycl.
John L Thorogood, 2015. The Macondo Inflow Test Decision: Implications for Well Control and Non-technical Skills Training. Presented at the Drilling Conference and Exhibition, Society of Petroleum Engineers or the International Association of Drilling Contractors, London.
Johnson, W.G., 1980. MORT Safety Assurance System - Google Scholar, Marcel Dekker Inc. ed.
Kim, T., Salman, N., Kjell, I.Ø., 2016. A STAMP-based causal analysis of the Korean Sewol ferry accident. Saf. Sci.
Knight, J.C., 2002. Safety critical systems: challenges and directions, in: Proceedings of the 24rd International Conference on Software Engineering, 2002. ICSE 2002. Presented at the Proceedings of the 24rd International Conference on Software Engineering, 2002. ICSE 2002, pp. 547–550.

Krauss, S.S., Rejzek, M., Hilbes, C., 2015. Tool Qualification Considerations for Tools Supporting STPA. Procedia Eng. 128, 15–24. doi:10.1016/j.proeng.2015.11.500
Laporte, J., 1988. Le rationalisme de Descartes. Presses Universitaires de France.
Larouzée, J., Guarnieri, F., 2015. From theory to practice: itinerary of Reasons' Swiss Cheese Model. ESREL 2015. CRC Press.
Larouzée, J., Guarnieri, F., 2014. Huit idées reçues sur le (s) modèle (s) de l'erreur humaine de James Reason. REE Rev. Electr. Electron. 5, 83–90.
Le Moigne, J.-L., 1990. La modélisation des systèmes complexes., Paris: Bordas. ed. Dunot.
Lederer, J., 1986. How far have we come? A look back at the leading edge of system safety eighteen years ago. Hazard Prev. 8.
Leveson, N., 2013a. A Systems Thinking Approach to Leading Indicators in the Petrochemical Industry.
Leveson, N., 2013b. A Systems Thinking Approach to Leading Indicators in the Petrochemical Industry [WWW Document]. URL http://esd.mit.edu/WPS/2013/esd-wp-2013-01.pdf (accessed 6.4.15).
Leveson, N., 2011. Engineering a Safer World: Systems Thinking Applied to Safety.
Leveson, N., 2004. A new accident model for engineering safer systems. Saf. Sci. 42, 237–270.
Leveson, N., 2002. A new approach to system safety engineering. Manuscr. Prep. Draft Can Be Viewed Httpsunnyday Mit Edubook2 Pdf.
Leveson, N., 2001. Evaluating Accident Models Using Recent Aerospace Accidents, Part 1: Event-Based Models.
Leveson, N., 1986. Software Safety: Why, What, and How, Computing Surveys. ACM Comput. Surv. CSUR.
Leveson, N., Dulac, N., 2005. Safety and Risk-Based Design in Complex Systems-of-Systems, in: 1st Space Exploration Conference: Continuing the Voyage of Discovery. American Institute of Aeronautics and Astronautics.
Leveson, N.G., 2016. Rasmussen's legacy: A paradigm change in engineering for safety. Appl. Ergon. doi:10.1016/j.apergo.2016.01.015
Llory, M., 1996. Accidents industriels: le coût du silence: opérateurs privés de parole et cadres introuvables., Editions L'Harmattan. ed.
McCarthy, S., 2013. A System Theoretic Safety Analysis of Friendly Fire Prevention in Ground Based Missile Systems. Citeseer.
Meadows, D.H. (Ed.), 1972. The Limits to growth; a report for the Club of Rome's project on the predicament of mankind. Universe Books, New York.
Miles, R.F., 1973. Systems concepts: Lectures on contemporary approaches to systems.
Morin, E., 2015. Introduction à la pensée complexe. Seuil.
Pasman, H.J., 2015. Risk Analysis and Control for Industrial Processes - Gas, Oil and Chemicals: A System Perspective for Assessing and Avoiding Low-Probability, High-Consequence Events. Butterworth-Heinemann.
Pelegrín, L., 2012. Integrating Safety into an Engineering Contractor's System Engineering process using the guidelines of STAMP (Systems-Theoretic Accident Mod el and Processes). MIT Press, Cambridge, Mass.
Peretti-Watel, P., 2004. Du recours au paradigme épidémiologique pour l'étude des conduites à risque. Rev. Fr. Sociol. 45, 103–132.
Perneger, T.V., 2005. The Swiss cheese model of safety incidents: are there holes in the metaphor? BMC Health Serv. Res. 5, 71. doi:10.1186/1472-6963-5-71

