Proposition d'architecture et de processus pour la résilience des systèmes : application aux systèmes critiques à longue durée de vie

Jean-René Ruault

▶ **To cite this version:**

Jean-René Ruault. Proposition d'architecture et de processus pour la résilience des systèmes : application aux systèmes critiques à longue durée de vie. Biomécanique [physics.med-ph]. Université de Valenciennes et du Hainaut-Cambresis, 2015. Français. NNT : 2015VALE0025 . tel-01273751

HAL Id: tel-01273751

https://theses.hal.science/tel-01273751v1

Submitted on 13 Feb 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Université de Valenciennes et du Hainaut-Cambrésis

Thèse de doctorat

Pour obtenir le grade de Docteur de l'Université de

VALENCIENNES ET DU HAINAUT-CAMBRESIS

Mention : **Automatique**
Spécialité : **Automatique, Génie Informatique**

Présentée et soutenue par

Jean-René RUAULT

Le 07/07/2015, à Valenciennes

École doctorale :

Sciences Pour l'Ingénieur (SPI)

Equipe de recherche, Laboratoire :

Département Automatique et Département Informatique, Laboratoire d'Automatique, de Mécanique et d'Informatique, industrielles et Humaines (LAMIH)

Proposition d'architecture et de processus pour la résilience des systèmes ; application aux systèmes critiques à longue durée de vie

cnrs dépasser les frontières

LAMIH LABORATOIRE D'AUTOMATIQUE DE MECANIQUE ET D'INFORMATIQUE INDUSTRIELLES ET HUMAINES

JURY

Président du jury

- Riera, Bernard, Professeur, CReSTIC, Université de Reims, Reims.

Rapporteurs

- Calvary, Gaëlle, Professeur, Laboratoire d'Informatique de Grenoble, Grenoble.
- Boy, Guy André, Professeur, Florida Institute of Technology, Melbourne, Floride, USA.

Examinateurs

- Chatty, Stéphane, Docteur, Chercheur à Ecole Nationale de l'Aviation Civile, Toulouse.
- Luzeaux, Dominique, Ingénieur Général de l'Armement, HdR, Ministère de la Défense et enseignant chercheur rattaché à la Chaire Ingénierie des Systèmes Complexes de l'Ecole Polytechnique.

Directeurs de thèse

- Kolski, Christophe, Professeur, UVHC, Valenciennes.
- Vanderhaegen, Frédéric, Professeur, UVHC, Valenciennes.

Membre invité

- Dohet, Alain, Ingénieur Général de l'Armement, Responsable du pôle Système de Systèmes de la DGA, DGA, Paris.

« L'imprévu est la norme » (AAE, 2013)

Remerciements

Je remercie beaucoup Monsieur Alain Kada de m'avoir donné l'opportunité d'effectuer ma thèse dans le cadre du droit individuel à la formation, ainsi que Madame Marie-Adélaïde Grandclément, Messieurs Hervé Moraillon, Didier Malet et tous mes collègues pour m'avoir soutenu et aidé tout au long de ma thèse.

Je remercie beaucoup Messieurs Christophe Kolski et Frédéric Vanderhaegen, pour m'avoir guidé, aidé le long du chemin, ainsi que les collègues du LAMIH de m'avoir chaleureusement accueilli parmi eux.

Je remercie Madame Gaëlle Calvary et Monsieur Guy Boy, rapporteurs ainsi que Messieurs Stéphane Chatty, Dominique Luzeaux, et Bernard Riera examinateurs du jury de thèse, Monsieur Alain Dohet, invité.

Des remerciements tout particuliers à Dominique Luzeaux pour nos aventures contre vents et marées et à Christian Colas qui, après de longues discussions, a exprimé ce besoin des opérateurs de comprendre la situation et qui a fait germer l'idée de la thèse, ainsi que Jean-François Avril qui m'a mis le pied à l'étrier.

Enfin, je remercie beaucoup Maman et toute ma famille, ainsi que mes amis pour m'avoir suivi dans cette voie, malgré les avanies et ma faible disponibilité.

Je dédicace ma thèse à Papa, qui nous a quittés il y a 10 ans, et aurait été fier de m'accompagner sur ce chemin, ainsi qu'à Robert Marcouf et à Pascal Cantot.

À eux, je dois cette très belle et très riche aventure. Tous mes chaleureux remerciements pour leur aide et leur soutien.

Table des matières

Tableaux et figures

Introduction générale

Enjeux de la résilience

De nombreux systèmes, tels que ceux des domaines de la production d'énergie, de l'aéronautique, du ferroviaire, de la défense, entre autres, présentent une durée de vie de plusieurs dizaines d'années. Les processus et activités pour concevoir, produire, qualifier, mettre en œuvre, maintenir puis démanteler de tels systèmes sont décrits dans des documents de bonnes pratiques (Meinadier & Fiorèse, 2012) et des normes (ISO, 2008). Ces documents préconisent de caractériser le besoin exprimé par les différentes parties prenantes, dont les utilisateurs, que le système doit satisfaire. Cette caractérisation du besoin s'appuie sur la description des processus métier, des activités des utilisateurs, représentés sous formes de scénarios opérationnels de référence. La sûreté de fonctionnement et la sécurité complètent ces scénarios en prenant en compte les événements redoutés probables que le système peut rencontrer. Cette caractérisation du besoin définit les fonctionnalités du système, c'est-à-dire les services qu'il doit rendre, les performances attendues et les mécanismes d'adaptation permettant au système de répondre aux perturbations prévisibles. L'équipe projet doit élaborer une solution qui satisfasse ce besoin au moindre coût. Cette solution doit être faisable avec les technologies disponibles, mise en œuvre de façon sûre par des opérateurs formés, et maintenue durant toute la vie opérationnelle du système. Ce dernier est conçu avec des réserves permettant d'effectuer périodiquement des rénovations pour prendre en compte les obsolescences des technologies et les évolutions attendues des performances. La définition du système décrit son architecture, l'organisation de ses différents composants, afin d'atteindre les performances attendues en toute sécurité dans des conditions d'emploi clairement définies.

Durant la durée de vie d'un système, les opérateurs s'approprient ce système, élaborent de nouveaux modes opératoires. L'organisme exploite le système à d'autres fins que celles pour lesquelles il a été conçu. Le déploiement du système génère des évolutions des pratiques et un accroissement des performances. Pour continuer à exploiter le système et accroître ses performances, les dispositifs de sécurité sont désactivés. Les opérateurs évoluent. Les premiers opérateurs, l'âge aidant et partant en retraite, sont remplacés par de jeunes opérateurs qui ont développé d'autres habitudes face aux technologies. Petit à petit, le système est mis en œuvre en dehors de son domaine de définition, en dehors du domaine d'emploi sûr pour lequel il a été conçu. Au fur et à mesure, les opérateurs sont susceptibles de perdre la capacité de comprendre son fonctionnement et par conséquent la capacité de le contrôler. Le système se trouve alors dans des situations imprévues, sans précédent, face auxquelles les opérateurs ne peuvent le mettre en œuvre de façon sûre. Cette dynamique du système n'est pas traitée par l'ingénierie système et la sûreté de fonctionnement. Ces démarches achoppent à rendre compte de ces situations imprévues, sans précédent, pour que les opérateurs puissent les traiter convenablement et ainsi éviter la survenue d'accidents. Il est donc nécessaire de compléter ces démarches pour prendre en compte cette dynamique et ces situations.

La restauration de la capacité des opérateurs à surveiller l'usage et l'état du système, à en comprendre sa dynamique, à évaluer sa position par rapport à une zone de danger, est un préalable pour que les opérateurs puissent contrôler le système, mettre en œuvre une démarche essai-erreur pour résoudre les problèmes qu'ils rencontrent et, ainsi, éviter la survenue d'accidents. Le système doit donc disposer des moyens pour informer les opérateurs

de son état, de son usage, de son environnement, sa position par rapport à son domaine d'emploi.

La résilience (Luzeaux, 2011) concerne la capacité d'un système à s'ajuster face à des événements perturbateurs, à s'adapter face à des situations sans précédent, lorsque les perturbations rencontrées sont en dehors du périmètre des mécanismes d'adaptation spécifiés. Cette capacité s'appuie sur la surveillance du système et la détection des excursions du système hors de son domaine d'emploi. Elle requiert qu'en cas d'événements sans précédent, imprévisibles, les opérateurs puissent comprendre la situation, adapter leur cadre de référence mental, pour improviser et conduire à vue. En ceci, la résilience satisfait au besoin de réintroduire la contrôlabilité du système par les opérateurs.

Notre travail s'inscrit dans ce contexte. Il s'agit, d'une part, dans la perspective de l'architecture du système, de faire évoluer celle-ci pour montrer aux opérateurs son état réel et, d'autre part, dans la perspective des processus d'ingénierie, de faire évoluer ces processus afin de prendre en compte la longue durée de vie du système et les situations imprévisibles qu'il sera amené à rencontrer.

Le premier objectif de la thèse est de proposer un patron de conception afin d'aider les ingénieurs à concevoir un système permettant aux opérateurs de comprendre l'état du système, sa situation réelle, son environnement et sa proximité par rapport à une zone de danger, afin que ces derniers puissent prendre des décisions appropriées et engager des actions pertinentes pour éviter la survenue d'un accident.

L'objectif de ce patron de conception est de surveiller l'état et l'usage du système et d'alerter les opérateurs quand le système s'éloigne de son domaine d'emploi et est à proximité d'une zone de danger. La solution consiste à intégrer un dispositif en charge de surveiller l'usage et l'état du système, et qu'une alerte soit communiquée aux opérateurs de façon adaptée à leurs tâches, à leurs modèles mentaux, aux dispositifs d'interface utilisateur mis en œuvre. Cette intégration génère des impacts sur l'architecture fonctionnelle et l'architecture physique du système. Le patron de conception vise à réduire ces impacts afin de faciliter la conception, l'intégration et la maintenance.

Le second objectif de la thèse est de proposer des évolutions des processus d'ingénierie afin de prendre en compte les évolutions de l'environnement, des performances, des usages, etc., tout au long de la durée de vie du système. En effet, ces évolutions de l'environnement, des usages et des performances ont pour conséquence que le système est mis en œuvre en dehors de son domaine de définition, dans des situations qui n'étaient pas envisagées. Cela se traduit par la prise en compte du processus d'appropriation, des franchissements de barrières, par l'ingénierie et l'ergonomie.

Ainsi, les processus d'ingénierie système doivent évoluer pour prendre en compte ce dispositif de surveillance et d'alerte, et le retour d'expérience (évolutions de l'environnement, évolutions des performances, évolutions des modes opératoires). Dans la perspective de la longue durée de vie du système, l'ergonomie évolue, elle aussi, en intégrant la prospective. À cet égard, le persona, représentation fictive d'un futur utilisateur, permet de rendre compte des utilisateurs représentatifs aux différents horizons temporels du système, sachant qu'ils ne sont parfois pas nés aux étapes amont d'ingénierie système.

Le mémoire ne saurait couvrir les nombreux impacts, tant du point de vue de l'architecture que des processus d'ingénierie. Les plus importants seront identifiés comme perspective de recherche.

Contenu du mémoire

État de l'art

L'état de l'art est consacré à présenter les concepts structurants du mémoire qui répondent aux deux objectifs, d'une part celui d'élaborer un patron de conception d'architecture d'un système résilient, et, d'autre part celui de proposer des processus à mettre en œuvre pour contribuer à la résilience d'un système.

Le Chapitre 1 intitulé « De la sûreté de fonctionnement à la résilience» commence en présentant les enjeux opérationnels de la résilience. Il s'agit en particulier de la longue durée de vie opérationnelle d'un système, des évolutions que connaît son environnement, ainsi que les évolutions des pratiques des opérateurs. À ce titre, l'accroissement des exigences de performance induit des franchissements de barrières ainsi que des migrations silencieuses. Ce chapitre se poursuit en traitant la sûreté de fonctionnement ainsi que la sécurité. Cette dernière vise à déterminer les risques que court un système, en caractérisant les probabilités et les conséquences d'événements redoutés pour définir le domaine d'emploi sûr du système. En outre, la sûreté de fonctionnement préconise de surveiller l'état du système durant son exploitation opérationnelle. La sûreté de fonctionnement mentionne que de nombreux accidents sont dus à des erreurs humaines. C'est dans ce contexte que le chapitre se poursuit pour traiter de la fiabilité humaine, du caractère inhérent à l'être humain de faire des erreurs et de mettre en œuvre des moyens de récupération de ces erreurs. Plusieurs facteurs de contexte et facteurs de performance interagissent pour contribuer, positivement ou négativement à la sécurité. Pour autant, la sécurité ne rend pas compte des situations imprévues, sans précédent, que connaît un système durant sa vie opérationnelle. Il s'agit d'aller au-delà du périmètre de la sécurité pour traiter des situations imprévisibles, sans précédent. La résilience, que nous présentons ensuite, en particulier dans sa fonction « éviter », offre la capacité de conduire à vue, lorsque le système fonctionne hors de son domaine d'emploi et est face à des situations imprévues, sans précédent. Pour conduire à vue, les opérateurs doivent comprendre la dynamique du système pour le contrôler, prendre à temps des mesures correctives, et engager des actions nécessaires afin de maintenir la sécurité du système. Pour cela, ils ont besoin de construire une conscience partagée de la situation qui leur permet de comprendre cette dynamique du système, dernier point que nous présentons dans ce chapitre.

Dans le Chapitre 2 intitulé « Ingénierie Système appliquée aux systèmes critiques », nous commençons par présenter ce qu'est un système artificiel, ainsi que les processus d'ingénierie pour concevoir, produire, qualifier, mettre en œuvre, maintenir et démanteler un système dont la vie opérationnelle peut durer plusieurs dizaines d'années. Nous poursuivons en montrant comment le système est organisé en décrivant ce que sont l'architecture fonctionnelle et l'architecture physique, les liens entre fonctions et entre composants, ainsi que la relation d'allocation des fonctions aux composants. Ces points nous sont utiles afin de faire évoluer ces architectures pour prendre en compte la résilience. Nous présentons le langage de modélisation SysML (*System Modelling Language*) et plusieurs de ses principaux diagrammes. Ces diagrammes sont utilisés pour modéliser l'architecture fonctionnelle et l'architecture physique de la résilience. Après quoi, nous montrons ce qu'est un système de surveillance de l'état et de l'usage en détaillant l'organisation de ses traitements et ses paramètres. Ce système de surveillance de l'état et de l'usage est la clef de voûte pour donner aux opérateurs une représentation de la dynamique du système.

Dans un premier temps, le Chapitre 3 intitulé « Éléments d'ergonomie et d'ingénierie des IHM : conception centrée utilisateur et architecture des systèmes interactifs » définit des

concepts de l'interaction homme-machine. Il se poursuit en présentant les processus de conception centrée utilisateur et en abordant le modèle de l'utilisateur, en particulier le concept de persona, et le modèle de tâche. Ces modèles sont pertinents pour rendre compte de futurs utilisateurs qui ne peuvent pas être sollicités en phase amont des projets. Nous poursuivons en présentant l'ergonomie prospective, puis en détaillant le processus d'appropriation, qui sont des clefs pour rendre compte de l'évolution des usages durant la longue vie opérationnelle du système. Les travaux sur l'architecture des IHM proposent des éléments de modélisation, en particulier pour des IHM distribués afin que les différents opérateurs puissent disposer de présentations adaptées à leurs modèles mentaux, à leurs tâches et aux différents dispositifs interactifs qu'ils utilisent.

Contribution

La contribution vise à réintroduire la contrôlabilité du système[1] afin que les opérateurs puissent s'autoréguler mutuellement. Pour cela, ils ont besoin de comprendre la situation réelle dans laquelle se trouve le système. En particulier ils ont besoin de comprendre les excursions du système en dehors de son domaine d'emploi et les situations imprévisibles, sans précédent, qu'il rencontre

Nous proposons de créer le patron de conception « surveiller et alerter », pour la fonction « éviter » de la résilience, offrant aux opérateurs la capacité de comprendre la dynamique du système, de le conduire à vue face à des situations imprévisibles, sans précédent afin d'éviter la survenue d'un accident. Nous proposons aussi de faire évoluer les processus d'ingénierie et de conception centrée utilisateur pour qu'ils contribuent à la résilience d'un système critique à longue durée de vie.

Cette contribution s'articule sur trois chapitres (le premier de ceux-ci se voulant avant tout introductif).

Le Chapitre 4 intitulé « Positionnement de la contribution par rapport à la problématique de la résilience des systèmes » vise à positionner la résilience dans le contexte de l'usage du système, afin de rendre explicite les migrations silencieuses et les excursions du système en dehors de son domaine de définition, ainsi que de présenter la décomposition fonctionnelle de la résilience.

Le système doit montrer sa dynamique, son usage, l'écart entre son état courant et l'état de référence de son domaine d'emploi pour que les opérateurs puissent comprendre sa dynamique, le conduire à vue. Cela implique de faire évoluer son architecture afin d'y insérer un dispositif de surveillance de l'usage et de l'état du système. Le Chapitre 5 intitulé « Proposition d'un patron de conception pour l'architecture d'un système résilient » décompose la fonction « éviter » de la résilience en sous-fonctions auxquelles sont alloués les composants du système de surveillance de l'usage et de l'état du système, ainsi que de l'interface utilisateur.

Enfin, le Chapitre 6 intitulé « Proposition de processus à mettre en œuvre pour contribuer à la résilience d'un système » consiste à envisager le système sur l'ensemble de sa durée de vie en mettant en œuvre et en complétant l'ergonomie prospective, c'est-à-dire pour se projeter sur le long terme. Cela se traduit en formalisant le processus d'appropriation, d'autre part pour concevoir en préparation de l'appropriation, pour l'appropriation, et, d'autre part de concevoir

[1] La contrôlabilité est définie ici comme la capacité des opérateurs à contrôler le système (Amalberti, 2002 ; Amalberti, 2006 ; Amalberti, 2009).

en profitant du retour d'expérience issu de l'appropriation, c'est-à-dire par l'appropriation. Par ailleurs, cela se traduit aussi en rendant compte des futurs utilisateurs, qui ne sont pas forcément nés lors de la conception, par le biais du persona.

Étude de cas

L'étude de cas consiste à appliquer le patron de conception « surveiller et alerter », proposé dans cette thèse, au domaine ferroviaire pour en valider la faisabilité, selon une approche de rétro-ingénierie. Nous y appliquons aussi le persona. Ces deux applications nous permettent d'identifier des améliorations potentielles des IHM.

Dans un premier temps, trois accidents de train sont présentés, avec une synthèse des rapports d'enquête technique rédigés par des organismes indépendants.

Le premier accident présenté est celui de Chatsworth, en Californie, le conducteur de train avait franchi un signal rouge. Le second accident est celui de Zoufftgen, à la frontière entre le Luxembourg et la France. Le chef de circulation de la gare de Bettembourg avait délivré un ordre écrit de franchissment de signal fermé à un conducteur de train, alors que la voie était occupée par un train de fret venant de France. Le troisième cas est l'accident d'Aldershot. Exceptionnellement, des travaux sur une voie amenaient la régulation à faire contourner ces travaux par le train. L'équipe d'exploitation n'a pas compris la situation. Le train s'est engagé avec une vitesse excessive sur une liaison limitée à 24 km/h. Le train dérailla.

Ces accidents sont analysés du point de vue de la résilience dans la perspective de donner aux opérateurs la capacité de comprendre la situation.

Après cette présentation des trois accidents et leur analyse du point de vue de la résilience, la faisabilité d'appliquer un scénario et des personas pour rendre compte de ces accidents est évaluée.

La troisème étape consiste à appliquer le patron de conception. L'objectif visé est d'évaluer la capacité de la proposition d'architecture à alerter les opérateurs afin qu'ils puissent éviter l'accident.

Enfin, après avoir appliqué le scénario, le persona et le patron de conception, nous proposons des améliorations des IHM susceptibles de satisfaire à la fonction « éviter » de la résilience.

Conclusion

Le rapport s'achève avec une conclusion reprenant en synthèse le mémoire et présentant des perspectives de recherche pour compléter les points soulevés qui nécessitent des travaux supplémentaires de recherche.

Partie 1 État de l'art

Table des matières de la partie 1

Chapitre 1.

De la sûreté de fonctionnement à la résilience

1.1. Introduction

Dans un premier temps, ce chapitre présente les enjeux opérationnels de la résilience. La longue durée de vie opérationnelle d'un système, les évolutions que connaît son environnement, ainsi que les évolutions des pratiques des opérateurs, en particulier les franchissements de barrières et les migrations silencieuses induits par l'accroissement des exigences de performance ont pour conséquences que le système peut se trouver rapidement dans une situation qui n'avait pas été prévue, envisagée.

Ce chapitre se poursuit en traitant la sûreté de fonctionnement ainsi que la sécurité. La sûreté de fonctionnement traite la sûreté du point de vue des défaillances que connaît le système, en mentionnant que la plupart des accidents sont dus à des erreurs humaines. De plus, la sûreté de fonctionnement postule que le concepteur ait une parfaite compréhension des conditions d'exploitation du système. La sécurité, quant à elle, offre un canevas pour évaluer et gérer les risques en s'appuyant sur les probabilités des événements redoutés et leurs conséquences, plus ou moins catastrophiques. Les méthodes les plus récentes prennent en compte la mise en œuvre réelle du système. Elles préconisent de surveiller les performances du système et d'analyser les données statistiques recueillies de l'exploitation du système. Pour autant, ces méthodes ne traitent pas des événements imprévisibles, des situations sans précédent que connaît un système durant sa vie opérationnelle. Par ailleurs, les analyses effectuées suite à des accidents mettent en œuvre la méthode de l'arbre de défaillance. Cette méthode met en évidence les non-respects des procédures qui ont des effets négatifs, mais ne rend pas compte des non-respects des procédures qui ont des effets positifs.

Après avoir traité de la sûreté de fonctionnement et de la sécurité, le chapitre aborde la question de la fiabilité humaine que soulèvent les documents de sûreté de fonctionnement. L'erreur est inhérente à toute activité humaine. Les opérateurs mettent en place des moyens de récupération. De plus, l'erreur contribue à l'apprentissage et à la régulation de l'activité. Les facteurs de contexte peuvent avoir des effets positifs ou négatifs sur la variabilité des performances et, à ce titre, doivent être pris en compte. Les travaux sur les erreurs humaines ont mis en évidence un ensemble de facteurs qui contribuent à générer ou à préserver des erreurs humaines. Il s'agit des travaux sur les facteurs de performance et les facteurs de contexte qui offrent un canevas pour structurer ce qui influence le comportement de l'ensemble des opérateurs qui mettent en œuvre un dispositif technologique.

Nous poursuivons en traitant la résilience. Elle offre un cadre pour comprendre comment les opérateurs improvisent face à des situations imprévues, sans précédent, conduisent à vue et d'apprennent les règles d'adaptation adéquates quand les perturbations sont en dehors du périmètre spécifié des mécanismes d'adaptation du système. À ce titre, la résilience concerne donc ce qui ne peut pas être anticipé. Nous présentons les quatre fonctions de la résilience que sont « éviter », « résister », « restaurer » et « s'adapter ».

Le chapitre se poursuit pour découvrir comment les opérateurs peuvent construire et maintenir une conscience partagée de la situation, c'est-à-dire un modèle dynamique du système et de

son environnement continuellement mis à jour. Cette conscience partagée de la situation est le préalable à la compréhension de la situation par les opérateurs pour pouvoir conduire à vue, réguler leur activité et mettre en œuvre une démarche essai-erreur pour résoudre les problèmes qu'ils rencontrent.

1.2. Enjeux opérationnels de la résilience

Un système critique conçu par l'homme présente une longue durée de vie, pouvant dépasser 50 ans. L'environnement opérationnel, dans lequel ce système sera mis en œuvre pour réaliser les missions pour lesquelles il aura été conçu, va évoluer durant cette longue période. Ces évolutions ne peuvent pas être complètement connues et prévues dans les phases amont du cycle de vie. De même, les missions peuvent évoluer. Les situations opérationnelles que ces systèmes rencontrent ne sont souvent pas prédictibles et ne peuvent pas être anticipées de façon systématique, comme le suggèrent les bonnes pratiques d'ingénierie système (ISO, 2008 ; Meinadier & Fiorèse, 2012). Dans le domaine militaire, la situation opérationnelle est, par construction, l'objet de surprises, et dépend des interactions entre les différents acteurs, lesquelles peuvent être malveillants (Desportes, 2004). Les incertitudes de l'environnement et des missions amènent le système à devoir s'adapter.

1.2.1. La longue durée de vie opérationnelle des systèmes

Les systèmes conçus par l'homme comprennent un ensemble d'éléments (matériels, logiciels, organisations et compétences humaines) en interaction, organisés pour répondre à un besoin. En ingénierie système, une situation opérationnelle de référence est définie afin de spécifier et de concevoir le système. Mais entre les étapes amont d'un programme et le moment où le système est mis en œuvre, l'ensemble de l'environnement politique, économique, social, technologique, environnemental et légal, voire culturel aura évolué. Au même titre que la conception des systèmes durant les décennies 80 et 90 ne prenait pas en compte la féminisation de l'armée (Kirke, 2005), aujourd'hui, nous ne savons pas quelles seront les évolutions sociétales ou géopolitiques qui pourront affecter les systèmes sociotechniques, tout au long de leur cycle de vie, et la façon dont seront mis en œuvre les systèmes techniques. Ainsi, les ingénieurs qui ont construit le site de Bio-Preparat sur l'île de Vozpojdiénié en 1948 (CI, 2001), n'envisageaient pas la Chute du Mur de Berlin et l'arrêt des activités de recherche sur ce site.

Les systèmes sur lesquels nous travaillons présentent des durées de vie de l'ordre de plusieurs dizaines d'années.

Par exemple, le Super Frelon est un hélicoptère qui a été conçu dans les années 50, dont le premier vol a eu lieu en 1962, mis en service en 1966 et retiré du service en 2010. Le B52, avion conçu dans les années 40 et mis en service en 1955, est toujours en service actif. Il est envisagé qu'il soit en service actif jusqu'en 2040, soit près d'un siècle. Quatre autres avions comptent plus de 50 ans de service actif. Ces systèmes sont régulièrement remis à niveau. Avant sa mise en service actif, il a été spécifié, conçu, réalisé et qualifié. Son retrait de service est la première étape du dernier stade du programme de démantèlement pouvant durer plusieurs années. Ces systèmes sont régulièrement remis à niveau. De l'idée originelle aux déchets ultimes, la durée de vie de ces systèmes est d'une soixantaine d'années, voire plus.

Le domaine ferroviaire comprend aussi des systèmes à longue durée de vie, que ce soit des infrastructures ou du matériel roulant. En ce qui concerne le matériel roulant, les rames MS61

de la ligne du RER parisien ont été commandées en 1963 et mises en service en 1967. Après rénovation, ces rames sont toujours en exploitation. La rénovation comprend l'installation de panneaux lumineux indicateurs de desserte, un système d'annonce vocale, des modifications du poste de conduite, l'esthétique avant et les couleurs de la rame, changeant substantiellement l'esthétique (cf. Figure 1.1) et laissant suggérer une remise à neuf. En revanche, la structure de la coque a été conservée, ce qui a une incidence sur la tenue au choc, mais aussi sur les flux entrant-sortant de la rame, induits par la largeur des portes.

Sources Internet [2]
Avant rénovation

Sources Internet[3]
Après rénovation

Figure 1.1. Illustrations de la rame MS61 avant et après rénovation.

Pour certains systèmes, la longue durée de vie est définie dès l'idée initiale et ils sont conçus dans cette perspective. Des plans de visites d'inspection et d'entretien sont programmés dès la conception de ces systèmes. Pour d'autres systèmes, en revanche, la durée de vie est prolongée au-delà de ce qui était initialement envisagé. Cette prolongation est due à différentes raisons. Les programmes des nouveaux systèmes devant les remplacer subissent du retard. La durée de vie des anciens systèmes est prolongée attendant que les nouveaux systèmes soient finis et prêts à être déployés. Les raisons économiques, manque d'argent pour acheter de nouveaux systèmes, sont aussi à l'origine de la prolongation de la vie de systèmes anciens.

Cette situation des systèmes existants, qui sont en service ou en fin de vie, est aussi celle des systèmes qui sont en cours de spécification, de conception ou de réalisation. Cette situation rend le travail des concepteurs et des ergonomes plus complexe et plus difficile. En effet, il s'agit de spécifier un système en effectuant des hypothèses sur ce que seront les missions qu'il sera amené à réaliser dans 30 ou 50 ans, avec des opérateurs (nous utilisons indifféremment opérateur et utilisateur dans la suite du mémoire pour désigner les opérateurs ainsi que les agents de maintenance) qui ne sont pas encore nés ou qui sont encore enfants au moment de la conception du système. Les concepts, méthodes et outils de l'analyse prospective sont d'ores et déjà mis en œuvre dans les grands projets d'infrastructure ou de défense pour identifier les scénarios opérationnels probables à horizon de 30 ans. Ces scénarios opérationnels probables issus d'une analyse prospective sont la clef de voûte des processus de spécification et de conception de futurs systèmes.

[2] Source : https://commons.wikimedia.org/wiki/File:Ms61_reuil.jpg

[3] Source : http://www.casimages.com/i/140402055141681289.jpg.html

1.2.2. L'incertitude de l'environnement

Faute de pouvoir se projeter en 2065 pour savoir quel sera l'environnement des systèmes conçus aujourd'hui, afin de les spécifier au regard de cet environnement, il est possible de se projeter en arrière, dans les années 60, lors de la conception des systèmes dont certains sont encore en service et d'autres retirés du service. Les ergonomes appliquaient des bonnes pratiques de l'ergonomie décrites dans les ouvrages de cette époque (Ombredane & Faverge, 1955). La démarche d'ergonomie s'appuyait sur ce qui était su des opérateurs et sur les opérations qu'ils étaient susceptibles de faire. Dans les années 50 à 70, il n'était pas envisagé de démonter et remonter le matériel pour mener des inspections approfondies pour évaluer si l'allongement de la durée de vie du système est possible, par exemple. Cette difficulté n'a trouvé sa réponse que dans les années 90 en incluant la modélisation des gestes d'entretien lors même de la conception de matériels. Cette situation rend les inspections plus difficiles et plus coûteuses. Aujourd'hui, en rétrospective (Colson & Cusset, 2008 ; Plassard, 2003), nous pouvons identifier les points qui n'ont pas pu être anticipés lors de la conception des systèmes existants ou qui ont été retirés du service. C'est le cas des systèmes qui ont été conçus à partir d'hypothèses implicites ou explicites sur les caractéristiques des opérateurs en charge de les mettre en œuvre ou sur les activités qu'ils sont supposés réaliser. Il s'avère que des changements sociaux, sociétaux et économiques modifient la population des opérateurs. Les opérateurs mettant en œuvre les systèmes ne présentent pas les mêmes caractéristiques que les opérateurs définis dans les hypothèses.

C'est le cas d'un système de drone aérien conçu et mis en œuvre au Royaume-Uni. Kirke (2004, 2005) montre les conséquences de l'introduction de ce système au sein de l'armée anglaise qui se féminise. Lorsque le système de drone a été conçu, il n'y avait pas de femme dans le corps de l'Artillerie Royale. Ce système de drone a donc été conçu pour être mis en œuvre par des hommes, en s'appuyant sur les capacités et données anthropométriques masculines. Le système de drone comporte une partie au sol (*Ground Data Terminal*), lourde à manipuler et déployée à un kilomètre de la station de contrôle (*Ground Control Station*) par une équipe de deux personnes. Dans la mesure où de nombreuses femmes ne peuvent pas manipuler la partie au sol (GDT), ni mener les activités de récupération de la partie volante du système de drone, l'équipe qui réalise ces activités ne comprend que des hommes. Dans ce contexte, les femmes sont alors employées dans les activités moins pénibles de logistique et de contrôle (GCS). Cette situation n'a pas pu être anticipée lors de la conception du système. La répartition des activités entre femmes et hommes selon leurs capacités physiques ne correspond pas à la coutume militaire selon laquelle le personnel doit tourner et réaliser plusieurs tâches différentes, pour s'approprier le métier. De plus cette répartition des activités entre hommes et femmes compromet aussi l'éthique de partage du fardeau au sein de l'armée (Kirke, 2004 ; Kirke, 2005). Nous trouvons une situation très proche dans le cas du programme Rafale. Le problème réside dans le décalage entre le poids minimum des pilotes de combat féminins, qui n'étaient pas d'actualité au lancement du programme, et la masse minimum à l'éjection nécessaire (sensiblement supérieure) pour la bonne cinétique du siège éjectable.

La prise en compte de la surcharge pondérale en ergonomie concerne tant le poste de travail des personnes en situation de surcharge pondérale que le poste de travail des personnes soignant des patients en surcharge pondérale. La conception des postes de travail dans les centres d'appel devient un enjeu en ergonomie pour prendre en compte la surcharge pondérale (Atlas Ergonomics, 2007). La surcharge pondérale a aussi des impacts pour la conception du mobilier (par exemple des chaises), des vêtements, des véhicules (Walter, 2012). Pour les soins des patients en situation de surcharge pondérale, les difficultés rencontrées concernent aussi bien les personnes vivantes, avec la conception de dispositifs dédiés telles que les

ambulances (Quémard, 2009), que les personnes décédées, les morgues devant être adaptées à cette situation (HB, 2010). Cette situation nouvelle, induite par l'épidémie de surcharge pondérale (WHO, 1998) n'était pas envisagée, il y a 25 ans.

Dans la perspective de construire un réseau de transport en commun ferroviaire, élargissant l'offre actuelle, les études prospectives du projet Grand Paris ont montré que les usagers, en moyenne, dans 10-15 ans, seront plus âgés et souffriront de surcharge pondérale, réduisant leur mobilité. Cela a des impacts sur les accès des stations et des trains. Cela nécessite de systématiser les ascenseurs et les escaliers mécaniques, en double, afin qu'il y en ait toujours un en service lorsqu'un autre est en panne ou en maintenance (Chérel, 2012).

Les enjeux résident dans la capacité à envisager et à décrire l'environnement, au sens large, dans lequel seront opérés les systèmes, durant leur stade d'exploitation, c'est-à-dire à horizon de 30 ou 50 ans, voire beaucoup plus, les impacts que cela peut avoir sur les futurs utilisateurs, en termes d'activité, de compétences, d'aptitudes attendues de leur part. Ils résident aussi dans la capacité à décrire les caractéristiques anthropométriques des futurs utilisateurs, leurs formations initiale et professionnelle, leurs aptitudes, etc. Enfin, les enjeux résident aussi dans la capacité offerte aux opérateurs d'ajuster et adapter les procédures et les artefacts technologiques pour répondre aux environnements et situations opérationnels qu'ils rencontreront, lesquels ne peuvent pas être décrits aujourd'hui.

1.2.3. Les franchissements de barrières, les violations des règles de sécurité et les migrations spontanées

Tout au long de cette période qui peut durer plusieurs dizaines d'années, l'environnement opérationnel évolue, les exigences de performance croissent. Les dispositifs de sécurité élaborés à partir des analyses de sécurité initiales sont désactivés pour maintenir ou accroître les performances du système.

Le franchissement de barrières (Vanderhaegen, 2003 ; Polet *et al.*, 2002 ; Vanderhaegen *et al.*, 2011) consiste, pour les opérateurs, à désactiver ou retirer les dispositifs de sécurité intégrés au système pour répondre aux exigences de maintien, voire d'accroissement des performances du système. Vanderhaegen (Vanderhaegen, 2003 ; Polet *et al.*, 2002 ; Vanderhaegen *et al.*, 2011) décrit comment les opérateurs contournent les dispositifs de sécurité ou créent de nouvelles procédures afin d'atteindre les niveaux de performance attendus et de réduire la charge de travail. L'analyse que font les opérateurs en matière de bénéfice, de coût et de déficit que génère ce retrait des barrières, subit des biais cognitifs, avec une surestimation des gains et une sous-estimation des risques (Vanderhaegen, 2003 ; Vanderhaegen *et al.*, 2011).

Vaughan (1996) décrit le phénomène de normalisation de la déviance comme une déviation des performances par rapport à la définition du système, se caractérisant par une augmentation régulière des critères de risques résiduels acceptables. Cette déviation devient une pratique routinière du groupe et s'institutionnalise. Progressivement, les ingénieurs et managers de la NASA instaurèrent une situation les autorisant à considérer que tout allait bien, alors qu'ils disposaient d'éléments montrant, au contraire, que quelque chose allait mal. Après chacun des incidents, à partir des analyses qu'ils conduisaient, les ingénieurs de la NASA considérèrent le risque comme acceptable, que la navette Challenger pouvait voler de façon normale et acceptable avec le défaut affectant le joint torique. Ils préconisaient la poursuite du programme sans que des tests et des études supplémentaires soient nécessaires. L'accumulation de ces décisions a progressivement conduit les ingénieurs à faire voler la navette avec de sérieuses anomalies, de façon routinière, jusqu'à la catastrophe du 28 janvier 1986.

Cette notion de normalisation de la déviance est aussi invoquée pour analyser les circonstances de l'accident de train qui eut lieu dans la nuit du 5 au 6 juillet 2013 à Lac Mégantic, au Québec, accident qui a fait 47 morts. Quelques jours plus tard, un expert en gestion des risques titrait un article « Un cas typique de «normalisation de la déviance» » dans le quotidien Le Devoir[4].

Amalberti (2006, 2009) montre que les dispositifs de sûreté, relevant de la réduction des risques, de l'optimisation, de la recherche de la qualité, réduisent les performances, et génèrent des comportements déviants pour maintenir les niveaux de performance requis par le management. Dans le cas de distributeur automatisé de médicaments que décrit (Amalberti (2009), le phénomène de migration peut débuter très vite dès la mise en œuvre du système automatisé. Amalberti montre ainsi que « les infirmières, avec la complicité des médecins, ont créé des faux patients pour refaire des stocks sauvages de médicament pour tous ces cas marginaux » que sont les cas où « le patient n'est pas encore enregistré dans la machine », ou « les situations de pertes de pilule en gériatrie ». Amalberti (2006) montre ainsi que les systèmes évoluent et migrent en silence, en s'éloignant de leur zone de sécurité.

La Figure 1.2 illustre les pressions générant les migrations spontanées et les violations routinières des règles de sécurité.

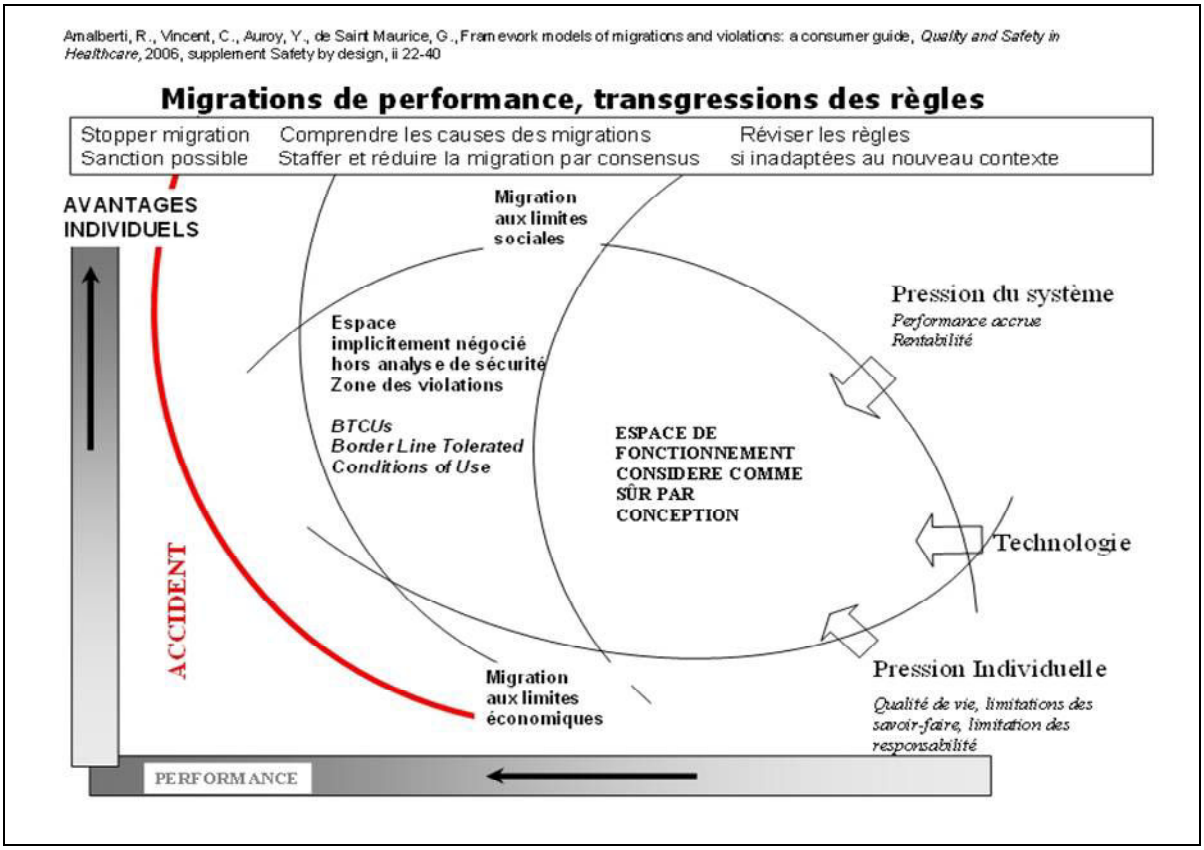

Figure 1.2. Modèle de migrations spontanées (Amalberti, 2009).

Les migrations surviennent pour prendre en compte les variations naturelles des conditions de l'activité, par exemple personnels absents, licenciement de personnels compétents (Amalberti, 2009). Elles surviennent aussi pour permettre d'atteindre une performance économiquement

[4] Sources : http://www.ledevoir.com/politique/villes-et-regions/382959/un-cas-typique-de-normalisation-de-la-deviance

viable, ou pour prendre en compte les évolutions de l'environnement opérationnel ; par exemple l'accroissement du trafic voyageur dans le domaine des transports en commun. Ces migrations, tolérées par la hiérarchie, fixent progressivement un fonctionnement officieux du système. Ce fonctionnement devient la norme, mais est exclu du champ du retour d'expérience. Le système est muet et ce fonctionnement est dans un angle mort, hors visibilité. Certaines pratiques continuent à migrer sans contrôle et finissent par provoquer des incidents, voire des accidents (Amalberti, 2009). Pour éviter ce phénomène de migration, il est nécessaire de laisser les opérateurs s'autoréguler mutuellement, c'est-à-dire de privilégier la sécurité régulée à la sécurité contrôlée (Amalberti, 2002). Des recherches sont menées pour mesurer ces migrations dans le domaine des systèmes dynamiques (Marseguerra, 2014).

D'une façon que nous pouvons juger complémentaire au processus de migration (Amalberti, 2009), Woods et Cook (2006) décrivent le mécanisme de décompensation. Face à des contraintes externes ou à des exigences croissantes de performance, les systèmes sociotechniques compensent pour maintenir leur capacité opérationnelle. Ce mécanisme de compensation réduit leur marge de sécurité et augmente leur vulnérabilité par rapport à des situations accidentelles qui génèrent alors des phénomènes de décompensation (Woods & Cook, 2006).

Un exemple dans le domaine médical peut illustrer ce mécanisme de compensation. Dans un système d'enregistrement de l'administration de médicaments qui ne fonctionne pas correctement, Woods & Cook (2006) montrent que les opérateurs ont dû improviser et effectuer une reprise manuelle du processus. Il s'avère que la capacité de reprise manuelle s'appuie essentiellement sur l'expérience des opérateurs qui comprennent comment fonctionne le système, dans quel état il est, et qui savent mettre en place une procédure complètement manuelle, efficace et fiable. Il est nécessaire que les opérateurs puissent identifier que le système fonctionne aux marges de son domaine de définition. Ce dernier mécanisme de compensation est composé de deux phases. Dans la première phase, une perturbation se développe petit à petit. Face aux effets de cette perturbation, le système s'adapte en mettant en œuvre un mécanisme de compensation qui lui permet de continuer à fonctionner et de maintenir ses performances. Ce mécanisme de compensation empêche de détecter l'origine et l'accroissement de cette perturbation. De plus, ce mécanisme exige plus de ressources et est plus coûteux que ne l'est le fonctionnement normal du système. La seconde phase, celle de décompensation *stricto sensu*, générant l'accident, désigne la dégradation du fonctionnement du système dès lors que le mécanisme de compensation est insuffisant face à l'accroissement de la perturbation ou devient excessivement coûteux.

En complément des propos d'Amalberti, il est nécessaire de détecter et de différencier la compensation, qui va générer une décompensation, et la migration qui est juste à la marge du domaine de définition et qui ne nécessite pas de ressources supplémentaires par rapport au fonctionnement normal. Cette détection repose sur l'évaluation et la comparaison de l'effort de contrôle face aux variations de l'environnement opérationnel par rapport à l'effort de contrôle prescrit. Ceci n'est possible que si l'effort de contrôle prescrit prend en compte les variations de l'environnement opérationnel.

Cet effet pervers de la recherche de la sûreté est induit par la réduction accrue de la nature adaptative du système sociotechnique, qui devient plus performant dans l'enveloppe prévue, mais aussi plus rigide et est extrêmement fragile hors de cette enveloppe, en situation de variation brutale du contexte (Paries, 2010).

Amalberti (1996) montre qu'il y a un paradoxe dans la recherche d'une augmentation de la performance en dégradant le compromis cognitif qu'a élaboré l'opérateur humain. De plus, l'automatisation et la conduite par objectifs génèrent une totale opacité du fonctionnement du

système automatisé pour l'opérateur. S'il doit reprendre la main lorsque l'automatisme cesse de fonctionner, cette opacité a pour conséquence que l'opérateur ne comprend pas la situation, l'état du système, et est incapable de prendre les actions appropriées.

Pour Amalberti (2009), la meilleure façon de contrôler le processus est de rendre visible la dynamique du système, puis de laisser les acteurs s'autoréguler mutuellement. Il est alors nécessaire de détecter et de surveiller la survenue et l'évolution des migrations. Il est aussi nécessaire de réintroduire la contrôlabilité du système, hors de son domaine de définition, hors du domaine de vol, pour prendre une analogie aéronautique (Amalberti, 2009).

Nous retenons deux points majeurs des propos d'Amalberti (2009) :

- « les déviations et les adaptations humaines resteront la règle dans tout système Homme-machine dont l'homme gardera le contrôle même partiel. Elles doivent donc être intégrées dès la conception des systèmes automatisés » ;
- « la cognition humaine est si flexible, les situations potentielles d'usage si nombreuses, que quel que soit l'outil mis entre les mains, il se trouvera toujours tôt ou tard des situations exceptionnelles qui déborderont le cadre sécuritaire procuré par l'outil, et feront même de la rigidité de l'outil la source de la perte de contrôle de la situation ; de même, l'homme (au sens du professionnel soumis aux contraintes de la compétitivité commerciale) finira toujours, pour des gains personnels ou professionnels, par adapter l'usage prévu et déborder les contraintes et consignes imaginées à la conception. Autant y penser dès la conception en résistant à des optimisations trop étroites et en utilisant des modèles de test des interfaces qui intègrent une pro-activité des demandes futures et des migrations futures ».

En vis-à-vis des migrations silencieuses, du franchissement de barrières, les opérateurs régulent leur activité et mettent en œuvre des moyens pour résoudre les problèmes auxquels ils font face. Ils essaient de donner un sens, une signification à la situation (Karsenty & Quillaud, 2011) et mettent en œuvre des méthodes d'essai-erreur afin de mettre en exergue une solution adaptée au problème qu'ils rencontrent (Vanderhaegen & Caulier, 2011 ; Ouedraogo *et al.*, 2013 ; Vanderhaegen & Zieba, 2014).

Cette présentation synthétique des enjeux opérationnels de la résilience nous ont montré que, pour différentes raisons, l'ensemble des situations opérationnelles que connaît un système tout au long de sa vie ne peut être décrit par des scénarios en phase amont des projets. Les méthodes, que nous présentons maintenant, contribuent, pour leur part, à identifier les événements redoutés dans le cadre d'une compréhension supposée complète de la part du concepteur. Ces méthodes achoppent à rendre compte de l'ensemble des situations que connaît un système, en particulier les situations imprévisibles, sans précédent. En revanche, la résilience, quant à elle, offre la capacité d'improviser face à des situations imprévues, sans précédent, de conduire à vue, de mettre en œuvre une démarche par essai-erreur et d'apprendre les règles d'adaptation adéquates quand les perturbations sont en dehors du périmètre spécifié des mécanismes d'adaptation du système.

1.3. Définitions et concepts de la résilience

La résilience est un terme polysémique, qui, dans les détails, diffère d'un domaine à l'autre.

En écologie, la résilience est la capacité d'un écosystème ou d'une espèce à récupérer un fonctionnement et/ou un développement normal après avoir subi un traumatisme. L'écosystème forestier qui se restaure sur une motte castrale médiévale ne revient pas à l'état

initial, mais atteint un état d'équilibre significativement différent de l'écosystème forestier avoisinant (cf. Figure 1.3) (Closset-Kopp & Decocq, 2015).

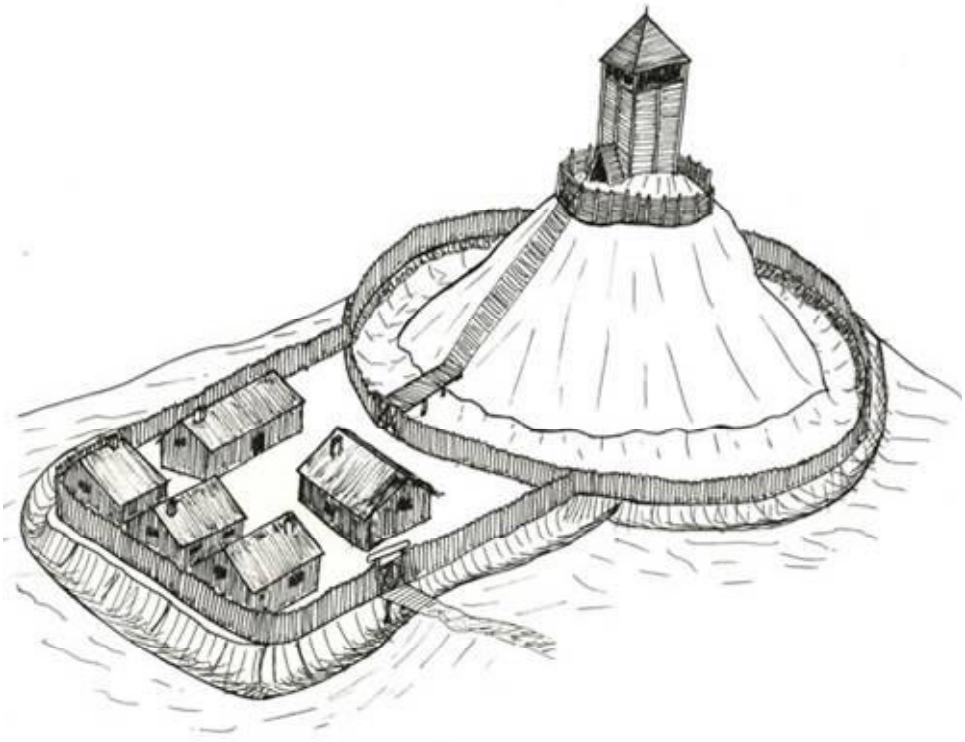

Figure 1.3.Reconstitution d'une motte castrale du Xe siècle et de sa basse-cour : un site urbain de l'époque médiévale © Silvère Decocq[5].

En économie, la résilience est la capacité à revenir sur la trajectoire de croissance après avoir encaissé un choc. En psychologie, « la résilience est la capacité d'une personne ou d'un groupe à bien se développer, à continuer à se projeter dans l'avenir, en dépit d'événements déstabilisants, de conditions de vie difficiles, de traumatismes parfois sévères » (Colas & Sarron, 2009).

Si nous analysons les définitions précédentes, nous voyons que la résilience se différencie de la notion de robustesse en ce sens que la robustesse caractérise l'aptitude du système à résister à un ensemble prévisible (au sens où on peut le caractériser qualitativement voire quantitativement, même s'il reste une part évidente de non-déterminisme) de perturbations d'ampleur *a priori* modestes, alors que la résilience considère plutôt un cas où la perturbation est importante et imprévisible. Par ailleurs, les performances attendues dans les deux cas ne sont pas les mêmes. Faire preuve de robustesse, c'est pouvoir maintenir le niveau de performance alors que les conditions exogènes ont un peu changé. Etre résilient, c'est « rebondir pour retrouver son équilibre », c'est la poursuite de la viabilité, au mépris éventuel des performances (Luzeaux, 2011).

En synthèse, la résilience caractérise la propriété de « faire face » dans l'adversité.

[5] Source : Des vestiges médiévaux à l'origine de véritables îlots de biodiversité au sein des forêts actuelles (http://www.cnrs.fr/inee/communication/breves/b105.html)

1.3.1. La sûreté de fonctionnement et la sécurité d'un système

Tandis que la communauté d'ingénierie système définit la norme (ISO, 2008) comme la norme de référence de la discipline autour de laquelle s'organisent les autres normes (EIA 632, IEEE 1220 …), que nous précisons dans la section 2.3 intitulé « Processus d'ingénierie », la communauté de sûreté de fonctionnement élabore sa propre norme de référence consacrée à l'ingénierie de la sûreté de fonctionnement des systèmes (EN, 2010).

Cette norme (EN, 2010) définit la sûreté de fonctionnement est comme « la capacité d'un système à fonctionner de manière à satisfaire aux objectifs spécifiques ainsi qu'aux conditions données. … La sûreté de fonctionnement d'un système implique que l'on puisse compter sur lui et qu'il soit capable d'exécuter sur demande le service souhaité afin de satisfaire aux besoins de l'utilisateur ». Cette norme définit le système comme étant « un ensemble d'éléments interdépendants considérés dans leur totalité et distinctement d'autres éléments, dans le contexte d'un objectif défini ». Les principaux attributs de la sûreté de fonctionnement d'un système sont la Fiabilité, la Maintenabilité, la Disponibilité et la Sécurité (EN, 2010), ces quatre disciplines sont regroupées sous l'acronyme FMDS. Cette norme traite la sûreté de fonctionnement principalement en termes de défaillance des composants matériels et logiciels. L'élément humain est appréhendé comme la source d'erreurs humaines. En effet, la norme mentionne que « la plupart des incidents industriels signalés et les principaux accidents étudiés sont dus à des erreurs humaines qui constituent la cause principale du dysfonctionnement d'un système ou de l'interruption d'un service d'aptitude à la fonction ». A ce titre, il est mentionné que « l'ergonomie soit intégrée dans les systèmes conçus ou exploités par des individus afin de réduire au minima le risque de défaillances critiques, la perte de biens, les atteintes à la sécurité ou les menaces pour la sécurité ». Nous traitons de façon plus détaillée la notion d'erreur humaine dans la section 1.3.2 « La fiabilité humaine, les facteurs de performance et les facteurs de contexte ».

Pour la réalisation des critères de la sûreté de fonctionnement, cette norme (EN, 2010) mentionne que ces critères reflètent :

- « une parfaite compréhension des objectifs d'aptitude à la fonction[6] ;
- une parfaite compréhension des conditions d'exploitation ;
- l'application effective des principes de la sûreté de fonctionnement dans l'infrastructure opérationnelle ;
- les conditions d'utilisation ;
- l'application de processus appropriés pour la réalisation du système ;
- l'utilisation des connaissances et de l'expérience acquises pour une introduction rentable de service fonctionnel ».

Ces critères sont basés sur le postulat que l'environnement est immuable tout au long du cycle de vie du système et que les concepteurs peuvent en acquérir une parfaite compréhension. Un tel postulat n'est pas pertinent puisque, en particulier pour les systèmes complexes critiques à longue durée de vie, il n'est pas possible de connaître *a priori*, toutes les situations potentielles d'usage, toutes les évolutions de l'environnement auxquelles le système sera confronté tout au long de sa vie opérationnelle (Amalberti, 2009 ; AAE, 2013 ; Conversy *et al.*, 2014).

[6] La fonction est définie comme « une opération élémentaire effectuée par un système qui, combinée à d'autres fonctions élémentaires (fonctions du système), permet au système d'effectuer une tâche donnée » (EN, 2010).

En complément à la sûreté de fonctionnement et de façon plus ciblée, le document MIL-STD 882E (2012), intitulé sécurité du système (*System safety*), la Recommandations pour la mise en œuvre de la maîtrise des risques (BNAE, 2013) et le livre de Hardy (2010) traitent spécifiquement de la sécurité des systèmes. Le document MIL-STD 882E (2012), décrit le processus en huit éléments que sont :

- documenter l'approche de la sécurité du système ;
- identifier et documenter les dangers ;
- évaluer et documenter les risques ;
- identifier et documenter les mesures de réduction des risques ;
- réduire les risques ;
- vérifier, valider et documenter la réduction des risques ;
- accepter et documenter le risque résiduel ;
- gérer les risques tout au long du cycle de vie du système.

La documentation et l'évaluation des risques (MIL-STD, 2012) reposent sur la description de ces risques en termes de sévérité et de probabilité, décrits dans les deux tableaux ci-dessous.

Le Tableau 1.1 identifie quatre catégories de sévérité et précise, pour chacune d'elles, les conséquences de façon graduée et objectivement mesurable.

Description	Catégorie de sévérité	Sévérité
Catastrophique	1	Peut résulter en une ou plusieurs conséquences suivantes : un mort, l'inaptitude totale permanente d'au moins une personne, des impacts environnementaux significatifs et irréversibles ou une perte financière égale ou supérieure à 10 millions de dollars.
Critique	2	Peut résulter en une ou plusieurs conséquences suivantes : l'inaptitude partielle permanente, des blessures ou une maladie professionnelle résultant dans l'hospitalisation d'au moins trois personnes, des impacts environnementaux significatifs réversibles, ou une perte financière entre un million de dollars et 10 millions de dollars.
Marginal	3	Peut résulter en une ou plusieurs conséquences suivantes : des blessures ou une maladie professionnelle nécessitant pour plus de dix jours d'arrêt de travail, des impacts environnementaux modérés réversibles, ou une perte financière entre cent mille dollars et un millions de dollars.
Négligeable	4	Peut résulter en une ou plusieurs conséquences suivantes : des blessures ou une maladie professionnelle ne nécessitant pas plus de 10 jours d'arrêt de travail, des impacts environnementaux réduits, ou une perte financière inférieure à cent mille dollars.

Tableau 1.1. Catégories de sévérité (MIL-STD, 2012).

Le Tableau 1.2 comprend six niveaux de probabilité (MIL-STD, 2012), et les décrit, d'une part pour un item individuel spécifique, par exemple une machine-outil, une usine de produit chimique, et d'autre part pour un ensemble d'items formant une flotte ou identifiés dans un inventaire, par exemple une flotte d'automobiles, l'inventaire de produits phytosanitaires dans une exploitation agricole.

Description	Niveau	Item individuel spécifique	Flotte ou inventaire
Fréquent	A	Est susceptible d'apparaître souvent durant la vie d'un item.	Apparaît continuellement
Probable	B	Est susceptible d'apparaître plusieurs fois durant la vie d'un item.	Apparaît fréquemment
Occasionnel	C	Est susceptible d'apparaître quelques fois durant la vie d'un item.	Apparaît plusieurs fois
Isolé	D	Peu probable, mais peut apparaître durant la vie d'un item.	Peu probable, mais on peut envisager que cela advienne
Improbable	E	Si peu probable qu'on peut prendre la responsabilité de dire qu'une telle occurrence ne peut advenir durant la vie d'un item.	Peu probable, mais possible
Éliminé	F	Ne peut jamais apparaître. Ce niveau est utilisé quand les dangers potentiels sont identifiés et puis éliminés.	Ne peut jamais apparaître. Ce niveau est utilisé quand les dangers potentiels sont identifiés et puis éliminés.

Tableau 1.2. Niveaux de probabilité (MIL-STD, 2012).

Le produit du croisement de la sévérité et de la probabilité est la criticité (MIL-STD, 2012) décrit dans une matrice d'évaluation des risques (cf. Tableau 1.3).

Sévérité / Probabilité	Catastrophique (1)	Critique (2)	Marginal (3)	Négligeable (4)
Fréquent (A)	Élevé	Élevé	Sérieux	Moyen
Probable (B)	Élevé	Élevé	Sérieux	Moyen
Occasionnel (C)	Élevé	Sérieux	Moyen	Faible
Isolé (D)	Sérieux	Moyen	Moyen	Faible
Improbable (E)	Moyen	Moyen	Moyen	Faible
Éliminé (F)	Éliminé			

Tableau 1.3. Matrice d'évaluation des risques (MIL-STD, 2012).

Le niveau de criticité des risques (MIL-STD, 2012) est ainsi évalué comme étant :

- élevé ;
- sérieux ;
- moyen ;
- faible ;
- et éliminé.

Outre les exigences générales à la sécurité d'un système, le document (MIL-STD, 2012) définit les tâches à effectuer :

- la gestion des risques ;

- l'analyse des risques ;
- l'évaluation des risques ;
- la vérification de la sécurité.

Ce document (MIL-STD, 2012) mentionne les actions pour identifier et documenter les mesures d'atténuation des risques. Une de ces actions consiste à inclure des systèmes de détection et d'alarme afin d'alerter le personnel de la présence d'une condition dangereuse ou de l'occurrence d'un évènement dangereux. Ce document précise aussi les actions pour gérer les risques durant le cycle de vie du système. Ces actions, menées après le déploiement du système, mentionnent que le bureau de programme utilise le processus de sécurité des systèmes pour identifier les dangers et maintenir le système de détection des dangers pendant le cycle de vie du système. Ceci vise à prendre en compte tous changements concernant, les missions réalisées, les données de santé du système, les données d'accident, les utilisateurs, le matériel et les logiciels, les interfaces. Si un nouveau danger est découvert ou si un danger connu présente un niveau de risque supérieur à celui évalué précédemment, le risque nouveau ou révisé doit être géré.

Ce document (MIL-STD, 2012) s'inscrit dans les phases amont des projets, dans la relation entre le client et le fournisseur. Quoiqu'il énonce que la sécurité d'un système s'applique à l'ensemble du cycle de vie de ce système, et qu'une tâche consiste à traquer les dangers affectant le système, il ne donne aucune indication ou aucune référence à un document décrivant comment surveiller le système lorsqu'il est en opération, afin de détecter de nouveaux dangers.

Dans le domaine ferroviaire, à l'instar d'autres domaines, la norme sur la sûreté de fonctionnement (NF, 2000) décline la sûreté de fonctionnement à toutes les étapes du cycle de vie du système. En particulier, elle prend en compte la « surveillance des performances du système » en formulant des exigences de collecte des statistiques relatives aux performances d'exploitation et à la FMDS. L'acquisition, l'analyse et l'évaluation des données relatives aux performances et la FMDS permettent de vérifier la pérennité de la validité des hypothèses de sécurité. Cela peut entraîner de nouvelles procédures d'exploitation et de maintenance, ainsi que des modifications du soutien logistique du système (NF, 2000). Ces démarches sont adaptées pour les risques qui sont identifiables et identifiés *a priori* et pour lesquels il est possible d'estimer la sévérité, la probabilité et la criticité.

L'analyse probabiliste peut être complétée par la prise en compte de l'incertitude (Fallet-Fidry *et al.*, 2012), pour autant, ces méthodes ne prennent pas en compte les situations imprévisibles qui ne peuvent pas être envisagées en phase amont des projets. Il en est de même des méthodes qui proposent des dispositifs d'apprentissage automatique (Aubry *et al.*, 2012 ; Hartert *et al.*, 2012 ; He *et al.*, 2012).

Dans son analyse de la sécurité d'un système, Hardy (2010) différencie la réalité des situations telle qu'envisagées et la réalité des situations vécues par le système. Cette différenciation ouvre la voie à l'analyse de l'écart entre la situation opérationnelle de référence et la situation opérationnelle réelle.

De son côté, Hollnagel (2006) montre que la sûreté se caractérise par l'absence d'effets négatifs. Dans cette perspective, suite à un accident, c'est-à-dire quand il y a des effets négatifs, la démarche consiste à élaborer l'arbre des causes après un accident pour comprendre l'origine de l'accident. Cet arbre des causes permet d'identifier les dysfonctionnements et le non-respect des procédures qui contribuent à la génération de l'accident. Une relation de causalité est tissée entre ces dysfonctionnements et l'accident. En revanche, la démarche ne préconise pas d'analyser les conséquences de ces

dysfonctionnements, conséquences qui peuvent être aussi bien positives (situations non accidentelles) que négatives (situations accidentelles). Hollnagel (2009) appelle ces situations non accidentelles « matière noire », par analogie avec la matière noire en astrophysique. De ce point de vue, les origines d'une exécution dans les situations non accidentelles ne sont pas analysées, et restent donc inconnues. On recherche les causes des échecs, mais pas les causes des réussites.

Sans traiter sur le fond des situations imprévues, sans précédent, les documents de référence ouvrent une voie en proposant de surveiller les performances du système, de recueillir et d'analyser des données relatives à l'exploitation pour vérifier la validité de la définition du système. Par ailleurs, cette section met en évidence la nécessité d'élargir la perspective de la sécurité pour prendre en compte les situations déviantes non accidentelles qui ne sont pas tracées aujourd'hui. Nous poursuivons cet état de l'art en abordant les notions de fiabilité humaine, d'erreurs humaines, qui sont mentionnées comme cause majeure de défaillance dans les documents de référence en sûreté de fonctionnement.

1.3.2. La fiabilité humaine, les facteurs de performance et les facteurs de contexte

De très nombreux articles et ouvrages ont été consacrés à la fiabilité humaine et à l'erreur humaine, à leur définition, aux méthodes pour les appréhender, aux moyens pour les mesurer (Swain & Guttmann, 1983 ; Leplat, 1985 ; Kirwan, 1992a ; Kirwan, 1992b ; Kirwan, 1998a ; Kirwan, 1998b ; Vanderhaegen, 2003 ; SAIC, 2005 ; Vanderhaegen *et al.*, 2011).

Pour Swain et Guttmann (1983), la fiabilité humaine est la capacité d'un opérateur humain à réaliser une tâche avec succès dans un temps donné, et à ne pas exécuter des tâches supplémentaires nuisibles au bon fonctionnement du système homme-machine. Dans la même perspective, ces auteurs définissent l'erreur humaine comme étant la capacité d'un opérateur humain de ne pas exécuter les tâches prescrites correctement ou d'exécuter des tâches supplémentaires nuisibles au bon fonctionnement du système homme machine. Pour ces auteurs, il y a erreur dès lors qu'il y a un écart par rapport à la tâche prescrite.

De nombreux travaux concernent les erreurs humaines en général (Leplat, 1985), ou les erreurs dans un contexte précis, par exemple dans le contexte des exigences d'utilisabilité et la formulation du critère d'ergonomie « Gestion des erreurs » comprenant la « Protection contre les erreurs », la « Qualité des messages d'erreur » et la « Correction des erreurs » (Bastien & Scapin, 1993).

Reason (1997) propose une définition alternative de l'erreur humaine. Il la définit comme un écart à l'intention. Cet écart à l'intention est dû à l'incapacité des actions planifiées à atteindre l'objectif attendu, dans le cadre d'une activité régulière sans l'intervention d'événement non prévue. L'erreur est inhérente à l'activité humaine. Dans leur activité, les opérateurs mettent en place des moyens de récupération des erreurs. Cette récupération est d'autant plus importante que les opérateurs sont experts. À ce titre, les erreurs contribuent à la régulation de l'activité, à l'apprentissage, et à la construction de la capacité d'adaptation, et donc de l'expérience, de l'expertise des opérateurs.

Reason (1997) différencie plusieurs types d'actions erronées :

- les ratés (*slips*) et les lapsus (*lapses*) qui sont des erreurs de routine. Elles correspondent à un dysfonctionnement lors de l'exécution de l'action (activités basées sur des automatismes, tâches routinières) ;

- les méprises (*mistakes*) qui sont des erreurs de connaissance. Ce sont des dysfonctionnements lors de la planification de l'action, une simplification excessive, des biais et heuristiques inadéquats (biais de confirmation …).

Par ailleurs, Reason (1997) distingue les erreurs et les violations. Ces dernières sont des transgressions volontaires de règles ou de procédures imposées, desquelles il exclut le sabotage malveillant (intention délibérée de nuire). Il différencie ces violations en trois types:

- les violations routinières consistent à couper au plus court pour réduire la charge de travail ;
- les violations d'optimisation, visant à optimiser les objectifs non fonctionnels, par exemple pour obtenir des sensations fortes, des frissons, pour montrer sa témérité à ses pairs ;
- les violations nécessaires, induites par les situations particulières d'activités, le non-respect des procédures est essentiel pour que la tâche soit réalisée.

Notre contribution s'inscrit dans le cadre des violations nécessaires, telles que les définit Reason, pour réintroduire la contrôlabilité du système, ainsi que le propose Amalberti. Nous détaillons cette notion de violation dans la section 1.2.3 « Les franchissements de barrières, les violations des règles de sécurité et les migrations spontanées ».

Plusieurs techniques de quantification considèrent actuellement les influences des facteurs humains sur la performance du système pour calculer la probabilité d'erreur humaine. Ces influences, appelées facteurs de performance (PSF pour *performance shaping factors*), peuvent être liées au temps dont disposent les opérateurs pour comprendre, décider et agir, à la qualité des interfaces utilisateur, à leur niveau de formation, entre autres (Kirwan, 1992a). Il est extrêmement difficile et délicat d'attribuer l'origine d'un accident à une cause unique, qui serait une défaillance du matériel ou une erreur humaine. En effet, les enquêtes menées après des accidents (BEA-TT, 2009 ; NTSB, 2010 ; BST, 2013) montrent qu'il n'y a pas une cause unique mais un ensemble de causes dont les interactions, à un moment donné, dans un contexte donné, sont à l'origine de l'accident.

Le Tableau 1.4 montre la liste des facteurs de performance identifiés dans le domaine des systèmes critiques nucléaires (SAIC, 2005).

Dans la même perspective, Hollnagel (Belmonte *et al.*, 2008 ; Hollnagel *et al.*, 2006) caractérise onze facteurs de contexte qui peuvent avoir des effets positifs ou des effets négatifs sur les performances de l'activité, et, à ce titre, contribuent à la variabilité de ces performances. Ces onze facteurs de contexte sont : 1) la disponibilité des ressources, 2) l'entraînement et l'expérience du collectif de travail, de l'équipage, 3) la qualité des communications entre les opérateurs, 4) la qualité des interfaces opérateurs-machines, 5) l'accessibilité et la disponibilité des méthodes et des procédures, 6) les conditions de travail, 7) le nombre d'objectifs simultanés auxquels les opérateurs doivent répondre, 8) le temps disponible pour mener les activités, 9) le rythme circadien, 10) la qualité de collaboration en équipe, 11) la qualité et le support de l'organisation. Ces onze facteurs de contexte (cf. Tableau 1.5) sont définis dans le cadre du management de risques industriels.

PSF	Libellé des facteurs de performance
PSF01	Applicabilité et pertinence de l'entrainement, de l'expérience
PSF02	Pertinence des procédures et des objectifs
PSF03	Disponibilité et clarté des modes opératoires
PSF04	Temps disponible et temps requis pour réaliser complètement l'action menée, incluant la concurrence entre les activités
PSF05	Complexité du diagnostic et de la réponse requis, du besoin d'une séquence spécial et de la familiarité de la situation
PSF06	Charge de travail, pression temporelle et stress
PSF07	Dynamique de l'équipage, caractéristiques de l'équipage
PSF08	Dotation en personnel disponible
PSF09	Qualité ergonomique de l'interface humain-système
PSF10	Environnement dans lequel l'activité doit être réalisée
PSF11	Accessibilité et capacité des équipements à être opérés, manipulés
PSF12	Besoin d'outils spécifiques
PSF13	Communication et conditions par lesquels quelqu'un peut être facilement écouté
PSF14	Besoins d'aptitudes spéciales
PSF15	Prise en compte de déviations et de détournements réalistes de séquences d'actions

Tableau 1.4. Liste des facteurs de performance (SAIC, 2005).

FC	Libellé des facteurs de contexte
FC01	Disponibilité des ressources
FC02	Entraînement et expérience du collectif de travail
FC03	Qualité des communications entre les opérateurs
FC04	Qualité des interfaces opérateurs-machines
FC05	Accessibilité et disponibilité des méthodes et des procédures
FC06	Conditions de travail
FC07	Nombre d'objectifs simultanés auxquels les opérateurs doivent répondre
FC08	Temps disponible pour mener les activités
FC09	Rythme circadien
FC10	Qualité de collaboration en équipe
FC11	Qualité et support de l'organisation

Tableau 1.5. Liste des facteurs de contexte (Belmonte *et al.*, 2008).

Ces facteurs de contexte, facteurs de performance, sont les leviers sur lesquels agir pour améliorer la résilience du système. C'est maintenant la résilience que nous traitons dans la section suivante.

1.3.3. La résilience des systèmes sociotechniques

Les méthodes de la sûreté de fonctionnement et de la sécurité permettent d'identifier toutes les situations prévisibles, et de proposer une solution sûre, en termes d'équipement, de procédure, de formation. Mais toutes les situations que rencontrent les opérateurs tout au long des missions opérationnelles ne peuvent être exhaustivement prévues et prévisibles. Il reste des situations imprévues et le traitement de ces situations imprévues est la norme de l'activité de ces opérateurs, « l'imprévu est le lot quotidien des aviateurs, pas l'exception », « l'imprévu est la norme » (AEE, 2013). Ces situations imprévues sont en dehors du périmètre des méthodes de la sûreté de fonctionnement et de la sécurité. N'étant ni prévues, ni prévisibles, il n'y a aucune procédure rédigée pour expliquer aux opérateurs comment faire face à ces situations imprévues. Le traitement de ces situations imprévues nécessite généralement beaucoup de ressources cognitives et génère beaucoup de stress, mettant à mal les capacités des opérateurs pour répondre à ces situations imprévues de la meilleure façon.

La résilience, quant à elle, concerne la capacité d'un système sociotechnique à s'ajuster face à des événements perturbateurs, à s'adapter face à des situations sans précédent. En cela, elle est complémentaire des démarches de sécurité traitant des risques prévisibles et anticipés. En effet, la diversité des situations est extrêmement importante et il est impossible d'en faire une analyse exhaustive *a priori* lors de la conception, pour un système dont la vie opérationnelle peut durer plus de 50 ans (Ruault *et al.*, 2014b).

De nombreux travaux ont été menés, ces dix dernières années, consacrés à la résilience des systèmes sociotechniques (Hollnagel *et al.*, 2006 ; Jackson, 2009 ; Jackson & Ferris, 2013). Dans l'ouvrage « Resilience engineering » (Hollnagel *et al.*, 2006), les auteurs proposent des définitions de la résilience. Pour Hollnagel (2006) « la résilience est la capacité d'un système ou d'une organisation à réagir et à récupérer après une perturbation, avec un minimum d'effet sur la stabilité dynamique du système ». Pariès (2006) précise que « la résilience est une propriété émergente des systèmes complexes ». Dekker (2006) écrit : « la sûreté et les risques ne peuvent pas être prédits ou modélisés sur la base des composants et de leurs interactions ». D'après Hollnagel et Woods (2006), « on peut mesurer seulement le potentiel de résilience, mais non la résilience elle-même ». Woods (2006) écrit « la résilience n'est pas seulement la capacité d'adaptation d'un système dans l'enveloppe pour laquelle il a été conçu, mais elle regarde aussi l'extérieur de cette enveloppe avec les événements perturbateurs qu'elle peut comporter ». Woljter (2008) définit la résilience comme « la capacité à reconnaître et s'adapter pour maîtriser une perturbation qui n'a pas pu être anticipée, qui interroge le modèle de compétence et requiert un changement dans les processus, la stratégie, la coordination…». Luzeaux (2011) caractérise la résilience par une « gestion à la frontière du domaine d'application du système ». La résilience est démontrée lorsqu'un système sociotechnique est capable de « gérer l'incertain, l'imprévisible, l'imprévu, l'accident, la transition entre le plus ou moins catastrophique en évitant la sanction de la catastrophe, le retour à un fonctionnement plus nominal ». Il s'agit non pas d'une caractéristique intrinsèque, mais d'un processus que nous préciserons plus loin. Ici, le terme de résilience concerne les systèmes sociotechniques comprenant traditionnellement trois niveaux (Belmonte *et al.*, 2008) : le niveau du système technique, le niveau humain et le niveau organisationnel (un équipage, un collectif de travail, par exemple).

Woods (Woods, 2006 ; Woods & Cook, 2006) définit les caractéristiques suivantes de la résilience :

- la réserve (*buffering capacity*), c'est-à-dire la taille ou le type de perturbation que le système peut absorber et accommoder sans qu'il n'y ait une rupture dans les performances ou la structure du système ;

- la flexibilité, c'est-à-dire la capacité du système à se restructurer en réponse à des perturbations de l'environnement ;
- la marge, c'est-à-dire le niveau de fonctionnement courant du système, coordonné ou précaire, par rapport à son domaine de définition ;
- la tolérance, c'est-à-dire la façon dont le système fonctionne aux limites de son domaine de définition, dégradation régulière des performances ou rupture brutale quand les perturbations de l'environnement excèdent ses capacités d'adaptation, par exemple les ailes supercritiques[7] (Amalberti, 2009) ;
- les interactions multi-niveaux, c'est-à-dire la sensibilité du système de niveau donné face à des perturbations et des interactions avec des composants de niveaux inférieurs.

Nous retenons les concepts de flexibilité, de marge et de tolérance, qui traitent du fonctionnement aux limites ou en dehors de son domaine de définition. C'est dans ce contexte que nous nous trouvons dans le cas situations imprévisibles, sans précédent.

De son côté, Westurm (2006) différencie trois types de menace, et précise les réponses possibles, appropriées pour ces différents types :

- face à une menace régulière, prévisible, il est possible de formuler une réponse standard et d'élaborer un algorithme approprié ;
- dans le contexte d'une menace irrégulière, si le problème est compréhensible, la faible probabilité d'occurrence des événements et le nombre de cas possibles rendent impossible une préparation à toutes les menaces irrégulières. L'organisation doit être capable d'improviser et de se réorganiser pour répondre à ce type de menace. Par exemple, un gymnase est transformé en hôpital de campagne, les véhicules banalisés sont utilisés pour servir d'ambulance en situation de crise grave ;
- le troisième type de menace, dans le cas d'événements sans précédent, imprévisibles, requiert encore plus de capacité d'improvisation que dans le second cas. Cela requiert aussi la capacité de changer rapidement de cadre de référence mental et de sérendipité.

Luzeaux (2011) propose une typologie des événements auxquels un système doit faire face que nous rapprochons des types de menace de Westurm (2006). Ces événements sont :

- « les événements habituels et prévisibles, par exemple les tremblements de terre dans des régions comme la Californie ou le Japon, des explosions dans une usine chimique ;
- les événements rares ou occasionnels, qui ne peuvent pas tous être décrits ou prévus ;
- les événements *a priori* imprévisibles, nécessitant bien plus d'improvisation que précédemment et un changement radical d'approche mental ».

