

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.

Mots clés

STAMP, CAST, FPSO, Modélisation, accident, pétrole et gaz

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*) (Leveson, 2012) 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 golf 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 événementielle. Le déroulement des événements est clairement décrit et un litige est remarqué dans le choix de la cause principale (événement 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 and 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; Hickey, 2012; Kwon, 2015; Leveson et al., 2016; Meaghan O'Neil, 2014; Samost, 2015; Spencer, 2012; Thammongkol, 2014; Vincent H. Balgos, 2002). Les principales étapes de l'analyse CAST sont au nombre de neuf :

Etapes	Description
1	Identifier les systèmes et les dangers impliqués dans le processus de l'accident.
2	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
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 commandes fournies dans le but de contrôler la sécurité de l'installation.
4	Déterminer les événements conduisant à la perte de contrôle du système.
5	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.
6	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 inférieur. 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.
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 : <ul style="list-style-type: none"> • Les instructions et les directives de sécurité • Les mécanismes et processus de contrôles <ul style="list-style-type: none"> - Contexte - Rôles et responsabilités. En général, la description du rôle de chaque composant dans la structure de contrôle doit comporter ce qui suit : <ul style="list-style-type: none"> • Les instructions et les directives de sécurité • Les mécanismes et processus de contrôles <ul style="list-style-type: none"> - Contexte - Rôles et responsabilités. - Facteurs environnementaux et conditionnement opérant (les mécanismes de conditionnement

	<p>du comportement, le contexte d'influence sur le processus de prise de décision).</p> <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> - 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.

1. 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'environ 2 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,) entraînent 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.

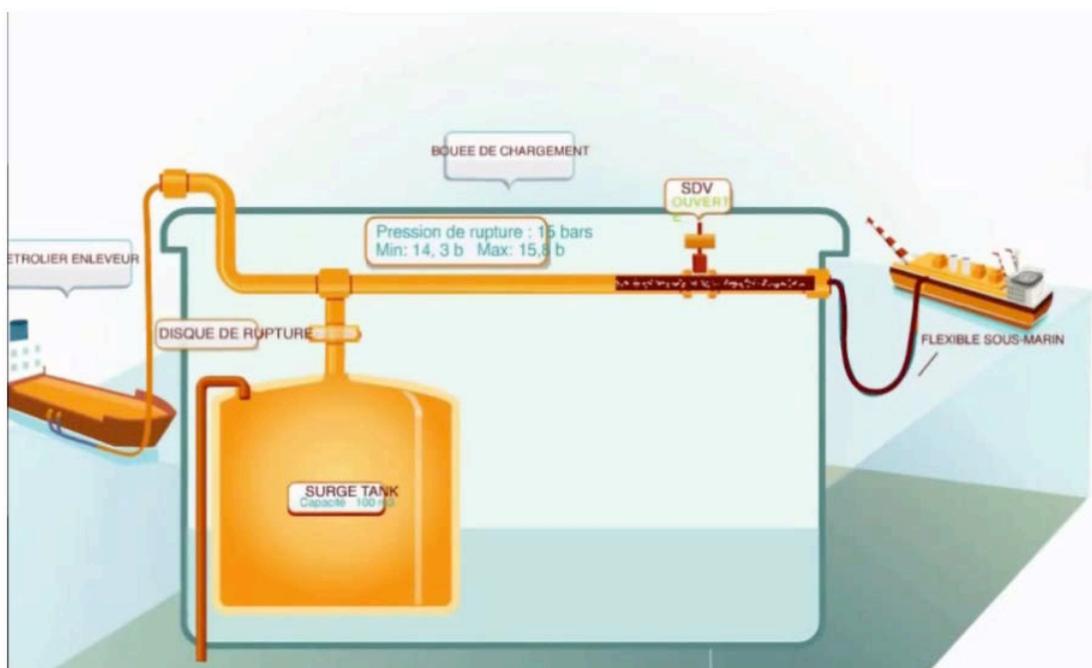


Figure 1 Système de transfert

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.

2. 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 :

- CS1. L'opération de transfert d'hydrocarbure est continuellement sous contrôle positif
- CS2. Des mesures doivent être préconisées pour protéger l'infrastructure et l'installation technique
- CS3. Des mesures doivent être préconisées pour protéger l'environnement
- CS4. Des mesures doivent être préconisées pour minimiser les pertes humaines et matérielles, si par inadvertance un incendie/explosion se produit.

3. 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.

