Gestion de procédures et prise en compte du danger lors de l'occurrence d'incidents combinés : Application à la supervision d'une ligne de métro

Delphine Paquereau

N° d'ordre: 2015-ISAL-0024 Année 2015

THÈSE

présentée devant

l'Institut National des Sciences Appliquées de Lyon

pour obtenir le grade de

Docteur

par

Delphine Paquereau

Laboratoire Ampère
École Doctorale : Électronique, Électrotechnique, Automatique (EEA)
Dans le cadre d'une convention CIFRE avec l'entreprise Thales.

Gestion de procédures et prise en compte du danger lors de l'occurrence d'incidents combinés : application à la supervision d'une ligne de métro

---

Soutenue le 30 mars 2015 devant le jury composé de :

Rapporteurs :	Christophe Berenguer	Professeur des Universités GIPSaLab - ENSE3
	Serge Haddad	Professeur des Universités LSV - CNRS - ENS de Cachan
Examinateurs :	Jean-Marc Faure	Professeur des Universités LURPA - CNRS - ENS de Cachan
	Armand Toguyeni	Professeur des Universités CRISTAL - Ecole Centrale Lille
	Laurent Bouresche	Responsable industriel Thales Communication & Security
Encadrants :	Éric Niel	Professeur des Universités AMPÈRE - INSA de Lyon
	Laurent Piétrac	Maître de Conférences AMPÈRE - INSA de Lyon

Remerciements

En préambule de mon mémoire de thèse, je tiens à remercier plusieurs personnes qui ont de près ou de loin contribué à son élaboration et m'ont aidée et soutenue au cours de mes trois années de thèse.

Je souhaite tout d'abord adresser mes remerciements aux rapporteurs de ce mémoire M. Christophe Berenguer et M. Serge Haddad pour l'intérêt qu'ils ont porté à mon étude ainsi que les remarques enrichissantes qu'ils m'ont formulées. Je remercie également M. Jean-Marc Faure et M. Armand Toguyeni de m'avoir fait l'honneur de participer au jury.

Je veux également exprimer mes sincères remerciements et ma reconnaissance aux trois personnes qui m'ont encadrée et soutenue tout au long de ma thèse. Tout d'abord, je remercie mes deux directeurs de thèse : Eric Niel, pour nos discussions et nos échanges qui m'ont permis de prendre du recul sur mes travaux, et Laurent Piétrac, de m'avoir encadré depuis mon master, de m'avoir guidée dans mes recherches et d'avoir combattu à de nombreuses reprises mon manque de confiance en moi et mes doutes. Ces remerciements sont également adressés à Laurent Bouresche, mon encadrant industriel, pour l'intérêt et l'investissement qu'il a porté à mes travaux, pour nos réunions presque hebdomadaire qui m'ont obligée à reformuler mes recherches et pour toutes les connaissances sur le monde industriel qu'il m'a transmises.

J'exprime ma reconnaissance à Thales et plus particulièrement au service ATSsoft qui m'a accueillie tout au long de ma convention CIFRE. Je ne peux pas citer ici toutes les personnes que j'ai pu croiser, mais j'aimerais les remercier du soutien, de l'aide et la confiance qu'ils m'ont accordés au cours de ces trois années passées en leur compagnie. Je souhaiterais également les remercier de m'avoir intégrée sans réserve à l'équipe ATSsoft et d'avoir partagé avec moi tous les aspects de leur travail. Je tiens à remercier plus particulièrement Vincent Beaugendre avec qui j'ai travaillé en collaboration au cours du projet innovant. Il a accepté d'assimiler toutes mes recherches et m'a permis de prendre du recul par rapport à mon travail.

Je remercie également la RATP et principalement les formateurs des opérateurs de supervision. En effet, sans être impliqué dans ma convention CIFRE, ils m'ont offert l'opportunité de suivre leur formation et ainsi d'acquérir l'ensemble des connaissances nécessaires à la réalisation de ce mémoire.

D'un pont de vue plus personnel, je souhaite exprimer mes remerciements chaleureux à l'ensemble de ma famille pour le soutien et l'aide qu'ils m'ont apportés tout au long de mes études et pas seulement au cours de ma thèse.

J'ai également une pensée pour mes amis, GMCA et PCSI2, pour tous ceux qui ont été près de moi pendant ces trois ans, notamment : Stéphanie pour nos longues discussions et nos trajets en bus, Karla pour nos pauses café, Thomas pour les weekend en Normandie, Brice pour nos soirées au restaurant, Sébastien pour les soirées et matchs de rugby. Je n'oublie pas non plus le club de Taekwondo de Clamart avec tous ses adhérents, et plus particulièrement Céline et

Tony, qui m'a permis d'évacuer le stress et me défouler au cours de ces trois ans. Je tiens aussi à remercier mes deux colocataires, Benjamin et Renaud, qui ont su être présents et me changer les idées à de nombreuses reprises. Une pensée également pour Thomas qui m'a accompagnée pendant la rédaction de ce mémoire et qui a su trouver les mots pour m'encourager et me motiver.

Pour finir, je n'oublierai pas ces trois jours vécus au cours de ma thèse : 01.03.2013 - 05.06.2014 - 09.09.2014.

Résumé

Titre :

« Gestion de procédures et prise en compte du danger
lors de l'occurrence d'incidents combinés :
Application à la supervision d'une ligne de métro. »

Durant l'exploitation d'une ligne de métro, l'opérateur de supervision est responsable de l'exécution de procédures pour la gestion des incidents. Cependant, lors de l'occurrence combinée d'incidents, les procédures utilisées peuvent se retrouver en concurrence. Dans ce cas, des situations ne garantissant pas la sécurité des personnes existent et un accident peut se déclencher.

La démarche d'étude des procédures intègre tout d'abord leur représentation graphique avec la notation BPMN. Ces modèles de procédure, compréhensibles et accessibles, constituent ainsi une base de connaissances pour les industriels concernés. Ces modèles sont ensuite interprétés sous forme de réseaux de Petri pour ajouter une dynamique au système étudié. La notion de contrôlabilité et l'influence du contexte d'exécution sont alors introduites dans l'étude de procédures de gestion d'incident.

Afin d'assurer la sécurité des personnes, des états interdits sont définis et identifiés parmi l'ensemble des états accessibles par l'application de la théorie du contrôle par supervision. Ces états interdits se caractérisent de manière originale : suivant leur inclusion dans un ensemble d'états particuliers mais également suivant la contrôlabilité de leurs transitions sortantes. Cette caractérisation innovante s'accompagne des algorithmes permettant de déterminer et d'éviter les états interdits.

Afin d'orienter l'opérateur de supervision dans les actions à exécuter lors d'incidents combinés, des critères de différenciation des trajectoires admissibles évitant les états interdits sont également définis. Les résultats obtenus permettent de proposer une assistance à l'opérateur de supervision sous forme d'alertes et de conseils.

Cette étude se base sur le système de supervision ATS développé par Thales et sur les procédures de gestion d'incident de l'un de leurs clients, la RATP. Un prototype de fonctionnalité d'aide à l'opérateur pour la gestion des incidents reposant sur le savoir-faire client a ainsi pu être intégré au logiciel de Thales.

Mots clés : Supervision, Système de transport, Théorie du contrôle par supervision, Réseaux de Petri, BPMN, Sûreté de fonctionnement, Procédure de gestion d'incident.

Abstract

Title :

« Procedures management and danger consideration
when combined incidents occur :
Application to metro line supervision. »

During metro line operations, the supervision operator is responsible for the procedures' execution when referring to incidents management. However, when combined incidents occur, procedures may be competing. In this particular case, situations which do not ensure people's safety exist and an accident might happen.

Firstly, the approach of studying these procedures integrates their graphical representation with the BPMN notation. These procedures' models, understandable and accessible, provide a significant amount of knowledge for industrials in this area. Secondly, these models are performed as Petri nets to add dynamic to the system of interest. That is why, the notion of controllability and the influence of the execution context are introduced in the study of incidents management procedures.

To ensure people's safety, forbidden states are defined and identified among the states space with the supervisory control theory. These states are characterized in an original way : depending on their inclusion in a set of states but also depending on the controllability of their outgoing transitions. In addition to this innovative characterization, algorithms allow to determine and to avoid forbidden states.

Criteria distinguish the admissible sequences which avoid forbidden states. These differentiation criteria are defined to steer the supervision operator through the actions he has to execute when combined incidents occur. Results allow us to provide assistance to the supervision operator with warnings and advice.

This study is based on ATS supervision system developed by Thales and one of their customers' incidents management procedures, the RATP. A prototype of operator support functionality for incidents management based on customer know-how has been implemented into Thales software.

Key words : Supervision, Transport system, Supervisory control theory, Petri nets, BPMN, Dependability, Incidents management procedures.

Table des matières

Liste des figures

Liste des tableaux

Introduction

Sommaire

1. Préambule

Autrefois, les sociétés et les individus étaient soumis à des dangers de type naturel comme les épidémies, les tremblements de terre, les sécheresses ou des dangers de type humains comme les guerres et les incendies. La révolution industrielle au XVIII^{e} siècle a introduit dans nos sociétés une nouvelle forme de danger dont la portée dépasse la dimension d'un seul homme. Depuis, les risques industriels ont évolué avec les technologies et les besoins des sociétés.

Progressivement, les systèmes informatiques ont été introduits et se sont développés afin de faciliter l'exécution de certaines tâches réalisées auparavant par des humains. Il sont aujourd'hui omniprésents et se trouvent autant dans les systèmes de grande envergure comme des centrales nucléaires, des réseaux de télécommunication, que dans des systèmes de taille plus modeste, avion, automobile, systèmes de production, jusqu'aux systèmes de petite taille à grande diffusion comme les cartes à puce, les machines à café et les téléphones portables.

Ces systèmes informatiques fournissant à l'opérateur humain une assistance dans l'exploitation des systèmes industriels se rapporte à la supervision. Un système de supervision doit remplir les fonctions de surveillance, de pilotage, de traitement des alarmes et de visualisation. Il permet d'augmenter la fiabilité, la disponibilité et la sûreté de fonctionnement du système concerné. Ainsi, dans le cadre de la supervision, des informations peuvent être données à l'opérateur afin de le conseiller dans ces choix, ces systèmes sont alors appelés systèmes d'aide à la décision.

Le rôle d'un système d'aide à la décision est d'assister un utilisateur en vue de la réalisation d'une tâche par celui-ci. C'est un outil évolué mis à disposition des utilisateurs plutôt qu'un assistant. Il n'est pas autonome mais cherche à aider un opérateur dans ses activités quotidiennes.

Malgré l'existence de systèmes de supervision et d'aide à la décision dans les systèmes industriels complexes, des accidents se produisent. Ces accidents surviennent parfois à la suite d'une succession d'événements anormaux qui sont inhérents à l'exploitation. Ils constituent donc une source permanente d'interrogations et d'analyses pour améliorer la sécurité des personnes et des systèmes.

2. Exemples d'accident

Deux accidents, tristement célèbres, l'un dans le domaine du nucléaire datant de plus de 35 ans et l'autre plus récent dans l'avionique, illustrent bien cette combinaison d'événements ayant conduit à des conséquences graves. Les accidents survenant dans ces deux domaines industriels sont rares mais leur gravité et les dommages provoqués sont toujours importants.

L'accident nucléaire de Three Miles Island [IRS13] qui s'est produit le 28 mars 1979 est le plus important accident nucléaire s'étant déroulé aux États-Unis. Les causes qui ont mené à la fusion du cœur du réacteur sont une succession, estimé très improbable, d'erreurs de conception, d'erreurs humaines et de pannes matérielles. Ainsi, l'enchaînement d'une défaillance de matériel, d'une faute de maintenance non prévue à la conception, d'au moins deux erreurs de conception et de la non-validité de la procédure de conduite à la disposition des opérateurs a mené à l'accident. Bien que la fusion partielle du cœur du réacteur ait eu lieu, il y a eu aucun mort ni blessé et la contamination radioactive fut restreinte à la suite de cet accident nucléaire.

L'accident de Three Mile Island a été un tournant considérable dans le développement mondial de l'industrie nucléaire et dans l'approche des études de sûreté de fonctionnement. Suite à l'étude de cette catastrophe évitée de peu, les exigences en termes de conception, de systèmes de contrôle, de formation des personnels et de procédures d'urgence ont été fortement renforcées et améliorées. Malgré la mise en place de ces mesures, des événements naturels extrêmes peuvent encore conduire à des accidents nucléaires majeurs comme en mars 2011 à Fukushima au Japon [IRS14]. À la suite d'un séisme, un tsunami s'est déclenché provoquant la perte d'alimentation électrique générale et de secours ainsi que l'arrêt du système de refroidissement. Cette succession d'incidents a entrainé la fusion partielle des cœurs des réacteurs nucléaires et d'importants rejets radioactifs dans l'environnement Ce type d'enchainement d'événements conduisant à un accident peut également se produire dans des domaines industriels autres que le nucléaire.

La survenue beaucoup plus récente du second accident présenté impose de prendre des précautions par rapport aux conclusions d'enquêtes en raison du peu de recul existant à l'heure actuelle face à cette tragédie.

Dans la nuit du 31 mai au 1er juin 2009, l'Airbus A330 exploité par la compagnie Air France s'est abîmé dans l'océan Atlantique. L'avion a décollé pour effectuer le vol régulier AF 447 entre Rio de Janeiro et Paris Charles de Gaulle, douze membres d'équipage et 216 passagers étaient à bord. Suite à une situation de décrochage, l'avion a subi une collision avec la mer.

Dans le rapport d'enquête final paru en juillet 2012 [BEA12], le Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile (BEA) présente les circonstances de l'accident, la combinaison des facteurs pouvant les expliquer ainsi que les recommandations des mesures à mettre en place pour éviter un nouvel accident similaire.

Selon ce rapport, l'accident résulte de la succession des facteurs suivants :
- l'incohérence temporaire entre la vitesse réelle et la vitesse mesurée ;
- des actions inappropriées sur les commandes ;
- l'identification tardive de l'écart de trajectoire et la correction insuffisante par le pilote,
- la non identification par l'équipage de la situation de décrochage et l'absence d'action permettant de la récupérer.

Suite à cet accident, le Bureau d'Enquêtes et d'Analyses a adressé 41 recommandations de sécurité qui portent notamment sur les enregistreurs de vol, la formation et l'entraînement des

pilotes, l'ergonomie du poste de pilotage et le retour d'expérience opérationnel et technique.

Les successions d'événements prévus les uns indépendamment des autres mais pas leur enchainement conduisent le plus souvent à des conséquences graves et à des accidents. Des mesures de sécurité par retour d'expérience, comme la formation des opérateurs, sont souvent établis après le déroulement d'un accident pour éviter une nouvelle occurrence.

3. Questionnement

Ces deux accidents mettent en avant la difficulté pour des humains de gérer une succession d'événements anormaux se produisant dans un système industriel complexe. Cet enchainement de facteurs est déstabilisant surtout si aucune démarche n'est prévue en amont pour gérer leur combinaisons.

Aussi, les questions suivantes se posent :

- Comment déterminer les successions d'événements anormaux pouvant se produire lors de l'exploitation d'un système industriel et pouvant conduire à un accident avant que celui-ci ne survienne ?
- Comment aider les opérateurs humains confrontés aux enchainements d'événements anormaux ?
- Est-il possible de prévenir en amont les opérateurs des conséquences possibles de leurs actions ?
- Comment tenir compte de ces situations rares lors du développement des procédures de gestion d'incidents ?
- Existe-t'il des solutions pour éviter ce type d'accident ?

Les travaux développés dans ce mémoire s'inscrivent dans le domaine des transports et plus particulièrement celui d'un transport en commun, le métro. L'étude propose, dans les cinq chapitres suivants, une démarche de réflexion et des réponses aux questions posées.

4. Organisation du mémoire

Le premier chapitre de ce mémoire présente le contexte industriel de l'étude. Il introduit tout d'abord des notions générales sur la supervision d'une ligne de métro puis détaille les particularités de l'exploitation de ce système de transport en précisant également les conditions d'exploitation avec incidents. Afin de cadrer l'étude, son périmètre et ses postulats sont précisés à la fin du chapitre.

Pour situer l'étude dans la communauté scientifique, le deuxième chapitre est quant à lui consacré à la présentation des recherches effectuées précédemment sur les différents thèmes abordés dans ce mémoire. Les problèmes traités sont ensuite développés ainsi que les objectifs recherchés. Le positionnement choisi et la démarche d'étude entreprise par la suite sont donnés en conclusion.

Le troisième chapitre présente la première partie de la démarche : la représentation et la modélisation des procédures de gestion d'incidents. Pour cela, le savoir-faire acquis est tout d'abord analysé. En se basant sur des descriptions textuelles, une représentation graphique et standardisée des procédures est réalisée. Ces procédures sont ensuite modélisées en les intégrant à leur environnement d'exécution.

La seconde partie de la démarche, l'analyse et la maitrise du danger, est exposée dans le quatrième chapitre de ce mémoire. Les notions nécessaires à cette analyse sont introduites au préalable et le vocabulaire employé est défini. Les solutions pour éviter un accident résultant d'une succession d'événements anormaux sont déterminées. De plus, une méthode pour aider et prévenir les opérateurs humains dans ces situations est proposée.

Le dernier chapitre de ce mémoire est consacré à une application de la démarche complète sur un exemple industriel réel. Ainsi, une combinaison de deux événements anormaux est étudiée dans le cadre de l'exploitation d'une ligne de métro. Cette mise en situation présente les solutions apportées pour prévenir et aider l'opérateur humain lors de cette situation et pour éviter un accident.

Enfin, la conclusion de ce mémoire donne un bilan des travaux et des apports réalisés. Les principales perspectives scientifiques et industrielles envisagées sont également exposées.

I Contexte industriel

Résumé

Pour gérer l'exploitation d'une ligne de métro, les industriels utilisent aujourd'hui des systèmes informatisés. Dans ce cadre, l'entreprise Thales développe une application ATS avec de nombreuses fonctionnalités pour superviser les lignes de métro. L'un de leurs clients, la RATP, est un exploitant expérimenté, notamment pour la gestion des incidents, qui a accepté de me transmettre son savoir-faire au cours d'une formation. Avec les connaissances acquises, le contexte ainsi que les postulats de l'étude ont ainsi pu être définis.

Sommaire

I.1 Supervision d'une ligne de métro

I.1.1 Présentation générale

Au cours du XIX^e siècle, la forte croissance économique et industrielle engendre une augmentation rapide de la population des villes. Le transport des personnes devient alors un élément crucial pour poursuivre le développement urbain. Afin de fluidifier le trafic des rues qui sont saturées, l'objectif est de construire un moyen de transport indépendant de cette circulation par voie souterraine ou aérienne. Un système de transport ferroviaire urbain de passagers est alors créé : le chemin de fer métropolitain, plus communément appelé métro. La première ligne est construite à Londres, puis dans plusieurs capitales mondiales, comme Paris, à la fin du XIX^e siècle. Le métro transporte des voyageurs dans les agglomérations urbaines avec une fréquence élevée de desserte et sur des distances de l'ordre de quelques kilomètres.

Le métro est un chemin de fer à traction électrique circulant en site propre uniquement, il n'y a pas de croisements avec d'autres moyens de transport. La plupart du temps, les voies de circulation sont en souterrain mais il existe également des parties aériennes où le métro circule sur des viaducs. Les voies admettent de faibles rayons de courbures grâce à la longueur des trains et de fortes déclivités existent.

Les trains sont des rames constituées d'automotrices commandées par le conducteur dans une cabine en tête du train pour les lignes non automatiques. La longueur des trains dépend des réseaux et varie suivant la capacité de transport voulue. Le roulement est effectué sur fer ou par pneumatiques suivant les caractéristiques géographiques de la ligne, les roulements à fer ne permettant pas de circuler sur des voies avec une déclivité importante.

Une ligne de métro est composée principalement de deux voies allant d'un terminus à un autre en desservant un certain nombre de stations plus ou moins distantes. En général, chacune des voies permet de parcourir la ligne dans un seul sens de circulation. Les portions de lignes comprises entre deux stations consécutives sont appelées interstations. Les terminus aux extrémités des lignes jouent un rôle administratif de gestion des conducteurs et du matériel roulant. Des voies de garage existent pour les rames dans ces terminus mais également dans certaines stations, terminus historiques de ligne avant extension. Des aiguillages ainsi que des emplacements de garage sont placés à divers endroits de la ligne pour le passage d'une rame d'une voie à l'autre en cas de problème.

Pour assurer leur mouvement, les métros actuels sont alimentés en énergie par le sol en courant continu de 600 à 750 V. Pour les lignes équipées de roulement à fer, l'un des rails de roulement est relié à la masse du courant de traction et l'énergie est distribuée par un troisième rail isolé. Pour les lignes accueillant des trains à roulement pneumatique, les deux rails de roulement sont doublés des guides verticaux, un de ces guides alimentant les trains en électricité. L'alimentation électrique des voies se fait en parallèle, ainsi, si le courant est coupé sur l'une des voies, les deux sens de circulation sont alors coupés.

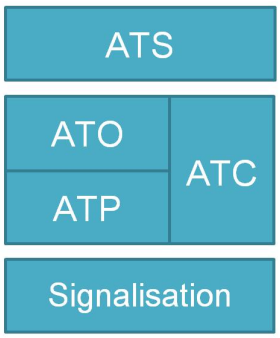
Pour assurer le suivi des trains tout au long de leur trajet et leur espacement, les voies sont découpées en portions de longueurs plus ou moins importantes. Ces portions de voies sont appelés Circuits De Voie (CDV). Un capteur équipe ces portions et informe de la présence ou non d'un train. La longueur d'un CDV est calculée en fonction de la distance de freinage maximale des trains pouvant circuler sur la voie. En effet, la sécurité ferroviaire repose sur ce cantonnement des voies en maintenant un espace suffisant entre deux trains et en ne laissant circuler qu'un seul

train par CDV. Un train est autorisé à circuler sur un CDV libre grâce à un système de dialogue sol-train appelé signalisation. Ces informations sont transmises aux conducteurs par des signaux dits d'espacement qui leur donne la possibilité de poursuivre ou non leur circulation.

La fréquentation des lignes de métro est globalement en constante augmentation et impose donc une fréquence des trains de plus en plus importante pour transporter les voyageurs et répondre à leur demande. Aujourd'hui l'enjeu est donc de réduire les intervalles entre chaque train pour diminuer le temps d'attente des voyageurs tout en assurant la sécurité des personnes. Cet enjeu a d'une part conduit à informatiser la gestion du mouvement des trains afin notamment de proposer un service au plus proche de la demande des voyageurs. D'autre part, un nouveau système de localisation a également été développé : le CDV devient alors mobile et évolue suivant la vitesse du train et l'occupation de la voie. Ainsi, l'intervalle de temps entre les trains est minimisé tout en garantissant une distance de freinage suffisante pour la sécurité. Par la suite, seule la partie concernant la supervision du mouvement trains sur la ligne sera étudiée.

I.1.2 Supervision informatique d'une ligne de métro

Depuis quelques années, la supervision d'une ligne de métro s'est transformée : l'activité de l'opérateur humain a été modifiée par le développement de systèmes informatiques de surveillance et de commande reposant sur une architecture à plusieurs niveaux (figure I.1.2). Ces différents niveaux sont en interaction les uns avec les autres afin de former un système global. Ainsi, l'ATS, *Automatic Train Supervision*, assure le contrôle de l'exécution de l'offre de transport en supervisant les systèmes d'acquisition et de commande directement reliés au terrain : l'ATC, *Automatic Train Control*, et la *Signalisation*.



La *Signalisation* gère l'acquisition et la commande des signaux et enclenchements terrain, elle empêche ainsi les mouvements de trains incompatibles dans les zones d'aiguillage. En effet, dans ces zones, les mouvements de trains sont plus risqués puisqu'ils peuvent changer de voie et donc se retrouver à contre sens de la circulation normale. Les enclenchements automatiques permettent ainsi d'éviter à deux trains de se retrouver face à face.

Le système de contrôle automatique des trains ATC assure la mise en sécurité du système et le pilotage automatique des trains. Il est composé de deux sous-systèmes : l'ATP, *Automatic Train Protection*, et l'ATO, *Automatic Train Operation*.

Le système automatique de protection des trains ATP protège les passagers, le personnel et les équipements contre les principaux dangers liés à la circulation ferroviaire (collisions entre trains, survitesses, déraillements). Le système active le freinage d'urgence en cas de non-respect de l'espacement entre les trains, de non-respect de signaux, de vitesses non compatibles avec un

arrêt avant un CDV occupé. Les fonctions de l'ATP sont des systèmes informatisés à très haut niveau de sécurité.

Le système ATO assure le pilotage des trains, il contrôle le profil de vitesse afin de respecter les horaires prévus pour la journée d'exploitation et gère ainsi les arrêts programmés et le respect du temps d'arrêt dans les stations. Dans le cas d'une ligne de métro automatique, sans conducteur, il gère également l'ouverture et la fermeture des portes et redémarre le train. Les fonctions de l'ATO ne sont pas réalisées en sécurité, la sécurité reposant sur l'intervention de l'ATP en cas de défaillance de l'ATO. Par exemple, si l'ATO provoque une accélération intempestive, l'ATP, qui contrôle le respect des limitations de vitesse, va déclencher un freinage d'urgence pour assurer la sécurité du train. L'approche sécurité de l'ATC considère comme possible une défaillance de l'ATO, la sécurité reposant sur les fonctions de l'ATP.

L'*Automatic Train Supervision*, ATS, est quant à lui le système informatique en charge de la gestion centralisée et automatisée du trafic de la ligne de métro et du contrôle de l'exécution de l'offre de transport. L'ATS assure la surveillance et la régulation de l'ensemble des sous-systèmes qui composent le système, du suivi des circulations et de l'état des enclenchements aux informations délivrées aux passagers afin de garantir une offre de transport au plus proche des horaires théoriques prévus. L'ATS est l'interface entre les opérateurs en charge de la supervision de la ligne et le système à contrôler en les assistant dans leurs tâches quotidiennes : contrôle et commande des équipements et gestion avancée de l'exploitation. Les fonctionnalités offertes par les ATS varient suivant les industriels fournissant le système et les besoins des exploitants de métro [Tha11a].

L'étude développée dans cette thèse porte sur la supervision d'une ligne de métro, le système ATS, le plus haut niveau dans l'architecture informatique de la gestion d'une ligne. Une présentation plus détaillée du système et des fonctionnalités proposées par l'ATS développé par Thales est donnée dans la partie suivante.

I.1.3 Application ATSsoft de Thales

Société Thales

Implantée dans plus de cinquante pays, la société Thales compte près de 65 000 collaborateurs. Ces activités de hautes technologies se répartissent dans cinq grandes divisions : l'Aéronautique, l'Espace, la Défense, la Sécurité et le Transport terrestre. Leader mondial des systèmes de transport intégrés, Thales est présent dans trois domaines : la signalisation ferroviaire grandes lignes et urbaine, les systèmes intégrés de communication et de supervision et les systèmes de billettique. Dans le cadre de ses activités de supervision, Thales développe une application ATSsoft pour la gestion du trafic de métro.

Thales a installé son premier système ATS de supervision d'une ligne de métro à Mexico en 1968 et possède donc un savoir-faire notable dans ce domaine. Entre les années 70 et 90, l'ATS de Thales a ensuite été mis en service chez des clients historiques en Amérique du Sud (Chili, Venezuela). À Santiago du Chili, une ligne de métro avec 49 trains transporte 1,5 millions de voyageurs par jour. Au début des années 2000, Thales obtient des contrats importants à Singapour puis Bruxelles et Athènes. Dernièrement, de nouvelles lignes de métro ont été mises en service à Saint-Domingue et Panama.

En France, les lignes 13, 3, 5 et 12 de la RATP à Paris sont supervisées par des systèmes ATS de Thales. La ligne 13 possède une configuration complexe avec notamment une séparation de la ligne à l'une de ses extrémités en deux branches de longueurs différentes. Dans ces conditions, le système permet à 500 000 usagers par jour de voyager sur la ligne parcourue par 53 trains en heure de pointe.

En opération depuis plus de 40 ans, la solution de gestion avancée de trafic ATSsoft de Thales permet de répondre aux différents niveaux de besoins de l'exploitation d'une ligne de métro.

Présentation de l'application ATSsoft

Pour assurer la gestion d'une ligne de métro, les opérateurs sont regroupés dans un centre de commande et contrôle et sont confinés à des tâches de surveillance dans la majeure partie de leur activité. Trois opérateurs sont au minimum nécessaires pour superviser une ligne de métro utilisant le système ATS développé par Thales, deux opérateurs gérant les terminus d'extrémités et un opérateur pour la ligne. Un écran panoramique leur donne une vision d'ensemble du système avec une représentation symbolique de la ligne comprenant notamment les positions des trains et l'état d'alimentation en courant. À son poste de travail, un opérateur dispose également de plusieurs écrans lui permettant d'obtenir des vues détaillées de la ligne et des représentations graphiques des tables détaillant les horaires des trains sur la ligne. Il peut ainsi intervenir sur le système en modifiant la circulation des trains, coupant l'alimentation électrique ou arrêtant par exemple un train en station.

L'application ATSsoft propose de nombreuses fonctionnalités au travers d'une interface intuitive :

- Des fonctions avancées de régulation et la gestion temps réel des conducteurs,
- La conception, l'optimisation et la gestion des tables horaires,
- La simulation de scénario et la formation des opérateurs.

Une partie de ces fonctionnalités [Tha11b] est gérée de manière automatique, d'autres fonctionnalités sont également proposées aux opérateurs comme aide à l'exploitation pour améliorer l'offre de transport. La représentation symbolique suivante de la ligne présente ces principales fonctionnalités (figure I.1).

Fonctionnalités automatiques

L'ATS acquiert les informations remontant des équipements terrains et les modélise dans une base de donnée temps réel, ces informations étant ensuite nécessaires pour les calculs. Par l'intermédiaire de boîtes de dialogue, les opérateurs de supervision peuvent également commander certains équipements tels que les feux d'autorisation de départ de station ou les aiguillages à travers le tracé des itinéraires des routes à suivre par les trains.

En début de journée, la table horaire souhaitée est chargée et correspond à la demande prévisionnelle des usagers. Cette table forme ainsi le programme d'exploitation voulu de la ligne de métro. L'ATS propose une représentation graphique de ce programme d'exploitation actualisée en temps réel en fonction des données de trafic et des trains, des conditions de circulation et des écarts mesurés.

Le module de suivi des trains est essentiel dans l'application. À partir des acquisitions terrains, des algorithmes déduisent la position des trains en ligne et dans les zones de manœuvre

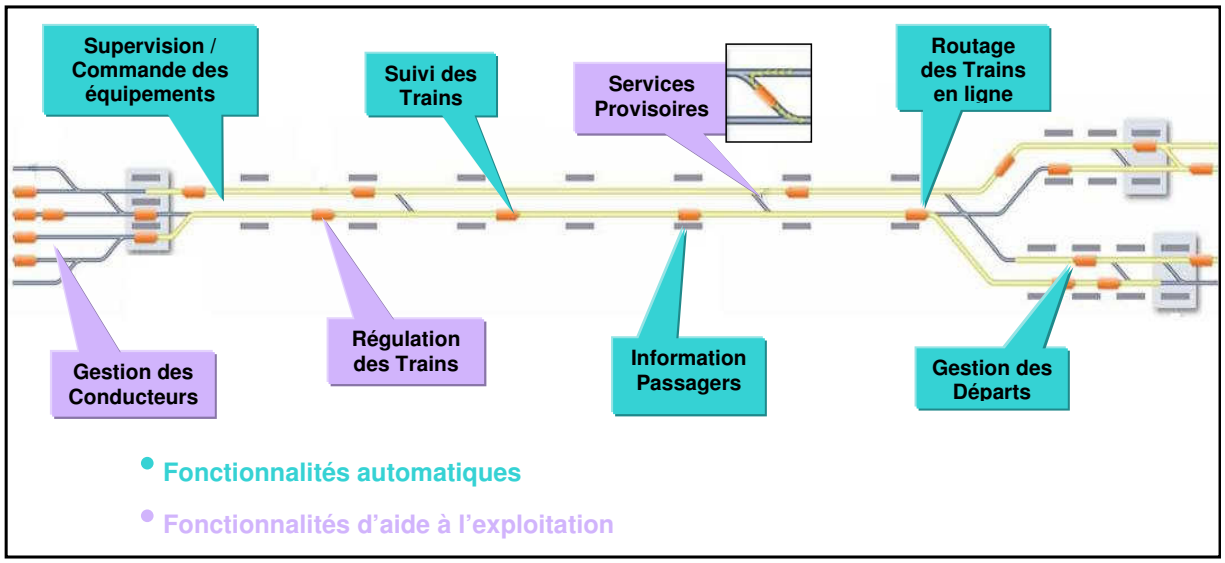


Figure I.1 – Fonctionnalités ATSsoft

ainsi que leur identification. Le routage gère la mise en mouvement des trains sur la ligne de manière automatique et centralisée. Il vérifie la conformité avec l'itinéraire prévu et résout d'éventuels conflits de priorité. La gestion des départs commande le cadencement des trains et assure le respect de l'ordre de marche lors de l'injection des trains sur la ligne.

Sur les quais de chaque station, des informations sur les prochains trains attendus sont affichées en temps réel à l'intention des passagers, telles que le temps d'attente, les retards ou la destination.

Fonctionnalités d'aide à l'exploitation

En plus de la supervision et du contrôle des trains, ATSsoft fournit aux opérateurs des fonctions de régulation avancées du trafic comme la ponctualité, la régularité, l'économie d'énergie et la gestion temps réel des conducteurs.

La régulation consiste, d'une part, à assurer que le trafic soit conforme au plan de transport théorique (horaires et intervalles prévus) et, d'autre part, à traiter les événements qui perturbent le fonctionnement normal de l'exploitation d'une ligne de métro. Il existe deux types de régulation : la régulation en terminus qui veille au respect de l'horaire de départ et à la fluidité prévisionnelle du trafic. La régulation en ligne, quant à elle, veille au respect des heures de passage prévues en station et à la fluidité générale du trafic en appliquant les corrections sur le temps de stationnement et l'allure des trains. La régulation peut avoir comme objectif de respecter au mieux l'horaire théorique d'un train (mode horaire) ou de conserver un intervalle constant entre les différentes circulations de trains (mode intervalle).

La gestion des conducteurs est un module optionnel de l'application qui pilote en temps réel l'affectation des conducteurs sur les trains et gère leur temps de repos.

Les services provisoires (figure I.2) sont des boucles indépendantes mises en place suite à des incidents et qui font circuler les trains sur une partie de la ligne. Ainsi la circulation n'est pas interrompue sur l'ensemble de la ligne et une partie des stations est desservie. Pour cela, une

série d'aiguillages fait passer les trains d'une voie à l'autre en dehors des terminus. L'ATS met alors à jour automatiquement le programme d'exploitation pour conserver l'ordre réel des trains sur la ligne.

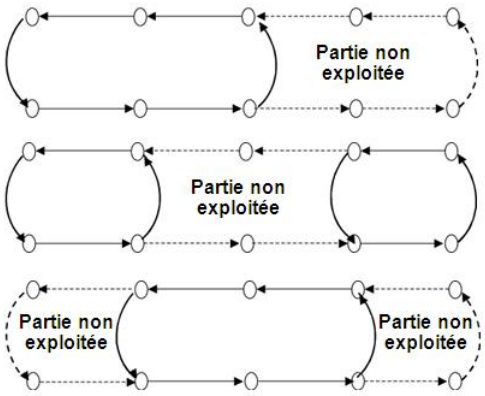


FIGURE I.2 – Trois exemples de service provisoire

Interface Homme Machine IHM

L'ensemble des informations acquises et calculées par l'ATS est transmis aux opérateurs au travers d'une interface dédiée [Tha11c] représentant d'une part l'état de la ligne et d'autre part le programme d'exploitation. L'image de la ligne donne aux opérateurs les informations sur la position des trains, les routes tracées par la position des aiguillages, l'état des signaux ainsi que l'état d'alimentation des différentes parties de la ligne. Le bandeau supérieur met en évidence les alarmes détectées en différenciant leur importance par un code de couleur. Cette image offre une vue globale de la ligne pour visualiser la position de l'ensemble des trains à un moment donné et permet donc de se faire une impression globale de la fluidité du trafic (figure I.3). Il est également possible d'obtenir des vues détaillées centrées sur chaque station pour avoir plus d'informations sur la station sélectionnée (figure I.4).

La deuxième représentation disponible pour les opérateurs est celle du programme d'exploitation (figure I.5). Il est affiché sous forme graphique où des modules représentent les circulations des trains passées, en cours ou futures à l'arrivée et au départ d'un terminus. Cet outil de visualisation est mis à jour en temps réel en prenant en compte les effets de la régulation. Il informe, au travers de l'inclinaison des liens entre les différents modules, des avances ou retards des trains par rapport à leur horaire théorique. Une interface intuitive permet aux opérateurs de résoudre des problèmes en intervenant directement sur les circulations des trains (ajout, suppression, déclassement) au travers de boîtes de dialogue.

Le programme d'exploitation est également représenté sous forme de graphe espace-temps et apporte ainsi un angle complémentaire dans la visualisation de l'état de la ligne. Cette représentation met en avant d'éventuels conflits qui pourraient apparaître entre les circulations. (annexe A)

Fonctionnalités avancées

ATSsoft s'intègre avec d'autres systèmes (SCADA, Web Services) et, grâce à son architecture, s'interface avec tout type de signalisation. L'application offre également la possibilité de réduire

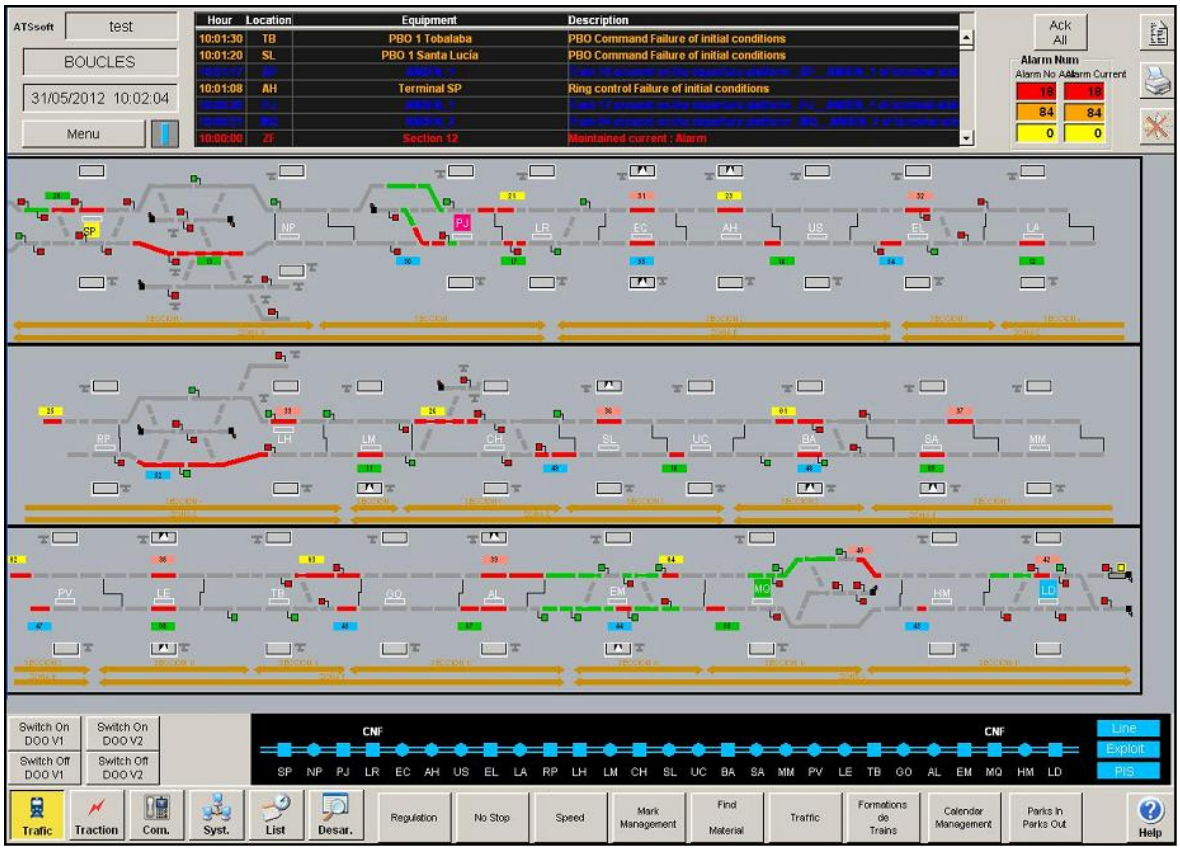


Figure I.3 – Image de la ligne - poste opérateur

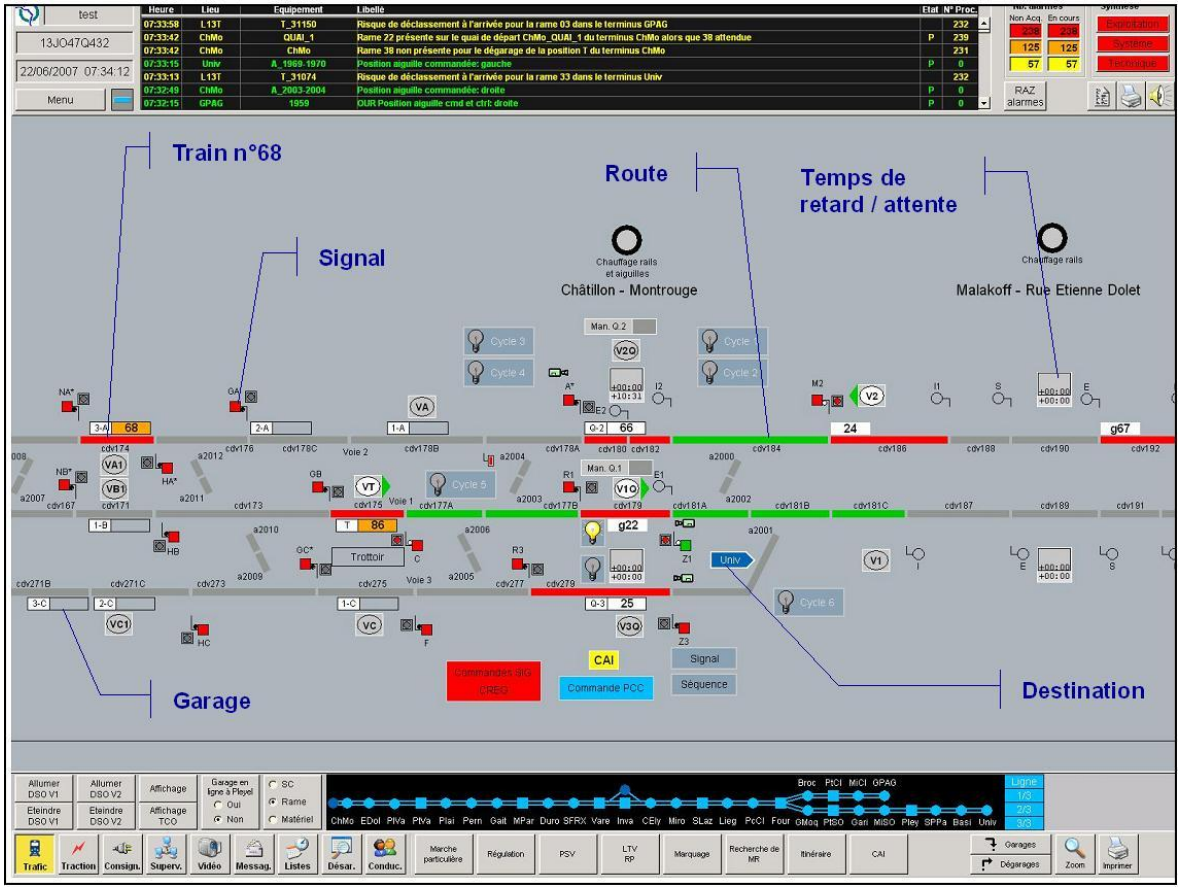


Figure I.4 – Image de la ligne, vue de détail - poste opérateur

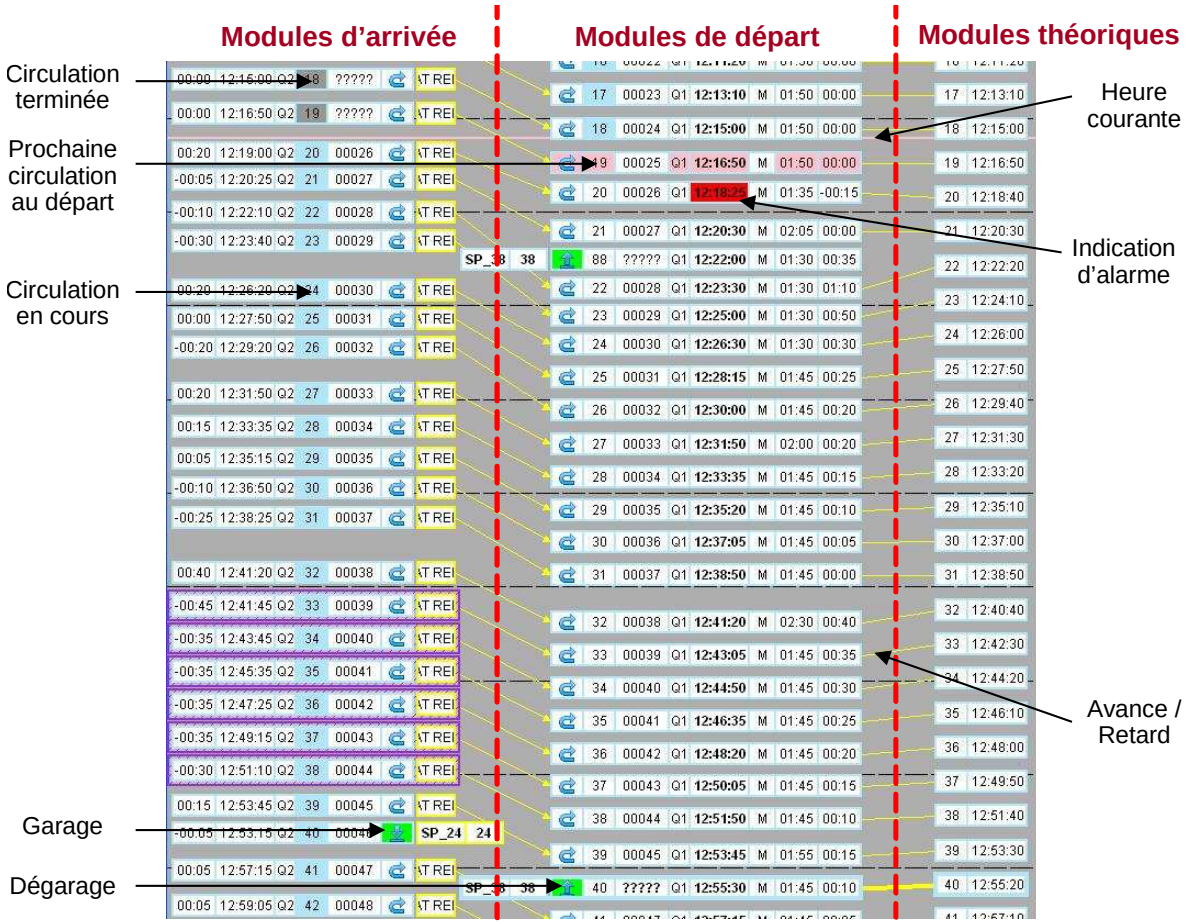


FIGURE I.5 – Programme d'exploitation

la consommation d'énergie électrique en optimisant en temps réel la vitesse des trains et la récupération de l'énergie lors du freinage. Une optimisation hors ligne détermine la table horaire théorique la plus économique, tandis que l'optimisation en ligne gère les trains en temps réel en prenant en compte les conditions de trafic. Il existe également un outil de création de scénarii qui simule les mouvements des trains et les conditions de signalisation à des fins de formation des opérateurs.

La RATP est l'un des clients les plus importants de Thales et possède une maturité et une expérience reconnues dans l'exploitation de ligne de métro. La section suivante présente de manière plus détaillée la gestion par la RATP du réseau de métro à Paris dans les situations nominales et lors de l'occurrence d'incidents.

I.2 Exploitation d'une ligne de métro à la RATP

I.2.1 Présentation du réseau de métro parisien géré par la RATP

Dès le XIX^{e} siècle à Paris, l'objectif de la municipalité est de désengorger les rues et de relier un grand nombre de quartiers : la première ligne de métro est inaugurée en 1900. Aujourd'hui le métro de Paris se caractérise par sa densité : les seize lignes existantes sont très rapprochées et interconnectées pour faciliter le déplacement des voyageurs. Dans le réseau, un grand nombre

de rames, entre 600 et 700, peuvent circuler en même temps avec un intervalle entre deux trains minimum de 90 secondes en heure de pointe.

Principales caractéristiques

À Paris, chaque ligne de métro est séquencée de deux manières différentes pour faciliter son exploitation, il existe tout d'abord un découpage par zones qui concerne l'alimentation électrique. Les rails traction d'une ligne sont segmentés en sections, sous-sections et sections élémentaires pour pouvoir isoler électriquement la totalité ou une portion de la ligne par une commande à distance ou locale. Une section est une portion de ligne englobant entre quatre et six stations. Ce découpage permet la mise en sécurité des personnes, des équipements électriques et du matériel roulant face aux dangers électriques ainsi que la poursuite de l'exploitation sur les parties alimentées. Par ailleurs, en cas de danger immédiat, l'alimentation électrique de la ligne complète ou d'une section de la ligne peut être coupée en urgence.

L'autre segmentation, beaucoup plus fine, en CDV se fait en fonction de la configuration de la ligne à la RATP. Ainsi, un canton peut représenter une distance maximale de 300 m en ligne droite ou 100 m voire 50 m selon le profil de la voie, une voie sinueuse nécessitant plus de signaux donc des cantons plus petits. Un CDV est donc inclus dans une section élémentaire d'énergie électrique. Une rame, mesurant 75 m de longueur, peut parfois occuper jusqu'à trois CDV simultanément.

Les rames circulent sur la voie de droite contrairement aux trains du réseau national français et la vitesse maximale est de l'ordre de 70 km/h. La vitesse d'une rame est optimisée afin de minimiser la consommation d'énergie en accélérant au départ de la station et en arrivant à la suivante en roue libre, pour limiter ainsi le freinage.

Chaque ligne est équipée d'un système de pilotage automatique (PA) permettant la régulation automatique de la vitesse du train selon le CDV, ainsi que le respect automatique de la signalisation. En choisissant ce mode de conduite, le conducteur actionne seulement la fermeture des portes en station et le départ des trains. Sa principale fonction est alors d'assurer la surveillance du mouvement du train et de gérer les avaries. À l'heure actuelle, deux des seize lignes, 1 et 14, sont même complètement automatisées et circulent sans conducteurs. Afin de remplacer la vision et la surveillance du conducteur sur ces deux lignes, de nombreuses caméras sont disposées le long de l'ensemble des quais ainsi que dans les rames.

Des feux de signalisation, appelés Départ Sur Ordre (DSO), sont installés en sortie de chacun des quais. S'il est allumé, le conducteur n'a pas l'autorisation de quitter la station et doit attendre son extinction pour reprendre sa marche. L'opérateur en charge de la supervision peut ainsi bloquer la rame en station en cas de problème sur la ligne ou pour réguler l'intervalle entre les trains.

La spécificité de la RATP est de rendre presque autonome chaque ligne de métro. Ainsi, le matériel roulant et le personnel sont propres à chaque ligne.

Fonctions des personnels

En moyenne 170 conducteurs travaillent sur chaque ligne. Dans les terminus, et plus précisément dans un poste de manœuvre local (PML), un agent de manœuvre est chargé des aiguillages

lors des déplacements des rames sur cette zone de la ligne. Un agent gradé et polyvalent est également présent, capable de conduire un train et prêt à se déplacer en cas de problèmes à proximité du terminus dont il dépend. Les chefs de départs sont responsables de la gestion des trains en terminus et de leur entrée sur la ligne.

Dans chaque station, un agent commercial est en charge de l'accueil, de l'information, du contrôle, de la vente de titres de transport et de la relation avec les clients. Il est formé à la notion de courant de traction sans toutefois être habilité à descendre sur les voies.

Des agents sont chargés de la maintenance et de l'entretien des installations tout le long de la ligne. Une fois que le service voyageur est terminé sur la ligne, les services de maintenance de la RATP réalisent les travaux nécessaires à son bon fonctionnement. Ces travaux se déroulent donc la nuit, pendant les cinq heures sans circulation, et nécessite une gestion de l'alimentation en traction de la ligne.

Les opérateurs de supervision, ou chef de régulation (CREG), travaillent depuis des centres de contrôle appelés postes de commande et de contrôle centralisés ou PCC à la RATP. Le chef de régulation a cinq grandes missions sur la ligne dont il a la charge :

- assurer la régularité du trafic,
- gérer l'énergie électrique de traction.
- traiter les incidents d'exploitation,
- participer à l'information des agents et des voyageurs en cas de perturbation,
- rédiger un rapport journalier sur l'exploitation de la ligne,

Les communications entre les conducteurs et le chef de régulation se font par Téléphone Haute Fréquence (THF). Ces communications donnent au CREG une vision complète de la ligne, reflétant ainsi la réalité du terrain.

La permanence générale est une structure pour la veille opérationnelle de l'ensemble des réseaux de la RATP (lignes de métro, RER et bus). Elle supervise et coordonne les informations afin d'alerter les usagers en cas de problèmes sur le réseau et mobiliser les services intervenant sur le réseau. Le Permanent des Réseaux Ferrés (PRF) est plus particulièrement responsable de cette coordination entre l'ensemble des lignes de métro.

Formation pour le poste de CREG

Le poste de chef de régulation est le poste à plus hautes responsabilités dans l'exploitation d'une ligne de métro à la RATP. Les personnes accédant à ce poste justifient en général d'une dizaine d'années d'expérience à la RATP et sont, la plupart du temps, d'anciens conducteurs connaissant donc les problèmes pouvant survenir sur une ligne de métro et familiarisés avec l'exploitation d'une ligne de métro et ses règles.

Une formation de deux mois est proposée, par groupe de six, aux personnes souhaitant obtenir la qualification pour ce poste. Cette formation s'organise en plusieurs phases : cours théoriques, mises en situation sur un simulateur de ligne et journées d'observation de supervision de lignes réelles. Au cours de la formation, six semaines sont consacrées à la gestion d'une ligne pendant la journée d'exploitation et deux semaines pour l'apprentissage de la supervision des travaux réalisés au cours de la nuit. La formation se termine par un examen pour valider les compétences acquises.

Grâce à la volonté et l'intérêt porté à mes recherches de deux formateurs de la RATP, j'ai pu participer en tant qu'auditrice libre à cette formation. Pour la première fois, un salarié

de la société Thales a pu s'instruire et échanger librement avec la RAPT, le principal client, sur la gestion des incidents pendant l'exploitation d'une ligne de métro et le rôle du chef de régulation. Le temps qui m'a été accordé est représentatif de la bienveillance de la RATP pour mon étude puisque j'ai passé deux mois à temps plein à la fin de ma première année de thèse dans leurs locaux. Cette formation m'a permis d'acquérir une grande partie des connaissances métier nécessaires pour la réalisation de cette thèse. Cette occasion unique a ainsi apporté à l'ensemble des participants un approfondissement de sa culture de l'exploitation d'une ligne de métro.

Deux types de PCC

À l'origine centralisés boulevard Bourdon à Paris (Métro Bastille), les PCC sont en cours de décentralisation auprès de leurs lignes respectives et de modernisation. En 2014, sept lignes sont supervisées à partir de PCC dits décentralisés alors que les neuf autres lignes sont gérées à partir du PCC centralisé de Bourbon. Les PCC des lignes 4 et 13 ont été délocalisés les premiers, respectivement fin 2001 et fin 2006. Le PCC de la ligne 14, sans conducteur, a été construit en 1998 en même temps que la ligne et est installé à Bercy.

Le PCC centralisé de Bourdon regroupe dans deux grandes salles la gestion de neuf lignes, chacune des lignes étant gérée par un chef de régulation (CREG). Une seule personne suffit par ligne pour la surveillance des deux sens de circulation. Il dispose d'un Tableau de Contrôle Optique (TCO) lui donnant une vision complète de la position des trains sur la ligne (occupation des CDV), de la position des aiguillages, de l'aspect des signaux de manœuvres ainsi que de l'état d'alimentation des sections. Les interrupteurs de coupure de courant par sections sont également situés sur ce TCO.

Les nouveaux PCC (figure I.6) proposent une organisation très différente, ils rassemblent le PCC et les deux postes de manœuvres des terminus dans une même salle pour la gestion du trafic en ligne et de la gestion des départs des terminus. En 2014, les PCC des lignes 3, 5 12 et 13 sont équipés avec le logiciel ATS de Thales pour la supervision de ces lignes. La mise en place de ce nouveau type de salle de contrôle relocalise les centres de régulation au plus près de la ligne et regroupe l'ensemble des intervenants dans une même pièce. Cette nouvelle organisation permet également une gestion plus globale des incidents.

I.2.2 Exploitation avec incidents

Contexte avec incident

Pour répondre à une augmentation constante du nombre de ses usagers, la RATP renforce son service en proposant une fréquence de trains de plus en plus importante. Par conséquent, le matériel est sollicité de manière plus régulière et le nombre de personnes présentes sur le réseau est en hausse. Ces facteurs sont en partie responsables des incidents se produisant quotidiennement et dans des situations variées sur les lignes de métro. Ces incidents ont des répercussions sur l'offre proposée aux usagers en ralentissant la circulation des trains sur la ligne. Ils peuvent également avoir un impact sur la sécurité des personnes, provoquer des dommages corporels sur les voyageurs et le personnel ainsi que des dégâts matériels.

Une ligne de métro fait intervenir différents systèmes multipliant ainsi les types possibles d'incidents. Ainsi, un incident informatique peut se produire sur le poste opérateur du chef de

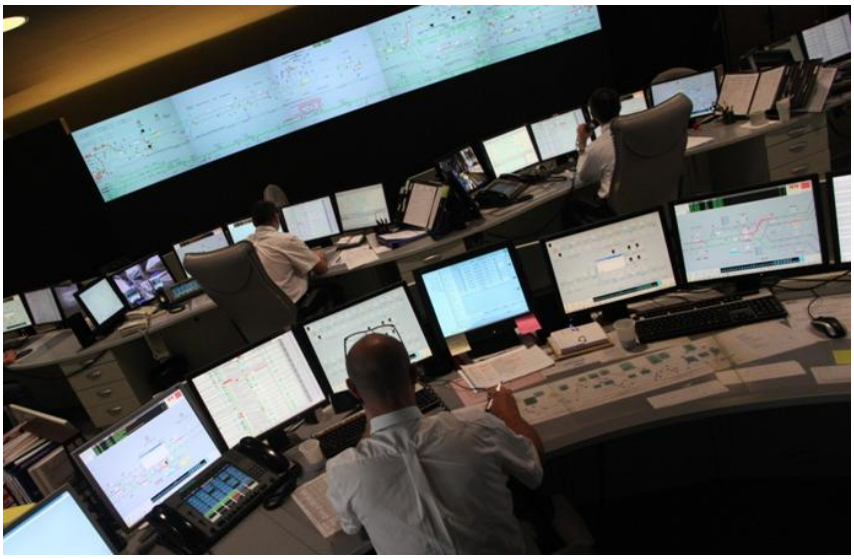


FIGURE I.6 – PCC Ligne 13 - Paris

régulation l'empêchant alors de superviser le trafic de la ligne. Ce problème peut être lié au serveur du système informatique ou à la perte des acquisitions et des communications avec le terrain. Le bâtiment dans lequel se situe le PCC est également une source d'incidents : problème d'alimentation électrique ou incendie par exemple. Cependant, la majeure partie des incidents perturbant l'exploitation d'une ligne de métro se produit directement sur le terrain et est ainsi liée à l'exploitation même de la ligne. **Par la suite, seul ce type d'incidents sera étudié**.