De ces types de menace et d'événements, nous retenons le besoin d'improviser, de se réorganiser, de changer de point de vue, pour faire face à des situations avec un faible niveau de probabilité d'occurrence, pour lesquelles les routines ne sont pas adaptées, ainsi qu'à des événements sans précédent.

Luzeaux (2011) caractérise la résilience comme « une gestion dynamique à la frontière du domaine d'application. Les défis liés à la résilience incluent la gestion de l'incertain, du non-planifié, des accidents, en évitant une catastrophe et permettant le retour à un fonctionnement opérationnel plus normal ». Luzeaux (2011) écrit « qu'améliorer la résilience d'un grand

[7] Les ailes supercritiques sont des ailes sophistiquées issues d'évolutions technologiques. Leur performance dans le domaine de vol prévu est parfaite. Mais elles ne supportent pas d'être utilisées en dehors du domaine de vol prévu et perdent immédiatement toute leur contrôlabilité hors du domaine (Amalberti, 2009).

système complexe implique de pouvoir disposer le moment venu d'une flexibilité au niveau de l'organisation responsable de l'exploitation du système… Trop figer ou verrouiller permet d'éviter les erreurs de fonctionnement mais diminue d'autant la part de proactivité, d'anticipation, d'improvisation, qui peut justement conférer au système sa propriété de résilience ». Pour cela, le système doit avoir une plus grande capacité à évaluer où il est par rapport à la zone de danger, par le biais d'un processus dynamique de « navigation à vue ». Le système doit être conçu « pour l'incertain ». Il faut donc définir l'enveloppe d'exécution exigée, souhaitable, voire acceptable, et d'exiger que le système reconnaisse les situations où il est susceptible de sortir de cette enveloppe. « Vue ainsi, la résilience s'obtient via la capacité à surveiller les conditions aux limites de l'enveloppe d'exécution, au sens de déterminer leur valeurs ainsi que l'écart courant par rapport à la frontière, et à adapter la commande en cours du système aux évolutions éventuelles de cette enveloppe. Les capacités requises vont donc être la capacité du système d'absorber des changements sans remettre en cause son exécution et sa structure ; la flexibilité de l'architecture, et en particulier la capacité du système de modifier une partie de sa structure si nécessaire ; le contrôle des marges et des tolérances, donc une capacité à évaluer sa propre dynamique, en vue de l'exploiter au voisinage de la frontière ».

Il est nécessaire d'élaborer des modes de régulation permettant au système de continuer de fonctionner dans ces différentes situations et en fonctions des différentes perturbations (Luzeaux, 2011). La résilience comprend aussi la détection de l'atteinte des limites des capacités d'adaptation. Elle concerne donc ce qui ne peut pas être anticipé (Luzeaux, 2011).

Pour qu'un système soit résilient, il faut (Luzeaux, 2011) :

- « fournir un point de vue indépendant pouvant remettre en cause des modes d'organisation courants ; cela permet de s'affranchir de certaines contraintes opérationnelles et de luttes de pouvoir ;
- avoir des informations sur l'état d'opération courant et les évolutions de cet état, notamment les différences par rapport au fonctionnement nominal prévu ;
- avoir une connaissance des marges de manœuvre et des points faibles de l'organisation et des éventuels décalages entre les manières d'opérer prescrites et ce qui est en fait réalisé : l'objectif n'est pas nécessairement de supprimer ces décalages mais d'exploiter la marge de manœuvre qu'ils sont susceptibles d'engendrer ».

L'objectif est de qualifier et quantifier la dérive du système vers l'état d'échec avant qu'une panne majeure ne survienne.

Galara (Galara, 2011) soulève les mêmes préoccupations dans le domaine de la conduite d'installations nucléaires. De mauvais choix en conception peuvent conduire les opérateurs à « percevoir et interpréter de façon erronée la situation de l'installation, être en surcharge cognitive face à une situation non vécue et faire de mauvais compromis entre sûreté et performances ». Galara montre que l'acceptabilité de l'erreur humaine « consisterait à surveiller que le système technique évolue dans des conditions explicites de fonctionnement normal, à surveiller les excursions de fonctionnement du système technique qui se rapprochent des exigences explicites de conception et réglementaires à satisfaire, à alerter les opérateurs de ces excursions et à proposer des stratégies de conduite pour revenir au fonctionnement nominal » pour éviter les accidents. Ces différentes situations amènent à dépasser la démarche traditionnelle de sûreté de fonctionnement menée *a priori*, sur des probabilités de risques, des conséquences et des dispositifs de sécurité (dont les barrières) pour empêcher les accidents afin de mettre en œuvre une démarche dynamique tenant compte des situations réellement rencontrées.

Dans la même perspective, l'analyse de l'accident du AF 447, Rio-Paris, montre que les pilotes n'ont pas compris la situation de décrochage dans laquelle ils étaient dans la mesure où les informations présentées sur l'IHM étaient incohérentes, ne leur permettant pas d'élaborer une représentation mentale, un modèle conceptuel, de l'avion en situation (Conversy *et al.*, 2014). Ainsi, le rapport du BEA (Bureau d'Enquêtes et d'Analyses), mentionne « en absence d'indication de vitesse fiable, la compréhension de la physique globale du vol à haute altitude par une approche synthétique des bilans énergétiques, équilibres de forces, plafonds de sustentation et propulsion, aurait pu considérablement aider les pilotes à anticiper la dégradation rapide de la situation et prendre à temps la mesure corrective adéquate : la mise en descente […] » (Conversy *et al.*, 2014).

Dans la mesure où toutes les situations ne peuvent pas être envisagées, que les opérateurs humains peuvent être face à des situations sans précédent, imprévisibles, que les dispositifs de sécurité sont inopérants face à ces situations, les opérateurs doivent pouvoir naviguer à vue et disposer des moyens pour faire face à l'adversité.

En résumé, la résilience concerne la capacité d'un système sociotechnique à s'ajuster face à des événements perturbateurs, à s'y adapter et à apprendre les règles d'adaptation adéquates, quand les perturbations sont en dehors du périmètre spécifié des mécanismes d'adaptation du système, c'est-à-dire des menaces irrégulières et des menaces sans précédent. En outre, la résilience comprend aussi la détection de l'atteinte des limites des capacités d'adaptation, en fonction de la configuration du système sociotechnique. La résilience concerne donc ce qui ne peut pas être anticipé (Luzeaux, 2011).

Les travaux consacrés à la résilience montrent les enjeux et les conditions de la résilience, mais n'apportent pas d'éléments pour concevoir un système afin qu'il soit résilient face à des situations imprévisibles, sans précédent. Ce sont des éléments de conception que nous proposons dans le cadre de ce mémoire. Nous allons regarder quels sont les principaux points de la résilience pour faire évoluer les concepts de l'ingénierie système afin de prendre en compte la résilience des systèmes sociotechniques.

1.3.4. Introduction aux quatre fonctions de la résilience

Parmi l'ensemble des travaux concernant la résilience (Hollnagel *et al.*, 2006 ; Jackson, 2009 ; Jackson & Ferris, 2013), nous nous appuyons sur ceux de Luzeaux (Luzeaux, 2011), en particulier sa définition des quatre fonctions de la résilience.

Ces quatre fonctions sont respectivement (Luzeaux, 2011) :

- éviter l'accident, qui repose sur la capacité d'anticipation ;
- résister face à l'accident, qui se traduit par une capacité d'absorption et de réduction des dommages ;
- s'adapter après un accident, qui se traduit par la capacité à évoluer face à des situations non envisagées et à se reconfigurer en conséquence ;
- recouvrer, qui consiste à restaurer un état opérationnel stable, au minimum dans une position de survie, voire avec des capacités et des performances opérationnelles réduites.

La résilience est le processus dynamique qui permet à l'équipage de comprendre la situation actuelle, d'apprendre et de développer des comportements adéquats pour prendre en compte les adversités de l'environnement et s'adapter aussi bien que possible. C'est la capacité d'un système sociotechnique pour continuer à accomplir sa mission opérationnelle malgré les

conditions difficiles, des contraintes sérieuses ou des événements imprévisibles, et éviter de graves conséquences.

Cette capacité d'ajustement est basée sur le processus dynamique « du pilotage à vue ». Le système doit avoir une grande capacité pour évaluer sa position par rapport à la zone dangereuse (Luzeaux, 2011). Le système doit être conçu pour faire face à l'incertitude. Il est nécessaire de spécifier le domaine de définition sûr, d'évaluer l'écart de la situation réelle par rapport à ce domaine de définition sûr, de qualifier et de quantifier la dérive du système vers une zone de danger avant qu'un accident majeur n'arrive. Dans de nombreux cas, le système a été conçu pour être sûr dans des conditions indiquées, mais il n'y a aucun moyen pour contrôler le système quand il fonctionne dans des conditions non spécifiées et réévaluer le risque réel. Dans de telles situations, la sécurité est ni évaluée, ni contrôlée.

La sûreté de fonctionnement, en particulier, la sécurité du système, permet de définir les risques probables que peut courir le système et caractérise la criticité en termes de probabilité et de conséquences d'événements redoutés. Cette analyse est réalisée sur un ensemble d'événements redoutés prévus ou prévisibles. En revanche, la sécurité achoppe à prendre en compte les situations imprévues, sans précédent, que peut rencontrer le système, en particulier lorsqu'il est amené à fonctionner hors de son domaine d'emploi.

La résilience du système, quant à elle, est la capacité du système à surveiller sa dynamique, de reconnaître les situations où il est susceptible de sortir de son domaine d'emploi, la capacité des opérateurs de conduire à vue et d'éviter un accident. Cela nécessite que les opérateurs puissent comprendre la dynamique du système, sa proximité par rapport à une zone de danger.

1.4. Comprendre la situation pour éviter l'accident

Dans la section 1.3 intitulée « Définitions et concepts de la résilience », nous avons pu constater que dans les situations imprévues, sans précédent, les opérateurs doivent pouvoir conduire à vue, mettre en œuvre des techniques de essai-erreur et, pour cela comprendre la dynamique du système afin d'éviter un accident (fonction « éviter » de la résilience). C'est dans ce contexte de compréhension de la dynamique d'un système que les travaux sur la conscience de la situation ont été menés. Nous montrons ce que sont les modèles de conscience de la situation, comment un ensemble d'opérateurs peuvent partager un cadre d'interprétation commun et comment se construit une conscience partagée de la situation au sein d'une équipe.

1.4.1. Modèles de conscience de la situation (*situation awareness*)

La conscience de la situation, *situation awareness* en anglais, peut être définie comme étant la représentation, la connaissance qu'un opérateur a de l'état d'un système et de l'état de l'environnement. Par extension, la conscience partagée de la situation, *shared situation awareness* en anglais, peut être définie comme étant la représentation collective qu'a un équipage de l'état du système et de son environnement, ou comme étant une compréhension partagée de cet état du système et de son environnement, par l'équipage.

Cette définition dérivée d'Endsley (1995a, 1995b) a été reprise et enrichie selon différentes approches que présente et synthétise Chalandon (2013). Il différencie quatre approches :

- l'approche linéaire, issue directement des travaux d'Endsley ;
- l'approche décisionnelle ;

- l'approche centrée sur la régulation ;
- l'approche néo-écologique.

Dans le contexte de l'approche linéaire (Endsley, 1995b), la conscience de la situation est appréhendée d'un point de vue normatif. Cette approche fait l'hypothèse qu'il y ait une conscience de la situation idéale ou maximale qui pourrait être définie *a priori* et par rapport à laquelle la conscience de la situation d'un opérateur pourrait être confrontée. Un écart par rapport à cette conscience de la situation maximale est alors appréhendé comme un manque de conscience de la situation de la part de l'opérateur, potentiellement source d'accident (Endsley, 1995a). Par ailleurs, la conscience de la situation est différenciée en trois niveaux (Endsley, 1995b), le niveau 1, de la perception, le niveau 2 de la compréhension et le niveau 3 de la projection. Le niveau 1, de la perception, concerne la surveillance du système et de son environnement pour y déterminer les statuts de leurs caractéristiques et leurs dynamiques. Le niveau 2, de la compréhension, consiste à synthétiser les éléments issus de la perception pour les interpréter et évaluer la situation. Le troisième niveau, de la projection, consiste à extrapoler, à partir des caractéristiques et dynamiques évaluées, l'état et la dynamique futurs du système et de son environnement, et d'organiser les actions à réaliser au regard de cet état et de cette dynamique futurs.

L'approche décisionnelle de la conscience de la situation se caractérise par un construit interne finalisé, une représentation mentale, qui n'interviendrait dans le cours d'actions qu'en cas de résistance du réel. Il s'agit d'un modèle descriptif de la façon dont les opérateurs expérimentés identifient et évaluent les situations, prennent des décisions et réalisent des actions dans des environnements incertains. Cette approche met en évidence l'impossibilité d'une analyse exhaustive de la situation sous contrainte temporelle. Cette impossibilité a pour conséquence que le critère d'optimalité doit être remplacé par le critère d'acceptabilité. Il s'agit de trouver une première option acceptable, pas nécessairement la meilleure option possible (Chalandon, 2013).

L'approche centrée sur la régulation définit la conscience de la situation comme étant une représentation fonctionnelle continuellement mise à jour, tendue entre l'adaptation immédiate et la définition de la tâche. Contrairement à l'approche décisionnelle, cette représentation n'est pas construite en réaction à l'occurrence d'un événement particulier, mais comme ajustement permanent d'une représentation en fonction de l'historique de la situation et des buts à atteindre. Une spécificité de cette approche, par rapport aux trois autres approches présentées jusqu'à maintenant, réside dans l'acceptation par l'opérateur de « ne pas comprendre la situation », au sens de compréhension maximale, exhaustive de la situation, car les ressources nécessaires à cette activité sont incompatibles avec la dynamique de la tâche. Par souci d'économie et d'opérativité, la régulation se traduit ici par le compromis cognitif que l'opérateur met en œuvre et contrôle par une activité métacognitive prenant en compte les exigences de la tâche, ses savoirs et savoir-faire et le niveau de risque accepté. Ce compromis cognitif est le niveau de compréhension minimal pour une efficacité maximale en termes d'objectifs d'action (Chalandon, 2013).

Enfin, pour l'approche néo-écologique, la conscience de la situation peut être définie comme « une conscience adaptative dirigée vers l'externe » ou comme « la perception des affordances spatio-temporelles de l'environnement ». Sans nier l'autonomie de l'opérateur, cette approche est prescriptive dans la mesure où elle cherche à encadrer, à former, son comportement adaptatif. Elle vise donc à spécifier à l'opérateur un espace problème de la tâche au sein duquel les trajectoires comportementales improvisées respectent des contraintes de performance et/ou de sécurité (Chalandon, 2013).

L'approche décisionnelle de la conscience de la situation est incomplète. En effet, pour que l'opérateur puisse prendre une décision adaptée, appropriée, en cas de résistance du réel, il est nécessaire que l'opérateur maintienne une conscience de la situation la plus fiable et la plus pertinente possible, de la situation courante, de l'ensemble des événements qui ont concouru à cette situation courante. Une représentation mentale qui n'interviendrait qu'en cas de résistance du réel ne permet pas de comprendre la dynamique y compris son historique. L'accident du vol Rio-Paris AF 447 (Conversy *et al.*, 2014) montre que les pilotes ne comprenaient pas la situation. En particulier ils n'ont pas compris les séquences d'événements désactivant le pilote automatique, les informations erronées concernant la vitesse, l'erreur de jugement qu'entrainaient l'horizon artificiel et les oscillations de l'alarme STALL.

Il faut donc prendre en compte le caractère dynamique dans l'élaboration de la conscience de la situation.

1.4.2. Conscience de la situation dans des environnements dynamiques

Les travaux de Sarter & Woods (1991) concernent la conscience de la situation dans des environnements dynamiques des systèmes critiques. Ils montrent que des déviations mineures ou des défaillances, qui ne sont pas critiques par elles-mêmes, peuvent évoluer ou interagir au cours du temps pour devenir une menace majeure. Il est alors essentiel pour l'opérateur d'observer, de prendre en compte ces événements et de s'en rappeler. Pour cela, il doit élaborer un modèle dynamique du monde qui est continuellement mis à jour en fonction des événements qui adviennent (Sarter & Woods, 1991).

Ainsi, la conscience de la situation concerne un système ouvert en continuel changement, comprenant une large variété de dispositifs et d'agents qui interagissent et sont imprévisibles. Dans cette perspective, une rétroaction adéquate de l'état et du comportement du système est essentielle pour la conscience de la situation de l'opérateur. Dans cette perspective, dans le cas d'une projection de l'état et le comportement futurs du système qui soit inappropriée, l'opérateur est plus susceptible de négliger des événements imprévisibles, parce que l'opérateur dirige ses ressources attentionnelles de façon inadéquate (Sarter & Woods, 1991).

1.4.3. Conscience partagée de la situation (*shared situation awareness*)

Au-delà du niveau individuel, la conscience partagée de la situation relève d'une représentation collective ou d'une compréhension partagée qu'un équipage élabore de l'état du système et de son environnement (Salembier & Zouinar, 2004 ; Grosjean, 2005 ; Villaren, 2013).

Ce sujet est un des points traités dans les modules de formation CRM (*Crew Resources Management*) en faveur de la sécurité aéronautique (cf. Figure 1.4).

Villaren (2013) différencie plusieurs configurations de conscience partagée de la situation dans le contexte des systèmes collaboratifs, que ce soit la conscience de la situation au sein d'une équipe, la conscience de la situation distribuée. Les questions soulevées par ces différentes configurations concernent les liens entre les consciences de la situation des membres de l'équipe et la conscience de la situation au niveau de l'équipe. Ainsi, en ce qui concerne la conscience de la situation au sein d'une équipe, sont caractérisées, d'une part la conscience partagée de la situation, qui est l'intersection des consciences de la situation des membres, et d'autre part, la conscience de la situation globale de l'équipe, qui est l'union des consciences de la situation des membres de l'équipe. Pour ce qui relève de la conscience de la

situation distribuée, elle s'inscrit dans les travaux sur la cognition distribuée et « elle est constituée des connaissances activées pour une tâche spécifique dans un système donné » (Villaren, 2013). Ces différentes configurations s'inscrivent dans l'approche linéaire, dans la lignée des travaux d'Endsley (1995b). Elles en héritent les éléments d'analyse que nous avons identifiés ci-dessus, et en particulier les limites pour traiter de la conscience de la situation dans le contexte d'événements imprévisibles, sans précédent. De plus, la question relative à la possibilité d'élaborer et de maintenir une représentation collective au sein d'un groupe en prenant en compte la communication entre les membres de ce groupe (Sperber & Wilson, 1989 ; Sperber, 1996) n'est pas traitée.

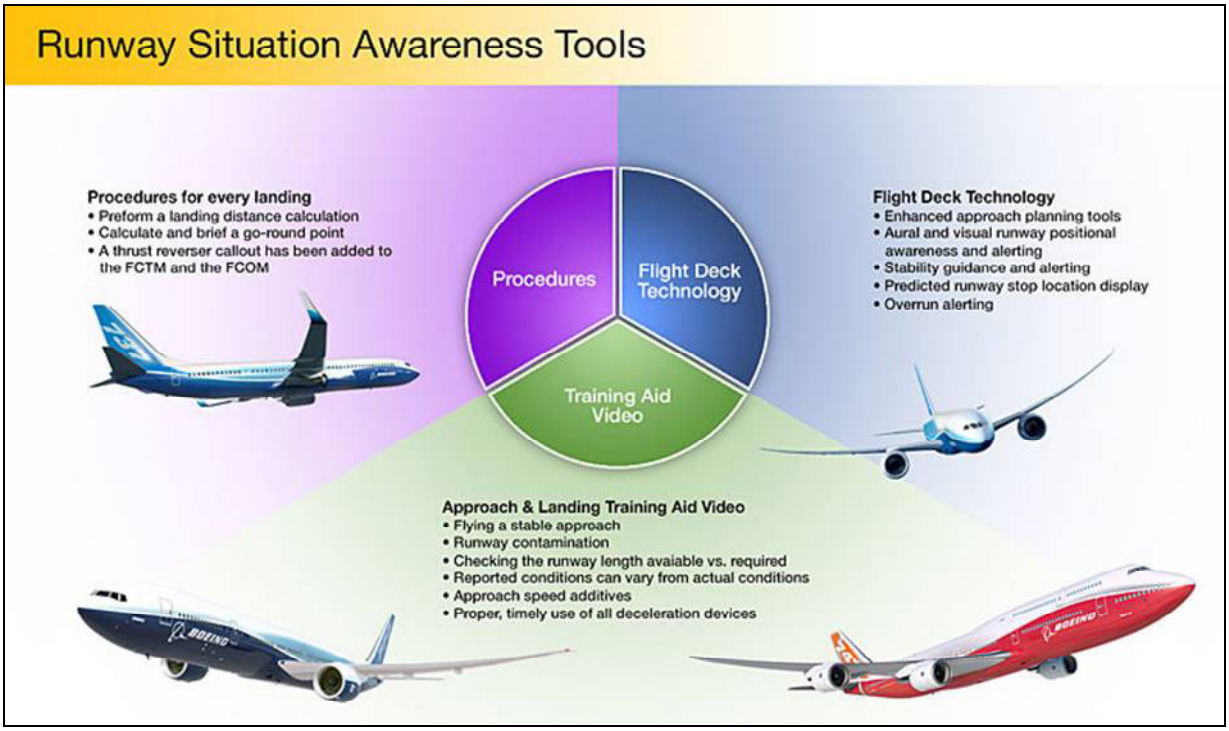

Figure 1.4. Formation relative à la conscience de la situation (sources Boeing©[8]).

La communication entre les membres de l'équipage est la clef de l'élaboration de cette conscience partagée de la situation. Au sein d'une équipe, les opérateurs peuvent communiquer par la parole (inter-audibilité) dès lors que l'ambiance est peu bruyante, qu'ils sont proches ou se rapprochent. Ils peuvent communiquer par des gestes, des postures, des mimiques (inter-visibilité), pour autant qu'ils puissent se voir, dépendant en cela de l'agencement spatial des différents postes. La communication est médiatisée par des moyens de communication lorsque les membres de l'équipe ne sont pas situés à un même endroit. Au-delà de la téléphonie, c'est-à-dire de la voix, les moyens de communication comportent maintenant d'autres média, dont le flux vidéo, les images, les données, etc. La communication peut être intrusive, un opérateur en interpelle un autre, ou bien ne pas être intrusive, quand un opérateur s'adresse à la cantonade ou rend manifeste à autrui quelque chose en le désignant du doigt et en attirant l'attention des autres sur cet élément. Ces échanges leur permettent de définir publiquement ce qu'il y a à voir et à entendre, et les catégories des éléments de la situation, de leur environnement. Ils définissent ainsi la situation et « un cadre d'interprétation

[8] Sources : http://www.boeing.com/commercial/safety/technology_saafer.html

commun qui n'existe pas en dehors de ce processus. C'est ce qui fonde l'intelligibilité mutuelle et le partage des significations » (Grosjean, 2005).

Plusieurs facteurs sont à prendre en compte pour obtenir cette capacité à se coordonner (Karsenty, 2008). Le premier est le contexte extérieur (moment et emplacement de l'interaction, orateur et auditeur, sujet de la discussion, forme et objectif de la communication). Deux opérateurs différents peuvent donner deux significations différentes à une même situation, selon leurs perceptions, attentions et compréhensions. La capacité pour partager de tels contextes dépend de la coprésence physique des différents opérateurs. Dans d'autres cas, s'ils sont localisés dans des endroits différents, ils peuvent communiquer en utilisant un media de télécommunication synchrone, tel qu'un téléphone, une téléconférence. Ils peuvent aussi communiquer de façon asynchrone, par l'intermédiaire de courrier, de fax, de courriel ou de tout autre genre de document. Dans le cas de la coprésence physique, chaque opérateur peut agir sur l'autre, s'assurer que le processus de compréhension mutuelle s'élabore correctement, en se basant sur la rétroaction, l'adaptation et les ajustements. Quand il n'y a pas de coprésence et que la rétroaction est réduite, voire absente, les risques d'incompréhension et de malentendu sont élevés. D'autres facteurs, tels l'obéissance à l'autorité, le contrôle social, l'influence affectent ce processus de communication. Les différents opérateurs peuvent appartenir à une même communauté qui élabore sa langue, ses croyances, ses valeurs, ou à différentes communautés, avec leurs croyances et valeurs respectives. Par ailleurs, chaque opérateur élabore des représentations des interlocuteurs avec lesquels il interagit. Si ces représentations sont fausses, erronées, ceci mène au malentendu entre les interlocuteurs. Ainsi, il est très important d'identifier des configurations de différents paramètres contribuant à la compréhension correcte, ou, en revanche, l'incompréhension, le malentendu, entre les opérateurs formant une équipe.

La compréhension commune dépend de trois paramètres principaux (Karsenty, 2008) :

- le niveau de partage de l'information contextuelle : plus l'information contextuelle est partagée, plus la compréhension mutuelle est facilité et fiable ;
- le niveau de disponibilité de l'information contextuelle partagée : plus l'information contextuelle partagée est disponible entre eux, plus la compréhension mutuelle est fiable ;
- le niveau de surveillance de la compréhension mutuelle : plus le niveau de surveillance est élevé, plus la compréhension mutuelle est fiable.

Karsenty (Karsenty, 2011) prouve que la confiance est la clef de voûte du travail d'équipe. Si la confiance aveugle est un facteur de risque important, l'absence de la confiance l'est tout autant. En effet, la « méfiance produirait de l'incertitude et ralentirait la décision et l'action » (Karsenty, 2011). Par effet de cascade, l'équipe perd la conscience partagée de la situation et peut moins détecter une situation pré-accidentelle et faire face à elle. La confiance est établie à partir de plusieurs facteurs : les relations d'affinité entre les interlocuteurs, les liens culturels, l'existence de cadres de référence partagés, l'acculturation et la socialisation.

1.4.4. Construction de la conscience partagée de la situation

Au-delà de la caractérisation statique de la conscience partagée de la situation, se pose la question du processus de construction de la conscience de la situation au sein d'une équipe. L'étude de Grosjean (2005) sur le PCC de la ligne A du RER parisien montre comment les opérateurs construisent une conscience partagée d'une situation et quelle est l'une des origines des malentendus qui peuvent survenir. L'agencement spatial influence l'accès à

l'information des opérateurs, mais aussi leur capacité à communiquer et à rendre leur comportement intelligible, signifiant, à autrui. Si certains opérateurs disposent de sources d'information dédiées qui leur permettent d'être autonomes, un opérateur est dépendant des autres pour le recueil des informations dont il a besoin. Cet agencement spatial et la disponibilité des informations sont dépendants de la culture de l'entreprise et des priorités affectées aux activités des opérateurs. Enfin, chaque opérateur poursuit une activité qui lui est propre, sur un objet spécifique, activité et objet qui sont le foyer de son attention. Les malentendus apparaissent lorsque les opérateurs ne partagent pas le même cadre d'interprétation sur une situation commune lorsqu'ils communiquent entre eux. Grosjean (2005) montre que « tout ce qui fait obstacle à cette définition de situation commune et empêche l'awareness va susciter le malentendu ». Il en est de même lorsque les agents sont impliqués dans des activités divergentes dont ils ne peuvent se rendre compte mutuellement au fur et à mesure et sans avoir à interférer avec l'activité de l'autre ». Ainsi Grosjean montre que, pour ce qui concerne Bakerloo Line à Londres, la coprésence des opérateurs « leur permet de construire une situation commune dans laquelle chacun peut poursuivre son activité, sans avoir à interrompre l'autre » (Grosjean, 2005).

Dans le cas du vol Rio-Paris AF 447, Conversy *et al*. (2014) mettent en évidence « qu'il n'y a pas de rétroaction dans le *sidestick*[9] du PNF (pilote non en fonction) des actions du PF (pilote en fonction) sur son *sidestick* ». De plus, les positions des *sidesticks* ne permettent pas à l'un des membres de l'équipage de savoir ce que fait l'autre. Ainsi que le soulignent les auteurs, cette situation ne favorise pas la conscience des activités des co-équipiers.

Dans la même perspective, Swain & Mills (2003) montrent comment les membres d'une équipe communiquent entre eux pour élaborer et maintenir une représentation de la situation. Ils utilisent des stratégies de communication implicites lorsqu'ils sont affrontés à un niveau élevé de stress. Cela suppose qu'ils partagent des connaissances communes sur les événements qui interviennent autour d'eux. Ces stratégies de communication implicite permettent de réduire la charge de communication et de coordination au sein du groupe. Ces auteurs montrent que les équipes qui ont l'habitude de travailler ensemble mettent plus facilement en œuvre des stratégies de communication implicite dans des situations nouvelles, par rapport aux équipes qui n'ont jamais travaillé ensemble antérieurement.

C'est dans ce contexte des différentes modalités de communication et de la capacité de rendre manifeste à autrui des informations relatives au système, à l'environnement, à l'activité, que nous nous inscrivons.

Pour obtenir la capacité de naviguer à vue et pour donner aux opérateurs les moyens de comprendre la situation dans laquelle se trouve le système, l'approche centrée sur la régulation de la conscience de la situation semble la plus appropriée à notre problématique. En effet, elle ne fait pas d'hypothèse d'une conscience de la situation omnisciente, hypothèse qui ne peut pas être retenue dans le contexte de situations imprévues, imprévisibles et sans précédent. Elle ne fait pas, non plus, l'hypothèse de la construction d'une représentation *ad hoc* pour répondre à un événement singulier dans l'environnement. Elle ne se limite pas à une origine externe qui influencerait et encadrerait la cognition et donc la conscience de la situation de l'opérateur. En articulant processus et produit (représentation mentale), l'approche centrée sur la régulation rend compte d'un modèle dynamique du monde, d'une conscience de la situation mise à jour en permanence, économe des ressources de l'opérateur, et permettant une compréhension minimale pour une efficacité maximale. Enfin, l'approche

[9] La manette latérale (en anglais *side-stick*) est une manette permettant d'actionner les gouvernes de roulis et tangage d'un avion équipé de commandes de vol électriques1.

centrée sur la régulation permet pleinement de prendre en compte la conscience de situations imprévisibles, sans précédent. Par ailleurs, cette conscience de la situation doit être collective, partagée par l'ensemble des opérateurs concernés. Cette conscience partagée de la situation se construit *via* les communications entre opérateurs, par ce qui est rendu manifeste à autrui, mais aussi par la capacité des artefacts technologiques, des systèmes interactifs à donner un cadre d'interprétation commun à chacun des opérateurs collaborant sur une même tâche.

Pour collaborer, coopérer, les opérateurs puissent construire un cadre commun d'interprétation de l'environnement et du système mis en œuvre. Il est nécessaire de prendre en compte que ces différents opérateurs ne sont pas nécessairement localisés au même endroit et ne travaillent pas au même moment. Les IHM doivent leur représenter cet environnement et ce système de façon appropriée à leurs modèles mentaux, à leurs tâches, aux différents systèmes interactifs qu'ils utilisent, en proximité ou en mode distant, en synchrone comme en asynchrone.

1.5. Synthèse et conclusion du chapitre

Dans le contexte des systèmes sociotechniques à longue durée de vie pour lesquels les situations opérationnelles qu'ils rencontrent ne peuvent être connues et prévisibles *a priori*, et qui sont susceptible de subir des migrations spontanées, les démarches de sûreté de fonctionnement ne traitent pas des situations imprévues, sans précédent, et doivent être complétées. La résilience offre une capacité de navigation à vue, d'ajustement et d'adaptation du système sociotechnique, en particulier lorsque le système fonctionne hors de son domaine d'emploi qui complète les démarches de sûreté de fonctionnement. L'évaluation de l'état courant du système, la détection d'anomalies et l'alerte des opérateurs pour les informer de la situation leur permettent d'interpréter, de comprendre cette situation dans laquelle se trouve le système. Cette compréhension du fonctionnement dynamique du système hors de son domaine d'emploi est l'étape préalable pour que les opérateurs puissent le contrôler, prendre à temps des mesures correctives, et engager des actions nécessaires afin de maintenir la sécurité du système.

Dans le chapitre suivant intitulé « Ingénierie Système appliquée aux systèmes critiques », nous montrerons les concepts et méthodes de l'ingénierie système sur lesquels nous nous appuierons dans notre contribution d'architecture et de processus pour la résilience des systèmes en particulier pour instrumenter le système de surveillance de l'usage et de l'état du système. Dans le chapitre Chapitre 3 intitulé « Éléments d'ergonomie et d'ingénierie des IHM : conception centrée utilisateur et architecture des systèmes interactifs », nous présenterons les concepts clefs de la conception centrée utilisateur pour concevoir une IHM appropriée pour que les opérateurs puissent comprendre la situation dans laquelle est le système.

Chapitre 2.

Ingénierie Système appliquée aux systèmes critiques

2.1. Introduction

Un système artificiel [10] est un ensemble intégré d'éléments — personnels, produits, processus —, connectés et reliés entre eux, en vue de satisfaire un ou plusieurs objectifs définis (ISO 2008 ; Luzeaux & Ruault, 2013).

Un système peut être appréhendé de deux points de vue, celui des processus mis en œuvre et celui de son architecture, lesquels se déclinent ainsi :

- les processus et activités mis en œuvre pour concevoir, produire, vérifier, distribuer, déployer, exploiter, maintenir en condition opérationnelle et retirer du service le système, plus largement, les processus et activités pour gérer la configuration du système, gérer les risques, maintenir à jour l'ensemble des données du système, etc. ;
- l'architecture[11] décrit l'organisation des fonctions (architecture fonctionnelle) et des composants (architecture physique) du système, sous les angles comportementaux, structuraux et dynamiques.

Ces deux points de vue, processus et architecture, complémentaires, sont traités chacun avec son focus et ses concepts qui lui sont propres.

Après avoir présenté les définitions et concepts des systèmes critiques, la section « Processus d'ingénierie » est consacrée aux processus et activités mis en œuvre pour produire le système. La section « Architecture système », quant à elle, est consacrée à la description de l'organisation des fonctions et des composants du système. Ensuite, la section intitulée « Surveiller l'usage du système : éléments d'architecture préalables pour concevoir un système résilient » présente l'architecture fonctionnelle du système de surveillance de l'usage et de l'état d'un système, et détaille les blocs de traitement. Ce chapitre se clôt avec une synthèse et une conclusion. Cette différenciation entre processus et architecture structure le rapport.

2.2. Définitions et concepts des systèmes

L'ingénierie système traite de systèmes artificiels conçus par les êtres humains. Ces systèmes sont des combinaisons d'éléments matériels, logiciels, procéduraux, visant un ou plusieurs buts définis (ISO, 2008 ; Meinadier & Fiorèse, 2012 ; Luzeaux & Ruault, 2013). Un système sociotechnique comprend une partie technique, relevant de l'ingénierie système, et une partie

[10] Un système artificiel est un système fait par l'homme, traduction de *man-made systems* (ISO, 2008), pour le distinguer d'un système naturel (par exemple, l'écosystème de la canopée amazonienne, ou l'écosystème de la toundra sibérienne).

[11] Pour des raisons pratiques, le terme *architecting* est utilisé pour désigner l'activité d'architecture, afin de la différencier de l'architecture du système.

humaine et organisationnelle relevant des sciences humaines et sociales. Le concepteur recherche que ces deux parties se complètent dans leurs interactions en prenant en compte les spécificités de chacune d'elles. En particulier, l'approche sociotechnique s'appuie sur l'autorégulation, le contrôle interne plutôt qu'au contrôle externe, ainsi que sur le processus d'appropriation de la partie technique par les opérateurs (Ruault, 2011). Nous pouvons reformuler et préciser cette définition.

Définition : système

Ensemble complexe de matériels, logiciels, personnels et processus opérationnels, organisés de manière à satisfaire les besoins et à remplir les services attendus, dans un environnement donné.

L'architecture du système d'intérêt (traduction de la notion de *system of interest* en anglais, on parle aussi de système principal), dans sa globalité, comprend, d'une part le système opérant qui réalise les missions qui sont affectés au système, répondant aux besoins des utilisateurs, des clients, et, d'autre part, des systèmes contributeurs qui n'interviennent pas directement dans la réalisation de ces missions mais jouent un rôle, par exemple le système de test et qualification du système d'intérêt (Meinadier & Fiorèse, 2012).

Par exemple, un système ferroviaire permettant de transporter des voyageurs d'un point à un autre comprend, entre autres :

- des produits et des services, que sont, entre autres, le transport de voyageurs, le transport de fret ;
- des équipements et des dispositifs produisant ces produits finis et services que sont des trains, des stations, des systèmes de gestion de trafic, des systèmes de vente ;
- des procédures pour mettre en œuvre ces dispositifs ;
- des utilisateurs finaux qui appliquent ces procédures et mettent en œuvre ces dispositifs pour réaliser les tâches qui leur sont prescrites ;
- des systèmes contributeurs pour réaliser des tests, des mesures, des activités d'ingénierie ;
- des ressources et des consommables, telle que l'électricité.

Le terme système est utilisé dans deux perspectives complémentaires (Meinadier & Fiorèse, 2012) :

- le « système à faire » est la solution conçue et réalisée pour répondre à un besoin, à une finalité, et comprend des sous-systèmes et constituants (matériels, logiciels, organisations et compétences humaines) et leurs interfaces ;
- le « système pour faire » comprend l'ensemble des dispositifs qui sont nécessaires pour faire le « système à faire ». Il s'agit là, entre autres, des activités de gestion de projet, ainsi que tout ce qui est nécessaire (produits contributeurs) pour faire le « système à faire ».

2.3. Processus d'ingénierie

Les principales phases du cycle de vie d'un système sont l'analyse de concepts, l'étude de faisabilité, le développement, la réalisation, la mise en service, l'utilisation et le retrait de service (Luzeaux & Ruault, 2013). Les différents processus mis en œuvre durant ces phases

relèvent pour certains d'entre eux des rôles et responsabilités du client, tandis que d'autres relèvent du fournisseur. L'expression du besoin, la définition des situations opérationnelles, le retour d'expérience relèvent de la responsabilité du client. Le fournisseur est en charge de l'architecture du système ainsi que du maintien de sa cohérence tout au long de la vie du système.

Définition : *systems engineering*

Interdisciplinary approach governing the total technical and managerial effort required to transform a set of stakeholder needs, expectations, and constraints into a solution and to support that solution throughout its life.

Dans un premier temps, l'ingénierie système s'est focalisée sur les phases amont, et peu sur les phases aval d'exploitation. Les étapes du cycle de vie sont la conception, le développement, la production, l'utilisation, la maintenance et le retrait de service (ISO, 2010c). Quoique mentionnée dans ces documents pour tracer les anomalies rencontrées lorsque le système est utilisé, en vue de les corriger dans les activités de rénovation à mi-vie, ces dernières sont peu formalisées dans les documents de référence (ISO, 2008 ; ISO, 2010c). Les démarches linéaires sont progressivement complétées par des démarches itératives et incrémentales (Boehm, 2009a ; Boehm, 2009b : Luzeaux & Ruault, 2013), prenant de plus en plus en compte le retour d'expérience.

La troisième édition de la norme, en cours d'élaboration actuellement (ISO, 2014), identifie et décrit les processus techniques que sont :

- le processus d'analyse métier ou de la mission (*Business or mission analysis process*) consiste à définir un problème ou une opportunité pour le métier ou une mission, caractériser l'espace solution et déterminer les types de solutions potentielles qui peuvent répondre au problème soulevé ou profiter de l'opportunité qui se présente ;
- le processus de définition des besoins et exigences des parties prenantes (*Stakeholder needs and requirements definition process*) consiste à définir les exigences des parties prenantes vis-à-vis d'un système qui peut fournir les capacités attendues par les utilisateurs et les autres parties prenantes dans un environnement identifié ;
- le processus de définition des exigences système (*System requirements definition process*) consiste à transformer les exigences des parties prenantes et les capacités attendues du point de vue des utilisateurs en une représentation technique d'une solution qui satisfait aux besoins opérationnels des utilisateurs ;
- le processus de définition de l'architecture (*Architecture definition process*) consiste à élaborer plusieurs alternatives d'architecture afin de sélectionner l'une d'entre elles répondant aux exigences formulées préalablement et de représenter cette solution d'architecture en modèles cohérents ;
- le processus de définition de la définition du système (*Design definition process*) consiste à définir le système de façon suffisamment détaillée pour le réaliser ;
- le processus d'analyse système (*System analysis process*) consiste à analyser le système et fournir des données rigoureuses pour une compréhension technique du système afin d'aider la prise de décision tout au long du cycle de vie du système ;
- le processus de réalisation (*Implementation process*) consiste à réaliser les composants du système spécifié ;
- le processus d'intégration (*Integration process*) consiste à intégrer un ensemble d'éléments afin de réaliser le système spécifié ;

- le processus de vérification (*Verification process*) consiste à fournir des preuves objectives que le système satisfait aux exigences et caractéristiques spécifiées ;
- le processus de transition (*Transition process*) consiste à montrer que le système a la capacité à fournir les services spécifiés par les exigences des parties prenantes dans l'environnement opérationnel ;
- le processus de validation (*Validation process*) consiste à fournir des preuves objectives que le système, quand il est utilisé, remplit la mission qui lui est assigné, avec l'usage attendu dans l'environnement opérationnel attendu ;
- le processus de maintenance (*Maintenance process*) consiste à maintenir la capacité du système à fournir un service ;
- le processus de démantèlement (*Disposal process*) consiste à retirer le système du service et à le démanteler en tenant compte des exigences légales et réglementaires.

Nous retenons du processus de définition des exigences système que ces exigences doivent être complètes, exhaustives. Cela suppose une parfaite compréhension des conditions d'exploitation, à l'instar des recommandations formulées par les documents de bonnes pratiques que nous avons pu identifier dans la section 1.3.1, « La sûreté de fonctionnement et la sécurité d'un système », du Chapitre 1. Nous retenons aussi qu'il est mentionné, pour le processus d'analyse métier ou de la mission, qu'il peut être mis en œuvre tout au long du cycle de vie du système pour prendre en compte des changements dans l'environnement, le besoin, etc.

Cette troisième édition de la norme ISO décrit le processus d'opération en mentionnant que ce processus établit les exigences et affecte le personnel pour mettre en œuvre le système et surveiller les services fournis par le système ainsi que ses performances.

Dans le but de fournir ces services de façon pérenne, ce processus d'opération identifie et analyse les anomalies en relation avec le contrat entre fournisseur et client, les exigences des parties prenantes et les contraintes opérationnelles.

Ce processus comprend plusieurs tâches :

- préparer la mise en œuvre du système ;
- mettre en œuvre le système, proprement dit ;
- gérer les performances du système et
- soutenir le client.

La tâche « mettre en œuvre le système » se décline en :

- utiliser le système dans l'environnement opérationnel attendu ;
- exploiter les matériels et les autres ressources, tel qu'exigé, pour mettre en œuvre le système et fournir ces services de façon pérenne ;
- surveiller le système en opération ;
- identifier et enregistrer les performances du système quand ces dernières sont hors des bornes acceptables ;
- exécuter des opérations *ad hoc* si nécessaire.

En détail, la surveillance du système consiste à :

- gérer l'adhésion à la stratégie qui préside à la mise en œuvre du système ;
- s'assurer que le système est mis en œuvre en toute sécurité et de façon conforme aux règlements concernant la sécurité au travail et la protection de l'environnement ;

- utiliser les mesures définies dans la stratégie et les analyser pour confirmer que les performances s'inscrivent dans les bornes acceptables.

Surveiller le système consiste à examiner si les performances du système s'inscrivent au sein de bornes acceptables en exploitant les résultats d'instrument mesurant périodiquement les performances et les délais de réponse. Nous rattachons cette proposition à celle énoncée dans les documents relatifs à la sûreté de fonctionnement (cf. section 1.3.1 « La sûreté de fonctionnement et la sécurité d'un système »). Le retour d'expérience des opérateurs est aussi une source pour évaluer les performances du système.

Quand ces performances sont hors des bornes acceptables, la tâche « identifier et enregistrer les performances du système quand ces dernières sont hors des bornes acceptables » est mise en œuvre.

La tâche « gérer les performances du système » comprend :

- enregistrer les résultats de la mise en œuvre opérationnelle et les anomalies détectées ;
- enregistrer les accidents et les problèmes tracer leur résolution ;
- maintenir la traçabilité des éléments mis en œuvre ;
- fournir les informations clefs qui sont sélectionnées pour la configuration de référence.

Cette tâche permet d'identifier les causes racines des accidents ou problèmes rencontrés, permettant des actions correctives, des actions d'amélioration et de capitaliser les leçons apprises. Ainsi, si un accident survient, les opérateurs enregistrent cet accident et appliquent les actions prescrites dans les procédures opérationnelles validées pour restaurer une situation normale. La traçabilité bidirectionnelle est maintenue entre les éléments opérationnels, les besoins de la mission, les concepts opérationnels et les exigences des parties prenantes afin de mener à bien une analyse d'impact.

Malgré les évolutions par rapport à la seconde édition de 2008, cette norme (ISO, 2014) ne décrit pas de façon détaillée les processus et activités clefs de la mise en œuvre du système, en particulier la communication aux opérateurs de l'état du système. Les informations concernant cet état sont transmises à ceux qui ont la charge de la maintenance du système. Le système technique est spécifié à partir de la définition d'une situation opérationnelle de référence, laquelle est élaborée dans un environnement opérationnel supposé stable (Ruault *et al*., 2012b). Cette situation opérationnelle est décrite et modélisée sous forme de scénarios opérationnels à partir desquels sont définies les fonctions à réaliser, en termes de services rendus par l'artefact technologique et de tâches menées par les opérateurs humains, y compris les actions correctives prescrites à mettre en œuvre en cas d'accident. Cela permet, d'une part de spécifier et de concevoir l'artefact technologique, et d'autre part de définir les profils des opérateurs, les compétences qu'ils doivent acquérir via des formations adaptées pour réaliser ces tâches. Cette démarche est adaptée aux systèmes pour lesquels le contexte et l'environnement opérationnels ainsi que les missions à réaliser sont connus et les performances stables. Elle connaît ses limites dès lors que l'environnement et les missions ne sont pas complètement connus et les performances fluctuantes. En particulier, il s'avère qu'il ne peut y avoir d'action corrective que les opérateurs doivent mettre en œuvre lorsque le système est hors de son domaine de définition et face à une situation imprévisible.

Dans le même esprit, la Figure 2.1 montre les activités menées par les différents partenaires (organisme concevant un système, son client, ses fournisseurs), leurs relations partant de l'expression du besoin pour aboutir à la validation du système (ASD-STAN, 2013).

L'ingénierie système évolue en mettant en œuvre des démarches de développement de concept et d'expérimentation (CD&E pour *concept development and experimentation*) (Hayes,

2009) itérative, incrémentale et participative (Pew & Mavor, 2007 ; Boehm, 2009a ; Boehm, 2009b). Si ces démarches agiles font participer les utilisateurs du système pour évaluer avec eux les solutions de conception alternatives et mûrir la solution la plus adaptée, ces démarches sont mises en œuvre dans les étapes amont des projets et ne traitent pas du stade d'exploitation, *a fortiori* des situations imprévisibles, sans précédent.

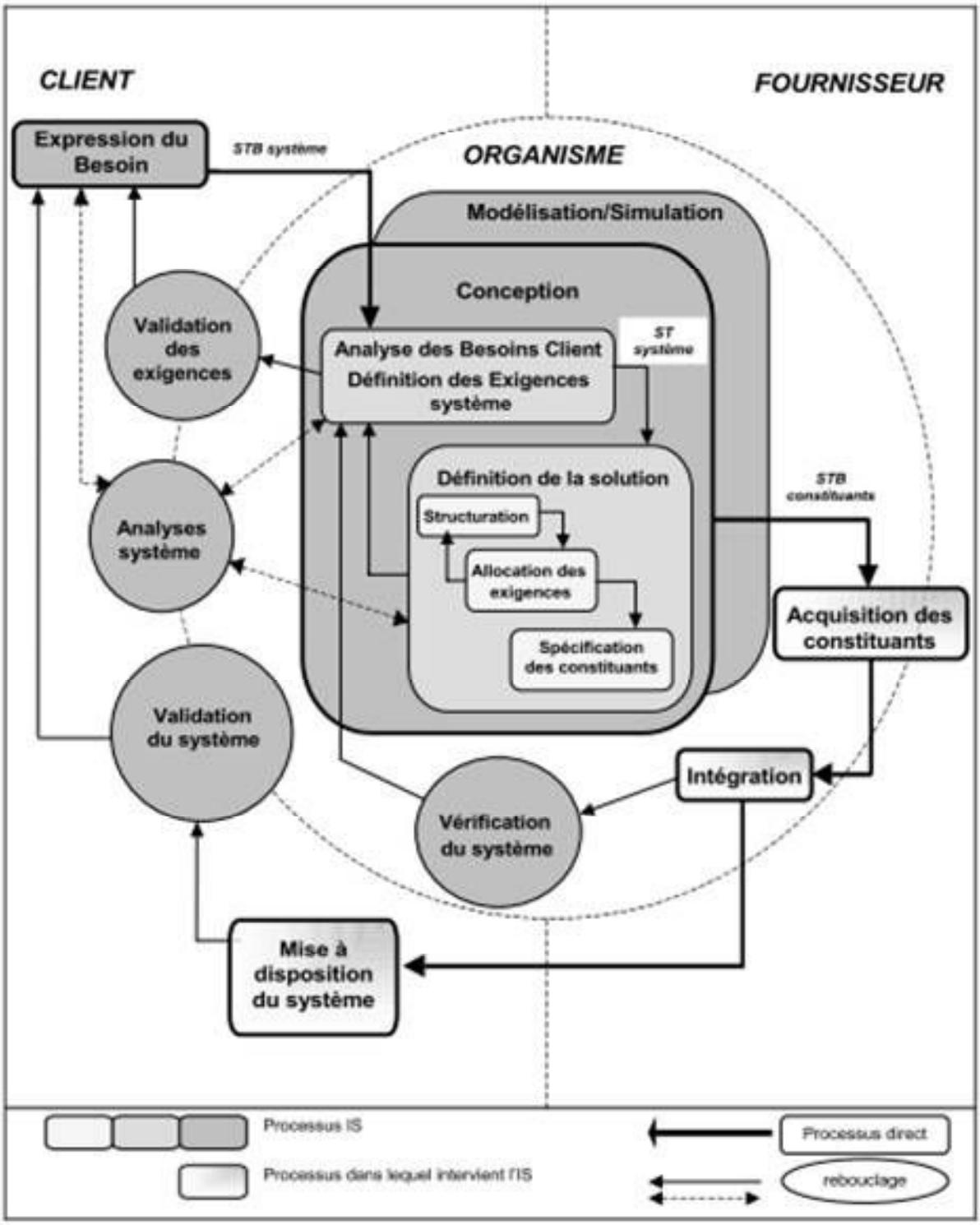

Figure 2.1. Interactions entre les activités techniques du processus d'ingénierie système (ASD-STAN, 2013).

2.4. Architecture système

L'architecture système décrit l'organisation du système à faire, sa structure, l'organisation des services qu'il fournit, ainsi que ses liens avec les systèmes de son environnement. On différencie plusieurs types d'architecture, dont l'architecture fonctionnelle et l'architecture physique (Luzeaux & Ruault, 2013).

2.4.1. Généralités sur l'architecture d'un système

Le système est d'abord regardé comme une boîte noire dans ses interactions avec son environnement. Identifier ces interactions permet d'identifier les services qu'il fournit à cet environnement, et donc les fonctions qu'il doit réaliser. L'architecture fonctionnelle décrit l'organisation de ces fonctions du système et leurs interrelations. Ces fonctions expriment ce que fait le système (le quoi), dans quel but (le pourquoi) indépendamment de la façon de faire du système (le comment).

Définition : *architecture*

Fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution (ISO, 2011).

Ces fonctions sont décomposées hiérarchiquement pour permettre d'identifier les fonctions terminales. La représentation simplifiée en est une arborescence fonctionnelle. Une fonction est une transformation des entrées qui lui sont fournies pour produire des résultats sous forme de sorties. Pour cela, la fonction s'appuie sur des ressources et suit un ensemble de règles. À titre illustratif, la Figure 2.2 décrit une fonction avec ses entrées, ses sorties, ses ressources et ses règles de contrôle, en utilisant la modélisation IDEF0 (ISO, 2012). D'autres modélisations existent que nous présentons succinctement dans la section « Autres langages de modélisation de l'architecture d'un système ». Notre contribution met en œuvre la modélisation SysML que nous détaillons. Les liens entre fonctions sont des relations logiques et temporelles. Les premières décrivent les liens entre fonctions telles que l'exclusion (effectuer cette fonction ou celle-là, mais pas les deux) et l'inclusion (effectuer cette fonction et celle-là). Les secondes concernent la séquentialité (effectuer cette fonction avant cette autre), le parallélisme (effectuer cette fonction en même temps que cette autre), l'itération (effectuer cette fonction n fois de suite). Des contraintes logiques ou temporelles peuvent être attachées aux fonctions. Chaque fonction est réalisée par un ou plusieurs composants. Cette relation s'appelle l'allocation des fonctions aux composants.

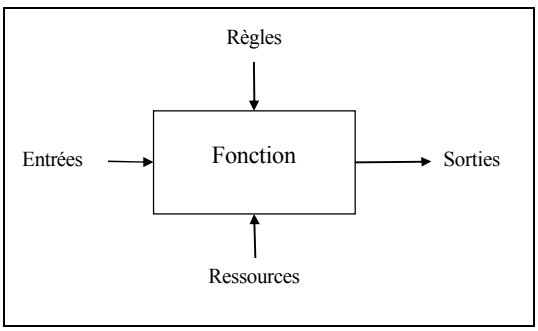

Figure 2.2. Description illustrative d'une fonction (Luzeaux & Ruault, 2013).

Il existe d'autres façons de représenter les fonctions principales d'un système, dont les cas d'utilisation ou les diagrammes d'activités. Ces solutions permettent de modéliser l'arborescence des fonctions, ainsi que les relations logiques et temporelles qu'elles entretiennent entre elles.

L'architecture physique, quant à elle, décrit l'organisation de ces composants qui réalisent les fonctions. Le choix parmi plusieurs architectures physiques candidates s'appuie sur une comparaison de ces architectures en tenant compte du coût et du niveau de maturité technologique (*Technology Readiness Level*) de ces composants. Des composants réalisent des fonctions différentes. Il n'y a donc pas de relation de bijection entre l'architecture fonctionnelle et l'architecture physique.

La description d'architecture (ISO, 2011) comprend l'ensemble des produits d'ingénierie décrivant l'architecture d'un système sous différents angles, différents points de vue, pour contribuer à :

- la formalisation du système et de ses évolutions ;
- la communication avec les parties prenantes ;
- l'évaluation et la comparaison des architectures de manière cohérente ;
- la planification, la gestion et l'exécution des activités de développement du système ;
- la formalisation des caractéristiques persistantes du système et les principes permettant des évolutions acceptables du système ;
- la vérification de l'implémentation du système conformément à la description de l'architecture ;
- l'enregistrement des contributions des savoirs et savoir-faire en architecture des systèmes à logiciel prépondérant.

Cette norme (ISO, 2011) présente les trois niveaux de point de vue d'architecture que sont :

- le niveau opérationnel : pourquoi le système est-il conçu et construit ? Quelles sont ses missions et buts ? Quelles sont les missions opérationnelles dans lesquelles il sera utilisé ?
- le niveau fonctionnel : comment sont organisés les services que le système fournit à son environnement ?
- le niveau physique : comment les composants du système interagissent ensemble pour fournir ces services ?

Cette norme ne prescrit pas un langage particulier pour décrire l'architecture d'un système.

2.4.2. Modélisation de l'architecture d'un système avec SysML

Le langage de modélisation SysML (*Systems Modeling Language*) est une extension du langage de modélisation UML (*Unified Modeling Language*). Si UML a été développé pour modéliser les logiciels, SysML est adapté pour traiter des systèmes. Ce langage a été sélectionné par l'Éducation nationale comme langage de modélisation des systèmes multi-physiques et inscrit dans les référentiels des formations, dont le baccalauréat STI2D (Sciences et Technologies de l'Industrie et du Développement Durable), ainsi que dans les formations de BTS (Brevet de Technicien Supérieur) et de préparation aux concours des grandes écoles. Le langage SysML reprend, complète ou retire des diagrammes issus d'UML (Friedenthal *et al.*, 2011 ; Luzeaux & Ruault, 2013). Certaines extensions d'UML, antérieures à la création de SysML, en particulier celles pour la modélisation des systèmes interactifs, n'ont pas été

traduites en SysML. Dans ce contexte, le mémoire comprend des diagrammes SysML quand il traite d'un système, et des diagrammes UML quand il concerne des IHM. Le langage de modélisation SysML exprime le comportement du système, l'organisation des composants pour réaliser ce comportement, du plus haut niveau au plus bas niveau.

Quelques-uns de ces diagrammes sont les suivants :

- le diagramme des cas d'utilisation permet de modéliser les services que rend le système à ses utilisateurs ;
- le diagramme d'activité permet de modéliser des flux d'activités en caractérisant les conditions de déclenchement ou d'arrêt de ces activités. Ce diagramme est complémentaire du précédent pour exprimer les flux d'activité des cas d'utilisation ;
- le diagramme de séquence, complémentaire du précédent, permet de modéliser les échanges entre fonctions au cours du temps ;
- le diagramme de définition de blocs représente la structure du système, fonctions ou composants, en montrant les liens de composition entre ces éléments ;
- le diagramme de bloc interne représente les caractéristiques des éléments du système, et les liens que ces éléments entretiennent entre eux, en particulier les interfaces et les flux.

Dans l'étude de cas à destination des enseignants de la filière STI2D[12] (Ruault *et al.*, 2014), les auteurs montrent la mise en œuvre des diagrammes SysML pour modéliser l'architecture d'une borne de rechargement de véhicules électriques. Plusieurs diagrammes sont élaborés.

La Figure 2.3 décrit l'environnement de la borne de rechargement en utilisant le diagramme de définition de blocs (Ruault *et al.*, 2014). L'objectif de ce diagramme consiste à définir la borne de rechargement par rapport aux systèmes de son environnement, avec lesquels elle est en interaction. Le système étudié est la borne de rechargement (stéréotype « *System* »), les autres items du diagramme sont des systèmes de son environnement (stéréotype « *Environment* »). Deux acteurs sont représentés dans le diagramme de contexte. Ces deux acteurs sont, d'une part un client qui recharge son véhicule électrique, d'autre part un agent de l'opérateur de bornes (opérateur est entendu ici comme la société qui gère et exploite les bornes), par exemple un agent de maintenance.

La Figure 2.4 décrit le cas d'utilisation « recharger les véhicules électriques » en utilisant le diagramme des cas d'utilisation (Ruault *et al.*, 2014a). Ce cas d'utilisation « recharger VE » est réalisé par la « borne de rechargement » et fait appel au « client », au « badge abonnement » du client et au « véhicule électrique » du client, qui sont à l'extérieur du périmètre de la borne de rechargement.

[12] L'étude de cas industriel, à destination des enseignants de la filière STI2D, a été réalisée dans le cadre du projet « Ingénierie système et SysML dans l'éducation nationale » mené en commun par l'AFIS, l'AIP-Priméca et l'Éducation nationale.

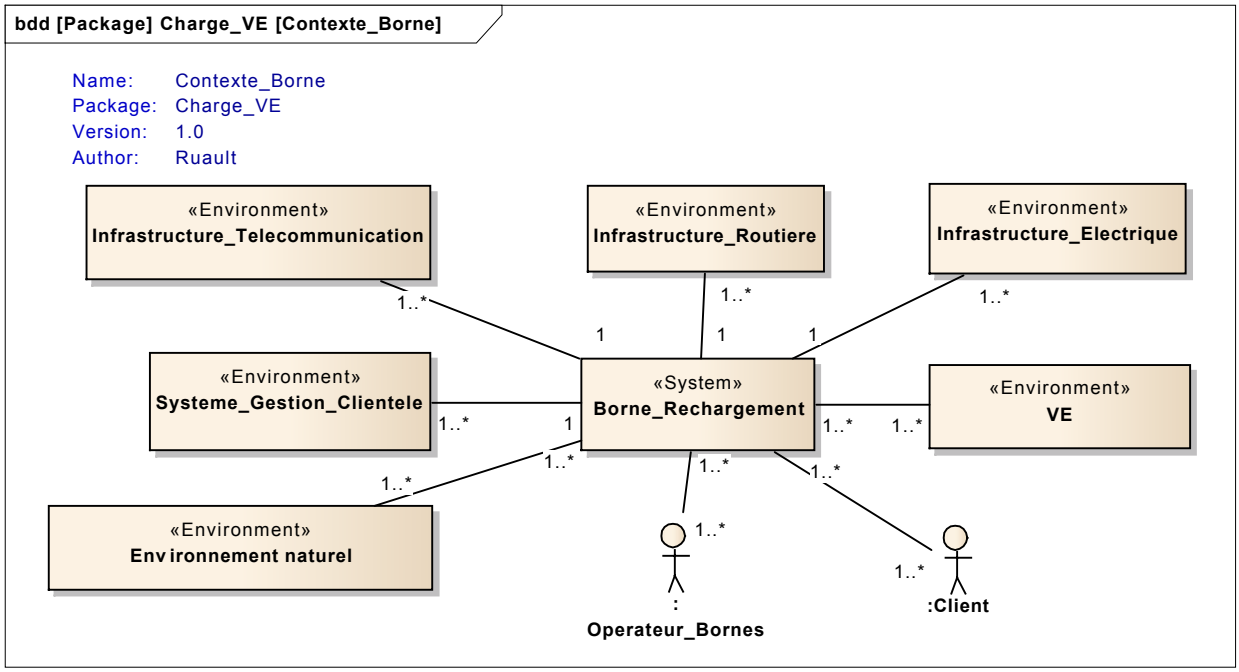

Figure 2.3. Borne de rechargement de véhicules électriques et son environnement (Ruault *et al.*, 2014a).

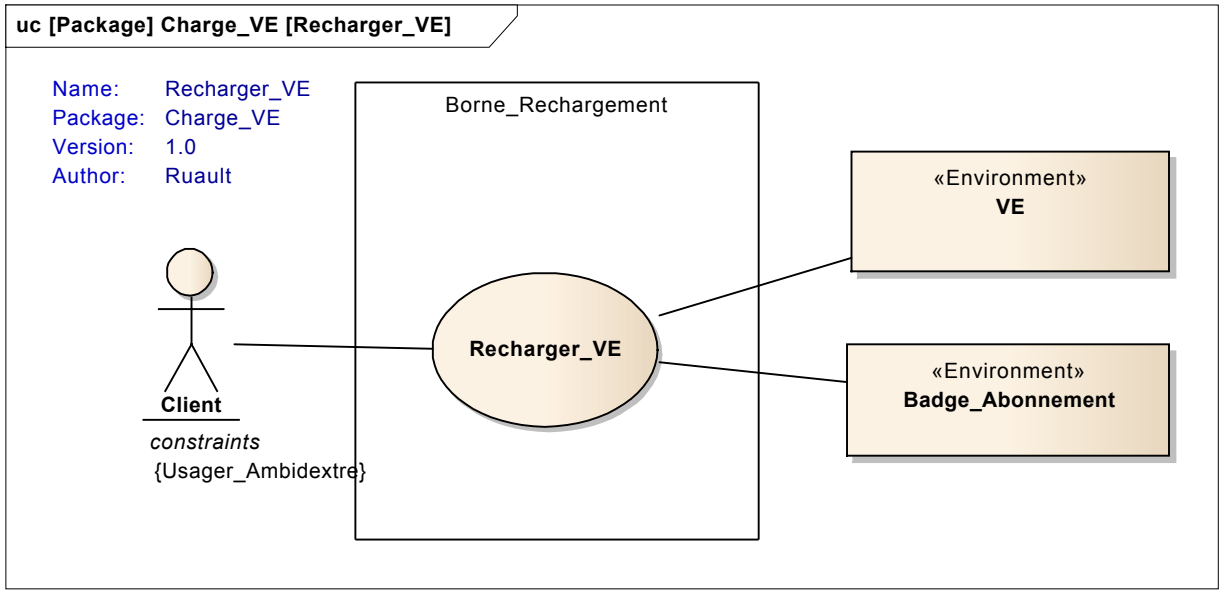

Figure 2.4. Diagramme des cas d'utilisation : gérer les bornes (Ruault *et al.*, 2014a).

En complément du diagramme des cas d'utilisation, la Figure 2.5 (diagramme d'activité SysML) représente l'architecture fonctionnelle de la fonction « recharger les véhicules électriques », c'est-à-dire les actions à mener pour réaliser cette fonction ainsi que les différents états des composants de la borne que ces actions modifient (Ruault *et al.*, 2014a).

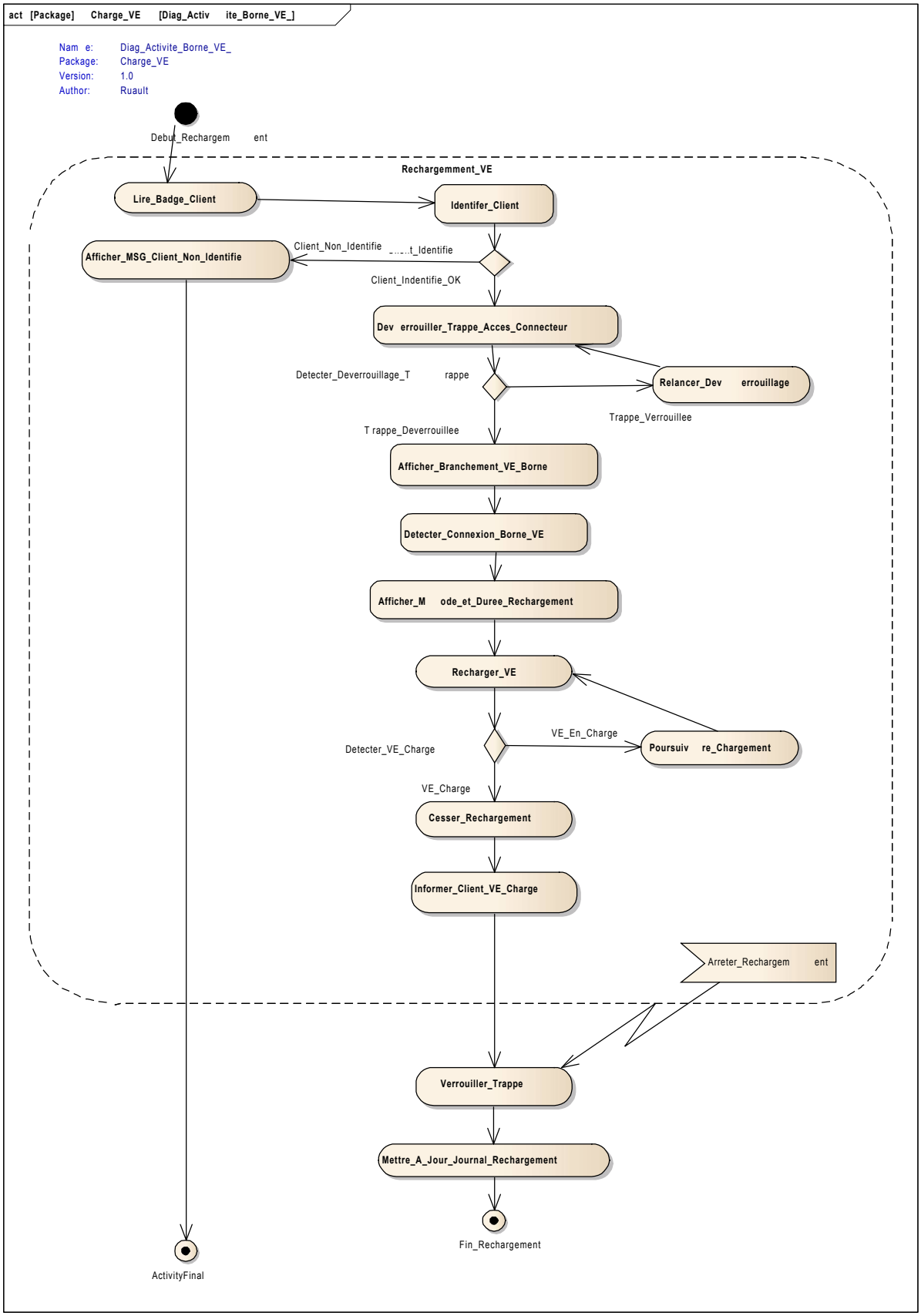

Figure 2.5. Architecture fonctionnelle détaillée de la fonction « recharger les véhicules électriques » (Ruault *et al.*, 2014a).

La Figure 2.6, basée sur un diagramme de bloc interne, modélise les liens entre la borne de rechargement de véhicules électriques et les systèmes de son environnement (Ruault *et al.*, 2014a). Dans les différents blocs, les attributs des systèmes sont représentés par des variables avec les valeurs qu'elles peuvent prendre, tandis que les services que rendent les systèmes sont représentés par un verbe à l'infinitif suivi de parenthèses. Enfin, les interfaces sont représentées par des carrés reliés entre eux par des flèches, lesquelles représentent les flux.

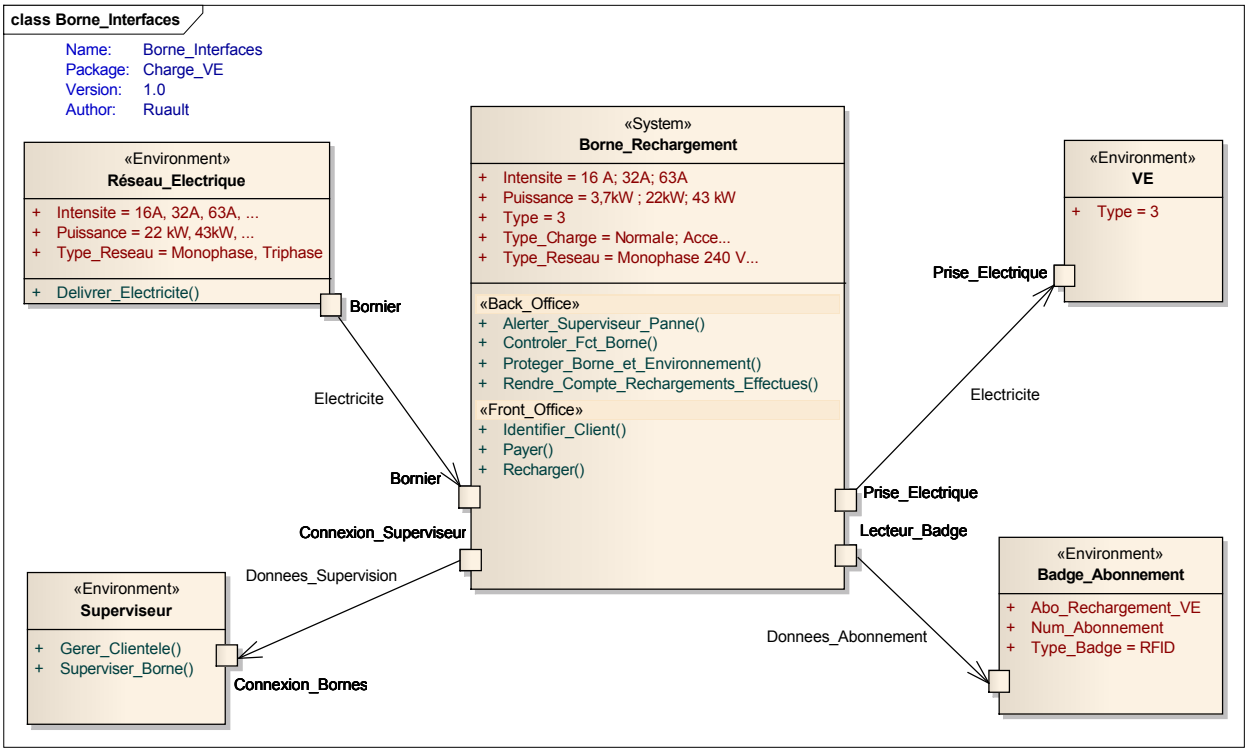

Figure 2.6. La borne de rechargement, ses fonctions, ses interfaces avec les systèmes environnants (Ruault *et al.*, 2014a).

Sans reprendre le diagramme SysML *ad hoc*, la Figure 2.7 montre l'allocation des fonctions de la borne de rechargement de véhicules électriques (VE) à ses composants.

Composants / Fonctions	Carcasse de la borne (socle)	Connecteur pour charger les VE	Cordons électriques d'alimentation des VE	Connexion au réseau électrique	Connexion au réseau de télécommunication	Dispositif de verrouillage du	Dispositif de protection électrique	Unité de contrôle	Interface humain-machine
Lire le Badge du Client									X
Identifier le Client								X	
Afficher message « Client Non Identifié »								X	X
Déverrouiller le Connecteur		X						X	
Relancer le Déverrouillage		X						X	
Afficher le Branchement entre le VE et la Borne								X	X
Détecter la Connexion entre la Borne et le VE		X	X					X	
Afficher le Mode et la Durée du Rechargement								X	X
Recharger le VE		X	X	X					
Poursuivre le Chargement		X	X	X					
Cesser le Rechargement		X	X	X				X	
Informer le Client que le VE est Chargé					X			X	
Verrouiller le Connecteur		X						X	
Mettre à jour le Journal des Rechargements								X	

Figure 2.7. Matrice d'allocation des fonctions aux composants de la borne de rechargement (Ruault *et al.*, 2014a).

Nous pouvons noter que ce langage achoppe à rendre compte de l'organisation géométrique du système, y compris au plus haut niveau quand cette organisation a des impacts sur les performances du système, par exemple pour décrire les tourbillons de portance, écoulements tourbillonnaires générés par un avion.

Nous utilisons SysML pour élaborer les modèles de notre contribution. Pour autant, ce n'est pas le seul langage de modélisation disponible. Sans montrer l'ensemble des langages de modélisation, la section 2.4.3 présente ci-dessous d'autres langages, à titre d'illustration.

2.4.3. Autres langages de modélisation de l'architecture d'un système

En complément de la section précédente, celle-ci présente à titre d'exemple, les langages de modélisation IDEF (*Integration Definition*) et OPM (*Object-Process Methodology*).

Développé pour l'US Air force dans le domaine de l'ingénierie système et du génie logiciel, le langage de modélisation IDEF (*Integration Definition*) comprend plus de quinze

diagrammes pour modéliser différents points de vue du système considéré. Parmi ces quinze diagrammes, nous relevons ceux consacrés à :

- la modélisation fonctionnelle (IDEF0). Le diagramme le plus connu et le plus utilisé de la gamme IDEF (cf. Figure 2.8) permet de modéliser la décomposition fonctionnelle dans une logique de boîte noire, c'est-à-dire indépendamment de la façon par laquelle les fonctions sont réalisées. Une fonction exploite des ressources et applique des règles de contrôle pour traiter les entrées et pour produire les sorties. La structure hiérarchique des diagrammes et les règles d'élaboration des diagrammes permettent de concevoir des diagrammes clairs et lisibles. D'autres diagrammes complètent la modélisation fonctionnelle IDEF0 pour exprimer les liens logiques et temporels entre fonctions.
- la modélisation des données (IDEF1, IDEF1X, IDEF4, IDEF5). Ces diagrammes sont utilisés dans le domaine du génie logiciel, entre autres.
- la modélisation des processus métier (IDEF3) caractérise ces processus sous forme de flux d'activité, en caractérisant les liens logiques et temporels entre ces différentes activités.

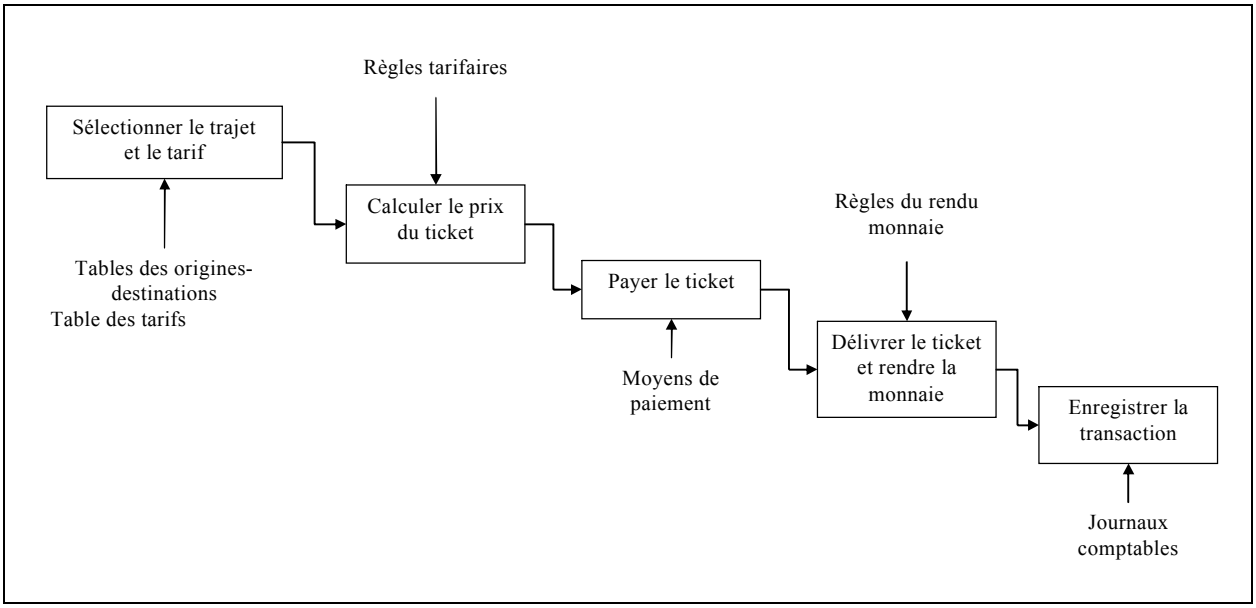

Figure 2.8. Diagramme IDEF0 pour l'achat d'un ticket de transport.

Souvent dans les langages de modélisation, les objets et les processus sont modélisés dans des diagrammes différents, ce qui limite l'expression de leurs liens. Le langage OPM (pour *Object-Process Methodology*) lève cette barrière (Dori, 2014). Face aux langages de modélisation comprenant de nombreux diagrammes, OPM comprend un seul diagramme qui décrit les processus et les objets, les liens entre eux, par exemple, un changement d'état d'un objet lance un processus. Il s'avère être complémentaire des autres langages, en particulier pour réaliser les premiers modèles en phase amont des programmes, lorsqu'il n'est pas nécessaire d'entrer dans des détails. La Figure 2.9 représente les processus et les objets de la prise en charge des bagages dans le domaine aéronautique.

OPM est basé sur une ontologie précise mettant clairement en évidence les liens entre, d'une part, ce qui est modélisé, quelque chose, objet ou phénomène, de la réalité, et d'autre part le modèle, c'est-à-dire la conceptualisation qui est faite de ce quelque chose (Dori, 2014). La Figure 2.9 met en évidence les deux concepts d'objet, ce qui existe (permanence spatiale et

temporelle), représentés sous la forme de rectangles, et de processus, ce qui advient (événement), représentés sous la forme d'ovales. Un processus s'applique à un objet et le transforme, par exemple en le créant, en changeant son état ou en le détruisant. Les objets sont représentés par des rectangles, tandis que les processus sont représentés par des ovales. Les uns et les autres sont reliés par des flèches exprimant des relations (Dori, 2014).