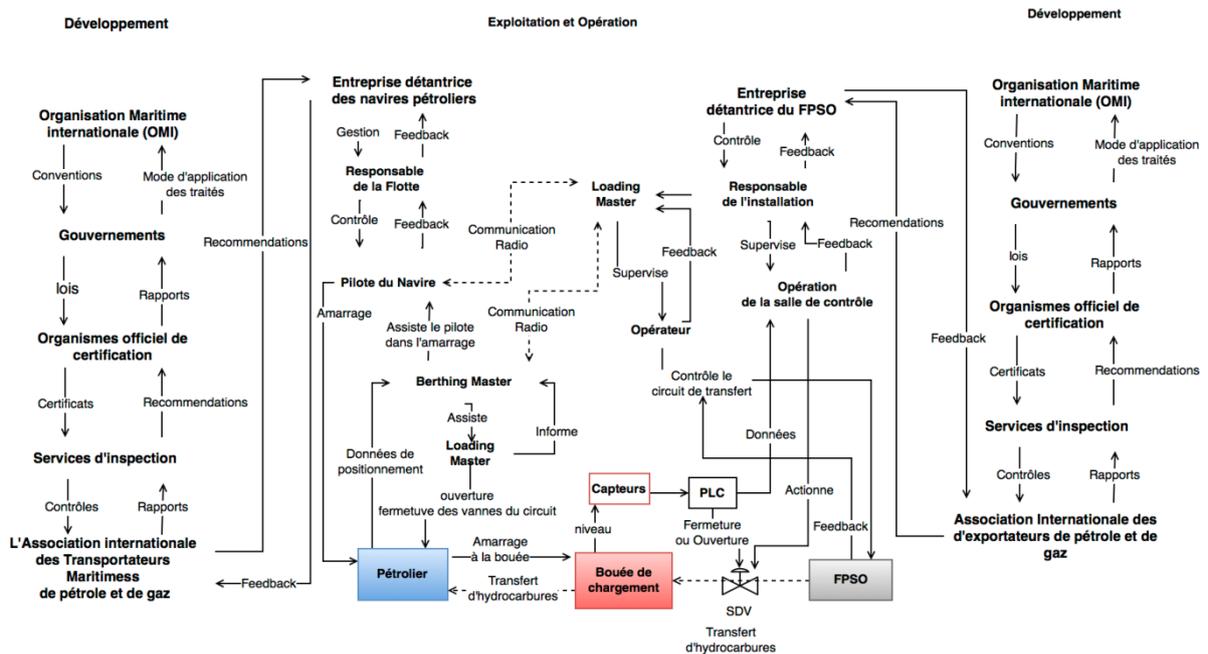


Figure 2 La structure de contrôle

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*.