Quand un incident lié à l'exploitation se produit, l'opérateur de supervision doit reprendre le contrôle des opérations et reste le seul décisionnaire des mesures d'urgences à prendre. Il est responsable de la sécurité des personnes présentes sur la ligne ainsi que du retour au plus tôt à une exploitation normale de la ligne. Il se trouve alors dans un environnement stressant au vue de ses responsabilités, intensifié par des contraintes extérieures. Ainsi, le nombre et la diversité des personnes présentes sur la ligne sont grandes : des usagers, conducteurs, agents de maintenance et agents en station, aux pompiers en cas d'incendie ou policiers pour des interpellations ou des enquêtes. De plus, sa vision et sa compréhension de la situation se déroulant sur la ligne se font à partir de communications avec les conducteurs et les agents de terrain présents, il n'a pas une visualisation directe de la situation de l'ensemble de la ligne. Ces échanges doivent donc être précis et structurés pour que les actions de l'opérateur soient en adéquation avec la situation. Ces contraintes sont à prendre en compte pour appréhender les responsabilités de l'opérateur de supervision en cas d'incident.

Dans tous les cas, les superviseurs s'efforcent, après la mise en sécurité des personnes, de réduire au minimum la zone où le trafic est impacté par l'incident afin de diminuer la gêne occasionnée aux voyageurs.

Gestion des incidents

Pour gérer les incidents liés à l'exploitation, la RATP prévoit et développe des réactions adaptées dépendant de la gravité de la situation et conçoit des mesures de sécurité à prendre. Il est important de différencier la gestion de l'incident et la gestion des impacts d'un incident sur le trafic et l'exploitation de la ligne. Suite à un incident lié à la sécurité, la circulation des

trains est perturbée et ne permet souvent pas d'offrir un service normal et adapté aux usagers. Le chef de régulation va alors réaliser des adaptations de l'exploitation afin que l'impact sur le trafic soit minimisé.

Pour gérer les incidents à proprement parler, une procédure définit l'ensemble des étapes à suivre et des actions à réaliser par l'opérateur. Trois types de procédures sont mises en place par la RATP : les procédures conducteurs, les procédures génériques et mémorisées par les chefs de régulation et les procédures spécifiques décrites dans un document de référence pour les chefs de régulation.

Les procédures conducteur sont regroupées dans un livret présent dans la cabine de conduite de chacun des trains. Ces procédures détaillent les actions à réaliser par le conducteur, avec l'accord du chef de régulation, en cas d'incident sur le matériel roulant. Le conducteur se réfère notamment à ce livret lorsqu'une avarie est signalée par un voyant dans sa cabine ou lorsque l'un des freins reste serré.

Pour les chefs de régulation, deux types de procédures existent : les génériques et mémorisées de type réflexe nécessitant un traitement dans les plus brefs délais afin de garantir la sécurité des personnes et les procédures décrites dans un document de référence, spécifiques à la topologie de chacune des lignes. Ce second type de procédures permet ainsi d'éviter de commettre une erreur lors de leur déroulé. Elles s'appliquent, par exemple, pour des problèmes d'aiguillages dans les terminus et détaillent l'ensemble des règles de sécurité à vérifier et la position de l'aiguillage à commander. Ces procédures prennent en considération le sens de parcours de l'aiguillage, l'état des signaux concernés et la position de l'aiguillage. Il existe ainsi des procédures spécifiques pour déterminer la cause de court-circuits persistants sur l'énergie électrique de traction.

Les procédures génériques et mémorisées par les chefs de régulation concerne la sécurité des personnes, ces procédures sont assez courtes et donc facilement mémorisables et répétables par les opérateurs. Par exemple, les conditions de reprise de la marche suite à un incident matériel sont mémorisées, tout comme la procédure de mise hors tension d'urgence.

Les deux premières parties de ce chapitre ont présenté le cadre de la supervision d'une ligne de métro : le vocabulaire utilisé, les fonctionnalités informatisées existantes, la solution ATS développée par Thales et l'exploitation des lignes à la RATP à Paris. L'étude effectuée ne traite pas de l'intégralité de la supervision d'une ligne de métro mais se focalise sur les procédures mémorisées développées par la RATP pour la gestion d'un type d'incidents. La partie suivante situe le périmètre de la recherche en exposant le contexte, les postulats et le cadre commerciale de la thèse.

I.3 Périmètre de l'étude

I.3.1 Contexte d'étude

L'étude présentée dans ce mémoire se base sur l'application ATS de Thales développée pour des exploitants pour la supervision de lignes de métro. Suivant les objectifs d'exploitation, les coutumes et habitudes du client, la configuration et l'utilisation du logiciel varient. L'étude se base sur la société RATP, exploitant du réseau des transports urbains de Paris, comme client référence. Comme décrit précédemment (section I.2.1), il existe deux types de centre de commande et contrôle (PCC) pour la gestion d'une ligne de métro à Paris. Une gestion

dite centralisée regroupant plusieurs lignes en un même lieu, et une gestion décentralisée et modernisée, rendant les lignes indépendantes les unes des autres. Seules les lignes modernisées utilisent l'application ATS développée par Thales pour gérer leur trafic, l'étude sera donc limitée à ce type de PCC.

La ponctualité et la fréquence des trains sont optimisées par l'ATS pour offrir le meilleur service possible aux passagers. Ces fonctionnalités sont automatiques et proposent une gestion satisfaisante du trafic. Elles ne seront pas étudiées par la suite car elles répondent aux demandes des exploitants et ne nécessitent pas aujourd'hui d'améliorations. L'étude se focalise donc sur la gestion des incidents pouvant se produire lors de la supervision d'une ligne de métro et concernant la sécurité des passagers et du personnel.

Parmi l'ensemble des incidents pouvant se produire dans le cadre de l'exploitation d'une ligne de métro (section I.2.2), seuls les incidents liés directement à l'exploitation de la ligne seront considérés. Pour gérer ce type d'incidents, il existe plusieurs types de procédures se différenciant par la personne les mettant en exécution ainsi que leur support de transmission. L'étude se concentrera sur les procédures exécutées et mémorisées par l'opérateur responsable de la supervision, le chef de régulation à la RATP.

L'étude se focalise donc sur les procédures de gestion d'incidents mémorisées par les opérateurs de supervision à la RATP. La mise en œuvre de ces procédures nécessite d'être en interaction avec le logiciel de supervision ATS de Thales et des évolutions semblent être réalisables dans ce cadre.

I.3.2 Postulats de l'étude

Dans ce contexte d'étude, plusieurs postulats ont été définis afin de préciser et limiter le périmètre de recherche de la thèse.

L'étude repose sur la supervision d'une ligne de métro lors de l'occurrence d'incidents. Un incident peut apparaître à tout moment et de manière incontrôlée sur une ligne de métro. En effet, rien ne peut empêcher un incident de se produire et donc interdire son apparition. Dans une situation avec incident, il existe un danger pour les personnes présentes pouvant conduire à un accident potentiel. Pour les protéger des incidents et éviter les situations où il existe un danger, il faudrait pouvoir assurer une sécurité absolue du système. Cependant, une sécurité absolue reviendrait à un système non disponible dans lequel aucune action serait réalisable et le système ne pourrait donc pas évoluer. Les incidents doivent donc être considérés pour l'étude du système réel.

Pour protéger les personnes et le matériel à la suite de l'occurrence d'un incident, des procédures existent et sont mises en œuvre à la RATP. Chacun des incidents est associé à une procédure exécutée dans un contexte particulier, celui de l'incident. Une procédure donne les actions à réaliser et permet ainsi de réagir lors de l'occurrence d'un incident se produisant sur une ligne de métro. La procédure gère alors l'incident de manière individuelle, sans tenir compte d'autres incidents éventuels. Les procédures analysées par la suite ont été apprises lors de la formation des chefs de régulation. Ainsi, ces procédures sont celles utilisées quotidiennement sur le réseau de métro de la RATP depuis de nombreuses années. Ces procédures sont donc sûres par usage et par expérience lors de l'exécution d'une seule procédure. De plus, ces procédures ont été développées afin de prendre en compte les incidents de leur apparition à leur dispari-

tion. L'opérateur de supervision pourra toujours exécuter une procédure et réaliser les actions préconisées jusqu'à la disparition de l'incident initialement géré.

L'opérateur humain de supervision met en œuvre des procédures et suit le déroulement des actions qui lui sont proposées. Aucune action n'est accomplie sans l'intervention de l'opérateur, il reste le seul décisionnaire des actions qu'il réalise. L'application des procédures repose donc sur des compétences humaines et les propres décisions de l'opérateur. Lors de l'étude, les erreurs humaines ne seront pas prises en considération. L'opérateur suit les procédures recommandées et respecte les réglementations de la sécurité ferroviaire, son intervention ne sera pas considérée comme aléatoire dans la suite de l'étude.

I.3.3 Cadre commercial

La présentation du contexte de l'étude a mis en évidence trois différents acteurs. La société Thales développe et vend son logiciel ATS pour la supervision de lignes de métro à l'exploitant de la ville de Paris, la RATP. La relation entre ces deux intervenants est de type fournisseur / client et fluctue suivant les affaires en cours. Les échanges d'informations et de données sont donc de type commercial.

L'étude réalisée se fait dans le cadre d'une thèse CIFRE, en collaboration avec la société Thales. Cette relation contractuelle permet d'obtenir l'ensemble des données nécessaires à la recherche ainsi qu'une transparence dans les difficultés rencontrées et les besoins d'amélioration.

L'échange d'informations avec la RATP s'est fait par la participation à la formation complète des chefs de régulation en tant qu'auditrice libre. Cette opportunité s'est présentée grâce à la volonté de personnes au sein de la RATP de partager leurs connaissances et leur savoir-faire, et avec le désir d'améliorer l'exploitation de leurs lignes. Cette entente est donc cordiale et repose sur une confiance réciproque dans l'utilisation des données échangées.

La recherche s'effectue donc en contrat avec un industriel et en partenariat avec l'un de leur client afin de réaliser une étude au plus proche des attentes des industriels du domaine. Suivant le point de vue de chacun de ces acteurs, des problèmes différents émergent lors de l'analyse des procédures de gestion d'incidents sur une ligne de métro.

II État de l'art et positionnement

Résumé

Afin de replacer mes recherches dans la communauté scientifique, un état de l'art est effectué. L'analyse d'études portant sur la supervision d'une ligne de métro permet d'identifier des problématiques déjà abordées. Ce type de supervision se rapporte à la gestion du trafic dont les objectifs principaux sont l'optimisation du flux et de la régulation des trains. Afin d'étudier les procédures de gestion d'incidents, une représentation sous forme de processus métier puis de système à événements discrets semble la plus appropriée. L'identification des situations dangereuses s'appuiera ensuite sur les analyses de sûreté de fonctionnement. L'application de la théorie du contrôle par supervision permettra finalement d'éviter les états interdits. Cet état de l'art permet d'identifier les différents problèmes abordés dans ce travail ainsi que les objectifs de l'étude. Les solutions et la démarche choisies sont également détaillées.

Sommaire

II.1 Quelles sont les études réalisées sur la supervision du métro ?

II.1.1 Présentation de deux projets

Depuis quelques années, l'augmentation de la complexité des systèmes de supervision des lignes de métro et la recherche d'une sécurité maximale ont conduit les industriels à réaliser des projets avec des universitaires dans le but d'innover. Les objectifs et réalisations de deux de ces projets, le projet SART et le projet SpicaRail, sont présentés.

Le projet SART

Entre les années 1995 et 2002, le projet SART, Système d'Aide à la Régulation du Trafic, a réuni l'Université Paris 6, l'Université Fédérale de Rio de Janeiro au Brésil ainsi que les exploitants de métro de Paris et de Rio de Janeiro, la RATP et Metrô, et impliqué plus d'une cinquantaine de personnes[Bre97][Bre00a]. Cette collaboration internationale avait pour objectif de réaliser un système intelligent d'aide à la décision à l'intention des opérateurs de supervision pour la gestion des situations d'incidents. L'objectif n'était pas d'automatiser la gestion d'incidents mais de développer un système pour assister l'opérateur dans ses activités quotidiennes. Ce projet a impliqué des informaticiens [Pas02] pour la modélisation du système et des ergonomes [Zan99][Zan03] pour l'intégration dans une interface homme machine informatisée.

En analysant les méthodes utilisées pour la gestion des incidents à la RATP, la notion de contexte est apparue comme essentielle pour ce projet afin de déterminer la bonne stratégie à appliquer. Le contexte définit la situation de la ligne et du trafic au moment de l'occurrence de l'incident. Un formalisme adapté à la prise en compte du contexte et à la modélisation de procédures a donc été développé : les graphes contextuels[Bre03][Bre00b]. Un système a été conçu pour enrichir la base de données des procédures de gestion d'incidents : un module enregistre la situation de la ligne au moment de l'incident ainsi que les actions réalisées par l'opérateur pour le résoudre. Les informations récoltées permettent de réaliser un raisonnement à partir de cas pour identifier et créer de nouvelles procédures. La structure de données est ensuite modélisée avec un graphe contextuel et transmise à l'opérateur de supervision si une situation identique se présente.

La collaboration avec des exploitants de ligne de métro a permis d'identifier les vraies attentes sur un système d'aide à la décision ainsi que les stratégies réellement utilisées par les opérateurs. Cependant, le développement et la mise en service d'un système d'aide à l'opérateur n'ont pas pu être réalisés. Ces étapes de test et d'utilisation par un opérateur nécessitent la participation du fournisseur du système de supervision afin de créer une aide intégrée dans l'interface de supervision du trafic déjà utilisée.

Le choix de développer un nouveau formalisme, les graphes contextuels, pour modéliser les procédures et tenir compte du contexte, a pu entrainer un manque de maturité et de recul par rapport à l'utilisation de ce formalisme et l'analyse des résultats obtenus. Ce formalisme est aujourd'hui utilisé dans d'autres domaines d'application comme la médecine [Bre07] mais n'a pas réussi à l'époque à convaincre les exploitants de métro de sa pertinence.

Le projet SpicaRail

Le projet SpicaRail (Supervision PICArde de transport par Rail) a débuté en 2005 et est principalement une collaboration entre l'université de technologie de Compiègne (UTC) et Alstom Transports[Bel06][Bel11], société qui développe des systèmes informatisés de supervision ATS pour les métros.

Le constat de départ de ce projet est que la supervision reste une opération humaine et que le stress de l'opérateur peut engendrer des prises de décision inadaptées et avoir des conséquences sur la sécurité des personnes. La démarche mise en place pour répondre à ces problèmes est d'étudier l'impact de la supervision réalisée à partir des postes de contrôle et commande d'une ligne de métro sur la sécurité ainsi que le comportement de l'opérateur humain. Pour cela, une démarche interdisciplinaire a été adoptée entre la sûreté de fonctionnement, la psychologie cognitive et l'ergonomie. L'objectif de ce projet est d'évaluer l'impact des systèmes de supervision ATS sur la sécurité avec comme objectif industriel d'identifier le niveau de sécurité qu'il serait possible d'attribuer à un ATS en tenant compte du facteur humain.

Ainsi, au cours du projet, des scénarios critiques de supervision ont été identifiés puis modélisés grâce à la méthode FRAM (Functional Resonance Analysis Method)[Bel08b]. Cette méthode prend en compte les composantes techniques, humaines et organisationnelles du système pour expliquer l'apparition d'un accident. Pour réaliser des tests avec des opérateurs sur l'impact du facteur humain, une plateforme avec un système ATS d'Alstom et un simulateur de trafic a été installé à l'UTC. Des expériences ont ainsi été réalisées pour étudier la réaction de différents opérateurs face à plusieurs cas d'accidents.

Pour conclure, le projet a montré que l'impact du facteur humain sur la sécurité est un aspect important qu'il faut prendre en considération lors de l'étude la supervision d'un système de transport. La méthode FRAM utilisée permet de comprendre et d'analyser des phénomènes complexes avec un regard interdisciplinaire mais n'apporte pas de solutions pour éviter les accidents et augmenter la sécurité des personnes. L'approche de la sécurité réalisée reste qualitative et ne fournit pas une liste exhaustive des défaillances possibles.

Conclusion

Ces deux projets d'envergure et en collaboration avec des industriels, fournisseurs comme exploitants, ont mis en avant des problématiques importantes concernant la gestion des incidents lors de la supervision d'une ligne de métro. L'existence de ces projets démontre aussi l'intérêt des industriels sur ce sujet et les possibilités d'améliorations dans ce domaine. En s'appuyant sur ces projets, des pistes de réflexion ont été identifiés :

- La **collaboration** nécessaire entre le fournisseur du système de supervision et l'exploitant pour répondre aux attentes des industriels et proposer une aide appropriée ;
- L'importance du choix d'une **représentation adaptée** à l'objectif de recherche ainsi qu'à la transmission d'informations aux industriels et aux opérateurs de supervision ;
- L'**influence de la situation courante** de la ligne de métro pour la gestion des incidents ;
- La prise en compte de la **sécurité des personnes** pour réaliser une analyse complète de la situation.

II.1.2 Compréhension du fonctionnement d'une ligne de métro

En dehors de l'étude et de l'amélioration du système de supervision d'une ligne de métro pour la gestion des incidents, des études sont réalisées sur d'autres aspects de son fonctionnement et apportent des précisions sur ce système complexe. Ces études permettent de préciser le cadre des recherches présentées dans ce mémoire.

Ainsi, des industriels ont effectué une étude sur les impacts du passage d'une ligne avec conducteurs à une ligne complètement automatique, sans conducteur. L'étude [Bel08a] concerne plus particulièrement le projet d'automatisation intégrale de la ligne 1 du métro de Paris. L'objectif est d'identifier les différents problèmes qui pourront être rencontrés lors de cette transformation qui doit être réalisée sans arrêter l'exploitation de la ligne. Trois difficultés ont été étudiées : la requalification des conducteurs de la ligne, les travaux à effectuer sur la ligne et la gestion de la transition entre l'ancien et le nouveau système. Cette étude a permis d'anticiper les problèmes d'une automatisation intégrale et apporte des précisions sur les problématique du fonctionnement d'une ligne en mode automatique. La gestion des incidents diffère suivant le type de ligne : avec conducteurs ou automatique. En effet, les procédures peuvent faire appel ou non à l'intervention des conducteurs. Dans la thèse présentée ici, **les lignes de métro seront avec conducteurs**.

En se plaçant du point de vue de l'opérateur qui gère la supervision d'une ligne de métro et plus du système informatique, il apparait que sa charge mentale peut compromettre la bonne utilisation du système. Cette charge mentale dépend notamment de la quantité d'informations reçues lors de la gestion d'un incident. Les auteurs de [Dji06] ont interrogé des opérateurs de supervision de la RATP sur leurs expériences personnelles pour analyser les conséquences de l'exécution de tâches sur leur mental. Suivant la ligne de métro concernée, les difficultés mises en avant sont différentes donc les recommandations proposées pour améliorer leurs conditions de travail varient. Dans la suite de cette thèse et afin de ne pas tenir compte de cette problématique, **l'opérateur humain sera considéré comme parfait**, ses actions sur le système et son comportement seront justes et idéals par rapport au système de supervision ATS. En effet, l'objectif pour Thales est d'améliorer son application de supervision en sachant que la maitrise complète des actions d'un opérateur n'est pas envisageable.

La supervision d'une ligne de métro peut également être étudiée sous l'angle des usagers. Dans [Foo96], Foot dresse un historique de la gestion des voyageurs à la RATP. Pour satisfaire au mieux leur demande, des adaptations sont constamment réalisées sur le réseau des lignes de métro et des nouvelles stratégies de transport sont développées, comme par exemple la modernisation et l'automatisation de certaines lignes. Amory [Amo12] propose une analyse en terme de dangers et de risques encourus par les voyageurs tout au long de leur trajet, et plus particulièrement lors des transferts entre le quai et le train. Des études et modélisations sont réalisées pour comprendre les facteurs impliqués dans cet incident et trouver des défenses possibles. **Le point de vue choisi dans la suite de la thèse est celui de l'opérateur de supervision** et non celui des voyageurs. Cependant lors de la gestion des incidents, l'objectif principal reste d'assurer la sécurité des voyageurs.

Pour que l'exploitation d'une ligne se déroule au mieux, les travaux de maintenance sont réalisés la nuit. Pendant cette période, l'opérateur de supervision est responsable de la gestion de l'énergie électrique, permettant ainsi aux techniciens de descendre sur les voies ou d'effectuer des tests. Dans ce cadre, un article [Jub10] étudie les causes de remises sous tension erronées de la ligne, interprète les erreurs et propose des solutions pour les éviter. Cette étude repose sur

des entretiens avec des opérateurs de supervision de la RATP, des observations de leur travail en situation ainsi que sur les rapports d'incident. Les incidents se produisant la nuit sont différents de ceux ayant lieu lors de l'exploitation de jour avec des voyageurs. Les problématiques et les procédures de gestion d'incident diffèrent donc entre l'exploitation de jour et les travaux de nuit. L'étude réalisée dans la thèse se concentre sur **les incidents au cours d'une journée d'exploitation avec voyageurs**.

II.1.3 Conclusion

Les études présentées dans cette partie apportent une meilleure connaissance du domaine de la supervision d'une ligne de métro en proposant des points de vue différents et donnent ainsi un aperçu des enjeux de l'exploitation d'une ligne de métro. Les thèmes mis en avant dans les projets SART et SpicaRail sont corroborés par les autres études, à savoir l'importance d'une collaboration avec un industriel et plus particulièrement avec des opérateurs de supervision ainsi que la nécessité de prendre en compte les aspects de sécurité pour la protection des voyageurs.

Le cadre de l'étude réalisée a également pu être précisé au travers des études présentées. Ainsi, la thèse porte sur la gestion des incidents se produisant sur les lignes de métro avec conducteurs et pendant une journée d'exploitation avec voyageurs. De plus, le point de vue adopté est celui de l'opérateur de supervision qui sera considéré comme parfait par la suite.

II.2 Comment étudier les systèmes de supervision ?

II.2.1 Systèmes de supervision

La supervision de système couvre un large éventail d'applications industrielles qui peuvent être séparées en deux catégories : les procédés industriels et la gestion du trafic. La supervision industrielle concerne, entre autres, le pilotage de systèmes, la surveillance de leur bon fonctionnement, l'acquisition et la synthèse d'informations, la commande d'équipements et le contrôle des performances.

Procédés industriels

Dans la supervision, il existe trois types de procédés industriels : les systèmes avec des variables qui évoluent dans le temps de manière continue, les systèmes discrets où les variables changent suivant l'occurrence d'événements et les systèmes hybrides utilisant les deux types de variables.

Les études suivantes reposent sur des systèmes avec des variables continues et concernent des domaines industriels variés. Ainsi, pour le traitement de l'eau dans une centrale thermique [Lak14], le système de supervision SCADA [1] fait l'acquisition des données et assure le contrôle de certains éléments du système. Le circuit d'extraction de l'eau est alors supervisé afin d'assurer des pertes minimales en eau. En biologie, afin d'étudier la biosynthèse industrielle de la tylosine, des procédures de surveillance du procédé sont développées [Alb01]. L'objectif de cette supervision est d'améliorer les performances de cette biosynthèse pour proposer une solution

1. Supervisory Control And Data Acquisition

de production avec un rendement industriel. Dans le domaine de la pétrochimie, et plus particulièrement la génération de vapeur, les auteurs de [Oul06][Med06] souhaitent développer un système d'aide à la décision afin de former un environnement intégré de supervision. L'analyse et la modélisation du système permettent la détection des fautes et la suppression des capteurs redondants. L'objectif du système de supervision est d'assurer un contrôle en temps réel du système lors du fonctionnement nominal et lors de la présence de défaillances.

Plusieurs études de systèmes de supervision ont également été réalisées sur des procédés industriels avec une évolution discrète. Dans l'analyse de la production dans une usine pharmaceutique [Ake99], l'objectif de la supervision est d'améliorer l'allocation des ressources disponibles pour diminuer les temps d'attente et ainsi augmenter la productivité. Pour la gestion du procédé d'extraction de sable [Blo00], la prise en compte de toutes les interactions existantes dans le système et l'utilisation d'un outil de décision permettent d'assurer une gestion optimisée de la flotte de camions.

Gestion du trafic

La supervision du trafic gère des éléments mobiles dans un environnement particulier soumis à des contraintes de sécurité, de rapidité et de productivité. La supervision contrôle la circulation des éléments et régule les flux en ayant pour objectif d'améliorer le mouvement des éléments et d'éviter les conflits.

En lien direct avec la supervision d'un site industriel et l'augmentation de la production, une étude a été réalisée sur le pilotage en ligne d'un système de véhicules autoguidés dans une usine de production [Arn09a][Arn09b]. L'objectif est de prendre en considération les contraintes liées à la régulation du trafic et à la gestion de conflits ainsi que les contraintes inhérentes à la production pour améliorer les flux de transport de produits au sein d'une usine. Afin d'optimiser les temps de parcours et éviter les conflits et blocages, les auteurs réalisent une modélisation puis une vérification du système. L'étude analyse les conflits entre trois véhicules sur un circuit simple restant assez loin de l'usage réel et des problèmes rencontrés lors de leur utilisation en usine.

Dans le transport aérien, les variations de capacités des secteurs à cause des modifications météorologiques compliquent le contrôle du trafic aérien. Afin de proposer une solution d'aide à l'opérateur pour le management du trafic d'un nombre important de vols, l'étude effectuée dans [Kam13] considère le système de trafic aérien comme un système à événements discrets. Une modélisation du système identifie les états indésirables définis par le cahier des charges et optimise ainsi le flux du trafic sur le réseau aérien.

Conclusion

La supervision des procédés appliquée à différents domaines industriels a pour objectif l'amélioration de la productivité du système, la prise en compte des pannes pouvant se produire et l'automatisation d'une partie des tâches à effectuer. Concernant la gestion du trafic, l'objectif est de réguler les flux afin d'éviter les conflits et d'optimiser les déplacements des éléments.

II.2.2 Gestion du trafic dans les transports de personnes

Dans le domaine du transport de personnes, la supervision est présente afin de proposer aux usagers l'offre de transport la plus large et la plus fiable possible. La plupart des études réalisées dans le domaine des transports s'intéresse à la gestion du trafic et à l'amélioration de la régulation des éléments roulants. Des analyses et recherches ont été effectuées sur les différents modes de transport afin de mieux comprendre les enjeux de la supervision dans ce domaine.

La voiture est un mode de transport personnel pour se déplacer sur des routes et dépendant du flux des autres véhicules. Ainsi, pour organiser au mieux le transport de personnes par véhicule, comme par exemple pour un service de taxi [Seo04], un système de supervision avec une intervention humaine peut planifier et réguler les services de transport de passagers en fonction de la circulation, des conditions de trafic, et des préférences de type de véhicule. En effet, le transport d'un lieu vers une destination donnée subit de nombreuses contraintes rendant son optimisation complexe, l'objectif principal étant de réaliser le trajet le plus rapidement possible.

La supervision informatique des voies de circulation est également possible. Ainsi, la gestion d'un réseau autoroutier [Ena93] est réalisée dans le but de limiter les accidents et leurs conséquences sur le trafic. Pour cela, il est nécessaire d'avoir une vision globale de la situation afin de connaître les événements perturbateurs se produisant, de pouvoir informer les utilisateurs et de mettre en œuvre des actions pour limiter les conséquences sur la circulation.

Le bus est un moyen de transport en commun utilisant la plupart du temps les mêmes voies de circulation que les voitures et est donc affecté par les mêmes contraintes. Pour améliorer le trafic des bus dans une agglomération, un système de supervision [Caz09] assure le suivi des bus et détecte les perturbations se produisant sur le réseau. La connaissance de leur position en temps réel permet, par exemple, à un superviseur en charge des lignes d'augmenter l'offre de transport et la disponibilité du service de bus [Pan08]. La régulation en temps réel de l'ensemble des bus diminue ainsi le temps d'attente des passagers aux arrêts et améliore donc le service proposé.

À la différence du bus, le train est un mode de transport en commun qui circule en site propre uniquement et n'est donc pas perturbé par les autres modes de transport. Un système de supervision sera donc moins ciblé sur la régulation des véhicules mais l'objectif reste le même : améliorer l'offre de transport proposée aux voyageurs. Dans cette perspective, l'étude de Gely [Gél10] présente un système de supervision pour minimiser les conséquences d'un incident sur la circulation des trains.

En raison de l'utilisation des voies de transport par plusieurs modes de transport, une supervision dite bimodale a également été développée. Ainsi, l'étude [Bho10] présente une gestion du trafic dans les intersections entre les bus et les voitures en privilégiant le transport en commun. L'objectif est de contrôler le flux des voitures afin d'améliorer le trafic et réduire le temps d'attente passé dans les embouteillages par les bus. Les retards par rapport à l'horaire théorique de passage aux arrêts sont ainsi diminués.

II.2.3 Aide à la décision dans les transports

De nombreuses études sur la supervision des modes de transport se basent sur des systèmes multi-agents. Un agent est une entité intelligente, physique ou virtuelle, caractérisé par son auto-

nomie qui ne lui permet pas d'avoir une vision globale de son environnement. Un système multi-agents réunit un ensemble d'agents en interaction et coopération pour résoudre collectivement des problèmes, ils forment ainsi le comportement global du système. Les études [Dav05][Oss05] recensent différentes approches de supervision de transport reposant sur une modélisation multi-agents du système et ayant pour objectif de fournir des éléments d'optimisation dans la gestion du trafic et de proposer une aide à la décision à l'opérateur.

En se basant sur une approche multi-agents, Ezzedine [Ezz08] développe une interface homme machine destinée à la gestion bimodale entre les bus et les tramways dans les villes. Le système de supervision adapte la coordination entre les deux transports en commun à la demande des usagers et leur propose une information sur le trafic en temps réel.

Dans le cadre d'une modélisation multi-agents du système [Bal05], le trafic des bus lors de perturbations est perfectionné grâce à la mise en place d'un système d'aide à la décision. Le système de supervision améliore ainsi la prise en compte des perturbations et donc la régulation des bus. En effet, la régulation nécessite la surveillance du réseau, le diagnostic des perturbations et la prise de décision des actions à réaliser. La régulation dépend donc de l'expérience de l'opérateur, de ses connaissances et de ses habitudes. Le système informatisé de supervision facilite la prise de décision des opérateurs pour améliorer la gestion du trafic des bus et donc l'offre proposée aux voyageurs.

Le rôle et l'expérience de l'opérateur sont également déterminants lors de l'utilisation de procédures de gestion d'incidents écrites. Dans ce cadre, des études ont été réalisées pour établir des procédures pour les pilotes dans les cockpits d'avions.

Ainsi, Degani [Deg97] présente les procédures comme une normalisation des actions de l'opérateur, limitant son rôle mais diminuant les erreurs lors de conditions normales et anormales de vol. Il propose une méthode pour l'élaboration de procédures pour le pilotage d'un avion. Sa méthode pourrait également être appliquée à la conception de procédures de gestion d'incident dans d'autres systèmes à hauts risques tels que les centrales nucléaires et les usines de production. L'auteur a également établi que le développement de procédures dépend entres autres de la philosophie et des pratiques de l'entreprise. Les procédures peuvent être écrites et dicter les actions que l'opérateur doit réaliser, elles donnent une ligne directrice à suivre ou bien sont mémorisées pour une application plus rapide.

Même si les procédures sont des aides, leur application reste le choix de l'opérateur. Les procédures peuvent ainsi ne pas être utilisées comme prévu initialement. Dans [dBr98][dBr99], l'auteur identifie des raisons pour expliquer les écarts entre la procédure écrite et les actions réalisées par l'opérateur. Ces décalages peuvent être perçus comme le besoin de gérer une situation différente de celle envisagée, le besoin de mieux comprendre la situation en cours ou la perte de contrôle de l'activité. L'auteur recherche des outils adaptés pour augmenter la fiabilité de l'exécution des procédures écrites en se rapprochant des personnes utilisant les procédures.

Ainsi, bien qu'il ne soit pas possible d'écrire une procédure pour toutes les situations rencontrées par un opérateur, la mise en place de procédure d'exploitation permet à l'opérateur de réagir plus sûrement et plus rapidement.

II.2.4 Conclusion

La supervision d'une ligne de métro rentre dans le cadre de la **gestion de trafic pour l'optimisation du flux et de la régulation des trains** sur la ligne. Pour les contraintes

existantes pour le transport métro, elles se rapprochent le plus du transport par train puisque la **circulation se fait en site propre** sans la perturbation des autres moyens de transport. L'étude réalisée se concentre sur **un seul mode de transport** et n'est donc pas multi-modale. L'étude et l'amélioration des procédures de gestion d'incidents sont effectuées dans le but de **développer une aide à la décision** pour les opérateurs pour faciliter leurs choix. Pour réaliser ces analyses, il est nécessaire d'avoir et de s'appuyer sur une représentation du système concerné.

II.3 Comment modéliser un système de supervision ?

II.3.1 Modélisation d'un système

La modélisation d'un système, que ce soit un système de production, un système de transport ou autres, est une transition fondamentale entre la réalité ou sa description textuelle et un objet graphique ou mathématique qui le représente. L'idée de la modélisation est de représenter de manière simplifiée les systèmes afin de les étudier, les analyser au travers d'indicateurs de performance, mieux les comprendre et les concevoir. De plus, un modèle est une représentation d'un système dans son environnement d'utilisation. La modélisation est une phase importante dans l'étude de processus afin de les définir d'une manière abstraite, d'obtenir une représentation graphique pour les visualiser et de les appréhender plus simplement selon un point de vue établi.

Dans l'étude des procédures de gestion d'incidents, une modélisation peut être réalisée pour obtenir une représentation graphique et pour analyser les actions de l'opérateur de supervision. Le langage choisi doit ainsi permettre de véhiculer le fonctionnement du processus et de représenter la manière dont les activités sont exécutées et ordonnées. L'étude d'un système nécessite souvent de construire plusieurs modèles complémentaires en fonction des objectifs que l'on souhaite atteindre.

II.3.2 Représentation de processus métier

Un processus métier décrit l'ordre d'exécution d'un ensemble d'activités à réaliser, les relations et interactions entre activités et les différents échanges entre les partenaires impliqués dans le processus. Pour modéliser un processus métier, plusieurs langages standardisés existent, parmi lesquels le BPMN, Business Process Model and Notation, et le diagramme d'activités UML, Unified Modeling Language. Les deux langages BPMN et UML sont des langages de haut niveau principalement utilisés par les industriels qui se basent sur une notation graphique pour décrire de manière intuitive des processus métier. Ces langages ne sont pas des langages d'exécution de processus mais des langages de représentation graphique.

Unified Modeling Language

UML est un langage de représentation graphique standardisé par l'Object Management Group (OMG) [OMG11b]. Le langage UML propose plusieurs diagrammes suivant les besoins et les exigences à exprimer et apporte une représentation graphique utilisée dans le développement orienté objet. UML n'étant pas une méthode mais seulement un langage, son utilisation est laissée à l'appréciation de chacun. Apparu dans le monde du génie logiciel, dans le cadre de la conception orientée objet, il est aujourd'hui appliqué à toutes sortes de systèmes ne se limitant pas au domaine informatique.

Parmi l'ensemble des diagrammes existants, le diagramme d'activités UML décrit sous forme de flux ou d'enchaînement d'activités le comportement d'un système et représente les interactions synchrones au sein du système. Une activité correspond à l'exécution d'un mécanisme, le déroulement d'étapes séquentielles. Dans l'article [Rus06], les auteurs présentent les diagrammes UML d'activités en évaluant leur pertinence pour la représentation de processus métier. D'après leur étude, ces diagrammes sont peu adaptés à la représentation des aspects organisationnels et du partage des ressources d'un processus.

Business Process Model and Notation

Norme internationale reconnue et adoptée par certaines entreprises [OMG11a][OMG10], le langage BPMN a été développé pour décrire des processus d'entreprise en mettant en mouvement l'ensemble des ressources humaines et matérielles. Il donne la possibilité pour tous les participants d'un processus de se comprendre grâce notamment à une notation simple et claire. La représentation d'un processus en BPMN offre différents niveaux de précision : de la simple représentation graphique à un processus exécutable dans un système d'information. Les processus BPMN peuvent également générer un langage XML [2] afin d'exécuter et de simuler le comportement décrit.

Dans l'étude [Che09], une méthode est présentée pour aider à la représentation graphique de processus métier par une approche de rétro-ingénierie. En effet, la représentation de processus métier est devenue une nécessité pour les comprendre, les maitriser et prévoir leur changement. Ainsi, un méta-modèle du langage BPMN est proposé avec différentes vues afin d'identifier l'ensemble des éléments nécessaires pour la définition d'un processus métier complet en BPMN. La méthode exposée est testée sur l'application PostBac permettant de gérer les admissions dans l'enseignement supérieur.

Comparaison UML / BPMN

Le langage BPMN a le même fonctionnel que les diagrammes d'activités UML mais propose une notation avec des symboles standardisés permettant d'avoir une description plus précise du processus. Dans [Whi04], l'auteur réalise une analyse des capacités graphiques des langages UML activité et BPMN, en comparant les structures existantes les unes après les autres. Son étude montre que les deux langages fournissent des solutions similaires pour la modélisation de processus métier mais que la différence se fait plus suivant l'objectif recherché par les utilisateurs. De plus, le BPMN est plus adapté pour une modélisation de certains processus métier car il supporte un plus grand nombre de structures. Cet aspect peut cependant être considéré comme une augmentation de la complexité du langage BPMN en raison du nombre d'éléments existant [Rec09].

Une étude [Pei08] a été réalisée pour évaluer les différences de lisibilité entre les deux langages. En se basant sur un même processus métier représenté dans les deux langages, un panel de personnes non utilisateurs habituels des langages a été consulté. Les résultats obtenus ne mettent pas en évidence de différence significative mais le choix des éléments du langage BPMN permettent une meilleure lisibilité du processus métier représenté.

2. eXtensible Markup Language

En se basant sur trois critères d'évaluation, C.Geambasu [Gea12] a également comparé les deux représentations de processus métier. Ses critères prennent en compte la capacité de compréhension, l'adéquation des éléments graphiques pour représenter un processus métier et la traduction dans un langage d'exécution. Les résultats sont similaires pour les deux solutions, sauf pour le dernier critère qui est plus facilement réalisable avec le BPMN.

Afin de comparer ces deux langages, le processus de commande d'une pizza est représenté avec le langage BPMN [OMG10] et UML [Ser14] (annexe B). Ces deux représentations graphiques du même processus mettent en évidence les conclusions des différentes études. En effet, le langage BPMN utilise plus d'éléments que le diagramme d'activités UML mais propose une meilleure lisibilité du processus de commande de pizza.

Conclusion

Bien qu'ils soient similaires, le BPMN est un langage plus orienté vers les industriels alors que les diagrammes d'activités UML ont été conçus pour le développement logiciel. Ils sont donc plus techniques et moins compréhensibles par des industriels non familiers de ce type de langage. **Le langage BPMN sera donc utilisé dans la suite de l'étude pour la représentation graphique des procédures de gestion d'incidents**.

Cependant, il n'existe pas de méthode mathématique sur ces langages pour la vérification de la conformité des processus avec les exigences du système. La vérification des propriétés dynamiques d'un système, concernant la sureté ou la vivacité par exemple, se rapporte à l'occurrence ou l'ordonnancement d'événements et requière donc une modélisation des processus métier et plus seulement une représentation graphique. En effet, avec un modèle formel, des méthodes et théories peuvent être appliquées pour vérifier la fiabilité du processus et détecter des erreurs par rapport aux exigences.

Afin de modéliser des processus métier en tenant compte de leur environnement d'exécution, il est donc nécessaire d'utiliser un langage de modélisation adapté aux processus métier, une approche de modélisation par systèmes à événements discrets est proposée dans la section suivante.

II.3.3 Analyse d'un processus représenté en BPMN

Systèmes à événements discrets

Les systèmes à événements discrets, au lieu de s'intéresser au déroulement continu des phénomènes, ne se soucie que de certains instants particuliers et de leur enchaînement logique. Leur évolution est conditionnée par l'occurrence des événements discrets qui peuvent être le début ou la fin d'un phénomène comme par exemple l'arrivée d'une pièce dans un stock, le dépassement d'un seuil dans un niveau de liquide, l'achèvement d'une tâche d'une machine de production.

Ces événements sont instantanés et se produisent de façon spontanée. De plus, aucune horloge ne séquence leur occurrence, ils sont donc asynchrones. Ainsi, aucune variable de temps n'est prise en compte pour l'étude de ces systèmes. Les systèmes à événements discrets représentent des comportements tels qu'une évolution parallèle, un partage de ressources et une mémorisation et lecture d'informations. Ils modélisent par exemple des systèmes informatiques, des réseaux de télécommunications, des réseaux de transport ou des chaines de production manufacturière.

Plusieurs outils de modélisation des systèmes à événements discrets existent pour appréhender l'ensemble des caractéristiques des systèmes [Cas99]. Ainsi, les automates à états modélisent l'ensemble des états accessibles et associent chaque transition entre états à un événement. Les files d'attente permettent de modéliser des processus stochastiques dont le comportement n'est que partiellement prévisible et relève du calcul des probabilités. Les réseaux de Petri (RdP) modélisent facilement différentes classes de système dont les comportements sont notamment caractérisés par des évolutions parallèles et des synchronisations. L'ensemble des états du système peut également être représenté explicitement.

Les recherches effectuées dans ce mémoire ne rentrent pas dans le cadre d'une modélisation par files d'attente puisqu'aucun calcul probabiliste est réalisé. De plus, les caractéristiques d'évolutions parallèles et de synchronisation des RdP apportent une facilité de modélisation des processus métier.

Transformation de processus métier vers un SED

Dans son article [Aal98], Aalst présente trois raisons d'utiliser les réseaux de Petri pour étudier des processus métier. Tout d'abord, l'existence d'une sémantique formelle ainsi qu'une représentation graphique accessible des réseaux de Petri favorise les échanges avec les personnes non initiées au formalisme. De plus, une modélisation basée sur les états facilite la représentation de processus métier. De nombreuses analyses techniques existent également pour vérifier les propriétés du système étudié. Des recherches [Loh09], [Rae07] ont été effectuées en utilisant une représentation graphique BPMN et une modélisation par réseaux de Petri. Ainsi, certaines d'entre elles étudient plus particulièrement la transformation entre ces deux langages (section II.3.3).

Les réseaux de Petri permettent de modéliser un comportement et de saisir le fonctionnement global des systèmes étudiés et apportent une représentation compacte, graphique et structurée des systèmes. Des propriétés mathématiques et des outils de vérification existent pour analyser les réseaux de Petri. Ainsi, il est possible de vérifier des propriétés attendues comme le bornage, la vivacité, la réinitialisation et la persistance. Les réseaux de Petri permettent également de simuler et d'évaluer les performances d'un système en termes de sécurité et de dynamique.

Les réseaux de Petri offrent plusieurs possibilité de modélisation. Parmi les différentes classes, les réseaux de Petri ordinaires associent des poids de 1 pour tous les arcs du réseau, alors que les réseaux généralisés n'imposent aucune contrainte au poids des arcs. Pour les systèmes avec une variable de temps, il existe les réseaux de Petri temporels et les réseaux temporisés. Les réseaux de Petri colorés spécifient une couleur pour chaque marque et permettent ainsi de modéliser des systèmes de grandes tailles de manière graphique et synthétique.

Une modélisation par réseaux de Petri permet l'évaluation du processus exécutable et sa vérification formelle pour s'assurer du bon fonctionnement. La modélisation donne aussi la possibilité d'optimiser et d'apporter des améliorations au processus étudié. **Suite à la représentation des procédures de gestion d'incidents avec le langage BPMN, ces modèles seront donc transformés en réseaux de Petri ordinaires afin de réaliser les analyses et vérifications souhaitées.**

Transformation de BPMN à RdP

Depuis une dizaine d'année et le déploiement du langage BPMN dans le monde industriel, des chercheurs étudient les modalités de transformation des modèles BPMN en réseaux de Petri et des articles présentent des correspondances possibles entre les éléments des langages tout en observant des limites. Le langage BPMN représente les étapes d'un processus sous forme d'activités et d'événements et les réseaux de Petri modélisent les différents comportements d'un système évoluant selon le franchissement de transitions. La transformation d'une modélisation à l'autre a donc été étudié et normalisé par de nombreuses recherches.

L'approche développée par Vijverberg [Vij06] propose d'utiliser un langage d'échange de réseaux de Petri au format XML, pour étudier des procédures décrites par le langage BPMN. Il précise cependant que seuls les éléments BPMN ayant un comportement bien définis sont traduisibles et les procédures ne doivent avoir qu'un seul événement de début et un seul de fin.

Dans [Dij08], les auteurs définissent de manière formel le langage BPMN et sa traduction en réseaux de Petri. Certains éléments ne sont également pas pris en compte et certaines restrictions sur les modèles sont posées. En se basant sur cette transformation, des applications ont été réalisées, comme par exemple le développement d'un processus de dématérialisation de flux courrier [Shr09].

L'étude [Ouy08] développe une méthode pour analyser l'évolution du flux d'un modèle BPMN avant son implémentation et son utilisation en se basant une approche par réseaux de Petri. Une transformation entre les deux langages est présentée et testée sur un exemple théorique de processus de commande. La méthode proposée dans l'étude est composée de quatre phases : l'analyse du problème, la transformation entre les deux représentations, la simulation du système pour vérifier les propriétés recherchées et enfin l'implémentation du processus pour son application.

II.3.4 Conclusion

Un modèle réseaux de Petri n'est pas facilement compréhensible par des utilisateurs industriels contrairement à un modèle BPMN qui peut être interprété par des industriels, simulé et analysé par RdP. Après la transformation, des informations représentées avec le langage BMPN comme le type des activités et des événements, les communications entre les différents intervenants de la procédure ne sont plus aussi clairement identifiées. Les réseaux de Petri ont en effet un autre objectif que la représentation graphique du langage BPMN, le but n'étant plus d'écrire des procédures compréhensibles par tous mais de modéliser des procédures sur lesquelles des vérifications de propriétés et exigences pourront être réalisées.

II.4 Comment évaluer les situations dangereuses ?

II.4.1 Vocabulaire

Définition

Pour toute étude sur la sûreté de fonctionnement, il est nécessaire d'utiliser un vocabulaire commun et spécifique [Vil88].

Définition 1 (Sûreté de fonctionnement) *La sûreté de fonctionnement est définie comme l'aptitude d'un élément du système à satisfaire une ou plusieurs fonctions requises dans des conditions données, elle est ainsi considérée comme la science des défaillances et des pannes.*

Définition 2 (Incident) *Un incident est une anomalie provoquant une perturbation dans le système. La cause d'un incident est due à l'environnement, à une erreur d'exploitation ou à une panne.*

Définition 3 (Danger) *Un danger est une situation où des facteurs aléatoires internes ou externes peuvent nuire à l'homme, la société ou à l'environnement et conduire à la réalisation d'un accident.*

Définition 4 (Risque) *Un risque est une mesure du danger, il associe l'occurrence d'un événement indésirable et ses effets ou conséquences. Un risque se différencie ainsi d'un danger par la prise en compte de la probabilité d'apparition du danger. Pour évaluer les risques d'une situation, il est nécessaire d'avoir des informations sur l'occurrence des événements s'y produisant.*

Définition 5 (Accident) *Un accident peut être l'une des conséquences d'un incident si celles-ci sont catastrophiques, c'est-à-dire qu'il y a des morts, des blessés graves ou des dommages majeurs pour l'environnement.*

Ainsi, selon les fondamentaux de la sûreté de fonctionnement (figure II.1) : une situation dangereuse est une situation où un danger identifié peut causer des dommages importants au système même ou à son environnement et entraîner pour l'homme la mort ou des dommages corporels. L'apparition d'un danger est due à l'occurrence d'un événement dangereux, appelé incident.

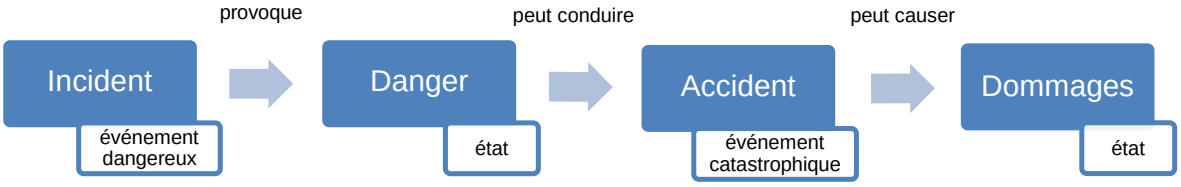


FIGURE II.1 – Propagation d'un incident

Différence Danger / Risque

Dans le cadre d'étude de la sûreté de fonctionnement, il est important de saisir la différence entre un danger et un risque. Ainsi, un risque se caractérise par la probabilité d'occurrence et l'amplitude de la gravité du danger [Mer04]. Ces deux critères sont le plus souvent gradués suivant quatre niveaux, adaptés selon le domaine d'application. Par exemple, les échelles peuvent être : faible, moyen, grave et très grave pour la gravité ; très improbable, improbable, probable et très probable pour la probabilité d'occurrence. Avec ces deux critères, une matrice de criticité est construite afin d'envisager toutes les combinaisons possibles.

L'évaluation des risques est utilisée dans différents domaines. Ainsi, en médecine, les risques d'apparition d'une maladie cardio-vasculaire [Mye07] sont évalués suivant plusieurs facteurs dont

notamment le mode de vie du patient. Pour parvenir à une bonne coopération dans le partage des ressources dans un réseau informatique, Liang [Lia05] propose un modèle de confiance prenant en compte la réputation et les risques pour les utilisateurs. L'évaluation du risque lié à l'utilisation des produits chimiques en entreprise [Vin00] est réalisée pour établir une démarche de prévention du risque et limiter ainsi les accidents. L'évaluation des risques peut donc avoir des objectifs différents selon l'application.

La perception du risque et les besoins étant différents suivant les domaines industriels concernés, une étude propose de considérer plus de deux critères pour caractériser le risque [Kli02]. L'évaluation du risque devient alors plus compliquée puiqu'elle nécessite plus d'informations sur le système étudié. Plus significative que l'analyse du danger, l'évaluation des risques nécessite cependant de connaitre les probabilités d'occurrence des événements considérés. Dans mes recherches, ces données n'étant pas connues, **l'étude portera sur une analyse du danger**.

II.4.2 Outils d'analyse

Présentation

Pour évaluer les situations dangereuses et à risque d'un système, plusieurs analyses peuvent être effectuées par les industriels en amont de la conception et lors du développement des systèmes afin d'améliorer leur sécurité. Des échanges sur les résultats obtenus sont ensuite réalisés entre client et fournisseur pour prendre en considération ces aspects le plus tôt possible. Par exemple, une analyse fonctionnelle précède une étude de sûreté de fonctionnement et permet de mieux comprendre les objectifs du système à concevoir.

Ainsi, au cours d'un projet européen d'aéronautique [Ake06], des méthodes et outils ont été mis en place en amont de la phase de conception pour évaluer et améliorer la sécurité du système embarqué développé. Plusieurs analyses sont nécessaires au développement de ce type de système complexe à haute sécurité. Afin de maitriser les risques de contamination possible de l'eau potable publique, une étude [Hel00] propose de réaliser une analyse du danger tôt dans le processus de production. Avec cette analyse, l'objectif est d'avoir l'assurance d'une qualité d'eau supérieure et de meilleures possibilités d'amélioration. Dans le domaine de l'exploitation minière [Kom08], une analyse préliminaire des risques est réalisée afin de caractériser les blessures existantes. Ainsi, les efforts à réaliser pour minimiser le nombre de ces blessures sont mis en évidence. Une matrice de criticité donne les différents niveaux de risque choisis (figure II.2).

Proposed risk matrix

	Severity		
	I	II	III
Frequency			
A (Frequent)	High	High	Serious
B (Probable)	High	Serious	Moderate
C (Occasional)	Serious	Serious	Moderate
D (Remote)	Serious	Moderate	Low
E (Rare)	Moderate	Low	Low

Figure II.2 – Matrice de criticité [Kom08]

Thales - RATP

Entre Thales et la RATP, lors du développement de nouveaux systèmes de supervision d'une ligne de métro, plusieurs analyses préliminaires sont également effectuées. L'analyse fonctionnelle [Tha04a] décrit les différentes fonctions de protection et de contrôle qui devront être supportées par le système. La figure II.3 présente les sous-fonctions d'une fonction principale d'exploitation : la commande des manœuvres.

Fonction Principale	Sous Fonction
La commande des manœuvres en ligne et en terminus	Commande manuelle des manœuvres ❑ Commandes Individuelles des Itinéraires (CII) ❑ Commandes Programmées d'itinéraires (CPI)
	Commande Automatique de Parcours (CAP)
	Commande Automatique des Itinéraires (CAI)

FIGURE II.3 – Exemple d'une fonction d'exploitation opérationnelle [Tha04a]

L'Analyse Préliminaire des Dangers (APD) [Tha04b] identifie et liste les événements redoutés pouvant conduire à des situations dangereuses et évalue la gravité de ces situations. Ainsi, pour l'accident *Déraillement du train*, il existe plusieurs causes possibles (figure II.4).

Description de l'accident	Cause(s) potentielle(s) à l'origine de l'accident non prise(s) en compte par le PCC	Cause(s) potentielle(s) à l'origine de l'accident prise(s) en compte par le PCC
Déraillement du train	❑ incident mécanique sur une rame (rupture d'essieu p.e.) ❑ incident mécanique des équipements sol (rail cassé, aiguille défectueuse, etc) ❑ Incident sur la voie (obstacle, travaux, etc) ❑ non respect des consignes par un conducteur (vitesse excessive en conduite manuelle, p.e.) ❑ Non respect par OURAGAN en mode de conduite automatique, des vitesses limites théoriques (fonction du profil de la voie)	❑ Survitesse du train due à la transmission erronée d'une Limitation Temporaire de Vitesse (LTV) ou d'un Ralentissement Provisoire (RP) entre le PCC et le système OURAGAN) dans le cas d'un rail cassé.

FIGURE II.4 – Exemple des causes à l'origine d'un accident [Tha04b]

L'Analyse Préliminaire des Risques (APR) [Tha04c] s'attache à déterminer et analyser les risques et estime la probabilité d'occurrence des situations dangereuses. Le registre des situations dangereuses [Tha09] assure la traçabilité complète du traitement des dangers depuis leur identification dans l'APD initiale jusqu'au contrôle des mesures de réduction de ces dangers.

Application aux transports ferroviaires guidés

Pour améliorer la sécurité des systèmes de transport dès la phase de conception, une analyse préliminaire des risques peut être réalisée. Dans [Gue08], F.Guenab présente une nouvelle approche et une description de l'ensemble des phases d'analyse à effectuer dans une analyse préliminaire des risques complète dans le domaine des transports. En parallèle de ces analyses, M.H.Mazouni [Maz09] propose une méthode pour modéliser les processus de déclenchement

d'accident afin de développer un outil pour le management du risque. Plusieurs recherches s'intéressent également à l'évaluation du risque [Bre08][Leg09][Beu06] et réalisent une analyse des événements conduisant à une défaillance du système avec pour objectif de maitriser ces risques.

Pour renforcer le processus d'analyse, un retour d'expérience peut être réalisé pour recréer le scénario qui a mené à un accident [Mej10]. Une modélisation des connaissances et l'utilisation de méthodes d'apprentissage automatiques donnent ainsi la possibilité d'améliorer la sécurité du système. Des barrières physiques, fonctionnelles et opérationnelles peuvent être développées dans le système pour éviter des accidents [Hol99].

L'ensemble de ces recherches sur la sûreté de fonctionnement s'applique au domaine des transports ferroviaires guidés dont fait partie le métro et se concentre principalement sur la notion de risque plus que sur celle de danger. De plus, l'objectif de ces analyses est de proposer des solutions pour éviter qu'un incident se produise soit en modifiant la structure du système soit en l'adaptant dès sa conception. **Ces études ne s'intéressent donc pas aux méthodes permettant de gérer un incident pour éviter l'apparition d'un accident**.

II.4.3 Recherches réalisées au LAAS de Toulouse

Plusieurs thèses ont été réalisées successivement au Laboratoire d'Analyse et d'Architecture des Systèmes (LAAS) de Toulouse avec pour objectif global l'amélioration de la conception des systèmes embarqués sûrs de fonctionnement. Leur méthode est basée sur une analyse qualitative du modèle réseau de Petri du système. Cette analyse permet d'extraire et d'identifier tous les types de comportements conduisant à des états pour lesquels la sécurité des utilisateurs n'est plus assurée. Elle détermine ainsi des scénarios redoutés et les caractérise en termes d'actions et de changements d'états.

Dans la thèse réalisée en 1998 [Mon98] et en collaboration avec PSA, G.Moncelet s'est intéressé à la sûreté de fonctionnement de systèmes mécatroniques. L'objectif de sa thèse est de proposer une méthode de mise en évidence des scénarios redoutés en s'appuyant sur une modélisation par réseaux de Petri coloré et une simulation de Monte Carlo pour estimer la probabilité d'occurrence des scénarios. La méthode d'identification de scénarios redoutés a été appliquée à un système de contrôle de pression de suspension hydraulique de véhicule.

Dans la continuité des travaux de G.Moncelet, le travail de thèse de S.Khalfaoui [Kha03] en 2003 se focalise sur l'aspect hybride des systèmes mécatroniques en séparant clairement les aspects discrets et continus du système étudié. Cette nouvelle approche limite l'ensemble des états à étudier à ceux impliqués dans l'apparition des scénarios redoutés.

La thèse de N.Sadou [Sad07] en 2007 a poursuivi les travaux précédents afin d'améliorer l'approche et d'aborder certains aspects non traités. Une définition formelle de la notion de scénario basée sur la logique linéaire a été proposée. La notion de minimalité a été introduite dans l'outil de génération de scénarios redoutés pour éliminer un bon nombre de scénarios non minimaux générés dans les versions précédentes.

La continuité et la progression dans ces recherches au sein d'un même laboratoire ont permis de développer un algorithme pour identifier les scénarios redoutés dans le domaine de la mécatronique. Les recherches effectuées au LAAS utilisent la modélisation des systèmes par réseaux de Petri pour mettre en évidence des événements redoutés sur des systèmes hybrides, discrets et continus. Le caractère hybride des systèmes étudiées différencie les recherches du LAAS et les

recherches présentées dans cette thèse puisque le système étudié est discret. Ainsi, les contraintes et les modélisations diffèrent. De plus, les probabilités d'occurrence des scénarios sont évaluées par simulation, ce qui implique une analyse des risques et pas seulement du danger. Cependant, l'identification des scénarios redoutés est effectuée par raisonnement arrière en partant des états à éviter. Ce type d'analyse permet une anticipation du danger examiné lors du développement d'aide à la décision comme dans cette thèse. Même si le domaine d'application et le type de système diffèrent entre les recherches du LAAS et mes recherches, la démarche réalisée pour **identifier des scénarios redoutés** pourra être exploitée pour une première analyse du système à étudier.

II.4.4 Recherches réalisées au laboratoire Ampère

Plusieurs travaux précédant mes recherches et en lien avec la sûreté de fonctionnement ont été effectués au sein du laboratoire Ampère pour améliorer la sécurité opérationnelle dans les systèmes automatisés de production. La sécurité opérationnelle est l'analyse des états du système pour reconnaitre les situations dangereuses et enclencher les actions de compensation nécessaires pour notamment assurer la continuité de service.

Dans sa thèse, N.Rezg [Rez96] définit un état interdit comme un état qui contient une incompatibilité avec la situation courante du système et peut représenter une violation des fonctionnements admissibles. Une zone d'influence regroupe l'ensemble des états nécessaires pour la représentation du danger. À partir de cette zone, il est important de déterminer les chemins de sécurité ne conduisant pas à un état interdit malgré la présence d'une défaillance. Des actions de compensation par retour d'état sont mises en place pour assurer la continuité du service après une défaillance ainsi que des boucles de surveillance pour des fonctions de détection et de diagnostic. La démarche proposée est appliquée sur un processus manufacturier de test.

En parallèle des recherche de N.Rezg, M.Nourelfath [Nou97] étudie la mise en place d'un mécanisme de surveillance d'un système en vue d'assurer la continuité de service en présence d'une défaillance jusqu'à sa correction. Au cours de ces travaux, une seule défaillance peut se produire à la fois. Pour cela, un module de surveillance est déterminé. Dans la continuité de la thèse précédente, O.Kamach [Kam04] poursuit l'étude dans le cas où plusieurs défaillances peuvent survenir. De plus, il caractérise également des ensembles de comportements en définissant des modes de fonctionnement et en considérant qu'une défaillance est une perturbation du mode de fonctionnement nominal. Il étudie également l'alternance entre les différents mode de fonctionnement d'un système.

La dernière thèse dans ce domaine effectuée au laboratoire Ampère a été soutenue en 2010 par G.Faraut [Far10]. Dans son étude, il propose une démarche de conception appliquée à une gestion modale. Cette nouvelle méthode respecte l'unicité du mode actif et complète l'étude sur l'alternance entre les modes. Ainsi, les différentes commutations entre les modes sont modélisées et respectent les exigences de sécurité du système.