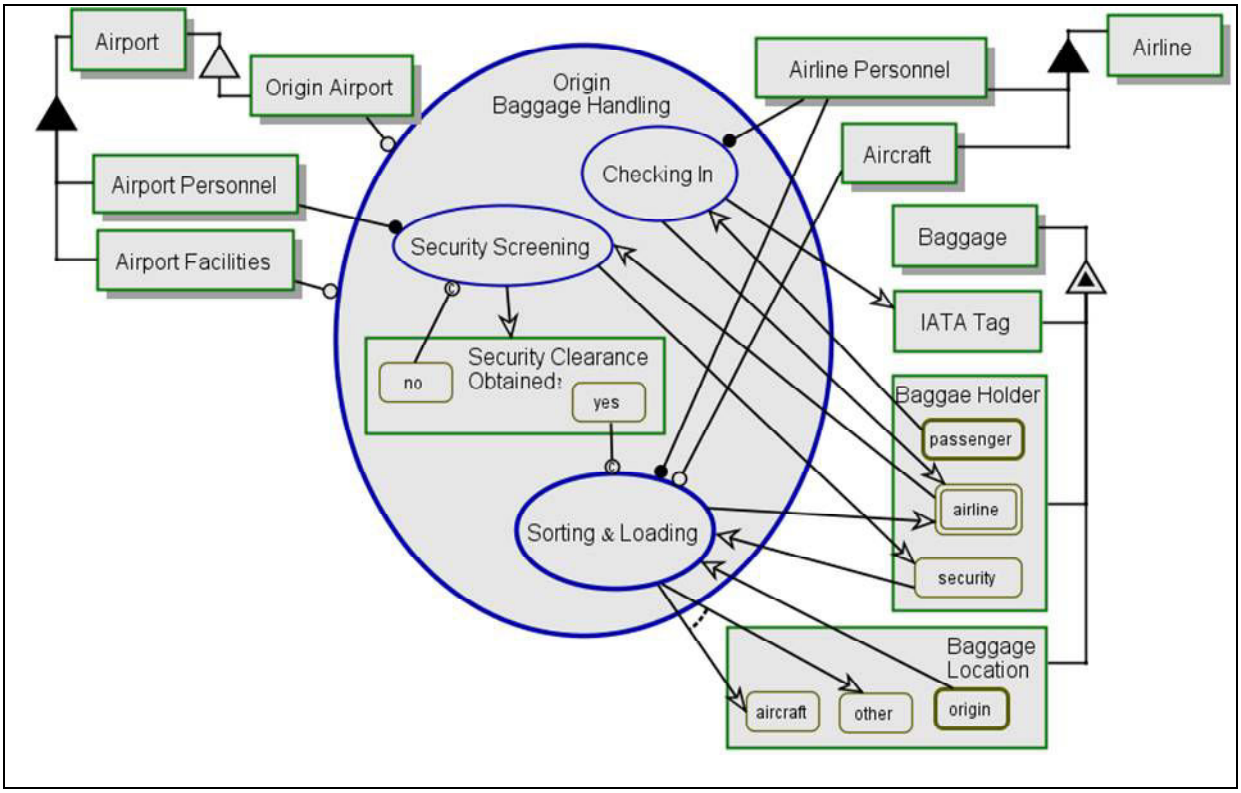

Figure 2.9. Diagramme OPM de la prise en charge des bagages dans le domaine aéronautique (Mordecai *et al.*, 2014).

2.4.4. Patrons de conception (*design patterns*)

Issus des travaux de l'architecte Christopher Alexander (1977), les patrons de conception (*design patterns* en anglais) ont été adaptés par quatre auteurs de la communauté de conception orientée objet, Erich Gamma, Richard Helm, Ralph Johnson et John Vlissides, dans le domaine du logiciel (Salloway & Trott, 2002) pour se généraliser ensuite en ingénierie système (Cloutier & Verma, 2007).

Un patron de conception est « une solution apportée à un problème dans un contexte donné » (Alexander *et al.*, 1977) et comprend quatre parties, un nom significatif, le contexte, le problème et la solution.

Ainsi, dans la construction montagnarde traditionnelle en Europe de l'ouest, le patron de conception, avec l'étable jouxtant le logement, est par exemple bien connu (une illustration est fournie à ce sujet en Figure 2.10). Cette solution du contexte montagnard est une réponse adaptée à la rudesse de l'hiver pour profiter de la chaleur produite par les animaux de l'étable.

En vis-à-vis du contexte montagnard, le contexte chinois présente un autre patron pour répondre au même problème. En Chine du nord, la maison est orientée nord-sud, avec les ouvertures vers le sud et adossée à une montagne au nord pour protéger la maison des vents

du nord. La Cité Interdite est construite sur cette base. D'autres principes d'ordres culturels et sociaux, dont la séparation entre la vie publique et la vie privée, président à la construction des maisons chinoises.

Figure 2.10. Exemple de patron de conception, l'architecture montagnarde (photo prise dans le village de Saint-Véran).

Dans le domaine du logiciel, un patron de conception est décrit par (Salloway & Trott, 2002) :

- un nom qui identifie le patron de conception de façon unique ;
- un objectif ;
- le problème auquel le patron de conception apporte une solution ;
- la solution apportée dans un contexte donné pour répondre au problème ;
- des participants et interlocuteurs qui sont des entités impliquées dans la réalisation du patron de conception ;
- les conséquences sur les différents intervenants et les impacts du patron de conception ;
- l'implémentation qui est la mise en œuvre, concrète, singulière, du patron de conception ;
- la référence du patron de conception dans le livre d'Erich Gamma et ses collègues.

À ce sujet, ces quatre auteurs, Erich Gamma, Richard Helm, Ralph Johnson et John Vlissides, (Salloway & Trott, 2002) ont élaboré des patrons de conception parmi lesquels nous pouvons trouver les patrons suivants :

- adaptateur (*Adapter*) ;

- pont (*Bridge*) ;
- proxy (*Proxy*) ;
- interpréteur (*Interpreter*) ;
- observateur (*Observer*) ;
- état (*State*) ;
- visiteur (*Visitor*).

Le patron de conception « observateur » répond au problème de communiquer un signal, un changement d'état, d'un composant, dit observable, à un ensemble de composants jouant le rôle d'observateurs. Le contexte est celui de la communication d'information entre composants indépendants les uns des autres. Ce patron de conception est très souvent lié à celui de « publier-souscrire ».

Ce patron de conception « publier-souscrire » répond au problème de la diffusion d'informations entre des composants, les uns publiant ces informations, les autres s'abonnant à ces informations. Ce patron de conception permet de découpler les composants et d'homogénéiser ces échanges d'informations en évitant les liens *ad hoc* entre ceux qui publient et ceux qui s'abonnent. En suivant ce patron de conception, un nouvel observateur peut s'abonner à des informations d'observables sans modifier l'architecture du système. Ce patron de conception est complémentaire du patron de conception « observateur ». En effet, l'observateur souscrit à un ensemble d'informations que publie un observable. L'observateur souscrit à des informations selon des thèmes ou des contenus définis.

Dans de nombreux systèmes, un courtier de messages (*broker*) gère les publications et les abonnements, ce qui réduit encore le couplage puisque les observables qui publient des informations n'ont pas à gérer la liste des observateurs qui souscrivent à ces informations. Le patron de conception « courtier de messages » (*broker*) gère des abonnements au profit des observables et des observateurs, les libérant des dépendances entre eux pour réduire le couplage entre ces composants. À ce titre, il complète le patron de conception « publier-souscrire ». Il médiatise les communications entre différents composants et minimise les connaissances mutuelles que ces composants doivent avoir, c'est-à-dire quels sont les composants abonnés ? A quelles informations sont-ils abonnés ? Quels sont les formats des échanges ?

Le patron de conception « proxy » (*proxy*) permet de fournir une interface à des systèmes, de contrôler des accès d'un système, d'un composant et de simplifier son utilisation, en particulier si ce composant doit être manipulé à distance (via un réseau).

De leur côté, Cloutier & Verma (Cloutier & Verma, 2007) déclinent les patrons de conception pour les systèmes en les caractérisant ainsi :

- nom du patron de conception ;
- alias ;
- mots-clés ;
- contexte du problème ;
- description du problème ;
- forces, c'est-à-dire les défis que représente le problème ;
- solution du problème ;
- modèle ;
- interfaces ;

- contexte résultant ;
- exemple ;
- usage connu ;
- patrons de conception connexes ;
- référence ;
- justification du patron de conception ;
- auteur du patron de conception.

Dans ce contexte, Cloutier & Verma (Cloutier & Verma, 2007) décrivent un patron de conception de réseau comprenant des centres (*hubs*) et des nœuds (*nodes*), un patron de conception d'un système de commande et de contrôle (C2). La Figure 2.11 est un des modèles du patron de conception du système C2.

La partie consacrée à « l'Ingénierie des Interactions Homme-Machine » présente des patrons de conception spécifiques du domaine des IHM (cf. Chapitre 3, § 3.4.1).

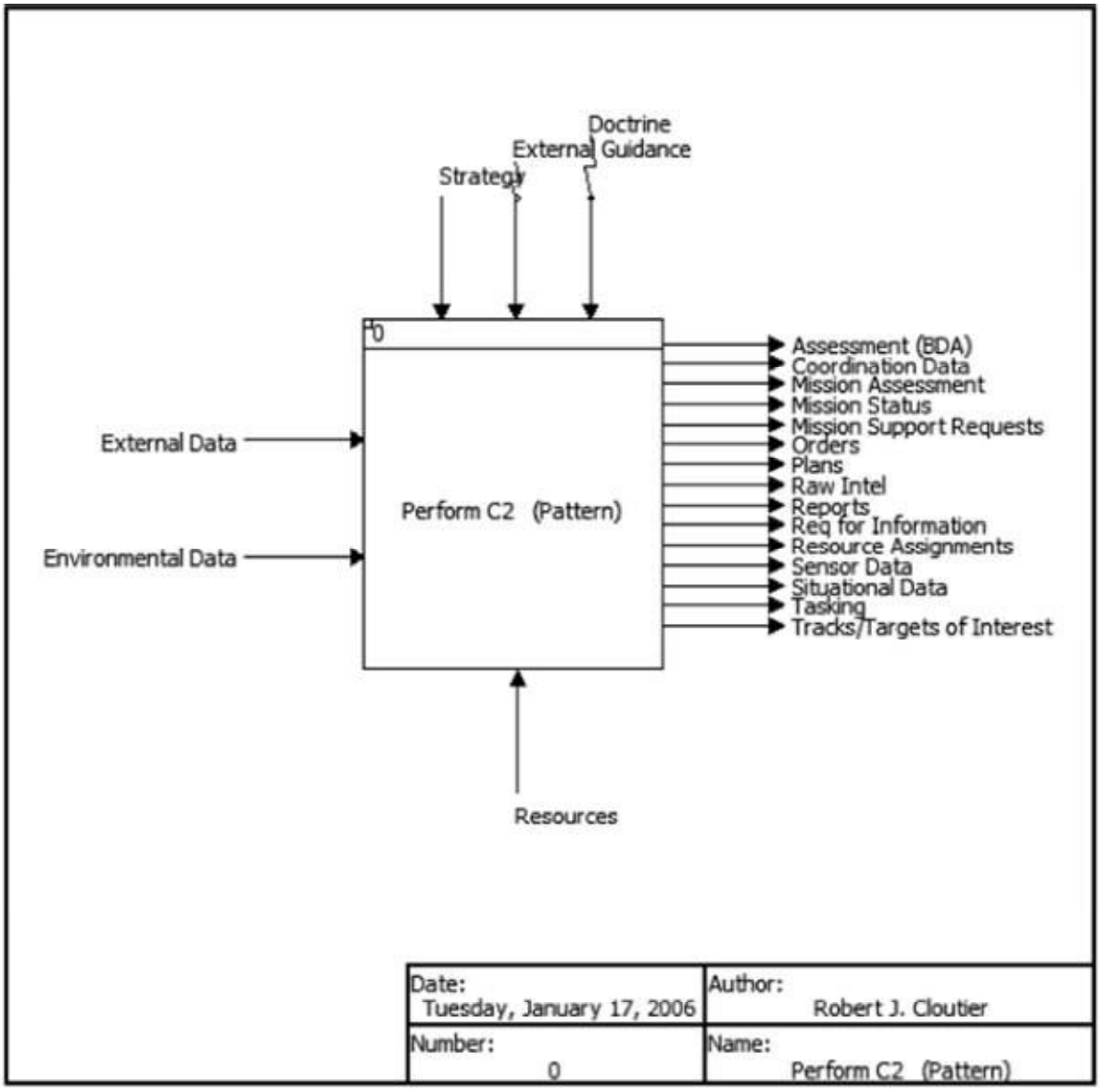

Figure 2.11. Patron de conception d'un système C2 (Cloutier & Verma, 2007).

2.5. Surveiller l'usage du système : éléments d'architecture préalables pour concevoir un système résilient

Pour développer une capacité de navigation à vue, il est nécessaire que les opérateurs sachent quel est l'état du système, dans quel environnement ils opèrent. C'est pourquoi nous décrivons ensuite les principes de système de surveillance de l'usage et de l'état d'un système (HUMS pour *healt and usage monitoring systems*) élaboré dans le domaine de la sûreté de fonctionnement, et plus particulièrement de la maintenance, susceptible de satisfaire le besoin des opérateurs de connaître l'état du système dont ils ont la charge.

2.5.1. Système de surveillance de l'usage et de l'état d'un système - HUMS- (*health and usage monitoring systems*)

Les systèmes HUMS (pour *Health and Usage Monitoring Systems*) sont élaborés et mis en œuvre pour surveiller l'état et l'usage des systèmes, en particulier pour améliorer leur fiabilité, leur disponibilité, pour optimiser la maintenance, ainsi que, dans certains cas, décider si la durée de vie opérationnelle des systèmes peut être, ou pas, prolongée, en tenant compte de leur état de vieillissement réel.

La surveillance d'un système permet « la détection des dérives de l'état de santé actuel afin de signaler l'apparition de tout comportement anormal indiquant un mode opératoire non optimal ou dégradé » (Abichou, 2013). « L'utilisateur est ainsi alerté rapidement en cas de déviation significative de l'état fonctionnel et/ou dysfonctionnel du système surveillé » (Abichou, 2013). Cette surveillance nécessite « de disposer d'informations reflétant l'état réel du système en temps réel et de façon continue » (Abichou, 2013).

Initialement élaborés dans le secteur de l'aéronautique, les HUMS sont maintenant mis en œuvre dans de nombreux secteurs dans lesquels le diagnostic sur l'état du système et le pronostic sur leur disponibilité sont des enjeux importants, tant opérationnels que financiers. L'objectif est de fournir aux utilisateurs une vision uniforme de l'état des machines (ISO, 2007). Ils sont utilisés pour la surveillance des systèmes critiques (Aubry *et al.*, 2012 ; Barros *et al.*, 2012 ; Fallet-Fidry *et al.*, 2012 ; Hartert *et al.*, 2012 ; He *et al.*, 2012 ; Sedki et al., 2012).

La surveillance des machines représente l'ensemble des données (niveau de vibration, température, pression…) reflétant les conditions d'exploitation de la machine. Les niveaux sont enregistrés et comparés aux données de référence précédemment relevées, aux alarmes préréglées ou au seuil de déclenchement. Toute modification de ces niveaux est soigneusement examinée car elle indique généralement le développement d'une anomalie néfaste pour l'état de la machine (ISO, 2003).

La connaissance de l'état de santé du « vieillissement » du système (Giraudeau, 2014) s'appuie sur les mesures de capteurs physiques, pour permettre :

- la reconstitution des stress physiques subis par le système ;
- la comparaison entre les spécifications et la réalité des stress ;
- la corrélation avec les circonstances de défaillances observées.

L'exploitation des paramètres mesurés (Giraudeau, 2014) permet la détection des anomalies, l'investigation sur les défaillances récurrentes en phase d'exploitation ainsi que la

transmission des défauts en temps réel au personnel d'exploitation et au personnel de maintenance pour anticiper et préparer les opérations de maintenance.

Les briques fonctionnelles d'un HUMS (Giraudeau, 2014) sont :

- la capture de données physiques et signaux ;
- la surveillance en permanence ;
- la détection des anomalies ;
- l'historisation des données ;
- l'extraction des données historiées (sécurité, confidentialité des données).

2.5.2. Architecture fonctionnelle d'un système de surveillance de l'usage et de l'état d'un système (HUMS)

L'architecture fonctionnelle d'un système de surveillance de l'usage et de l'état d'un système est organisée en six blocs fonctionnels de traitement distincts, structurés en couches, décrits dans les documents OSA-CBM (*Open Systems Architecture for Condition-Based Maintenance*) de l'alliance MIMOSA (*Machinery Information Management Open Standards Alliance*, wwww.mimosa.org) ainsi que dans les normes relatives à la surveillance et au diagnostic d'état des machines (ISO, 2003 ; ISO, 2007 ; ISO, 2010a). Ces six blocs sont :

- l'acquisition des données (DA pour *Data Acquisition*) dont le rôle est de convertir les résultats du conditionneur du capteur en paramètres numériques ;
- la manipulation des données (DM pour *Data Manipulation*) calcule les descripteurs significatifs à partir des données acquises ;
- la détection d'un état (SD pour *State Detection*) facilite la création et la maintenance de « profils de référence » normaux, puis la recherche des anomalies à chaque acquisition de nouvelles données et détermine à quelle zone d'anomalie éventuelle appartiennent les données collectées (alerte ou alarme) ;
- l'évaluation de l'état (HA pour *Health Assessment*) diagnostique tous les défauts et définit l'état actuel des équipements ou des procédés en tenant compte de toutes les informations d'état ;
- l'évaluation du pronostic (PA pour *Prognostic Assessment*) détermine l'état futur et les modes de défaillance d'après l'évolution de l'état actuel et les conditions d'utilisation envisagées pour les équipements et les procédés ainsi que d'après les prévisions de la vie utile restante ;
- la génération de conseils (AG pour *Advisory Generation*) fournit les informations d'actions relatives aux modifications de maintenance ou d'exploitation nécessaires à l'optimisation de la durée de vie du procédé et/ou des équipements.

L'architecture des blocs se présente alors comme décrit Figure 2.12 (ISO, 2007).

Ces six blocs de traitement sont accompagnés d'autres éléments que sont (ISO, 2003 ; ISO, 2007) :

- l'archivage des données afin d'historisation et de statistiques ;
- la configuration des blocs pour (1) l'identification des sites de surveillance, (2) l'orientation et la position relative des capteurs, (3) les données de réglage des capteurs, (4) la fréquence d'appel de la surveillance, (5) les autres paramètres pertinents d'étalonnage des blocs ;

- la fiabilisation des données sur l'ensemble de la chaîne de traitement (fiabilité des capteurs, exigences relatives à la transmission par le réseau …) ;
- les méthodes d'échange, dont le processus et le format d'accès distant aux données, d'importation et d'exportation de ces données avec un langage de requête ;
- l'affichage et la présentation des informations aux utilisateurs, détaillée dans la section 3.4.5 intitulée « Représentation de l'usage et de l'état du système via les HUMS ».

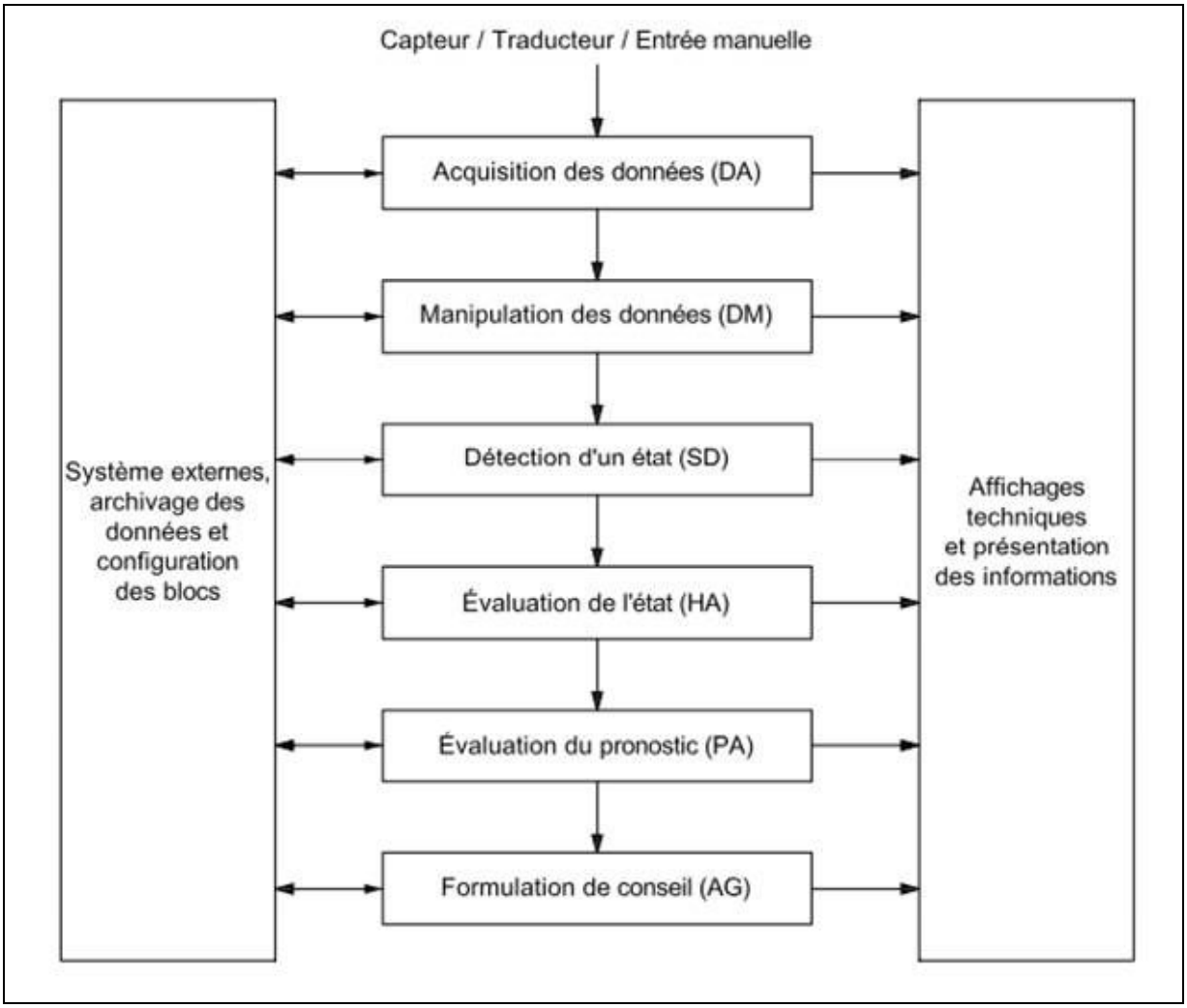

Figure 2.12. Organigramme du traitement des données[13] (ISO, 2007).

[13] « Les extraits de la norme NF ISO 13374-2 : 2007, « Surveillance et diagnostic d'état des machines, Traitement, échange et présentation des données, Traitement des données ». sont reproduits avec l'accord d'AFNOR. Seul le texte original et complet de la norme telle que diffusée par AFNOR Editions – accessible *via* le site internet www.boutique.afnor.org – a valeur normative »

2.5.3. Décrire l'usage et l'état d'un système (HUMS)

Nous détaillons maintenant le fonctionnement de ces six blocs de traitement.

Le **bloc d'acquisition** des données transforme la sortie d'un transducteur ou d'un essai échantillonné en une représentation numérique mise à l'échelle (ISO, 2007). Ce bloc :

- collecte des données analogiques, numériques ou manuelles ;
- convertit les données analogiques en données numériques.

Ce bloc est sollicité par un signal de déclenchement de commande d'acquisition de données ou par un signal de synchronisation d'acquisition de données. Il reçoit des paramètres de configuration.

Les données de sortie de ce bloc sont marquées d'un indicateur de qualité des données, par exemple : *mauvais*, *bon*, *à l'étude* ou *inconnu*.

Le **bloc de manipulation des données** calcule les caractéristiques décrivant l'état des machines à partir des données acquises du capteur échantillonné (ISO, 2007). À partir de ses paramètres de configuration, ce bloc :

- réalise le traitement du signal ;
- réalise les moyennes synchrones et asynchrones ;
- réalise des calculs algorithmiques ;
- réalise l'extraction des caractéristiques.

Le **bloc de détection d'un état** compare les valeurs de sortie des blocs d'acquisition de données et de manipulation de données à des valeurs attendues de profils de référence ou à des limites d'exploitation, afin d'émettre des indicateurs d'état avec des alertes de limite de seuil respectives (ISO, 2007). À partir de ses paramètres de configuration, ce bloc :

- calcule les valeurs courantes des indicateurs d'état et des statistiques ;
- évalue l'état courant ;
- contribue à l'évaluation d'un diagnostic, du bloc éponyme ;
- peut fournir des signaux de commande pour le module de capteur (signaux de déclenchement d'acquisition et de traitement de données).

Les sorties de ce bloc sont :

- les alertes de limite de seuil ;
- la gravité de l'écart au-dessus ou en-dessous de la limite de seuil ;
- la fréquence d'alerte ;
- le degré d'anomalie ;
- l'analyse statistique.

Le **bloc d'évaluation de l'état** met en œuvre une expertise humaine ou d'intelligence artificielle pour déterminer l'état courant de l'équipement et diagnostiquer les états défectueux existants, en fusionnant les données des blocs d'acquisition de données, de manipulation de données et de détection de l'état (ISO, 2007). À partir de ses paramètres de configuration, ce bloc :

- évalue l'état courant ;
- établit un diagnostic de défauts ou de défaillances ;

- formule des recommandations ;
- produit des preuves et des explications.

Les sorties de ce bloc sont :

- l'état, les défauts et les défaillances diagnostiqués ;
- des recommandations ;
- des preuves ;
- des explications ;
- un coefficient de criticité courant.

Le **bloc d'évaluation du pronostic** prévoit l'état futur de l'équipement surveillé en combinant des modèles de pronostic et leurs algorithmes, y compris les modèles d'exploitation opérationnelle future envisagés en fonction de l'historique d'exploitation (ISO, 2007). À partir de ses paramètres de configuration, ce bloc :

- évalue l'état futur ;
- prévoit les défauts et défaillances ;
- évalue la durée de vie restante ;
- formule des recommandations ;
- produit des preuves et des explications ;
- calcule le coefficient de criticité futur.

Les sorties de ce bloc sont :

- l'état futur ;
- la durée de vie restante ;
- des recommandations ;
- des preuves et explications ;
- le niveau de confiance ;
- le coefficient de criticité futur.

Le **bloc de génération de conseils** produit des recommandations d'actions et des solutions alternatives en tenant compte de l'historique d'exploitation, y compris d'utilisation et de maintenance, des profils de mission courants et futurs, des objectifs assignés et des contraintes de ressources (ISO, 2007). À partir de ses paramètres de configuration, ce bloc :

- intègre les informations pour formuler des conseils relatifs à l'exploitation et à la maintenance ;
- notifie des alertes aux opérateurs d'exploitation et de maintenance.

Les sorties de ce bloc sont :

- des conseils ;
- les alertes.

2.5.4. Paramètres pour la surveillance de l'usage et l'état d'un système (HUMS)

Après avoir détaillé les six blocs de fonctions, nous précisons les activités à mener à bien pour surveiller l'état d'un système. Il est nécessaire de commencer par identifier les fonctions et

équipements à surveiller selon leur criticité, d'élaborer un schéma synoptique de la fiabilité (taux de défaillance, temps moyen de réparation, redondance, dommages consécutifs ou indirects) en précisant les conditions de fonctionnement ainsi que les plages de fonctionnement des fonctions et des équipements, d'identifier les modes de défaillance, leurs effets et leur criticité (ISO, 2010a). Dès lors qu'ils sont mesurables, il faut identifier les paramètres à mesurer en établissant un ordre de priorité, sélectionner les techniques de mesurage en tenant compte de la sensibilité de la mesure par rapport aux paramètres à mesurer et de la fiabilité des mesures, les emplacements où sont réalisées les mesures, de caractériser les conditions des défauts (augmentation, diminution ou autre variation de valeurs particulières), de définir, régler ou réviser les critères d'alarme ainsi que la fréquence de surveillance (échantillonnage continu ou périodique). En cours d'opération, après avoir exécuté les mesures et lu les tendances, la comparaison des paramètres mesurés aux critères d'alerte/d'alarme permet de déterminer les actions de maintenance à réaliser.

Les critères initiaux d'alerte/d'alarme doivent être fixés de manière à signaler l'occurrence d'un défaut dès que possible (ISO, 2010a). Les critères d'alerte/d'alarme peuvent être des valeurs simples ou des niveaux multiples, croissants ou décroissants. De même, ils peuvent être le résultat de traitement de plusieurs mesures. Les valeurs de référence sont issues de données mesurées ou observées dans des conditions de fonctionnement réputées comme admissibles et stables (ISO, 2010a). Des mesures ultérieures peuvent être comparées à ces valeurs de référence afin de déceler des changements. Les mesures peuvent être effectuées en ligne ou hors ligne et comprendre des données collectées lors de rondes, des enregistrements ainsi que les tendances de mesure (ISO, 2010a). Lorsque les valeurs mesurées sont acceptables comparées aux critères d'alerte/d'alarme, aucune action n'est nécessaire excepté l'enregistrement des valeurs et la poursuite de la surveillance. Lorsque les valeurs mesurées ne sont pas acceptables comparées aux critères d'alerte/d'alarme, il convient de déclencher un processus de diagnostic (ISO, 2010a).

Le processus de diagnostic est déclenché par la détection d'une anomalie. Cette détection est le résultat d'une comparaison entre les descripteurs courants d'une machine ou d'une comparaison avec des machines similaires ou sélectionnées sur la base de l'expérience, des spécifications du fabricant, des essais de mise en service calculés sur la base de données statistiques, par exemple, une moyenne à long terme (ISO, 2010a).

Lorsqu'un critère d'alerte/d'alarme est atteint, les décisions types (ISO, 2010a) sont :

- aucune action, poursuivre la surveillance programmée ;
- réduire l'intervalle avec la mesure nécessaire suivante ;
- modifier, en diminuant ou augmentant, la charge, la vitesse ou le débit de la machine ;
- arrêter la machine ;
- inspecter la machine ou avancer la maintenance programmée ;
- effectuer une maintenance corrective.

Enfin, il est recommandé d'enregistrer toutes les activités de maintenance réalisées et les changements apportés aux machines, y compris les détails relatifs aux pièces de rechange utilisées, les procédés appliqués et les connaissances mises en œuvre (ISO, 2010a) pour établir et mettre à jour un historique qui facilitera les diagnostics et pronostics ultérieurs.

Nous remarquons que ces documents présentent les activités pour identifier les paramètres à mesurer, les fréquences de mesure, les critères d'alerte, ainsi qu'un exemple d'affichage (cf. section 3.4.5 « Représentation de l'usage et de l'état du système via les HUMS »), mais sont muets sur les activités de conception centrée utilisateurs pour identifier les paramètres à

représenter sur l'interface utilisateur et l'adaptation de cette représentation au contexte d'usage (tâche, modèle de l'utilisateur, dispositif d'interface mis en œuvre).

2.6. Synthèse et conclusion du chapitre

Dans ce chapitre, nous avons présenté les définitions et concepts des systèmes, les processus d'ingénierie, en particulier le processus d'opération. Dans ce dernier, il est mentionné une exigence de surveiller les services fournis par le système, ainsi que les performances. Cette surveillance du système en opération consiste à examiner si les performances s'inscrivent au sein de bornes acceptables. Dans le cas contraire, lorsque les performances sont hors des bornes acceptables, il est nécessaire d'identifier, de tracer et d'enregistrer ces performances, les accidents et les problèmes rencontrés afin d'effectuer une analyse des causes racines des accidents.

En vis-à-vis de cette exigence de surveillance du système en opération, la mise en œuvre d'un système de surveillance de l'état et de l'usage du système d'intérêt permet de détecter les dérives de l'état de santé actuel afin de signaler aux opérateurs l'apparition de tout comportement anormal. Les opérateurs sont rapidement alertés en cas de déviation significative du système surveillé et de son état. Cette surveillance nécessite de disposer d'information reflétant l'état réel du système en temps réel et de façon continue.

Intégrer un tel système de surveillance implique de modéliser et de faire évoluer les architectures fonctionnelle et physique du système d'intérêt. Le langage de modélisation SysML permet d'effectuer ces modélisations de ces architectures

La prochaine étape est de représenter cet usage et cet état du système aux opérateurs de façon appropriée à leur tâche, à leur environnement, entre autres. C'est ce point que nous abordons dans le Chapitre 3 intitulé « Éléments d'ergonomie et d'ingénierie des IHM : conception centrée utilisateur et architecture des systèmes interactifs ».

Chapitre 3.

Éléments d'ergonomie et d'ingénierie des IHM : conception centrée utilisateur et architecture des systèmes interactifs

3.1. Introduction

L'interaction homme-machine articule plusieurs disciplines différentes, des sciences et techniques de l'ingénieur, d'un côté, des sciences humaines, d'un autre côté, pour formuler un corpus conceptuel, théorique et méthodologique cohérent pour concevoir et évaluer les systèmes interactifs.

De nombreux sites, de recherche, professionnels, associatifs, sont consacrés à ce sujet, dont celui du SIGCHI[14] (*Special Interest Group on Computer–Human Interaction*) de l'ACM (*Association for Computing Machinery*) et celui de l'AFIHM[15] (Association Francophone d'interaction Homme-Machine). Le site *HCI Bibliography : Human-Computer Interaction Resources* (http://hcibib.org/) comprend des ressources riches et variées.

Plus largement, un site gouvernemental américain (http://www.usability.gov/) est dédié à ce sujet, sous le terme d'utilisabilité (*usability*). Ce site, de large audience, présente des méthodes et outils pour la conception dite centrée utilisateur ou sur l'utilisateur (ou sur l'opérateur humain), ainsi que des outils pour calculer le retour sur investissement de la conception de ce type. Le domaine est vaste et nous nous limitons à présenter les thèmes adaptés à notre problématique.

Après avoir présenté la définition et les principaux concepts de l'interaction homme-machine, à l'instar de la différenciation définie entre processus et architecture (cf. Chapitre 2 intitulé « Ingénierie Système appliquée aux systèmes critiques »), nous différencions, d'une part, les processus et méthodes de conception centrée utilisateur, et, d'autre part, l'architecture des systèmes interactifs.

Une première étape consiste à modéliser l'utilisateur. En complément de cette première étape, dans les contextes pour lesquels cette modélisation d'un utilisateur n'est pas suffisante, la notion de persona, que nous présentons dans la section « Persona individuel / collectif » de ce chapitre, permet d'élaborer une représentation fictive de l'utilisateur, d'une classe d'utilisateurs, voire un groupe d'utilisateurs collaborant dans une activité collective. Nous poursuivons en modélisant la tâche de l'utilisateur, ainsi qu'en présentant l'ergonomie prospective pour prendre en compte l'inscription de l'ergonomie dans la durée, caractéristique des systèmes à longue durée de vie. Nous terminons cette section consacrée au processus de conception en présentant le processus d'appropriation, c'est-à-dire la façon dont les utilisateurs s'approprient un nouveau dispositif, adaptant leur activité, mais aussi adaptant ce nouveau dispositif dans le cadre de leur activité.

La section concernant l'architecture des IHM présente la modélisation de cette architecture, puis des modèles d'architecture en IHM. Elle se poursuit en traitant l'architecture pour les

[14] Site SIGCHI : http://www.sigchi.org/

[15] Site AFIHM : http://afihm.org/

IHM distribuées puis la conception orientée aspect. Elle se termine par un exemple de représentation de l'usage et de l'état suggéré par la norme consacrée aux HUMS (ISO, 2003).

3.2. Définition et concepts de l'interaction homme-machine

L'interaction homme-machine forme une discipline visant à concevoir, réaliser et évaluer des systèmes de traitement de l'information interactifs pour les êtres humains, faciles et agréables à utiliser, performants, efficients. La définition ci-dessous est celle du SIGCHI.

Définition : *Human-computer interaction* (interaction homme-machine)

Human-computer interaction is a discipline concerned with the design, implementation and evaluation of interactive computing systems for human use and with the study of major phenomenon surrounding them (définition de ACM SIGCHI).

Les principaux concepts des interactions homme-machine concernent, d'une part, les caractéristiques des utilisateurs (novice, expert…), leurs tâches (professionnelle, domestique, ludique), les environnements dans lesquels ils mettent en œuvre les systèmes interactifs (mobilité…), et, d'autre part, les modalités d'interaction (interface haptique, interface vocale, interface tangible, réalité augmentée…), les dispositifs d'entrée et de sortie des systèmes interactifs (souris, clavier, gant numérique…), l'architecture de ces systèmes interactifs. Plus largement, ils concernent aussi les systèmes multimodaux et multimédia, les systèmes qualifiés d'adaptatifs, d'intelligents ou encore sensibles au contexte, d'aide aux utilisateurs, par exemple au profit de personnes handicapées, les systèmes collaboratifs et les réseaux sociaux. Au-delà des systèmes technologiques, les interactions homme-machine concernent aussi les bonnes pratiques, les méthodes, modèles et outils de conception et d'évaluation de ces interactions homme-machine. Les domaines d'application sont vastes et variés, et les normes de plus en plus nombreuses (cf. à ce sujet par exemple la section 3.3 ci-dessous). Enfin, de volumineux manuels sont publiés et régulièrement réédités (Helander *et al*., 1997 ; Shneiderman & Plaisant, 2009 ; Sears & Jacko, 2012).

3.3. Processus de conception centrée utilisateur

Le processus de conception centrée utilisateur fait appel à des principes et met en œuvre des activités spécifiques formalisés dans la norme intitulée « Conception centrée sur l'opérateur humain pour les systèmes interactifs » (ISO, 2010b).

Cette norme (ISO, 2010b) énonce les principes de la conception centrée utilisateur suivants :

- « la conception est basée sur une compréhension explicite des utilisateurs, des tâches et des environnements ;
- les utilisateurs sont impliqués dans la conception et le développement ;
- la conception est dirigée et précisée par l'évaluation centrée sur l'utilisateur ;
- le processus est itératif ;
- la conception couvre l'expérience de l'utilisateur dans son intégralité ;
- l'équipe de conception inclut des compétences et des points de vue pluridisciplinaire ».

Cette norme (ISO, 2010b) décrit les activités suivantes :

- comprendre et spécifier le contexte d'utilisation, c'est-à-dire décrire le contexte d'utilisation, de façon suffisamment détaillée pour rendre la conception possible ;
- spécifier les exigences utilisateur, c'est-à-dire identifier les besoins de l'utilisateur et des autres parties prenantes, spécifier les exigences utilisateur, spécifier les tâches, trouver le compromis entre les exigences utilisateur, assurer la qualité de la spécification des exigences utilisateur ;
- (1) produire des solutions de conception, c'est-à-dire concevoir l'interaction et l'interface utilisateur, afin de satisfaire aux exigences exprimées, (2) matérialiser les solutions de conception, (3) effectuer des évaluations formatives avec les utilisateurs, en mettant en œuvre les méthodes d'évaluation centrée sur l'utilisateur adaptées au contexte d'usage et au projet, et (4) modifier ces solutions de conception sur la base des résultats des évaluations formatives ;
- effectuer une évaluation sommative mettant en évidence la satisfaction du besoin exprimé.

Des travaux ont été menés, d'abord pour articuler les activités de la conception centrée utilisateur avec les activités du génie logiciel (Barthet, 1988 ; Lim & Long, 1994) et de la gestion de projet. Ces travaux se poursuivent en articulant les activités de la conception centrée utilisateur avec les processus et activités de l'ingénierie système (Ruault, 2004 ; Pew & Mavor, 2007 ; ASD-STAN 2013 ; Boy & Narkevicius, 2014).

La Figure 3.1 montre la correspondance entre les processus techniques de la norme ISO/IEC 15288, dans son édition de 2008, avec les activités de la norme ISO 9241-210. Cette démarche vise à faciliter la mise en œuvre de la conception centrée sur l'utilisateur humain au profit des systèmes complexes mettant en œuvre les processus d'ingénierie système.

Processus UCD ISO 9241-210	**Processus du cycle de vie du système** – ISO/CEI 15288:2008										
	Processus de définition des exigences des parties prenantes	Processus d'analyse des exigences	Processus de conception d'architecture	Processus de mise en œuvre	Processus d'intégration	Processus de vérification	Processus de mise à disposition	Processus de validation	Processus opérationnel	Processus d'entretien	Processus de mise au rebut
Comprendre et spécifier le contexte d'utilisation	☑	☑						☑	☑		☑
Spécifier les exigences de l'utilisateur et d'organisation	☑	☑						☑	☑	☑	☑
Produire des solutions de conception	☑	☑	☑	☑							
Evaluer la conception par rapport aux exigences	☑	☑				☑		☑	☑		

Figure 3.1. Grille de correspondance des processus techniques de l'ISO/CEI 15288:2008 et des activités de l'ISO 9241-210 (ASD-STAN, 2013).

Cette norme (ISO, 2010b) préconise de comprendre les exigences des utilisateurs, il s'avère nécessaire de les caractériser afin de concevoir un système satisfaisant leur besoin.

3.3.1. Modèle de l'utilisateur

L'une des premières activités de la conception centrée sur l'utilisateur humain est de caractériser les utilisateurs du système à concevoir, ainsi que le contexte dans lequel les utilisateurs mettront en œuvre ce système.

Caractériser les utilisateurs, c'est identifier qui ils sont, leur âge, leur genre, leurs compétences dans le domaine d'application du système à concevoir, leurs habilités avec les dispositifs des systèmes de traitement de l'information interactifs, mais aussi leur(s) éventuel(s) handicap(s), ainsi que les croyances et pratiques culturelles qui sont les leurs (Vaske & Grantham, 1990 ; Helmreich & Merritt, 1998). Autant de caractéristiques nécessaires à prendre en compte pour que le système à concevoir réponde aux besoins, soit adapté aux utilisateurs et facile et agréable à utiliser, en leur procurant une bonne expérience utilisateur. C'est aussi s'appuyer sur des données démographiques, sociologiques, économiques, des études de marché pour tracer et justifier les exigences et les implications pour l'interface utilisateur (Robert, 2003). C'est enfin prendre les utilisateurs dans leur contexte, dans la mesure où ils sont fortement influencés par les systèmes qu'ils utilisent et qu'ils pensent en termes de logique d'utilisation (Barthet, 1988 ; Robert, 2003).

La première source concernant les caractéristiques des utilisateurs provient de l'analyse de l'activité laquelle exploite des données empiriques (Leplat & Hoc, 1983 ; Leplat, 2002). Les études en ergonomie, plus largement dans le domaine des sciences humaines et sociales, ont produit de nombreuses données pour caractériser les utilisateurs. En particulier, les données anthropométriques permettent de rendre compte de la diversité des utilisateurs, mais aussi permettent de spécifier le système afin qu'il soit adapté aux utilisateurs identifiés. C'est par exemple le cas d'un système de drone aérien conçu et mis en œuvre au Royaume-Uni. Kirke (Kirke, 2004 ; Kirke, 2005), mais aussi du siège éjectable de l'avion Rafale. Ces modèles des utilisateurs prennent aussi en compte les éléments physiologiques qui ont des impacts sur l'utilisation du système à concevoir, que ce soit le stress, la fatigue, ainsi que le cycle circadien.

3.3.2. Persona individuel / collectif

Les méthodes pour caractériser l'utilisateur, présentées dans le section précédent, se caractérisent par l'absence de prise en compte (Broadbent, 2010 ; Cahour & Lancry, 2011 ; Karsenty, 2011) : 1) des dimensions sociales et émotionnelles ayant des impacts sur les activités des opérateurs, sur les performances et sur la sécurité ; 2) des aspects intimes des opérateurs qui ont des impacts sur leurs activités ; 3) des caractéristiques de futurs utilisateurs pour lesquels il n'est pas possible de disposer de données empiriques (par exemple les opérateurs qui exploiteront dans 20 ans les systèmes conçus actuellement) ; 4) de la dynamique des organisations.

Les tentatives d'introduire des caractéristiques plus fines dans la notion générique d'utilisateur et le développement de la notion d'expérience utilisateur (ISO, 2010) ont contribué à la définition d'un concept et d'une méthode permettant de résoudre ces difficultés. Ce sont ceux de persona. Ils ont d'abord été utilisés dans le domaine du marketing et sont maintenant mis en œuvre pour la conception des IHM, avec pour objectif d'incarner les futurs utilisateurs du système, de prendre en compte l'ensemble des points structurant dans la conception des IHM et de stimuler les idées des concepteurs (Courage & Baxter, 2005 ; Brangier *et al.*, 2011). Cette démarche complète les analyses de l'activité menées en prenant en compte les caractéristiques ci-dessus, et ne s'y substitue pas. Le persona complète le

modèle de l'utilisateur, en particulier pour synthétiser les caractéristiques structurantes des utilisateurs modélisées dans des scénarios d'usage.

Le persona est la représentation fictive et simplifiée, d'un utilisateur (opérateur, agent de maintenance, agent de maîtrise...), ou d'une classe d'utilisateurs du futur système dans une situation où, pour des raisons éthiques ou matérielles, il n'est pas possible de faire appel à des êtres humains en chair et en os, pour mener des analyses ou des expérimentations. Dans la mesure où plusieurs utilisateurs ou classes d'utilisateurs ont des liens, à un titre ou à un autre, avec le système, il y a autant de personas différents qu'il y a d'utilisateurs ou de classes d'utilisateurs différents. Le persona synthétise les traits dimensionnant et structurant des objectifs, des comportements et des caractéristiques des utilisateurs, complétant les méthodes de l'ergonomie l'IHM et les formalismes existants (Pruitt & Adlin, 2006).

Le persona est conforme aux principes et critères de conception centrée sur l'humain (ISO, 2002 ; ISO, 2010b). Il peut être élaboré à partir de données d'enquêtes, d'entretiens, d'observations, d'analyse de l'activité et d'analyse des traces, entre autres. Il peut être complété par les résultats de rapports d'enquête technique faisant suite à des accidents (Ruault *et al.*, 2012). Enfin, il peut être enrichi de données prospectives, en particulier lorsque le système est nouveau ou présente une longue durée de vie, ce qui fait que les futurs utilisateurs peuvent être différents des utilisateurs actuels. Dans les cas où l'âge du départ à la retraite est retardé, le persona permet de représenter un utilisateur âgé dans une situation de travail. Le persona complète les modèles des utilisateurs, avec des informations sur les attitudes, l'intimité (Broadbent, 2011), sur la confiance envers autrui (Karsenty, 2011). Les différentes caractéristiques qui peuvent être intégrées dans un persona sont décrites dans plusieurs articles (Brangier & Bornet, 2009 ; Idoughi *et al.*, 2010 ; Idoughi *et al.*, 2012 ; Pruitt & Adlin, 2006 ; Seffah *et al.*, 2009).

Cette première analyse nous permet de montrer que les caractéristiques du persona complètent les principales caractéristiques de l'utilisateur ou de l'opérateur des autres démarches d'ergonomie. Des dimensions telles que des relations sociales extra-professionnelles, des relations de séduction peuvent influencer l'activité des opérateurs (Helmreich & Merritt, 1998 ; Rosnet *et al.*, 2004 ; Ruault *et al.*, 2012).

L'expression d'un persona peut être formulée sous forme tabulaire, comprendre une photographie, pour donner plus de réalité au persona, ou tout autre élément incarnant l'utilisateur. Elle peut être formulée sous une forme narrative, propice à être intégrée dans un scénario. Enfin, comme le suggèrent Idoughi (Idoughi *et al.*, 2010 ; Idoughi *et al.*, 2012), elle peut s'appuyer sur les méthodes et outils du génie logiciel, dont le diagramme des cas d'utilisation enrichi des caractéristiques de la notion d'acteur (Ruault & Van Eylen, 1997).

Les différentes caractéristiques qui peuvent être intégrées dans un persona selon (Brangier *et al.*, 2011), principalement, ainsi que (Idoughi *et al.*, 2010 ; Idoughi *et al.*, 2012 ; Pruitt & Adlin, 2006 ; Seffah *et al.*, 2009) sont les suivantes :

- données personnelles / identité : photographie, nom, prénom, date de naissance, lieu de naissance, nationalité, adresse postale, adresse électronique ;
- données physiologiques : sexe, âge, poids, handicap physique ;
- personnalité : type de personnalité, sexualité, objectifs personnels, amertume, croyances, attitudes, loisirs pratiqués ;
- socialité : besoin de leadership, ambition sociale, appartenance à des réseaux sociaux, influence sociale ;

- données économiques et financières : statut professionnel, classe sociale, revenus, propriétaire /locataire de son logement ;
- mode de vie : type d'habitat, mode de vie urbain ou rural ;
- formation, compétences, habiletés : formation initiale, formation professionnelle, compétences professionnelles, compétences linguistiques ;
- contexte de l'activité : activité professionnelle/ domestique, contraintes de sécurité/réglementaires, fréquence d'usage, niveau de difficulté de l'activité, disponibilité d'aide et de documentation, niveau d'activité (novice/confirmé/expert).

Un persona collectif est un ensemble de différents persona individuels qui communiquent et agissent ensemble au sein d'un groupe, d'une organisation (Gibouin, 2011 ; Matthews *et al.*, 2011 ; Judge *et al.*, 2012). La communication est l'un des enjeux du persona collectif puisqu'elle permet à ces différents personas individuels de partager l'information, de se coordonner afin de collaborer. Chaque persona individuel élabore ses représentations et croyances, à propos de son environnement, de ses activités, et de la situation spécifique à laquelle il fait face. Afin de se coordonner, les personas individuels doivent communiquer et se comprendre.

3.3.3. Modèle de la tâche

Le modèle de la tâche prescrit la façon dont les futurs utilisateurs sont supposés mettre en œuvre le système à concevoir, les procédures à suivre. Il s'appuie sur l'analyse de l'activité (Leplat & Hoc, 1983, Leplat, 2002). Il existe de nombreuses propositions dans la littérature pour la modélisation des tâches humaines (Diaper et Stanton, 2004).

La décomposition hiérarchique de la tâche (*Hierarchical Task Analysis*) (Annett & Duncan, 1967) a ouvert la voie à de nombreuses méthodes de modélisation de la tâche, dont MAD (Méthode Analytique de Description des tâches) (Scapin & Bastien, 2001) et son évolution K-MAD (Baron *et al.*, 2006), ou encore Diane (Barthet, 1988). La tâche est décrite en termes d'objectifs et d'actions à mener pour atteindre les objectifs. Ces actions sont organisées avec des liens logiques et temporels (alternative, parallélisme, itération ...) entre elles. Les pré-conditions pour mettre en œuvre une tâche, son état final, ses attributs (itérative, interruptible, ou non, prioritaire, optionnelle), mais aussi sa fréquence de mise en œuvre, sont exprimées sous plusieurs formes, tabulaire ou graphique. Ces modélisations de la tâche permettent de rendre compte de tâches concurrentes, par exemple ConcurTaskTrees (Paternò, 2004). La Figure 3.2 illustre la modélisation de tâches concurrentes.

L'analyse des fonctions cognitives (Boy, 1998) permet de concevoir des IHM complexes pour des situations de travail critique, à haut risque (systèmes dynamiques très contraints). Les fonctions cognitives sont dérivées d'une analyse conjointe de la tâche et de l'activité. Les descripteurs de la fonction cognitive permettent de la caractériser. Les fonctions cognitives identifiées sont ventilées selon les quatre dimensions suivantes :

- les exigences de la tâche ;
- le « background » de l'utilisateur et la complexité de l'artefact, du système sur lequel l'opérateur agit ;
- les buts de l'utilisateur, ses intentions d'actions ;
- les évènements extérieurs, les actions réactives.

Les blocs d'interaction proposent un canevas et une représentation cognitive pour décrire les dialogues homme-machine (Boy, 1998). Nous retrouvons dans ces blocs d'interaction les informations structurantes de la tâche (Boy, 1998) :

- une description de la situation initiale ;
- les pré-conditions qui déclenchent le processus ;
- l'action réalisée ;
- la description du contexte ;
- les conditions anormales de fin ;
- une indirection vers les stratégies mises en œuvre dans le cas de fin anormale ;
- le but à atteindre ;
- la stratégie normale à déclencher en fin de bloc.

Aux liens logiques et temporels de l'analyse hiérarchique de la tâche, Boy (1998) ajoute des informations adaptées pour la conception d'IHM de systèmes complexes. En particulier, il prend en compte les exceptions, les conditions anormales (actions erronées de la part de l'utilisateur), ainsi que les actions de récupération. Enfin, Boy (1998) met en évidence le besoin de conscience de la situation dans des environnements dynamiques, particulièrement avec une forte pression temporelle.

Les modèles de la tâche peuvent être traduits à l'aide de technique de modélisation très utilisés en génie logiciel, par exemple les cas d'utilisation d'UML (Ruault & Van Eylen, 1997), ou les réseaux de Pétri (Palanque & Bastide, 1997 ; Abed *et al.*, 2001), pour en faciliter l'appropriation par les ingénieurs en charge de la spécification et de la conception du futur système. Le langage UML a été étendu pour modéliser les tâches et les systèmes interactifs (Roberts *et al.*, 1998 ; Nunes & Cunha, 2001 ; Ruault, 2002).

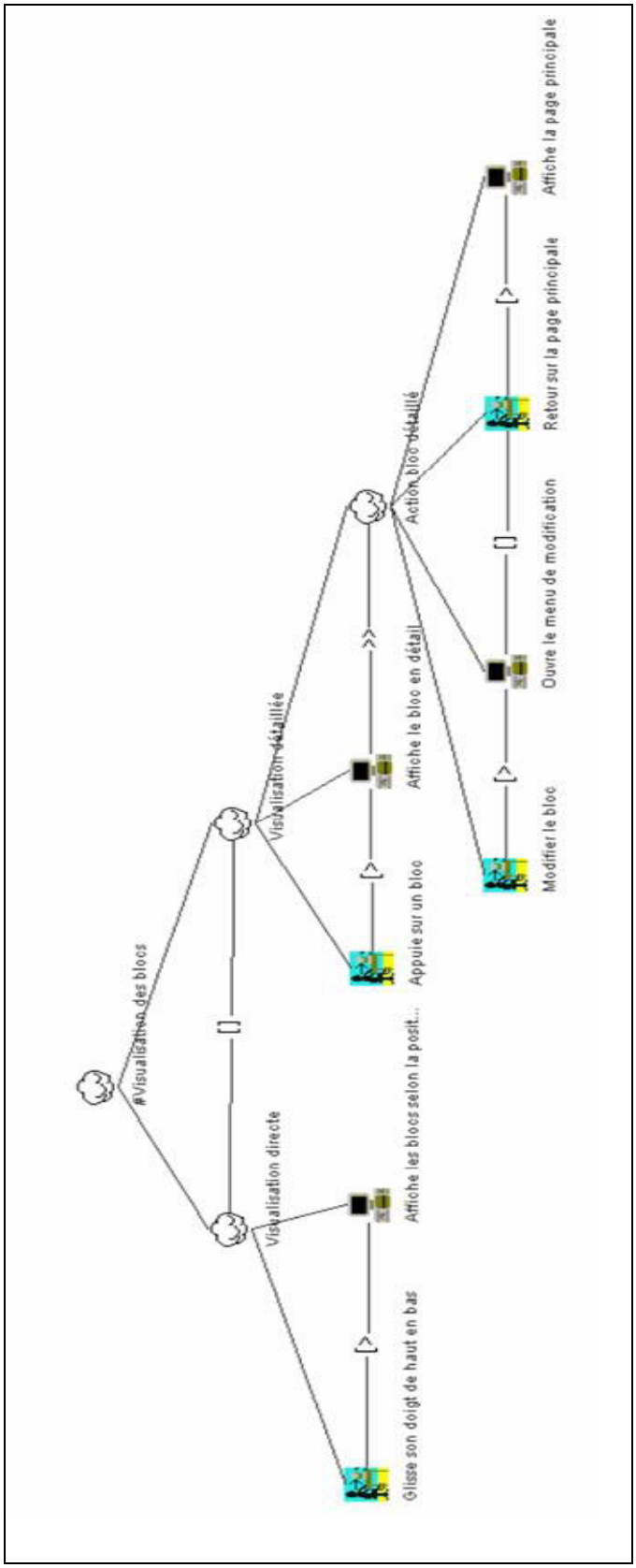

Figure 3.2. Exemple de modèle de tâche avec ConcurTaskTrees (Gruchociak & Rosa, 2004).

3.3.4. Ergonomie prospective

Complétant l'ergonomie corrective et l'ergonomie préventive (de conception), l'ergonomie prospective (Robert & Brangier, 2009) est la partie de l'ergonomie qui a pour objectif d'anticiper les besoins et les activités des êtres humains dans le but de créer de nouveaux artefacts qui seront utiles et fourniront une expérience positive aux utilisateurs. Elle met en œuvre les concepts et méthodes classiques de la conception centrée sur l'utilisateur, en mettant l'accent sur l'investigation sur l'usage d'artefacts pour découvrir leur force(s) et faiblesse(s), les sources de satisfaction et d'insatisfaction, qui peuvent mener à améliorer les artefacts et la conception d'artefacts nouveaux. C'est une approche interdisciplinaire mettant en œuvre les théories, modèles, méthodes et outils des sciences humaines et sociales pour anticiper et définir les besoins et activités des êtres humains ; sans prétendre être exhaustif : anthropologie, sociologie, ethnographie, psychologie, marketing sont impliqués (Robert & Brangier, 2009). Ces auteurs comparent l'ergonomie prospective à l'ergonomie corrective et à l'ergonomie préventive sur un ensemble de dimensions. Nous compléterons cette structuration dans notre proposition en section 6.3 du Chapitre 6 intitulée « Contribution du processus d'appropriation à l'ergonomie prospective » afin de prendre en compte les systèmes à longue durée de vie.

Représenter une situation nouvelle du monde réel à horizon de 20 ans est difficile, *a fortiori* quand l'horizon est encore plus lointain (Nelson *et al.*, 2012). La conception de scénario d'usage aide à anticiper l'usage futur de nouveaux produits et services en prenant en compte l'acceptation de ces nouveaux produits et services, ainsi que leur appropriation. Mais la portée de cette anticipation est réduite et ne couvre pas les 50 ans voire plus de service actif.

L'ergonomie prospective peut se nourrir d'études de prospective, à l'instar de l'étude « Forces terrestres futures » menée par le Ministère de la défense (Rapport FTF 2025, 2010). Cette étude esquisse le portrait type des personnels de l'Armée de terre à l'horizon 2025. Elle met en exergue les facteurs qui dimensionnent le plus, en prenant en compte les évolutions possibles de l'environnement, en élaborant un scénario de référence et des ruptures possibles et en évaluant leurs impacts sur les ressources humaines.

La prospective ergonomique, appliquée aux systèmes à longue durée de vie, concerne des opérateurs qui, pour certains, ne sont pas encore nés lors des stades amont des programmes, lorsque l'on conçoit ces systèmes. Il s'avère difficile de les impliquer dans la conception de ces systèmes, ainsi que le préconisent les principes de conception centrée sur l'humain. Mais il ne faut pas pour autant les écarter, les ignorer. Le persona, en tant que représentation abstraite, fictive, d'un utilisateur ou d'une classe d'utilisateur, s'avère être pertinent pour les prendre en compte. Le persona peut être enrichi de données prospectives. Ce point sera détaillé dans le Chapitre 6 intitulé « Proposition de processus à mettre en œuvre pour contribuer à la résilience d'un système ».

3.3.5. Processus d'appropriation

Au fil du temps, de nouvelles technologies apparaissent, que les opérateurs s'approprient ou pas. Elles peuvent perturber l'activité des opérateurs en générant des doubles tâches entravant l'activité (Ruault *et al.*, 2012, NTSB, 2010), mais aussi peuvent contribuer à améliorer les performances et la sécurité en accroissant la conscience partagée de la situation et en réduisant les délais d'intervention lors de situation de crise (Luzeaux, 2011).

Les utilisateurs peuvent détourner de leurs fonctions initiales les dispositifs qu'ils utilisent à un autre usage. C'est ainsi que le message de service (SMS) dans le domaine des

télécommunications a été détourné de sa fonction initiale (message d'information de l'opérateur téléphonique à ses clients) pour devenir un mode de communication complémentaire à la voix entre les clients des différents opérateurs téléphoniques et une ressource financière importante pour ces opérateurs dans la mesure où le coût d'acheminement des SMS est très réduit pour ces opérateurs. En effet, les SMS sont transportés par les canaux de signalisation sans consommer la bande passante allouée à la voix. Un autre exemple de détournement fonctionnel est celui de l'utilisation du radar pour cuire des œufs[16], durant la seconde guerre mondiale, à l'origine de l'invention du four à micro-ondes.

Fidock et ses collègues (2008, 2010) définissent « l'appropriation comme un processus dans lequel une technologie est explorée, évaluée et adoptée ou rejetée par les utilisateurs. Les résultats de ce processus, sont soit l'appropriation, c'est-à-dire que la technologie est adaptée et intégrée dans l'activité quotidienne des utilisateurs, soit le rejet, lorsque les utilisateurs n'utilisent la technologie ou cessent de l'utiliser. La compréhension, par le concepteur, du processus d'appropriation du système par les utilisateurs et de l'utilisation qu'ils en font, lui fournit un éclairage sur pourquoi et comment le système est transformé par l'usage ». Fidock et ses collègues (2008, 2010) montrent comment l'usage et la technologie interagissent en tenant compte des contingences du contexte opérationnel et évoluent en fonction de ces interactions. Les caractéristiques de la technologie ne sont pas stables mais dépendent de la pratique. De plus, la technologie n'est pas nécessairement utilisée selon les intentions de son concepteur.

La technologie telle que conçue (*technology-as-design*) fait référence aux artefacts technologiques qui sont fournis aux utilisateurs. Ils sont conçus à partir du modèle implicite, ou explicite, que le concepteur se fait des utilisateurs et de l'utilisation qu'ils sont supposés avoir de ces artefacts. Nous retrouvons cette différenciation entre modèle du concepteur et modèle de l'utilisateur dans les travaux de Barthet (1988) et Norman (1988) ainsi que la différenciation entre tâche et activité, entre prescrit et réel (Leplat, 1985 ; Lundberg, 2009). Ces artefacts comprennent des règles sur la façon de mener les activités, des ressources qui doivent être utilisées, des compétences que les opérateurs sont supposés maîtriser, des caractéristiques que les opérateurs sont supposés avoir. Ces artefacts offrent un ensemble de possibilités d'usage aux utilisateurs.

L'évaluation *a priori* fait référence aux attentes positives ou négatives des utilisateurs, quant aux fonctionnalités de ces artefacts, à leur facilité d'usage, ou à d'autres critères tels qu'esthétiques ou de mode, avant même qu'ils puissent les tester. Cette évaluation *a priori* peut déboucher sur le choix de ne pas adopter ces artefacts, ou de les essayer et de les utiliser. La non adoption n'est pas définitive puisque de nouvelles informations peuvent amener les utilisateurs à réviser leur position et à faire une nouvelle évaluation *a priori*.

Le processus d'appropriation décrit la découverte en mode interactif et itératif de ces artefacts par les utilisateurs. Les utilisateurs apprennent à utiliser ces artefacts, adaptent leur pratique à ces artefacts et les artefacts à leur pratique. Le résultat de ce processus d'appropriation peut être l'appropriation vers un usage routinier, ou, en revanche, le rejet, l'abandon de ces artefacts.

L'appropriation décrit la transition entre le processus d'appropriation et l'usage routinier des artefacts technologiques. Le rejet décrit la situation dans laquelle les utilisateurs cessent

[16] Percy Spencer, ingénieur chez Raytheon, passant à proximité d'un magnétron en activité, ressentit de la chaleur dans la poche de sa blouse et constata qu'une barre de chocolat y avait fondu. Il eut ainsi l'idée d'utiliser les micro-ondes pour cuire les aliments.

d'utiliser ces artefacts. Cela peut advenir précocement ou tardivement y compris pour des artefacts technologiques qui sont utilisés de façon routinière, par exemple quand de nouvelles technologies répondent mieux au besoin. C'est par exemple le cas du remplacement de la photographie argentique par la photographie numérique.

L'usage routinier de la technologie (*technology-in-use*) décrit la manière dont les utilisateurs utilisent de façon routinière les artefacts technologiques stabilisés. L'absence de renforcement ou une réévaluation de l'usage pour différentes raisons amène à rejeter les artefacts technologiques. Certaines technologies restent stables durant de longues périodes, tandis que d'autres sont amenées à évoluer, avec un retour au processus d'appropriation.

La conception par l'appropriation désigne le retour d'expérience de l'usage routinier vers le processus de conception, afin que cette dernière prenne en compte l'usage réel.

La conception pour l'appropriation désigne la prise en compte de l'appropriation dès les étapes de spécification et de conception afin que la solution conçue soit adaptée au processus d'appropriation, c'est-à-dire que les utilisateurs puissent l'adapter, la faire évoluer, afin de l'adopter et l'utiliser de façon routinière.

Dans le contexte des systèmes à longue durée de vie, mis en œuvre dans des environnements complexes et dynamiques évoluant rapidement, les utilisateurs sont amenés à adapter la technologie en permanence (Bachatène *et al.*, 2008).

3.3.6. Synthèse du processus de conception centrée utilisateur

Cette partie était consacrée au processus de conception centrée utilisateur. Elle a précisé le modèle de l'utilisateur, le persona, représentation fictive d'un utilisateur archétypique, qui apporte une perspective innovante sur le modèle de l'utilisateur. En particulier, le persona peut être enrichi de données issues de la prospective pour prendre en compte les utilisateurs à différents horizons temporels des systèmes à longue durée de vie. Cette a présenté les modèles de tâche qui permettent de structurer les systèmes interactifs au regard des activités des opérateurs. Cette partie a aussi précisé les fondements de l'ergonomie prospective, laquelle complète l'ergonomie de correction et l'ergonomie de conception pour anticiper les besoins et activités des opérateurs. À ce titre, elle est adaptée à la conception des systèmes à longue durée de vie. Enfin, elle se clôt en présentant le processus d'appropriation du système par l'utilisateur. Ce processus rend compte de l'adaptation et de l'adoption des technologies par les utilisateurs, en les détournant aussi de leurs fonctionnalités initiales.

3.4. Architecture des systèmes interactifs

À l'instar de l'architecture système, l'architecture des systèmes interactifs [17] décrit l'organisation des éléments d'interactions homme-machine, tant sur le plan fonctionnel que sur le plan structural et sur le plan comportemental. L'architecture des IHM (Coutaz & Nigay, 2001) prend en compte les spécificités des interactions homme-machine, en particulier pour découpler ces interactions d'avec les traitements internes du système de traitement de l'information. Le système interactif comprend les composants de l'interface utilisateur pour les différentes modalités d'interaction, visuelle, auditive (Stanton, 1994 ; Stanton & Baber,

[17] Le terme « architecture des IHM » est aussi usité.

1997 ; Stanton & Stammers, 1998 ; Stanton & Baber, 2008), haptique, ainsi que la réalité augmentée (Fuchs *et al.*, 2010 ; Hugues *et al.*, 2010 ; Cieutat, 2013), entre autres.

Nous rappelons que les informations présentées, leur agencement, les modalités d'interaction concourent à la capacité d'un opérateur de construire et entretenir une conscience de la situation et comprendre la dynamique du système (Conversy *et al.*, 2004). A ce titre, la qualité des IHM contribue à la résilience des systèmes sociotechniques (SAIC, 2005 ; Belmonte *et al.*, 2008 ; Hollnagel *et al.*, 2006). C'est dans ce contexte et avec cet objectif que nous présentons l'architecture des systèmes interactifs.

Après avoir présenté des modèles d'architecture de systèmes interactifs, nous présentons la modélisation de l'architecture des systèmes interactifs avec UML. Nous continuons en traitant l'architecture d'IHM distribuée, ainsi que des principes de conception orientée aspect, pour finalement faire le lien entre architecture et conscience partagée de la situation.

3.4.1. Modèles d'architecture de systèmes interactifs

Les modèles d'architecture en IHM aident à structurer le système interactif en un ensemble de composants en interaction, pour découpler le noyau applicatif de l'interface et pour gérer les dispositifs qui concourent au système interactif. Le premier modèle d'architecture, dans le domaine des IHM, est le modèle « Modèle-Vue-Contrôleur » (MVC) élaboré dans les années 70 dans le cadre de l'implémentation du langage Smalltalk et largement utilisé aujourd'hui pour la conception web. Ce modèle d'architecture comprend trois parties :

- un modèle, en l'occurrence le modèle de données ;
- une vue qui correspond à l'affichage des informations aux utilisateurs;
- un contrôleur qui gère et contrôle les saisies effectuées par l'utilisateur et gère les événements (clic de la souris).

La Figure 3.3 illustre la modélisation des IHM en mettant en œuvre le modèle d'architecture MVC dans le domaine des systèmes financiers.

Dans la même logique de structurer la conception des IHM, Joëlle Coutaz (1987) propose le modèle d'architecture « Présentation-Abstraction-Contrôle » (PAC).
Ces trois facettes du modèle d'architecture PAC sont organisées ainsi :

- la présentation concerne l'interaction avec l'utilisateur, dont l'affichage et les saisies, tant avec le clavier que la souris ou autre dispositif. La présentation est complètement dédiée à l'IHM ;
- l'abstraction gère l'ensemble des données, dont celles à présenter à l'utilisateur *via* la présentation. C'est le noyau fonctionnel, c'est-à-dire la partie du logiciel qui satisfait au besoin fonctionnel, ce pourquoi il a été conçu ;
- le contrôle assure la correspondance entre la présentation et l'abstraction, traduisant l'une en l'autre et inversement, afin de conserver la cohérence des données interne et de les convertir afin qu'elles soient utilisables par l'utilisateur.

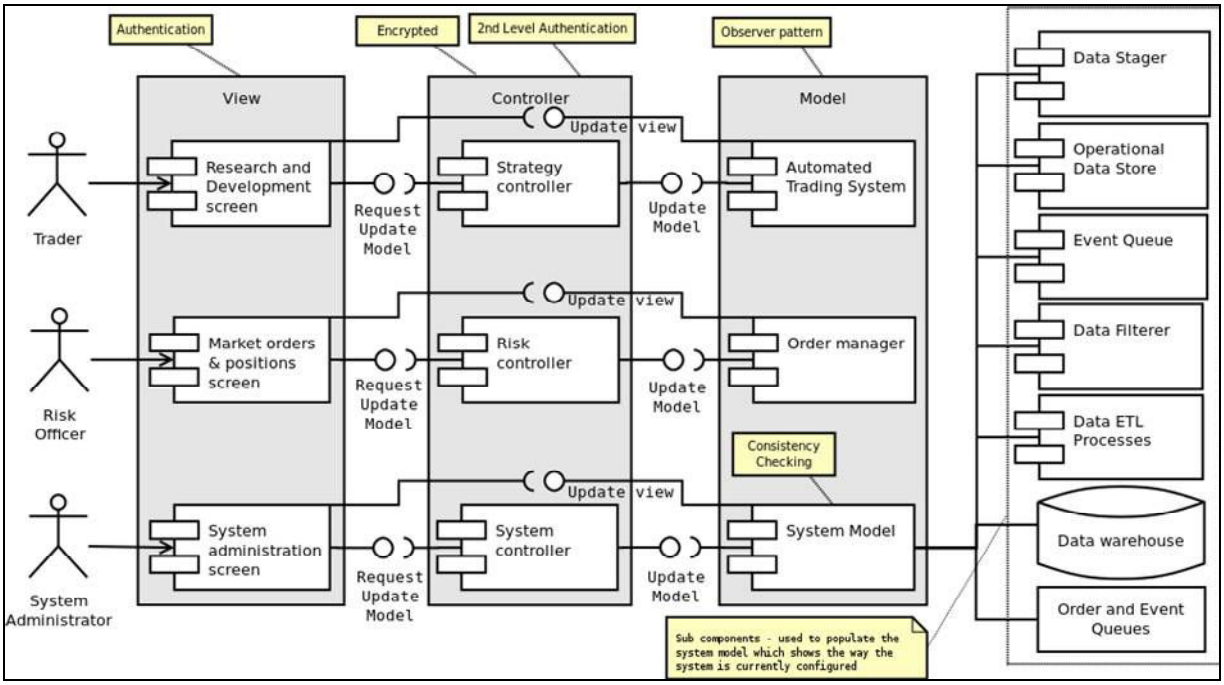

Figure 3.3. Modèle MVC basé sur UML dans le domaine des systèmes financiers (source http://www.turingfinance.com/algorithmic-trading-system-architecture-post/).

Enfin, le modèle d'architecture Arch (Bass *et al*., 1991) développe celui de Seeheim (Pfaff & Hagen, 1985) par une organisation en cinq composants :

- le noyau fonctionnel contient les données et les traitements que réalise le programme ;
- l'adaptateur du noyau fonctionnel est une couche assurant le lien entre le noyau fonctionnel et le contrôleur de dialogue avec pour objectif de coordonner l'un et l'autre tout en conservant leur cohérence interne propre ;
- le contrôleur de dialogue gère le séquencement des tâches en tenant compte de leurs contraintes propres au métier de l'utilisateur ;
- la présentation logique assure la médiation entre le contrôleur de dialogue et la présentation physique, rendant le contrôleur de dialogue indépendant de la présentation physique ;
- la présentation physique inclut les différents périphériques d'interaction et les composants logiciels d'interaction.

Ces modèles d'architecture « PAC » et « Arch » permettent une séparation claire entre l'IHM et le noyau fonctionnel. Ils sont particulièrement utiles, par exemple, pour les IHM qualifiées de plastiques fonctionnant sur plusieurs dispositifs d'IHM différents tels qu'une station de travail, un smartphone, un serveur vocal, etc. (Calvary, 2007 ; Calvary *et al.*, 2003). Le noyau fonctionnel peut fonctionner indépendamment de la façon dont ces différents dispositifs traitent des entrées-sorties selon leurs spécificités. Ainsi, il peut y avoir autant de présentations et de contrôles qu'il y a de dispositifs différents. Chacun de ces contrôles assure la traduction entre la présentation spécifique à tel ou tel dispositif et l'abstraction.

La Figure 3.4 illustre cela en présentant une application (Ruault, 2002) faisant appel, d'une part, au modèle d'architecture « PAC », séparant l'abstraction (*information model*) du contrôle (*task*), et d'autre part au modèle d'architecture « publier-souscrire » (cf. section 2.4.4 intitulée « Patrons de conception (*design patterns*) »).

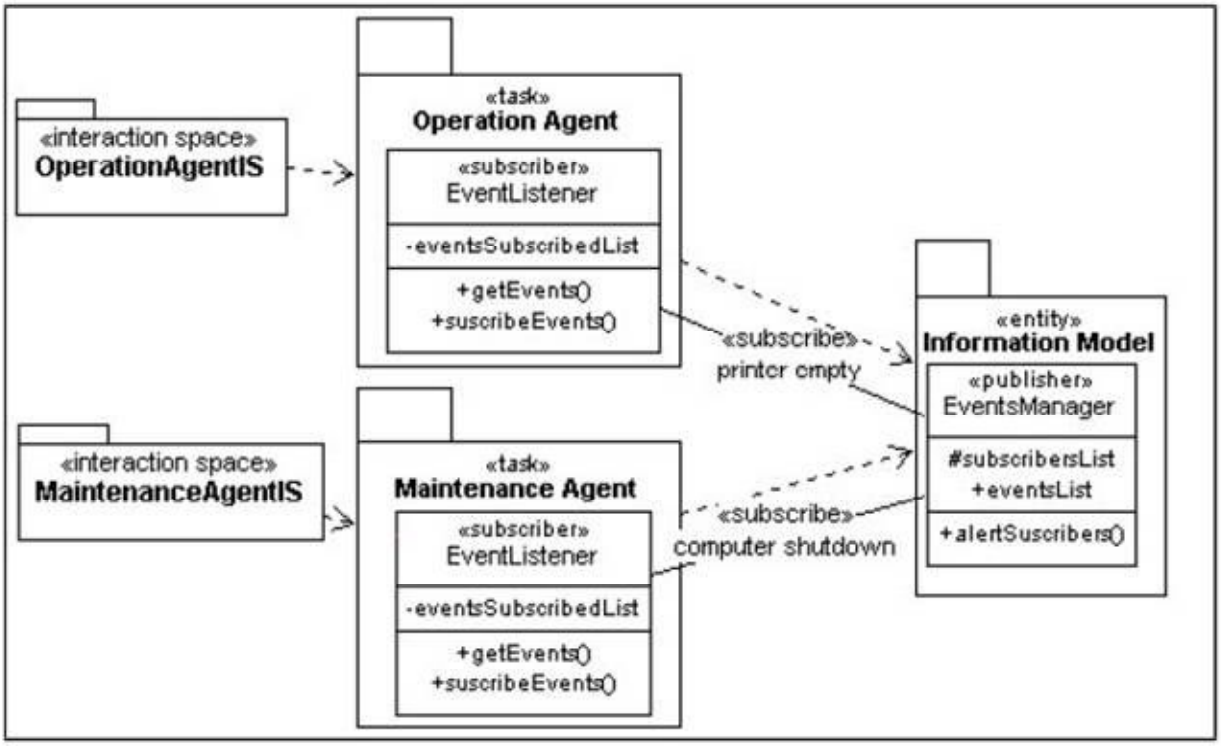

Figure 3.4. Illustration des modèles d'architecture « PAC » et « publier-souscrire » (Ruault, 2002).

Cette illustration montre que les modèles d'architecture répondent au problème des applications qui doivent avoir des interfaces homme-machine différenciées afin de satisfaire aux besoins spécifiques de plusieurs types différents d'utilisateurs.

3.4.2. Modélisation de l'architecture des IHM avec UML

Dans la mesure où le langage UML est générique et pas particulièrement adapté aux IHM, très rapidement, des adaptations d'UML ont été proposées pour mieux répondre aux spécificités des interactions homme-machine (Roberts *et al*, 1998 ; Nunes & Cunha, 2001 ; Ruault, 2002 ; Ribeiro *et al.*, 2007 ; Ahmed *et al.*, 2013). Nous y retrouvons les diagrammes UML (diagramme des cas d'utilisation, diagramme de classe, diagramme de séquence…) lesquels sont complétés de stéréotypes UML afin d'élaborer un profil UML adapté aux IHM. La Figure 3.5 (Nunes & Cunha, 2001) une des premières tentatives d'adaptation avec les stéréotypes de frontière, de contrôle, d'entité, de tâche et de vue, pour les classes UML[18].