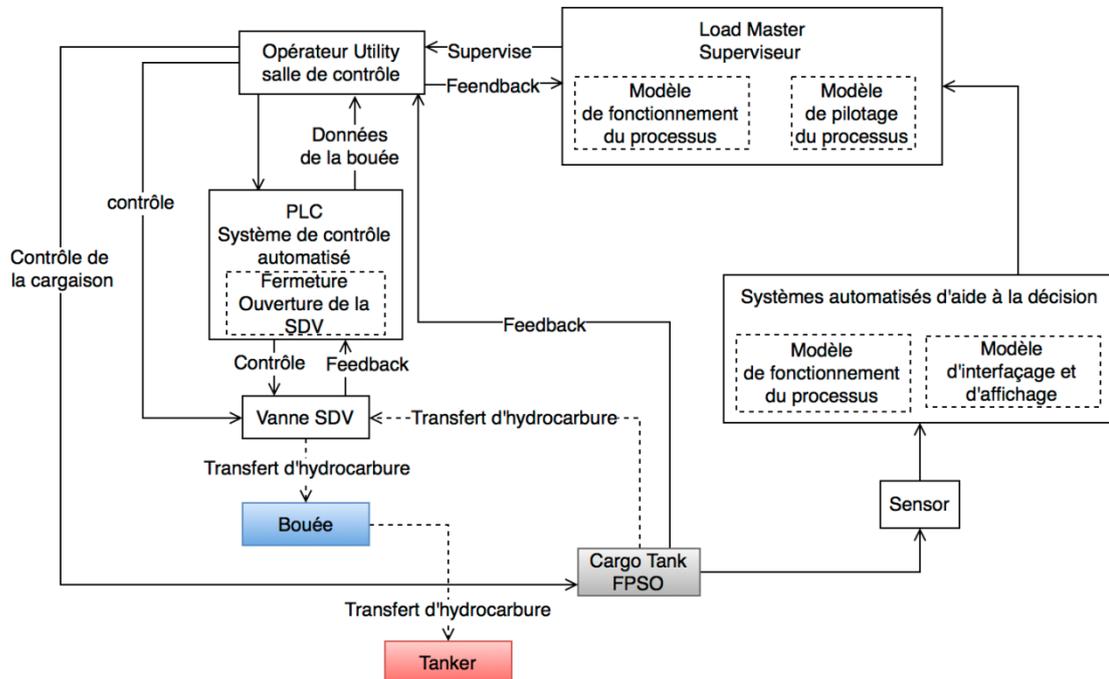


Figure 3 Modèle d'une structure de contrôle du processus de chargement d'un navire tanker

4. 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.

5. 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

5.1. 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.

5.2. 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.

5.3. 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.

6. 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 à 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 inférieur 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.

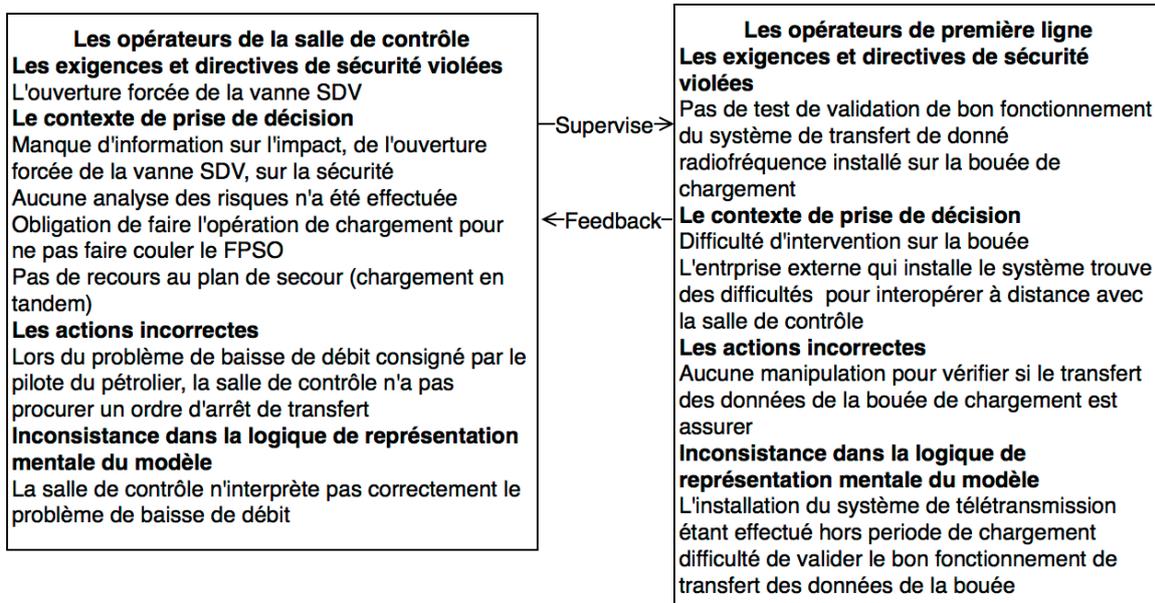


Figure 4 Analyse du comportement de l'opérateur

7. 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.

7.1. 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.

7.2. 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

7.3. 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 pas prise en considération par l'équipe du FPSO, qui ne déclenche pas l'arrêt de transfert.

8. 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.