Même si le contexte d'application a changé, passant des systèmes automatisés de production aux systèmes embarqués, et maintenant au monde des transports, il existe une **continuité dans les recherches** effectuées au sein du laboratoire Ampère. En effet, l'analyse et la synthèse des systèmes étudiées, avec comme objectif principal d'**améliorer la sécurité des systèmes**, se basent sur les même principes et progressent au cours des thèses.

II.5 Comment éviter des situations dangereuses ?

II.5.1 Contrôle des systèmes

Pour éviter de rencontrer des situations de danger lors du fonctionnement d'un système, il faut s'intéresser à l'évolution du système, sans se préoccuper des aspects de performance, et en gardant pour objectif de contrôler le système. Des méthodes formelles ont ainsi été développées pour s'assurer que les systèmes soient fiables et que leurs comportements satisfassent les exigences de sécurité à respecter. Pour cela, deux types d'approches existent : la vérification et le contrôle par supervision des systèmes.

Les méthodes de vérification testent le modèle d'un système par rapport au respect des exigences et des propriétés recherchées avec des techniques comme le model-checking, l'analyse statique et les tests. Ainsi, à partir de spécifications formelles décrites par formules de logiques temporelles et d'une abstraction du comportement du système, les algorithmes de model-checking vérifient si le système satisfait les spécifications.

L'approche du contrôle par supervision peut s'appliquer si le système à étudier n'est pas encore conçu mais que les contraintes à considérer sont connues. Des contrôleurs sont alors calculés afin de contraindre le système pour que seuls les comportements autorisés soient possibles. Un contrôleur est un système qui interagit avec le système étudié pour s'assurer que les exigences soient respectées. L'objectif est donc de s'assurer qu'il est possible de respecter les spécifications et de savoir comment le système peut les satisfaire.

Ces deux approches se basent sur l'occurrence et l'impossibilité d'occurrence des événements se produisant dans un système et s'appliquent donc sur des modèles de systèmes à événements discrets. Ainsi, pour vérifier des propriétés de cohérence sur des processus métier, une approche a été proposée dans [Sba13] et [Sba10] en se basant sur les techniques de model-checking. Les processus sont tout d'abord traduits dans le langage Promela [3] pour décrire le comportement du système sous forme de réseaux de Petri puis associés à des propriétés exprimées en Logique Temporelle Linéaire (LTL). Ces propriétés sont ensuite vérifiées avec des algorithmes de model checking. La vérification se fait donc sur des systèmes à événements discrets et pas directement sur les modèles de processus.

Dans notre étude, l'**approche du contrôle par supervision** a été choisie afin de calculer un système évitant des états de danger. En effet, dans le cadre de la sûreté de fonctionnement, le système doit prendre en compte les exigences de sécurité *a priori* et non *a posteriori* par vérification, la sécurité des personnes devant être prise en compte dès la conception des systèmes.

II.5.2 Théorie du contrôle par supervision

Présentation

Pour déterminer un contrôleur garantissant à un système (le procédé) de respecter un ensemble d'exigences (les spécifications) et ainsi connaitre les évolutions acceptables du système (le procédé sous contrôle), une théorie a été développée : la Théorie du Contrôle par Supervision (TCS). Cette théorie a été initiée par Wonham et Ramadge en 1987 [Won10][Ram87][Ram89] et permet donc de séparer la modélisation d'un système à événements discrets et celles des

3. Process Meta Language

spécifications qu'il doit respecter. Cette théorie est basée sur des formalismes mathématiques comme la théorie des langages [Car08] et les automates à états [Cas99] pour la représentation graphique. La théorie du contrôle par supervision est une approche générale pour synthétiser le contrôle des systèmes à événements discrets.

Les spécifications sont de deux types : les spécifications de sécurité et les spécifications de vivacité. Les spécifications de sécurité représentent ce que le système ne doit pas faire, ce qui consiste à interdire des successions d'événements dangereuses. Les spécifications de vivacité expriment ce que le système doit faire, ce qui revient à n'autoriser qu'un certain nombre d'événements dans un état donné.

Par synthèse du procédé et de ses spécifications, un modèle de commande complet qui respecte l'ensemble des propriétés voulues est déterminé : un superviseur. Ce superviseur, s'il existe, va contraindre le comportement du procédé en interdisant et autorisant des événements. Il contrôle le procédé en l'empêchant dynamiquement de générer des événements qui auraient pu être générés, le procédé sous contrôle est ainsi défini et calculé. La théorie du contrôle par supervision démontre qu'en associant un procédé et ses spécifications, il existe toujours un superviseur optimal vérifiant les propriétés du cahier des charges et permettant au système d'accomplir sa tâche. Le superviseur synthétisé est dit permissif car il laisse au système la plus grande liberté possible en terme de génération d'événements, tout en respectant les limites fixées par le cahier des charges.

La théorie considère également une propriété de sécurité : la contrôlabilité des systèmes [Bra90] [Bra00]. Le superviseur est un dispositif de sécurité qui empêche le procédé d'exécuter des événements qui conduiraient le système contrôlé à un comportement non autorisé dans le cahier des charges. Cependant, le superviseur ne peut pas interdire certains événements dits incontrôlables. Le superviseur doit également être non bloquant et garantir ainsi qu'au moins un état final puisse être atteint par tous les états accessibles du système contrôlé.

Le critère d'observabilité d'un événement est également intégré dans la théorie du contrôle par supervision et lors de la synthèse du superviseur. Un événement est observable s'il est visible par le superviseur et inobservable sinon. L'étude réalisée dans cette thèse se place dans un cadre idéal où le superviseur a une vision parfaite du système et observe tous les événements se produisant dans le système : **l'ensemble des événements est donc observable**.

Pour résumer, la théorie du contrôle par supervision garantit l'existence d'un superviseur permissif au maximum, contrôlable et non bloquant pour un procédé et des spécifications données. Le résultat obtenu peut être l'ensemble vide si aucune trajectoire ne respecte l'ensemble des spécifications ou si elles ne sont pas contrôlables. Le calcul du superviseur par la théorie du contrôle par supervision peut être long en raison de l'explosion combinatoire de la taille des modèles.

Deux approches existent pour formuler les spécifications que le système doit respecter : l'approche langage et l'approche état. Suivant l'approche choisie, le superviseur exprimera un langage à respecter en se basant sur les événements ou un ensemble d'états à éviter. L'approche langage décrit les spécifications sous forme de successions d'événements modélisées par automates à états alors que l'approche état considère les états du système à interdire.

L'étude développée dans ce mémoire propose d'éviter un ensemble d'états identifiés comme dangereux dans un système à événements discrets et liés à la structure même du système. **En s'appuyant sur la théorie du contrôle par supervision, l'approche état est donc plus**

adaptée puisque les exigences sont exprimées en termes d'états à éviter, les états interdits, et non en terme de comportements permettant d'atteindre ces états.

Problème des états interdits

Dans [Hol90], L.E.Holloway propose une solution algorithmique efficace pour résoudre le problème du contrôle des états interdits et l'applique à la coordination de chariots guidés dans une usine. En modélisant le système étudié par réseaux de Petri et en identifiant les marquages à ne pas atteindre, l'application de la théorie du contrôle par supervision permet d'obtenir un contrôleur maximum permissif assurant l'évitement des états non désirés.

L'étude [Gha03b] développe les recherches effectuée par L.E.Holloway pour les étendre aux réseaux de Petri prenant en compte la contrôlabilité des transitions. Les états interdits sont alors caractérisés par des contraintes sur le marquage du RdP en définissant des bornes limites sur les marquages. Une zone d'influence pour un état donné regroupe l'ensemble des états qu'il faut éviter pour assurer que cet état ne soit pas atteignable dans le système. Les états de cette zone sont tous liés les uns aux autres par au moins une transition incontrôlable.

B.Gaudin [Gau03] définit l'ensemble des séquences d'événements pour éviter d'atteindre un état interdit. Dans son étude, le contrôle du procédé, modélisé comme un automate à état asynchrone et hiérarchique, est réalisé afin de résoudre le problème de contrôle d'évitement d'état. Résolu localement, un superviseur global assurant la propriété globale est donné. Dans sa thèse[Gau04], il généralise son approche au problème d'interdiction d'états pour des systèmes concurrents modélisés par des réseaux de Petri saufs et conservatifs.

Le problème étudié dans ces publications consiste à contrôler le système de manière à ce que celui-ci **évolue dans un ensemble d'états admissibles et n'atteigne pas un ensemble d'états interdits** correspondant à des caractéristiques du système. Les séquences d'événements menant à un état interdit sont analysées et selon leur contrôlabilité, sont autorisées ou interdites.

Choix de la modélisation

Initialement basé sur les automates à états finis, la théorie du contrôle par supervision s'applique également aux réseaux de Petri par différentes intégrations [Hol97][Bou05][Lee06], dont les états interdits. L'approche état de la théorie du contrôle par supervision semble même plus adaptée à une modélisation par réseaux de Petri puisqu'un état interdit peut être défini par un marquage complet ou partiel. Inversement, pour l'approche langage, les spécifications à respecter sont plus facilement exprimées par des automates à états puisqu'elles décrivent des comportements à éviter et sont donc associées aux séquences d'événements des automates.

Dans notre étude, **la modélisation du système étudié se fera par réseaux de Petri** afin d'appliquer l'approche états de la théorie du contrôle par supervision pour éviter un ensemble d'états définis comme dangereux dans le système. Après avoir identifié l'ensemble des états à ne pas atteindre pour respecter les exigences, l'existence d'un contrôleur doit être vérifiée puis le contrôleur pourra être intégré au système pour obtenir le procédé sous contrôle du système étudié.

II.5.3 Intégration du contrôle dans un réseau de Petri

La méthode développée par A.Giua dans [Giu92] utilise des conditions associées aux marquages des places pour résoudre le problème d'interdiction d'états. Il définit les contraintes généralisées d'exclusion mutuelle (Generalized Mutual Exclusion Constraints, GMEC) comme une condition qui limite le nombre de marques dans un sous-ensemble de places. Chaque état interdit correspond alors à une contrainte linéaire sur les marquages à respecter. Les auteurs présentent comment passer d'un marquage interdit à une contrainte linéaire équivalente. Cette méthode est applicable seulement si le réseau de Petri modélisant le système est sauf et conservatif.

La théorie des régions, utilisée dans [Gha03a], généralise l'approche précédente en considérant les transitions des réseaux de Petri comme contrôlables ou incontrôlables. Cette méthode génère des contraintes pour empêcher le système d'atteindre les états interdits et réduit ainsi l'espace d'états atteignable par le système. Même si le nombre de contraintes engendrées peut être important pour s'assurer que les exigences soient respectées, le comportement autorisé par ces contraintes est maximum permissif.

À partir de l'ensemble des marquages autorisés et définis sous forme de contraintes linaires, A.Dideban [Did08][Did13] développe deux méthodes pour simplifier ces contraintes et ainsi réduire leur taille et leur nombre. En effet, le nombre de places de contrôle à intégrer dans le réseau de Petri pour satisfaire les exigences est égal au nombre de contraintes décrivant ces exigences. La complexité du réseau de Petri contrôlé obtenu dépend donc du nombre de ces contraintes. La méthode de simplification proposée par A.Dideban se base sur l'approche de A.Giua et se limite également aux réseaux de Petri conservatifs et saufs. Ces deux propriétés doivent donc être vérifiées avant d'appliquer la démarche complète.

La théorie présentée par A.Giua combinée aux méthodes de simplifications proposées par A.Dideban garantit l'équivalence entre les exigences définies par un ensemble d'états interdits et les contraintes simplifiées obtenues. Pour prendre en compte ces contraintes et déterminer le système sous contrôle, il faut intégrer un contrôleur au réseau de Petri sous forme de places de contrôle.

K.Yamalidou [Yam96] propose une méthode pour construire un contrôleur à partir des contraintes linéaires. Elle présente le calcul de la matrice d'incidence d'un réseau de Petri, représentant la structure du réseau, complétée par des places de contrôle pour ainsi décrire la structure complète du réseau contrôlé. Cependant, les recherches de K.Yamalidou ont montré que le contrôleur calculé est maximum permissif seulement si tous les événements sont contrôlables. A.Dideban [Did07] a démontré que la propriété de maximum permissif était également vérifiée s'il existait des transitions incontrôlables dans le système pour des réseaux de Petri conservatifs et saufs.

II.5.4 Recherches réalisées au laboratoire Ampère

L'application, l'étude et l'extension de la théorie du contrôle par supervision (TCS) sont des sujets de recherche abordés au sein du laboratoire Ampère.

Ainsi, pour parvenir à la sécurité opérationnelle d'un système, N.Rezg [Rez96] se base sur des principes de la TCS. Son objectif de recherche consiste à déterminer des états admissibles à partir desquels l'atteignabilité des états interdits est exclue par l'adjonction d'un contrôle approprié. Le comportement des systèmes étudiés est décrit par réseaux de Petri et dans l'ensemble des états

accessibles, la méthode du chainage arrière permet d'identifier la transition qui a mené à un état interdit. L'objectif de supervision est donc de garantir la non accessibilité d'un ensemble prédéfini d'états interdits par analyse du graphe d'accessibilité et en tenant compte de la contrôlabilité des événements. Après avoir évalué la sécurité du système au travers des états accessibles, l'étude a identifié le moyen d'éviter ces situations en mettant en place un contrôle du système.

Dans les études portant sur la conception de modèles représentant un comportement modal, l'application de la théorie du contrôle par supervision assure que les modèles créés sont sûrs par construction. Dans ces recherches réalisées sur les modes de fonctionnement, O.Kamach [Kam04] propose une extension de la TCS pour la gestion des modes de fonctionnement. L'objectif est de pouvoir définir un contrôleur pour chaque mode de fonctionnement. En adoptant une approche multi-modèle, un modèle est défini pour chaque comportement du système dans un mode donné. G.Faraut [Far10] s'appuie également sur la TCS pour construire les modèles de modes et assurer que les contraintes spécifiées sur les commutations du système soient respectées tout en garantissant une contrôlabilité du système.

Dernièrement, une étude a été effectuée avec une application dans le monde des transports. Dans [Haj13], S.Hajjar développe une méthode de conception sûre de systèmes utilisant des COTS [4] pour du matériel embarqué. La méthode permet d'éviter les situations dans lesquelles il serait possible de réaliser des actions de contrôle-commande incorrectes voire dangereuses pour le système complet.

Des travaux plus théoriques sur l'extension de la théorie du contrôle par supervision ont également été effectués [Sar99] en se basant sur la structure vectorielle des systèmes à événements discrets. L'objectif de ces travaux est d'assurer la stabilisation et le contrôle optimal de trajectoires en cas de défaillance dans un système de production.

L'ensemble de ces travaux précédant ma recherche et effectués dans le laboratoire Ampère montre l'intérêt depuis près de 20 ans pour l'étude de la théorie du contrôle par supervision et les nombreuses compétences acquises dans ce domaine. L'application de la TCS dans mes recherches se place donc dans la continuité de précédents travaux. **L'originalité réside dans le domaine d'application : l'étude de procédures de gestion d'incidents se produisant pendant l'exploitation d'une ligne de métro et la définition complémentaire et distincte des états interdits.**

II.6 Problématique

II.6.1 Problèmes constatés par l'industriel

Au préalable de notre étude, plusieurs problèmes avaient été constatés par l'industriel Thales. Ces problèmes concernent autant un manque d'aide apportée à l'opérateur de supervision que les problèmes de ses propres clients qu'il souhaite résoudre. Le constat de ces problèmes a motivé la réalisation mes recherches.

Problèmes de l'industriel Thales

Thales développe son logiciel de supervision d'une ligne de métro ATS suivant les projets réalisés, ses propres connaissances du métier d'exploitant et son expérience. Cependant, concer-

4. Commercial off-the-shelf

nant la gestion des incidents, il existe un savoir-faire métier qui est propre à chacun de leurs clients et inconnu pour Thales. Ce manque d'informations sur les incidents entraîne une compréhension insuffisante des attentes client dans ce domaine de la supervision. En effet, après avoir été choisi pour superviser une nouvelle ligne, Thales configure son logiciel ATS pour qu'il corresponde au cahier des charges défini par le client. L'application adaptée à la ligne de métro est ensuite utilisée par les opérateurs de supervision pour gérer le trafic des trains, sa principale fonctionnalité. Concernant la gestion des incidents, les clients de Thales mettent en place leurs propres procédures. Ces procédures ne sont pas présentées dans les cahiers des charges et sont donc inconnues pour Thales. Aussi, il peut en résulter un manque de savoir-faire métier pour Thales sur la gestion des incidents réalisée par ses clients. Ce défaut provoque un manque de visibilité des attentes client et potentiellement une inadéquation entre les besoins et les services apportés pour la gestion des incidents pendant l'exploitation d'une ligne de métro.

Le système ATS développé par Thales signale par alarmes les dysfonctionnements en lien direct avec le trafic ou concernant l'acquisition des données effectuée sur la ligne. Lorsqu'un incident d'exploitation lié à la sécurité des personnes se produit, le logiciel apporte des outils à l'opérateur pour gérer l'impact de l'incident sur le trafic et l'exploitation. Ces outils donnent la possibilité à l'opérateur de supervision d'offrir aux passagers le meilleur service possible. Cependant, à l'heure actuelle, l'aide ainsi présentée aux opérateurs est insuffisante puisqu'elle ne propose pas des solutions pour une gestion globale de l'incident mais seulement des outils pour le gérer.

L'aide, aujourd'hui insuffisante, apportée à l'opérateur ne s'organise pas dans une fonctionnalité spécifique pour la gestion des incidents. Le logiciel n'intègre pas de système d'aide à la décision pour conseiller à l'opérateur un ensemble d'actions à réaliser, ordonnés suivant une démarche particulière, étudiée et optimisée pour la sécurité et le retour à une exploitation de la ligne.

Problèmes Client

Comme détaillé dans les postulats (section I.3), l'étude se restreint aux incidents gérés par des procédures mémorisées par les opérateurs de supervision. La mise en œvre de ces procédures dépend donc de la mémoire des opérateurs et peut changer suivant la personne les exécutant. En effet, suivant l'expérience et les habitudes, la stratégie mise en place peut varier selon les opérateurs. La connaissance d'une situation similaire peut également aider l'opérateur dans sa prise de décisions et ainsi améliorer sa réactivité face à un incident. L'application des procédures mémorisées n'est donc pas forcément uniforme entre les opérateurs de supervision et les conséquences sur la sécurité des personnes et le trafic peuvent ainsi varier pour un même incident.

Le contexte de la gestion d'incidents a été décrit dans la section I.2.2 ainsi que les responsabilités de l'opérateur de supervision associées. L'opérateur se trouve dans un environnement stressant susceptible de diminuer sa concentration voire d'altérer son jugement de la situation. Face à une situation d'incident, le contexte difficile peut également inhiber ou fausser sa prise de décisions. Un opérateur peut oublier les actions qu'il doit réaliser ou agir de manière trop précipitée sans vérifier toutes les conditions d'application d'une action, même si les opérateurs de supervision sont formés pour gérer ce type de situations.

La découverte de nouvelles situations avec incidents se fait la plupart du temps seulement lorsque l'incident se produit et n'a pas pu se faire avant. À ce moment-là, il est difficile pour

l'opérateur de prendre les bonnes décisions et de savoir comment réagir puisqu'il n'a pas été formé à cette situation et qu'aucune procédure existe pour gérer l'incident. Il est souvent nécessaire d'attendre un accident inédit pour développer la procédure permettant de le gérer par retour d'expérience. Le développement de nouvelles procédures est malheureusement souvent l'une des conséquences d'un accident et correspond à une mesure prise pour éviter une nouvelle occurrence.

II.6.2 Problèmes révélés par l'étude

Au début de l'étude et suite à l'acquisition du savoir-faire métier sur la supervision d'une ligne de métro, d'autres problèmes ont été identifiés.

Les procédures de gestion d'incidents ont été développées pour réagir chacune à un type d'incidents spécifique. Lorsqu'au moins deux incidents se produisent de manière conjointe, il existe une procédure pour gérer chacun de ces incidents mais il n'y a pas de coordination entre les procédures. En effet, les procédures ont été définies de manière indépendantes les unes des autres. Elles ne permettent donc pas de gérer plusieurs incidents de façon coordonnée et en tenant compte des interactions possibles entre ces procédures. Une évolution simultanée de plusieurs procédures peut potentiellement conduire à une situation plus dangereuse que la situation initiale et être non maitrisable par l'opérateur de supervision. Un accident grave est parfois la conséquence de l'addition de plusieurs circonstances exceptionnelles associées à un manque d'informations sur les réactions appropriées à avoir dans un tel moment.

Les procédures de gestion d'incidents liées à la sécurité des personnes sont apprises par les opérateurs de supervision de la RATP au cours d'une formation et à partir d'un document décrivant les procédures de manière textuelle dans un langage informel uniquement. La description des procédures ne repose donc pas sur une représentation standardisée mais seulement sur un texte. Ce type de représentation des procédures ne permet pas de les analyser et de les étudier de manière uniforme en s'appuyant sur principes établis. Ainsi, il serait difficile de s'appuyer sur un texte pour identifier d'éventuelles interactions entre procédures.

Pour superviser une ligne de métro, l'opérateur a besoin de nombreuses informations sur l'état de la ligne qui doivent être disponibles à tout moment. Ces informations lui sont notamment communiquées au travers de l'interface homme-machine de son poste de travail. L'opérateur doit être capable d'assimiler ces informations, de les analyser et de réagir en conséquence. Cependant, plus le nombre d'informations est grand, plus il est difficile pour l'opérateur d'identifier rapidement les informations prioritaires et donc d'être réactif. L'ergonomie de l'interface et la hiérarchie des éléments à lui transmettre sont à prendre en considération pour aider l'opérateur de supervision dans sa gestion des incidents et ne pas au contraire compliquer son jugement.

Lorsqu'un incident se produit, la situation atteinte est la plupart du temps une situation de danger. Une évaluation de ce danger peut alors permettre d'appréhender et de mieux comprendre la situation atteinte. À l'heure actuelle, lors de l'occurrence d'un incident sur une ligne de métro et de l'exécution de la procédure correspondante, aucune évaluation du danger encouru par les personnes concernées par l'incident n'est réalisée.

II.6.3 Objectifs

Afin d'analyser et de répondre à l'ensemble de ces problèmes, plusieurs objectifs d'étude sont spécifiés.

Le premier objectif de cette étude est d'acquérir du savoir-faire métier sur l'exploitation d'une ligne de métro et plus particulièrement sur la gestion des incidents, liés à la sécurité des personnes, pouvant s'y produire. Ce premier objectif est essentiel et permet d'obtenir une base de connaissances et de données nécessaires pour la suite de l'étude. Le but est également de prendre conscience des difficultés rencontrées par les exploitants lors de la supervision d'une ligne et d'identifier les contraintes du métier d'exploitant. L'ensemble de ce savoir ne doit pas seulement être acquis par une personne mais doit également être transmis à l'industriel Thales. Ainsi, l'enrichissement de ses connaissances et de ses compétences pourra lui permettre de concevoir des produits au plus proche des attentes de ses clients.

Après avoir acquis cet ensemble de connaissances sur la gestion des incidents, le but est d'analyser et d'approfondir les procédures développées et utilisées par la RATP. Pour faciliter cette étude, une standardisation de l'écriture des procédures est nécessaire. Le deuxième objectif est donc de choisir une représentation adaptée et pertinente pour l'étude des procédures de gestion d'incidents. Cette représentation doit également pouvoir encourager et avantager la transmission d'informations et les échanges entre Thales et ses clients.

Lors de l'occurrence d'incidents, les voyageurs et le personnel présents sur la ligne de métro se retrouvent potentiellement dans une situation de danger. Pour identifier et caractériser ces situations, il faut tenir compte et étudier le contexte dans lequel la ligne se trouve au moment de la gestion de l'incident. L'objectif est de replacer les procédures dans l'environnement dans lequel elles sont exécutées et ainsi déterminer le contexte dans lequel les personnes présentes seraient en sécurité.

Pour apporter une aide à l'opérateur de supervision, l'objectif est d'implanter dans le logiciel les procédures décrivant la succession des activités à réaliser lors de la gestion d'incidents. La transmission d'informations doit se faire dans un langage normalisé de modélisation de processus métier pour faciliter la compréhension et améliorer l'efficacité. Une intégration des procédures dans l'interface proposée aux opérateurs de supervision leur apporterait une visualisation en temps réel de l'évolution des procédures en cours et les informerait sur les actions à réaliser. Ainsi, l'application ne donnerait pas seulement des outils pour gérer ces situations, comme c'est le cas aujourd'hui, mais également des méthodes d'utilisation.

Pour éviter les situations pouvant porter atteinte à la sécurité des personnes, l'objectif est d'implanter dans le logiciel, non seulement les procédures de gestion d'incidents, mais également des séquences d'activités sûres afin de conseiller les opérateurs lors de la supervision d'une ligne de métro. En réalisant une analyse en temps réel du niveau de danger atteint, des alertes et des conseils pourront être proposés aux opérateurs en cas d'évolution simultanée de plusieurs procédures. L'opérateur serait ainsi orienté dans la succession des actions à réaliser pour assurer au mieux la sécurité des voyageurs et du personnel présents sur la ligne.

II.7 Positionnement et démarche d'étude

II.7.1 Positionnement

Pour traiter les problèmes de l'étude identifiés et atteindre les objectifs définis, des solutions ont été choisies en s'appuyant sur les recherches déjà effectuées dans la communauté scientifique et présentées dans l'état de l'art.

Les projets SART et SpicaRail (section II.1.1) réalisés sur la supervision d'une ligne de métro, et plus particulièrement sur la gestion des incidents, ont permis de définir des problèmes abordés dans notre étude. Les conclusions de ces travaux ont permis d'améliorer ma compréhension de la supervision d'une ligne de métro, mes connaissances sur ces contraintes et enjeux et mettre en avant certains problèmes classiques. Aussi, une collaboration entre l'industriel Thales, fournisseur du système d'exploitation ATS et la RATP, exploitant de métro, a été réalisée. De plus, une notation graphique adaptée et facilement compréhensible par les industriels, le BPMN, a été choisi. L'influence de la situation courante a été prise en considération lors de la modélisation par réseaux de Petri du système étudié, avec l'objectif principal d'améliorer la sécurité des personnes présentes sur la ligne.

Plusieurs études sur l'exploitation d'une ligne de métro ont permis de spécifier le cadre de l'étude. Ainsi, seuls les incidents se produisant sur les lignes avec conducteurs et pendant une journée d'exploitation seront étudiées. De plus, le point de vue adopté est celui de l'opérateur de supervision qui sera considéré comme parfait. L'étude de la supervision d'une ligne de métro se focalisera donc sur un seul mode de transport. Parmi les objectifs de recherche des systèmes de supervision, et plus particulièrement sur la gestion du trafic : l'étude se focalisera sur l'amélioration de la sécurité.

Pour effectuer l'étude des procédures de gestion d'incidents, il est nécessaire d'avoir une représentation abstraite du système et donc de le modéliser. Chaque modèle permet de répondre à un objectif précis, plusieurs représentations doivent donc être réalisées : tout d'abord avec le langage BPMN pour les processus métier puis avec des réseaux de Petri pour l'analyse du système. Ainsi, le langage BPMN représente graphiquement l'aspect fonctionnel des procédures et permet le partage des connaissances. Les réseaux de Petri apportent, quant à eux, une modélisation formelle de l'évolution du système et permettent de vérifier la concordance entre les comportements et les exigences. Une transformation entre les deux représentations est également développée pour assurer une continuité dans l'étude.

L'un des objectifs de l'étude étant d'identifier les situations dangereuses atteignables, il est important d'utiliser un vocabulaire adapté et conforme à la sûreté de fonctionnement pour définir les situations à étudier. L'étude porte donc sur l'analyse du danger afin de gérer la situation atteinte à la suite d'un incident et afin d'éviter l'apparition d'un accident. Mes travaux se positionnent dans la continuité des recherches effectuées au laboratoire Ampère dans le cadre de la sûreté de fonctionnement dans le sens où l'objectif est d'améliorer la sécurité du système étudié.

Pour ne pas atteindre un ensemble d'états dangereux ne garantissant pas la sécurité des personnes, l'approche du contrôle par supervision est adoptée. Ainsi, en appliquant la théorie du contrôle par supervision dans son approche état au modèle réseaux de Petri du système et en considérant l'ensemble des événements observable, un contrôle est déterminé. L'intégration du contrôle dans le modèle permettra d'obtenir le système contrôlé dans lequel les états interdits ne sont pas atteints.

II.7.2 Structure de la démarche d'étude

Une démarche composée de huit étapes a été développée [Paq13b] (figure II.5). Ces huit étapes sont regroupées dans trois parties : la première correspond aux deux premières étapes et est une étude de l'existant, de l'ensemble des procédures de gestion d'incidents mémorisées.

La seconde partie est composée des cinq étapes de l'étude des combinaisons de procédures et la dernière partie a été réalisée en collaboration avec Thales.

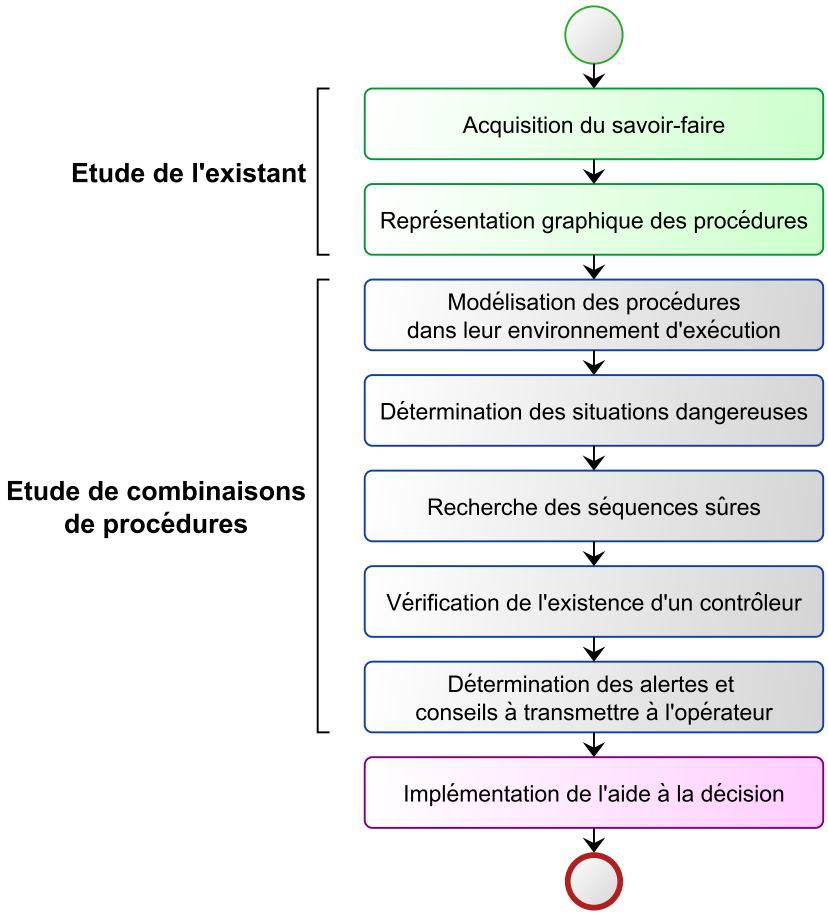


FIGURE II.5 – Démarche d'étude

Chacune des étapes de la démarche est développée dans la suite du mémoire.

- L'acquisition du savoir-faire métier sur la supervision d'une ligne de métro et plus particulièrement sur les méthodes et techniques développées pour gérer des incidents se fait au travers de la collaboration avec les industriels impliqués dans l'étude, Thales et la RATP [Paq13a] ;

- Le savoir-faire acquis est ensuite représenté graphiquement avec le langage BPMN pour obtenir des procédures de gestion d'incidents standardisées et favoriser les échanges avec les industriels ;

- Afin d'analyser ces procédures, le système d'une ligne de métro sera, dans un second temps, modélisé sous la forme d'un système à événements discrets en utilisant les réseaux de Petri. Cette modélisation sera obtenue à partir d'une transformation des modèles BPMN et intégrera les procédures dans leur environnement d'exécution ;

- En se basant sur cette modélisation par réseaux de Petri, les situations dangereuses pouvant être atteintes seront caractérisées et définies pour déterminer l'ensemble des états interdits ne garantissant pas la sécurité des personnes ;

- Afin d'éviter cet ensemble d'états, les séquences sûres seront déterminées. Pour cela, des algorithmes sont développés en se basant sur la théorie du contrôle par supervision [Paq14] ;

- Pour s'assurer de la possibilité d'éviter les états interdits, un contrôleur est calculé. La vérification de son existence est réalisée à partir du modèle réseaux de Petri du système et se base sur plusieurs études antérieures. Le système contrôlé permet ensuite de vérifier si les propriétés recherchées sont respectées ;

- À partir du système contrôlé et de l'ensemble des séquences sûres, une analyse des successions d'actions réalisables par l'opérateur de supervision est effectuée. Les alertes et conseils à transmettre à l'opérateur de supervision ainsi que le moment où ils doivent être délivrés sont alors déterminés ;

- Les résultats obtenus permettront ainsi d'implémenter une aide à la décision pour les opérateurs de supervision directement dans l'application développée par Thales. Les opérateurs pourront ainsi visualiser les procédures de gestion d'incident représentées avec la notation BPMN et être orientés lors d'incidents combinés.

III Représentation et modélisation des procédures

Résumé

L'acquisition du savoir-faire d'une exploitation de lignes de métro sur la gestion des incidents donne lieu à la classification, suivant différents critères, des incidents et des procédures permettant de les gérer. Afin d'obtenir un modèle graphique, synthétique et standardisé, les procédures sont représentées avec le langage BPMN. Pour considérer les interactions entre les procédures et le contexte de la ligne de métro, le système constitué des procédures, des signalements d'incidents et des ressources décrivant le contexte est modélisé par réseaux de Petri. Dans ce cadre, une démarche de transformation de procédures BPMN en réseaux de Petri est également développée. Ainsi, ce chapitre développe les trois premières étapes de la démarche d'étude (figure II.5).

Sommaire

III.1 Acquisition du savoir-faire

III.1.1 Présentation et objectif

Le métro est un moyen de transport utilisé par de nombreuses personnes dans les villes équipées. Tous les usagers connaissent le principe de fonctionnement général d'une ligne de métro mais subissent parfois les conséquences de problèmes d'exploitation sans en comprendre les raisons. L'exploitation et la gestion d'une ligne de métro requièrent de nombreuses personnes ayant chacune une fonction bien particulière, des compétences et des connaissances spécifiques. Le chef de régulation à la RATP (section I.2.1) est responsable de l'exploitation d'une ligne de métro, de la gestion du trafic à la gestion des incidents. Il dirige le personnel présent sur le terrain et prend les mesures nécessaires pour assurer leur sécurité et celle des voyageurs.

L'objectif de cette première étape de recherche est d'acquérir des connaissances et des compétences sur la gestion des incidents. Pour cela, la participation à une formation de chef de régulation à la RATP a permis tout d'abord de connaitre les compétences recherchées chez un chef de régulation pour assurer ses responsabilités. Le poste requière la faculté d'analyser rapidement une situation, de la réactivité dans la prise de décision, de la clarté et de la rigueur dans les communications et les ordres donnés au personnel présent sur le terrain, du calme et de la maitrise face aux incidents. Ces compétences s'améliorent progressivement avec l'expérience acquise en gérant des situations avec des incidents.

Le suivi de la formation a également permis de découvrir l'ensemble des procédures enseignées pour la gestion des incidents à la RATP. Ces procédures sont décrites sous forme de texte dans un document papier distribué au début de la session de formation à l'ensemble des stagiaires. Leur apprentissage se fait à l'aide de ce document donnant une description brute de la procédure ainsi que des explications et mises en contexte des formateurs. Les échanges avec des opérateurs de supervision et les observations de leur travail au quotidien ont également permis de connaitre les habitudes et techniques développées par ces opérateurs en marge de la théorie apprise au cours de la formation.

Avec les procédures de gestion d'incidents, d'autres données ont été collectées tout au long de la formation comme les incidents et les perturbations pouvant se produire au cours d'une journée d'exploitation. Un incident déclenche l'utilisation d'une procédure, il est donc important de les étudier. Afin de mieux comprendre l'influence et les conséquences de chaque incident sur le système, des classifications suivant la gravité et la cause de l'incident ont été réalisées.

III.1.2 Classifications des incidents

L'augmentation de la fréquence des métros et du nombre de voyageurs provoquent de plus en plus d'avaries et d'incidents qui se produisent dans des situations variées. Plusieurs types de classifications des incidents sont mis en place à la suite de l'acquisition et de l'analyse des données afin d'identifier certaines caractéristiques.

Gravité de l'incident

L'impact d'un incident sur le trafic et la régulation de la ligne varie suivant la gravité de l'incident : deux grandes catégories sont identifiées. Un incident sera considéré comme mineur si

son impact sur le trafic est faible et est géré par l'application ATS contrairement à un incident majeur qui doit être géré par une procédure et dont l'impact sur le trafic est important.

Ainsi, l'impact d'un incident mineur est progressivement absorbé par les algorithmes de régulation en temps réel de l'ATS ou nécessite seulement des actions simples de l'opérateur sur l'exploitation. Pour ces incidents mineurs qui requièrent au moins une action de l'opérateur, l'application de supervision ATS permet de réaliser des adaptations simples sur le planning d'exploitation des trains afin de garantir un service continu aux voyageurs. L'interface propose à l'opérateur de nombreux dialogues permettant entre autres d'ajouter ou de supprimer des circulations de trains, de garer un train, de modifier le temps d'arrêt en station. Ces adaptations diminuent l'impact de l'incident sur le trafic qui devient alors transparent pour les voyageurs.

Ce type d'incident engendre seulement de faibles retards et des temps de stationnement plus longs en station. Par exemple, quand de nombreux voyageurs veulent monter dans un des trains, il est possible que le train reste plus longtemps que prévu en station et soit en retard par rapport à l'horaire planifié. L'avance des trains amont et aval sera alors automatiquement modifiée par la régulation pour réduire les écarts entre les trains.

Les incidents majeurs, quant à eux, nécessitent l'intervention des opérateurs de supervision et peuvent être la conséquence de divers événements d'exploitation dont l'origine varie, comme par exemple un voyageur descendu sur les voies ou une avarie de la signalisation. Les répercussions sur la sécurité des passagers et l'exploitation de la ligne seront donc plus importantes. Il existe deux types d'incidents majeurs : les incidents ayant besoin d'une réaction rapide pour assurer au plus vite la sécurité des personnes et les incidents liés à la topologie de la ligne. Le premier type d'incidents est géré par des procédures génériques et mémorisées par l'opérateur de supervision et le second par des procédures spécifiques décrites dans un document de référence, en raison des nombreux paramètres à prendre en considération.

L'impact sur le trafic d'un incident majeur peut varier suivant le contexte dans lequel il se produit et suivant la rapidité de prise en charge par l'opérateur. Ainsi, le déclenchement d'un signal d'alarme dans un train pendant l'heure de pointe aura un impact plus important sur le trafic que lors d'une période creuse de la journée en raison du nombre de trains présents sur la ligne. Les incidents majeurs peuvent donc plus facilement être classés suivant leur cause que leur impact sur le trafic qui est variable suivant le contexte. Par la suite, seuls les incidents considérés comme majeurs et gérés par des procédures mémorisés seront pris en compte puisque les incidents mineurs sont déjà en grande partie gérés par le système de supervision développé par Thales et ne nécessitent pas l'application d'une procédure.

Cause de l'incident

Suivant le type d'éléments concernés, les incidents se produisant lors de l'exploitation d'une ligne de métro sont classés dans cinq catégories : les installations fixes, le matériel roulant, l'énergie de traction, les voyageurs et les événements extérieurs. La gestion de l'incident, son impact sur le trafic et la durée de perturbation seront différents suivant le type d'incident.

Les installations fixes concernent l'ensemble des éléments terrain assurant la circulation des trains : les feux de signalisation, les aiguillages, les rails, l'éclairage et la structure du tunnel. Par exemple, une anomalie d'un signal de manœuvre perturbera le trafic pendant environ un quart d'heure et un problème au niveau des rails provoquera un ralentissement du trafic sur la partie impactée.

Les incidents liés au matériel roulant se rapportent à l'ensemble des avaries pouvant se produire sur les trains. Ils touchent donc notamment les motrices, les freins, les portes ; un tel incident pouvant au pire provoquer le déraillement du train. Lors d'un déraillement, l'exploitation de la ligne est perturbée pendant plusieurs heures et des dommages corporels peuvent être engendrés aux voyageurs.

En ce qui concerne les incidents liés à l'énergie, ils occasionnent la plupart du temps une coupure de l'énergie de traction. Si le circuit électrique d'alimentation des trains est mis hors tension, tous les trains sont alors à l'arrêt jusqu'à la remise sous tension de la ligne ou à des remises sous tension par sections. Ces incidents sont par exemple un court-circuit, une coupure de courant non désirée, le maintien du courant dans une zone après l'ouverture du circuit. Ces incidents impactant directement la possibilité de circulation des trains, les conséquences sur le trafic sont rapidement importantes, tout comme la durée de la perturbation.

De nombreux incidents sont également liés aux voyageurs avec des conséquences variant suivant la gravité de l'accident. Par exemple, lorsqu'une personne descend sur les voies de circulation, la perturbation peut durer seulement quelques minutes si la personne remonte sur le quai de sa propre initiative mais s'il s'agit d'un accident, le temps de perturbation peut aller jusqu'à plusieurs heures si une enquête policière est nécessaire. Ce type d'incidents concerne également un malaise d'un voyageur dans un train, une personne coincée entre le train et le quai en station, le ralentissement de la fermeture des portes en cas de forte affluence.

Une partie des incidents a une cause extérieure à l'exploitation de la ligne mais provoque d'importantes perturbations sur la circulation des trains. Ces incidents sont variés : présence d'un colis suspect dans un train ou sur un quai, départ d'un incendie, passage d'un animal sur les voies, infiltration d'eau dans un tunnel.

Pour résumer, en terme d'impact sur l'exploitation, 60% des retards sur le réseau des métros parisiens sont causés par des incidents liés aux voyageurs, avec environ 300 accidents graves de voyageurs par an sur l'ensemble des 16 lignes. 20% des retards proviennent des avaries du matériel roulant ou des installations fixes, les causes de retard restantes ayant des origines diverses.

III.1.3 Classification des procédures

Pour prendre en compte chacun de ces incidents, une procédure définit l'ensemble des étapes à suivre et des actions à réaliser par l'opérateur. Comme précisé lors de la mise en contexte (section I.3), l'étude se focalise sur les procédures mémorisées par les chefs de régulation à la RATP pour gérer des incidents liés à la sécurité des personnes et se déroulant lors de l'exploitation d'une ligne de métro.

Le tableau III.1 présente la liste des onze procédures de gestion d'incidents apprises par les chefs de régulation au cours de leur formation et étudiées au cours des travaux de thèse.

Bien que les procédures soient indépendantes les unes des autres, leur analyse a permis d'identifier des successions d'actions identiques à réaliser par l'opérateur de supervision dans plusieurs procédures. Ces séquences d'actions communes sont alors regroupées pour définir des sous-procédures et mettre en avant des interactions entre les procédures. Ainsi, une sous-procédure peut être présente dans différentes procédures où l'on retrouve une même séquence. Par exemple, après une mise hors tension de la ligne complète, certaines procédures décrivent l'ensemble des actions à réaliser pour remettre sous tension les parties de la ligne non concernées pour que des trains puissent y circuler et ainsi assurer une partie de l'exploitation de la ligne. Cette séquence

TABLE III.1 – Procédures de gestion d'incident mémorisées

Procédures
- Disjonction d'alarme (DA)
- Mise hors tension différée
- Rame stationnée en interstation
- Alerte Feu Fumée (AFF)
- Mise hors tension d'urgence
- Signalement d'une personne sur les voies (ISF36)
- Évacuation d'un train
- Avertisseur d'alarme hors service (AA HS)
- Non ouverture d'un signal de manœuvre
- Anomalie d'un signal d'espacement (SS/SSO)
- Arrêt automatique du train

d'actions se retrouve par exemple dans la procédure *Disjonction d'Alarme* et lors du *Signalement d'une personne sur les voies* (*ISF 36*).

De plus, il est possible qu'une procédure inclue une séquence d'actions correspondant à une procédure complète. Ainsi, pour gérer un train qui stationne en interstation, l'opérateur, en suivant la procédure correspondant à l'incident, peut être amené, selon la situation de la ligne, à évacuer les voyageurs du train. La procédure *Évacuation* peut également être exécutée de manière indépendante si des voyageurs forcent l'ouverture des portes et descendent sur les voies.

Ces analyses ont permis d'identifier des interactions et des liens entre les procédures étudiées, ces dépendances sont résumées dans les graphes suivants (figure III.1 et III.2).

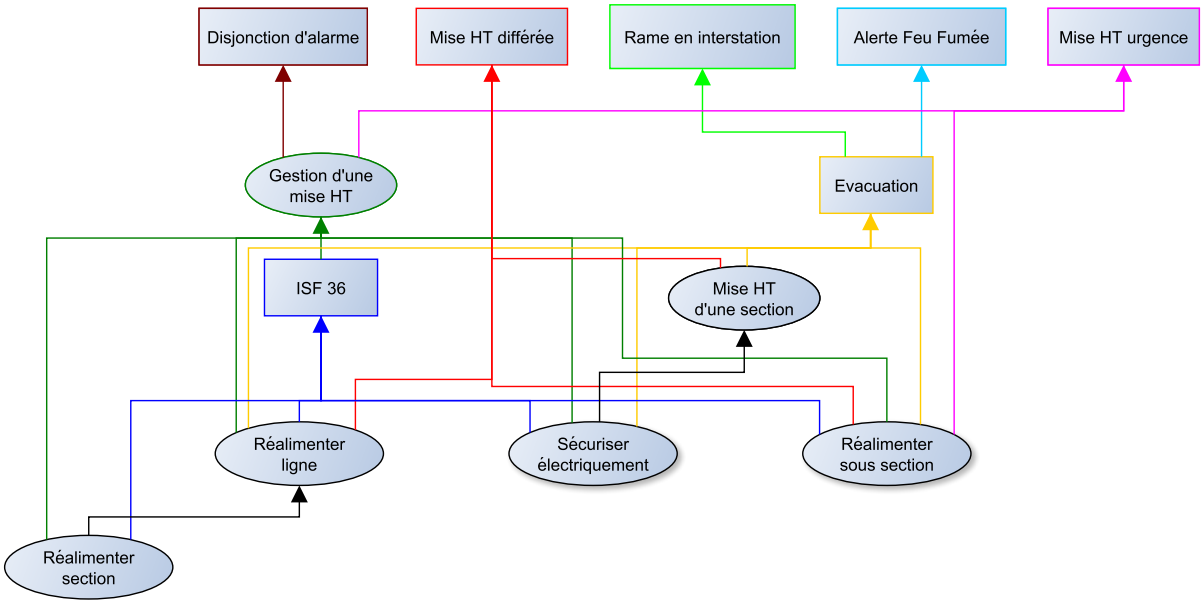


FIGURE III.1 – Graphe des dépendances

Dans ce graphe des dépendances, les procédures mémorisées par les opérateurs, déclenchées par l'occurrence d'un incident, sont représentées par des rectangles. Les sous-procédures, représentées par une ellipse, ont pour but de regrouper un ensemble d'actions et ne permettent pas de

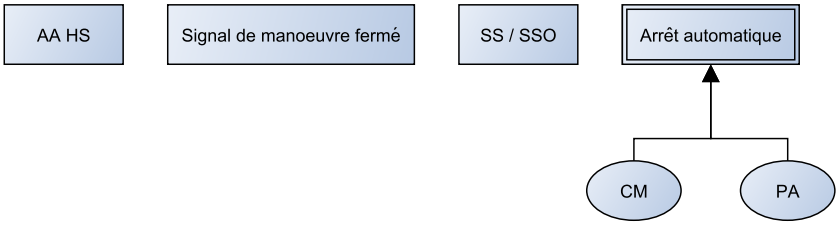


Figure III.2 – Graphe des dépendances - suite

gérer seul un incident. Les flèches symbolisent les différentes inclusions entre les éléments. Ainsi, dans le graphe des dépendances, la procédure *ISF 36* est incluse dans la sous-procédure *Gestion d'une mise HT*. Les relations entre les différentes procédures ne sont donc pas une simple hiérarchisation mais il existe de nombreuses inclusions et interactions entre elles, mises en évidence grâce aux sous-procédures.

La sous-procédure *Réalimenter section* est incluse dans *Réalimenter ligne* car il faut réalimenter l'ensemble des sections pour réalimenter la ligne complète. Cependant, la sous-procédure *Réalimenter sous-section* n'est pas incluse dans *Réalimenter section* puisque les technologies utilisées permettent de remettre le courant sur une section en une seule fois sans passer sous-section par sous-section. La sous-procédure *Réalimenter sous-section* détaille les actions à réaliser pour avoir une sous-section alimentée et une section hors tension dans la même section.

Ces différentes classifications ont pour objet de mettre en évidence des similitudes entre les procédures et des regroupements possibles. La deuxième étape de la démarche d'étude (figure II.5) présente leur représentation graphique dans le langage BPMN. Ainsi, les procédures globales seront représentées indépendamment les unes des autres tout en identifiant les sous-procédures qu'elles emploient avec un élément spécifique du langage BPMN.

III.2 Représentation graphique des procédures

III.2.1 Objectif

Après avoir classifié les incidents et les procédures suivant différents critères, il est nécessaire de représenter ces procédures d'exploitation dans un langage facilement compréhensible et accessible par des industriels afin de favoriser les échanges et les discussions. L'objectif de cette étape est d'obtenir une représentation graphique et synthétique des procédures pour visualiser de manière globale les actions accomplies par le chef de régulation, leurs liens et leur ordre d'exécution. La représentation doit également mettre en évidence les différentes liaisons entre les membres du personnel de la RATP, ces communications sont indispensables et nombreuses lors de la gestion d'un incident. Cette représentation graphique est également réalisée pour d'étudier le déroulement et l'organisation des procédures.

Le langage doit être adapté aux objectifs de la représentation, être standardisé et s'appuyer sur une norme reconnue par les industriels. La notation graphique standardisée BPMN 2.0 (Business Process Model and Notation) [OMG11a] a donc été choisie. Ce langage a notamment été retenu par la société Thales pour intégrer des processus embarqués de gestion d'alarmes dans une application de supervision globale de systèmes complexes et le BPMN a également permis de documenter les processus systèmes utilisés. Ce choix s'inscrit dans une démarche globale d'innovation des logiciels de l'entreprise Thales.

Afin de réaliser cette représentation graphique des procédures, le logiciel yEd GraphEditor a été utilisé car il intègre le langage BPMN2 2.0. Ce langage va tout d'abord être présenté puis le passage des procédures textuelles pour la gestion des incidents de la RATP vers une représentation graphique de ce savoir-faire sous forme de procédures BPMN va ensuite être exposé.

III.2.2 Langage BPMN 2.0

Comme présenté dans la section II.3, le langage BPMN est un standard de modélisation utilisant une notation graphique. Ce langage propose des éléments spécifiques permettant de décrire des processus métier et des procédures, comme des flux de messages, des couloirs d'activités par participants, des types d'activité. Suivant l'objectif recherché, la description d'un enchainement d'activités est donnée par un processus pour présenter la finalité des actions ou par une procédure pour décrire la mise en œuvre d'un processus. Le langage BPMN met donc en évidence certaines caractéristiques de procédures comme les différents échanges entre les intervenants et la progression parallèle de certaines séquences. Cette notation est un intermédiaire entre une description littérale des procédures d'exploitation d'une ligne de métro et leur représentation abstraite.

Description des objets

Le langage BPMN propose trois types de diagramme pour décrire des workflows : les diagrammes de conversation pour représenter principalement des communications, les diagrammes de chorégraphie pour décrire des processus du point de vue de plusieurs participants en même temps et les diagrammes de collaboration qui modélisent les échanges entre les intervenants. L'objectif étant d'obtenir une représentation graphique de la succession des actions à réaliser lors de procédures de gestion d'incident, du point de vue d'un opérateur de supervision, les diagrammes de collaboration sont les plus adaptés et sont utilisés par la suite. Ces diagrammes de collaboration BPMN s'articulent autour de trois catégories d'éléments : les objets pour décrire le flux, les connecteurs et les conteneurs graphiques. Il existe trois types d'objets pour décrire le flux : les activités, les événements et les branchements (figure III.3).

Une activité est un élément spécifique correspondant à l'action qui doit être réalisée. Il existe deux sortes d'activités. Une tâche représente une activité atomique d'une procédure non décomposable en sous-activités contrairement aux sous-procédures [+] qui représentent une activité subdivisible pouvant contenir d'autres activités. Pour chaque tâche, il est possible de spécifier la nature de l'action à réaliser en ajoutant un pictogramme en haut à gauche du symbole de l'activité. Par exemple, la tâche peut être du type envoi ou réception d'un message, action avec l'assistance d'un logiciel ou réalisée manuellement.

Les événements d'une procédure représentent un fait qui se produit pendant le déroulement et qui affecte le flux. Les événements de début et de fin doivent toujours être présents dans une procédure BPMN pour lui donner une structure finie. L'événement de début est représenté par un cercle fin de couleur verte et indique le point de départ. L'événement de sortie est représenté par un cercle épais de couleur rouge et indique la fin d'une procédure. L'événement intermédiaire est quant à lui symbolisé par un double trait jaune. Un sigle à l'intérieur de la forme circulaire de l'événement qualifie son type (message, annulation, minuterie).

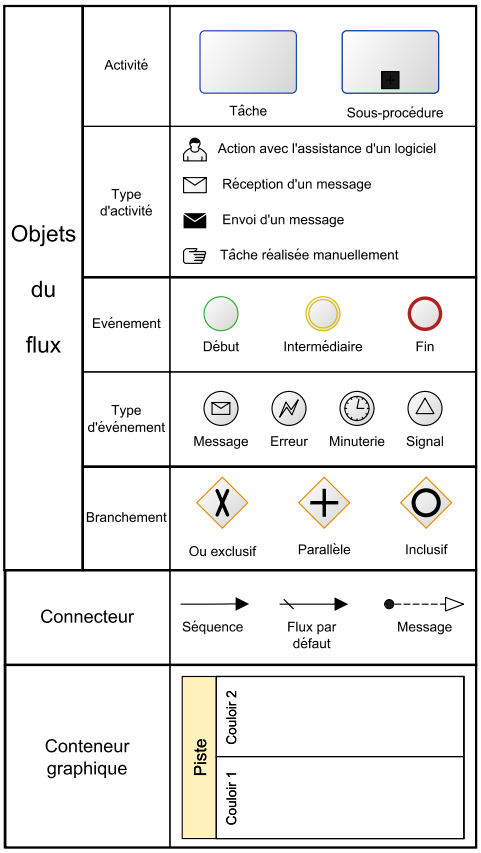


Figure III.3 – Objets BPMN

Les branchements sont les éléments de contrôle de flux représentant une condition de routage entre des flux entrant et sortant. Si le branchement contient un lien entrant et plusieurs liens sortants, il s'agira d'une décision (divergence). Dans le cas contraire il s'agira d'une jonction (convergence). Le symbole à l'intérieur du losange identifie le comportement du branchement : inclusif, exclusif, parallèle ou complexe.

Des connecteurs relient et séquencent l'ensemble de ces éléments. Les flèches en trait plein représentent les enchainements d'activités, le flux entre deux tâches. Une flèche avec un petit trait la barrant donne la marche à suivre avant un branchement si jamais aucune condition n'est vérifiée, elle indique ainsi le flux par défaut. Les messages, représentés par un trait en pointillés, décrivent les échanges entre intervenants dans la procédure.

Les pistes sont des conteneurs graphiques séparant les ensembles d'activités selon les personnes intervenant pour les exécuter. Les couloirs sont des subdivisions de piste utilisés pour différencier par exemple des rôles hiérarchiques au sein d'une entreprise. Ces éléments de structuration du langage BPMN mettent ainsi en évidence les échanges d'informations sous forme de flux de messages et l'ordonnancement des activités entre les participants.

III.2.3 Analyse du document de formation pour les CREG

Le support écrit distribué aux stagiaires CREG au début de leur formation est un document référence pour l'apprentissage du métier à la RATP. Les formateurs, assistés d'un CREG en poste, apportent des compléments et des précisions au document. Les heures de formations permettent également une mise en pratique des procédures pour faire face directement aux

situations qu'ils auront à gérer sur la ligne de métro qu'ils superviseront.

La description des procédures dans le document se fait sous forme textuelle, utilisant des structures assez hétérogènes pour présenter les actions que l'opérateur doit faire pour gérer les différents incidents.

Certaines procédures sont exposées sous forme de tableau pour différencier les cas dépendant du contexte dans lesquels peuvent se produire l'incident. Cette structure met en évidence des séquences d'actions exclusives à réaliser suivant la situation. Par exemple, elle est utilisée pour différencier deux cas d'incident dans la procédure *Arrêt automatique du train* (figure III.4).

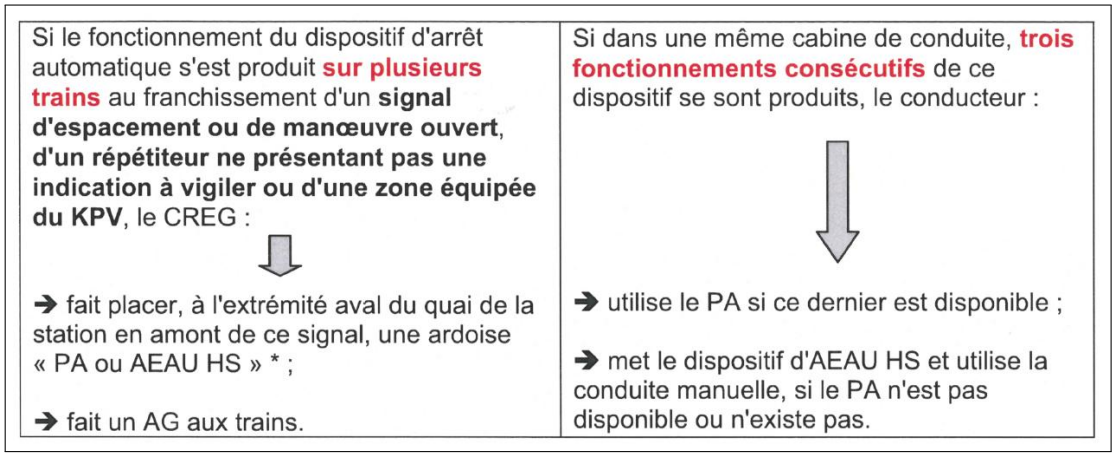


FIGURE III.4 – Extrait de la procédure *Arrêt automatique du train*

Pour certaines procédures, des listes numérotées détaillent l'enchainement des actions à exécuter. Ces procédures sont le plus souvent linéaires avec une succession de tâches : lorsque que l'une est achevée, l'opérateur entreprend la suivante. La figure III.5 est un extrait de la procédure *Mise Hors Tension différée* qui utilise cette structure pour présenter la succession d'actions à réaliser.

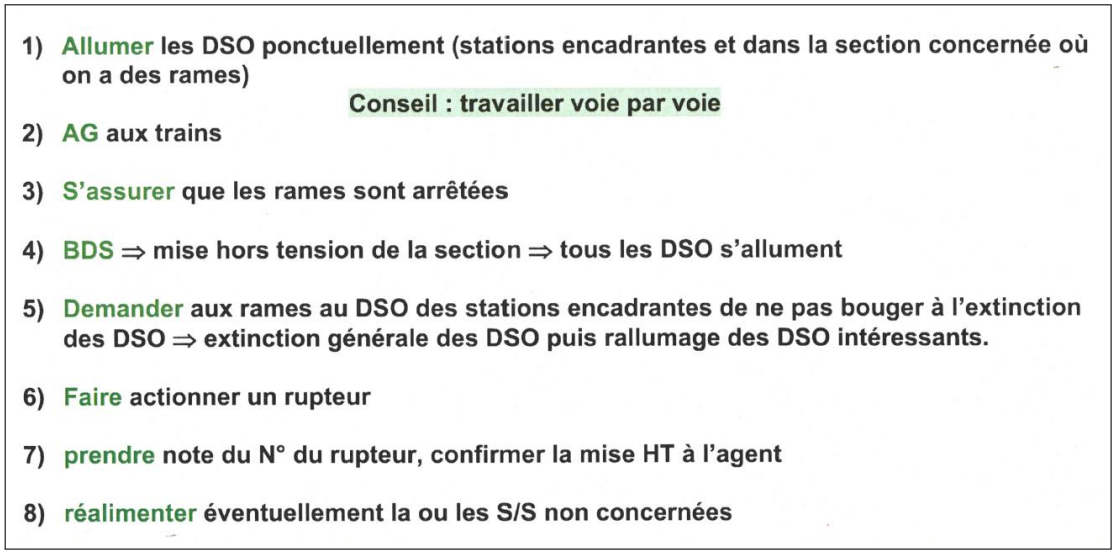


FIGURE III.5 – Extrait de la procédure *Mise Hors Tension différée*

Pour d'autres procédures, la liste numérotée ne définit pas une chronologie à suivre mais une distinction entre plusieurs cas possibles suivant le contexte de la ligne. Des flèches énumèrent ensuite, étape par étape, la série d'actions à entreprendre. L'extrait de la procédure *Signalement*

d'une personne sur les voies (figure III.6) présente un cas d'utilisation de cette structure.