Les principaux concepts, comme l'illustre la Figure 3.5 (Nunes & Cunha, 2001), sont :

- *entity* : élément persistant comprenant les données persistantes et une partie de la logique métier ;
- *control* : élément contrôlant le déroutement des actions, comprenant une partie de la logique métier et le modèle de tâche ;
- *boundary* : élément périphérique des entrées-sorties avec l'utilisateur.

[18] Notons que la représentation de composant a évolué depuis dans les versions les plus récentes d'UML (cf. ww.uml.org).

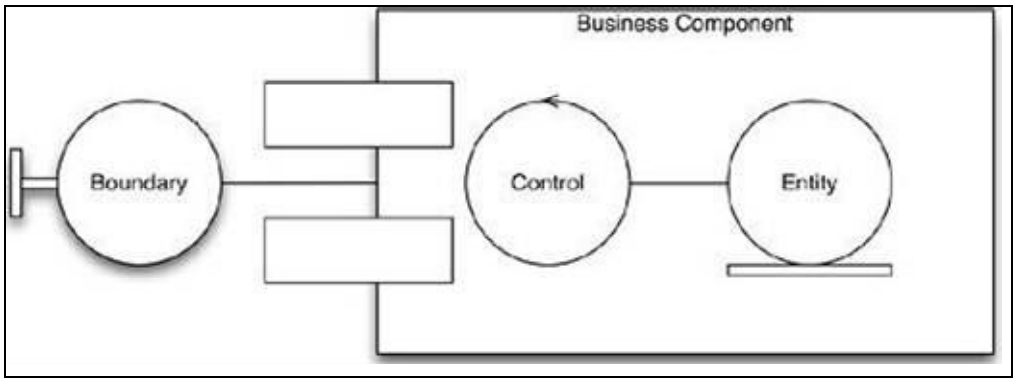

Figure 3.5. Stéréotypes UML de frontière, de contrôle et d'entité (Nunes & Cunha, 2001).

Ces stéréotypes facilitent la modélisation de ce qui contribue aux interactions homme-machine, dont la tâche, ainsi que la vue, le contrôle, notions précisées dans la partie « Modèles d'architecture en IHM » (cf. section 3.4.1) en cohérence avec ces modèles d'architecture. La Figure 3.6 (Nunes & Cunha, 2001) complète les précédents éléments avec les notions de tâche et de vue, et regroupe ces éléments en matière de modèle d'analyse et de modèle d'interaction.

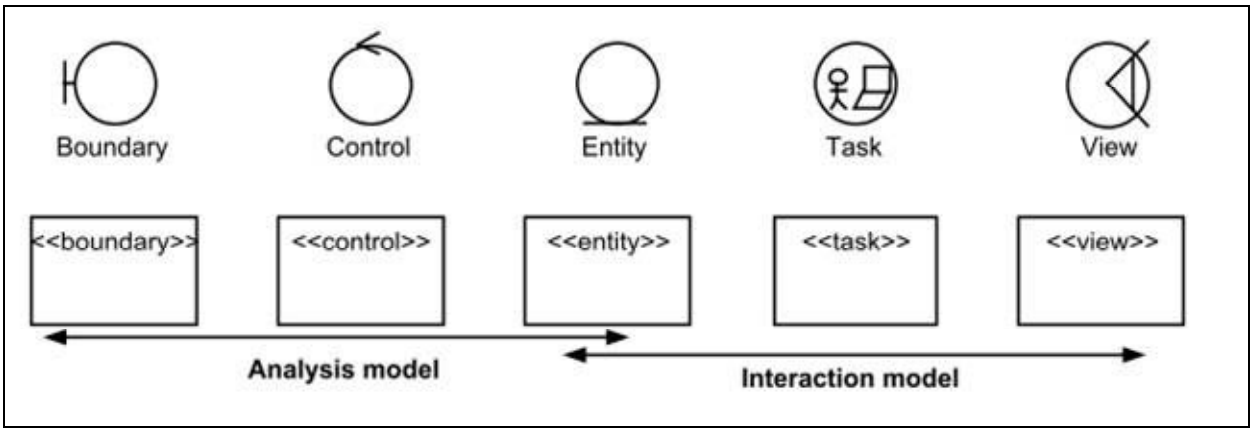

Figure 3.6. Stéréotypes de classes UML (Nunes & Cunha, 2001).

3.4.3. Architecture pour les IHM distribuées

Les premiers travaux consacrés aux interactions homme-machine se sont focalisés sur des architectures simples, que nous pouvons résumer par un utilisateur effectuant une tâche dans un contexte et un environnement donnés en mettant en œuvre un dispositif de traitement de l'information fonctionnant avec un système d'exploitation et une application spécifiques (Vanderdonckt, 2010). L'élaboration d'une conscience collective de la situation met en œuvre des activités collaboratives et nécessite des IHM appropriées.

Les activités collaboratives, tant dans le domaine éducatif, que dans celui de la simulation de trafic ou de gestion de crise (Kolski *et al*., 2014) font évoluer les interactions homme-machine. En effet, plusieurs utilisateurs collaborant ensemble, réalisant les tâches identiques ou des tâches complémentaires, à un même endroit ou dans plusieurs endroits différents, avec des

dispositifs de traitement de l'information différents, doivent partager des données, les modifier, les communiquer, etc.

Le Tableau 3.1 illustre les impacts des évolutions des interactions homme-machine sur les principales dimensions de ces interactions. La colonne « avant » indique l'organisation de ces dimensions dans les interactions homme-machine traditionnelles, tandis que la colonne « après » montre la pluralité et la diversité de ces dimensions dans le contexte des interactions distribuées.

	Avant	**Après**
Dispositif	Un	Plusieurs
Plate-forme, système d'exploitation	Un	Plusieurs
Utilisateur	Un	Plusieurs
Environnement	Un	Plusieurs
Contexte d'usage	Un	Plusieurs
Domaine d'application et tâche	Un	Plusieurs

Tableau 3.1. Evolution des interactions homme-machine vers les interactions distribuées (d'après Vanderdonckt, 2010).

Les évolutions permettent de distribuer les interactions entre plusieurs dispositifs, plusieurs utilisateurs réalisant des tâches identiques ou complémentaires, voire différentes, qu'ils soient co-localisés ou situés dans des endroits différents, que ces tâches soient synchrones ou asynchrones (Elmqvist, 2011). Cette distribution des interactions homme-machine peut être déployée sur une vaste variété de dispositifs hétérogènes, par exemple, des ordinateurs de bureau, des téléphones portables, des tablettes, des tables interactives (Lepreux *et al*., 2011). De même, les tâches et les interactions peuvent être variées, pouvant aller du transfert de documents d'un dispositif à un autre (Tesoriero, 2014), le travail collaboratif dans une classe dans laquelle un élève demande à un autre élève de l'aider à résoudre un problème, sous le contrôle de l'enseignant, à l'aide du système de communication distribué (Fardoun *et al*., 2011), l'informatique en nuage pour faciliter aux différents membres de la communauté éducative (enseignants, tuteurs, élèves, parents …) de partager des informations (Fardoun *et al*., 2012), par exemple.

Le fait que plusieurs utilisateurs puissent partager des informations, les manipuler, les modifier, voire avec des impacts sur des objets physiques (qualifiés aussi de tangibles), ou en revanche, à partir de la modification de l'état d'objets physiques (Lepreux *et al.*, 2012 ; Kubicki *et al.*, 2012) génère d'importantes contraintes sur les interactions homme-machine distribuées. Les données doivent être pérennes et intègres, c'est-à-dire ne pas être modifiées en dehors des modifications voulues par les différents utilisateurs. Les modifications des données doivent être répercutées à l'ensemble des utilisateurs avec un minimum de latence, quels que soient les différents endroits où ils sont situés, quels que soient les différents dispositifs de traitement de l'information, pour qu'il n'y ait pas de confusion et d'incompréhension dans leur collaboration. Ces modifications doivent signifier la même chose aux différents utilisateurs.

Ces contraintes ainsi que l'adaptation des données aux différents dispositifs et aux tâches des utilisateurs ont des impacts sur les modèles d'architecture des interactions homme-machine (tels MVC et PAC) qui doivent évoluer pour prendre en compte les interactions distribuées (Elmqvist, 2011).

Dans un premier temps, une stratégie doit être définie pour établir les relations qu'entretiennent les dispositifs entre eux dans différents contextes d'usage, par exemple, avec

un dispositif maître et des dispositifs esclaves (Lepreux *et al.*, 2012). Dans ce contexte, le dispositif maître prend la responsabilité pour sélectionner le mode de représentation adéquat à la plate-forme cible. Alternativement, les différents dispositifs peuvent être autonomes, dans une relation de parité, formant un graphe dans lequel chaque nœud correspond à un dispositif. Dans ce contexte, la distribution peut se traduire par une duplication totale des interactions, une duplication partielle, une extraction partielle, entre autres (Lepreux *et al.*, 2012). Par exemple, la migration d'éléments d'interface d'un dispositif à un autre fait appel à plusieurs capacités de ces éléments, dont celle d'être détachés du dispositif source, de migrer vers le dispositif cible, de disposer de la plasticité pour s'adapter aux spécificités du dispositif cible (Calvary, 2007) et de celle de s'attacher aux autres éléments d'interface du dispositif cible (Vanderdonckt, 2010).

Les trois piliers du contexte d'usage[19] sont (Calvary *et al.*, 2003) :

- l'utilisateur, qui représente un utilisateur stéréotype du système interactif, celui-ci pouvant être basé sur le modèle du processeur humain (Card *et al*., 1983), avec ses capacités perceptives et cognitives ;
- la plate-forme qui comprend l'ensemble des dispositifs matériels ainsi que les composants logiciels (système d'exploitation …), prenant en compte l'hétérogénéité des systèmes (téléphone intelligent, station de travail, mur d'images, table interactive…) ;
- l'environnement, qui comprend l'ensemble des objets, des personnes, des événements en périphérie de l'activité mais qui peuvent avoir des impacts sur le système interactif et sur le comportement des utilisateurs.

Plusieurs configurations de la plate-forme peuvent être envisagées (Balme *et al.*, 2004), une configuration statique dans laquelle l'ensemble des dispositifs sont intégrés préalablement à la mise en œuvre de la plate-forme, et une configuration dynamique dans laquelle les dispositifs sont intégrés ou retirés à la volée. De plus, ces dispositifs peuvent être homogènes ou hétérogènes.

Pour réaliser ces configurations, CAMELEON-RT (Balme *et al.*, 2004) est un modèle d'architecture modélisant les composants, observant leurs évolutions et permettant d'adapter l'interface en fonction ces évolutions. Ce modèle d'architecture comprend trois couches :

- la couche de la plate-forme ;
- la couche du système interactif comprend le système interactif avec lequel l'utilisateur interagit, mais aussi l'interface méta-utilisateur qui permet à l'utilisateur de configurer, contrôler, évaluer l'état du système interactif ;
- la couche de l'intergiciel Distribution-Migration-Plasticité (DMP), clef de voûte du modèle, permet de modéliser l'espace physique, de supporter les regroupements hétérogènes dynamiques de dispositifs et d'adapter l'interface utilisateur quand une distribution ou une migration intervient.

Pour cela, la couche intergiciel DMP comprend :

- l'infrastructure du contexte, qui construit et maintient un modèle de l'espace physique, des capteurs aux systèmes d'exploitation ;
- le gestionnaire de la plate-forme et l'outil d'interaction, lesquels gèrent le système interactif, à l'instar d'X Window ;

[19] Le contexte est très étudiés par la communauté au niveau international depuis les années 90 (Boy, 1991 ; Dey, 1998…).

- le gestionnaire d'adaptation et d'ouverture, composant clef du modèle CAMELEON-RT, inclut des observateurs (au sens patron de conception). Ces observateurs, au sein de la plate-forme, de l'environnement physique, du système interactif et observant l'utilisateur, élaborent la situation *hic et nunc*, communiquent cette situation au moteur d'évolution pour enclencher l'adaptation du système interactif en fonction des évolutions qui adviennent dans l'environnement ou au niveau de la plate-forme.

Cette architecture permet d'intégrer et de retirer des dispositifs hétérogènes à la volée, de migrer des éléments d'un dispositif à un autre, en conservant la cohérence de la tâche et l'utilisabilité des dispositifs. Selon ses auteurs, cette architecture offre la souplesse pour effectuer des adaptations à la volée, au sein d'une session de travail.

La Figure 3.7 représente le modèle d'architecture de CAMELEON. Une version plus détaillée est disponible sur le site *Model-based User Interfaces Incubator Group* (http://www.w3.org/2005/Incubator/model-based-ui/wiki/Cameleon_reference_framework).

Le modèle CAMELEON (Calvary *et al.*, 2003) articule l'interface autour de quatre types de modèles :

- les modèles de tâches et du domaine de la tâche décrivent la tâche comme un ensemble structuré de sous-tâches et les concepts du domaine d'application de la tâche ;
- les modèles de l'interface utilisateur abstraite (AUI pour *Abstract User Interface*) décrivent des composants d'interface abstraits indépendants des différentes plateformes d'accueil. Par exemple, sélectionner un élément dans une liste indépendamment de la façon dont la liste est réalisée sur une plate-forme spécifique ;
- les modèles de l'interface concrète (CUI pour *Concrete User Interface*) décrivent les composants de l'interface mis en œuvre par les différentes plateformes d'accueil, en tenant compte des *widgets* disponibles ;
- les modèles de l'interface finale (FUI pour *Final User Interface*) représentent le module logiciel qui va être exécuté sur la plateforme qu'utilise l'opérateur en utilisant les librairies de cette plateforme.

Le modèle WWHT (*What, Which, How, Then*) (Pruvost, 2013) met en œuvre des règles pour l'adaptation de la présentation en cours d'exécution. Ces règles s'appuient sur ces quatre dimensions pour effectuer cette adaptation :

- *What* : il s'agit de définir le sous-ensemble d'informations à présenter en fonction du contexte ;
- *Which* : l'objet de la règle est de choisir les modalités à utiliser pour chacune de ces informations, en sélectionnant la présentation adaptée ;
- *How* : au-delà de la sélection de la modalité, pour chaque élément, l'instanciation consiste à définir les caractéristiques des présentations (taille et couleur de texte, niveau sonore d'une sonnerie…) ;
- *Then* : l'objet de cette règle est de faire évoluer la présentation, soit par raffinement, sans changer les composants d'interaction, soit par mutation qui consiste en un changement radical des modalités, en fonction du contexte. Par exemple, passant d'un environnement lumineux et bruyant à un environnement sombre et silencieux, le changement sera radical, remplaçant l'écran par la synthèse vocale.

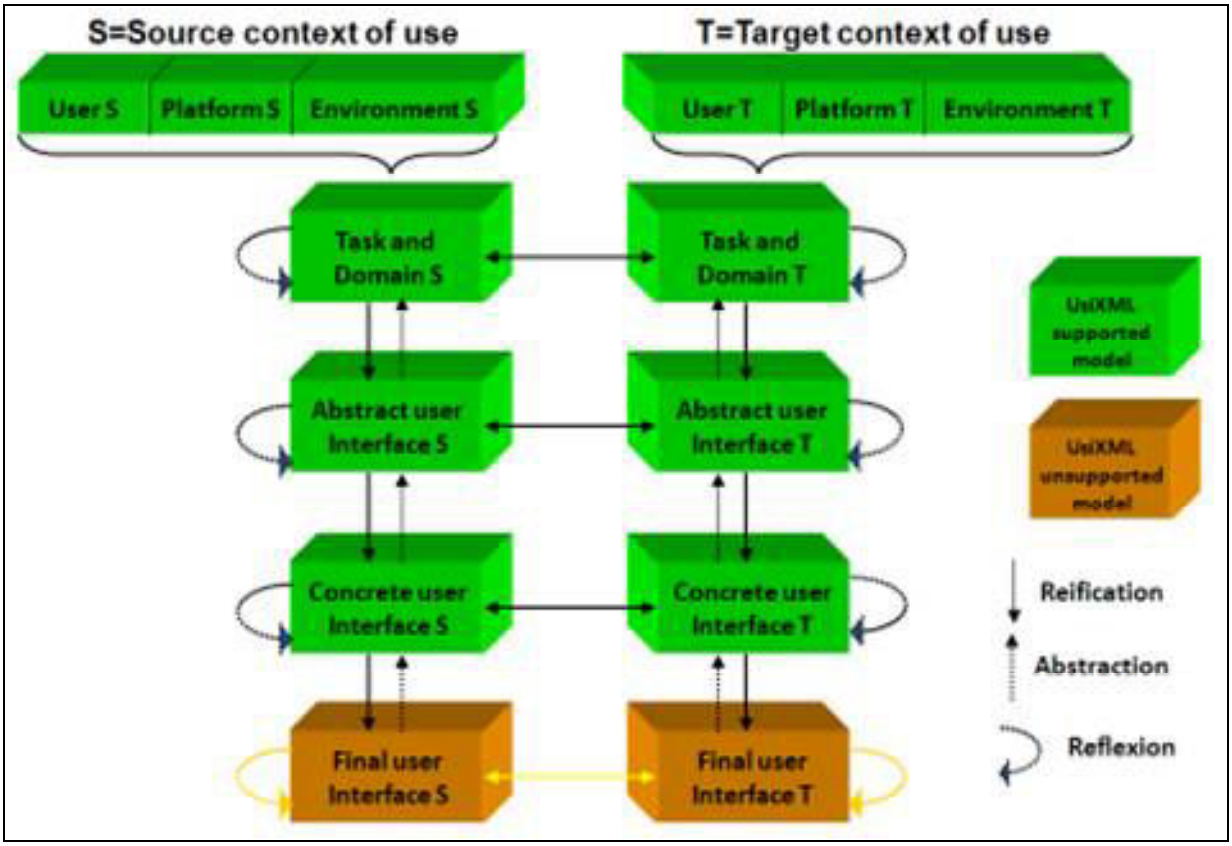

Figure 3.7. Modèle de référence CAMELEON (source http://www.w3.org/2005/Incubator/model-based-ui/wiki/UsiXML).

Enfin, le modèle KUP (*Knowledge, User, Presentation*) (Pruvost, 2013) prend en compte la zone géographique, espace de rayonnement d'un dispositif, qui lui permet d'interagir avec un autre dispositif.

3.4.4. Conception orientée aspect

Issue de la programmation orientée aspect (traduction de *aspect-oriented programming*), la conception orientée aspect permet de factoriser et donc de rendre plus cohérentes les fonctionnalités transversales. En l'occurrence, pour ce qui nous intéresse (sécurité, sûreté…), l'objectif est de réduire le couplage avec les autres fonctionnalités, dites métier, et de faciliter la maintenance de ces fonctionnalités transversales. Cette conception orientée aspect est reconnue comme étant un patron de conception.

A ce titre, elle sépare les préoccupations (ou aspects pour reprendre le terme anglais) dits techniques des préoccupations (aspects) métier, en utilisant la modularité des composants. Les modules métier soutiennent les activités des utilisateurs. Dans un système de contrôle et de commande, de tels modules transmettent des ordres, ou élaborent et maintiennent l'image opérationnelle. D'autres modules, comme l'authentification, contribuent à la sécurité du système. Ces modules ne contribuent pas directement aux activités des utilisateurs et ne relèvent pas de leur métier, mais d'autres préoccupations plus transversales, par exemple la sécurité. Le même raisonnement applique aux modules de test ou aux modules qui mesurent la charge d'un réseau. Ces aspects s'enchevêtrent entre eux. Les relations entre ces modules sont limitées aux points d'intersection. Un module de dépistage fonctionne dans chaque

module métier. Aux points d'intersection, le module de dépistage est activé de façon non intrusive. Ces points d'intersection sont placés aux emplacements appropriés des modules métier, par exemple, pour évaluer les performances de ces modules. Chaque module est cohérent et traite seulement un aspect.

Les concepts clés, nécessaires pour mettre en œuvre la conception orientée aspect, sont les suivants (Tarby *et al.*, 2009 ; Ruault, 2009) :

- le point de jonction, représente la localisation de l'insertion de l'aspect dans le flux des fonctions de l'architecture ;
- la méthode qui est activée quand un point de jonction est atteint ;
- l'aspect, qui est un module qui traite d'un sujet particulier, parmi les sujets, il y a le domaine métier du système, la sécurité du système, sa surveillance ;
- le point de césure capture le contexte d'exécution au point de jonction, afin de le conserver et le restituer après l'achèvement de la méthode activée.

La Figure 3.8 montre la comparaison entre, d'une part, l'architecture traditionnelle (partie gauche de la figure), dans laquelle les différents aspects sont mélangés, et d'autre part, l'architecture orientée aspect (partie droite de la figure), dans laquelle les différents aspects sont clairement séparés puis ensuite tissés, afin de rendre l'architecture plus structurée, plus facile à élaborer et à maintenir.

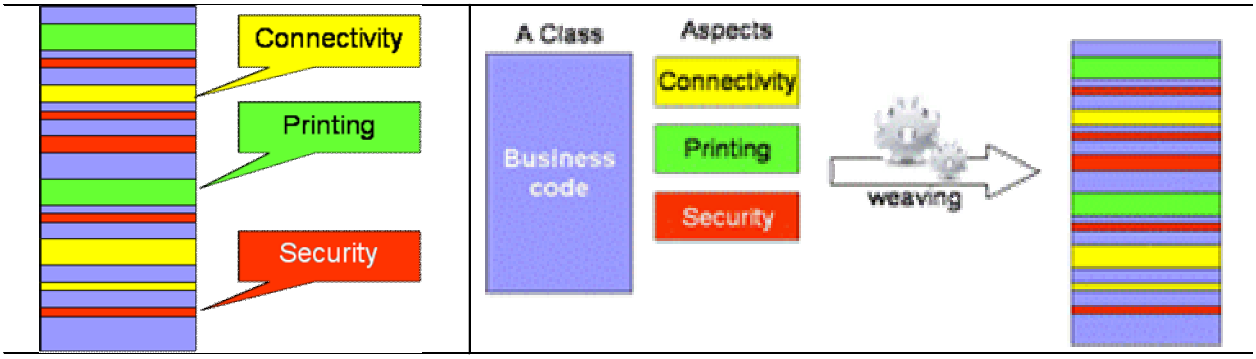

Figure 3.8. Comparaison entre l'architecture traditionnelle et l'architecture orientée aspect (Tarby *et al.*, 2009).

Les concepts suivants (Cisternino & Vaucouleur, 2009) complètent ceux de (Tarby *et al.* (2009) :

- l'aspect, un module définissant un greffon et traitant un aspect spécifique ;
- l'enchevêtrement des aspects ;
- le tissage d'aspects, insertion statique ou dynamique dans un composant d'un appel de greffon ;
- le greffon, est la partie du composant qui est activée au point d'intersection ;
- l'emplacement des greffons dans les composants.

Les exemples de conception orientée aspect incluent (Cisternino & Vaucouleur, 2009) :

- l'identification et l'authentification ;
- la gestion des exceptions et des défaillances ;

- le contrôle des performances ;
- la détection des changements et des mises à jour.

3.4.5. Représentation de l'usage et de l'état du système via les HUMS

Le document normatif consacré aux HUMS (ISO, 2003), présenté dans la section « Système de surveillance de l'usage et de l'état d'un système » du Chapitre 2, comprend une partie consacrée à l'affichage de l'état du système aux utilisateurs, opérateurs d'exploitation ou opérateurs de maintenance. Cet affichage reprend les informations clefs que sont l'état de la machine, le dépassement du seuil d'alerte, le pronostic et les conseils et les organise pour les rendre compréhensibles à ces opérateurs. La Figure 3.9, extrait de cette norme (ISO, 2003) illustre cela par l'affichage d'une chaudière. Cette représentation montrant les blocs d'affichage est assez sommaire et ne semble pas prendre en compte les contraintes spécifiques du modèle mental de l'opérateur, de la tâche, et du dispositif d'affichage. Nous remarquons que l'organisation par blocs de l'affichage fait écho à l'architecture structurée par blocs de traitements des documents consacrés aux HUMS.

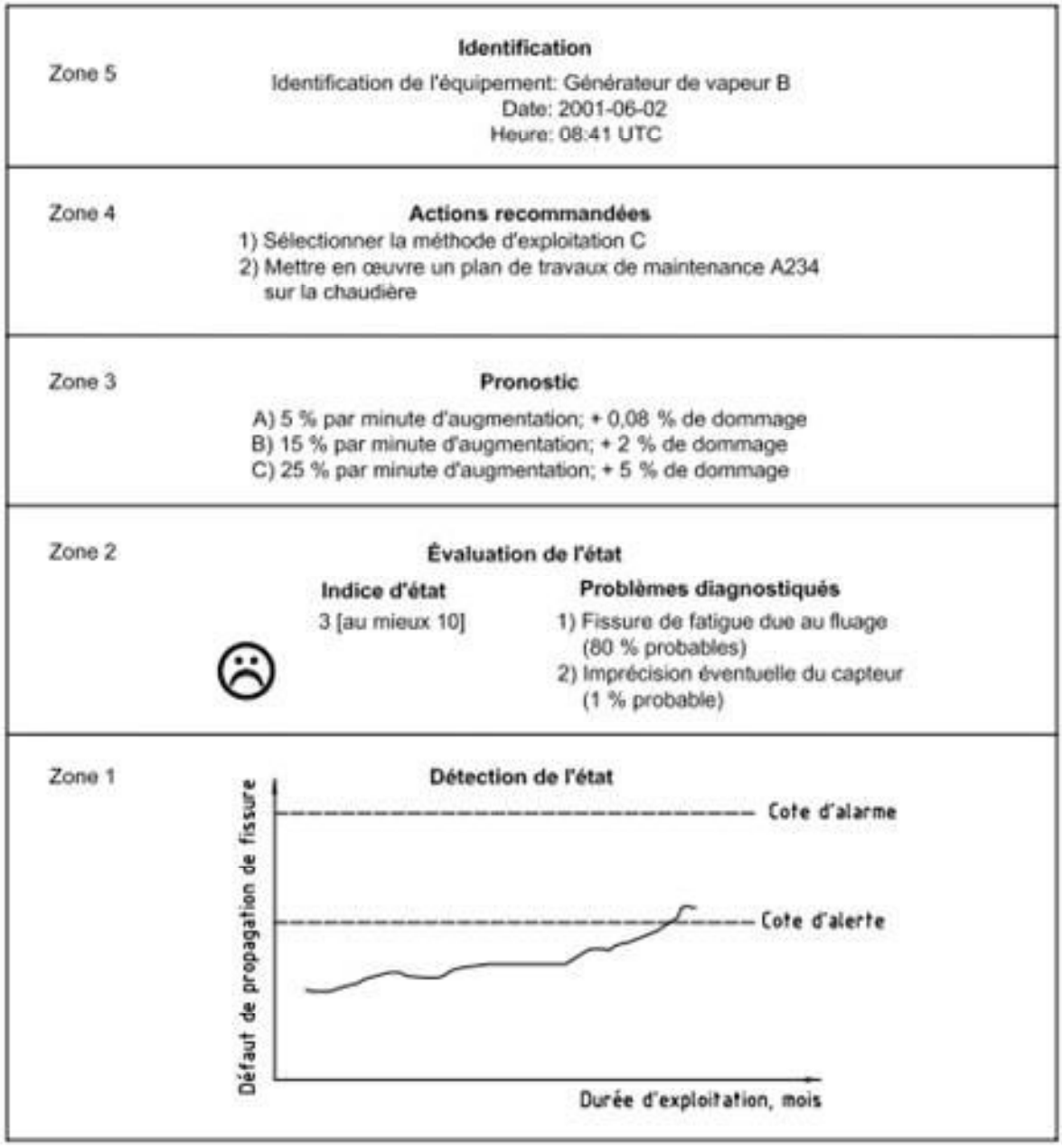

Figure 3.9. Exemple d'affichage d'une chaudière[20] (ISO, 2003).

Cependant, on peut remarquer que cette norme (ISO, 2003) ne mentionne pas la mise en œuvre d'un processus de conception centrée utilisateur pour concevoir et évaluer de telles méthodes d'affichage des informations de l'état du système aux utilisateurs, opérateurs d'exploitation ou opérateurs de maintenance.

[20] « Les extraits de la norme NF ISO 13374-1 :2003 « Surveillance et diagnostic d'état des machines, Traitement, échange et présentation des données, Lignes directrices générales » sont reproduits avec l'accord d'AFNOR. Seul le texte original et complet de la norme telle que diffusée par AFNOR Editions – accessible *via* le site internet www.boutique.afnor.org – a valeur normative »

3.5. Synthèse et conclusion du chapitre

Dans ce chapitre, après avoir présenté une définition et des concepts des interactions homme-machine, nous avons précisé le processus de conception centrée utilisateur, en particulier la notion de persona, celle d'ergonomie prospective ainsi que celle de processus d'appropriation.

L'ergonomie prospective élargit le périmètre de l'ergonomie de correction et de l'ergonomie de conception pour anticiper les besoins et activités des futurs utilisateurs. En particulier, elle se nourrit des résultats d'analyses prospectives de différents domaines, dont la démographie, pour caractériser ces futurs utilisateurs. À ce titre, elle est adaptée pour la conception des systèmes à longue durée de vie pour lesquels les derniers utilisateurs ne sont pas encore nés lors de la conception de ces systèmes.

Le processus d'appropriation met en évidence comment les utilisateurs s'approprient les systèmes, peuvent les détourner de leurs fonctions initiales pour de nouveaux usages, pour les intégrer dans leur activité quotidienne, routinière. À faisant, le système sera mis en œuvre dans des situations qui n'auront pas été envisagées, voire imprévisibles, sans précédent.

S'appuyant sur les travaux du modèle de l'utilisateur, le persona est une représentation fictive d'un utilisateur, ou d'une classe d'utilisateurs du futur système. Le persona collectif permet de rendre compte de la dynamique au sein d'une équipe de personas individuels. Le persona est adapté pour représenter un utilisateur d'un système à longue durée de vie pour lequel il n'est pas possible de disposer d'utilisateurs représentatifs aux différentes échéances de la vie opérationnelle de ce système.

La modélisation de l'architecture des systèmes interactifs, permet d'organiser, de structurer, les composants des systèmes interactifs afin qu'ils soient adaptés aux tâches à des opérateurs qui collaborent, qui coopèrent dans leurs activités, qui soient aussi adaptés aux dispositifs qu'ils utilisent pour réaliser ces tâches. Les systèmes interactifs contribuent à la construction et au maintien de la conscience de la situation des opérateurs. En particulier, les IHM distribuées offrent à un ensemble d'opérateurs, qui doivent collaborer ensemble, un cadre d'interprétation de la situation du système, de son environnement, qui leur soit commun.

Sachant que les systèmes seront mis en œuvre dans des situations qui ne peuvent pas être systématiquement envisagées en phase amont des projets, il est nécessaire d'anticiper leur usage, de donner aux opérateurs les moyens de s'approprier ces systèmes. Pour qu'ils puissent les contrôler, mettre en œuvre des démarches essai-erreur pour répondre à un problème, les opérateurs ont besoin d'un cadre d'interprétation commun leur permettant de construire et maintenir une conscience partagée de la situation.

Il est nécessaire que les opérateurs sachent positionner le fonctionnement courant du système par rapport à son domaine de définition, mesurer l'écart entre les deux, évaluer la proximité d'une zone de danger, comprendre les dérives que subit le système. C'est dans cette perspective que s'inscrit notre contribution développée à partir du Chapitre 4.

Partie 2 Contribution

Table des matières de la partie 2

Chapitre 4.

Positionnement de la contribution par rapport à la problématique de la résilience des systèmes critiques

4.1. La problématique de la résilience des systèmes

Dans l'état de l'art, (cf. Chapitre 1, « De la sûreté de fonctionnement à la résilience »), nous avons pu constater que pour différentes raisons (incapacités à tout maîtriser en phase amont des projets, accroissement des performances, franchissement des barrières, détournement fonctionnel…), les opérateurs peuvent faire face à des situations imprévisibles, sans précédent. Dans ces situations, les opérateurs doivent comprendre l'état du système et la situation dans laquelle il se trouve afin de faire face à l'adversité, naviguer à vue et mettre en œuvre une démarche essai-erreur.

Nous avons pu identifier, aussi, que, par construction, les exigences relatives au système sont supposées complètes, exhaustives. Les concepteurs sont supposés avoir une parfaite compréhension des conditions d'emploi. Les recommandations sont formulées pour surveiller le système en opération et pour prendre en compte les changements des situations opérationnelles, des besoins, des performances. Les résultats de la surveillance du système sont dirigés vers les concepteurs et les agents de maintenance, non pas vers les opérateurs.

De leur côté, les opérateurs doivent appliquer les procédures et modes opératoires définis au regard du domaine d'emploi. Ce dernier est défini à partir de la supposée parfaite compréhension des conditions d'emploi qu'ont les concepteurs.

Enfin, nous avons pu constater que les évolutions du contexte opérationnel, les déviations, les franchissements de barrières et les migrations silencieuses ne sont pas tracées, *a fortiori* évaluées et communiquées aux opérateurs pour les alerter.

Il s'avère que, lorsque les opérateurs sont face à une situation imprévisible, sans précédent, ils n'ont pour seuls repères que les modes opératoires définis par le domaine d'emploi. Ces derniers sont inadaptés pour faire face à une telle situation.

De plus, les opérateurs ne sont pas informés de l'état du système. En particulier, ils n'ont pas les moyens pour comprendre la situation, pour évaluer l'écart entre la situation dans laquelle se trouve le système et son domaine d'emploi supposé sûr. Faute de pouvoir élaborer et entretenir une conscience partagée de la situation, les opérateurs ne comprennent pas la dynamique du système et ne peuvent pas prendre les décisions appropriées et mettre en œuvre une démarche d'essai-erreur qui leur permettrait d'élaborer et de tester des hypothèses pour résoudre le problème auquel ils sont affrontés.

Nous reprenons et adaptons le modèle de migrations spontanées décrit dans la section 1.2.3 « Les franchissements de barrières, les violations des règles de sécurité et les migrations spontanées ». Le complément vise à tracer ce qui se déroule dans l'espace compris entre l'espace de fonctionnement considéré comme sûr par conception et l'accident (cf. Figure 1.2).

Dans cette perspective, nous différencions (cf. Tableau 4.1) :

- les scénarios et situations opérationnels de référence : description de la situation opérationnelle, telle qu'elle est envisagée (résultat d'une analyse prospective) et qui sert à spécifier et qualifier le futur système technique (*system as designed*), l'espace de fonctionnement considéré comme sûr par conception, à partir des exigences supposées complètes et d'une supposée parfaite[21] compréhension de l'emploi par les concepteurs ;
- les scénarios et situations opérationnels réels, halo d'emploi : situations réelles d'emploi du système, prenant en compte le contexte ici et maintenant (*system as used*), la réalité des situations vécues par le système. L'usage n'est pas très éloigné de la situation opérationnelle de référence. L'usage est le résultat du processus d'appropriation du système technique par les opérateurs humains, sans qu'il y ait détournement fonctionnel, et d'adaptations face aux facteurs de contexte. Les adaptations sont mineures, ne modifient pas la définition du système. L'effort de contrôle et d'adaptation reste contenu, sans nécessité de compensation. L'usage est à l'intérieur ou aux limites du domaine de définition du système ;
- l'usage hors du domaine de définition ; détournement, contournement : l'usage est éloigné de la situation de référence et est au-delà du domaine de définition du système dans une situation qui n'a pas été envisagée. L'usage hors du domaine de définition s'appuie sur le mécanisme de compensation exigeant des efforts et des ressources pour compenser les perturbations. Le risque de décompensation est élevé. Une vigilance accrue doit être mise en œuvre ;
- l'usage risqué : usage dans une situation très éloignée de la situation de référence, risqué et susceptible de générer un accident.

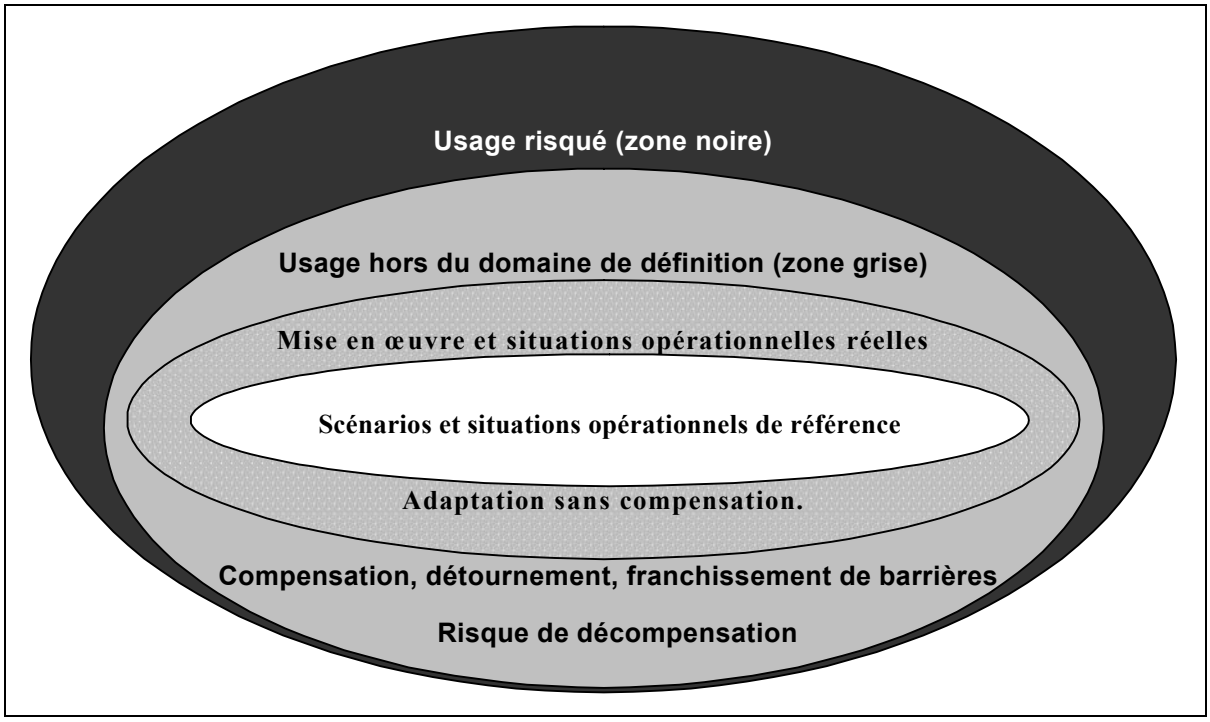

Figure 4.1. Contrôle entre la situation de référence et l'usage risqué du système.

[21] Le document (EN, 2010) mentionne « les critères de la sûreté de fonctionnement reflètent une parfaite compréhension des objectifs d'aptitude à la fonction et une parfaite compréhension des conditions d'exploitation ».

Les deux premiers types de situation et d'usage entrent dans le périmètre de la sûreté de fonctionnement. En revanche, les deux derniers items sont hors du périmètre de la sûreté de fonctionnement. En effet, ces derniers items ne sont pas connus en phase d'ingénierie, c'est-à-dire des cas pour lesquels il n'est pas possible d'attribuer des probabilités et d'évaluer des conséquences. De plus, ce sont dans ces deux derniers types que les situations imprévisibles, sans précédent, peuvent survenir. À ce titre, ils relèvent de la résilience, de la capacité de conduire à vue pour éviter la survenue d'un accident.

Il n'y a pas d'analyse différenciée permettant de caractériser les situations aux limites du domaine de définition (zone grise tâchée sur la Figure 4.1), les situations plus éloignées de ce domaine de définition (zone grise sur la Figure 4.1) et celles qui en sont très éloignées (zone noire sur la Figure 4.1). Les trois dernières situations sont confondues, en zone aveugle. Ainsi les nécessaires adaptations et les mécanismes de compensation ne sont pas différenciés.

Dans la mesure où les migrations sont silencieuses et que le mécanisme de compensation cache les perturbations et leur accroissement, le passage hors du périmètre du domaine de définition du système n'est pas explicite. L'écart entre la situation opérationnelle de référence et la situation opérationnelle réelle n'est pas mesuré.

Il est nécessaire d'aider les opérateurs à se positionner sur l'ensemble de l'aire afin qu'ils modulent, qu'ils régulent, leur niveau de vigilance en l'accroissant dans les zones grises et noires (au sens de la Figure 4.1).

Nous retenons aussi que l'analyse d'un accident se fait toujours dans une analyse de la cause (cf. section 1.3.1 « La sûreté de fonctionnement et la sécurité d'un système »), en mettant en exergue l'écart entre la procédure prescrite et la procédure qui a été mise en œuvre comme l'origine de l'accident, analyse qui se fait toujours *a posteriori*. Cela génère un biais. En effet, l'analyse de l'arbre des causes n'est effectuée qu'en cas d'accident, c'est-à-dire quand les conséquences sont négatives. En revanche, il n'y a jamais d'analyse de ce type lorsqu'il y a des écarts entre la procédure prescrite et la procédure mise en œuvre et que les conséquences sont positives.

		Conséquences	
		Positives (non accident)	**Négatives (incident, accident)**
Application des procédures	**Respect**	Indique que le système sociotechnique fonctionne dans son domaine de définition.	Met en évidence que l'environnement est différent de la situation de référence. Le respect de la procédure est un échec.
	Non respect	Relève de l'adaptation par le système sociotechnique à un environnement qui a changé ou d'un mécanisme de compensation par le système sociotechnique.	Relève soit d'un mécanisme d'adaptation inadapté, soit de l'échec d'un mécanisme de compensation. C'est un signal indiquant la probabilité d'un accident.

Tableau 4.1. Conséquences de l'application du respect ou non des procédures spécifiées (d'après Ruault *et al.*, 2012b).

Nous pouvons différencier les différentes situations de respect / non-respect des procédures spécifiées, ainsi que les conséquences positives (non accidents) / négatives (accidents) qui leurs sont associées (cf. Figure 4.1). Cela permet de comprendre pourquoi le système fonctionne correctement, y compris en tenant compte des aléas, sans se limiter à une tentative de compréhension de dysfonctionnements dans les seules situations accidentelles. Une analyse systématique croisant l'application des procédures (respect des procédures/non respect des procédures) avec les conséquences observées (conséquences positives, pas

d'accident/conséquences négatives, accident) met en évidence quatre possibilités représentées dans le Tableau 4.1. Actuellement, le cas du non respect des procédures ayant des conséquences positives n'est pas tracé, ni analysé. Analyser ce non respect des procédures est une perspective de recherche pour les années à venir (cf. Conclusion générale, section « Perspectives de recherche dans le domaine de la résilience des systèmes »).

Le Tableau 4.2 illustre et synthétise, pour les types de situation et d'usage, d'une part, les constats, les conséquences, d'autre part, les suggestions d'actions à mener. Notre contribution couvre la capacité de se situer par rapport aux trois types de situation.

Type de situation	**Conséquences, constats**	**Suggestions d'actions à prendre**
Scénarios et situations opérationnels réels	Le contexte opérationnel évolue, les procédures prescrites sont inadéquates. L'adaptation et les ajustements ne nécessitent pas de compensation. Pour autant, un début de migration silencieuse peut se déclencher.	Il est nécessaire de tracer les ajustements et détecter le déclenchement et l'orientation de la migration.
Usage hors du domaine de définition	Le phénomène de migration silencieuse se poursuit. Le contexte opérationnel a radicalement évolué et les procédures prescrites sont inadaptées.	Pour rendre explicite la migration, au fil de l'eau, il est nécessaire de : • évaluer l'effort de contrôle ; • accroître la vigilance ; • comprendre la raison du bon fonctionnement du système à ses limites du domaine de définition et les mécanismes de compensation ; • comprendre la raison qui pousse les opérateurs à détourner l'usage du système, à l'utiliser hors de son domaine de définition.
	Cette situation nécessite de mettre en œuvre un mécanisme de compensation.	La mise en œuvre d'un tel mécanisme de compensation doit générer une alerte et un accroissement de la vigilance. Il est nécessaire de comprendre les origines de la compensation afin, d'une part de réduire les efforts de compensation et passer d'un mode de compensation à un mode d'adaptation et, d'autre part de les prendre en compte dans la rénovation du système et la conception de futurs systèmes.
	Lorsque le mécanisme de compensation est insuffisant, un phénomène de décompensation a lieu.	Lorsqu'une décompensation advient, il est nécessaire de la comprendre afin de compléter l'analyse de la compensation.
Usage risqué	Le phénomène de migration silencieuse se poursuit présentant un usage risqué potentiellement ayant pour conséquence un accident, mais aussi une voie nouvelle.	Il est nécessaire de tracer cet usage risqué et le traiter en termes d'analyse des risques et des opportunités (sérendipité).

Tableau 4.2. Types de situation et suggestions des actions à prendre.

Après avoir caractérisé ces différentes situations, il est nécessaire de comprendre quels sont les chemins amenant d'une situation à une autre, et, pour reprendre le modèle de migration spontanée, quel est le chemin entre l'espace de fonctionnement considéré comme sûr par conception et l'accident (cf. Figure 1.2 de la section 1.2.3, « Les franchissements de barrières, les violations des règles de sécurité et les migrations spontanées »).

Nous proposons de représenter un de ces chemins possibles d'une migration silencieuse et de franchissements de barrières dans la Figure 4.2. Cette figure exprime la différence entre deux comportements : d'une part, la dynamique prescrite (ligne fine noire continue), d'autre part, la dynamique réelle (ligne fine noire pointillée).

La première prend en compte la variabilité locale prescrite incluse dans des marges de tolérance (ligne fine noire continue), c'est la variabilité habituelle, ou normale comme définie *a priori*.

La dynamique réelle présente, elle aussi, une variabilité locale réelle (ligne fine noire pointillée) qui dépend des aléas rencontrés, des conditions inhabituelles, dont l'évolution des situations environnementales ou des conditions de travail nouvelles et imprévisibles. La dynamique réelle prend en compte le contournement de barrières (cercle numéroté).

Outre les conditions inhabituelles, l'écart entre ces deux dynamiques (double flèche, couleur bleue) est dû aux dérives qui ne sont pas quelques cas isolés, mais une tendance structurelle. Ces dérives se caractérisent par le retrait de barrières, des nouvelles procédures non écrites ou la normalisation de la déviance (cf. section 1.2.3 « Les franchissements de barrières, les violations des règles de sécurité et les migrations spontanées »).

La dynamique réelle est une migration qui amène le système à fonctionner en dehors de son domaine de définition matérialisé par le trait noir épais continu. Sortant de ce domaine de définition, les barrières franchies (trait rouge épais discontinu), le système migre (trait noir fin continu). Les barrières de sécurité sont positionnées, par construction, aux limites de la dynamique prescrite pour préserver des actions dangereuses. Le système s'approche plusieurs fois de zones de danger, matérialisées par des symboles « danger » de différentes tailles (la taille indiquant la criticité du risque). S'écartant beaucoup (écart matérialisé par une double flèche épaisse grise) de son domaine de définition (position marquée E), le système est en zone de danger important (taille du symbole « danger »), un accident survient.

La Figure 4.2 montre les étapes de cette migration. En venant d'A, la dynamique réelle contourne la barrière à 1, se déplace vers B, puis C, pour rejoindre D et E en contournant de nouveaux la barrière en 2 et 3. Cette dynamique réelle de A à E exprime un écart qui peut être loin de la dynamique prescrite, comme c'est le cas en B. Personne ne peut évaluer cet écart. Il n'y a aucune conscience de situation, aucune capacité d'évaluer le risque induit par la dérive. Étape après étape, les actions dangereuses augmentent les risques (signal de proximité du danger), jusqu'à l'accident (E).

Notre contribution consiste à réintroduire la contrôlabilité du système par les opérateurs, en particulier en rendant visible le processus de migration, en permettant aux opérateurs de comprendre la dynamique du système, l'état dans lequel il est et l'état de l'environnement dans lequel se situe le système, afin de les laisser s'autoréguler mutuellement et mettre en œuvre une démarche d'essai-erreur et, *in fine*, éviter qu'un accident ne survienne. Pour cela, il est nécessaire d'obtenir en temps réel des informations sur la dynamique du système et de présenter ces informations aux opérateurs de façon appropriée à leur tâche pour qu'ils entretiennent cette conscience de la situation.

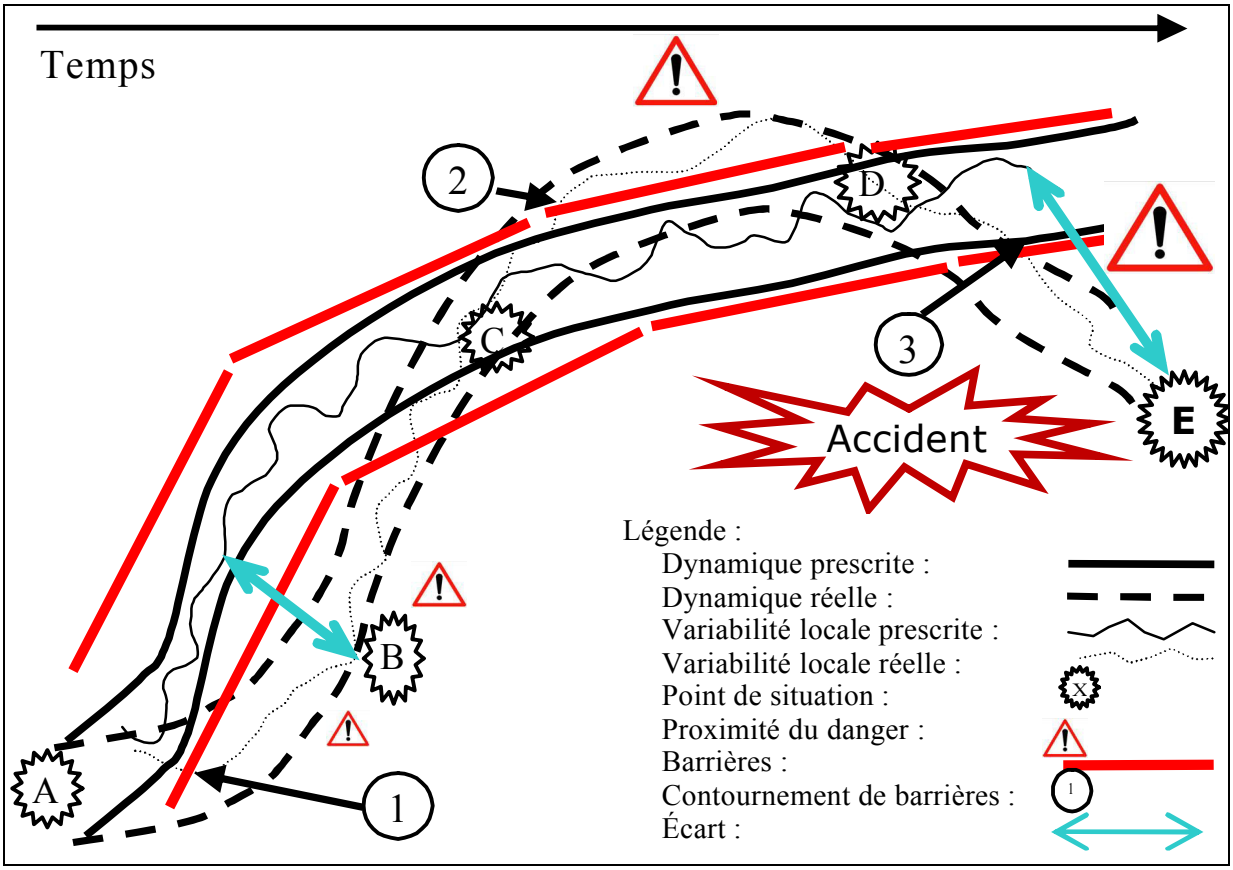

Figure 4.2. Dynamique prescrite et dynamique réelle (adapté de Ruault *et al.*, 2013).

Rendre les migrations et les mécanismes de compensation visibles par les opérateurs implique que le système technique soit conçu pour être transparent, qu'il explicite son domaine de définition aux opérateurs et leur offre les moyens de positionner la situation actuelle par rapport à ce domaine de définition. Cela a des conséquences sur les modèles d'ingénierie du système technique et sur son architecture.

Nous proposons d'intégrer un système de surveillance de l'usage et de l'état[22] (cf. section 2.5.1, « Système de surveillance de l'usage et de l'état d'un système - HUMS- (*health and usage monitoring systems*) ») afin d'obtenir ces informations, puisqu'un tel système permet d'alerter, en temps réel et de façon continue, les opérateurs de l'état du système (cf. section 1.4.4, « Construction de la conscience partagée de la situation »). Cette information doit être présentée de façon appropriée aux opérateurs, en tenant compte des contextes d'usage, de leurs modèles mentaux, de leurs tâches et des dispositifs interactifs qu'ils utilisent (cf. section 3.4 « Architecture des systèmes interactifs »).

L'architecture système doit évoluer et être conçue de telle sorte que les opérateurs puissent élaborer un modèle mental adéquat du système pour reprendre la main sans discontinuité en cas d'arrêt. De plus, elle doit intégrer les moyens permettant aux opérateurs de réguler leurs activités et évaluer les écarts entre les procédures prescrites et les procédures réalisées, pour détecter, au plus tôt, des migrations ou des mécanismes de compensation. Cela s'appuie par la

[22] Par la suite, dans le mémoire, le « système de surveillance de l'usage et de l'état » fait référence à notre contribution qui est une adaptation des HUMS. La notion de HUMS est réservée pour la norme ISO (2003) et les documents connexes.

capacité de surveillance du système technique. Cette dernière vise à déterminer les configurations sur le terrain, d'identifier les adaptations réalisées, pour nourrir le processus de retour d'expérience. Cela implique que l'architecture du système technique soit conçue pour être adaptable et instrumentée pour permettre cette surveillance. L'architecture système doit être suffisamment facile à mettre en œuvre par les opérateurs, tolérante, pour répondre à des situations qui n'avaient pas été envisagées sans que cela entraîne des accidents. Les procédures rigides réduisent en effet les capacités de résilience du système.

Dans la section 1.3.2 intitulée « La fiabilité humaine, les facteurs de performance et les facteurs de contexte », nous avons présenté les facteurs de performance (PSF) et les facteurs de contexte (FC).

Nous reprenons ces PSF et FC pour décrire leurs liens avec la sécurité et la résilience. Pour chacun d'eux, nous mentionnons les spécificités du contexte et de notre proposition.

- PSF01 : Applicabilité et pertinence de l'entraînement, de l'expérience ; l'entraînement ne prend pas en compte la gestion des situations imprévisibles, sans précédent, la capacité de gérer ces situations de façon adaptée et sûre dépend étroitement de l'expérience propre de l'équipage ;
- PSF02 : Pertinence des procédures et des objectifs ; les procédures prescrites ne prennent pas en compte les situations imprévisibles, sans précédent, rencontrées lorsque le système fonctionne hors de son domaine d'emploi ;
- PSF03 : Disponibilité et clarté des modes opératoires ; les modes opératoires pour traiter les situations imprévisibles, sans précédent, ne sont pas faciles à utiliser et ne sont pas limpides ;
- PSF04 : Temps disponible et temps requis pour réaliser complètement l'action menée, incluant la concurrence entre les activités ; le temps requis pour traiter les situations imprévisibles, sans précédent, n'est pas cohérent avec le temps disponible, puisqu'il faut changer de mode de fonctionnement (d'automatique à résolution de problème), d'autant que les activités routinières génèrent de l'ennui comblé par la mise en œuvre d'autres activités, potentiellement concurrentes des premières ;
- PSF05 : Complexité du diagnostic et de la réponse requise, du besoin d'une séquence spéciale et de la familiarité de la situation ; le diagnostic n'est pas trivial et la réponse requise n'est pas routinière, les opérateurs ne sont pas familiers de la situation et il est nécessaire qu'ils puissent passer d'une réponse routinière à une réponse de type résolution de problème ;
- PSF06 : Charge de travail, pression temporelle et stress ; les spécificités des situations imprévisibles, sans précédent, l'effet de surprise qu'elles génèrent, sont sources de stress, de pression temporelle et accroissent la charge de travail ; par effet de bord, elles induisent l'appel à des heuristiques et des biais (persévération…) empêchant de gérer ces situations de façon sûre et adaptée ;
- PSF07 : Dynamique de l'équipage, caractéristiques de l'équipage ; les caractéristiques de l'équipage (compétences, expérience des membres de l'équipage …), la dynamique de l'équipage (mode de leadership, communication …) freinent ou favorisent l'élaboration et l'entretien d'une conscience partagée de la situation propre à gérer plus facilement les situations imprévisibles, sans précédent, auquelles l'équipage fait face ;
- PSF08 : Dotation en personnel disponible ; les limites de dotation en personnel disponible génèrent un accroissement de la charge de travail pour traiter les situations imprévisibles, sans précédent, situations non envisagées lorsque la dotation est planifiée au regard des situations prévisibles et envisagées dans le domaine d'emploi du système ;

- PSF09 : Qualité ergonomique de l'interface humain-système et FC04 : Qualité des interfaces opérateurs-machines ; l'interface utilisateur doit montrer l'état et l'usage du système afin que les opérateurs puissent élaborer et maintenir une représentation dynamique du système et de son environnement ;
- PSF10 : Environnement dans lequel l'activité doit être réalisée ; l'environnement dans lequel l'activité est réalisée n'est pas connu et prévisible en phase d'ingénierie, de plus c'est un environnement duquel les opérateurs ne sont pas familiers, ce qui nécessite plus d'effort cognitif de leur part pour en comprendre la dynamique ;
- PSF11 : Accessibilité et capacité des équipements à être opérés, manipulés ; les équipements doivent montrer leur état, leur usage, expliciter leur défaillance qui ont des impacts sur la sécurité ;
- PSF13 : Communication et conditions par lesquels quelqu'un peut être facilement écouté ; le mode de fonctionnement au sein de l'équipage et entre l'équipage et des opérateurs éloignés, la qualité de la communication, la coordination au sein de l'équipage, affectent les capacités d'écoute et, in fine, la capacité à élaborer et entretenir une conscience partagée de la situation pour gérer de façon sûre et adaptée les situations imprévisibles, sans précédent ;
- PSF14 : Besoin d'aptitudes spéciales ; la gestion des situations imprévisibles, sans précédent, nécessite de faire appel à des aptitudes spéciales, pour communiquer au sein de l'équipage au-delà de la communication routinière, pour élaborer et entretenir une conscience partagée de la situation nécessaire pour piloter à vue, et pour rompre les heuristiques et les biais empêchant de traiter ces situations imprévisibles et sans précédent de façon sûre et adaptée ;
- PSF15 : Prise en compte de déviations et de détournements réalistes de séquences d'actions ; les déviations et détournements doivent être pris en compte, en particulier pour les rendre explicites aux opérateurs et montrer l'écart entre ces déviations et le domaine d'emploi prescrit du système ;
- FC03 :Qualité des communications entre les opérateurs et FC10 : Qualité de collaboration en équipe ; la qualité des communication entre les opérateurs et celle de la collaboration doivent être prises au sens large, au-delà du périmètre de l'équipage, puisque des opérateurs distants l'un de l'autre, mais concourant à une même tâche ou l'un exerce à l'égard de l'autre des contraintes spécifiques, doivent pouvoir se coordonner explicitement, soit directement, soit par l'intermédiaire d'un dispositif technologique ;
- FC07 : Nombre d'objectifs simultanés auxquels les opérateurs doivent répondre ; les objectifs de sécurité et les objectifs de performance sont en concurrence, générant les migrations silencieuses.

Les autres facteurs de performance et facteurs de contexte peuvent être peu ou prou indirectement concernés, mais les liens sont plus ténus.

Après avoir présenté la problématique de la résilience des systèmes sociotechniques et les spécificités des situations rencontrées, nous regardons comment la résilience répond à ce contexte.

4.2. La décomposition fonctionnelle de la résilience ; esquisse d'impacts sur l'ingénierie et l'architecture système

Pour que les opérateurs puissent naviguer à vue, détecter les migrations silencieuses, les dérives, comprendre la situation dans laquelle est le système et le danger potentiel qu'il court, avant qu'un accident ne se produise, il est nécessaire qu'ils aient les moyens d'éviter l'accident, d'adapter leur activité, le niveau de régulation, au regard de la situation rencontrée et son caractère dangereux.

Nous avons décrit les quatre fonctions de la résilience dans le chapitre Chapitre 1 intitulé « De la sûreté de fonctionnement à la résilience », nous rappelons ce qu'elles sont :

- éviter l'accident, qui repose sur la capacité d'anticipation ;
- résister face à l'accident, qui se traduit par une capacité d'absorption et de réduction des dommages ;
- s'adapter après un accident, qui se traduit par la capacité à évoluer face à des situations non envisagées et à se reconfigurer en conséquence ;
- recouvrer, qui consiste à restaurer un état opérationnel stable, au minimum dans une position de survie, voire avec des capacités et des performances opérationnelles réduites.

La Figure 4.3 (diagramme de définition de blocs SysML) illustre la décomposition de la résilience et de ses quatre fonctions.

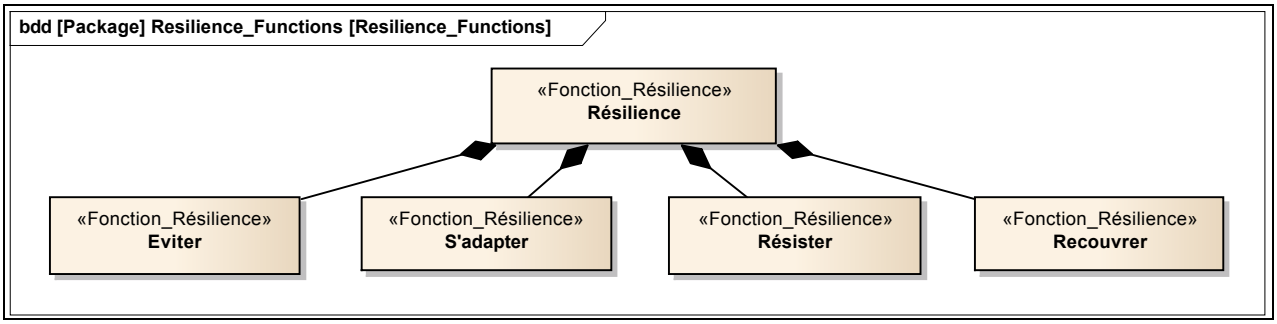

Figure 4.3. Les quatre fonctions de la résilience (Ruault, 2012b).

Ces fonctions ont des impacts sur l'ingénierie et l'architecture du système sociotechnique, à savoir (Ruault *et al.*, 2012b) :

- la mise en œuvre de la conception centrée sur l'opérateur humain au sein de l'ingénierie système, en matière d'expérience utilisateur et de processus d'appropriation ;
- la détermination des éléments suivants contribuant à la surveillance du système et à l'alerte des opérateurs :
    - des mesures permettant d'évaluer si le système fonctionne dans son domaine d'emploi ou, en revanche, est mis en œuvre hors de son domaine d'emploi ;
    - des mesures permettant de caractériser l'état courant du système, de sa dynamique ;
    - des capteurs qui peuvent fournir ces mesures ;
    - des critères de criticité ;
    - des valeurs de référence auxquelles comparer les valeurs courantes mesurées ;

    - du seuil d'alerte et des informations à présenter aux opérateurs ;
    - des traitements à effectuer pour fiabiliser ces mesures et évaluer le niveau de confiance à accorder à ces mesures, en particulier pour ne pas présenter aux opérateurs des informations fausses, erronées, pouvant les induire en erreur ;
- l'intégration des dispositifs de surveillance de l'usage et de l'état du système en tenant compte des impacts de cette intégration dans l'architecture du système ;
- la conception d'IHM basées sur le modèle conceptuel des opérateurs et reflétant les états réels du système et de son environnement, ainsi que les écarts entre ces états et les états de référence tels que spécifiés ;
- la prise en compte du retour d'expérience des opérateurs et de leur apprentissage, d'une part dans les évolutions du système, d'autre part dans la conception de nouveaux systèmes.

Ces préconisations sont conformes aux exigences « surveiller le système en opération », « utiliser les mesures définies dans la stratégie et les analyser pour confirmer que les performances s'inscrivent dans les bornes acceptables », « enregistrer les résultats de la mise en œuvre opérationnelle et les anomalies détectées », et « enregistrer les accidents et les problèmes, tracer leur résolution » de la norme consacrée au processus du cycle de vie des systèmes (ISO, 2014).

4.3. La structure de notre contribution

Notre contribution porte sur la fonction « éviter » de la résilience. Les trois autres fonctions de la résilience sont des sujets de recherche visant à compléter ce mémoire (cf. Conclusion générale, section « Perspectives de recherche dans le domaine de la résilience des systèmes »).

Notre contribution s'articule sur les deux perspectives différentes et complémentaires que sont le « système à faire » et le « système pour faire ».

La première perspective, celle du système à faire, est l'objet du Chapitre 5 intitulé « Proposition d'un patron de conception pour l'architecture d'un système résilient ». Nous proposons de créer le patron de conception « surveiller et alerter », pour la fonction « éviter » de la résilience, offrant aux opérateurs la capacité de comprendre la dynamique du système, de le conduire à vue face à des situations imprévisibles, sans précédent afin d'éviter la survenue d'un accident. L'objectif est de faire évoluer le système à faire (appelé simplement système par la suite) afin de donner aux opérateurs les moyens pour effectuer une navigation à vue. À cette fin, le système doit évoluer pour comprendre des moyens de surveillance de son usage et de son état et pour les représenter aux opérateurs *via* une IHM adaptée. Pour cela, il est nécessaire de faire évoluer l'architecture fonctionnelle et l'architecture physique du système, ainsi que l'architecture du système interactif.

Par ailleurs, pour prendre en compte les évolutions du besoin opérationnel, de l'environnement, en particulier d'un système avec une longue durée de vie, il est nécessaire d'organiser les activités pour réaliser ces évolutions.

La seconde perspective, objet du Chapitre 6 intitulé « Proposition de processus à mettre en œuvre pour contribuer à la résilience d'un système », est consacrée aux activités, méthodes et moyens pour faire évoluer ce système. Nous proposons de faire évoluer les processus d'ingénierie et de conception centrée utilisateur pour qu'ils contribuent à la résilience d'un système critique à longue durée de vie. Ce chapitre traite des impacts sur les processus d'ingénierie système, sur l'ensemble de la durée de vie du système Par ailleurs, il traite aussi

de la contribution du processus d'appropriation à l'ergonomie prospective, en particulier pour prendre en compte ce processus d'appropriation dans la conception et le retour d'expérience. Il traite aussi du persona comme moyen pour rendre compte des futurs utilisateurs. Cette contribution a pour objectif, dans une prochaine étape, d'enrichir les démarches de conception de système, en particulier dans une logique de développement agile, itératif et incrémental. En effet, les enseignements issus du processus d'appropriation et du retour d'expérience sont les entrées majeures des activités de rénovation à mi-vie et des évolutions du système, qu'elles soient majeures ou mineures. L'évolution des démarches agiles pour prendre en compte l'ergonomie prospective et le processus d'appropriation est une perspective de recherche à développer (cf. Conclusion générale, section « Perspectives de recherche dans le domaine de l'ingénierie et l'architecture système »).

Ces deux perspectives sont complémentaires puisque l'intégration dans le système à faire de dispositifs pour connaître son usage permet, au fur et à mesure que ce système est mis en œuvre, d'obtenir des informations qui sont utilisées dans les processus et activités du système pour faire.

Enfin, les critères de fiabilité et de pertinence de la représentation fonctionnelle feront aussi l'objet de certaines de nos perspectives de recherche pour les années à venir (cf. Conclusion générale, section « Perspectives de recherche dans le domaine des IHM et de l'ergonomie »). Il en sera de même de l'évaluation du patron de conception « surveiller et alerter » (cf. Conclusion générale, section « Perspectives de recherche pour la validation du patron de conception « surveiller et alerter » »).

En synthèse notre contribution consiste à :

- proposer un système de surveillance de l'usage et de l'état pour que les opérateurs puissent connaître l'état du système, sa dynamique et l'état de l'environnement (cf. § 5.2.3 « Système de surveillance de l'usage et de l'état du système ») ;
- offrir aux opérateurs concernés un cadre d'interprétation commun pour construire une représentation fonctionnelle, continuellement mise à jour, la plus fiable et la plus pertinente possible de la situation courante du système et de son environnement (cf. § 5.2.4 « Système interactif : représentation de la situation à l'opérateur ») ;
- mettre en évidence un certain nombre de conséquences sur les processus d'ingénierie système (cf. § 6.2 « Contribution à des évolutions des processus d'ingénierie système ») ;
- proposer d'articuler le processus d'appropriation avec les processus d'ingénierie et de compléter l'ergonomie prospective (cf. § 6.3 « Contribution du processus d'appropriation à l'ergonomie prospective ») ;
- proposer de mettre en œuvre le persona et le compléter pour rendre compte des utilisateurs de systèmes à longue durée de vie (cf. § 6.4 « Contribution aux adaptations du persona individuel / collectif aux systèmes critiques à longue durée de vie »).

Chapitre 5.

Proposition d'un patron de conception pour l'architecture d'un système résilient

5.1. Introduction

Ce chapitre est consacré au système à faire. Il traduit la fonction « éviter » de la résilience (les quatre fonctions de la résilience étant « éviter », « s'adapter », « résister » et « recouvrer », cf. section 1.3.4 intitulée « Introduction aux quatre fonctions de la résilience ») en sous-fonctions et alloue ces dernières aux composants de surveillance de l'usage et de l'état du système et aux composants de l'interface utilisateur.

Par la suite, le « système » et le « système principal » dénotent le système à faire, celui qui répond au besoin exprimé par les parties prenantes, tandis que le « système de surveillance de l'usage et de l'état » et le « système interactif » dénotent réciproquement des composants du système principal.

La prise en compte de la fonction « éviter » affecte l'architecture fonctionnelle et l'architecture physique du système. L'architecture fonctionnelle modélise l'organisation des fonctions. L'architecture physique modélise l'organisation des composants. Les fonctions sont allouées à des composants qui réalisent ces fonctions (cf. Tableau 5.1). La relation d'allocation des fonctions aux composants est modélisée par une matrice d'allocation.

	Éléments	**Relations entre éléments**
Architecture fonctionnelle	Fonctions	Les fonctions sont allouées aux composants
Architecture physique	Composants	Les composants réalisent les fonctions

Tableau 5.1. Liens entre architecture fonctionnelle et architecture physique.

Nous commençons en présentant le patron de conception pour la fonction « éviter » et nous poursuivons en décomposant cette fonction et en l'allouant aux composants du système de surveillance de l'usage et de l'état et du système interactif.

5.2. Patron de conception pour la fonction « éviter » de la résilience

Nous proposons un patron de conception pour des systèmes résilients, permettant de découpler le système opérant, le système de surveillance de l'état et de l'usage et le système interactif. Ce patron de conception se veut indépendant des domaines dans lesquels il peut être appliqué et indépendant des technologies utilisées pour le mettre en œuvre.

Le Tableau 5.2 présente ce patron de conception « surveiller et alerter ».

Caractéristiques	**Patron** de conception « **surveiller et alerter** »
Nom :	Surveiller et alerter.
Objectif :	Surveiller l'état et l'usage d'un système quand le système s'éloigne de son domaine d'emploi (migration silencieuse, franchissement de barrières…) et est à proximité d'une zone de danger, évaluer l'écart entre la dynamique réelle et la dynamique prescrite, et alerter les opérateurs.
Problème :	Intégrer un système de surveillance de l'usage et de l'état du système, et d'alerte des opérateurs en fonction de l'état et de l'usage détectés.
Solution :	Intégrer ce système de surveillance de l'usage et de l'état du système, et d'alerte des opérateurs en fonction de l'état et de l'usage détectés en minimisant les impacts sur l'architecture du système opérant.
Modèle :	• Architecture fonctionnelle ; • Architecture physique.
Interfaces :	• Interface avec le système opérant ; • Interface avec le système interactif.
Impacts :	Impacts sur l'architecture du système Impacts sur les activités des concepteurs (intégration du système de surveillance au sein du système principal).
Implémentation :	Réalisation des capteurs de l'état et de l'usage du système, des composants de stockage de l'information, des modules de traitement de l'information et de l'interface utilisateur appropriée au contexte d'usage des opérateurs.
Patrons de conception connexes :	• Observateur ; • Proxy.
Justification du patron de conception :	Ce patron de conception permet de découpler le système opérant, le système de surveillance de l'état et de l'usage et le système interactif. Il est indépendant des différents domaines dans lesquels il peut être appliqué et indépendant des technologies utilisées pour le mettre en œuvre.

Tableau 5.2. Canevas du patron de conception « surveiller et alerter ».

Ce patron de conception traduit la fonction « éviter » dans une architecture fonctionnelle, puis dans une architecture physique. Ce sont ces architectures que nous détaillons maintenant.

5.2.1. Fonction « éviter » : décomposition fonctionnelle

Le but de la fonction « éviter » est de donner aux opérateurs les moyens leur permettant d'élaborer et de maintenir une conscience de la situation, une représentation continuellement renouvelée de la dynamique du système, les éventuelles dérives par rapport au domaine d'emploi de référence, les éventuels contournements de barrières et la proximité d'une zone de danger.

Cette fonction « éviter » se décompose dans les sous-fonctions suivantes (Ruault *et al.*, 2012b) :

- obtenir une représentation de l'environnement du système ;
- obtenir une représentation de la dynamique de système ;
- évaluer des dérives par rapport au domaine d'emploi prescrit ;
- évaluer la proximité d'une zone de danger ;
- alerter, conseiller, les opérateurs.

La Figure 5.1 (diagramme de définition de bloc SysML) illustre cette décomposition de la fonction « éviter » en sous-fonctions.

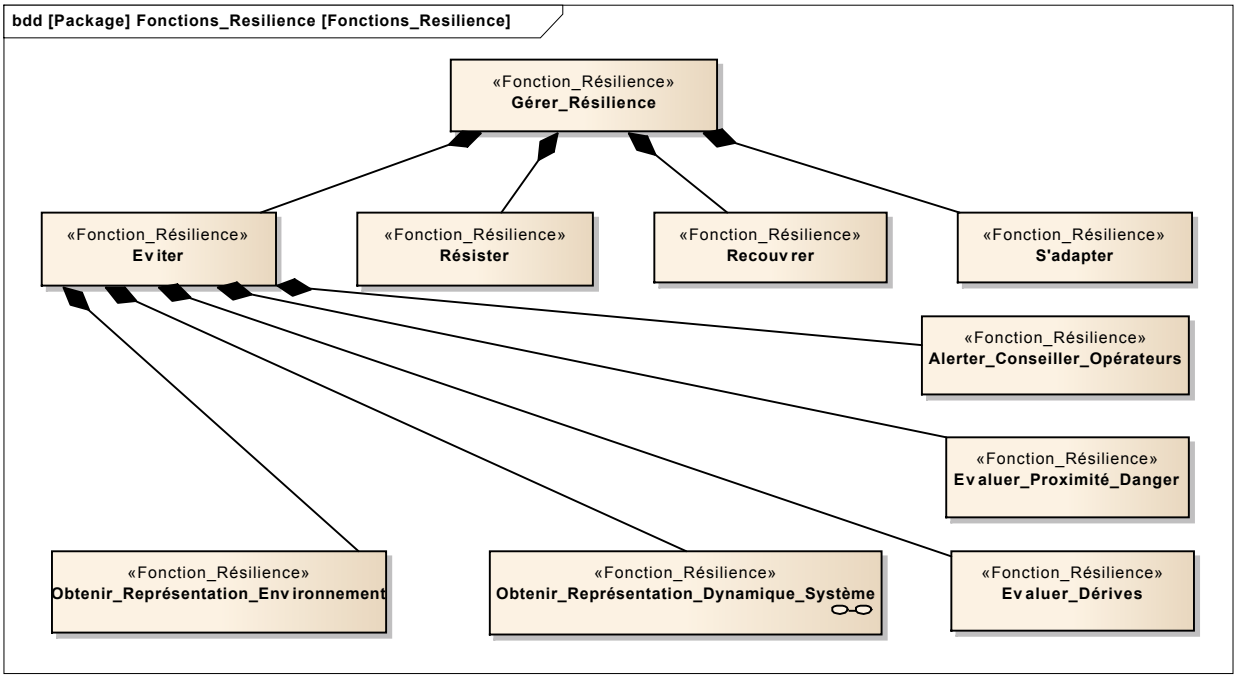

Figure 5.1. Décomposition fonctionnelle de la fonction « éviter »[23].

La relation de décomposition est exprimée par un symbole formé d'un losange noir suivi d'un trait, reliant la fonction (côté losange noir) à une sous-fonction. Cette relation peut être exprimée à plusieurs niveaux de décomposition fonctionnelle. Le symbole en bas à droite du bloc « obtenir une représentation de la dynamique de système » indique que l'on peut naviguer vers un autre diagramme auquel le bloc est lié.

La Figure 5.2 (diagramme d'activité SysML) montre l'organisation logique et temporelle des fonctions les unes par rapport aux autres.

Ces fonctions sont organisées en trois parties, en trois régions au sens SysML du terme :

- l'une de recueil des informations ;
- la seconde d'évaluation de la situation (usage, état) ;
- la troisième consacrée à l'alerte et au conseil des opérateurs.

[23] Rappel : même si la décomposition au premier niveau couvre les quatre fonctions de la résilience que sont « éviter », « s'adapter », « résister » et « recouvrer », seule la fonction « éviter » est traitée dans le cadre de la thèse.

Le flux entre fonctions commence par un état initial, représenté par un rond noir, et s'achève avec un état final, représenté par un point noir dans un cercle blanc. Chaque région comprend une ou deux fonctions. Les régions sont séparées par des barres marquant le début et la fin de fonctions concurrentes (fonctions menées en parallèle), barres représentées par des épais traits noirs.

Ainsi, pour le « recueil des informations », les fonctions « obtenir une représentation de l'environnement » et « obtenir une représentation de la dynamique du système » sont menées en parallèle. Les informations recueillies (par exemple, l'état des barrières) sont exploitées par les fonctions « évaluer les dérives » et « évaluer la proximité du danger ». Les informations issues de ces fonctions servent à alerter et conseiller les opérateurs lorsque le système est mis en œuvre hors de son domaine d'emploi et est à proximité d'une zone de danger.