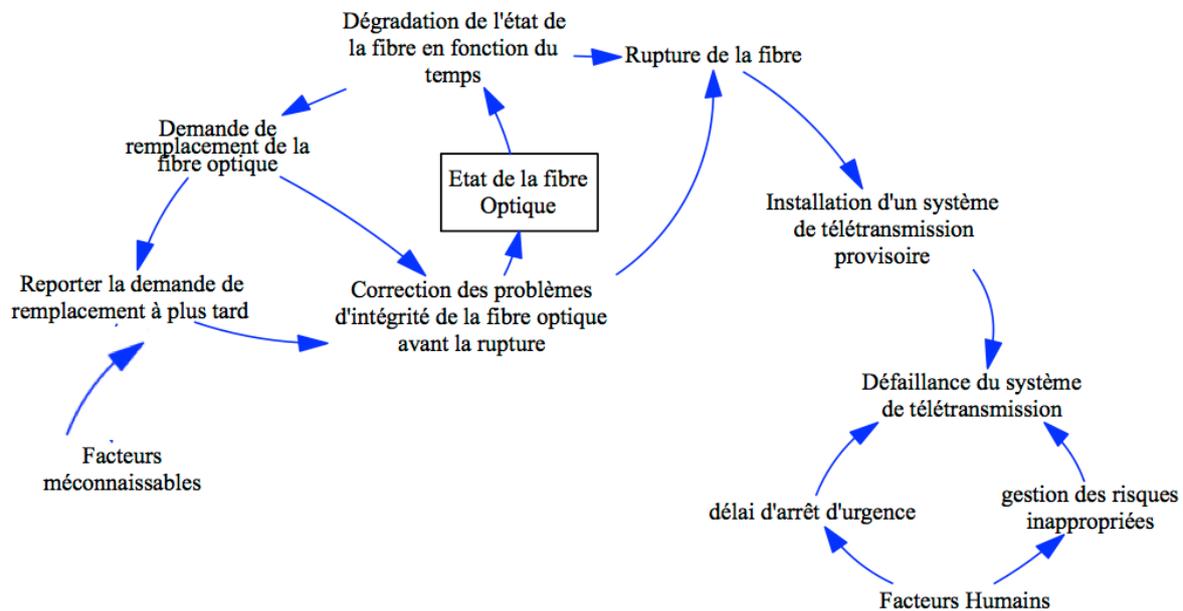


Figure 5 modèles simplifiés de l'accident

9. 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 apparaître un ensemble de recommandations. Pour l'accident du FPSO, elles sont classées selon 4 catégories :

9.1. 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).

9.2. Gestion de l'entreprise

Dans le cas du FPSO, il y a la compagnie pétrolière et la compagnie maritime. Chacune doit veiller de son côté 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.

9.3. 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 raisons 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.

9.4. 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

- Carlson, S.J. (Stephen J., 2014. Understanding government and railroad strategy for crude oil transportation in North America (Thesis). Massachusetts Institute of Technology.
- Dong, A., others, 2012. Application of CAST and STPA to railroad safety in China. Massachusetts Institute of Technology.
- Hardy, K., Guarnieri, F., 2012. Modéliser les accidents et les catastrophes industrielles, Lavoisier. ed, Sciences du risque et du danger.
- Hickey, J.J.P., 2012. A system theoretic safety analysis of US Coast Guard aviation mishap involving CG-6505. Massachusetts Institute of Technology.
- International Association of Oil and Gas Producers, 2006. Guideline for managing marine risks associated with FPSOs (No. 377).
- Kwon, Y., 2015. System Theoretic Safety Analysis of the Sewol-Ho Ferry Accident in South Korea. Massachusetts Institute of Technology.
- Leveson, N., 2012. Engineering a Safer World: Systems Thinking Applied to Safety. The MIT Press Cambridge Massachusetts London, England.
- Leveson, N., Samost, A., Dekker, S., Finkelstein, S., 2016. A Systems Approach to Analyzing and Preventing Hospital Adverse Events.
- Meaghan O'Neil, 2014. Application of CAST to Hospital Adverse Events. Massachusetts Institute of Technology.
- Oueidat, D., Guarnieri, F., Garbolino, E., Rigaud, E., 2015. Evaluating the Safety Operations Procedures of an LPG Storage and Distribution Plant with STAMP. *Procedia Eng.* 128, 83–92. doi:10.1016/j.proeng.2015.11.507
- Samost, A., 2015. A systems approach to patient safety: preventing and predicting medical accidents using systems theory. Massachusetts Institute of Technology.
- Spencer, M.B., 2012. Engineering financial safety: a system-theoretic case study from the financial crisis. Massachusetts Institute of Technology.
- Syvrtsen, R.-A.H., 2012. Modeling the Deepwater Horizon blowout using STAMP. 79.
- Thammongkol, P., 2014. The system theoretic accidental analysis of a crude unit refinery fire incident. Massachusetts Institute of Technology.
- Thorogood, J.L., 2015. The Macondo Inflow Test Decision: Implications for Well Control and Non-technical Skills Training. Society of Petroleum Engineers. doi:10.2118/173123-MS
- Underwood, P., 2013. Examining the systemic accident analysis research-practice gap (Thesis). © Peter Underwood.
- Vincent H. Balgos, 2002. Systems Theoretic Application to Design for the Safety of Medical Diagnostic Devices. Massachusetts Institute of Technology.

Mots clés

STAMP, CAST, FPSO, Modélisation, accident, pétrole et gaz