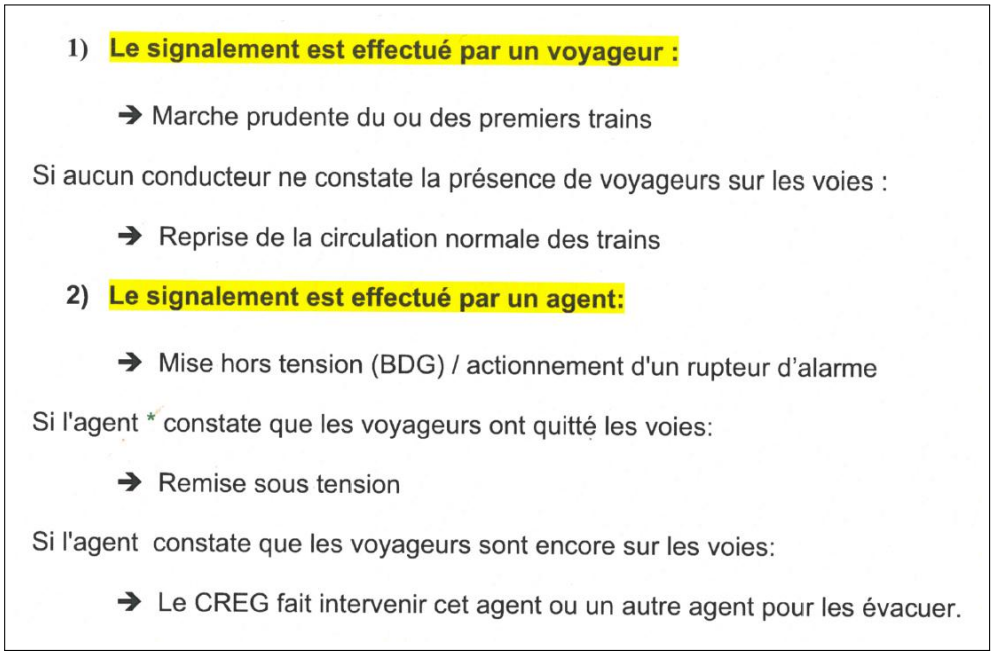


Figure III.6 – Extrait de la procédure *Signalement d'une personne sur les voies*

Plusieurs procédures sont expliquées en s'appuyant sur un extrait d'article d'Instruction de Sécurité Ferroviaire (ISF). Ces documents d'exploitation spécifient les règles à appliquer pour garantir la sécurité du transport ferroviaire, ils définissent le règlement que doit respecter le CREG ainsi que tout le personnel RATP. Ainsi, la procédure *Train stationné en interstation* repose sur plusieurs extraits d'articles pour présenter les différentes stratégies envisageables (figure III.7).

Figure III.7 – Extrait de la procédure *Train stationné en interstation*

Des notes internes, faisant suite à des incidents s'étant produits sur le réseau, complètent la description de certaines procédures. Ces retours d'expérience viennent apporter des éléments concrets à leur description et préciser certains aspects qui ont pu paraitre imprécis à l'opérateur pendant la gestion de l'incident.

Finalement, l'apprentissage des procédures se fait surtout par la transmission d'informations et les explications données par les formateurs de manière orale. Les stagiaires prennent alors leurs propres notes pendant ces cours et transcrivent, à leur façon, sans suivre de standard, les procédures qu'ils ont à connaître.

L'analyse et la représentation des procédures apprises par les CREG sont d'autant plus compliquées que leur descriptions textuelles ne sont pas uniformes au niveau de la syntaxe ni standardisées mais utilisent une forme simple pour les présenter et les expliquer au mieux.

III.2.4 Représentation des procédures

L'objectif de la représentation avec le langage BPMN est d'obtenir une standardisation et une homogénéisation de l'écriture des procédures. Ces procédures étudiées sont exécutées par les chefs de régulation et doivent donc être représentées de leur point de vue.

Afin de représenter graphiquement les procédures mémorisées par les CREG, plusieurs étapes sont nécessaires. Il faut tout d'abord identifier les personnes intervenant lors de l'exécution de la procédure, autres que le chef de régulation. Ces personnes peuvent envoyer des messages au CREG pour lui rendre compte de la situation sur le terrain, recevoir des ordres d'actions à réaliser, interroger le CREG sur l'état global de la ligne. Ces personnes sont le plus souvent les conducteurs de la ligne en interaction permanente avec le CREG, les agents présents sur le terrain et en relation avec les usagers, le permanent des réseaux ferrés surveillant l'ensemble du réseau. Cette première étape détermine ainsi le nombre de pistes, dans le modèle BPMN, nécessaire pour représenter la procédure. Les flèches pointillées représentent les flux de message entre ces intervenants (figure III.8).

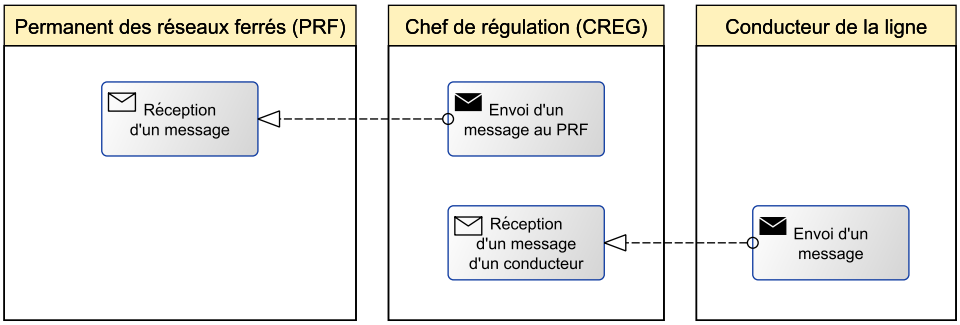


FIGURE III.8 – Interactions entre intervenants

La deuxième étape consiste à identifier les différents flux dépendant de la situation de la ligne et les séquences d'actions devant se dérouler en parallèle. Ces flux se visualisent au niveau BPMN par des branchements divergents pour la séparation et convergent pour la jonction des flux. Ces branchements sont de type exclusif si les actions à réaliser sont différentes suivant la situation de la ligne (figure III.9) et de type parallèle pour les séquences évoluant simultanément (figure III.10). Cette étape donne un aperçu de la structure des flux du modèle BPMN de la procédure.

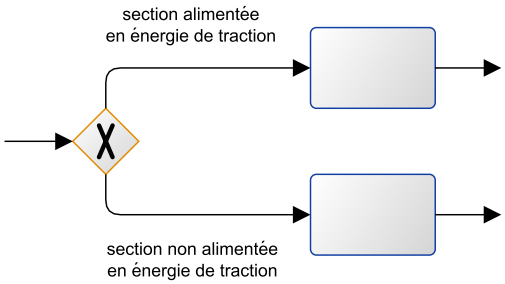


FIGURE III.9 – Branchement divergent exclusif

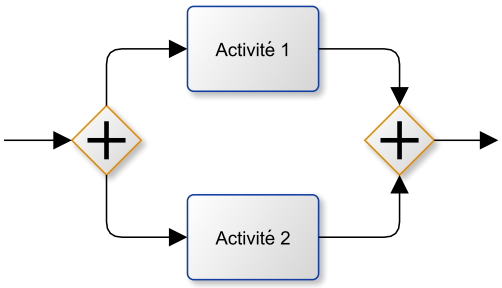


FIGURE III.10 – Branchement parallèle

Comme décrit dans la section III.1.3, des séquences communes d'actions ont été identifiées dans plusieurs procédures et regroupées dans des sous-procédures. Dans la troisième étape, les

sous-procédures sont définies, chacune d'entre elles doit également être modélisée en BPMN en suivant la même démarche. La représentation graphique de ces sous-procédures dans le langage BPMN permet ainsi d'obtenir une représentation plus compacte des procédures en agrégeant un ensemble d'actions (figure III.11).

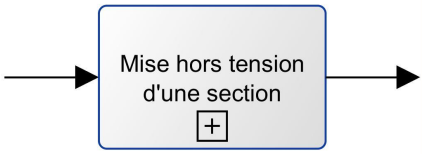


Figure III.11 – Sous-procédure

Il est ensuite important de repérer la chronologie des actions à réaliser par le chef de régulation dans le document textuel pour comprendre l'évolution de la procédure. L'élément déclencheur de la procédure et la fin de la procédure sont également à déterminer afin de connaître ses limites. Chaque action élémentaire exécutée est modélisée par une tâche. Le type de la tâche, quant à lui, qualifie l'action réalisé (figure III.12). Ainsi, si l'opérateur doit agir sur l'exploitation au travers de l'interface de l'ATS, l'activité sera de type *Usager* car l'opérateur agit grâce au système informatique, comme par exemple allumer des feux en station. Si le chef de régulation doit prévenir l'ensemble des conducteurs de la ligne par exemple d'une limitation temporaire de la vitesse pour cause de travaux dans l'une des interstations de la ligne, l'activité correspondant à l'appel général qu'il fera par téléphone sera de type *Envoi de message*. Pour mettre hors tension la ligne, l'action est représentée par une activité BPMN de type *Manuelle*. En effet, l'opérateur doit utiliser un bouton d'urgence qui n'est pas intégré au système de supervision ATS pour exécuter l'action.

Figure III.12 – Différents types d'activités

En se basant sur le document reçu lors de la formation et sur les connaissances acquises, onze procédures et six sous-procédures ont ainsi pu être représentées graphiquement dans le langage BPMN. Les procédures *Mise hors tension différée* et la sous-procédure *Sécuriser électriquement* sont données en exemple dans les figures III.13 et III.14. Les modèles des procédures *Arrêt automatique du train* et *Non ouverture d'un signal de manœuvre*, plus longues et complexes, sont présentés dans l'annexe C.

III.2.5 Conclusion

La représentation graphique des procédures avec le langage BPMN apporte une vision globale des interactions et du déroulement des actions tout en mettant en évidence les séquences de flux parallèles et exclusives. Une représentation graphique, synthétique et standardisée des procédures est ainsi déterminée. Cependant ce langage ne représente pas la situation courante de la ligne, c'est-à-dire le contexte dans lequel se déroule la procédure. Afin de poursuivre l'étude des procédures de gestion d'incidents d'une ligne de métro, il est maintenant nécessaire de transformer les modèles de ces procédures dans un autre langage. Ainsi, il sera possible d'intégrer

les procédures dans leur environnement en modélisant les éléments qui composent la ligne de métro.

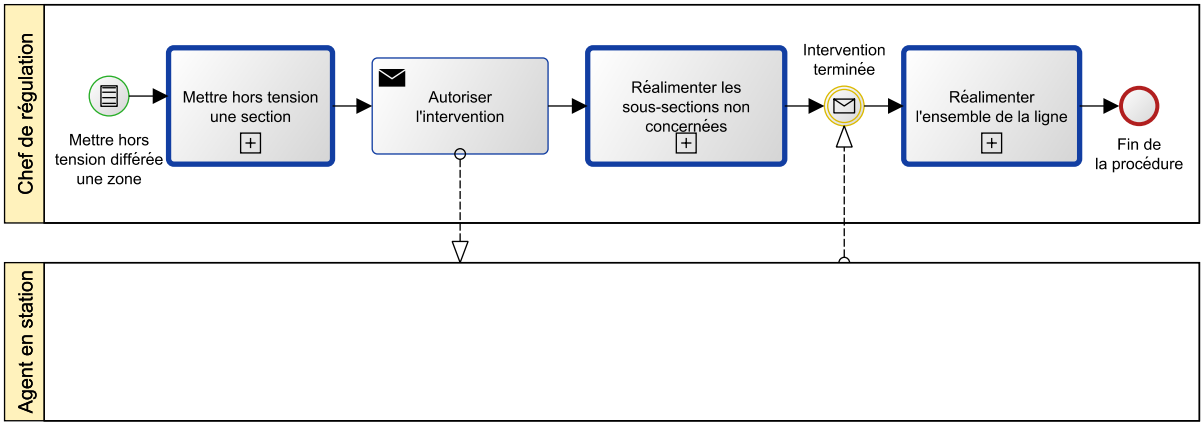


FIGURE III.13 – Procédure BPMN *Mise hors tension différée*

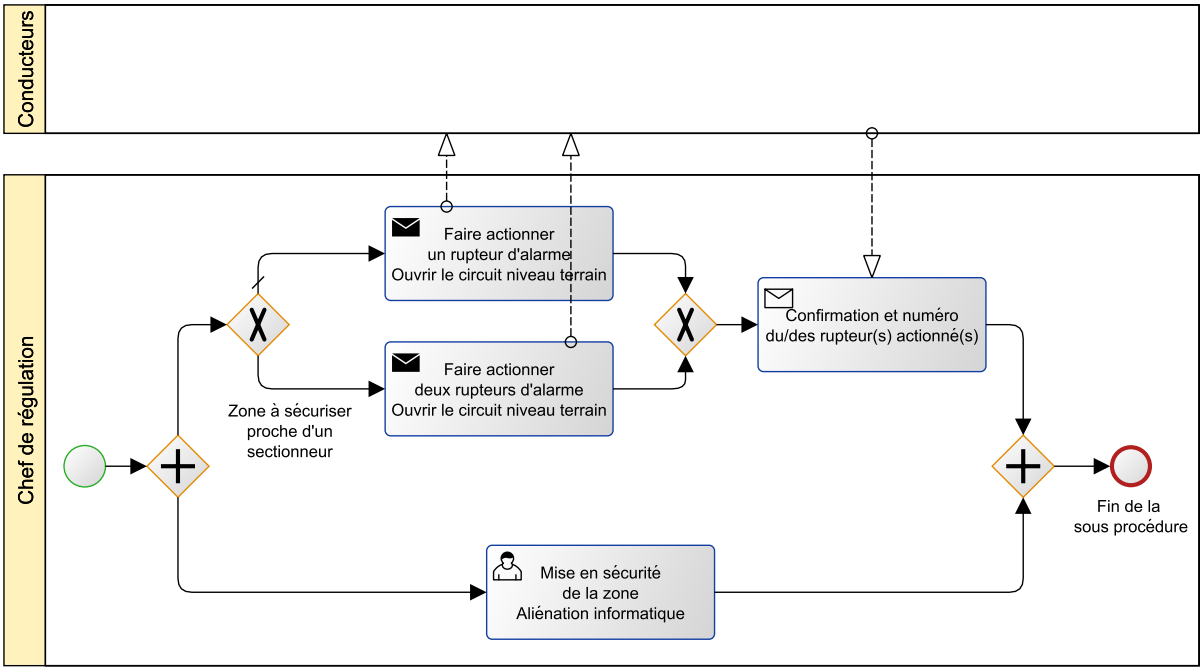


FIGURE III.14 – Sous-procédure BPMN *Sécuriser électriquement*

III.3 Modélisation du système

III.3.1 Objectif

Intégration du contexte

La représentation graphique des procédures de gestion d'incidents avec le langage BPMN apporte une standardisation dans l'écriture de ces procédures. Cependant, le langage BPMN n'est pas défini pour étudier des procédures en termes de danger rencontré par les voyageurs et le personnel. L'un des objectif de la thèse étant d'analyser les situations dangereuses dans lesquelles peuvent se retrouver ces personnes, il est nécessaire de replacer les procédures dans l'environnement dans lequel elles sont utilisées et de ne plus considérer uniquement l'enchaînement des actions à réaliser par le chef de régulation lors d'un incident.

Pour cela, le contexte dans lequel la procédure se déroule doit être pris en considération pour répondre à l'objectif recherché. Le contexte est déterminé par les éléments qui composent une ligne de métro et qui potentiellement ont un impact sur le déroulement d'une procédure. De plus, une procédure est exécutée suite au signalement d'un incident. Pour étudier les procédures, il faut donc également prendre en considération l'élément qui va les déclencher.

Définition 6 (Système étudié) *Le système étudié est composé des procédures de gestion d'incidents, des signalements des incidents ainsi que du contexte de la ligne décrit par des ressources.*

Afin d'identifier les situations dangereuses accessibles, il est nécessaire de réaliser une représentation abstraite du système. Cette représentation sera une modélisation de la réalité du système mais elle doit tenir compte des différentes caractéristiques du système. Ainsi, les éléments d'une ligne de métro constituent un ensemble et sont liés les uns aux autres, le modèle devra donc restituer ces interactions. Cette modélisation doit également être dynamique afin de pouvoir observer les différents états accessibles par le système lors de l'occurrence d'incidents et donc lors de la mise en œuvre de procédures.

Modélisation de l'évolution du système

Cette troisième étape de la démarche globale (figure II.5) décrit le passage d'une représentation statique des procédures en BPMN à une représentation dynamique du système, prenant en considération le contexte de la ligne de métro. Le système étudié évolue seulement à certains instants associés à l'occurrence d'événements ponctuels, comme la fin de réalisation d'une activité BPMN ou la modification de l'état d'un des éléments de la ligne. Le système sera modélisé sous forme d'un système à événements discret pour conserver ses caractéristiques d'évolution.

Les réseaux de Petri modélisent des systèmes à événements discrets caractérisés par des évolutions parallèles et des interactions entre les éléments du système. Le lecteur non familier avec les réseaux de Petri pourra se référer à l'annexe D. Ce langage propose donc des solutions pour intégrer les procédures de gestion d'incidents dans l'environnement de la ligne de métro et ainsi modéliser le système à étudier. Les réseaux de Petri utilisés sont ordinaires et saufs.

Méthode utilisée

Les éléments de la ligne de métro, les signalements des incidents et les procédures de gestion d'incidents définissent donc le système étudié. Pour passer de la notation graphique BPMN des activités à la modélisation du système, une démarche est propopsée pour modéliser chacun des éléments du système par des réseaux de Petri, les assembler et ainsi construire le modèle complet du système à étudier. Ces éléments sont tout d'abord modélisés de manière indépendante puis reliés par leurs interactions.

Après avoir présenté l'identification des ressources et des signalements d'incident, les règles de transformation des modèles BPMN des procédures vers des réseaux de Petri seront ensuite définies. Pour obtenir le modèle global du système, l'ensemble de ces éléments sera assemblé en tenant compte de leurs interactions.

III.3.2 Identification des ressources

Pour étudier l'évolution des procédures dans leur environnement, la modélisation du contexte est importante. Le contexte d'une ligne de métro correspond à l'ensemble des éléments de la ligne intervenant lors de l'exécution des procédures. Ces éléments, appelés ressources du système, sont en interaction avec les procédures et leurs états peuvent être modifiées par celles-ci à la suite de l'occurrence d'un incident.

Méthode d'identification

Une méthode a été développée pour identifier les éléments de la ligne essentiels à la modélisation du système : les ressources. Cette identification se base sur les modèles BPMN de procédures réalisés lors de l'étape précédente de la démarche globale. Une bonne connaissance du fonctionnement et de la supervision d'une ligne de métro est également nécessaire afin de répertorier l'ensemble des ressources. Ces éléments de la ligne peuvent prendre différents états, comme pour un feu de signalisation par exemple, *Allumé* ou *Éteint*. Une ressource décrit le contexte de la ligne de métro lié à un train et à la zone dans lequel celui-ci se trouve. La démarche d'identification des ressources est la suivante :

1. Mettre en évidence par expertise, au sein de chaque procédure BPMN, les activités qui modifient l'état d'un ou de plusieurs éléments de la ligne.
2. Répertorier d'autres ressources, procédures par procédures, en identifiant les activités des procédures BPMN nécessitant un état particulier d'un élément de la ligne pour être exécutées.
3. Analyser tous les éléments de la ligne identifiés au cours des deux premières étapes pour identifier les ressources ainsi que les différents états qu'elles peuvent prendre.
4. Déterminer, par expertise, les liens et contraintes entre les états de l'ensemble des ressources. Ces relations sont, par exemple, des états de différentes ressources incompatibles ou le changement d'état d'une ressource lié à une autre ressource.

Ainsi, en analysant les procédures de gestion d'incidents de la RATP, la ressource *Sécurisation électrique* a par exemple été identifiée. Cet élément de la ligne correspond à la protection ou

non d'une partie de la ligne contre une remise sous tension. En effet, lorsque l'une des sections est hors tension, une sécurisation électrique est mise en place afin d'éviter toute remise sous tension non voulue.

Cette ressource existe dans quatre états différents, une section électrique est :
- *Hors sécurité* si aucun dispositif n'a été actionné,
- *Sécurité terrain* si seul le dispositif d'ouverture du circuit a été déclenché sur le terrain,
- *Sécurité informatique* si l'aliénation informatique du système de remise sous tension a été réalisée,
- *Double sécurité* si l'aliénation informatique et l'ouverture du circuit sur le terrain ont été effectuées.

Après avoir identifié par expertise les ressources utiles à la modélisation du système, des regroupements possibles de ressources apparaissent.

Classification des ressources

À la suite de l'identification des ressources, celles-ci ont été classées dans quatre groupes. Une partie des ressources concerne le train et les caractéristiques liées à sa circulation, une autre les éléments de la ligne en lien avec l'énergie de traction. Des ressources décrivent les caractéristiques topologiques de la ligne, ces caractéristiques sont intrinsèques de la zone géographie où se situe le train et varient suivant sa position sur la ligne. Le dernier groupe rassemble les ressources en rapport avec la réglementation ferroviaire et qui contraignent le train.

Le tableau III.2 suivant présente les ressources identifiées classées par groupe, avec également les différents états qu'elles peuvent prendre.

Table III.2 – Groupes des ressources

Groupe	Ressource	États
Circulation du train	Position	Station / Tunnel
	Mode de conduite	Pilote automatique / Manuelle
	Conducteur	Cabine / Hors cabine / Indisponible
	Occupation	Avec voyageurs / Sans voyageur / En évacuation
Énergie	Alimentation	Sous tension / Hors tension
	Sécurisation	Hors sécurité / Terrain / Informatique / Double
Ligne	Environnement	Souterrain / Aérien
	Déclivité	Nulle / Positive / Négative
	Avertisseur d'Alarme	En service / Hors service
	Lien avec le réseau	Avec raccords / Sans raccord
	Sectionneur	Sans sectionneur / Avec sectionneur
Règlementation	Feux de station	Éteint / Allumé
	Droit de circulation	Autorisé / Interdit
	Allure	Normale / Marche à vue

Les ressources sont également différenciées suivant un autre critère : la connaissance de leur

état par l'application de supervision ATS. En effet, l'acquisition et le traitement de nombreuses données venant du terrain par l'application ATS permettent de connaître en temps réel la position du train par exemple et donc l'état de la ressource *Position du train*. Cependant, le *Droit de circulation* d'un conducteur étant donné par le chef de régulation par communication téléphonique, l'application ATS ne connait pas directement l'état de cette ressource.

La recherche de l'ensemble des ressources requière de bonnes connaissances sur l'exploitation d'une ligne de métro : il est difficile de déterminer l'ensemble des ressources de manière exhaustive. Les ressources présentées dans le tableau III.2 ont été identifiées avec mon niveau intermédiaire d'expertise et de connaissance de l'exploitation d'une ligne de métro. Pour obtenir une identification plus complète, la validation d'un expert, client de l'application ATS de Thales, serait nécessaire. Le modèle du système sera d'autant plus proche de la réalité de l'exploitation d'une ligne de métro que le nombre de ressources, et donc d'éléments décrivant la ligne, sera important. Les ressources ne sont pas de simples indicateurs de l'état du système mais une représentation de l'ensemble des comportements possibles d'une ligne de métro et des interactions existent entre ces ressources.

Les ressources décrivent le contexte dans lequel se trouve la ligne de métro, leurs différents états respectent les contraintes existantes lors de l'exploitation d'une ligne de métro. Ainsi certains états de ressources sont liés à l'état d'une autre ressource. Par exemple, la ressource *Position du train* ne peut changer d'état, passage d'une station à un tunnel, seulement si la ressource *Alimentation électrique* est dans l'état *Sous tension*.

La figure III.15 présente les contraintes existantes entre les ressources identifiées, certaines ressources ne sont pas en interaction avec les autres.

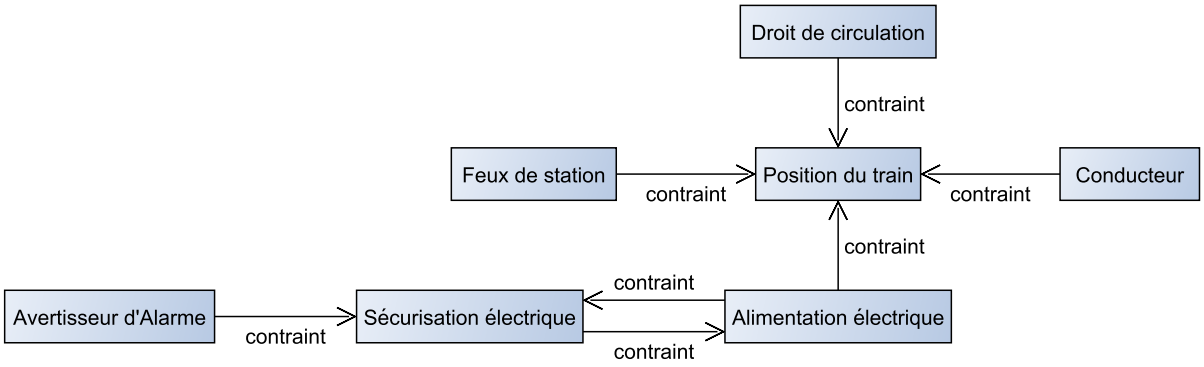


FIGURE III.15 – Contraintes entre les ressources

L'identification des ressources mises en jeu lors de l'exploitation d'une ligne de métro révèle les liens et contraintes entre les procédures de gestion d'incidents et le contexte de la ligne. La définition des états des ressources du système permet d'obtenir une représentation plus réaliste du système afin de faire apparaitre d'éventuels états de danger. L'objectif de cette section est d'intégrer les procédures de gestion d'incident dans l'environnement dans lequel elles sont utilisées. Pour cela, le système modélise également le signalement des incidents qui déclenchent les procédures.

III.3.3 Signalement des incidents

Lors de l'acquisition du savoir-faire (section III.1.2), les incidents rencontrés ont été répertoriés selon différents types. Les incidents étudiés dans cette thèse déclenchent l'exécution d'une procédure mémorisée par le chef de régulation. Afin de modéliser le comportement du système, il faut intégrer des modèles de signalement des incidents pour avoir l'information qu'un incident s'est produit.

Un signalement d'incident donne l'information de la présence ou de l'absence d'un incident. Ainsi, pour chaque incident étudié, le réseau de Petri est constitué de deux places représentant l'*Absence* ou la *Présence* du signalement. La transition vers la présence du signalement est franchie lors de l'occurrence de l'incident. Il n'existe pas d'interactions entre les différents incidents mais entre les incidents et les procédures : un incident autorise l'enclenchement de la procédure permettant sa gestion.

III.3.4 Modélisation des procédures

La représentation graphique des procédures à partir de leur description textuelle a été présentée dans la section III.2.4. Cette représentation a été réalisée dans le langage BPMN et les procédures doivent maintenant être modélisées par des réseaux de Petri (RdP) pour leur intégration dans le système. Le passage des procédures BPMN vers le RdP n'est pas une simple traduction comme présentée section II.3.3 mais doit également prendre en considération des éléments complémentaires, tels que le système complet, les interactions entre les procédures et le contexte de la ligne de métro.

La transformation des modèles BPMN des procédures en RdP se compose de quatre étapes. Chacune de ces étapes va être présentée au travers d'un exemple théorique d'une procédure (figure III.16) regroupant plusieurs éléments BPMN.

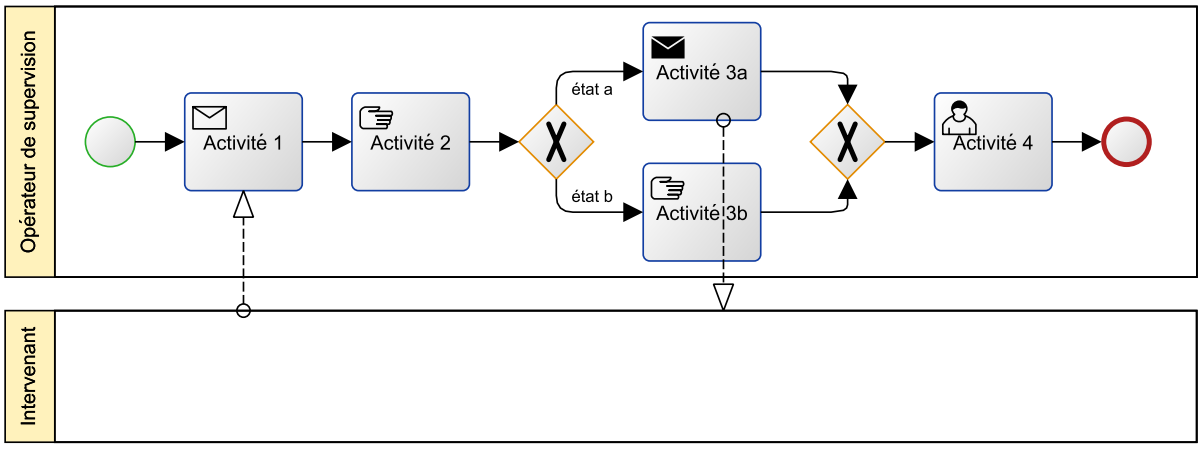


Figure III.16 – Modèle BPMN initial de la procédure

Pour la transformation en réseau de Petri, certaines informations contenues dans la procédure BPMN ne sont pas essentielles. Ainsi, seules les activités réalisées par l'opérateur de supervision sont transformées, les liens avec les autres intervenants ne sont donc pas conservés. De même, les types des activités n'ont pas d'impact sur la transformation des activités. Ainsi, la procédure

exemple (figure III.17) est formée de cinq activités, d'un événement initial, d'un événement final et d'un branchement de type *Ou exclusif* séparant les deux cas possibles : *état a* et *état b*.

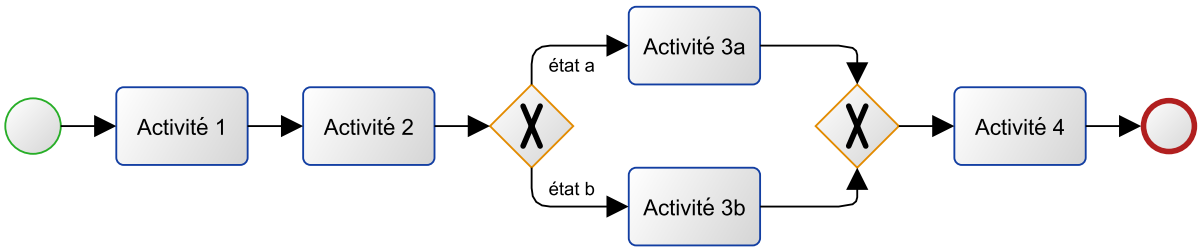


FIGURE III.17 – Modèle BPMN simplifié de la procédure

1. Identification des interactions entre la procédure et le système (figure III.18)

   Pour chaque activité, il faut identifier s'il existe un lien avec un signalement d'incident (*Événement initial*, *Activité 4*), si l'activité dépend de l'état d'une ressource (*Branchement Ou exclusif*) ou si l'activité modifie l'état d'une ressource (*Activité 2*). Cette étape est à réaliser en lien avec l'identification des ressources accomplie par expertise des procédures.

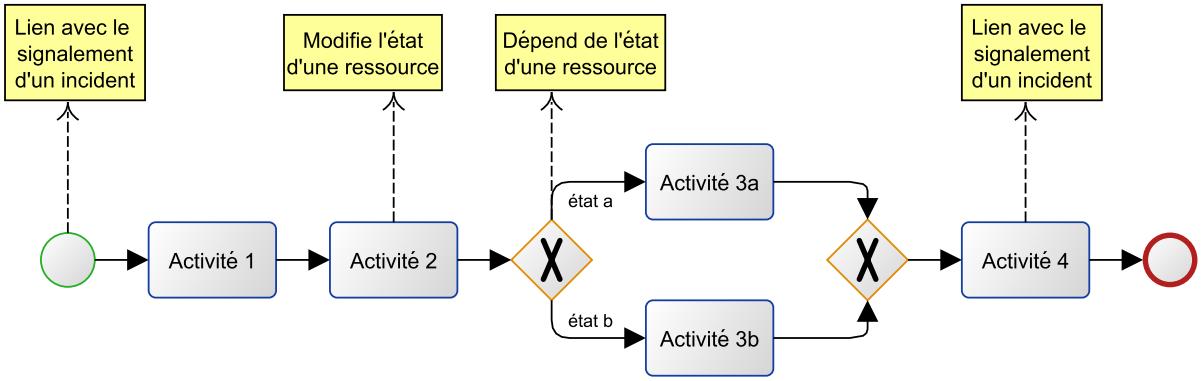


FIGURE III.18 – Identification des interactions entre la procédure et le système

2. Traduction des éléments en se basant sur les recherches de Dijkman [Dij08](figures III.19 et III.20)

   Chaque élément de la procédure BPMN est traduit en un module constitué d'une place, d'une ou deux transitions et d'une place. Les modules sont ensuite reliés les uns aux autres en fusionnant les places en pointillées pour former un réseau de Petri et respecter l'alternance des places et des transitions. L'identification des liens avec le système complet doit être conservée. À l'état initial, seule la place du module correspondant à l'événement initial de la procédure BPMN est marquée. Une procédure étant exécutée de manière séquentielle du début à la fin, une seule marque est nécessaire dans le réseau de Petri, celui-ci est donc sauf. Dans la figure III.20, les règles de traduction R1, R4, R5, R6 et R8 sont utilisées pour transformer la procédure BPMN exemple en réseau de Petri. Le modèle obtenu est composé de onze places et onze transitions après avoir fusionné les places des modules adjacents. Les différents modules réseaux de Petri formés suite à la traduction sont identifiés par la lettre *M*.

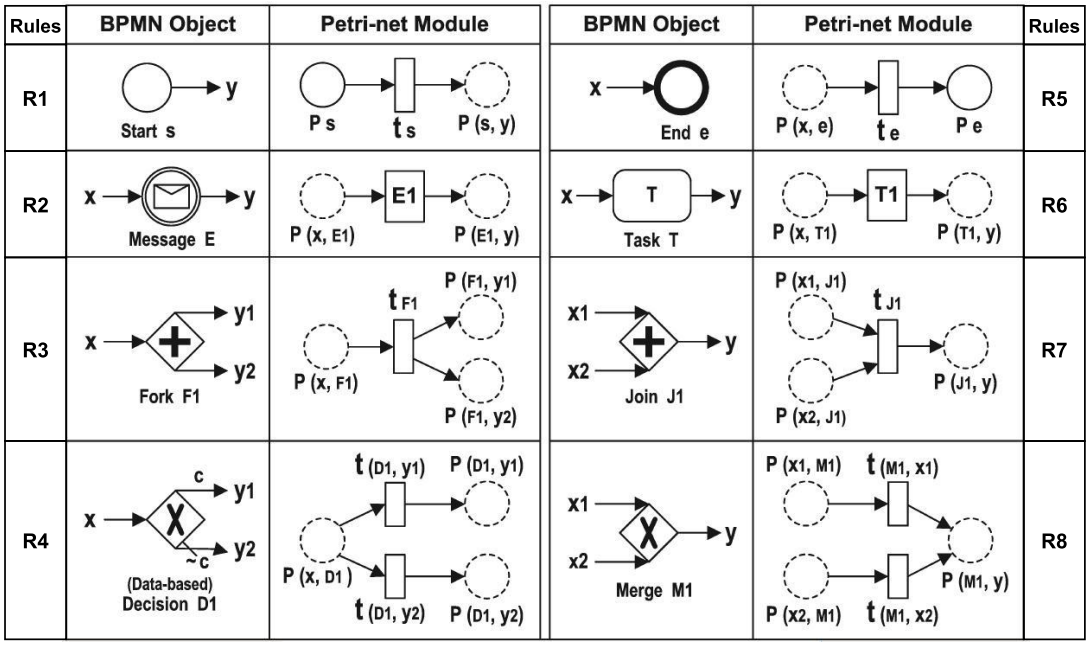


Figure III.19 – Transformation présentée par Dijkman dans [Dij08]

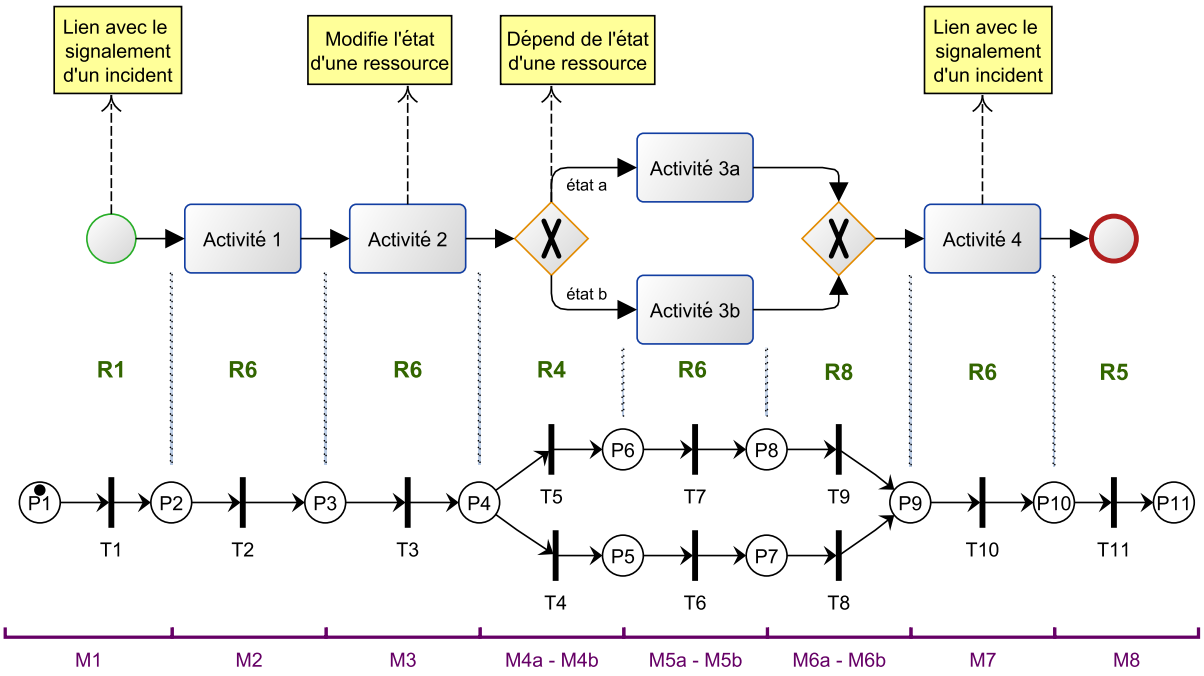


Figure III.20 – Traduction des éléments

3. Simplification du RdP en fonction des interactions avec le système (figure III.21)

   Afin de simplifier le réseau de Petri obtenu, seuls les modules issus de la traduction et ayant un lien avec le système sont conservés. Une agrégation des modules est ensuite réalisée afin de garder uniquement ceux nécessaires à la modélisation du système. Les premier et dernier modules, qui sont la traduction des événements de début et de fin de la procédure BPMN, ne sont pas supprimés du modèle et sont donc toujours conservés lors de la simplification du RdP. Ainsi, dans l'exemple proposé, les modules *M2*, *M5a* et *M5b* sont supprimés et

les places *P2* et*P3* fusionnent, ainsi que les places *P6* et*P8* et *P5* et*P7*.

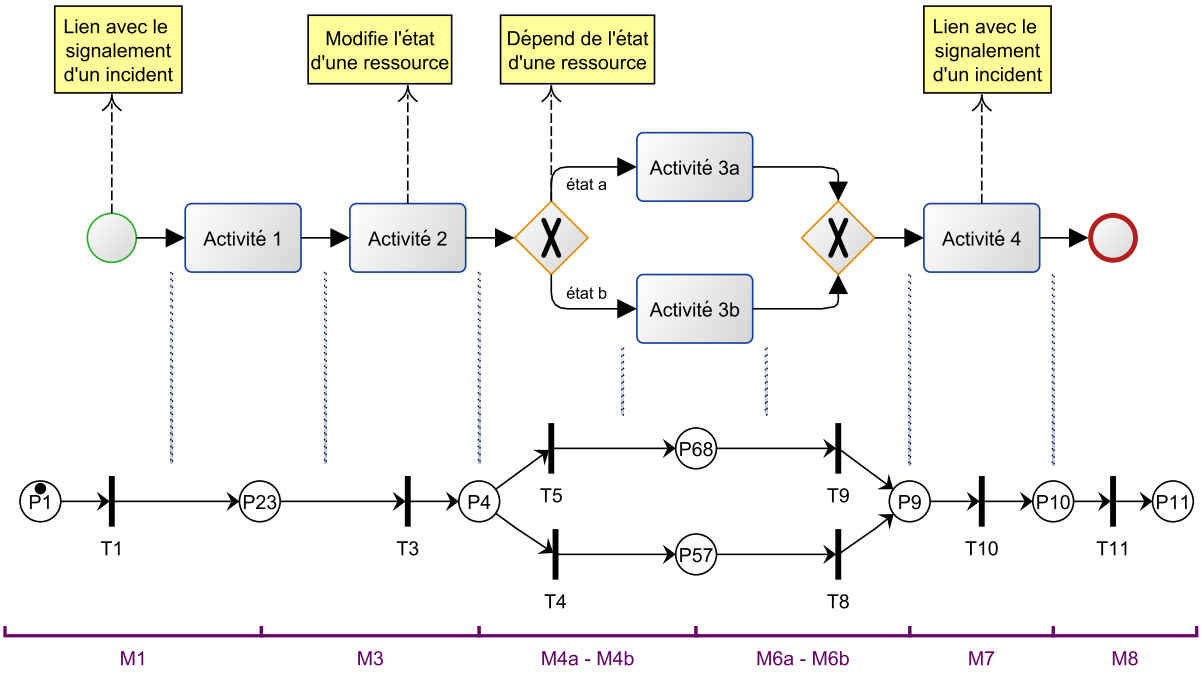


FIGURE III.21 – Simplification du RdP

4. Intégration de la procédure dans le système (figure III.22)

   Pour intégrer la procédure dans le système, les transitions des modules modifiant une ressource du système modélisée par deux états doivent être dédoublées. En effet, suivant l'état de la ressource, la procédure devra vérifier que celle-ci est bien dans l'état voulu ou bien modifier son état. Ainsi, la transition *T3* qui est liée à l'*Activité 2* et modifie l'état d'une ressource à deux états est dédoublée en deux transitions *T3i* et *T3j*. Pour les modèles des ressources constitués de plus de deux états, la modification de la transition doit être faite au cas par cas, suivant le lien entre les différents états possibles.

   De plus, pour modéliser le système, il faut prendre en compte le fait que les procédures peuvent être exécutées plusieurs fois. Le modèle réseau de Petri de la procédure doit donc être cyclique, la première et la dernière place du RdP sont fusionnées. Dans l'exemple figure III.22, les places *P1* et *P11* sont fusionnées et un arc relie la transition *T11* à la place fusionnée *P111*.

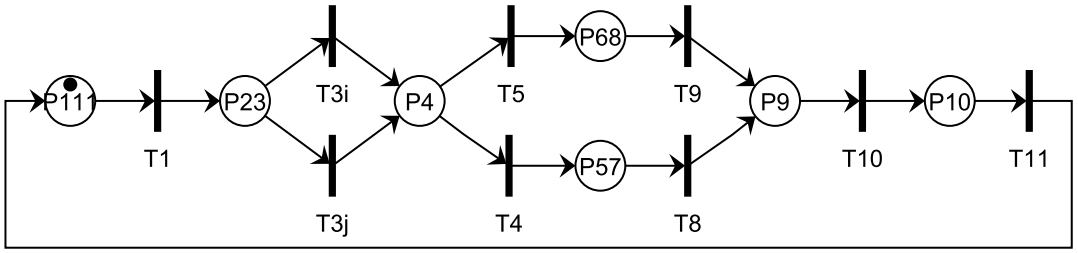


FIGURE III.22 – Intégration de la procédure dans le système

Le modèle réseau de Petri de la procédure ainsi obtenu peut être intégré dans la modélisation

globale du système.

III.3.5 Modélisation réseaux de Petri du système

Tous les éléments du système doivent maintenant être assemblés pour construire le modèle réseaux de Petri complet du système. Ils sont tout d'abord modélisés puis reliés par leurs interactions.

Concernant les signalements d'incident, le réseau de Petri est sauf puisqu'un incident ne peut pas être *Présent* et *Absent* en même temps. À l'état initial, il n'y a aucun incident en cours, la place *Absence* est donc marquée. Chaque signalement d'incident doit être lié à la procédure permettant de le gérer. Ainsi, une procédure est déclenchée seulement si il y a présence du signalement de l'incident correspondant (figure III.23).

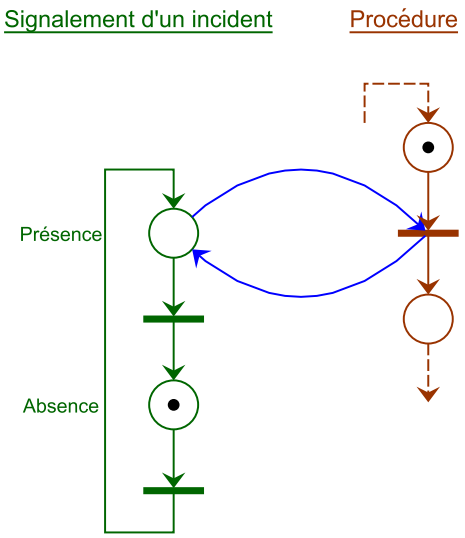


Figure III.23 – Interaction *Signalement d'un incident* et *Procédure*

Pour la prise en compte du contexte, des ressources ont été identifiées ainsi que les différents états qu'elles peuvent prendre. Chaque état d'une ressource est modélisé par une place dans le réseau de Petri et les transitions correspondent au passage d'un état à un autre. Une ressource ne pouvant être dans deux états différents en même temps, il y a donc une seule marque dans le réseau de Petri modélisant une ressource. Ce réseau de Petri est donc sauf. L'état par défaut ou le plus courant d'une ressource est choisi pour le marquage initial.

Les différents liens entre les ressources et les procédures doivent ensuite être modélisés pour associer les procédures à leur contexte. Ainsi, les transitions dédoublées des procédures sont reliées à la ressource modifiée (arcs bleus sur la figure III.24). De plus, la procédure ayant forcé la ressource à être dans un état particulier, il est nécessaire de conserver la ressource dans cet état précis. Pour cela et empêcher une modification de l'état de la ressource, il faut autoriser la sortie de l'état seulement si la procédure de gestion d'incident est terminée. Ainsi, la transition sortante de cet état doit être franchissable uniquement si la procédure n'est pas en cours d'exécution (arcs verts sur la figure III.24). Les ressources contraintes par les ressources en lien avec les procédures étudiées sont également ajoutées au système complet. Leurs interactions sont représentées par différents arcs entre les places et les transitions des ressources.

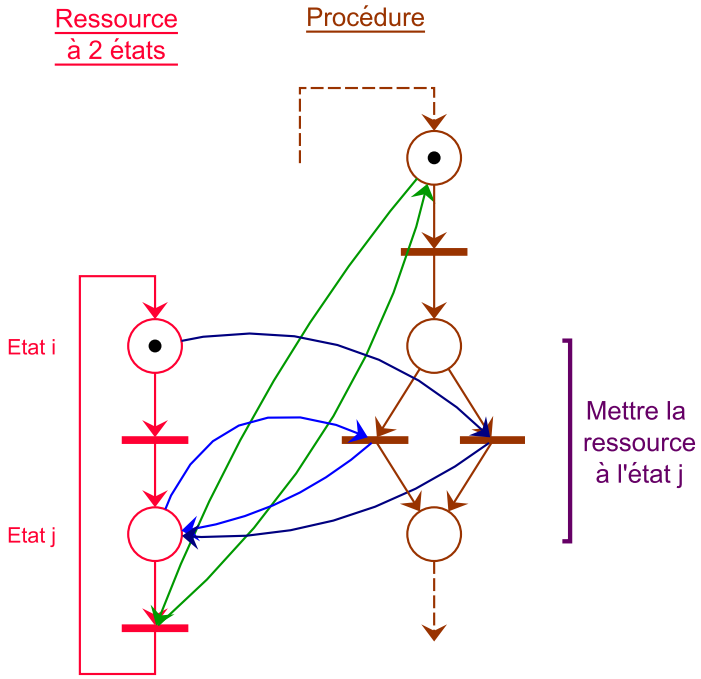


FIGURE III.24 – Interaction *Ressource* et *Procédure*

L'objectif de la modélisation du système est d'identifier les états dans lesquels des personnes pourraient se retrouver en danger suite à l'occurrence d'incidents. L'un des postulats de l'étude (section I.3) affirme qu'une procédure est sûre par usage et par expérience. Un système avec une seule procédure de gestion d'incident n'aurait donc pas d'intérêt par rapport à l'objectif d'étude du danger recherché. Le système étudié et modélisé doit donc au minimum intégrer deux procédures de gestion d'incident.

III.3.6 Conclusion

Le modèle RdP global du système obtenu intègre les procédures à étudier, les signalements des incidents concernés ainsi que les interactions entre les procédures et le contexte de la ligne au travers des ressources, l'influence des ressources sur les procédures sera donc prise en compte au cours de l'étude.

Pour l'analyse des procédures et des états de danger pouvant être atteints, il faut maintenant définir quelles sont ces états et les caractériser. Ces éléments permettront également d'identifier des critères pour choisir les combinaisons de procédures à étudier.

III.4 Conclusion sur la représentation et la modélisation des procédures

L'acquisition du savoir-faire auprès des industriels sur l'exploitation d'une ligne de métro et plus particulièrement la gestion des incidents a permis de classer les incidents rencontrés suivant leur gravité et leur cause. De plus, des interactions et dépendances entre les différentes procédures de gestion d'incident ont été identifiées. En se basant sur une description textuelle

non standardisée des procédures, une représentation graphique de l'ensemble des procédures a été réalisée avec la notation BPMN.

Pour analyser ces procédures, leur intégration dans leur environnement d'exécution était nécessaire. Ainsi, en modélisant par réseaux de Petri les signalements des incidents, le contexte de la ligne sous forme de ressources avec les procédures, le système étudié a été créé. Cette modélisation a nécessité le développement d'une démarche de transformation se basant sur les représentations BPMN des procédures et conduisant à une modélisation réseaux de Petri du système étudié.

IV Analyse et maitrise du danger

Résumé

Dans ce chapitre 4, les états de danger pouvant être atteints lors de l'exécution conjointe d'au moins deux procédures sont caractérisés et définis en intégrant la notion de contrôlabilité d'un événement. Les états critiques à éviter sont ainsi identifiés. Afin de maîtriser le danger accessible, la recherche des séquences sûres est effectuée en se basant sur l'application de la théorie du contrôle par supervision. Après s'être assuré de l'existence d'un contrôleur, les séquences d'événements sont ensuite caractérisées pour déterminer les conseils et alertes potentiels à transmettre à l'opérateur de supervision. Afin d'évaluer l'intégrabilité de mes recherches et de réaliser un démonstrateur, un projet est réalisé par des développeurs de l'équipe ATS de Thales pour ajouter une fonctionnalité d'aide à la décision dans l'application ATS. Ce chapitre présente donc les étapes quatre à huit de la démarche d'étude (figure II.5).

Sommaire

IV.1 Éléments pour l'analyse et la maitrise du danger

Après avoir défini et modélisé le système à étudier, il est important, dans le cadre de la gestion d'incidents, d'analyser les états de danger pouvant être atteints afin de maitriser leur accessibilité. L'analyse vise à mettre en évidence les types d'états pour lesquels la sécurité des utilisateurs n'est plus assurée. Elle a pour but de les déterminer et les caractériser par rapport aux différents éléments du système. La maitrise de l'accessibilité à ces états sera ensuite effectuée par une commande.

IV.1.1 Objectif

Suivant les postulats définis au début de l'étude, l'état atteint après l'occurrence d'un seul incident ne sera pas considéré comme un état de danger puisqu'une procédure existe pour gérer la situation et qu'aucune aide supplémentaire ne pourrait être apportée à l'opérateur. Seuls les états de danger faisant suite à l'occurrence d'au moins deux incidents seront analysées (figure IV.1). L'exécution d'une procédure prend en compte le danger, modifie et adapte les éléments de la ligne de métro, les ressources, pour protéger au mieux les voyageurs et le personnel présents.

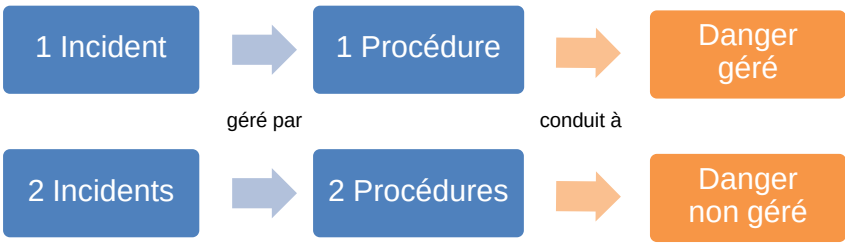


FIGURE IV.1 – Phénomène étudié

L'objectif de cette partie est de montrer que les procédures définies pour répondre à un incident peuvent conduire à un danger lorsque au moins deux incidents apparaissent successivement. Pour cela, il faut tout d'abord déterminer et caractériser l'ensemble des états accessibles. En se basant sur plusieurs critères, notamment la contrôlabilité, les états critiques atteints seront identifiés.

IV.1.2 Automate à états et contrôlabilité

Pour étudier les états de danger pouvant être atteints, il est nécessaire de connaître l'ensemble des états accessibles. Un modèle comportemental à base de réseaux de Petri permet d'obtenir le graphe de tous les marquages accessibles, c'est-à-dire les états accessibles. Les lecteurs non familiers avec les propriétés des réseaux de Petri liées au graphe d'accessibilité pourront se référer aux définitions de l'annexe D. Dans ce graphe, les nœuds représentent l'ensemble des états atteignables et chaque arc correspond au franchissement d'une transition.

Les outils logiciels travaillant avec les réseaux de Petri, comme CPN Tools, calculent et génèrent automatiquement le graphe d'accessibilité d'un réseau de Petri. Pour la suite de l'étude et l'application de la théorie du contrôle par supervision, le graphe des marquages est transformé en automate à états fini (définition 7) afin de définir l'ensemble des événements se produisant et de prendre en compte leur contrôlabilité.

Définition 7 (Automate à état) *Un automate à états fini et déterministe G [Cas99] est un quintuplet :*

$$G = (Q, \Sigma, \delta, q_0, Q_m)$$

- *Q l'ensemble fini des états,*
- *Σ l'ensemble non vide et fini des événements,*
- *$q_0 \in Q$ l'état initial,*
- *$Q_m \subseteq Q$ l'ensemble des états finaux ou marqués,*
- *δ une application telle que $\delta : Q \times \Sigma \to Q$.*

Soit $\sigma \in \Sigma$ un événement et $q \in Q$ un état de l'automate : dans cet état, σ peut se produire seulement si $\delta(q, \sigma)$ est défini.

Soit $G = (Q, \Sigma, \delta, q_0, Q_m)$ l'automate représentant le graphe d'accessibilité d'un réseau de Petri :

- Q l'ensemble des nœuds du graphe,
- Σ l'ensemble des événements correspondant aux noms des transitions impliquées dans les tirs menant d'un marquage à un autre,
- $q_0 \in Q$ le nœud du graphe associé au marquage initiale du RdP,
- $Q_m = \{q_0\}$ dans cette étude car le système est cyclique et le RdP est donc réinitialisable,
- δ décrit les arcs du graphe d'accessibilité.

Définition de la contrôlabilité

Pour différencier les actions maitrisées par l'opérateur de supervision des autres actions qu'il ne peut que constater, la notion de contrôlabilité a été introduite. La contrôlabilité informe sur la possibilité d'interdire ou non le changement entre deux états successifs dans un système à événements discrets.

Au sens de la théorie du contrôle, un événement est contrôlable si le superviseur peut interdire les occurrences de cet événement. Et inversement, un événement est incontrôlable si le superviseur ne peut pas interdire son occurrence. Ces deux ensembles d'événements sont donc disjoints et complémentaires par rapport à l'ensemble des événements d'un système à événements discret.

Définition 8 (Contrôlabilité des événements) *Soit Σ l'ensemble des événements d'un système à événements discrets. Σ_{uc} est l'ensemble des événements incontrôlables et Σ_c l'ensemble des événements contrôlables : $\Sigma = \Sigma_c \cup \Sigma_{uc}$. Σ_{uc}^* définit l'ensemble des séquences d'événements tous incontrôlables.*

Dans un réseau de Petri, le franchissement d'une transition entre deux places se produit instantanément. Dans cette étude, nous considèrerons que le franchissement des transitions correspond à un événement dans le graphe d'accessibilité et donc dans l'automate à états associé. Ainsi, la notion de contrôlabilité d'un événement est transposée au niveau des transitions dans un réseau de Petri : une transition est contrôlable s'il est possible d'interdire son tir.

Dans l'étude, la contrôlabilité différencie l'apparition d'un incident d'une action de l'opérateur de supervision pour exécuter une procédure ou pour modifier le contexte de la ligne au travers d'une ressource. En effet, dans nos représentations BPMN, le passage entre deux étapes

d'une procédure est contrôlable car son déroulement est décidé par un être humain, il peut ne pas être réalisé. L'opérateur de supervision choisit le moment où il débute l'action décrite dans la procédure et contrôle donc le flux des activités. Pour des raisons similaires, les transitions des modèles de ressources sont aussi contrôlables. En effet, l'opérateur de supervision commande les équipements terrains, comme l'énergie de traction, ainsi que l'arrêt ou le mouvement des trains, qui sont représentés par les ressources.

Cependant, contrairement aux procédures et aux ressources, rien ne peut empêcher un incident de se produire : les transitions entre les deux places de signalement d'incident sont donc incontrôlables. L'indication d'un incident peut être effectuée par des moyens de communication qui ne sont pas reliés au système de supervision pour le type de procédures étudiées. L'opérateur doit signaler au système qu'il a reçu une information venant de l'extérieur et ainsi en valider sa réception. Ce signalement est incontrôlable puisqu'il correspond à la validation d'une indication venant de l'extérieur.

Ainsi, la notion de contrôlabilité distinguera l'accessibilité des différents états du système et caractérisera les états de danger atteignables en considérant la maitrise ou non de l'état par l'opérateur de supervision.

IV.1.3 Définitions des ensembles d'étas

Pour différencier les états de danger accessibles, les *Signalements d'un incident* et les *Ressources* composant le système sont utilisés.

États de danger

Les états de danger, notés Q_{danger}, sont caractérisés par les *Signalements d'un incident* et appartiennent à un sous-ensemble des états accessibles noté Q.

Définition 9 (État de danger) *Un état est un état de danger Q_{danger} si au moins deux signalements d'incident sont en cours : $Q_{danger} \subseteq Q$.*

Cependant, le danger réellement encouru par les voyageurs et le personnel dépend également du contexte dans lequel se trouve le système et donc de l'état des ressources. L'ensemble des états de danger va ainsi être affiné.

États sécuritaires et états dangereux

Pour classer les états de danger, les éléments *Ressources* du système sont utilisés, ils décrivent l'environnement dans lequel une procédure est exécutée. Ainsi, selon leur état, les éléments de la ligne protègent ou non les personnes des incidents. Par expertise du système, une identification des combinaisons de ressources garantissant, pour chaque incident, la sécurité des personnes est réalisée. Ces états sécuritaires sont atteints au cours de l'exécution des procédures. Par complémentarité, l'ensemble des états dangereux est ensuite déterminé comme l'ensemble des états de danger dont l'état des ressources ne protège pas les personnes. Dans un état de danger, un état dangereux se caractérise donc par les états des ressources du système.