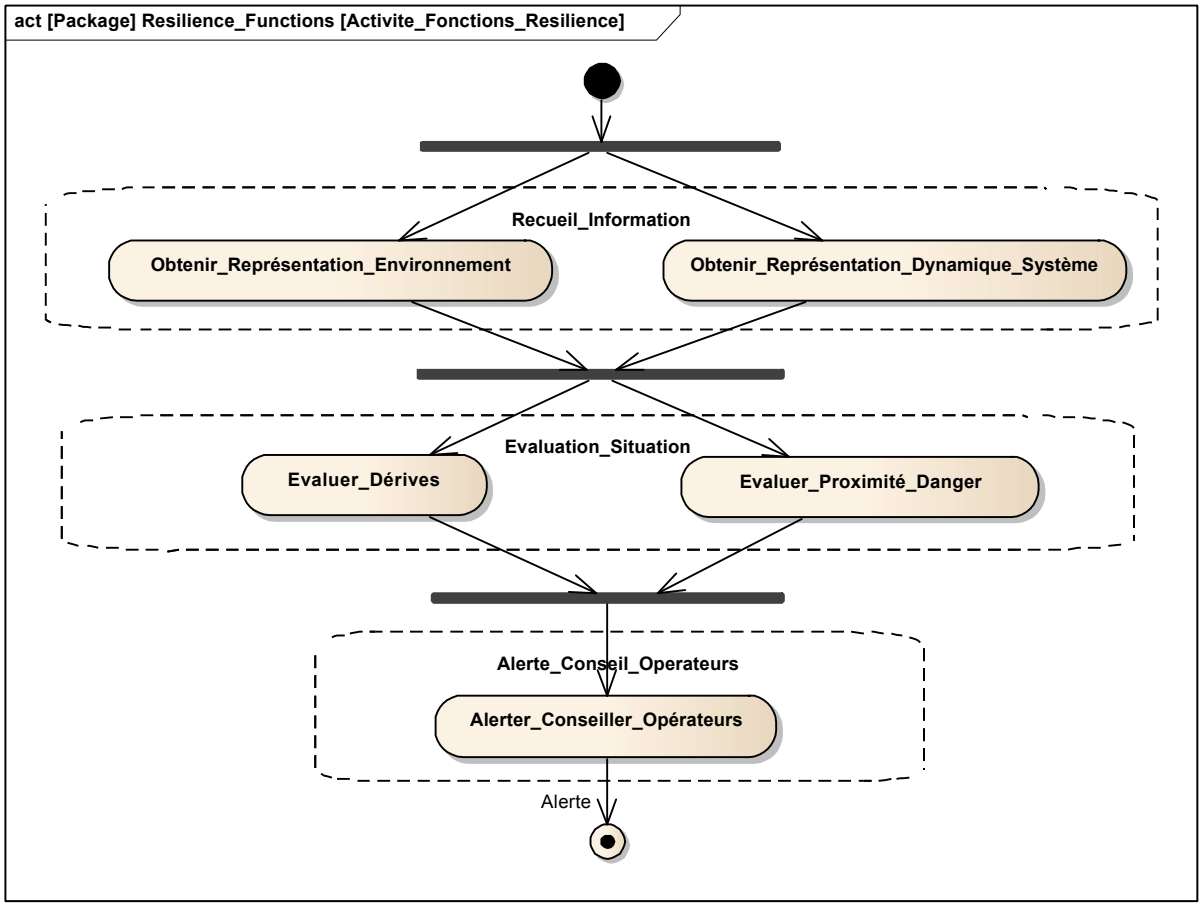

Figure 5.2. Diagramme d'activité de la fonction « éviter ».

Les sous-fonctions de la fonction « éviter » de la résilience ressemblent aux fonctions des HUMS sans pour autant être identiques. En effet, les objectifs sont différents. Les objectifs des fonctions HUMS, dans le cadre de la maintenance, visent à détecter l'usure de composants, leur vieillissement prématuré. Les objectifs des sous-fonctions de la fonction « éviter » de la résilience visent à connaître l'état et l'usage du système, son environnement, afin d'en informer les opérateurs pour qu'ils puissent élaborer et maintenir une représentation dynamique du système et de son environnement. Ces différences se traduisent par le choix des indicateurs mesurés, des types de traitements qui sont effectués sur les mesures obtenues, des critères d'alerte adaptés aux exigences de la résilience et par les valeurs de seuil qui sont déterminées par le domaine d'emploi prescrit. Ces différences se traduisent aussi par la façon de présenter ces alertes aux opérateurs. Le Figure 5.3 montre, de façon synthétique, la

correspondance entre les items des sous-fonctions de la fonction « éviter » de la résilience et les fonctions HUMS.

La prochaine étape est d'allouer les sous-fonctions de la fonction « éviter » aux composants du système de surveillance de l'usage et de l'état et aux composants du système interactif.

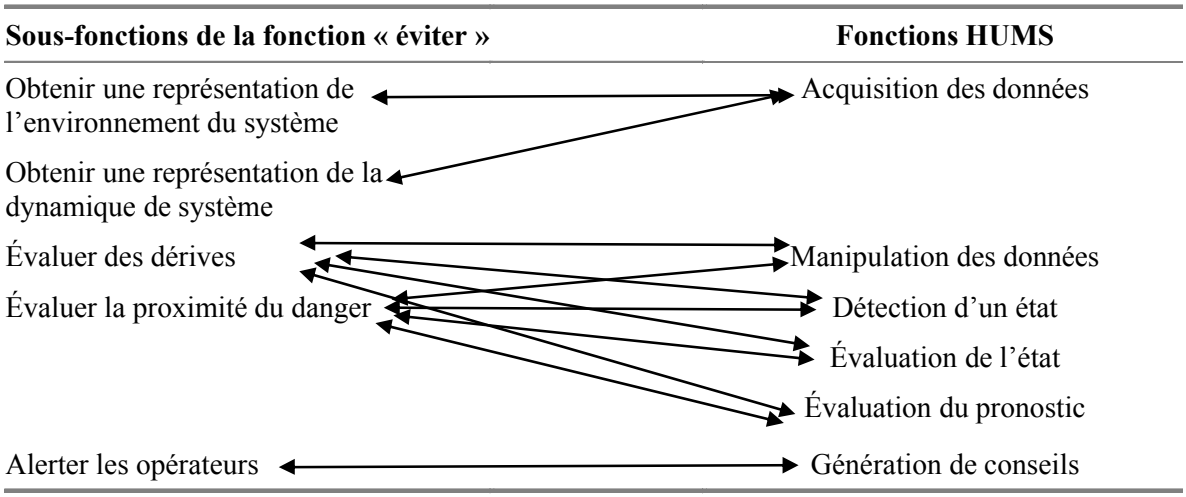

Figure 5.3. Correspondance entre les fonctions HUMS et les sous-fonctions de la fonction « éviter ».

5.2.2. Sous-fonctions de la fonction « éviter » : allocation au système de surveillance de l'usage et de l'état du système et au système interactif

Ces sous-fonctions de la fonction « éviter » sont réalisées par le système de surveillance d'usage qui comprend les composants suivants :

- les proxys[24] de capteur d'usage sont étroitement emboîtés aux dispositifs de sécurité ou d'autres composants du système. Ces proxys rassemblent les états et l'usage de ces composants pour les communiquer aux capteurs d'usage respectifs. Les proxys :
  - collectent des données analogiques, numériques ou manuelles ;
  - convertissent les données analogiques en données numériques ;
- les capteurs d'usage obtiennent des proxys, les états et les usages de dispositifs de sécurité et des composants des systèmes qu'ils traduisent pour être analysés. Les capteurs d'usage :
  - réalisent le traitement du signal ;
  - réalisent les moyennes ;
  - réalisent des calculs algorithmiques ;
  - réalisent l'extraction des caractéristiques critiques pour la résilience (franchissement de barrières, …) ;

[24] La traduction française de proxy est procuration, mais il est d'usage de conserver le terme technique de proxy.

- le dépôt des données courantes, données de la réalité des situations vécues par le système, stocke les données venant des capteurs d'usage et effectue les calculs pour évaluer l'état courant. Pour cela le dépôt des données courantes ;
  - calcule les valeurs courantes des indicateurs d'état et des statistiques ;
  - évalue l'état courant ;
  - stocke ces valeurs calculées ;
- le dépôt des données de référence contient les modèles de sécurité, tenant compte de la variabilité, des caractéristiques des barrières, ainsi que des données plus spécifiques. Ces modèles concernent le plan, ce qui est prévu et prévisible ;
- le moteur de comparaison compare les états actuels et les états de référence, pour évaluer les dérives et évaluer la proximité de danger. Il communique des niveaux d'alerte, des marges de sécurité et des informations sur les dérives aux proxys d'interface utilisateur. Pour cela le moteur de comparaison ;
  - évalue les dérives ;
  - établit l'état, les défauts et les défaillances diagnostiqués ;
  - détermine les alertes de limite de seuil ;
  - détermine la gravité de l'écart au-dessus ou en-dessous de la limite de seuil ;
  - détermine le niveau de criticité ;
  - produit des preuves et des explications ;
  - formule des recommandations
- les proxys d'interface utilisateur sont étroitement emboîtés à d'autres éléments de l'interface utilisateur du système. Les proxys d'interface utilisateur traduisent les alertes provenant du moteur de comparaison en informations conformes au modèle métier de l'utilisateur.

Le patron de conception « proxy » est choisi pour réduire le couplage entre les systèmes opérant, de surveillance de l'usage et interactif. Le proxy, déporté dans le système opérant ou dans le système interactif, ne comporte que les éléments nécessaires et suffisants pour assurer l'interface, par exemple pour recueillir les informations nécessaires dans le cadre d'un capteur. Les autres éléments font partie intégrante du système de surveillance de l'usage et de l'état. Cette solution d'architecture permet de faire évoluer les différents systèmes en limitant les impacts sur les autres systèmes. Dans la même perspective, cette solution d'architecture est cohérente avec une conception orientée aspect en séparant ce qui relève, d'un côté du système opérant et de l'autre côté du système de surveillance de l'usage et de l'état. Dans ce contexte, les points d'insertion, au sens de la conception orientée aspect, sont les proxys. L'aspect concerné relève du domaine « surveillance ».

Les traitements peuvent s'appuyer sur les travaux menés sur la surveillance des systèmes critiques (cf. section 2.5.1, « Système de surveillance de l'usage et de l'état d'un système - HUMS- (health *and usage monitoring systems)* »). Ces traitements font partie de nos pespectives de recherche pour les prochaines années (cf. Conclusion générale, section « Perspectives de recherche dans le domaine de la résilience des systèmes »).

Le Tableau 5.3 montre l'allocation possible des sous-fonctions de la fonction « éviter » aux composants du système de surveillance d'usage et au système interactif. Ce Tableau 5.3 montre que des fonctions s'appuient sur des mêmes composants. Ainsi, les capteurs d'usage réalisent les fonctions « Obtenir une représentation de l'environnement du système »,

« Identifier l'état de l'environnement », et « Obtenir une représentation de la dynamique de système ».

Nous pouvons les regrouper en trois ensembles, représentés par les groupes de cellules grisées dans le Tableau 5.3, en écho à l'organisation des fonctions en trois parties dans la Figure 5.2 (diagramme d'activité) :

- obtenir une représentation de la dynamique de système et de son environnement ;
- évaluer les dérives et la proximité du danger ;
- alerter les opérateurs lorsque le système est proche d'une zone de danger, conseiller les opérateurs en proposant un mode opératoire sûr.

Le premier et le troisième ensembles sont connectés avec des composants du système, ils ont donc des interfaces externes au système de surveillance de l'état et de l'usage. Le second ensemble recueille les informations du premier et communique des notifications au troisième. Il ne présente pas d'interface externe.

Fonctions / **Composants**	Obtenir une représentation de l'environnement du système	Obtenir une représentation de la dynamique de système	Evaluer des dérives	Évaluer la proximité du danger	Alerter et conseiller les opérateurs
Proxy de capteur d'usage	X	X			
Capteur d'usage	X	X			
Dépôt des données courantes			X	X	
Dépôt des données de référence			X	X	
Moteur de comparaison des états			X	X	
Proxy de l'interface utilisateur					X
Interface utilisateur					X

Tableau 5.3. Allocation des sous-fonctions de la fonction « éviter » aux composants du système de surveillance d'usage et d'état du système et à l'interface utilisateur.

L'architecture du système principal comprend le système opérant, le système de surveillance d'usage et le système interactif. Nous différencions ces trois systèmes qui sont trois des sous-systèmes du système principal. Par commodité de langage, nous conservons les notions de système opérant, de système de surveillance d'usage et de système interactif. La Figure 5.4 (diagramme de définition de bloc SysML) illustre cette structure du système principal.

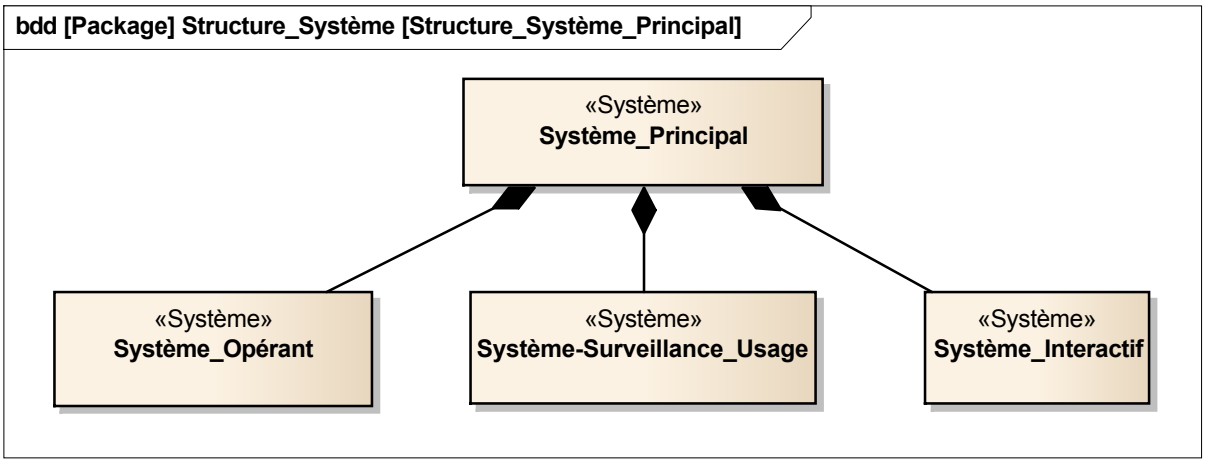

Figure 5.4. Structure du système principal.

5.2.3. Système de surveillance de l'usage et de l'état du système

Nous présentons de façon plus détaillée le système de surveillance d'usage dans cette section et le système interactif dans la section 5.2.4 intitulée « Système interactif : représentation de la situation à l'opérateur », sans entrer dans les détails du système opérant et des autres systèmes contributeurs qui ne participent pas directement à la résilience du système.

Le diagramme de définition de bloc SysML de la Figure 5.5 montre l'architecture physique du système de surveillance d'usage, ainsi que chaque composant avec ses opérations et attributs, lesquels doivent être adaptés aux spécificités de domaine et des objectifs de sécurité. Outre la relation de décomposition marquée par le symbole du losange noir, ce diagramme présente les cardinalités, ainsi, le système de surveillance d'usage comprend un ou plusieurs proxys d'interface utilisateur. Chaque composant est caractérisé par ses interfaces externes et les flux propres à ces interfaces.

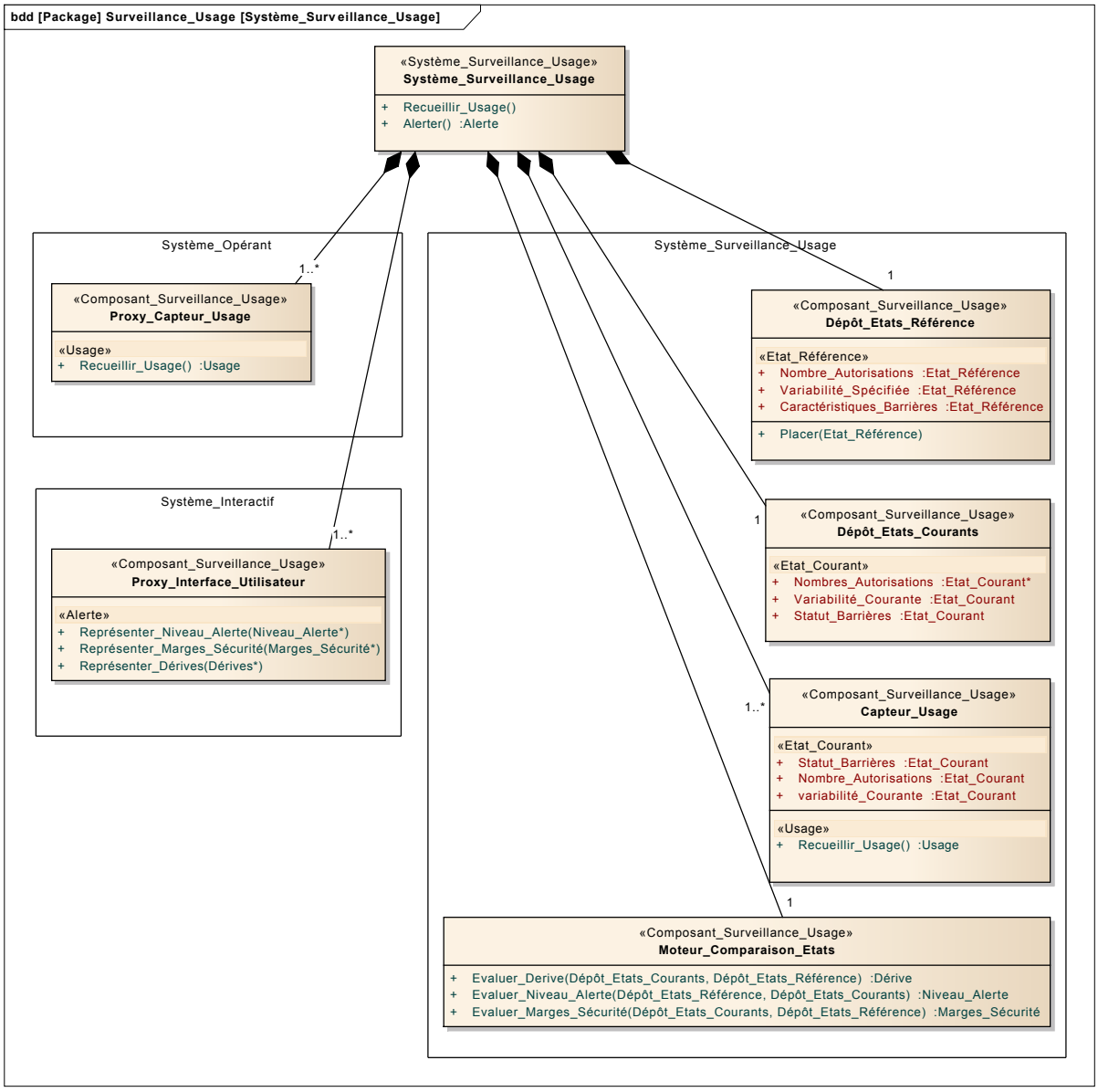

Figure 5.5. Architecture physique du système de surveillance d'usage et d'état du système.

Ce diagramme montre que le proxy de capteur et le proxy interface utilisateur, quoique faisant partie fonctionnellement du système de surveillance de l'usage et de l'état du système principal, sont physiquement dans le système opérant et dans le système interactif. Cette solution d'architecture permet de réduire le couplage entre le système opérant et le système de surveillance de l'usage et de l'état du système principal.

Ces trois systèmes, système opérant, système de surveillance d'usage et système interactif, communiquent entre eux. Le système opérant expose, montre, son usage, son état, l'état de l'environnement dans lequel il est, au système de surveillance d'usage. Cela peut consister à présenter l'état des barrières de sécurité, ou la variabilité de son fonctionnement. Le système de surveillance d'usage notifie au système interactif les alarmes, les informations nécessaires aux opérateurs pour qu'ils puissent élaborer une représentation de la situation. Ces informations, de type alerte, peuvent concerner les dérives, les marges de sécurité, ou la proximité du danger, par exemple. Le diagramme de bloc interne SysML de la Figure 5.6 représente les interfaces et les flux entre ces trois systèmes.

Il est important de noter que notre proposition des informations de type alerte est à compléter et à adapter en fonction du système à surveiller, des informations dont les opérateurs ont besoin pour élaborer et maintenir une représentation dynamique du système et de son environnement.

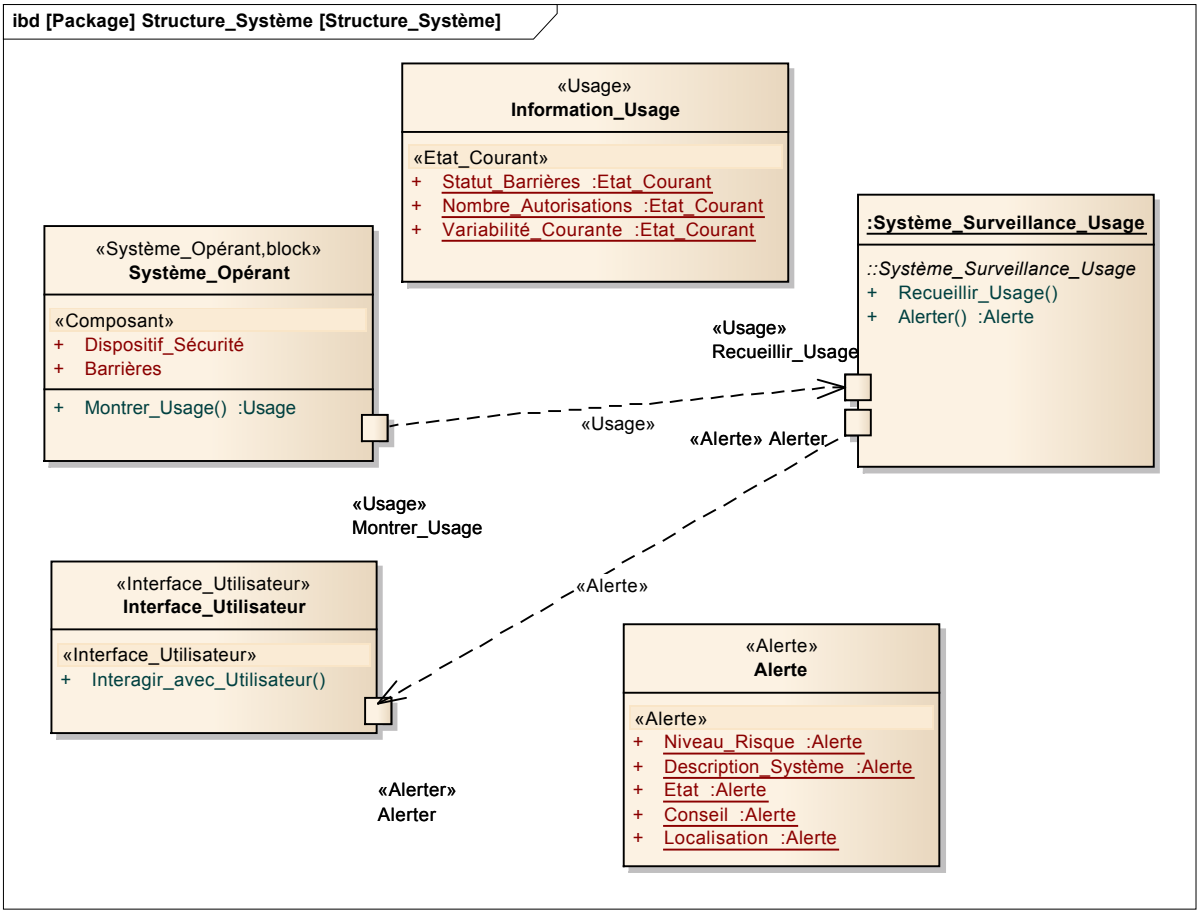

Figure 5.6. Interfaces et flux entre systèmes opérant, surveillance d'usage et interactif (interface utilisateurdans la figure).

Ces informations de type « alerte », sont structurées en six blocs :

- le niveau de risque :
  - la sévérité (catastrophique, critique, marginal, négligeable) ;
  - la probabilité (fréquent, probable, occasionnel, isolé, improbable) ;
  - la criticité (élevé, sérieux, moyen, faible) ;
- la description du système :
  - l'identifiant du composant du système concerné ;
- l'état évalué :
  - les données historiées de l'état du système ;
  - le problème diagnostiqué (défaut, défaillance…) ;
  - les dérives constatées ;
  - l'état courant ;
  - l'état de référence ;

    - l'écart entre l'état courant et l'état de référence ;
    - la proximité d'une zone de danger ;
    - le type de danger identifié ;
    - les marges de réserves disponibles ;
- les conseils :
    - les actions recommandées, pouvant comporter des alternatives.
- le contexte de l'alerte :
    - horodatage ;
    - localisation (coordonnées GPS…) ;
- le niveau de confiance de l'alerte :
    - niveau de confiance.

La Figure 5.7 (diagramme de bloc interne SysML) illustre le modèle de données des informations de type « alerte » échangées entre les systèmes.

Ces alertes sont normalisées et adaptées aux domaines métier afin que les différents systèmes fournissent des alertes avec un format et une signification que tous les systèmes peuvent interpréter.

Figure 5.7. Modèle de données des alertes échangées entre systèmes.

Cette proposition d'architecture peut être mise en œuvre dans de nombreux domaines. La Figure 5.8 (diagramme de bloc interne SysML) illustre cette proposition dans le domaine du transport, comprenant des systèmes de différents types.

Ce domaine comprend, entre autres, des systèmes de supervision de trafic, des systèmes d'infrastructure (aéroport, gare, voies, infrastructure électrique…), des trains, des avions, des bateaux, etc. Chacun de ces différents systèmes comprend un système opérant, un système de surveillance d'usage et un système interactif.

Cette organisation peut être appliquée à des systèmes d'autres domaines. Ainsi, le système de gestion du trafic, comme le train et l'infrastructure et l'avion, sont des systèmes qui héritent des caractéristiques du système de transport, par exemple les règlements qui s'y appliquent. Chacun de ces systèmes présente les interfaces du système opérant, du système de surveillance d'usage et du système interactif qui le composent, caractérisées par les stéréotypes adéquats. Dans le diagramme de définition de bloc SysML de la Figure 5.8, outre la relation de composition (symbole présentant la forme d'un losange noir suivi d'un trait), le symbole formé par une flèche vide dénote la relation de généralisation.

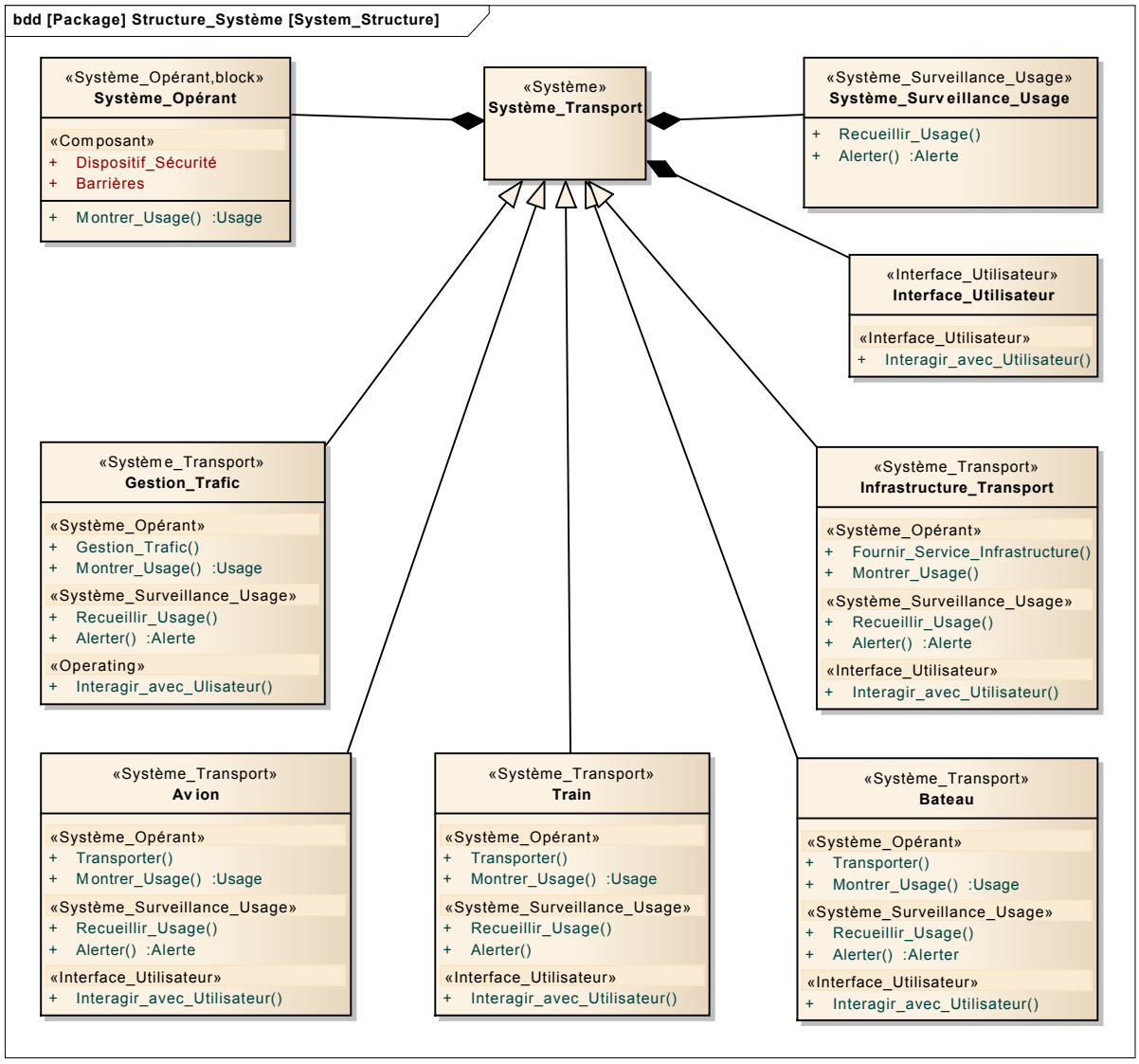

Figure 5.8. Architecture de systèmes dans le domaine du transport héritant de l'architecture comprenant un système opérant et un système de surveillance d'usage.

Ces différents systèmes ne sont pas indépendants les uns des autres. Ils interagissent les uns avec les autres afin de produire les services attendus. Par construction, certains systèmes communiquent à d'autres systèmes des informations ; c'est par exemple le cas du système de régulation de trafic ferroviaire qui communique aux conducteurs de train les consignes, *via* les signaux des voies. En revanche, toujours par construction, certains systèmes communiquent avec d'autres systèmes de façon sommaire, voire ne communiquent pas du tout. Ainsi, dans certains cas de figure, seuls des indicateurs sonores et visuels de proximité sont utilisés directement entre l'infrastructure ferroviaire et les trains lorsqu'il y a des travaux sur les voies. Traditionnellement, le système de régulation a en charge de médiatiser cette communication.

Plusieurs systèmes différents, hétérogènes, interagissent, qu'ils soient co-localisés ou en revanche distants les uns des autres, de façon synchrone ou asynchrone, dans un même domaine métier, ou dans des domaines métier différents. Dans certains cas, les interactions sont indirectes et se résument à l'utilisation de ressources communes, lesquelles nécessitent de mettre en œuvre des règles de sécurité ou des règles d'accès exclusif temporaire aux ressources communes ou parce qu'un système génère des contraintes sur un autre, même s'ils n'ont aucun lien fonctionnel entre eux. Dans certains contextes, des systèmes différents, concourant à un même processus global, doivent se passer le relais (*handover*) et se coordonner. Enfin, il n'y a pas nécessairement un ordonnanceur commun qui organise la coordination entre systèmes et avec lequel les autres systèmes seraient dans une relation maître-esclave. Il s'agit de systèmes autonomes, interagissant avec les autres systèmes dans une relation de parité. L'ensemble de ces systèmes pourrait être formalisé en un graphe, un système pouvant passer d'une clique[25] à une autre, dynamiquement, à la volée.

Dans le domaine aéronautique, ainsi que l'illustre la Figure 5.9, le système *Automatic Dependent Surveillance* Broadcast (ADS-B) (Ali *et al.*, 2015), (O'Brien, 2010), permet aux avions qui en sont équipés de diffuser à rythme régulier des informations aux avions et dispositifs de contrôle aérien terrestre qui disposent des récepteurs adaptés.

[25] Dans la théorie des graphes, une clique est un ensemble de sommets deux-à-deux adjacents (notion de graphe complet).

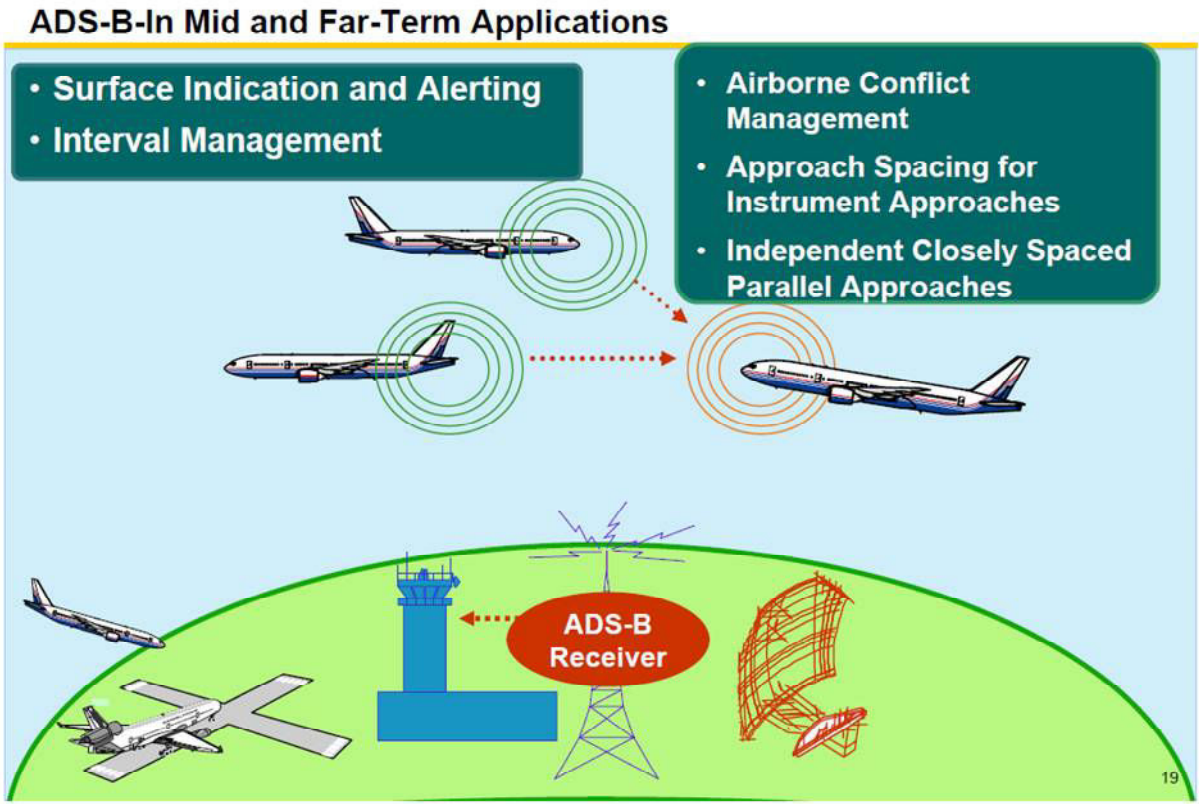

Figure 5.9. Communication d'information entre avions avec l'ADS-B, Boeing© (O'Brien, 2010).

La Figure 5.10 (diagramme de bloc interne SysML) illustre cette connexion entre systèmes. Chacun d'eux comprend un système opérant, un système de surveillance d'usage et un système interactif, ainsi que les interfaces associées. Chacun d'eux comprend aussi une interface avec les autres systèmes, communiquant les alertes (valeur et orientation des dérives, marges de sécurité…) de façon bidirectionnelle.

La première étape de notre contribution a consisté à recueillir les informations relatives à l'état et à l'usage du système, puis à traiter ces informations pour détecter les dérives, la proximité d'une zone de danger. Ces informations de type alerte doivent maintenant être adaptées en fonction de la tâche des opérateurs, des systèmes interactifs dont ils disposent pour réaliser cette tâche. Cette adaptation fait l'objet de la section suivante.

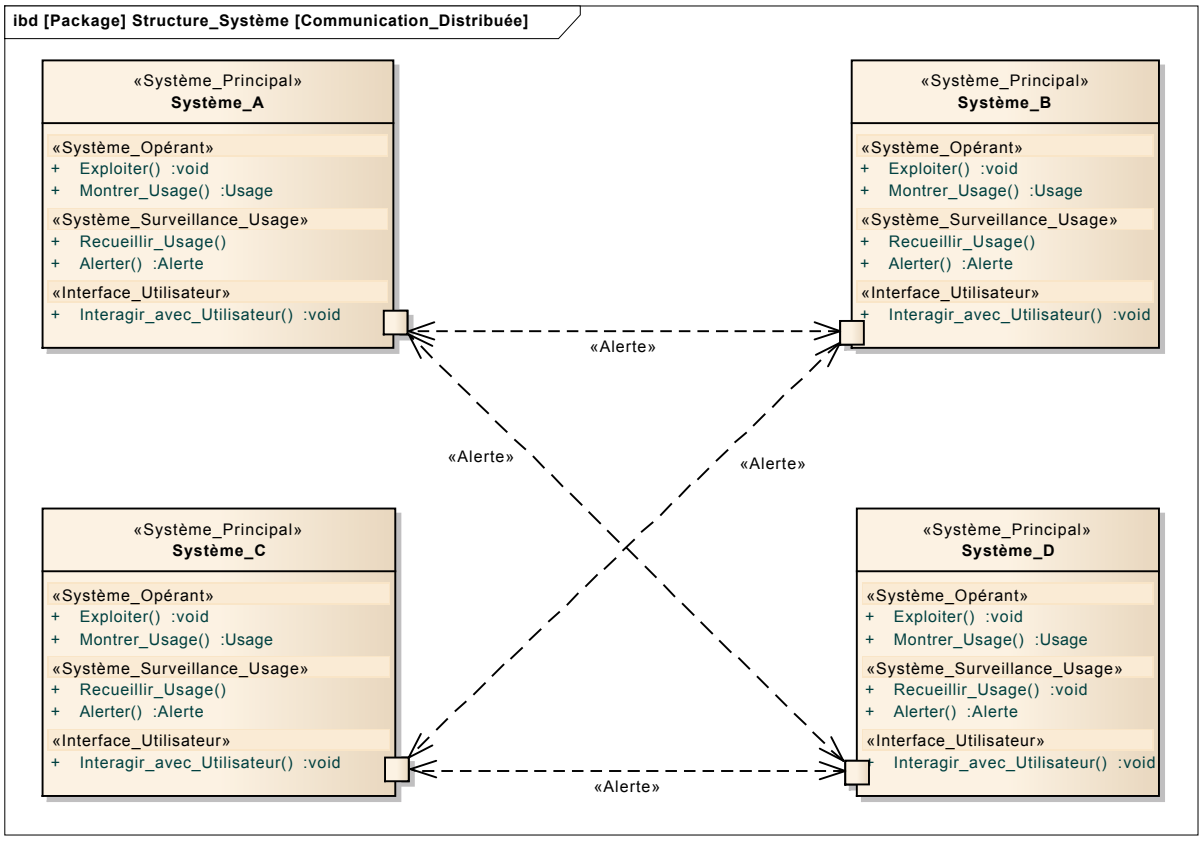

Figure 5.10. Communication des alertes entre systèmes.

5.2.4. Système interactif : représentation de la situation à l'opérateur

Les éléments clés de la résilience résident en partie dans la qualité des IHM (cf. section 1.3.3, « La résilience des systèmes sociotechniques ») et leur capacité à donner aux opérateurs les moyens de comprendre la situation et l'état du système réel par rapport à la situation et à l'état de référence (Ruault *et al.*, 2013), pour détecter les migrations et les compensations qui ont lieu et pour permettre une navigation à vue. Par ailleurs, la qualité des IHM est essentielle lorsque les opérateurs mettent en œuvre une démarche d'essai-erreur et ont besoin d'informations pertinentes produites par leurs essais afin de comprendre les réussites et les erreurs (cf. section 1.2.3, « Les franchissements de barrières, les violations des règles de sécurité et les migrations spontanées »). Après avoir recueilli l'état réel du système, celui de son environnement, et les avoir comparés avec leurs états de référence, les informations doivent être adaptées aux modèles que les opérateurs ont du système et de son fonctionnement pour construire les IHM (cf. section 1.3.3, « La résilience des systèmes sociotechniques »). Des IHM qui ne représenteraient pas l'état réel du système, des informations erronées ou dont la représentation ne seraient pas adaptée aux modèles qu'en ont les opérateurs généreraient des confusions et seraient une source d'accidents (cf. section 1.3.3, « La résilience des systèmes sociotechniques »).

Dans la perspective de l'approche centrée sur la régulation, le système interactif doit offrir aux opérateurs les moyens pour qu'ils puissent élaborer, partager et maintenir une conscience de la situation, une représentation fonctionnelle et dynamique du système et de son environnement, continuellement mise à jour en fonction des évènements qui adviennent (cf. section 1.4, « Comprendre la situation pour éviter l'accident »). Cette représentation leur permet de mettre en œuvre une sécurité régulée et un ajustement permanent à l'environnement

dynamique que le système rencontre. Le système interactif doit fournir un cadre d'interprétation commun, cohérent et non ambigu, dans lequel chacun peut poursuivre ses activités sans interrompre l'autre, basée sur une stratégie de communication implicite. Les opérateurs doivent avoir les moyens de comprendre l'état du système qu'ils opèrent, mais aussi des systèmes de l'environnement avec lesquels le système interagit, en particulier lorsque ces systèmes se trouvent dans des situations pouvant affecter la sécurité.

Les modalités d'élaboration et d'entretien d'une conscience partagée de la situation, en particulier dans le contexte de situations imprévisibles, sans précédent, font partie de nos perspectives de recherche pour les prochaines années (cf. Conclusion générale, section « Perspectives de recherche dans le domaine des IHM et de l'ergonomie »).

Les informations de type « alerte » ne sont pas des signaux temporaires, fugaces, présentant un état instantané, voire qui apparaissent puis disparaissent alternativement sous l'effet d'oscillations erratiques, lesquels signaux ne permettent pas aux opérateurs de comprendre la situation et la dynamique du système. Ces alertes doivent exprimer, représenter, les évolutions temporelles des états, les tendances sur le long cours, la position du système par rapport à son environnement, ainsi que la position du système par rapport à une zone supposée sûre et aux zones de danger. Ces alertes doivent être pondérées en fonction du niveau de criticité de la situation.

Ces informations communiquées entre systèmes sont des informations abstraites, indépendamment de la façon dont elles sont représentées aux opérateurs de ces différents systèmes (cf. section 3.4.3 intitulée « Architecture pour les IHM distribuées »). En effet, les représentations de ces informations doivent être adaptées à la tâche des opérateurs, à leurs modèles mentaux, aux caractéristiques et contraintes des dispositifs d'interaction homme-machine (cf. section 3.4.3 intitulée « Modèle de la tâche »). Ces adaptations doivent conserver intègre la signification des alertes qui sont présentées aux opérateurs, par exemple le niveau de criticité, sans remettre en cause des contraintes de dialogue. Elles doivent donc être transformées afin d'être présentées aux opérateurs de façon appropriée, en tenant de l'environnement, de la tâche. En effet, l'alerte doit être présentée aux opérateurs en s'inscrivant dans leurs tâches, en étant plus ou moins intrusive en fonction du niveau de criticité. La transformation des informations abstraites en représentations adaptées aux besoins des opérateurs s'appuie sur les composants des systèmes interactifs.

En adaptant le modèle CAMELEON, présenté dans la section 3.4.3 « Architecture pour les IHM distribuées », nous différencions, d'une part ce qui relève du contexte, et, d'autre part ce qui relève des composants des systèmes interactifs. Le contexte concerne les caractéristiques des utilisateurs (abordées dans les sections 3.3.1 « Modèle de l'utilisateur », 3.3.2 « Persona individuel / collectif » et 3.3.3 « Modèle de la tâche »), les caractéristiques de l'environnement, et celles de la plateforme des systèmes interactifs (cf. Figure 5.11). Les composants des systèmes interactifs concernent le domaine métier et la tâche (abordée dans la section 3.3.3 « Modèle de la tâche »), les composants abstraits, les composants concrets et les composants finaux de l'interface (cf. Figure 5.12).

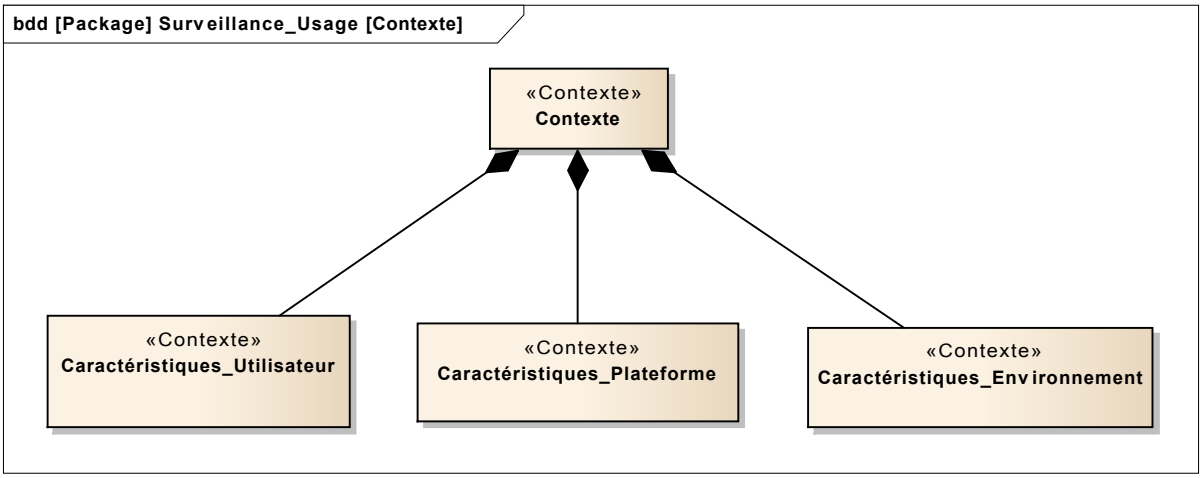

Figure 5.11. Modèle du contexte (adapté de Calvary *et al.*, 2003).

Le contexte présente un ensemble de contraintes que prennent en compte les composants des systèmes interactifs pour effectuer les transformations. Ainsi le besoin d'opérateurs postés dans une salle de contrôle comprenant des panneaux synoptiques et dans laquelle la luminosité et le niveau sonore sont régulés est différent du besoin d'opérateurs rondiers mettant en œuvre un dispositif mobile, par exemple une tablette ou un téléphone mobile, dans un environnement lumineux et sonore non maîtrisé. Le contexte concerne aussi les caractéristiques des utilisateurs exprimées par le persona. Le persona peut rendre compte du niveau de vigilance d'un opérateur, ainsi que le comportement de franchissement de barrières par un groupe d'opérateurs. Ces besoins différents peuvent se traduire, dans le premier cas, par une représentation globale du processus sur une vue synoptique tandis que dans le second cas seront présentées des informations de proximité sur un dispositif mobile.

Les composants de l'interface utilisateur doivent comprendre l'ensemble des moyens pour traduire une alerte afin de la présenter aux opérateurs de façon appropriée au contexte.

Ces composants peuvent traduire une alerte en signal sonore et en message oral produit par un composant de synthèse de la parole dans le contexte où cette modalité est plus appropriée que la modalité visuelle (faible luminosité, modalité visuelle sollicitée par une autre dimension de la tâche…) (cf. section 3.4, « Architecture des systèmes interactifs »). Ces composants peuvent aussi traduire cette alerte en retour d'effort pour indiquer la proximité d'une zone de danger ou la limite par rapport au domaine de fonctionnement sûr. Enfin, les composants de l'interface utilisateur peuvent mettre en œuvre les ressources de la réalité augmentée. Il est ainsi possible de surimposer l'image d'un obstacle qui est hors du champ visuel sur l'IHM de l'opérateur (cf. section 3.4, « Architecture des systèmes interactifs »).

Ces composants doivent être adaptés aux types de réponses que les opérateurs mettent en œuvre, des réponses routinières ou des réponses de type résolution de problème. Ces adaptations des composants font l'objet de certaines de nos perspectives de recherche (cf. Conclusion générale, section « Perspectives de recherche dans le domaine des IHM et de l'ergonomie »).

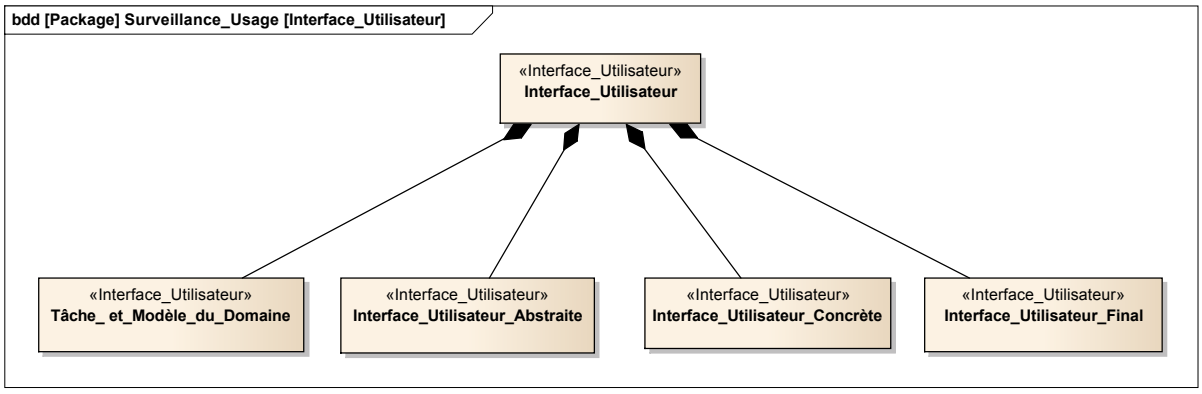

Figure 5.12. Modèle des composants de l'interface utilisateur (adapté de Calvary *et al.*, 2003).

Dans une logique de bout en bout, les informations d'alerte, abstraites, issues des systèmes de surveillance de l'usage sont communiquées au proxy d'interface utilisateur. Le proxy d'interface utilisateur reçoit les notifications des alertes émises par les autres systèmes. Il les traduit en concepts du domaine pour les communiquer aux composants éponymes de l'interface utilisateur (cf. Figure 5.13). Les transformations se suivent en cascade, des concepts du domaine en objets d'interface abstraits, puis en objets d'interface concrets, puis en objets d'interface final (cf. Figure 5.13).

Ces transformations successives visent à traduire les alertes en composants d'interface adaptés aux opérateurs, à leurs tâches, ainsi qu'aux plateformes utilisées pour ces tâches.

Les traitements et l'implémentation de la chaîne de transformation entre le message d'alerte et l'interface utilisateur sont à approfondir dans de futures recherches (cf. Conclusion générale, section « Perspectives de recherche dans le domaine des IHM et de l'ergonomie »).

Ainsi, les opérateurs peuvent régler leurs activités, évaluer les différences entre la situation de système actuelle et le domaine de référence du système, détecter, dès que possible, la migration ou les mécanismes de compensation. Nous suggérons une solution qui exprime la dérive progressive de la situation sûre à une situation à risque élevé (Ruault *et al.*, 2013).

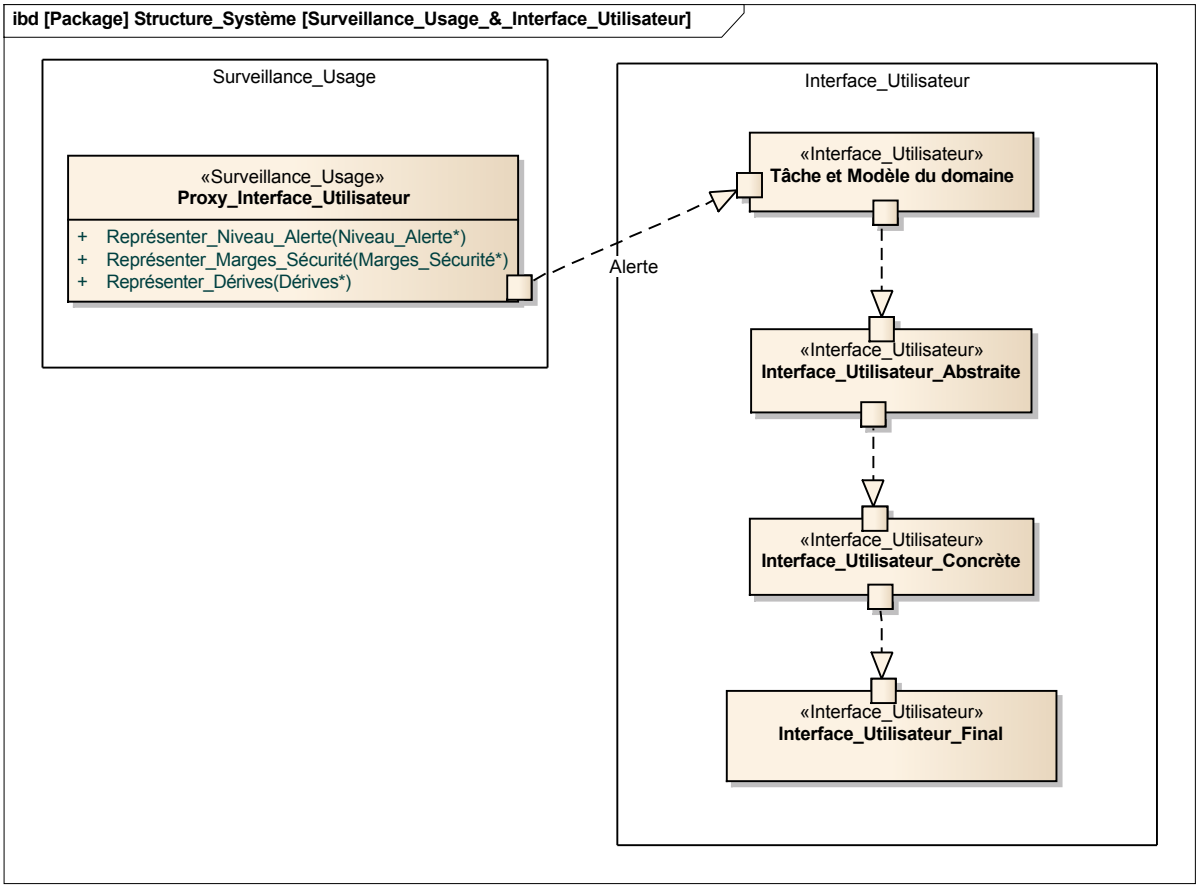

Figure 5.13. Transformation des informations au sein de l'architecture CAMELEON (adapté de Calvary *et al.*, 2003).

La Figure 5.14 illustre cette solution, basée sur la matrice de criticité (MIL-STD, 2012), en montrant aux opérateurs que le système dérive et peut même se retrouver dans une zone à haut risque avec des conséquences catastrophiques. Pour les systèmes à longue durée de vie, une telle dérive peut s'inscrire dans la durée et être complètement banalisée dans la mise en œuvre régulière du système. Cela la rend d'autant moins perceptible à l'œil nu par les opérateurs et un dispositif mettant en évidence une telle dérive d'autant plus nécessaire.

Sévérité / Probabilité	Catastrophique (1)	Critique (2)	Marginal (3)	Négligeable (4)
Fréquent (A)	Élevé	Accident	Sérieux	Moyen
Probable (B)	Élevé	Élevé	Sérieux	Moyen
Occasionnel (C)	Élevé	Sérieux	Moyen	Faible
Isolé (D)	Sérieux	Moyen	Moyen	Faible
Improbable (E)	Moyen	Moyen	Moyen	Faible
Éliminé (F)	Éliminé			

Figure 5.14. IHM montrant les étapes de la dérive (1, 2, 3) vers une zone de risque élevé aux conséquences catastrophiques (Ruault *et al.*, 2013).

Dans la perspective où plusieurs opérateurs collaborent ensemble, cela doit se traduire par une architecture distribuée des interfaces utilisateurs. Une alerte est envoyée aux différents systèmes interactifs des différents opérateurs. Chacun de ces systèmes interactifs transforme l'alerte afin de la présenter aux opérateurs de façon appropriée à leurs tâches, aux dispositifs d'interface utilisateur qu'ils utilisent.

Ainsi, l'ensemble des opérateurs concernés sont informés de l'alerte, et pour chacun d'eux, cette information est appropriée à sa tâche et la signification est univoque afin que cette alerte contribue à la représentation dynamique que les opérateurs maintiennent et au cadre commun d'interprétation de la situation et des événements de l'environnement.

Dans la même perspective que la chaîne de transformation entre le message d'alerte et l'interface utilisateur sera l'objet de futures recherches, la conception de l'interface utilisateur doit aussi être une perspective de recherche pour que cette interface soit adaptée à la tâche de l'opérateur (cf. Conclusion générale, section « Perspectives de recherche dans le domaine des IHM et de l'ergonomie »).

5.3. Synthèse et conclusion du chapitre

Notre contribution relative à l'architecture d'un système résilient s'articule sur le patron de conception « surveiller et alerter ». L'objectif de ce patron de conception est de surveiller l'état et l'usage du système opérant et d'alerter les opérateurs quand le système opérant s'éloigne de son domaine d'emploi et est à proximité d'une zone de danger.

Ce patron de conception permet de modéliser l'architecture fonctionnelle de la résilience d'allouer les sous-fonctions de la fonction « éviter » de la résilience aux composants que sont, d'une part le système de surveillance de l'usage et de l'état du système et, d'autre part le système interactif. Il reprend et adapte les travaux sur le HUMS.

En particulier, ce patron de conception structure les fonctions et les composants afin de réduire le couplage entre eux. Ainsi, cette solution d'architecture permet de faire évoluer les fonctions et les composants en limitant les impacts sur les autres éléments.

Il propose un modèle de données pour l'alerte qui ouvre la voie à la communication d'une alerte entre systèmes dans la perspective de communication distribuée.

Enfin, l'alerte est traduite par le système interactif afin de présenter cette information aux opérateurs de façon appropriée et adaptée à leurs modèles mentaux, à leurs tâches et aux dispositifs d'interaction qu'ils utilisent.

Ainsi les différents systèmes interactifs contribuent à diffuser les informations sur la situation réelle, la situation courante, la comparant avec la situation de référence supposée sûre, et donc permettre aux opérateurs de partager un même référentiel, un même cadre d'interprétation pour élaborer une conscience partagé de la situation et naviguer à vue.

Cette proposition répond au besoin de restaurer la contrôlabilité des systèmes afin que les opérateurs puissent naviguer à vue et s'autoréguler mutuellement.

Cette contribution devra être évaluée pour valider la capacité de la solution proposée à donner aux opérateurs une représentation de la dynamique du système et de son environnement, en temps réel, afin qu'ils puissent conduire à vue et contrôler le système. Cela implique d'instrumenter un système et de le mettre en œuvre dans des situations imprévisibles, sans précédent, avec des opérateurs, dans un simulateur. Cela permet de mesurer leur capacité à naviguer à vue, de contrôler le système. Une telle évaluation (dans le cadre de situations

réelles) n'est pas traitée dans ce mémoire et correspond à une de nos perspectives de recherche pour les années à venir (cf. Conclusion générale, section « Perspectives de recherche pour la validation du patron de conception « surveiller et alerter » »). Par contre, les études de cas du Chapitre 7 « Application au domaine ferroviaire du patron de conception « surveiller et alerter » et du persona » présentent la faisabilité de l'instrumentation du système en appliquant le patron de conception pour la fonction « éviter » de la résilience.

Ce chapitre, consacré au patron de conception « surveiller et alerter » pour l'architecture d'un système résilient, est complété, dans le chapitre suivant, de la proposition de processus à mettre en œuvre pour contribuer à la résilience d'un système. Cette proposition suggère des évolutions des processus d'ingénierie système, intègre la contribution du processus d'appropriation à l'ergonomie prospective et les adaptations des personas individuel et collectif aux systèmes critiques à longue durée de vie.

En synthèse notre contribution du patron de conception « surveiller et alerter » pour l'architecture d'un système résilient vise à :

- recueillir l'état et l'usage du système opérant, évaluer le niveau de risque, la proximité d'une zone de danger et envoyer une alerte à l'interface utilisateur ;
- représenter aux utilisateurs cette alerte de façon adaptée aux dispositifs d'interface qu'ils utilisent, à leurs modèles mentaux, à leurs tâches, afin qu'ils puissent élaborer et entretenir une représentation fonctionnelle et continuellement mise à jour de l'environnement et du système.

Chapitre 6.
Proposition de processus à mettre en œuvre pour contribuer à la résilience d'un système critique à longue durée de vie

6.1. Introduction

Ce second chapitre de contribution est consacré au « système pour faire », c'est-à-dire l'ensemble des processus et activités menés pour faire le système et, plus particulièrement, pour le concevoir (processus de conception), et effectuer le retour d'expérience pour faire évoluer le « système à faire ».

La démarche globale consiste à tisser les liens entre les différents concepts présentés dans l'état de l'art, de les organiser entre eux afin de les appliquer à la conception des systèmes à longue durée de vie. *In fine*, l'objectif est que ces systèmes mènent à bien les missions qui leur seront confiées, dans des environnements opérationnels qui ne peuvent pas être décrits de façon claire, précise et systématique, comme le préconisent les bonnes pratiques de l'ingénierie système. Ces systèmes devront s'adapter à des situations qui sont inconnues et inimaginables lors de leur conception. Nous nous inscrivons dans une démarche de conception itérative sur le long terme s'appuyant sur le retour d'expérience de l'usage routinier et sur les résultats de la veille pour adapter le système aux environnements et situations opérationnels qui ne pouvaient être envisagés lors de la conception initiale.

Cette démarche de conception itérative est à la fois et de façon complémentaire proactive et réactive (Boy, 2013). Proactive, puisque cette démarche doit être planifiée, organisée au plus tôt, avec des impacts tant sur l'architecture du système que sur les processus d'ingénierie. Réactive puisqu'il s'agit de s'adapter à des situations qui ne peuvent pas être prévues et anticipées. Pour disposer d'une cohérence globale, cette démarche s'appuie sur une logique d'organisation et de planification. Afin de ne pas hypothéquer les activités et technologies futures, et de réagir face à des aléas et à des événements sans précédent, elle conserve une logique d'ouverture et d'adaptabilité. Elle propose les moyens d'apprendre en marchant et que cet apprentissage permette d'anticiper avec un bon niveau de confiance.

Nous commençons en proposant des évolutions des processus d'ingénierie système. Nous continuons en articulant l'ergonomie prospective avec le processus d'appropriation. Nous poursuivons en faisant évoluer le processus d'appropriation pour prendre en compte la veille et le retour d'expérience. Nous continuons en développant les notions de conception pour l'appropriation et de conception par l'appropriation. Nous montrons l'adaptation de l'ergonomie prospective aux spécificités des systèmes à longue durée de vie. Nous finissons le chapitre en mettant en œuvre le concept de persona.

6.2. Contribution à des évolutions des processus d'ingénierie système

Les processus d'ingénierie système doivent évoluer pour intégrer les processus de conception centrée utilisateur (ISO, 2010b), faire évoluer l'architecture[26] pour prendre en compte l'intégration du système de surveillance de l'usage et de l'état et prendre en compte les processus d'appropriation et d'adaptation du système technique par les opérateurs (Ruault, 2009).

Les premiers impacts de l'intégration du système de surveillance de l'usage et de l'état concernent les processus techniques d'ingénierie système (cf. section 2.3 « Processus d'ingénierie »).

Il s'agit de déterminer les mesures permettant d'évaluer si le système est mis en œuvre dans son domaine d'emploi ou fonctionne hors de ce domaine d'emploi. Ces mesures doivent aussi caractériser l'état courant du système, sa dynamique dans le temps, mais aussi l'état et la dynamique de l'environnement avec lequel le système interagit. La détermination et la sélection de ces mesures, parmi la multitude de mesures potentiellement disponibles, doivent être pilotées par la gestion des risques et l'analyse préliminaire de sécurité. En effet, la surveillance du système hors de son domaine d'emploi est complémentaire de l'analyse de sécurité qui détermine les événements redoutés, évalue les conséquences de leur survenue et leur probabilité d'occurrence.

Il s'agit aussi de caractériser les barrières mises en place pour réduire ces occurrence et/ou ces conséquences, obtenir leur état et tracer dans le système les justifications de ces barrières et les éléments de sécurité qu'elles préservent. Il est nécessaire de déterminer les empans de recueil de ces mesures, les moyens de stockage et les traitements permettant de mettre en évidence les tendances.

Connaissant ces mesures, il faut ensuite déterminer les capteurs qui peuvent fournir ces mesures. Il s'agit aussi de stocker dans le système les données de référence de sa définition à partir desquelles seront effectuées les comparaisons pour évaluer l'écart entre un état courant et un état de référence. Ces données doivent êtres mises à jour lorsque la définition du système change.

Il s'agit de déterminer les seuils d'alerte, tant à partir d'un changement d'état d'un capteur que des données calculées.

L'ensemble de ces mesures, de ces données et des traitements associés doit être fiabilisé. En effet, des informations qui ne seraient pas fiables entraîneront des présentations non fidèles au niveau des IHM et en cascade des erreurs de jugement de la part des opérateurs. En outre, des informations qui ne seraient pas fiables jetteraient un important discrédit sur le système, une perte de confiance de la part des opérateurs et au-delà de la méfiance, de la défiance par rapport au système. Pour autant, il paraît nécessaire d'affecter un niveau de confiance aux informations, à l'instar du niveau de confiance attribué aux prévisions météorologiques. Enfin, il faut élaborer l'adaptation des alertes aux différents dispositifs des systèmes interactifs qui seront utilisés par les opérateurs.

[26] Architecture au sens de l'activité, de la pratique, le terme *architecting* est souvent utilisé pour marquer la différence par rapport à l'architecture en tant qu'organisation du système traitée dans le Chapitre 5, « Proposition d'un patron de conception pour l'architecture d'un système résilient ».

Le processus visant à déterminer les mesures, les capteurs, les données et les traitements peut être l'objet d'un document de bonnes pratiques, par exemple une norme, pour aider les concepteurs dans leur activité. De plus, ce processus doit être intégré dans les documents majeurs de l'ingénierie système (ISO, 2014). C'est une action à mener (cf. Conclusion générale, section « Actions à mener dans le domaine de la normalisation »).

Cela se aussi traduit par une plus grande prise en compte des processus de conception centrée utilisateur dans des processus d'ingénierie système. Au-delà des propositions qui ont déjà été faites à ce sujet (cf. section 3.3, « Processus de conception centrée utilisateur »), il s'agit d'articuler la conception pour l'appropriation (cf. section 6.3.1 « Concevoir pour l'appropriation » de ce chapitre) avec les processus et activités d'ingénierie système. Tant la conception pour l'appropriation que l'intégration du système de surveillance de l'usage et de l'état du système principal affectent les processus d'analyse métier ou de la mission, de définition des besoins et exigences des parties prenantes, de définition des exigences système, de définition de l'architecture, de définition de la définition du système (ISO, 2014).

Dans la même perspective, les documents majeurs (ISO, 2010b ; ISO, 2014) doivent prendre en compte le processus d'appropriation dans une future mise à jour (cf. Conclusion générale, section « Actions à mener dans le domaine de la normalisation »).

L'anticipation en amont de l'usage qui pourra être fait du futur système peut s'appuyer sur la modélisation de scénarios. Dans le cadre des travaux consacrés au Grand Paris (Chérel, 2012), des scénarios d'usage sont élaborés. Les usagers des transports, exploitant les ressources des technologies de l'information et des communications, recalculent leur itinéraire en fonction des perturbations de trafic. Cette situation, au niveau individuel, doit être analysée globalement pour envisager dynamiquement les impacts sur la charge des itinéraires alternatifs et gérer cette surcharge pour maintenir un trafic régulier, malgré les perturbations locales.

De plus, cela se traduit aussi par la capacité d'effectuer un retour d'expérience des situations opérationnelles pour prendre en compte les adaptations que mettent en œuvre les opérateurs et les nécessaires évolutions du système technique. Cela concerne en priorité le processus de définition des exigences des parties prenantes, le processus d'analyse des exigences, le processus de définition de l'architecture (ISO, 2014), ainsi que le processus de gestion des exigences (ISO, 2009). Le retour d'expérience nourrit aussi le processus de maintenance du système à élaborer. Ce retour d'expérience doit être clairement identifié comme le processus d'ingénierie système clef de voûte pour apporter une capacité de résilience du système technique dans la mesure où il contribue à améliorer la compréhension, par les ingénieurs, de la manière dont le système s'adapte et à quelles gammes ou sources de variation. Ce retour d'expérience doit rendre compte des migrations et des mécanismes de compensation, ainsi que des variations et des évolutions du contexte opérationnel.

Ce processus de retour d'expérience se nourrit des données produites et stockées par le système de surveillance de l'état et de l'usage du système principal. En effet, si la première vocation de ce système de surveillance est d'alerter les opérateurs et leur permettre de naviguer à vue, les informations recueillies par le système de surveillance entrent dans le processus de retour d'expérience pour faire évoluer le système (cf. section 6.3.3 « Activité de veille et retour d'expérience »).

Par ailleurs, le retour d'expérience doit tracer les dérives, tant celles qui fonctionnent bien que celles qui génèrent des incidents. Pour les premières, le retour d'expérience doit aider à différencier, d'une part les compensations qui cachent potentiellement un grave accident lorsqu'il y a décompensation, et d'autre part les ajustements adaptés aux évolutions de

l'environnement et qui ne bouleversent pas l'équilibre du système, en particulier des ajustements qui ne génèrent pas des compensations sources de risque (cf. Tableau 4.2).

Les documents normatifs (ISO, 2010c ; ISO, 2014) sont muets sur le retour d'expérience et sur les activités de rénovation à mi-vie qui peuvent profiter du retour d'expérience. Dans ce contexte, une action doit être envisagée afin que soient formalisées et décrites ces activités dans une prochaine édition des documents normatifs (ISO, 2014). Ces activités doivent être anticipées et prises en compte le plus tôt possible puisqu'elles affectent l'ensemble des processus, et en particulier celui de définition de l'architecture.

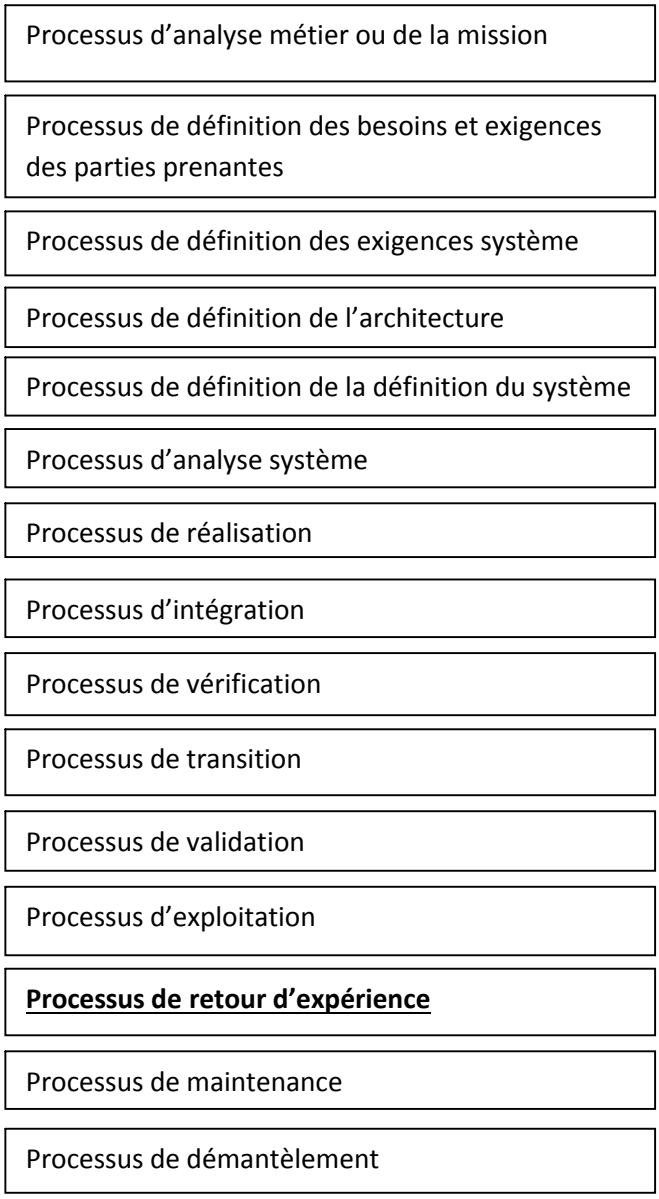

Figure 6.1. Insertion du processus de retour d'expérience dans les processus techniques de la norme ISO 15288 (adapté de ISO, 2014).

La Figure 6.1 illustre notre proposition d'intégration du processus de retour d'expérience au sein des processus techniques décrits dans la norme (ISO, 2014). Ce processus de retour d'expérience s'appuie sur les informations issues du processus d'exploitation pour enrichir le

processus de maintenance. Une action est à mener afin de mener à bien cette intégration (cf. Conclusion générale, section « Actions à mener dans le domaine de la normalisation »).

6.3. Contribution du processus d'appropriation à l'ergonomie prospective

La durée de vie opérationnelle des systèmes critiques peut être très longue, de l'ordre d'une cinquantaine d'années. Au moment où ces systèmes sont conçus, les utilisateurs auxquels les ergonomes peuvent faire appel ne sont pas représentatifs de l'ensemble des utilisateurs aux différents horizons temporels qui jalonnent la durée de vie de ces systèmes. Effectuer une approximation à partir des utilisateurs représentatifs lors de la conception est source d'erreur. Les travaux d'ergonomie en amont des projets ne peuvent pas rendre compte de la façon dont les utilisateurs vont s'approprier ces systèmes au fur et à mesure, feront l'usage de nouvelles technologies dans le futur.

La Figure 6.2 illustre la proposition d'articulation et d'évolution des processus d'appropriation et processus de conception, en s'appuyant sur l'ergonomie prospective.

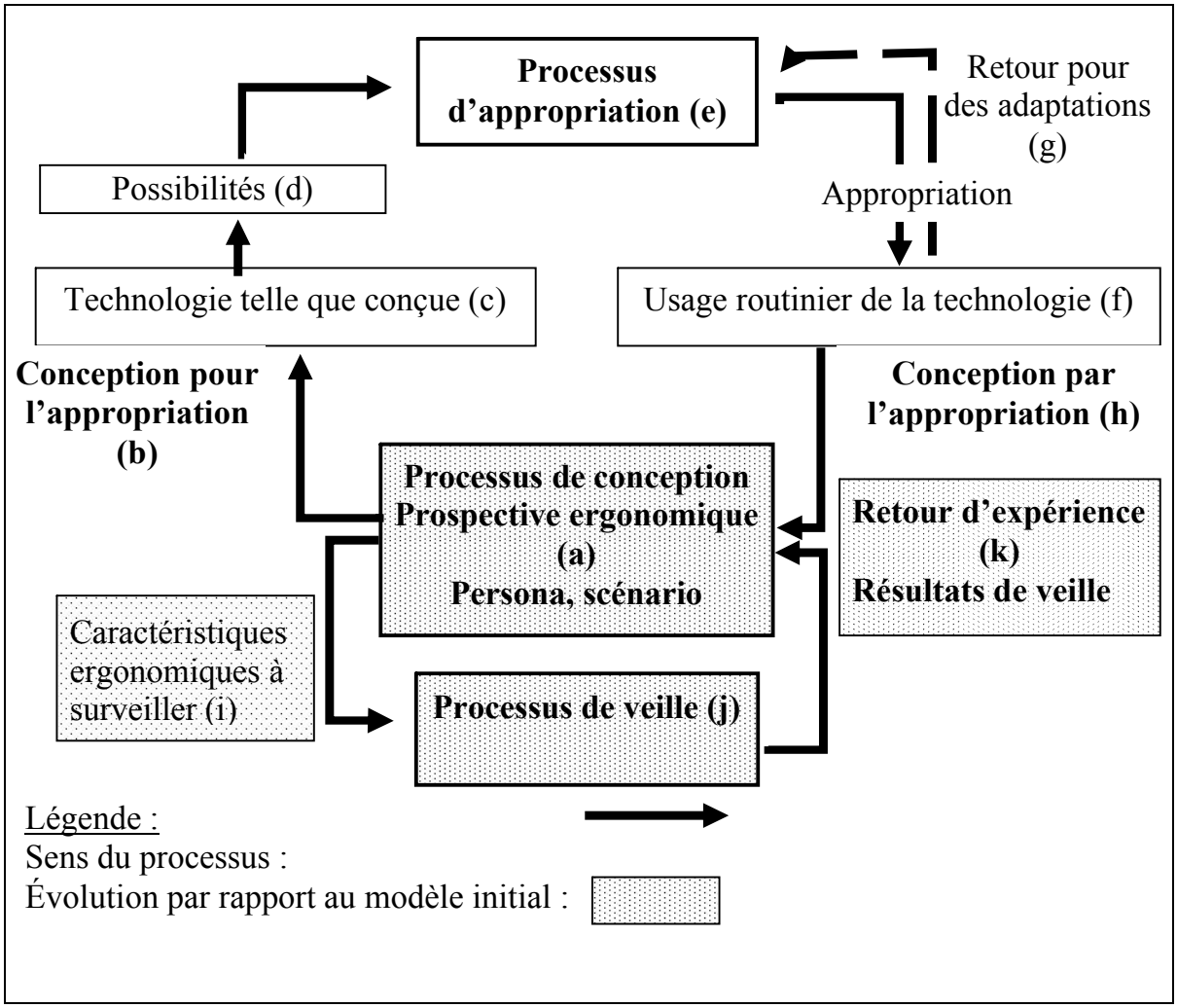

Figure 6.2. Proposition d'évolution des processus d'appropriation et processus de conception (Ruault *et al.*, 2014b).

Dans ce contexte, nous proposons de faire appel à l'ergonomie prospective ainsi qu'aux travaux consacrés au processus d'appropriation. Nous les articulons pour prendre en compte les évolutions de l'usage des systèmes.

Le processus de conception (a) évolue pour intégrer l'ergonomie prospective (cf. section 6.3 « Contribution du processus d'appropriation à l'ergonomie prospective »). Ce processus de conception (a) s'appuie sur les scénarios et les personas (cf. section 6.4 «

Contribution aux adaptations du persona individuel / collectif »). Le processus de conception (a) devient itératif afin d'être mis en œuvre à rythme régulier tout au long du cycle de vie des systèmes dans une logique de conception pour l'appropriation (b). La technologie ainsi conçue (c) offre un ensemble de possibilités (d) afin que les opérateurs puissent l'évaluer et l'adapter dans le processus d'appropriation (e), en fonction des environnements et situations opérationnels qu'ils rencontrent dans leurs missions, et en faire un usage routinier (f). Les évolutions de l'environnement au fil du temps obligent à retourner vers le processus d'appropriation pour ajuster, adapter, les artefacts technologiques et les pratiques (g). Ces retours pour des adaptations doivent être tracés dans le cadre du retour d'expérience (k).

La conception par l'appropriation (h) recueille les informations de retour d'expérience de l'activité routinière et des adaptations réalisées ainsi que les résultats de la veille. Le processus de veille (j), en parallèle au processus d'appropriation (e), surveille comment les caractéristiques ergonomiques (i) évoluent au cours du temps. Ces caractéristiques ergonomiques à surveiller sont celles dont les évolutions ont des impacts pour les systèmes à longue durée de vie, à l'instar de la féminisation des armées présentée au Chapitre 1. Elles sont ajoutées au persona (cf. section 6.4 « Contribution aux adaptations du persona individuel / collectif aux systèmes critiques à longue durée de vie») et sont l'objet d'une attention particulière de la part de l'ergonomie prospective (cf. section 6.3.4 « Proposition de compléments à l'ergonomie prospective»).