Perrin, L., Muñoz-Giraldo, F., Dufaud, O., Laurent, A., 2012. Normative barriers improvement through the MADS/MOSAR methodology. Saf. Sci. 50, 1502–1512. doi:10.1016/j.ssci.2012.02.002
Perrow, C., 1984. Normal accidents: Living with high risk systems.
Pidgeon, N.F., 1991. Safety Culture and Risk Management in Organizations. J. Cross-Cult. Psychol. 22, 129–140. doi:10.1177/0022022191221009
Pitiporn Thammongkol, 2014. The system theoretic accidental analysis of a crude unit refinery fire incident (Thesis). Massachusetts Institute of Technology.
Qureshi, Z.H., 2007. A review of accident modelling approaches for complex socio-technical systems, in: Proceedings of the Twelfth Australian Workshop on Safety Critical Systems and Software and Safety-Related Programmable Systems-Volume 86. Australian Computer Society, Inc., pp. 47–59.
Rasmussen & Svedung, 2000. Proactive risk management in a dynamic society. Swedish Rescue Services A, Place of publication not identified.
Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. Saf. Sci. 27, 183–213. doi:10.1016/S0925-7535(97)00052-0
Reason, J., 2016. Managing the Risks of Organizational Accidents. Routledge.
Reason, J., 2013. L'erreur humaine. Presses des MINES.
Reason, J., 1995. A systems approach to organizational error. Ergonomics 38, 1708–1721. doi:10.1080/00140139508925221
Reason, J., 1990. Human Error. Cambridge University Press.
Reason, J., Hollnagel, E., 2006. Revisiting the «Swiss cheese» model of accidents. J. Clin. Eng. 27 2006 110-115.
Revet, S., 2009. «Vivre dans un monde plus sûr». Cult. Confl. 33–51. doi:10.4000/conflits.17693
Roberts, K.H., 2009. Managing the unexpected: six years of HRO-literature reviewed. Journal of Contingencies and Crisis Management,. J. Contingencies Crisis Manag.
Rodrigo, P., 2011. Le jeu causal dans la Politique d'Aristote : eidétique et typique [WWW Document]. URL https://halshs.archives-ouvertes.fr/halshs-01194645/ (accessed 9.1.16).
Rolf-Arne Haugen Syvertsen, 2012. Modeling the Deepwater Horizon blowout using STAMP.
Rosenblueth, A., Wiener, N., Bigelow, J., 1943. Behavior, Purpose and Teleology. Philos. Sci. 10, 18–24.
Rosnay, J.D., 2014. Le Macroscope. Vers une vision globale. Seuil.
Rosnay, J.D., 1975. "Le macroscope." Vers une vision globale, Edition du Seuil. ed.
Sagvolden, E.H., 2013. Statistical analysis of failures and failure propagation in railway track.
Samadi, J., 2012a. Development of a systemic risk management approach for CO2 capture, transport and storage projects. Ecole Nationale Supérieure des Mines de Paris.
Samadi, J., 2012b. Development of a systemic risk management approach for CO2 capture, transport and storage projects (phdthesis). Ecole Nationale Supérieure des Mines de Paris.
Samadi, J., Garbolino, E., 2011. A new dynamic risk analysis framework for CO2 Capture, Transport and Storage chain,. Presented at the 29th International Conference of the System Dynamics Society, p. 17 pages-ISBN 978-1-935056-08-9-http://www.systemdynamics.org/conferences/2011/proceed/.