Deux sous-ensembles des états de danger sont ainsi définis :

- Les états sécuritaires Q_s correspondant aux états où toutes les mesures de prévention ont été prises en suivant la procédure, c'est-à-dire que l'état des ressources protège au mieux les personnes du danger ;

- Les états dangereux Q_d où l'état des ressources ne protège pas les personnes du danger, la combinaison des états des ressources ne garantit donc pas la sécurité des personnes présentes sur la ligne. Si aucun des états accessibles n'est dangereux, alors la sécurité des personnes sera assurée par l'exécution des procédures de gestion d'incident.

Définition 10 (État dangereux) *Un état est considéré comme un état dangereux si l'état appartient à Q_{danger} et si les ressources sont dans une combinaison particulière, définie par une expertise du système, qui ne protège pas les voyageurs et le personnel. Cet ensemble est donc inclus dans l'ensemble des états accessibles du système et l'ensemble des états de danger. L'ensemble des états dangereux du système G est noté $Q_d \subseteq Q_{danger} \subseteq Q$.*

Définition 11 (État sécuritaire) *Un état est sécuritaire s'il appartient à Q_{danger} mais n'appartient pas Q_d. Ainsi, Q_s est le complémentaire de Q_d dans Q_{danger} : $Q_d \cup Q_s = Q_{danger}$.*

États critiques

Lorsqu'un état dangereux Q_d est atteint, les voyageurs et le personnel se trouvent dans un état où leur sécurité n'est pas garantie. L'important dans un tel état est de savoir si l'opérateur de supervision peut agir sur le système pour sortir de cet état et ainsi protéger au mieux ces personnes. La notion de contrôlabilité des transitions permet de savoir si le passage d'un état à un autre est maitrisable par l'opérateur de supervision. Ainsi, les états dangereux sont classés suivant la contrôlabilité de leurs transitions sortantes : l'ensemble des états critiques Q_{cr} est alors défini.

Définition 12 (État critique) *Un état critique Q_{cr} est un état dangereux dont il est seulement possible de sortir par des transitions incontrôlables, c'est-à-dire la disparition de l'un des incidents ou l'apparition d'un nouveau. Ainsi, $Q_{cr} \subseteq Q_d$.*

Cette définition est provisoire, elle sera précisée avec des notions mathématiques dans la partie suivante (IV.2.3).

Inclusion des ensembles

Pour caractériser les états de danger atteignables dans le système, plusieurs ensembles d'états ont été définis. Ces ensembles sont tous des sous-ensembles de l'ensemble des états accessibles du système Q, déterminé à partir du modèle réseaux de Petri. Un autre sous-ensemble d'état constituant le mode nominal est également spécifié.

Définition 13 (État nominal) *Les états nominaux correspondent aux états où aucun incident ne s'est produit et aucune procédure de gestion d'incident n'est en cours. Ces états représentent un fonctionnement nominal, sans incident, et sont notés Q_n.*

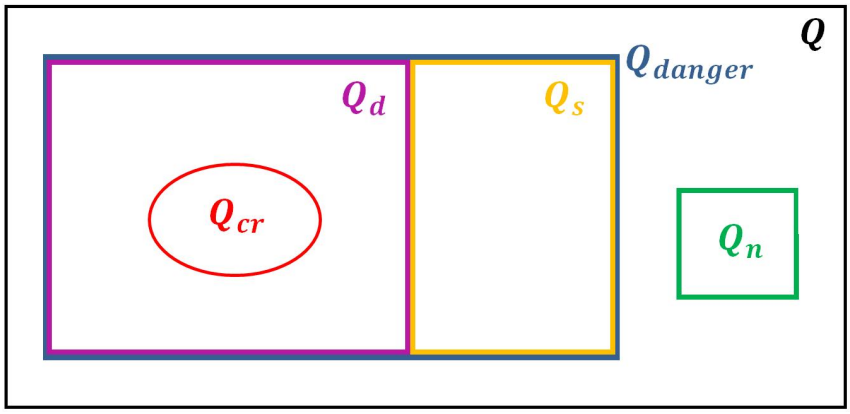


FIGURE IV.2 – Inclusion des ensembles

La figure IV.2 met en évidence les différentes inclusions entre tous ces ensembles.

L'ensemble des états Q du système a été caractérisé en définissant plusieurs sous-ensembles. Pour éviter les états critiques Q_{cr}, il est nécessaire d'étudier les enchainements d'événements conduisant à ces états et les solutions envisageables pour en sortir afin de garantir la sécurité des personnes. L'objectif est donc de mettre en place un mécanisme de contrôle sur les états critiques identifiés afin de les éviter.

IV.2 Recherche des séquences sûres

IV.2.1 Objectif

L'étude des évolutions possibles menant aux états critiques Q_{cr} est maintenant à réaliser. L'objectif de contrôle recherché est d'empêcher le système d'atteindre ces états en déterminant l'ensemble des évolutions incontrôlables menant à ces états et en identifiant ainsi les évolutions admissibles du système. Pour que le système respecte l'objectif de contrôle, les comportements possibles du système sont ainsi réduits pour les limiter aux comportements garantissant la sécurité des personnes.

Pour éviter d'atteindre l'ensemble des états critiques, l'étude se base sur la théorie du contrôle par supervision. Ainsi, les séquences d'événements incontrôlables conduisant aux états critiques seront identifiées. Cependant, contrairement aux approches présentées dans la section II.5.2, les états critiques Q_{cr} à interdire se définissent non seulement par leur inclusion dans l'ensemble défini des états dangereux Q_d mais également par la contrôlabilité de leurs transitions sortantes. Une approche complémentaire et distincte de la base théorique du contrôle par supervision est donc proposée dans cette étude en s'appuyant sur la définition des états critiques.

Dans cette partie, après avoir différencié l'objectif de contrôle et les problèmes classiques d'interdiction d'états, les ensembles des états critiques et redoutés sont définis formellement puis déterminés par algorithme. Un exemple illustrera les différentes étapes à suivre.

IV.2.2 Problème d'interdiction d'états

Dans notre étude, les exigences ne sont pas décrites par des comportements désirés, sous forme d'automates à états, comme lors de l'application de la théorie du contrôle par supervision

(TCS) dans son approche langage ayant pour but de synthétiser un superviseur. Ici, l'objectif de contrôle est défini par un ensemble d'états à interdire et la TCS est appliquée dans son approche état.

Dans les approches se basant sur des systèmes modélisés par réseaux de Petri présentées dans la section II.5.2, l'ensemble des états interdits est défini par des contraintes sur le marquage des places (Mutuelle Exclusion). Dans notre étude, l'ensemble des états interdits n'est pas un paramètre connu. Ainsi, le calcul de l'ensemble des états à éviter ne pourra pas uniquement se faire en appliquant les résultats de recherches antérieures mais requière le développement d'une nouvelle méthode de détermination prenant en compte non seulement l'inclusion d'un état dans un ensemble donné mais également la contrôlabilité des transitions.

Pour atteindre l'objectif de contrôle, un algorithme est développé pour identifier l'ensemble des états critiques et, en se basant sur [Gau03][Gau04], pour déterminer l'ensemble des états à éviter. Pour son implémentation, l'algorithme est développé dans le langage Python et s'appuie sur l'outil DESlab [Cla12], une librairie pour l'analyse et la synthèse de systèmes à événements discrets modélisés par des automates à états.

IV.2.3 Ensemble des états critiques

Comme présenté précédemment, un état critique Q_{cr} est un état dangereux Q_d dans lequel l'opérateur ne peut pas agir sur le système pour modifier l'état des ressources et ainsi atteindre un état sécuritaire. Pour déterminer cet ensemble d'états, il ne suffit pas de déterminer les états dangereux à partir duquel il est seulement possible de sortir par un événement incontrôlable. En effet, il faut également identifier les boucles d'états dont il est seulement possible de sortir de manière incontrôlable. Ces boucles sont des composantes fortement connexes du graphe d'accessibilité.

Le lecteur pourra se référer à l'annexe E sur les graphes orientés et les composantes fortement connexes. La notion de composante fortement connexe d'un graphe orienté permet de définir mathématiquement et plus précisément la définition 12 de l'ensemble des états critiques.

Définition 14 (État critique) *Un état critique est un état appartenant à l'ensemble des états dangereux Q_d et appartenant à une composante fortement connexe $\mathscr{C}_i$ de l'ensemble $\mathscr{C}$ des composantes fortement connexes de l'automate G, $\mathscr{C}_i \in \mathscr{C}$. L'état est critique s'il est seulement possible de sortir de la composante fortement connexe à laquelle il appartient par un événement incontrôlable Σ_{uc}.*

L'ensemble des états critiques Q_{cr} de G est défini formellement par :

$$Q_{cr} = \{q \in Q_d \wedge q \in \mathscr{C}_i \mid \forall \delta(q,\sigma) : \sigma \in \Sigma_{uc} \vee \delta(q,\sigma) \in \mathscr{C}_i\}$$

Exemple

L'exemple suivant présente la méthode à suivre pour identifier l'ensemble des états critiques. L'automate exemple (figure IV.3) est une partie d'un automate déterministe, seulement onze états sont considérés. Les transitions qui ne sont pas prises en compte sont représentées par des traits pointillés. Pour les autres transitions, la contrôlabilité est notée par la lettre C si la

transition est contrôlable et par UC sinon. Les événements ne sont pas étudiés ni représentés ici, seul leur contrôlabilité est examinée.

L'ensemble des états dangereux est un paramètre connu et déterminé par expertise du système, ces états sont coloriés en jaune. Les états critiques, cerclés de rouge, sont déterminés à partir de la définition 14.

Pour cet exemple, les états $\{5, 6, 7, 8\}$ sont définis comme des états dangereux. En analysant le graphe, deux de ces états sont identifiés comme critiques : $Q_{cr} = \{7, 8\}$. En effet, la seule transition sortante de l'état 7 est incontrôlable et cet état forme une composante fortement connexe à un seul sommet. L'état 8, quant à lui, appartient à la composante fortement connexe à deux sommets $\{4, 8\}$ et la seule transition sortante de l'état 8 et ne menant pas à un état de la composante fortement connexe est incontrôlable. Cependant, il existe au moins une transition sortante contrôlable pour les états $\{5, 6\}$.

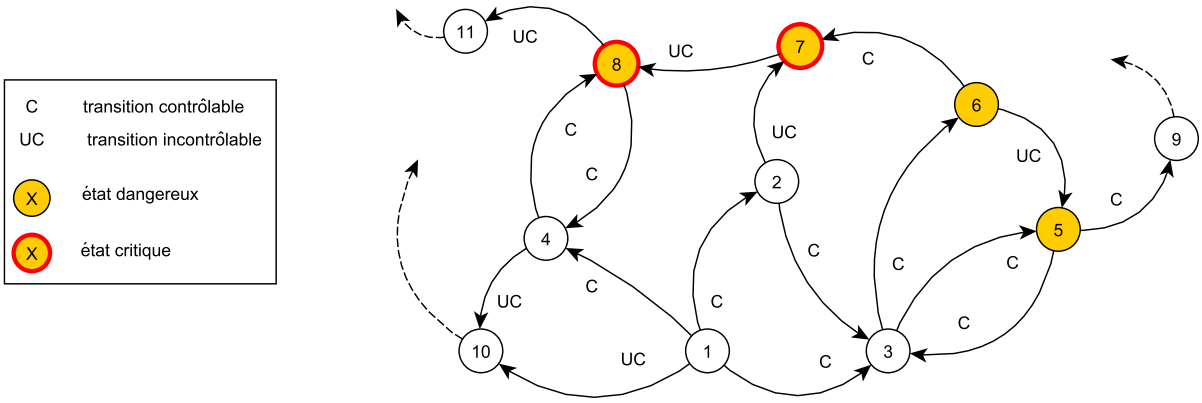


FIGURE IV.3 – États dangereux et critiques

Algorithme

Pour déterminer l'ensemble des états critiques Q_{cr} d'un automate à états G donné, l'algorithme 1 a été défini.

L'objectif recherché est d'éviter d'accéder à l'ensemble des états critiques. L'algorithme développé permet de déterminer l'ensemble des états critiques, il faut ensuite étudier les séquences d'événements menant à ces états critiques afin de contrôler leur accès.

IV.2.4 Ensemble des états redoutés

Pour éviter d'atteindre un état critique, l'ensemble des états redoutés est défini.

Définition 15 (État redouté) *Un état redouté est un état à partir duquel il est possible d'atteindre au moins un état critique par une séquence d'événements incontrôlables. Par définition, tous les états critiques sont des états redoutés. L'ensemble Q_{re} des états redoutés du système G est défini par :*

$$Q_{re} = Q_{cr} \cup \{q \in Q \backslash Q_{cr} \mid \exists s \in \Sigma_{uc}^* : \delta(q, s) \in Q_{cr}\}$$

Algorithme 1 Calcul des états critiques Q_{cr}

Entrées : G, Q_d, Σ_{uc}, Σ_c

Soit $Q_{cr} = \{\ \}$
Pour tout $e \in \Sigma_{uc}$
  Supprimer toutes les transitions avec e de G
Calculer $\mathscr{C}$: ensemble des composantes fortement connexe de G
Pour tout composante fortement connexe $c \in \mathscr{C}$:
  Pour tout état $q \in c$:
    Si $\exists \sigma \in \Sigma_c \mid \delta(q, \sigma) \notin \mathscr{C}$ **alors** :
      Supprimer c de $\mathscr{C}$
Pour tout $c \in \mathscr{C}$:
  Pour tout $q \in c$:
    Si $q \in Q_d$ **alors** :
      Ajouter q dans Q_{cr}

Sorties : Q_{cr}

Pour maitriser l'accessibilité des états redoutés, les transitions contrôlables menant aux états redoutés, les transitions à proscrire, sont identifiées.

Définition 16 (Transition à proscrire) *Les transitions à proscrire sont l'ensemble des transitions qui mènent aux états redoutés Q_{re} par un événement contrôlable :*

$$\Delta_p = \{(q, \sigma, p) \mid q \in Q, \sigma \in \Sigma_c, p \in Q_{re} \wedge \delta(q, \sigma) = p\}$$

Exemple

Après les états critiques, les états redoutés Q_{re} et les transitions proscrites Δ_p sont maintenant déterminés dans l'exemple. Sur l'automate exemple, les états redoutés sont encadrés en orange et les transitions à proscrire menant à un état redouté par un événement contrôlable sont barrées par une croix bleue.

En se basant sur les définitions et pour l'exemple présenté, l'ensemble des états redoutés $Q_{re} = \{2, 7, 8\}$ contient trois états (figure IV.4). Les états 7 et 8 sont des états critiques donc ils appartiennent à l'ensemble des états redoutés et l'état 2 est le seul état à partir duquel il est possible d'atteindre un des états critiques par une séquence de transitions incontrôlables, réduite ici à une seule transition. Les trois transitions : $1 \xrightarrow{C} 2$, $4 \xrightarrow{C} 8$ et $6 \xrightarrow{C} 7$ sont ensuite identifiées comme à proscrire pour ne pas atteindre l'ensemble des états redoutés.

Après avoir déterminé les états redoutés et les transitions à proscrire et en considérant l'automate après avoir supprimé les trois transitions à proscrire identifiées, il n'existe plus qu'une seule transition sortante de l'état 6. De plus, cette transition est incontrôlable et l'état 6 est dangereux. Il est également possible d'atteindre cet état puisque la transition $3 \xrightarrow{C} 6$ est autorisée. L'objectif de contrôle n'est donc pas respecté car l'état 6 est critique et il est possible d'y accéder. Une nouvelle recherche de l'ensemble des états critiques et des états redoutés présents dans l'automate doit donc être réalisée.

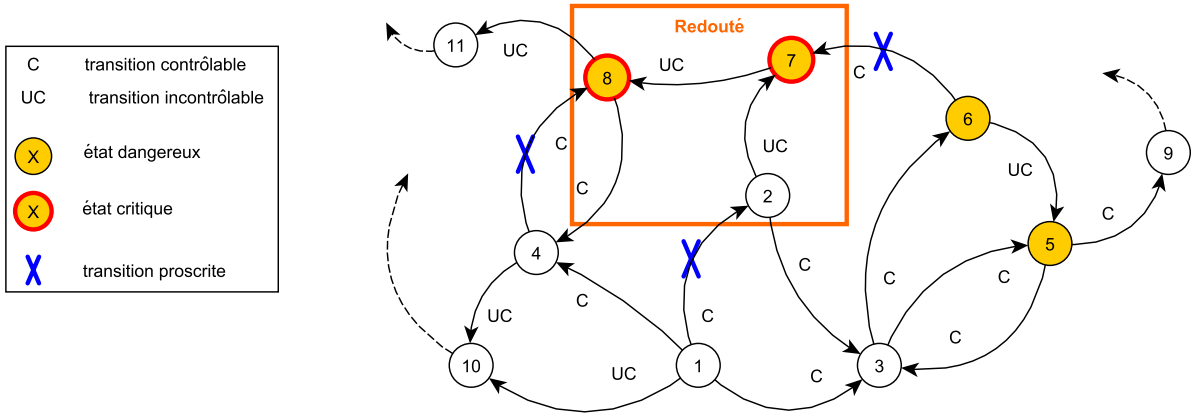


FIGURE IV.4 – Résultat de la première itération

Pendant la seconde itération de calculs (figure IV.5), un nouvel état critique est identifié et l'ensemble des états critiques devient alors $Q_{cr} = \{6, 7, 8\}$. L'ensemble des états redoutés est aussi étendu : $Q_{re} = \{2, 6, 7, 8\}$. Pour empêcher le système d'atteindre cet ensemble d'états, une autre transition doit être proscrite : $3 \xrightarrow{C} 6$.

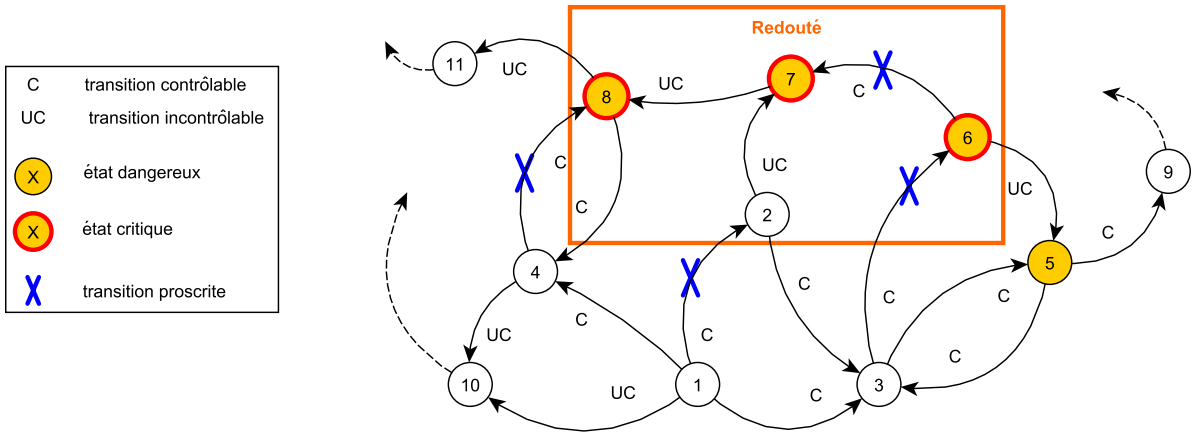


FIGURE IV.5 – Résultat de la seconde itération

À la fin de cette seconde itération, l'état dangereux 5 est encore accessible mais il existe une transition contrôlable $5 \xrightarrow{C} 9$ permettant d'en sortir, l'état 5 n'est donc pas critique. En réalisant une nouvelle itération de calculs, l'ensemble des états critiques obtenu serait le même que lors de l'itération précédente. Ainsi, si deux itérations successives donnent les mêmes ensembles d'états critiques et redoutés, ces ensembles seront considérés comme stables et la détermination de ces ensembles sera terminée. Pour conclure, deux itérations sont donc nécessaires pour l'exemple considéré ici pour respecter l'objectif de contrôle.

L'exemple présenté a mis en évidence l'importance d'un calcul itératif des ensembles des états critiques et redoutés. L'algorithme suivant présente la détermination de ces ensembles et des transitions à proscrire afin de respecter l'objectif de contrôle recherché. Il s'applique sur le graphe d'accessibilité du système calculé précédemment.

Algorithme

Seuls les événements contrôlables peuvent être interdits c'est pourquoi l'ensemble des états redoutés, à partir desquels il est possible d'atteindre un état critique par une séquence d'événements incontrôlables, est déterminé. Pour éviter ces états critiques, toutes les transitions contrôlables menant à un état redouté sont donc à proscrire. Cependant, comme l'exemple l'a mis en évidence, cette interdiction modifie le nombre de transitions sortantes de certains états. Pour respecter l'objectif de contrôle, le calcul des états critiques et redoutés doit donc être itératif jusqu'à ce que deux itérations successives donnent les mêmes ensembles.

En effet, l'étude recherche l'ensemble des états inclus dans l'ensemble des états dangereux avec seulement des sorties incontrôlables. L'objectif de contrôle conduit à interdire le franchissement des transitions contrôlables et un état dangereux peut devenir un nouvel état critique si ces transitions sortantes non interdites sont uniquement incontrôlables. Ainsi, après avoir déterminé les états critiques et redoutés lors de la première itération de l'algorithme, les transitions contrôlables à proscrire sont identifiées. En interdisant ces transitions, l'ensemble critique peut être étendu et de nouveaux états redoutés apparaissent.

L'algorithme 2 calcule de manière itérative les ensembles des états critiques et redoutés jusqu'à la construction de deux ensembles successifs identiques. Les itérations de calcul des ensembles Q_{cr} et Q_{re} convergent puisque $Q_{cr} \subseteq Q_d \subseteq Q$, $Q_{re} \subseteq Q$ et que l'ensemble des états Q est un ensemble fini. Ainsi, si lors d'une itération $Q_{cr} = Q_{re} = Q$, l'itération suivante donnera les mêmes ensembles.

Algorithme 2 Calcul des ensembles Q_{cr} et Q_{re}

Entrées : G, Q_d, Σ_{uc}, Σ_c

Soit $G_\Delta = G$
Soit $Q_{cr_0} = \{\ \}$

Calculer Q_{cr_1} de G_Δ en appliquant l'algorithme 1
Soit $n = 1$
Tant que $Q_{cr_n} \neq Q_{cr_{n-1}}$ **Faire :**
  Calculer Q_{re_n} de G_Δ
  Calculer Δ_{p_n} de G_Δ
  Pour tout $t \in \Delta_{p_n}$ **:**
    Supprimer t de G_Δ
  Calculer $Q_{cr_{n+1}}$ de G_Δ
  $n = n + 1$

Sorties : Q_{cr_n}, Q_{re_n}

Les ensembles des états critiques Q_{cr} et des états redoutés Q_{re} évoluent donc entre deux itérations, la figure IV.6 présente une évolution possible entre l'itération n et $n + 1$.

Les états nouveaux critiques identifiés lors de l'itération $n + 1$ ne sont pas inclus dans les états redoutés Q_{re_n}. En effet, les transitions à proscrire sont des transitions menant à l'ensemble des états redoutés et ne peuvent donc pas être des transitions sortantes de ces états. L'ensemble $Q_{re_{n+1}}$ inclut les états redoutés Q_{re_n} de l'itération précédente, les nouveaux états critiques de

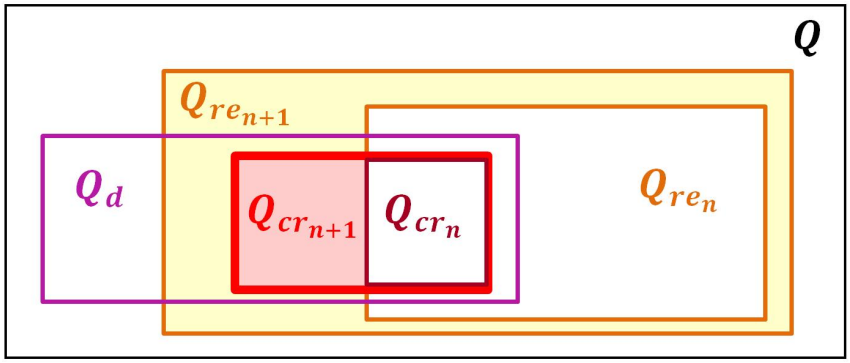


FIGURE IV.6 – Inclusion des ensembles lors de leur calcul itératif

$Q_{cr_{n+1}}$ et les nouveaux états redoutés identifiés : $Q_{re_n} \subseteq Q_{re_{n+1}}$ et $Q_{cr_{n+1}} \subseteq Q_{re_{n+1}}$. De plus, $Q_{cr_n} \subseteq Q_{cr_{n+1}}$.

La prise en compte de la contrôlabilité des transitions dans la définition des états critiques impose un calcul itératif des états critiques et redoutés pour atteindre l'objectif de contrôle. En supprimant l'ensemble des états redoutés, l'espace d'états obtenu décrit alors l'évolution admissible, les états et les séquences d'événements admissibles, répondant à l'objectif de contrôle défini.

IV.2.5 Conclusion

Le problème d'évitement des états critiques solutionné dans cette partie se différencie du problème des états interdits de la théorie du contrôle par supervision par la définition même des états interdits. En effet, en ajoutant à la contrainte d'inclusion des états dans un ensemble une contrainte sur la contrôlabilité des transitions sortantes et une inclusion dans une composante fortement connexe, la méthode de calcul est alors différente et se doit d'être itérative afin de déterminer tous les états interdits.

L'objectif de contrôle est d'identifier l'ensemble des états menant de manière incontrôlable aux états critiques et de calculer l'ensemble des états à éviter. Dans la quatrième étape de la démarche globale d'étude des procédures de gestion d'incidents d'une ligne de métro (figure II.5), les états pouvant porter atteinte à la sécurité des personnes et non maitrisable par l'opérateur de supervision sont alors déterminées aux travers des états redoutés calculés.

L'ensemble des états à éviter est maintenant connu mais il est nécessaire de vérifier l'existence d'un contrôle. Cette existence permettrait ainsi d'assurer qu'il existe une solution pour l'opérateur de supervision d'une ligne de métro pour éviter les situations où la sécurité des personnes n'est pas garantie.

IV.3 Vérification de l'existence d'un contrôleur

IV.3.1 Objectif

Après avoir déterminé l'ensemble des états redoutés, il est nécessaire de vérifier l'existence d'un contrôleur permettant d'éviter ces états. L'objectif est de formaliser le système contrôlé respectant l'objectif de contrôle pour ainsi obtenir l'ensemble des états admissibles.

En ajoutant des arcs et des places dans le modèle RdP, le contrôleur permet d'éviter les comportements indésirables identifiés pour obtenir ainsi un RdP contrôlé. Ce contrôleur doit également être le plus permissif possible pour garantir une intervention minimale sur le comportement du système en interdisant uniquement d'atteindre l'ensemble des états redoutés. Le système contrôlé ayant intégré des places de contrôle permettra de vérifier que les propriétés du modèle initial : non blocage, maximum permissif, inclusion du comportement minimum et réinitialisable, sont conservées.

Pour la gestion des incidents se produisant sur une ligne de métro, la vérification de l'existence d'un système contrôlé obtenu après l'interdiction de certains états est importante. En effet, l'objectif est d'éviter ces états tout en assurant que l'exécution des procédures est toujours possible, le système doit rester disponible.

IV.3.2 Intégration du contrôle dans le modèle du système

En s'appuyant sur les travaux effectués et présentés dans la section II.5.3, des places de contrôle vont être intégrées au modèle réseau de Petri pour éviter les états redoutés. Seule la démarche de détermination des places de contrôle est présentée ici, les détails sur les méthodes de calcul sont donnés dans les références citées.

Contraintes linéaires

L'accessibilité ou la non accessibilité de l'ensemble des marquages d'un modèle s'exprime sous forme d'un ensemble de contraintes linéaires, des GMEC (Generalized Mutual Exclusion Constraints). Une GMEC est une condition qui limite la somme pondérée de marques dans un ensemble de places pour un réseau de Petri sauf et vivant. Ainsi, pour éviter un ensemble d'états, les spécifications peuvent être exprimées sous forme de contraintes linéaires entre les marquages des places du RdP sauf. L'ensemble des marquages atteignables est donc réduit et doit vérifier ces contraintes.

L'ensemble des états à éviter correspond aux états redoutés, chacun de ces états est caractérisé par son vecteur marquage du réseau de Petri. Soit $q_{re} \in Q_{re}$ un état redouté ayant pour marquage $M_{q_{re}}^T = [m_1, m_2, ..., m_n]$ avec n le nombre de places du réseau de Petri.

Le support d'un vecteur marquage définit l'ensemble des places marquées, c'est-à-dire les valeurs du vecteur marquage non nulles. Ainsi : $Support(M_{q_{re}}) = \{p_1, p_2, ..., p_m\}$ correspondant à l'ensemble des m places marquées de q_{re}. Pour un réseau de Petri sauf, la contrainte linéaire interdisant cet état est définie, avec $m \leq n$ par :

$$\sum_{k=1}^{n} m_k \leq Card(Support(M_{q_{re}})) - 1$$

$Card(Support(M_{q_{re}}))$ est égal au nombre de places marquées dans le marquage de l'état q_{re} et définit la borne supérieure de la contrainte linéaire de l'état redouté. En effet, pour que l'état q_{re} ne soit pas accessible, l'ensemble de ses places marquées ne doit pas pouvoir être marqué en même temps.

La méthode développée par Giua [Giu92] pour transformer un ensemble d'états interdits en contraintes linéaires s'applique à notre étude réalisée sur les procédures de gestion d'incidents d'une ligne de métro. Pour cela, il faut montrer que le modèle réseaux de Petri du système étudié

est sauf et conservatif. Comme présenté dans la section III.3, le système est composé de trois types d'éléments : les procédures de gestion d'incidents, les ressources décrivant l'état de la ligne de métro et les signalements d'incident permettant le déclenchement des procédures. Chacun de ces éléments est modélisé par un réseau de Petri sauf. De plus, les procédures, les ressources et les signalements d'incident ne peuvent pas être dans deux états contradictoires en même temps. L'ensemble des places modélisant chacun de ces éléments forme donc un P semi-flot du réseau de Petri du système. Le réseau de Petri du système étudié est donc bien sauf et conservatif et les états redoutés peuvent être décrits par des contraintes linéaires en utilisant les recherches de Giua.

Simplification des contraintes

Pour que le contrôleur calculé soit optimal, il faut minimiser le nombre de contraintes et ainsi limiter le nombre de places de contrôle à ajouter dans le système pour qu'il vérifie l'objectif de contrôle. En s'appuyant sur les recherches de Dideban [Did08][Did13] (section II.5.3), les contraintes linéaires sont simplifiées lors de deux étapes successives : la simplification par l'invariant et la simplification par l'invariant partiel.

Pour cela, l'ensemble des P semi-flots du RdP sauf est déterminé. Cet ensemble est noté : $\Phi = \left\{ Y \mid Y^T = [m_1, m_2, ..., m_n] \right\}$ avec, dans le vecteur marquage, $m_k = 1$ si la place appartient au P semi-flot et 0 sinon. À chaque P semi-flot Y est associée une égalité telle que la somme des marques présentes dans le support de son vecteur marquage soit égale à 1. En effet, le réseau de Petri étant conservatif, une seule des places du support du P semi-flot peut être marquée.

En se basant sur les invariants du système, Dideban propose tout d'abord une simplification par l'invariant des contraintes linéaires. Cette simplification diminue le nombre de contraintes linéaires appliquées au système. Cependant, le contrôleur ainsi obtenu n'est pas optimal et peut encore être simplifié en s'appuyant sur la méthode de simplification par l'invariant partiel.

Les deux simplifications diminuent le nombre des contraintes tout en conservant l'équivalence avec l'ensemble des états redoutés à éviter. Si le système respecte les inégalités de marquages décrites par les contraintes linéaires, les états redoutés ne seront pas atteignables. Pour intégrer le contrôleur au modèle du système, des places de contrôle sont ajoutées, chaque contrainte correspondant au marquage de l'une des places. Pour cela, la démarche développée par Yamalidou [Yam96] est appliquée et la matrice d'incidence du système contrôlé est calculée.

IV.3.3 Propriétés du système contrôlé

La détermination de places de contrôle empêchant d'atteindre l'ensemble des états redoutés prouve ainsi l'existence d'un contrôle possible. Une analyse du système contrôlé peut ensuite permettre de vérifier que les propriétés du système initial, non blocage, maximum permissif, inclusion du comportement minimum et réinitialisable, n'ont pas été dégradées avec ce contrôle.

L'objectif est de garantir que les spécifications de sécurité et de vivacité soient respectées mais également d'être maximum permissif. En effet, le contrôleur doit interdire l'ensemble des états à éviter mais ne doit pas interdire des comportements admissibles. Les recherches de Yamalidou et Dideban garantissent la détermination d'un contrôleur maximum permissif.

Le système obtenu doit également pouvoir évoluer sans atteindre un blocage. En effet, un blocage lors de l'exécution d'une procédure de gestion d'incident signifierait qu'il existe aucune

solution pour sortir de l'état en cours et que le système va rester indéfiniment dans cet état, ce qui n'est pas acceptable. Cette propriété est garantie par les méthodes de détermination du contrôle appliquées.

De plus, il est important que le système puisse revenir à son état initial, lorsqu'aucune procédure est en cours ni aucun incident. Cette propriété peut se vérifier directement sur le modèle réseau de Petri contrôlé en s'assurant que le RdP soit réinitialisable. Elle se vérifie également sur son graphe d'accessibilité. Ainsi, si le graphe d'accessibilité généré est accessible et coaccessible, tous les états sont atteignables et à partir de tous les états il est donc toujours possible d'atteindre l'état initial.

La mise en place d'un contrôle interdit l'accès à certains états, cependant, les états appartenant au mode nominal (section IV.1.3) doivent toujours être accessibles lors de l'exploitation d'une ligne de métro. Ces états décrivent l'évolution possible du système lorsqu'aucun incident ne s'est produit et le comportement minimal que le système doit toujours pouvoir réaliser quel que soit le contrôle déterminé. Ainsi, le graphe d'accessibilité du système contrôlé doit inclure l'ensemble de ces états.

Ainsi, en déterminant le réseau de Petri contrôlé du système, il est possible de vérifier que les propriétés du système étudié soient conservées. De plus, la détermination d'un contrôle assure l'existence d'une solution pour éviter l'ensemble des états redoutés. Pour poursuivre l'objectif d'améliorer la sécurité des voyageurs et du personnel lors de la gestion des incidents sur une ligne de métro, les séquences d'événements admissibles vont être analysées pour guider l'opérateur de supervision lors de l'exécution des actions.

IV.4 Analyse des trajectoires et assistance à l'opérateur

IV.4.1 Objectif

L'existence d'un contrôle pour éviter l'ensemble des états redoutés peut être vérifiée en appliquant la méthode développée dans la partie précédente. L'étude concerne cependant des actions réalisées par un opérateur humain de supervision, ces actions ne sont donc pas automatisées. Ainsi, il est possible en théorie d'éviter les états où la sécurité des passagers et du personnel lors de la gestion d'incidents sur une ligne de métro n'est pas garantie, mais il n'est pas envisageable de limiter les actions de l'opérateur de supervision. L'objectif est donc de conseiller et d'alerter l'opérateur sur ce qu'il y a de mieux à faire pour assurer la sécurité des personnes et de le lui indiquer le plus tôt possible. Les successions d'actions que l'opérateur de supervision peut réaliser et pouvant mener à des états redoutés sont donc analysées et classées suivant notamment leur état de destination.

L'étude de ces trajectoires ne peut pas être effectuée sur le système contrôlé puisque les transitions à ne pas franchir ne seraient pas présentes et aucune alerte préalable ne pourrait être donnée. De plus, la différence entre des transitions interdites par le contrôle et des transitions interdites par le système lui-même ne serait plus perceptible. L'existence d'un contrôle et donc d'une solution pour éviter les états redoutés ayant été montrés, le graphe d'accessibilité du système non contrôlé est utilisé pour identifier les informations à transmettre à l'opérateur de supervision.

En replaçant cette étape dans la démarche globale de l'étude (figure II.5), l'analyse des trajectoires et leur caractérisation correspondent à un objectif plus global d'alerter et de conseiller

les opérateurs de supervision pour la gestion des incidents, la septième étape. Ces alertes et conseils se feront sous forme de messages délivrés aux opérateurs et apporteront une indication sur les actions à ne pas exécuter, s'ils en existent, et des conseils sur les actions à privilégier et qui mèneraient à un état moins dangereux pour les voyageurs et le personnel. L'opérateur sera ainsi orienté et guidé dans la succession d'actions à réaliser pour assurer au mieux la sécurité des passagers et éviter les états critiques. Les états où un message sera transmis à l'opérateur de supervision sont regroupés dans l'ensemble Q_{mess}.

Pour différencier et caractériser les trajectoires admissibles, des critères de différenciation ont été retenus. Ces critères sont définis pour déterminer quelles indications doivent être transmises ainsi que le moment où elles doivent être données à l'opérateur de supervision pendant la gestion d'incidents. Les trajectoires conseillées seront ainsi optimisées par rapport aux critères choisis afin de protéger au mieux les personnes lors d'incidents. Ces indications informent l'opérateur de supervision sur les conséquences possibles de leurs actions, les possibilités d'atteindre certains états et le dirigent vers une meilleure gestion des incidents simultanés.

IV.4.2 Caractérisation des transitions

Critères de différentiation

L'ensemble des états redoutés à éviter a été déterminé précédemment, l'étude porte maintenant sur les transitions menant à ces états. Plusieurs critères ont été définis pour les différencier et ainsi donner à l'opérateur de supervision un message utile et délivré au meilleur moment.

Le message adressé à l'opérateur pour le conseiller dans la succession des activités qu'il exécute doit se rapporter à une action qu'il peut réaliser. Ainsi, seules les transitions contrôlables seront étudiées puisqu'elles correspondent aux seules actions que l'opérateur maîtrise.

De plus, des messages sont délivrés à l'opérateur seulement si au moins deux incidents sont en cours. En effet, suivant un des postulats de l'étude (section I.3), les procédures sont justes par usage lorsqu'elles sont utilisées pour gérer un incident, seul le déroulement de plusieurs procédures conjointes est susceptible de conduire à des états critiques. Pour gérer un seul incident, l'opérateur n'a pas besoin de conseil supplémentaire qui pourrait réduire son attention plutôt que l'aider dans l'exécution de la procédure dédiée.

Ensembles de transitions frontières

Chacune des transitions sortantes d'un état frontière par un événement contrôlable appartient à un et un seul ensemble et est appelée transition frontière. L'ensemble des transitions frontières est noté Δ_{fr}. Quatre ensembles distincts de transitions frontières sont définis suivant l'état de destination de la transition : $\Delta_{Rouge_{fr}}$, $\Delta_{Jaune_{fr}}$, $\Delta_{Violette_{fr}}$ et $\Delta_{Verte_{fr}}$ (figure IV.7).

Ainsi, les ensembles des transitions sont des ensembles disjoints :

$$\Delta_{fr} = \Delta_{Rouge_{fr}} \cup \Delta_{Jaune_{fr}} \cup \Delta_{Violette_{fr}} \cup \Delta_{Verte_{fr}}$$

Pour chaque état frontière, chacune des transitions sortantes est associée à l'un des quatre ensembles et est ainsi caractérisé en fonction de son état de destination. La définition de ces quatre ensembles de transitions donne également une indication sur la distance aux états redoutés. En effet :

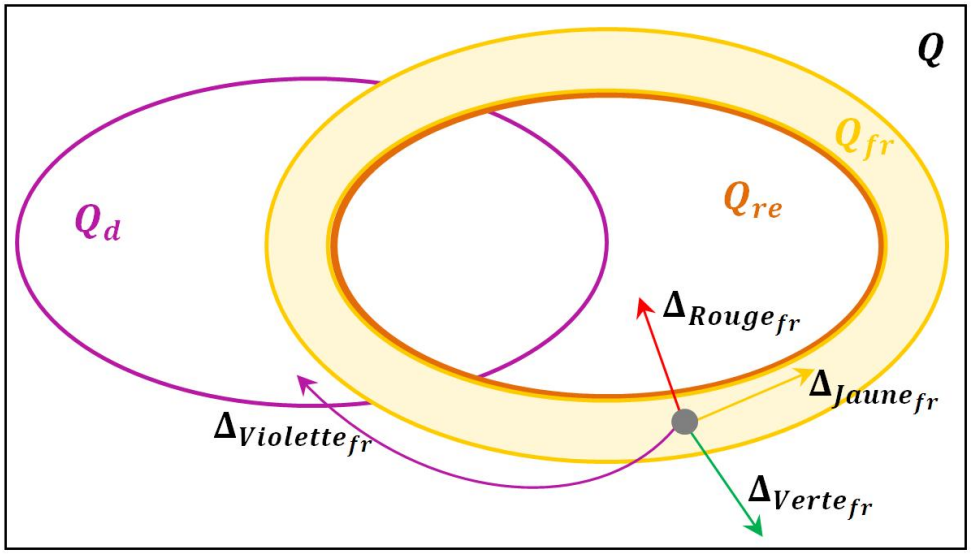


Figure IV.7 – Transitions sortantes des états frontières

- une transition Rouge Frontière conduit directement à un état redouté,
- une transition Jaune Frontière reste à la même distance d'un état redouté et ne permet donc pas de s'en éloigner,
- une transition Violette Frontière s'éloigne d'un état redouté mais conduit à un état dangereux,
- une transition Verte Frontière s'éloigne d'un état redouté et mène à un état non dangereux.

Définitions formelles des états et transitions frontières

Définition 17 (État frontière) *Un état frontière est un état où au moins deux incidents sont en cours, donc appartenant à l'ensemble des états de danger Q_{danger}, et à partir duquel il est possible d'atteindre au moins un état redouté par un événement contrôlable. De plus, un état frontière n'appartient pas à l'ensemble des états redoutés. L'ensemble des états frontières, noté Q_{fr}, est défini par :*

$$Q_{fr} = Q_{danger} \cap \{q \in Q \backslash Q_{re} \mid \exists \sigma \in \Sigma_c : \delta(q, \sigma) \in Q_{re}\}$$

Définition 18 (Transition Rouge Frontière) *Une transition Rouge Frontière est une transition menant, par un événement contrôlable, d'un état frontière à un état redouté. Par définition de Q_{fr}, l'ensemble des transitions Rouge Frontière contient au moins une transition par état de Q_{fr}. L'ensemble des transitions Rouge Frontière, noté $\Delta_{Rouge_{fr}}$, est défini par :*

$$\Delta_{Rouge_{fr}} = \{(q, \sigma, p) \mid q \in Q_{fr} \wedge \sigma \in \Sigma_c \wedge p \in Q_{re}\}$$

Définition 19 (Transition Jaune Frontière) *Une transition Jaune Frontière est une transition menant, par un événement contrôlable, d'un état frontière à un état frontière. L'ensemble des transitions Jaune Frontière, noté $\Delta_{Jaune_{fr}}$, est défini par :*

$$\Delta_{Jaune_{fr}} = \{(q, \sigma, p) \mid \sigma \in \Sigma_c \wedge (q, p) \in Q_{fr} \times Q_{fr}\}$$

Définition 20 (Transition Violette Frontière) *Une transition Violette Frontière est une transition menant, par un événement contrôlable, d'un état frontière à un état dangereux qui n'est ni un état redouté ni un état frontière. L'ensemble des transitions Violettes Frontière, noté* $\Delta_{Violette_{fr}}$*, est défini par :*

$$\Delta_{Violette_{fr}} = \{(q, \sigma, p) \mid q \in Q_{fr} \wedge \sigma \in \Sigma_c \wedge p \in Q_d \wedge p \notin Q_{re} \wedge p \notin Q_{fr}\}$$

Définition 21 (Transition Verte Frontière) *Une transition Verte Frontière est une transition partant, par un événement contrôlable, d'un état frontière et n'appartenant pas aux ensembles des transitions Rouge Frontière, Jaune Frontière et Violette Frontière. L'ensemble des transitions Verte Frontière, noté* $\Delta_{Verte_{fr}}$*, est défini par :*

$$\Delta_{Verte_{fr}} = \{(q, \sigma, p) \mid q \in Q_{fr} \wedge \sigma \in \Sigma_c \wedge p \notin Q_d \wedge p \notin Q_{re} \wedge p \notin Q_{fr}\}$$

Méthode de détermination

L'algorithme 3 présente la méthode de caractérisation des transitions contrôlables sortant d'un état frontière suivant leur état de destination. Plusieurs étapes sont nécessaires pour caractériser ces transitions suivant les quatre ensembles $\Delta_{Rouge_{fr}}$, $\Delta_{Jaune_{fr}}$, $\Delta_{Violette_{fr}}$ et $\Delta_{Verte_{fr}}$. Les transitions contrôlables menant aux états redoutés sont tout d'abord identifiées et regroupées dans l'ensemble des transitions $\Delta_{Rouge_{fr}}$. Ces transitions sont les transitions à ne pas franchir pour ne pas atteindre l'ensemble des états redoutés, les états d'origine de ces transitions sont alors nommés les états frontières.

Algorithme 3 Caractérisation des transitions

Entrées : Q, Q_d, Q_{danger}, Q_{re}, G, Σ_c

Calculer $\Delta_{Rouge_{fr}}$ et Q_{fr} en utilisant les définitions 18 et 17

Déterminer $\Delta_{fr} = \{(q, \sigma, p) \mid q \in Q_{fr} \wedge \sigma \in \Sigma_c\}$: ensemble des transitions contrôlables sortantes des états frontières

Pour tout $t = (q, \sigma, p) \in \Delta_{fr} \backslash \Delta_{Rouge_{fr}}$:
  Si $p \in Q_{fr}$ **alors :**
    Ajouter t dans $\Delta_{Jaune_{fr}}$
  Sinon :
    Si $p \in Q_d$ **alors :**
      Ajouter t dans $\Delta_{Violette_{fr}}$
    Sinon :
      Ajouter t dans $\Delta_{Verte_{fr}}$

Sorties : Q_{fr}, $\Delta_{Rouge_{fr}}$, $\Delta_{Jaune_{fr}}$, $\Delta_{Violette_{fr}}$, $\Delta_{Verte_{fr}}$

IV.4.3 Caractérisation des trajectoires amont

Après avoir caractérisé les transitions sortantes des états frontières, une étude des trajectoires menant aux états frontières est réalisée. Cette étude permet d'anticiper l'approche des états frontières pour informer au préalable l'opérateur de supervision. L'étude se limite à une partie des trajectoires menant aux états frontières, les trajectoires amont.

États et transitions amont

Les trajectoires amont mènent à un sous-ensemble des états frontières, les états dont les transitions sortantes appartiennent uniquement aux ensembles $\Delta_{Jaune_{fr}}$ et $\Delta_{Rouge_{fr}}$. Ces états frontières sont nommés états frontières amont $Q_{fr_{amont}}$. Il est important d'identifier ce sous-ensemble des états frontières puisque la distance aux états redoutés reste la même après avoir franchi une transition. Les transitions composant les trajectoires menant à ces états sont donc déterminées pour identifier des solutions pour les contourner et alerter au plus tôt l'opérateur de supervision. Une indication pourra ainsi lui être transmise pour anticiper l'approche d'un état redouté et si possible l'éviter. Pour cela, un sous-ensemble des états accessibles par lesquels passent les trajectoires amont est défini : l'ensemble des états amont.

Les transitions sortantes des états amont sont caractérisées selon leur état de destination (figure IV.8), comme pour les états frontières. Ainsi :

- une transition Bleue Amont $\Delta_{Bleue_{amont}}$ mène d'un état amont à un autre état amont ou un état frontière amont,
- une transition Jaune Amont $\Delta_{Jaune_{amont}}$ mène d'un état amont à un état frontière,
- une transition Violette Amont $\Delta_{Violette_{amont}}$ conduit d'un état amont à un état dangereux,
- une transition Verte Amont $\Delta_{Verte_{amont}}$ mène d'un état amont à un état non dangereux et n'appartenant pas à l'ensemble des états amont.

Les transitions $\Delta_{Bleue_{amont}}$ constituent donc les trajectoires amont puisqu'elles relient les états amont entre eux. Il n'existe pas de transitions Rouge Amont puisque par définition, les transitions Rouge mène à un état redouté à partir d'un état frontière.

Définitions formelles des états et transitions amont

Définition 22 (État frontière amont) *Un état frontière est un état frontière amont si ses transitions sortantes mènent soit à un état redouté Q_{re} soit à un autre état frontière Q_{fr}. Ainsi, ses transitions sortantes appartiennent donc uniquement aux ensembles de transitions $\Delta_{Jaune_{fr}}$ et $\Delta_{Rouge_{fr}}$. L'ensemble des états frontières amont, noté $Q_{fr_{amont}}$, est défini par :*

$$Q_{fr_{amont}} = \{q \in Q_{fr} \mid \forall \sigma \in \Sigma_c : \delta(q, \sigma) \in (Q_{re} \cup Q_{fr})\}$$

Définition 23 (État amont) *Un état est un état amont si au moins une de ses transitions sortantes mène soit à un état frontière amont $Q_{fr_{amont}}$ soit à un autre état amont. De plus, ses états successeurs doivent uniquement mener à des états amont, des états frontières amont ou des états frontières. Ainsi, l'ensemble des états amont, noté Q_{amont}, est défini par :*

$$\begin{aligned} Q_{amont} = \{q \in Q \mid \exists \sigma \in \Sigma_c : \delta(q, \sigma) \in Q_{amont} \cup Q_{fr_{amont}} \\ \wedge \ \forall e \in \Sigma_c : \delta(\delta(q, \sigma), e) \in Q_{amont} \cup Q_{fr_{amont}} \cup Q_{fr}\} \end{aligned}$$

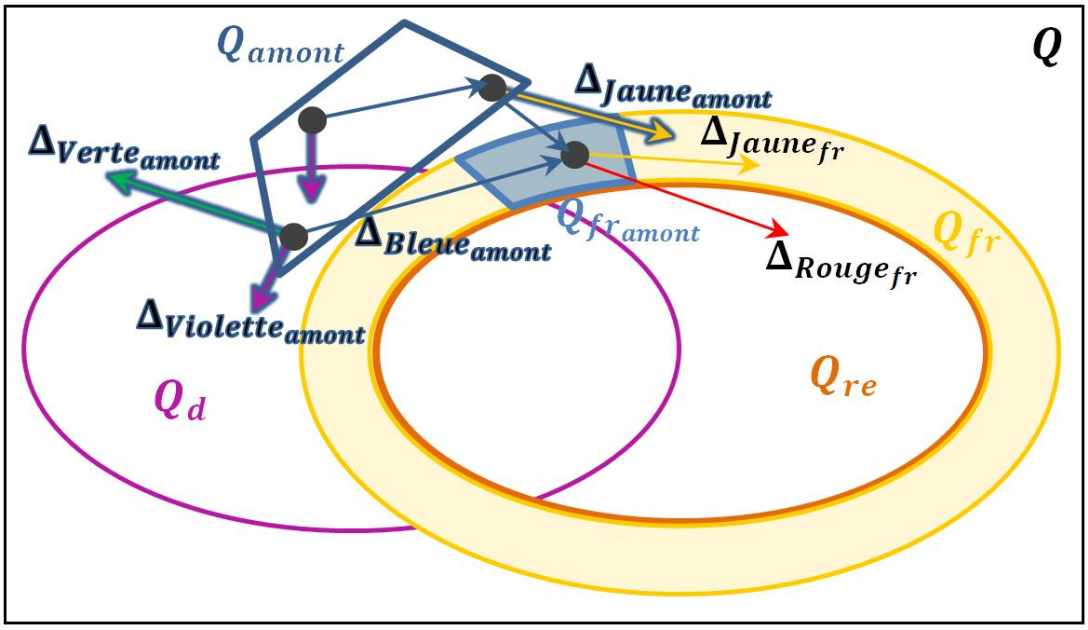


FIGURE IV.8 – Trajectoires amont

La définition des états amont est donc une définition inductive et l'ensemble des états amont est un plus petit point fixe.

Définition 24 (Transition Bleue Amont) *Une transition Bleue Amont est une transition menant, par un événement contrôlable, d'un état amont à un autre état amont ou un état frontière amont. L'ensemble des transitions Bleue Amont, noté $\Delta_{Bleue_{amont}}$, est défini par :*

$$\Delta_{Bleue_{amont}} = \{(q, \sigma, p) \mid q \in Q_{amont} \wedge \sigma \in \Sigma_c \wedge p \in Q_{amont} \cup Q_{fr_{amont}}\}$$

Définition 25 (Transition Jaune Amont) *Une transition Jaune Amont est une transition menant, par un événement contrôlable, d'un état amont à un état frontière. L'ensemble des transitions Jaune Amont, noté $\Delta_{Jaune_{amont}}$, est défini par :*

$$\Delta_{Jaune_{amont}} = \{(q, \sigma, p) \mid q \in Q_{amont} \wedge \sigma \in \Sigma_c \wedge p \in Q_{fr}\}$$

Définition 26 (Transition Violette Amont) *Une transition Violette Amont est une transition menant, par un événement contrôlable, d'un état amont à un état dangereux qui n'est ni un état frontière ni un état amont. L'ensemble des transitions Violettes Amont, noté $\Delta_{Violette_{amont}}$, est défini par :*

$$\Delta_{Violette_{amont}} = \{(q, \sigma, p) \mid q \in Q_{amont} \wedge \sigma \in \Sigma_c \wedge p \in Q_d \backslash (Q_{fr} \cup Q_{amont})\}$$

Définition 27 (Transition Verte Amont) *Une transition Verte Amont est une transition partant, par un événement contrôlable, d'un état amont à un état n'appartenant pas aux ensembles des états amont, des états dangereux et des états frontières. L'ensemble des transitions Verte Amont, noté $\Delta_{Verte_{amont}}$, est défini par :*

$$\Delta_{Verte_{amont}} = \{(q, \sigma, p) \mid q \in Q_{amont} \wedge \sigma \in \Sigma_c \wedge p \notin Q_{amont} \wedge p \notin Q_d \wedge p \notin Q_{fr}\}$$

Méthode de détermination

L'algorithme 4 détermine l'ensembles des transitions et des états amonts susceptibles de mener à des états redoutés.

Algorithme 4 Caractérisation des trajectoires amont

Entrées : Q_{fr}, Q_d, Q_{re}, G, Σ_c

Déterminer $Q_{fr_{amont}}$ en utilisant la définition 22
Soit $Q_{test} = Q_{fr_{amont}}$: états à tester
Tant que $Q_{test} \neq \emptyset$:
  Calculer $\Delta_{amont} = \{(q, \sigma, p) \mid q \notin Q_{fr}, \sigma \in \Sigma_c, p \in Q_{test}\}$
  $Q_{test} = \{\}$
  Soit $test = 0$
  Pour tout $(q, \sigma, p) \in \Delta_{amont}$:
    Ajouter (q, σ, p) dans $\Delta_{Bleue_{amont}}$
    Pour tout $e \in \Sigma_c$ avec $e \neq \sigma$:
      Si $\delta(q, e) \in Q_{fr} \backslash Q_{fr_{amont}}$ **alors :**
        Ajouter $(q, e, \delta(q, e))$ dans $\Delta_{Jaune_{amont}}$
      Si $\delta(q, e) \in Q_d \backslash Q_{fr}$ **alors :**
        Ajouter $(q, e, \delta(q, e))$ dans $\Delta_{Violette_{amont}}$
        $test = 1$
      Sinon :
        Ajouter $(q, e, \delta(q, e))$ dans $\Delta_{Verte_{amont}}$
        $test = 1$
    Si $test = 0$ alors :
      Ajouter q dans Q_{test}

Sorties : $\Delta_{Bleue_{amont}}$, $\Delta_{Jaune_{amont}}$, $\Delta_{Violette_{amont}}$, $\Delta_{Verte_{amont}}$

IV.4.4 Caractérisation des trajectoires aval

Après avoir caractérisé les trajectoires amont, une étude des trajectoires sortant des états frontières est réalisée. Cette étude permet de conseiller l'opérateur de supervision jusqu'à parvenir à un état où la sécurité des voyageurs est garantie. Cette partie étudie donc les trajectoires sortant des états frontières jusqu'à atteindre un état non dangereux, les trajectoires aval.

États et transitions aval

Dans l'ensemble des états frontières, les états n'ayant pas de transitions sortantes appartenant à $\Delta_{Verte_{fr}}$ mais au moins une transition appartenant à $\Delta_{Violette_{fr}}$ sont étudiés. Ces états frontières appartiennent aux états frontières aval $Q_{fr_{aval}}$. Les trajectoires partant d'un état frontière aval jusqu'à atteindre un état n'appartenant ni aux états frontières Q_{fr} ni aux états dangereux Q_d sont donc identifiées, les trajectoires aval. Un sous-ensemble des états accessibles par lesquels passent les trajectoires aval est défini : l'ensemble des états aval.

Les états frontières aval correspondent à des états à partir desquels la distance à un état redouté va diminuer puisqu'il existe une transition sortante appartenant à l'ensemble des transitions Violettes $\Delta_{Violette_{fr}}$. Cependant, l'état de destination appartiendra à l'ensemble des états dangereux Q_d puisqu'il n'existe pas de transition sortante appartenant à l'ensemble $\Delta_{Verte_{fr}}$. Avec les trajectoires aval, l'opérateur de supervision pourra ainsi être guidé jusqu'à un état acceptable par rapport au danger encouru par les voyageurs et le personnel.

Les transitions sortantes des états aval sont caractérisées selon leur état de destination (figure IV.9) et constituent les trajectoires aval. Ainsi :

- une transition Jaune Aval $\Delta_{Jaune_{aval}}$ mène d'un état aval à un état frontière,
- une transition Violette Aval $\Delta_{Violette_{aval}}$ conduit d'un état aval à un état dangereux,
- une transition Verte Aval $\Delta_{Verte_{aval}}$ mène d'un état aval à un état n'appartenant pas à l'ensemble des états aval, des états dangereux ni des états frontières.

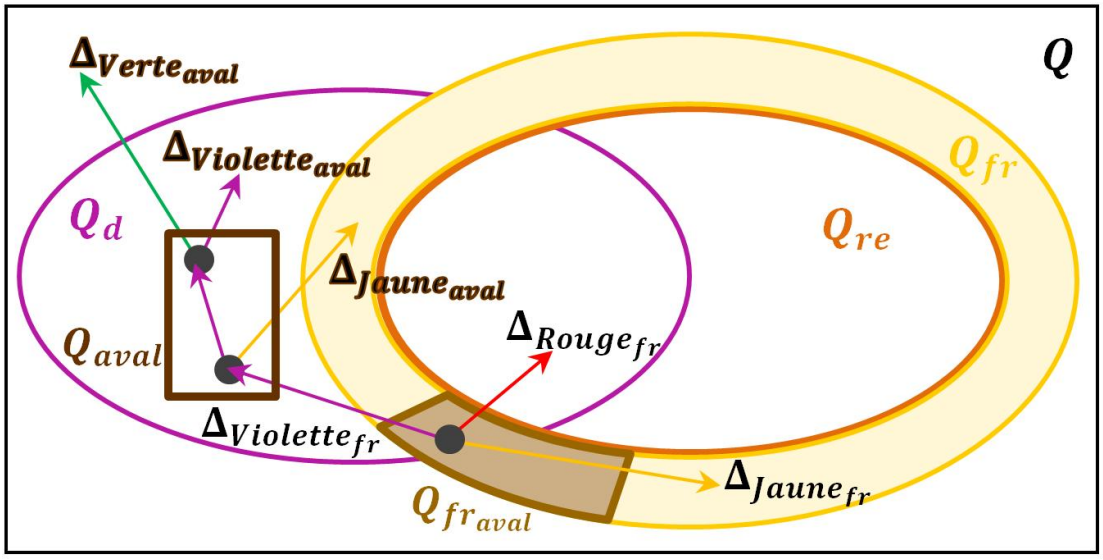


FIGURE IV.9 – Trajectoires aval

Ainsi, la recherche des états aval se poursuit jusqu'à trouver un état ayant une transition sortante appartenant à $\Delta_{Verte_{aval}}$. Les transitions $\Delta_{Violette_{aval}}$ constituent donc les trajectoires aval puisqu'elles relient les états aval entre eux. Comme pour les transitions amont, il n'existe pas de transitions Rouge Aval.