Nous poursuivons en détaillant les deux points de vue, concevoir pour l'appropriation et concevoir par l'appropriation, ainsi que l'activité de veille et de retour d'expérience.

6.3.1. Concevoir pour l'appropriation

Dans la Figure 6.2, la conception pour l'appropriation (b) offre aux opérateurs un ensemble de possibilités (d) pour ajuster, adapter les artefacts technologiques à leur besoin, au fil de l'eau, dans une navigation à vue. Elle se décline, d'une part, dans une architecture modulaire, ouverte, ajustable, malléable et évolutive, d'autre part, dans l'insertion, au sein du système, de capteurs pour recueillir les informations sur les environnements et situations opérationnels rencontrés.

Cette architecture permet aux opérateurs d'ajouter de nouveaux artefacts, de nouveaux services, de les organiser entre eux, en termes logiques et temporels, pour réaliser les missions qui leur sont confiées. Une telle architecture s'appuie sur une composition des services et une structure des préoccupations (architecture orientée *aspect*) permettant cette composition. Dans une démarche de conception itérative, l'architecture initiale doit être ouverte et propre à évoluer par ajout et par retrait de fonctions et de composants. Cette architecture permet une adaptation *hic et nunc* au contexte rencontré. L'insertion de capteurs permet de recueillir l'usage du système, dans les conditions réelles des environnements et situations opérationnels rencontrés, ainsi que de la variabilité des performances réalisées.

L'évaluation des impacts de la conception pour l'appropriation sur l'architecture du système est une de nos perspectives de recherche (cf. Conclusion générale, section « Perspectives de recherche dans le domaine de l'ingénierie et l'architecture système »).

Le système de surveillance de l'usage et de l'état peut mesurer des informations relatives à l'appropriation et à l'usage, telles que les services ajoutés, les fonctions utilisées et leur durée d'utilisation, les performances réalisées, leur variabilité, les défaillances et les pannes rencontrées. Il peut aussi recueillir les informations sur l'organisation des artefacts technologiques employés, lesquels, dans quel ordre, selon quel mode opératoire. En complément des méthodes de recueil de données des sciences humaines, ces informations sont une des sources du retour d'expérience sur l'appropriation et l'usage routinier.

6.3.2. Concevoir par l'appropriation

En vis-à-vis de la conception pour l'appropriation, dans laquelle le système est architecturé et instrumenté pour favoriser l'appropriation et le recueil d'informations sur cette appropriation, la conception par l'appropriation consiste à s'appuyer sur ces informations pour que la conception prenne en compte l'usage réel. Il s'agit là des grandes révisions et des programmes de rénovation à mi-vie. Nous sommes dans une démarche itérative se poursuivant tout au long du cycle de vie du système. Dans ce contexte, il faut tracer la façon dont les opérateurs adaptent les artefacts technologiques, les agencent entre eux pour réaliser leurs activités. Les détournements fonctionnels qu'ils font de tel ou tel artefact, sont autant d'éléments qui orientent les nouvelles itérations de conception. L'usage routinier d'une technologie se caractérise par une forte intégration entre pratique et artefact qu'il faut prendre en compte dans les évolutions d'architecture lors d'itérations successives pour ne pas rompre des routines, sources de performance. Ce retour d'expérience permet de généraliser les adaptations au sein de l'organisation, et d'inscrire ces adaptations au sein même de la structure de l'organisation et du système technologique.

6.3.3. Activité de veille et retour d'expérience

L'analyse des risques, la simulation de scénarios tendanciels et de rupture et les valeurs seuil générant telle ou telle trajectoire, permettent d'identifier les caractéristiques ergonomiques les plus susceptibles d'évoluer et dont l'évolution présente d'importantes conséquences. Ces caractéristiques ergonomiques doivent faire l'objet du retour d'expérience ainsi que d'une veille afin d'évaluer régulièrement leur évolution.

Le retour d'expérience consiste à capitaliser les différents environnements et situations opérationnels, le contexte d'usage réel, le déroulement du processus d'appropriation, les usages routiniers et les adaptations effectuées tant sur dans les activités que sur l'artefact technologique.

On recueille les performances réalisées, leur variabilité, et les écarts par rapport au tolérancement envisagé. Ces informations sont fournies, d'une part, par les méthodes de recueil d'information de l'ergonomie, que sont l'analyse de l'activité, d'enquête, l'analyse des traces, etc., et, d'autre part, par les données recueillies *via* les capteurs insérés dans le système, décrits dans la section 6.3.1 « Concevoir pour l'appropriation ».

La Figure 6.3 illustre l'adaptation du modèle des stades du cycle de vie d'un système (ISO, 2010c) en intégrant le retour d'expérience durant le stade d'utilisation. Le modèle initial ne

prend pas en compte ce qui se passe durant le stade d'utilisation (en grisé dans la figure). En effet, le modèle de définition issu de C est directement repris par E, court-circuitant D.

L'évolution du modèle des stades du cycle de vie intègre le retour d'expérience, représenté par des flèches verticales, durant le stade d'utilisation. Ce retour d'expérience permet d'enrichir le modèle de définition, issu de C, du modèle d'usage routinier issu du processus d'appropriation mis en œuvre durant le stade d'utilisation (D). Ainsi, le modèle de définition de E prend en compte le modèle de définition de C et le modèle d'usage routinier de D.

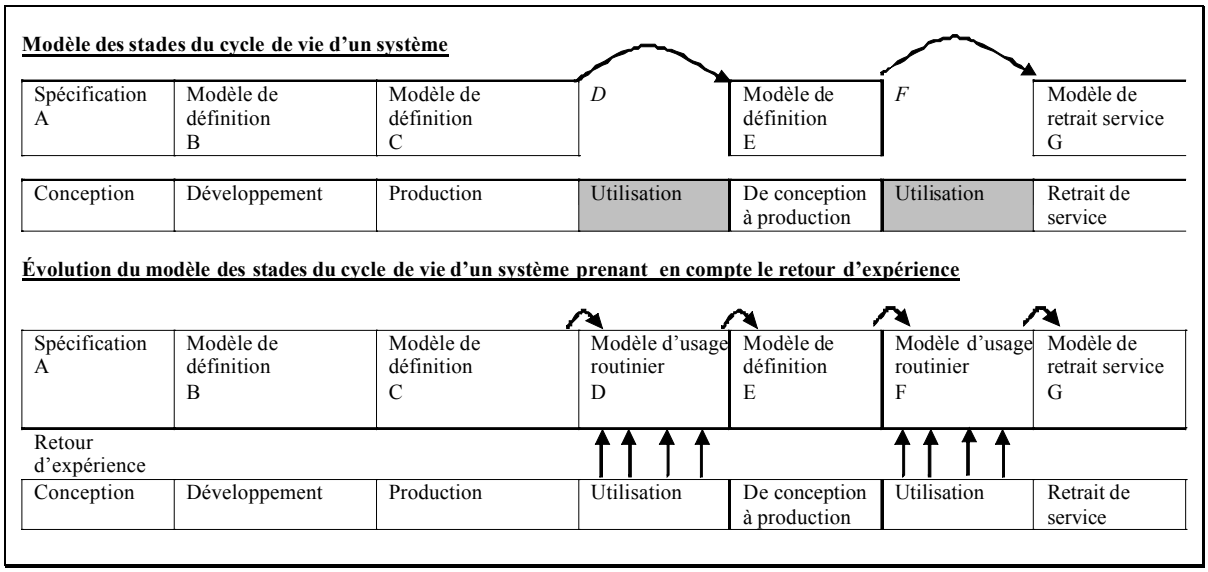

Figure 6.3. Retour d'expérience et prise en compte du modèle d'usage routinier dans le modèle de définition du système (adapté de Bachatène *et al.*, 2008).

Lorsque des valeurs seuil sont détectées par le retour d'expérience (par exemple, nouveaux environnements opérationnels détectés) ou par l'activité de veille (par exemple, évolution des caractéristiques de la population), les scénarios sont rejoués en prenant en compte des valeurs réelles mesurées par le retour d'expérience pour évaluer les conséquences immédiates et moyen terme des évolutions. Les résultats de ces scénarios sont utilisés pour envisager les impacts sur les hypothèses et la conception et orienter les évolutions des procédures ou du système. La difficulté réside dans la détermination des valeurs seuil. En effet, il est nécessaire de différencier *a priori*, d'une part, les écarts minimes entre l'hypothèse et la situation réelle, écarts liés à des ajustements conjoncturels, normaux, d'autre part, les écarts significatifs montrant un changement structurel, radical, une tendance longue. La veille consiste à obtenir des informations sur les évolutions que connaissent les opérateurs ou qui affecteront les opérateurs à terme. Ces évolutions procèdent tant des aspects réglementaires et juridiques (âge du départ à la retraite), que des modes de vie (utilisation des technologies de l'information et des communications), et des évolutions sociétales.

6.3.4. Proposition de compléments à l'ergonomie prospective

La première étape de la démarche consiste à compléter le modèle de l'ergonomie prospective présenté par Robert et Brangier (2009), en l'adaptant aux systèmes à longue durée de vie. Comme précisé ci-dessus, la temporalité propre de ces systèmes s'inscrit dans le futur lointain, avec plusieurs horizons temporels intermédiaires, par exemple, 10 ans, 20 ans et 30 ans. Les systèmes auxquels nous nous intéressons ne sont pas des produits de grande consommation,

mais des systèmes complexes, tels que des réseaux de transport ferroviaires, comprenant les infrastructures, le matériel roulant, les procédures d'exploitation, etc.

Les organismes en charge d'exploiter ces systèmes sont les clients qui expriment leur besoin auprès de fournisseurs, des bureaux d'ingénierie et des cabinets d'ergonomie. Le point de départ est alors une demande du client (cf. Tableau 6.1). Une caractéristique majeure de ces systèmes réside dans l'absence d'utilisateurs représentatifs aux différents horizons temporels envisagés. En effet, pour les horizons temporels les plus éloignés de la conception, les utilisateurs ne sont pas encore nés. Il est donc matériellement impossible d'effectuer des études d'ergonomie avec eux.

Ainsi que l'illustre la Figure 6.2 (Ruault *et al.*, 2014b), la nature de l'activité de l'ergonomie relève, d'une part, de la veille (j), de la prospective (a), et, d'autre part, de la mise en place des dispositions permettant le processus d'appropriation par les futurs utilisateurs (e) pendant toute la durée du stade d'exploitation opérationnelle desdits systèmes.

Le premier point focal de l'activité de l'équipe de projet (cf. Tableau 6.1) relève de l'activité de prospective (a). Elle identifie les variables significatives, du point de vue de l'ergonomie (activités, compétences, attitudes …), mesure les évolutions récentes de ces variables et réalise des simulations pour évaluer comment ces variables vont évoluer dans le futur.

Dans la mesure où il n'est pas possible de faire appel à des utilisateurs représentatifs aux horizons temporels de la prospective (cf. Tableau 6.1), nous proposons de faire appel aux personas (la contribution relative aux personas est détaillée dans la section 6.4 « Contribution aux adaptations du persona individuel / collectif aux systèmes critiques à longue durée de vie »). Les résultats de ces simulations sont injectés dans les personas, lesquels servent à élaborer les scénarios tendanciels et les scénarios de rupture et, in fine, spécifier le futur système ou une future version d'un système existant. Le second point focal relève de l'activité de veille (j).

L'équipe de projet met en place les moyens et dispositifs de veille sur ces variables significatives. Les résultats de cette veille, les tendances qui s'en dégagent, les ruptures qui ont eu lieu sont comparés aux hypothèses de prospectives initiales et aux simulations. Les tendances constatées alimentent la mise à jour des modèles, des personas et des simulations, bases de l'étape suivante de prospective pour faire évoluer les scénarios tendanciels et de rupture. Les nouvelles versions de ces scénarios sont les données d'entrée des activités de mise à niveau et de rénovation à mi-vie des systèmes.

L'autre point focal de l'activité concerne l'élaboration des moyens permettant le processus d'appropriation, décrits cf. (c) dans le Tableau 6.1. Aux disciplines identifiées par Robert et Brangier (2009), nous ajoutons la démographie (cf. Tableau 6.1), la veille pour prendre en compte les évolutions du marché du travail et des opérateurs (pyramide des âges, évolution de l'âge moyen des opérateurs), les évolutions réglementaires, ainsi que l'ingénierie système pour articuler les activités de l'ergonomie et celles de l'ingénierie système (Robert, 2003 ; Ruault, 2004 ; Pew & Mavor, 2007 ; ASD-STAN, 2013).

Les sources des données (cf. Tableau 6.1) sont, d'une part, le retour d'expérience des situations opérationnelles et des usages, et d'autre part, les résultats de la veille sur les dimensions à prendre en compte, sociétale, démographique, anthropométrique, entre autres. Au sein des équipes de projet, le statut des facteurs humains (cf. Tableau 6.1) contribue à une démarche interdisciplinaire sur l'ensemble du cycle de vie des systèmes.

L'intervention de l'équipe de projet (cf. Tableau 6.1) s'inscrit donc sur cette durée afin de prendre en compte la dynamique des opérateurs dans les évolutions, les mises à niveau et rénovations à mi-vie des systèmes.

La production de cette intervention (cf. Tableau 6.1) comprend :

- la définition des variables significatives et des caractéristiques ergonomiques (i) qui sont les objets de l'activité de veille (j), par exemple l'épidémie d'obésité, la féminisation des postes de travail ;
- les simulations à partir de ces variables significatives permettent d'évaluer les impacts des évolutions de ces variables sur le système, sur plusieurs horizons temporels ;
- la définition des informations que les dispositifs du retour d'expérience (h) doivent recueillir afin d'organiser l'activité de retour d'expérience, tracer les données recuillies et déterminer les seuils d'alerte à appliquer sur ces données pour mesurer leurs évolutions ;
- la définition des moyens d'adaptation et d'appropriation ;
- la définition des personas qui regroupent les caractéristiquer ergonomiques majeures à surveiller ;
- un socle d'artefacts modulaire, ajustable et malléable permettant la mise en œuvre de la conception pour l'appropriation (b).

Dans une logique de conception par l'appropriation (h), le recueil de l'usage routinier des technologies (f) s'appuie sur des dispositifs de capitalisation, de retour d'expérience des situations opérationnelles et des usages, qui sont introduits dans le système.

Caractétistiques	**Ergonomie prospective**
Temporalité	Futur lointain, avec plusieurs horizons temporels
Nature de l'activité de l'ergonome	Prospective, veille et mise en place des dispositions permettant le processus d'appropriation par les futurs utilisateurs
Point de départ	Demande du client
Point focal	Démarche prospective et de veille sur les variables significatives Élaboration des personas à partir des résultats de simulations Élaboration des moyens permettant le processus d'appropriation
Échantillon des utilisateurs	Absence d'utilisateurs représentatifs à l'horizon temporel de la prospective
Disciplines associées	Les mêmes que Robert & Brangier (2009), plus : démographie, prospective, veille, ingénierie système
Sources des données	Retour d'expérience des situations opérationnelles et des usages Veille (sociétale, anthropométrique, démographique …)
Statut des facteurs humains	Contribution à une démarche interdisciplinaire
Nature de l'intervention	Prise en compte de la dynamique des opérateurs dans les évolutions, mises à niveau et rénovations à mi-vie des systèmes
Production	Définition des variables significatives et les caractéristiques ergonomiques objets de l'activité de veille Simulations à partir de ces variables significatives Définition des informations que les dispositifs du retour d'expérience doivent recueillir Définition des moyens d'adaptation et d'appropriation Définition des personas Création d'un socle d'artefacts permettant la mise en œuvre de la conception pour l'appropriation.

Tableau 6.1. Complément au modèle de l'ergonomie prospective de Robert et Brangier (2009) adapté aux systèmes à longue durée de vie.

La proposition a mis en évidence les articulations et les compléments de l'ergonomie prospective adaptés aux systèmes à longue durée de vie. À l'issue de cette proposition, les recommandations pour la conception des systèmes à longue durée de vie se déclinent sur l'ensemble des disciplines de l'équipe de projet (ergonomie, IHM, ingénierie système, architecture système…).

Les recommandations concernant l'ergonomie prospective sont les suivantes :

- l'équipe de projet contribue aux activités de prospective en :
  - identifiant les variables ergonomiques significatives ;
  - élaborant les personas adaptés :
  - intégrant les personas aux scénarios ;
  - évaluant les évolutions de ces variables dans les simulations et
  - spécifiant le système ;
- l'équipe de projet contribue aux activités de retour d'expérience opérationnel, en particulier pour prendre en compte les évolutions de l'activité des opérateurs, les adaptations qu'ils font des artefacts technologiques, les routines mises en œuvre ;
- l'équipe de projet mène des activités de veille dans plusieurs domaines (démographie, épidémiologie …) dont les résultats sont exploités pour faire évoluer le système en fonction des évolutions économiques, sociétales, des comportements, des attitudes, sans ignorer les ruptures qui peuvent émerger.

6.4. Contribution aux adaptations du persona individuel / collectif aux systèmes critiques à longue durée de vie

Après avoir présenté la méthode de persona dans la section 3.3.2 intitulée « Persona individuel / collectif », nous appliquons cette notion dans une démarche d'élaboration de profils de comportements humains adaptés aux systèmes critiques résilients. Cela implique d'adapter cette notion aux enjeux de cette démarche. En effet, ainsi que nous l'avons vu, le persona a été principalement utilisé dans une logique de production de biens de masse pour exprimer le besoin des consommateurs (Brangier *et al.*, 2011). Des caractéristiques de la notion de persona, pertinentes dans le contexte du marketing et de la production de masse, le sont moins dans le domaine des systèmes critiques. En contrepartie, des caractéristiques pertinentes dans le domaine des systèmes critiques sont de peu d'intérêt dans le domaine du marketing. Nous chercherons donc à identifier ces caractéristiques, nécessaires et suffisantes en priorité, dans le contexte des systèmes critiques, que nous compléterons avec des caractéristiques moins prioritaires. Après les avoir identifiées nous compléterons le persona.

6.4.1. Évolution du persona individuel

Dans un premier temps, nous identifions les caractéristiques pertinentes du persona à prendre en compte pour la conception de systèmes critiques, étape préalable à l'extension de la notion de persona.

Pour identifier ces caractéristiques, nous développons quatre thématiques, détaillées ci-dessous, qui se révèlent être des sources majeures d'écart entre la situation de référence et les situations réelles que rencontre le système tout au long de sa vie opérationnelle. Pour autant,

de nombreuses autres sources interviennent dont nous ne pourrions faire une analyse exhaustive dans le cadre de cette thèse (Hardy, 2010).

Quel que soit leur rôle vis-à-vis du système, opérateurs, agent de maintenance, ou tout autre rôle, les acteurs humains évoluent. Ils s'approprient le système (Ruault *et al.*, 2014b), apprennent de nouvelles pratiques. Sur des périodes longues, ils gagnent du poids et/ou perdent de l'acuité visuelle. En outre, les évolutions du droit du travail amènent des évolutions des opérateurs générant des situations qui n'avaient pas été envisagées initialement. C'est par exemple le cas de la féminisation de l'armée (Kirke, 2004 ; Kirke, 2005).

Les opérateurs élaborent des routines correspondant aux situations qu'ils rencontrent régulièrement. Les routines décrites de différentes manières (Rasmussen, 1983 ; Soulier *et al.*, 2008) et les biais cognitifs (Tversky & Kahneman, 1974) ont pour objectif de réduire la charge de travail. Lorsque apparaissent des situations exceptionnelles relatives à la sécurité, hors du cadre de ces routines et ces biais, la prégnance de ces routines et de ces biais réduit la perception et la compréhension de ces situations exceptionnelles (Carrol, 1976 ; Morel, 2002).

Ces biais génèrent des accidents, tel que celui du DC8 d'United Airlines en 1978 à Portland (Morel, 2002). L'équipage détecta un problème avec les indicateurs de sortie du train d'atterrissage, se focalisa toute son attention sur ce point au détriment des autres paramètres, en particulier les limites des réserves en carburant. Il s'avéra que le train fonctionnait correctement. L'équipage s'éloigna excessivement de l'aéroport et se crasha à cause d'une panne sèche.

L'accident d'Aldershot (BST, 2013) montre une autre situation dans laquelle un biais cognitif a perturbé la conscience de la situation des conducteurs. Le changement de voie, ce jour-là, de la voie 2 à la voie 3, était exceptionnel. Ainsi que le mentionne le rapport, dans 99% des cas, le type de train concerné par cet accident circulait sur la voie 2. Les seuls signaux sur les voies n'ont pas permis de rompre ce biais cognitif. De plus, les conducteurs n'avaient pas été informés, que des travaux sur la voie 1 empiétaient sur la voie 2 et nécessitaient que le train circule sur la voie 3 à hauteur de ces travaux, lorsqu'ils préparaient ce voyage, ou durant ce voyage.

Des événements peuvent affecter la vie des parties prenantes (opérateur, agent de maintenance …), les amenant à avoir des pensées errantes (Lemercier *et al.*, 2014). Ces pensées errantes apparaissent lorsque les acteurs réalisent des tâches monotones. Elles peuvent être conscientes ou inconscientes, parfois avec une charge émotionnelle importante, voire relever de la rumination. Elles fonctionnent comme des secondes tâches, réduisant l'attention des personnes qui en sont affectées. Les auteurs montrent que ces pensées, qui distraient l'attention, sont à l'origine du quart des accidents de la route et que les épisodes de pensée errante représentent plus d'un tiers de la vie quotidienne.

Au regard de l'analyse à laquelle nous venons de procéder, nous proposons de sélectionner et d'adapter les caractéristiques du persona appropriées aux systèmes critiques résilients en intégrant les caractéristiques liées aux acteurs ou au contexte de l'activité que nous venons d'identifier. Nous proposons d'élargir le domaine de définition du persona en l'appliquant à d'autres acteurs qui ont un rôle vis-à-vis du système, outre les opérateurs, il y a aussi les agents de maintenance, les ingénieurs de conception, ainsi que les responsables des services dans lesquels travaillent les opérateurs (Ruault *et al.*, 2014).

Nous reprenons la notion d'acteur du diagramme des cas d'utilisation de SysML que nous enrichissons des caractéristiques du persona. Dans la Figure 6.4, à chacune de ces caractéristiques est attachée une clef utilisée pour la description d'un persona. Ces caractéristiques, avec les clefs entre crochets, sont les suivantes :

- [Informations_Personnelles] données personnelles : nom, prénom, date de naissance et photographie ;
- [Données_Physio] données physiologiques : sexe, âge, poids, handicap ;
- [Personnalité] personnalité : objectifs personnels ;
- [Socialité] socialité : besoin de leadership, influence sociale, confiance, partage, don ;
- [Formation] formation, entraînement : formation initiale et continue, entraînement, certification ;
- [Expérience] compétences, habiletés : durée de l'expérience professionnelle dans le domaine, niveau de maîtrise des modes opératoires, des règles établies, de la langue dans laquelle sont écrits ces modes opératoires et ces règles ;
- [Activité] contexte de l'activité : propriétés de l'activité en termes logique et temporels ;
- [Routines] charge de travail, vigilance : durée du poste, durée quotidienne de travail, caractère routinier de l'activité ;
- [Contournement] contournement des barrières : contournement des barrières, migrations silencieuses, normalisation de la déviance ;
- [Événement] événement personnel affectant la vie des parties prenantes : séparation, deuil ;
- [XXXX_t0+YY] évolution de ces caractéristiques au fil du temps : évolution de ces caractéristiques sur plusieurs horizons temporels, par exemple, la série [Formation_t0], [Formation_t0+5ans], [Formation_t0+10ans], [Formation_t0+15ans].

Ces caractéristiques ne sont pas exhaustives. Elles doivent être identifiées et adaptées aux spécificités et contraintes des systèmes concernés et de leur durée de vie. Les aspects liés à la personnalité peuvent avoir des conséquences critiques dans le domaine aéronautique, tel que le démontre l'accident du vol 4U9525 de la compagnie Germanwings, le 24 mars 2015, avec le suicide du pilote affecté de troubles psychiatriques.

La réalisation de scénarios prospectifs, en faisant appel à ces personas dans des simulations et des expérimentations, doit permettre d'évaluer les conséquences des évolutions des caractéristiques des opérateurs, par exemple la surcharge pondérale, ainsi que les évolutions de l'environnement technologique, économique et social sur plusieurs horizons temporels. Ces dernières peuvent avoir des impacts sur la formation (réduction de budget, du temps de formation), sur le recrutement (marché du travail, orientations sociétales) sur les compétences générales (compétences de lecture et d'écriture, nouveaux médias et nouvelles façons de s'exprimer …) ou bien encore la légalisation du mariage pour les personnes de même sexe avec les impacts sur les systèmes d'information RH des entreprises, de la CAF, etc.

La Figure 6.4 illustre la modélisation des caractéristiques du persona avec SysML.

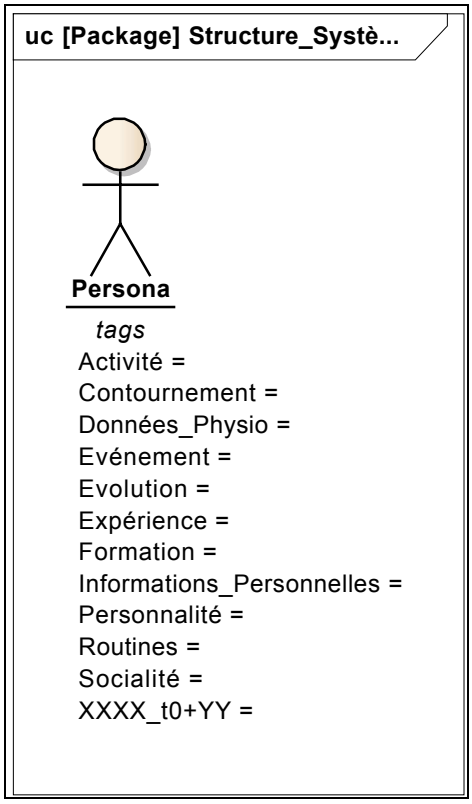

Figure 6.4. Modélisation SysML des caractéristiques du persona (Ruault *et al.*, 2014c).

Dans ce contexte, les personas peuvent être décrits dans les scénarios de façon diachronique pour montrer leur évolution entre plusieurs horizons temporels, par exemple en modélisant la prise de poids ou encore l'apparition de problèmes visuels sur le long terme, et de façon synchronique pour décrire une activité qui se déroule à un horizon temporel donné. Au fil des itérations, les personas et les scénarios sont révisés en tenant compte des résultats de la veille et du retour d'expérience. Ils sont alors rejoués dans des simulations et des expérimentations pour analyser les impacts de ces évolutions sur l'architecture du système, lequel peut être modifié pour intégrer ces évolutions. Ce sont les entrées des processus d'ingénierie menés pour les grandes visites et les programmes de rénovation à mi-vie.

6.4.2. Évolution du persona collectif

Par ailleurs, un opérateur n'est jamais complètement seul. Un conducteur de train est en lien avec le contrôleur du train, ainsi qu'avec l'opérateur qui régule le trafic ferroviaire. Dans de nombreux cas, les opérateurs forment une équipe. Depuis de nombreuses années, la formation des pilotes d'avion intègre un module consacré à la gestion des ressources de l'équipe (CRM en anglais pour *Crew Resource Management*). Ce module prend en compte de nombreuses dimensions d'un travail en équipe, tant la communication entre les membres de l'équipage que le mode de leadership et les spécificités culturelles etc.

Dans ce contexte, la notion de persona collectif adapte la notion de persona individuel à cette problématique de coordination entre opérateurs et de travail en équipe dans le domaine des systèmes critiques complexes. Nous complétons cette notion de persona individuel et identifions les caractéristiques pertinentes du persona collectif. Les membres d'équipage communiquent ensemble afin de coordonner, pour informer l'équipe de relève de la situation actuelle, pour contrôler leurs activités.

Les caractéristiques du persona collectif appropriées aux systèmes complexes résilients sont les suivantes :

- la structure du persona collectif : le nombre de personas individuels, leurs fonctions et activités respectives, les rôles et responsabilités des différents personas individuels au sein du persona collectif ; les relations hiérarchiques, l'autorité, la délégation ;
- la dynamique au sein de l'équipe : certains membres restent, tandis que d'autres membres viennent et partent, ce qui affecte les relations éloignées, plus ou moins étroites, entre les membres ;
- le type d'activité menée en commun : activité créative, activité de surveillance ;
- le type de communication : les moyens de communication mis en oeuvre, communication en coprésence, synchrone et à distance physique, liaison asynchrone, au sein d'un persona collectif et entre des personas collectifs ;
- l'intégration au sein de communautés : participation au sein d'une même communauté (communauté nationale…) ou de différentes communautés ;
- les habitudes : les attitudes courantes, les croyances et les comportements des membres ;
- le respect ou le non-respect des règles : le respect ou le non-respect des règles, des modes opératoires prescrits, les dérives et franchissement de barrières ;
- la confiance au sein du collectif : la confiance que les membres du persona collectif entretiennent entre eux.

Différents personas interagissant ensemble au sein d'un persona collectif, utilisent des moyens de communication, des artefacts techniques mettant en œuvre des systèmes interactifs. Dans ce cas, ces systèmes interactifs doivent être conçus afin d'aider les membres à communiquer et se coordonner

La Figure 6.5 illustre les communications, qu'elles soient médiatisées ou non par des systèmes interactifs, des personas individuels au sein de personas collectifs.

Les personas individuels sont représentés par des rectangles avec un fond crème. Les personas collectifs sont représentés par des ellipses de couleur mauve. Le système technique avec IHM est représenté par une ellipse de couleur brune. Les communications entre personas individuels, au sein de personas collectifs et entre personas collectifs sont représentées par des doubles flèches. Cette figure illustre que certaines communications entre les personas individuels sont médiatisées par le système technique avec IHM, tandis que d'autres, en particulier au sein des personas collectifs, ne sont pas médiatisées par le système technique avec IHM.

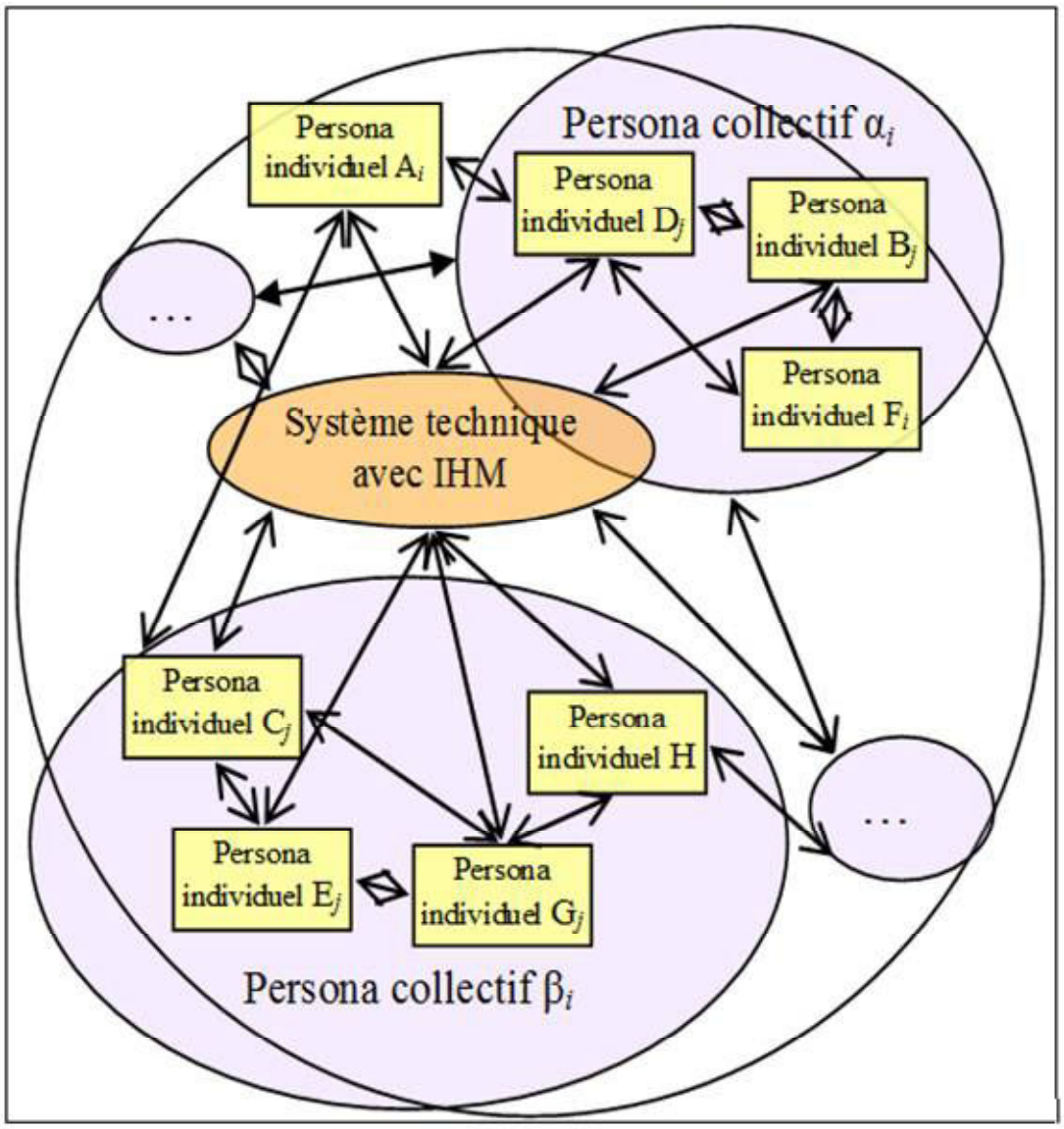

Figure 6.5. Communications, médiatisées ou non, par des systèmes techniques avec IHM, des personas individuels au sein de personas collectifs.

La façon dont les personas individuels communiquent entre eux *via* le système technique et ses IHM est la clef de voûte pour l'élaboration d'une conscience partagée de la situation.

6.4.3. Facteurs de performance et persona

La violation des règles de communication employées pour se coordonner et coopérer, les artefacts inadéquats qui ne permettent pas de rendre manifeste à autrui un ensemble d'actions, les systèmes interactifs ne restituant pas une représentation de la situation actuelle du système sur laquelle les opérateurs élaborent leur décision sont autant des facteurs de performance qui génèrent des risques de défaillance et d'accident.

En vis-à-vis, les évolutions, les améliorations de ces facteurs sont des contributeurs de la résilience. C'est à ce titre que les facteurs de performance (PSF) sont déclinés et précisés pour tracer ces contributions. Les facteurs de performance identifiés dans les personas individuels et collectifs peuvent affecter les fonctions de la résilience, en particulier la fonction « éviter ».

Pour chacun des risques identifiés, nous proposons une solution d'interface utilisateur afin d'augmenter la résilience et réduire le risque.

Dans le Tableau 6.2, nous identifions un ensemble de facteurs de performance caractéristiques des personas individuels et collectifs contribuant à la résilience du système. Ces facteurs de performance complètent la liste définie par SAIC (SAIC, 2005). Pour différencier notre proposition de cette liste, nous avons ajouté les lettres 'pc' entre l'acronyme PSF et le numéro du facteur de performance, signifiant persona collectif.

PSF	Libellé du facteur de performance adapté au persona collectif
PSFpc01	Type de communication : moyens de communication (téléphone, …), communication synchrone de proximité, avec co-présence, communication synchrone à distance, communication asynchrone, à l'intérieur d'un persona collectif et entre plusieurs personas collectifs
PSFpc02	Structure du persona collectif : nombre de personas individuels ; activités, rôles et responsabilités des personas individuels ; relations entre personas individuels, autorité, délégation
PSFpc03	Dynamique du persona collectif : pérennité ou brièveté de la présence des personas individuels au sein du persona collectif tout au long d'un projet ou d'une activité de collaboration
PSFpc04	Dynamique de groupe ; qualité de la communication au sein du persona collectif, avec des impacts tels que la confiance ou la défiance entre les personas individuels
PSFpc05	Type de management : autocontrôle, délégation, management hiérarchique et contrôle externe
PSFpc06	Habileté et management : management de situation d'urgence
PSFpc07	Culture : communauté, langage
PSFpc08	Habitudes : routines mises en œuvre par les membres, attitudes et croyances, par exemple violation des modes opératoires prescrits
PSFpc09	Type d'activité : réversibilité des actions ; contexte spécifique opposé à contexte coutumier, usuel ; activité de surveillance et de contrôle …
PSFpc10	Qualité de l'interface utilisateur : représentation claire et compréhensible de la situation dans laquelle se trouve le système
PSFpc11	Situation du système technique : fiabilité,

Tableau 6.2. Description des facteurs de performance contribuant à la fonction « éviter » de la résilience.

Ces facteurs de performance ne sont pas une liste définitive. Cette liste pourra être corrigée, amendée, complétée, à partir de futurs travaux afin de comprendre les facteurs de performance qui contribuent le plus à la résilience.

6.5. Synthèse et conclusion du chapitre

Après avoir présenté les évolutions des architectures fonctionnelle et physique que génère la résilience, dans le Chapitre 5 (Proposition d'un patron de conception pour l'architecture d'un système résilient), le présent chapitre a montré des impacts sur les processus d'ingénierie. En particulier, en s'inscrivant dans une démarche de conception itérative sur le long terme, les processus d'ingénierie système doivent évoluer pour prendre en compte la conception du système de surveillance d'usage et du système interactif dans la perspective de conception

d'un système résilient. Ils doivent aussi évoluer pour intégrer le processus de retour d'expérience.

La prise en compte de l'ergonomie prospective et du processus d'appropriation a des impacts sur la conception qui se déclinent de deux axes complémentaires. La conception pour l'appropriation vise à offrir aux opérateurs un ensemble de possibilités pour adapter et ajuster le système à leur besoin, dans le contexte des évolutions du contexte opérationnel. En vis-à-vis, la conception par l'appropriation consiste à recueillir les données issues de l'appropriation afin de les injecter dans la conception afin qu'elle prenne en compte l'usage réel lors des rénovations à mi-vie.

À ce titre, les activités de veille et de retour d'expérience jouent un rôle crucial pour recueillir ces données et pour identifier les évolutions qui affectent les opérateurs et le système.

L'ergonomie prospective, quant à elle, évolue pour prendre en compte les spécificités des systèmes à longue durée de vie. Par rapport à l'ergonomie de correction et de l'ergonomie de conception, elle évolue pour prendre en compte, entre autres, la veille, la prospective et le retour d'expérience.

Dans la mesure où il n'est pas possible de faire appel à des utilisateurs représentatifs aux différents horizons temporels d'un système à longue durée de vie, le persona, représentation fictive d'un utilisateur ou d'une classe d'utilisateurs, permet de rendre compte les futurs utilisateurs qui ne peuvent pas être sollicités en phase amont des projets, ou des évolutions des caractéristiques des utilisateurs au fil du temps. À ce titre, le persona complète le modèle utilisateur. Le persona collectif, quant à lui, permet de rendre compte de la dynamique de personas individuels au sein d'un collectif, par exemple l'intégration au sein de communautés, la confiance au sein du collectif, le respect ou le non respect des règles.

La prise en compte de ces propositions devrait se traduire par des évolutions des documents de bonnes pratiques, dont des documents normatifs (ISO, 2010b ; ISO, 2014), dans leurs futures mises à jour (cf. Conclusion générale, section « Actions à mener dans le domaine de la normalisation »).

La validation de ces propositions est une de nos perspectives de recherche pour les années à venir (cf. Conclusion générale, section « Perspectives de recherche pour la validation du patron de conception « surveiller et alerter » »). Pour aller dans ce sens, la prochaine étape du mémoire est d'appliquer ces contributions sur trois études de cas afin d'en évaluer la faisabilité et la pertinence.

Partie 3 Application au domaine ferroviaire

Table des matières de la partie 3

Chapitre 7.

Application au domaine ferroviaire du patron de conception « surveiller et alerter » et du persona

7.1. Introduction

Le patron de conception « surveiller et alerter » pour l'architecture d'un système résilient et la proposition d'évolution du persona sont appliqués à trois études de cas dans le domaine ferroviaire. Ces études de cas correspondent à trois accidents qui ont donné lieu à des rapports d'enquête technique. L'objectif de cette application est de démontrer la faisabilité de notre proposition sur des cas réels.

Dans un premier temps, nous effectuons une synthèse des rapports d'enquête technique, en mettant en évidence les phénomènes qui ont des impacts sur la sécurité (franchissement de barrières, normalisation de la déviance, absence de conscience partagée de la situation par les différents acteurs impliqués, entre autres).

Nous poursuivons en élaborant un scénario Yorktown, synthétisant les points clefs identifiés dans les accidents et en appliquant le patron de conception « surveiller et alerter » à ce scénario. La démarche basée sur le scénario et le persona (cf. section 7.3) est la première étape pour modéliser des accidents sous forme générique indépendamment de leurs singularités.

Cette modélisation du patron de conception « surveiller et alerter » pour l'architecture d'un système résilient rend compte des informations à échanger pour que les opérateurs puissent élaborer et entretenir une représentation dynamique partagée de la situation (cf. section 7.4).

Nous concluons ce chapitre en présentant des améliorations des interfaces utilisateur (cf. section 7.5) qui sont proposées pour donner aux opérateurs une représentation dynamique partagée de la situation afin d'éviter la survenue d'un accident.

7.2. Synthèse des rapports d'enquête technique d'accidents ferroviaires

Dès qu'un accident survient, une enquête technique est diligentée par un organisme indépendant. Ces organismes sont, entre autres, dans le domaine aéronautique, le Bureau d'enquêtes et d'analyses (BEA) en France, dans le domaine des transports terrestres, le Bureau d'enquêtes sur les accidents de transport terrestre (BEA-TT) en France, le *National Transportation Safety Board* (NTSB) aux USA, le Bureau de la sécurité des transports au Canada/*Canadian Transportation Accident Investigation and Safety Board* (CTAISB) au Canada.

Une telle enquête technique ne vise pas à déterminer les responsabilités pénales et civiles des protagonsistes, mais à déterminer les causes de l'accident afin d'élaborer des

recommandations d'actions correctives. Un rapport d'enquête relate les circonstances de l'accident et détermine l'arbre des causes. Les recommandations formulées par les rapports d'enquête technique peuvent donner lieu à des évolutions et mises à jour des règlements d'application obligatoire dans ces différents domaines.

Les synthèses des rapports d'enquête ne reprennent que les éléments de justification de notre proposition.

7.2.1. Analyse du point de vue de la résilience de l'accident de Chatsworth

L'accident de train de Chatsworth, en Californie, le 22 septembre 2008, entraîna la mort de 25 personnes, il y eut 102 personnes blessées (NTSB, 2010). Deux trains, l'un de fret et l'autre de voyageurs, devaient emprunter une section à voie unique. La sécurité de la circulation de ces deux trains sur cette section est assurée par le respect de la signalisation par les conducteurs. Le conducteur du train de voyageurs était seul dans sa cabine, pour un travail largement automatisé dont la durée journalière est longue et fractionnée, réduisant son niveau de vigilance. Le conducteur du train de voyageurs prit son service à 5h54, puis s'arrêtat de 9h26 à 14h00. Durant cette pause méridienne, le conducteur fit une sieste de deux heures. A la sortie de la gare de Chatsworth, le conducteur du train de voyageurs ne vit pas le feu rouge et continua sans freiner.

Durant son service, alors qu'il conduisait, cet après-midi du 22 septembre, le conducteur de train de voyageurs échangea sept SMS et a eu deux communications téléphoniques avec une personne étrangère au service. Sur la totalité de cette journée, il a reçu 21 SMS et envoya 21 SMS durant son service. La Figure 7.1 représente l'évolution du nombre de SMS envoyés et reçus le jour de l'accident et les sept jours précédent l'accident. Pour chaque jour, cette figure montre le nombre total de SMS envoyés/reçus durant la journée, le nombre de SMS envoyés/reçus durant le service en matinée et le nombre de SMS envoyés/reçus durant le service en soirée.

Lorsque le train passa alors que le feu était rouge, rien ni personne n'avertit le conducteur du train de voyageurs. Il n'y avait pas, non plus, de dispositif permettant d'arrêter le train à distance. Cette pratique d'envois de SMS et d'appels téléphoniques déroge à la procédure de sécurité. Le conducteur du train de voyageurs a échangé une quarantaine de SMS par jour, durant le mois précédent l'accident, à la fois avec des collègues, mais aussi avec des personnes étrangères au service, des adolescents passionnés par le domaine ferroviaire. L'avant-veille de l'accident, il a échangé 125 SMS.

Cette situation n'est pas spécifique à ce conducteur de train. De son côté, le conducteur de train de fret reçut et envoya aussi 41 SMS durant son service. Une enquête menée depuis 2005 a montré que sur 14 observations, 10 n'étaient pas conformes aux règles appliquées au sein de l'entreprise relatives à l'usage des téléphones portables et d'autres dispositifs de télécommunications et 3 personnes avaient leur téléphone personnel allumé (NTSB, 2010).

L'analyse, du point de vue de la résilience mentionne les facteurs de performance, les facteurs de contexte (cf. section 4.1, « La problématique de la résilience des systèmes »), les comportements tels que la normalisation de la déviance, entre crochets, et montre que :

- le système sociotechnique de référence, tel qu'il a été conçu, largement automatisé [PSF10][27], et sans dispositif de communication personnel (la motrice du train date de

[27] PSF : Facteurs de performance (*Performance Shaping Factors*)

1992) [FC03][28], [FC10] est différent du système sociotechnique réel puisqu'il y a insertion des téléphones portables, à la fois professionnels et personnels [PSF09], [FC04] ;

- le conducteur conduisait souvent des trains sur cette section. Il avait fait le même service les quatre jours précédant l'accident, générant une activité routinière, automatisée, propre à réduire l'attention [PSF10] (NTSB, 2010). En revanche, la structure du réseau ferroviaire, en grande partie à voie unique entre les stations Montalvo et Van Nuys (NTSB, 2010), génère des risques élevés d'accident [PSF05]. Le tronçon où eut lieu l'accident disposait d'une seule barrière de type feu rouge [PSF09] laquelle ne nécessite pas un acquittement ou un geste volontaire de violation. Le conducteur doit faire preuve d'une attention soutenue pour éviter les accidents [PSF05], [FC07] ;
- il y a détournement de l'interface utilisateur [PSF09], [FC04] et des procédures [PSF02] pour rompre la solitude, l'ennui et la baisse de vigilance ; ce détournement est indépendant du contexte réel de l'activité [PSF02], il n'y a pas de régulation entre la part consacrée à l'activité principale et celle consacrée à la double tâche [FC07] ; il s'agit d'une situation de déviance [PSF15].

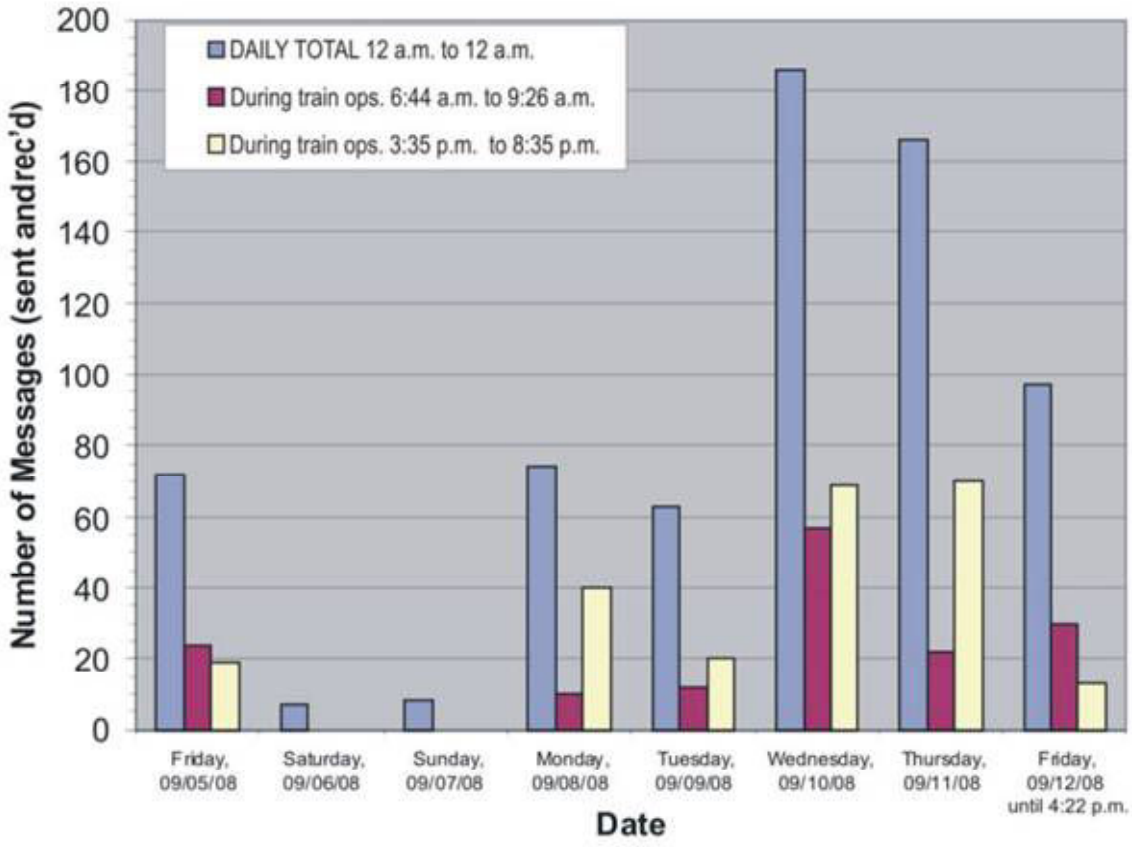

Figure 7.1. Nombre de SMS reçus et envoyés, le jour de l'accident et les 7 jours précédent l'accident (NTSB, 2010).

[28] FC : Facteurs de contexte

7.2.2. Analyse du point de vue de la résilience de l'accident de Zoufftgen

L'accident de Zoufftgen a eu lieu à la frontière entre le Luxembourg et la France, le 11 octobre 2006, et a fait six morts, deux blessés graves et quatorze blessés légers (BEA-TT, 2009). L'une des deux voies de la section de ligne internationale Thionville-Bettembourg était neutralisée pour travaux depuis trois semaines. Les trains des deux sens de circulation empruntaient la même voie. Alors que venant de Thionville, un train de fret circulait sur cette voie en direction de Bettembourg, un train de voyageurs a été engagé en sens inverse sur la même voie par la gare de Bettembourg vers 11h42. Ces deux trains sont entrés en collision frontale vers 11h44 sur le territoire français à quelques dizaines de mètres de la frontière, à Zoufftgen.

Cet accident s'est déroulé entre les gares de Bettembourg, au Luxembourg, et Thionville, en France. Dans la mesure où l'une des deux voies (voie 2) était en travaux, les trains circulaient sur l'autre voie (voie1), en sens alterné. Les équipes de Bettembourg et de Thionville se coordonnaient pour faire passer les trains à tour de rôle. Les gares de Bettembourg et de Thionville disposent d'installations de sécurité empêchant d'engager un train quand la section est déjà occupée par un autre train (BEA-TT, 2009).

La Figure 7.2 montre les voies entre les gares de Bettembourg et de Thionville. Le jour de l'accident, la voie 1 était utilisée à contresens de Thionville vers Bettembourg.

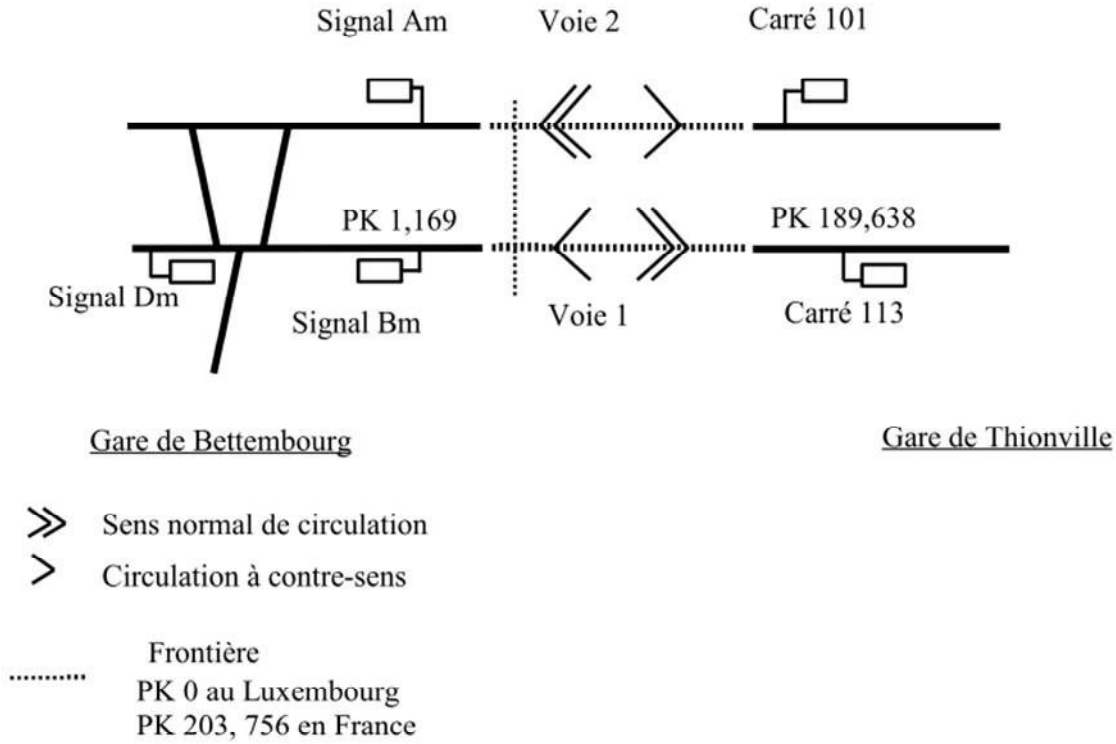

Figure 7.2. Voies et signaux entre Bettembourg et Thionville (BEA-TT, 2009).

La localisation des signaux est indiquée par le point kilométrique de leur position (PK). Le signal Dm, en sortie de gare de Bettembourg, interdit l'accès à la section entre Bettembourg et Thionville tant qu'il y a un train entre le signal Bm et le Carré 113 (intervalle BM-113).

Dans le Poste Directeur Central de Bettembourg (PDC), les dispositifs de sécurité, qui commandent les signaux sur les voies, sont respectivement le tableau de contrôle optique (TCO) et l'installation permanente de contresens (IPCS). Le TCO présente les informations

des installations de sécurité de la zone de Bettembourg, dont la partie luxembourgeoise de la section Bettembourg-Thionville. Il montre, entre autres, l'état d'occupation des sections, l'établissement des itinéraires, l'état des signaux ouverts ou fermés. Le TCO présente des contrôles à trois états, sauf pour la section Bettembourg-Thionville pour laquelle les contrôles ont deux états (BEA-TT, 2009).

À ce TCO s'ajoute l'IPCS, exclusivement entre Bettembourg et Thionville. Il s'agit d'un dispositif de sécurité installé à demeure s'opposant à l'expédition de deux trains en sens contraire en maintenant les signaux fermés. Les boutons et contrôles de l'IPCS ont été ajoutés sur le côté droit du TCO, en marge des voyants et contrôles du TCO, et sans y être complètement intégrés (cf. Figure 7.3).

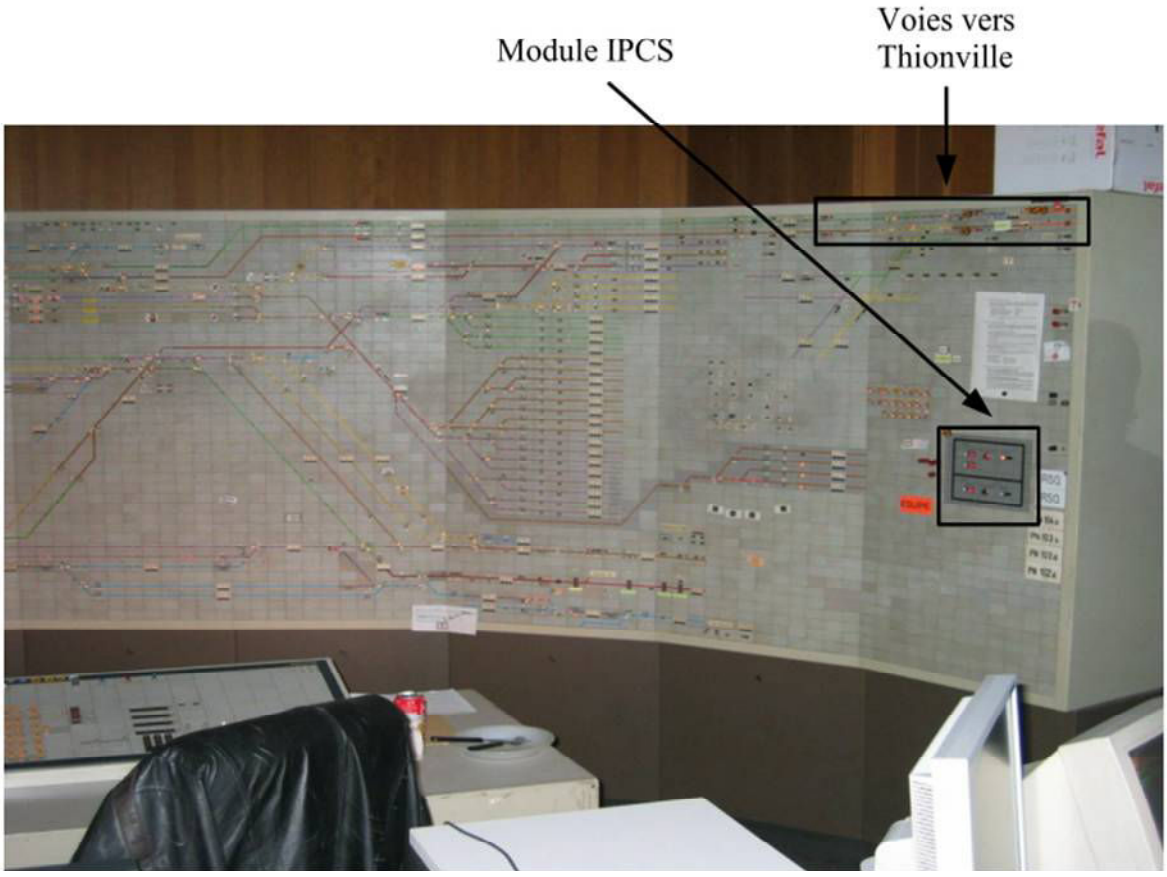

Figure 7.3. Intégration du module IPCS dans le TCO (BEA-TT, 2009).

De plus, les voyants et contrôles de l'IPCS ont une signification en partie différente de celles des voyants et contrôles du TCO (BEA-TT, 2009).

Le Tableau 7.1 montre la signification des voyants et contrôles du TCO et de l'IPCS. Nous remarquons que pour la section Bettembourg-Thionville, l'état non-occupé est représenté par un voyant allumé au blanc, tandis que ce même état est représenté par un voyant éteint pour les autres sections, sur le territoire du Luxembourg. Par ailleurs, un voyant allumé au rouge signifie tout autant un état occupé qu'un dispositif de sécurité en dérangement.

Signification des voyants et contrôles	**TCO**		**IPCS**
	Luxembourg	**Bettembourg-Thionville**	
Éteint	Non occupé Aucun itinéraire établi		
Blanc	Libre Itinéraire formé	Non occupé	Libre
Rouge	Occupé ou en dérangement	Occupé ou en dérangement	Occupé

Tableau 7.1. Signification des voyants et contrôles du TCO et de l'IPCS.

À Bettembourg, au sein du PDC, quatre opérateurs occupent les postes de (BEA-TT, 2009) :

- chef de circulation ;
- annonceur de train ;
- aiguilleur 1 et aiguilleur 2.

Le chef de circulation et l'annonceur de train ont la même qualification. Il y a alternance des postes chaque mois. De plus, pour assurer un service continu, les équipes d'opérateurs se relaient aux relèves. Les équipes du PDC appliquent des procédures décrites dans des règlements (BEA-TT, 2009).

Lorsque le chef de circulation établit un itinéraire, il doit effectuer un ensemble de contrôles, entre autres : que les voyants du TCO et de l'IPCS sont en blanc, qu'il n'y ait aucun train en circulation sur le registre d'annonce des trains (BEA-TT, 2009). Lorsqu'il n'est pas possible d'établir un itinéraire, par exemple en cas de dérangement, le chef de circulation peut utiliser le mode dérogatoire qui est l'émission d'un ordre écrit de franchissement d'itinéraire en marche à vue, en appliquant des fiches *ad hoc* et un formulaire adapté (ordre écrit A).

Le règlement décrit la procédure pour effectuer les relèves entre les équipes du matin et celles du soir (BEA-TT, 2009). Les activités des équipes sont tracées dans le registre d'annonce des trains (RAT) et dans le registre de prises et remises de service. Lors des relèves de service, les deux agents, celui qui remet le service et celui qui le prend, doivent certifier ces deux registres en apposant leur signature et en mentionnant l'heure exacte de la relève (BEA-TT, 2009).

Les circonstances de l'accident du 11 octobre 2006 s'inscrivent dans la relève entre l'équipe du matin et celle du soir (BEA-TT, 2009). Le chronogramme des évènements et des actions des opérateurs qui ont précédé l'accident (cf. Tableau 7.2) montre la dynamique de la relève, les impacts sur la capacité des opérateurs à élaborer, entretenir et diffuser une conscience partagée de la situation. Le chronogramme comprend les colonnes suivantes :

- l'horodatage (heure et minute) ;
- l'équipe du matin (les croix dans les colonnes indiquent la présence, une croix en gras indique un changement d'état départ ou arrivée) ;
    - CDC : le chef de circulation matin ;
    - Ann : l'annonceur train matin ;
    - Aig1 : l'aiguilleur 1 matin ;
    - Aig2 : l'aiguilleur 2 matin ;
- l'équipe du soir (signification des croix identique à l'équipe du matin) ;
    - CDC : le chef de circulation soir ;
    - Ann : l'annonceur train soir ;

    - Aig1 : l'aiguilleur 1 soir ;
    - Aig2 : l'aiguilleur 2 soir ;
- les évènements et actions des opérateurs ;
- l'analyse du point de vue de la résilience mentionne les facteurs de performance[29], les facteurs de contexte[30] et les comportements tels que la normalisation de la déviance, formulés entre crochets, ainsi que des éléments remarquables pour l'analyse.

[29] PSF : Facteurs de performance (*Performance Shaping Factors*)

[30] FC : Facteurs de contexte

Horo-datage	Équipe du matin				Équipe du soir				Évènements et actions des opérateurs (BEA-TT, 2009)	Analyse du point de vue de la résilience
	CDC	Ann	Aig1	Aig2	CDC	Ann	Aig1	Aig2		
11h15	X	X	**X**	X					L'aiguilleur 1 matin effectue la relève avec l'aiguilleur 2 matin. L'aiguilleur 1 matin quitte son poste.	
11h25	X	X		X			**X**		L'aiguilleur 1 soir arrive au PDC (Poste Directeur Central de Bettembourg). L'aiguilleur 1 soir effectue la relève avec l'aiguilleur 2 matin au titre des deux postes d'aiguillage (l'aiguilleur 2 soir n'est pas encore arrivé au PDC).	[PSF02], [FC03], [FC10]
11h26	X	X		**X**			X		L'aiguilleur 2 matin quitte le PDC.	
11h27	X	X					X		Le poste de circulation de Thionville informe l'annonceur matin de Bettembourg, du départ du train de fret circulant à contresens. Ce train a un retard de 43 minutes. L'annonceur train matin inscrit le train de fret avec une indication de contresens sur le registre d'annonce des trains. L'heure d'arrivée du train de fret n'est pas indiquée sur le registre d'annonce des trains. Il est toujours en route.	[PSF02], [PSF05], [PSF10] Horaire un peu exceptionnel du train de fret
11h27	X	X					X		Les trois agents présents sont le chef de circulation matin, l'annonceur train matin et l'aiguilleur 1 soir.	
11h27	X	X					X		Le chef de circulation matin et l'annonceur train matin sont informés de la circulation du train de fret à contresens.	[PSF02], [FC03], [FC10]
11h27	X	X					X		L'aiguilleur 1 soir n'est pas informé du passage du train de fret. L'aiguilleur 2 matin ne lui en a pas parlé lors de la relève.	Cela ne rélève pas de leur responsabilité
11h28	X	X				**X**	X		L'annonceur train soir arrive au PDC. L'annonceur train matin est relevé par l'annonceur train soir. Il l'informe de l'arrivée du train de fret à contresens.	[PSF02], [FC03], [FC10]
11h30	X	X				X	X		Le chef de circulation matin a inscrit sur un papier de brouillon blanc l'information que le train de fret circulait à contresens. L'utilisation d'une feuille « brouillon » est d'usage courant au PDC de Bettembourg.	[PSF02], [FC03], [FC10] [déviance] ; usage du papier « brouillon »

Horo-datage	Équipe du matin				Équipe du soir				Évènements et actions des opérateurs (BEA-TT, 2009)	Analyse du point de vue de la résilience
	CDC	Ann	Aig1	Aig2	CDC	Ann	Aig1	Aig2		
11h30	X	X				X	X		Le chef de circulation matin assure la relève de son poste avec l'annonceur train soir sans attendre l'arrivée du chef de circulation soir. Le chef de circulation matin indique le train de fret à contresens. Le chef de circulation matin remet la feuille « brouillon » à l'annonceur train soir. C'est une pratique contraire au règlement mais apparamment habituelle. L'annonceur train soir, disposant des habilitations de chef de circulation exerce brièvement l'intérim de chef de circulation soir, le temps que ce dernier arrive.	[PSF02], [FC03], [FC10], [PSF15], [déviance]
11h30	X	**X**				X	X		L'annonceur train matin quitte son service. Il entend le chef de circulation matin informer l'annonceur train soir de tout ce qui concerne la fonction de chef de circulation.	[FC03], [FC10]
11h31	X					X	X		Le chef de circulation matin a inscrit toutes les opérations importantes qui restent en vigueur pour les collègues de l'après-midi. Avant de partir, il a déposé cette feuille « brouillon » sur le bureau du chef de circulation.	[PSF02], [FC03], [FC10], [PSF15], [déviance]
11h32	**X**					X	X		Le chef de circulation matin quitte le PDC.	
11h33						X	X		L'annonceur train soir effectue l'intérim de chef de circulation	[PSF02], [FC03], [FC10]
11h35					**X**	X	X		Le chef de circulation soir prend son poste au PDC, légèrement en retard de 5 minutes. Le chef de circulation soir effectue la relève avec l'annonceur train soir. Les déclarations du chef de circulation soir et de l'annonceur train soir sont contradictoires à propos de la mention, ou pas, lors de la relève, du train de fret à contresens. L'annonceur train soir informe le chef de circulation soir du « brouillon » établi par le chef de circulation matin.	[PSF02], [FC03], [FC10], [PSF15], [déviance]

Horo-datage	Équipe du matin				Équipe du soir				Évènements et actions des opérateurs (BEA-TT, 2009)	Analyse du point de vue de la résilience
	CDC	Ann	Aig1	Aig2	CDC	Ann	Aig1	Aig2		
11h36					X	X	X		A l'annonce du train de voyageurs côté Luxembourg (un peu avant 11h37), l'aiguilleur 1 soir trace l'itinéraire entre l'entrée de la gare de Bettembourg et le signal Dm. A 11h37, l'annonceur train soir annonce le train de voyageurs à l'agent circulation de Thionville qui enregistre cette annonce sans commentaire. L'annonceur train se dirige alors derrière le TCO pour chercher le menu d'une pizzeria voisine pour commander des repas. Pendant ce temps, l'aiguilleur 1 trace l'itinéraire « origine Dm vers la frontière française ». L'itinéraire se forme sur le TCO mais le signal Dm ne s'ouvre pas.	[PSF02], [PSF05], [FC03], [FC10], [PSF15], [déviance] [déviance], [PSF15], [FC07]
									Il n'est pas rare qu'un signal ne s'ouvre pas lors de la commande d'un itinéraire, mais en réitérant celle-ci on obtient son ouverture ce qui permet d'éviter la délivrance d'un ordre de franchissement. Le chef de circulation soir demande donc à l'aiguilleur soir de recommencer.	Problème de fiabilité du dispositif de sécurité
11h36					X	X	X		Revenu à son poste, l'annonceur train demande à ses collègues qui est intéressé par une commande de nourriture pour le déjeuner. Le chef de circulation soir lui demande de commander un plat de lasagnes. L'annonceur train en commande deux, pour le chef de circulation et pour lui-même. L'aiguilleur 1 informe le chef de circulation soir que le signal Dm ne s'ouvre toujours pas malgré la seconde tentative de commande de l'itinéraire.	[PSF02], [FC07], [FC03], [FC10], [PSF15], [PSF10], [déviance]
11h37					X	X	X		Le chef de circulation soir signe le registre de prises et remises de service. Il regarde le TCO et constate l'arrivée du train de voyageurs habituel. Il prend connaissance des télégrammes et ordres du jour, ainsi que de ses courriers électroniques.	[PSF02], [PSF05], [PSF15], [double tâche]
11h37					X	X	X		Les trois agents présents sont le chef de circulation soir, l'annonceur train soir et l'aiguilleur 1 soir.	

Horo-datage	Équipe du matin				Équipe du soir				Évènements et actions des opérateurs (BEA-TT, 2009)	Analyse du point de vue de la résilience
	CDC	Ann	Aig1	Aig2	CDC	Ann	Aig1	Aig2		
11h37					X	X	X		Aucun des voyants du TCO situés sur la partie haute du TCO, où sont symbolisées les voies en direction de Thionville, n'indique que le train de fret circule sur la voie 1 à contresens de Thionville vers Bettembourg. Seules les indications du module IPCS pourraient permettre de s'apercevoir qu'un train est susceptible de circuler à contresens sur la voie 1 entre Thionville et Bettembourg, un voyant étant au rouge. Le registre d'annonce des trains porte la mention de la circulation du train de fret à contresens.	[PSF02], [PSF05], [PSF09], [FC04] Problème de l'IHM du TCO ne représentant pas la situation réelle (le train de fret à contresens)
11h40					X	X	X		A 11h40, le train de voyageurs approche du signal Dm fermé et freine pour venir s'y arrêter. A ce moment : • les voyants d'occupation de voie des zones situées à l'amont de ce signal sont au rouge puisqu'elles sont occupées par le train de voyageurs ; • les voyants d'occupation de voie des zones situées entre le signal Dm et le signal Bm sur la voie 1 sont au blanc, l'itinéraire ayant été commandé et toutes les conditions relatives à ces zones étant remplies ; • le voyant bleu de l'anti-répétiteur clignote, les conditions relatives à l'intervalle Bm-113 ne sont pas remplies ; • les voyants d'occupation de voie des zones situées entre le signal Bm et la frontière sont également au blanc, aucun train ne circulant dessus ; • le voyant de contrôle du signal Dm est au rouge ; • le voyant de contrôle du signal Bm est au rouge, l'itinéraire de rentrée au triage du train de fret n'a pas été commandé.	[PSF09], [FC04]

Horo-datage	Équipe du matin				Équipe du soir				Évènements et actions des opérateurs (BEA-TT, 2009)	Analyse du point de vue de la résilience
	CDC	Ann	Aig1	Aig2	CDC	Ann	Aig1	Aig2		
11h40					X	X	X		Les voyants de la voie n°1 du module IPCS présentent les indications ci-après : • un voyant est au rouge, un train de fret circule sur cette portion de voie ; • un voyant est éteint, Thionville ayant pris le sens (contresens établi) ; • le commutateur sens-secours est éteint, celui-ci n'a pas été actionné ; • le voyant de contresens est éteint.	[PSF09], [FC04]
11h40					X	X	X		Le chef de circulation est persuadé que la circulation sur la voie 1 s'effectue dans le sens normal, c'est-à-dire vers Thionville. Les informations qu'il a pu effectivement acquérir convergent pour créer cette impression et le monde autour de lui se comporte comme si tel était bien le cas : • tous les trains programmés dans la tranche horaire 11h30 – 13h30 sont des trains réguliers de sens normal (voie 1 vers Thionville), ce qui est le cas du train de voyageurs qui arrive ; • le train de voyageurs est à l'heure et est annoncé à Thionville sans observation particulière ; • l'aiguilleur 1 cherche à tracer l'itinéraire vers Thionville, qui se forme effectivement mais le signal Dm ne s'ouvre pas ; • il n'a noté, à l'occasion de la relève, aucune mention de la circulation du train de fret. Les deux indications sur le TCO signalant une situation réelle plus complexe étaient : • le clignotement de l'anti-répétiteur, que le chef de circulation a constaté mais dont il ne se préoccupe pas ; • l'extinction du voyant de sens des IPCS de la voie 1, qu'il ignore n'ayant pas consulté le module IPCS sur le TCO. La circulation du train de fret à contresens est également portée sur le registre d'annonce des trains, mais le chef de circulation ne l'a pas consulté.	Absence de conscience de la situation de la part du chef de circulation de Bettembourg. Les informations génèrent un biais de confirmation. Le caractère exceptionnel du train de fret n'est pas perçu

Horo-datage	Équipe du matin				Équipe du soir				Évènements et actions des opérateurs (BEA-TT, 2009)	Analyse du point de vue de la résilience
	CDC	Ann	Aig1	Aig2	CDC	Ann	Aig1	Aig2		
11h41					X	X	X		Compte tenu de sa conviction que le sens de circulation est établi vers Thionville, le chef de circulation du PDC ne procède pas à l'ensemble des vérifications préalables prescrites avant de délivrer un ordre écrit de franchissement. Il regarde la partie supérieure droite du TCO ; il voit que tous les voyants à l'aval du signal Dm sont au blanc ce qui signifie que l'itinéraire est formé pour la partie de voie concernée de la gare de Bettembourg, à l'avant de Bm, et qu'il n'y a pas de train vers la frontière française, coté Luxembourg. Bien que le voyant bleu de l'anti-répétiteur clignote, signalant que toutes les conditions ne sont pas remplies pour établir l'itinéraire à l'aval de Dm, le chef de circulation soir ne regarde pas le module IPCS, omission qui paraît avoir été assez courante au PDC de Bettembourg 1. Le chef de circulation soir ne constate donc pas que le voyant de contrôle de l'intervalle BM-113 est au rouge (intervalle occupé ou en dérangement) et que celui du sens SN BM-113 est éteint (contresens établi ou dérangement), ce qui l'aurait informé de la situation réelle. Il n'appelle pas non plus le chef de circulation de Thionville, action prescrite dans la consigne d'exploitation frontalière, qu'il réalise habituellement avant de délivrer un ordre de franchissement, peut-être à cause de son retard à la prise de poste et de son souhait de se retrouver au plus vite en situation courante ; il ne veut pas retarder le train de voyageurs. Il conclut donc que le signal Dm est en dérangement, en omettant d'effectuer certains des contrôles réglementaires notamment ceux qui concernent la condition IPCS dans l'ouverture du signal Dm (le signal ne peut pas s'ouvrir si le contresens est établi).	[PSF09], [FC04], [FC03], [FC10], [PSF15], [Déviance] Problème des IHM du TCO et de l'IPCS non intégrés Problème de l'absence de faibilité des dispositifs de sécurité souvent en dérangement Problème de conscience de la situation par le chef de circulation
11h39					X	X	X		A 11h39, le chef de circulation soir décide de dicter par radio un ordre de franchissement du signal Dm au conducteur du train de voyageurs. On peut noter qu'à cet instant, la tête du train de fret se trouve vers le PK 197.	[FC03], [FC10], [PSF15], [déviance] ; appel à une procédure dérogatoire

Horo-datage	Équipe du matin				Équipe du soir				Évènements et actions des opérateurs (BEA-TT, 2009)	Analyse du point de vue de la résilience
	CDC	Ann	Aig1	Aig2	CDC	Ann	Aig1	Aig2		
11h40					X	X	X		Le chef de circulation soir demande au central radio sol-train de le mettre en relation avec le conducteur du train de voyageurs. A 11h40, le chef de circulation soir commence à dicter l'ordre de franchissement du signal Dm (ordre modèle A1) au conducteur, le train de voyageurs étant arrêté au pied du signal.	[FC03], [FC10], [PSF15], [déviance] ; appel à une procédure dérogatoire
11h42					X	X	X		A 11h42, l'ordre de franchissement est dicté et le train de voyageurs reprend sa marche vers Thionville vers 11h42'10".	[FC03], [FC10]
11h43					X	X	X	**X**	L'aiguilleur 2 soir arrive au PDC vers 11h43.	
11h43					X	X	X	**X**	Alerté de son erreur, le chef de circulation soir demande d'effectuer une alerte générale radio et de couper le courant de traction. Les deux moyens pour éviter l'accident échouent. La radio du train de fret ne fonctionne pas. La coupure de courant n'a pas été effectuée dans les temps.	Absence de fiabilité des dispositifs de sécurité de secours pour corriger l'erreur
11h44					X	X	X	X	Le train de voyageurs et le train de fret entrent en collision frontale. Leurs vitesses sont respectivement de 78 km/h et 79 km/h.	

Tableau 7.2. Chronogramme des événements et actions des opérateurs dans les minutes qui ont précédé l'accident du 11 octobre 2006.

Par ailleurs, au sein des chemins de fer luxembourgeois (CFL), il a été établi un système de gestion de la sécurité garantissant la maîtrise de tous les risques créés par les activités ferroviaires. Le système vise notamment à bien connaître et évaluer en permanence la situation et l'évolution de la sécurité sur le terrain, afin de détecter les risques apparaissant et prendre les mesures préventives utiles (BEA-TT, 2009).

L'organisation de ce système de gestion de la sécurité repose sur un comité directeur de la sécurité qui se réunit trois à quatre fois par an. Il regroupe la direction générale, les chargés de gestion des services d'exploitation et le service qualité, sécurité et environnement (QSE). En cas d'augmentation statistiquementmentment significative de la fréquence de certains évènements, le comité de direction de la sécurité examine les mesures préventives et correctives à prendre (BEA-TT, 2009).

L'évaluation des risques repose sur (BEA-TT, 2009) :

- l'analyse des risques ;
- les audits de sécurité ;
- le suivi régulier des indicateurs de sécurité ;
- les enquêtes sur les incidents graves et les accidents.

Les évènements enregistrés dans une base de données mise à jour quotidiennement et les statistiques sur les indicateurs de sécurité sont présentés régulièrement au comité directeur de la sécurité dans le but de déceler les points forts et les points faibles de la gestion de la sécurité (BEA-TT, 2009).

Néanmoins, le retour d'expérience montre que 843 ordres écrits de franchissement ont été délivrés dans les 3 mois précédent l'accident sur l'ensemble du réseau des chemins de fer luxembourgeois, dont 300 sans motif tracé.