Sanseverino-Godfrin, V., 2010. Le cadre juridique de la gestion des pollutions et des risques industriels. Technique & Documentation - Lavoisier.
Sefer, E., Gallina, B., Muccini, H., Lundqvist, K., 2015. A model-based safety analysis approach for high-integrity socio-technical component-based systems.
Shannon, C.E., 2001. A mathematical theory of communication. ACM SIGMOBILE Mob. Comput. Commun. Rev. 5, 3–55.
Silje Frost Budde, 2012. Modeling Blowouts During Drilling Using STAMP and STPA.
Skelt, S., 2002. Methods for accident analysis (No. ROSS (NTNU) 2000208).
Spiegel, D., Hosse, R.S., Welte, J., Schnieder, E., 2013. Integration of Petri Nets into STAMP/CAST on the example of Wenzhou 7.23 accident.
Suo, D., Thomas, J., 2014. An STPA tool, in: STAMP 2014 Conference at MIT.
Syvertsen, R.-A.H., 2012a. Modeling the Deepwater Horizon blowout using STAMP.
Syvertsen, R.-A.H., 2012b. Modeling the Deepwater Horizon blowout using STAMP. Norwegian University of Science and Technology.
Thammongkol, P., 2014. The system theoretic accidental analysis of a crude unit refinery fire incident (Thesis). Massachusetts Institute of Technology.
Thomas, J., Lemos, F., Leveson, N., 2012. Evaluating the safety of digital instrumentation and control systems in nuclear power plants. NRC Tech. Researcy Report2013.
Thomas, J.P., 2013. Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis. Massachusetts Institute of Technology.
Torgauten, A.O.A., 2013. Classifying and Defining Operational and Organizational Aspects of Barriers for the Offshore Oil and Gas Industry.
Trist, E.L., 1951. Some Social and Psychological Consequences of the Longxwall Method of Coal-Getting: An Examination of the Psychological Situation and Defences of a Work Group in Relation to the Social Structure and Technological Content of the Work System. Hum. Relat. 4, 3–38. doi:10.1177/001872675100400101
Underwood, P., 2013. Examining the systemic accident analysis research-practice gap. \copyright Peter Underwood.
Underwood, P., Waterson, P., 2014. Systems thinking, the Swiss Cheese Model and accident analysis: A comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models. Accid. Anal. Prev. 68, 75–94. doi:10.1016/j.aap.2013.07.027
Unnikrishnan, G., Rajab, A., others, 2008. Integrating Systems Approach in Accident and Incident Investigations, in: SPE International Conference on Health, Safety, and Environment in Oil and Gas Exploration and Production. Society of Petroleum Engineers.
Vaughn, D., 1996. The Challenger launch decision, U. Chicago. ed. Chicago.
Villemeur, A., Caseau, P., D'Harcourt, A., 1988. Sûreté de fonctionnement des systèmes industriels: fiabilité, facteurs humains, informatisation. Eyrolles, 1988, Paris, France.
Volpe, J.A., 2014. A Transportation Systems Safety Hazard Analysis Tool.
Wiener, N., 1961. Cybernetics : Control and Communication in the Animal and the Machine, MIT Press. ed.
Wilpert, B., Fahlbruch, B., 1998. Safety related interventions in interorganisational fields. Saf. Manag. Chall. Change.
Woods, P.D.D., Leveson, P.N., Hollnagel, P.E., 2012. Resilience Engineering: Concepts and Precepts. Ashgate Publishing, Ltd.

Yang, Q., Tian, J., 2015. A Formal Approach to Causal Analysis based on STAMP (CAST). Presented at the The First International Conferen ce on Reliability Systems Engineering.
Yang, X., Haugen, S., 2014. A Fresh Look at Barriers from Alternative Perspectives on Risk.

Résumé

En vue d'éviter ou de diminuer l'importance des dégâts causés par les accidents majeurs, il convient de modéliser les fonctions et les relations entre les composants d'un système industriel. Pour cela, dans cette thèse, on utilise la démarche de modélisation par la méthode STAMP (Systems-Theoretic Accident Model and Processes) pour représenter la structure hiérarchique du système, ainsi que les mécanismes de contrôle nécessaire pour préserver la sécurité d'un processus industriel. Afin de traiter les problématiques liées aux contrôles de la sécurité industrielle, on propose l'utilisation de l'outil de simulation Anylogic. Cet outil, permet modéliser et de simuler le comportement du système en fonction du temps en mode normal et en mode dégradé.

L'objectif de ces travaux est donc de proposer une démarche basée à la fois sur la modélisation et la simulation pour analyser les risques et prévenir les accidents d'un site de stockage et distribution de GPL (Gaz Pétrole liquéfié).

Mots Clés

Anylogic, STAMP (Systems-Theoretic Accident Model and Processes), Analyse des risques, Accident, GPL

Abstract

In this thesis, system thinking concepts and simulation tools are used to model control actions and operator's behaviour at a French liquefied petroleum gas (LPG) storage and distribution facility. In France, such facilities are classified and the subject of special legislation and safety regulations. Their supervision is the responsibility of a control and regulatory body. A technological risk and prevention plan is provided, where all the dangerous phenomena likely to occur in addition to the safety control measures are listed in the safety report. Safety is therefore addressed through rules, and control mechanisms ensure that the system complies with safety constraints. Taking this facility as a case study, we use the STAMP (Systems-Theoretic Accident Model and Processes) theoretical framework coupled with AnyLogic simulation tool to model technical elements and human and organizational behaviour. We simulate how the system evolves over time and the strategies that are deployed in a loss of control scenario. The aim is to assess whether the prescribed safety program covers all of the system's phases; namely operations and audits. The results enrich other research that focuses on the contribution of system dynamics to risk analysis and accident prevention.

Keywords

STAMP (Systems-Theoretic Accident Model and Processes), risk analysis, LPG plant, Anylogic, Accident