Définitions formelles des états et transitions aval

Définition 28 (État frontière aval) *Un état frontière est un état frontière aval si au moins une de ces transitions sortantes appartient à l'ensemble des transitions Violette frontière et si aucune de ces transitions sortantes appartient à l'ensemble des transitions Verte frontière. L'ensemble des états aval, noté $Q_{fr_{aval}}$, est défini par :*

$$Q_{fr_{aval}} = \{q \in Q_{fr} \mid \exists \sigma \in \Sigma_c : (q, \sigma, p) \in \Delta_{Violette_{fr}} \wedge \nexists e \in \Sigma_c : (q, e, p) \in \Delta_{Verte_{fr}}\}$$

Définition 29 (État aval) *Un état est un état aval si il appartient à l'ensemble des états dangereux mais n'appartient pas à l'ensemble des états frontières et des états redoutés, si au*

moins un de ces états prédécesseurs p appartient à l'ensemble des états frontières aval $Q_{fr_{aval}}$ ou à l'ensemble des états aval. De plus, les états successeurs de l'état p doivent uniquement appartenir à l'ensemble des états dangereux Q_d, l'ensemble des états frontières Q_{fr} ou à l'ensemble des états aval. L'ensemble des états aval, noté Q_{aval}, est défini par :

$$Q_{aval} = \{q \in (Q_d \backslash (Q_{fr} \cup Q_{re})) \mid (\exists \sigma \in \Sigma_c \wedge \exists p \in Q_{fr_{aval}} \cup Q_{aval} : \delta(p, \sigma) = q)$$

$$\wedge (\forall e \in \Sigma_c : \delta(p, e) \in Q_d \cup Q_{fr} \cup Q_{aval})\}$$

La définition des états aval est donc une définition inductive et l'ensemble des états aval est un plus petit point fixe.

Définition 30 (Transition Jaune Aval) *Une transition Jaune Aval est une transition menant, par un événement contrôlable, d'un état aval à un état frontière. L'ensemble des transitions Jaune Aval, noté $\Delta_{Jaune_{aval}}$, est défini par :*

$$\Delta_{Jaune_{aval}} = \{(q, \sigma, p) \mid q \in Q_{aval} \wedge \sigma \in \Sigma_c \wedge p \in Q_{fr}\}$$

Définition 31 (Transition Violette Aval) *Une transition Violette Aval est une transition menant, par un événement contrôlable, d'un état aval à un état dangereux qui n'est pas un état frontière. L'ensemble des transitions Violettes Aval, noté $\Delta_{Violette_{aval}}$, est défini par :*

$$\Delta_{Violette_{aval}} = \{(q, \sigma, p) \mid q \in Q_{aval} \wedge \sigma \in \Sigma_c \wedge p \in Q_d \wedge p \notin Q_{fr}\}$$

Définition 32 (Transition Verte Aval) *Une transition Verte Aval est une transition partant, par un événement contrôlable, d'un état aval et menant à un état n'appartenant pas aux ensembles des états avals, des états dangereux et des états frontières. L'ensemble des transitions Verte Aval, noté $\Delta_{Verte_{aval}}$, est défini par :*

$$\Delta_{Verte_{aval}} = \{(q, \sigma, p) \mid q \in Q_{aval} \wedge \sigma \in \Sigma_c \wedge p \notin Q_{aval} \cup Q_d \cup Q_{fr}\}$$

Méthode de détermination

L'algorithme 5 identifie les trajectoires partant d'un état frontière aval et menant à un état non dangereux.

IV.4.5 Génération des messages pour l'opérateur de supervision

Les différentes caractérisations réalisées ont permis d'associer un certain nombre de transitions à des ensembles de couleurs. Les transitions concernées sont les transitions sortantes des états frontières et les transitions composant les trajectoires amont et les trajectoires aval. Cinq ensembles liés à une couleur ont ainsi été définis : les transitions Rouge, Bleue, Jaune, Violette et Verte, attachés aux états frontières, amont et aval. L'objectif recherché est de transmettre à l'opérateur de supervision des messages dans certains cas précis pour l'orienter dans les actions

Algorithme 5 Caractérisation des trajectoires aval

Entrées : Q_{fr}, Q_d, Q_{re}, G, Σ_c, $\Delta_{Violette_{fr}}$, $\Delta_{Verte_{fr}}$

Déterminer $Q_{fr_{aval}}$ en utilisant la définition 28
Soit $Q_{test} = Q_{fr_{aval}}$: états à tester
Soit $Q_{aval} = \{\}$
Tant que $Q_{test} \neq \emptyset$:
  Calculer $Q_{aval_{test}} = (Q_d \backslash (Q_{fr} \cup Q_{re})) \cap \{\delta(q, \sigma) \mid q \in Q_{test} \wedge \sigma \in \Sigma_c\}$
  $Q_{test} = \{\}$
  Soit $test = 0$
  Si $Q_{aval_{test}} \backslash Q_{aval} \neq \emptyset$ **alors :**
    Pour tout $p \in Q_{aval_{test}} \backslash Q_{aval}$:
      Ajouter p dans Q_{aval}
      Pour tout $e \in \Sigma_c$:
        Si $\delta(p, e) \in Q_{fr}$ **alors :**
          Ajouter $(p, e, \delta(p, e))$ dans $\Delta_{Jaune_{aval}}$
        Sinon :
          Si $\delta(p, e) \in Q_d$ **alors :**
            Ajouter $(p, e, \delta(p, e))$ dans $\Delta_{Violette_{aval}}$
          Sinon :
            Ajouter $(p, e, \delta(p, e))$ dans $\Delta_{Verte_{aval}}$
            $test = 1$
      Si $test = 0$ alors :
        Ajouter p dans Q_{test}

Sorties : $\Delta_{Jaune_{aval}}$, $\Delta_{Violette_{aval}}$, $\Delta_{Verte_{aval}}$

qu'il exécute. Le message qui sera transmis correspond à l'intitulé de l'événement associé à la transition puisque celui-ci explicite l'action que l'opérateur effectue.

Ainsi, les transitions Rouge et Bleue sont associées à des messages d'alerte indiquant l'action que l'opérateur ne doit pas réaliser. En effet, les transitions Rouge conduisent à l'ensemble des états redoutés qu'il faut éviter pour garantir au mieux la sécurité des personnes. Les transitions Bleue constituent quant à elles les trajectoires amont. Ces trajectoires conduisent aux états frontières amont qu'il est préférable d'éviter.

Les messages de conseil transmis concernent les transitions associées aux couleurs Jaune, Violette et Verte. Cependant, il existe une hiérarchisation entre ces couleurs, cette hiérarchisation s'explique par l'état de destination des transitions. En effet, il est préférable d'aller dans un état non dangereux et non frontière des états redoutés par une transition Verte, ces états assurant mieux la sécurité des personnes. De plus, un état dangereux est à privilégier face à un état frontière. Ainsi, lors de la transmission des messages à un état donné, s'il existe plusieurs conseils possibles, l'ordre de choix est la transition Verte, la transition Violette puis la transition Jaune.

IV.4.6 Conclusion

En étudiant les transitions frontières, les trajectoires amont et les trajectoires aval, leur caractérisation par des ensembles de couleur Δ_{Rouge}, Δ_{Bleue}, Δ_{Jaune}, $\Delta_{Violette}$ et Δ_{Verte} identifie les alertes et conseils à transmettre aux opérateurs de supervision pour qu'aucun état redouté ne soit atteint. Pour chaque état accessible, si un message doit être transmis à l'opérateur de supervision, l'état appartient donc à Q_{mess} et au moins une de ses transitions sortantes est associée à l'un des ensembles de couleur. Ainsi, si une des transitions appartient à l'ensemble Δ_{Rouge} ou Δ_{Bleue}, le message est une alerte à ne pas franchir cette transition. Avec cet alerte, un conseil peut également être donné par les transitions appartenant aux ensembles Δ_{Jaune}, $\Delta_{Violette}$ ou Δ_{Verte} selon leur hiérarchisation.

Ces caractérisations sont définies dans le but d'apporter à l'opérateur de supervision une aide sous forme de messages pour la gestion des incidents combinés pouvant se produire lors de l'exploitation d'une ligne de métro. Les messages délivrés à l'opérateur de supervision le conseillent pour répondre à l'objectif de l'étude : proposer des solutions pour éviter des états où la sécurité des voyageurs et du personnel ne serait pas garantie et où l'opérateur aurait aucune maitrise de la situation.

IV.5 Développement d'un démonstrateur

IV.5.1 Cadre du projet innovant

Chaque année, au sein de Thales Communications & Security, un appel à projet est lancé dans le but de faire émerger des idées innovantes et de financer leur mise en œuvre au travers de démonstrateurs. Ainsi, une dizaine de projets portant sur de nouvelles études, concepts, systèmes est développée tous les ans par des ingénieurs Thales. Les objectifs de ces projets sont de renforcer les différenciateurs techniques, de démontrer la faisabilité de nouvelles idées et d'évaluer les résultats obtenus en termes d'industrialisation. Les critères principaux de sélection d'un projet sont son caractère innovant et les opportunités d'utilisation et de vente du projet auprès des clients Thales.

Pour l'année 2014, 152 projets avaient été préselectionnés et suite à deux présentations successives devant un comité de sélection, 11 projets ont été choisis. Parmi ces projets, pour le département Systèmes Ferroviaire Intégrés (SFI), le projet « Decision Support System pour la gestion d'incidents sur une ligne de métro » a été retenu. Ce projet repose sur mes travaux de recherche effectués en collaboration avec Thales et vise à une intégration des résultats obtenus dans l'application ATS de Thales.

IV.5.2 Présentation du projet

L'origine de ce projet est basée sur deux constats réalisés au cours de mes recherches et de mon apprentissage du métier d'exploitant d'une ligne de métro. Tout d'abord, lors de l'occurrence d'un incident sur une ligne de métro, l'ATS développé par Thales ne propose pas d'aide suffisante à l'opérateur de supervision pour la mise en œuvre des procédures permettant la gestion de l'incident. De plus, si plusieurs incidents se produisent de manière simultanée, il est difficile pour l'opérateur de maitriser le niveau de danger dans lequel se trouvent les voyageurs et le personnel de la ligne.

Dans ce cadre, deux objectifs ont été proposés :

- Intégrer une représentation graphique BPMN des procédures de gestion d'incidents opérationnels dans l'interface de l'ATS. Ainsi, une aide et un support seraient apportés à l'opérateur de supervision dans la succession des activités à réaliser et il lui serait possible de visualiser en temps réel l'évolution des procédures en cours ;
- Proposer des alertes et des conseils aux opérateurs en cas d'évolution simultanée de plusieurs procédures (incidents combinés). En réalisant une analyse en temps réel du niveau de danger, l'opérateur pourrait éviter les états dans lesquels il ne dispose plus de moyen d'agir et est obligé d'attendre la fin des incidents. Il serait également orienté dans la succession des actions à réaliser pour assurer au mieux la sécurité des personnes.

L'ensemble des développements réalisés pour atteindre ces objectifs ne correspond pas exactement à la théorie présentée dans ce mémoire. Par exemple, des apports ont été fait pour donner une visualisation animée en temps réel des procédures BPMN et permettre à l'opérateur de suivre son évolution. De même, la transformation des procédures BPMN vers la modélisation du système en réseaux de Petri ne suit pas exactement celle proposée dans la partie III.3.4. En effet, afin d'identifier facilement les activités BPMN où les messages sont transmis, l'étape de simplification du réseau de Petri n'a pas été implémentée.

À l'heure actuelle, les *Decision support systems* actuels développés par les différents industriels dans leur application pour la supervision d'une ligne de métro se limitent le plus souvent à des présentations hypertextes de procédures Oui/Non. Plusieurs aspects sont donc novateurs pour la gestion de l'exploitation d'une ligne de métro par un ATS :

- La représentation avec le langage BPMN de procédures de gestion d'incidents ;
- La transmission à l'opérateur de supervision, en temps réel, d'une aide appropriée et tenant compte de l'état courant de l'exploitation de la ligne de métro ;
- La maitrise de l'évolution simultanée de procédures de gestion d'incidents avec une analyse en temps réel du danger encouru par les personnes ;
- L'intégration d'un outil de guidage de l'opérateur dans la gestion des incidents à la manière d'un « GPS » : avec des conseils sur le meilleur « itinéraire » à suivre dans le déroulé des procédures et des alertes pour éviter de prendre des « sens interdits ». Cependant, l'opérateur reste le seul décisionnaire des actions à réaliser.

La valeur ajoutée d'un tel projet pour Thales et leur application ATS est identifiable. En effet, il permet de proposer une fonctionnalité *Decision Support System* dans l'application pour l'exploitation de la ligne mais également dans le système de formation pour l'apprentissage des procédures de gestion d'incidents par les opérateurs. L'utilisation du langage BPMN pour la représentation des procédures de gestion d'incidents et leur animation dans l'interface de l'ATS apporte un différenciateur par rapport aux concurrents.

Une des perspectives du projet pour l'ATS serait d'étendre le mécanisme développé à des procédures non liées à la gestion d'un incident mais dédiées à l'amélioration et l'aide à l'exploitation de la ligne. Par exemple, à la suite d'une interruption de traffic, l'opérateur de supervision facilite la reprise de l'exploitation normale de la ligne en supprimant notamment des départs

de trains à partir d'un terminus pour récupérer le retard accumulé. De même, lors de la mise en place d'un service provisoire permettant aux trains de changer de voies de circulation au milieu de la ligne, plusieurs actions doivent être réalisées par l'opérateur de supervision. Ainsi, en représentant graphiquement ces ensembles d'actions sous forme de procédures BPMN et en les intégrant dans l'application ATS, il serait possible d'apporter une assistance supplémentaire aux opérateurs de supervision pour améliorer l'exploitation des lignes de métro.

IV.5.3 Démarche d'implémentation choisie

Deux modules sont nécessaires au développement de la fonctionnalité *Decision support systems* dans l'application ATS. Le premier module, hors ligne, détermine les alertes et conseils à transmettre à l'opérateur suivant l'état courant de la ligne et les incidents en cours. Le second module, en ligne et temps réel, permet à l'opérateur de suivre l'exécution d'une procédure et informe par messages des actions à réaliser ou non en se basant sur les résultats déterminés par le premier module.

Les données d'entrées du premier module sont :
- Les procédures de gestion d'incident stockées sous forme de fichiers .bpmn (avec l'outil jBPM) ;
- Les ressources utilisées par ces procédures sous forme de fichiers .xml ;
- Les liens entre les ressources et les procédure et l'état sécuritaire associé pour l'étude du danger.

Ainsi, ce module charge l'ensemble des procédures écrites avec le langage BPMN existantes, les transforme en réseaux de Petri en utilisant les règles définis dans cette thèse et construit les modèles des ressources nécessaires. Il calcule ensuite le graphe d'accessibilité correspondant et détermine, par application des algorithmes définis, la liste des états à partir desquels il faut transmettre un message à l'opérateur et la description du système correspondant (état des ressources).

Le second module est exécuté en temps réel. Il prend en données d'entrée :

- Les procédures métiers au format .bpmn ;
- Les listes des états avec les indications et la description du système correspondant, obtenus à partir du premier module.

L'objectif recherché est de permettre à l'opérateur de suivre l'exécution des procédures métiers et de l'informer sur les états dangereux. Ainsi, lors de l'occurrence de plusieurs incidents, si le système se trouve dans un état avec message, une indication est donnée à l'opérateur. Ce module fonctionnant en temps réel, l'état de l'ensemble des ressources est connu au travers des acquisitions terrains présentes dans l'ATS.

IV.5.4 Conclusion

La sélection de mon étude dans le cadre des projets innovants au sein de l'entreprise Thales révèle l'intérêt de l'industriel pour les recherches effectuées et les résultats obtenus. Elle signifie également le souhait de les mettre en application afin de valider une éventuelle industrialisation de la fonctionnalité. De plus, le développement de ce projet montre la faisabilité de l'intégration d'une aide à la décision dans l'application ATS de Thales et l'applicabilité des résultats obtenus.

La fonctionnalité *Decision support systems* est implémentée dans le démonstrateur de l'application représentant une ligne réelle et toutes les fonctionnalités disponibles. Elle se base sur l'exemple présenté dans le chapitre suivant du mémoire et conserve le périmètre défini ainsi que les hypothèses prises au cours de la recherche. Un bilan intermédiaire de ce projet est proposé à la fin de l'application de la démarche sur l'exemple.

IV.6 Conclusion sur l'analyse et la maitrise du danger

Dans ce chapitre, l'objectif était d'analyser et de maitriser le danger encouru par les voyageurs et le personnel d'une ligne de métro. Pour caractériser l'ensemble des états accessibles, la notion de contrôlabilité des événements est utilisée. Ainsi, une définition des états interdits est proposée pour répondre à l'objectif de l'étude. Cette définition s'inscrit dans l'application de la théorie du contrôle par supervision mais se distingue par la caractérisation de ces états interdits. En effet, en plus de la contrainte d'inclusion dans un ensemble d'états, un état interdit se définit également par la contrôlabilité de ses transitions sortantes. Cette originalité a conduit au développement d'algorithmes spécifiques pour les identifier puisque leur calcul se doit d'être itératif.

En déterminant un contrôleur permettant d'éviter les états interdits, l'existence d'une solution est montrée. Dans l'objectif de développer une aide à la décision pour l'opérateur de supervision, les états où un message doit être transmis sont identifiés. Ces messages sont des alertes et des conseils afin d'assurer au mieux la sécurité des personnes en cas d'évolution simultanée de plusieurs procédures. En effet, bien que les actions pour la gestion des incidents ne soient pas automatisés, il est possible d'orienter les opérateurs de supervision lors de l'exécution des procédures et de les aider à assurer la sécurité des personnes. L'intégration, par un développeur de Thales, d'une nouvelle fonctionnalité d'aide à la décision dans l'application ATS de Thales souligne l'intérêt porté à mes recherches par l'industriel.

V Application sur l'exemple

Résumé

La démarche présentée dans les chapitres 3 et 4 est appliquée sur un scénario réaliste et concret de l'occurrence de deux incidents. Les incidents choisis sont le *Dégagement de fumée* dans un tunnel et la *Présence d'une personne sur les voies* de circulation. Les procédures exécutées à la RATP pour gérer ces incidents sont donc modélisées et analysées en suivant les étapes exposées précédemment : BPMN, réseaux de Petri puis graphe d'accessibilité. Après avoir identifié les séquences sûres, des scénarios d'incidents sont détaillés afin de mettre en évidence les moments où l'opérateur de supervision serait conseillé dans la démarche à suivre par des messages. Un bilan de l'application de la démarche à l'exemple ainsi que de son implémentation dans le cadre du projet de Thales est ensuite effectué.

Sommaire

V.1 Présentation de l'exemple

V.1.1 Contexte des incidents à la RATP

D'après les postulats de l'étude, la démarche présentée s'applique lorsqu'au moins deux incidents se produisent de manière simultanée pendant l'exploitation d'une ligne de métro. Ainsi, pour l'exemple traité, seulement deux incidents sont considérés pour se placer dans le contexte le plus simple mais représentatif de l'étude. Ces deux incidents sont un *Dégagement de fumée* et la *Présence d'une personne sur les voies* de circulation du métro.

Dégagement de fumée

Un *Dégagement de fumée* peut survenir dans différentes situations et se déclencher dans différents lieux : sur les voies de circulation, dans un train ou sur un quai. Ainsi, la fumée peut par exemple provenir d'une poubelle installée sur un quai suite au jet d'un objet incandescent. Le dégagement de fumée peut également être occasionné par un problème électrique, un échauffement lors du freinage d'un train voire un incendie déclenché de manière volontaire. Dans un train, les origines et les causes d'un dégagement de fumée sont aussi multiples. De plus, l'ampleur et l'intensité du dégagement de fumée varient suivant les circonstances et l'environnement. En effet, si la fumée se trouve dans une zone de la ligne de métro aérienne, elle pourra se dissiper dans l'air facilement. Inversement, si le dégagement de fumée a lieu dans un tunnel, l'espace confiné va amplifier la progression de la fumée et compliquer sa prise en charge.

Un dégagement de fumée sera considéré comme maitrisable si sa cause est identifiée et si son extinction rapide et efficace est envisageable par un agent de la RATP, sans l'intervention des pompiers. Il sera considéré comme non maitrisable si son expansion est rapide ou si sa cause ou son origine n'est pas déterminée.

Pour les personnes présentes, la fumée peut provoquer un fort stress, une intoxication voire une asphyxie. Les conséquences sur l'exploitation de la ligne varient selon l'ampleur du dégagement de fumée. Ainsi, une fumée épaisse peut obstruer le tunnel, diminuer fortement la visibilité des conducteurs et donc empêcher la circulation des trains en plus d'être un danger pour la santé des voyageurs et du personnel.

Présence d'une personne sur les voies

L'incident *Présence d'une personne sur les voies* se produit lorsqu'une personne non autorisée descend volontairement ou non sur les voies de circulation. Cette personne est le plus souvent extérieure à l'exploitation et n'est donc pas formée aux risques encourus. Si celle-ci descend au niveau d'un quai en station et reste aux abords du quai, dans ce cas, son interception et son contrôle sont assez faciles puisque la personne reste dans une zone accessible. Cependant, si elle choisit de se déplacer sur les voies de circulation et dans les tunnels, sa position exacte est difficilement connue et cela engendre des problèmes plus importants.

Pour la personne descendue sur les voies de circulation, le principal danger est l'électrocution par les rails d'alimentation des trains. Le risque est important puisque les trains sont alimentés en énergie électrique par le sol (section I.1.1). Le deuxième danger est la collision avec un train en circulation, entrainant alors de graves blessures pouvant aller jusqu'à la mort. Les conséquences sur l'exploitation de la ligne sont en général relatives au temps passé par la personne sur les

voies. Ainsi, si la personne remonte rapidement sur le quai, de sa propre initiative et sans intervention extérieure, les conséquences peuvent juste être un court stationnement pour les trains. Cependant, s'il y a une collision avec un train ou une électrocution provoquant un accident grave de voyageur, l'arrêt de l'exploitation peut durer pendant plusieurs heures dans la zone concernée.

Classification des incidents

En se basant sur la classification des incidents présentée dans la section III.1.2, la gravité et la cause des deux incidents vont être déterminées. La cause des deux incidents est différente. En effet, l'incident *Présence d'une personne sur les voies* appartient à la catégorie *Voyageurs* puisqu'il est directement lié au comportement inconscient d'un voyageur. Le *Dégagement de fumée* a une cause extérieure à l'exploitation de la ligne, il peut venir de diverses origines et est la plupart du temps la conséquence d'un incendie.

Concernant leur gravité, les deux incidents sont des incidents majeurs puisqu'il y a une intervention de l'opérateur de supervision. De plus, sa réaction doit être rapide puisque la sécurité des voyageurs est en jeu dans les deux cas présentés. Ces incidents seront donc gérés par des procédures mémorisées par l'opérateur qui sont présentées dans la partie suivante. La démarche présentée est donc bien applicable à l'étude de ces deux incidents.

V.1.2 Procédures pour la gestion des incidents

Alerte Feu Fumée

La procédure *Alerte Feu Fumée* permet de gérer l'incident étudié *Dégagement de fumée*. Lorsqu'un conducteur observe un dégagement de fumée qu'il qualifie de non maitrisable et qui représente un danger potentiel pour la sécurité des voyageurs et du personnel, il alerte l'opérateur de supervision suivant la réglementation de la RATP et répète le message « Alerte feu fumée » à deux reprises. Après avoir localisé le dégagement de fumée sur la ligne, l'opérateur est chargé de l'évacuation des voyageurs qui sont dans les trains se situant dans la zone enfumée. Ainsi, il arrête les trains au quai de la prochaine station. L'opérateur va ensuite informer le permanent des réseaux ferrés (PRF) de la RATP alors responsable du système de ventilation pour le désenfumage du tunnel. Celui-ci va ainsi pouvoir lui notifier la zone de la ligne qu'il est possible d'exploiter pendant la gestion du dégagement de fumée.

La procédure *Alerte Feu Fumée* décrit donc la succession des tâches à exécuter. Afin de faciliter l'étude réalisée, un contexte d'incident est choisi : le dégagement de fumée est localisé dans un tunnel, à proximité d'un train en circulation. Une partie de la procédure concerne l'évacuation des voyageurs des trains impliqués. L'ensemble de ces actions correspond à une sous-procédure et ne sera pas considéré dans l'étude de l'exemple afin de limiter le nombre d'actions et la complexité de la procédure. De plus, une fois que le dégagement de fumée est maitrisé et terminé, le tunnel et la partie de la ligne concernés ne seront pas endommagés et la circulation des trains pourra reprendre de manière normale.

Signalement d'une personne sur les voies

La procédure *Signalement d'une personne sur les voies*, plus communément appelée *ISF 36* à la RATP, est exécutée lors de l'incident *Présence d'une personne sur les voies*. Pour simplifier

cette procédure et favoriser la compréhension de l'exemple développé, l'incident sera étudié dans un contexte particulier et prédéfini. Ainsi, le signalement de l'incident est réalisé et confirmé par un des conducteurs de la ligne.

Lorsqu'un conducteur aperçoit une personne sur les voies alors que celle-ci n'est pas autorisée, il demande à l'opérateur de supervision une mise hors tension de l'ensemble de la ligne en répétant par deux fois le message d'alerte « Couper le courant ». Dans ces conditions, l'objectif est de protéger la personne de tout risque d'électrocution et de collision avec un train. Une fois que la zone est sécurisée électriquement et qu'il n'y a plus de danger pour la personne sur les voies, le conducteur va tenter de faire remonter la personne à une station. Dans le contexte de l'exemple, la personne restera toujours visible par au moins un conducteur ou un agent de la RATP. Dans le cas contraire, la procédure à exécuter est plus complexe : elle impose un temps d'attente avant de déclarer la fin de l'incident et fait intervenir plus de personnes. Une fois que le conducteur confirme que la personne n'est plus sur les voies de circulation, l'opérateur pourra remettre sous tension l'ensemble de la ligne et ainsi reprendre une exploitation normale.

Afin de protéger au mieux la personne des dangers électriques, plusieurs actions dans la procédure se rapportent à la sécurisation électrique de la zone concernée. Ces parties de la gestion de l'alimentation électrique de la ligne ne seront pas étudiées dans l'exemple afin de limiter les ressources impliquées.

V.1.3 Conclusion

Les procédures de gestion d'un *Dégagement de fumé* et de la *Présence d'une personne sur les voies* ont ainsi été choisies pour illustrer l'étude réalisée. En effet, lorsqu'un dégagement de fumé est détecté sur une ligne, l'opérateur de supervision doit essayer de tout faire pour que les trains puissent arriver en station et ainsi évacuer les voyageurs à quai pour garantir leur sécurité. Cependant, lorsqu'une personne est descendue sur les voies dans la même zone de la ligne, le conducteur va de manière instinctive et pour garantir la sécurité de la personne, demander une coupure de courant généralisée. Dans cette configuration d'incidents, il est donc possible d'avoir des trains avec des voyageurs bloqués dans un tunnel enfumé et ne pouvant plus se déplacer.

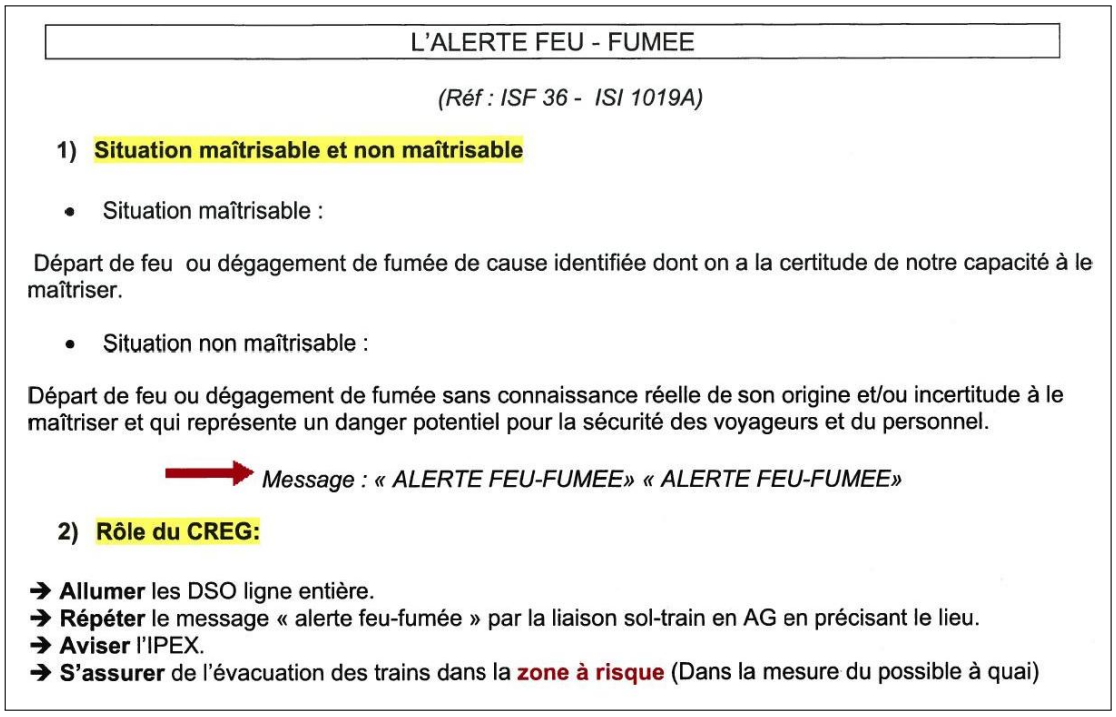
V.2 Du système réel à la modélisation

V.2.1 Description textuelle des procédures

La première présentation des procédures, pour leur apprentissage, est donnée par le document de formation des chefs de régulation (CREG) de la RATP. La description textuelle des procédures est réalisée en utilisant des structures hétérogènes (section III.2.3). Ainsi, la procédure *Alerte Feu Fumée* (figure V.1 [1]) présente deux points à prendre en compte dans une liste numérotée. Le premier item différencie une situation maitrisable d'une situation non maitrisable. Le second présente le rôle du chef de régulation lors de l'exécution de la procédure. Ce rôle est décrit sous forme d'une liste chronologique d'actions à réaliser, chaque action étant identifiée par une flèche.

Trois extraits d'article d'Instruction de Sécurité Ferroviaire illustrent également certains aspects de la réglementation. Ainsi, un extrait (figure V.2) précise les informations que l'agent

1. L'IPEX est l'ancienne dénomination du Permanent des Réseaux Ferrés (PRF) à la RATP



L'ALERTE FEU - FUMEE

(Réf : ISF 36 - ISI 1019A)

1) Situation maîtrisable et non maîtrisable

- Situation maîtrisable :

Départ de feu ou dégagement de fumée de cause identifiée dont on a la certitude de notre capacité à le maîtriser.

- Situation non maîtrisable :

Départ de feu ou dégagement de fumée sans connaissance réelle de son origine et/ou incertitude à le maîtriser et qui représente un danger potentiel pour la sécurité des voyageurs et du personnel.

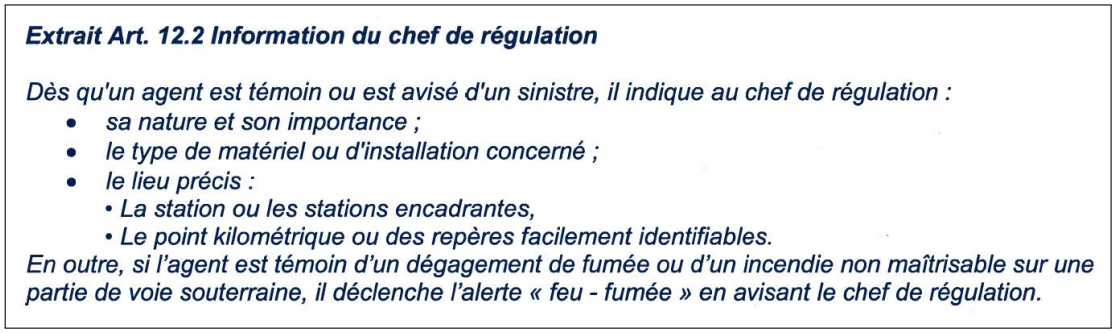
→ *Message : « ALERTE FEU-FUMEE» « ALERTE FEU-FUMEE»*

2) Rôle du CREG:

➔ **Allumer** les DSO ligne entière.
➔ **Répéter** le message « alerte feu-fumée » par la liaison sol-train en AG en précisant le lieu.
➔ **Aviser** l'IPEX.
➔ **S'assurer** de l'évacuation des trains dans la **zone à risque** (Dans la mesure du possible à quai)

FIGURE V.1 – Extrait de la procédure *Alerte Feu Fumée*

de la RATP témoin du dégagement de fumée doit transmettre au chef de régulation. Ce dernier est ainsi informé de points importants qu'il doit connaitre lors de l'exécution de la procédure.



Extrait Art. 12.2 Information du chef de régulation

Dès qu'un agent est témoin ou est avisé d'un sinistre, il indique au chef de régulation :

- *sa nature et son importance ;*
- *le type de matériel ou d'installation concerné ;*
- *le lieu précis :*
  - *La station ou les stations encadrantes,*
  - *Le point kilométrique ou des repères facilement identifiables.*

En outre, si l'agent est témoin d'un dégagement de fumée ou d'un incendie non maîtrisable sur une partie de voie souterraine, il déclenche l'alerte « feu - fumée » en avisant le chef de régulation.

FIGURE V.2 – Extrait d'article d'Instruction de Sécurité Ferroviaire

Pour la gestion de l'incident *Présence d'une personne sur les voies*, la procédure *Signalement d'une personne sur les voies* est décrite sous forme d'une liste numérotée qui fait la distinction entre les deux cas possibles : le signalement est effectué par un voyageur et le signalement est effectué par un agent. Des items fléchés décrivent ensuite dans l'ordre chronologique les actions à réaliser par le chef de régulation.

V.2.2 Représentation graphique des procédures

Les deux procédures étudiées dans l'exemple sont représentées graphiquement en utilisant le langage BPMN et en se focalisant sur les actions réalisées par le chef de régulation. Ainsi, dans les différentes pistes des modèles BPMN présentés, seule celle décrivant les actions du chef de régulation sera renseignée. Cette représentation se base sur le document de formation des chefs de régulation de la RATP ainsi que sur les connaissances acquises lors de la formation,

des échanges et des observations réalisés. Les modèles BPMN complets, sans les simplifications effectuées, sont donnés en annexe C.

Alerte Feu Fumée - figure V.3

L'analyse de la procédure textuelle *Alerte Feu Fumée* a permis d'identifier trois intervenants : le chef de régulation, l'ensemble des conducteurs de la ligne concernée et le permanent des réseaux ferrés. Trois pistes sont donc nécessaires dans le modèle BPMN pour mettre en évidence les échanges de messages entre ces intervenants. Avec les hypothèses de l'exemple, cette procédure est linéaire : les actions à réaliser s'enchainent les unes après les autres après avoir été exécutées. La procédure est déclenchée par le chef de régulation lorsqu'il prend en considération le message « Alerte Feu Fumée » de l'un des conducteurs de la ligne. Elle se termine lorsqu'il n'y a plus de dégagement de fumée et qu'une personne sur le terrain lui a confirmé que la reprise de l'exploitation était possible.

La représentation graphique de la procédure utilisant le langage BPMN (figure V.3) est constitué de trois événements : un initial et un intermédiaire de type conditionnel et un événement final. Elle est également composée de cinq activités correspondant en partie aux échanges à effectuer avec les autres intervenants. Les activités sont de type envoi ou réception de messages et action avec l'assistance d'un opérateur.

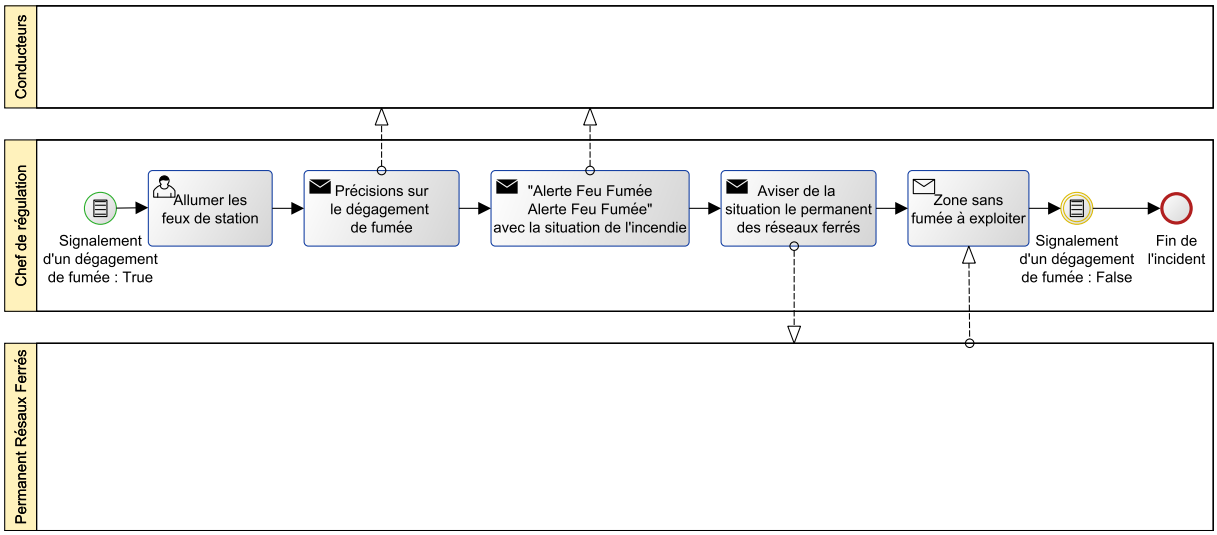


Figure V.3 – Alerte Feu Fumée - Modèle BPMN

Une fois que l'opérateur de supervision prend en considération le signalement d'un dégagement de fumée, il allume les feux de station pour empêcher les trains de sortir de station une fois qu'ils y sont arrêtés. Il demande ensuite au conducteur ayant annoncé l'incident des précisions sur le dégagement de fumée : son importance, sa localisation précise et sa cause si elle est connue. Il confirme ensuite à l'ensemble des conducteurs la présence d'un dégagement de fumée et l'exécution de la procédure correspondante. Il avise le permanent des réseaux ferrés pour que celui-ci déclenche les systèmes de ventilation et en fonction de ces installations, lui indique la zone où les trains peuvent continuer de circuler sur la ligne sans danger. Après avoir reçu l'indication que l'incident était terminé, la procédure est alors terminée.

Signalement d'une personne sur les voies - figure V.4

La procédure *Signalement d'une personne sur les voies* fait intervenir les conducteurs de la ligne et le permanent des réseaux ferrés en plus du chef de régulation. En appliquant les hypothèses de l'exemple, la procédure BPMN (figure V.4) est composée de trois événements et quatre activités. Après avoir reçu le signalement d'une personne sur les voies par un conducteur, l'opérateur de supervision met hors tension la ligne de métro pour éviter au mieux un accident. Il demande ensuite des précisions au conducteur sur la personne descendue sur les voies afin d'avoir une vision plus claire de la situation. Il sollicite ensuite le conducteur pour essayer de faire remonter la personne sur un quai, si cela est possible.

Suite à cette intervention, si la personne est remontée à un quai et n'est donc plus en danger, l'incident est terminé et la procédure s'arrête. Cependant, si la personne reste sur les voies de circulation, l'opérateur de supervision signale l'incident au permanent des réseaux ferrés pour qu'il demande une intervention extérieure des services de sécurité ou des forces de l'ordre. L'opérateur de supervision reprend alors contact avec le conducteur pour savoir si la personne a changé de position ou de comportement et exécute de nouveau les activités jusqu'à ce que la personne ne soit plus sur les voies de circulation et que l'exploitation puisse redevenir normale.

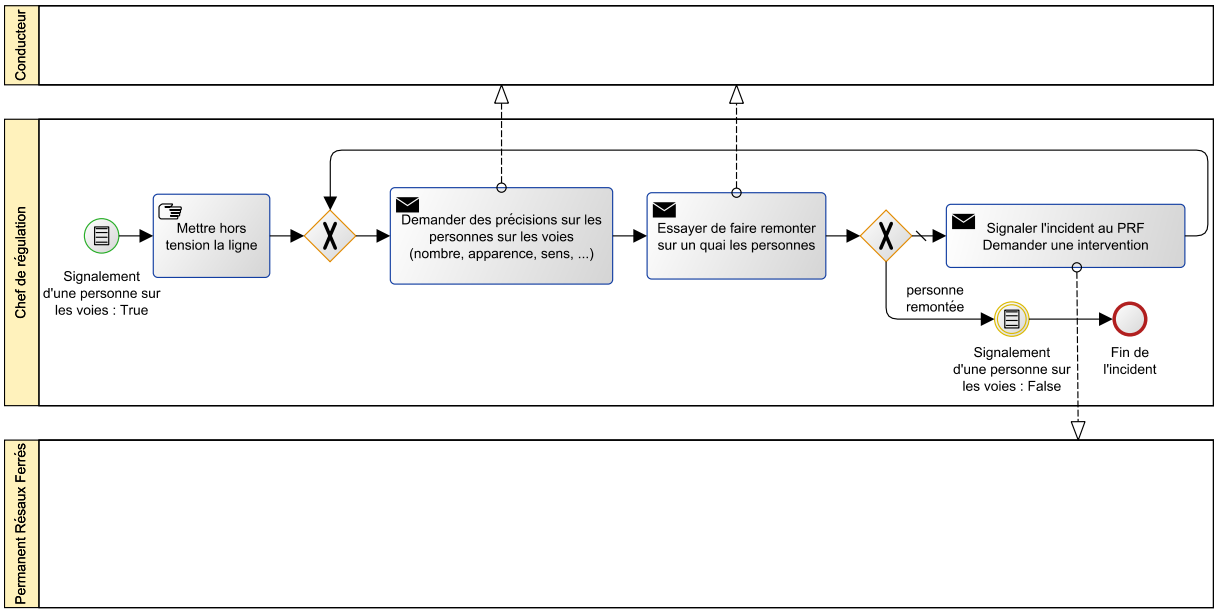


FIGURE V.4 – Signalement d'une personne sur les voies - Modèle BPMN

V.2.3 Modélisation du système

Afin d'étudier les procédures en termes de danger rencontré par les voyageurs et le personnel, il faut les replacer dans l'environnement dans lequel elles sont utilisées en identifiant les ressources impliquées et les signalements d'incident correspondant. Pour cela, les procédures modélisées en BPMN sont transformées en réseaux de Petri en suivant la méthode présentée dans la section II.3.3. Un modèle réseau de Petri sauf du système étudié est ensuite établi, sur lequel se baseront les analyses des situations dangereuses. Pour rappel, le système étudié est composé des procédures de gestion d'incidents, des signalements des incidents ainsi que du contexte de la ligne décrit par des ressources (définition 6).

Identification des ressources

Les ressources nécessaires à l'étude sont identifiées en analysant les procédures et en déterminant les éléments de la ligne intervenant lors de leur exécution. Ainsi, pour la procédure *Alerte Feu Fumée*, la première activité *Allumer les feux de station* modifie un élément de la ligne, les feux de signalisation en station. Ces feux, lorsqu'ils sont allumés, interdisent aux conducteurs de sortir de la station où ils sont arrêtés. Les deux états de la ressource *Feux de station* sont *Allumé* (*« FSallume »*) et *Éteint* (*« FSeteint »*). Le modèle réseau de Petri de cette ressource est constitué de deux places et deux transitions (*Allumer - « AllFS »*) et *Éteindre - « EteFS »*) (figure V.5), l'état *« FSeteint »* est marqué à l'état initial.

Concernant la procédure *Signalement d'une personne sur les voies*, l'activité *Mettre Hors Tension* modifie un des éléments de la ligne puisqu'elle va couper l'alimentation en énergie électrique des trains et les empêcher de circuler. Ainsi, la ressource *Alimentation* décrit les deux états possibles de la ligne : *Sous tension* (*« ST »*) et *Hors tension* (*« HT »*). Lorsque la ligne est *Hors tension*, les trains présents ne peuvent alors plus bouger puisqu'ils ont besoin d'énergie pour être en mouvement. Cette ressource est également modélisée par un réseau de Petri avec deux places et deux transitions (*Mise sous tension - « MiseST »* et *Mise hors tension - « MiseHT »*) (figure V.5) permettant de passer de l'état *Sous tension*, initialement marqué, à l'état *Hors tension* et inversement.

Les deux ressources *Feux de station* et *Alimentation* sont en lien direct avec un autre élément de la ligne, la position du train sur la ligne. En effet, pour ces ressources, il est important de faire la différence entre la situation d'un train en station ou hors station, c'est-à-dire dans les tunnels de circulation. La ressource *Position* indique donc si un train est en *Station* ou dans un *Tunnel*. Si la ressource *Feux de station* est à l'état *Allumé*, le train concerné n'est pas autorisé à sortir de la station, ce qui correspond au franchissement de la transition entre l'état *Station* et *Tunnel* de la ressource *Position*. La ressource *Alimentation* quant à elle contraint la position du train en interdisant tous les mouvements de train si l'alimentation électrique est *Hors tension*. Un train peut changer de position seulement si la ligne est *Sous tension*. Ainsi, les deux transitions de la ressource *Position*, *Entrer en station* (*« EntStation »*) et *Sortir de station* (*« SorStation »*), sont franchissables seulement si l'état *Sous tension* est marqué. À l'état initial, la place *Tunnel* de la ressource *Position* est marquée.

Afin de se focaliser sur l'étude des procédures de gestion d'incident en termes de sécurité pour les voyageurs et le personnel, le périmètre des ressources sera limité à l'étude d'un seul train. Ainsi, les deux incidents sont détectés par le même train et les deux procédures appliquées à ce même train, il est donc nécessaire de modéliser une seule instance de chacune des ressources. Cette hypothèse permet d'éviter d'étudier un système avec un nombre d'états important et de se concentrer sur l'objectif principal : l'analyse du danger.

Le modèle réseau de Petri des trois ressources et de leurs interactions à prendre en compte pour l'étude des deux procédures est donc présenté figure V.5.

Signalement des incidents

Les deux incidents étudiés ici sont le *Dégagement de fumée* et la *Présence d'une personne sur les voies de circulation*. Les modèles réseau de Petri de signalement de ces deux incidents sont constitués de deux places correspondant à la *Présence* (*« Fumee_P »* et *« PersV_P »*) et

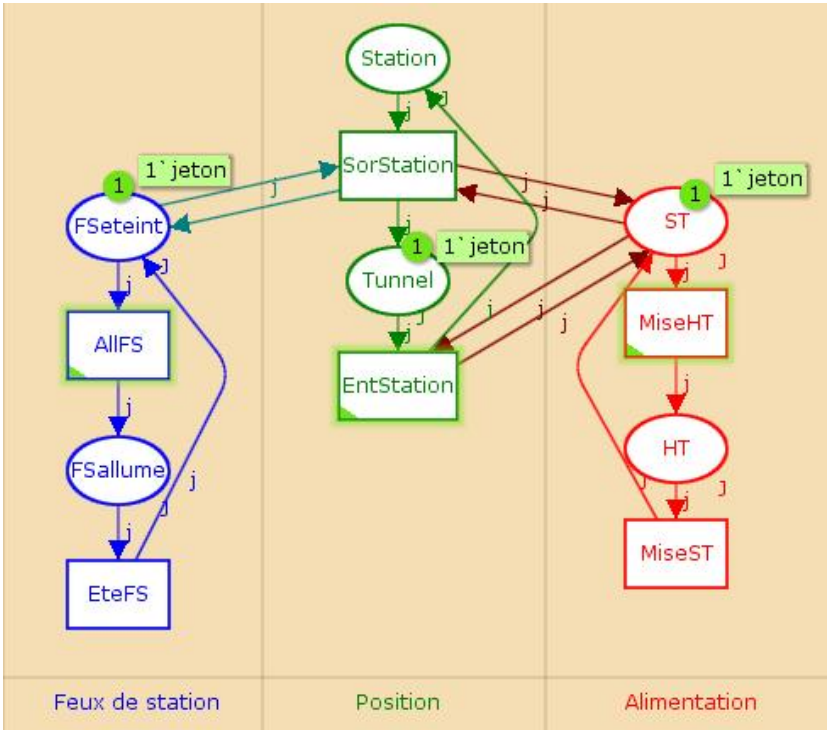


FIGURE V.5 – Réseaux de Petri des ressources

l'*Absence* (« *Fumee_A* » et « *PersV_A* ») des incidents et de deux transitions permettant de passer d'un état à l'autre. À l'état initial, les deux places *Absence* sont marquées (figure V.6).

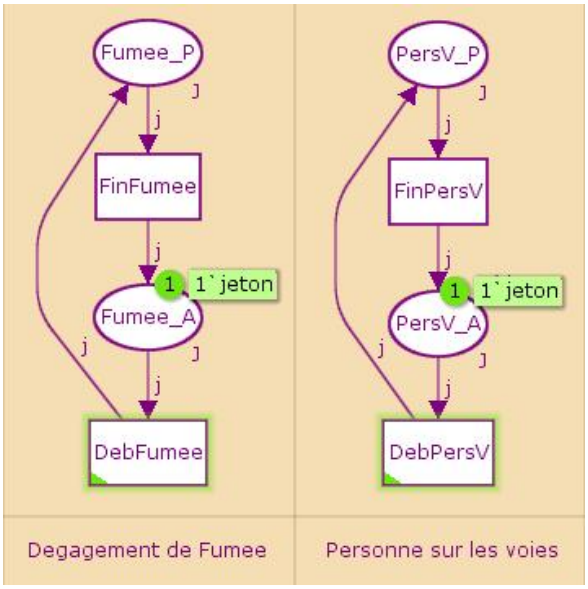


FIGURE V.6 – Réseaux de Petri des signalements d'incident

Modélisation des procédures

La démarche de modélisation des procédures par des réseaux de Petri (section III.3.4) comporte quatre étapes et se base sur les modèles BPMN des procédures. La transformation d'un langage à l'autre est présentée et détaillée pour la procédure *Alerte Feu Fumée* de l'exemple (figure V.7).

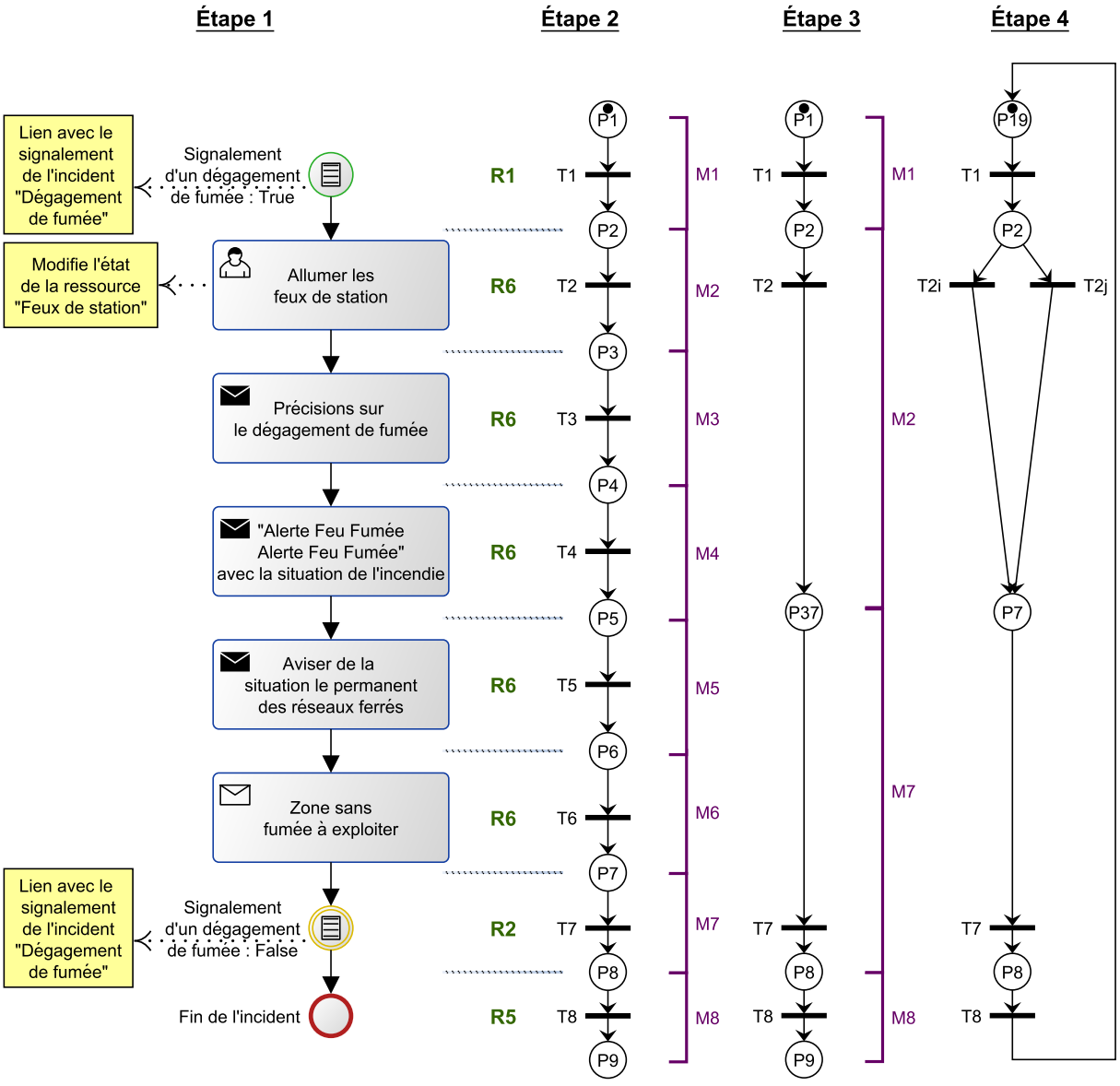


Figure V.7 – Modélisation des procédures

1. Identification des interactions entre la procédure et le système

   Lors de la recherche des ressources impliquées dans l'exemple, l'activité *Allumer les feux de station* a été identifiée comme changeant un élément de la ligne de métro : les *Feux de station*. Cette activité modifie donc l'état de l'une des ressources du système. Cette procédure est également liée au signalement de l'incident *Dégagement de fumée*. Ainsi, l'événement initial est déclenché par la présence de l'incident. L'événement intermédiaire de la procédure est également directement relié à l'état du signalement d'incident.

2. Traduction des éléments

   La seconde étape se base sur les recherches de Dijkman (figure III.19). Pour la procédure *Alerte Feu Fumée*, les règles R1, R2, R5 et R6 sont appliquées afin d'obtenir la traduction du modèle BPMN en réseau de Petri. Après avoir fusionné les places des modules adjacents, le réseau de Petri déterminé est constitué de neuf places et huit transitions, seule la place

P1 étant marquée.

3. Simplification du réseaux de Petri

   Lors de la simplification, seuls les modules ayant un lien avec le système et les premiers et dernier modules sont conservés. Ainsi, les modules M1, M2, M7 et M8 sont retenues pour former le réseau de Petri de la procédure. Après agrégation des modules restants, le réseau de Petri comporte alors cinq places et quatre transitions.

4. Intégration de la procédure dans le système

   Pour intégrer la procédure dans le système, la transition T2 doit être dédoublée puisqu'elle modifie l'état de la ressource *Feux de station*. Ainsi, si les feux sont déjà allumés, la transition T2i sera franchie tandis que la transition T2j sera franchie si les feux sont éteints et modifiera alors l'état de la ressource. Afin de pouvoir exécuter la procédure de manière cyclique, la place P9 et P1 sont fusionnées et un arc relie la transition T8 et la place P19.

Modélisation du système

De manière similaire à la procédure *Alerte Feu Fumée*, la procédure *Signalement d'une personne sur les voies* est transformée pour obtenir son modèle réseau de Petri constitué de quatre places et cinq transitions. L'activité BPMN *Mettre Hors Tension* modifie l'état de la ressource *Alimentation*, la transition correspondant au module de cette activité a donc été dédoublée afin de prendre en compte tous les cas possibles d'évolution. La procédure est également liée au signalement de l'incident *Présence d'une personne sur les voies*.

Après avoir modélisé l'ensemble des éléments du système nécessaires à l'étude des deux procédures, il faut les assembler pour construire le modèle réseau de Petri complet du système (figure V.8). Ainsi, les trois ressources *Feux de station* et *Alimentation* sont reliées aux procédures au niveau des transitions qui ont été dédoublées (*AFFbi et AFFbj*, *PVbi et PVbj*). De plus, pour maintenir les ressources dans les états *FSallume* et *HT* voulus par les procédures, les transitions *EteFS* et *MiseST* doivent être franchissables seulement si les procédures liées ne sont pas en cours d'exécution. Pour cela, comme les réseaux de Petri sont saufs, un double arc relie la place *AFF1* et la transition *EteFS* et un autre la place *PV1* et la transition *MiseST*. Les deux signalements d'incident sont liés au déclenchement des procédures et donc aux premières transitions des procédures *AFFa* et *PVa* ainsi qu'à la fin de gestion de l'incident *AFFc* et *PVc*.

L'intégration des trois types d'élément dans un même modèle va permettre d'étudier les procédures dans leur environnement d'exécution. À l'état initial, le train est sous tension, en tunnel et les feux de station sont éteints. Les deux signalements d'incident sont à l'état *Absence* et les procédures liées sont donc dans leur état initial. Ainsi, il n'y a pas de dégagement de fumée ni de personne descendue sur les voies. Cet état correspond à une exploitation normale de la ligne de métro.

V.2.4 Espace d'état du système

Le graphe d'accessibilité du réseau de Petri du système étudié dans l'exemple est calculé et généré automatiquement par l'outil utilisé, CPN Tools. Ce graphe est constitué de 288 nœuds et 1360 arcs, correspondant à l'ensemble des états réellement accessibles du système et aux

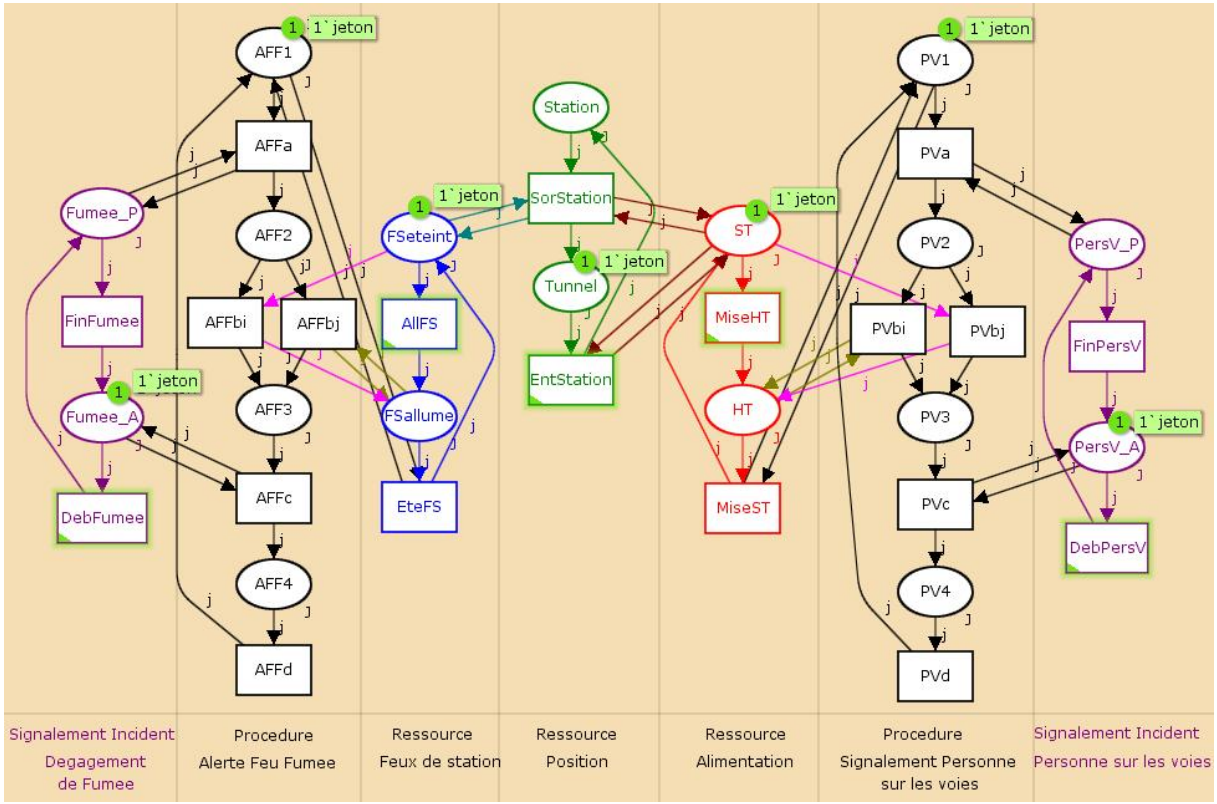


Figure V.8 – Modèle RdP du système

franchissements des transitions qui permettent de passer d'un état à l'autre. L'étude réalisée va maintenant se baser sur ce modèle du système pour analyser les états présentant un danger pour les voyageurs et le personnel de la ligne.