À Bettembourg, sur la même période, 107 ordres écrits de franchissement un signal fermé ont été délivrés, dont 90 au PDC de Bettembourg, soit un par jour. Sur ces 90 ordres écrits de franchissment, 42 avaient pour cause un dérangement, et 27 une cause indéterminée. 60% des dérangements ont des causes inconnues. Ce problème de fiabilité du système réduit l'attention des opérateurs portée sur les vérifications à mener systématiquement avant de délivrer un ordre écrit de franchissment (BEA-TT, 2009).

L'utilisation routinière de la procédure dérogatoire d'émission d'ordres écrits de franchissement de signal procède de la normalisation de la déviance en réponse au problème récurrent de fiabilité des dispositifs de sécurité régulièrement en dérangement. A cette utilisation routinière d'ordre de franchissement d'itinéraire s'ajoute le caractère exceptionnel du passage d'un train de fret à cette heure (entre 11h30 et 13h30). Enfin, les déviations dans la relève ont contribué à l'absence d'une conscience partagée de la situation par l'ensemble des opérateurs en place.

7.2.3. Analyse du point de vue de la résilience de l'accident d'Aldershot

Le troisième cas concerne l'accident d'un train de voyageurs qui eut lieu à Aldershot, Ontario, au Canada, le 26 février 2012. Le train était conduit par deux mécaniciens et un apprenti mécanicien. L'accident entrainant la mort des trois membres de l'équipe d'exploitation (BST, 2013).

Après un arrêt à la gare d'Aldershot, le train est reparti sur la voie 2. Dans 99% des cas, le train de la compagnie circulait sur la voie 2. Ce jour-là, des travaux étaient réalisés sur la voie

1 et la voie 2 faisait partie de l'emprise des travaux. Un permis d'occuper la voie (POV) fut octroyé à l'équipe en charge de ces travaux par le contrôleur de la circulation ferroviaire (CCF). Le CCF a opté pour aiguiller le train de voyageurs sur un itinéraire qui contournait la zone d'application du POV sur la voie 2. Le CCF a orienté les aiguillages de la voie pour amener le train de la voie 2 à la voie 3 par la liaison nº 5. Le CCF n'a pas communiqué le POV ni le changement d'itinéraire à l'équipe d'exploitation du train de voyageurs. Il n'était pas tenu de le faire. De plus, l'équipe d'exploitation du train n'a pas été informée de ces travaux lors de la séance de briefing avant le départ du train à l'intention de l'équipe (BST, 2013).

La vitesse sur cette liaison nº 5 était limitée à 24 km/h (15 mi/h). Cette consigne était communiquée par les signaux de voie que l'équipe d'exploitation est supposée appliquer à la lettre. Le train est entré sur la liaison nº 5 à une vitesse de 108 km/h (67 mi/h). La locomotive a déraillé et percuté les fondations d'un bâtiment adjacent à l'emprise. Les membres de l'équipe d'exploitation ont subi des blessures mortelles, et 45 personnes (44 voyageurs et le directeur des services) ont subi diverses blessures (BST, 2013).

Les deux mécaniciens étaient qualifiés, satisfaisaient aux normes de repos, connaissaient bien le territoire et comptaient chacun plus de 30 ans d'expérience ferroviaire. Au cours des 16 derniers mois, ils avaient régulièrement formé équipe. L'apprenti, quant à lui, mécanicien stagiaire, était un mécanicien de locomotive qualifié comptant 22 ans d'expérience ferroviaire. Il venait d'être embauché comme stagiaire en octobre 2011 par la compagnie (BST, 2013).

Dans les trois mois précédent l'accident, les trains ont fait un arrêt à Aldershot dans 97% des cas. Les trains ont été dirigés sur la liaison à vitesse limitée à 24 km/h (15 mi/h) dans moins de 1% du temps. Enfin, les trains circulaient sur la voie 2 avec une vitesse normale plus de 99% du temps (BST, 2013).

Ce jour là, l'enquête montre que l'équipe d'exploitation a rencontré un signal « de vitesse normale à vitesse limitée » sans dépasser 45mi/h (72 km/h) à l'approche d'Aldershot. Après l'arrêt à la gare d'Aldershot, l'équipe d'exploitation est repartie, reprenant une vitesse normale. Elle a rencontré un signal « avancer, petite vitesse », sans dépasser 15 mi/h (24 km/h) juste avant la liaison n°5.

Le chronogramme des évènements et des actions des opérateurs qui ont précédé l'accident (cf.Tableau 7.3) montre la dynamique du train et l'incapacité des opérateurs de comprendre la situation. Le chronogramme comprend les colonnes suivantes :

- l'horodatage (heure et minute) ;
- la vitesse du train (en km/h) ;
- les évènements et actions des opérateurs ;
- l'analyse du point de vue de la résilience mentionne les facteurs de performance, les facteurs de contexte, formulés entre crochets.

L'analyse nous montre que l'équipe d'exploitation ne semble pas avoir conscience de la situation, le contexte spécifique de cet itinéraire exceptionnel puisque devant contourner la zone de travaux, itinéraire pour lequel elle n'avait reçu aucune information. L'équipe d'exploitation a subi l'effet d'un biais cognitif, ne percevant la situation que trop tard.

Horo-datage	Vitesse du train (km/h)	Évènements et actions des opérateurs (BST, 2013)	Analyse du point de vue de la résilience
13h06 :00		L'équipe du train prend son service à Niagara Falls.	
14h04 :40		Le train quitte Niagara Falls.	
14h04 :58		Le POV est transmis à l'agent d'entretien des signaux entre Alderhot East et Burlington West.	[PSF02], [FC03], [FC10]
14h47 :39		Le train quitte Grimsby.	
15h12 :56		La liaison n°5 est orientée de la voie 2 à la voie 3 pour que le train puisse contourner l'équipe de travaux.	
15h14 :42	66,46	Le train franchit le signal indiquant « de vitesse normale à vitesse limitée ».	
15h16 :23	85,61	Le train franchit le signal avancé indiquant « de vitesse normale à petite vitesse ».	[PSF15], [PSF02], [PSF10], [PSF09]
15h16 :45	38,46	Le train arrive à l'extrémité est de la gare d'Aldershot sur la voie 2.	
15h17 :19	0	Le train arrive à la gare d'Aldershot.	
15h23 :26	1,6	Le train quitte la gare d'Aldershot sur la voie 2.	
15h25 :18	94,46	Le kaxon est actionné.	
15h25 :21		Les barrières sont actionnées au passage à niveau de King Road.	
15h25 :22	96,07	Le mécanicien avance la manette de vitesse de la position 6 à la position 8 (accélérer).	[PSF09], [FC04]
15h25 :26	98,97	Le kaxon est actionné par intermittence.	[PSF09], [FC04]
15h25 :33	104	Le train franchit le signal indiquant « de petite vitesse à vitesse limitée ».	[PSF15], [FC10], [PSF10], [PSF09]
15h25 :37	105,41	Coup de kaxon.	[PSF09], [FC04]
15h25 :39	107,18	La manette de vitesse est ramenée de la position 8 à la position 6 (ralentir).	[PSF09], [FC04]
15h25 :40	107,18	La manette de vitesse est ramenée de la position 6 à la position 3 (ralentir).	[PSF09], [FC04]
15h25 :41	107,18	Le kaxon est désactivé.	[PSF09], [FC04]
15h25 :42	107,18	Second coup de klaxon.	[PSF09], [FC04]
15h25 :43	107,66	Entrée de la locomotive sur la liaison n°5.	[PSF15],
15h25 :44	107,18	La manette de vitesse est ramenée de la position 3 à la position de ralenti (0), tandis que la locomotive déraille à la sortie de la liaison n°5.	[PSF09], [FC04], [PSF15],
15h25 :51	0	La locomotive s'immobilise sur le côté.	

Tableau 7.3. Chronogramme des événements et actions des opérateurs dans les minutes qui ont précédé l'accident du 26 février 2012.

7.2.4. Synthèse de l'analyse des accidents, du point de vue de la résilience

Nous avons présenté les analyses des trois accidents, du point de vue de la résilience. Cette synthèse met en évidence les points cruciaux de ces analyses à partir desquels seront définis les scénarios, modélisés les personas. Ces points d'entrée structureront le patron de conception « surveiller et alerter » pour l'architecture d'un système résilient, dans le domaine ferroviaire.

En synthèse, des trois rapports d'enquête technique, nous retenons que :

- le conducteur du train de voyageurs, à Chatsworth, téléphonait et envoyait des SMS pour rompre l'ennui généré par son activité routinière. Le réseau présentait des sections à voie unique plus dangereuses et nécessitant une vigilance accrue. La double tâche (envoi des SMS) était indépendante du contexte et perturba la vigilance du conducteur de trains de voyageurs lorsqu'il devait être plus attentif, il franchit un feu rouge ;
- l'absence de fiabilité des dispositifs de sécurité de Bettembourg généra l'émission routinière d'ordres écrits de franchissement de signal. De plus, le train de fret circulait entre 11h30 et 13h30, période de la journée durant laquelle la plupart des trains qui circulent sont des trains de voyageurs. À cause de l'absence d'intégration de l'interface utilisateur du TCO et de l'IPCS, la plupart du temps les opérateurs ne regardaient pas l'IPCS pour effectuer les contrôles préalables à l'émission d'ordres écrits de franchissement de signal. Suite à une relève qui ne respectait pas les consignes, le chef de circulation du soir et l'annonceur train du soir ne partageaient pas une représentation fonctionnelle partagée de la situation. Le chef de circulation n'a pas compris qu'un train de fret circulait en contresens lorsqu'il a émis l'ordre écrit de franchissement de signal ;
- l'équipe d'exploitation n'a pas compris la situation. Normalement, le train circule sur la voie 2 à vitesse normale. L'opérateur de régulation qui avait donné la permission d'effectuer des travaux n'avait pas communiqué cette information à l'équipe d'exploitation.

Dans l'ensemble de ces situations, les opérateurs ne partagent pas une représentation fonctionnelle dynamique de la situation, qu'elle qu'en soit la raison.

Faute de cette représentation fonctionnelle partagée de la situation, ils ne comprennent que trop tard la situation, au-delà du point de non retour.

L'objectif est d'alerter les opérateurs, en particulier en leur communiquant les informations relatives au risque couru et à la proximité du danger afin de rompre les biais cognitifs qui perturbent leur représentation de la situation et d'agir pour éviter un accident.

Après avoir présenté et analysé les trois d'accidents, nous appliquons le persona individuel et le persona collectif au domaine ferroviaire pour en évaluer la faisabilité.

7.3. Application des processus à mettre en œuvre pour contribuer à la résilience d'un système ; du scénario au persona

Dans cette section, nous appliquons le persona individuel et le persona collectif (cf. section 6.4 « Contribution aux adaptations du persona individuel / collectif aux systèmes critiques à longue durée de vie ») au domaine ferroviaire en nous appuyant sur les rapports d'enquête technique (cf. section 7.2 « Synthèse des rapports d'enquête technique d'accidents ferroviaires »). L'objectif de cette application est d'identifier les caractéristiques structurantes ayant des impacts sur la résilience et qui sont à prendre en compte pour la conception des interfaces utilisateur. Les caractéristiques structurantes sont rappelées par des mots-clefs entre crochets. Il en est de même des facteurs de performance affectant les fonctions de la résilience (cf. section 4.1 « La problématique de la résilience des systèmes »).

7.3.1. Le persona individuel pour la conception des IHM des systèmes résilients

Nous commençons par formuler le scénario d'un accident (accident fictif agrégeant les caractéristiques pertinentes relatives à la résilience) faisant appel aux personas (cf. Figure 7.4). Après quoi, nous décrivons les deux personas de ce scénario. Ces deux personas (personnages fictifs, agrégeant les caractéristiques pertinentes relatives à la résilience et complétement indépendants des individus qui ont eu des accidents), sont celui d'un conducteur de train, Patrick Davidson et celui d'un contrôleur de trafic, Sarah Sanchez, pour évaluer les impacts du persona sur la conception du système.

Le scénario d'un accident faisant appel aux personas

Les trains d'une compagnie ferroviaire circulent sur les voies exploitées par un opérateur d'infrastructure ferroviaire. Ce sont deux entreprises différentes.

L'opérateur d'infrastructure ferroviaire réalise des travaux pour rénover ces infrastructures à bout de souffle. Le tronçon concerné comporte trois voies en parallèles. Ces travaux sur une voie (voie 1) impliquent d'arrêter le trafic sur la voie adjacente (voie 2) et d'aiguiller les trains sur une troisième voie (voie 3). Traditionnellement, lorsqu'il y a des travaux, une sentinelle est postée en amont des travaux pour avertir les trains des travaux en cours. La sentinelle est un facteur clef de la sécurité. Ce rôle de sentinelle est connu des opérateurs des deux compagnies qui sont habitués à ce fonctionnement et se fient à leur fonction de sécurité. Pour des raisons de réduction de budget, dans la mesure où il n'y eut pas d'accident, l'opérateur d'infrastructure ferroviaire a décidé de supprimer la sentinelle lorsqu'il y a des travaux sur les voies [PSF08], -[PSF15], [Contournement], sans en informer les compagnies ferroviaires, puisque rien ne l'oblige à le faire. Du coup, la sécurité relève du contrôleur de train et des signaux sur la voie. La voie 2 est utilisée traditionnellement par une compagnie ferroviaire qui y fait passer plus de 99% de ces trains [PSF05], [Routines]. Un de ces trains est conduit par Patrick Davidson qui fait ce parcours régulièrement [PSF05].

Le jour de l'accident, Sarah Sanchez positionne les signaux de voie. Sarah Sanchez est soucieuse de la santé de sa fille, Esther [Événement]. Patrick Davidson, quant à lui, est très préoccupé par la santé de sa femme [Événement]. Il téléphone à l'hôpital dans lequel elle est hospitalisée pour connaître son état de santé. Il procède comme d'habitude [PSF05], [Routines] et n'a pas vu le signal de réduction de vitesse [PSF15]. Quand il comprend la situation, il freine, mais c'est trop tard. Le train prend la liaison avec une vitesse excessive et déraille. Patrick Davidson est gravement blessé dans l'accident, et mettra de nombreux mois à se remettre de cet accident.

Figure 7.4. Scénario faisant appel aux personas.

Ce scénario décrit les circonstances d'un accident. Il mentionne des caractéristiques et des facteurs de performance marqués entre crochets. Il fait appel aux deux personas Sarah Sanchez et de Patrick DAVIDON que nous décrivons maintenant (cf. Figure 7.5 « Persona fictif de conducteur de train. » et Figure 7.6 « Persona fictif du contrôleur de circulation ferroviaire. »).

Ce scénario et ces personas mettent en évidence que les personas ne partagent pas un cadre commun d'interprétation de la situation qui leur permet de se coordonner. De plus, ces personas expriment le besoin de ce cadre ainsi que d'être alertés lorsque le système est à proximité d'une zone de danger. Enfin, le persona présente aux concepteurs des informations importantes pour la conception du système.

Le persona : Patrick Davidson (personnage fictif)

Patrick Davidson est conducteur de train depuis 30 ans. Après une formation secondaire, il est entré comme cheminot et a suivi des cours du soir [Formation]. Il est ainsi devenu conducteur de train, activité qui est la sienne depuis 30 ans [Expérience]. À 57 ans, pesant plus de 105kg, il souffre de surpoids et prend des médicaments anticholestérolémiant [Physio]. Il souffre de presbytie et porte des lunettes pour lire [Physio].

Sa femme, Mary DAVIDSON, vient d'avoir un accident vasculaire cérébral. Il est très inquiet pour sa femme [Événement].

Patrick Davidson est un homme ouvert, expansif, passionné par son travail [Personnalité]. Il aime partager son enthousiasme avec d'autres personnes et souhaite devenir président de l'association ferrivophile de sa ville [Socialité]. Il est difficile à convaincre, peu sensible aux idées des autres et en fait un peu à sa tête [Personnalité]. Patrick Davidson est considéré par sa hiérarchie comme étant un professionnel confirmé [Expérience].

L'activité de conduite de train est largement automatisée [PSF06], routinière et morcelée [Activité]. Patrick Davidson est seul dans sa cabine et communique par la radio avec le chef de train et l'opérateur du poste de contrôle. Cette activité routinière [PSF06] et solitaire [PSF13] génère chez lui de l'ennui. Mais les exigences de sûreté impliquent une grande vigilance de sa part [PSF14], [Activité].

Les organismes de tutelle ont publié des règlements relatifs à l'usage de dispositifs électroniques dans le cadre de l'activité professionnelle, en particulier par les conducteurs de train, dans l'activité de conduite [PSF15], [Contournement].

Pourtant Patrick Davidson ne s'explique pas comment il a pu violer une barrière symbolique (signaux de voie) réduisant la vitesse du train pour s'engager dans l'aiguillage [PSF15]. Patrick Davidson déplore de ne pas avoir de représentation commune de la situation [PSF07] pour se coordonner et réguler leur activité avec le contrôleur de circulation.

Figure 7.5. Persona fictif de conducteur de train.

Après avoir décrit le persona de Patrick Davidson, conducteur du train, nous poursuivons en décrivant le persona de Sarah Sanchez, contrôleur de circulation ferroviaire.

Le persona : Sarah Sanchez (personnage fictif)

A 45 ans, Sarah Sanchez est contrôleur de circulation ferroviaire depuis 15 ans [Expérience]. Elle a complété sa formation initiale par une formation continue dans le domaine ferroviaire avant de rejoindre la compagnie dans laquelle elle travaille aujourd'hui [Formation]. Sarah Sanchez a une petite fille de 10 ans, Esther [Info_Perso]. Gravement malade, Esther subit des examens médicaux. Leurs résultats préoccupent beaucoup Sarah [Événement].

Toujours souriante, Sarah est réservée [Personnalité]. Elle est trésorière d'une association qui fait du soutien scolaire au profit d'enfants de milieux défavorisés [Socialité]. Sarah est connue

pour sa rigueur et son professionnalisme [Expérience].

Elle contrôle les trains sur un tronçon qui est en travaux depuis plusieurs mois pour rénover les infrastructures à bout de souffle [Activité].

En tant qu'agent de l'opérateur d'infrastructure ferroviaire, Sarah Sanchez a été informée que les équipes de chantiers n'ont plus de sentinelle [PSF08], [PSF15] [Contournement]. Son activité nécessite une plus grande vigilance de sa part puisque la sécurité repose essentiellement sur les positions des signaux de voie [PSF14], [Activité]. Mais préoccupée par la santé d'Esther, elle a oublié d'informer Patrick Davidson des travaux sur la voie [PSF13], nécessitant que le train que conduit Patrick Davidson circule sur la voie 3 [PSF05].

Sarah Sanchez s'en veut beaucoup de ne pas avoir informé Patrick Davidson des travaux [PSF13] et de leurs impacts sur la circulation des trains [PSF15]. Sarah Sanchez souhaite disposer des moyens pour mieux comprendre la situation opérationnelle [PSF08] et pour communiquer avec les conducteurs de train [PSF07], [PSF13].

Figure 7.6. Persona fictif du contrôleur de circulation ferroviaire.

La Figure 7.7 illustre la modélisation du persona Patrick Davidson via un acteur dans un diagramme. Les caractéristiques du persona sont celles identifiées dans la section 6.4.1 « évolution du persona individuel» du chapitre précédent. Les valeurs des champs correspondent à la description du persona (cf. Figure 7.5).

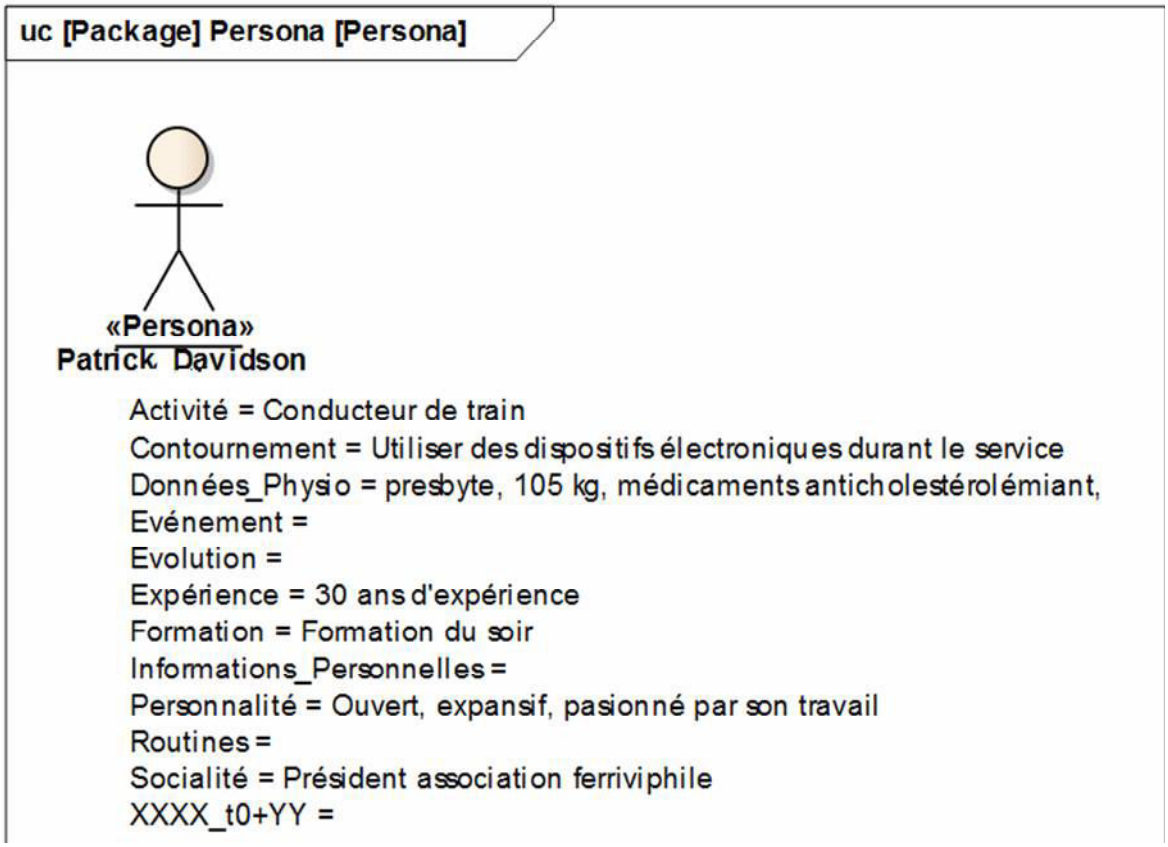

Figure 7.7. Modélisation du persona via un acteur SysML.

7.3.2. Application de l'ergonomie prospective et du persona

Après avoir décrit Patrick Davidson (cf. Figure 7.5), dans la perspective de l'ergonomie prospective, nous décrivons comment, à l'horizon de 10 ans, il réalise son activité de conduite de train, en utilisant les artefacts technologiques qui n'existent pas encore, mais qui sont imaginés dans des études prospectives sur les technologies du futur (cf. Figure 7.8).

Patrick Davidson a 67 ans [Données_Physio] et continue son activité de conduite de train [Activité]. Il utilise les artefacts technologiques [PSF09], [FC04] que les acteurs économiques ont développé pour les seniors [Données_Physio] dans la perspective de les assister dans leur activité [Activité]. Il poursuit son activité parce que la caisse de retraite n'a pas suffisamment d'argent pour payer sa pension et il n'y a personne qui puisse le remplacer [PSF08]. Sachant que les postes opérateurs peuvent être tenus aussi bien par des seniors que des personnes plus jeunes, les dispositifs doivent être configurables afin d'être adaptés aux opérateurs, jeunes ou âgés [PSF09] et [FC04], qui tiennent le poste, à tour de rôle. Pour l'aider dans son activité, Patrick Davidson dispose d'une IHM présentant l'état du réseau [PSF09], [FC04] et, en incrustation de réalité virtuelle, une représentation des trains du réseau, en particulier ceux qui sont devant et derrière le train, sans qu'il y ait inter-visibilité [PSF05].

Figure 7.8. Application de l'ergonomie prospective et du persona.

L'application de l'ergonomie prospective et du persona met en évidence les évolutions sociétales et économiques, leurs impacts sur le personnel, l'activité et les artefacts adaptés aux seniors. En particulier, ce sont des informations qui sont à tracer pour justifier d'une conception.

7.3.3. Le persona collectif pour la conception des IHM des systèmes résilients

Le persona collectif appliqué au domaine ferrovaire permet de rendre compte de la dynamique au sein d'un persona collectif et des coordinations entre deux personas collectifs, celui de l'équipe de contrôle du trafic ferroviaire de la gare de La Fayette, au Greenland (cf. Figure 7.9), et celui de l'équipe de régulation de trafic de la gare de Yorktown, Yellowland (cf. Figure 7.10).

Persona collectif : l'équipe de la salle de régulation de trafic de La Fayette

L'équipe de contrôle de la circulation de la gare de La Fayette dans le pays de Greenland doit contrôler et commander le trafic entre la station de La Fayette et la frontière entre le Greenland et le pays de Yellowland [PSF09], [PSFpc09]. La prochaine gare de Yellowland est Yorktown. L'équipe de La Fayette se compose de trois différentes personas, respectivement, d'Anne Jameson, contrôleur en chef du trafic, d'Arnold Stoner, annonceur de train, et d'Ingmar Jorgensen, aiguilleur [PSF02], [PSFpc02]. Ils sont habitués à travailler ensemble et ils se connaissent bien [PSF04], [PSFpc04]. Ils partagent tous la culture de la sécurité et communiquent étroitement entre eux [PSF04], [PSFpc04], [FC03], [FC10]. La société favorise les relations d'égal à égal plutôt que les relations hiérarchiques [PSF5], [PSFpc05]. Ainsi l'équipe a l'habitude d'effectuer des auto-contrôles afin d'améliorer la sécurité [PSF6], [PSFpc06]. Les membres de l'équipe parlent Greenlandish entre eux, et parlent Globish avec leurs collègues de Yorktown [PSF07], [PSFpc07].

Figure 7.9. Persona collectif de l'équipe de la salle de régulation de trafic de La Fayette.

Persona collectif : l'équipe de la salle de régulation de trafic de Yorktown

L'équipe de contrôle de la circulation de Yorktown doit contrôler et commander le trafic entre la station de Yorktown et la frontière entre le Greenland et le Yellowland [PSF09], [PSFpc09]. L'équipe comprend des personas individuels, respectivement, Laura Fromgarden, contrôleur du trafic du matin, Henry Martin, contrôleur du trafic du soir (contrôleurs en chef et responsables de l'activité de contrôle de la circulation), Claude Buick, annonceur train du matin, Phil Vernes, annonceur train du soir, Theresa Cruz, aiguilleur du matin et Elisabeth Tang, aiguilleur du soir [PSF02], [PSFpc02]. Henry Martin, Phil Vernes et Elisabeth Tang relèvent, respectivement, Laura Fromgarden, Claude Buick et Theresa Cruz [PSF03], [PSFpc03].

Ils sont amenés à travailler ensemble mais communiquent peu entre eux [PSF04], [PSFpc04], [FC03], [FC10]. La culture de la société favorise les relations hiérarchiques [PSF05], [PSFpc05]. Ainsi l'équipe accorde sa confiance au contrôleur en chef, sans commentaire ou discussion au sujet des décisions prises [PSF05], [PSFpc05].

Ils régulent la circulation des trains qui circulent entre Yorktown et La Fayette, dont le train de voyageurs conduit par David Chung [PSF05], [PSFpc05].

Les membres de l'équipe de la gare de Yorktown parlent la langue de Yellowland entre eux et le Globish avec leurs collègues de gare de La Fayette [PSF07], [PSFpc07].

Figure 7.10. Persona collectif : équipe de la salle de régulation de trafic de Yorktown.

Après avoir décrit les deux personas collectifs des gares de La Fayette et de Yorktown, nous élaborons le scénario dans lequel les deux personas sont amenés à communiquer. Les difficultés de communication et de coordination entre les deux personas collectifs sont à l'origine d'un accident. Ce scénario (cf. Figure 7.11) décrit la dynamique de l'échange à l'origine de l'accident.

Persona collectif : Le scénario de communication au sein et entre des personas collectifs

Laura Fromgarden et Anne Jameson communiquent ensemble [PSF01], [PSFpc01] afin de préparer la circulation de deux trains, un de fret, de La Fayette à Yorktown, et un train de voyageurs, de Yorktown à La Fayette. Les deux trains voyagent sur la même voie en sens alterné puisque l'autre voie est en travaux [PSF11], [PSFpc11]. Ils conviennent de l'ordre de passage de ces trains, d'abord le train fret, puis le train de voyageurs [PSF05], [PSFpc05].

La procédure à appliquer à la gare de Yorktown (Règlements généraux) stipule que l'opérateur du matin communique à l'opérateur du soir les consignes et les évènements en cours lors de la relève [PSF02], [PSFpc02]. Henry Martin est un peu en retard [PSF08], [PSFpc08]. Laura Fromgarden prépare la relève avec Phil Vernes [PSF01], [PSFpc01], [PSF08], [PSFpc08] à qui elle fait part de la situation du train de fret circulant de La Fayette à Yorktown.

Quand Henry Martin arrive, Phil Vernes est occupé à élaborer un compte-rendu d'activité et oublie de lui faire part de la circulation exceptionnelle du train de fret [PSF09], [PSFpc09]. En prenant son poste [PSF09], [PSFpc09], Henry Martin regarde la visualisation principale et ne voit pas l'indicateur de train de fret mentionné sur un affichage secondaire que personne ne regarde [PSF10], [PSFpc10], [PSF09], [PSFpc09].

Henry Martin demande à Theresa Cruz d'ouvrir la voie entre Yorktown et La Fayette pour la circulation du train de voyageurs que conduit David Chung [PSF01], [PSFpc01], [PSF02], [PSFpc02]. Puisqu'elle ne peut pas ouvrir la voie, en raison d'un défaut récurrent, connu et non encore réparé [PSF11], [PSFpc11], Henry Martin formule un ordre écrit de franchissement de signal à David Chung [PSF01], [PSFpc01], [PSF15]. David Chung n'est pas surpris. Les

problèmes de fiabilité des dispositifs de sécurité que rencontre l'équipe de Yorktown l'oblige à émettre des ordres écrits de franchissement de signal. C'est une pratique routinière.

L'établissement d'ordre écrit de franchissement suit une procédure dérogatoire, formulée dans les règlements généraux, qui définit scrupuleusement la séquence de contrôles à effectuer et les formulaires à remplir [PSFpc09]. Les règlements généraux stipulent qu'il n'y ait pas plus d'un ordre de franchissement émis par mois [PSFpc09].

Tandis qu'Henry Martin communique l'ordre écrit de franchissement du signal à David Chung, un collègue essaie de lui téléphoner pour l'alerter au sujet de son erreur dans la mesure où le train de fret n'est pas encore arrivé à Yorktown [PSF01], [PSFpc01], PSF05], [PSFpc05], [PSF09], [PSFpc09].

Après avoir reçu l'ordre écrit [PSF01], [PSFpc01], [PSF15], David Chung quitte la station de Yorktown pour se rendre à La Fayette [PSF09], [PSFpc09]. Peu de temps après avoir quitté la station de Yorktown, David Chung accélère et, comme d'habitude, téléphone à sa femme pour l'informer qu'il finit son service bientôt [PSFpc08].

Le collègue réussit enfin à téléphoner à Henry Martin pour l'alerter de son erreur [PSFpc01], [FC03], [FC10].

Via les signaux sur la voie, Henry Martin prescrit à David Chung de ralentir afin de s'arrêter et lance une alerte radio générale. Occupé à téléphoner, David Chung n'entend pas l'alerte radio et ne voit pas les signaux sur la voie limitant la vitesse du train [PSFpc08], [PSFpc09]. Lorsque David Chung voit le train de fret venant en face, il freine mais ne peut éviter la collision frontale avec le train de fret [PSFpc09].

Peu de temps après, Henry Martin apprend la collision entre le train de fret et le train de voyageurs, la mort des deux conducteurs et de cinq passagers.

Figure 7.11. Le scénario de communication au sein et entre des personas collectifs.

Le diagramme de séquence modélise une partie du scénario en exprimant la communication et la coordination entre les personas individuels (cf. Figure 7.12).

Le diagramme illustre le décalage entre, d'un part la relève effectuée entre Laura Fromgarden et Phil Vernes, au départ de Laura Fromgarden, et, d'autre part la relève effectuée entre Phil Vernes et Henry Martin à l'arrivée de ce dernier.

La fragilité de la relève et de la coordination entre Phil Vernes et Henry Martin provient du faible niveau de communication entre les personas individuels et de la culture de la société favorisant les relations hiérarchiques, exprimés comme des contraintes dans le diagramme de séquence SysML (rectangle avec le coin en haut à droit écorné).

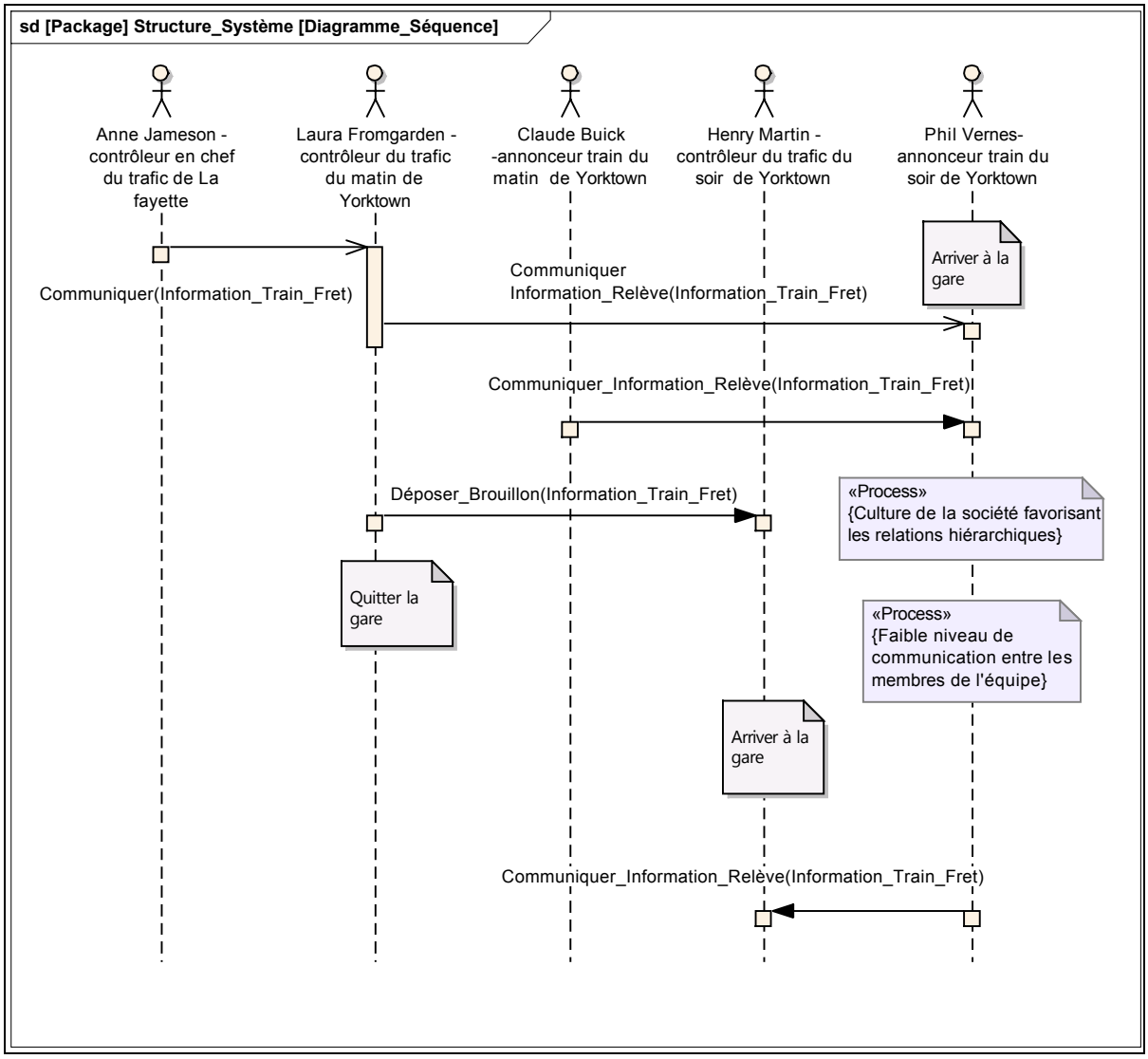

Figure 7.12. Séquence d'action de la communication d'information lors de la relève au sein du persona collectif au sein de la salle de régulation de trafic de Yorktown.

Le diagramme des cas d'utilisation (cf. Figure 7.13) illustre la sécurité de la relève en identifiant les informations qui sont communiquées entre ceux qui effectuent la relève de « départ » et ceux qui effectuent la relève d'« arrivée ». Les informations de la relève doivent leur permettre d'élaborer et d'entretenir une conscience partagée de la situation courante. Nous détaillons les suggestions d'amélioration des IHM dans la section 7.5 « Proposition d'amélioration des IHM ».

Outre la communication de la relève au sein de la gare de Yorktown, la capacité d'élaborer et d'entretenir une conscience partagée de la situation doit être commune à l'équipe de Yorktown et de celle de La Fayette pour les trains circulant entre les deux gares. Là encore, des suggestions d'amélioration des IHM sont effectuées en section 7.5 « Proposition d'amélioration des IHM ».

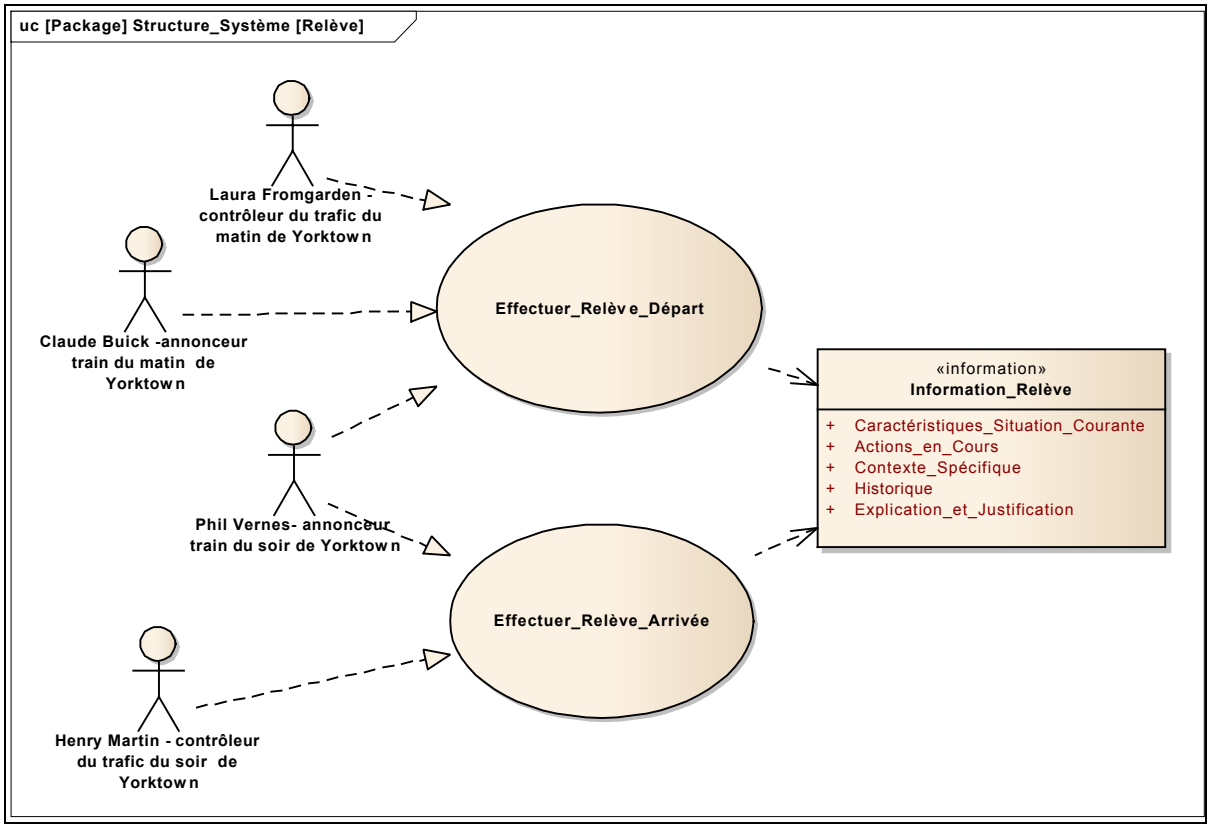

Figure 7.13. Communication d'information lors de la relève au sein de la salle de régulation de trafic de Yorktown.

7.4. Application du patron de conception « surveiller et alerter » pour l'architecture d'un système résilient au scénario de Yorktown

Cette section vise à appliquer le patron de conception « surveiller et alerter » pour la fonction « éviter » (cf. 5.2 « Patron de conception pour la fonction « éviter » de la résilience ») au domaine ferroviaire en s'appuyant sur le scénario Yorktown, issu de la synthèse des rapports d'enquête technique (cf. 7.2 « Synthèse des rapports d'enquête technique d'accidents ferroviaires »).

Cette section présente d'abord le cas de l'émission d'un ordre écrit de franchissement de signal, puis le cas d'une consigne de vitesse du scénario de Yorktown

7.4.1. Cas de l'émission d'un ordre écrit de franchissement de signal du scénario de Yorktown

Nous appliquons le patron de conception « surveiller et alerter » (cf. Tableau 5.2) au scénario de Yorktown (cf. Tableau 7.4). Chaque élément du patron de conception est complété des informations du domaine ferroviaire du scénario présenté en section 7.3 « Application des processus à mettre en œuvre pour contribuer à la résilience d'un système ; du scénario au persona ».

Caractéristiques	Patron « surveiller et alerter »
Nom :	Surveiller l'émission d'ordres écrits de franchissment de signal et alerter les opérateurs des risques encourus.
Objectif :	Surveiller l'émission d'ordres écrits de franchissement de signal et alerter les opérateurs lors d'émission d'ordres écrits, sur les risques encourus.
Problème :	Le manque de fiabilité du dispositif de sécurité de la gare de Yorktown génère un comportement déviant de la part des opérateurs (contrôleur du trafic, annonceur train) et l'inflation d'émissions d'ordres écrits de franchissement de signal.
Solution :	La solution consiste à tracer les émissions d'ordres écrités de franchissement de signal et à alerter les opérateurs des risques encourus lorsqu'un ordre écrit est émis alors qu'un train circule sur la voie.
Modèle :	Le modèle invoqué est celui du processus prescrit d'émission d'ordre écrit de franchissement, y compris les contrôles à effectuer et les formulaires à remplir.
Interfaces :	Ce dispositif est en interface avec le centre de régulation de trafic de La Fayette, ainsi qu'avec les trains circulant entre Yorktown et La Fayette.
Impacts :	Il y a des impacts dans les moyens de recueil des ordres écrits de franchissement de barrières et dans les IHM des opérateurs concernés.
Implémentation :	L'implémentation consiste à réaliser les capteurs mesurant les émissions d'ordres écrits de franchissement de signa, le traitement adapté des valeurs mesurées et à réaliser les interfaces utilisateur adaptées aux opérateurs, les alertant des risques encourus.
Patrons de conception connexes :	Les patrons de conception connexes sont ceux relatifs aux HUMS.
Justification du patron de conception :	Le patron permet de réaliser le système visant à alerter les opérateurs des risques encourus, du niveau de criticité et de l'éminence d'un danger.

Tableau 7.4. Application du patron de conception « surveiller et alerter » au scénario Yorktown.

La Figure 7.14 illustre comment, à partir des informations recueillies du système de régulation de trafic (statut des voies occupées, état du signal fermé, ordre de franchissement de signal formulé), le système de surveillance de l'usage et de l'état génère une alerte. Cette alerte est communiquée aux interfaces utilisateur de régulation de trafic, c'est-à-dire le contrôleur de régulation de Yorktown et celui de La Fayette. Cette communication de l'alerte contribue à la construction d'un cadre commun d'interprétation partagé par tous les opérateurs concernés. Ainsi, ces opérateurs disposent des mêmes informations, en particulier celles relatives au niveau de risque et les conseils formulés.

Cette alerte présente les informations suivantes :

- niveau de risque :
    - sévérité : catastrophique ;
    - probabilité : probable ;
    - criticité : élevé;
- description du système :

    - identifiant : centre de régulation de Yorktown ;
- état évalué :
    - données historiées : liste historiée des ordres écrits de franchissement de signal ;
    - problème diagnostiqué : franchissement de barrières déviant ;
    - dérives constatées : inflation des émissions d'ordres écrits de franchissement ;
    - état courant : émission d'un ordre écrit de franchissement par jour ;
    - état de référence : moins d'un ordre écrit de franchissement émis par mois ;
    - écart entre l'état courant et l'état de référence : à évaluer ;
    - proximité d'une zone de danger ; danger imminent
    - type de danger identifié : risque de collision frontale ;
    - marges de réserves disponibles : positionner les signaux de voie sur « arrêt » effectuer une alerte radio; couper le courant de traction ;
- conseils :
    - actions recommandées : systématiser et tracer les contrôles préalables à l'émission d'un ordre écrit de franchissement, émettre un ordre écrit prescrivant un ordre de marche à vue (vitesse réduite permettant de freiner devant un obstacle) ;
- contexte de l'alerte :
    - date : 02/02/2020 ;
    - heure ; 15h15
    - localisation ; gare de Yorktown
- niveau de confiance de l'alerte :
    - niveau de confiance : élevé.

Cette suggestion est détaillée dans la section 7.5 « Proposition d'amélioration des IHM ».

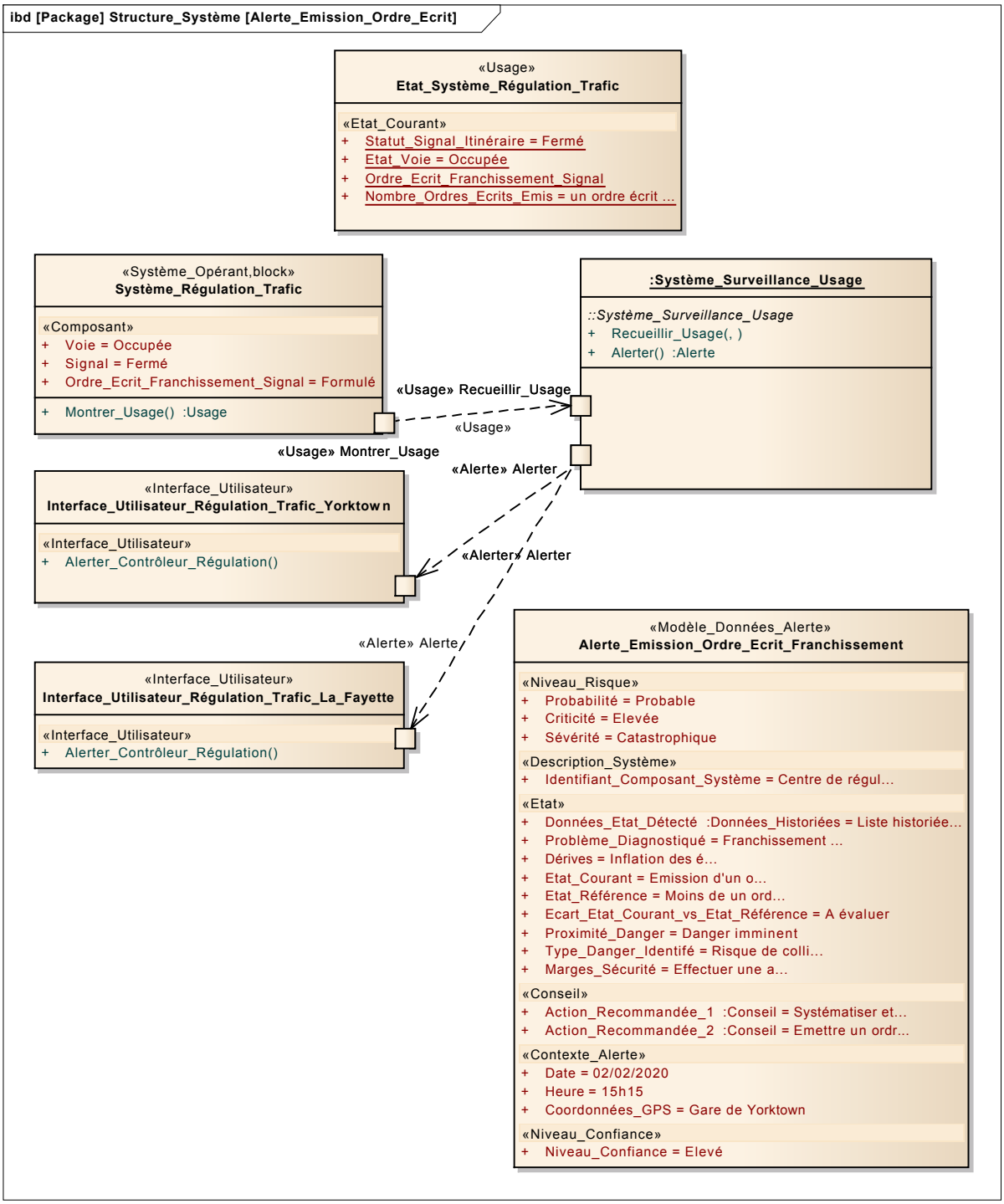

Figure 7.14. Diffusion de l'alerte relative à l'ordre écrit.

Après avoir montré la faisabilité de la solution proposée en l'appliquant à l'émission d'un ordre écrit de franchissement de signal du scénario de Yorktown, nous poursuivons en l'appliquant à la consigne de vitesse du scénario de Yorktown.

7.4.2. Cas de la consigne de vitesse du scénario de Yorktown

Le conducteur de train de voyageurs, David Chung, n'a pas compris la situation exceptionnelle qui amenait le train à devoir ralentir et s'arrêter. En effet, il avait reçu l'ordre écrit de franchissement du signal fermé, comme cela lui était arrivé souvent.

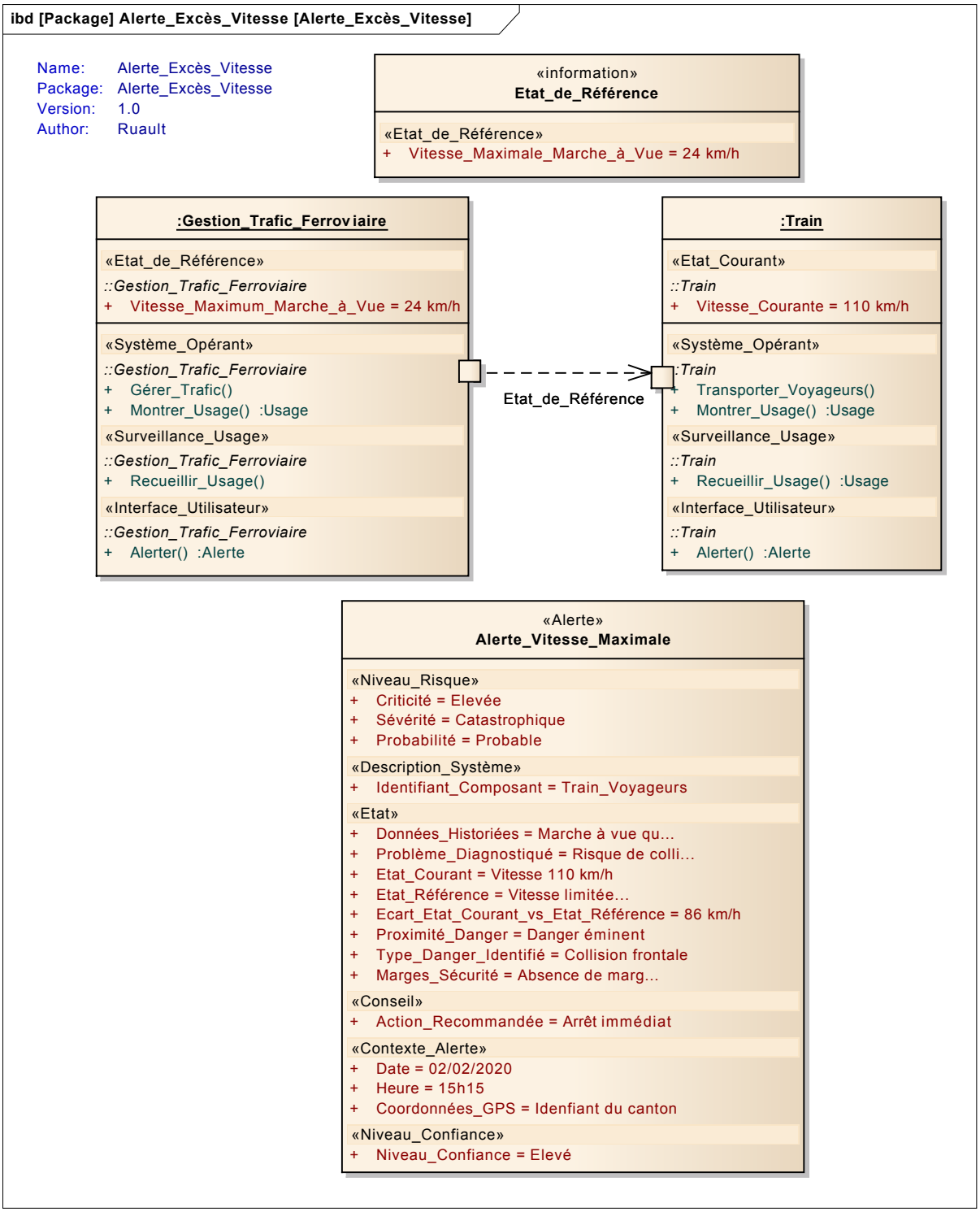

Figure 7.15. Communication de la consigne de vitesse et de l'alerte entre le gestionnaire de trafic et le train.

La proposition consiste en la communication, par le système de gestion de trafic ferroviaire au train, des informations de consigne de vitesse et d'alerte (cf. Figure 7.15). La consigne de vitesse stipule une vitesse de marche à vue maximale de 24 km/h. L'alerte met en exergue le risque de collision frontale dont la criticité est élevée et la sévérité catastrophique et mentionne que l'arrêt immédiat est l'action recommandée.

L'alerte communiquée à David Chung prend en compte le caractère exceptionnel du ralentissement et de l'arrêt. Dans la mesure où cette situation est exceptionnelle, il est nécessaire de mettre le risque en exergue afin qu'il ressorte par rapport aux routines habituelles. La présentation de cette alerte à David Chung doit prendre en compte son activité et les risques courus dûs à l'excès de vitesse. Ces points seront détaillés dans la section 7.5 suivante.

Ainsi après avoir appliqué le scénario, le persona et le patron de conception au domaine ferroviaire, nous identifions les suggestions d'amélioration pour les IHM.

7.5. Proposition d'amélioration des IHM pour les sous-fonctions de la fonction « éviter » de la résilience

Après avoir analysé trois rapports d'enquête technique, les avoir traduits pour identifier des scénarios et des personas, et proposé une architecture contribuant à la résilience du système, nous poursuivons ce chapitre par une proposition d'amélioration des IHM pour les sous-fonctions de la fonction « éviter ».

7.5.1. Obtenir une représentation de l'environnement

Obtenir une représentation de l'environnement est une étape préalable à l'élaboration d'une conscience de la situation, puis de prendre des décisions et mettre en œuvre des actions pour éviter un accident.

Il n'y a pas de communication [PSF13] et représentation partagée de la situation entre les différents acteurs (conducteur de train, contrôleur de la circulation ferroviaire, équipe de chantier) [FC03], [FC10], en conséquence, il n'y a pas de boucle de rétroaction et de régulation de l'activité.

Recommandation

Une solution consiste à donner une représentation partagée de la situation aux différents acteurs, en particulier en zone de danger de telle sorte qu'un risque qui ne serait pas perçu par l'un mais perçu par un autre soit identifié et déclenche les actions adéquates.

Comme suggéré par le patron de conception, l'amélioration des IHM proposée consiste à représenter l'environnement du système aux opérateurs. En l'occurrence, dans le cas de la consigne de vitesse, il est envisageable que l'alerte soit présentée en réalité augmentée sur le pare-brise de la motrice (cf. Figure 7.18) et que la consigne de vitesse se traduise par un dispositif de retour d'effort sur la manette de vitesse.

Dans le cas de l'émission de l'ordre écrit de franchissement de signal de Yorktown, il est envisageable que la zone frontière soit représentée sur une IHM distribuée qui soit partagée par les gares de Yorktown et de La Fayette. Cette IHM partagée leur permet d'élaborer et d'entretenir une conscience partagée de la situation qui leur soit commune concernant les trains circulant entre les deux gares (cf. Figure 7.16). En particulier, cette IHM partagée permet aux opérateurs de voir au-delà de leur zone

de responsabilité pour savoir quels sont les évènements qui vont survenir dans le proche avenir dans cette zone de responsabilité. Elle permet aux deux équipes, l'une passant la main, l'autre prenant la main, de partager les mêmes informations sur le train (référence du train, mission du train, vitesse, etc.), et, *in fine*, d'élaborer une conscience partagée de la situation.

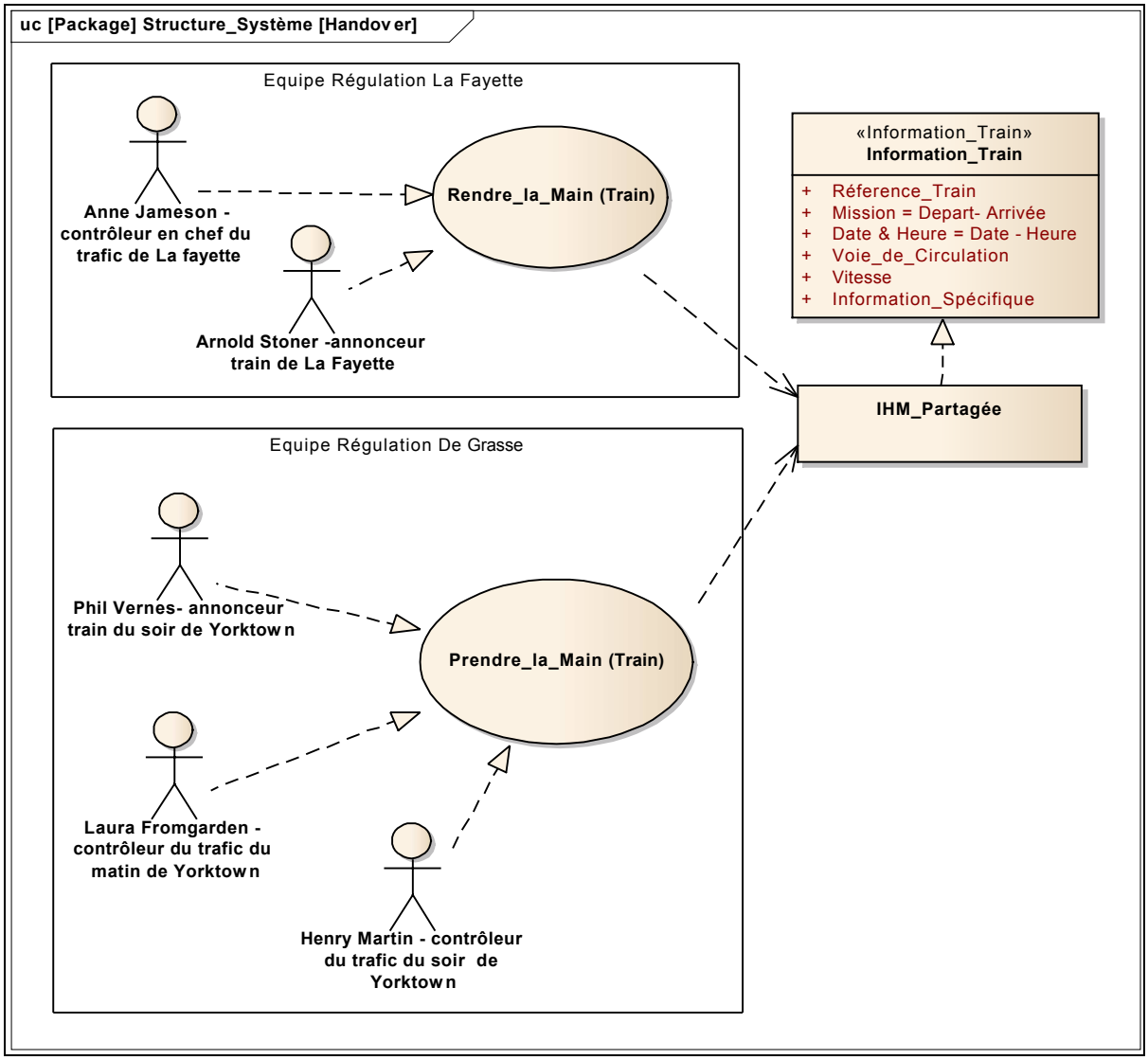

Figure 7.16. IHM partagée entre l'équipe de régulation de Yorktown et l'équipe de régulation de La Fayette.

7.5.2. Obtenir une représentation de la dynamique du système

Obtenir une représentation de la dynamique du système est une autre étape préalable à l'élaboration d'une conscience de la situation, avec les mêmes finalités.

Recommandation

Une solution consiste à montrer le futur état du système en fonction des évènements qui ont eut lieu et des trajectoires que ces évènements ont déclenchées.

Dans le cas de l'accident de l'émission d'un ordre écrit de franchissement de signal, outre la meilleure intégration IHM de la visualisation secondaire au sein de la visualisation principale, il est ensvisageable que la visualisation principale représente non seulement l'état courant de la voie, mais aussi l'état à court terme, sachant qu'un train est en train d'arriver et que la voie sera bientôt occupée.

La Figure 7.17 illustre cette représentation de la dynamique du système système dans un contexte sans lien cette fois avec le ferroviaire. En l'occurrence, il s'agit de l'image du trafic aérien en région parisienne qui montre les aéronefs qui circulent (en jaune sur l'image). Il est possible de visualiser l'identifiant d'un aéronef, en l'occurrence celui qui est indiqué en rouge et dont l'identifiant est inscrit dans une étiquette blanche.

Figure 7.17. Image dynamique du trafic aérien en région parisienne (source : capture d'écran de Flightradar24).

7.5.3. Evaluer la distance, voire la proximité, du système par rapport aux zones de danger

L'évaluation de la proximité du système par rapport aux zones de danger est insuffisante. Les opérateurs prennent conscience trop tardivement du danger, après avoir dépassé le point de non retour.

Dans tous les cas de figure, qu'elle qu'en soit la raison (absence d'intervisibilité …), les opérateurs n'avait pas une conscience du risque et de la proximité du danger.

Recommandation

Une solution consiste à montrer aux opérateurs la proximité du danger, par anticipation.

Elle consiste aussi à avertir les deux conducteurs de trains et l'opérateur du poste de contrôle qu'il y a deux trains sur le même canton et déclencher un freinage d'urgence des trains circulant sur le même canton avant qu'il y ait intervisibilité.

En complément, une autre solution consiste à incruster dans l'IHM du conducteur de train, *via* une technologie de réalité augmentée, une représentation de l'obstacle sur la voie ou le train venant en face, avant qu'il n'y ait intervisibilité (cf. Figure 7.18).

La Figure 7.18 illustre cette solution d'incrustation d'un obstacle dans l'IHM du conducteur de train. Une image de train venant en constresens et un signal de danger sont incrustés sur la vitre de la cabine, en vision tête haute, utilisant la technologie de la réalité augmentée. En complément, le tableau de bord présente les informations de l'alerte.

Une telle inscrutation dans un dispositif tête-haute a été développée pour l'Automatic dependent surveillance-broadcast (ADS-B) dans le domaine aéronautique, ainsi que l'illustre la Figure 7.19 (O'Brien, 2010). Ces principes nous semblent réutilisables dans d'autres domaines, dont celui du ferroviaire.

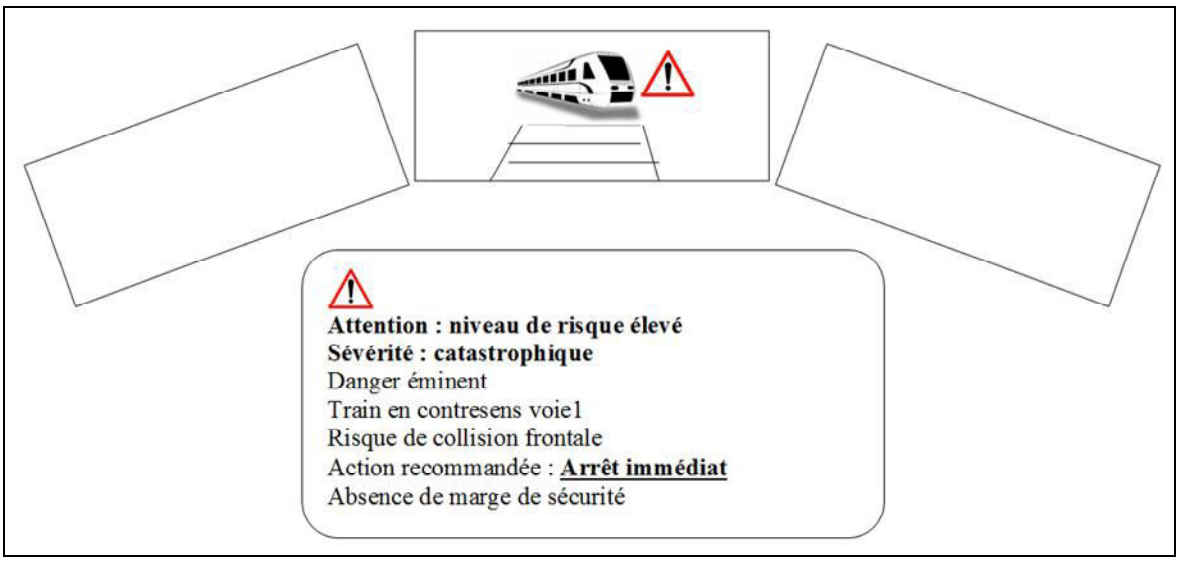

Figure 7.18. Exemple de solution IHM par incrustation d'un obstacle via une technologie de réalité augmentée.

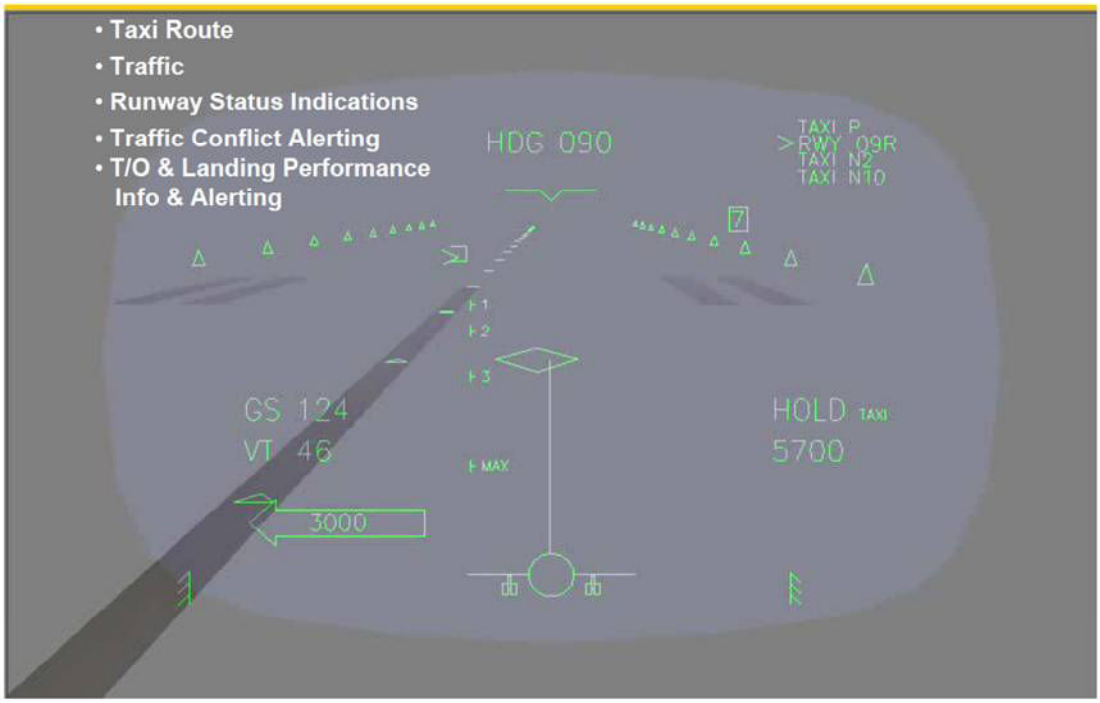

Figure 7.19. Visualisation tête-haute de l'ADS-B (Display of automatic dependent surveillance (ADS-B), Boeing© (O'Brien, 2010)

Les solutions d'amélioration des IHM contribuent à réaliser les sous-fonctions de la fonction « éviter ». À ce titre, ces solutions permettent aux opérateurs de partager un cadre commun d'interprétation de la situation, de la comprendre, de savoir anticiper et de prendre les initiatives appropriées au plus tôt.

7.6. Synthèse et conclusion du chapitre

L'application du scénario, du persona individuel et du persona collectif nous a montré que ces méthodes peuvent être employées, en particulier pour élaborer des modèles utilisateurs dans des conditions où cela est rendu difficile (aspect juridique et éthique de rendre compte des opérateurs impliqués dans un accident) et pour rendre compte des évolutions d'un opérateur dans la durée, dans un environnement qui ne peut pas être évalué en phase d'ingénierie.

L'application du patron de conception « surveiller et alerter » a montré que les informations recueillies à partir d'un système permettent de générer une alerte communiquée aux opérateurs. Cette alerte les aide à comprendre la situation, à élaborer une conscience partagée de la situation pour éviter la survenue d'un accident. Enfin, à partir de l'analyse des accidents, des traductions qui en sont faites en termes de persona, d'architecture, nous avons montré quelles sont les améliorations des IHM que nous pouvons suggérer (et ceci sans souci d'exhaustivité, mais plutôt de représentativité). Ces améliorations des IHM permettent de représenter une alerte contextuelle, adaptée au dispositif d'interface utilisateur, aux tâches des opérateurs, à leurs modèles mentaux. Ces améliorations des IHM permettent aussi à des groupes distants de partager une partie d'une IHM afin de construire un cadre commun d'interprétation. Au-delà de la faisabilité de notre proposition qui vient d'être esquissée en s'appuyant sur trois rapports d'enquête technique dans le domaine ferroviaire, nous identifions plusieurs perspectives de recherche.

Une première perspective consiste à valider expérimentalement, sur simulateur, le patron de conception « surveiller et alerter » en démontrant que des opérateurs mettant en œuvre un système disposant de l'architecture proposée pourront significativement mieux éviter un accident que ceux qui mettent en œuvre un système ne disposant pas d'une telle architecture (cf. Conclusion générale, section « Perspectives de recherche pour la validation du patron de conception « surveiller et alerter » »).

Une seconde perspective de recherche consiste à évaluer la faisabilité d'implémenter cette architecture proposée dans des systèmes existants, lors de rénovation mi-vie, ou en cours de définition, en s'appuyant sur les HUMS existants (cf. Conclusion générale, section « Perspectives de recherche dans le domaine de l'ingénierie et l'architecture système »).

Une troisième perspective de recherche consiste à valider la faisabilité de l'implémentation et de la mise en œuvre d'une architecture IHM distribuée, basée sur ADS-B (*Automatic Dependent Surveillance - Broadcast*), (Ali *et al.*, 2015) et CAMELEON (cf. section 3.4.3 « Architecture pour les IHM distribuées »), communiquant une alerte à plusieurs systèmes indépendants, mais générant des contraintes de sécurité les uns à l'égard des autres, comme c'est le cas aux passages à niveau (cf. Conclusion générale, section « Perspectives de recherche dans le domaine des IHM et de l'ergonomie »).

Enfin, des travaux doivent être menés sur les fonctions « résister », « restaurer » et « adapter » de la résilience afin que les systèmes soient résilients vis-à-vis des situations imprévisibles, sans précédent, auxquelles ils font face (cf. Conclusion générale section « Perspectives de recherche dans le domaine de la résilience des systèmes »).

Conclusion générale

Notre mémoire se clôt avec la conclusion générale qui synthétise l'état de l'art, notre proposition et présente les perspectives de recherche que nous avons identifiées, perspectives pour poursuivre les travaux initiés et répondre aux questions que ces travaux posent quant à la résilience des systèmes critiques à longue durée de vie.

Synthèse sur l'état de l'art

L'état de l'art nous a permis de présenter les concepts structurants du mémoire dans la perspective, d'une part d'élaborer le patron de conception « surveiller et alerter » pour l'architecture d'un système résilient, et, d'autre part de proposer des processus à mettre en œuvre pour contribuer à la résilience d'un système.

Le Chapitre 1 intitulé « De la sûreté de fonctionnement à la résilience» présenta les enjeux opérationnels de la résilience pour les systèmes à longue durée de vie, en particulier les franchissements de barrières et les migrations silencieuses. La sûreté de fonctionnement et de la sécurité préconisent de surveiller l'état du système durant son exploitation opérationnelle. Pour autant, la sécurité ne rend pas compte des situations imprévisibles, sans précédent, que connaît un système durant sa vie opérationnelle. La résilience, en particulier dans sa fonction « éviter », offre cette capacité de conduire à vue, lorsque le système fonctionne hors de son domaine d'emploi et est face à des situations imprévisibles, sans précédent. Pour cela, les opérateurs doivent comprendre la dynamique du système pour le contrôler, prendre à temps des mesures correctives, et engager des actions nécessaires afin de maintenir la sécurité du système. Ils ont besoin de construire une conscience partagée de la situation qui leur permet de comprendre cette dynamique du système.

L'ingénierie système, que nous avons présentée dans le Chapitre 2, est la clef pour concevoir, produire, qualifier, mettre en œuvre, maintenir et démanteler un système dont la vie opérationnelle peut durer plusieurs dizaines d'années. L'organisation de ce système est décrite par l'architecture fonctionnelle et l'architecture physique, lesquelles peuvent être représentées par des diagrammes du langage de modélisation SysML (*System Modelling Language*). Ces diagrammes sont utilisés pour modéliser l'architecture du système de surveillance de l'état et de l'usage et du système interactif pour recueillir les informations relatives à l'état du système.

C'est en ergonomie et en IHM, dans le Chapitre 3, que nous puisons les méthodes et concepts sur lesquels nous nous appuyons pour traduire les informations issues du système de surveillance et d'usage en représentations adaptées aux dispositifs d'interaction qu'utilisent les opérateurs, à leurs modèles mentaux et aux tâches qu'ils ont à effectuer. Ces méthodes et concepts sont ceux de l'ergonomie prospective, du persona, mais aussi de l'architecture des IHM distribuées.

Synthèse de la proposition

Nous avons vu que les enjeux de la résilience consistent à restituer la capacité des opérateurs de naviguer à vue, de contrôler le système qu'ils mettent en œuvre, en particulier dans les situations imprévisibles, sans précédent qu'ils rencontrent. De plus, dans le contexte d'un système critique à longue durée de vie, le contexte opérationnel évolue, les opérateurs

s'approprient le système, le management le met en œuvre pour réaliser des fonctionnalités pour lesquelles il n'avait pas été conçu. Par ailleurs, le système migre silencieusement et est mis en œuvre hors de son domaine de définition. Les opérateurs sont ainsi amenés à faire face à des situations imprévues, imprévisibles, sans précédent, qui n'avaient pas été envisagées lors des phases d'ingénierie du système, pouvant aller jusqu'à perdre le contrôle du système et subir des accidents.

Notre objectif consiste à réintroduire la capacité des opérateurs à contrôler le système. Ils ont besoin de comprendre sa dynamique, l'état dans lequel il est et l'état de l'environnement dans lequel il est mis en œuvre. Cette capacité de contrôler le système permet aux opérateurs de s'autoréguler, de mettre en œuvre une démarche d'essai-erreur et, *in fine*, éviter qu'un accident ne survienne. Pour cela, il est nécessaire d'obtenir en temps réel des informations sur la dynamique du système et de présenter ces informations aux opérateurs de façon appropriée à leur tâche.

Nous avons créé et proposé le patron de conception « surveiller et alerter » que nous avons appliqué à la fonction « éviter » de la résilience, pour donner aux opérateurs la capacité de comprendre la dynamique du système, de le conduire à vue face à des situations imprévisibles, sans précédent afin d'éviter la survenue d'un accident. Nous proposons aussi de faire évoluer les processus d'ingénierie et de conception centrée utilisateur pour qu'ils contribuent à la résilience d'un système critique à longue durée de vie.

L'objectif est de surveiller l'état et l'usage du système opérant et d'alerter les opérateurs quand le système opérant s'éloigne de son domaine d'emploi et est à proximité d'une zone de danger. À cette fin, le patron de conception « surveiller et alerter » reprend et adapte les travaux sur le HUMS (*Health and Usage Monitoring System*) et ceux sur les IHM.

Ce patron de conception permet d'allouer les sous-fonctions de la fonction « éviter » de la résilience aux composants, d'une part du système de surveillance de l'usage et de l'état du système et, d'autre part du système interactif. Ce patron de conception propose un modèle de données de l'alerte. Cela ouvre la voie à la communication d'une alerte entre systèmes dans une perspective de communication distribuée. Cette alerte est traduite par le système interactif afin de présenter cette information aux opérateurs de façon appropriée et adaptée à leurs modèles mentaux, à leurs tâches et aux dispositifs d'interaction qu'ils utilisent. Cette alerte permet aux opérateurs de partager un même cadre d'interprétation pour élaborer et entretenir une conscience partagé de la situation, de restaurer leur capacité de contrôler un système et de naviguer à vue.

Nous avons fait évoluer le processus d'appropriation pour y intégrer l'ergonomie prospective. Nous avons proposé de formaliser le processus de retour d'expérience afin de faire évoluer les documents de bonnes pratiques (normes) pour que ces documents le prennent en compte dans leur prochaine édition.

Nous avons fait évoluer, aussi, le persona pour l'adapter aux systèmes critiques à longue durée de vie.

Nous nous inscrivons dans une démarche de conception itérative adaptée aux systèmes critiques à longue durée de vie. La seconde contribution (cf. Chapitre 6 « Proposition de processus à mettre en œuvre pour contribuer à la résilience d'un système critique à longue durée de vie ») met en évidence les évolutions des processus d'ingénierie système. Il s'agit de prendre en compte la conception du système de surveillance d'usage et du système interactif, ainsi que le processus de retour d'expérience. Par ailleurs, cette proposition montre aussi les impacts de la prise en compte de l'ergonomie prospective et du processus d'appropriation. La

conception *pour* l'appropriation vise à offrir aux opérateurs un ensemble de possibilités pour adapter et ajuster le système à leur besoin, en fonction des évolutions du contexte opérationnel. La conception *par* l'appropriation consiste à recueillir les données issues de l'appropriation afin de les injecter dans la conception afin qu'elle prenne en compte l'usage réel lors des rénovations à mi-vie. Denier point de notre contribution, le persona, représentation fictive d'un utilisateur ou d'une classe d'utilisateurs, permet de rendre compte des futurs utilisateurs qui ne peuvent pas être sollicités en phase amont des projets, ou des évolutions des caractéristiques des utilisateurs au fil du temps. Le persona collectif permet de rendre compte de la dynamique de personas individuels au sein d'un collectif, par exemple l'intégration au sein de communautés, la confiance au sein du collectif, le respect ou le non respect des règles.