V.3 De l'analyse du danger au contrôle des procédures

V.3.1 Analyse des états dangereux

Contrôlabilité des transitions

Comme présenté dans la partie IV.1.2, un événement est contrôlable s'il est possible de l'interdire, il est donc lié à une action maitrisable par l'opérateur de supervision. Rien ne peut empêcher un incident de se produire, que ce soit le début d'un dégagement de fumée ou qu'une personne descende sur les voies de circulation. De même, l'opérateur de supervision ne contrôle pas la fin de ces incidents. Ainsi, les quatre transitions des modèles réseaux de Petri des signalements d'incident sont incontrôlables (« *FinFumee* », « *DebFumee* », « *FinPersV* » et « *DebPerV* »).

Inversement, les actions réalisées par l'opérateur de supervision pendant l'exécution des procédures de gestion d'incident sont des actions qu'il maitrise et qu'il peut choisir de réaliser ou non. L'ensemble des dix transitions des modèles des deux procédures étudiées *Alerte Feu Fumée* et *Signalement d'une personne sur les voies* sont donc contrôlables.

En ce qui concerne les ressources nécessaires à la description de l'environnement dans lequel se produisent les incidents, leur changement d'état est contrôlé par l'opérateur de supervision. En

effet, il décide d'allumer ou non les *Feux de station*, il maitrise l'état d'*Alimentation* électrique de la ligne et peut ordonner à un conducteur d'arrêter son mouvement, contrôlant ainsi la *Position* des trains sur la ligne.

Finalement, sur les vingt transitions du modèle réseau de Petri du système, seulement quatre transitions sont incontrôlables du point de vue de l'opérateur de supervision.

Caractérisation des états accessibles

L'objectif de cette partie est d'analyser l'ensemble des états du graphe d'accessibilité du système afin de calculer les sous-ensembles d'états caractérisant les états de danger atteignables.

Un état de danger est caractérisé par l'état *Présence* d'au moins deux signalements d'incident dans l'ensemble des états accessibles d'un système. Pour l'exemple étudié, seuls deux incidents sont considérés. Ainsi, l'ensemble Q_{danger} contient l'ensemble des états du graphe d'accessibilité où les places *« Fumee_P »* et *« PersV_P »* sont marquées. Cet ensemble contient 72 états sur les 288 au total, donc exactement un quart des états. Cette proportion s'explique par le fait que ce marquage représente un marquage des signalements d'incident sur les quatre possibles.

Pour chaque incident, il existe une combinaison des ressources assurant la sécurité des personnes. L'ensemble des états de Q_{danger} correspondant à cette combinaison appartient aux états sécuritaires Q_s. Par complémentarité des ensembles, les états dangereux Q_d sont des états de danger de Q_{danger} dans lesquelles la combinaison des états des ressources ne garantit pas la sécurité des personnes. Pour l'incident *Dégagement de fumée*, les personnes sont protégées si le train est en station et que les personnes peuvent ainsi évacuer la zone enfumée. La combinaison de ressources sécuritaire est donc *Position à l'état Station*. Lors de la *Présence d'une personne sur les voies*, celle-ci est en sécurité si l'énergie électrique pour alimenter les trains est coupé. Ainsi, l'état *Alimentation à l'état Hors Tension* correspond à la combinaison sécuritaire pour cet incident. Lors de l'occurrence des deux incidents étudiés, l'ensemble des états sécuritaires se caractérise par la combinaison des ressources : *Position à l'état Station* et *Alimentation à l'état Hors Tension*. Pour le système étudié, 24 états sont sécuritaires. Par complémentarité des ensembles, 48 états de l'ensemble des états accessibles appartiennent à l'ensemble des états dangereux Q_d.

Lorsqu'aucun des deux signalements d'incident est à l'état *Présence* et que les deux procédures ne sont pas en cours, les états atteints appartiennent alors à l'ensemble des états nominaux Q_n. Pour l'exemple, il existe 8 états nominaux représentant toutes les combinaisons possibles d'exploitation des ressources du système.

Le tableau 3. récapitule la taille de chacun de ces ensembles d'états par rapport à l'ensemble des états Q accessibles du système.

Table V.1 – Ensembles d'états

	Q	Q_{danger}	Q_s	Q_d	Q_n
Nombre d'états	288	72	24	48	8
Proportion	1	0.25	0.08	0.17	0.03

V.3.2 Recherche des états admissibles

La notion de contrôlabilité est maintenant introduite pour différencier les états dangereux Q_d présents dans le système et identifier les états dans lesquels l'opérateur de supervision ne peut pas agir sur le système : les états critiques Q_{cr}. Un état critique (définition 12) est un état du système dans lequel au moins deux signalements d'incident sont à l'état *Présence*, où l'état des ressources n'assurent pas la sécurité des personnes pour les incidents en cours et dont il est seulement possible de sortir par des transitions incontrôlables.

L'étude de l'enchainement des états menant de manière incontrôlable aux états critiques est également réalisée. L'objectif est d'empêcher le système d'atteindre des états critiques en déterminant l'ensemble des évolutions incontrôlables menant à ces états. Pour rappel (définition 15), un état redouté est un état à partir duquel il est possible d'atteindre au moins un état critique par une séquence d'événements incontrôlables. Pour calculer l'ensemble des états critiques Q_{cr} et l'ensemble des états redoutés Q_{re}, les algorithmes 1 et 2 présentés dans la partie IV.2 sont appliqués au système étudié en se basant sur le graphe d'accessibilité.

À la première itération, un seul état critique existe dans le système. Dans cet état, les deux signalements d'incident sont à l'état *Présence*, les procédures sont dans l'état d'attente de la fin des incidents (*AFF3* et *PV3*). Concernant les éléments de la ligne, le train est en *Tunnel*, les feux de station sont *Allumé* et l'alimentation électrique est *Hors Tension*. Ainsi, l'état sécuritaire pour l'incident *Dégagement de fumée* n'est pas atteint puisque le train est en *Tunnel*. L'état est donc bien un état dangereux. De plus, seules les transitions incontrôlables « *FinFumee* » et « *FinPersV* » sont franchissables. Ainsi, l'état déterminé par l'algorithme est un état critique du système qu'il faut éviter pour garantir la sécurité des personnes. Avec les algorithmes, quatre états redoutés sont identifiés pour ne pas atteindre l'état critique. Cependant, comme présenté dans la partie IV.2, le calcul des états critiques et redoutés doit être itératif afin de déterminer l'ensemble de ces états.

Le tableau V.2 présente les résultats obtenus lors de l'application de l'algorithme 2, itération par itération. Ainsi, six itérations sont nécessaires pour calculer des ensembles complets et stables d'états critiques et redoutés. Finalement, pour l'exemple étudié, il existe 12 états critiques et 48 états redoutés dans le système étudié.

Table V.2 – États critiques et redoutés

Itération	**1e**	**2e**	**3e**	**4e**	**5e**	**6e**
Q_{cr}	1	3	5	8	11	12
Q_{re}	4	12	20	32	44	48

V.3.3 Vérification de l'existence d'un contrôleur

L'ensemble des états à éviter pour assurer la sécurité des voyageurs et du personnel est connu, il faut maintenant vérifier l'existence d'un contrôle et l'intégrer dans le modèle réseau de Petri du système afin d'obtenir l'ensemble des états admissibles et vérifier les propriétés du système contrôlé.

Après avoir déterminé les invariants du système étudié, les simplifications des contraintes sont appliquées à l'ensemble des états redoutés qu'il faut éviter pour respecter l'objectif de contrôle

défini. Ainsi, en simplifiant les 48 contraintes initiales correspondant aux états redoutés, seules les trois contraintes suivantes liées au marquage sont nécessaires pour décrire l'ensemble des états redoutés à éviter.

$$m_{AFF1} + m_{AFF2} + m_{Tunnel} + m_{HT} + m_{PV2} \leq 3 \quad (1)$$

$$m_{AFF3} + m_{AFF4} + m_{Tunnel} + m_{HT} + m_{FSallume} + m_{PV2} \leq 4 \quad (2)$$

$$m_{Tunnel} + m_{HT} + m_{PV3} \leq 2 \quad (3)$$

La figure V.9 présente le modèle réseaux de Petri du système contrôlé, avec les trois places de contrôle calculées en appliquant la démarche développée par Yamalidou [Yam96]. Chaque contrainte correspond au marquage d'une place de contrôle à intégrer au modèle réseau de Petri du système. La borne supérieure de la contrainte limite le nombre de marques présent dans la place et permet le calcul du marquage initial de la place de contrôle. Dans le système contrôlé, l'ensemble des états critiques et l'ensemble des états redoutés sont vides.

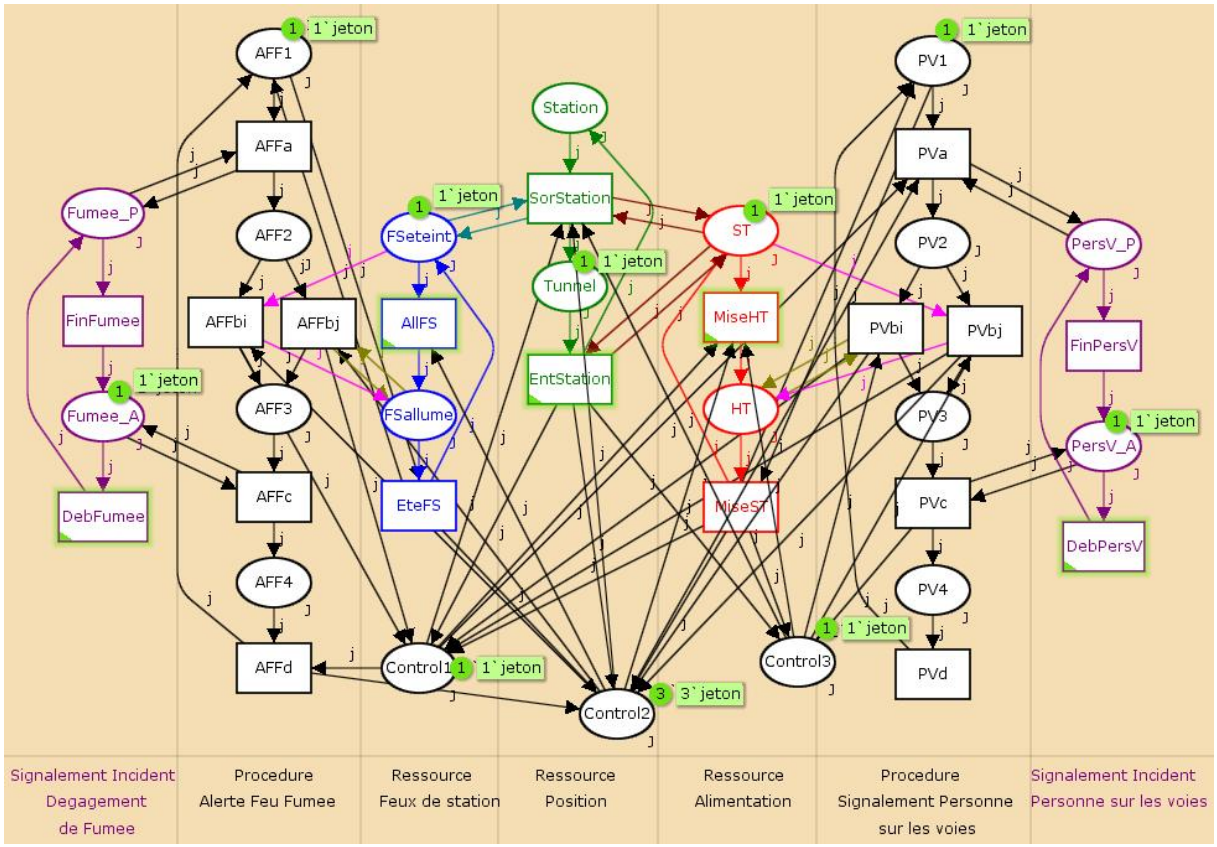


FIGURE V.9 – Modèle RdP du système contrôlé

La détermination des trois places de contrôle prouve ainsi l'existence d'un contrôleur pour le système étudié. Il existe donc une solution pour éviter les 48 états redoutés identifiés. Cette existence montre également que le système contrôlé est maximum permissif et non bloquant. Le graphe d'accessibilité du modèle réseaux de Petri du système contrôlé est accessible et co-accessible au sens des automates à états, il est donc possible de retourner à l'état initial même lorsque les états redoutés sont évités. De plus, l'ensemble des états nominaux de Q_n est inclus

dans le système contrôlé ce qui assure que le comportement minimal souhaité du système est toujours réalisable. En effet, les trois places de contrôle ajoutées au système n'empêchent pas les trois ressources d'évoluer lorsqu'aucun incident ne s'est produit et qu'aucune procédure n'est en cours.

V.4 Implémentation de l'assistance à l'opérateur

V.4.1 Analyse et caractérisation des trajectoires

Après avoir calculé l'ensemble des états redoutés à éviter et vérifié l'existence d'un contrôleur, l'objectif est d'étudier les trajectoires menant à aux états redoutés et de les caractériser. En effet, le système n'est pas automatique mais décrit les actions d'un opérateur dont il n'est pas possible de limiter les actions. Ainsi, les 48 états redoutés de l'exemple ne peuvent pas être interdits car les décisions pour la supervision d'une ligne de métro sont toujours prises par l'opérateur. Cependant, il est possible de donner à l'opérateur de supervision des alertes et conseils sous forme de messages pour l'orienter et le guider lors d'incidents simultanés et ainsi garantir au mieux la sécurité des personnes.

Plusieurs critères ont été définis dans la partie IV.4.2 pour différencier et caractériser les trajectoires menant aux états redoutés. Ainsi, seules les trajectoires contrôlables sont étudiées, correspondant aux franchissements des transitions des trois ressources et des deux procédures de l'exemple. De plus, à l'état d'origine de ces trajectoires, les deux incidents *Dégagement de fumée* et *Présence d'une personne sur les voies* doivent être en cours. Des messages sont transmis à partir du moment où le système a atteint un état frontière.

Pour différencier les transitions sortantes des états frontières, quatre ensembles ont été définies suivant l'état de destination de la transition : *Rouge*, *Jaune*, *Violette* et *Verte*. Dans l'exemple, 12 états appartiennent à l'ensemble des états frontières Q_{fr}. Les transitions sortantes de ces états se répartissent de la manière suivante :

Table V.3 – Caractérisation des transitions frontières

Q_{fr}	$\Delta_{Rouge_{fr}}$	$\Delta_{Jaune_{fr}}$	$\Delta_{Violette_{fr}}$	$\Delta_{Verte_{fr}}$
12	18	16	12	0

Les trajectoires menant à un état redouté et passant par un état frontière dont les transitions sortantes sont soit *Jaune* soit *Rouge* et définissant ainsi les états frontières amont $Q_{fr_{amont}}$ sont ensuite analysées. Pour l'exemple étudié, il n'existe aucun état frontière amont $Q_{fr_{amont}}$. En effet, tous les états frontières ont une transition sortante appartenant à l'ensemble $\Delta_{Violette_{fr}}$.

Les trajectoires sortant d'un état frontière et n'ayant pas de transitions sortantes appartenant à $\Delta_{Verte_{fr}}$ mais au moins une transition dans $\Delta_{Violette_{fr}}$ sont également étudiées. Ces états appartiennent à l'ensemble des états frontières aval $Q_{fr_{aval}}$. Or, d'après le tableau V.3, l'ensemble des transitions $\Delta_{Verte_{fr}}$ pour les états frontières est vide. De plus, chaque état frontière a une transition sortante dans l'ensemble $\Delta_{Violette_{fr}}$. Ainsi, pour l'exemple, tous les états frontières sont des états aval : $Q_{fr} = Q_{fr_{aval}}$. Le tableau V.4 répertorie le nombre d'états Q_{mess} dans lesquels un message est transmis à l'opérateur et les transitions caractérisées lors de cette étape de l'analyse.

TABLE V.4 – Caractérisation des trajectoires aval

Q_{mess}	$\Delta_{Jaune_{aval}}$	$\Delta_{Violette_{aval}}$	$\Delta_{Verte_{aval}}$
18	14	38	18

Finalement, l'analyse des trajectoires a permis de caractériser les transitions sortantes de 30 états à partir desquels il pourra être intéressant de transmettre un message à l'opérateur de supervision et appartenant donc à l'ensemble Q_{mess} (tableau V.5).

TABLE V.5 – Caractérisation des transitions

Q_{mess}	Δ_{Rouge}	Δ_{Jaune}	$\Delta_{Violette}$	Δ_{Verte}
30	18	30	50	18

Les transitions identifiées dans les quatre ensembles correspondent aux messages qu'il sera possible de délivrer à l'opérateur de supervision lors de l'occurrence des deux incidents étudiés. Ces ensembles caractérisent les transitions et donc les messages donnés à l'opérateur, en différenciant les alertes (Δ_{Rouge}) et les conseils (Δ_{Verte}, $\Delta_{Violette}$ et Δ_{Jaune}). De plus, les conseils sont hiérarchisés suivant la couleur de leur ensemble d'appartenance correspondant au danger défini, les conseils de l'ensemble Δ_{Verte} étant préférables. Les actions réalisées dans une procédure sont également privilégiées. Les états de Q_{mess} et les messages qui leurs sont associés sont présentés dans l'annexe F.

Bilan

Le tableau V.6 présente un bilan des ensembles d'états et de transitions déterminés dans le système étudié.

TABLE V.6 – Ensembles d'états et de transitions

États critiques	Q_{cr}	12
États redoutés	Q_{re}	48
États dangereux	Q_{d}	48
États frontières	Q_{fr}	12
États nominaux	Q_{n}	8
États avec message	Q_{mess}	30
Transitions Rouge	Δ_{Rouge}	18
Transitions Jaune	Δ_{Jaune}	30
Transitions Violette	$\Delta_{Violette}$	50
Transitions Verte	Δ_{Verte}	18

V.4.2 Présentation de scénarios d'aide à la décision

Afin d'illustrer les résultats obtenus, des scénarios de gestion d'incidents sont présentés pour mettre en évidence différents cas possibles. Chacune des lignes des figures suivantes décrit l'état du système et la couleur de fond caractérise l'appartenance de l'état à l'un des ensembles précédemment définis. Les flèches reliant les lignes précisent le ou les éléments du système qui changent d'état. Les changements incontrôlables sont représentés par des flèches en pointillé. Lorsqu'une indication doit être donnée à l'opérateur de supervision, une ligne est attachée à l'état du système pour indiquer les messages transmis et la catégorie de couleur de la transition concernée.

Scénario avec un incident

D'après les hypothèses de l'étude, lors de l'occurrence d'un seul incident, les états atteints ne sont pas considérés comme dangereux car une procédure, juste par usage, existe pour les gérer. Le scénario de la figure V.10 présente les évolutions du modèle du système lors de l'occurrence uniquement d'un dégagement de fumée, aucun message n'est donc transmis à l'opérateur. L'état initial est un état nominal ainsi que l'état atteint lorsque la procédure de gestion d'incident est terminée.

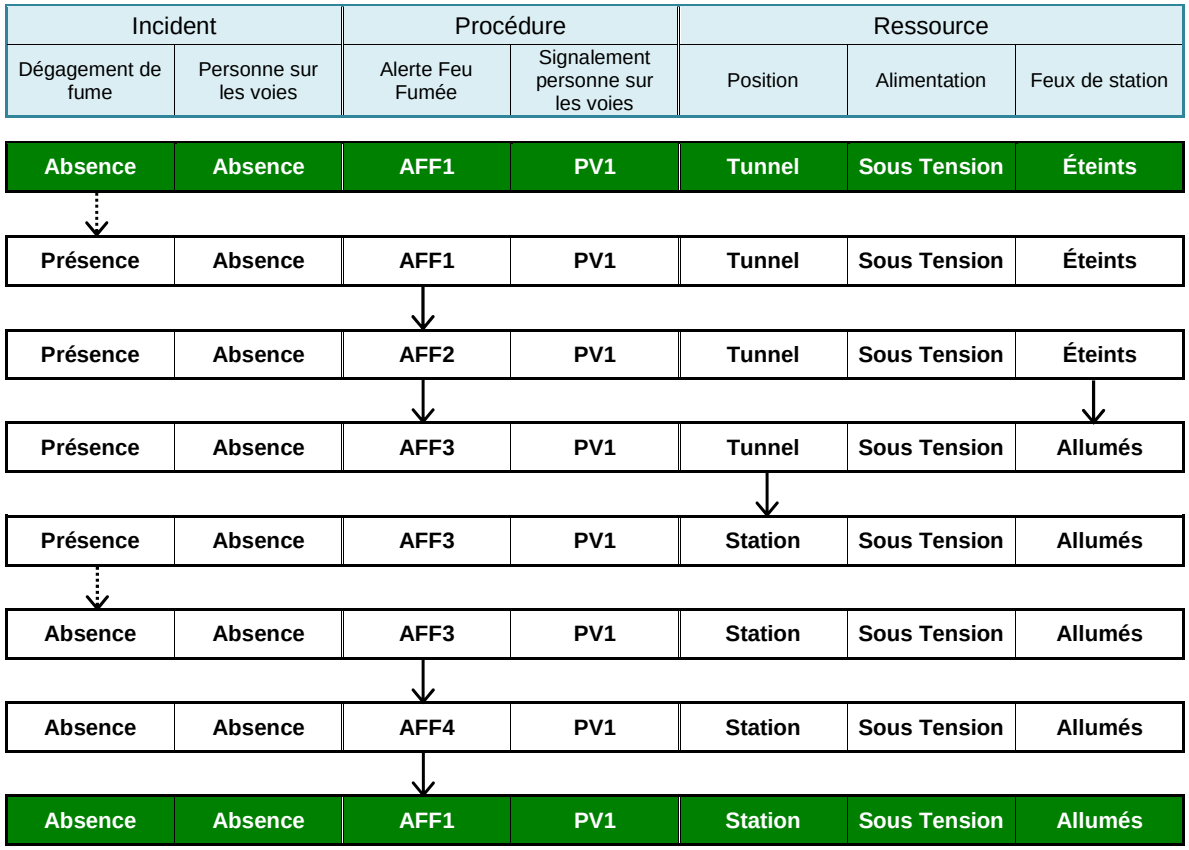


Figure V.10 – Scénario avec un incident

Scénario avec deux incidents et messages

Le scénario de la figure V.11 étudie la gestion des deux incidents de l'exemple se produisant directement l'un après l'autre. Le troisième état est donc un état dangereux Q_d. L'opérateur de supervision débute ensuite successivement les deux procédures pour gérer les deux incidents en cours. L'état atteint est un état frontière Q_{fr} : il existe donc au moins une transition contrôlable menant à un état redouté qu'il faut éviter. Des indications sont par conséquent transmises à l'opérateur de supervision. Deux alertes lui déconseillent de mettre la ligne *Hors Tension* en progressant dans la procédure ou simplement en changeant l'état de la ressource *Alimentation*. Un conseil de couleur *Violette* lui est également donné : faire entrer le train en station en modifiant l'état de la ressource *Position*. La couleur de ce message indique cependant que l'état atteint sera toujours un état dangereux. Une fois que le train est entré en station, un nouveau conseil est transmis à l'opérateur : mettre la ligne *Hors Tension*. Ce message étant *Vert*, l'état des ressources sera sécuritaire pour les incidents en cours. La suite de l'évolution des procédures et du système pour retourner à un état nominal n'est pas présentée puisqu'aucun autre message ne sera donné et que la sécurité des voyageurs et du personnel est maintenant garantie.

Si l'opérateur de supervision ne suit pas les indications qui lui sont transmises et met la ligne *Hors Tension* lorsque cela lui est déconseillé, un état redouté sera atteint. À partir de ce moment-là, un accident pourra potentiellement se produire, sans aucune maitrise possible, et porter alors atteinte à la sécurité des voyageurs et du personnel. En respectant les indications qui lui sont transmises, l'opérateur protège au mieux ces personnes.

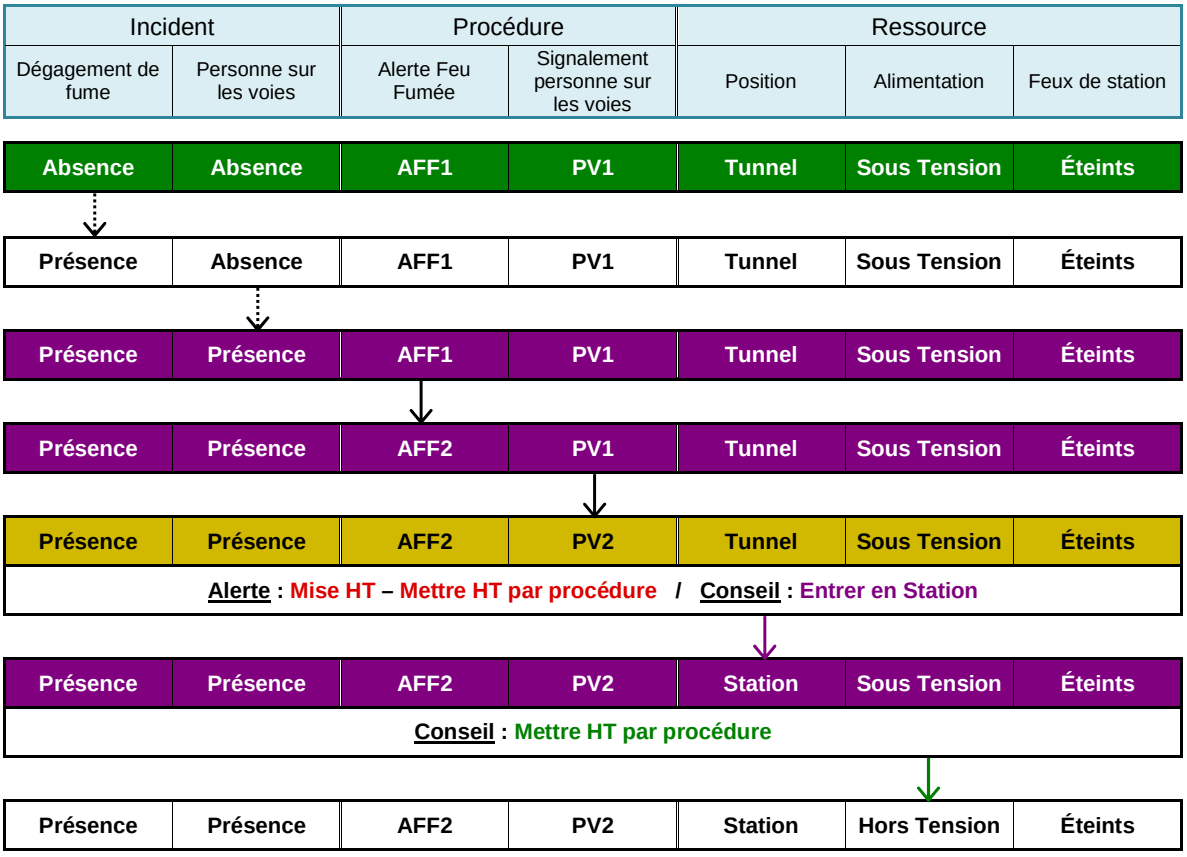


FIGURE V.11 – Scénario avec deux incidents et messages

Scénario avec deux incidents vers un état critique

Un autre scénario avec deux incidents est présenté figure V.12. Dans ce scénario, des états critiques sont atteints sans qu'aucun message ne soit transmis à l'opérateur de supervision, il montre ainsi une des limites de l'étude réalisée. En effet, dans cet exemple, une personne descend sur les voies de circulation et l'opérateur de supervision exécute la procédure de gestion de cet incident. Une fois qu'il a mis la ligne *Hors Tension*, un deuxième incident se produit : un *Dégagement de fumée*. L'opérateur exécute alors la procédure *Alerte Feu Fumée*. Cependant, le train est en *Position : Tunnel* et comme la ligne de métro n'est plus alimentée, le train ne peut pas se déplacer et doit rester en *Tunnel*. L'état alors atteint dans ce scénario est à éviter : l'état n'est pas sécuritaire et l'opérateur ne peut pas agir sur le système, il ne peut qu'attendre la fin de l'un des deux incidents. Dans cet état, des dommages sur la santé des personnes présentes dans le train stationnant dans le tunnel enfumé pourraient alors être constatés. La seule possibilité pour sortir de cet état est que le *Dégagement de fumée* s'arrête ou que la *Personne sur les voies* remonte sur l'un des quais. L'état alors atteint serait néanmoins toujours un état redouté.

Ce scénario existe car lorsque l'une des deux procédures est en cours d'exécution, il est possible que l'état des ressources corresponde à l'état sécuritaire pour l'incident géré mais pas pour un autre incident. Ainsi, si la procédure est trop avancée, aucune aide ne peut être donnée à l'opérateur de supervision pour garantir au mieux la sécurité des personnes avec les critères d'assistance retenue pour cette étude.

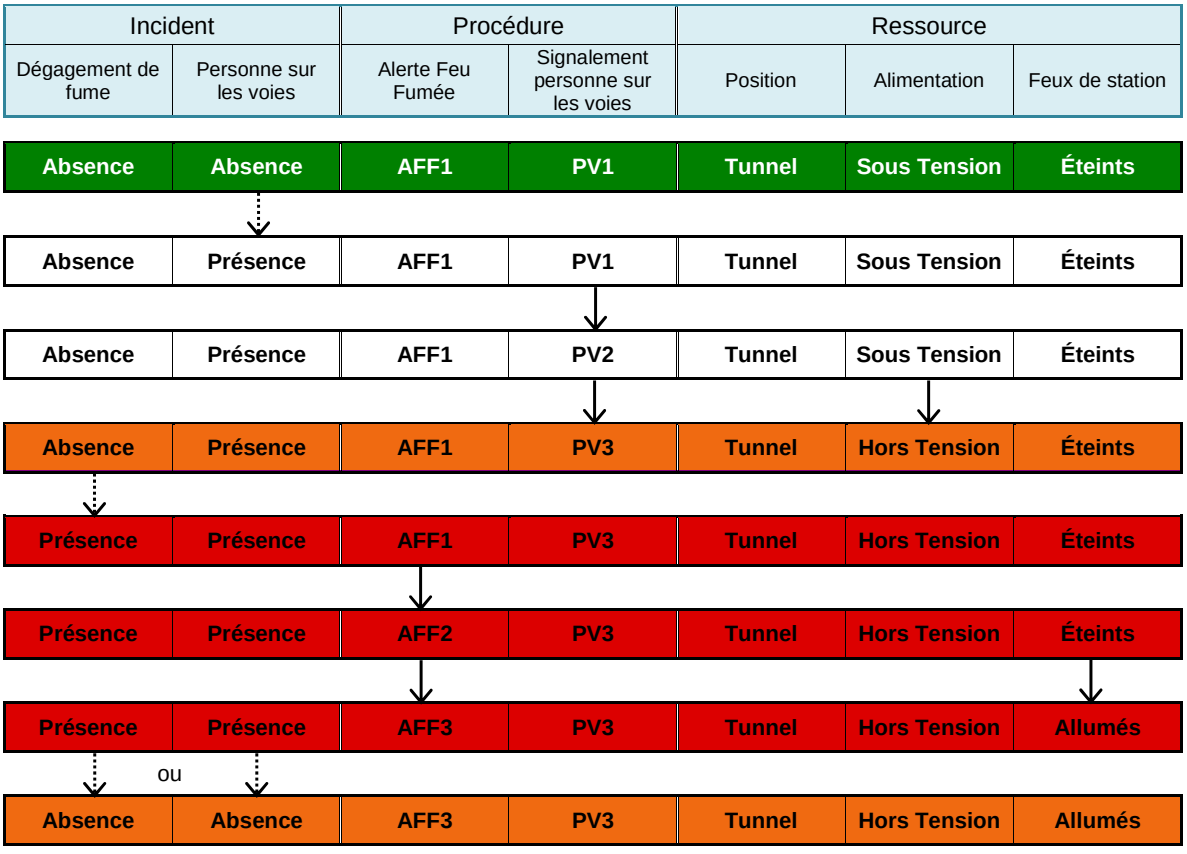


Figure V.12 – Scénario avec deux incidents sans messages

V.5 Bilan sur l'application de l'exemple et son implémentation

La démarche de modélisation de procédures de gestion d'incident et d'analyse et de maîtrise du danger a été appliquée sur deux procédures exécutées par les opérateurs de supervision de la RATP : *Alerte Feu Fumée* et *Signalement d'une personne sur les voies*. Le projet innovant réalisé par Thales et présenté dans la partie IV.5 se base également sur les deux mêmes procédures pour ajouter une fonctionnalité *Decision Support System* au démonstrateur de l'application ATS de Thales. Lors de l'implémentation de la démarche d'étude proposée dans cette thèse, les développeurs travaillant sur le projet ont choisi d'intégrer les procédures BPMN de gestion d'incident complètes et non celles simplifiées comme présentées dans ce chapitre. Les opérateurs de supervision ont en effet besoin de la description de l'ensemble des activités à réaliser. Un bilan de l'application de l'exemple et de son implémentation est effectué en mettant en évidence les difficultés rencontrées, les apports réalisés ainsi que les limites identifiées.

L'une des étapes importante à réaliser au cours du projet innovant était la modélisation du système étudié en réseaux de Petri. En effet, cette étape comporte l'automatisation de la transformation entre les modèles BPMN des procédures et les modèles réseaux de Petri et l'intégration des ressources et des signalements d'incident. La démarche de transformation a été présentée dans la partie III.3.4 mais son automatisation n'avait pas été réalisée dans le cadre de mes recherches. Le projet innovant a donc permis de développer cette automatisation non sans difficultés puisqu'elle nécessite la prise en compte, notamment, des liens avec les ressources.

Une des difficultés rencontrées a été l'identification des ressources impliquées dans l'exécution des deux procédures étudiées. En effet, cette identification nécessite une connaissance avancée de l'exploitation d'une ligne de métro et de la gestion des incidents. Le choix a donc été fait de ne considérer que trois ressources essentielles pour l'exemple. De plus, cette limitation a permis d'éviter une explosion de la taille du modèle réseaux de Petri généré et ainsi de garder un graphe d'accessibilité de taille « raisonnable ».

En décrivant plusieurs scénarios possibles d'évolution du système étudié, une limite de l'étude a été mise en évidence. En effet, il existe des évolutions où aucun message ne sera transmis à l'opérateur de supervision alors qu'un état critique est atteint. Ce qui signifie que l'opérateur ne pourra plus agir au sein des procédures et sur les ressources pour modifier l'état alors que les voyageurs et le personnel seront dans une situation dangereuse. Ce type de scénarios existe en raison de l'un des critères choisis pour l'assistance à l'opérateur. En effet, l'opérateur de supervision commence à recevoir des messages seulement à partir du moment où au moins deux incidents sont en cours. La gestion d'un seul incident n'est pas un cas particulier de l'exploitation d'une ligne de métro et n'est pas concernée par l'étude réalisée dans cette thèse. Ainsi, l'état des ressources peut correspondre à un état dangereux pour un second incident, mais il n'est pas possible d'avertir l'opérateur de supervision avant le déclenchement de cet incident. Sinon, les messages reçus lui paraîtraient incohérents par rapport à la situation courante de la ligne et capteraient son attention inutilement.

L'application de la démarche a également permis de mettre en avant certains apports de l'étude. Lors de l'occurrence des deux incidents étudiés dans l'exemple, si un message d'alerte est transmis à l'opérateur de supervision pour lui indiquer de ne pas réaliser une action correspondant à une activité dans l'une des procédures BPMN, le conseil donné en même temps est une action à réaliser sur les ressources. Le fait que le conseil soit lié aux ressources révèle que

les deux procédures ne sont pas adaptées pour une exécution conjointe et que leurs activités ne suffisent pas à la gestion simultanées des deux incidents. S'il fallait créer une procédure pour la gestion conjointe des deux incidents, des activités supplémentaires liées aux ressources devraient alors être intégrées à cette procédure. Les conseils transmis correspondent à ces actions supplémentaires.

L'implémentation de la démarche par des développeurs de Thales a tout d'abord validé son automatisation et son intégration dans une application temps réel en se basant sur des acquisitions terrains, mais également son intérêt pour un industriel. En cohérence avec les objectifs présentés dans la partie IV.5, le projet a permis d'intégrer le modèle de deux procédures BPMN pour la gestion d'incident avec une visualisation en temps réel de leur évolution. De plus, des alertes et des conseils adaptés à la situation courante de la ligne sont transmis à l'opérateur de supervision lors de l'occurrence des deux incidents. Il est ainsi orienté dans les actions à effectuer pour assurer au mieux la sécurité des voyageurs et du personnel.

Lors de l'occurrence de plusieurs incidents sur une ligne de métro, il est possible d'apporter une assistance à l'opérateur de supervision afin d'éviter les états qu'il ne peut pas maitriser et dans lesquelles les voyageurs et le personnel sont en danger. Le démonstrateur développé dans le cadre du projet innovant repose sur l'exemple présenté dans cette partie et a permis d'identifier certaines limites et améliorations possibles dans le résultat obtenus. Ces perspectives sont exposées dans la conclusion générale de ce mémoire sous forme d'approfondissements possibles de la démarche proposée.

Conclusion générale

Sommaire

1. Contributions de la thèse

Le travail présenté dans ce mémoire propose des réponses aux questionnements initiaux basés sur la gestion d'une succession d'événements anormaux se produisant dans un système industriel complexe, et plus particulièrement lors de l'exploitation d'une ligne de métro. En déterminant l'ensemble des situations dans lesquelles la sécurité des voyageurs et du personnel n'est pas assurée, une assistance est proposée à l'opérateur de supervision. L'opérateur est prévenu en amont d'un danger potentiel et a la possibilité d'adapter ses actions pour protéger les personnes. En conclusion, lors de l'occurrence d'incidents combinés sur une ligne de métro, il est possible d'apporter une assistance à l'opérateur de supervision afin d'éviter l'avènement d'un accident.

Pour arriver à cette conclusion et répondre aux problèmes posés, une démarche d'étude constituée de huit étapes a été développée et est présentée dans ce mémoire.

L'acquisition du savoir-faire métier sur la supervision d'une ligne de métro et plus particulièrement sur la gestion des incidents s'est faite au travers de la collaboration avec les industriels impliqués dans l'étude, Thales et la RATP. Une classification suivant différents critères des incidents et des procédures permettant de les gérer a ainsi pu être réalisée. L'acquisition des connaissances métier lors du suivi de la formation des opérateurs de supervision à la RATP constitue une base de données importante pour Thales. En effet, ces données et pratiques client leur étaient inconnues auparavant.

Le savoir-faire acquis est ensuite représenté graphiquement avec le langage BPMN pour obtenir des procédures de gestion d'incidents standardisées. La notation BPMN propose une représentation graphique adaptée et facilement compréhensible par les industriels. Elle favorise les échanges et le partage des connaissances avec eux. Les procédures représentées en BPMN regroupent également des données intéressantes pour Thales puisque elles leur offrent une vision plus précise de la réalité de l'exploitation avec incidents.

Pour analyser les procédures de gestion d'incidents, leur intégration dans leur environnement d'exécution a été réalisée. Cette intégration comprend l'introduction de la notion de contrôlabilité dans l'étude des procédures et la prise en compte de l'influence du contexte de la ligne sous forme de ressources. Pour cela, le système étudié est modélisé sous la forme d'un système à événements

discrets, par réseaux de Petri. L'intégration dans leur environnement d'exécution a nécessité le développement d'une démarche de transformation des procédures représentées avec la notation BPMN à une modélisation réseaux de Petri de l'ensemble des éléments constituant le système étudié. Ces éléments sont : les procédures de gestion d'incidents, les signalements d'incidents et les ressources décrivant le contexte de la ligne de métro.

En se basant sur cette modélisation par réseaux de Petri, les situations dangereuses pouvant être atteintes sont ensuite caractérisées et définies. L'ensemble des états interdits ne garantissant pas la sécurité des personnes est alors déterminé. Dans ces travaux, une caractérisation originale des états interdits a été proposée. En effet, en plus de la contrainte d'inclusion traditionnelle dans un ensemble d'états, un état interdit se définit également par la contrôlabilité de ses transitions sortantes.

Cette nouvelle définition des état interdits a conduit au développement d'algorithmes spécifiques pour les identifier et les éviter dans le cadre de l'application de la théorie du contrôle par supervision, les séquences sûres sont ainsi connues. L'originalité de la caractérisation des états interdits suivant leurs transitions sortantes impose également de les déterminer de manière itérative afin de tous les éviter. La vérification de l'existence d'un contrôleur permettant d'éviter ces états interdits est ensuite réalisée à partir du modèle réseaux de Petri du système et se base sur plusieurs études antérieures. Le système contrôlé permet alors de vérifier si les propriétés recherchées sont respectées.

À partir du système contrôlé et de l'ensemble des séquences sûres, une analyse des successions d'actions réalisables par l'opérateur de supervision est effectuée. Dans l'objectif de développer une aide à la décision et de transmettre des messages à l'opérateur de supervision, des critères de différenciation des trajectoires admissibles ont été définis. Ces critères se basent notamment sur l'état de destination des transitions mais offrent également la possibilité d'étudier les trajectoires en amont et en aval des états interdits. Des alertes et des conseils ainsi que le moment où ils doivent être transmis à l'opérateur de supervision sont alors déterminés.

Les résultats de mes travaux ont permis à Thales, au travers d'un projet innovant, d'implémenter le prototype d'une nouvelle fonctionnalité dans leur application ATS. Les opérateurs pourront ainsi visualiser les procédures de gestion d'incident représentées avec la notation BPMN et être orientés lors d'incidents combinés. Cette fonctionnalité d'aide à la décision pour les opérateurs de supervision donne la possibilité à Thales de se différencier de sa concurrence. Elle leur permet également d'être au plus près des attentes clients qui souhaitent garantir la sécurité de leurs voyageurs tout en exploitant au maximum les capacités de leurs lignes de métro.

Au cours de ces travaux, des apports ont ainsi été réalisés dans au niveau scientifique mais également dans le domaine industriel. La démarche de réflexion proposée s'est confrontée à certaines limites et a également amené à se poser de nouvelles questions dans le but d'améliorer les solutions apportées.

2. Limites

Une des premières difficultés mise en évidence lors de l'application de la démarche a été l'identification des ressources impliquées dans l'exécution des procédures. En effet, cette identification nécessite une connaissance avancée de l'exploitation d'une ligne de métro et de la gestion

des incidents. L'expertise d'un exploitant s'avère donc essentielle pour étudier les incidents combinés afin de ne pas négliger certains éléments du contexte de la ligne ayant une incidence sur la sécurité des personnes.

Dans les travaux présentés dans ce mémoire, les éléments du contexte décrivant la ligne, les ressources, existent de manière unique. Ainsi dans l'exemple développé, la ressource *Position du train* se réfère à un seul train sur la ligne et une seule section pour l'alimentation électrique est considérée. L'étude est donc restreinte à un seul train et une partie de la ligne alors que le logiciel de supervision gère l'ensemble de la ligne et plusieurs trains. Cette différence a compliqué l'implémentation du prototype d'aide à l'opérateur qui est donc adapté aux recherches effectuées et limité à une partie de la ligne.

Comme pour de nombreuses études de systèmes à événements discrets, notre étude est confrontée à l'explosion combinatoire de la taille des modèles. Dans l'exemple, le choix a été fait d'étudier uniquement la combinaison de deux procédures. Pour étudier l'ensemble des combinaisons possibles entre toutes les procédures, il faudrait modéliser également l'ensemble des ressources impliquées. Cette étude complète engendrerait un modèle de taille trop importante et probablement difficile à déterminer. Il semble donc plus approprié d'étudier les combinaisons de procédures 2 à 2, voire 3 à 3, pour éviter ces complications et limiter ainsi les temps de calcul. Un seuil de probabilité d'occurrence d'incidents combinés pourrait ainsi restreindre les combinaisons de procédures à étudier.

3. Perspectives

Plusieurs idées pourront permettre de poursuivre et d'approfondir le travail réalisé du côté scientifique et du côté industriel.

Perspectives scientifiques

Afin de se rapprocher du fonctionnement global de la supervision d'une ligne, il serait intéressant de modéliser un système avec plusieurs trains et plusieurs sections électriques. Pour obtenir un modèle de taille raisonnable et compact, il serait alors judicieux de changer la classe des réseaux de Petri en passant de réseaux ordinaires à des réseaux colorés et de haut niveau. Cependant, il faudra également prendre en considération les nouvelles interactions entre les ressources et probablement modifier la modélisation du système. En effet, si un incident se produit sur une section électrique, des répercussions vont exister sur les sections voisines. Alors que si les incidents sont situés aux deux extrémités de la ligne, ils auront peu d'influence l'un sur l'autre. Les interactions entre les ressources et leur partage devront donc également être étudiées lors de l'élargissement du périmètre de l'étude.

Une autre évolution du périmètre de l'étude pourrait également être envisagée si des données sur la probabilité d'occurrence des incidents étaient connues. Ainsi, l'étude ne porterait plus sur le danger mais sur les risques encourus. Une modélisation du système par réseaux de Petri stochastiques pourrait ainsi être envisagée et les combinaisons de procédures à étudier seraient choisies suivant la probabilité d'occurrence des incidents combinés. Un nouveau critère de différenciation des trajectoires pourrait aussi être retenu pour améliorer le choix des alertes et conseils à transmettre à l'opérateur de supervision.

La représentation graphique des procédures avec la notation BPMN a permis de mettre en évidence des regroupements d'activités présents dans plusieurs procédures. L'élément sous-procédures a ainsi été employé pour obtenir une représentation des procédures plus compact mais également mettre en évidence des dépendances entre ces procédures. Il serait donc intéressant de s'interroger sur une utilisation possible des sous-procédures lors de l'implémentation de l'aide à la décision. Des niveaux de détails des procédures pourraient ainsi être proposés aux opérateurs de supervision suivant leur profil et leur expérience.

L'une des hypothèses de l'étude définit la transition entre deux états d'une ressource comme contrôlable, c'est-à-dire que l'opérateur de supervision peut interdire son franchissement. Cependant, pour certaines ressources, la changement d'un état à l'autre peut être fait par une autre personne que l'opérateur et devient donc incontrôlable pour celui-ci. Par exemple, la mise hors-tension d'une section de la ligne s'effectue de plusieurs manières : par l'opérateur au travers de l'application de supervision (transition contrôlable) mais également par un conducteur, tout au long de la voie, sans avoir prévenu l'opérateur de supervision au préalable (transition incontrôlable). Pour s'approcher du comportement réel, il serait donc plus approprié de considérer le passage entre les deux états d'une ressource comme contrôlable, pour les actions du superviseur, et incontrôlable, pour les actions terrain. Cependant, la définition de deux transitions, l'une contrôlable et l'autre incontrôlable, entre deux états aurait sûrement des impacts importants sur l'étude, notamment sur l'application de la théorie du contrôle par supervision et les résultats obtenus.

Perspectives industrielles

Du point de vue industriel, plusieurs perspectives sont envisageables. Il est en effet possible d'étendre la démarche de l'étude des procédures de gestion d'incidents à des procédures de gestion de l'exploitation. Au cours d'une exploitation nominale de la ligne, l'opérateur doit réaliser un ensemble d'actions qu'il serait possible de représenter sous forme de procédure avec la notation BPMN et ainsi d'introduire ces procédures dans la fonctionnalité *Decision Support System* développée. L'objectif de ces procédures ne serait pas de garantir la sécurité des voyageurs et du personnel comme pour la gestion des incidents mais d'améliorer le service proposé.

L'application de l'étude à l'exemple a permis de mettre en évidence que les conseils transmis à l'opérateur en temps réel lors d'incidents combinés sont des actions à réaliser sur les ressources. L'opérateur exécute donc deux procédures indépendantes et la fonctionnalité d'aide à la décision lui propose de réaliser des actions en dehors de ces procédures sur les ressources impliquées. Une autre application enrichissante des résultats obtenus pourrait être de créer en amont des procédures permettant de gérer deux incidents combinés. En prenant en compte les recommandations faites par l'étude, des activités liées aux ressources devraient alors être intégrées à ces procédures conjointes.

Même si les travaux sont appliqués au domaine des transports, et plus particulièrement au métro, notre étude peut s'adapter à d'autres types de systèmes industriels dans lesquels des successions d'événements anormaux peuvent se produire et conduire à des accidents et où l'on souhaite améliorer la sécurité des personnes.

Liste des acronymes

AEAU	Arrêt automatique du train
AFF	Alerte Feu Fumée
AG	Appel Général
APD	Analyse Préliminaire des Dangers
APR	Analyse Préliminaire des Risques
ATC	Automatic Train Control
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ATS	Automatic Train Supervision
BEA	Bureau Enquête Analyse
BPMN	Business Process Model and Notation
CDV	Circuit De Voie
CIFRE	Convention Industrielle de Formation par la REcherche
CREG	Chef de RÉGulation
DSO	Départ Sur Ordre
FRAM	Functional Resonance Analysis Method
GMEC	Generalized Mutual Exclusion Constraints
HT	Hors Tension
IHM	Interface Homme Machine
ISF	Instruction de Sécurité Ferroviaire
LAAS	Laboratoire d'Analyse et d'Architecture des Systèmes
OMG	Object Management Group
PA	Pilote Automatique
PCC	Poste de Commande Centralisé
PRF	Permanent des Réseaux Ferrés
PV	Personne sur les Voies
RATP	Régie Autonome des Transports Parisiens
RdP	Réseau de Petri
SART	Système d'Aide à la Régulation du Trafic
SCADA	Supervisory Control And Data Acquisition
SED	Systèmes à Événements Discrets
ST	Sous Tension
TCS	Théorie du Contrôle par Supervision
UML	Unified Modeling Language
XML	eXtensible Markup Language

Liste des notations

Notation	Signification	Définition
$G = (Q, \Sigma, \delta, q_0, Q_m)$	Automate à états fini et déterministe	7 - p.98
Q	Ensemble fini des états	
Σ	Ensemble non vide et fini des événements	
δ	Application telle que $\delta : Q \times \Sigma \rightarrow Q$	
$q_0 \in Q$	État initial	
$Q_m \subseteq Q$	Ensemble des états finaux ou marqués	
Σ_c	Ensemble des événements contrôlables	8 - p.98
Σ_{uc}	Ensemble des événements incontrôlables	
Σ_{uc}^*	Ensemble des séquences d'événements tous incontrôlables	
$\sigma \in \Sigma$	Événement	
Q_{danger}	Ensemble des états de danger	9 - p.99
Q_s	Ensemble des états sécuritaires	11 - p.100
Q_d	Ensemble des états dangereux	10 - p.100
Q_{cr}	Ensemble des états critiques	14 - p.102
Q_n	Ensemble des états nominaux	13 - p.100
Q_{re}	Ensemble des états redoutés	15 - p.103
Q_{mess}	Ensemble des états où un message sera transmis	
Q_{fr}	Ensemble des états frontières	17 - p.112
$Q_{fr_{amont}}$	Ensemble des états frontières amont	22 - p.114
$Q_{fr_{aval}}$	Ensemble des états frontières aval	28 - p.117
Q_{amont}	Ensemble des états amont	23 - p.114
Q_{aval}	Ensemble des états aval	29 - p.117
Δ_p	Ensemble des transitions à proscrire	16 - p.104
Δ_{fr}	Ensemble des transitions frontières	
Δ_{Rouge}	Ensemble des transitions Rouge	
Δ_{Bleue}	Ensemble des transitions Bleue	
Δ_{Jaune}	Ensemble des transitions Jaune	
$\Delta_{Violette}$	Ensemble des transitions Violette	
Δ_{Verte}	Ensemble des transitions Verte	
$\Delta_{Rouge_{fr}}$	Ensemble des transitions Rouge frontières	18 - p.112
$\Delta_{Jaune_{fr}}$	Ensemble des transitions Jaune frontières	19 - p.112
$\Delta_{Violette_{fr}}$	Ensemble des transitions Violette frontières	20 - p.113
$\Delta_{Verte_{fr}}$	Ensemble des transitions Verte frontières	21 - p.113
$\Delta_{Bleue_{amont}}$	Ensemble des transitions Bleue amont	24 - p.115
$\Delta_{Jaune_{amont}}$	Ensemble des transitions Jaune amont	25 - p.115
$\Delta_{Violette_{amont}}$	Ensemble des transitions Violette amont	26 - p.115

Notation	Signification	Définition
$\Delta_{Verte_{amont}}$	Ensemble des transitions Verte amont	27 - p.115
$\Delta_{Jaune_{aval}}$	Ensemble des transitions Jaune aval	30 - p.118
$\Delta_{Violette_{aval}}$	Ensemble des transitions Violette aval	31 - p.118
$\Delta_{Verte_{aval}}$	Ensemble des transitions Verte aval	32 - p.118

Annexe

Sommaire

A Graphe espace-temps de l'ATS Thales

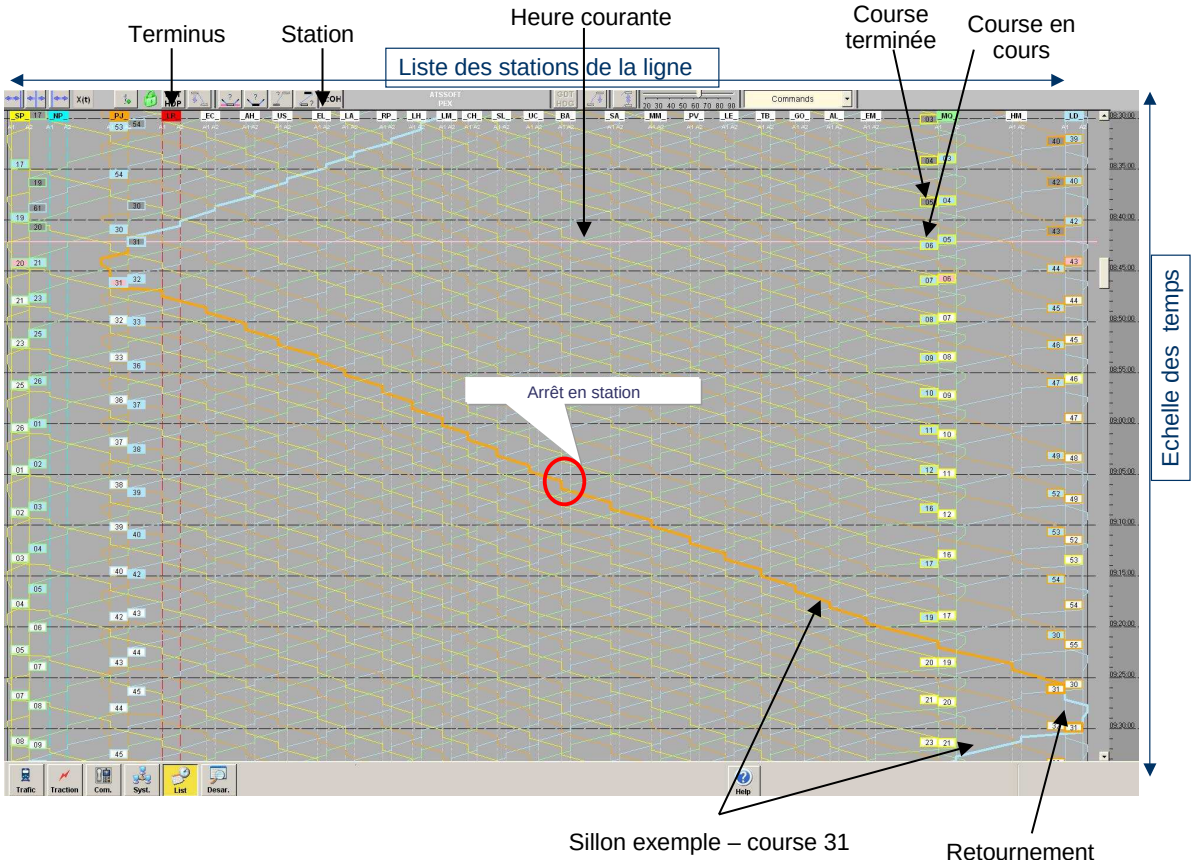


Figure A1 – ATSsoft - Graphe espace-temps

B Comparaison BPMN / UML : Commande d'une pizza

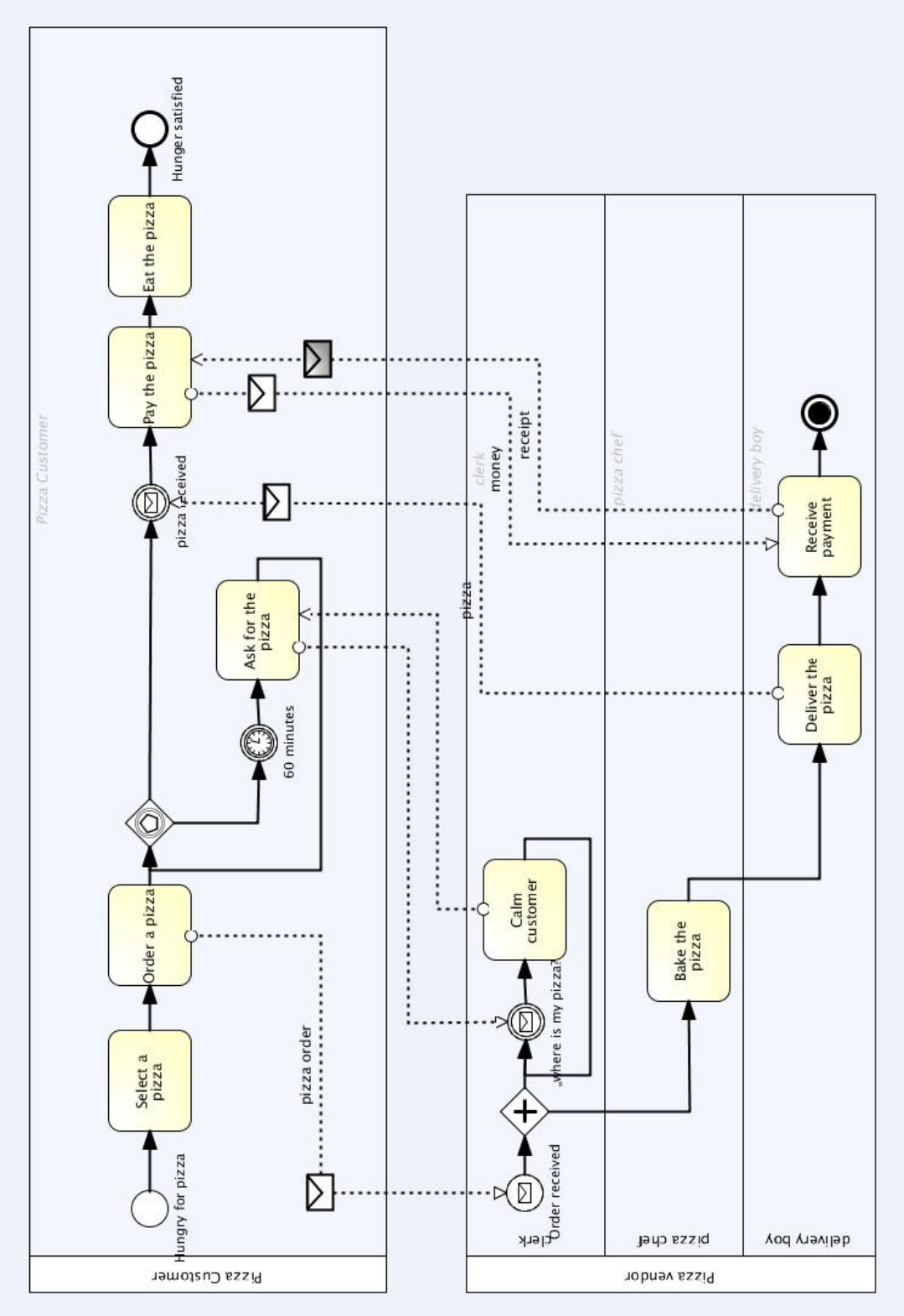


Figure B2 – BPMN [OMG10]

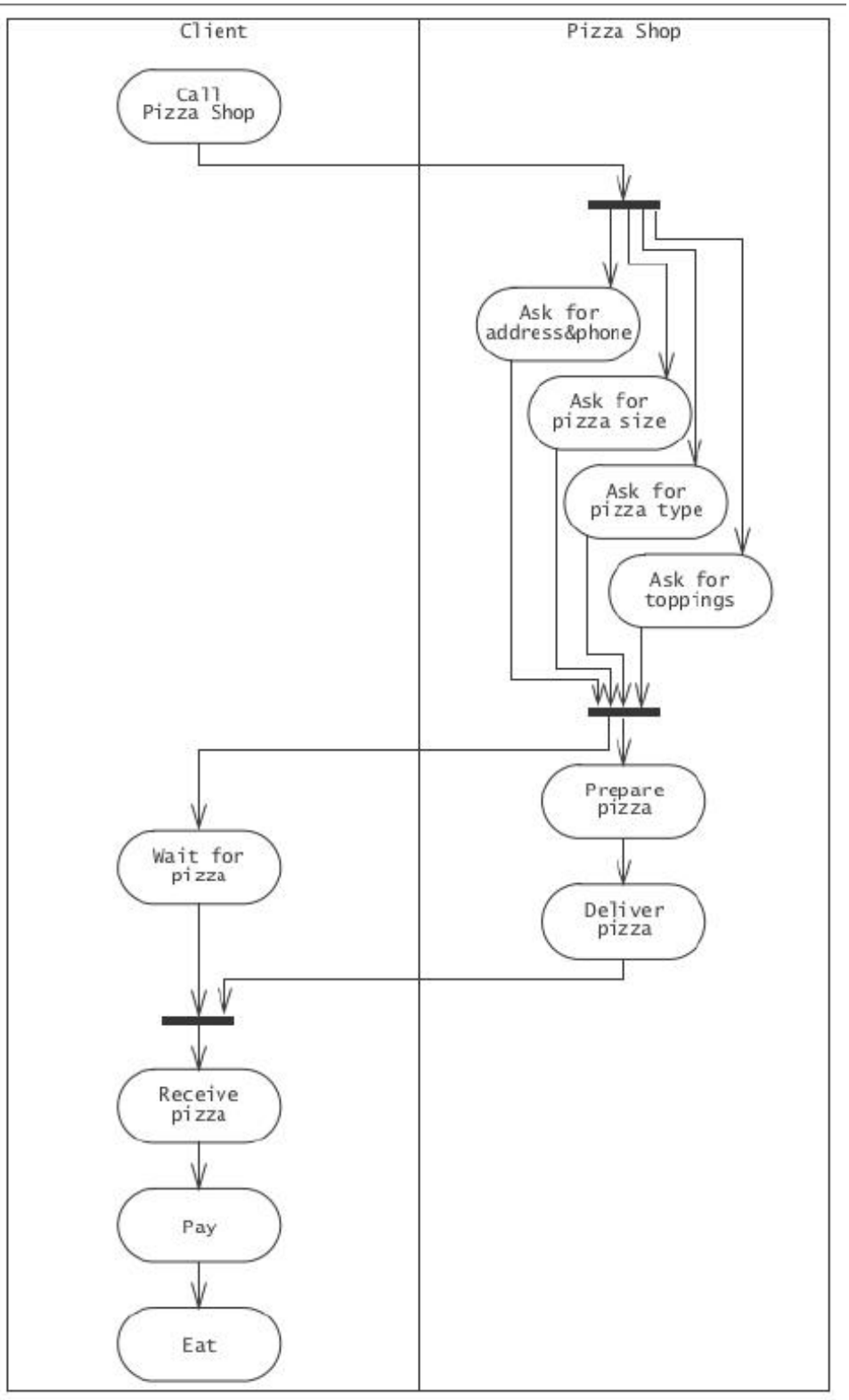


Figure B3 – UML [Ser14]

C Procédures BPMN

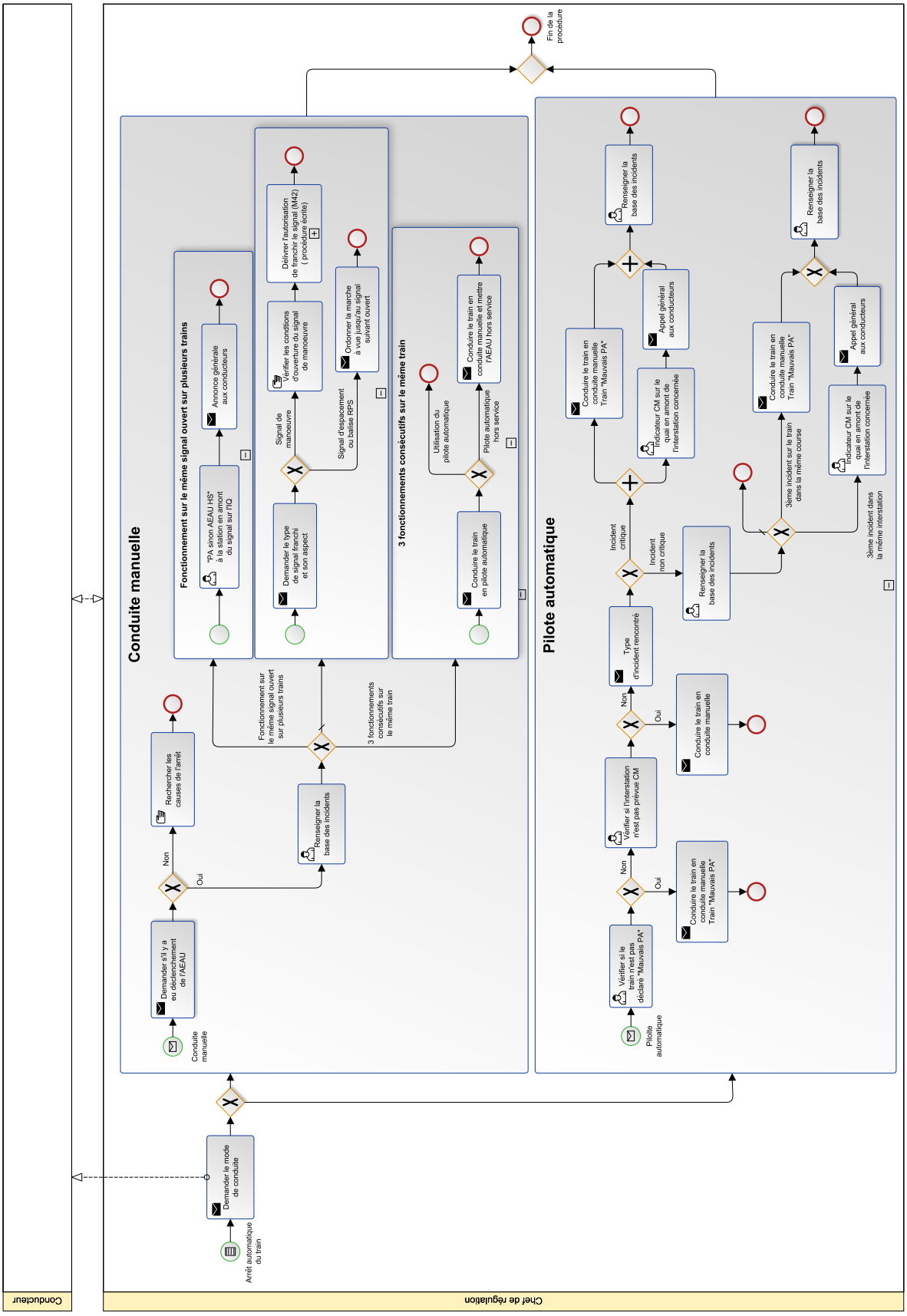


Figure C4 – Procédure BPMN *Arrêt automatique du train*

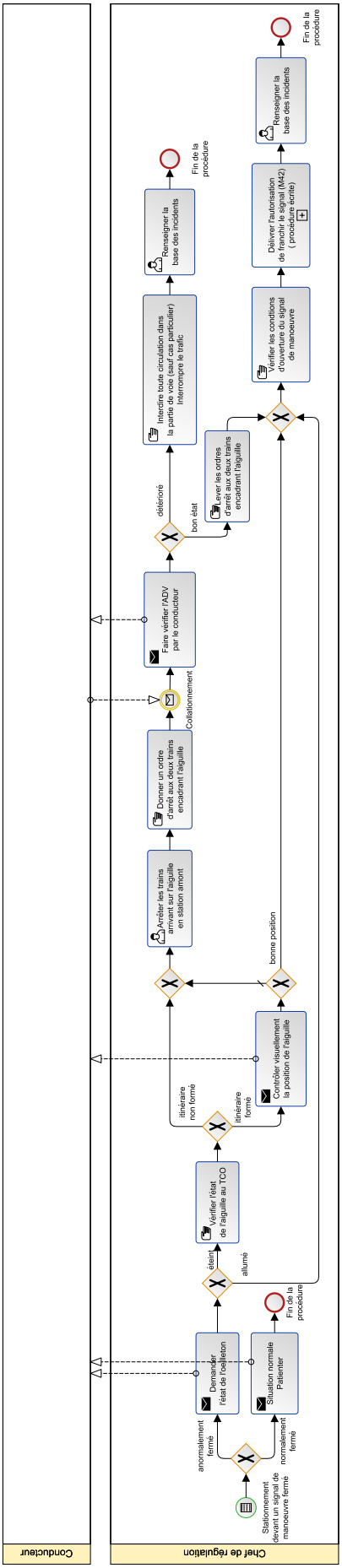


Figure C5 – Procédure BPMN *Non ouverture d'un signal de manœuvre*

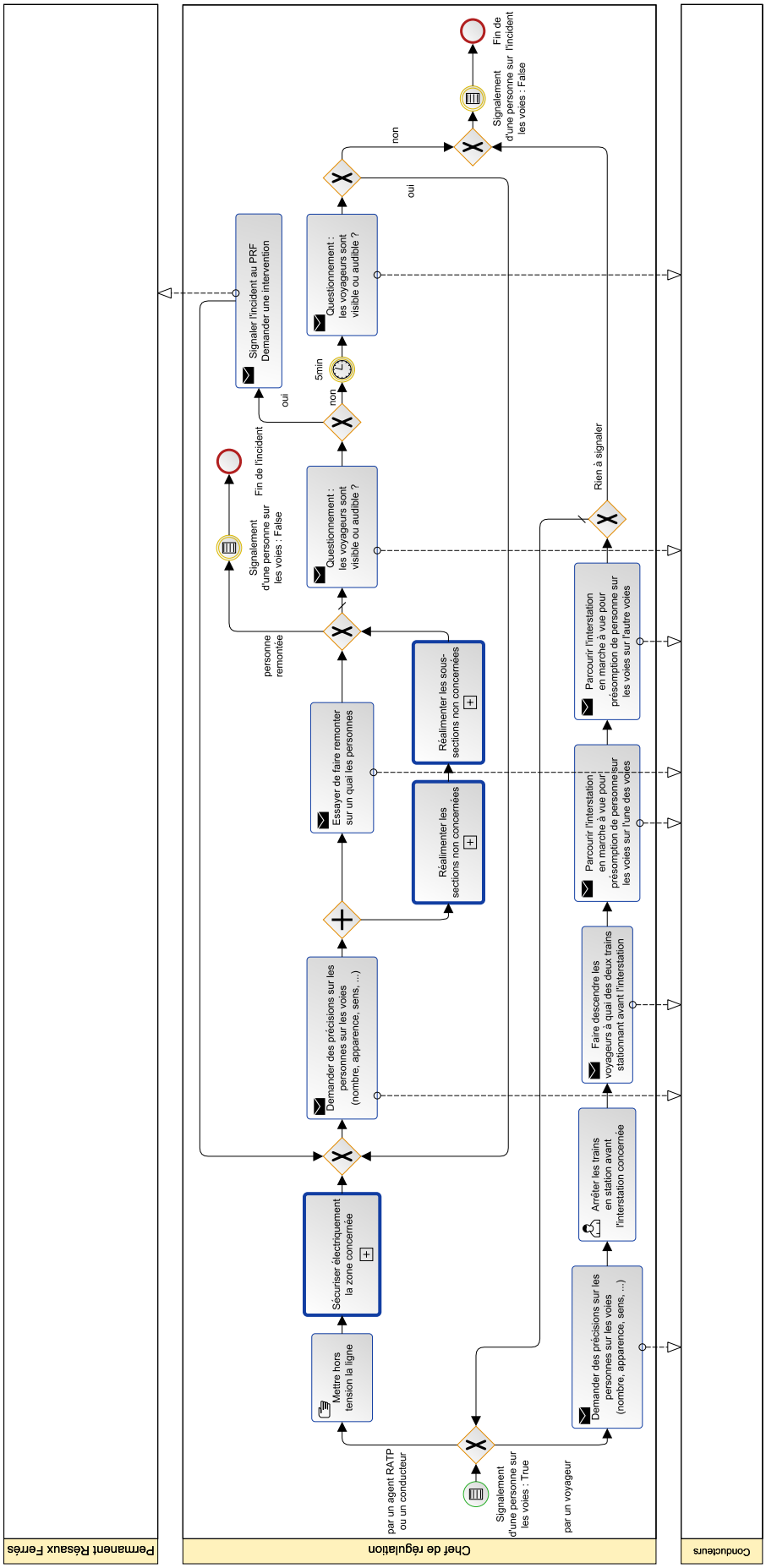


Figure C6 – Procédure BPMN *Signalement d'une personne sur les voies*

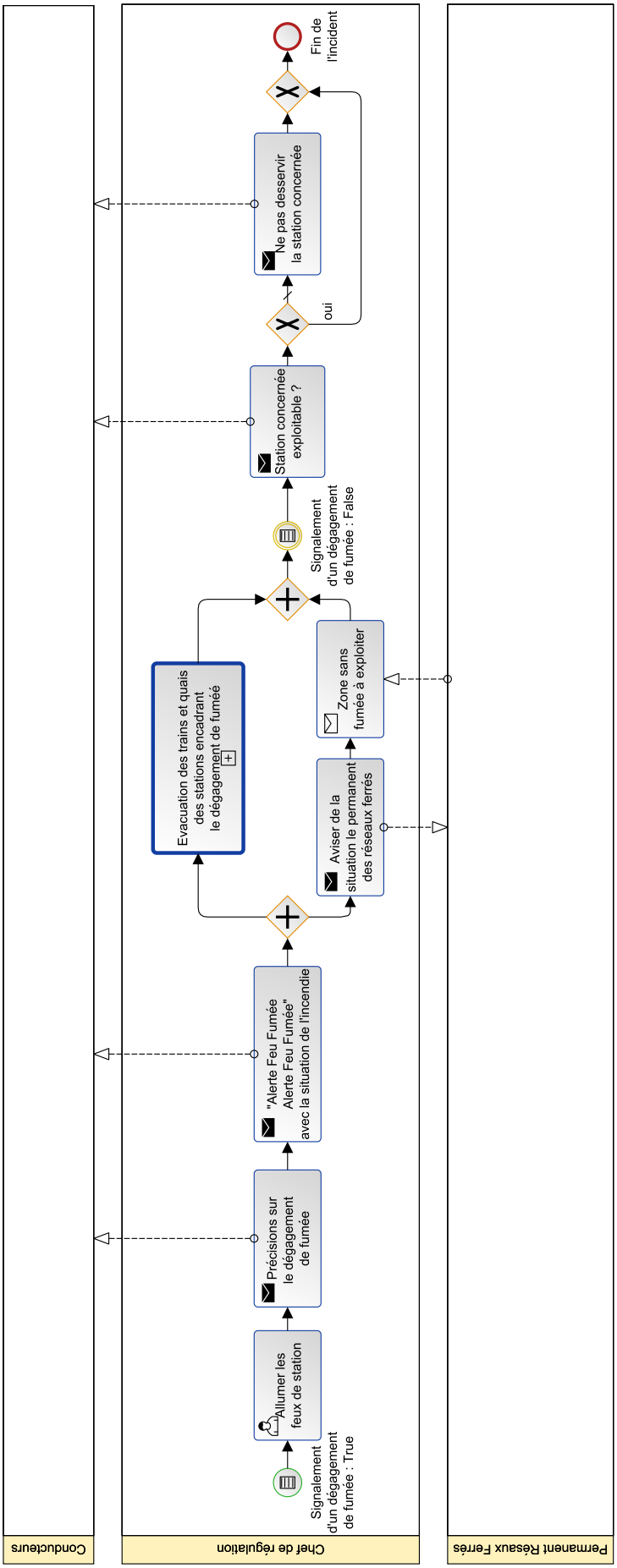


Figure C7 – Procédure BPMN *Alerte Feu Fumée*

D Réseaux de Petri

Références : [Dia13] [Cas99] [Mur89]

Un Réseau de Petri (RdP) est un ensemble de places, notées graphiquement par des cercles, et de transitions, notées graphiquement par des barres ou des rectangles. Des arcs orientés porteurs de poids relient les places aux transitions et les transitions aux places en suivant toujours ce type d'enchaînement. Dans cette structure, des jetons ou marques se déplacent et sont susceptibles de franchir les transitions selon certains critères de franchissement qui seront explicités ultérieurement.

La figure D8 représente un réseau de Petri avec trois places P1, P2 et P3 et trois transitions T1, T2 et T3 qui s'enchainent de manière cyclique, avec des arcs de poids égaux à un et avec une unique marque dans la place $P1$.

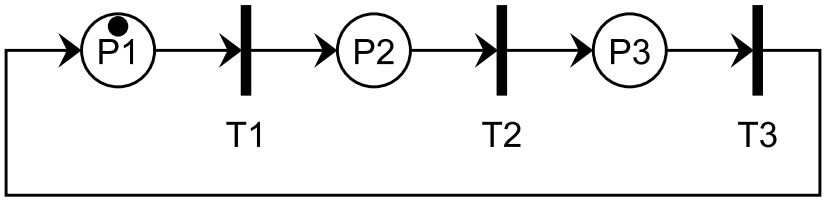


Figure D8 – Exemple d'un réseau de Petri

Définition 33 (Définition formelle) *Un réseau de Petri R se définit comme un quadruplet $R = (P, T, Pré, Post)$ avec :*

- $P = \{P_1, P_2, ..., P_n\}$ *un ensemble fini non vide de places,*
- $T = \{T_1, T_2, ..., T_m\}$ *un ensemble fini non vide de transitions,*
- $Pré : P \times T \to \mathbb{N}$ *une application d'incidence avant où* $Pré(P_i, T_j)$ *correspond au poids de l'arc en amont de la transition* T_j*,*
- $Post : T \times P \to \mathbb{N}$ *une application d'incidence arrière où* $Post(T_i, P_j)$ *correspond au poids de l'arc en aval de la transition* T_i*,*

Si tous les poids sont égaux à 1, le réseau est appelé réseau de Petri ordinaire. Inversement s'il existe au moins un poids supérieur à 1, le réseau est appelé réseau de Petri généralisé.

D.1 Marquage

Définition 34 (Marquage) *Le marquage d'un réseau de Petri est une fonction $M : P \to \mathbb{N}$ qui associe à chaque place le nombre de marques qu'elle contient. Le marquage initial d'un réseau de Petri est noté M_0.*

Cette fonction est représentée graphiquement en plaçant des marques dans les places du réseau de Petri. Ainsi, une place peut être soit marquée si elle possède une ou plusieurs marques, soit non marquée si elle est vide. Ces marques sont indivisibles et infusionnables.

Définition 35 (Réseau de Petri sauf) *Un réseau de Petri est dit sauf pour un marquage initial M_0 si et seulement si le nombre de marques dans chacune des places est borné par 1.*

D.2 Évolution

L'évolution d'un RdP correspond à l'évolution de son marquage au cours du temps et donc à l'évolution de l'état du système. Elle se traduit par un déplacement de marques entre les places du RdP, déterminer l'évolution d'un RdP correspond en fait à le simuler en réalisant l'ensemble des déplacements des marques possibles.

Définition 36 (Sensibilisation d'une transition) *Une transition T_i est dite sensibilisée ou franchissable si et seulement si toutes les places d'entrée, celles précédant immédiatement T_i, possèdent au moins un nombre de marques égal au poids de l'arc correspondant.*

Définition 37 (Franchissement d'une transition) *Une transition peut être franchie si et seulement si elle est sensibilisée.*

Le franchissement d'une transition conduit à un changement du marquage. Le passage du marquage M_k au marquage M_l par franchissement de la transition T_{kl} est noté : $M_k \stackrel{T_{kl}}{\rightarrow} M_l$. À partir d'un même marquage, il peut être possible de franchir plusieurs transitions, menant ainsi à des marquages différents. L'ensemble des marquages accessibles à partir du marquage M_0 est l'ensemble des marquages obtenus à partir de M_0 par franchissements successifs d'une ou plusieurs transitions.

Définition 38 (Séquence de franchissements) *Une séquence de franchissement $\mathscr{S}$ est une suite de transitions telles que le franchissement de chacune d'elles conduit à la sensibilisation de la suivante pour passer d'un marquage M_i à un marquage M_j : $M_i \stackrel{\mathscr{S}}{\rightarrow} M_j$.*

Lors du franchissement d'une transition, toujours supposé instantané, un nombre de marques égal au poids respectif de l'arc reliant la place à la transition est prélevé dans chacune des places d'entrée et un nombre de marques égal au poids respectif de l'arc reliant la transition à la place est déposé dans chacune des places de sortie. Dans un réseau de Petri, plusieurs transitions franchissables ne sont jamais franchies simultanément, l'évolution du RdP se fait donc par le franchissement d'une seule transition à la fois. Quand plusieurs transitions sont simultanément franchissables, il n'est pas possible de savoir dans quel ordre elles seront effectivement franchies, l'évolution n'est donc pas unique.

D.3 Graphe d'accessibilité

Définition 39 (État accessible) *Un état E' est accessible à partir d'un état E s'il existe une séquence de franchissement menant de E à E'. Le marquage associé à un état accessible du réseau de Petri est appelé marquage accessible.*

Définition 40 (Ensemble des marquages accessibles) *L'ensemble des marquages accessibles $\mathscr{M}(R, M_0)$ d'un réseau de Petri R avec le marquage initial M_0 se définit par le plus petit ensemble :*

$$M_0 \in \mathscr{M} \text{ et si } M_i \in \mathscr{M} \text{ et } M_i \stackrel{T_{ij}}{\rightarrow} M_j \text{ alors } M_j \in \mathscr{M}.$$

L'ensemble A définit l'ensemble des marquages accessibles par un ensemble de vecteurs indiquant le nombre de marques dans chaque place du réseau.

Définition 41 (Graphe des marquages) *Si l'ensemble des marquages accessibles est fini, le graphe des marquages accessibles $G(R, M_0)$ d'un réseau de Petri R avec le marquage initiale M_0 est défini comme le graphe dont les nœuds sont les marquages accessibles de $\mathscr{M}(R, M_0)$ et les arcs sont le libellé des transitions impliquées dans les tirs menant d'un marquage à un autre.*

D.4 Représentation matricielle

Matrice d'incidence

Un réseau de Petri se définit formellement par $R = (P, T, Pré, Post)$ (voir définition 33, page 163), il existe également une représentation matricielle. Ainsi, pour un réseau de Petri généralisé, deux matrices à coefficients entiers positifs ou nuls sont définies : $C^-(p,t)$, la matrice d'entrée ou matrice PRE, et $C^+(p,t)$, la matrice de sortie ou matrice POST. La matrice $C^-(p,t)$ fait le bilan des arcs amont aux transitions, et la matrice $C^+(p,t)$ fait le bilan des arcs aval aux transitions, le nombre de lignes est égal au nombre de places et le nombre de colonnes est égal au nombre de transitions. Une intersection (p,t) dans $C^-(p,t)$ correspond à la pondération associée à l'arc menant de la place p à la transition t, tandis qu'une intersection (p,t) dans $C^+(p,t)$ correspond à la pondération associée à l'arc menant de la transition t à la place p.

Définition 42 (Matrice d'incidence) *Pour un un réseau de Petri R pur (sans boucle élémentaire) et fortement connexe, la matrice d'incidence $C(p,t)$ est définie par :*

$$\forall p \in P, \forall t \in T : C(p,t) = C^+(p,t) - C^-(p,t)$$

La matrice $C(p,t)$ seule ne représente que la structure du réseau de Petri, c'est-à-dire le réseau non marqué. Les propriétés obtenues avec cette matrice sont donc des propriétés structurelles car indépendantes du marquage initial M_0. Cette matrice fait le bilan des incidences du tir de chaque franchissement des transitions. Une colonne de cette matrice correspond à la modification du marquage apporté par le franchissement de la transition correspondante.

Grâce à la matrice d'incidence, il est possible de calculer le marquage M_k d'un réseau de Petri obtenu par le franchissement d'une séquence de transitions $\mathscr{S}$ à partir du marquage M_i (voir définition 38).

Définition 43 (Relation générale des RdP) *Soient M_k et M_i deux marquages accessibles d'un réseau de Petri R et $\mathscr{S}$ une séquence de franchissement tel que : $M_i \xrightarrow{\mathscr{S}} M_k$, alors :*

$$M_k = M_i + C(p,t).\mathscr{S}^T$$

Définition 44 (P semi-flot) *Un P semi-flot est un vecteur $Y \neq 0$ de dimension égale au nombre de places du réseau de Petri et à composantes entières strictement positives ou nulles tel que :*

$$Y^T.C(p,t) = 0$$

Un P semi-flot est dit élémentaire s'il ne couvre pas strictement un autre P semi-flot.

Propriétés d'un réseau de Petri

Définition 45 (Réseau de Petri conservatif) *Un réseau de Petri est dit conservatif s'il existe un P semi-flot complet, c'est-à-dire à composantes entières toutes positives.*

Définition 46 (Réseau de Petri réinitialisable) *Un RdP est réinitialisable si à partir de chaque marquage, il existe toujours une séquence franchissable permettant d'atteindre le marquage initial du modèle.*

Définition 47 (Réseau de Petri vivant) *Un RdP est vivant s'il est tout le temps possible d'atteindre tous les marquages.*

Exemple

Pour le réseau de Petri figure D9 :

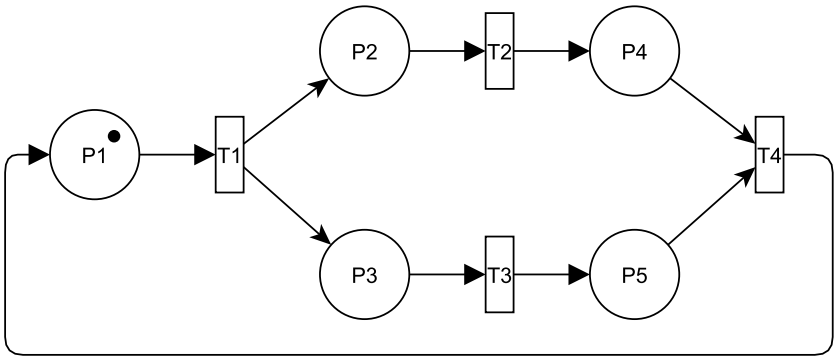


Figure D9 – Exemple d'un réseau de Petri

$$C^+(p,t) = \begin{array}{c} \\ P_1 \\ P_2 \\ P_3 \\ P_4 \\ P_5 \end{array} \begin{array}{c} \begin{array}{cccc} T_1 & T_2 & T_3 & T_4 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array} \qquad C^-(p,t) = \begin{array}{c} \\ P_1 \\ P_2 \\ P_3 \\ P_4 \\ P_5 \end{array} \begin{array}{c} \begin{array}{cccc} T_1 & T_2 & T_3 & T_4 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

$$C(p,t) = C^+(p,t) - C^-(p,t) = \begin{array}{c} \\ P_1 \\ P_2 \\ P_3 \\ P_4 \\ P_5 \end{array} \begin{array}{c} \begin{array}{cccc} T_1 & T_2 & T_3 & T_4 \end{array} \\ \begin{pmatrix} -1 & 0 & 0 & 1 \\ 1 & -1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \end{array}$$

Ce réseau de Petri a deux P semi-flots :

$$Y_1^T = [1\ 1\ 0\ 1\ 0] \qquad Y_2^T = [1\ 0\ 1\ 0\ 1]$$

$$Support(Y_1) = \{P_1, P_2, P_4\} \text{ et } Card(Support(Y_1)) = 3$$

E Graphe orienté et composante fortement connexe

Références : [Mon06]

Soit $G = (S, A)$ un graphe orienté avec S l'ensemble des sommets et A l'ensemble des arcs reliant les sommets. Un automate à états fini est un graphe orienté dans lequel les sommets sont des états, les arcs sont des transitions et où sont définis un état initial et un ensemble d'états finaux.

Définition 48 (Chemin - Graphe orienté) *Un chemin C est une suite (S_n) de sommets d'un graphe orienté $G = (S, A)$ tel que deux sommets consécutifs quelconque S_i et S_{i+1} sont reliés par un arc de G : $\forall i, 0 \leq i \leq n-1, (S_i, S_{i+1}) \in A$*

Les sommets S_0 et S_n sont respectivement l'origine et l'extrémité du chemin C.

Le chemin C est formé de $n+1$ sommets et de n arcs mis bout à bout, sa longueur est n.

Un chemin peut comporter un seul sommet.

Définition 49 (Circuit - Graphe orienté) *Un circuit H est un chemin de longueur non nulle dont le sommet d'origine et le sommet d'extrémité sont identiques.*

Définition 50 (Composante fortement connexe - Graphe orienté) *Une composante fortement connexe $\mathscr{C}$ d'un graphe $G = (S, A)$ est un sous-ensemble maximal de sommets tels que deux quelconques sommets d'entre eux soient reliés par un chemin.*

Si $x \in \mathscr{C}$, alors :

$\forall y \in \mathscr{C}$, il existe un circuit passant par x et y,

$\forall z \in S \backslash \mathscr{C}$, il n'existe pas de circuit passant par x et z.

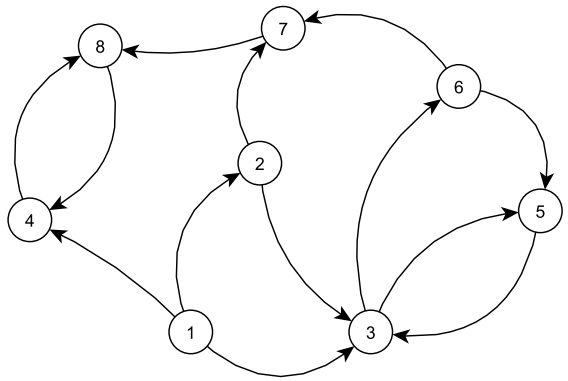


Figure E10 – Exemple d'un graphe orienté

Dans le graphe orienté de la figure E10 :
- {6, 7, 8} et {2} sont des chemins,
- {1, 3, 4} n'est pas un chemin,
- {3, 6, 5} est un circuit et une composante fortement connexe,
- {4, 8} et {2} sont des composantes fortement connexes.

F Messages transmis à l'opérateur de supervision

Signalement d'incident		Ressource			Procédure		Message	
Dégagement de fumée	Personne sur les voies	Alimentation	Position	Feux de station	Alerte Feu Fumée	Signalement Personne sur les voies	Alerte	Couleur transition / Conseil
Fumee_P	PersV_P	ST	Tunnel	FSallume	AFF3	PV2	MiseHT / PVbj	Violet / EntStation
Fumee_P	PersV_P	ST	Station	FSallume	AFF1	PV2		Vert / PVbj
Fumee_P	PersV_P	ST	Station	FSallume	AFF3	PV2		Vert / PVbj
Fumee_P	PersV_P	ST	Tunnel	FSallume	AFF4	PV1		Violet / AFFd
Fumee_P	PersV_P	ST	Station	FSallume	AFF4	PV2		Vert / PVbj
Fumee_P	PersV_P	ST	Station	FSallume	AFF4	PV1		Vert / MiseHT
Fumee_P	PersV_P	HT	Tunnel	FSallume	AFF2	PV1	PVa	Violet / MiseST
Fumee_P	PersV_P	ST	Station	FSeteint	AFF2	PV2		Vert / PVbj
Fumee_P	PersV_P	ST	Tunnel	FSallume	AFF2	PV2	MiseHT / PVbj	Violet / EntStation
Fumee_P	PersV_P	HT	Tunnel	FSallume	AFF3	PV1	PVa	Violet / MiseST
Fumee_P	PersV_P	ST	Station	FSallume	AFF2	PV2		Vert / PVbj
Fumee_P	PersV_P	HT	Tunnel	FSallume	AFF4	PV1	PVa	Violet / MiseST
Fumee_P	PersV_P	ST	Tunnel	FSallume	AFF4	PV2	MiseHT / PVbj	Violet / EntStation
Fumee_P	PersV_P	ST	Station	FSallume	AFF3	PV1		Vert / MiseHT
Fumee_P	PersV_P	HT	Tunnel	FSallume	AFF1	PV1	PVa	Violet / MiseST
Fumee_P	PersV_P	ST	Tunnel	FSallume	AFF2	PV2	MiseHT / PVbj	Violet / EntStation
Fumee_P	PersV_P	HT	Tunnel	FSeteint	AFF2	PV1	PVa	Violet / MiseST
Fumee_P	PersV_P	ST	Tunnel	FSallume	AFF3	PV1		Violet / EntStation
Fumee_P	PersV_P	ST	Tunnel	FSeteint	AFF2	PV2	MiseHT / PVbj	Violet / EntStation
Fumee_P	PersV_P	ST	Station	FSallume	AFF1	PV1		Vert / MiseHT
Fumee_P	PersV_P	ST	Station	FSeteint	AFF1	PV2		Vert / PVbj
Fumee_P	PersV_P	ST	Station	FSallume	AFF2	PV1		Vert / MiseHT
Fumee_P	PersV_P	ST	Station	FSeteint	AFF2	PV1		Vert / MiseHT
Fumee_P	PersV_P	ST	Tunnel	FSallume	AFF1	PV1		Violet / AFFa
Fumee_P	PersV_P	ST	Tunnel	FSeteint	AFF1	PV2	MiseHT / PVbj	Violet / EntStation
Fumee_P	PersV_P	ST	Station	FSeteint	AFF1	PV1		Vert / MiseHT
Fumee_P	PersV_P	ST	Tunnel	FSeteint	AFF1	PV1		Violet / AFFa
Fumee_P	PersV_P	HT	Tunnel	FSeteint	AFF1	PV1	PVa	Violet / MiseST
Fumee_P	PersV_P	ST	Tunnel	FSeteint	AFF2	PV1		Violet / AFFbi

Figure F11 – Messages transmis à l'opérateur

Bibliographie

[Aal98] W.M.P. Aalst : Three good reasons for using a Petri-net-based workflow management system. *Information and Process Integration in Enterprises*, pages 161–182, 1998.

[Ake99] K. Akesson et M. Fabian : Implementing supervisory control for chemical batch processes. *In Proceedings of IEEE Conference on Control Applications, Hawaii, USA*, 1999.

[Ake06] O. Akerlund, P. Bieber, E. Boede, M. Bozzano, M. Bretschneider, C. Castel, A. Cavallo, M. Cifaldi, J. Gauthier, A. Griffault *et al.* : ISAAC, a framework for integrated safety analysis of functional, geometrical and human aspects. *In European Congress on Embedded Real Time Software (ERTS 2006), Toulouse, France*, 2006.

[Alb01] S. Albert et R.D. Kinley : Multivariate statistical monitoring of batch processes : an industrial case study of fermentation supervision. *TRENDS in Biotechnology*, 19(2):53–62, 2001.

[Amo12] J. Amory et A. Cointet : Le transfert de voyageurs quai - train dans le métro parisien. *In 18e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Tours, France*, 2012.

[Arn09a] Y. Arnaud, J.L. Boimond, J. Cury, J.J. Loiseau, C. Martinez *et al.* : Using UPPAAL for the secure and optimal control of agv fleets. *In Acts of the 7th Workshop on Advanced Control and Diagnosis ACD09, Zielona Góra, Pologne*, 2009.

[Arn09b] Y. Arnaud, J. Cury, JJ Loiseau, C. Martinez *et al.* : Pilotage sûr et optimal d'une flotte de véhicules autoguidés. *In Actes des 3e Journées Doctorales MACS, Angers, France*, 2009.

[Bal05] F. Balbo et S. Pinson : Dynamic modeling of a disturbance in a multi-agent system for traffic regulation. *Decision Support Systems*, 41(1):131–146, 2005.

[BEA12] Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile BEA : Rapport final, accident survenu le 1er juin 2009 à l'Airbus A330, Rio de Janeiro Paris. Rapport technique, Ministère de l'Écologie, du Développement durable et de l'Energie, 2012.

[Bel06] F. Belmonte, J.L. Boulanger, W. Schon et K. Berkani : Automatic supervision survey for SpicaRail program. *In EAM 06 European Annual Conference on Human Decision-Making and Manual Control, Valenciennes, France*, 2006.

[Bel08a] M. Belmonte, G. Churchill, W. Schon, J.L. Boulanger *et al.* : Automatisation intégrale de la ligne 1 : étude et modélisation du trafic mixte. *In 16e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Avignon, France*, 2008.

[Bel08b] F. Belmonte, W. Schon, J.L. Boulanger, R. Capel *et al.* : Evaluation du facteur humain dans le domaine de la supervision de trafic ferroviaire : le projet SpicaRail. *In 16e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Avignon, France*, 2008.

[Bel11] F. Belmonte, W. Schon, L. Heurley et R. Capel : Interdisciplinary safety analysis of complex socio-technological systems based on the functional resonance accident model : An application to railway traffic supervision. *Reliability Engineering and System Safety*, 96(2):237–249, 2011.

[Beu06] J. Beugin : *Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé*. Thèse de doctorat, Université de Valenciennes, 2006.

[Bho10] N. Bhouri, F. Balbo et S. Pinson : A multi-agent system to regulate bimodal urban traffic. *In 13th International IEEE Conference Intelligent Transportation Systems (ITSC), Madeira Island, Portugal*, 2010.

[Blo00] S. Blouin, M Guay et K. Rudie : An application of discrete-event theory to truck dispatching. Rapport technique, Department of Computing and Information Science, Queen's University, Ontario, Canada, 2000.

[Bou05] A. Boufaden, L. Piétrac et S. Gabouj : L'usage des réseaux de Petri dans la théorie de contrôle par supervision. *Sciences et Technologies de l'Automatique (e-STA), revue électronique de la SEE*, 2:10p, 2005.

[Bra90] R.D. Brandt, V. Garg, R. Kumar, F. Lin, S.I. Marcus et W.M. Wonham : Formulas for calculating supremal controllable and normal sublanguages. *Systems and Control Letters*, 15(2):111–117, 1990.

[Bra00] B. Brandin, R. Malik et P. Dietrich : Incremental system verification and synthesis of minimally restrictive behaviours. *In American Control Conference, Chicago, USA*. IEEE, 2000.

[Bre08] J.J. Breuils et G. Dupin : Un réferentiel d'évaluation des risques du système de transport métro. *In 16e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Avignon, France*, 2008.

[Bre97] P. Brezillon, C. Gentile, I. Saker et M. Secron : SART : A system for supporting operators with contextual knowledge. *In Interdisciplinary Conference on Modeling and Using Context (CONTEXT-97), Rio de Janeiro, Brazil*, 1997.

[Bre00a] P. Brezillon, R. Naveiro, M. Cavalcanti et J.C. Pomerol : SART : an intelligent assistant system for subway control. *Pesquisa Operacional*, 20(2):247–268, 2000.

[Bre00b] P. Brezillon, L. Pasquier et J.C. Pomerol : Reasoning with contextual graphs. *European Journal of Operational Research*, 136(2):290–298, 2000.

[Bre03] P. Brezillon : Représentation de pratiques dans le formalisme des graphes contextuels. *In Actes des 2e Journées d'Etude en Psychologie Ergonomique–EPIQUE, Boulogne-Billancourt, France*, 2003.

[Bre07] P. Brezillon et D. Racoceanu : A context model for content based medical image retrieval. *Medical Imaging Technology*, 25(5):327–332, 2007.

[Car08] O. Carton : *Langages formels, calculabilité et complexité.* Vuibert, 2008.

[Cas99] C.G. Cassandras et S. Lafortune : *Introduction to discrete event systems.* Boston, MA : Springer Science, 1999.

[Caz09] T. Cazenave, F. Balbo et S. Pinson : Monte-carlo bus regulation. *In 12th International IEEE Conference on Intelligent Transportation Systems, St. Louis, USA*, 2009.

[Che09] A.B. Cheikh, D. Rieu *et al.* : Une méthode de rétro-ingénierie des processus métier basée sur un méta-modèle multi-vues. *In 27e Congrès INFORSID, Toulouse, France*, 2009.

[Cla12] L.B. Clavijo, J.C. Basilio et L.K. Carvalho : DESLAB : A scientific computing program for analysis and synthesis of discrete-event systems. *Discrete Event Systems*, 11(1):349–355, 2012.

[Dav05] P. Davidsson, L. Henesey, L. Ramstedt, J. Törnquist et F. Wernstedt : An analysis of agent-based approaches to transport logistics. *Transportation Research part C : emerging technologies*, 13(4):255–271, 2005.

[dBr98] G. de Brito : Study of the use of Airbus flight-deck procedures and perspectives for operational documentation. *In Proceedings of HCI-Aero'98, Montreal, Canada*, 1998.

[dBr99] G. de Brito et G. Boy : Situation awareness and procedure following. *In Proceedings of CSAPC'99, Lille, France*, 1999.

[Deg97] A. Degani et E.L. Wiener : Procedures in complex systems : The airline cockpit. *Systems, Man and Cybernetics, Part A : Systems and Humans, IEEE*, 27(3):302–312, 1997.

[Dia13] M. Diaz : *Petri nets : fundamental models, verification and applications.* John Wiley and Sons, 2013.

[Did07] A. Dideban : *Synthèse de contrôleurs discrets par simplification de contraintes et de conditions.* Thèse de doctorat, Université Joseph Fourier, Grenoble, 2007.

[Did08] A. Dideban et H. Alla : Reduction of constraints for controller synthesis based on safe Petri nets. *Automatica*, 44(7):1697–1706, 2008.

[Did13] A. Dideban, M. Zareiee et H. Alla : Controller synthesis with highly simplified linear constraints. *Asian Journal of Control*, 15(1):80–94, 2013.

[Dij08] R.M. Dijkman, M. Dumas et C. Ouyang : Semantics and analysis of business process models in BPMN. *Information and Software Technology*, 50(12):1281–1294, 2008.

[Dji06] S. Djibo, G. Vallery et A. Lancry : Charge mentale et régulation de systèmes complexes. *@ctivités*, 3(1):117–139, 2006.

[Ena93] F. Enaud et J.C. Grimaldi : L'intégration de systèmes dans la supervision des transports routiers. *L'Onde Electrique*, 73(3):38–41, 1993.

[Ezz08] H. Ezzedine, T. Bonte, C. Kolski et C. Tahon : Integration of traffic management and traveller information systems : basic principles and case study in intermodal transport system management. *International Journal of Computers, Communications and Control (IJCCC)*, 3:281–294, 2008.

[Far10] G. Faraut : *Commutations sûres de mode pour les systèmes à événements discrets.* Thèse de doctorat, INSA de Lyon, 2010.

[Foo96] R. Foot : La représentation du voyageur et la RATP : une analyse par les dispositifs de transport. *Cahier de recherche du Gip Mutation industrielles*, 70:15–26, 1996.

[Gau03] B. Gaudin et H. Marchand : Modular supervisory control of asynchronous and hierarchical finite state machines. *In European Control Conference, ECC 2003, Cambridge, United Kingdom*, 2003.

[Gau04] B. Gaudin : *Synthèse de contrôleurs sur des systèmes à évènements discrets structurés.* Thèse de doctorat, Université de Rennes 1, 2004.

[Gea12] C.V. Geambasu : BPMN vs. UML : Activity diagram for business process modeling. *Journal of Accounting and Management Information Systems*, 11(4):637–651, 2012.

[Gél10] L. Gély : *Modélisation et optimisation de la gestion opérationnelle des circulations en cas d'aléas.* Thèse de doctorat, Université Sciences et Technologies, Bordeaux I, 2010.

[Gha03a] A. Ghaffari, N. Rezg et X. Xie : Design of a live and maximally permissive Petri net controller using the theory of regions. *IEEE Transactions on Robotics and Automation*, 19(1):137–142, 2003.

[Gha03b] A. Ghaffari, N. Rezg et X. Xie : Feedback control logic for forbidden-state problems of marked graphs : application to a real manufacturing system. *IEEE Transactions on Automatic Control*, 48(1):18–29, 2003.

[Giu92] A. Giua, F. DiCesare et M. Silva : Generalized mutual exclusion contraints on nets with uncontrollable transitions. *In International Conference on Systems, Man and Cybernetics, IEEE, Chicago,* USA, 1992.

[Gue08] F. Guenab, J.L. Boulanger, W. Schon *et al.* : Sécurité des systèmes de contrôle-commande et signalisation ferroviaire : nouvelle approche d'analyse préliminaire des risques. *In 5^{e} Conférence Internationale Francophone d'Automatique CIFA'08, Bucarest, Roumanie*, 2008.

[Haj13] S. Hajjar : *Conception sûre de systèmes embarqués à base de COTS.* Thèse de doctorat, INSA de Lyon, 2013.

[Hel00] K. Hellier : Hazard analysis and critical control points for water supplies. *In Proceedings of 63rd Annual Water Industry Engineers and Operators Conference, Warrnambool, Australia*, 2000.

[Hol90] L.E. Holloway et B.H. Krogh : Synthesis of feedback control logic for a class of controlled Petri nets. *IEEE Transactions on Automatic Control*, 35(5):514–523, 1990.

[Hol97] L.E. Holloway, B.H. Krogh et A. Giua : A survey of Petri net methods for controlled discrete event systems. *Discrete Event Dynamic Systems*, 7(2):151–190, 1997.

[Hol99] E. Hollnagel : Accident analysis and barrier functions. Rapport technique, Svenska Banverket, 1999.

[IRS13] Institut de Radioprotection et de Sûreté Nucléaire IRSN : Accident de Three Mile Island (USA) 1979. Disponible sur : `www.irsn.fr/FR/connaissances/Installations_nucleaires/Les-accidents-nucleaires/three-mile-island-1979`, 2013.

[IRS14] Institut de Radioprotection et de Sûreté Nucléaire IRSN : Accident à la centrale de Fukushima Daiichi (Japon) 2011. Disponible sur : `www.irsn.fr/FR/connaissances/Installations_nucleaires/Les-accidents-nucleaires/accident-fukushima-2011`, 2014.

[Jub10] F. Jubert : Vers une gestion innovante des risques de réalimentation du rail de traction du métro parisien. *In 17e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, La Rochelle, France*, 2010.

[Kam04] O. Kamach : *Approche multi-modèle pour les systèmes à événements discrets : application à la gestion des modes de fonctionnement.* Thèse de doctorat, INSA de Lyon, 2004.

[Kam13] M.A. Kammoun : *Méthodes de modélisation formelles basées sur les systèmes à événements discrets pour le management du trafic aérien.* Thèse de doctorat, Université de Lorraine, 2013.

[Kha03] S. Khalfaoui : *Méthode de recherche des scénarios redoutés pour l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile.* Thèse de doctorat, Institut National Polytechnique de Toulouse-INPT, 2003.

[Kli02] A. Klinke et O. Renn : A new approach to risk evaluation and management : Risk-based, precaution-based and discourse-based strategies. *Risk analysis*, 22(6): 1071–1094, 2002.

[Kom08] D. Komljenovic, W.A. Groves et V.J. Kecojevic : Injuries in US mining operations : a preliminary risk analysis. *Safety Science*, 46(5):792–801, 2008.

[Lak14] M.N. Lakhoua : Analysis and supervision of the water extraction of a thermal power plant. *International Journal of Physical Sciences*, 9(10):243–249, 2014.

[Lee06] E.J. Lee : *Reconfiguration dynamique de la commande d'un système manufacturier : approche par la synthèse de la commande.* Thèse de doctorat, Ecole Centrale de Lille, 2006.

[Leg09] D. Legros : *Maitrise des risques dans les systèmes de transport : proposition d'une nouvelle approche de modélisation dynamique.* Thèse de doctorat, Ecole Nationale Superieure des Mines de Paris, 2009.

[Lia05] Z. Liang et W. Shi : PET : A personalized trust model with reputation and risk evaluation for P2P resource sharing. *In Proceedings of the 38th Annual International Conference on System Sciences HICSS'05, Hawaii, USA*. IEEE, 2005.

[Loh09] N. Lohmann, E. Verbeek et R. Dijkman : Petri net transformations for business processes : a survey. *Transactions on Petri Nets and Other Models of Concurrency*, 2:46–63, 2009.

[Maz09] M.H. Mazouni, J.F. Aubry *et al.* : De l'analyse préliminaire de risque au système d'aide à la décision pour le management des risques. *In 8e Congrès International pluridisciplinaire en Qualité et Sûreté de Fonctionnement, Qualita, Besançon, France*, 2009.

[Med06] K. Medjaher, A.K. Samantaray, B. Ould Bouamama et M. Staroswiecki : Supervision of an industrial steam generator. part II : Online implementation. *Control Engineering Practice*, 14(1):85–96, 2006.

[Mej10] L. Mejri, H. Hadj-Mabrouk et P. Caulier : Vers une ontologie pour le domaine de l'analyse de sécurité des systèmes de transport automatisés. *In Terminologie et Ontologie : Théories et applications TOTh'10, Annecy, France*, 2010.

[Mer04] M.M. Merad : Appui technique aux comités nationaux d'harmonisation des pratiques des études de dangers et des expertises. Rapport technique, Ministère de l'Ecologie et du Développement Durable, INERIS, 2004.

[Mon98] G. Moncelet : *Application des réseaux de Petri à l'évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile.* Thèse de doctorat, Université de Toulouse, 1998.

[Mon06] G. Montcouquiol : *Théorie des graphes.* IUT Orsay, 2006.

[Mur89] T. Murata : Petri nets : Properties, analysis and applications. *Proceedings of the IEEE*, 77(4):541–580, 1989.

[Mye07] J. Myers, M. Lee et J. Kiratli : Cardiovascular disease in spinal cord injury : an overview of prevalence, risk, evaluation, and management. *American journal of Physical Medicine and Rehabilitation*, 86(2):142–152, 2007.

[Nou97] M. Nourelfath : *Extension de la théorie de la supervision à la surveillance et à la commande des systèmes à événements discrets : application à la sécurité opérationnelle des systèmes de production.* Thèse de doctorat, INSA de Lyon, 1997.

[OMG10] Object Management Group OMG : *BPMN 2.0 by Exemple.* `www.bpmn.org`, 2010.

[OMG11a] Object Management Group OMG : *Business Process Model and Notation BPMN version 2.0.* `www.bpmn.org`, 2011.

[OMG11b] Object Management Group OMG : *Unified Modeling Language, Infrastructure, version 2.4.1.* `www.uml.org`, 2011.

[Oss05] S. Ossowski, J.Z. Hernandez, M.V. Belmonte, A. Fernandez, A. Garcia-Serrano, J.L. Pérez-de-la Cruz, J.M. Serrano et F. Triguero : Decision support for traffic management based on organisational and communicative multiagent abstractions. *Transportation Research part C : emerging technologies*, 13(4):272–298, 2005.

[Oul06] B. Ould Bouamama, K. Medjaher, A.K. Samantaray et M. Staroswiecki : Supervision of an industrial steam generator. Part I : Bond graph modelling. *Control Engineering Practice*, 14(1):71–83, 2006.

[Ouy08] C. Ou-Yang et Y.D. Lin : BPMN-based business process model feasibility analysis : a Petri net approach. *International Journal of Production Research*, 46(14):3763–3781, 2008.

[Pan08] C. Pangilinan, N. Wilson et A. Moore : Bus supervision deployment strategies and use of real-time automatic vehicle location for improved bus service reliability. *Journal of the Transportation Research Board*, 2063(1):28–33, 2008.

[Paq13a] D. Paquereau, L. Piétrac, E. Niel et L. Bouresche : Démarche de formalisation et de synthèse de procédures d'exploitation d'une ligne de métro. *In Journée des Doctorants MACS, Strasbourg, France*, 2013.

[Paq13b] D. Paquereau, L. Piétrac, E. Niel et L. Bouresche : Démarche de modélisation et d'évaluation de procédures d'exploitation d'une ligne de métro. *In Modélisation des Systèmes Réactifs - MSR, Rennes, France*, 2013.

[Paq14] D. Paquereau, L. Piétrac, E. Niel et L. Bouresche : Determining of critical and dreaded states achieved during metro line supervision. *In 22nd Mediterranean Conference of Control and Automation - MED, Palerme, Italie*, 2014.

[Pas02] L. Pasquier : *Modélisation de raisonnements tenus en contexte : application à la gestion d'incidents sur une ligne de métro.* Thèse de doctorat, Université Pierre et Marie Curie - Paris 8, 2002.

[Pei08] D. Peixoto, V. Batista, A . Atayde, E. Borges, R. Resende et C. Pádua : A comparison of BPMN and UML 2.0 activity diagrams. *In VII Simposio Brasileiro de Qualidade de Software, Florianópolis, Brazil*, 2008.

[Rae07] I. Raedts, M. Petkovic, Y.S. Usenko, J.M. Van Der Werf, J.F. Groote et L. Somers : Transformation of BPMN models for behaviour analysis. *In 5th International Workshop on Modelling, Simulation, Verification and Validation of Enterprise Information Systems (MSVVEIS), Funchal, Madeira, Portugal*, 2007.

[Ram87] P.J. Ramadge et W.M. Wonham : Supervisory control of a class of discrete event processes. *SIAM Journal on Control and Optimization*, 25(1):206–230, 1987.

[Ram89] P.J. Ramadge et W.M. Wonham : The control of discrete event systems. *Proceedings of the IEEE*, 77(1):81–98, 1989.

[Rec09] J. Recker, M. Muehlen, K. Siau, J. Erickson et M. Indulska : Measuring method complexity : UML versus BPMN. *In 15th Americas Conference on Information Systems AMCIS, Chicago, USA*, 2009.

[Rez96] N. Rezg : *Contribution à la Sécurité Opérationnelle des systèmes : Mise en oeuvre d'une structure de surveillance basée sur les réseaux de Petri Objets Contrôlés.* Thèse de doctorat, INSA Lyon, 1996.

[Rus06] N. Russell, W.M.P. Aalst, A. Ter Hofstede et P. Wohed : On the suitability of UML 2.0 activity diagrams for business process modelling. *In Proceedings of the 3rd Asia-Pacific conference on Conceptual modelling, Hobart, Australia*, 2006.

[Sad07] N. Sadou : *Aide à la conception des systèmes embarqués sûrs de fonctionnement.* Thèse de doctorat, Université Paul Sabatier-Toulouse III, 2007.

[Sar99] P. Sarri : *Stabilisation optimale des systèmes à événements discrets à structure vectorielle : application à la sécurité opérationnelle des systèmes de production.* Thèse de doctorat, INSA de Lyon, 1999.

[Sba10] Z. Sbaï : *Contribution à la modélisation et à la vérification de processus workflow.* Thèse de doctorat, Conservatoire national des arts et metiers-CNAM, 2010.

[Sba13] Z. Sbaï et K. Barkaoui : Vérification formelle des processus workflow collaboratifs. *Ingénérie des systèmes d'information*, 18(5), 2013.

[Seo04] K.T. Seow et M. Pasquier : Supervising passenger land-transport systems. *IEEE Transactions on Intelligent Transportation Systems*, 5(3):165–176, 2004.

[Ser14] A. Serebrenik : Activity diagrams and state machines. Rapport technique, University of Technology Eindhoven, 2014.

[Shr09] A. Shraideh : *Analyse et optimisation d'un processus à partir d'un modèle BPMN dans une démarche globale de conception et de développement d'un processus métier : application à la dématérialisation de flux courrier du projet GOCD (PICOM).* Thèse de doctorat, Ecole Centrale de Lille, 2009.

[Tha04a] Thales et RATP : Analyse fonctionnelle du PCC générique : PCC L13, L3 et L5. Documentation interne, 2004.

[Tha04b] Thales et RATP : Analyse préliminaire des dangers du PCC générique. Documentation interne, 2004.

[Tha04c] Thales et RATP : Analyse préliminaire des risques du PCC générique. Documentation interne, 2004.

[Tha09] Thales et RATP : Registre des situations dangeureuses du PCC générique. Documentation interne, 2009.

[Tha11a] Thales : Formation ATS - ECE, présentation. Document interne, 2011.

[Tha11b] Thales : Spécifications fonctionnelles ATSsoft. Document interne, 2011.

[Tha11c] THALES : User manual for ATSsoft demonstrator : a simple scenario. Document interne, 2011.

[Vij06] W.M. VIJVERBERG : *Translation of Process Modeling Languages*. Thèse de doctorat, Eindhoven University of Technology, 2006.

[Vil88] A. VILLEMEUR : *Sûreté de fonctionnement des systèmes industriels*. Eyrolles, 1988.

[Vin00] R. VINCENT, F. BONTHOUX et C. LAMOISE : Evaluation du risque chimique, hiérarchisation des risques potentiels. *Cahiers de Notes Documentaires - Hygiène et sécurité du travail (INRS)*, 178(1):29–34, 2000.

[Whi04] S.A. WHITE : Process modeling notations and workflow patterns. BPTrends, 2004.

[Won10] W.M. WONHAM : *Supervisory Control of Discrete Event Systems*. Systems Control Group, University of Toronto, Canada, Notes de cours, 2010.

[Yam96] K. YAMALIDOU, J. MOODY, M. LEMMON et P. ANTSAKLIS : Feedback control of Petri nets based on place invariants. *Automatica*, 32(1):15–28, 1996.

[Zan99] C. ZANARELLI, I. SAKER et L. PASQUIER : Un projet de coopération ergonomes/concepteurs autour de la conception d'un outil d'aide à la régulation du trafic du métro. *In Actes de la Conférence Ingénierie des Connaissances, Paris, France*, 1999.

[Zan03] C. ZANARELLI : Caractérisation des stratégies instrumentales de gestion d'environnements dynamiques : analyse de l'activité de régulation du métro. *In 38e Congrès de la Société d'Ergonomie de Langue Française (SELF), Paris, France*, 2003.

INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

FOLIO ADMINISTRATIF

THÈSE SOUTENUE DEVANT L'INSTITUT NATIONAL DES SCIENCES APPLIQUÉES DE LYON

NOM : PAQUEREAU

DATE de SOUTENANCE : 30 mars 2015

Prénoms : Delphine

TITRE : GESTION DE PROCEDURES ET PRISE EN COMPTE DU DANGER LORS DE L'OCCURRENCE D'INCIDENTS COMBINES : APPLICATION A LA SUPERVISION D'UNE LIGNE DE METRO.

NATURE : Doctorat

Numéro d'ordre : 2015 - ISAL - 0024

Ecole doctorale : Électronique, Électrotechnique, Automatique (EEA)

Spécialité : Automatique

RESUME :

Durant l'exploitation d'une ligne de métro, l'opérateur de supervision est responsable de l'exécution de procédures pour la gestion des incidents. Cependant, lors de l'occurrence combinée d'incidents, les procédures utilisées peuvent se retrouver en concurrence. Dans ce cas, des situations ne garantissant pas la sécurité des personnes existent et un accident peut se déclencher.

La démarche d'étude des procédures intègre tout d'abord leur représentation graphique avec la notation BPMN. Ces modèles de procédure, compréhensibles et accessibles, constituent ainsi une base de connaissances pour les industriels concernés. Ces modèles sont ensuite interprétés sous forme de réseaux de Petri pour ajouter une dynamique au système étudié. La notion de contrôlabilité et l'influence du contexte d'exécution sont alors introduites dans l'étude de procédures de gestion d'incident.

Afin d'assurer la sécurité des personnes, des états interdits sont définis et identifiés parmi l'ensemble des états accessibles par l'application de la théorie du contrôle par supervision. Ces états interdits se caractérisent de manière originale : suivant leur inclusion dans un ensemble d'états particuliers mais également suivant la contrôlabilité de leurs transitions sortantes. Cette caractérisation innovante s'accompagne des algorithmes permettant de déterminer et d'éviter les états interdits.

Afin d'orienter l'opérateur de supervision dans les actions à exécuter lors d'incidents combinés, des critères de différenciation des trajectoires admissibles évitant les états interdits sont également définis. Les résultats obtenus permettent de proposer une assistance à l'opérateur de supervision sous forme d'alertes et de conseils.

Cette étude se base sur le système de supervision ATS développé par Thales et sur les procédures de gestion d'incident de l'un de leurs clients, la RATP. Un prototype de fonctionnalité d'aide à l'opérateur pour la gestion des incidents reposant sur le savoir-faire client a ainsi pu être intégré au logiciel de Thales.

MOTS-CLÉS : Supervision, Système de transport, Théorie du contrôle par supervision, Réseaux de Petri, BPMN, Sûreté de fonctionnement, Procédure de gestion d'incident.

Laboratoire de recherche : AMPERE

Directeur de thèse: Éric NIEL

Président de jury : Jean-Marc FAURE

Composition du jury :

Christophe BERENGUER, Serge HADDAD
Jean-Marc FAURE, Armand TOGUYENI
Laurent BOURESCHE (responsable industriel)
Éric NIEL (Directeur), Laurent PIÉTRAC (co-directeur)