Les propositions, d'une part, de patron de conception « surveiller et alerter » pour l'architecture d'un système résilient et, d'autre part le persona, sont appliquées à trois études de cas dans le domaine ferroviaire. Ces études de cas correspondent à trois accidents qui ont donné lieu à des rapports d'enquête technique. L'objectif de cette application est de démontrer la faisabilité de notre proposition sur des systèmes réels du domaine ferroviaire (train, système de régulation de trafic …).

L'application du scénario, du persona individuel et du persona collectif a montré que ces méthodes peuvent être employées, en particulier pour élaborer des modèles utilisateurs dans des conditions où cela est rendu difficile et pour rendre compte des évolutions d'un opérateur dans la durée, dans un environnement qui ne peut pas être évalué en ingénierie.

L'application du patron de conception « surveiller et alerter » a montré que les informations recueillies à partir d'un système permettent de générer une alerte communiquée aux opérateurs. Cette alerte les aide à comprendre la situation, à élaborer une conscience partagée de la situation pour éviter la survenue d'un accident.

Enfin, à partir de l'analyse des accidents, des traductions qui en sont faites en termes de persona, d'architecture, nous avons montré quelles sont les améliorations des IHM, que nous pouvons suggérer, basées sur les préconisations du patron de conception et adaptées à la fonction « éviter » de la résilience.

Au-delà de notre proposition et de sa faisabilité, nous identifions plusieurs perspectives de recherche que nous présentons maintenant.

Perspectives de recherche

La recherche menée dans le cadre de mémoire a soulevé un ensemble de questions qui n'ont pas pu être traitées dans ce cadre et qui constituent autant de perspectives de recherche.

Nous reprenons les points identifiés dans les chapitres 4, 5, 6 et 7 du mémoire, points que nous développons dans les groupes consacrés aux sujets suivants :

- la validation du patron de conception « surveiller et alerter » pour l'architecture d'un système résilient ;
- le domaine de l'ingénierie et l'architecture système ;
- le domaine des IHM et de l'ergonomie ;
- le domaine de la résilience et de la sécurité.

Perspectives de recherche pour la validation du patron de conception « surveiller et alerter »

L'évaluation de faisabilité du patron de conception « surveiller et alerter » est une première étape pour vérifier expérimentalement sa pertinence et sa capacité d'éviter des accidents.

La **validation expérimentale du patron de conception « surveiller et alerter »** devra faire l'objet de futures recherches. Les travaux initiaux consistent à instrumenter un simulateur en intégrant un système de surveillance de l'usage et de l'état du système mis en œuvre par des opérateurs. Cette instrumentation permettra aux opérateurs d'élaborer et d'entretenir une représentation fonctionnelle dynamique de la situation.

Des scénarios d'accidents seront rejoués sur ce simulateur, avec une condition témoin (simulateur non instrumenté) et une condition expérimentale (simulateur instrumenté mettant en œuvre la solution d'architecture proposée). Nous faisons l'hypothèse qu'en condition expérimentale, les opérateurs pourront significativement mieux éviter les accidents que les opérateurs mettant en œuvre un système basé sur l'architecture témoin.

Le simulateur pourra être complété avec des architectures alternatives pour évaluer, parmi les architectures candidates, celles qui présentent les meilleures performances et augmentent significativement les probabilités d'éviter un accident.

La validation expérimentale sur simulateur est une première étape. Elle devra être complétée par une simulation avec matériel dans la boucle comprenant, d'une part un système réel avec son dispositif de surveillance de son état et de son usage et des IHM adaptées, d'autre part un simulateur pour générer l'environnement dangereux. En effet, il est exclu de mener une expérimentation dans un environnement dangereux réel pour valider le patron de conception.

Enfin, des expérimentations pourront être menées sur simulateur dans d'autres domaines d'application, le transport maritime par exemple, pour valider la généricité de l'architecture proposée. Nous faisons l'hypothèse que le patron de conception « surveiller et alerter » peut être appliqué utilement dans d'autres domaines et que sa mise en œuvre permet aux opérateurs d'éviter des accidents.

Perspectives de recherche dans le domaine de l'ingénierie et l'architecture système

La proposition et son application ont mis en évidence des impacts dans le domaine de l'ingénierie et de l'architecture système, impacts à évaluer.

L'**évolution des démarches agiles pour prendre en compte l'ergonomie prospective ainsi que le processus d'appropriation** est une perspective de recherche pour les prochaines années. L'objectif est de poursuivre les travaux actuels (Pew & Mavor, 2007) et d'étendre les concepts et méthodes des démarches agiles sur l'ensemble du cycle de vie d'un système adaptant ces concepts pour prendre en compte l'ergonomie prospective et le processus d'appropriation.

L'**intégration de l'architecture ouverte, malléable, ajustable, appropriée au processus d'appropriation, affecte l'architecture globale du système.** Il s'agit d'évaluer les impacts de cette intégration, en particulier lorsque la définition de l'architecture est l'objet de certification, ainsi que c'est le cas dans le domaine aéronautique. L'étude d'intégration pourra s'appuyer sur ce qui a déjà été fait dans le cadre des HUMS et profiter de leurs ressources pour limiter les impacts sur les systèmes opérants.

La **communication des alertes entre plusieurs systèmes** est aussi à explorer. Cette communication a des impacts sur l'architecture de chacun des systèmes concernés, en particulier au niveau de leurs interfaces externes. Cette exploration peut s'appuyer sur les travaux actuels concernant l'ADS-B[31]. Cette exploration devra prendre en compte la sécurité de la communication, au sens de la sécurité des systèmes d'information (ANSSI, 2012 ; ISO 2013) et être adaptée au domaine de la résilience des systèmes. Cette exploration visera, d'une part à évaluer la faisabilité d'un tel dispositif, et d'autre part à mesurer la capacité de ce dispositif d'offrir aux opérateurs une représentation de la dynamique des systèmes de l'environnement afin de prendre en compte les aléas qui affectent ces systèmes. Cette exploration visera, aussi, à évaluer les impacts de l'intégration de la sécurité des systèmes d'information dans l'architecture globale du système, ainsi que sur le patron de conception « surveiller et alerter ». Enfin, il est nécessaire de prendre en compte que les systèmes ne disposent pas tous des mêmes fonctionnalités à un moment donné. L'hétérogénéité des systèmes et leurs évolutions non synchrones ont pour conséquence que certaines fonctions, dont celle de surveiller et d'alerter, ne sont pas couvertes ou ne le sont qu'en partie. Dans ce contexte, les opérateurs doivent être avertis des capacités des différents systèmes d'émettre et de recevoir des alertes. En effet, il est nécessaire de différencier un système qui n'émet pas d'alerte parce qu'il est en position sûre et un système qui n'émet pas d'alerte parce qu'il ne dispose pas des capacités d'en émettre, mais qui est dans une zone de danger. Nous pouvons prendre le cas des passages à niveau, principale cause d'accidents dans le domaine ferroviaire, pour avertir les trains qu'il y a des véhicules sur la voie et alerter le conducteur du train pour qu'il puisse freiner. Cela peut être, par exemple, un bus scolaire bloqué sur un passage à niveau diffusant un message d'alerte pour avertir du danger les trains circulant sur les voies afin que les conducteurs freinent à temps.

Perspectives de recherche dans le domaine des IHM et de l'ergonomie

La **validation de notre proposition relative au processus d'appropriation, à l'ergonomie prospective et au persona** est plus complexe à mettre en œuvre.

En effet, tant le processus d'appropriation que l'ergonomie prospective s'inscrivent dans la durée, dans le temps long, et nécessitent une démarche longitudinale. Il s'agit de suivre comment les opérateurs s'approprient un système, comment ils peuvent l'adapter pour accroître ses performances, l'utiliser à des usages qui n'avaient pas été pris en compte en phase d'ingénierie (l'ensemble des cas exceptionnels qui sont connus par l'expérience mais non tracés dans la mémoire collective), le mettre en œuvre dans des environnements qui n'avaient pas été envisagés, voire le détourner pour de nouveaux usages. Les études longitudinales, comprenant des analyses de l'activité, des analyses des traces et des entretiens, permettent d'identifier les informations dont les opérateurs ont besoin pour comprendre la dynamique du système et comment ils élaborent leur propre stratégie pour comprendre cette dynamique.

Dans la même perspective, les impacts dans le domaine de l'ergonomie et des IHM doivent être évalués dans de futures recherches.

Les **critères de fiabilité et de pertinence de la représentation fonctionnelle** pourront faire l'objet de recherches en IHM et en ergonomie. S'appuyant sur les recherches menées sur les

[31] Le système ADS-B (*automatic dependant surveillance-broadcast*) permet à des aéronefs de diffuser aux autres aéronefs et des systèmes au sol qui disposent de l'ADS-B des informations, telle que leur identifiant, leur vitesse, leur altitude, etc.

modèles mentaux, sur les images opératives, la conscience partagée de la situation (Chalandon, 2013), la compréhension dans la communication (Karsenty, 2008), ainsi que sur la théorie de la pertinente[32] (Sperber & Wilson, 1989), les travaux viseront à déterminer des critères de fiabilité et de pertinence de la représentation fonctionnelle et à élaborer une grille d'évaluation de ces critères. Ces critères seront validés avec les opérateurs du domaine d'application, avec une démarche de simulation et d'expérimentation. Le retour d'expérience des situations réellement rencontrées en environnement opérationnel les enrichira. Ces recherches prendront en compte les effets des heuritiques et des biais sur l'élaboration de la représentation fonctionnelle et sur le processus de prise de décision (Tversky & Kahneman, 1974).

Les **évolutions du répertoire de réponses des opérateurs, d'un répertoire de réponses routinières à un répertoire de réponses de type résolution de problème** ont des impacts sur l'IHM. Ces impacts pourront faire l'objet de recherches visant à déterminer les différents types de répertoires de réponses des opérateurs, leurs contraintes propres (information locale / information globale, temps de traitement, besoin de rompre des effets d'heuristiques et de biais) et à concevoir des IHM adaptées à ces differents types de réponses des opérateurs

Les **modalités d'élaboration et d'entretien d'une conscience partagée de la situation dans le contexte de situations imprévisibles et sans précédent** sont également à creuser dans les prochaines années. Une telle recherche s'appuiera sur les données et les résultats d'études menées, par exemple les résultats de REACT[33], ainsi que sur les travaux sur la construction du sens (*sensemaking*). En effet, outre les informations de type alerte que présentent les systèmes interactifs aux opérateurs, il est nécessaire que ces derniers échangent entre eux, au-delà d'une simple communication implicite, pour élaborer explicitement un cadre commun d'interprétation. Les travaux viseront à déterminer l'influence des moyens de communication disponibles, des IHM, de l'expérience menée en commun, de l'apprentissage collectif, sur la capacité d'élaborer un cadre d'interprétation commun d'une situation imprévisible, sans précédent.

La **définition et l'implémentation des traitements de la chaîne de transformation, entre le message d'alerte et l'interface utilisateur** font aussi l'objet de perspectives de recherche à mener. En effet, cette chaîne de transformation doit conserver la sémantique de l'alerte (cricité, proximité d'une zone de danger …) tout en adaptant ces informations au dispositif d'interaction qu'utilise l'opérateur, à son modèle mental, à sa tâche et au contexte de sa tâche. En particulier, dans le cas où une alerte est communiquée entre différents systèmes, il est nécessaire que les chaînes de transformation de ces différents systèmes ne génèrent pas des représentations incohérentes qui empêcheraient les opérateurs d'élaborer un cadre commun d'interprétation, voire, au pire, produiraient des ambiguités et des confusions pour les opérateurs. La validation de cette chaîne de traitement sera basée sur des expérimentations menées sur simulateur. La fidélité de la chaîne de traitement sera évaluée en fonction de sa capacité à donner aux opérateurs un cadre commun d'interprétation de la situation.

La **définition et l'implémentation d'une architecture IHM distribuée, basée sur CAMELEON, communiquant une alerte à plusieurs systèmes indépendants** peuvent faire

[32] La théorie de la pertinence concerne le principe d'économie dans le langage, visant à ne dire que ce qui est pertinent. Le but central de la communication humaine est de reconnaître, grâce à un effort coopératif, l'intention communicative de l'interlocuteur.

[33] Projet de recherche DGA (contrat de recherche n° 2009.34.0035) sur le thème de la réaction d'un collectif de travail face à l'imprévu (groupement Université de Valenciennes/LAMIH, Université Technologique de Troyes/TECH-CICO et Dédale).

aussi l'objet de nombreux travaux à venir. Une telle architecture IHM distribuée est pertinente dans le contexte où plusieurs systèmes sont indépendants mais génèrent des contraintes de sécurité les uns à l'égard des autres. Ces recherches peuvent s'appuyer sur les travaux consacrés aux ADS-B (cf. Conclusion générale section « Perspectives de recherche dans le domaine de l'ingénierie et l'architecture système »), en particulier ceux consacrés aux IHM (Bailey *et al.*, 2008), dont sur la composition des IHM (Calvary *et al.*, 2013).

Les travaux sur le **persona individue**l et sur le **persona collectif** sont à poursuivre. Ils'agira d'évaluer la pertinence du persona pour transférer une problématique d'un domaine à un autre, par exemple la pertinence du transfert de la VACMA (veille automatique à contrôle de maintien d'appui) du domaine ferroviaire au domaine de la conduite automobile. Il s'agira aussi d'évaluer la mise en œuvre de la démarche avec des acteurs professionnels et des opérateurs pour jouer des scénarios opérationnels sur simulateur ou en expérimentation. L'objectif sera alors de pouvoir approximer le comportement d'un opérateur futur vis-à-vis d'une situation opérationnelle envisageable.

Enfin, au même titre que le dispositif de surveillance de l'état et de l'usage du système permet de connaître l'état du système et de son environnement opérationnel, la **compréhension de l'état des opérateurs** tels que l'état de fatigue, le rythme circadien, l'inattention, etc. (Causse *et al.*, 2013 ; Dehais *et al.*, 2014 ; Dehais *et al.*, 2015) permet de connaître les risques potentiels et d'alerter les opérateurs en cas de besoin. L'état des opérateurs et celui du système technique sont à intégrer pour élaborer l'état du système sociotechnique. Cela permet de comprendre les interactions que ces états établissent entre eux et comment ces interactions contribuent à la prise de risque.

Perspectives de recherche dans le domaine de la résilience des systèmes

Enfin, la première étape, consacrée à la fonction « éviter » de la résilience, doit être poursuivie pour les trois autres fonctions de la résilience et complétée pour effectuer le retour d'expérience du non-respect des procédures ayant des conséquences positives et sur la détermination des informations d'alerte à communiquer aux opérateurs.

Les **trois autres fonctions de la résilience** pourront faire l'objet de recherches visant à compléter nos travaux et fournir une architecture globale pour la résilience des systèmes.

Pour ce qui relève des **traitements effectués par le système de surveillance de l'usage et de l'état du système opérant**, il s'agira d'articuler notre proposition d'architecture aux travaux menés pour la surveillance des systèmes critiques (Aubry *et al.*, 2012 ; Barros *et al.*, 2012 ; Fallet-Fidry *et al.*, 2012 ; Hartert *et al.*, 2012 ; He *et al.*, 2012 ; Sedki et al., 2012), et de caractériser, différencier et tracer les adaptations sans détournement fonctionnel et les adaptations comprenant un détournement fonctionnel. Dans ce second cas, la surveillance devient plus difficile et plus complexe à mettre en œuvre. En effet, il s'agit d'identifier les nouveaux usages du système et les nouveaux contextes d'usage. Cela conduit à reviser la définition du système et son domaine d'emploi.

Analyser, caractériser, tracer et capitaliser le **non respect procédures ayant des conséquences positives** nécessitent des travaux complémentaires. Il sera nécessaire d'effectuer un retour d'expérience sur les « non accidents » hors du périmètre de sécurité pour les mettre en perspective par rapport aux situations de non respect des procédures qui génèrent des accidents. Ces dernières sont les seules à être tracées actuellement. Ce non respect des procédures ayant des conséquences positives peut être lié à des évolutions de

l'environnement opérationnel ou des contraintes nouvelles qui ne permettent pas d'appliquer les procédures de façon sûre et performante.

La **détermination des informations d'alerte dont les opérateurs ont besoin** est une autre perspective de recherche. Le modèle de criticité tel que formulé dans les documents de référence (MIL-STD, 2012) présente des limites intrinsèques. En effet, lorsque la sévérité des conséquences d'un événement redouté est très élevée et que sa probabilité d'occurrence est très faible, la criticité, qui est le produit mathématique de la sévérité et de la probabilité, est indéterminée. Le modèle de criticité doit être évalué en fonction de sa pertinence (Sperber & Wilson, 1989) pour les opérateurs et de la confiance qu'ils peuvent lui accorder. Pour le moins, il doit être complété pour que l'alerte soit pertinente. Dans la masse de données collectées, il est nécessaire d'identifier les signaux faibles, les tendances imperceptibles, de les différencier du bruit de fond et d'en évaluer la pertinence pour ne présenter aux opérateurs que les informations dont ils ont besoin. Enfin, en complément des informations recueillies par le dispositif de surveillance et d'alerte, le retour d'expérience est la clef de voûte pour déterminer les informations d'alerte. Pour un domaine d'application donné, en fonction des situations déjà rencontrées, des contraintes opérationnelles, des activités des opérateurs, il s'agira de déterminer les informations d'alerte dont les opérateurs ont besoin pour élaborer et entretenir une représentation partagée de la situation. Au-delà d'un poste opérateur ou d'un équipage, il s'agira d'identifier les autres systèmes en interface avec lesquels communiquer les informations d'alerte pour que l'ensemble des opérateurs concernés ait un cadre d'interprétation commun de la situation.

Au-delà des travaux sur la résilience des systèmes sociotechniques complexes, il s'avère nécessaire de chercher à comprendre comment des organisations ayant déployé une démarche, des méthodes et des outils en faveur de la sécurité des systèmes qu'elles réalisent et mettent en œuvre, développent une **complaisance qui les affranchit des règles qu'elles s'infligent**, complaisance qui contribue aux migrations silencieuses. Rasmussen (1997) et Amalberti (2009) montrent que la concurrence entre, d'une part la performance opérationnelle et la recherche de réduction des coûts et, d'autre part la sécurité, génère des migrations silencieuses. Vanderhaegen et ses collègues (Vanderhaegen, 2003 ; Vanderhaegen *et al.*, 2011 ; Polet *et al.*, 2002 ; Polet *et al.*, 2009) montrent les mécanismes à l'origine du contournement des barrières. Vanderhaegen (2012, 2014) montre aussi que les dissonances pertubent les opérateurs et génèrent des accidents. L'automatisation des activités routinières ainsi que l'accumulation permanente des routines de travail réduisent la vigilance et contribuent à négliger les informations marginales (March & Simon, 1958). Vaughan (1996), quant à elle, décrit la normalisation de la déviance. Enfin, se focalisant sur les tâches prescrites à affectuer, les travaux d'ingénierie ne prennent pas suffisamment en compte les activités réelles des opérateurs, les adaptations qu'ils font des tâches en fonction des aléas, des situations opérationnelles, des contraintes de performance (Leplat & Hoc, 1983 ; Leplat, 2002 ; Boy, 2013). Dans le cas de l'accident qui a eu lieu à Zoufftgen, nous avons pu constater une normalisation de la déviance alors même qu'une politique de sécurité avait été déployée. Aux confins des sciences de l'ingénieur et des sciences humaines et sociales, il s'agira d'identifier et de caractériser les comportements individuels (comportements pervers, injonctions paradoxales …), collectifs (conformité au groupe, régulations sociales …) et organisationnels (culture d'organisation consistant à cacher les problèmes et ne montrer que les succès …) qui sont les moteurs de cette **complaisance** et des migrations silencieuses. Dès lors, la transgression des règles pose la question de la sécurité des systèmes critiques à longue durée de vie.

Autres actions à mener

Outre les perspectives de recherche, nous avons identifié des actions à mener, principalement dans le domaine de la normalisation, actions que nous détaillons maintenant.

L'**intégration de l'ergonomie prospective, du processus d'appropriation, entre autres, au sein des processus et activités de l'ingénierie système** se traduit par un ensemble d'actions, en particulier visant à compléter les documents de référence (ISO, 2014) lors des futures mises à jour. En particulier, il s'agit de prendre en compte le processus de retour d'expérience et le processus d'appropriation dans les documents de référence (ISO, 2010b ; ISO, 2014).

Dès lors que plusieurs systèmes différents doivent échanger des alertes, il est nécessaire que ces alertes échangées aient la même signification pour ces différents systèmes. L'activité de **normalisation des alertes** devrait consister à rédiger des **normes relatives au format des alertes, à la signification des informations de ces alertes, mais aussi au protocole d'échange**. Par ailleurs, ces normes devraient prendre en compte les contraintes de la **sécurité des systèmes d'information**, afin que ces alertes ne soient pas altérées, corrompues ou compromises.

Bibliographie

[AAE, 2013] Académie de l'Air et de l'Espace (2013). Le traitement de situations imprévues en vol ; une amélioration de la sécurité aérienne. Dossier n°37.

[Abed *et al.*, 2001] Abed M., Ezzedine H., & Kolski C. (2001). Modélisation des tâches dans la conception et l'évaluation des systèmes interactifs : la méthode SADT/Petri. In Kolski C. (Ed.), Analyse et Conception de l'IHM. Interaction Homme-machine pour les SI, Vol. 1, Hermès, Paris, pp. 145-174.

[Abichou, 2013] Abichou B. (2013). Contribution à la formalisation de bilans / états de santé multi-niveaux d'un système pour aider à la prise de décision en maintenance : intégration d'indicateurs par l'intégrale de Choquet. Engineering Sciences ; Université de Lorraine ; 2013 ; thèse n°tel-00839731.

[AFIS, 2008] AFIS (2008). Site Internet de l'AFIS ; http://www.afis.fr.

[AFIS, 2009] AFIS (2009). Fiche Processus – Activité – Tâche ; élaborée par le GT SdS.

[AFNOR, 2003] AFNOR (2003). NF Z 67-288 ; 2003, Processus de cycle de vie des systèmes.

[Ahmed *et al.*, 2013] Ahmed Z., Helfrich-Förster C., & Dandekar T. (2013). Integrating Formal UML Designs and HCI Patterns with Spiral SDLC in DroLIGHT Implementation. Recent Patents on Computer Science, vol. 6, n° 2, pp. 85-98.

[Alexander, 1977] Alexander C., Ishikawa S., & Silverstein M. (1977). A Pattern Language: Towns, Buildings, Construction. Oxford University Press, New-York.

[Ali *et al.*, 2015] Ali B-S., Ochieng WO., Schuster W., Majumdar A., Chiew T-K. (2015). A safety assessment framework for the Automatic Dependent Surveillance Broadcast (ADS-B) system. Safety Science, vol. 78, October 2015, pp. 91–100.

[Amalberti, 1996] Amalberti R. (1996). La conduite des systèmes à risques. PUF, Paris.

[Amalberti, 2002] Amalberti R. (2002). Approche ergonomique des erreurs et des risques. In Gilbert, C. (Ed.), Risques collectifs et situations de crise: Apports de la recherche en sciences humaines et sociales, pp. 187-198.

[Amalberti, 2006] Amalberti R. (2006). Violations et migrations ordinaires dans les activités à risques : conséquences pour la résilience globale

et la gestion du retour d'expérience en entreprise. Actes de la conférence Ergo'IA 2006, Biarritz.

[Amalberti, 2009] Amalberti R. (2009). Violations et migrations ordinaires dans les interactions avec les systèmes automatisés. Journal Européen des Systèmes Automatisés, vol 43, n° 6, pp. 647-660.

[Annett & Duncan, 1967] Annett J., & Duncan K. (1967). Task Analysis and Training Design. Occupational Psychology, n°41, pp. 211-227.

[ANSSI, 2012] ANSSI (2012). Cas pratique. La cybersécurité des systèmes industriels.

[Atlas Ergonomics, 2007] Atlas Ergonomics (2007). Addressing the Challenge of Obesity and Ergonomics in the Office Environment. An Atlas Ergonomics White Paper, site visité le 13 décembre 2014, http://atlas-ips.com/media/1079/callcenterobesity020907.pdf.

[ASD-STAN, 2013] ASD-STAN (2013). prEN 9277, Guide pour le management de l'ingénierie Système.

[Aubry *et al.*, 2012] Aubry J-F., Babykina G., Brinzei N., Medjaher S., Barros A., Berenguer C. Grall A. Langeron Y., Ngoc Nguyen D., Deleuze G., De Saporta B., Dufour F., & Zhang H. (2012). Projet APPRODYN : approches de la fiabilité dynamique pour modéliser des systèmes critiques. In Matta N., Vandenboomgaerde Y. & Arlat J. (Eds.), Supervision, surveillance et sûreté de fonctionnement des grands systèmes, Hermès, Paris, pp. 181-222.

[Bachatène *et al.*, 2008] Bachatène H., Garnier J.-L., & Ruault J.-R. (2008). Adaptability of software intensive systems, facing new threats and opponents new tactics. Symposium OTAN Agility, Resilience and Control in Network Enabled Capabilities (NEC), RTA-SCI-187, Amsterdam.

[Bailey *et al.*, 2008] Bailey L., Wilson J., baley G., Zimmerman K., Armstrong R. (2008). Display of Automatic dependent surveillance (ADS-B) information on head-up diplay. United States Patent, n° US 7,342,514 B1.

[Balme *et al.*, 2004] Balme L., Demeure A., Barralon N., Coutaz J., & Calvary G. (2004). Cameleon-rt: A software architecture reference model for distributed, migratable, and plastic user interfaces. In Markopoulos P., Eggen B., Aarts E & Crowley J-L. (Eds.), Ambient intelligence, Springer, Berlin Heidelberg, pp. 291-302.

[Baron *et al.*, 2006] Baron M., Lucquiaud V., Autard D., & Scapin D. (2006). K-MADe : un environnement pour le noyau du modèle de description de l'activité, 18ème Conférence Francophone sur l'Interaction Homme-Machine (IHM'2006), ACM Press, Montréal, pp. 287-288.

[Barros *et al.*, 2012] Barros A., Levrat E., Fouladirad, M., Le Son K., Ruin T., Iung B., Voisin A. Monnin M., Despujols A., Rémy E., & Bénétrix L. (2012). Modélisation de la dégradation et du pronostic. In Matta N., Vandenboomgaerde Y. & Arlat J. (Eds.), Supervision, surveillance et sûreté de fonctionnement des grands systèmes, Hermès, Paris, pp. 95-114.

[Barthet, 1988] Barthet M-F. (1988). Logiciels interactifs et ergonomie, modèles et méthodes de conception. Dunod, Paris, 219 p.

[Bass *et al.*, 1991] Bass L., Little R., Pellegrino R., & Reed S. (1991). The Arch Model: Seeheim revisited. Proceedings of User Interface Developpers'Workshop, Seeheim 1991.

[Bastien & Scapin, 1993] Bastien J.M.C., & Scapin D.L. (1993). Critères ergonomiques pour l'évaluation d'interfaces utilisateurs. Rapport technique INRIA n° 156, INRIA, Le Chesnay.

[BEA-TT, 2009] BEA (Bureau d'enquêtes sur les Accidents de transport terrestre et Administration des enquêtes techniques) (2009). Rapport d'enquête technique sur la collision ferroviaire survenue le 11 octobre 2006 à la frontière franco-luxembourgeoise à Zoufftgen (Moselle).

[Belmonte *et al.*, 2008] Belmonte F., Boulanger J.-L., & Schön W. (2008). Utilisation d'un modèle d'accident systémique comme référentiel commun à une analyse de risque interdisciplinaire. Conférence Internationale Francophone d'Automatique, Bucarest, 2008.

[Bernonville *et al.*, 2006] Bernonville S., Leroy N., Kolski C., & Beuscart-Zéphir M. (2006). Association des réseaux de Petri et des critères d'ergonomie des logiciels pour la modélisation et la réingénierie de systèmes interactifs, cas de la prescription thérapeutique en milieu hospitalier. ErgoIA 2006, "L'humain comme facteur de performance des systèmes complexes", Biarritz, pp. 55-62.

[Boehm, 2006] Boehm B. (2006). Some Future Trends and Implications for Systems Engineering and Software Engineering Processes. Systems Engineering, vol. 9, n° 1, pp. 1-19.

[Boehm, 2009a] Boehm B. (2009). Scaling Up Agility: The Architected Agile Approach. International software development conference (JAOO), Aarhus.

[Boehm, 2009b] Boehm B. (2009). Balancing Agility and Architecture. International software development conference (JAOO), Aarhus.

[Boy, 1991] Boy G. (1991). Indexing Hypertext Documents in Context. Proceeding HYPERTEXT '91 Proceedings of the third annual ACM conference on Hypertext, pp. 51-61.

[Boy, 1998] Boy G. (1998). Cognitive functions analysis. Ablex, Stamford, 201 p.

[Boy, 2013] Boy G. (2013). Orchestrating Human-Centered Design. Springer, London, 233 p.

[Boy & Narkevicius, 2014] Boy G., & Narkevicius J-McG (2014). Unifying Human Centered Design and Systems Engineering for Human Systems Integration. In Aiguier M. *et al.* (Eds.), Complex Systems Design and Management, Springer, London, pp. 1-12.

[Brangier & Bornet, 2011] Brangier E., & Bornet C. (2011). Persona: A method to produce representations focused on consumers' needs. In W. Karwowski M. Soares & N. Stanton (Eds.), Human Factors and ergonomics in Consumer Product Design, Taylor and Francis, London, pp. 38-61.

[Brangier *et al.*, 2012] Brangier É., Bornet C., Bastien J. M. C., Michel G., & Vivian R. (2012). Effets des personas et contraintes fonctionnelles sur l'idéation dans la conception d'une bibliothèque numérique. Le travail humain, vol. 75, n° 2, pp. 121-145.

[Broadbent, 2011] Broadbent S. (2011). L'intimité au travail : la vie privée et les communications personnelles dans l'entreprise. FYP éditions, Limoges, 192 p.

[BST, 2013] BST (Bureau de la sécurité des transports du Canada) : (2013). Rapport d'enquête ferroviaire R12T0038, Déraillement en voie principale du train de voyageurs numéro 92 exploité par VIA Rail Canada Inc au point milliaire 33,23 de la subdivision d'Oakville du Canadien National à Aldershot (Ontario) le 26 février 2012.

[BNAE, 2013] BNAE (2010). RG00039B, Recommandations générales Aéronautiques 000 39B - Management de programme - Recommandations pour la mise en œuvre de la maîtrise des risques.

[Cahour & Lancry, 2011] Cahour B., & Lancry A. (2011). Émotions et activités professionnelles et quotidiennes. Le travail Humain, vol. 74, n° 2, pp. 97-106.

[Calvary *et al.*, 2003] Calvary G., Coutaz J., Thevenin D., Limbourg Q., Bouillon L., & Vanderdonckt J. (2003). A unifying reference framework for multi-target user interfaces. Interacting with Computers, vol. 15, n°3, pp. 289-308.

[Calvary, 2007] Calvary G. (2007). Plasticité des Interfaces Homme-Machine. Habilitation à Diriger des Recherches. Université Joseph Fourier – Grenoble I.

[Calvary et al., 2013] Calvary G., Dery-Pinna A. M., Occello A., Renevier P., & Gabillon Y. (2013). Composition of User Interfaces. In Calvary G., Delot T., Sedes F., Tigli J.Y. (Eds.), Computer Science and Ambient Intelligence, Wiley, pp. 203-224.

[Carrol, 1976] Carrol J.S. (1976). The Effect of Imagining an Event on Expectations for the Event: An Interpretation in Terms of the Availability Heuristic. Journal of Experimental Social Psychology, 1978, n°14, pp. 88-96.

[Card *et al.*, 2011] Card S.K, Moran, T. P., & Newell A. (1983). The Psychology of Human-Computer Interaction. Erlbaum Associates. Hillsdale, USA.

[Causse *et al.*, 2013] Causse M., Péran P., Dehais F., Caravasso C-F., Zeffiro T. & Sabatini U. (2013). Affective decision making under uncertainty during a plausible aviation task: An fMRI study. NeuroImage, vol. 71, pp. 19-29.

[CE, 2011] Commission européenne (2011). Décision de la commission du 26 avril 2011 concernant une spécification technique d'interopérabilité relative au sous-système «infrastructure» du système ferroviaire transeuropéen conventionnel.

[Chalandon, 2013] Chalandon X. (2013). Conscience de la situation : invariants internes et invariants externes. Thèse de Doctorat d'Ergonomie soutenue le 2 mai 2007 (CNAM).

[CI, 2001] Courrier International (2001). Nouvelle catastrophe écologique en mer d'Aral. Courrier International, n° 536, 8 février 2001, (Obchtchaïa Gazeta).

[Cieutat, 2013] Cieutat J-M. (2013). Quelques applications de la réalité augmentée : Nouveaux modes de traitement de l'information et de la communication. Effets sur la perception, la cognition et l'action. Mémoire pour l'obtention du titre d'Habilitation à Diriger des Recherches, Spécialité : Informatique, Université Paul Sabatier, Toulouse, 13 mars 2013.

[Cisternino & Vaucouleur, 2009] Cisternino A., & Vaucouleur S. (2009). Aspect Oriented Programming Made Easy: An Embedded Pointcut Language. 20th Asia-Pacific Software Engineering Conference (APSEC), pp. 215-222.

[Closset-Kopp & Decocq, 2015] Closset-Kopp D., & Decocq G. (2015). Remnant artificial habitats as biodiversity islets into forest oceans. Ecosystems, published online: 10 February 2015, DOI: 10.1007/s10021-015-9843-3.

[Cloutier & Verma, 2007] Cloutier R., & Verma D. (2007). Applying of the Concept of Patterns to Systems Architecture. Systems Engineering, vol. 10, n°2, pp. 138-154.

[Colas & Sarron, 2009] Colas C., & Sarron J.-C. (2009). Résilience des hommes et des systèmes militaires, document interne.

[Collins, 2009] Collins J. (2009). Transition strategy: A manual for all seasons. Armed Forces Journal, April 2009, revue en ligne, site de

l'article : http://www.armedforcesjournal.com/transition-strategy-a-manual-for-all-seasons/.

[Colson & Cusset, 2008] Colson A., & Cusset Y. (2008). Retour sur un exercice de prospective : Réflexions pour 1985. La Documentation française, Horizons stratégiques, vol. 1, n°7, pp. 142- 150.

[Conversy *el al.*, 2014] Conversy S., Chatty S., Gaspard-Boulinc H., & Vinot J-L. (2014). L'accident du vol AF447 Rio-Paris, un cas d'étude pour la recherche en IHM. IHM'2014, Villeneuve d'Ascq, pp. 60- 69.

[Courage & Baxter, 2005] Courage, C., & Baxter, K. (2005). Understanding Your Users: A Practical Guide to User Requirements Methods, Tools, and Techniques. Elsevier, San Francisco.

[Coutaz, 1987] Coutaz J. (1987). PAC, on Object Oriented Model for Dialog Design. Proceedings Interact'1987, Elsevier Science Publishers B.V.

[Coutaz, & Nigay, 2001] Coutaz, J., & Nigay. L. (2001). Architecture logicielle conceptuelle des systèmes interactifs. In C. Kolski (Ed.), Analyse et conception de l'IHM, Interaction Homme-Machine pour les Systèmes d'Information, vol. 1. Hermès, Paris, pp. 208-246.

[Dehais *et al.*, 2014] Dehais F., Causse M., Régis N., Menant E., Vachon F. & Tremblay S. (2014). Failure to Detect Critical Auditory Alerts in the Cockpit Evidence for Inattentional Deafness. Human Factors, vol. 56, n°4, pp. 631-644.

[Dehais *et al.*, 2015] Dehais F., Peysakhovich V., Scannella S., Fongue J.& Thibault G. (2015). "Automation Surprise" in Aviation: Real-Time Solutions. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, pp. 2525-2534.

[Dekker, 2006] Dekker S. (2006). Resilience engineering: chronicling the emergence of confused consensus. In E. Hollnagel, D. Woods & N. Levenson (Eds.), Resilience Engineering. Concepts and precepts, Ashgate, Aldershot, pp. 77-92.

[Desportes, 2004] Desportes V. (2004). Décider dans l'incertitude. Economica, Paris.

[Dey, 1998] Dey A. K. (1998). Context-aware computing: The CyberDesk project. Proceedings of the AAAI 1998 Spring Symposium on Intelligent Environments, 51-54. Menlo Park, CA: AAAI Press.

[Diaper & Stanton, 2004] Diaper D., & Stanton N. (2004). The Handbook of Task Analysis for Human-Computer Interaction. Lawrence Erlbaum Associates, Mahwah.

[Mordecai *et al.*, 2014] Mordecai Y., Orhof O., & Dori D. (2014). Modeling Software Agent Awareness of Physical-Informatical Essence Duality. Proc. SwSTE'14, Tel Aviv, Israel.

[Elmqvist, 2011] Elmqvist N. (2011). Distributed User Interfaces: State of the Art. DUI 2011 -Distributed User Interfaces-, Vancouver, Canada.

[EN, 2000] EN (2000). EN 50126-1, Applications ferroviaires; spécifications et démonstration de la fiabilité, de la maintenabilité et de la sécurité (FMDS); Partie 1 : Exigences de base et procédures génériques.

[EN, 2010] EN (2010). EN 60300-3-15, Gestion de la sûreté de fonctionnement – Partie 3-15 : Guide d'application- Ingénierie de la sûreté de fonctionnement des systèmes.

[Endsley, 1995a] Endsley M.R. (1995). Measurement of situation awareness in dynamic systems. Human Factors, vol. 37, n° 1, pp. 65–84.

[Endsley, 1995b] Endsley M.R. (1995). Toward a theory of situation awareness in dynamic systems. Human Factors, vol. 37, n° 1, pp. 32–64.

[Fallet-Fidry *et al.*, 2012] Fallet-Fidry G., Duval C., Simon C., Levrat E., Weber P., & Iung B. (2012). Maîtrise et analyse des risques des systèmes intégrant les domaines techniques, humains, organisationnels et environnementaux. In Matta N., Vandenboomgaerde Y. & Arlat J. (Eds.), Supervision, surveillance et sûreté de fonctionnement des grands systèmes, Hermès, Paris, pp. 309-334.

[Fardoun *et al.*, 2011] Fardoun H.M., Romero López S., & Villanueva P. G. (2011). Improving E-Learning Using Distributed User Interfaces. Proceedings Workshop DUI'2011 "Distributed User Interfaces", at CHI'2011, Vancouver.

[Fardoun *et al.*, 2012] Fardoun H.M., Ciprés A.P., & Alghazzawi D.M. (2012). CSchool: DUI for Educational System using Clouds. In Proceedings of the 2nd Workshop on Distributed User Interfaces: Collaboration and Usability, DUI 2012, In Conjunction with CHI 2012, Austin.

[Fidock, 2006a] Fidock J. (2006). Organisational Structure and Information Technology (IT): Exploring the Implications of IT for Future Military Structures. Defence Science and Technology Organisation, Edinburgh.

[Fidock, 2006b] Fidock J. (2006). The model of technology appropriation: A lens for understanding the process of human systems integration. Defence Science and Technology Organisation, Edinburgh.

[Fidock & Carroll, 2010] Fidock J., & Carroll J. (2010). Theorising about the Life Cycle of IT Use: An appropriation perspective, in Information Systems Foundations: Theory building in information systems. In Dennis N. Hart and Shirley D. Gregor (Eds.), The Australian National University Press, Canberra, pp. 79-112.

[Fidock *et al.*, 2010] Fidock J., Carroll J., & Rynne A. (2010). Evaluating information systems: an appropriation perspective. Information Systems

Foundations workshop, The Australian National University Press, Canberra, pp 121-141.

[Friedenthal *et al.*,2011] Friedenthal S., Moore A., & Steiner R. (2011). A Practical Guide to SysML. Morgan Kaufmann, Waltham.

[Funk, 2013] Funk K. (2013). Process Analysis and Modeling Using IDEF0.IE 366, Work Systems Engineering course, Oregon State University (http://classes.engr.oregonstate.edu/mime/winter2013/ie366-001/Slides/01-2%20(lab)%20-%20IDEF0.pdf).

[Fuchs *et al.*, 2010] Fuchs P., Hugues O., & Nannipieri O. (2010). Proposition d'une Taxonomie Fonctionnelle des Environnements de Réalité Augmentée. AFRV2010. Cinquième Journées de l'Association Française de Réalité Virtuelle et de l'Interaction 3D, décembre 2010, Orsay, France. <hal-00536787>

[Galara, 2010] Galara D. (2011). Vers un langage de représentation des schémas mentaux des exploitants de systèmes de production complexes et à risques. Génie logiciel, n°96, pp. 11-21.

[Gibouin, 2011] Gibouin A. (2011). From Individual to Collective Personas; Modeling Realistic Groups and Communities of Users (and not Only Realistic Individual Users). ACHI 2011: The Fourth International Conference on Advances in Computer-Human Interactions, Gosier, Guadeloupe, France.

[Giraudeau, 2014] Giraudeau M. (2014). Apport des HUMS à la sûreté de fonctionnement et au soutien. Conférence GIFAS Health and Usage Monitoring Systems (HUMS) dans les équipements aéroportés, Paris.

[Grosjean, 2005] Grosjean M. (2005). L'awareness à l'épreuve des activités dans les centres de coordination. @ctivités, vol. 2, n°1, pp. 76-98.

[Gruchociak & Rosa, 2014] Gruchociak B. & Rosa S. (2014). Rapport de TP I.H.M - Analyse de la tâche et Maquettage. ISTV, Université de valenciennes et du Hainaut-Cambrésis.

[Halfpenny, 2005] Halfpenny A. (2005). pHUMS—Prognostic Health and Usage Monitoring of Military Land Systems. site visité le 13 décembre 2014, http://www.ncode.com/fileadmin/mediapool/nCode/downloads/Whitepaper_nCode-HUMS_Prognostic_Monitoring_of_Military_LandSystems-Halfpenny.pdf.

[Hardy, 2010] Hardy T-L. (2010). The system safety skeptic. Author-House, Bloomington

[Hartert *et al.*, 2012] Hartert L., Nuzillard D., & Sayed-Mouchaweh M. (2012). Approche à base d'apprentissage dynamique pour la surveillance et le suivi de fonctionnement du générateur de vapeur des

réacteurs à neutrons rapides Prototype Fast Reactors. In Matta N., Vandenboomgaerde Y. & Arlat J. (Eds.), Supervision, surveillance et sûreté de fonctionnement des grands systèmes, Hermès, Paris, pp. 255-272.

[Hayes, 2009] Hayes R. (2009). Concept Development and Experimentation. Command and Control Research Program, United States Department of Defense.

[HB, 2010] Health Business UK (2010). Ergonomics and obesity. Health Business UK, site visité le 13 décembre 2014, http://www.healthbusinessuk.net/features/145/1603-ergonomics-and-obesity.

[He *et al.*, 2012] He X., Mourot G., Maquin D., Ragot J., Beauseroy P., Smolarz A., & Grall-Maës E. (2012). Apprentissage multi-tâches pour le diagnostic d'un parc de machines. In Matta N., Vandenboomgaerde Y. & Arlat J. (Eds.), Supervision, surveillance et sûreté de fonctionnement des grands systèmes, Hermès, Paris, pp. 155-180.

[Helander *et al.*, 1997] Helander M-G., Landauer T.K., & Prabhu P.V. (1997) Handbook of Human-Computer Interaction, Second Edition. North Holland.

[Helmreich & Merritt, 1998] Helmreich R., & Merritt A. (1998). Culture at work in aviation and medicine; national, organizational and professional influences. Ashgate, Aldershot.

[Hollnagel *et al.*, 2006] Hollnagel E., Woods D. D., & Leveson N. (réds.) (2006). Resilience engineering. Concepts and precepts. Ashgate, Aldershot.

[Hollnagel, 2008] Hollnagel E. (2008). How to be safe by fostering successes rather than reducing failures. The 26th International System safety Conference, Vancouver.

[Hollnagel, 2009] Hollnagel E. (2009). The ETTO Principle: Efficiency-Thoroughness Trade-Off; Why Things That Go Right Sometimes Go Wrong. Ashgate, Aldershot.

[Hollnagel, 2012] Hollnagel E. (2012). FRAM: The Functional Resonance Analysis Method. Ashgate, Aldershot.

[Hugues *et al.*, 2010] Hugues O., Cieutat J-M., & Guitton P. (2010). Plateforme Expérimentale de Réalité Augmentée pour l'Aide à la Navigation Maritime. Association Française de Réalité Virtuelle, février 2010, Lyon, France. <hal-00459782>.

[Idoughi *et al.*, 2010] Idoughi D., Kolski C., & Seffah, A. (2010). Design Principles of Web-based Services in Large-Scale e-Logistics Processes. Proc. LSS2010, Villeneuve d'Ascq.

[Idoughi *et al.*, 2012] Idoughi D., Seffah A., & Kolski C. (2012). Adding user experience into the interactive service design loop: a persona-based approach. Behaviour & Information Technology, vol. 31, n° 3, pp. 287-303.

[IEEE, 2005] IEEE (2005). IEEE Std 1220, Standard for Application and Management of the Systems Engineering Process.

[ISO, 2002] ISO (2002). ISO/TR 16982, Méthodes d'utilisabilité pour la conception centrée sur l'opérateur humain - Ergonomie de l'interaction homme-système.

[ISO, 2003] ISO (2003). NF ISO 13374-1, Surveillance et diagnostic d'état des machines, Traitement, échange et présentation des données, Lignes directrices générales.

[ISO, 2007] ISO (2007). NF ISO 13374-2, Surveillance et diagnostic d'état des machines, Traitement, échange et présentation des données, Traitement des données.

[ISO, 2008] ISO (2008). ISO/IEC/IEEE 15288, Systems engineering — System life cycle processes.

[ISO, 2009] ISO (2009). ISO/IEC WD 29148.3, Software and systems engineering, Life cycle processes, Requirements engineering.

[ISO, 2010a] ISO (2010). PR NF ISO 17359, Surveillance et diagnostic d'état des machines, Lignes directrices générales.

[ISO, 2010b] ISO (2010). ISO 9241-210:2010, Ergonomie de l'interaction homme-système - Partie 210: Conception centrée sur l'opérateur humain pour les systèmes interactifs.

[ISO, 2010c] ISO (2010). ISO/IEC TR 24748-1:2010(E), Systems and software engineering - Life cycle management - Part 1: Guide for life cycle management.

[ISO, 2011] ISO (2011). ISO/IEC/IEEE 42010, Ingénierie des systèmes et des logiciels - Description de l'architecture.

[ISO, 2012] ISO (2012). ISO/IEC/IEEE 31320, Technologies de l'information - Langages de modélisation - Partie 1: Syntaxe et sémantique pour IDEF0.

[ISO, 2013] ISO (2013). ISO/IEC 27001, Information Technology – Security Techniques – Information Security management systems – Requirements.

[ISO, 2014] ISO (2014). ISO/IEC/IEEE FDIS 15288, Systems engineering, System life cycle processes (revision of ISO/IEC/IEEE 15288:2008).

[ISO, 2015] ISO (2015). ISO/IEC/IEEE 15288, Systems engineering — System life cycle processes.

[Jackson, 2009] Jackson S. (2009). Architecting Resilient Systems: Accident Avoidance and Survival and Recovery from Disruptions. Wiley, Hoboken.

[Jackson & Ferris, 2013] Jackson S., & Ferris T. (2013). Resilience principles for engineered systems, Systems Engineering, vol. 16, n° 2, pp. 152–164.

[Jouvenel, 2002] Jouvenel H. de (2002). La démarche prospective ; Un bref guide méthodologique. Revue Futuribles, n°247, pp 47-68.

[Judge *et al.*, 2012] Judge T.K., Matthews T., & Whittaker, S. (2012). Comparing Collaboration and Individual Personas for the Design and Evaluation of Collaboration Software. CHI Conference on Human Factors in Computing Systems (CHI'12), Austin, pp. 1197-2000.

[Julien *et al.*, 1975] Julien P-A., Lamonde P., & Latouche D. (1975). La méthode des scénarios en prospective. L'Actualité économique, vol. 51, n° 2, pp. 253-281.

[Karsenty & Quillaud, 2010] Karsenty L., & Quillaud A. (2010). Réactivité à l'imprévu et sense-making : Analyse de récits et témoignages de situation de gestion de l'imprévu. Livrable F07, contrat de recherche DGA n° 2009.34.0035, Dédale (36 p.), Paris.

[Karsenty, 2008] Karsenty L. (2008). L'incompréhension dans la communication (Misunderstandings in communication). Presses universitaires de France, Paris.

[Karsenty, 2011] Karsenty L. (2011). Confiance interpersonnelle et communication de travail ; Le cas de la relève de poste. Le travail Humain, vol. 74, n° 2, pp. 131-155.

[Karsenty & Quillaud, 2011] Karsenty L., & Quillaud A. (2011). Gestion de l'imprévu et construction collective du sens de la situation : Quelques leçons tirées de l'analyse d'incidents. 46ème congrès international. Société d'Ergonomie de Langue Française, pp. 261-265.

[Kirke, 2004] Kirke C. (2004). Organizational culture: the unexpected force. Journal of battlefield technology, vol. 7, n°2, pp. 11-15.

[Kirke, 2005] Kirke C. (2005). Organizational Culture : Can systems designers ignore it?. Proceedings of the IEE and HFI DTC Symposium on People and Systems: Who are we designing for? London, pp. 9-15.

[Kirwan, 1992a] Kirwan B. (1992). Human error identification in human reliability assessment Part 1: Overview of approaches. Applied Ergonomics, vol. 23, n°5, pp. 299-318.

[Kirwan, 1992b] Kirwan B. (1992). Human error identification in human reliability assessment - Part 2: Detailed comparison of techniques. Applied Ergonomics, vol. 23, n°6, pp. 371-381.

[Kirwan, 1998a] Kirwan B. (1998). Human error identification techniques for risk assessment of high risk systems—Part 1: review and evaluation of techniques. Applied Ergonomics, vol. 29, n°3, pp. 157-177.

[Kirwan, 1998b] Kirwan B. (1998). Human error identification techniques for risk assessment of high risk systems-Part 2: towards a framework approach. Applied Ergonomics, vol. 29, n°5, pp. 299-318.

[Kolski *et al.*, 2014] Kolski C., Garbay C., Lebrun Y., Badeig F., Lepreux S., Mandiau R., & Adam E. (2014). Interactive Surfaces, Tangible Interaction: Perspectives for Risk Management. In P. Millot (Ed.), Risk Management in Life critical Systems, ISTE-Wiley, London, pp. 351-373, ISBN 978-1-84821-480-4.

[Kubicki *et al.*, 2012] Kubicki S., Lepreux S., & Kolski C. (2012). Context Model for Distributed UI on Interactive Table(s). 2nd Workshop on Distrubuted User Interfaces: Usability and Collaboration DUI'12 in conjunction with CHI'12. May 5th, Austin, Texas, USA.

[Lemercier *et al.*, 2014] Lemercier C. *et al*. (2014). Inattention behind the wheel: How factual internal thoughts impact attentional control while driving. Safety Science, vol. 62, n° 1, pp. 279–285.

[Leplat & Hoc, 1983] Leplat J., & Hoc J-M. (1983). Tâche et activité dans l'analyse psychologique des situations. Cahiers de Psychologie Cognitive, vol. 3, n°1, pp. 49–63.

[Leplat, 1985] Leplat J. (1985). Erreur humaine, fiabilité humaine dans le travail. Armand Colin, Paris.

[Leplat, 2002] Leplat J. (2002). De l'étude de cas à l'analyse de l'activité. PISTES, vol. 4, n°2, pp. 1–31.

[Lepreux *et al.*, 2011] Lepreux S., Kubicki S., Kolski C., & Caelen J. (2011). Distributed interactive surfaces: A step towards the distribution of tangible and virtual objects. In Gallud J. A., Tesoriero R. & V. Penichet M. R. (Eds.), Distributed user interfaces: Designing interfaces for the distributed ecosystem, Springer, New York, pp. 133–143.

[Lepreux *et al.*, 2012] Lepreux S., Kubicki S., Kolski C., & Caelen J. (2012). From Centralized interactive tabletops to Distributed surfaces: the Tangiget concept. International Journal of Human-Computer Interaction, Taylor & Francis: STM, vol. 28, n° 11, pp.709-721.

[Levenson, 2004] Levenson N. (2004). A new accident model for engineering safer systems. Safety Science, vol. 42, n°4, pp. 237-270.

[Levenson *et al.*, 2006] Levenson N., Dulac N., Zipkin D., Cutcher-Gershenfeld J., Carroll J., & Barrett B. (2006). Engineering resilience into safety-critical systems. In Hollnagel E., Woods D. D. &

Leveson N. (Eds.), Resilience Engineering. Concepts and precepts, Ashgate, Aldershot, pp. 95-123.

[Lewandowski *et al.*, 2007] Lewandowski A., Bourguin G., & Tarby, J-C. (2007). De l'Orienté Objet à l'Orienté Tâches – Des modèles embarqués pour l'intégration et le traçage d'un nouveau type de composants. Revue d'Interaction Homme-Machine, vol 8, n° 1, pp. 1-33.

[Lim & Long, 1994] Lim K-Y., & Long J (1994). The Muse method for usability engineering. Cambridge University Press, New York.

[Lundberg *et al.*, 2009] Lundberg J., Rollenhagen C., & Hollnagel E. (2009). What-You-Look-For-Is-What-You-Find – The consequences of underlying accident models in eight accident investigation manuals. Safety Science, vol. 47, n°10, pp. 1297–1311.

[Luzeaux, 2011] Luzeaux D. (2011). Ingénierie des grands systèmes complexes. In Luzeaux D., Ruault J.-R. & Wippler J.-L. (Eds.), Maîtrise de l'ingénierie des systèmes complexes et des systèmes de systèmes : études de cas, Hermes-Lavoisier, Paris, pp. 21-106.

[Luzeaux *et al.*, 2011] Luzeaux D., Ruault J.-R., & Wippler J.-L. (2011). Maîtrise de l'ingénierie des systèmes complexes et des systèmes de systèmes. Hermes-Lavoisier, Paris.

[Luzeaux & Ruault 2013] Luzeaux D., & Ruault J.-R. (2013). L'ingénierie système. Collection 100 questions pour comprendre et agir, AFNOR éditions, Paris.

[Maier & Rechtin, 2003] Maier M., & Rechtin E. (2003). The Art of Systems Architecting. CRC Press, New York.

[Mäkinen, 2013] Mäkinen T. (2013). Talking vehicles make driving cooperative. In Rouhiainen, V., Research highlights in safety and security, VTT Technical Research centre of Finland, 19p.

[Maley *et al.*, 2007] Maley S., Plets J., & Phan N. (2007). US Navy Roadmap to Structural Health and Usage Monitoring. The Present and Future American Helicopter Society 63rd Annual Forum, Virginia Beach.

[March & Simon, 1958] March, J.-G. & Simon, H.-A. (1958). Organisations. New York, Wiley & Sons.

[Marseguerra, 2014] Marseguerra M. (2014). Early detection of gradual concept drifts by text categorization and Support Vector Machine techniques: The TRIO algorithm. Reliability Engineering & System Safety, vol. 129, September 2014, pp. 1–9.

[Matthews *et al.*, 2011] Matthews T., Whittaker S., Moran T., & Yuen, S. (2011). Collaboration Personas: A New Approach to Designing Workplace Collaboration Tools. ACM CHI Conference on Human Factors in Computing Systems (CHI'11), Vancouver, BC, Canada, pp. 2247-2256.

[Meinadier, 1998] Meinadier J.-P. (1998). Ingénierie et intégration des systèmes. Hermes-Lavoisier, Paris.

[Meinadier & Fiorèse, 2012] Meinadier J-P., & Fiorèse S. (eds.) (2012). Découvrir et Comprendre l'Ingénierie Système. Cépaduès, Toulouse.

[Melchior *et al.*, 2011] Melchior J., Vanderdonckt J., & Van Roy P. (2011). A model-based approach for distributed user interfaces. In Proceedings of the 3rd ACM SIGCHI symposium on Engineering interactive computing systems, ACM, pp. 11-20.

[MIL-STD, 2012] MIL-STD-882E (2012). System Safety. Department of Defense Standard Practice.

[Millot & Pacaux-Lemoine, 2013) Millot P., & Pacaux-Lemoine M-P. (2013). Coopération homme-machine et Situation Awareness. In P. Millot (Ed.), Ergonomie des systèmes homme-machine, Hermes-Lavoisier, Paris, pp. 31-63.

[Moati, 2003] Moati P. (2003). Esquisse d'une méthodologie pour la prospective des secteurs ; une approche évolutionniste. Cahier de recherche, n°187 du CREDOC.

[Morel, 2002] Morel C. (2002). Les Décisions absurdes : Sociologie des erreurs radicales et persistantes. Gallimard, Paris.

[Nelson, 2010] Nelson J., Buisine S., & Aoussat A. (2010). Creativity as a tool for prospective use analysis in the design of innovative products. Actes de la conférence Ergo'IA 2010, Biarritz.

[Nelson, 2012] Nelson J., Buisine S., & Aoussat A. (2012). A methodological proposal to assist scenario-based design in the early stages of innovation projects. Le travail humain, vol. 75, n°3, pp. 279-305.

[Norman, 1998] Norman D. (1988). The Psychology of Everyday Things. Doubleday, New York.

[NTSB, 2010] NTSB (National Transportation Safety Board) (2010). Accident report, Collision of Metrolink Train 111 With Union Pacific Train LOF65-12, Chatsworth, California, September 12, 2008, NTSB/RAR-10/01, PB2010-916301.

[Nunes & Cunha, 2001] Nunes N-J., & Cunha J-F. (2001). Wisdom- Whitewater Interactive System Development with Object Models. In Mark Van Harmelen (Ed.), Object Modeling and User Interface Design, Addison -Wesley, Boston, pp. 197-243.

[O'Brien, 2010] O'Brien K. (2010). Boeing Position on Automatic Dependent Surveillance-Broadcast (ADS-B). CAAC-Thales ADS-B Flight Operation Seminar June 2010, Beijing, China.

[Ombredane & Faverge, 1955] Ombredane A., & Faverge J-M. (1955). L'analyse du travail ; facteur d'économie humaine et de productivité. PUF, Paris.

[Ouedraogo *et al.*, 2013] Ouedraogo K-A., Enjalbert S., & Vanderhaegen F. (2013). How to learn from the resilience of Human–Machine Systems? Engineering Applications of Artificial Intelligence, vol. 26, n° 1, pp. 24–34.

[Palanque & Bastide, 1997] Palanque P., & Bastide R. (1997). Synergistic modelling of tasks, users and systems using formal specification techniques. Interacting with Computers, vol. 9, n°2, pp. 129-153.

[Pantoquilho & Moreira, 2004] Pantoquilho M., & Ana Moreira A. (2004). Aspect-Oriented Logical Architecture Design A Layered Perspective Applied to Data Warehousing. DSOA'2004, Iberian workshop on Aspect Oriented Software Development.

[Pariès, 2006] Pariès J. (2006). Complexity, emergence, resilience. In Hollnagel E., Woods D. D. & Leveson N. (Eds.), Resilience Engineering. Concepts and precepts, Ashgate, Aldershot, pp. 43-53.

[Pariès, 2010] Pariès J. (2010). De la fiabilité à la résilience, Les nouveaux défis de la sécurité ?. Entretiens Jacques Cartier novembre 2010, Université de Grenoble, Campus de Saint-Martin-d'Hères.

[Paternò, 2004] Paternò F. (2004). ConcurTaskTrees: an engineered approach to model-based design of interactive systems. In Diaper D. & Stanton N. (Eds.), The handbook of analysis for human-computer interaction, Lawrence Erlbaum Associates, Mahwah, pp. 483-500.

[Pellen-Blin *et al.*, 2004] Pellen-Blin M., Bry A., & Chouvy N. (2004). La conception d'organisations futures et les IBEOs (Illustrateur de Besoin d'Exploitation Opérationnelle). Actes de la conférence ERGO-IA 2004, Biarritz.

[Pew & Mavor, 2007] Pew R., & Mavor A. (Eds.) (2007). Human-System Integration in the System Development Process. The national Academies Press, Washington.

[Pfaff & Hagen, 1985] Pfaff G., & Ten Hagen P.J.W. (eds.) (1985). Seeheim Workshop on User Interface Management Systems. Springer- Verlag, Berlin, 1985.

[Plassard, 2003] Plassard F. (2003). Rétrospective de la prospective; la prospective dans le domaine des transports, recherche critique. PREDIT, Ministère de l'Équipement.

[Polet *et al.*, 2002] Polet P., Vanderhaegen F., & Wieringa P. A. (2002). Theory of safety-related violations of system barriers. Cognition, Technology & Work, vol. 4, n° 3, pp. 171-179.

[Polet *et al.*, 2009] Polet P., Vanderhaegen F., & Chaali-Djelassi A. (2009). Prédiction du comportement des opérateurs humains, le cas des déviations volontaires. Application à la conduite automobile.

Journal Européen des Systèmes Automatisés, vol 43, n°6, pp. 661-681.

[Pruitt & Adlin, 2006] Pruitt J., & Adlin T. (2006). The Persona Lifecycle: Keeping People in Mind Throughout Product Design. Morgan Kaufmann, Waltham.

[Pruvost, 2013] Pruvost G. (2013). Modélisation et conception d'une plateforme pour l'interaction multimodale distribuée en intelligence ambiante. Université Paris Sud - Paris XI, thèse n° tel-00805487.

[Quémard, 2009] Quémard E. (2009). Une Ambulance adaptée aux obèses à Marseille. La Gazette Santé Social, site visité le 13 décembre 2014 http://infos.gazette-sante-social.fr/1207/une-ambulance-adaptee-aux-obeses-a-marseille.

[Rapport FTF 2025, 2010] Rapport FTF 2025 (2010). Rapport d'étude portant sur les Forces terrestres futures : étude de la population militaire mixte à horizon 2025, document interne.

[Rasmussen, 1983] Rasmussen J. (1983). Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models. IEEE Transactions on systems, man and cybernetics, vol. 13, n° 3, pp. 257-266.

[Rasmussen, 1997] Rasmussen J. (1997). Risk management in a dynamic society: a modelling problem. Safety Science, vol. 27, n° 2/3, pp. 183-213.

[Reason, 1997] Reason J. (1997). Managing the Risks of Organizational Ashgate, Aldershot.

[Ribeiro *et al.*, 2007] Ribeiro AN., Campos JC., & Martins F. (2007). Integrating HCI into a UML based Software Engineering course, March. Proceedings HCI Educators 2007, pp. 48-57, Aveiro, Portugal.

[Rigaud, 2008] Rigaud E. (2008). Le Management de la Sécurité ; Du management des risques au management de la résilience. Forum Académique de l'AFIS 2008, Nîmes.

[Robert, 2003] Robert J-M. (2003). Que faut-il savoir sur les utilisateurs pour réaliser des interfaces de qualité ?. In Boy G. (Ed.), Ingénierie cognitive : IHM et cognition, Hermès Science Publications Lavoisier, Paris, pp. 249-283.

[Robert & Brangier, 2009] Robert J-M., & Brangier E. (2009). What Is Prospective Ergonomics? A Reflection and a Position on the Future of Ergonomics. In Karsh B.-T. (Ed.), Ergonomics and Health Aspects of Work with Computers, Springer-Verlag, Berlin, pp. 162–169.

[Roberts *et al.*, 1998] Roberts D., Berry D., Isensee S., & Mullaly J. (1998). Designing for the User with OVID: Bridging User Interface Design and Software Engineering. Mac-millan Technical Publishing, Indianapolis.

[Rosnet *et al.*, 2004] Rosnet E., Jurion S., Cazes G., & Bachelard C. (2004). Mixed-Gender Groups: Coping Strategies and Factors of Psychological Adaptation in a Polar Environment. Aviation, Space, and Environmental Medicine, vol. 75, n°4, pp. C10-C13.

[Roques, 2013] Roques P. (2013). Modélisation des systèmes complexes avec SysML. Eyrolles, Paris.

[Rosson & Carroll, 2002] Rosson M-B., & Carroll J-M. (2002). Scenario-Based Design, Chapter 53. In Jacko J. & Sears A. (Eds.), The Human-Computer Interaction Handbook, Lawrence Erlbaum Associates, Hillsdale, pp. 1032-1050.

[Ruault & Van Eylen, 1997] Ruault J.-R., & Van Eylen H. (1997). Convergence entre cas d'utilisation (OOSE) et notion de tâches. 9èmes Journées francophones sur l'Interaction Homme-Machine (IHM'97), Poitiers.

[Ruault, 2002] Ruault J.-R. (2002). UML and Interactive System, another step forward. Computer-Aided Design of User Interfaces (CADUI 2002), Valenciennes.

[Ruault, 2004] Ruault J.-R. (2004). Bridging System Engineering and Human Factors Engineering: a step forward. 14th Annual INCOSE International Symposium, Toulouse.

[Ruault, 2008] Ruault J.-R. (2008). La place de l'humain dans le contexte des systèmes de systèmes. In Luzeaux D. & Ruault J.-R. (Eds.), Systèmes de systèmes ; concepts et illustrations pratiques, Hermes-Lavoisier, Paris, pp. 179-242.

[Ruault, 2009] Ruault J.-R. (2009). Adaptabilité des systèmes à logiciel prépondérant. Journal Européen des Systèmes Automatisés, vol. 43, n°6, pp. 683-710.

[Ruault *et al.*, 2011] Ruault J.-R., Luzeaux D., Colas C., & Sarron J.-C. (2011). Résilience des systèmes sociotechniques Application à l'ingénierie système. Génie logiciel, n° 96, pp. 40-52.

[Ruault *et al.*, 2012a] Ruault, J-R., Kolski, C., &Vanderhaegen, F. (2012). Persona pour la conception de systèmes complexes résilients. Actes de la conférence Ergo'IHM 2012, Biarritz.

[Ruault *et al.*, 2012b] Ruault J-R., Vanderhaegen F., & Luzeaux D. (2012). Sociotechnical systems resilience. 22nd Annual INCOSE International Symposium, Rome.

[Ruault *et al.*, 2013] Ruault J-R., Vanderhaegen F., & Kolski C. (2013). Sociotechnical systems resilience: a dissonance engineering point of view. 12th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design, and Evaluation of Human-Machine Systems, Las Vegas.

[Ruault *et al.*, 2014a] Ruault J.-R., Fanmuy G., & Colet F. (2014). Borne de rechargement de véhicules électriques ; Cas Industriel pour la filière STI 2D. Projet AFIS – Éducation Nationale.

[Ruault *et al.*, 2014b] Ruault J.-R., Gardinetti E., Kolski C., & Vanderhaegen F. (2014). Adaptation de l'ergonomie prospective aux systèmes à longue durée de vie. Le Travail humain, vol. 77, n°3, pp. 257-280.

[Ruault *et al.*, 2014c] Ruault J.-R., Kolski C., & Vanderhaegen F. (2014). Contribution du persona à la résilience des systèmes. Journal Européen des Systèmes Automatisés, vol. 48, n°4-6, pp. 373-396.

[Salembier & Zouinar, 2004] Salembier P., & Zouinar M. (2004). Intelligibilité mutuelle et contexte partagée, inspirations conceptuelles et réductions technologiques. @ctivités, vol. 1, n°2, pp. 64-85.

[Salloway& Trott, 2002] Salloway, A., & Trott, J.R. (2002). Design patterns par la pratique. Eyrolles, Paris.

[Sarter & Woods, 1991] Sarter N.B., & Woods D.D. (1991). Situation awareness: A critical but ill-defined phenomenon. International Journal of Aviation Psychology, vol. 1, n°1, pp. 45–57.

[Seffah *et al.*, 2009] Seffah A., Kolski C., & Idoughi D. (2009). Persona comme outil de design de services interactifs: principes et exemple en e-maintenance. 21ème Conférence de l'Association Francophone sur l'Interaction Homme-Machine, Grenoble.

[SAIC, 2005] SAIC (2005). Good Practices for Implementing Human Reliability Anakysis (HRA), final report, reference NUREG 1792. US Nuclear Regulatory Commission, Washington DC.

[Scapin & Bastien, 2001] Scapin D., & Bastien C. (2001). Analyse des tâches et aide ergonomique à la conception: l'approche MAD*. In Kolski C. (Ed.), Analyse et conception de l'IHM, Interaction homme-machine pour les Systèmes d'Information, vol. 1, Hermès, Paris, pp. 85-116.

[Sears & Jacko, 2012] Sears A., & Jacko J. (2012). The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies and Emerging Applications, Second Edition (Human Factors and Ergonomics). CRC Press, New York.

[Sedki *et al.*, 2012] Sedki K., Polet P., & Vanderhaegen F. (2012). Intégration des facteurs humains organisationnels dans le modèle BCD pour l'analyse des risques : une approche à base de digramme d'influence. In Matta N., Vandenboomgaerde Y. & Arlat J. (Eds.), Supervision, surveillance et sûreté de fonctionnement des grands systèmes, Hermès, Paris, pp. 335-360.

[Shneiderman & Plaisant, 2009] Shneiderman B., & Plaisant C. (2009). Designing the User Interface: Strategies for Effective Human-Computer Interaction (5th Edition). Prentice Hall, Upper Saddle River.

[Soulier *et al.*, 2008] Soulier E., Bugeaud, F., & Ruault, J-R. (2008). Nouveaux concepts pour la collaboration entre experts des facteurs humains et ingénieurs des systèmes. Actes de la conférence ErgoIA 2008, Biarritz.

[Sperber & Wilson, 1989] Sperber D., & Wilson D. (1989). La Pertinence; communication et cognition. Les Editions de Minuit, Paris.

[Sperber, 1996] Sperber D. (1996). La contagion des idées. Éditions Odile Jacob, Paris.

[Stanton, 1994] Stanton N-A. (1994). Human factors in alarm design. Taylor & Francis, Abingdon.

[Stanton & Baber, 1997] Stanton N-A., & Baber C. (1997). Comparing speech versus text displays for alarm handling. Ergonomics, vol. 40, n° 11, pp. 1240-1254.

[Stanton & Stammers, 1998] Stanton N-A., & Stammers R-B. (1998). Alarm initiated activities: matching formats to tasks. International Journal of Cognitive Ergonomics, vol. 2, n° 4, pp. 331-348.

[Stanton & Baber, 2008] Stanton N-A., & Baber C. (2008). Modelling of human alarm handling responses times: a case of the Ladbroke Grove rail accident in the UK. Ergonomics, vol. 51, n° 4, pp. 423-440.

[Swain & Guttmann, 1983] Swain A. D., & Guttmann H. E. (1983). Handbook on Human Reliability Analysis with Emphasis on Nuclear Power Plant Application. NUREG/CR-1278. SAND 80-0200 RX, AN. Final Report.

[Swain & Mills, 2003] Swain K., & Mills, V. (2003). Implicit Communication in Novice and Expert Teams. DSTO, Edinburgh.

[Tarby et al., 2009] Tarby J-C., Ezzedine H., & Kolski C. (2009). Trace-based Usability Evaluation Using Aspect-oriented Programming and Agent-based Software Architecture. In: Seffah A., Vanderdonckt J. and Desmarais M. (Eds.), Human-Centered Software Engineering: Architectures and Models-Driven Integration, Springer HCI Series, pp. 257-276.

[Tesoriero, 2014] Tesoriero R. (2014). Distributing User Interfaces. 4th Workshop on Distributed User Interfaces and Multimodal Interaction, 14th International Conference on Web Engineering ICWE 2014. Toulouse.

[TSB, 2012] TSB (Transportation Safety Board of Canada) (2013). Railway Investigation Report R12T0038, Main-track Derailment VIA Rail Canada Inc. Passenger Train No. 92 Mile 33.23, Canadian

National Oakville Subdivision Aldershot, Ontario 26 February 2012.

[Tversky & Kahneman, 1974] Tversky A., & Kahneman D. (1974). Judgment under Uncertainty: Heuristics and Biases. Science, vol. 185, n° 4157, pp. 1124-1131.

[Valaskakis. 1975] Valaskakis K. (1975). Prospective, rétrospective et perspective : un essai de modélisation du temps. L'Actualité économique, vol. 51, n° 2, pp. 209-228.

[Vanderdonckt, 2003] Vanderdonckt J. (2010). Distributed User Interfaces: How to Distribute User Interface Elements across Users, Platforms, and Environments. Interaccion'2010, Valencia.

[Vanderhaegen, 2003] Vanderhaegen F. (2003). Analyse et contrôle de l'erreur humaine. Hermès-Lavoisier, Paris.

[Vanderhaegen *et al.*, 2011] Vanderhaegen F., Zieba S., Enjalbert S., & Polet P. (2011). A Benefit/Cost/Deficit (BCD) model for learning from human errors. Reliability Engineering & System Safety, vol. 96, n° 7, pp. 757-766.

[Vanderhaegen & Caulier, 2011] Vanderhaegen F., & Caulier P. (2011). A multi-viewpoint system to support abductive reasoning. Information Sciences, vol. 181, n° 24, pp. 5349-5363.

[Vanderhaegen, 2012] Vanderhaegen F. (2012). Dissonance engineering for risk analysis: a theoretical framework. Workshop on Risk Management in Life Critical Systems, Florida Institute of Technology.

[Vanderhaegen, 2014] Vanderhaegen F. (2014). Dissonance Engineering: A New Challenge to Analyse Risky Knowledge When using a System. International Journal of Computers, Communications and Control, vol. 9, n°6, pp. 776-785.

[Vanderhaegen & Zieba, 2014] Vanderhaegen F., & Zieba S. (2014). Reinforced learning systems based on merged and cumulative knowledge to predict human actions. Information Sciences, vol. 276, pp. 146–159.

[Vaske & Grantham, 1990] Vaske J., & Grantham C-E. (1990). Socializing the Human-Computer Environment. Intellect Books, Bristol.

[Vaughan, 1996] Vaughan D. (1996). The Challenger launch decision. The University of Chicago Press, Chicago.

[Villaren, 2013] Villaren T. (2013). Modèles et mécanismes d'adaptation de l'interaction Homme-Machine aux changements de contexte. Télécom Bretagne, Université de Bretagne-Sud ; thèse n°tel-00816385.

[Walter, 2012] Walter L. (2012). Safety 2012. Ergonomic Strategies for Managing Obesity in the Workplace, site visté le 14 décembre

2014, http://ehstoday.com/health/safety-2012-ergonomic-strategies-managing-obesity-workplace.

[Westrum, 2006] Westrum R. (2006). A typology of resilience situations. In Hollnagel E., Woods D. D. & Leveson N. (Eds.), Resilience Engineering. Concepts and precepts, Ashgate, Aldershot, pp. 55-65.

[Wiig, 2006] Wiig J. (2006). Optimization of fault diagnosis in helicopter health and usage monitoring systems. Thèse de doctorat, École Nationale Supérieure d'Arts et Métiers, décembre 2006.

[WHO, 1998] WHO (World Health Organization) (1998). Obesity : preventing and managing the global epidemic. Report of a WHO Consultation on Obesity, Geneva, 3-5 June 1997.

[Woltjer, 2008] Woltjer R. (2008). Resilience assessment based on models of functional resonance. Proceedings of the 3rd Symposium on Resilience Engineering, Antibes Juan-les-Pins.

[Woods, 2006] Woods D. (2006). Essential characteristics of resilience. In Hollnagel E., Woods D. D. & Leveson N. (Eds.), Resilience Engineering. Concepts and precepts, Ashgate, Aldershot, pp. 21-33.

[Woods & Cook, 2006] Woods D., & Cook R. (2006). Incidents – Markers of resilience or brittleness?. Hollnagel E., Woods D. D. & Leveson N. (Eds.), Resilience Engineering. Concepts and precepts, Ashgate, Aldershot, pp. 69-76.

[Zieba *et al.*, 2010] Zieba S., Polet P., Vanderhaegen F., & Debernard S. (2010). Principles of adjustable autonomy: a framework for resilient human machine cooperation. Cognition, Technology and work, vol. 12, n° 3, pp. 193-203.

[Zieba *et al.*, 2011] Zieba S., Polet P., &Vanderhaegen F. (2011). Using adjustable autonomy and human-machine cooperation for the resilience of a human-machine system, Application to a ground robotic system. Information Sciences, vol. 181, n°3, pp. 379-397.

Résumé / summary

Résumé

Pour répondre aux enjeux de la longue vie opérationnelle des systèmes et de l'incertitude de l'environnement, la résilience complète la sûreté de fonctionnement pour prendre en compte les situations imprévisibles, sans précédent : l'objectif est de comprendre la situation pour éviter un accident. La qualité de l'interaction homme-machine est essentielle pour atteindre cet objectif. L'état de l'art présente la résilience des systèmes sociotechniques comme complémentaire à la sécurité. Mettre en œuvre la résilience affecte tant l'architecture système que les processus d'ingénierie système. Enfin, elle affecte aussi l'interaction homme-machine, tant son processus de conception centrée utilisateur, ses modèles utilisateur (persona), que ses modèles d'architecture. Nous avons créé le patron de conception « surveiller et alerter » appliqué à la fonction « éviter » de la résilience, pour donner aux opérateurs la capacité de comprendre la dynamique du système, le conduire à vue face à des situations imprévisibles, sans précédent afin d'éviter la survenue d'un accident. La proposition comprend aussi des processus à mettre en œuvre pour contribuer à la résilience d'un système critique à longue durée de vie. L'application au domaine ferroviaire s'appuie sur l'analyse de rapports d'enquête technique d'accidents. Elle se décline sur le patron de conception « surveiller et alerter » et sur le persona, *in fine* pour proposer des améliorations des interfaces utilisateur. Des perspectives de recherche complètent le mémoire.

Mots-clés :

Résilience, interaction homme-machine, architecture système, système de surveillance de l'état et de l'usage, conscience partagée de la situation, ergonomie prospective, persona

Summary

The long operational lifecycle of systems and the uncertainty of the environment are a great challenge to engineers. Resilience enhances reliability and safety to take into account the unforeseeable situations, without precedent. The goal is to understand the situation to avoid an accident. The quality of the human-machine interaction is the key issue to achieve this goal. The state of the art explains that sociotechnical systems resilience completes safety approach. Implementaing resilience impacts both system architecture and systems engineering processes. At the end, implementing resilience impacts human-computer interaction, user centred design as well as architecture models. We created the design pattern "to monitor and alert" applied to the function "to avoid" of the resilience. Its goal is to give to the operators the capacity to understand the dynamics of the system, to control at sight vis-a-vis unforeseeable situations, in order to avoid an accident. The proposal contents the processes to be implemented to contribute to the resilience of long lifecycle critical systems. The application to the railway domain is based on the analysis of three accident technical reports. It is declined, on the processes to be implemented to contribute to the resilience of a system, on the design pattern "to monitor and alert" for the architecture of a resilient system and to propose improvements of the user interface. Research forecasts supplement the report.

Key-words:

Resilience, systems engineering, systems architecture, health and usage monitoring system, human-computer interaction, shared situation awareness, prospective ergonomics, persona